Brunel
UNIVERSITY
LONDON

School of Engineering and Design

QoS-AWARE CONTENT ORIENTED FLOW ROUTING IN OPTICAL COMPUTER NETWORK

Mohammed M. Saeed Abdullah AL-MOMIN

A thesis submitted in partial fulfilment of the requirements
of the degree of Doctor of Philosophy (PhD) to:
Electronic and Computer Engineering
School of Engineering and Design
Brunel University
United Kingdom

October, 2013

School of Engineering and Design

QoS-AWARE CONTENT ORIENTED FLOW ROUTING IN OPTICAL COMPUTER NETWORK

A thesis submitted in partial fulfilment of the requirements
of the degree of Doctor of Philosophy (PhD) to:
Electronic and Computer Engineering
School of Engineering and Design
Brunel University
United Kingdom

By:

Mohammed M. Saeed Abdullah AL-MOMIN

Supervised by:

Prof. John Cosmas

October, 2013

Dedicated to all whom had helped me

Abstract

In this thesis, one of the most important issues in the field of networks communication is tackled and addressed. This issue is represented by QoS, where the increasing demand on high-quality applications together with the fast increase in the rates of Internet users have led to massive traffic being transmitted on the Internet. This thesis proposes new ideas to manage the flow of this huge traffic in a manner that contributes in improving the communication QoS. This can be achieved by replacing the conventional application-insensitive routing schemes by others which take into account the type of applications when making the routing decision. As a first contribution, the effect on the potential development in the quality of experience on the loading of Basra optical network has been investigated. Furthermore, the traffic due to each application was dealt with in different ways according to their delay and loss sensitivities. Load rate distributions over the various links due to the different applications were deployed to investigate the places of possible congestions in the network and the dominant applications that cause such congestions.

In addition, OpenFlow and Optical Burst Switching (OBS) techniques were used to provide a wider range of network controllability and management. A centralised routing protocol that takes into account the available bandwidth, delay, and security as three important QoS parameters, when forwarding traffics of different types, was proposed and implemented using OMNeT++ networks simulator. As a novel idea, security has been incorporated in our QoS requirements by incorporating Oyster Optics Technology (OOT) to secure some of the optical links aiming to supply the network with some secure paths for those applications that have high privacy requirements. A particular type of traffic is to be routed according to the importance of these three QoS parameters for such a traffic type. The link utilisation, end to end delays and securities due to the different applications were recorded to prove the feasibility of our proposed system.

In order to decrease the amount of traffic overhead, the same QoS constraints were implemented on a distributed Ant colony based routing. The traditional Ant routing protocol was improved by adopting the idea of Red-Green-Blue (RGB) pheromones routing to incorporate these QoS constraints. Improvements of 11% load balancing, and 9% security for private data was achieved compared to the conventional Ant routing techniques. In addition, this Ant based routing was utilised to propose an improved solution for the routing and wavelength assignment problem in the WDM optical computer networks.

Declaration

This is to certify that:

(i) the thesis comprises only my original work towards the PhD except where indicated,

(ii) due acknowledgement has been made in the text to all other material used,

Mohammed M. Saeed Abdullah AL-MOMIN

Publications

During the course of this project, a number of publications have been introduced. These publications are based on the work presented in this thesis. They are listed here for reference.

- Mohammed Al-Momin, John Cosmas, Kassim Al-Hassani, and Safaa Jassim, “Policy Based Management of Optical Fibre Networks Carrying Multiple Application Traffic”, Second Communications Conference held by the Ministry of Communications in Baghdad, IRAQ in cooperation with IEEE-IRAQ SECTION. 14-16 March 2011. It has been accepted and awarded a trophy.

- Mohammed Al-Momin, John Cosmas, and Saman Amin “Adaptive Three-Layer Weighted Links Routing Protocol for Secure Transmission over Optical Networks”, *WSEAS transactions on communications*, Issue 8, Volume 11, pp. 287-298, August 2012. http://www.wseas.org/multimedia/journals/communications/2012/55-236.pdfM

- Mohammed Al-Momin, John Cosmas, “The Impact of Content Oriented Routing on OpenFlow Burst Switched Optical Network”, Proceedings of Advanced Information Networking and Applications Workshops (AINA-2013), IEEE Computer Society, Barcelona, Spain, March 25-28, 2013.

- Mohammed Al-Momin, John Cosmas, and Saman Amin, “RGB Pheromones QoS- Aware Secure Ant Routing in Optical Fibre Networks”, *Journal of Security and Communication Networks*, submitted and it is now under review, March 2013.

- Mohammed Al-Momin, John Cosmas, Zaharias D. Zaharis, Pavlos Lazaridis, and Saman Amin “QoS-Aware Ant Routing with Security Constraints in Optical Fibre Networks by Using RGB Pheromones”, *IEEE Transactions on Cybernetics*, Submitted, July 2013.

- Mohammed Al-Momin, John Cosmas, Saman Amin, “Enhanced ACO based RWA on WDM Optical Networks Using Requests Accumulation and Re-Sorting Method”, 5th Computer Science & Electronic Engineering Conference- IEEE sponsored, Sussex, UK, Accepted Paper, August 2013.

Acknowledgements

I would like to thank my parents, family and everyone who had helped me in my study or had supplied me with appreciated advices, especially my dear supervisor, Professor John Cosmas.

Contents

List of Figures ... xii

List of Tables ... xviii

Glossary ... xix

Chapter 1 ... 1

Introduction ... 1

1.1 Background ... 3
1.2 Motivation ... 4
1.3 Aim and Objectives ... 6
1.4 Contributions ... 7
1.5 Thesis Outline ... 8

Chapter 2 ... 12

Network Data Switching and Routing Techniques ... 12

2.1 Network Switching ... 13
2.1.1 Circuit Switching ... 13
2.1.2 Packet Switching ... 16
2.1.3 Optical Burst Switching (OBS): ... 17
2.1.4 OpenFlow Switching Technology ... 23
2.2 Network Routing ... 28
2.2.1 Centralised Routing ... 28
2.2.2 Distributed Routing ... 29
2.3 Ant Colony Based Routing ... 29
2.3.1 Biological Ants Foraging ... 30
2.3.2 Ants Routing Modelling ... 31
2.3.3 Ants Routing Algorithm ... 34
2.3.4 Ants Routing Flowchart ... 36

2.3.5 Ant Protocol Stagnation 36
2.4 Summary 38
Chapter 3 40
Wavelength Division Multiplexing in Optical Networks 40
3.1 Transmission in Optical Fibre 40
3.1.1 Single Mode Fibre 44
3.1.2 Multimode Fibre 44
3.2 Attenuation in Optical Fibres 45
3.3 Dispersion in Optical Fibres 47
3.3.1 Intermodal Dispersion 47
3.3.2 Material or Chromatic Dispersion 47
3.3.3 Waveguide Dispersion 48
3.4 Non Linearity in Optical Fibres 48
3.4.1 Non Linear Refractive Index 48
3.4.2 Stimulated Raman Scattering (SRS) 48
3.4.3 Stimulated Brillouin Scattering (SBS) 49
3.4.4 Four-Wave Mixing (FWM) 49
3.5 Couplers 49
3.6 Fibre Cross-Connect Elements 50
3.6.1 Generic Directive Switches 51
3.6.2 Gate Switches 53
3.7 Optical Demultiplexers 53
3.8 Optical multiplexers 54
3.9 Wavelength Routers 55
3.9.1 Non-reconfigurable Wavelength Routers 55
3.9.2 Reconfigurable Wavelength Routers 56
3.10 Wavelength Conversion 57
3.10.1 Optoelectronic Wavelength Conversion 58
3.10.2 Coherent Effects based Wavelength Conversion 59

3.10.3 Cross Modulation based Wavelength Conversion 60
3.11 Wavelength Conversion Switches 60
3.12 Summary 62
Chapter 4 63
Dimensioning the Flow over the Basra Optical Network under Different Quality of Experience Scenarios. 63
4.1 Introduction 64
4.2 Previous Work 64
4.3 Details of Modelling Approach 65
4.4 Network Modelling 66
4.5 Application Modelling 68
4.6 Applications' Quality Scenarios 70
4.6.1 Residential Broadband Scenario 71
4.6.2 Improved Media Resolution Scenario 72
4.6.3 Maximum Media Resolution Scenario 73
4.6.4 3D Web Browsing and Video Contents 74
4.7 Traffic Flow Modelling 75
4.8 The Hourly Usage of Applications 77
4.9 Results and Discussion 77
4.9.1 Results of Residential Broadband Scenario 78
4.9.2 Results of Improved Media Resolution Scenario 85
4.9.3 Results of Maximum Media Resolution Scenario 91
4.9.4 Results of 3D Web Browsing and Video Contents Scenario 97
4.10 Summary 103
Chapter 5 105
The Impact of Content Oriented Routing on OpenFlow Burst Switched Optical Networks 105
5.1 Application Based Routing 106
5.2 Network Modelling and Applications Categories 109

5.3 Results and Discussion 111
5.3.1 Load Balancing 111
5.3.2 Max Delays (OEO switching delay) 114
5.3.3 Losses Over The overloaded Links 115
5.3.4 Load Rates over Links Due To the Various Applications 115
5.4 Comparison with the Other Conventional Routing Protocols 117
5.5 Summary 118
Chapter 6 120
Adaptive Three-Layer Weighted Links Routing Protocol for Secure Transmission over Optical Networks 120
6.1 Introduction 120
6.2 Related Work 121
6.3 QoS Requirements 123
6.3.1 Bandwidth 123
6.3.2 Delay 125
6.3.3 Security 125
6.4 Three-Layer Weighted Link Routing Protocol (TLWLRP) 128
6.4.1 Applications and QoS Requirements 130
6.4.2 Securing Channels on Optical Networks 132
6.5 TLWLRP Enabled Weighted Djikstra Routing Algorithm 133
6.6 System Simulation 135
6.7 Results 136
6.7.1 Bandwidth Gain 136
6.7.2 Delay Gain 137
6.7.3 Security Gain 139
6.7.4 Load Balance 141
6.7.5 Comparison with Other Routing Protocols 143
6.8 Summary 147
Chapter 7 149

Distributed RGB Pheromones Ant Routing with Enhanced QoS on Optical WDM Networks 149

7.1 RGB Pheromones Ant Routing 149

7.1.1 Related Work 151

7.1.2 Traffic Types 152

7.1.3 Network Modelling 153

7.1.4 Traffic Flow Modelling 154

7.1.5 Results and Discussion 155

7.1.5.1 Tuning of the Load Rates Balance Parameter 156

7.1.5.2 Tuning of the Security Parameter 158

7.1.5.3 Tuning of the Delay Parameter 160

7.1.5.4 Mixing Traffics of Different QoS Preferences 162

7.1.6 Comparison with the Conventional Ant Routing Protocol 164

7.2 Enhanced Ant Colony Optimisation (ACO) based RWA on WDM Optical Networks Using Requests Accumulation and Re-Sorting Method. 166

7.2.1 RWA Types 167

7.2.2 Wavelength Conversion Scenarios 168

7.2.3 Routing and Wavelengths Assignment based on Ant Colony Optimisation (ACORWA) 169

7.2.4 Simulation 174

7.2.5 Re-Sorting Connection Requests 175

7.2.6 Accumulative Requests RWA 178

7.3 Summary 180

Chapter 8 182

Conclusion and Future Work 182

8.1 Conclusion 182

8.2 Future Work 183

References 185

List of Figures

Figure 1.1 Thesis Outline.. 10

Figure 2.1 A circuit switched network.. 15

Figure 2.2 Circuit Switching Event Timing Diagram.. 16

Figure 2.3 Packet Switching Event Timing Diagram 17

Figure 2.4 Just In Time timing event timing diagram 18

Figure 2.5 Explicit Setup and Explicit Release Event Timing Diagram 19

Figure 2.6 Explicit Setup and Estimated Release Event Timing Diagram....................... 19

Figure 2.7 Estimated Setup and Explicit Release Event Timing Diagram....................... 20

Figure 2.8 Estimated Setup and Estimated Release Event Timing Diagram.................... 21

Figure 2.9 Just Enough Time event timing diagram.. 22

Figure 2.10 Horizon signalling protocol event timing diagram....................................... 22

Figure 2.11 OpenFlow Network's Structure.. 24

Figure 2.12 OpenFlow Switch's Architecture 25

Figure 2.13 an OpenFlow Flow Table Entry 26

Figure 2.14 Ants Foraging Behavioure.. 30

Figure 2.15 Ants with Dead End Path 31

Figure 2.16 Ant Routing Flowchart 37

Figure 3.1 Optical Fibre Cross Section.. 41

Figure 3.3 Light Propagation in Step and Graded Index Fibres 42

Figure 3.5 Light Propagation through Single Mode and Multimode Fibres..................... 45

Figure 3.6 Loss-Wavelength Relationship in Optical Fibre 46

Figure 3.7 Splitter, Combiner, and Coupler.. 50

Figure 3.8 A 2×2 Cross Connect Elements Operation States 50

Figure 3.9 Generic Directive Switches 52

Figure 3.10 A 2×2 Gate Switch Using Optical Amplifiers... 53

Figure 3.11 Prism Optical Demultiplexer 54

Figure 3.12 Prism Optical Multiplexer 54

Figure 3.13 A 4×4 Optical Wavelength Router 55

Figure 3.14 A P×P Reconfigurable Wavelength Router with M Wavelengths 56

Figure 3.15 WDM with and without Wavelength Conversion 57

Figure 3.16 Optoelectronic Wavelength Converter 59

Figure 3.17 Wavelength Conversion Using SOA 60

Figure 3.18 A Wavelength Conversion Switch with a Standalone Wavelength Converter for Each Individual Inbound Wavelength 61

Figure 3.19 A Wavelength Conversion Switch with Shared Wavelength Converters 62

Figure 4.1 Basra’s Optical Network 67

Figure 4.2 Total Network's Load Rate due to the Different Application Types 79

Figure 4.3 Total Load Rate on the Different Network's Links at Busy Hour 79

Figure 4.4 Busy Hour Load Rates on the Link Ashar-Basra due to the Different Application Types 80

Figure 4.5 Per Hour Load Rate on Link Ashar-Basra 81

Figure 4.6 Busy Hour Load Rates on the Link Basra-Ashar due to the Different Application Types 82

Figure 4.7 Per Hour Load Rate on Link Basra-Ashar 82

Figure 4.8 Busy Hour Load Rates on the Link Basra-AlZubair due to the Different Application Types 83

Figure 4.9 Per Hour Load Rate on Link Basra-Al-Zubair 83

Figure 4.10 Busy Load Rates on the Link Server-Basra due to the Different Application Types 84

Figure 4.11 Per Hour Load Rate on Link Server-Basra........ 84

Figure 4.12 Total Network's Load Rate due to the Different Application Types........ 85

Figure 4.13 Total Busy Hour Load Rate on the Different Network's Links........ 86

Figure 4.14 Busy Hour Load Rates on the Link Server-Basra due to the Different Application Types........ 87

Figure 4.15 Per Hour Load Rate on Link Server-Basra........ 87

Figure 4.16 Busy Hour Load Rates on the Link Basra-Ashar due to the Different Application Types........ 88

Figure 4.17 Per Hour Load Rate on Link Basra-Ashar 88

Figure 4.18 Load Rates on the Link Ashar-Basra due to the Different Application Types 89

Figure 4.19 Per Hour Load Rate on Link Ashar-Basra 90

Figure 4.20 Load Rates on the Link Basra-Zubair due to the Different Application Types 91

Figure 4.21 Per Hour Load Rate on Link Basra-AlZubair 91

Figure 4.22 Total Network's Load Rate due to the Different Application Types........ 92

Figure 4.23 Total Load Rate on the Different Network's Links at Busy Hour........ 93

Figure 4.24 Busy hour Load Rates on the Link Server-Basra due to the Different Application Types........ 94

Figure 4.25 Per Hour Load Rate on Link Server-Basra........ 94

Figure 4.26 Busy Hour Load Rates on the Link Basra-Ashar due to the Different Application Types........ 95

Figure 4.27 Per Hour Load Rate on Link Basra-Ashar 96

Figure 4.28 Busy Hour Load Rates on the Link Basra-AlZubair due to the Different Application Types........ 96

Figure 4.29 Per Hour Load Rate on Link Basra-AlZubair 97

Figure 4.30 Total Network's Load Rate due to the Different Application Types............ 98

Figure 4.31 Total Load Rate on the Different Network's Links at Busy Hour................ 99

Figure 4.32 Busy Hour Load Rates on the Link Server-Basra due to the Different Application Types 100

Figure 4.33 Per Hour Load Rate on Link Server-Basra... 100

Figure 4.34 Busy Hour Load Rates on the Link Basra-Ashar due to the Different Application Types 101

Figure 4.35 Per Hour Load Rate on Link Basra-Ashar 101

Figure 4.36 Load Rates on the Link Basra-AlZubair due to the Different Application Types... 102

Figure 4.37 Per Hour Load Rate on Link Basra-AlZubair 103

Figure 5.1 NSFNET Topology. 110

Figure 5.2 Load Rates Distribution due to rerouting of delay insensitive traffic (P2P) . 112

Figure 5.3 Load Rates Distribution Due to Web Browsing... 113

Figure 5.4 Load Rates Distribution Due to VoIP 113

Figure 5.5 End to End Number of Hops of the Different Applications from Node0 to Node11 114

Figure 5.6 Percentage Losses of the Different Applications on the Link from Node12 to Node5 115

Figure 5.7 Load Rates on the Link from Node0 to Node1 116

Figure 5.8 Load Rates on the Link from Node7 to Node8 116

Figure 5.9 End to End Delays From Node0 to Node11 in Load Balance-aware Routing Protocol 117

Figure 5.10 Load Rate Distribution in Latency-aware Routing Protocol....................... 118

Figure 6.1 Using Oyster Transceivers for Securing Optical Channel [86]..................... 123

Figure 6.2 A Network with Best Effort Protocol.. 124

Figure 6.3 Optical Tapping Using Splitter and Coupler Method 127

Figure 6.4 Typical Packet’s Structure with TOS Entry 128

Figure 6.5 Internet Layered System with TLWLRP... 129

Figure 6.6 TLWLRP Enabled Weighted Djikstra Routing Flowchart 134

Figure 6.7 Optical Network with Secure and Unsecure Links 135

Figure 6.8 Link x3-x17 Utilisation Due To P2P File Sharing 137

Figure 6.9 Load Rates on the Various Network’s Links due to Interactive Gaming...... 138

Figure 6.10 Number of Hops Required For the Various Applications To Transmit From X1 to X8... 139

Figure 6.11 Load Rates over the Various Links due to VoIP 140

Figure 6.12 Security Percentages of Different Applications for the Traffics from X1 To X8... 141

Figure 6.14 Total Number of Hops Required for the Various Applications to Transmit from X1 to X8 in Latency-Aware Routing 143

Figure 6.15 Total Load Rates on the Various Links due to All Applications in Latency-Aware Routing 144

Figure 6.16 Security Percentages of Different Applications for the Traffics from X1 to X8 in Latency-Aware Routing... 145

Figure 6.17 Total Load Rate on the Various Network’s Links due to all Applications in Congestion-Aware Routing 146

Figure 6.18 Total Number of Hops Required for the Various Applications to Transmit from X1 to X8 in Congestion-Aware Routing.. 147

Figure 6.19 Security Percentages of Different Applications for the Traffics from X1 to X8 in Congestions-Aware Routing... 147

Figure 7.1 NSF Network.. 154

7.2 Throughput Balance due to different values of ‘a’ 158

Figure 7.3 Load Rates on the Different Network’s Links when a=1............................. 158

Figure 7.4 Average End to End Security due to different values of ‘c’ 159

Figure 7.5 Load Rates on the Different Network’s Links when c=1 160

Figure 7.6 Average End to End Delay due to different values of ‘b’ 161

Figure 7.7 Load Rates on the Different Network’s Links when b=1 162

Figure 7.8 Average End to End Percentage of Security for the Different Applications. 162

Figure 7.9 Average End to End Delays for the Different Applications 163

Figure 7.10 Total Load Rates for a Mix of Applications’ Preferences (Balance= 70%) 164

Figure 7.11: Total Load Distribution in the Conventional Congestion-Aware Latency-Aware Routing Protocol (Balance= 56%) 165

Figure 7.12 Average End to End Delays for the Different Applications in the Conventional Congestion-Aware Latency-Aware Routing Protocol Hops) 165

Figure 7.13 Average End to End Percentage of Security for the Different Applications in the Conventional Congestion-Aware Latency-Aware Routing Protocol 166

Figure 7.14 WDM with Two Wavelengths 168

Figure 7.15 Percentage of Blockings Versus the Number of Wavelengths using ACO. 174

Figure 7.16 Example Network 176

Figure 7.17 Blockings with and without Requests’ Re-Sorting in Wavelength Continuity Constraint Scenario 176

Figure 7.18 Blockings with and without Requests’ Re-Sorting in Full Wavelength Conversion Scenario 177

Figure 7.19 Blockings with and without Requests’ Re-Sorting in Partial Wavelength Conversion Scenario (4-Conversions) 177

Figure 7.20 Percentage of Blocking Vs the Applied Load in Conventional Dynamic RWA and Accumulative Dynamic RWA 179

List of Tables

Table 2.1: An Example of the Node's Routing Table 32

Table 4.1 Number of Users of the Different Sectors of Basra.. 68

Table 4.2 Residential Broadband Scenario 71

Table 4.3 Improved Media Resolution Scenario 72

Table 4.4 Maximum Media Resolution Scenario 73

Table 4.5 3D Web Browsing and Video Contents... 74

Table 4.6 Hourly Distribution of Applications' % Load during the Whole Day 78

Table 5.1 Loss Percentage Limits 108

Table 5.2 Applications Categories 111

Table 6.1 QoS Requirements Weightings for the Different Applications 132

Table 7.1 Traffic Type Categories 153

Table 7.2: Applications Types Specifications and User Behaviour 155

Glossary

ACO: Ant Colony Optimization

ACORWA: Ant Colony Optimisation based Routing and Wavelength Assignment

FWC: Full Wavelength Conversion

FWM: Four-Wave Mixing

JET: Just Enough Time

JIT: Just In Time

OBS: Optical Burst Switching

OEO: Optical-Electric-Optical

PWC: Partial Wavelength Conversion

QoS: Quality of Service

RAN: Regional Area Network

RGB: Red-Green-Blue

RWA: Routing and Wavelength Assignment

SBS: Stimulated Brillouin Scattering

SPF: Shortest Path First

SRS: Stimulated Raman Scattering

TLWLRP: Three-Layer Weighted Link Routing Protocol

WCC: Wavelength Continuation Constraint

WDM: Wavelength Division Multiplexing

Chapter 1

Introduction

As a consequence of the information technology revolution, the wide range of applications intended to take place on the Internet, and the wide range of electronic devices to share information on a common medium, the need for a fast communication medium has risen. Optical cables can be considered as the only candidate that may meet the requirements of future fast Internet backbone. A lot of research efforts have been dedicated to improve the speed of optical cable to the extent that it could satisfy the ambitions of professional users. These research efforts have resulted in 100 terabits per second optical fibre so far. Moreover, the invention of Wavelength Division Multiplexing (WDM) has made this dream of having a very fast communication medium more realistic. In WDM more than one information signal can be carried on the same cable simultaneously but in different frequency slots.

Although the speed of communication medium is a prime factor that affects the speed of information flow, the routing technique plays a vital role in controlling Quality of Service (QoS) of the end to end communications. Routing Algorithms could be classified into two main types centralised and distributed routing protocols [1-3]. In centralised routing, a centralised database which has information of the whole network status and controls the process of choosing the appropriate paths to the different destinations. For such a routing type to keep track of any changes in the network, this centralised database is to be updated periodically costing a time delay and a large memory consumption to store the whole network resources statuses; this makes this type of routing less efficient in the case of dynamic routing when the state of the network changes repetitively, whereas it is more suitable for small intra-domain static routings [4, 5]. The routing table in this routing technique is kept in one central entity which should be consulted every time a node needs to send data [6], where the routing decision is depending on the globally monitored information of the network state. On the other hand, distributed routing is more suitable for large and state changing networks [2]. Each node in this routing technique has its own routing table and exchanges the routing and links information with the other nodes. In other words, the routing database is distributed among all the network's nodes. One main advantage of distributed routing is its reliability in restoring any possible failures in the network's resources at any time. Another major advantage in distributed routing systems is its capability to track any network change that can happen dynamically in the run time, such as users' redistribution, using artificial intelligence concepts.

Routing may also be further classified from another aspect into static and dynamic, where in static routing, routing tables are to be set up in the initialisation stage of the communication network, and remains unchanged through all other stages [7, 8]. A vital drawback of such a routing technique is its inability to detect the network's topology changes. In dynamic routing, the routing tables are updated periodically. In this dissertation, flow measurement software for optical networks was designed to predict the amount of data flows and investigate the places of possible congestions across these optical networks. Furthermore different policies were suggested to manage and control these congestions.

Moreover, different routing techniques were proposed in this dissertation aiming to improve the end to end QoS. These proposed QoS routing protocols were designed to be content oriented in their nature, where they differentiate among the different application types and offer a different routing algorithm for each applications class. Figures and tables were derived from our results to verify the feasibility of our proposed routing techniques. Single and multiple wavelengths within optical cables were tested with these QoS aware routing protocols. Security was dealt with as one of the significant QoS requirements as well as the other requirements such as delay and bandwidth. Most papers which worked on security were completely isolated from the other QoS requirement awareness, where they only aim to provide a secure communication medium, whereas our scheme mixes among security and other QoS factors to come up with a mixture of specifications that precisely complies each of the different applications QoS requirements.

1.1 Background

Ultra high speed switches are currently used in the modern communication networks in order to offer fast response to the sudden network changes. These changes may happen due to the dynamically changing service demands or the other network abnormalities such as links or nodes failures. The innovation of very high bandwidth optical cables has expedited the research community to improve the switching speed to the extent that it can match high speed optical cables, otherwise this speed gain which was obtained from using optical cables will be wasted in the network switching operations. Electronic switches and routers on one hand are very smart in the matter of processing data and are very easy to control and manage, but they offer slow route setup response times.

Optical switches on the other hand, are very fast but they offer only a limited range of data processing, storage and management capabilities. The reason is that it is technically infeasible to manufacture optical memories that can store data at the very high bit rates used in optical cables so far. To facilitate the process of data processing on optical networks, electronic switches are being used with Optical-Electronic-Optical (O-E-O) converters to convert light signals on the optical cables to electronic form, process it, and then convert it back to light in order to be transmitted on the output optical link. This O-E-O conversion will also be accompanied by a time delay causing the network performance to be degraded. In order to expedite the operation, only the header information is processed electronically, whereas the payload is bypassed optically through the Semi-Optical switches. Optical delay lines are used with this technique to help in delaying the optical information till the switches are configured and the path for the payload is set up according to the information existing in the packet header.

OpenFlow switching technology was invented in order to reduce the number of O-E-O conversions required, where the OpenFlow switch reads the header of the arriving packet, makes a decision upon the information existing in that header to forward it to the proper output port. Packets of the same type are dealt with exactly as that first packet, and will be forwarded through the same allocated path without a need to make repeated decisions. In this work, these packets of the same type of applications are to be aggregated in a bigger flow units called flow bursts instead of single packets at the ingress port of the OpenFlow switch and forwarded through the proper egress port in units of flow bursts.

The aggregation of same kind of flows has been invested in this work to offer different treatments of the different traffic classes, where traffics were classified according to their QoS requirements. Oyster Optics technology [9] was further used in this dissertation to introduce a new QoS factor, namely: security. Different routing techniques were offered to the different traffic classes to improve the QoS. The newly proposed QoS-aware routing protocol was tested on both centralised routing and distributed routing represented by swarm routing technique. Furthermore this routing technique was also applied to both single and multiple wavelengths fibres through the use of Wavelength Division Multiplexing (WDM).

1.2 Motivation

In spite of the extensive studies on routing over optical fibres, the currently used routing protocols still suffer from serious drawbacks. Each of these drawbacks should be studied and addressed individually in order to reach technological solutions that can meet the future Internet requirements. Some of these disadvantages are related to the optical cable itself such as how to distribute the cable's wavelengths among the different traffic types in an optimal manner so that the connection request blocking operations are minimised and high degree of QoS is achieved [10]. Such a blocking occurs when there is no any available un-busy path connecting the request's source and destination. A lot of researchers have also studied how to minimise the number of blocking operations, but not how to combine this with QoS routing.

Other disadvantages are general for all network types, no matter what is the kind of medium that connects the different nodes, such as the lack of routing table scalability. For instance, the number of Internet users is dramatically increasing, where one can imagine this increase since we know that the world Internet population has been doubled only in the last five years [11]. How huge will routing tables need to be to address all these internet resources? Another problem arises from the amount of data such a huge population downloads and uploads over the network. How to manage this huge amount of traffic in a way that guarantees an acceptable QoS for all application types. The equality in dealing with different traffic types is also a major problem when using the Best Effort routing protocol as used commonly nowadays in Internet.

QoS routing protocols used nowadays on optical cables lacks an important QoS factor which is the information security because security has been dealt with separately. Researchers on optical networks have either focused on securing the whole optical network at the time when most of the traffic transmitted over the network does not belong to private information, and does not need that level of security which costs too much. On the other hand, some other researchers have dedicated their efforts to improve the QoS, but they have forgotten that security as one of the crucial QoS factors. No researchers have dedicated effort to examine the feasibility of partially securing the network's links, maybe only within the main backbone of the network or more likely only a few wavelengths from all the optical links connecting the network's nodes, to offer an acceptable range of security for some private communications needed to take place over the network.

These issues were addressed in this thesis by proposing a flow model that uses OpenFlow routers to send data in units of flows instead small packets in Internet system architecture to reduce the number of routing decision making processes. In this scheme, flows will be globally addressed to main Regional Area Network (RAN) routers instead of individual PCs. The optical network backbone will serve like highways for the flow units, and each OpenFlow router within that backbone will serve as a border router and a service gateway to the individual users within its RAN. Moreover, a new routing technique that differentiates among the different traffic types and chooses a proper routing algorithm for each of these types has been proposed in this dissertation. This can be achieved by a minor change in the architecture of the currently used routers by cooperation between application layer and network layer in the TCP/IP layered model. Consequently, the router would be smart enough to recognise the different traffic types and assign a suitable routing algorithm for each type aiming to improve the QoS for each traffic type rather than remaining with the compromised QoS requirements for all the types of traffics, which will on average improve the overall QoS slightly. Oyster Optics Technology was used here together with swarm based routing to solve the problem of Routing and Wavelength Assignment (RWA) in multiple wavelength optical cables in a manner that it tries to achieve less data blocking operations and an acceptable QoS.

1.3 Aim and Objectives

The objectives of this thesis can be highlighted in four main points which are:

- Dimensioning the load flow throughout networks by calculating the load rates on different links at both busy hour and in per hour basis.
- Investigating the places of potential congestions on the network.
- Predicting the network loading pattern for different offered quality of experience scenarios.
- Proposing an efficient routing algorithm that differentiates among the different traffics types by offering a better selectivity for each particular type.
- Suggesting a new technique for routing information over WDM network that guarantees less number of connections requests blocking and therefore offers a substantial improvement in the overall communication’s QoS.

Satisfying all these objectives will lead to the main aim of this thesis which is improving the QoS.

1.4 Contributions

The contributions of this dissertation can be divided into five main parts. Firstly, a flow modelling tool has been developed to dimension the expected amount of traffics over the different network's links and investigate the locations of possible congestions under different services qualities assumptions. In other words, it is a tool to dimension the network before the design. One of the major merits of this model is its scalability in the manner that it can be applied to a very large fixed infrastructure, namely national or metropolitan networks such as the UK, Iraqi, or European optical networks.

The second contribution that this dissertation introduces is categorizing the different application types according to their delay and loss sensitivities and identifying different routing algorithms for each application class in order not to exceed pre-set acceptable amounts of delay and loss. In addition, applications were assigned different priorities to control the amount of shedding in the case of overloaded links. This routing technique was named content oriented routing, and it contributed to improve the performance of links utilisations and balancing the load over the different network's links.

The third contribution is proposing a new adaptive three-layer weighted links routing protocol for secure transmission over optical networks. This routing protocol makes use of Oyster Optics Technology to partially secure the optical network aiming to provide secure end to end routes for the private information transmitted over the network. Each application type has been assigned different values of delay, available bandwidth, and security requirements of that application to reflect the sensitivity of that application to each of these QoS factors. Unlike the majority of other efforts in the field of QoS routing, security has been taken into account to qualify the offered network services.

Another contribution is in combining the ideas of Oyster Optics Technology with the newly proposed modified version of the traditional ant colony based routing to come up with a novel intelligent distributed routing technique. The traditional ant based routing algorithm optimises the routes of the different traffic demands according to an optimization function that takes into account the length and available capacity, then it scales the effects of these two factors on the final decision of the best route. Important modifications to that routing algorithm have been achieved here. The traditional ant routing algorithm selects a route for all the connection demands according to its unique optimisation function without the differentiation among the different types of traffics which need to be routed. In the newly proposed version, ants used to learn the network to choose the optimal path to destination have been divided into three types, red, green, and blue, where each type has its own optimisation function and is used to select the routes of a particular traffic type, where traffic has also been categorized according to their QoS requirements into red, green and blue traffics.

Finally, the ant colony based routing has been utilised to introduce an improvement to the solution of the problem of Routing and Wavelength Assignment (RWA) in Wavelength Division Multiplexing (WDM) fibre networks. This proposed solution provides fewer connection requests blockings. Moreover, all three possible configurations of multiple wavelengths optical networks have been considered to test this improved RWA solutions. These configurations are WDM network with wavelength conversion, WDM network with partial conversions wavelength, and WDM network with wavelength continuation.

1.5 Thesis Outline

This dissertation focuses on improving the quality of service in optical networks. It is organised in a way that it first gives detailed technical background information on the fields on which this thesis made contributions. Thereafter, it moves to the contributions themselves, discusses the results, and gives conclusions. Figure 1.1 shows the overall thesis organization.

Chapter 1 gives an introduction about optical networks and the importance of QoS routing on such networks, brief information about the motivation behind this work, contributions, and thesis organization.

Chapter 2 deals with the methods used nowadays in switching and routing data over optical networks, where it presents a scientific background on the types of data switching and the benefits and drawbacks of each kind. It also discusses the different types of routing protocols focusing on ant based routing protocol as a kind of artificial intelligence oriented distributed routing. This chapter has been enriched with figures, tables and equations in order to well clarify the idea.

Chapter 3 is concerned with optical networks with multiple wavelengths. This chapter explains the problem of assigning different wavelengths to data traffics taking into account the wavelength continuity constraints, where three possible cases were studied; these cases are when all the network's nodes have wavelength conversions capability, some networks has such a capability, or no node can convert the wavelength of the received traffics.

Chapter 4 introduces the first contribution by dimensioning the traffics over the different network's links with different applications' qualities assumptions. The contribution of each particular application type to the total network load is calculated at both busy hour and on per-hour basis during a whole 24 hours day.

Chapter 5 presents another contribution by proposing categorising traffic into different classes according to their loss and delay sensitivities then forwards this traffic to their destinations using different routing algorithms to ensure an acceptable QoS for all traffic types.

Chapter 6 introduces a novelty in the field of QoS secure routing in optical networks, where it mixes the ideas of Oyster Optics Security Technology with the idea of content oriented routing, which is proposed in this chapter to support the security of private applications over the network.

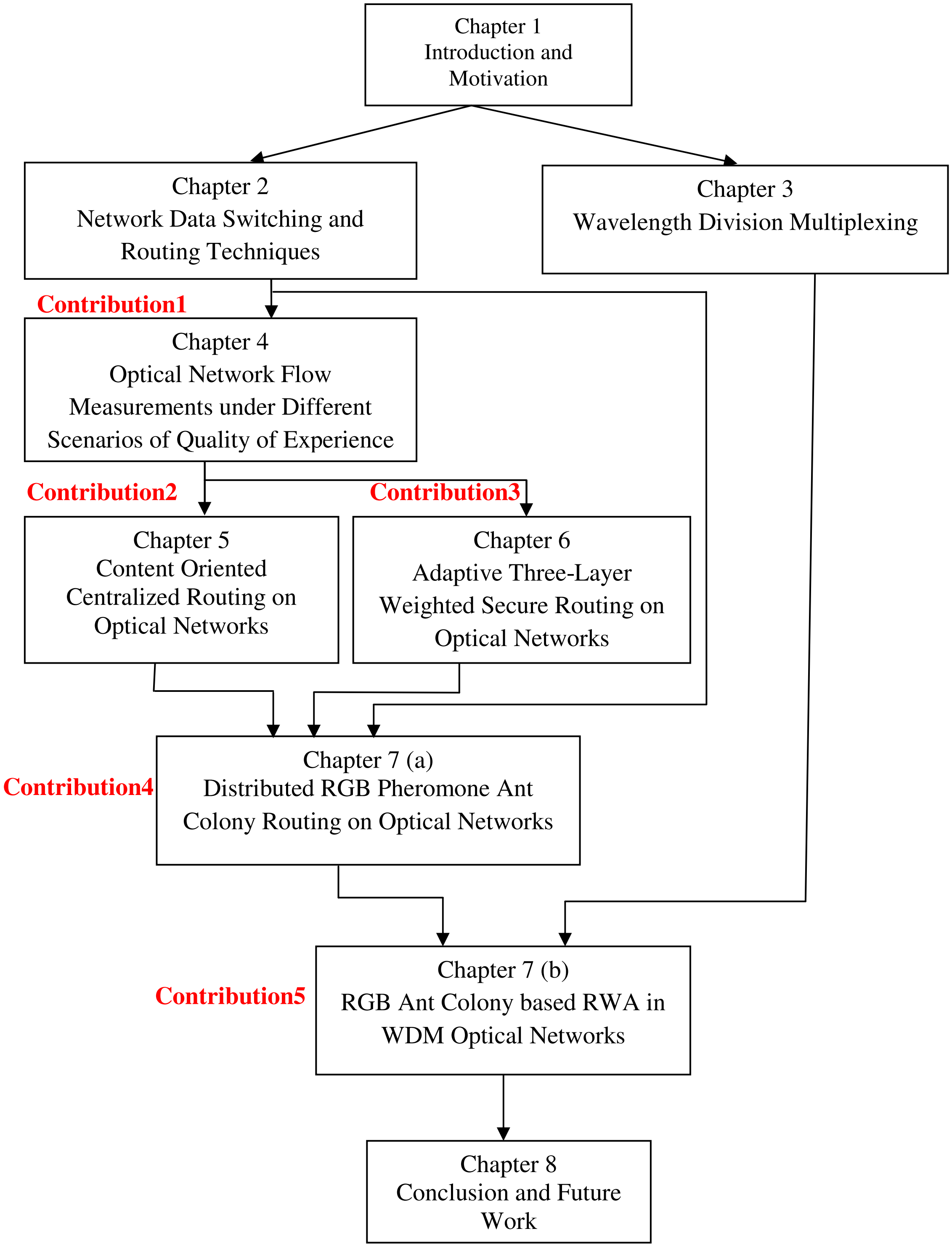

Chapter 1
Introduction and Motivation
Chapter 2
Network Data Switching and Routing Techniques
Chapter 3
Wavelength Division Multiplexing
Contribution1
Chapter 4
Optical Network Flow Measurements under Different Scenarios of Quality of Experience
Contribution2
Contribution3
Chapter 5
Content Oriented Centralized Routing on Optical Networks
Chapter 6
Adaptive Three-Layer Weighted Secure Routing on Optical Networks
Contribution4
Chapter 7 (a)
Distributed RGB Pheromone Ant Colony Routing on Optical Networks
Contribution5
Chapter 7 (b)
RGB Ant Colony based RWA in WDM Optical Networks
Chapter 8
Conclusion and Future Work

Figure 1.1 Thesis Outline

Chapter 7 moves to the distributed routing to add another novelty in improving the performance of ant based routing by proposing RGB ant based routing algorithm to fortify the idea of content oriented routing in such a distributed and fast recoverable routing method, where this routing approach is characterised by its fast response to any network change. In addition, this chapter introduces a new improved solution to the problem assigning wavelengths to different network flows in order to achieve two main benefits over the traditional solutions. Firstly, reducing the number of data blocking operations, which negatively affect the performance of the network, and secondly, reducing the number of wavelengths required to achieve the same level of performance.

Chapter 8 summarises all the contributions and outcomes gained from this thesis. Furthermore, it highlights some ideas for the future work.

Chapter 2

Network Data Switching and Routing Techniques

The major three methods used nowadays for switching data over Internet are circuit switching, packet switching, and burst switching [12-15]. Circuit switching has proved to be so elementary and simple that it does not enable network managers to flexibly control the network [8], however it is faster and cheaper than the other technologies since there is no buffering memories, not as much decision making and no data manipulation. Packet switching on the other hand requires a large amount of buffering memory [8]. Providing an optical memory is the major challenge in the field of optical networking. Optical memories are so expensive to implement that it is impractical to manufacture it in a large capacity as required by most packet routers and switches [16]. Even if we can afford to pay for the expensive optical memory, it is impossible for this memory to track the high bandwidth of optical transmission [16-19]. A potential solution is to use Optical-Electronic converters followed by an electronic buffer then data can be converted back to light using Electronic-Optical converter, but this adds additional delays to the latency of the transmitted data due to the required conversions.

Burst Switching (BS) can be considered to be the hybrid between packet and circuit switching, where instead of providing huge memory for queuing packets at every intermediate node and making the decision upon each packet's header, packets of the same destinations are aggregated together electronically in a larger units called bursts at the ingress node only [20-22].

Another new data switching technology, which seems to have a promising future for application in the next generation's networks, will be discussed in this chapter, OpenFlow technology. This technology offers a good stimulus to deal with data as flow units rather than packets or even bursts intending to provide a wider scope of network management [23, 24].

Network routing plays an important role in the field of data communication. Improving the routing algorithm for a network significantly affects the performance of that network by providing a better QoS for the whole communication process through the network. The both main types of routing techniques, namely, centralised and distributed will be discussed here with an emphasis on ant colony based routing which will be used in chapter 7 in this thesis to suggest a new distributed QoS aware routing protocol that is suitable for large networks with minimum amount of traffic overhead.

2.1 Network Switching

This section introduces the different network switching methods used to switch information among the various network's switching equipment. Circuit switching, packet switching, optical burst switching, and OpenFow switching technologies will be discussed in this section.

2.1.1 Circuit Switching

In circuit switching, data belonging to a particular user are directed to their destination by allocating a certain path from the source of information to that destination; this path is termed circuit. As a consequence to each user connection demand, a circuit establishment process is initiated by sending a stream of control information by means of a signalling mechanism. The control signals which are considered as overhead are used to order network switches to setup a connection between particular input and output ports in order to provide a path for the forthcoming data. Depending on the protocol being used, this path may survive for a period of time allowing the data to pass or may disconnect as soon as the data has completed transmission. In circuit switching, the source node sends a SETUP control message to the destination which in turn, sends CONFIRM to the source party permitting it to send the data, or in case there is no available free path to the destination, the intermediate node will return a BLOCKED message to the source informing it that the path is currently in use, and the source party should wait until a path to the destination becomes free. When the source node receives a CONFIRM message from the destination node, it starts transmitting the data. When the data is completed, the source node sends a RELEASE message to the destination through the path's links to release these links. Figure 2.1 illustrates the work of circuit switching.

Figure 2.1 shows a simple circuit switched network that consists of three basic elements, terminal nodes, transmission media, and switching nodes. The Switching node represents the fundamental element in circuit switching, where it consists of signalling element and control elements. This switching can either be made by electronic or optical components depending on the physical media used for the communication. Each switch consists of two parts, signalling part and control part. The signalling part monitors the statuses of the of the incoming lines and sends an appropriate control signal to the control part, which in turn establishes a connection according to this control information sent by the signalling part. The events timing diagram for circuit switching is shown in Figure 2.2. When the two terminals A and B want to communicate, the source node, for example Terminal (1), sends a setup message to switch SW A. This setup message reaches SW A after a propagation time delay Dp. Supposing that it is not busy, SW A processes the setup message and establishes a connection with Terminal (1) in order to provide a connection for the data flow to take place on it. This process causes an extra amount of delay called processing delay, Dn, at each intermediate switching node. SW A then forwards the setup message to SW B, which in turn receives it after Dp, processes it and establishes a new connection of the data path after a processing delay of Dn. SW B then forwards the setup message to the destination, Terminal (2). As soon as the destination node receives the setup message it processes it, establishes a connection with SW B for the data flow, and then it returns a confirm message to the source terminal via switches, SW B and SW A respectively. The confirm message on its way to the source node experiences only one type of delay which is Dp since the route between the source and destination nodes is already connected and no processing delays are needed in the intermediate nodes. Figure 2.2 shows the case when for any abnormality cause, such as switch busyness, SW A rejects the setup message [25]. In this case there is no need to forward the setup message to downstream nodes. According to this delay analysis, the total delay prior to sending data, which is called circuit setup delay, equals h(2Dp + D n) + D n, where h is the number of hops between the source and the destination.

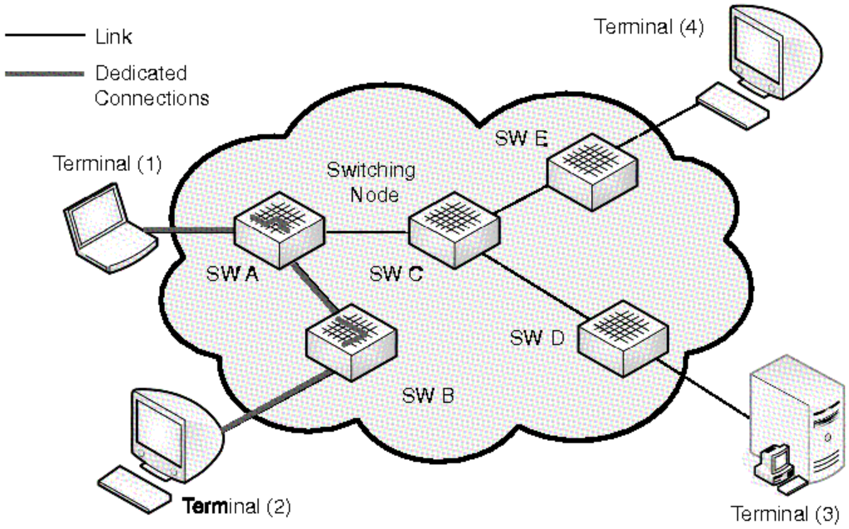


Figure 2.1 A circuit switched network [26]

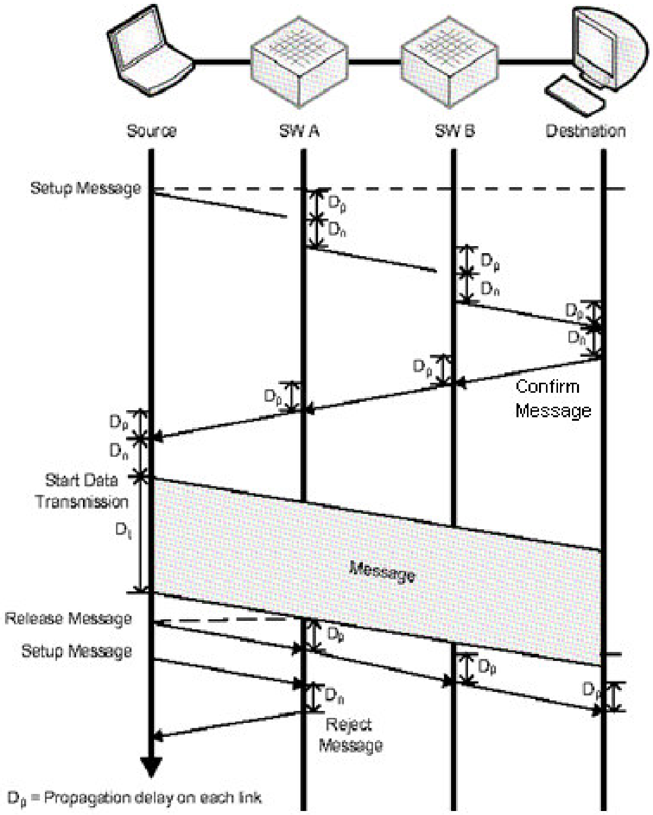


Figure 2.2 Circuit Switching Event Timing Diagram [26]

If the Data transmission delay Dt is less than or equal to circuit setup time, then circuit switching becomes inefficient resulting in low utilisation of network resources. On the other hand, high efficiency and network resources utilisation is offered by circuit switching when Dt is much larger than the setup delay.

2.1.2 Packet Switching

In Packet switching, the data to be sent is divided into small units called packets. The control information is sent together with the data packet as a header [27]. No pre-allocated route is required for the packet to pass, but instead the next-hop decision happens instantaneously as the packet reaches the switch or router according to the information present in the header of this packet. The header of the packet is to be processed at each intermediate node to forward the packet to the correct port by using a routing table. Unlike circuit switching, the other arriving packets are buffered during the period of processing the header of the current packet. No feedback occurs at this level to ensure the packet has been successfully received, where the packet is dropped if the output port is unavailable. Figure 2.3 shows the event timing diagram in packet switching.

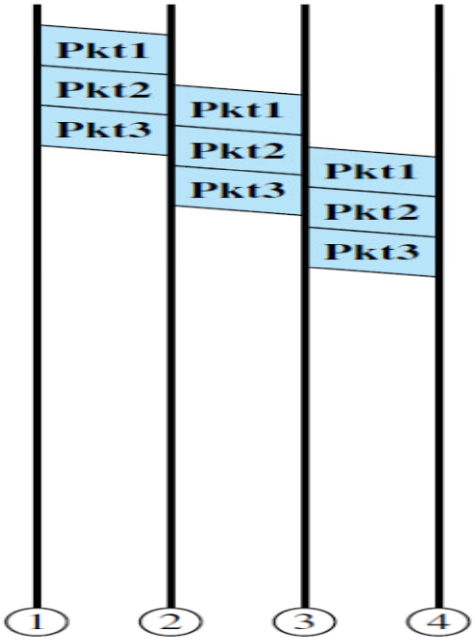


Figure 2.3 Packet Switching Event Timing Diagram [28]

2.1.3 Optical Burst Switching (OBS):

OBS combines the benefits of circuit switching and packet switching [29]. Data packets are aggregated at the ingress of the source node forming larger data units called a burst. The burst is preceded by a control packet as a header. The control packet is sent via a reserved optical channel at the beginning to setup a circuit to the destination. The burst body is then sent through this circuit. These bursts are to be sent to the egress of the intermediate nodes in order to reach its destination. OBS is used to facilitate sending data over all-optical networks, where it is infeasible to use packet switching due to the impracticality of processing each packet electronically since it is extremely difficult to manufacture optical buffers that are able to store or process packets in all-optical networks [30]. The following three signalling protocols are used to set up paths to the different destinations.

2.1.3.1 Just In Time (JIT) Signalling Protocol:

In JIT protocol, the source node sends a setup message to the switches along the path to the destination node to setup a connection. This setup message is followed by an offset to give time for setup message processing and switch configuration to reserve a bandwidth for the soon-coming burst. Bursts are transmitted in order of the setup messages arrival times, where the burst which is belonging to the first coming setup message is served first as shown in Figure 2.4 [31].

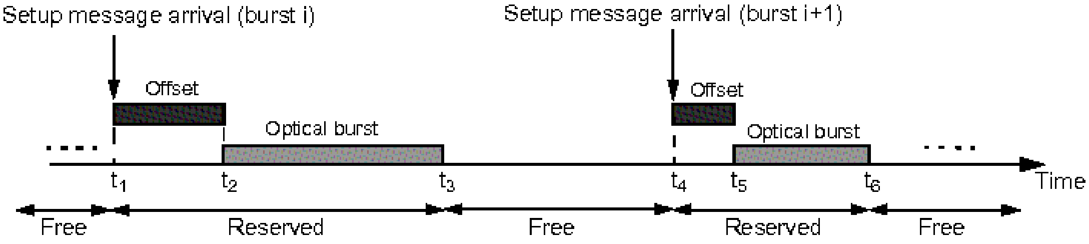


Figure 2.4 Just In Time timing event timing diagram [31]

Four signalling schemes are used here to allocate bandwidth to the burst as follows:

2.1.3.1.1 Explicit Setup and Explicit Release

In this scheme, the source node sends a setup message to the switches leading to the destination node in order to allocate a path for the forthcoming burst. After this path has been allocated, the transmission of the burst starts. When this burst ends, a release message is sent through all the hops to the destination in order to set this path free for the next burst. Figure 2.5 shows the event timing diagram for this signalling scheme.

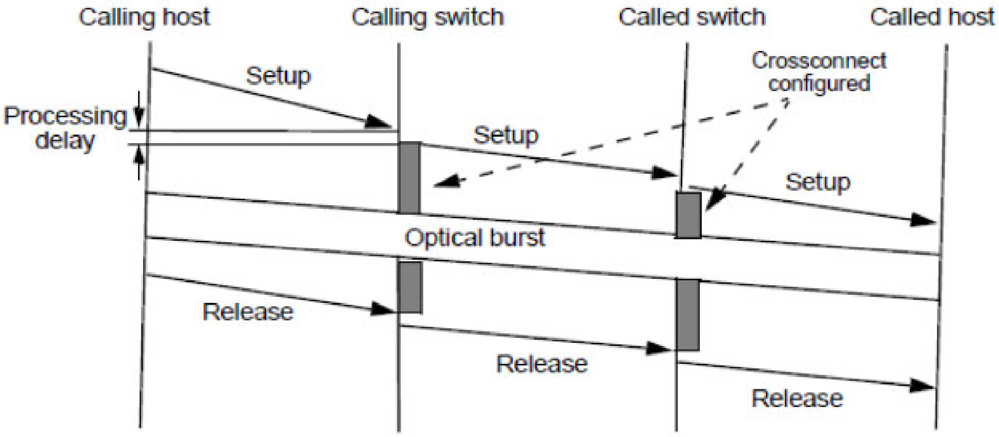


Figure 2.5 Explicit Setup and Explicit Release Event Timing Diagram [31]

2.1.3.1.2 Explicit Setup and Estimated Release:

The setup message here has information of the forthcoming burst size. This enables the network to release the path after sending the corresponding burst as shown in Figure 2.6. Therefore, there is no need to send a release message from the source as it is the case in the previous scheme.

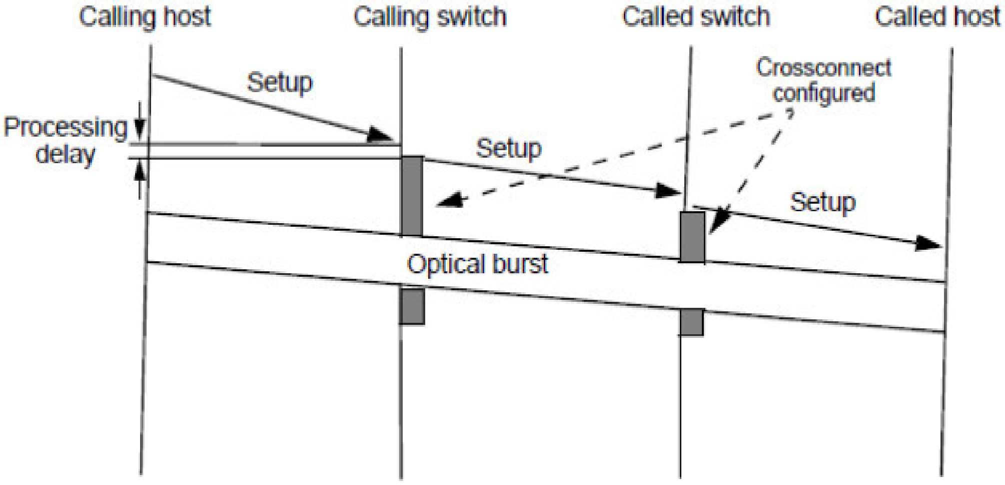


Figure 2.6 Explicit Setup and Estimated Release Event Timing Diagram [31]

2.1.3.1.3 Estimated Setup and Explicit Release:

Here, the setup message holds information about the estimated time of the burst's arrival; therefore, the path will not be initiated as soon as the setup message arrives and processed, but instead it will be allocated at a predetermined time as shown in Fig. 2.7. After the path has been initiated, the optical burst is sent, and a release message is sent to the path switches when this burst ends.

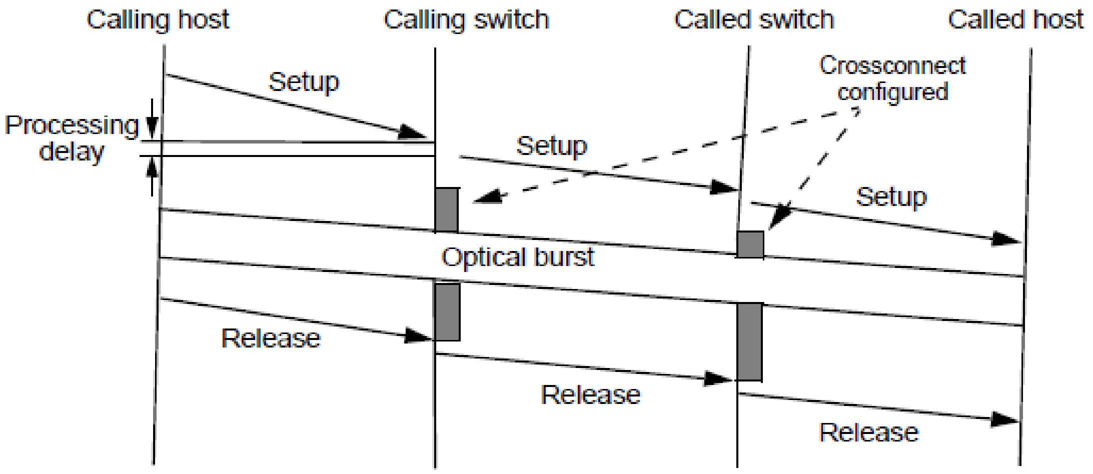


Figure 2.7 Estimated Setup and Explicit Release Event Timing Diagram [31]

2.1.3.1.4 Estimated setup and Estimated Release

In this scheme, the header contains information about the estimated burst arrival time and burst length. Here, whenever a setup message reaches a switch, this switch will wait until the burst arrival time is due, then the switch configures itself to connect the burst to the appropriate output port. No release message is required here since the estimated time of burst end is obtained from the setup message.

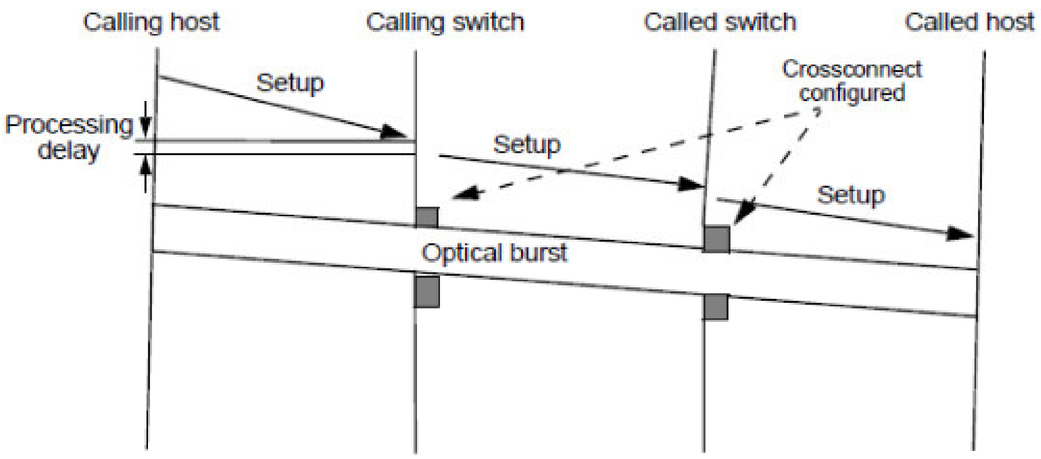


Figure 2.8 Estimated Setup and Estimated Release Event Timing Diagram [31]

2.1.3.2 Just Enough Time (JET) Signalling Protocol

Unlike JIT protocol, in this scheme the incoming bursts are not necessarily allocated paths in order of their setup messages arrival times. In this signalling protocol, the source node sends a setup message to the ingress switch; the switch in turn runs a void filling algorithm waiting for any other setup message coming during the offset interval of the first setup message. If a new setup message arrives during this interval, the switch checks the burst's arrival time and length. If this burst fits in the time slice between its arrival time and a few moments before the first bit of the first burst start transmission, just giving time for the switch to reconfigure itself, then this burst is accepted and a path is allocated for it, otherwise it is refused and dropped. This protocol is the best known signalling protocol because it improves the network resources utilisation [32].

In Figure 2.9 , if a setup message of burst A arrives to the ingress switch at time t_1 and the setup message of burst B arrives at t_2, the switch compares the arrival times of the two bursts stored in their setup messages. Supposing that burst B arrives and ends before the estimated arriving of burst A, the path for passing Burst B is to be setup before the path for burst A, even though the setup message of Burst B came later.

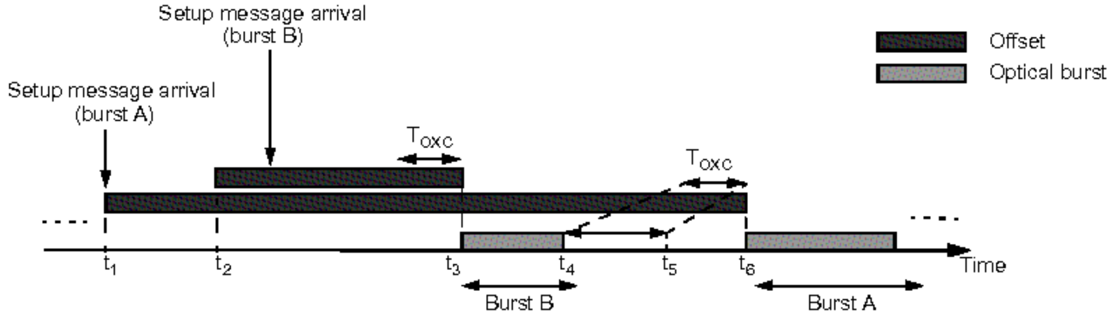


Figure 2.9 Just Enough Time event timing diagram [31]

2.1.3.3 Horizon Signalling Protocol

Here, each outgoing path (or wavelength) will be assigned a horizon time. The next burst will not be scheduled until the horizon time has been exceeded. As soon as the setup message is received, the horizon will be updated. Figure 2.10 supposes that the setup message of burst i was received at t_1, the end time for burst i was estimated from the setup message to be t_4. Giving an extra time unit for the switch to be reconfigured, the horizon will be t_5. Then burst2 will not be scheduled for transmission unless its arrival time is later than t_5. Since burst2 starts transmission at t_6, then it will be accepted. After scheduling of the burst2 the horizon of this channel is updated to t_8 to allow the transmission of burst2 to be completed and the switch is prepared for the next transmission, supposing that switch configuration process consumes one time unit [33, 34].

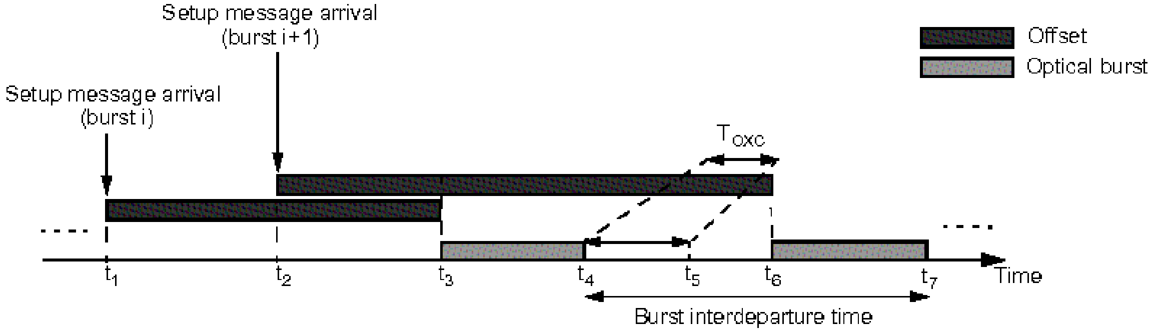


Figure 2.10 Horizon signalling protocol event timing diagram [31]

2.1.4 OpenFlow Switching Technology

Open Flow is a set of elements used to help network administrators to control the behaviour of the network. These elements may be hardware such as controller, or software such as protocols. Open Flow recognizes a set of packets (called flow) of a specific characteristics, i.e. they satisfy particular conditions such as the destination, the bandwidth, or the type of application, and define a path for each type of applications in order to gain an improved network performance such as balancing load over the network, reducing the latency of specific end to end communications, reducing the number of hops or reducing the energy needed for traffic to reach its destination [23, 35].

In the traditional switches and routers, the data forwarding and control actions are performed by the same switch or router. In Open Flow, these functions have been separated into two planes, namely: data path and control path. Data path presents a flow table with some entries, where each entry defines a certain flow. When a packet of new type arrives to the open flow switch, the controller creates an entry for this type of traffic in the flow table in order for the future traffic of this type to follow along a path it has just established. On the other hand, if the packet is known by the switch, i.e. since it already has a flow table entry, the switch will deal with it and pass it as the previous packets of this type on an already established path, without a need to communicate with the controller [23, 24].

An OpenFlow network is that network which consists of one or more OpenFlow switches with one or more controller. This controller make decisions to create an entry in the flow table or to delete an entry when shedding and throttling are required. The controllers are connected to the switches by a secure channel. A signalling protocol is required as well in the OpenFlow network. Figure 2.11 shows the structure of OpenFlow network [36].

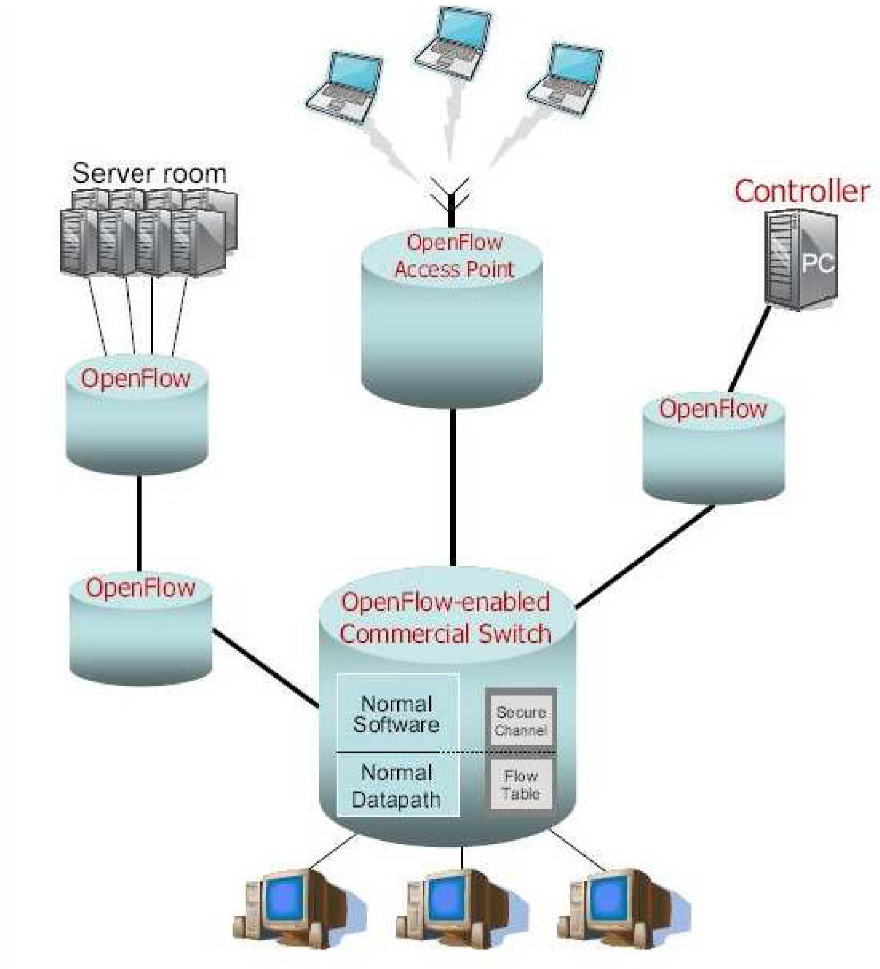


Figure 2.11 OpenFlow Network's Structure [23]

2.1.4.1 OpenFlow Switch

OpenFlow switch may either be implemented using Ternary Content Addressable Memory TCAM (a unique memory that is capable of doing memory lookups in only one clock cycle in a parallel manner [23, 24]), and the operating system of the switch, where in this case it is called hardware OpenFlow switch or it may be implemented entirely using Linux or Unix, where it is called software based OpenFlow switch.

In general, the OpenFlow switch consists of three major parts, namely: 1- Flow Table: which is a set of entries, each entry specifies accurately how to deal with its corresponding flow. 2- Secure channel: The switch is connected to the remote controller in a secure way via this channel. This channel allows those packets that the switch has not been trained for yet, as well as the commands from the controller to the data path of the switch to create a new flow table entry or to remove an existing entry from the flow table. 3- OpenFlow Protocol: It provides a means of communication between the switch and the remote controller. The Architecture of the OpenFlow switch is shown in Figure 2.12 below.

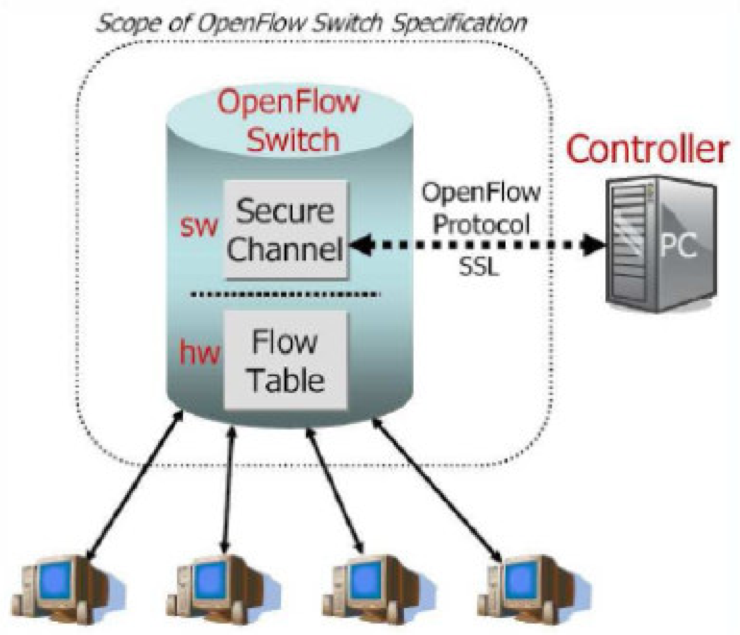
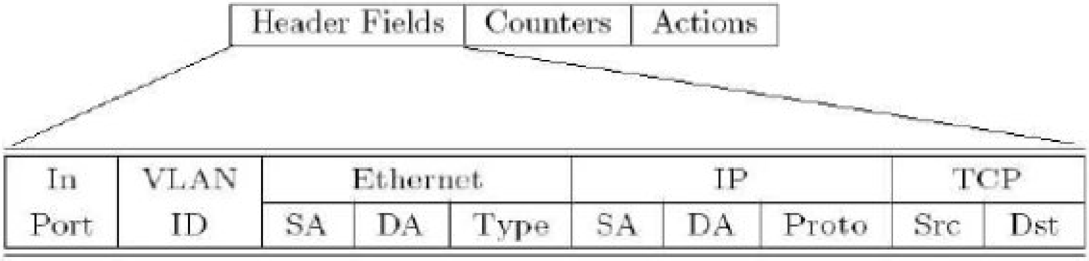


Figure 2.12 OpenFlow Switch’s Architecture [23]

2.1.4.2 Flow Table

The flow table entry consists of three main fields: namely, the header to identify the flow, the counters to provide some statistical information such as the count of the packet within the flow and time since the last packet in this flow, and the actions to guide the switch how to deal with this packet and where to pass it (to which port) [36]. There are two tables used to define flows: 1- Linear table which uses wild cards to match the flows and define some general criteria of the flow such as the MAC address, IP address and TCP port. This information does not give an accurate description to the defined flows. 2- The exact match table whose entries precisely depict the flow. It uses criteria such as input port, MAC source/destination address, Ethernet protocol type, IP MAC source/destination address, network protocol, source/destination port,...). The entry of the flow table is shown in Figure 2.13.



Header Fields	Counters	Actions

In Port	VLAN ID	Ethernet			IP			TCP	
		SA	DA	Type	SA	DA	Proto	Src	Dst

Figure 2.13 an OpenFlow Flow Table Entry [23]

2.1.4.3 OpenFlow Switch Actions

The OpenFlow switch performs three major actions. These actions are summarized below [37]:

1. Forwarding the packets of the flow to their destinations. If the switch was previously trained for this type of flow, i.e. if it had previously received a packet belonging to this flow, then it will automatically pass it through the same path that was chosen for the former packet.

2. If the switch was not trained for this sort of packets, it encapsulates and forwards this packet to the controller through a secure channel in order to make a decision regarding this flow type, where it either creates an entry in the flow table for this flow to guide the switch how to deal with this kind of packets and where to send it in the future without returning to the controller, or it sometimes decides to

forward all the packets of this flow to the controller in the future for processing information such as shedding a certain percentage from this type of traffic.

3. Sometimes, the controller decides to drop the packets of a particular flow either for purposes of security or to reduce the amount of traffic to relieve congestions. Many technologies can make use of this OpenFlow facility such as the VLAN (Virtual Local Area Network) where OpenFlow can create isolated local network for a number of identified users [23]. This can be achieved by preventing data flows of strange users (users not authenticated) from accessing their destinations by dropping such flows. Another technology that can benefit from this facility is proxy/non-proxy network management, in which only the authorized users can access network resources directly, whereas guest users can access only via proxy [23].

2.1.4.4 OpenFlow Controller

The Controller is the OpenFlow element which manages the traffic over the network. It either adds or removes entries from the flow table statically or sometimes it monitors the performance of the network, and makes decisions dynamically according to the status of the network, such as monitoring the congestions and decides to throttle the traffic.

2.1.4.5 OpenFlow Secure Channel

All the OpenFlow switches in the OpenFlow network are connected to the controllers through this secure channel. This channel should be secure and all data passing through it whether these data are commands from the controller to manage the switch, or packets passing between the controller and the switch, all these data should be well secured and encrypted using Secure Sockets Layer SSL (a security protocol that enables encrypted communication between server and client) in order to prevent network attackers from damaging the network.

2.1.4.6 OpenFlow protocol

The OpenFlow protocol is used to initiate the communication between the controller and the switch. This protocol serves as the language to make the controller and the switch understand each other. This protocol supports three types of messages: 1- controller-to-switch messages which are used to enable the controller to configure switches and manage the network. 2-Synchronous messages which are sent by the switch, then directed to the controller to keep it up to date with the status of the switches and the network. 3-Symmetric messages which are sent without any solicitation from the controller or the switch such as the Hello message, which is exchanged between the switch and the controller at the connection start-up stage, Echo message which can be sent from one direction and a reply should return from the other direction to confirm the connectivity between the controller and the switch, or vendor message to offer additional functionality by the OpenFlow switch [23].

2.2 Network Routing

Network routing is defined as the process of finding path from a particular sending source node in the network to the desired receiving destination node. An efficient routing protocol should provide proper routes for the traffic in order to save the network resources. Furthermore, the good routing protocol must deal efficiently with all the conditions of network abnormality such as links or nodes failures. Many algorithms have been introduced for that purpose, but in general, routing algorithms can be classified into two main classes, namely, centralised, and distributed routing algorithms. Information on the network is directed to its destination by means of routing tables, where the different nodes in the network consult the routing tables in the processes of making decision of which is the proper output port to forward each particular incoming traffic to it.

2.2.1 Centralised Routing

In centralised routing algorithms, the whole network will be managed by one controlling entity (e.g. server) that monitors and manages the transmission of data on the network. In this routing scheme, only one node, the central node, possesses a routing table, and has the authority to make routing decisions. All other node must consult this central node when any routing decision is required. Here, only the central node has access to monitor the network resources statuses and it makes the routing decisions according to this information. Network's status information such as links' connectivity and loading is gathered by this controlling node either only one time in the network setup phase as it is the case in *Static Routing Protocols*, or this status information is collected from time to time to help the central node updating the network's unique routing table accordingly as in *Dynamic Routing Protocols* or sometimes called *Adaptive Routing Protocols*. Centralised routing protocols generate an amount of undesired overhead that is directly proportional to the network size due to interchanging information between the network's nodes and the controlling entity. For this reason, it is not suitable for large network. On the other hand, if the network is small and the bandwidth is sufficient, the static routing protocol's simplicity will represent a stimulus to use such a routing technique.

2.2.2 Distributed Routing

In this type of routing systems, each of the network's nodes has its own routing table, and there is no controlling entity that updates the routing tables of other nodes in the network but instead, nodes cooperate to update their own routing tables. This system is more reliable than centralised routing since the routing decisions are not made by the same central party which is exposed to potential failures that may break all the routing system. In this routing scheme, each node gathers information about links loads and statuses from its neighbouring nodes, and then constructs its own routing table depending upon this information. Any change in the status of the network will be sensed by the adjacent nodes then this information will be conveyed to the other nodes in the network.

2.3 Ant Colony Based Routing

This section covers the background of ant routing algorithm which was inspired from the foraging behaviour of real ant swarms. Deneubourg showed that ants use self-organisation behaviour to perform fairly complicated tasks with minimal individual intelligence [37]. The

Ant colony optimisation algorithm was first proposed by Marco Dorigo in 1992 to solve the problem of finding the best path in a graph [38]. This routing algorithm tries to mimic the collective behaviour of real ants when they move between their nest and a source of food, where they usually use the shortest path for their movements [39-42]. Ant colony can be seen as a distributed system with each ant representing a mobile agent. Each mobile agent has a very limited experience but by gathering the experiences of all the agents, the system will be able to predict the optimal path among a number of possible paths.

2.3.1 Biological Ants Foraging

Initially, ants take different directions from their nest looking for food. While they are exploring the area around the nest, ants deposit a chemical substance called pheromone in their path [43-47]. Other ants will follow those paths of more pheromone concentration. Supposing that one ant discovered a food source, this ant returns to the nest currying a piece of that food. On its way back to the nest the pheromone concentration increases to double. Consequently, other ants will follow that path to bring the other pieces of food to the nest. This process of indirect communication among the ants is biologically termed *stigmergy* [48, 49]. Figure 2.14 depicts this foraging behaviour of ants. Supposing that there are two routes leading to the same food source and the ants deposit pheromone at the same speed, then the shortest path will have more pheromone concentration than the other path. This will encourage other ants to follow that shortest path.

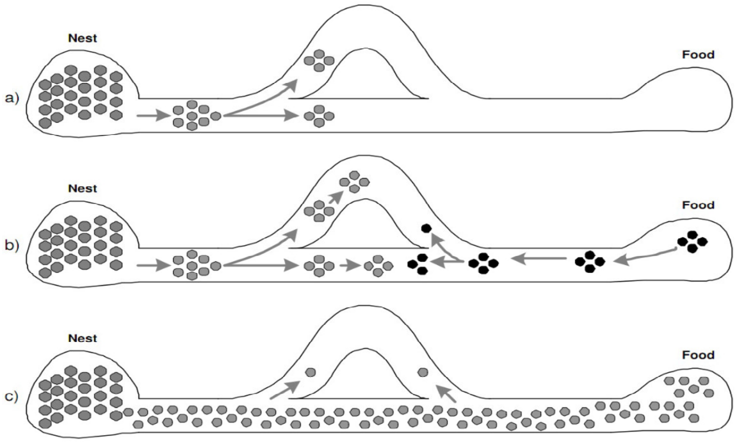


Figure 2.14 Ants Foraging Behaviour [50]

To avoid the case of concentrating the pheromone at the dead ends when a path is closed, i.e. does not lead to the food as in Figure 2.15 the ants holding pieces of the food and returning back to the nest deposit more pheromone than the other ants with empty hands [48].

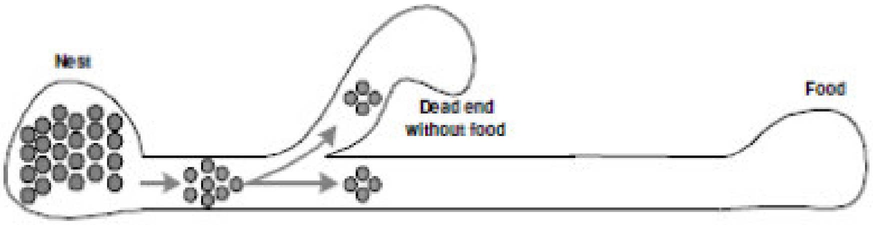


Figure 2.15 Ants with Dead End Path [50]

2.3.2 Ants Routing Modelling

The biological behaviour of ant foraging has been imitated in a distributed routing algorithm for communication networks, where some nodes are chosen to send small size packets called Forward Ants to random destinations, periodically to explore the available paths towards these destinations. Each node i within the network of size N nodes has its own routing table, which is constructed from N-1 rows representing the different network's destinations and M columns to represent the next hop neighbour, which should be visited in order to reach that destination, where M is the number of neighbours of node i.

2.3.2.1 Routing Table

Each entry in the routing table is addressed by the destination, d, and the next hop neighbour, j, and contains $\tau_{i,j,d}$ which represents the probability to choose neighbour node j as a next hop when an ant moves towards its destination from node i. The value of τ is represented by a figure between 0 and 1 and the sum of the probabilities of selecting this destination through the different neighbours equals 1 as shown in Table 2.1.

Table 2.1: An Example of the Node's Routing Table

	j_1	j_2	$\cdots$	j_M	
d_1	0.825	0.125	…	0.002	$\sum = 1$
d_2	0.175	0.645	…	0.005	$\sum = 1$
. . .	. . .	. . .	…	. . .	
d_{D-1}	0.050	0.050	…	0.725	$\sum = 1$

2.3.2.2 Routing Table Updating

The ant records information about the path it has travelled through in its forward trip such as the load on the different links which construct that path, the whole path's number of hops, etc. When an ant reaches its destination, a Backward Ant is sent back along the same path, which has been followed by the corresponding forward ant. Through its way, the backward ant updates the routing tables and link information tables of the nodes it traverses. When a backward ant reaches node i, it updates that entry of the node's routing table, which corresponds to the source of this backward ant (which is the destination of its corresponding forward ant), where it increases the probability of the neighbour it is coming from and decreases the probabilities of the other neighbours according to equations (2.1) and (2.2), assuming that the backward ant has visited node j at time t.

$$\tau_{i,k,d}(t+1) = \frac{\tau_{i,k,d}(t)+\delta_r}{1+\delta_r} \qquad if\ (k=j) \qquad (2.1)$$

and

$$\tau_{i,k,d}(t+1) = \frac{\tau_{i,k,d}(t)}{1+\delta_r} \qquad if\ (k \neq j) \qquad (2.2)$$

where:

δ_r is the reinforcement parameter which is derived from the path's information collected by the ant, and can be calculated from equation (2.3).

$$\delta_r = \alpha . \delta_p + (1 - \alpha) . \delta_c \qquad 0 \leq \alpha \leq 1 \qquad (2.3)$$

δ_p is the amount of reinforcement corresponding to the path's length, and can be calculated from equation (2.4).

δ_c is the amount of reinforcement corresponding to the path's business, and can be calculated from equation (2.5).

$$\delta_p = e^{-\beta . \Delta p} \; , \quad \Delta p = p - p_{min} \qquad (2.4)$$

$$\delta_c = e^{\gamma . c} - 1 \qquad (2.5)$$

where p is the actual path's length, p_{min} is the length of the shortest path found by ants and c is the percentage of free capacity along the path. β and γ are design parameters used to control the performance of the algorithm. The proportion of the path's free capacity, c, can be computed by equation (2.6).

$$c = \frac{Unused\ Bandwidth}{Total\ Path's\ Capacity} \qquad (2.6)$$

In order for the network to track any abnormality such as link or node failures, or redistribution of population among the network's nodes, the ants are supposed to be generated repeatedly at fixed time intervals. Another possibility may occur that prevent ants from reselecting the currently most appropriate path when the pheromones are concentrated on the former best path, and this will attract other ants to continue following that path even in the event when another path has become best due to the change of network state. To avoid this case, the deposited pheromone evaporates after a period of time. This evaporation will serve to redistribute the concentrations of pheromone giving the chance for the new best route to be selected since the new deposited pheromone will concentrate on that route.

Two main advantages of such a routing technique could be observed: Firstly, there is no main dominant managing entity which monitors the status of the whole network and gives routing decisions accordingly, thus it needs a huge memory for large networks, but instead, nodes communicate together to exchange routing information and links' statuses in a distributed manner. Secondly, the ants are generated periodically, enabling the network to discover any change in the routes and update the routing tables consequently. Note that the network needs first to be trained by sending a number of ant packets across the different paths. During this stage, no data should be sent since nodes have no idea of the places of other nodes, where all the entries of the routing tables are set to zero at the beginning. Furthermore, in the case of dynamic network changes, the network remains using the former routing tables until it is trained again to track these changes according to a set of predefined QoS preferences of the different traffic types.

2.3.3 Ants Routing Algorithm

For the ant routing model to work successfully, the following algorithm should be precisely followed.

```
START
{
Initialization of Routing table: The next-hop probabilities of each node's routing table are to be distributed uniformly, such that:
        • $\tau_{i,j,d} = \frac{1}{M}$ , where M= Number of neighbours of node i
        • $C_{i,j} = 0$ , ∀ j ∈ $\{j_1, j_2, j_3, \dots, j_M\}$, where $C_{i,j}$ is the available bandwidth of the link connecting node j with node j
DO (in parallel)
{
```

```
STEP 1: Each node sends forward ants to random destinations in regular time intervals.

DO (in parallel, for each forward ant)

    {

        STEP 2: Determine the next hop according to the probabilities in the routing table of the current node with a probability of (1- $P_{noise}$), or to choose a random neighbour with a probability of $P_{noise}$ in order to solve the problem of ant protocol stagnation which will be defined later in this chapter.

        STEP 3: While the next node is already visited?

            - If there are unvisited neighbours, choose another next hop neighbour.
            - Else Delete the ant.

        STEP 3: Each node keeps record of the information of followed path so far, such as the length of the path (L) and the available bandwidth (C).

        STEP 4: When a forward ant reaches its destination, return a backward ant to the source node reversely on the same path which was used for forwarding the forward ant.

    }

DO (in parallel, for each backward ant)

    {

        STEP 5: Each backward ant updates the routing tables of the nodes it traverses according to equations (2.1) and (2.2).

        STEP 6: When a backward ant reaches its destination, delete it.
```

```
            }
}
END
```

2.3.4 Ants Routing Flowchart

In order to better explain how the ant routing algorithm works, the flowchart in Figure 2.16 was included in this chapter.

2.3.5 Ant Protocol Stagnation

Ant Protocol Stagnation is defined as the inability of the network to sense the network changes. Where and when the network detects the best path it increases the probability of following that path by other ants and decreases the probabilities of following other paths. Supposing that sudden changes have happened to the network's statuses causing that path to no longer be the best. These changes may include node disconnections, link failures, or load changes over the network's links. In these cases, the network will still send ants through that route, since it is of the highest probability, and consequently will still reinforce the probability of following that path by other ants. This problem is called ant protocol stagnation. To solve this problem the network should give a chance for a percentage of the incoming ants to test other paths. This can be easily achieved if each node selects to send the incoming ant according to its routing table with a percentage of $(1 - P_{noise}$), and to a random destination with a percentage of P_{noise}. A value between 05% and 15% is suitable for P_{noise} to help to obtain a fast tracking of the network reconfiguration. Note that there is no particular criterion to choose the value of this design parameter (P_{noise}) since its value depends on many factors including the size and the topology of the network. The way for choosing this value is mainly depends on the experiment. In our network we found that the best performance results if P_{noise} is given a value between 05% and 15%.

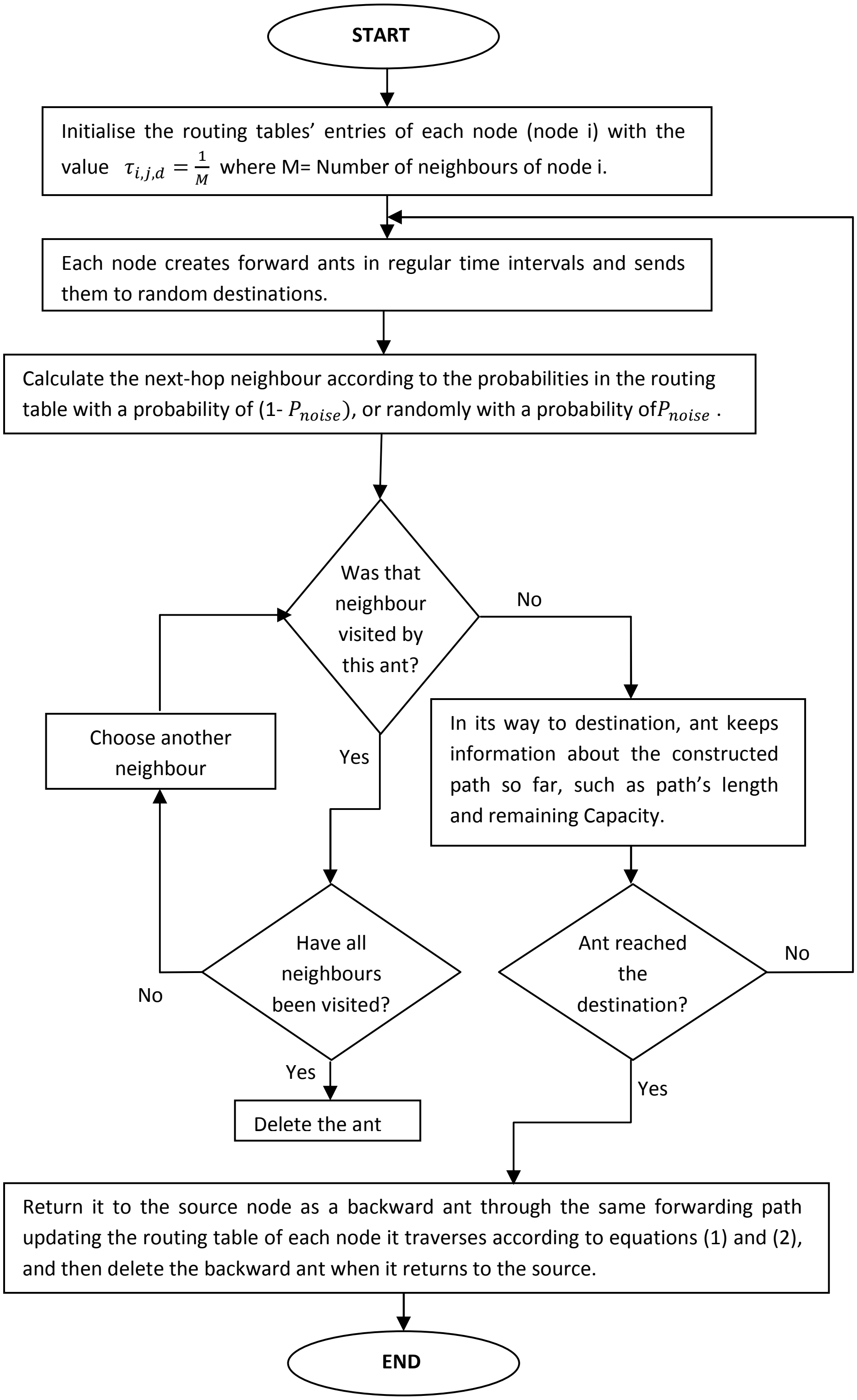

START
Initialise the routing tables' entries of each node (node i) with the value $\tau_{i,j,d} = \frac{1}{M}$ where M= Number of neighbours of node i.
Each node creates forward ants in regular time intervals and sends them to random destinations.
Calculate the next-hop neighbour according to the probabilities in the routing table with a probability of (1- P_{noise}), or randomly with a probability ofP_{noise} .
Was that neighbour visited by this ant?
No
Yes
Choose another neighbour
In its way to destination, ant keeps information about the constructed path so far, such as path's length and remaining Capacity.
Have all neighbours been visited?
No
Yes
Delete the ant
Ant reached the destination?
No
Yes
Return it to the source node as a backward ant through the same forwarding path updating the routing table of each node it traverses according to equations (1) and (2), and then delete the backward ant when it returns to the source.
END

Figure 2.16 Ant Routing Flowchart

2.4 Summary

Optical information is switched among the network's nodes using either optical circuit switching, packet switching, or burst switching. Optical circuit switching provides no level of processing during data transmission since no buffers are available to handle the information. A light path is allocated prior to the transmission of information in circuit switching. This light path is released whenever this information reaches its destination.

On the other hand, Optical packet switching provides a wider range of data control, but it needs a large buffer at each node to process the different packets according to their headers. Packets arriving any node at the same time should be buffered, processed, and then forwarded to their suitable next hops according to their destination addresses declared in their headers.

In Optical bursts switching, optical packets are assembled at the ingress of the source node. A control packet is sent prior to the burst. This control packet includes information about the burst such as the destination address. The control packet sets up a light path circuit for the subsequent burst. At the end, the burst is disassembled at the destination node and submitted to the end user as regular packets. No buffers are needed at the intermediate nodes since bursts are transmitted in a circuit switching fashion through the core of the network. Consequently, it is possible to send bursts through an all optical core.

OpenFlow switches, provides a wider range of data management, where the control plane is separated from the data plane in OpenFlow switches. Packets of similar specifications are forwarded through the same route and dealt with in a similar fashion by the OpenFlow switches. Only the first packet of a particular type needs to be signalled to the controller (via a secure channel) in order to assign rules to handle it and its later following packets.

Ant routing (or sometimes called swarm routing) is inspired from the natural social behaviour of real ant colony. Ant routing represents a kind of artificially intelligent distributed routing protocol. No central entity is required to update the routing tables of the different network's nodes when a change in the network's status occurs. Instead nodes update their own routing tables according to the information held by the ant as soon as a new ant is received.

At the beginning artificial ants (ant packets) are launched through random paths to the destinations. Each ant has a small memory to keep track of the specifications of the whole path it passed through to reach its destination. When an ant reaches its destination, it is sent back to the source node through the same route it used in its forwarding phase. During its backward phase, ant updates the routing tables of all the nodes it traverses based on a goodness function, which it evaluates from the goodness of the different alternative paths according to the information it knew about that path, such as the path's length, and/or bandwidth.

Most of the time, ants are forwarded through different paths on the network according to the routing tables, whereas sometimes they select random paths to allow the discovery of new paths. The probability with which the ant selects a random next hop is termed as P_{noise}. Data is then sent to its destination through the most appropriate path.

Chapter 3

Wavelength Division Multiplexing in Optical Networks

The last few years have witnessed tremendous developments in the field of optical networks. These developments came as a consequence of the vast popularity of the Internet together with the unprecedented improvements and growth of Internet services and applications [51-55]. One of the most significant developments that optical network experienced in the last decade is the support of multiple wavelengths on a single optical fibre or what is commonly known as Wavelength Division Multiplexing (WDM). This technique was mainly found to support the increasing bandwidth demand of some applications which require high bandwidth [56, 57]. In WDM it is possible to send two or more signals or data traffics on the same optical cable but on different non overlapping frequency bands. In other words, the optical link is divided into a number of channels, where each channel is operating in a distinct wavelength and representing a single end-to-end communication. Although allowing multiple bandwidths on a single fibre can support the huge bandwidth demand of current and future Internet applications and services, there are still efforts which improve the network architectures and protocols to match such a development in optical fibres [58, 59].

In order to better understand WDM, one should study the optical fibre and its components. This chapter will deal with these components, and will be supported with figures and block diagrams in order to develop a deeper understanding of this technology.

3.1 Transmission in Optical Fibre

It is very necessary to understand the characteristics of optical fibres and how the data is transmitted through it. Fibre is actually a thin core of very pure glass about of the human hair’s diameter used to transmit light signals. This core is coated with another optical material with a different refraction index to help in reflecting the light path falling on its surface back into the core. This coating material is called cladding which is in turn covered with a plastic coating to protect the fibre from damage. The refraction index of a material is scientifically defined as the ratio of the speed of light in the vacuum to the speed of light in this material [51, 60]. Figure 3.1 shows a cross section of an optical fibre.

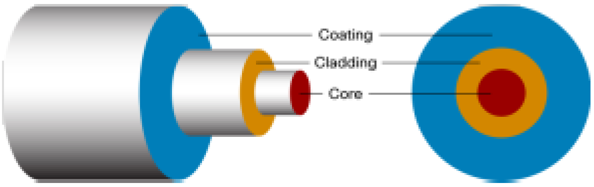


Figure 3.1 Optical Fibre Cross Section [61]

Light paths are propagating along the fibre due to the consecutive reflections from the cladding inner surface, where a maximum performance is yielded if the light is totally internally reflected. The idea is that when the light path is transferred from one material to another of a different refractive index, it is refracted at an angle in the second material which depends on the refractive indexes of the two materials and the angle this light path makes with the two materials' interface surface is called the incident and refractive angles. Snell's law states that [51]:

$$n_1 sin\theta_1 = n_2 sin\ \theta_2 \qquad (3.1)$$

Where $n_1\ and\ n_2$ are the refractive indexes of the first and second materials respectively; θ_1 and θ_2 are the angles the incident and the refracted lights make with the normal to the interface surface at the point of refraction respectively. See Figure 3.2.

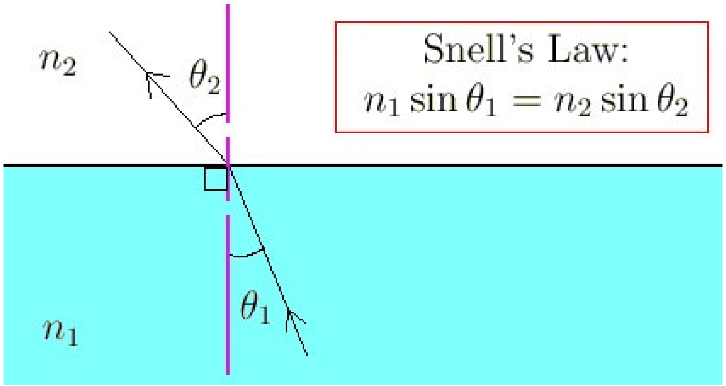


Figure 3.2 Snell's Law for Refraction [62]

There are two main types of optical fibres, namely, step index and graded index fibres. In step index fibre, the core is manufactured from one material with a particular refractive index, whereas the refractive index of the core in the graded index fibre decreases as it goes away from the centre of the fibre causing the light to propagate in an oscillatory fashion. Figures 3.3 (a) and (b) show the light propagation in step and graded indexes fibres respectively.

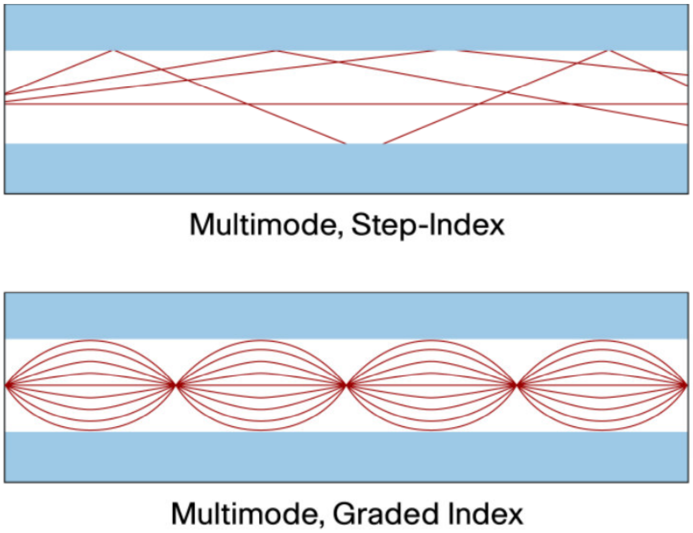


Figure 3.3 Light Propagation in Step and Graded Index Fibres [61]

In order to get a total internal light reflection on step index fibre, the core angle θ_{core} should exceed some critical value $\theta_{critical}$ that corresponds to a cladding angle θ_{clad} = 90°.

According to Snell's law:

$$\sin\theta_{clad} = \frac{n_{core}}{n_{clad}}\sin\theta_{core}$$

For θ_{core}= $\theta_{critical}$,

$$\theta_{critical} = sin^{-1}(\frac{n_{clad}}{n_{core}}) \qquad (3.2)$$

Therefore, for the total internal reflection

$$\theta_{critical} > sin^{-1}(\frac{n_{clad}}{n_{core}})$$

Another issue should be taken into account when total internal reflection is desired, where the light should be directed to fall on the air-core boundary with an angle that guarantees such a total reflection on the core-cladding boundary. From Figure 3.4, it can be seen that the maximum value of θ_{air} can be calculated as follows:

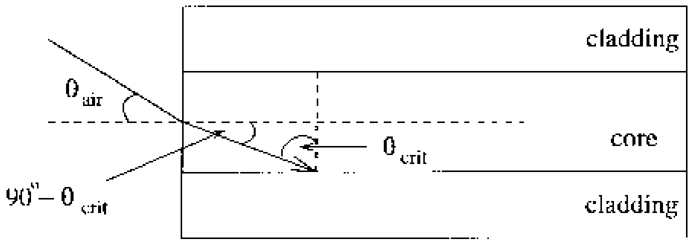


Figure 3.4 Fibre's Numerical Aperture [51]

$$n_{air}\, sin\theta_{air} = n_{core}\, sin(\,90° - \theta_{critical})$$

$$= n_{core}\sqrt{1 - sin^2\theta_{critical}} \qquad (3.3)$$

But $sin(\,\theta_{critical})$ =n_{clad}/n_{core}, therefore

$$n_{air}\, sin\theta_{air} = \sqrt{n_{core}^2 - n_{clad}^2} \qquad (3.4)$$

Where:

$n_{air}\, sin\theta_{air}$ is called the Numerical Aperture (NA) of the fiber.

θ_{air} is the maximum angle of the light incident on the air-core interface surface that causes total internal reflection in the fibre.

There are two main types of fibres that govern the way in which light is propagating through the fibre. These are single mode and multiple modes fibres.

3.1.1 Single Mode Fibre

When a light source on one end of an optic fibre is directed to the fibre's core, a light ray may propagate on a straight path in the core of the fibre, some other rays may fall on the core-cladding boundary at different angles causing them to propagate in a zigzagged way with different path lengths through the fibre's core. Each ray transmitted through the optical fibre is termed as a mode, and due to the fact that different rays have different path lengths to the light receiver on the second end of the fibre, the light rays are received at different times forming a light pulse at the receiver end. The single mode fibre is an optical fibre with a small diameter, typically less than 10 microns [51]. This small diameter allows only one light ray to transmit through the fibre. This type of fibre offers a higher bandwidth than the multimode fibre type but its problem arises from the difficulty of coupling the light source to the fibre [63, 64].

3.1.2 Multimode Fibre

In multimode fibre, the core is thick enough to facilitate the process of light source coupling. The core's diameter is big enough to hold more than one light mode propagating through the fibre. Different modes require different delays to reach their destination forming a pulse of light rays received at the receiver end. This phenomenon is called intermodal dispersion.

Dispersion reduces the total fibre's bandwidth since successive input lights need to be separated enough in frequency domain to avoid their output pulses being overlapped. Figure 3.5 shows the light propagation through single mode and multimode fibres. Note that no intermodal dispersion happens in single mode fibres.

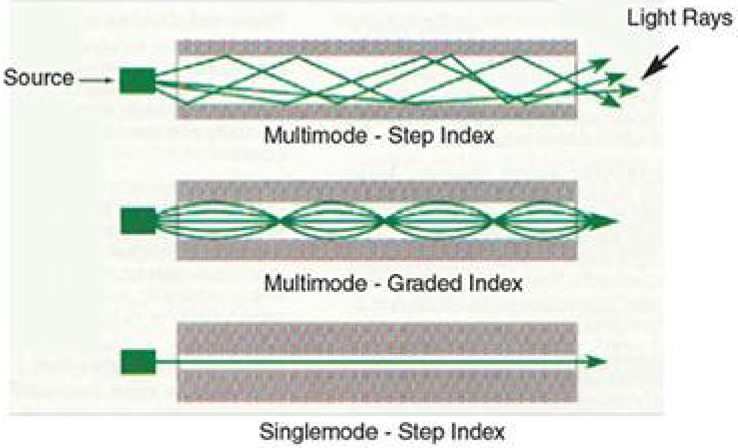


Figure 3.5 Light Propagation through Single Mode and Multimode Fibres [65]

3.2 Attenuation in Optical Fibres

Optical fibre attenuation is defined as the loss or reduction in the power of the optical signal as this signal propagates through an optical fibre. Attenuation in optical fibres is a function of the distance from the light source. For a given transmitter output power and the receiver sensitivity, the more the distance a light signal propagates, the more the attenuation it suffers from, therefore, the attenuation is calculated in dB/Km. Supposing that P (0) is the power at transmitter output (or the power at distance 0), L is the distance from the transmitter, the power at distance L can be calculated by equation (3.5).

$$P(L) = 10^{-\frac{AL}{10}} P(0) \qquad (3.5)$$

Where A is the attenuation constant of the fibre measured in dB/Km. In order to recognise a light signal at distance L, its power P(L) should be greater than or equal to the receiver's sensitivity (P_r), therefore the maximum distance between the transmitter and the receiver can be determined from equation (3.6)

$$L_{max} = \frac{10}{A} log_{10} \frac{P(0)}{P_r} \qquad (3.6)$$

If the actual distance between the transmitter and receiver exceeds L_{max} , amplifiers should be used to retrieve the signal. Supposing that all the amplifiers have sensitivities equal to the receiver's sensitivity, and their output power equal to P(0), i.e. they fully retrieve the signal to its original power, then an amplifier should be placed at every L_{max} or less.

Attenuation in optical fibres depends also on the operating wavelength as shown in Figure 3.6 [51]. It is clear from this figure that the lowest attenuation occurs between 1300nm and 1550nm.

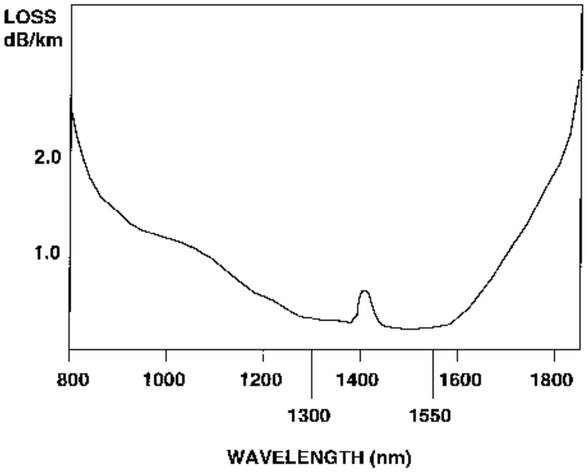


Figure 3.6 Loss-Wavelength Relationship in Optical Fibre [51]

Attenuation can happen due to light scattering, where a part of the light is reflected in all directions escaping from the core or returning back to the light source, while the light signal is propagating through the optical fibre. This scattering happens due to the variations in the density of the core's glass material, where in order to change the refractive index, impurities are added to the core’s material. These impurities create density variations in the material of the core. Consequently, more scattering happens. Since more impurities are used in multimode fibres, they suffer from higher level of attenuation than single mode fibres. Attenuation can also happen because the particles of the impurities which are added to the fibre’s core absorb a part of the light at specific wavelengths and dissipate it as heat energy. In addition, the bending of a fibre represents another cause of attenuation since it helps the light to escape from the core of the fibre.

3.3 Dispersion in Optical Fibres

Transmission in optical fibres is usually accompanied with dispersion. Dispersion is defined as the widening of the light pulse duration while it is propagating through the fibre. There are three types of dispersions that exist in optical fibres.

3.3.1 Intermodal Dispersion

This kind of dispersion happens due to the transmission of more than one mode of the same light signal in different velocities along the same fibre. It happens only in multimode fibres.

3.3.2 Material or Chromatic Dispersion

Due to the fact that there is no light source, even a laser, can emit an exact single wavelength, and the fact that the refraction index of a material depends on the wavelength of the light transmitted through it, different wavelengths transmit on the same fibre at different velocities creating what is known as material dispersion.

3.3.3 Waveguide Dispersion

This kind of dispersion occurs because the propagation of wavelength depends, to a particular extent, on the wave guide properties such as the shape and indexes of the fibre's core and cladding.

3.4 Non Linearity in Optical Fibres

Non linearity in optical fibres can lead to constraints in spacing between adjacent wavelength channels in Wavelength Division Multiplexing (WDM). Consequently, it limits the maximum power transmitted on the channel or the channel's maximum bit rate. This non linearity can be caused by several factors as follows.

3.4.1 Non Linear Refractive Index

Since the refractive index of a material depends on the intensity of the light that traverses this material, the light signal travelling down a fibre faces shifts in its phase while it is propagating along the fibre. The change in the power of the transmitted light signal creates what is known as Self Phase Modulation (SPM), whereas the change in the intensity of light signal belonging to the other wavelength channels creates Cross Phase Modulation (XPM).

3.4.2 Stimulated Raman Scattering (SRS)

This phenomenon was first discovered by a scientist named Dr. Raman who discovered that a light can interact with vibrating molecules by changing its frequency [66]. A light scientifically is composed of a stream of photons. Every material is composed of molecules, and these molecules are vibrating all the time. The warmer the material, the faster the molecules vibrate, and vice versa. As a light hits some vibrating molecules, the molecule steals from the incident light energy to vibrate faster. When a light with a particular wavelength falls on the vibrating molecule of the material from which the fibre's core is manufactured, it creates a scattered light signal at a longer wavelength. In other words, portions of the different wavelengths' travelling lights will change their frequencies to lower values. These lower frequency light signals are called the Stocks. When the power of the input signal increases, the power is transferred to stock signals, which grows sharply. In the condition of very high power input light, all the input signal's power will be transferred to the stock waves due to the SRS phenomenon [66]. Consequently, in WDM, some of the short wavelength channels will lose some of their power.

3.4.3 Stimulated Brillouin Scattering (SBS)

When a light traverses a dielectric material such as optical fibre, it interacts with the acoustic waves which are already present in every material. This interaction results in backward stock waves with a frequency downshifted from the incident light frequency by an amount equal to the acoustic wave frequency. When the input power exceeds a certain threshold, called Brillouin threshold, the stock waves can carry most of the incident light's power. Therefore one on the ways used to reduce the effect of SBS is to make the input power below this threshold. SBS leads to crosstalk when two WDM channels hold light of frequencies different in their amounts by Brillouin shift, i.e. stock wave frequency [67].

3.4.4 Four-Wave Mixing (FWM)

It was found that when three optical signals with different wavelengths travel on a non-linear medium such as the optical fibre at the same time, a fourth signal is generated with a wavelength equals the sum or difference of the original three signals. A problem of overlapping occurs when the new frequency is already used by another WDM channel [68], since this will disrupt the information over that channel.

3.5 Couplers

A coupler is a general term that is used for both splitter and combiner, where the splitter is a device used to split a light out of an optical fibre, and the combiner is a device used to combine lights into an optical fibre. The splitting ratio is defined as the power on each output port of a splitter. A widely used splitter is 1: 2 with a splitting ratio of 50:50. A 2:2

coupler is actually a 2:1 combiner followed by 1:2 splitter as shown in Figure 3.7. A 2:2 is basically broadcasts signals from two input fibres onto two output fibres.

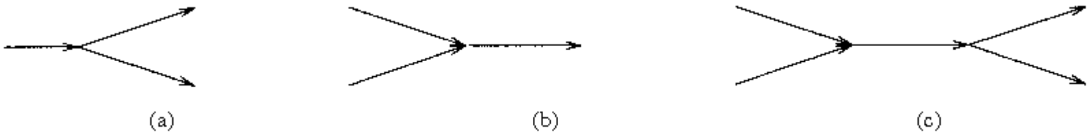


Figure 3.7 Splitter, Combiner, and Coupler 44]

3.6 Fibre Cross-Connect Elements

A fibre cross connect is an optical switch used to connect each input port to a particular output port. A 2×2 cross connect is the simplest example of such a device, where it contains two input ports and two output ports. It supports two connection states, either cross connection where the upper input port is switched to the lower output port whereas the lower input port is switched to the upper output port, or bar connection where the upper input port is connected to the upper output port and the lower input port is connected to the lower output port, as shown in Figure 3.8. Always one wavelength is applied to each input port because fibre cross connect devices do not have the capability to demultiplex different wavelengths transmitted over the same channel since such devices are wavelength insensitive.

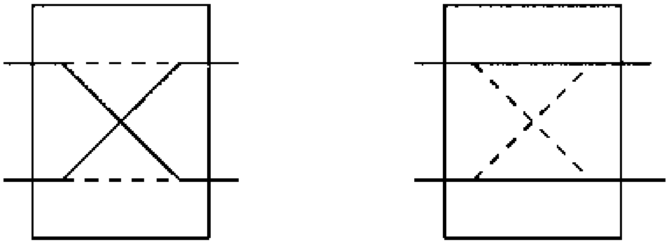


Figure 3.8 A 2×2 Cross Connect Elements Operation States [51]

Fibre cross connect devices can be classified into two major kinds, namely, generic directive switches and gate switches.

3.6.1 Generic Directive Switches

Generic Directive Switch is a coupler with two parallel optical waveguides that are placed in close proximity to allow for signal exchange through some finite interaction length. The interaction length, the amount of separation between the two waveguides, and waveguide's confinement factor determine the coupling strength. The waveguide's confinement factor is defined as the fraction of the power that is within the waveguide's core. Placing electrodes over the waveguides, as shown in Figure 3.9 (a), helps in increasing the difference in propagation constants of the two waveguides leading to total isolation in the case if a positive voltage applied. Thus, no light coupling occurs between the two waveguides, i.e. bar connection state. On the other hand if zero voltage is applied on the electrode, the optical signal propagating on one of the waveguides will be coupled on the second waveguide via an evanescent wave which is that part of the optical signal that propagates along or outside the boundary of the waveguide and decays exponentially with the distance from that boundary. Two problems are associated with such a one voltage switch; first, the interaction region length needs to be very accurate for this coupler to offer a good isolation. Furthermore, these couplers are considered wavelength specific, i.e. they do not work on a wide range of wavelengths.

In order to find switches that offer good switching performance as well as wider range of working wavelengths, reversed delta-beta coupler was designed, where the electrode was divided into two sections as shown in Figure 3.9 (b). If two equal but opposite voltages are applied to the electrodes, a cross connection state is achieved.

A third type of such switches is called balanced bridge interferometric switch, where it consists of a 3-db coupler with two sufficiently separated waveguides to prevent coupling. Each waveguide is an electrode to control the selectivity of a proper path for the input signal. To achieve cross connection of this kind, no voltage is applied to the electrodes, where in this case, the signals on each waveguide of the coupler will couple on the other waveguide [51, 69]. On the other hand applying two equal but opposite voltages on the two electrodes results in bar connection. See Figure 3.9 (c).

Figure 3.9 (d) shows another type of these generic switches, which is called intersection waveguide switch. This switch is characterized by having two intersected waveguides. When well fabricated, this switch can achieve both cross and bar connections with good crosstalk performance.

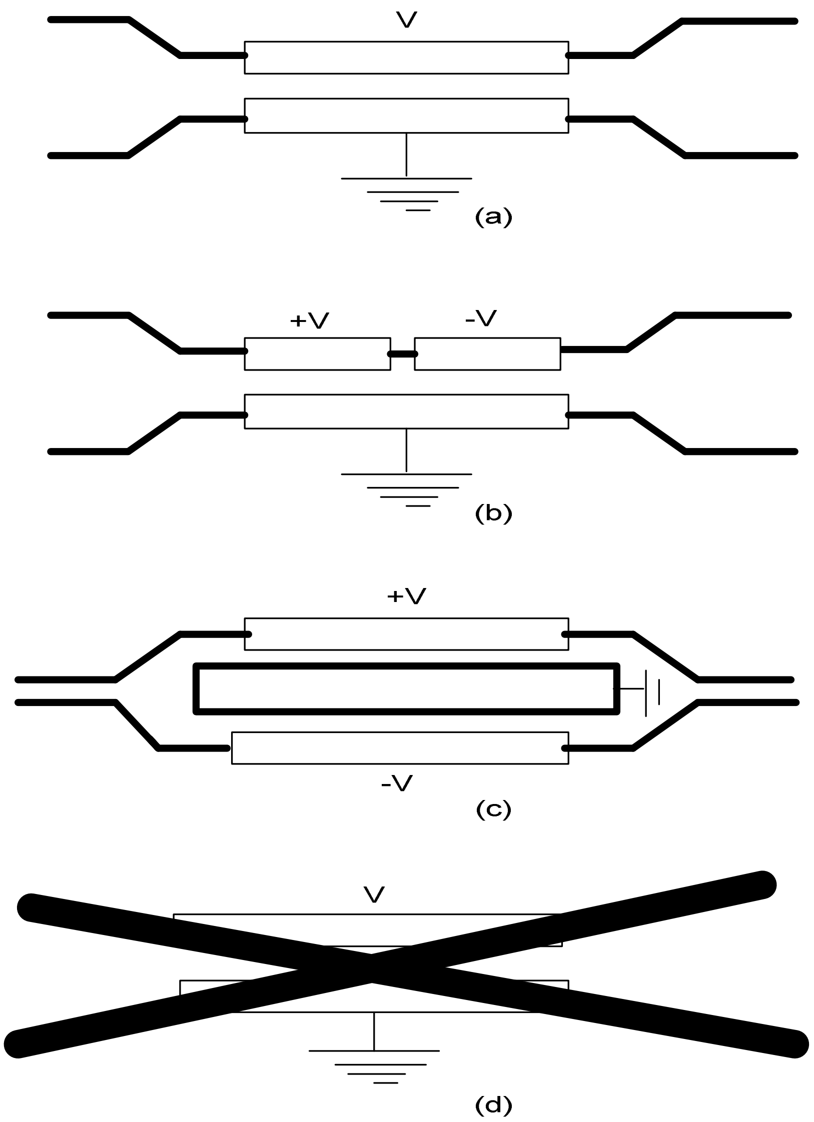


Figure 3.9 Generic Directive Switches [51]

3.6.2 Gate Switches

This type of fibre cross connect element is sometimes used as alternatives to the generic switches. Each input in an N×N gate is split into N outputs via 1×N splitter; these outputs are then connected to N^2 gate elements which are used to switch each input signal to the appropriate path. The outputs of the gate elements are then recombined to N outputs using N×1 combiners. The optical amplifiers can be used as gate elements in this type of switch, where each amplifier can be turned on or off to connect the input signal to one of its output ports. One of the major advantages of using the optical amplifier here is to use their amplification characteristics to compensate for the amount of losses that have resulted due to the numerous splitting and combinations of the signal. Figure 3.10 shows a simple 2×2 gate switch.

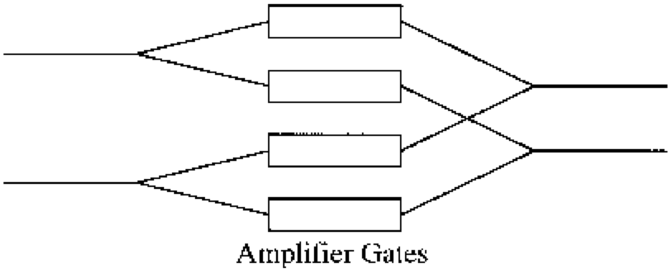


Figure 3.10 A 2×2 Gate Switch Using Optical Amplifiers [51]

3.7 Optical Demultiplexers

The main purpose of an optical demultiplexer is to split the compound light into its elementary wavelengths. In WDM the light transmitted on the optical fibre does not represent the data of one optical signal, but instead it includes several optical signals combined all together in different frequency slots. Figure 3.11 shows an optical demultiplexer that used a prism to separate the different input light's wavelengths, where each wavelength is refracted with an angle different from the other wavelengths.

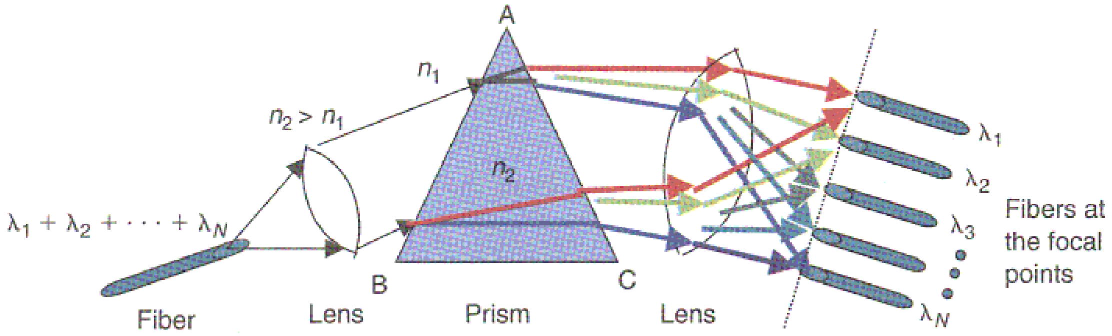


Figure 3.11 Prism Optical Demultiplexer [70]

3.8 Optical multiplexers

Optical multiplexer works in a reverse manner of demultiplexer, where it receives the different wavelengths from the wavelength fibres, and combine them on a single optical signal that travels on one fibre at the same time but in different frequency slots. Figure 3.12 shows a simple prism based optical multiplexer. This multiplexer uses a prism with two lenses in order to focus the different input wavelengths on the same output fibre [51].

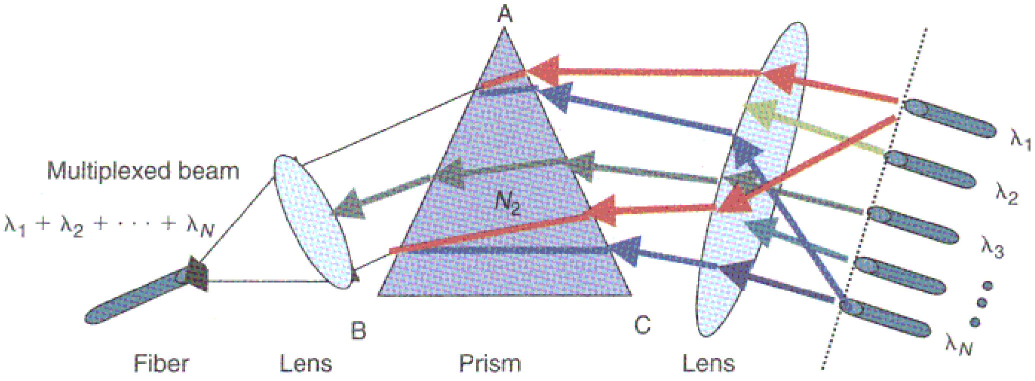


Figure 3.12 Prism Optical Multiplexer [70]

3.9 Wavelength Routers

Wavelength routers are of two types, either reconfigurable or non-reconfigurable. In a non-reconfigurable wavelength router, a certain wavelength is always routed to the same route. In a reconfigurable router on the other hand, the route for a particular input wavelength can be controlled electronically.

3.9.1 Non-reconfigurable Wavelength Routers

In this type of optical router, each input signal is first demultiplexed to extract the different wavelengths from the input optical fibre. The outputs of the optical demultiplexers are hardwired directly to multiplexers in order to recombine the different wavelengths within their appropriate output fibres. Since the demultiplexers and the multiplexers are hardwired, then these routers offer no control on the output path for a particular input wavelength. In other words, when a particular wavelength signal enters the router, it takes the same path as the other signals of similar wavelength. That is why these routers are called non reconfigurable routers. The fixed paths for the different wavelengths are determined by the routing matrix of the router. This routing matrix precisely depicts which demultiplexer's output is connected to which multiplexer's input for all the available bandwidths. Figure 3.13 illustrates a 4×4 optical wavelength router with four wavelengths λ_1,λ_2, λ_3 and λ_4 .

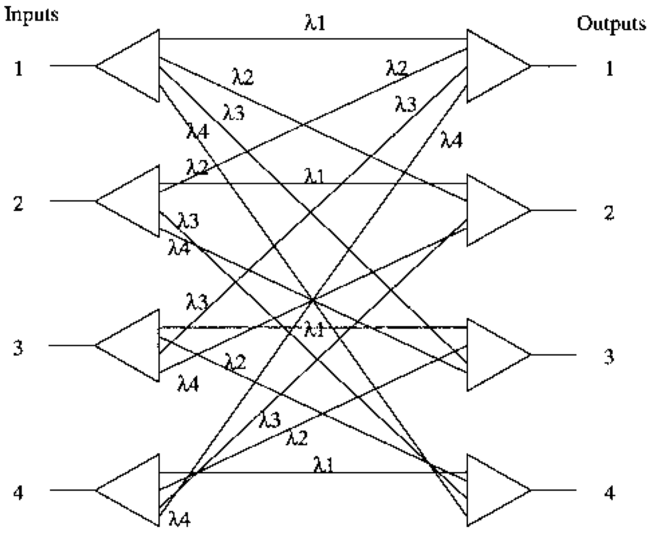


Figure 3.13 A 4×4 Optical Wavelength Router [51]

3.9.2 Reconfigurable Wavelength Routers

Reconfigurable wavelength routers have the same architecture of non-reconfigurable routers except that the outputs of the optical demultiplexers are not directly hardwired to the multiplexer but instead these different wavelengths from the demultiplexers are sent to switches. The switch, which may be built from optical cross connect elements, controls the out path for each particular wavelength. In a reconfigurable wavelength router, there is either a separate switch for each individual wavelength, or all the wavelengths that output from demultiplexers are directed to the same switch. Figure 3.14 shows a P×P reconfigurable wavelength router with M wavelengths. A reconfigurable wavelength router is also sometimes called a Wavelength-Selective Cross Connect (WSXC), and may also be referred as reconfigurable Wavelength Routing Switch (WRS). Unlike the non-reconfigurable wavelength routers, the optical signals of the same wavelength are sent to the same switch, and then the switch itself decides to which output multiplexer each of these signals should be sent. The switch makes such a decision according to an electronic control signal.

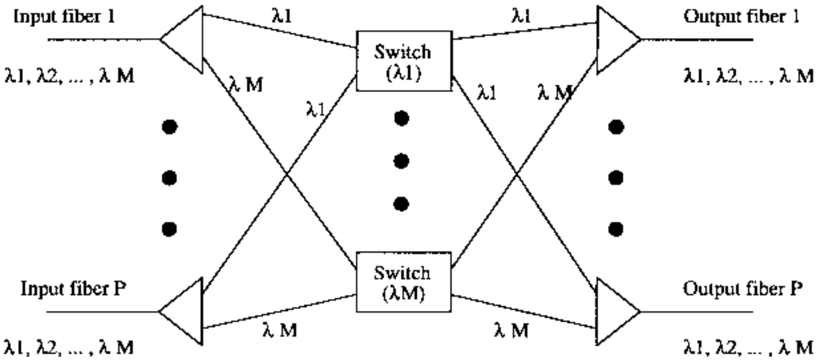
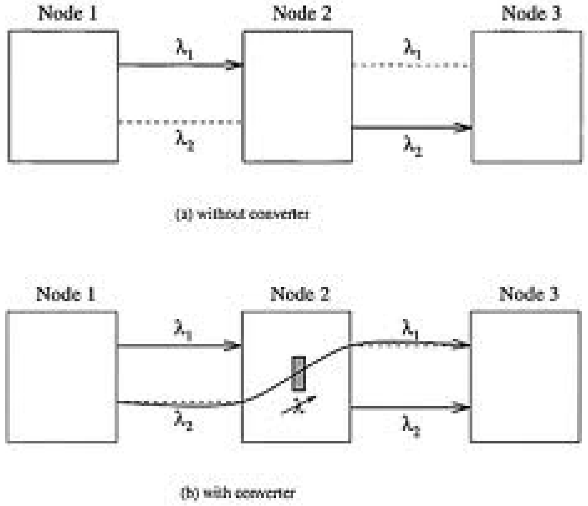


Figure 3.14 A P×P Reconfigurable Wavelength Router with M Wavelengths [51]

3.10 Wavelength Conversion

In order to fully utilise the bandwidth of an optical fibre, WDM with wavelength conversion capability was developed. Wavelength conversion is a significant function in WDM because it helps in reducing the number of data blockings, which occur when no available channel with sufficient bandwidth exists. In Figure 3.15, a simple example of two wavelengths fibres was presented to explain the importance of wave length conversion in WDM systems.



(a) without converter

(b) with converter

Figure 3.15 WDM with and without Wavelength Conversion [51]

Suppose two connections are taking place at the same time, where Node 1 is communicating with Node 2 on the wavelength λ_1 , and Node 2 is communicating with Node 3 on the wavelength λ_2 . What happens if another connection demand directed from Node 1 to Node 3 happens while these two connections are active? The answer will be basically dependent on whether Node 2 has the wavelength conversion capability or not. If it does not have such a capability, see Figure 3.15 (a), this demand is blocked since λ_2 is already occupied by another communication. This problem is called wavelength continuity constraint. On the other hand, if Node 2 has the capability of wavelength conversion, then Node 1 will use the wavelength λ_2 to communicate with Node 2. Node 2 will receive the data from Node 1, convert the wavelength to λ_1 , then forward this data to Node 3 on the wavelength λ_1 . See Figure 3.15 (b).

It is clear from this example that using wavelength converters helps in utilizing the fibres' bandwidths more efficiently, and it reduces number of blockings resulting in a better network performance. Wavelength conversion techniques can be classified into two main kinds: optoelectronic wavelength conversion, in which the optical signal need first to be converted into its electronic form where it is easy to convert its wavelength in the electronic domain, and all-optical wavelength conversion, in which the wavelength will be converted in optical domain with no need to convert the optical signal into an electronic signal. Moreover, all-optical wavelength conversions are sub classified into two sub types, namely, coherent effects based conversions and cross modulation based conversions.

3.10.1 Optoelectronic Wavelength Conversion

In this type of wavelength conversion, the optical signal is first applied to O/E converter to convert it into an electronic signal. O/E converter can be as simple as a photo detector, which basically converts light into electronic signal. This electronic signal is then processed to convert its wavelength and converted back to an optical signal by means of E/O converters. Wavelength conversion in electronic domain and E/O conversion can be achieved by applying the electronic signal to a tuneable laser diode. Since the electronic wavelength conversion process occurs in the electronic domain, it will be much slower than the photo detector's bit reception rate. Therefore, a buffer is required to store the electronic information when it is received by the photo detector. In other words, if the photo detector receives data on a particular wavelength faster than the conversion rate of the converter, the input data should be accumulated at a particular buffer to give the converter time to match such a speedy data arrival rate. These conversions support a maximum bit rate of 10 G bit/sec, and this conversion technique should not be used for higher bit rates. Figure 3.16 shows an optoelectronic wavelength converter using photo detector and tuneable laser.

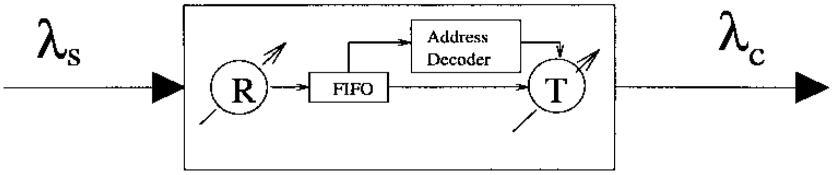


Figure 3.16 Optoelectronic Wavelength Converter [51]

3.10.2 Coherent Effects based Wavelength Conversion

The transmitting medium shows nonlinearity behaviours when two or more signals of different wavelengths travel through it. In this wavelength conversion technique, this nonlinearity property was invested to change the wavelengths of optical signals. Two types of nonlinearity can help in converting the wavelength of a desired optical signal. These types are discussed below.

3.10.2.1 Four-Wave Mixing (FWM)

Wavelength conversion happens when three optical signals of distinct wavelengths interact in a WDM fibre. Suppose that a WDM fibre carries three optical signals of frequenciesf_i, f_j and f_k. Due to the nonlinearity properties of the optical fibre, a fourth signal with frequency f_{ijk} is generated. The frequency of this generated signal is given by equation (3.7).

$$f_{ijk}= f_i + f_j - f_k \qquad (3.7)$$

FWM can also be obtained on semiconductor waveguides or Semiconductor Optical Amplifiers (SOA). This wavelength conversion method offers conversion of high bit rate signals' wavelength.

3.10.2.2 Difference Frequency Generation (DFG)

This conversion happens as a consequence to two different wavelength signals travelling across a non-linear medium. Most of the wavelength conversion techniques add spontaneous emission noise to the signal therefore they offer limited transparency. DFG on the other hand, presents a wavelength conversion of full transparency with no excess noise [71]. However, this method also has its own limitations, such as the low efficiency and the high polarization sensitivities. Other limitations consist of the difficulty in matching the phases of the interacting waves, which is a crucial condition in this conversion, and the difficulty in fabricating low loss waveguides, which is necessary for high conversion efficiency [51].

3.10.3 Cross Modulation based Wavelength Conversion

These wavelength conversion methods belong to a class called optical-gating wavelength conversion. These techniques use active semiconductor optical devices such as Semiconductor Optical Amplifiers (SOAs) in order to achieve the wavelength conversion.

Figure 3.17 shows a cross modulation based wavelength converter that uses SOA. The intensity modulated input signal modulates the gain of the SOA, which in turn modulates the phase of the Control Wave (CW), which has a wavelength equal to the desired wavelength of the output frequency. As a result the output signal will have a frequency as desired; meanwhile it carries information of the original input signal information modulated within it.

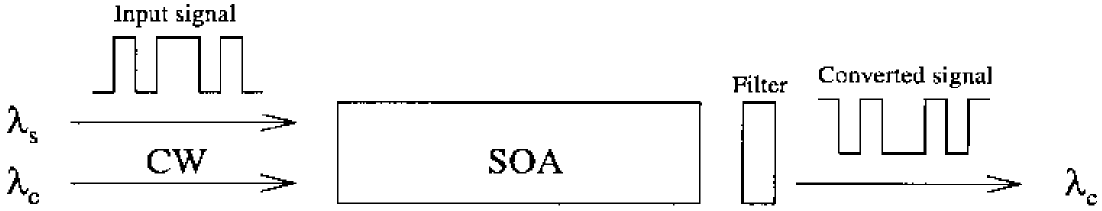


Figure 3.17 Wavelength Conversion Using SOA [51]

3.11 Wavelength Conversion Switches

A switch is called Wavelength Conversion Switch (WCS) if it has the capability of changing the wavelength of the incoming signal. A WCS may be supplied with a standalone Wavelength Converter (WC) for each individual inbound wavelength within the switch as shown in Figure 3.18. In some situations, not all the wavelengths need a wavelength conversion since the wavelengths of some signals on the inbound fibre are still available on the outbound fibre. In order to cut costs, not all the different wavelengths are supplied with WCs, but instead there are a few publicly used WCs which are shared among the different wavelengths.

However, in the shared wavelength converters switches, the converters can be collected in a converter bank, which can be accessed by any inbound wavelength as shown in Figure 3.19 (a). A converter bank is a collection of wavelength converters with identical characteristics. Each of these converters has the capability of changing any incoming wavelength. Only those wavelengths that need to be converted are sent to the converter bank. The outputs of the converter bank are connected to an optical switch to select the appropriate outbound fibre. Figure 3.19 (b) shows the architecture of the wavelength converter's switches where each outbound fibre has its own shared WCs which are only accessible by those wavelengths that are going to be multiplexed on this outbound fibre.

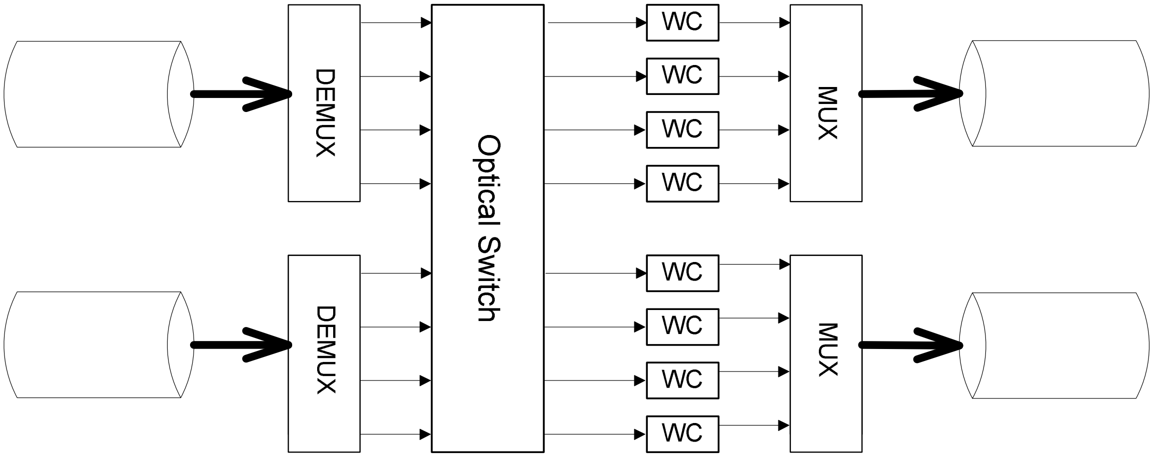


Figure 3.18 A Wavelength Conversion Switch with a Standalone Wavelength Converter for Each Individual Inbound Wavelength [51]

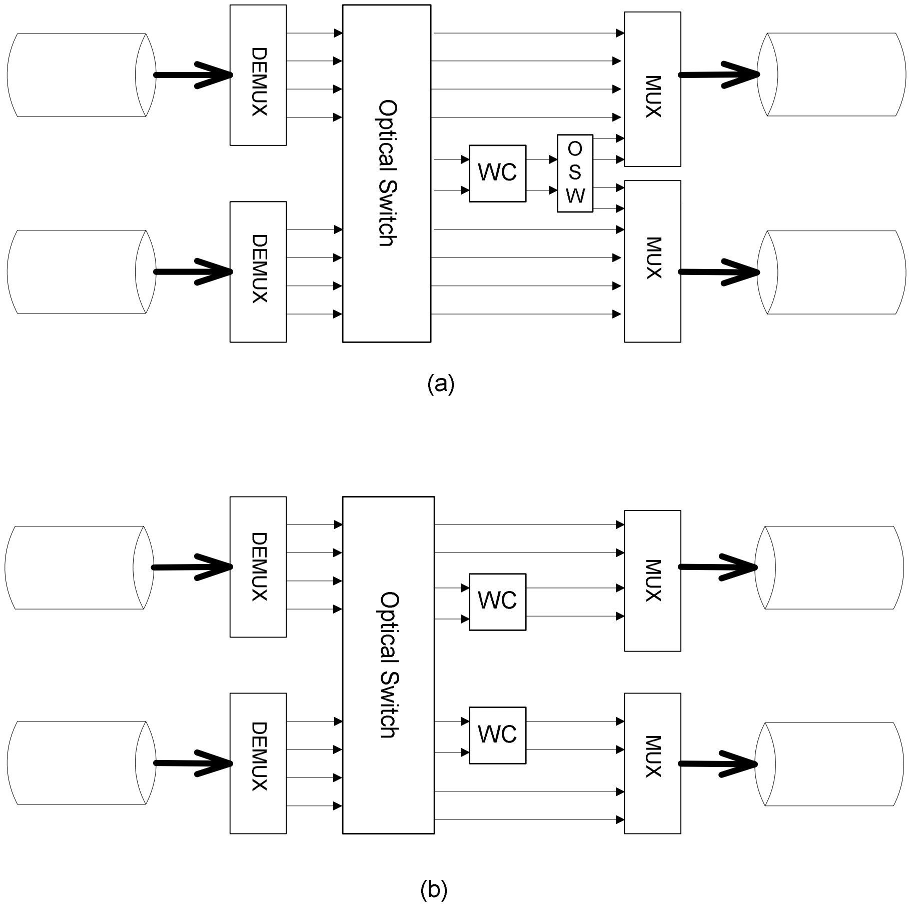


Figure 3.19 A Wavelength Conversion Switch with Shared Wavelength Converters [51]

3.12 Summary

In this chapter, optical cable types and characteristics were briefly reviewed. The basic principles of transmission of light through these cables were also studied. Attenuation, dispersion and other problems that may face signals as they travel through the optical fibres were discussed. Furthermore, WDM benefits in optical transmission were highlighted, and the optical components used to support WDM were explained. Finally, the different techniques of wavelength conversion, as an efficient approach to reduce the number of blocking events, were described in this chapter.

Chapter 4

Dimensioning the Flow over the Basra Optical Network under Different Quality of Experience Scenarios

In order to plan for 21st century's broadband communication networks with the increasing number of users who are using such a communication, together with the fast enhancements to the software specifications of applications transmitted over broadband communication networks [51-55], an easily changeable, scalable and hierarchical OMNeT++ model was developed. This model has been used to create a flow model representing the teletraffic within the Basra national optical network. This model was tested and is reported in this chapter for different possible use case scenarios of applications qualities. Analysis was performed based on the number of people within each sector in addition to the percentage of people using each sort of application and their flows over that network aiming to obtain an insight about the distribution of flow on the different network's links, the contribution of each application to the total throughput of the links, and the hourly variation of bit rates on the various network's links.

-What's new: In this chapter, Network's loading change due to the potential future improvements in the quality of experience offered to the end-users was investigated.

4.1 Introduction

Optical cables were found to provide a high communications speed to satisfy the dramatically increasing demands on a better quality of experience [72]. This prospective development in the quality of experience, such as using HDTV format for IPTV and video communications, calls for a scalable simulation platform, such as OMNet++, in order to easily plan for these imminent application deployments.

Planning for this optical fibre network requires designing a flow model to simulate such a network in order to keep track of the traffic over the various network's links and to postulate "what if" scenarios such as increased demand, increased types of services, increased quality/resolution of media, structuring of service positioning servers, link breakages, additional links, co-working with cellular, microwave, broadcast and satellite networks. The quality of the simulation results is highly dependent on the characterization of user behaviours e.g. how many times an application is used each day and how often, regional based behavioural patterns, such as which applications are used in city, town and rural areas.

Consequently, this can help to choose an appropriate link capacity for each optical fibre connection given current user behaviours. Moreover, such a model will be helpful to predict where it is better to add or remove some links. This flow model has was designed and simulated in this work in order to have an idea about the distribution of flow on the different network's links and to investigate the effects of potential improvements in the applications quality on the traffic throughout the network. Although this model was applied to Iraqi optical network, it can be easily applied to any other network, whatever its topology.

4.2 Previous Work

In [73], Motorola Labs Network Research used an excel work sheet for modelling their small network. It was difficult to extend their network or to use more sophisticated scenarios due to the lack of scalability of the worksheet model. In [74], the problem of scalability was partially solved using MATLAB, which provides more flexibility in analysing the model and in showing the results. However, this approach was still not flexible enough, that we could include more RANs or consider more "What-If" scenarios, especially for different network configurations. In our research, OMNeT++ was used to provide a completely scalable platform that modelled the flow of communication traffic in Basra using the already existing optical network backbone.

The OMNeT++ model developed in this chapter serves as an excellent tool for dimensioning the flow traffic on the any optical network, monitoring the places of potential congestions on the different links, and testing the level of tolerance of such a network when the quality of information transmitted through this network improves. This flow model of the network can then be used to make predictions of the demands on link loads given increasing sophistication of applications and number of users supported in the network.

4.3 Details of Modelling Approach

The open source network simulator OMNeT++ has been utilised in this chapter to create a flow model that is capable of dimensioning the traffic flow on any network. The model was designed in a way that it supports a high level of scalability through its validity to work on any sized network even in a continental scope. Another strength that this model inherits from the OMNeT++ simulator is the ease of implementing new ideas through a very easily modifiable software platform offered by OMNet++. Instead of providing the network resources as fixed unchangeable already built software parts, OMNeT++ offers a way to reconstruct these resources via changing the software in order to implement the entirely new ideas.

Our Traffic dimensioning model’s work is concisely described by calculating the average amount of traffic flow rate directed from each source node to each destination node. This amount of traffic is determined according to the expected user behaviour statistics for each kind of services offered to the user. These expectations of the users’ data consumption behaviour are based from statistical data collected from relevant research papers. The amount of expected traffic flow generated from each node will be mathematically described in section 4.7 (Traffic Flow Modelling).

In the model used in this chapter, traffics generated from source nodes are routed to their destinations using the well-known un-weighted Djikstra routing algorithm throughout the shortest available paths. In this routing algorithm links stayed un-weighted and the only factor that affects the routing decision is the path's total number of hops, where the path of the least number of hops will be selected to route the traffic corresponding to any *Origin-Destination* connection request. Traffics on the links due to different connection requests are then summed to estimate the total flow rate on the links.

What is missing in our model is the ability to determine the instantaneous variations of flow rates on the links, where this requires the simulation model to work in packet basis rather than in flow basis.

4.4 Network Modelling

Figure 4.1 below shows the map of the optical fibre cables installed in the region of Basra. This map was used to create an OMNeT++ model to simulate the southern region of Iraq, named Basra. The population of Basra is distributed according the statistics of United Nations Office for the Coordination of Humanitarian Affairs (OCHA) in [75]. Each city in Basra was represented by a node with a particular number of users according to [75] as shown in Table 4.1.

It was supposed that we have one server for this region located at Basra. In addition, links were considered to have infinite capacities in order to dimension the amount of bandwidth required for each link to accommodate all the traffic passing through it. The resulting network is illustrated as shown in Figure 4.1. Applications can be classified into two major types: Firstly, those applications that require data to be uploaded or downloaded to or from the server, e.g. web browsing, streaming audio, streaming video and IPTV; secondly, those applications that do not need a server contribution but communicate between two parties such as VoIP, video communication, interactive gaming, P2P file sharing and other miscellaneous audio clips up/downloads and other miscellaneous video clips up/downloads. In this chapter, OMNeT++ was utilised to provide a completely scalable platform for flow modelling the network in the southern region of Iraq using the already existing optical network backbone so that it could be used to help plan the architecture of Iraq's future optical fibre network. It should be mentioned here, that every node in our model represents a Regional Area Network (RAN); therefore, it is not a single computer, but it is instead a number of computers connected together as a network and has a particular Number Of Users (NOU).

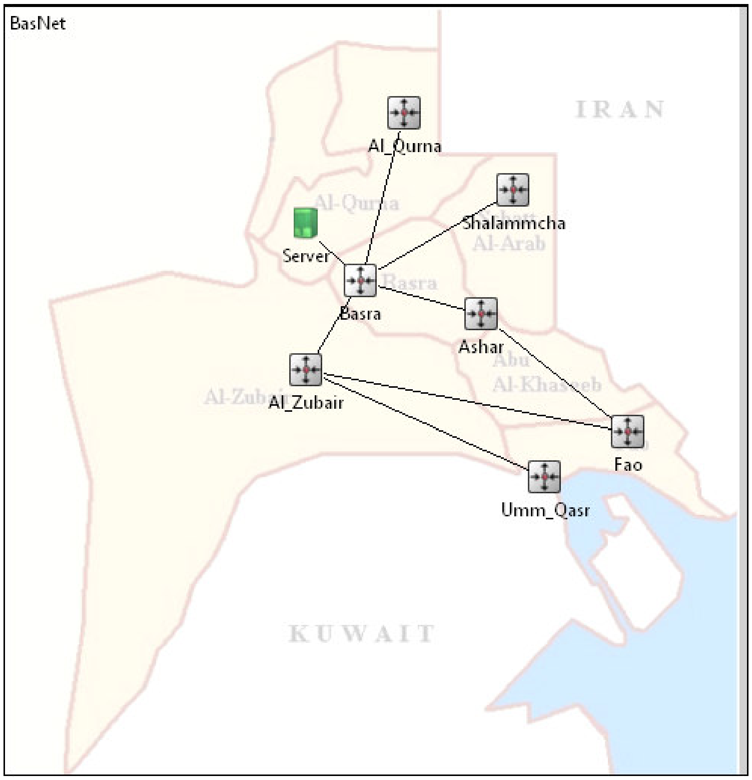


Figure 4.1 Basra's Optical Network

Table 4.1 Number of Users of the Different Sectors of Basra

City	**Number of Users (NOU)**
Basra	475827
Ashar	475827
Al_Zubair	320523
Shalamcha	104089
Umm_Qasr	9445
Fao	9445
Al_Qurna	13237

4.5 Application Modelling

Ten application types were used here, to investigate the effect of each individual type on the traffic over our model. These applications are the followings:

1- Web Browsing: This is the most commonly used service on the Internet nowadays. Results show that the throughput generated due to this application is most congested on the link from the node "Basra" to the node "Server", this is because of two major facts: firstly, the node " Basra" serves as the only connector to the server, secondly, this type of application request uploading data from the sending node to the server and downloading from the server to the communicating node.

2- Streaming Audio: In this type of application, nodes only receive data from the server, and do not upload anything. This happens when a user uses Internet to hear online news. The flow rate for these sorts of applications depends on the format of these audio streams which governs the quality of the sound.

3- Streaming Video: It is also one of the most commonly used applications over the Internet [76]. Again, the flow rate depends on the video format being used. Improving the quality of the video requires more capacity of the Internet to keep up with increasing sizes of image formats. This type of application also needs a server contribution with zero upload, since nodes download from server only.

4- IPTV: Watching TV over the Internet is becoming more pervasive these days, but it is still less popular than streaming video [74]. Different video qualities were implemented in this research. In IPTV the communicating nodes download data from the server with no need to upload.

5- VoIP: Voice-over-IP application does not need a server contribution, since the two communicating parties exchange data directly without passing these data through the server. This type of application causes no traffic over the link from node "Basra" to node "Server". VoIP nowadays outweighs the use of classical phones [77]. An example of peer-to-peer VoIP applications is the Skype. Toll quality voice codec was used here.

6- Video Communication: The real time video communication is not as popular as other applications over the Internet, where a percentage of 5% of users use this kind of application when they participate in PC-based video calling or when they open their webcam for chatting [74, 78]. The higher the video quality used the more the busy hour bit rate over the links due to this application. Web quality video format was used here in the broadband applications' quality scenario.

7- Interactive Gaming: This type of applications contributes significantly to today's overall Internet traffic [79]. It is reported in [80] that 3-4% of the overall Internet traffic is associated with only 6 popular games. The problem with these sorts of applications is the difficulty to predict the traffic pattern caused by such an application, since each game represents a standalone application itself [81]. In general games can be divided into two types: slower-paced games such as adventure games, and faster-paced gamed such as the racing games which produces heavier traffic and the latter was considered in this chapter.

8- P2P File Sharing: Supposing that we have N communicating entities sharing the file, then each entity has to send the file to be shared to N-1 other entities (N was assumed to equal 5 in this chapter). For this reason this application produces heavy traffic over the network. The greatest contributing factor to this heavy traffic is the Bit Torrent application, which represents about 60% of the total P2P traffic [82].

9- Miscellaneous audio upload/download: This includes the other uploaded and downloaded audio clips.

10- Miscellaneous video upload/download: This type includes the other uploaded and downloaded audio clips.

4.6 Applications' Quality Scenarios

Applications' quality and media resolutions have a great effect on the amount of traffic flow passing through the network's links. According to [73] and [74], four scenarios have been studied in this chapter to show the contributions of each application type to the overall network traffic. These four scenarios are: Residential Broadband Scenario, Improved Media Resolution Scenario, Maximum Media Resolution Scenario, 3D Web Browsing and Video Contents. All the statistics of applications’ usages in Tables 4.2 through 4.5 were driven from [73] and [74].

4.6.1 Residential Broadband Scenario

In this use case scenario, 2D web browsing was used, Toll format was utilised for streaming audio, Web quality resolution was used for streaming video, video communications and for the other miscellaneous video clips. In addition, IPTV was represented by SDTV format, and Toll quality used for VoIP and the miscellaneous audio clips.

Table 4.2 Residential Broadband Scenario

Application Type	Quality	Packet payload Size (Byte)	Packet Overhead size (Bytes)	Packet Inter-arrival Time (sec)	Sessions / Day	% of Users with Application	Total Load per User per Day (Mbytes)	Peak Hour %	Traffic Asymmetry (%) (upload/download)	Average per user Busy Hour Rate Download / upload (bits/sec)
Web Browsing	2D	489350	40		2.5	75.0	15.599	7.9	10.1	2462 / 277
Streaming Audio	Web Quality	65	40	0.026	1.5	25.0	0.454	2.4	0	24 / 0
Streaming Video	Web Quality	20000	400	0.48	1.0	50.0	6.375	6.1	0	864 / 0
IPTV	SDTV	90000	2400	0.48	1.0	0.50	2.888	9.4	0	60 / 0
VoIP	Toll Quality	160	40	0.02	2.0	15.0	0.630	5.7	50.0	40 / 40
Video Comm.	Web Quality	20000	400	0.48	0.5	5.0	0.319	7.7	50.0	27 / 27
Interactive Gaming	Interactive Gaming	83	767	0.4	1.0	33.0	2.525	6.25	46.4	188 / 163
P2P File Sharing	P2P File Sharing	16380	470		0.14	5.0	11.500	5.3	83.6	222 / 1132
Misc. Audio	Web Quality	65	40	0.026	2,0	50.0	1.211	7.9	10.4	191 / 22
Misc. Video	Web Quality	20000	400	0.48	0.07	50.0	5.355	7.9	10.4	842 / 98
Total										4921 / 1759

4.6.2 Improved Media Resolution Scenario

In this scenario the resolutions of media files or frames were increased by upgrading, where streaming video, video communications, and other miscellaneous video clips were encoded by SDTV format instead of web quality. Furthermore, VoIP format was upgraded from Toll quality to MP3.

Table 4.3 Improved Media Resolution Scenario

Application Type	Quality	Packet payload Size (Byte)	Packet Overhead size (Bytes)	Packet Inter-arrival Time (sec)	Sessions / Day	% of Users with Application	Total Load per User per Day (Mbytes)	Peak Hour %	Traffic Asymmetry (%) (upload/download)	Average per user Busy Hour Rate Download / upload (bits/sec)
Web Browsing	2D	489350	40		2.5	75.0	15.599	7.9	10.1	2462 / 277
Streaming Audio	Web Quality	65	40	0.026	1.5	25.0	0.454	2.4	0	24 / 0
Streaming Video	SDTV	90000	2400	0.48	1.0	50.0	28.875	6.1	0	3914 / 0
IPTV	SDTV	90000	2400	0.48	1.0	0.50	2.888	9.4	0	60 / 0
VoIP	MP3	418	40	0.026	2.0	15.0	1.110	5.7	50.0	70 / 70
Video Comm.	SDTV	90000	2400	0.48	0.5	5.0	1.444	7.7	50.0	124 /124
Interactive Gaming	Interactive Gaming	83	767	0.4	1.0	33.0	2.525	6.25	46.4	188 / 163
P2P File Sharing	P2P File Sharing	16380	470		0.14	5.0	11.500	5.3	83.6	222 / 1132
Misc. Audio	MP3	65	40	0.026	2,0	50.0	5.285	7.9	10.4	831 / 97
Misc. Video	SDTV	90000	2400	0.48	0.07	50.0	24.255	7.9	10.4	3815 / 443
Total										15833 / 2305

4.6.3 Maximum Media Resolution Scenario

The resolution of all the video information was improved in this scenario to HD format, whereas all the audio contents were encoded by 5.1 surround sound format to improve their quality.

Table 4.4 Maximum Media Resolution Scenario

Application Type	Quality	Packet payload Size (Byte)	Packet Overhead size (Bytes)	Packet Inter-arrival Time (sec)	Sessions / Day	% of Users with Application	Total Load per User per Day (Mbytes)	Peak Hour %	Traffic Asymmetry (%) (upload/download)	Average per user Busy Hour Rate Download / upload (bits/sec)
Web Browsing	2D	489350	40		2.5	75.0	15.599	7.9	10.1	2462 / 277
Streaming Audio	5.1 Surround	1792	88	0.032	1.5	25.0	6.609	2.4	0	353 / 0
Streaming Video	HDTV	480000	12000	0.48	1.0	50.0	153.75	6.1	0	20842 / 0
IPTV	HDTV	90000	2400	0.48	1.0	0.50	18.45	9.4	0	3854 / 0
VoIP	5.1 Surround	1792	88	0.032	2.0	15.0	3.701	5.7	50.0	234 / 234
Video Comm.	HDTV	480000	12000	0.48	0.5	5.0	7.688	7.7	50.0	658 / 658
Interactive Gaming	Interactive Gaming	83	767	0.4	1.0	33.0	2.525	6.25	46.4	188 / 163
P2P File Sharing	P2P File Sharing	16380	470		0.14	5.0	11.500	5.3	83.6	222 / 1132
Misc. Audio	5.1 Surround	1792	88	0.032	2,0	50.0	17.652	7.9	10.4	2772 / 322
Misc. Video	HDTV	480000	12000	0.48	0.07	50.0	1291.5	7.9	10.4	20315 / 2358
Total										51900 / 5144

4.6.4 3D Web Browsing and Video Contents

In this scenario, the web browsing, streaming video, IPTV, video communications, and other miscellaneous video clips have been upgraded from 2D to 3D. Other applications remain the same as in the third scenario.

Table 4.5 3D Web Browsing and Video Contents

Application Type	Quality	Packet payload Size (Byte)	Packet Overhead size (Bytes)	Packet Inter-arrival Time (sec)	Sessions / Day	% of Users with Application	Total Load per User per Day (Mbytes)	Peak Hour %	Traffic Asymmetry (%) (upload/download)	Average per user Busy Hour Rate Download / upload (bits/sec)
Web Browsing	3D	665820	40		2.5	75.0	21.224	7.9	10.1	3350 / 376
Streaming Audio	5.1 Surround	1792	88	0.032	1.5	25.0	6.609	2.4	0	353 / 0
Streaming Video	3D + HDTV	9953280	12000	0.48	1.0	50.0	3114.150	6.1	0	422140 / 0
IPTV	3D + HDTV	9953280	12000	0.48	1.0	0.50	373.698	9.4	0	78061 / 0
VoIP	5.1 Surround	160	40	0.02	2.0	15.0	3.701	5.7	50.0	234 / 234
Video Comm.	3D + HDTV	9953280	12000	0.48	0.5	5.0	155.708	7.7	50.0	13322 / 13322
Interactive Gaming	Interactive Gaming	83	767	0.4	1.0	33.0	2.525	6.25	46.4	188 / 163
P2P File Sharing	P2P File Sharing	16380	470		0.14	5.0	11.500	5.3	83.6	222 / 1132
Misc. Audio	5.1 Surround	65	40	0.026	2,0	50.0	17.652	7.9	10.4	2772 / 322
Misc. Video	3D + HDTV	9953280	12000	0.48	0.07	50.0	2615.89	7.9	10.4	411473 / 47760
Total										932116 / 63310

4.7 Traffic Flow Modelling

The different traffics flow through the network as flow batches, where each batch is identified by three fields, namely, the source address, the destination address and the type of application that generated this traffic. In order to determine the distribution of the flow traffic generated by the different applications on the various network's links, the amount of traffic due to each application, which is directed from each possible source to each possible destination, has been calculated using the statistics of user behaviour and applications' specifications defined in Tables 4.1 through 4.5. This is highly dependent on the applications' qualities scenario being used.

The total traffic generated from a source node A and directed to a particular destination B is estimated as follows:

The total packet size PSZ_{Total} is calculated using equation (4.1).

$$PSZ_{Total}= PSZ_{Payload}+ PSZ_{Overhead}\ldots\ldots\ldots\ldots \text{(4.1)}$$

where $PSZ_{Payload}$ is the size of the payload within the packet, and $PSZ_{Overhead}$ is the size of packet's overhead.

The number of packets per session due to one user (PPS_{User}), and the number of packets per day due to one user (PPD_{User}) can be calculated by equations (4.2) and (4.3) respectively.

$$PPS_{User} = \frac{Session\ Time}{Packet\ Interarrival\ Time} \ldots\ldots\ldots\ldots\ldots\ldots \text{(4.2)}$$

Note that the number of packets per session for web browsing applications is 17 [74].

$$PPD_{User} = \quad PPS_{User} \times Sessions\ Per\ Day\ldots\ldots \text{(4.3)}$$

Thus, the total load generated by the NOU_A users of node A per whole day due to a particular application (denoted by $Load_A$) is given by equation (4.4)

$$Load_A \text{ (measured in Bytes)} = PPD_{User} \times NOU_A \times \% \, Users \times PSZ_{Total} \; \ldots.. \; (4.4)$$

where $\% \, Users$ is the average percentage of users who are using this application (this is to be taken from Tables 4.2-4.5).

The total bytes per day generated by node A and directed towards the destination node B is denoted as (LD_{A-B}) and to be estimated by equation (4.5).

$$LD_{A-B} = Load_A \times \frac{NOU_B}{NOU_{Total}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \; (4.5)$$

where NOU_B is the number of users of node B and NOU_{Total} is the total number of users of the whole network.

Finally, the average busy hour load rate (bandwidth) for the traffic from node A to node B $(LDR_{BusyHour})$ measured in bits/sec is to be determined by equation (4.6).

$$LDR_{BusyHour} = \frac{LD_{A-B} \times 8 \times \%BH}{3600} \ldots\ldots\ldots\ldots\ldots\ldots... \; (4.6)$$

Where %BH is the average percentage of the per day load traffic generated at the busy hour (to be taken from Table 2-5).

4.8 The Hourly Usage of Applications

Equations in section 4.7 can be used to determine the average throughput of the different applications on the various network's links at busy hour. The variation of this traffic throughout the whole day requires more knowledge about the per-hour usage of these different application types. Table 4.6 shows the hourly percentage of load generated due to each application with respect to the whole day amount of load as extracted from [83].

4.9 Results and Discussion

This section records the flow distribution on the most congested links of the network shown in Figure 4.1. It also shows the contribution of the different application types to the total links' throughputs. Furthermore, the per hour distribution of the flow generated due to each type of applications, and the hourly total flow on these congested links are presented. Since four applications' quality scenarios have been used, this section will be partitioned into four sub-sections. Each sub-section will be concerned with one scenario. Note that the load rates due to the different applications types on each link has been represented in this section by a vector of 10 elements, each element represents the load rate due to a particular application type. The ten applications types were numbered from 0 to 9 corresponding to web browsing, streaming audio, streaming video, IPTV, VoIP, video communications, interactive gaming, P2P file sharing, other miscellaneous audio clips up/downloading, and other miscellaneous video clips up/downloading. Therefore, the load rate of link x to y due to IPTV as an example, will be represented in the figures through these sections as load rate vector on link from x to y due to application [3].

Table 4.6 Hourly Distribution of Applications' % Load during the Whole Day

Time Applic.	**01:00**	**02:00**	**03:00**	**04:00**	**05.00**	**06:00**	**07:00**	**08:00**	**09:00**	**10:00**	**11:00**	**12:00**	**13:00**	**14:00**	**15:00**	**16:00**	**17:00**	**18:00**	**19:00**	**20:00**	**21:00**	**22:00**	**23:00**	**00:00**
Web	5.7	4.2	1.9	2.2	1.3	0.6	1.2	2.7	4.2	7.2	6.1	4.8	6.0	4.2	4.3	4.6	4.0	1.6	4.2	7.9	4.5	4.8	6.1	5.2
Str. Audio	2.2	1.2	0.7	0.4	2.1	5.8	8.6	9.6	10.8	9.4	5.8	4.4	5.0	4.4	3.5	4.4	4.9	4.4	3.1	2.4	2.1	1.7	1.7	1.4
Str. Video	6.8	5.6	4.7	2.6	1.0	0.8	0.7	1.0	1.5	1.9	2.5	3.1	3.7	4.3	4.3	4.3	4.8	6.8	5.3	6.1	6.4	7.0	8.2	6.8
IPTV	2.2	1.2	0.7	0.4	0.3	0.7	1.4	2.3	2.6	2.7	2.7	3.1	3.3	3.4	3.4	4.4	5.7	7.6	8.5	9.4	6	6	8.3	4.4
VoIP	0.7	0.2	0.2	0.1	0.1	0.4	0.7	1.6	2.7	5.1	7.7	8.5	8.5	8.0	7.6	6.6	6.0	5.7	5.5	5.7	6.0	6.2	4.7	1.6
Vid. Comm.	2.0	0.9	0.5	0.4	0.4	0.5	0.6	1.0	1.5	2.7	4.0	5.0	5.5	5.6	5.8	6.0	6.1	6.5	6.9	7.7	8.5	9.2	8.0	4.5
Gamin g	3.13	3.13	3.13	3.13	3.13	3.13	3.13	3.13	3.13	3.13	3.13	3.13	5.21	5.21	5.21	5.21	6.25	6.25	6.25	6.25	4.17	4.17	4.17	4.17
P2P	3.0	3.4	3.2	2.7	2.7	2.6	2.5	2.8	3.3	3.6	4.1	4.7	4.9	4.9	5.3	4.9	4.1	4.9	4.9	5.3	5.9	6.1	5.6	4.5
Misc. Aud.	5.7	4.2	1.9	2.2	1.3	0.6	1.2	2.7	4.2	7.2	6.1	4.8	6.0	4.2	4.3	4.6	4.0	1.6	4.2	7.9	4.5	4.8	6.1	5.2
Misc. Vid.	6.8	11.7	10.0	7.8	9.8	6.8	7.1	7.6	2.7	1.5	2.2	1.0	2.0	2.7	1.5	2.2	1.0	2.0	2.7	1.5	2.2	1.0	2.0	4.4

4.9.1 Results of Residential Broadband Scenario

This sub section shows the traffic distribution of the residential broadband applications' quality scenario. Figure 4.2 below represents the contribution of the traffic generated by each application type to the overall network's traffic. It is clear from this figure that P2P file sharing application generates more than half of the total network's traffic. Web browsing on the other hand, represents the second most throughput generating application. The dominance of P2P file sharing traffic is attributed to the high per user bit rate consumption of such applications (see Table 4.2), and the large number of entities sharing the files, where if a particular user demands a certain file, the file should be assembled from all the other users this file is partitioned and distributed among them. Consequently, extra traffic will be added to the network.

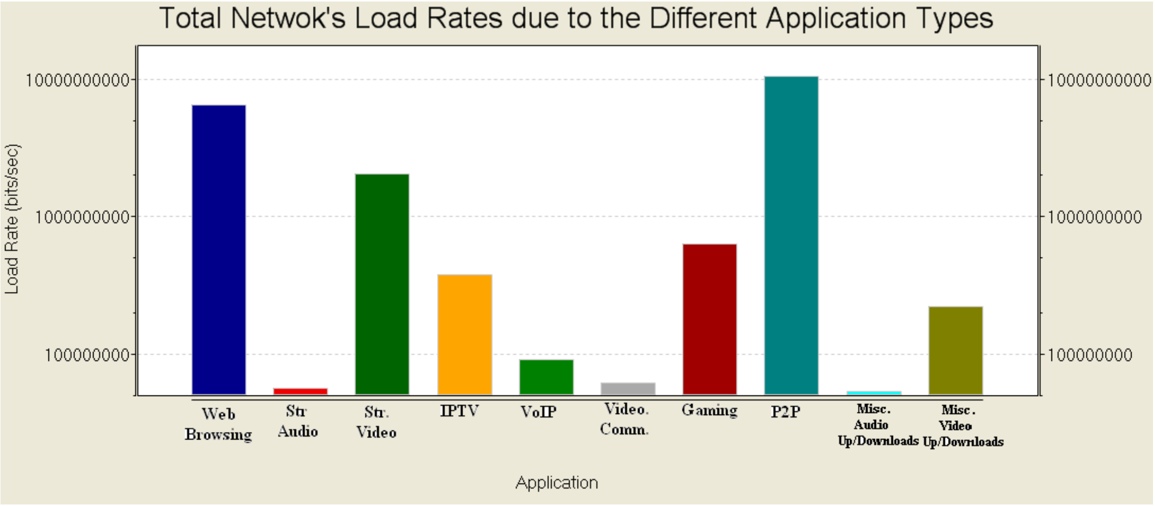


Figure 4.2 Total Network's Load Rate due to the Different Application Types

On the other hand, web browsing occupies the second rank in terms of bandwidth consumption because of the popularity of such applications, where about 75% users use this application at any particular time. This reason together with the high per user throughput generated by this applications type (see Table 4.2) makes web browsing the second dominant application in this scenario.

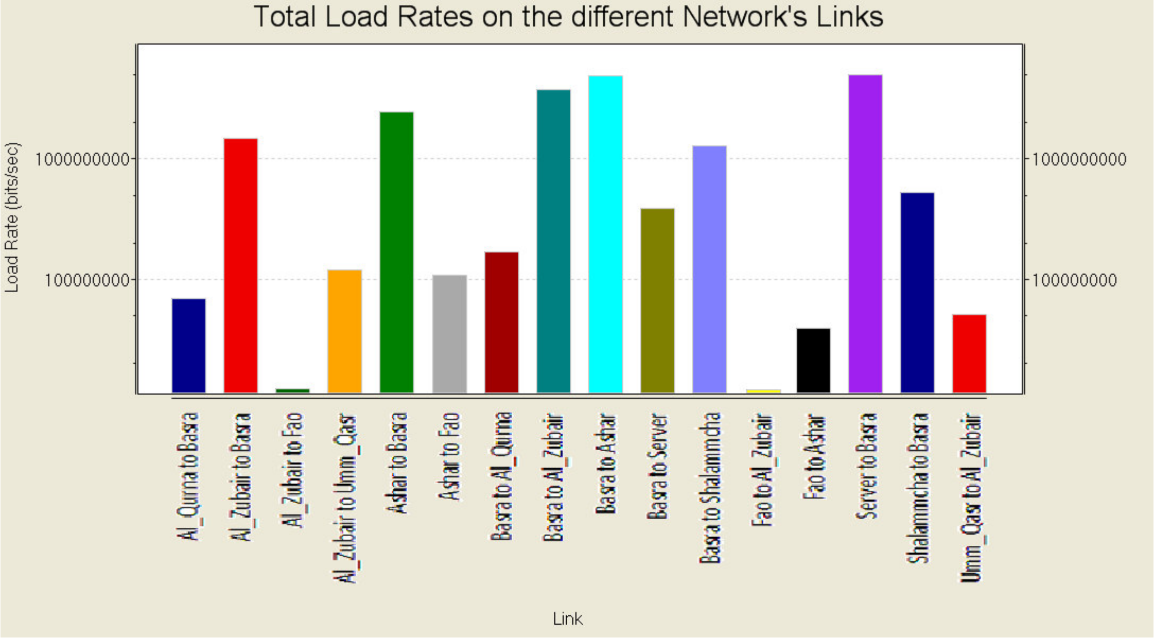


Figure 4.3 Total Load Rate on the Different Network's Links at Busy Hour

Figure 4.3 above represents the total throughputs on the various network's links at busy hour. It is clear that links [Basra-Ashar] and [Server-Basra] are the most congested links. The first link is congested because the source node (Basra) and the destination node (Ashar) have the highest populations among the network's nodes. The second link on the other hand (Server-Basra) is congested because this link serves as the only gateway for the bulky web browsing traffic to get downloaded to all the other network's nodes.

Figure 4.4 shows that P2P file sharing throughput at busy hour dominates the traffic over the link [Ashar-Basra] to the extent that the traffic generated by the other applications can be neglected compared to this application's traffic. A question may arise here, where the traffic of the competitive application (web browsing) has gone? The answer is obvious in Table 4.2 and the topology of the network shown in Figure 4.1 where this link holds only the upload component of the web browsing traffic to the server which has very a low per user busy hour bit rate as shown in Table 4.2. Note that no loads are transmitting on this link due to streaming audio, streaming video, and IPTV applications since these applications generate one way traffics from the server to the other nodes (opposite to this link's direction).

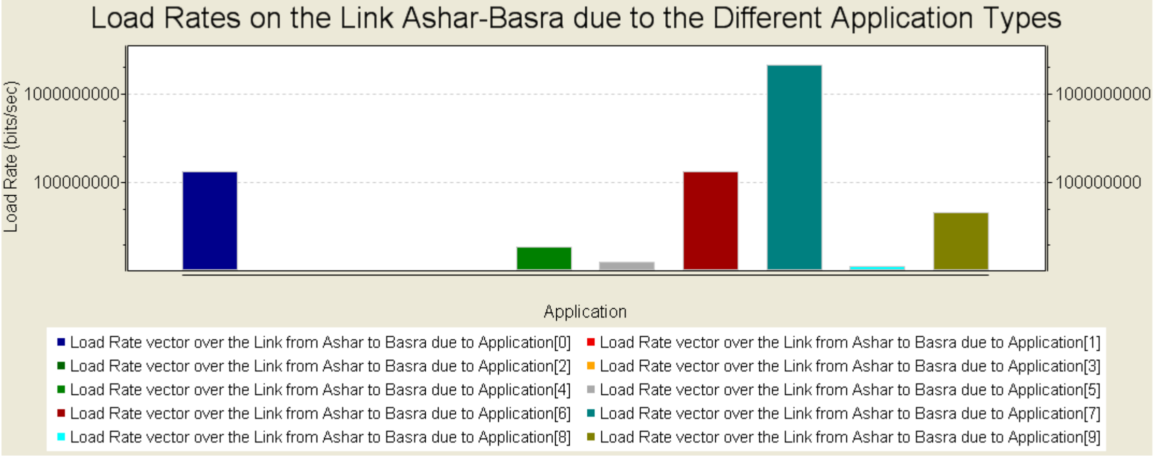


Figure 4.4 Busy Hour Load Rates on the Link Ashar-Basra due to the Different Application Types

The hourly distributions of flow due to the different application types together with the resulting total per hour flow (coloured red) are shown in Figure 4.5. It is obvious in this figure that the per-hour total rate on the link [Ashar-Basra] largely inherits the shape of P2P traffic's distribution since it is the only dominant application on this link.

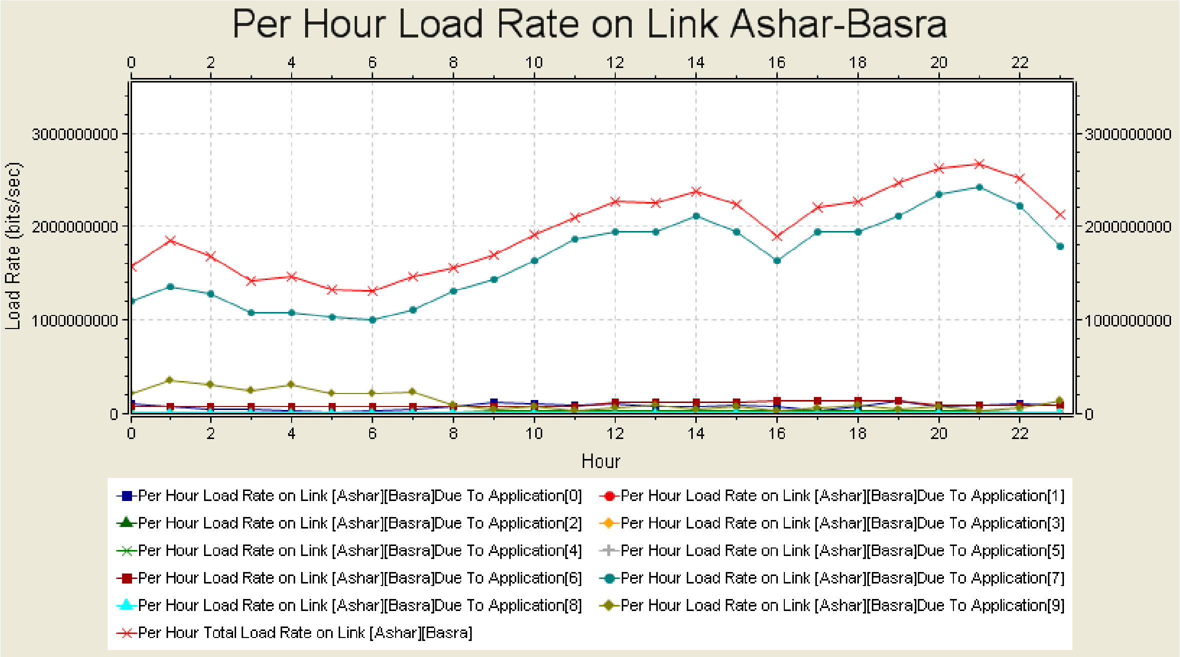


Figure 4.5 Per Hour Load Rate on Link Ashar-Basra

The busy hour bandwidth consumption contribution of the different applications' traffics on the two links [Basra-Ashar] and [Basra-Zubair] will include the bulky bandwidth consuming component of web browsing (download) causing the effect of the competitive application (web browsing) to reappear on the overall link's loading as shown in Figures 4.6 and 4.7 respectively.

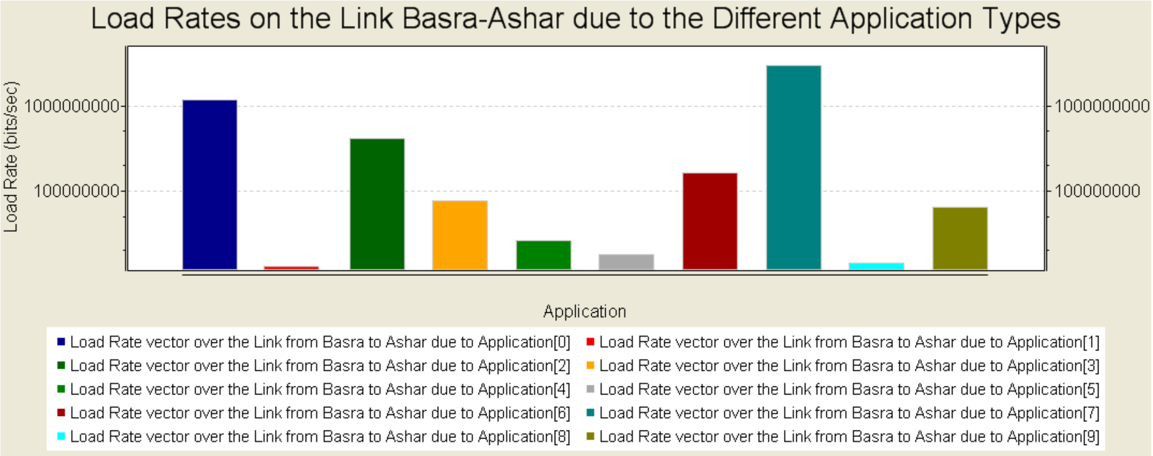


Figure 4.6 Busy Hour Load Rates on the Link Basra-Ashar due to the Different Application Types

Although the bandwidth consumed by the web browsing applications is substantial here on the links [Basra-Ashar] and [Basra-Zubair], the per hour total load rate distributions on these links shown in Figures 4.8 and 4.9 respectively is still dominated by the P2P file sharing since it generates much more throughput than the web browsing.

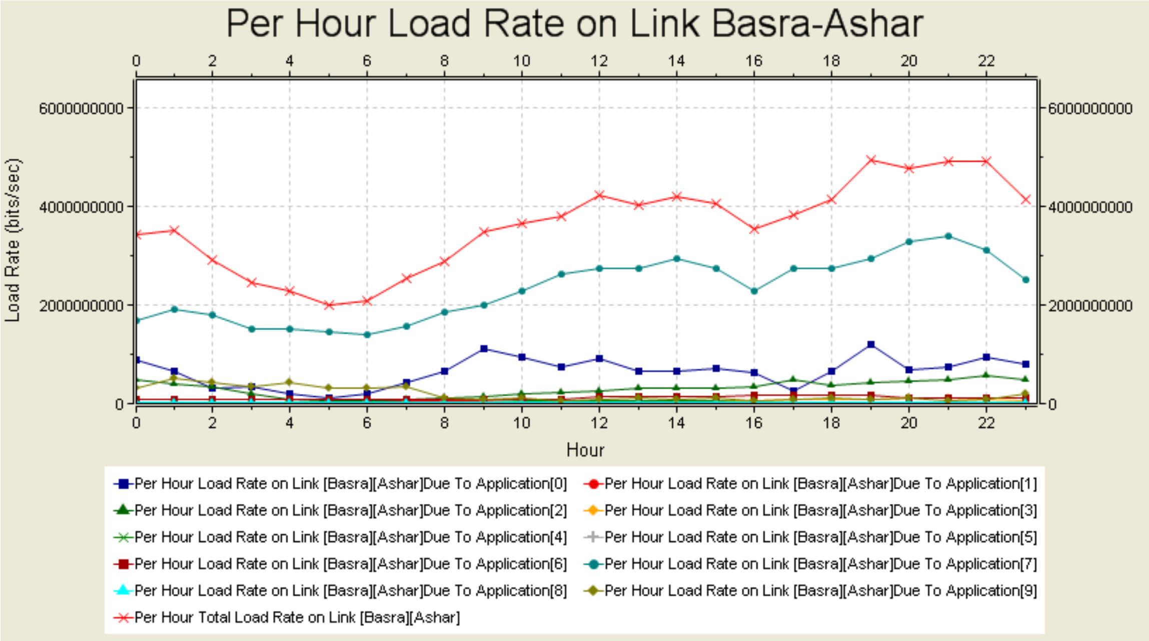


Figure 4.7 Per Hour Load Rate on Link Basra-Ashar

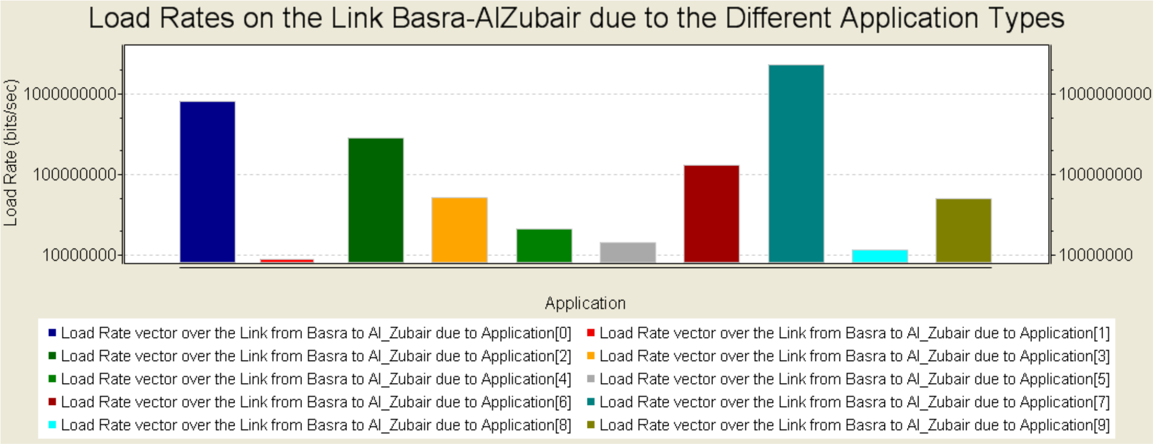


Figure 4.8 Busy Hour Load Rates on the Link Basra-AlZubair due to the Different Application Types

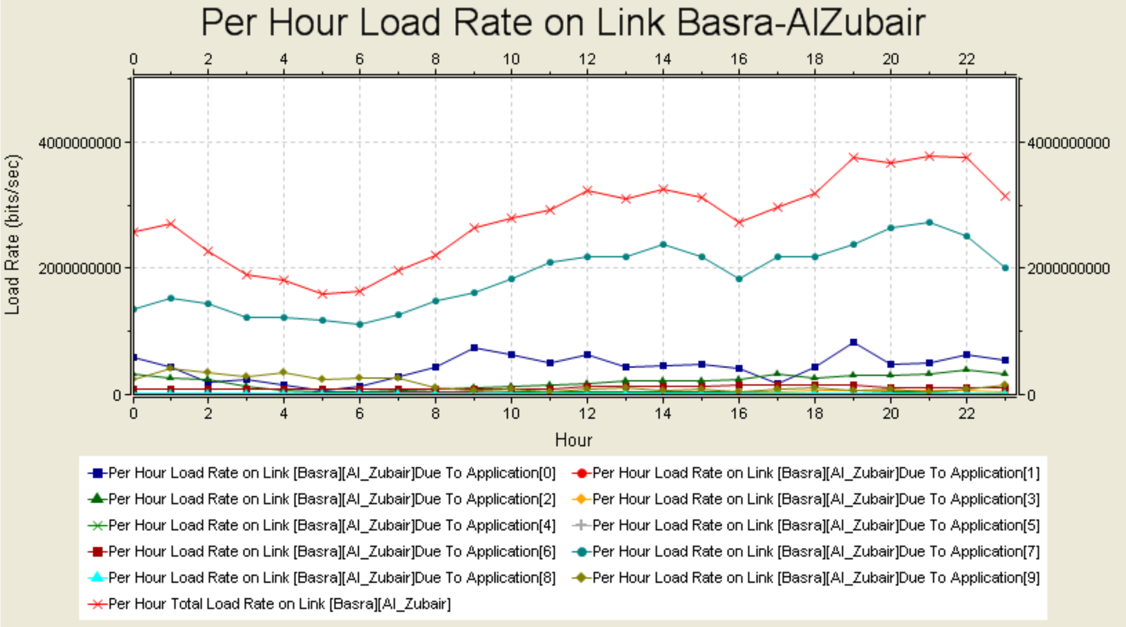


Figure 4.9 Per Hour Load Rate on Link Basra-Al-Zubair

The loading pattern on the link [Server-Basra] due to the various applications types shown in Figure 4.10 is different from the loading patterns of the other links since only four applications contribute to construct the download of the link. These four applications are those they send broadcasting data from the server to other nodes, i.e., web browsing streaming audio streaming video, and IPTV.

Other applications are characterised to be point to point based where they do not need to have their traffic sent/received to/from the server. In other words, they do not need server contribution in their communications. Therefore, they do not send traffic through this link.

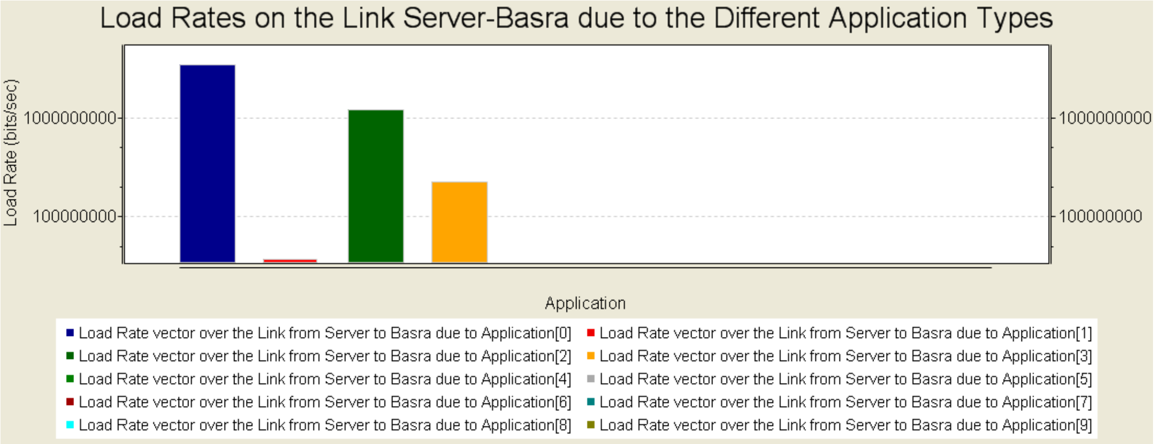


Figure 4.10 Busy Load Rates on the Link Server-Basra due to the Different Application Types

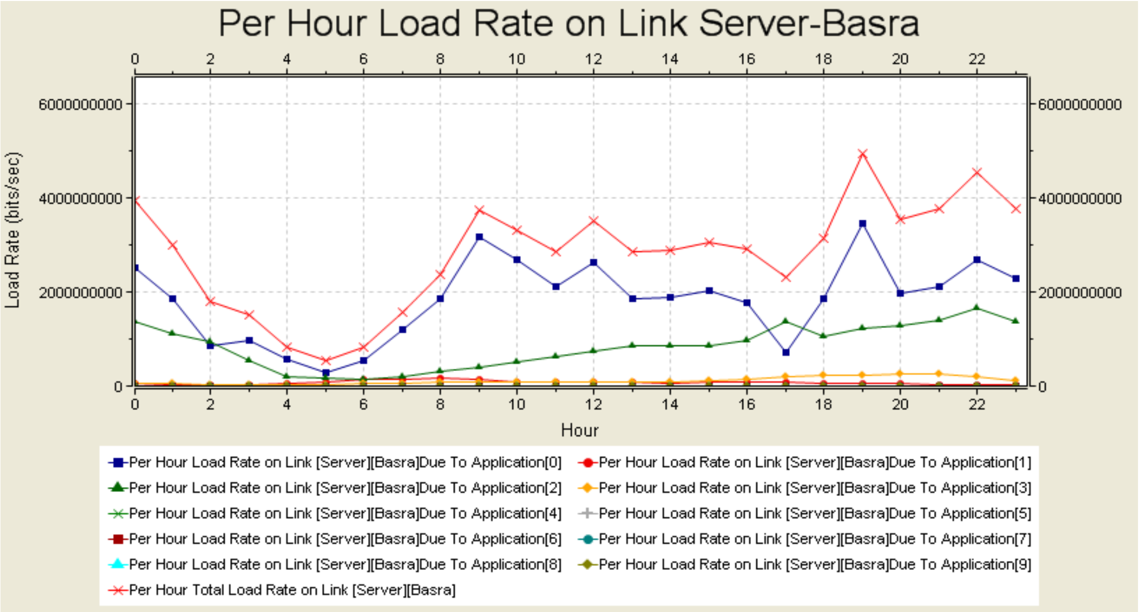


Figure 4.11 Per Hour Load Rate on Link Server-Basra

Since no P2P traffic exists on the link [Server-Basra], web browsing applications will play the role of the dominant applications type in terms of bandwidth consumption. As a result, the per hour total flow distribution will take the shape of web browsing per hour load distribution as shown in Figure 4.11.

4.9.2 Results of Improved Media Resolution Scenario

This sub-section shows the distribution of load rates on the most congested links and the bandwidth consumption of each traffic type when the media contents quality is improved in this scenario. Figure 4.12 shows the contribution of each traffic type to the overall network's traffic. It is clear from this figure that the traffic of streaming video has been substantially increased to add a second competitor to the P2P file sharing traffic. This dramatically increased bandwidth consumption of streaming video is attributed to the large improvement of the quality of information generated due to this applications type and the wide popularity of this application type compared to the other improved applications.

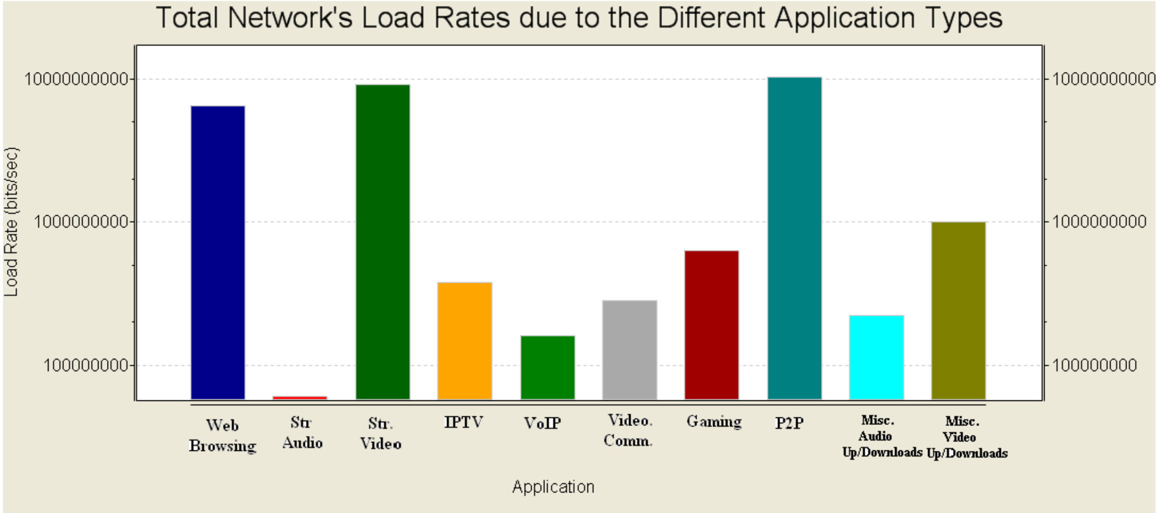


Figure 4.12 Total Network's Load Rate due to the Different Application Types

Figure 4.13 below shows the total load rates distribution of the different links calculated at busy hour. While the streaming video traffic has substantially increased, the percentage of P2P traffic contribution to the total network's traffic has decreased. Since the streaming video applications type is server-based, the traffic on the link [Server-Basra] increases due to the quality improvement of this application type.

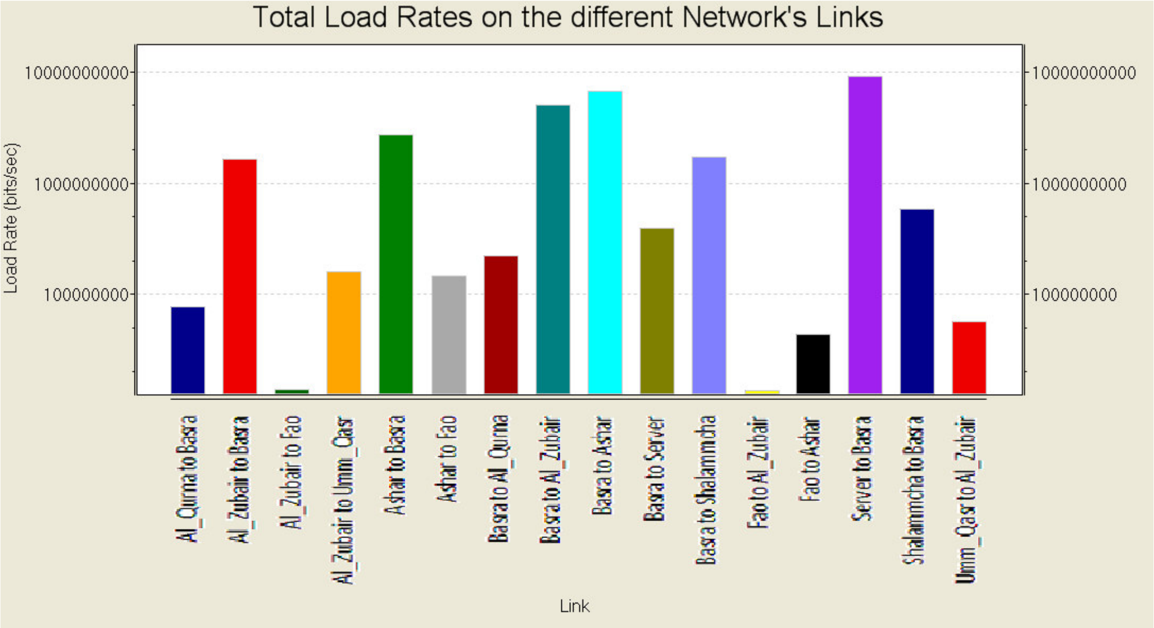


Figure 4.13 Total Busy Hour Load Rate on the Different Network's Links

Figure 4.14 shows the busy hour load rates of the different traffic types on the link [Server-Basra]. Note that in this scenario, the throughput has been dominated by streaming video applications rather than web browsing applications because of the dramatic improvement in streaming video quality.

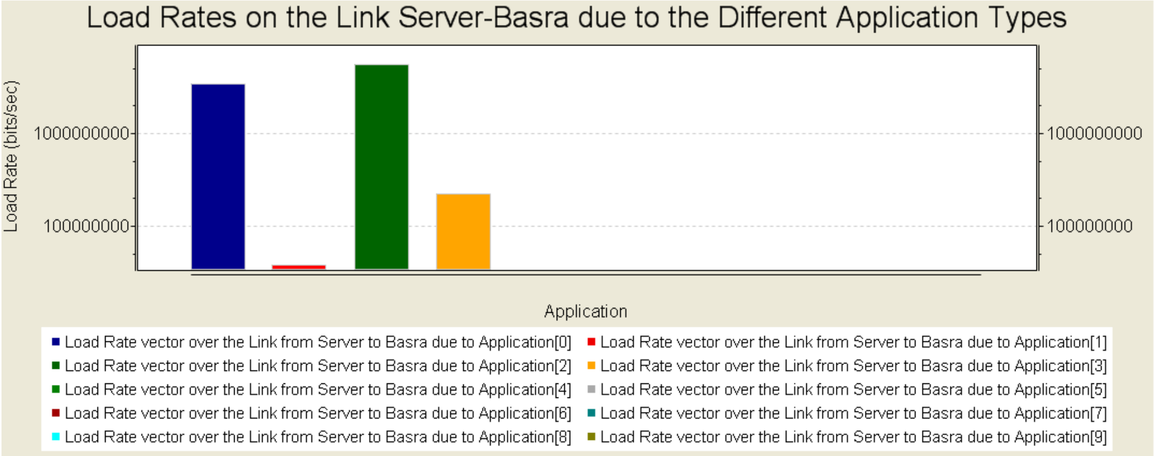


Figure 4.14 Busy Hour Load Rates on the Link Server-Basra due to the Different Application Types

As a result to the dominance of streaming video and web browsing applications on the link [Server-Basra] traffic, the total per hour link's load will be affected mainly by these applications as shown in Figure 4.15. Recall that there is no P2P file sharing traffic that exists on this link to affect the total per hour traffic distribution.

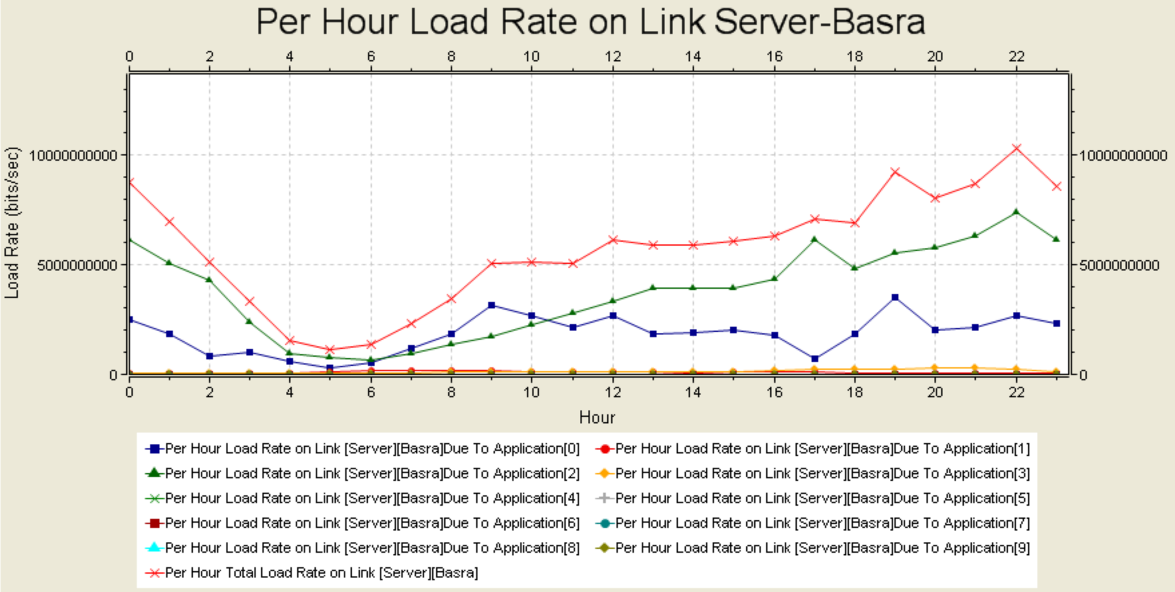


Figure 4.15 Per Hour Load Rate on Link Server-Basra

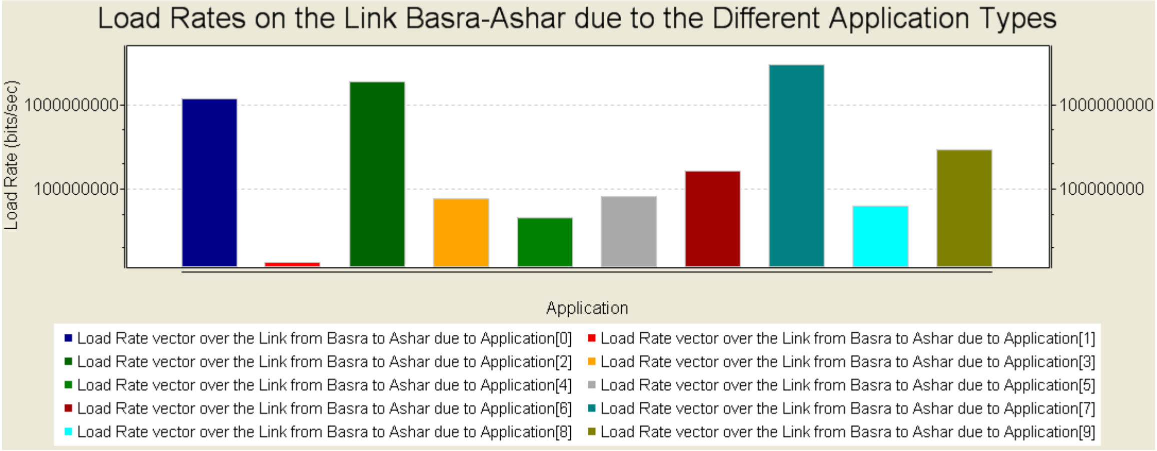


Figure 4.16 Busy Hour Load Rates on the Link Basra-Ashar due to the Different Application Types

With the existence of the dominant P2P file sharing traffic on the link [Basra-Ashar] at busy hour as shown in Figure 4.16, the hourly distribution of total traffic on this link takes a shape that comprises the traffic variations of the three dominant applications, i.e., P2P File sharing, streaming video, and web browsing applications as shown in Figure 4.17.

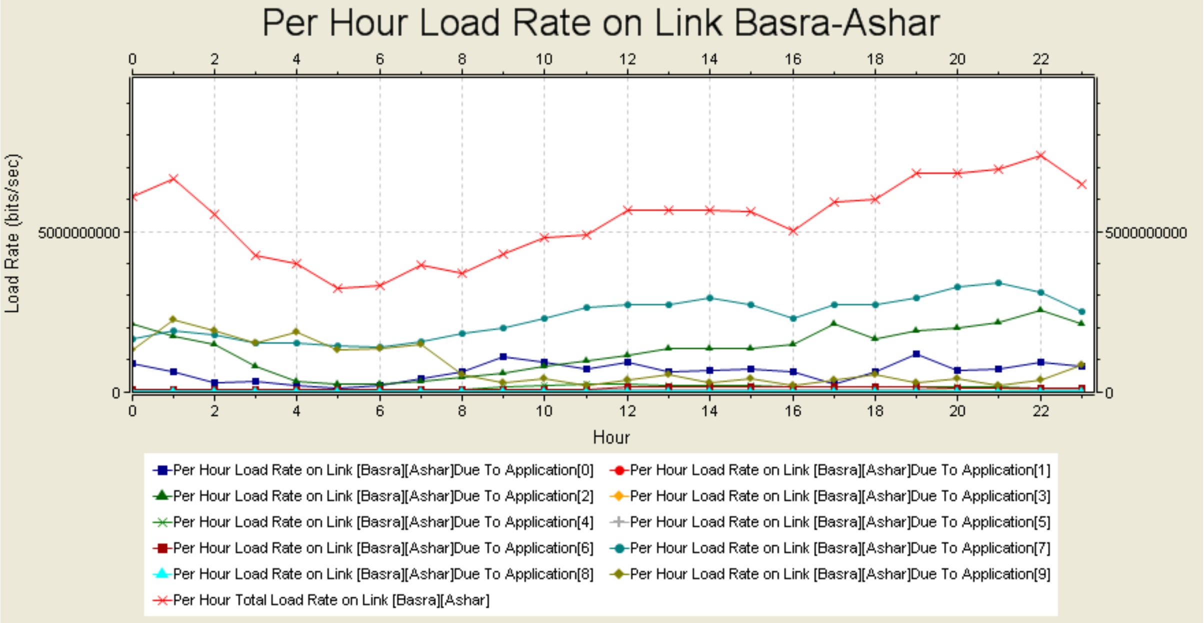


Figure 4.17 Per Hour Load Rate on Link Basra-Ashar

The link [Ashar-Basra] is directed to hold only upload components of the sever-based applications, therefore, no load traverses this link due to streaming audio, streaming video, and IPTV since they have zero upload components (the load is down streaming from the server to the other nodes and not conversely). In addition, the upload component of the web browsing application is very low as opposed to its download component in this scenario. These reasons make the P2P file sharing the only dominant application on this link's traffic as shown in Figure 4.18.

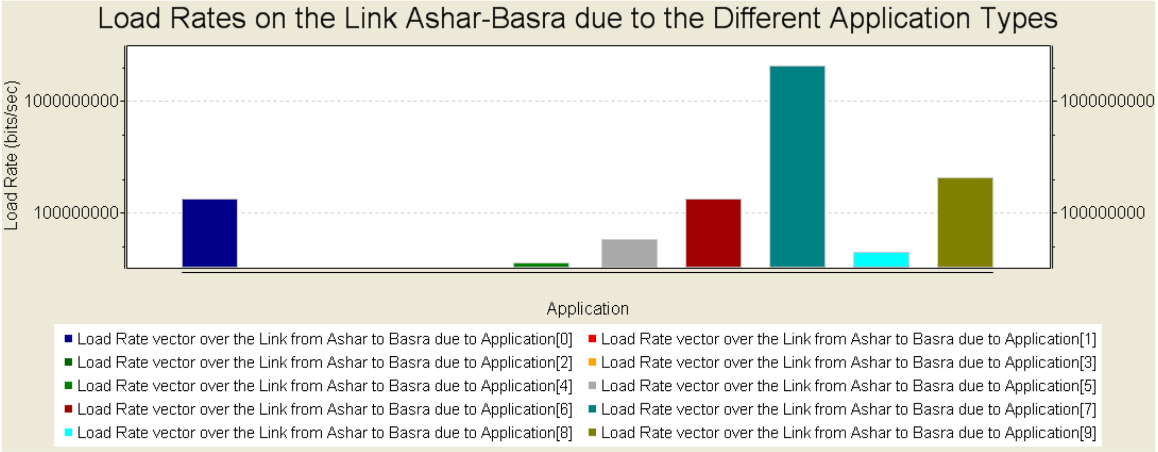


Figure 4.18 Load Rates on the Link Ashar-Basra due to the Different Application Types

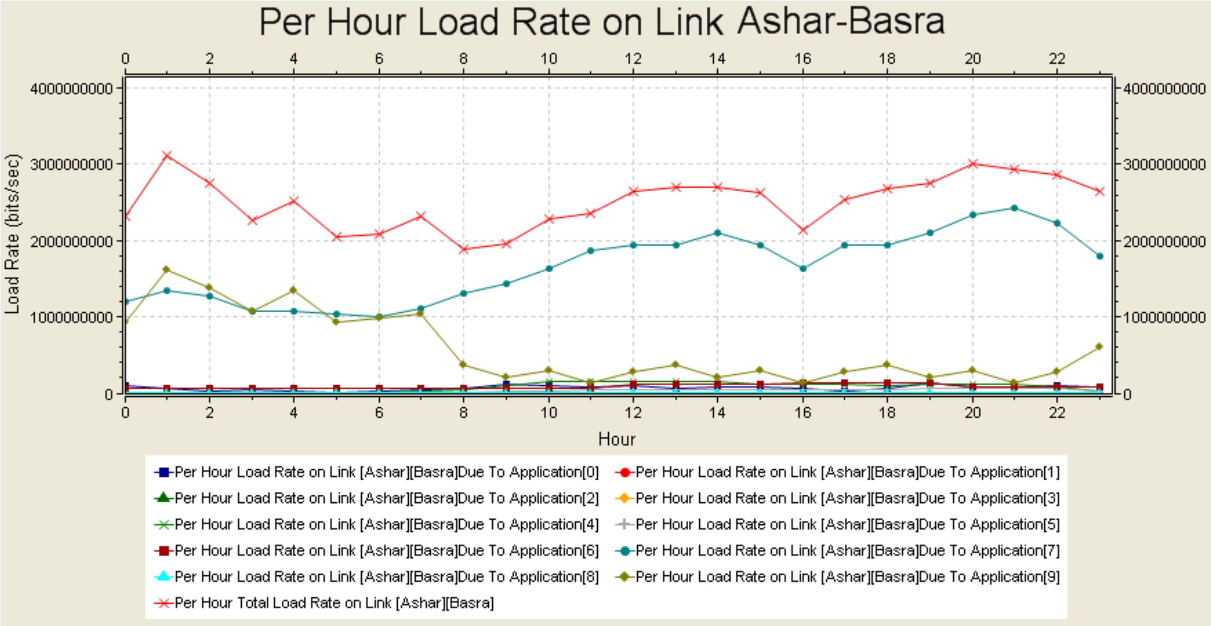


Figure 4.19 Per Hour Load Rate on Link Ashar-Basra

Similarly, the per-hour distribution of the total throughput on this link is dominated by the P2P file sharing traffic’s distribution as shown in Figure 4.19.

Since the link [Basra-AlZubair] has the all three dominant traffic types (P2P file sharing, Streaming video and we browsing traffics) at busy hour as shown in Figure 4.20, the hourly throughput distribution on this link will also be dominated by these three traffic types, and the per-hour load rate distribution takes a shape that comprises of the hourly variations in these traffics as shown in Figure 4.21.

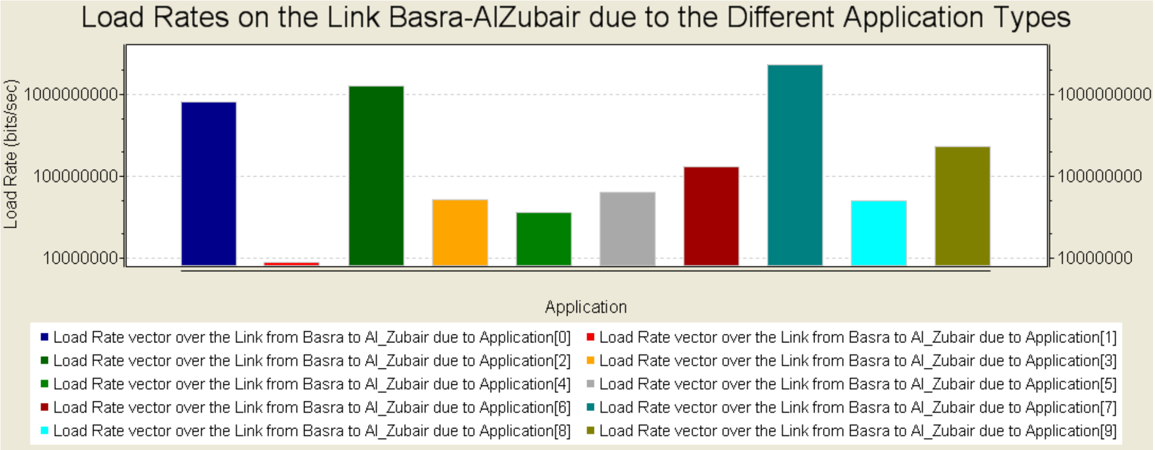


Figure 4.20 Load Rates on the Link Basra-Zubair due to the Different Application Types

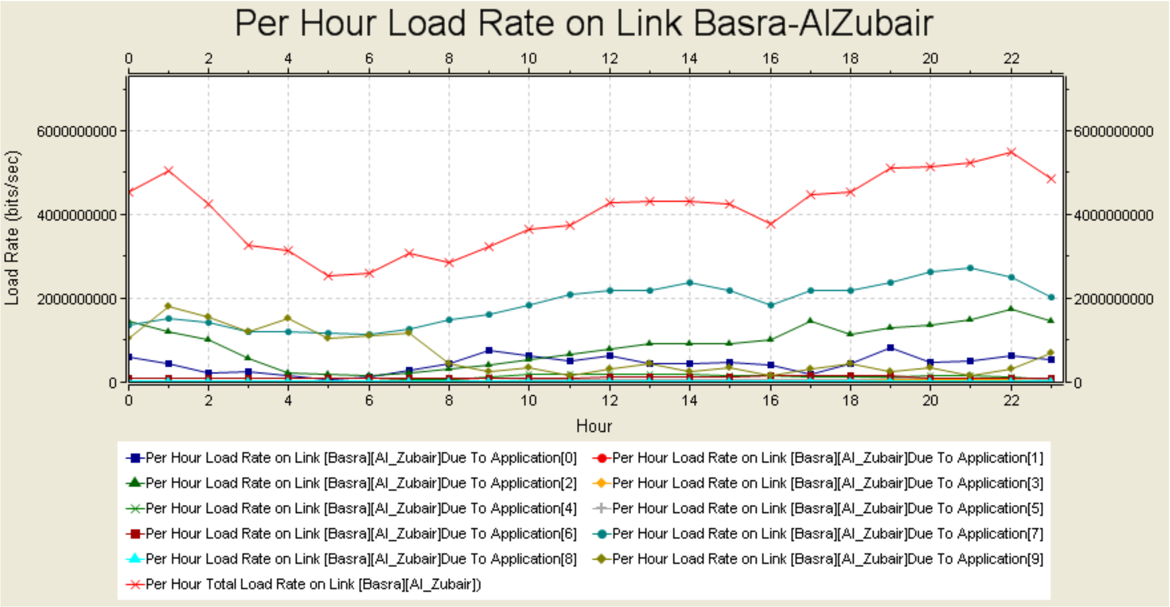


Figure 4.21 Per Hour Load Rate on Link Basra-AlZubair

4.9.3 Results of Maximum Media Resolution Scenario

In this subsection, the load rates have been tested when maximum resolution has been assigned to audio and video contents. All audio contents were upgraded to 5.1 surround format and all videos are now in HD format. Again, streaming video traffic will be the most affected traffic as a result of this quality improvement since streaming video is the most popular media application which generates zero intra-node traffic (i.e. 100% inter-node traffic). If an application generates intra-node traffic, i.e., traffic inside nodes, then this will decrease the amount of traffic going outside nodes through the network's links.

Figure 4.22 shows that the streaming video traffic largely dominates the total network's traffic due to the large increase in the per user busy rate accompanied by this improvement in the quality of streaming video information to HD.

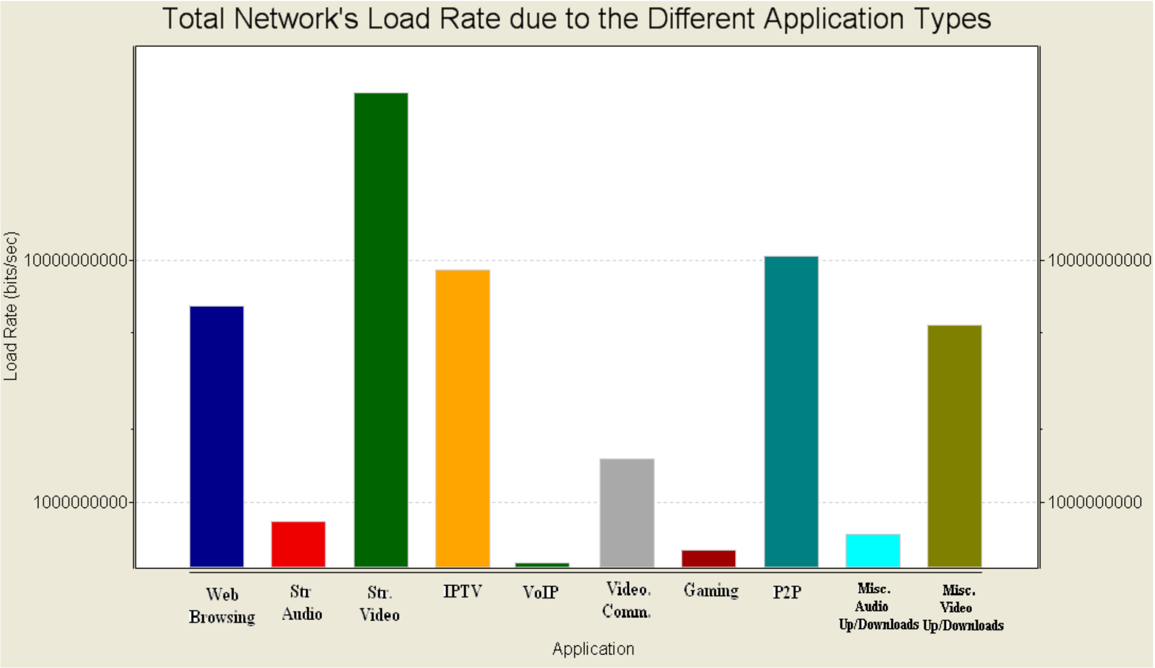


Figure 4.22 Total Network's Load Rate due to the Different Application Types

Figure 4.23 shows the total throughput on the different network's links. In this scenario, link [Server-Basra] is loaded much higher than the other links. This is a rational consequence to the large dominance of the streaming video traffic, because all this traffic which is characterised as being sourced at the server, which passes through the link [Server-Basra] to provide the streaming video service to all the other nodes.

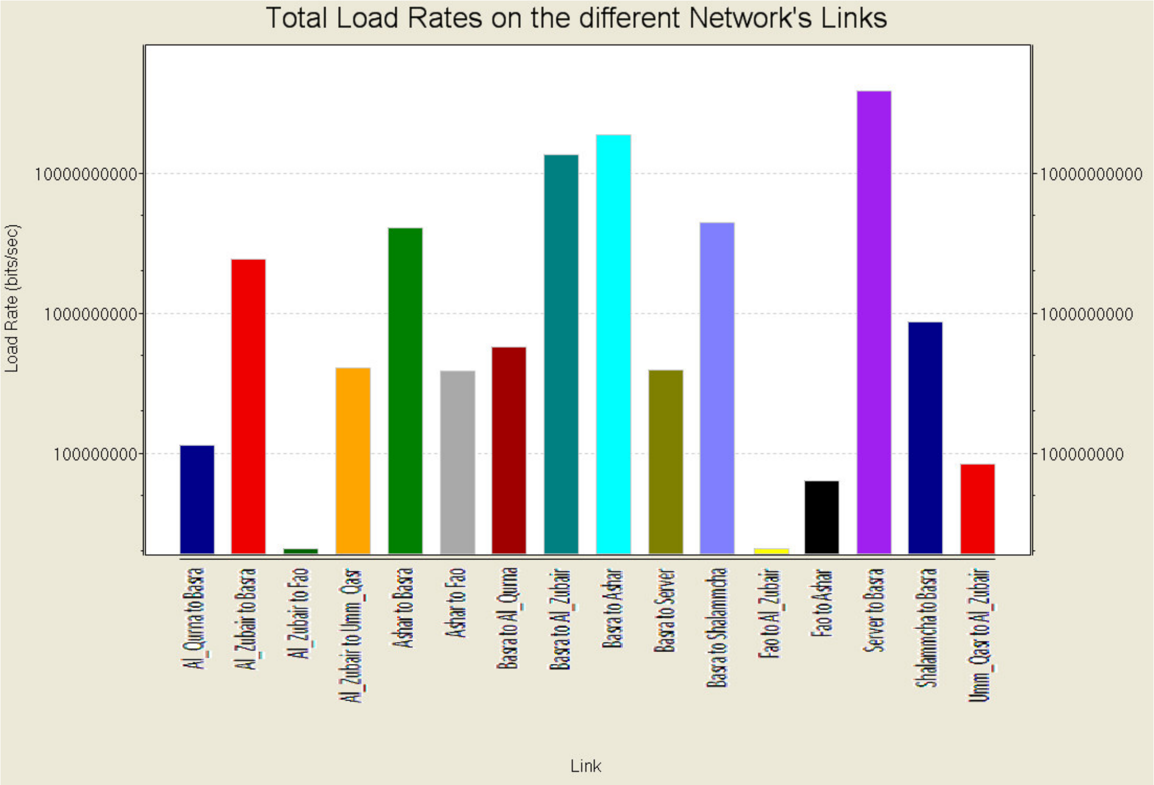


Figure 4.23 Total Load Rate on the Different Network's Links at Busy Hour

Figure 4.24 shows the busy hour load rates of the different traffic types on the most congested link [Server-Basra]. It is clear that this congestion is mainly caused by the high bandwidth consumed by the streaming video service. However, this is the cost of the high level of resolution supported by this service.

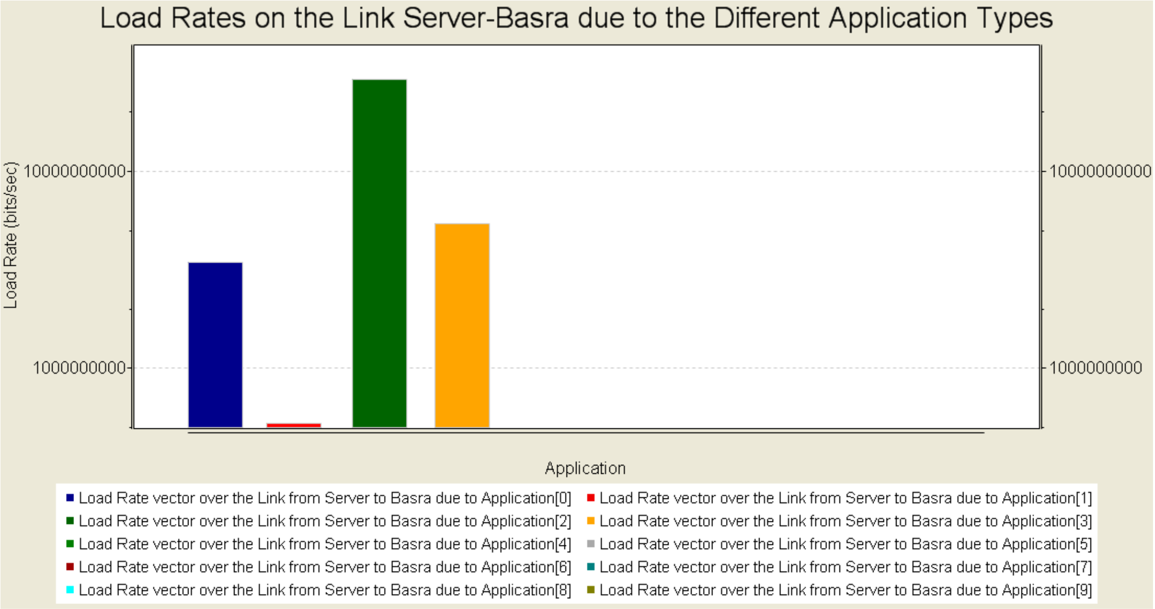


Figure 4.24 Busy hour Load Rates on the Link Server-Basra due to the Different Application Types

Figure 4.25 on the other hand shows the variation of the load rates due to the different applications during a whole day. As expected, the large dominance of streaming video traffic will cause the total load rate shape to inherit the shape of the streaming video bandwidth throughout the whole day.

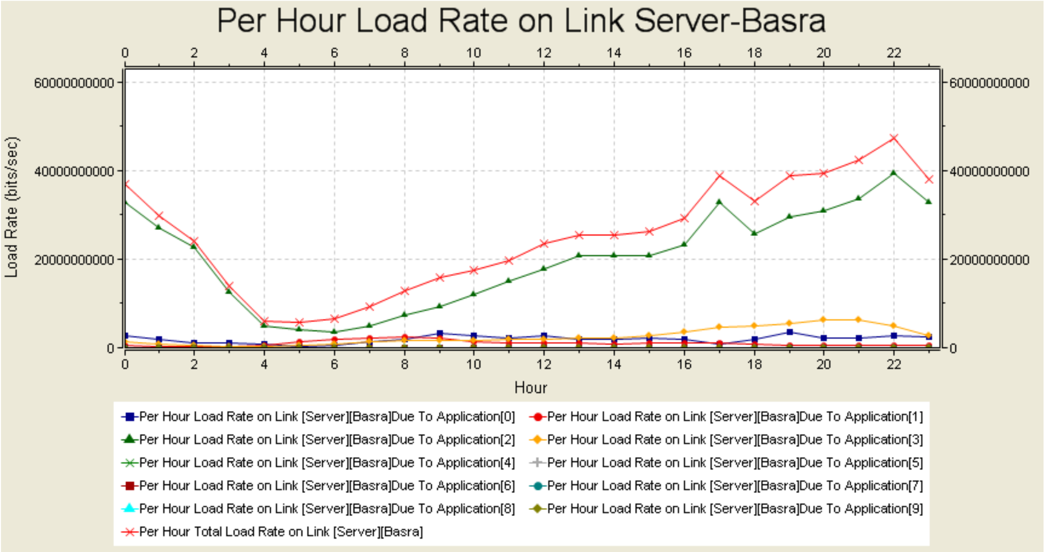


Figure 4.25 Per Hour Load Rate on Link Server-Basra

Link [Basra-Ashar] represents the second most congested link. Its loading is shown in Figure 4.26. Even the bulky bandwidth consuming P2P file sharing application has been outweighed by the throughput generated due to the improved streaming video service.

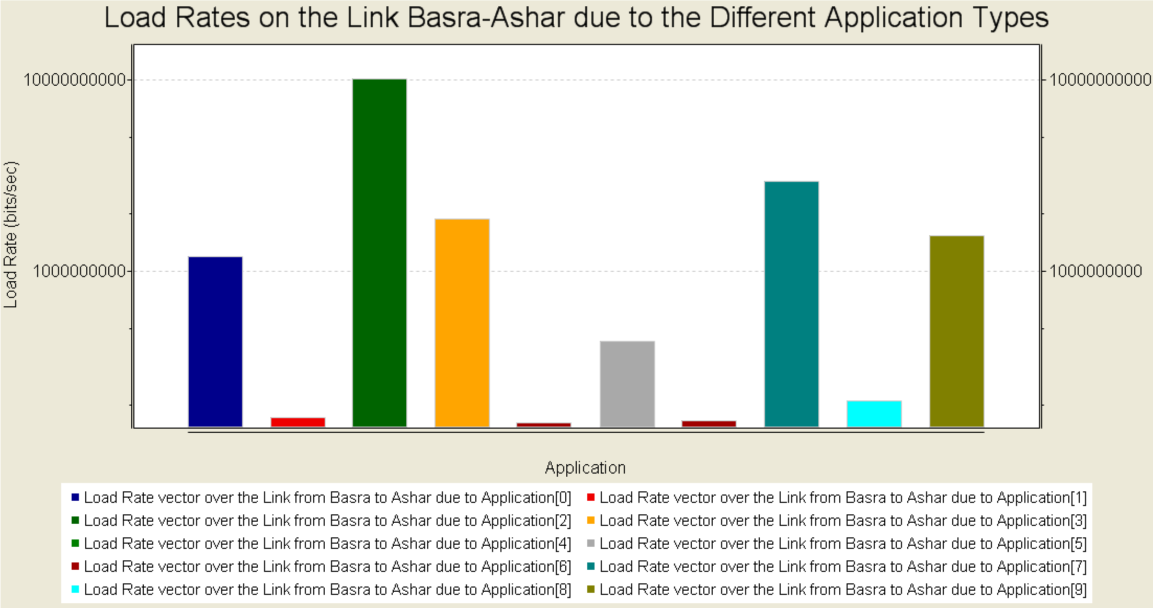


Figure 4.26 Busy Hour Load Rates on the Link Basra-Ashar due to the Different Application Types

In Figure 4.27, which displays the per-hour throughput change on the link [Basra-Ashar], it is obvious that streaming video largely governs the shape of per hour total load rate except at early hours of the day where the miscellaneous video clips up/downloading usage is active as shown in Table 4.6.

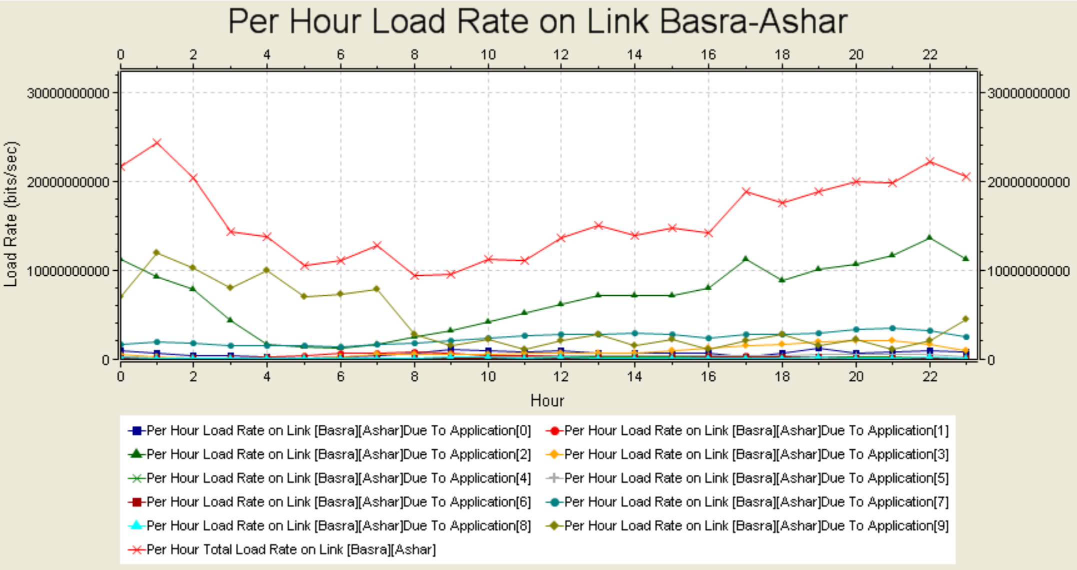


Figure 4.27 Per Hour Load Rate on Link Basra-Ashar

The loading pattern on the link [Basra-AlZubair] will not be very different from the link [Basra-Ashar] except that traffic rates due to all the applications are less, but the link is still dominated by the streaming video traffic as shown in Figure 4.28.

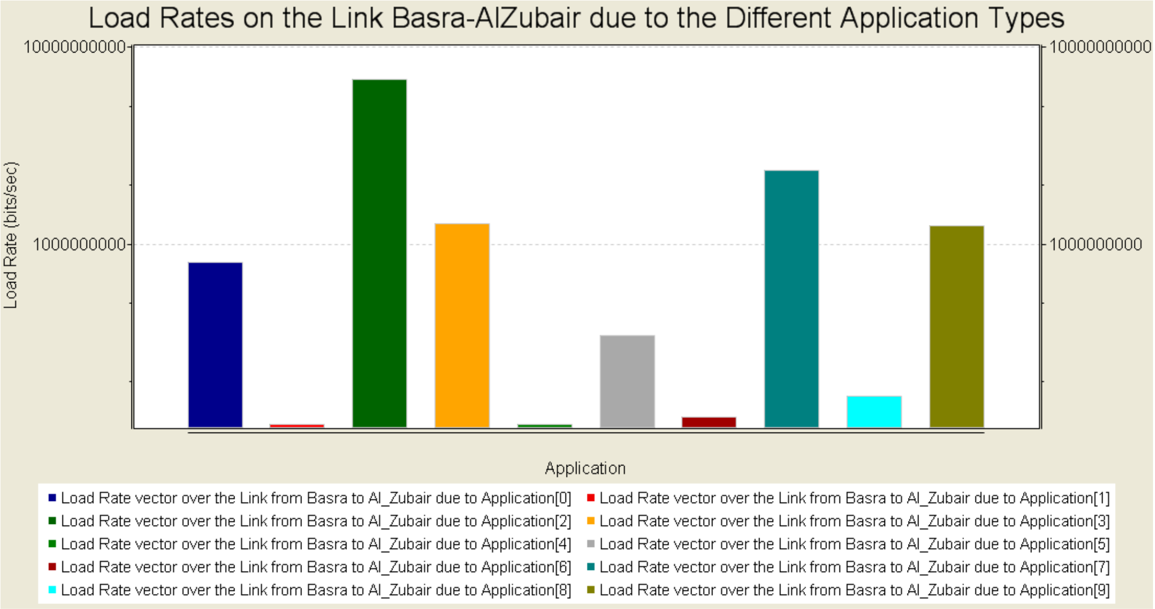


Figure 4.28 Busy Hour Load Rates on the Link Basra-AlZubair due to the Different Application Types

Even the hourly load rates distribution on this link, shown in Figure 4.29 is very similar to the previous link except in terms of amplitudes.

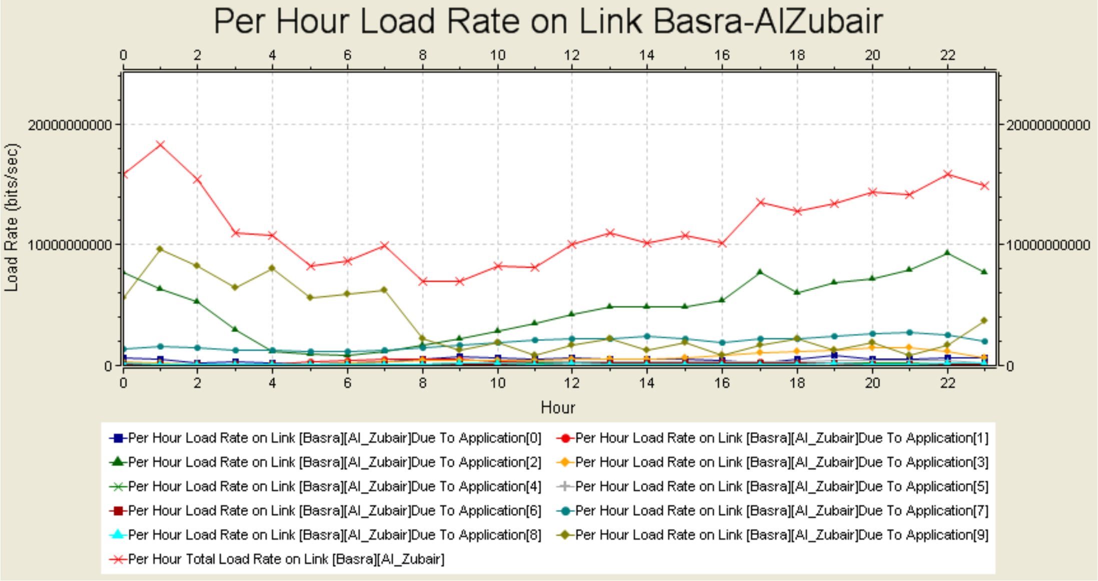


Figure 4.29 Per Hour Load Rate on Link Basra-AlZubair

4.9.4 Results of 3D Web Browsing and Video Contents Scenario

This subsection displays the results of the fourth applications' quality scenario, where 3D technology was implemented with the video contents and the web browsing applications. Figure 4.30 shows that this move to 3D technology has significant influence on the throughputs of the different applications. Here, the streaming video has the largest share of this influence, where its consumption of bandwidth is increasing more and more by this quality improvement. Again this largest influence of streaming video by the quality improvement is attributed to the same two main reasons, the popularity of this applications type and the full inter-node traffics direction.

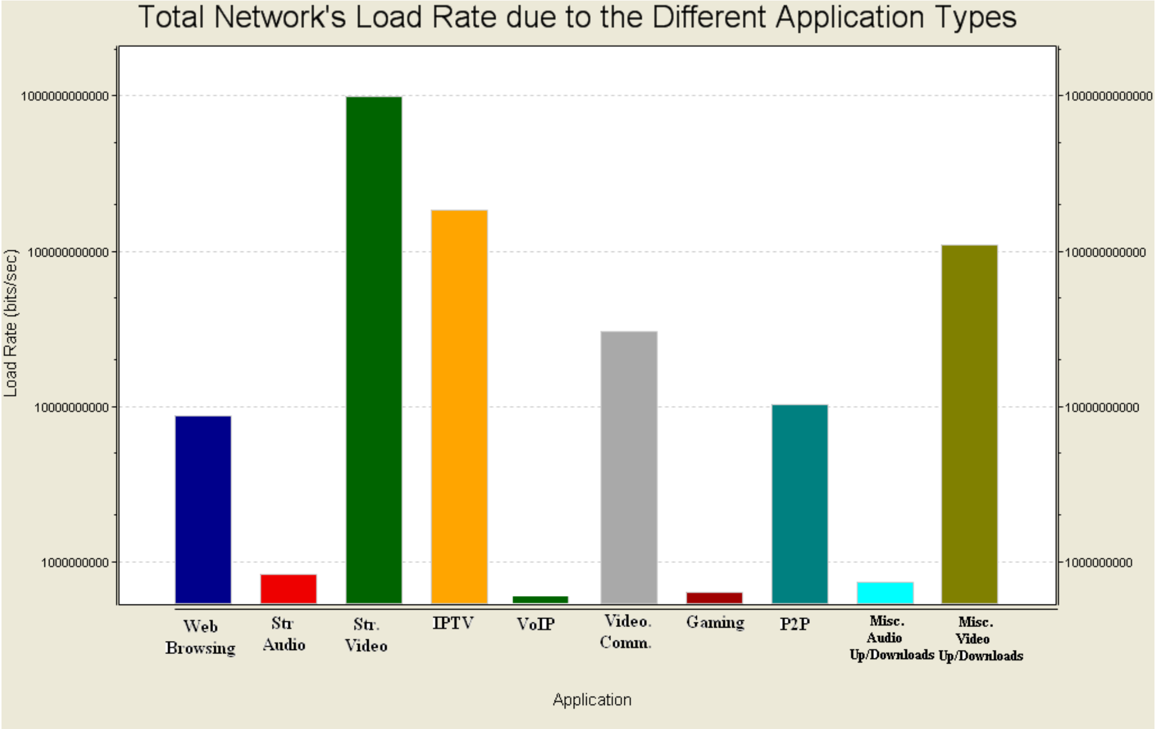


Figure 4.30 Total Network's Load Rate due to the Different Application Types

Even though the web browsing applications have been upgraded to 3D, the rise in the throughput generated by web browsing is still incomparable with the rise of the throughput generated by steaming video. This is due to small increase in the per user bit rate when web browsing is switched to 3D which is met by the large increase in the per user bit rate of streaming video when it is moved to 3D (see Table 4.5).

No wonder, this high bandwidth streaming video traffic will be more concentrated on the link [Server-Basra] as it is the only gateway from the server causing this link to be highly congested at the busy hour compared to the others as shown in Figure 4.31.

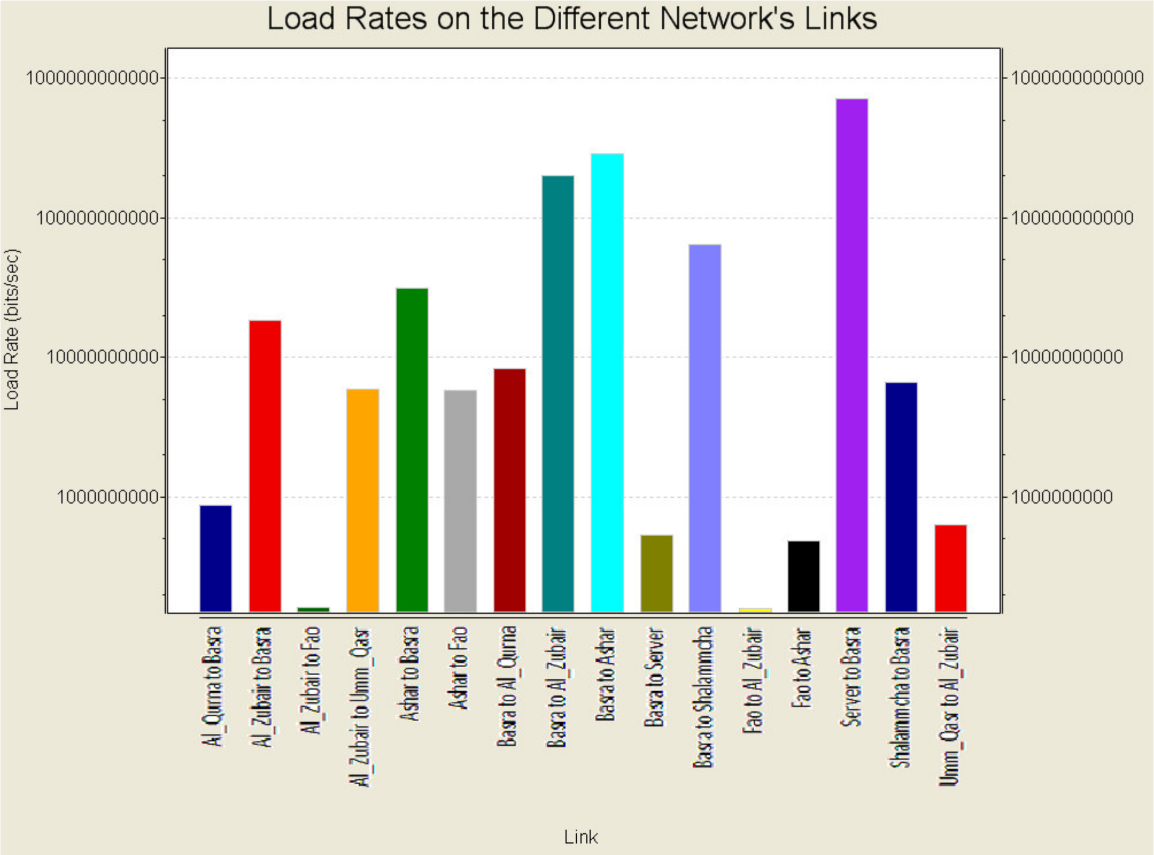


Figure 4.31 Total Load Rate on the Different Network's Links at Busy Hour

Figures 4.32 and 4.33 show the busy hour load rates on the link [Server-Basra] at the busy hour and in per hour bases during the whole day respectively. It is obvious in both figures that the streaming video traffic dominates and governs the total rate value and per hour variation shape.

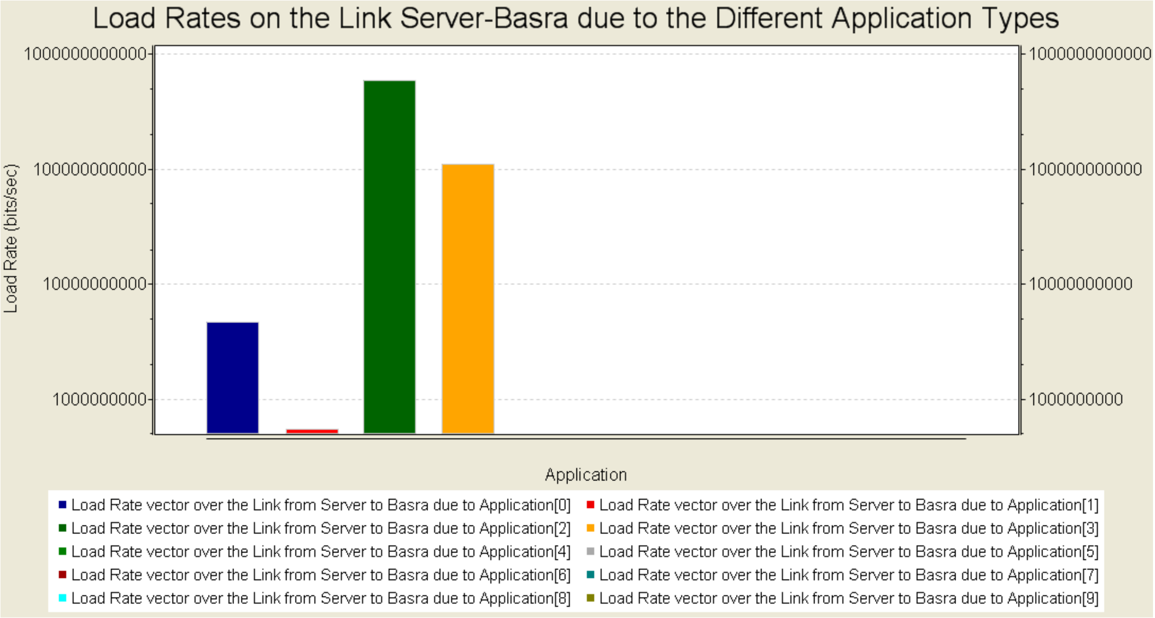


Figure 4.32 Busy Hour Load Rates on the Link Server-Basra due to the Different Application Types

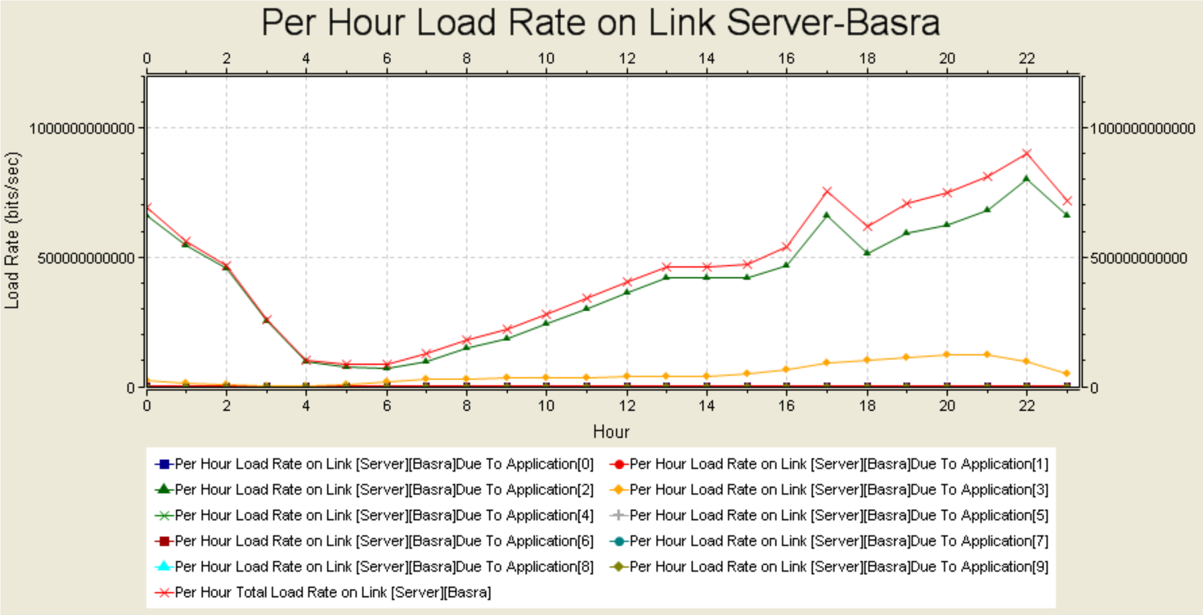


Figure 4.33 Per Hour Load Rate on Link Server-Basra

In the link [Basra-Ashar], the existence of the non-server-based busy hour traffics did not add substantial contributions to the total load since the streaming video’s load is much higher than any other traffic type in this scenario as shown in Figure 4.34.

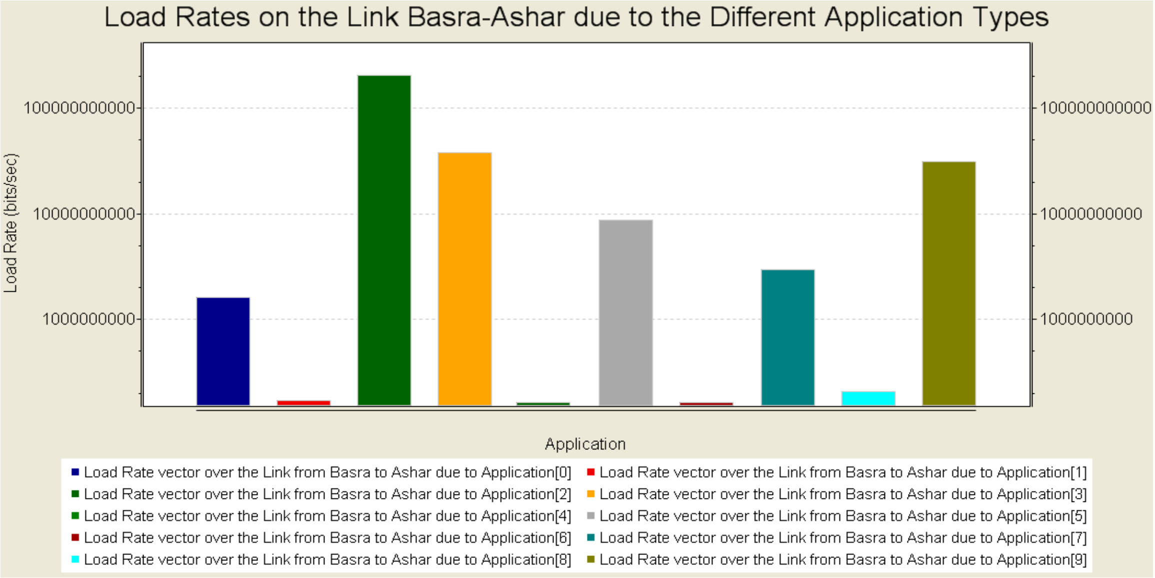


Figure 4.34 Busy Hour Load Rates on the Link Basra-Ashar due to the Different Application Types

The significance of the traffic generated by all the applications other than the streaming video has been lessened in this scenario due to the huge gap between the throughputs of streaming video and all the other applications. However, the low usage of streaming video service confronted by the high level of the miscellaneous video clips up/downloading usage at the early day's hours made the influence of the latter to appear on the per hour total load rate on this link as shown in Figure 4.35.

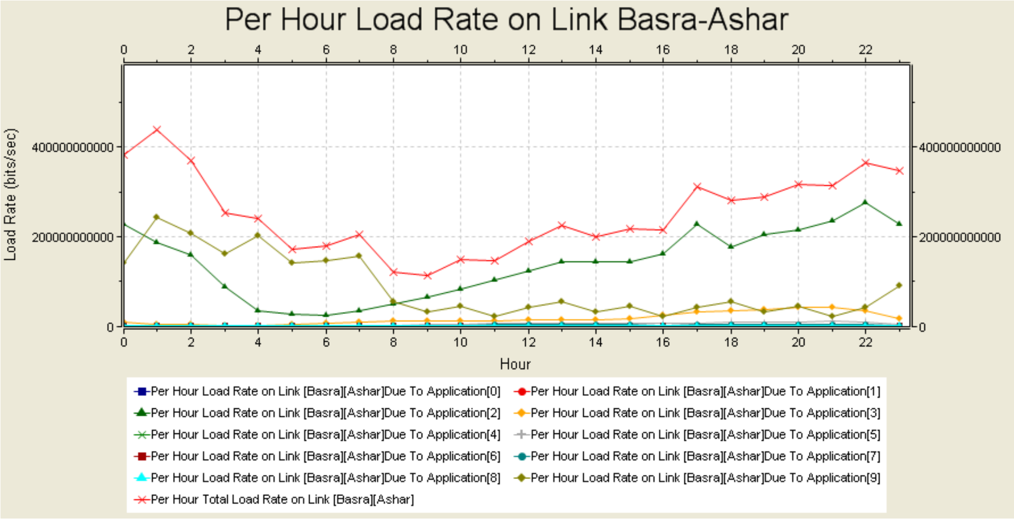


Figure 4.35 Per Hour Load Rate on Link Basra-Ashar

The link [Basra-AlZubair] also holds traffics of all types. Again, this link is similar to the link [Basra-Ashar] in terms of the dominance of streaming video load rate, but the lesser destination's population has led to lower bandwidth consumption for all the applications as shown in Figure 4.36.

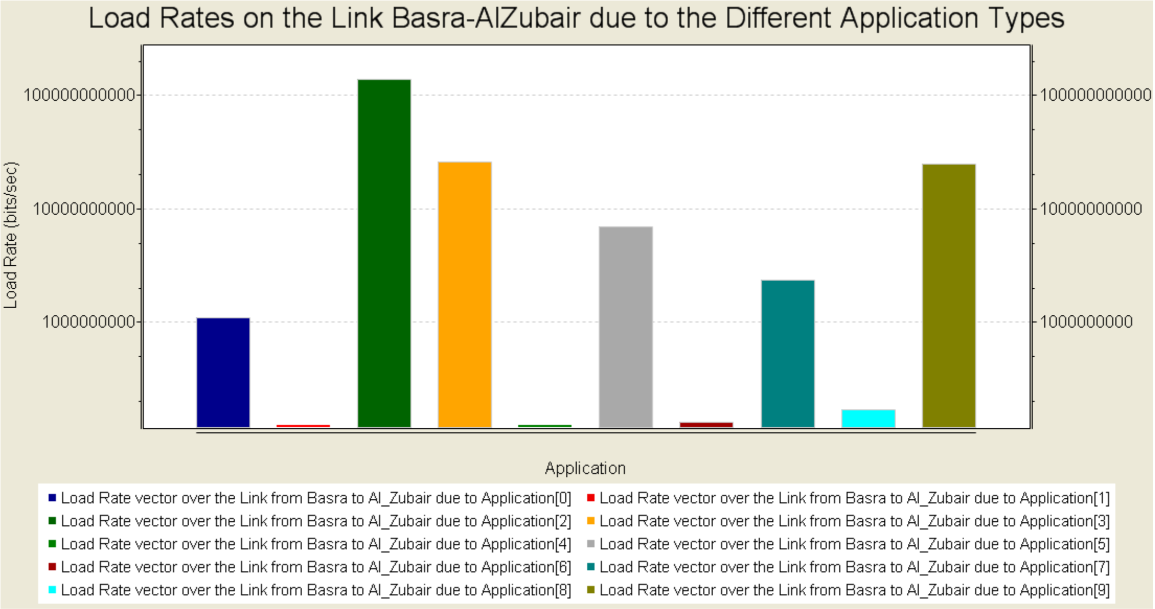


Figure 4.36 Load Rates on the Link Basra-AlZubair due to the Different Application Types

Figure 4.37 shows the hourly variation of load rates due to the different application types together with resultant total per hour throughput on the link [Basra-AlZubair]. This figure indicates that the total per hour rate shape is governed by the dominant streaming video application's traffic after 8:00 AM. On the other hand, it is more dominated by the miscellaneous video clips up/downloads' traffic before 8:00 AM because of the increasing use of this application in this period of time as shown in Figure 4.37.

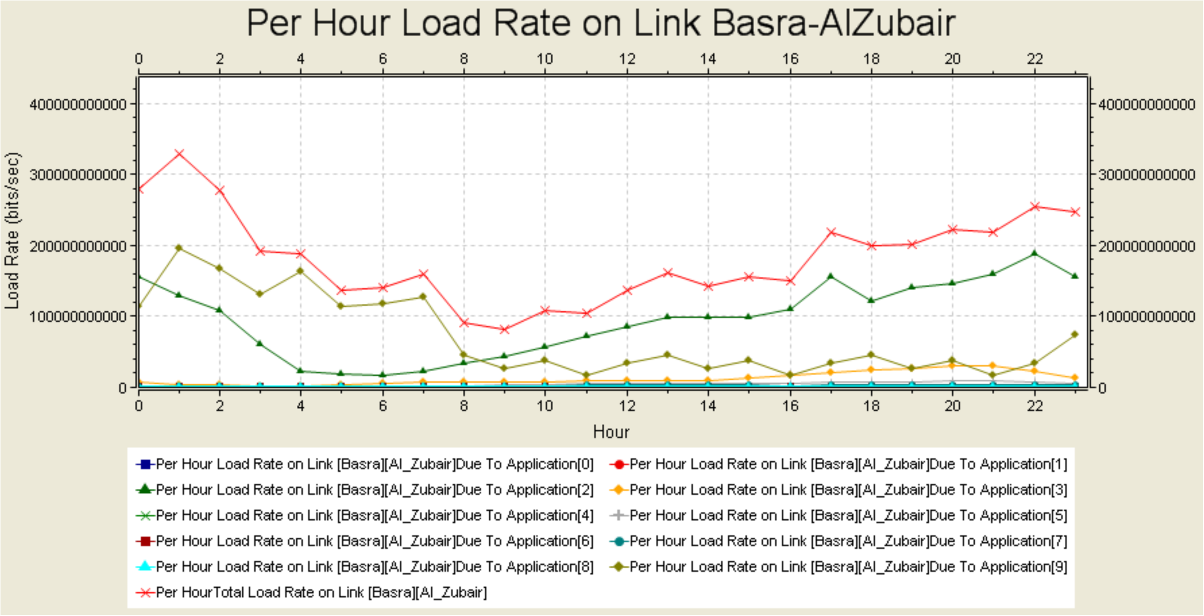


Figure 4.37 Per Hour Load Rate on Link Basra-AlZubair

4.10 Summary

Basra national optical network has been simulated in this chapter. The total average load rates on the different network's links have been calculated, and the bandwidth of the traffics generated by the different applications types has also been determined against different application's quality input scenarios. Furthermore, the contribution of each type of applications to the total network load rate has been dimensioned for each resolution scenario. The links' peak-hour bit rates obtained for each of the four scenarios in Figures 4.3, 4.13, 4.23, and 4.31 provide a clear indication of the required dimensioning of these transmission links.

The links' throughputs due to the different application types have been calculated both at busy hour and on an hourly basis during a 24 hour period, and the total link's throughput through the whole day has also been investigated accordingly. In addition, the places of potential congestions on the different network's links together with the contribution of each application type to that congestion have also been revealed in this chapter.

The effect of enhancing the quality of the services offered to users on the network loading has been studied extensively aiming to put a corner stone for establishing an efficient network that satisfies the demands of future internet which is expected to be characterised by its huge bandwidth consumption yields due to the enhancements in the offered services qualities and the dramatic increase in the number of users.

Chapter 5

The Impact of Content Oriented Routing on OpenFlow Burst Switched Optical Networks

The Internet has revolutionized how the world has accessed information and communicated it but continued development in optical and electronic technologies has resulted in higher bit rates, bandwidths, and functionalities and has enabled the spawning of a multitude of different applications and services that can be accessed on it. This has exposed fundamental shortcomings to the existing Internet architecture.

Three shortcomings of the current Best Effort (BE) routing protocol, which is widely used on Internet currently, has been addressed in this chapter. First, the equal treatment of all traffic types can be considered a great deficiency in the BE protocol since applications sensitivities towards delay and packet loss are different [84]. This chapter proposes dealing in different ways with the different traffic types to offer an enhanced QoS. Secondly, the blind view of BE routing protocol to the type of traffic results in an unbalanced distribution of traffic over network links causing some links to become congested and others not and is a second drawback in the current Internet [85]. Weighted Dijktra Algorithm was deployed in this chapter to balance the load over the links, which in turn will decrease the amount of loss and thus enhance the QoS. Finally, another challenge was tackled through this chapter to provide an extra free space over the network's links to widen the scope of services being offered to the users, such as including broadcast multicasting, whilst maintaining the QoS within an acceptable range. A lot of Internet providers have struggled to include TV broadcasting with their services, since most of these attempts failed to provide a known QoS [86]. Balancing loads over links will also help to increase link utilisation in the network. Finally, the propagation delays and traffic losses for traffics over the links were recorded to prove the feasibility of our new traffic management technique, represented by the proposed content oriented routing, for the future Internet. Loads over links were also monitored in this work to find out to what extent our load balancing technique helps to relieve network's congestions.

Section 5.1 introduces the idea of application based routing. Section 5.2 is concerned with network modelling and how the real national network had been implemented in the software. Furthermore, this section lists the types of applications used in our model and categorizes these applications into three main classes according to their QoS requirements. In Section 5.3 the network's performance was analysed and the results were discussed. Finally the Section 5.4 concludes this chapter.

-What's new: A routing protocol was suggested to maintain the different applications in our flow model within pre-set QoS levels.

5.1 Application Based Routing

OMNeT++ simulator was used in this chapter to investigate the feasibility of using an application based routing to manage loss and delay through load balancing on the tested network assuming that the optical network is switched using some form of burst/flow based switching and managed using a centralized OpenFlow management system. A mix of ten application types, namely, web browsing, streaming audio, streaming video, IPTV, VoIP, video communication, interactive gaming, P2P file sharing and miscellaneous upload/download, were transmitted through this network, where all the applications supported by Internet nowadays could be organised under these types. Motorola's research group user behaviour and applications specifications statistics were used in this chapter on our reference optical network, i.e. NSFNET. This user behaviour model, uses parameters such as the number of users for each application, the number of sessions per day, session time, per user download and upload rates for the various applications and other applications usage statistics [87]. Our network model can easily be changed to another suite of applications and usage statistics for analysis, if required.

These applications were put into different categories according to their tolerance to loss and delay as shown in Table 5.1. An application may require minimum loss and delay such as VoIP, whereas some other application may be satisfied by low loss but unguaranteed delay such as streaming audio. Furthermore, another application may be considered to have no concern about loss and delay such as P2P file sharing.

In our model, streaming applications and web browsing are considered to be loss sensitive applications, therefore their packet loss should not exceed 10% to provide an acceptable QoS [87, 88], whereas real time applications such as VoIP, video communication and interactive gaming do not tolerate more than 3% loss [89, 90]. In addition, these real time applications require end to end delays not exceeding 150 ms to provide acceptable qualities [89, 91]. These applications were set to their desired small loss limits on the account of the other loss insensitive applications such as P2P and miscellaneous applications.

Traffic generated due to these applications was dealt with using different routing techniques and priorities. Furthermore applications were prioritized to allow different amounts of traffic shedding limits. OMNeT++ software was deployed here to determine which are the congested links and identify them by colouring them red during and after the end of the simulation.

Table 5.1 Loss Percentage Limits

Application	Loss	Delay
Web Browsing	≤ 10%	≤ 1s
P2P File Sharing	≤ 100%	≤ 1s
Miscellaneous up/download	≤ 100%	≤ 1s
Streaming Audio	≤ 10%	≤ 1s
Streaming Video	≤ 10%	≤ 1s
IPTV	≤ 5%	≤ 1s
VoIP	≤ 3%	≤ 150ms
Video Communication	≤ 3%	≤ 150ms
Interactive Gaming	≤ 3%	≤ 150ms

Dijkstra's routing algorithm was used to select the route with the least end to end delay for the information which required the least delay. On the other hand, other applications such as P2P file sharing and miscellaneous up/download can be rerouted since they are not so delay sensitive. These delay insensitive applications are routed using weighted Dijkstra's routing algorithm. Finally, the end to end delays for traffics and traffic losses over the links were recorded to show the feasibility of our new routing technique. Broadcasting IPTV data was transmitted over the network's links in a multicasting way, where each node broadcast the TV data to all its neighbouring nodes except those that have been served by the other nodes.

In this chapter, dynamic routing was adopted in order to keep track of any changes that occur to the network such as link or node failures. The applications here were prioritized and divided into categories, and the Djikstra routing algorithm was used to choose those routes of the least propagation delay for the delay sensitive applications. On the other hand, the least congested routes were used to reroute the loss sensitive applications. However, the network’s routers are supposed to be intelligent enough to apply the suitable routing table to each kind of traffic passing through them. In BE routing protocol when a link gets congested so that the link's capacity is exceeded, the network will discard packets randomly no matter what application these packets belong to [92-94]. This could be considered a drawback and can be solved by the application based routing proposed in this chapter, where the amount of shedding depends on the priority of the application, where loss sensitive applications will be given higher priorities.

5.2 Network Modelling and Applications Categories

The 14 Nodes NSFNET in Figure 5.1 below was chosen in this chapter to test the proposed routing protocol. This network was chosen instead of Basra network because it has a larger size with a better interconnectivity. As a result, more links and more alternative routes to the various destinations exist. This will help us in examining the feasibility of the proposed protocol more efficiently. This sample network has been used to analyse loss, end to end delays and load balance over the various fibre links. Each node in the OMNeT++ model was associated with 1.5 million users communicating over a 40 GB bidirectional links optical network. The residential broadband applications’ quality and user behaviour statistics discussed in chapter 4 were used in this chapter to calculate the amount of load rates on the different links due to the various application types.

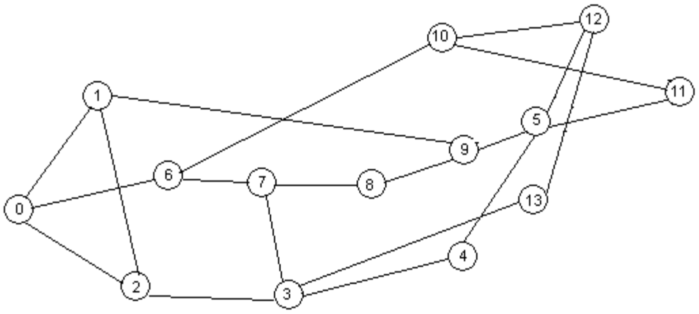


Figure 5.1 NSFNET Topology.

Applications were categorised into three categories according to their QoS metrics: delay and loss sensitivity as shown in Table 5.2. These three categories are: loss sensitive and delay sensitive, loss sensitive and delay insensitive, loss insensitive and delay insensitive. Whenever the router receives traffic, it looks to the type of that traffic by supposing that there is an identification byte in the header of each byte and identifies the type of application to which this traffic belongs. The router will then select either to send this traffic using the shortest path routing algorithm, if it is delay sensitive, or using least congested path if it is not. Moreover, if any overloading happens in one of the network's links, traffics will be throttled according to the loss sensitivity characteristics of the application type that generated this traffic.

Table 5.2 Applications Categories

	Loss			Delay		
	Low	Acceptable	High	Low	Acceptable	High
P2P File Sharing			✓			✓
Misc. up/download			✓			✓
Web Browsing		✓				✓
Str.Audio		✓				✓
Str. Video		✓				✓
IPTV		✓				✓
VoIP	✓			✓		
Video Comms.	✓			✓		
Gaming	✓			✓		

5.3 Results and Discussion

Results were discussed through four aspects in which the new routing protocol has contributed to improve the QoS offered to the end users. These aspects are: load balancing, max delays, losses over the overloaded links, and load rates over links due to the various applications.

5.3.1 Load Balancing

To investigate the feasibility of the proposed content oriented routing, a comparison was made among the load distribution of the different application types over the network's links. Figures 5.2 and 5.3 show that the loads tend to be balanced among the links, that is because these application types i.e. web browsing and P2P file sharing are delay insensitive, thus they tolerate the more delays enabling the routers to choose those routes that are least congested to avoid the unnecessary data loss. On the other hand, delay is a crucial factor for VoIP since this application needs to be routed to the destination very fast through the least delayed routes even though such routes are highly congested as shown in Figure 5.4. Furthermore, these applications, i.e. VoIP, video communications, and interactive gaming were given higher priorities and lower loss limits than some other applications preventing their traffic from being lost in the case of congestion since they are loss sensitive as well. Three routing algorithms were used for the proposed scheme depending on the type of traffic to be routed, where those routes of the least delays were selected for the delay sensitive applications. On the other hand, the least congested routes were chosen for the loss sensitive and delay insensitive applications to avoid overloads and then shedding by choosing alternative non-congested links to pass this information on. In addition, applications were prioritized to allow different shedding for different applications according to their loss sensitivity.

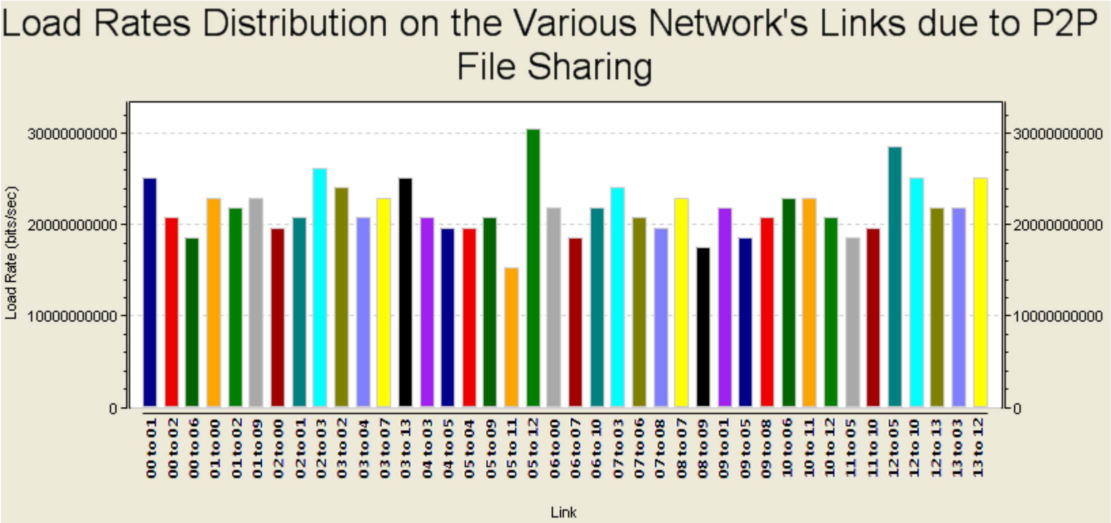


Figure 5.2 Load Rates Distribution due to rerouting of delay insensitive traffic (P2P)

When a link becomes overloaded, i.e., the applied traffic exceeds its capacity, then the link is located at the bottleneck and there is no alternative to shedding the surplus data, but the shedding process will not be achieved randomly as it is the case in the best effort protocol. The amount of dropped information in our proposed routing protocol will be dependent on the class of the application. The maximum amount of shedding was set to be 3% for real time applications such as VoIP, video communications, and interactive gaming since they are considered to be loss sensitive.

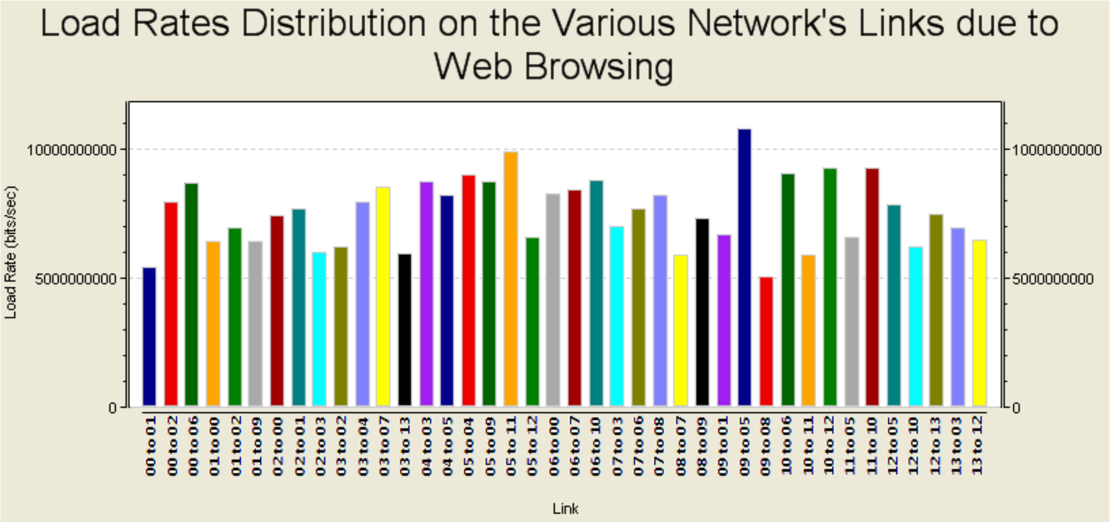


Figure 5.3 Load Rates Distribution Due to Web Browsing

Streaming audio and video as well as web browsing were not allowed to be shed with more than 10%. P2P and miscellaneous up/download were allowed to be shed without constraints to completely relieve the congestions as shown in Table 5.1.

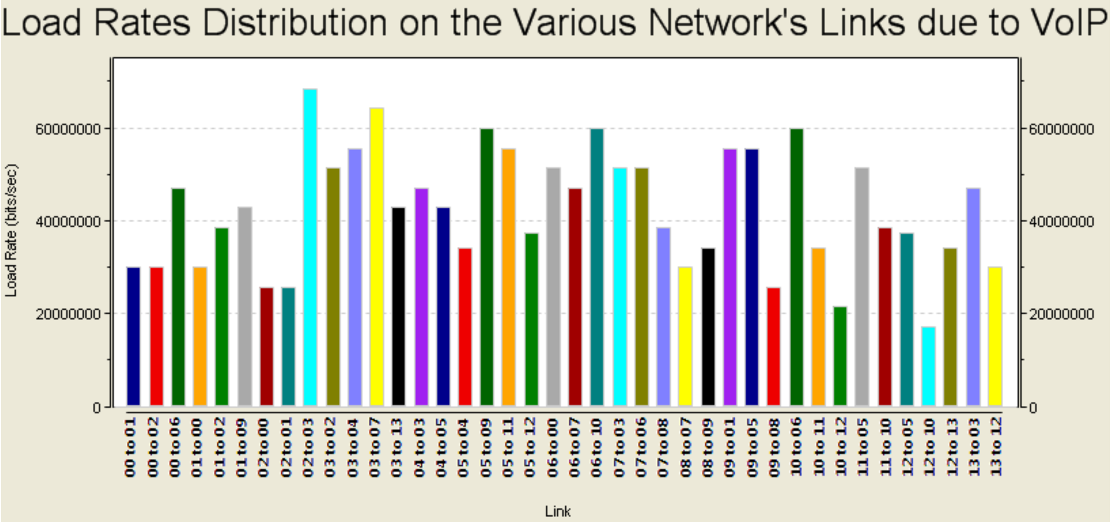


Figure 5.4 Load Rates Distribution Due to VoIP

5.3.2 Max Delays (OEO switching delay)

In hybrid optical networks, optical signals need to be converted to an electronic form, processed and converted back to light at each hop. Propagation delay through an optical cable could be neglected since the optical signal is transmitted across it at the light speed. The process of converting light to electrons and back to light is called Optical-Electronic-Optical (OEO) conversion, which is the most time consuming process in the end-to-end communication. The time consumed through this conversion is called OEO switching delay. The OEO delays of the different applications between the two most distant nodes (Nodes 0 and 11) in the network shown in Figure 5.1 were recorded. Note that this delay is calculated in number of hops since an OEO conversion is required for each hop.

Figure 5.5 shows that VoIP, video communication and interactive gaming experienced the least delay as they are very delay sensitive. Note the maximum limits of the delay for all the applications in Table 5.1 were not exceeded. This shows that a good quality of service was gained for our proposed routing protocol.

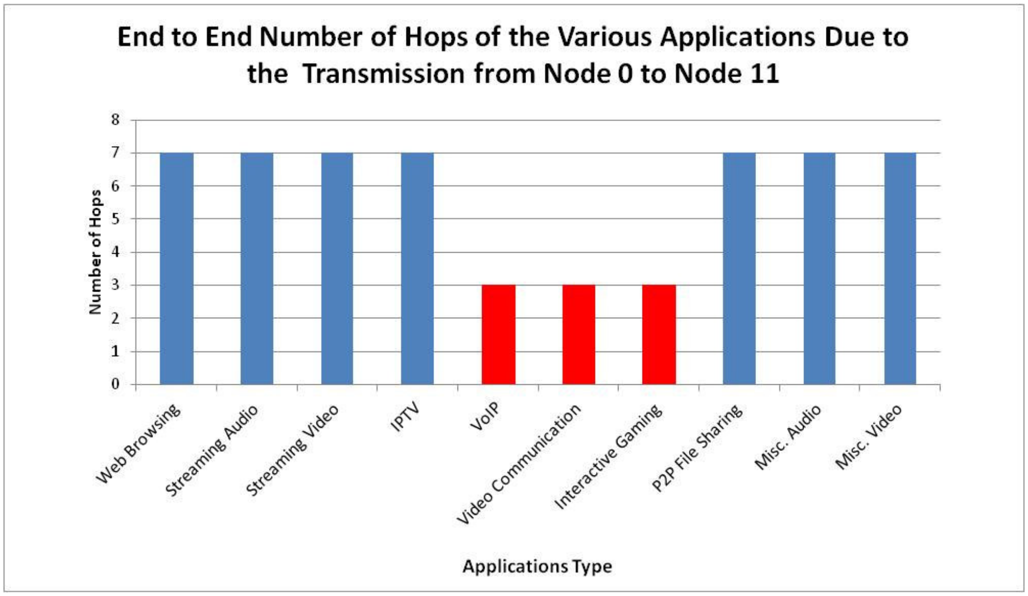


Figure 5.5 End to End Number of Hops of the Different Applications from Node0 to Node11

5.3.3 Losses Over The overloaded Links

The link from Node2 to Node3 has been chosen as an example of overloaded links. This link has been selected to show the percentage losses of the different applications over these links as shown Figure 5.6.

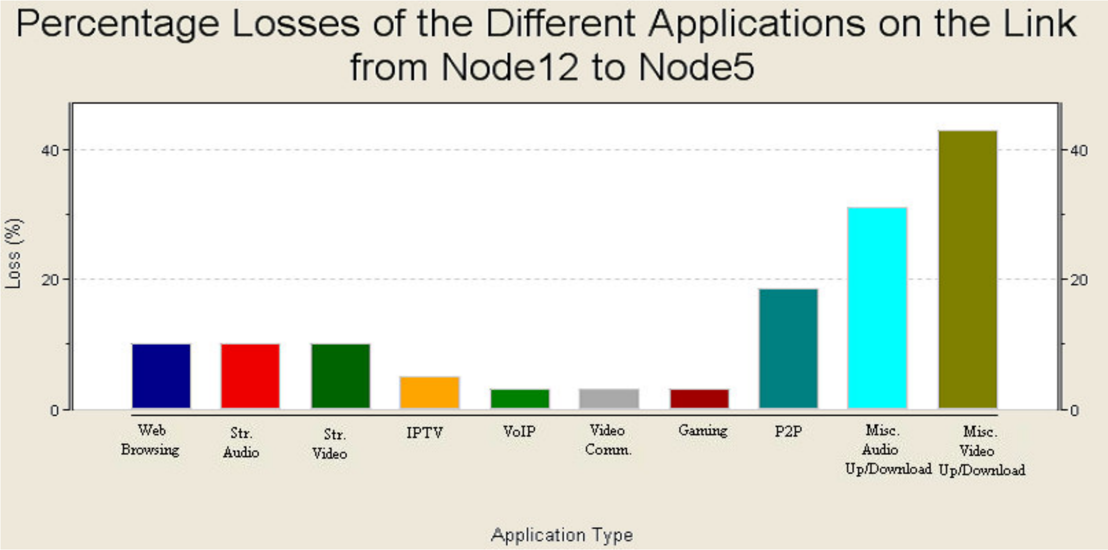


Figure 5.6 Percentage Losses of the Different Applications on the Link from Node12 to Node5

Figure 5.6 shows that losses for web browsing, streaming audio, streaming video, IPTV, VoIP, video communication, interactive gaming were restricted to the dimensioned limits as specified by the network manager, whereas P2P file sharing, miscellaneous audio up/downloads, and miscellaneous video up/downloads experienced 18% , 31% and 43% losses respectively.

5.3.4 Load Rates over Links Due To the Various Applications

Our software is also capable of computing the load rates over the different links due to the various applications. We have selected two links as an example, namely, link 0-1 and link 7-8. Figures 5.7 and 5.8 show the load rates on these two links due to each application type. The bars in these two figures represent the load rates due to web browsing, streaming audio, streaming video, IPTV, VoIP, video Communications, interactive gaming, P2P file sharing and the other miscellaneous up/downloads respectively, where these applications were numbered from 0 to 9 in the figures. It is clear from these figures that the P2P application is the dominant application over these links where most of the traffic is due to this application.

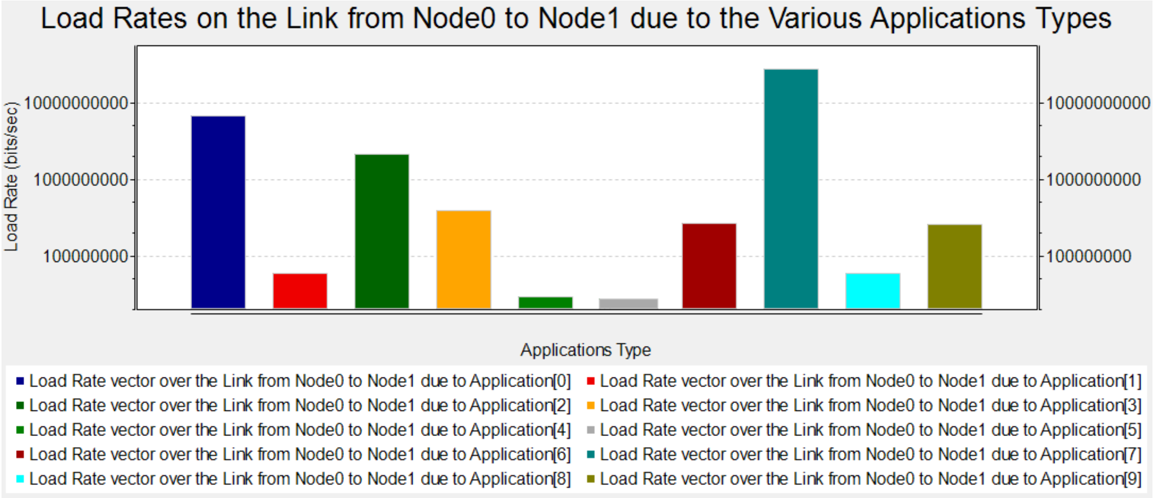


Figure 5.7 Load Rates on the Link from Node0 to Node1

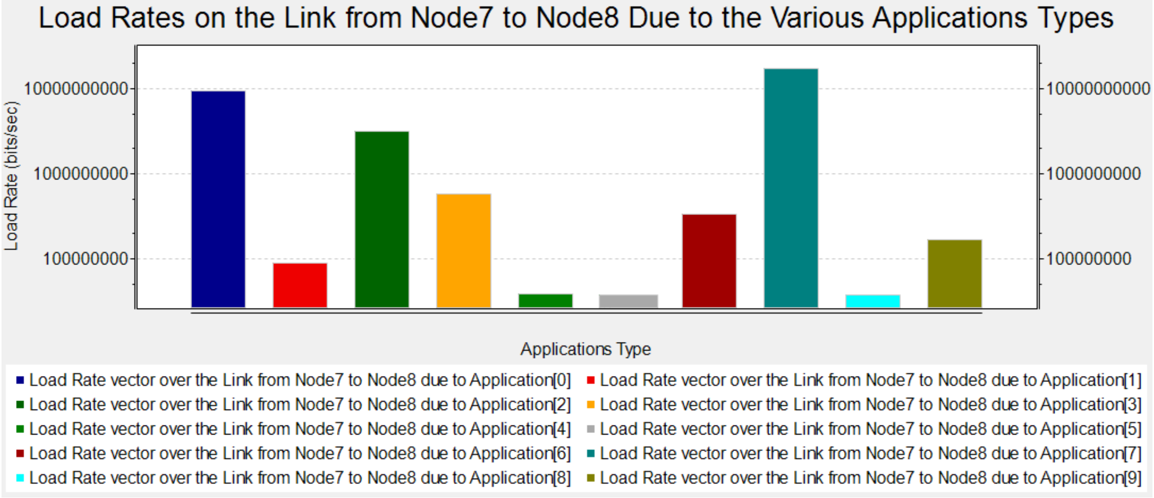


Figure 5.8 Load Rates on the Link from Node7 to Node8

5.4 Comparison with the Other Conventional Routing Protocols

Figures 5.9 and 5.10 highlight the benefits of our proposed routing techniques over the traditional load-balance-only-aware and latency-only-aware routing protocols respectively. From Figure 5.9, the load-balance-only-aware routing algorithm resulted in more end to end delays for the delay sensitive applications (5 hops) compared to our proposed scheme with 3 hops. On the other hand, Figure 5.10 shows that the latency-only-aware routing protocol misuses the links by concentrating the load on some links (the shortest paths links) and leaving the others with lowly congested. In other words it pays no attention to the balance of load over the different links resulting in a bad links' loads balance.

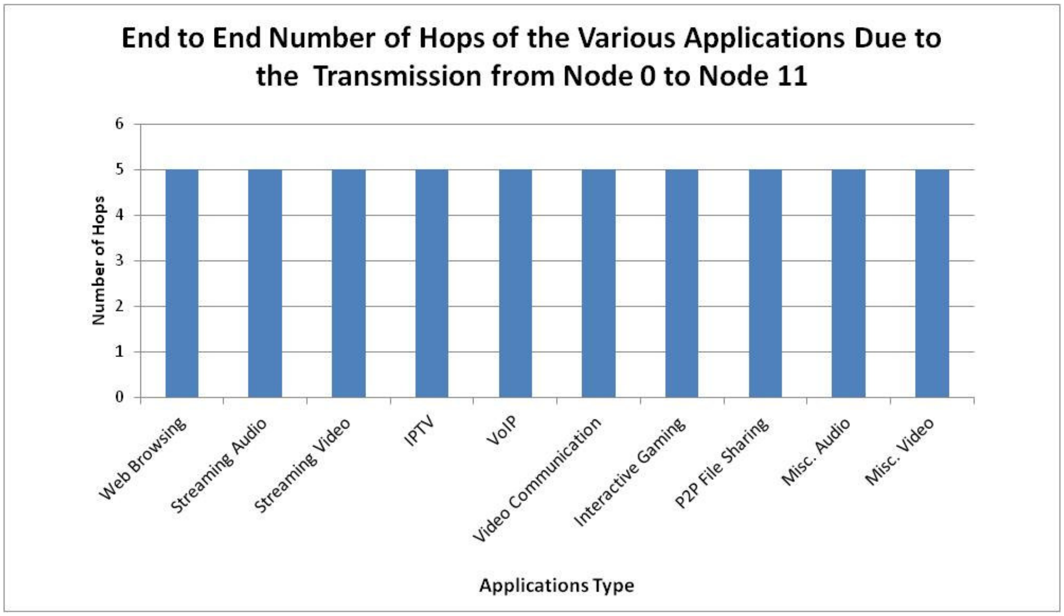


Figure 5.9 End to End Delays From Node0 to Node11 in Load Balance-aware Routing Protocol

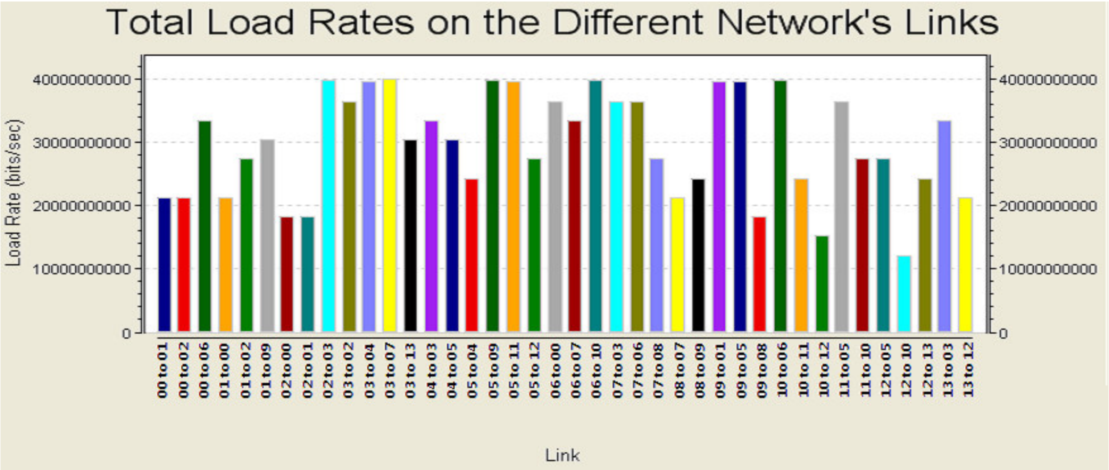


Figure 5.10 Load Rate Distribution in Latency-aware Routing Protocol

5.5 Summary

In this chapter, we developed a model that combined the optical burst switching technology with OpenFlow technology. This made the system inherit the fast information delivery gained from the characteristics of burst switching on one hand. On the other hand, it inherits the benefits of OpenFlow technology in making it easy to control and manage the network. Furthermore, dealing with traffic according to its contents provided users with a better QoS since it reduces the required number of hops for the delay sensitive applications, gives a more balanced links' flow distribution, and reduces the percentage of loss for the loss sensitive applications in the case of link's overloading. This could be a starting point to obtain a reasonable QoS despite the expected massive rise of user demands in the future Internet. OpenFlow represents a promising approach for managing the flow of traffic within networks which provides a wider range of traffic control compared to the other traditional switching techniques such as optical circuit switching, packet switching, and burst switching techniques.

Although separating control plane from the data plane in the switches creates an extra amount of traffic due to the communication of control signalling between these switches and their controllers via the secure channel, this amount of traffic is insignificant when compared to the bursts sizes. Only the first packet of burst which the network has not been trained for should be signalled to the controller, whereas the other packets within the burst are transmitted directly to the next hops without a need to process every packet's header.

When using fixed path least number of hops routing, the overloaded links must be shed resulting in data loss distributed amongst the application types on a bases of priority, where the higher priority application will experience less shedding. Our proposed routing protocol contributes to provide improved link utilization and link efficiency especially for those applications which are delay insensitive. Such applications will tolerate rerouting through the least congested links contributing to fairly distribute load rates over links. However, the qualities of service provided by our proposed scheme for all traffic types were within their acceptable limits. This network model could be the basis of a powerful OpenFlow network management tool for the future Internet.

Chapter 6

Adaptive Three-Layer Weighted Links Routing Protocol for Secure Transmission over Optical Networks

Bandwidth, latency and data security are the three major factors that affect the Quality of Service (QoS) for any computer network. Different applications running on a network have different requirements of these three factors, and dealing with all applications types in a similar manner is an inefficient approach. This chapter proposes a routing protocol that recognizes the type of traffic and routes it accordingly to provide the optimal QoS. Different data types are to be routed through different routes to satisfy the preferred QoS requirements of these data types. The weights of the network's links were partitioned in this chapter into three layers to accommodate these three QoS requirements factors.

-What's new: Security was introduced as a new significant QoS requirement for some applications, and a centralized security-ware QoS routing algorithm was proposed to accommodate these security requirements.

6.1 Introduction

Efficient routing algorithm must take into account that the data traffic on the Internet is not of the same type since they do not belong to a single class of applications. These different traffic types have different quality requirements and need to be dealt with differently. Some of the traffic over the Internet requires more bandwidth than others, whereas some other applications need less end-to-end delay (Latency). Furthermore, there are some other data that need to be dealt with most securely. For instance, phone-to-phone delay needs to be no more than 150 milliseconds delay to allow a comprehensible phone communications [95, 96]. Non real time applications like web browsing and email are less delay sensitive, but loss sensitive instead, therefore the Internet operator should allocate a sufficient bandwidth for them, otherwise when there is network congestion, their packets may be shed. When optical cable was first produced, it was considered to be immune against espionage. It has since been proven that it is not only possible to be insecure, but also, it could be simpler to tap than other predecessor technologies [9]. Oyster Optics Technology uses a sort of secure phase modulation to provide an efficient way for securing optical cables even in physical layer [9]. This technology, which is extensively explained in [9], has been utilised in this chapter to introduce security as one of the significant QoS qualifiers. Metrics used in this chapter to characterise applications' QoS requirements are the Available Bandwidth, Latency and Security.

This chapter is organized as follows. Section 6.2 will describe the related works proposed to enhance the QoS in computer networks. In section 6.3, the three QoS requirements considered in this chapter will be explained. In section 6.4, the proposed Three-Layer Weighted Link Routing Protocol (TLWLRP) will be explained. Section 6.5 explains the TLWLRP enabled weighted Djikstra routing algorithm. In section 6.6, an OMNeT++ model was created to simulate a sample optical network with the new routing protocol. Section 6.7 is concerned with the simulation results and their discussions. Finally, section 6.8 states some conclusions from this chapter.

6.2 Related Work

Research in the last decades focused on two issues of computer networking, namely, the QoS and the security, by dealing with them as two separate issues. Most of these works was achieved on Mobile Ad-hoc Networks (MANETs). In [97], three QoS requirements were considered to propose an enhanced QoS routing protocol for MANETs. These three requirements are bandwidth, latency and node lifetime. In addition to the fact that this protocol was proposed for MANETs whereas our proposal applies to optical networks, the last QoS requirement is more related to wireless Ad-hoc networks because they do not have a fixed infrastructure. In such networks, at any certain time, a node failure may occur since it is determined by the minimum battery lifetime of the node.

In [98], a system was presented to secure data over wireless Ad-hoc network as well. Elliptic curve cryptography was used to protect the privacy of information between the communicating nodes. It uses the idea of clustering to increase the system reliability. A limitation with [98] is that it considers only one QoS requirement, which is the security, ignoring other parameters.

Several researches have been made on QoS routing for optical networks [99-101]. These researches have two drawbacks. First, they did not consider the security as a factor that affects the QoS, whereas in this chapter security was considered as a third crucial parameter that contributes to the QoS in addition to bandwidth and delay. Secondly, they have treated each QoS requirement separately as an independent parameter, whereas some applications over the Internet need a mix of certain amounts of the different QoS requirements. For instance, VoIP communications need both high levels of latency and security, and an acceptable amount of bandwidth. On demand media can accept a lower level of security but high levels of bandwidth and latency.

In most research papers, security was dealt with separately, apart from being a QoS parameter, whereas other papers, which are interested in security, have no concern of the QoS and vice versa. An innovative way of protecting optical links from being tapped was proposed in [9]. Oyster optics' technologies attach a pair of secure oyster transceiver cards to every secure channel as shown in Figure 6.1 below.

This innovative idea for securing optical channels will be used in this chapter to introduce the security as a new QoS parameter to our proposed QoS routing protocol.

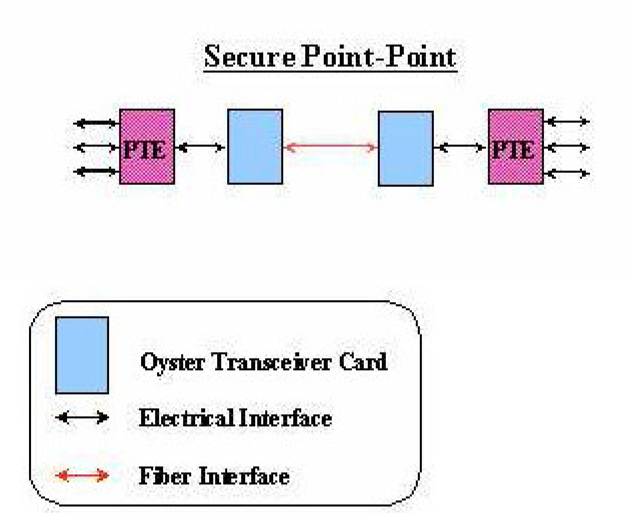


Figure 6.1 Using Oyster Transceivers for Securing Optical Channel [9]

6.3 QoS Requirements

Internet nowadays offers a wide range of services, such as web browsing, email, on demand audios and videos and other services. The main motivation behind the next generation research is to control the quality of services being offered to the users, and the range of these services. The current Internet uses the best effort protocol in dealing with all information types transmitted on it. In best effort technique, only one route is allocated for each source-destination pair, where all the traffic directed to the same destination is sent through the same path regardless of the traffic type. Therefore, it provides the same level of quality to all application types transmitted on it.

Three QoS factors were considered in this chapter: Bandwidth, Delay and Security.

6.3.1 Bandwidth

In traditional non QoS-aware optical burst switching, there is just one path to follow for each destination [102]. In the case that a link is congested, the information will be dropped negatively affecting the QoS. The network in this protocol never guarantees that all the sent data will be received without loss as shown in Figure 6.2. In this chapter, the required bandwidth for the data flow belonging to a particular application is estimated first, the available bandwidth of the paths leading to the destination is checked, and then the data will be transmitted across that path in which this data fit.

Applications differ in terms of the bandwidth they require. For instance, P2P file sharing is the most bandwidth consuming application, therefore, any shortfall in the channel's bandwidth will lead to a data loss. If the congestions of links are not taken into account, much of information will be lost. Note that the available bandwidth of a link is changing with the link's load. Therefore, our routing protocol checks the statistics of the links every time traffic is to be sent, and it chooses the available least congested path to transmit those applications with high bandwidth sensitivity to avoid data losses. This selection of the least congested routes will contribute to balance the load over the different networks' links. Packets lost en-route will either be retransmitted as it is the case in the TCP applications, or ignored possibly resulting in an impaired quality of the application output as in the case of UDP applications. In the first case retransmitting the lost data will increase congestion in the network and cost more delay for the application, and in the second case, the data will be lost at the application, therefore in both cases this will result in a lower QoS.

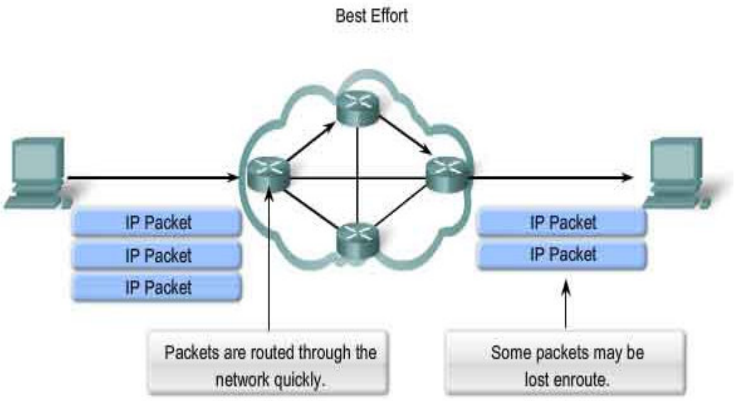

Best Effort
IP Packet
IP Packet
IP Packet
IP Packet
IP Packet
Packets are routed through the network quickly.
Some packets may be lost enroute.

Figure 6.2 A Network with Best Effort Protocol [103]

6.3.2 Delay

The end-to-end delay is another crucial requirement that affects the QoS [104]. In general, real time applications usually need special care in that requirement, because some applications cannot tolerate long delays and need to be dealt with as delay sensitive applications. The end-to-end delay between any two communicating parties is composed of four sub-delays: queuing delay, processing delay, transmission delay and propagation delay. In the optical networks, which is the case considered in this chapter, the speed of data transmission and propagation is so high that these delays can be neglected.

Queuing delay is the time required for a packet to wait until it can be processed (processing time) in the node's buffer and sent when the transmission channel is ready. It is directly proportional to buffer size. When the packet arrival rate at a particular optical router exceeds the buffer's packet transmission rate, the packets will be accumulated in the buffer, and when the buffer fills, the surplus packets will be dropped.

If the packet arrival rate of a particular queue is more than its packet departure rate, the packet loss rate will be unpredictable and will sharply increase. Consequently, a feedback could be sent to the sending entity to regulate its transmission rate. However, a queuing delay and a processing delay are also required at each hop, therefore, reducing the number of hops will reduce the total time consumed due to traffic queuing and processing.

In optical networks, it is currently technologically infeasible to have an optical cache that keeps a store of the high bandwidth traffic transmitted on the optical cables. To solve this problem, the optical data should be first converted to electronic form, queued in an electronic buffer, processed electronically in that queue, and then converted back to its optical form. This can be performed by Optical-Electronic-Optical converters.

6.3.3 Security

Data security is one of the most significant QoS factors. Although the Internet represents a completely insecure media for exchanging information, some private information needs to be transmitted on the Internet. This information needs to be transmitted securely without being revealed or attacked by intruders. Using cryptography is one of the methods used to protect the privacy of information, where data is converted into an encrypted form. The original data is called plain text, and the encrypted data is called cipher text. Only the authorised user at the destination will be able to decrypt the message. Cryptography is an efficient way of protecting data from unauthorized access to these data, but it still has its own drawbacks. One drawback is that its protocols run in the presentation layer of OSI model, or below the high level application protocols and above the TCP/IP layer in TCP/IP model. That means that it will leave all the underlying layers insecure. So it does not work to protect data in the physical layer, where intruders still have the opportunity to extract data by tapping the cable connecting the communicating entities.

Another problem with cryptography is that it depends on a mathematically solvable algorithm, with one secret key. There is no real existence of what is so called unbreakable cryptographic scheme, since by using the new technologies, fast processors and brute force algorithms, the secret key can be derived [105]. However, cryptography has a small usability rate due to the difficulties in implementation and maintaining and the high cost associated with using it [106].

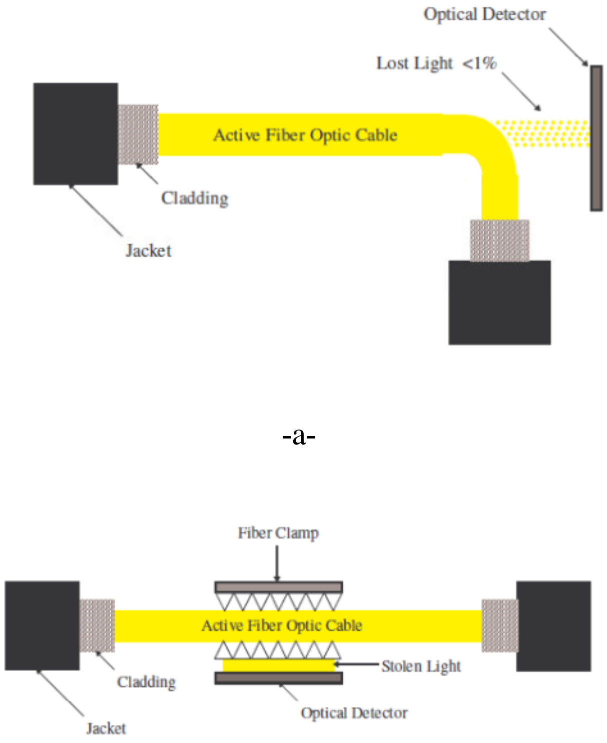
In optical networks there are a lot of techniques used by intruders to tap the optical cable. All of these tapping techniques fall into one of these optical tapping categories:

A- Splicing: This tapping method is done by splicing the optical cable between the two communicating parties, and inserting a sensor between the two splices. This sensor allows the two communicating parties to exchange information, but sends this information to a third party (intruder) as well.

B- Splitter and Coupler: In this method no splicing is necessary. The cable is either bent to allow a small amount of the light to escape from the optical cable to be captured by photo-detector equipment as shown in Figure 6.3-a, or a clamp with an optical detectors is placed somewhere on the cable to detect the information as in Figure 6.3-b. Receiving just 1% from the light of signal in the cable will be enough to detect the information transmitted on that link.

C- Non-touching tapping: In this method no interference with the optical cable is required, because this method depends on capturing the small amount of light naturally radiated from the cable.

Since cryptography does not work in the physical layer as mentioned before, it is infeasible to use it in protecting the optical cables tapping. As an alternative, Oyster Optics technology can be used to supply some of the network's links with a high level of security at the physical layer.



-a-

-b-

Figure 6.3 Optical Tapping Using Splitter and Coupler Method

Oyster Optics technology uses a patented method of secure phase modulation for securing data over the optical link. This security technique is fully explained in [9].

Two application types, namely, VoIP and video communications, were assigned high security sensitivity in this chapter, and ten links in our optical network were secured using Oyster Optics technology to supply the network with secure routes for the transmission of these private data.

6.4 Three-Layer Weighted Link Routing Protocol (TLWLRP)

This chapter suggests breaking the link weight into three sub weights (layers), namely, the available bandwidth, the latency, and the security. Each packet over the network has TOS (Type Of Service) bits in its header to define the class of traffic as shown in Figure 6.4. Each application has three coefficients (k1, k2, k3), one to reflect the importance of each of the QoS requirements to this application type. The sum of these coefficients equals 1. For instance, interactive gaming traffic is a very small bandwidth consuming application; therefore, the bandwidth is not of real importance since just a little amount of it will be sufficient, so k1 is set to the value of 10%. On the other hand, this application type is very delay sensitive, therefore, traffic due to this type needs to be routed as fast as possible [101], k2=90%. Security is not of real importance for this class of traffic, k3=0%. The resultant link weight, which will be used to choose the optimal path to the destination according to these QoS requirements, will be calculated using equation (6.1) below.

$$\begin{aligned}\text{Total Weight} = {} & (\text{k1} \times \text{Available Bandwidth}) \\ & + (\text{k2} \times \text{End-to-End Speed}) \\ & + (\text{k3} \times \text{Security}) \qquad (6.1)\end{aligned}$$

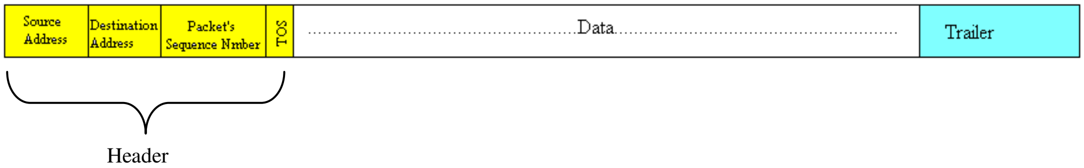


Figure 6.4 Typical Packet's Structure with TOS Entry

The weighted Djikstra routing algorithm, with some changes to accommodate these three-layer sub weights, was used in this chapter in an OMNeT++ simulation platform to select the desired routes to the different destinations.

Note that the percentage of the available bandwidth is calculated using equation (6.2) below [107].

$$B\_A= \left[1 - \left(\frac{Used\ Bandwidth}{Channel\ Capacity}\right)\right] \times 100\ \% \qquad (6.2)$$

Where B_A is the available bandwidth of the optical link. As the name of our proposed protocol implies, the available bandwidth is to be adapted and updated with time to give the protocol a clear image of how the link is utilized.

The network layer is responsible for the routing protocols; therefore, our TLWLRP function should be placed at that layer as shown in Figure 6.5 below. A signalling system is used supply TLWLRP with QoS requirements of the different applications from the application layer, and link utilization information from the physical layer.

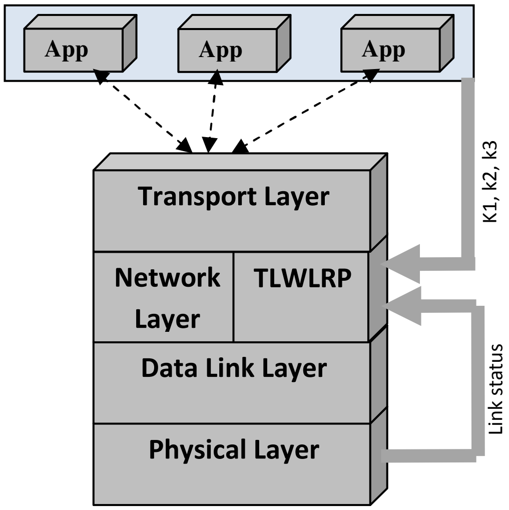


Figure 6.5 Internet Layered System with TLWLRP

Using TLWLRP means that applications between the same source and destination nodes may take different routes according to the QoS requirements of the application and the route characteristics. The proposed routing protocol offers high reliability in cases of nodes or cable failure. This is because the protocol will automatically choose the alternative second optimal route to deliver the traffic.

6.4.1 Applications and QoS Requirements

Different applications have dissimilar QoS requirements. Nine application types were considered in this chapter. These application types cover all types of possible applications used on the Internet nowadays [73, 74]. These applications are: web browsing, streaming audio, streaming video, IPTV, VoIP, video communication, interactive gaming, P2P file sharing and miscellaneous uploads and download.

However, the applications on the current Internet are categorized into two main categories:

A- Asymmetric Applications:

Those applications, which do not request equal resource consumptions on the both end-point hosts, are termed as asymmetric applications.

B- Symmetric Applications:

The applications under this category request the same amount of resource consumptions on the both end point hosts.

According to this classification, each of our applications used in this chapter falls into one of the following classes: Non Real Time and Asymmetric, Real Time and Asymmetric, Real Time and Synchronous.

6.4.1.1 Non Real Time and Asymmetric

This class includes those applications, which do not have any demanding delay and loss QoS requirements. The best way to deal with these applications is by using the first-come, first-served technique, or what is well known as best effort protocol. Examples of these applications are:

- Web browsing
- Miscellaneous uploads and downloads.
- Streaming Audio and video applications.

-P2P file Sharing.

Notice that all the non-real time applications are asymmetric. This is because in the non-real time applications, a client requests services from a server.

6.4.1.2 Real Time and Asymmetric

Those applications with real time requirements need an acceptable latency since they use real time protocols e.g. UDP and do not have time to invoke an Automatic Repeat Request (ARQ) protocol. Security is not an important QoS requirement for these applications because the nature of the traffic being communicated is not private. Interactive gaming falls in this class.

6.4.1.3 Real Time and Synchronous

Some applications request stringent QoS requirements. Applications in this class are considered bandwidth insensitive since they require very little amount bandwidth, latency sensitive and are security sensitive. Examples of the application in this class are:

-VoIP.

- Video Communications.

The values of factors K1, K2 and K3 in Table 6.1 were derived from the QoS requirements statistics for the different applications in [95] and [96].

Table 6.1 QoS Requirements Weightings for the Different Applications

Application	K1	K2	K3
Web Browsing	0.75	0.25	0
Streaming Audio	0.40	0.60	0
Streaming Video	0.50	0.50	0
IPTV	0.30	0.70	0
VoIP	0.10	0.45	0.45
Video Communications	0.05	0.47	0.48
Interactive Gaming	0.10	0.90	0
P2P File Sharing	0.90	0.10	0
Misc. Up/Download	0.50	0.50	0

6.4.2 Securing Channels on Optical Networks

Oyster Optics, Inc. represents a way for securing links in an encryption-free manner by using secure modulation approach [9]. Since this security operation takes place in the physical layer, all the upper layers will be protected as well [9]. One of the major benefits of this security technique is its possibility to be applied to the already existing infrastructure. It is infeasible to change the entire optical communication infrastructure in order to get all the data transmitted over the network secured, as this will be a costly process. In addition, some applications do not need their traffics to be secured. The best solution is to replace the transceivers of some optical links by secure Oyster transceiver cards in order to create some secure paths across the already existing optical network as shown in Figure 6.1. Our proposed routing protocol was employed to route the security-sensitive data through these secure paths.

6.5 TLWLRP Enabled Weighted Djikstra Routing Algorithm

The weighted Djikstra algorithm for finding the preferred path used in chapter 6 has been modified here to accommodate the novelty of breaking the link's weight into 3 layers. The flowchart of the modified algorithm is shown in Figure 6.6 below.

However this Algorithm serves centralized routing, where it assumes that there is a central party that periodically monitors the status of the different network's links. Any change in the loading of the network or any connectivity failure occurs in the network will be detected by the central monitoring entity and consequently all the nodes' routing tables will be updated accordingly. Of course adopting such assumption will cost the network a substantial amount of overhead. This amount of overhead will increase as the monitoring and routing tables updating frequency increases. This is considered as a drawback of centralized routing protocols, but this will be the cost of offering automatically reconfigurable QoS routing.

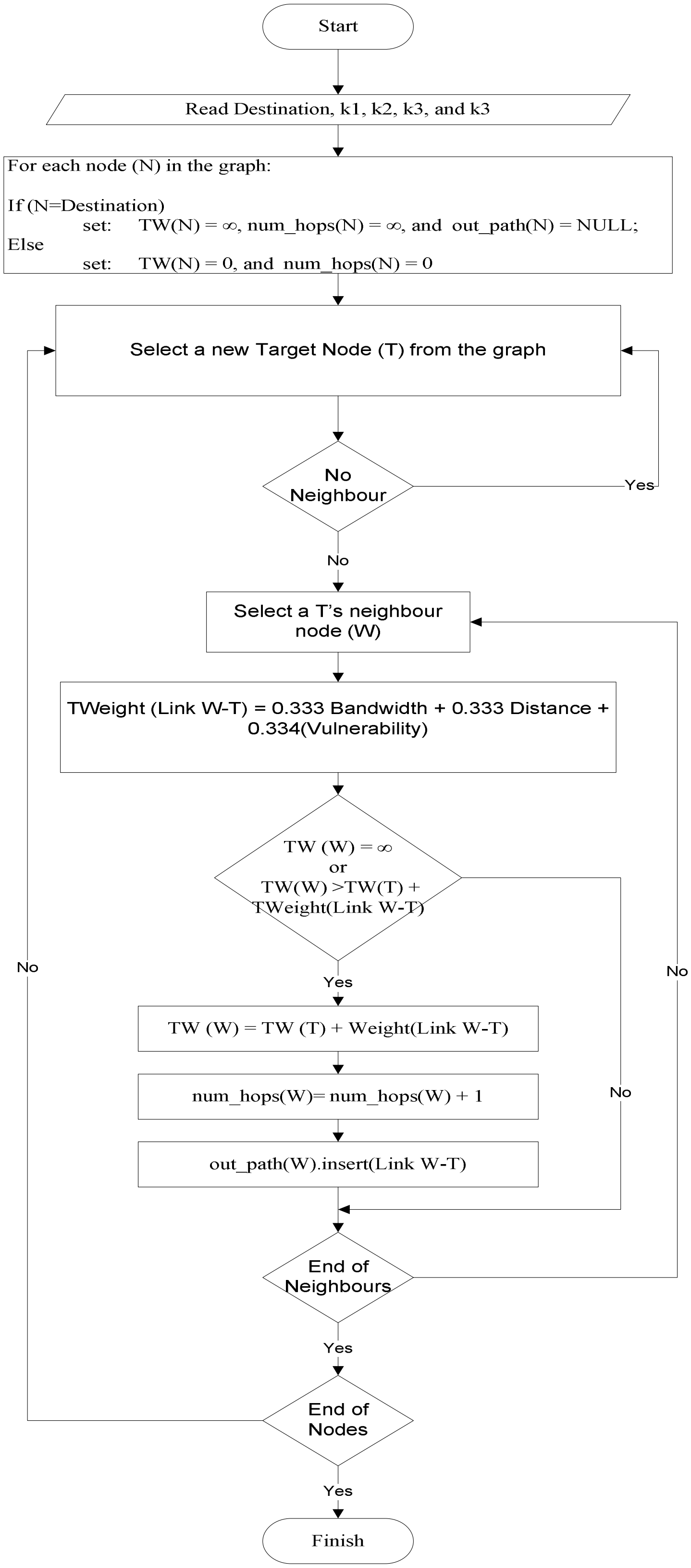

Start
Read Destination, k1, k2, k3, and k3
For each node (N) in the graph:
If (N=Destination)
set: TW(N) = ∞, num_hops(N) = ∞, and out_path(N) = NULL;
Else
set: TW(N) = 0, and num_hops(N) = 0
Select a new Target Node (T) from the graph
No Neighbour
Yes
No
Select a T's neighbour node (W)
TWeight (Link W-T) = 0.333 Bandwidth + 0.333 Distance + 0.334(Vulnerability)
TW (W) = ∞ or TW(W) >TW(T) + TWeight(Link W-T)
Yes
No
TW (W) = TW (T) + Weight(Link W-T)
num_hops(W)= num_hops(W) + 1
out_path(W).insert(Link W-T)
No
No
End of Neighbours
Yes
End of Nodes
Yes
Finish

Figure 6.6 TLWLRP Enabled Weighted Djikstra Routing Flowchart

6.6 System Simulation

The optical network shown in Figure 6.7 was simulated using OMNeT++ simulator to investigate the QoS improvements gained using our proposed routing protocol. Nineteen nodes were interconnected through both secure and unsecured optical links. Each node represents a Regional Area Network (RAN) with 10000 users. Ten links were secured using the Oyster Optics technology mentioned in section 6.4.2.

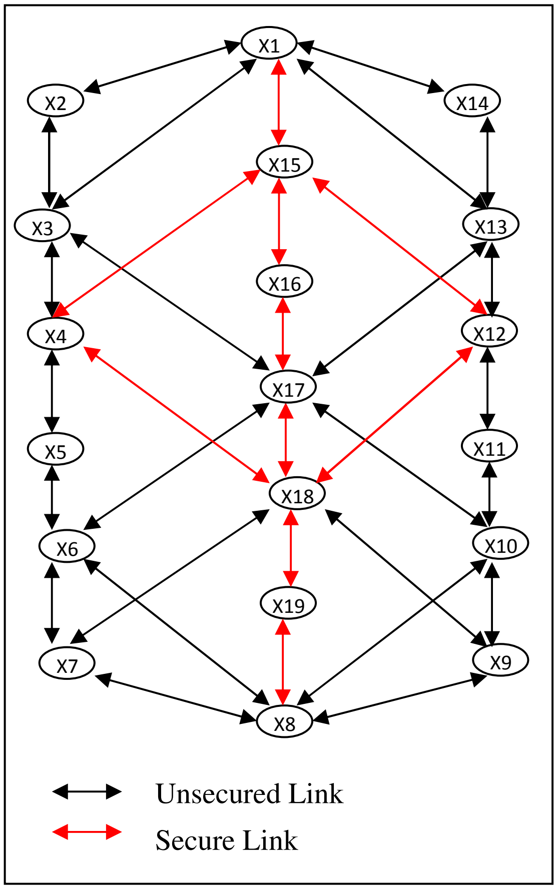


Figure 6.7 Optical Network with Secure and Unsecured Links

The nine application types defined in Table 6.1 were applied to the network. In order to easily investigate the feasibility of our proposed routing protocol, and to clarify the behaviour of the proposed routing technique against different QoS requirements, the traffic over the network links due to three application types were focused on and analysed. These three applications are: P2P file sharing, interactive gaming and VoIP. These three applications were chosen because P2P has (0.9, 0.1, 0.0) QoS requirements as shown in Table 6.1, therefore, it is extremely bandwidth sensitive. Consequently, it can be analysed to prove the efficiency of bandwidth selectivity in our proposed scheme. Interactive gaming (0.1, 0.9, 0.0) on the other hand is a very delay sensitive application, and was analysed to show the delay latency selectivity. Finally, VoIP (0.1, 0.45, 0.45) was used to test the security selectivity of TLWLRP. Traffic load rates were computed in the same manner as in chapter 5.

6.7 Results

To investigate the feasibility of this proposed routing protocol clearly, three application types, namely, P2P file sharing, interactive gaming and video communications, were put under the focus, and the traffics due to them were calculated on the different networks' links. The QoS requirements patterns for these application types are (0.9, 0.1, 0.0), (0.1, 0.9, 0.0) and (0.1, 0.45, 0.45). Mainly, four benefits were gained from our proposed routing protocol: releasing more bandwidth from the congested links to avoid data loss when the amount of traffic exceeds the channel capacity, reducing the end to end delay for the delay sensitive applications, securing the private data over the network and links' load balancing.

6.7.1 Bandwidth Gain

Figure 6.8 shows that the rate of increase in the used bandwidth of the link (link utilization) due to P2P file sharing decreases with the increase of the total network load rate corresponding to that application type to allow spreading load over the other links leading to an improved links' utilisations. The available bandwidth is a vital factor in choosing the optimal route for this application type. This enhances the links' utilisations because the traffics select the route with the most available bandwidth and avoid the congested ones.

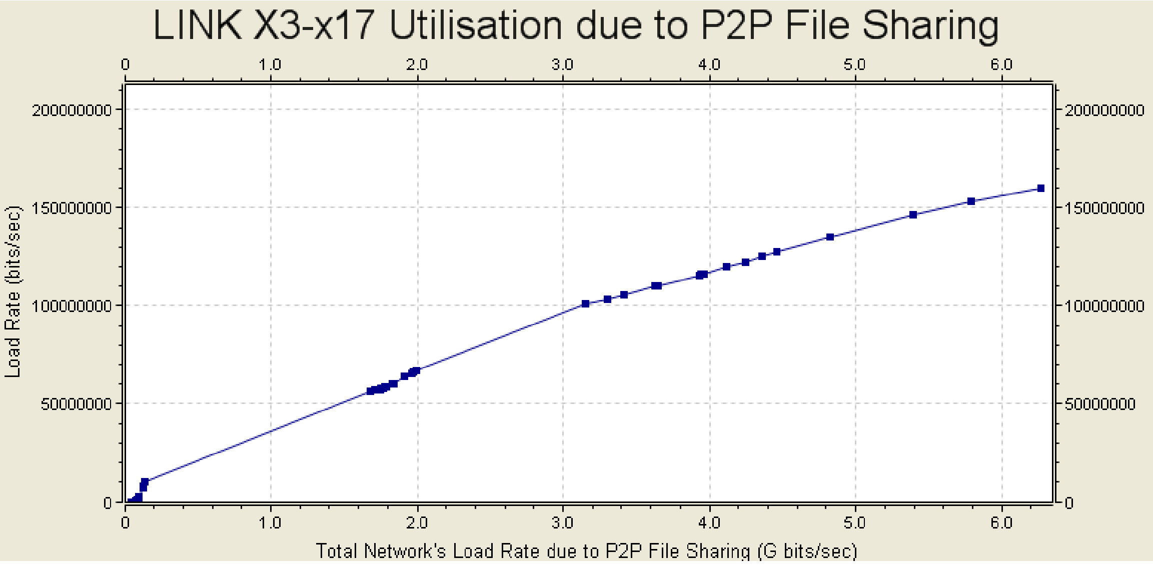


Figure 6.8 Link x3-x17 Utilisation Due To P2P File Sharing

6.7.2 Delay Gain

The traffics over the various network's links due to interactive gaming (0.1, 0.9, 0.0) are shown in Figure 6.9. This type of traffic prefers those routes with the minimum end to end delay. Since our network is optical, the link speed is very high and we assume that the propagation time is negligible. The Optical-Electronic-Optical (O-E-O) conversions are the most time consuming operations. Since one O-E-O conversion is required for each hop, the optimal route to be chosen is that of the minimum number of hops. Most of the high bars in Figure 6.9 represent the load over the sloping (diagonal) links in Figure 6.7 because these links serve to decrease the number of the required hops to their destinations. Therefore, these routes will be loaded more than the others with this QoS requirements pattern.

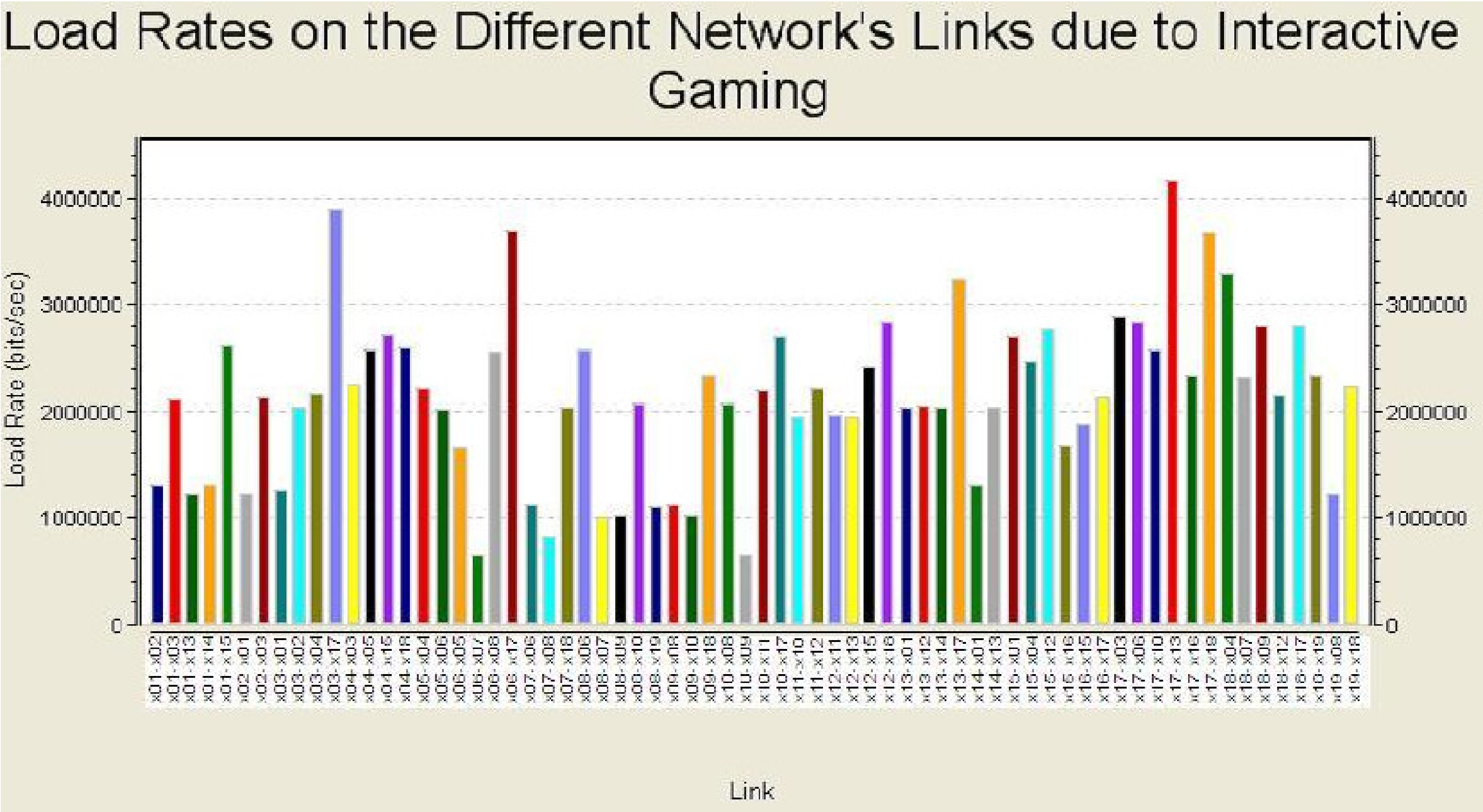


Figure 6.9 Load Rates on the Various Network’s Links due to Interactive Gaming

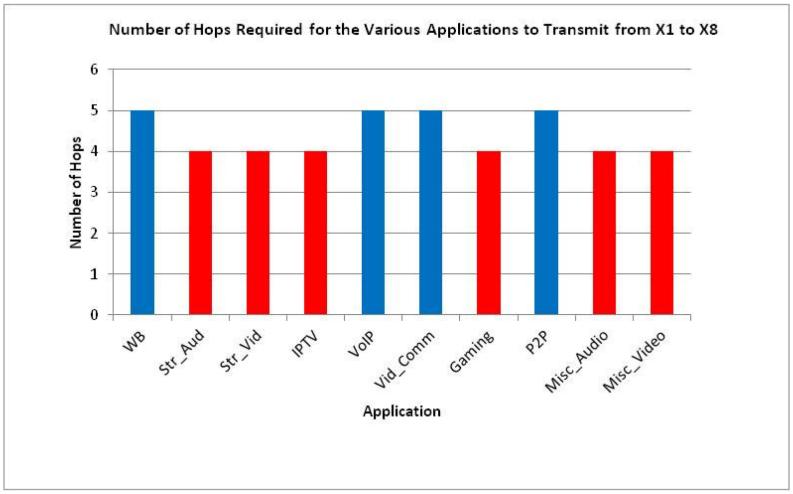


Figure 6.10 Number of Hops Required For the Various Applications to Transmit From X1 to X8

Figure 6.10 shows the number of hops required for the different applications in our application mix to transmit from X1 to X8. The diagonal routes (x1-x3-x17-x6-x8) and (x1-x13-x17-x10-x8) represent the available minimum number of hops routes from X1 to X8 with four hops. Therefore, interactive gaming, IPTV, streaming audio, streaming video and miscellaneous up/downloads follow these routes since they all have relatively high delay sensitivity. On the other hand, P2P file sharing and web browsing are bandwidth sensitive applications, thus they select those routes of the highest available bandwidth, i.e., they avoid the congested links which were allocated for the five delay sensitive applications even if they are the shortest path routes. The two remaining application types, VoIP and video communications are security and delay sensitive applications. Consequently they look for minimum delay and maximum security available routes to send their traffics through. Even though these applications tolerate one more hop than the minimum number of hops but that would be at the expense of increasing the path's security as shown in Figure 6.12.

6.7.3 Security Gain

Figure 6.11 below shows the traffics over the links due to VoIP. From this figure, it is clear that the secure links (red links in Figure 6.7) are the most congested links because the traffics due to this type of application is security sensitive, thus it prefers transmitting data over the secure links.

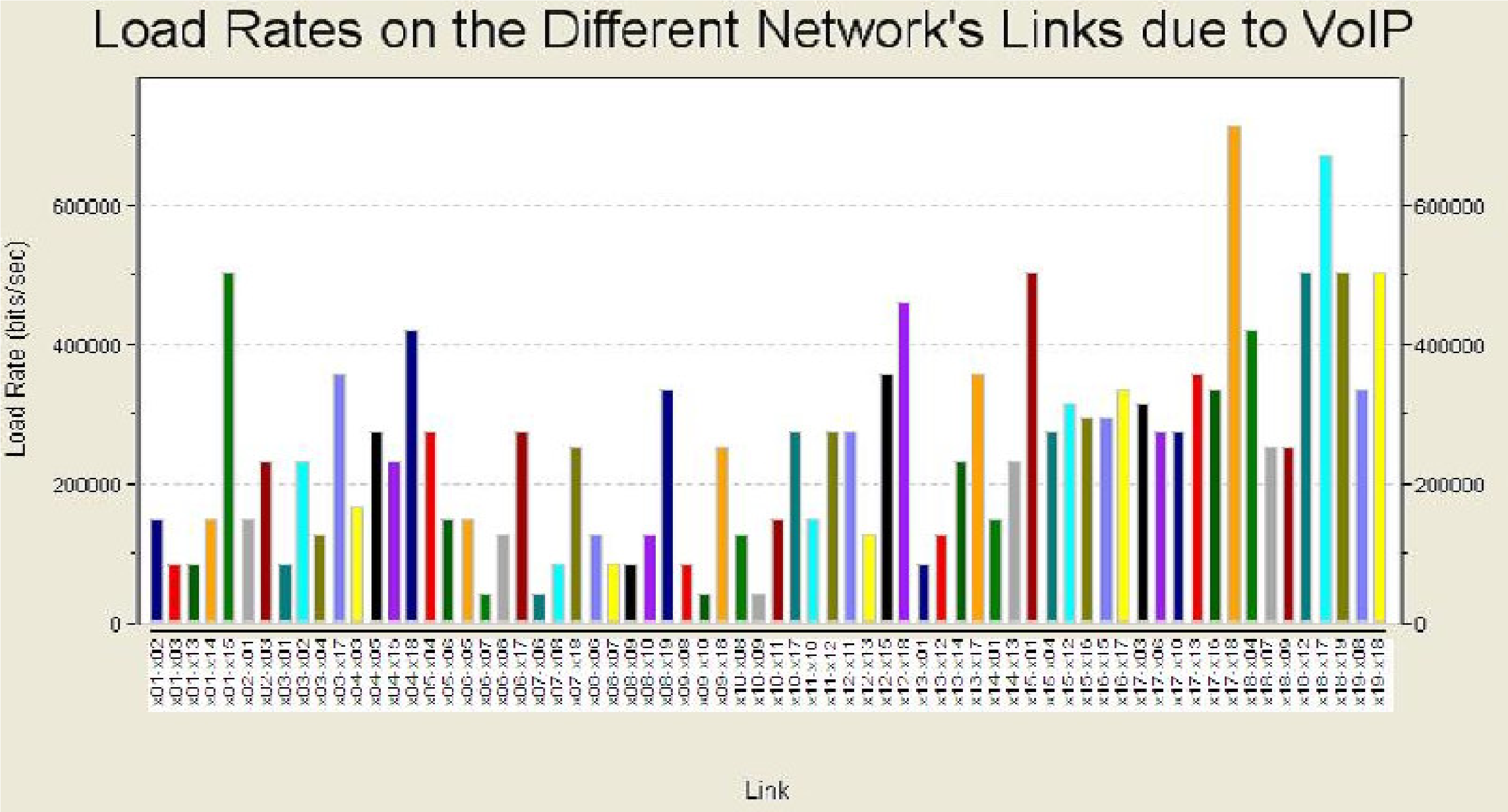


Figure 6.11 Load Rates over the Various Links due to VoIP

From Fig.7.12 note that VoIP and video communication were completely secured to a percentage of 100% by transmitting through the routes (X1-X15-X4-X18-X19-X8) and (X1-X15-X12-X18-X19-X8), whereas web browsing and P2P file sharing were partially secured to 60%. That is not because we need them to be secured, but because their routes are through some secure links to avoid the congestion of the other links since they have relatively high bandwidth sensitivity.

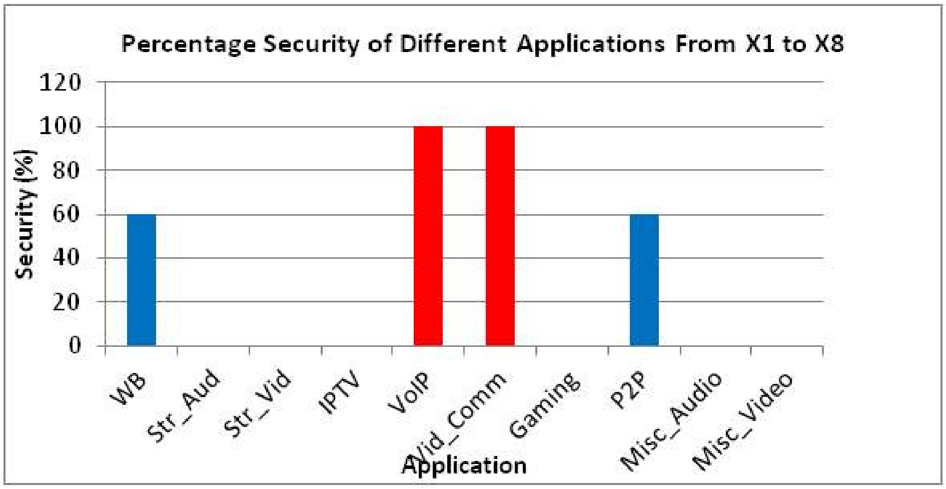


Figure 6.12 Security Percentages of Different Applications for the Traffics from X1 to X8

6.7.4 Load Balance

Bandwidth sensitive applications will also contribute to improve the link utilization efficiency as a consequence of balancing load rates over the different links. Figure 6.13 clarifies how the P2P File Sharing load rate is balanced over the various links.

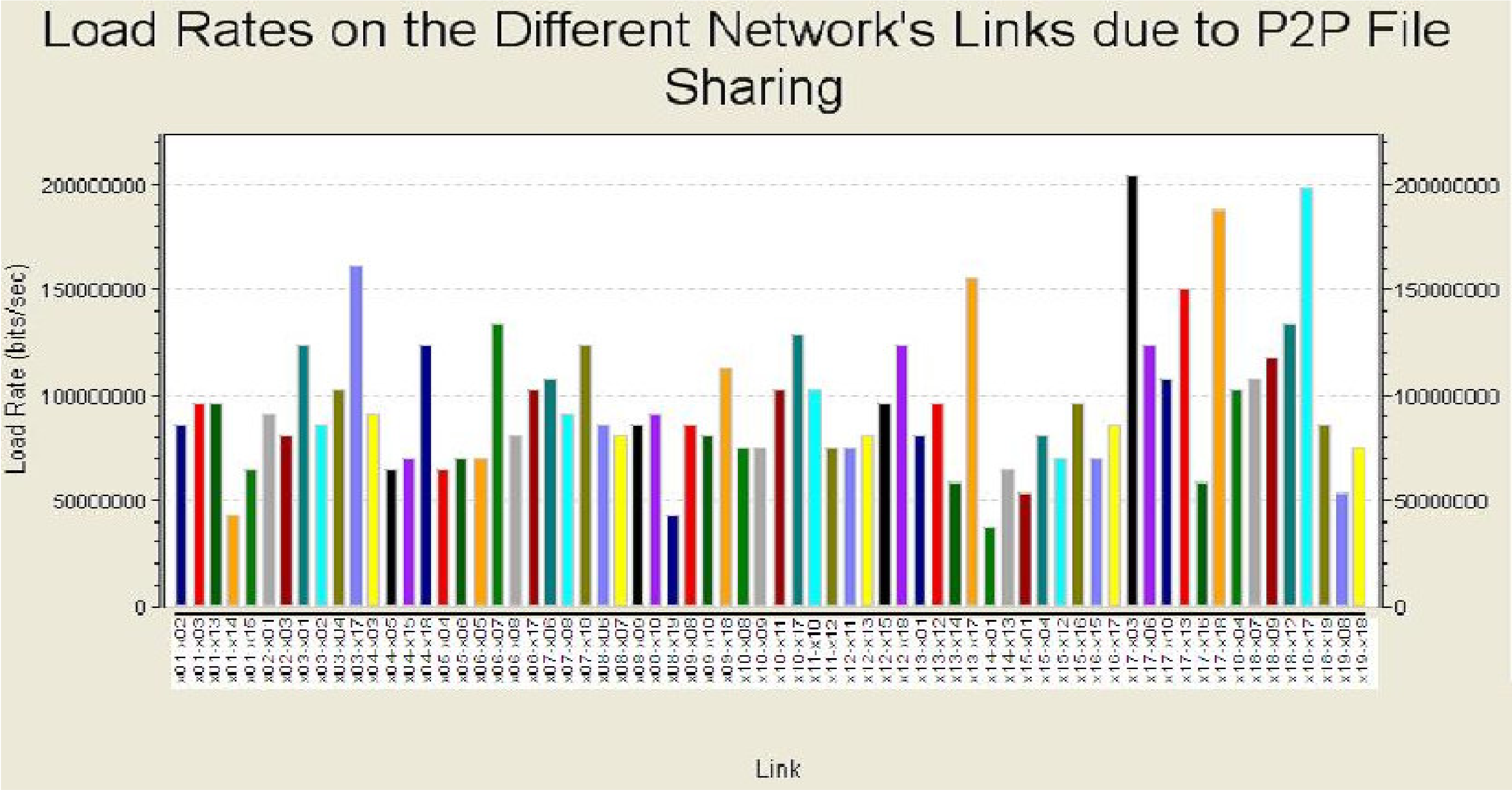


Figure 6.13 Load Rates over the Various Links due to P2P File Sharing

6.7.5 Comparison with Other Routing Protocols

Two conventional routing protocols were selected here to compare our proposed routing with them. These protocols are: Latency-Aware Routing Protocol and Congestion Aware Routing Protocol.

a) Latency-Aware Routing Protocol

In latency-aware routing, the end to end delays for all traffics types are minimised, where it is clear from Figure 6.14 that the number of hops from X1 to X8 was minimised to only four hops regardless how sensitive this information is to delay, but on the other hand, it does not differentiate among the different traffic types. This creates congestions over the fast delivery routes (diagonal links) as is shown in Figure 6.15 below, where it is clear that the load is not fairly distributed over the network's links and the network's links are inefficiently utilised.

The current latency-aware and congestion-aware routing techniques conventionally offer 0% security for all information since no links were secured in these conventional routing techniques. However, the security results will still be discussed in this section supposing that the predefined links are still OOT secured since such securing was performed in the hardware phase. Figure 6.16 shows that the latency-aware routing technique offers 0% security for all information even though the secure links still exist because the preferred (shortest) path between x1 and x8 (x1-x3-x17-x6-x8 or x1-x13-x17-x10-x8) has no secured portions throughout its length.

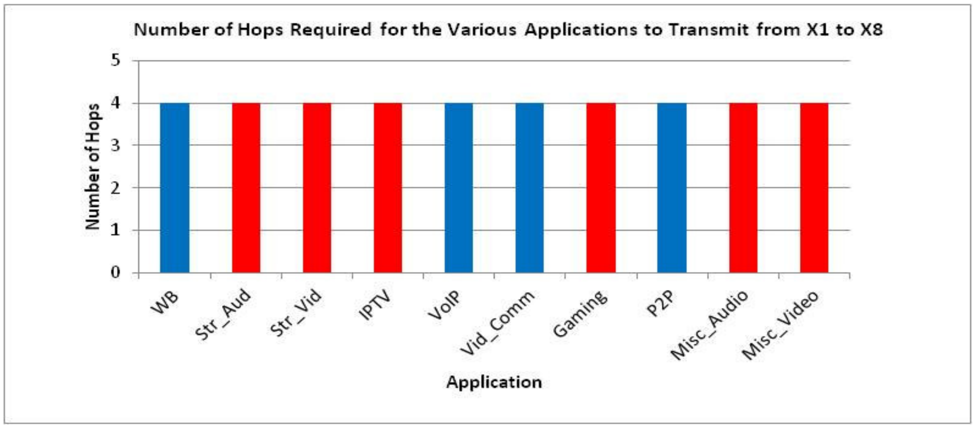


Figure 6.14 Total Number of Hops Required for the Various Applications to Transmit from X1 to X8 in Latency-Aware Routing

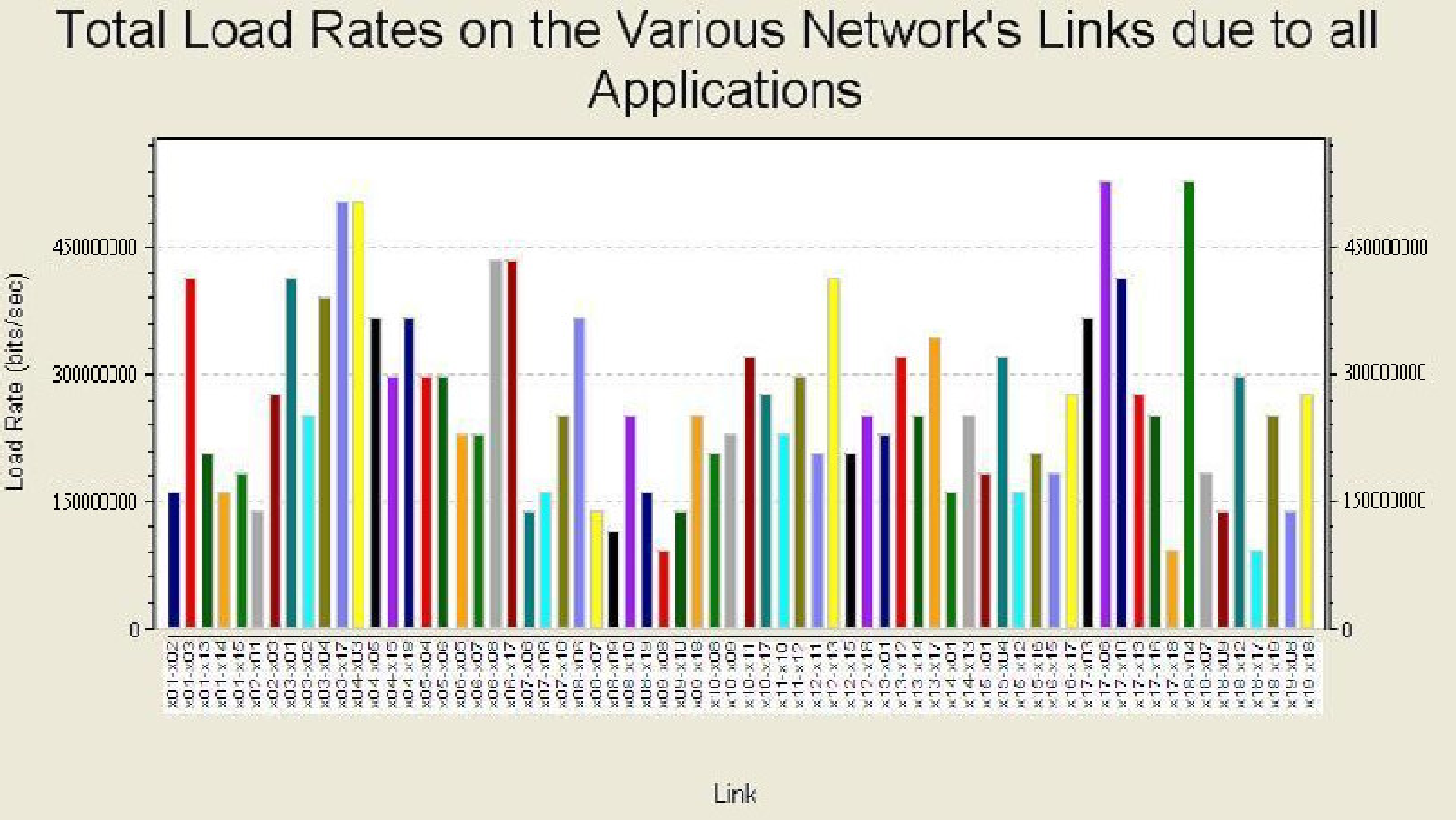


Figure 6.15 Total Load Rates on the Various Links due to All Applications in Latency-Aware Routing

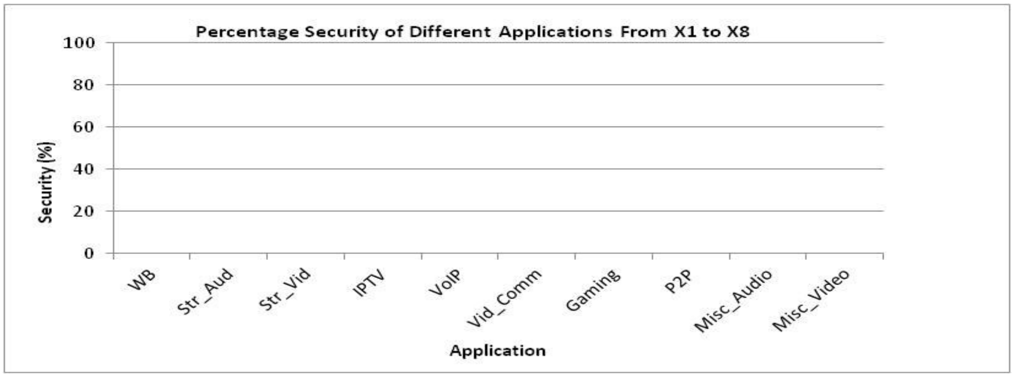


Figure 6.16 Security Percentages of Different Applications for the Traffics from X1 to X8 in Latency-Aware Routing

b) Congestion-Aware Routing Protocol

This routing technique enhances the links' efficiencies by balancing the load over them as shown in Figure 6.17, but it still does not differentiate among the traffic types, and does not offer any QoS other than the congestion avoidance. The achieved load balance will be at expense of extra end to end delays for the information as shown in Figure 6.18. Again, conventional congestion-aware types offer 0% security level since oyster optics secured links has not been used with this routing technique. Figure 6.19 shows the percentage of security achieved by the latency-aware routing protocol when these predefined secure links still exist. This figure shows that the information will inadvertently gain a low level of security (20%) since the security is not the QoS factor of consideration by this routing protocol.

These results show that our proposed routing technique outperforms other routing protocols since it differentiates among the different traffic types, utilizes all the bandwidth, whilst meeting the desired latency and security QoS requirements by making suitable routing decisions.

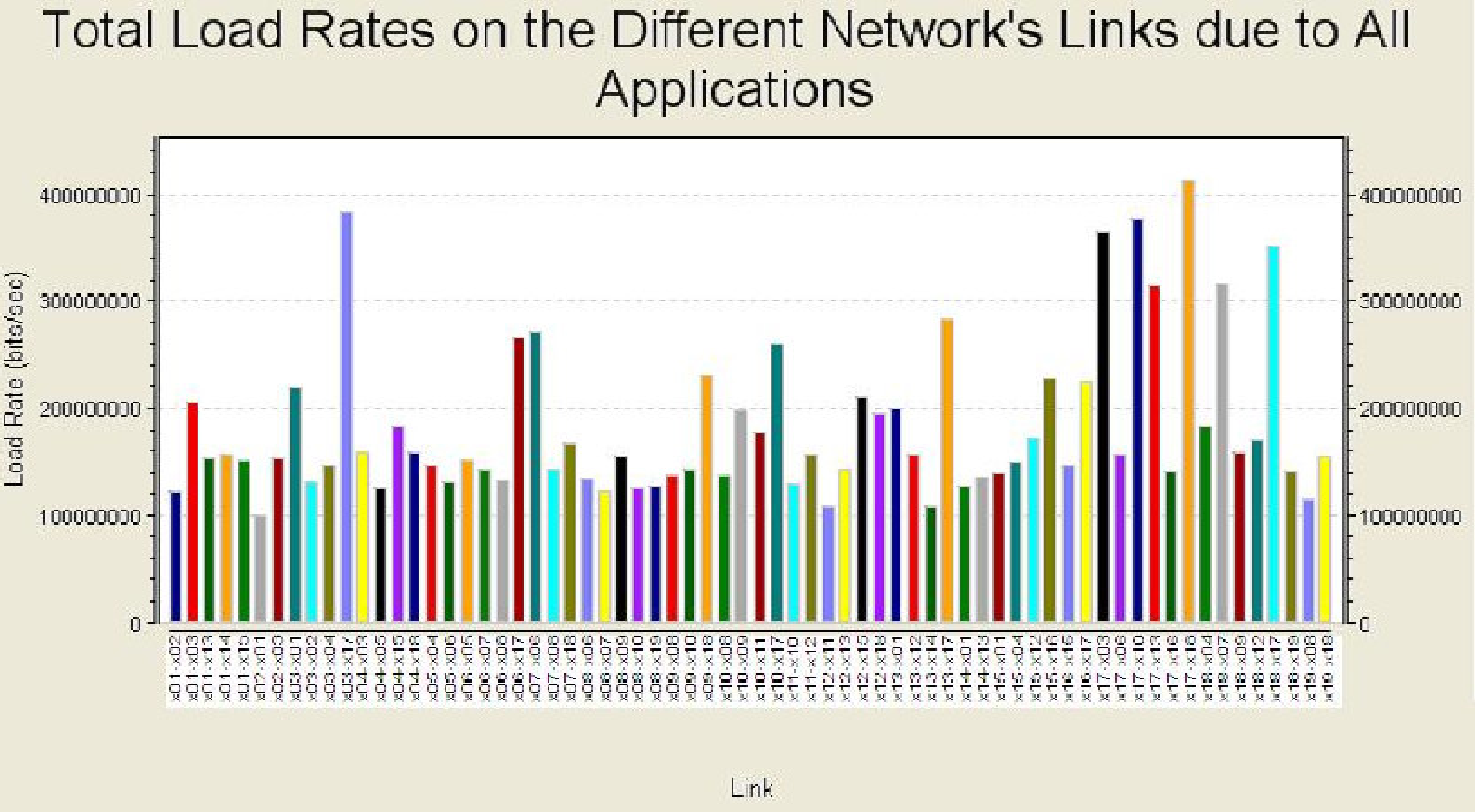


Figure 6.17 Total Load Rate on the Various Network’s Links due to all Applications in Congestion-Aware Routing

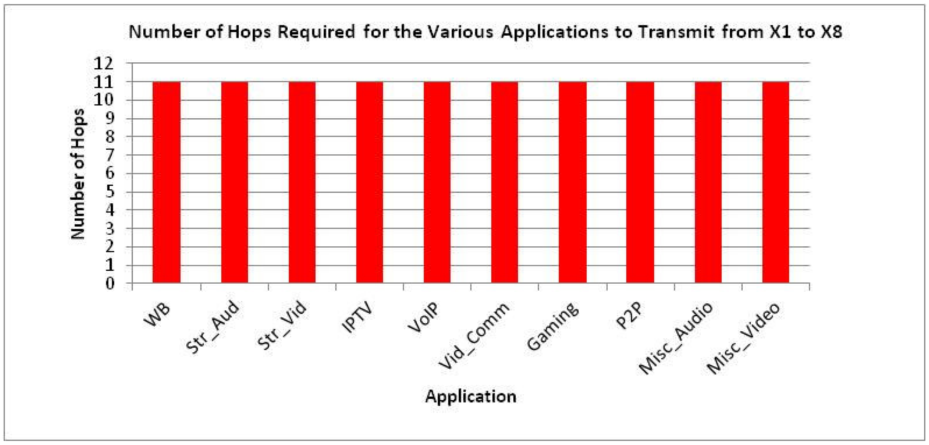


Figure 6.18 Total Number of Hops Required for the Various Applications to Transmit from X1 to X8 in Congestion-Aware Routing

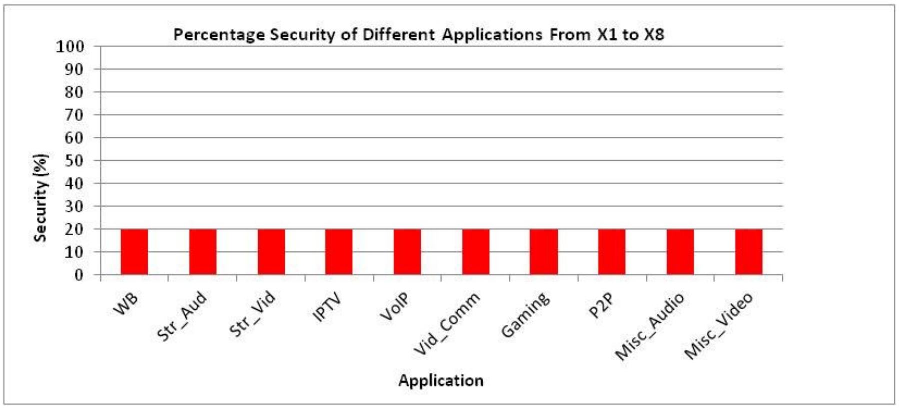


Figure 6.19 Security Percentages of Different Applications for the Traffics from X1 to X8 in Congestions-Aware Routing

6.8 Summary

This chapter proposes a novel routing protocol for improving the QoS in optical computer networks. Three QoS issues have been addressed here, namely: bandwidth, delay and security. Oyster Optics security technology was used by inserting some transceiver cards on some optical links in order to get them secured.

A mix of nine application types was applied to a sample optical network with some secure links. Each of these applications was assigned three factors k1, k2, and k3 to reflect the significance of available bandwidth, end-to-end delay, and security issues to that application. The optical link weight was divided into three layers to accommodate these three QoS significance factors.

By keeping a track of the load rate changes on the different network's links, this routing protocol is able to be adaptive, since it continuously reads and updates links' statuses by using physical layer sensors to inform TLWLRP in the network layer of the new links' statuses. This information together with the information of QoS requirements from the application layer is used by TLWLRP to select the optimal route for each type of traffic.

The results of our simulations shows that the benefits of this routing technique is that, compared to more conventional techniques, it releases more links' bandwidths, provides more efficient links utilisation, decreases the end-to-end delay for the delay sensitive applications, provides secure transmission for private data, and balances load rates on the different network's links. Overall, it clearly improves the QoS offered by the network.

However, a modified Djikstra routing algorithm has been used in this chapter on a centralized adaptive routed network. The amount of data overhead rises from using such a centralized routing protocol, due to signalling and routing table updates, propagation can be conceived as a cost for the level of QoS offered to the network. However this problem of overhead will be resolved to a large extent in the next chapter (chapter 8) by adopting an artificially intelligent distributed routing protocol called ant routing protocol.

Chapter 7

Distributed RGB Pheromones Ant Routing with Enhanced QoS on Optical WDM Networks

This chapter proposes two new ideas in the field of Wavelength Division Multiplexing (WDM) based optical networking aiming to improve the overall communication's QoS. The first idea in this chapter introduces a new improved distributed QoS-aware routing protocol by adopting the idea of RGB pheromone Ant routing. On the other hand, the second idea introduces a new method for solving one of the most significant problems that faces the network vendors when designing WDM optical networks. This problem is well known as Routing and Wavelength Assignment (RWA) problem. The new proposed idea is featured by its lower percentage of connection request blockings.

-What's new: (1) The high overhead centralized QoS-aware secure routing algorithm used in chapter 6 has been replaced in this chapter by a distributed (low overhead) artificially intelligent QoS-aware secure routing algorithm, *Ant Routing*. (2) A new approach that suggests accumulating and re-ordering the incoming requests before serving them has been introduced in this chapter aiming to reduce the percentage of requests blocking or the number of required wavelengths.

7.1 RGB Pheromones Ant Routing

Supposing that there are multiple paths leading ants to a food source, the ant which is taking the shortest path will reach to the food faster than the other ants, which have taken the other paths. This ant, which has reached its intended destination first, returns by following the path that it came from. During its return journey, the ant reinforces that path with more pheromone while the other ants on the other paths are still on their way to the food source. Other ants coming from the nest will follow that path of more pheromone concentration, which is of course the shortest path. Consequently, the concentration of pheromone on the shortest path will increase dramatically compared to other paths. Finally all the ants will follow the shortest path leaving the pheromone on the other paths to evaporate. This swarm foraging behaviour has been imitated to solve many problems; one of these problems is the network's routing [49, 108-111].

Each outgoing ant has been artificially represented by a single and small packet in the network called the forward ant. During its way, this packet records information about the path that it takes to reach its destination. The destination node in turn (i) receives these ants which have taken different paths to reach it, (ii) calculates the goodness of the selected path according to some goodness function that is based on the path's status, and finally, (iii) it deletes the forward ant, and returns a backward packet, called backward ant, to the source node of the ant through the same route. This backward ant updates the selection probability (alternative term for pheromone) of each node it traverses according to the result of the goodness function [49, 111].

The goodness function attempts to provide a certain level of QoS that comprises the requirements of all the traffic types moving over the network. In traditional swarm routing, two QoS factors are to be taken into account. These factors are the delay along the path and the current congestion over that path. However, traffics that are generated due to the different services presented by the network have different views of these QoS factors. Some types of traffics need more awareness of congestion than delay, whilst others need more awareness of delay than congestion, whilst some other types do not care the amount of delay, and so on. In this chapter, we present a novel way to provide levels of QoS factors that are better matched with the requirements of each category of application [49].

This section proposes a new idea in QoS routing on optical networks. Network traffic was classified according to their preferred levels of QoS parameters into three main classes, namely, red traffic, green traffic, and blue traffic. In addition, three types of ants were launched in the network, red ants, green ants, and blue ants. Each type of ant is responsible for establishing the eligibility of the different possible network's routes according to its corresponding traffic type preferences. For instance, the red coloured ants are used to qualify the routes according to their levels of securities and latencies, which are crucial factors for the red traffic class. Preferences of the other traffic's classes are extensively explained later in this section.

7.1.1 Related Work

Ant based routing protocols have been an interesting research topic in the last decade. Research papers on this area can be classified into two categories. Papers in the first category, such as [112], [113], and [114], seek to improve the ant based routing techniques by accelerating the network learning phase in order to get the results to converge in a shorter period of time. On the other hand, papers in the second category tried to offer a better QoS for ant routing [115-117]. lThese researchers focused on the optimality function of ants to compromise among different QoS parameters. Most of this research has taken into account only two QoS measures, which are end to end delays and path congestions. What is always missing in the QoS papers is network security which is covered in this chapter.

In chapters 5 and 6, centralised QoS aware routing protocols that take into account the QoS requirements of the different traffic were proposed. This idea has been broadened in this chapter by applying it to a distributed ant based routing algorithm. The traditional security-blind QoS routing algorithms have been replaced by a novel security enabled traffic-aware routing algorithm, which adopts the idea of classifying traffic into different classes according to their QoS requirements aiming to provide satisfactory levels of QoS factors to each class. This will of course increase the overall QoS offered by the network. Again in this chapter, Oyster Optics Technology (OOT), which is well explained in [9] and [118], has been exploited to add the security as a crucial QoS factor that should be taken into account transmitting some private information.

7.1.2 Traffic Types

Traffic over the network was categorised according their sensitivities towards three orthogonal QoS factors. These factors are (i) path's residual bandwidth, (ii) end to end delay, and (iii) security (see Table 7.1). Let us define a new term which is the path's goodness G ∈ [0,1]. G= 1 indicates that the route is extremely good, whereas G=0 implies that the route is extremely bad. The goodness of a path depends on the category of the traffics, and each QoS factor has its own effect on G.

Assuming that the aggregation of the effects of these factors on the Goodness of a path equals 1, then different traffic types have different values for these effects. For example, some traffic types consider the delivery speed as the most important factor giving it a percentage of effect on the path's goodness equal to 70%, whilst the other QoS factors shares the remaining 30%. Some other traffic types may have a different view to these QoS factors. Private real time traffic such as VoIP and video communications for instance, may assign 45% to the importance of the security, 45% to the communication speed, and only 10% to the bandwidth since such traffic comprises only a small portion of the overall network's traffic in the real world according to [73] and [74]. The importance of available bandwidth (a), delivery speed (b) and security (c), for a particular type of traffic will be denoted in this chapter by the 3-tuple (a, b, c) and will be referred as the QoS requirements pattern.

Traffic in each category was assigned a distinct colour. The colour red was assigned to the traffic that need to be transmitted with high security, high speed and any available bandwidth and was allocated a QoS requirements pattern (0.0%, 35%, 65%). The colour blue, on the other hand, was assigned to the traffic that is considered delay sensitive and which was required to be transmitted with the minimum possible delay and was allocated a QoS requirements pattern (15%, 85%, 0.0%). Finally, the colour green was assigned to the traffic that considers the bandwidth as the most important QoS factor and was allocated a QoS requirements pattern of (85%, 15%, 0.0%), therefore requiring traffic to be transmitted through paths with sufficient residual bandwidth avoiding the congested paths. Hence, the last category of traffic will contribute to balancing of the load over the different network's links and consequently improve the network's links utilisation.

Table 7.1 Traffic Type Categories

Red Traffic (0.0%, 35%, 65%)	**Green Traffic** (85%, 15%, 0.0%)	**Blue Traffic** (15% , 85% , 0.0%)
• VoIP • Video Communications	• Web Browsing • P2P File Sharing • Streaming Video • Miscellaneous Audio up/downloads • Miscellaneous Video up/downloads	• Interactive Gaming • IPTV • Streaming Audio

7.1.3 Network Modelling

The US National Science Foundation (NSF) network with 14 nodes, shown in Figure 7.1, was used in this chapter to demonstrate the feasibility of our proposed QoS aware ant routing protocol. Each node in the network represents a whole Regional Area Network (RAN) with a presumed number of users of 4,000,000. Only those links constructed the backbone of the network that are coloured red (see Figure 7.1) are configured to be secure using Oyster Optics Technology, which has been extensively discussed in [9]. The amount of traffic flow that is moving on the different links was estimated using the applications' specifications of usage statistics in [74]. To expedite the network's training process, nodes in the network send streams of ants to random destinations across the network. Ants were not allowed to visit a node which was previously visited through their path. If there is no way to a destination except through a previously visited node, then the ant is killed. Ants are also killed if they exceed their pre-set life time or Time To Live (TTL) as it is usually termed in ant routing terminology.

7.1.4 Traffic Flow Modelling

The different traffics flow through the network as flow batches, where each batch is identified by three fields, namely, the source address, the destination address and the type of application that generated this traffic. The different network applications responsible for providing the various network services nowadays have been classified into ten application types according to [73, 74], where any network application currently in use can be incorporated in one of these types. These types are: web browsing, streaming audio, streaming video, IPTV, VoIP, video communications, gaming, P2P file sharing, other miscellaneous audio up/downloads, and other miscellaneous video up/downloads. Characteristics of such applications together with their users' behaviour have been taken from [74] and summarised in Table 7.2.

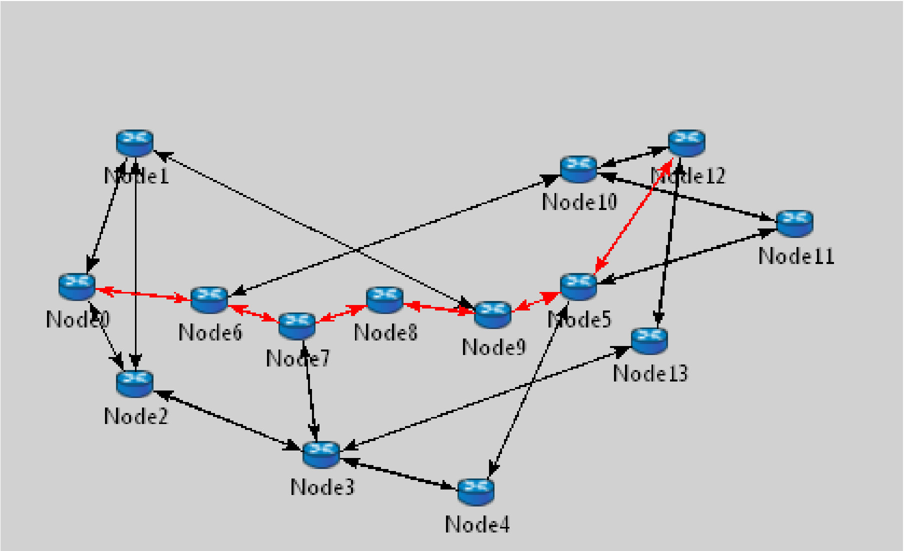


Figure 7.1 NSF Network

The total traffic generated from a source node A and directed to a particular destination B is estimated, as previously explained in chapter 4, based on the user behaviour statistics shown in Table 7.2 below.

Table 7.2: Applications Types Specifications and User Behaviour

Applications Type	**Quality**	**Packet payload Size (Byte)**	**Packet Overhead size (Bytes)**	**Packet Inter-arrival Time (sec)**	**Session Time (sec)**	**Packets Per Session**	**Sessions per Day**	**%BH**	**% of users per application**
Web Browsing		489350	40		300	17	2.5	7.9	75%
Streaming Audio	MP3	418	40	0.026	300		1.5	2.4	25%
Streaming Video	Web Quality	20000	400	0.48	300		1	6.1	50%
IPTV	SDTV	90000	2400	0.48	3600		1	9.4	0.5%
VoIP	Toll Quality	160	40	0.02	210		2	5.7	15%
Video Communications	Web Quality	20000	400	0.48	300		0.5	7.7	5%
Interactive Gaming	FPS	83	767	0.4	3600		1	6.25	33%
P2P File Sharing		16380	470			97500	0.14	5.3	5%
Miscellaneous Audio Up/Downloads	Web Quality	65	40	0.026	300		2	7.9	50%
Miscellaneous Video Up/Downloads	Web Quality	20000	400	0.48	3600		0.07	7.9	50%

7.1.5 Results and Discussion

A new parameter δ_s introduced in this chapter to incorporate the security in the measure of path goodness, where δ_s is defined as a new reinforcement component that depends on the path, and is calculated by equation (7.1). Consequently, equation (2.3) is updated to equation (7.2) shown below to incorporate this security component. Finally, the routing entries of nodes are updated according to equations (2.1) and (2.2) explained in chapter 2.

$$\delta_s = e^{\gamma.s} - 1 \qquad , \gamma \text{ is a new design parameter.} \qquad (7.1)$$

$$\delta_r = a.\delta_p + b.\delta_c + c.\delta_s \qquad ,a + b + c = 1 \qquad (7.2)$$

No particular criteria exists for choosing the values of the design parameters α, β and γ in ant routing, where the optimal values depends to a large extent on the topology of the network and the amount of the input traffic [10, 49]. In this study α, β and γ were assigned values of 0.8 since it was found by trial that such values of these parameters achieves the best performance in terms of the network convergence speed (speed of the training) and solution accuracy.

The efficiency of the proposed routing protocol was examined through investigating the performance of the network with different levels of QoS parameters. The value of each element in QoS pattern (a, b, c) was changed to show the performance of the network with different levels of the QoS component that is associated with this element. Remember that ‘a’ reflects the emphasis on congestion avoidance (or in other word load balance); ‘b’ concerns the level of latency offered; and ‘c’ is relates to the level of security introduced for the private information.

To clearly show the feasibility of this QoS-aware routing protocol, traffic transmitted through the network is supposed to belong to the same type. For instance, to study the effect of the parameter ‘a’ on load balance, all the traffic transmitted on the network’s links are supposed to be balance related.

7.1.5.1 Tuning of the Load Rates Balance Parameter

In this test procedure, the parameter ‘a’ was assigned different values from 0 to 1, and the resulting load balance due to each value was monitored and recorded. The average balance of load rates on the links is calculated by determining the average link ripple with respect to the link’s mean load. Equations (7.3) through (7.5) were used to calculate the average balance of load on the network's links.

$$L_{av} = \frac{\sum_{i=1}^{l} L_i}{\ell} \tag{7.3}$$

$$R_{av} = \frac{\sum_{i=1}^{l} |L_i - L_{av}|}{\ell} \times 100 \tag{7.4}$$

Since the percentage of balancing can be expressed by the un-rippling through the load rates on the different links, then the percentage of balancing can be computed as follows:

$$B_{av} = 100\% - R_{av} \tag{7.5}$$

Where:

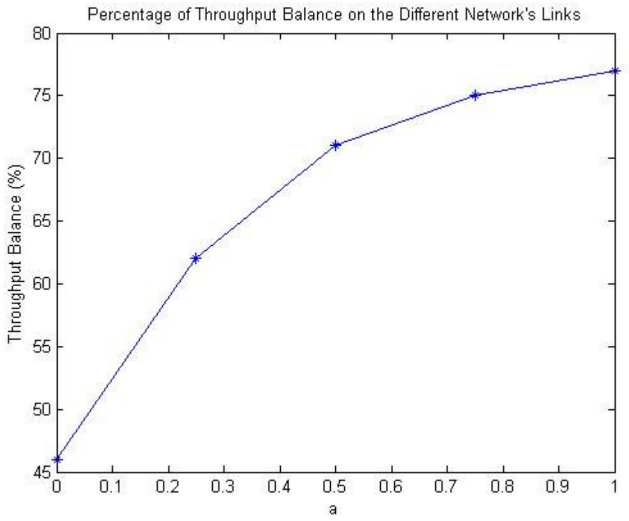
L_{av} is the average load rate on links.

R_{av} is the average percentage of throughputs rippling, where rippling defined as the oscillation of links' load (flow) rates around the average flow rate value per link, and is calculated by summing the differences of each particular link's flow rate from the this average value.

B_{av} is the average percentage of throughputs balance.

l is the number of links and L_i refers to a particular link.

Figures 7.2 Shows the load percentage of balance achieved when applying different values of the QoS patterns (a, b, c). The patterns applied are: (0, 0, 1), (0.25, 0, 0.75), (0.5, 0, 0.5), (0.75, 0, 0.25), and (1, 0, 0) respectively. Here, the whole network's traffic was graded from being purely balance sensitive to purely security sensitive.



7.2 Throughput Balance due to different values of ‘a’

Figure 7.3 shows the throughput distribution when ‘a’ is set to its maximum value, i.e. when the QoS pattern is (1, 0, 0). Observe that increasing the value of the parameter ‘a’ can raise the level of load balance from 46% to 77 as shown in Figure 7.2.

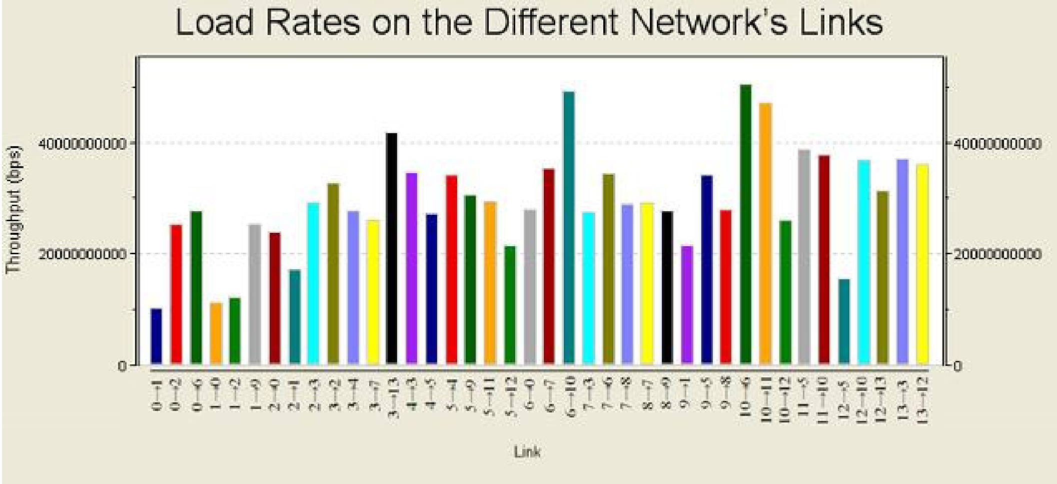


Figure 7.3 Load Rates on the Different Network’s Links when a=1

7.1.5.2 Tuning of the Security Parameter

The value assigned to parameter ‘c’ of the QoS pattern can significantly affect the overall percentage of security offered to the traffic. Figure 7.4 clearly shows the effect of tuning the parameter ‘c’ on the obtained security. Five QoS patterns have been examined in this figure. These patterns are (1, 0, 0), (0.75, 0, 0.25), (0.5, 0, 0.5), (0.25, b, 0.75), and (0, 0, 1). Again all the traffics transmitted across the network’s links belong to the same class, i.e., have the same QoS preferences.

Figure 7.4 shows that the average security percentage offered to the data on the network can be raised by up by 22.4% (From 33.7% to 56.1%) by tuning the parameter ‘c’. However, this maximum percentage of security obtained can be significantly increased by incorporating more secure links across the network. These obtained results were conducted when only the backbone links of the network were secured as shown in Figure 7.1 (red links).

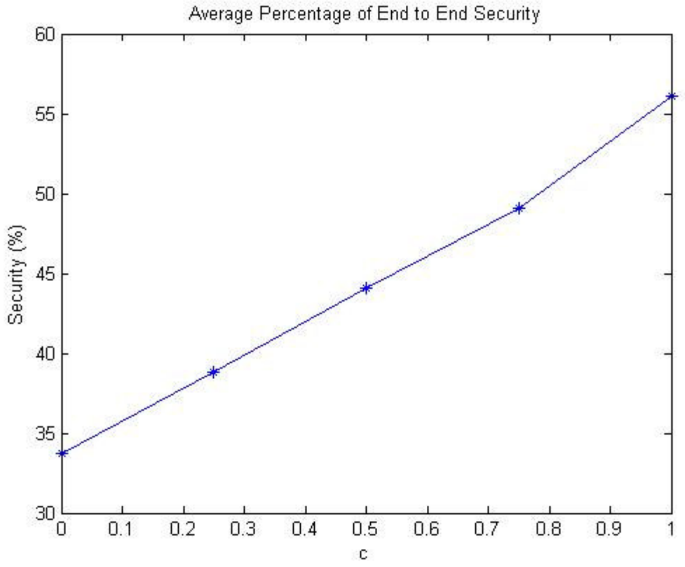


Figure 7.4 Average End to End Security due to different values of ‘c’

The results presented in Figure 7.3 shows a network with a highly balanced (77%) distribution of throughputs on the various network’s links, and one might conjecture how would this distribution be when the value of the parameter ‘a’ is 0, i.e. when the traffic on the links is minimally balanced. The answer to this question was differed to this section from section 7.1.5.1 where the balance was compared with security by increasing the parameter ‘a’ at the expense of parameter ‘c’. Therefore, the extremely unbalanced traffic distribution is supposed to be extremely secured. Figure 7.5 shows this relatively highly unbalanced (balance=46%) highly secured (security=56.1%) traffic distribution. On the other hand, Figure 7.3 which was previously introduced in section 7.1.5.1 shows the throughput distribution on the links when the traffic is on the opposite extreme, i.e., relatively highly balanced (balance = 77%) relatively lowly secured (security=33.7%).

It is clearly noticeable from Figure 7.5 that the traffic flow is highly concentrated on the secured links (red links in Figure 7.1). This is basically because the traffic in this case is supposed to be security sensitive, therefore such traffic will be preferably routed through the secured links rather than the other unsecured links.

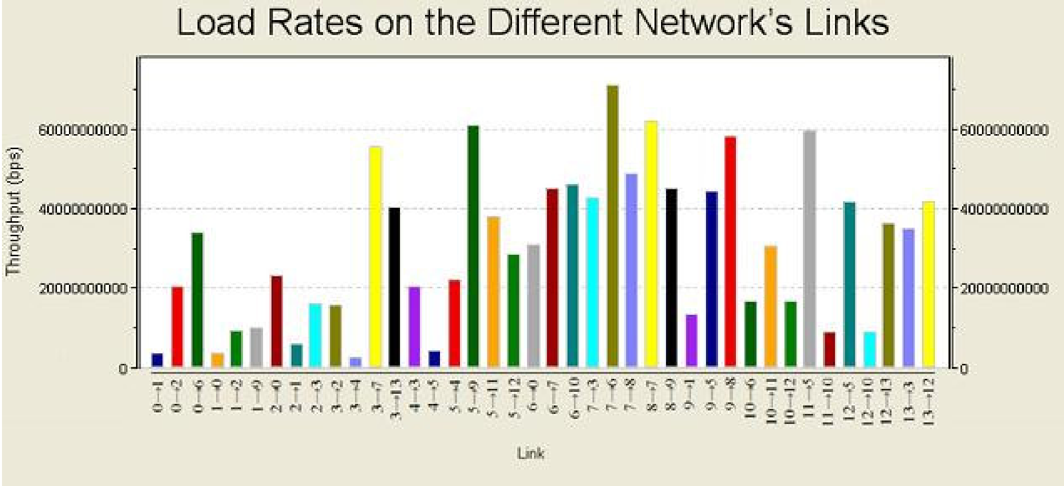


Figure 7.5 Load Rates on the Different Network’s Links when c=1

7.1.5.3 Tuning of the Delay Parameter

The sensitivity of the proposed routing protocol to delay can be adjusted according to the preferences of the traffic type being transmitted through the network. This adjustment can be performed by tuning the parameter ‘b’ which is responsible for the end to end delay. Figure 7.6 shows how the average end to end number of hops decreases as the value of the parameter ‘b’ increases. It is clear from this figure that the average end to end delay has been dropped from 2.553 hops to 2.186 hops as the value of ‘b’ increases from 0 to 1. For the purpose of analysis, the entire network’s traffic was also supposed to have the same QoS preferences. The patterns (0.0, 0.0, 1), (0.0, 0.25, 0.75), (0.0, 0.5, 0.5), (0.0, 0.75, 0.25), and (0.0, 1, 0).

Figure 7.7 on the other hand, shows the distribution of traffic on the different network's links when the value of b=1, i.e., the traffic is extremely delay sensitive. The congestion here will be on the those links that are parts of the shortest path to the destination of many source-destination requests, such as links: 3-7, 3-13, 6-10, 7-3, 6-7, 10-11, 10-6, 11-10 and 13-3.

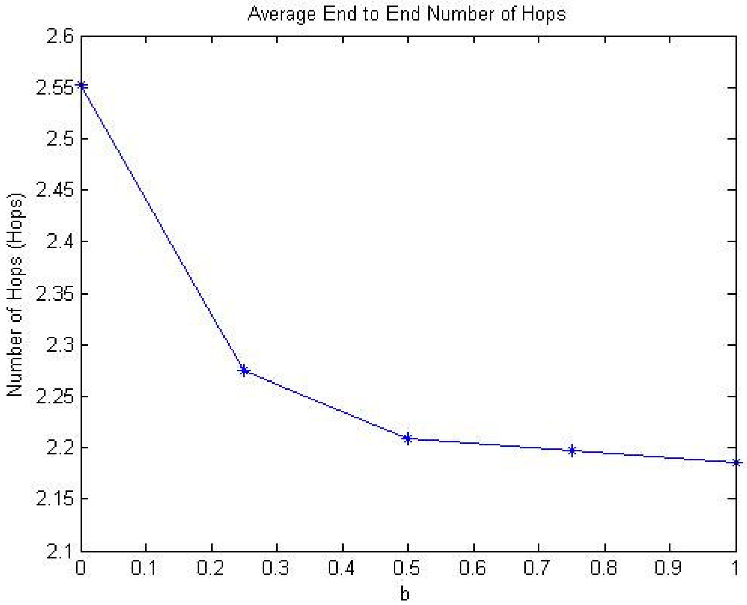


Figure 7.6 Average End to End Delay due to different values of 'b'

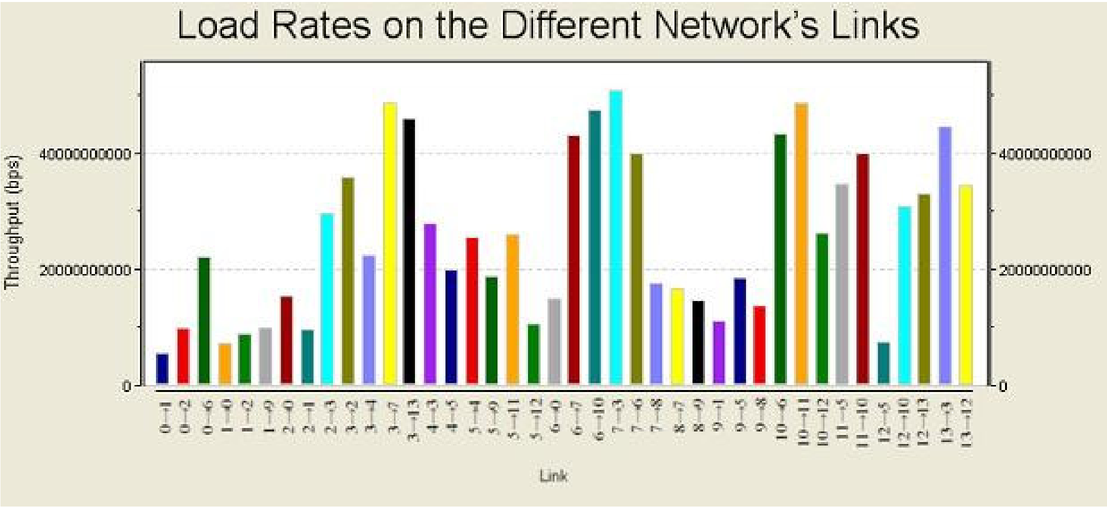


Figure 7.7 Load Rates on the Different Network's Links when b=1

7.1.5.4 Mixing Traffics of Different QoS Preferences

After examining the feasibility of the proposed routing technique by tuning the QoS parameters for traffic of a single type, the applications in this scenario were assigned the QoS preferences that were originally chosen for them in Table 7.1. The overall routing performance was monitored and recorded in Figures 7.8 through to 7.10. Figure 7.8 shows the average end to end security levels obtained for the different applications using the proposed QoS-aware routing protocol.

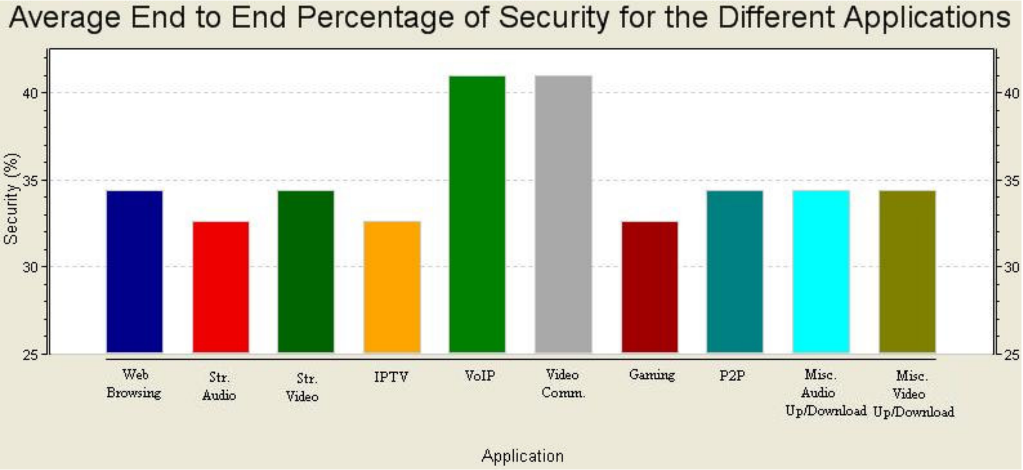


Figure 7.8 Average End to End Percentage of Security for the Different Applications

This figure clearly shows that the VoIP and video communications were offered the highest level of security when the traffic is routed via the network. Traffic generated due to the other applications was also partially secured. This partial securing happened inadvertently since these traffic types have not been banned from passing through the secure network's backbone. However for large networks with a long backbone, the range of offered security can be extended so that more security will be offered for the private information, and less security levels are given for the other non-private data, especially when more alternative routes are available for the connection requests demands.

On the other hand Figure 7.9, shows the average end to end delays for the different applications (measured in hops) when the mix of applications' QoS preferences is applied. As expected, the traffic generated due to the blue applications such as streaming audio, IPTV and gaming experienced less delay when transmitted to the destinations. VoIP and video communications come in the second stage in terms of the speed of communications. Again the range of the difference in the end to end delays can be extended if the network is enlarged so that many alternative paths will be available.

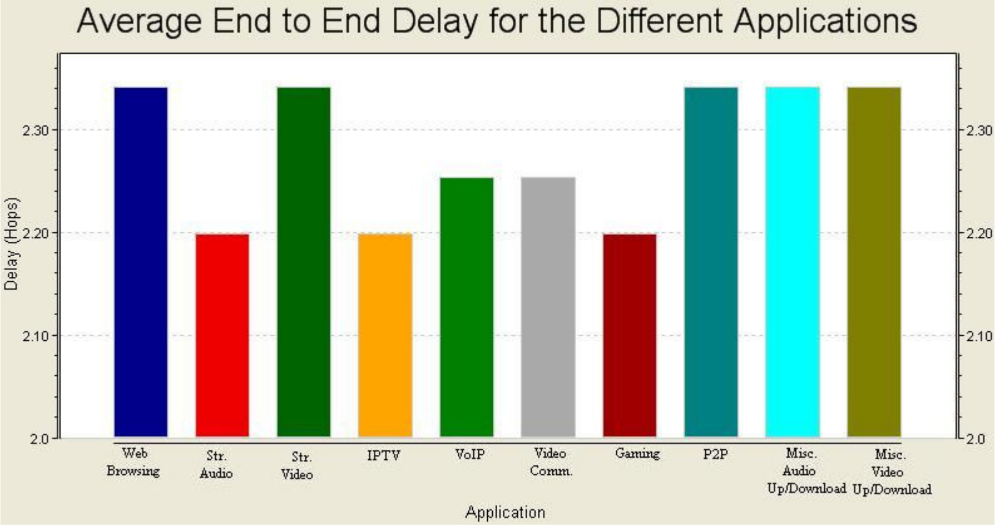


Figure 7.9 Average End to End Delays for the Different Applications

Moreover, the total throughputs distribution on the various network's links has also been shown in Figure 7.10. This data flow distribution has an acceptable level of balance with a percentage of 70%.

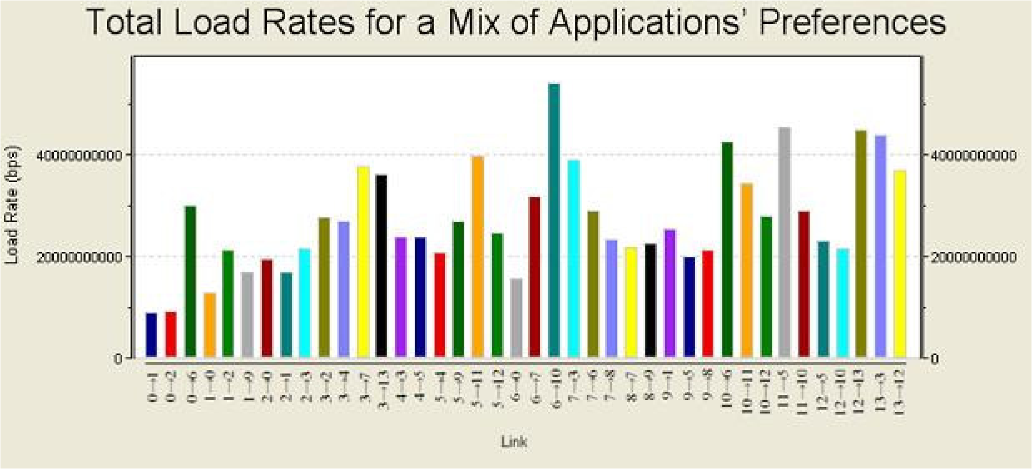


Figure 7.10 Total Load Rates for a Mix of Applications' Preferences (Balance= 70%)

7.1.6 Comparison with the Conventional Ant Routing Protocol

The traditional single pheromone ant routing technique supports a single criterion to update the nodes' pheromone tables. In this routing protocol a single goodness function is used to partially enhance the overall network's QoS. On the other hand it does not accommodate for the different QoS preferences of the different applications. It does not provide distinct QoS-aware routes for each one of the traffic classes according to its preferences, but instead, it provides routes that, to a particular extent, compromise the different QoS requirements of the different traffic types.

In this sub section the conventional congestion-aware and latency-aware routing protocol will be analysed for the purpose of comparison. This protocol is assumed to give equal importance to both the congestion avoidance and delay avoidance criteria with 50% emphasising on each one. Figure 7.11 shows the total flow traffic distribution on the network's links. The percentage of balance of this distribution is only 59%, whereas the balance obtained from the proposed protocol is 70%. That means that the proposed routing protocol provides more balanced links' throughputs, i.e. better link utilisation is achieved.

Figures 7.12 and 7.13 show the average end to end delays and security percentages that are obtained by the conventional congestion-aware latency-aware routing protocol respectively. These two figures clearly show that the conventional ant routing protocol offers no differentiation among the different traffic types in terms of both the end to end delay and the security.

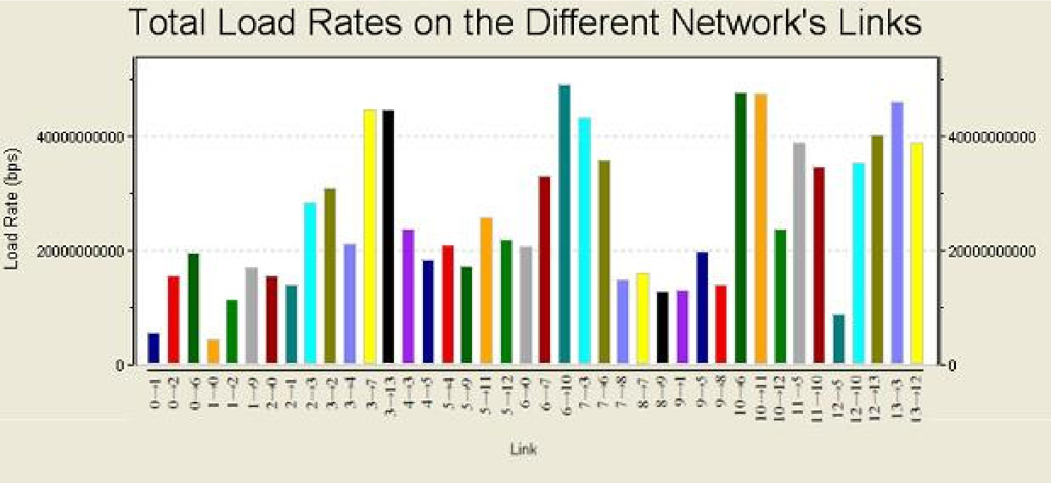


Figure 7.11: Total Load Distribution in the Conventional Congestion-Aware Latency-Aware Routing Protocol (Balance= 56%)

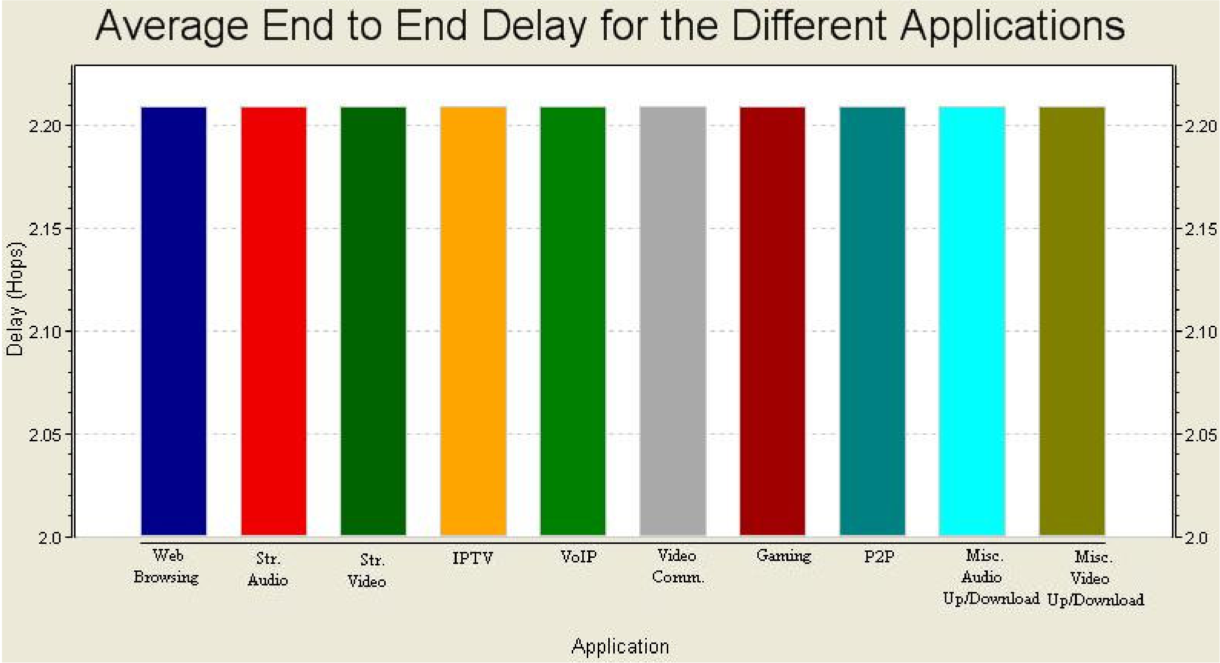


Figure 7.12 Average End to End Delays for the Different Applications in the Conventional Congestion-Aware Latency-Aware Routing Protocol (Delay=2.20879 Hops)

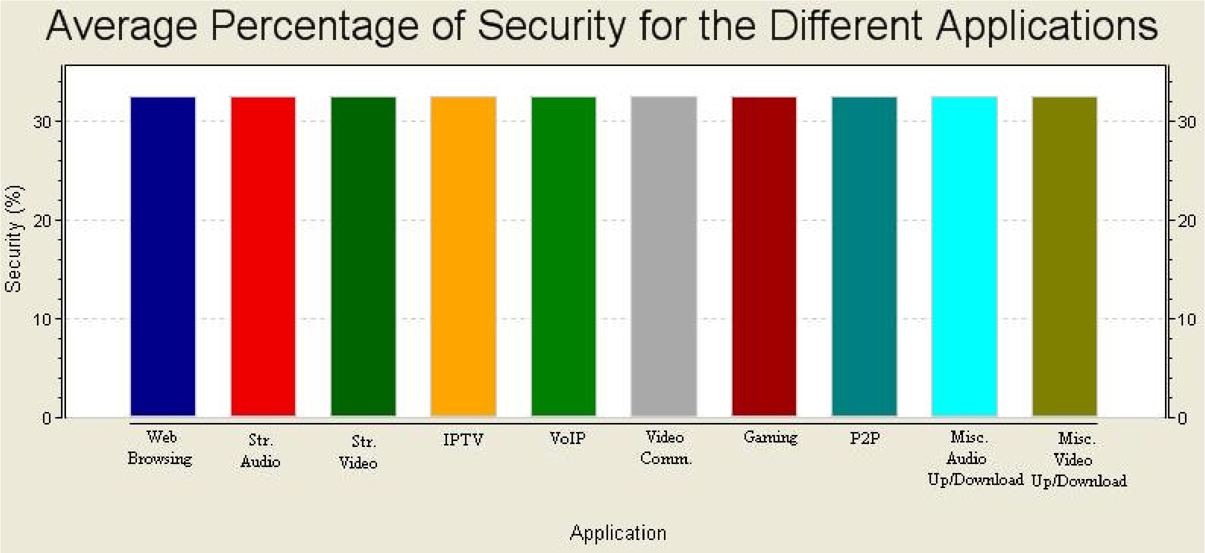


Figure 7.13 Average End to End Percentage of Security for the Different Applications in the Conventional Congestion-Aware Latency-Aware Routing Protocol (Security= 32.5%)

7.2 Enhanced Ant Colony Optimisation (ACO) based RWA on WDM Optical Networks Using Requests Accumulation and Re-Sorting Method.

The way of solving the Routing and Wavelength Assignment (RWA) problem is one of the most important issues that determine the efficiency of transmitting data over multiple light paths of optical fibre using Wavelength Division Multiplexing WDM technique. Ant Colony Optimisation technique was proved to dramatically introduce a more efficient solution for this problem compared with other traditional solutions such as Shortest Path First (SPF) and Load Balanced Shortest Path (LBSP) [119-122]. RWA problem can be applied to one of three scenarios. Firstly, routing and wavelength assignment with Wavelength Continuity Constraint (WCC), where the data requests should be transmitted on a fixed wavelength throughout their whole path from source to destination. Secondly, routing and wavelength assignment with total wavelength conversion, where all the network’s nodes possess the capability of converting the wavelength of the incoming light paths. Unlike WCC, the wavelength of requests can be changed during its way to the destination according to the path preferences. Thirdly, Partial Wavelength Conversion

(PWC), where the network is partially wavelength continuity constrained, i.e., some nodes can achieve the wavelength conversion operation and others cannot. These three scenarios will be covered in this section with the support of results to analyse the system performance in each case.

7.2.1 RWA Types

RWA problem can be classified into two types according to the state of data requests to be allocated paths and wavelengths. These types are [123, 124]: (i) static RWA or sometimes called Static Light Path Establishment (SLE) problem, and (ii) dynamic RWA. Data request is defined as the desire of an origin (source) node to send data to a particular destination node. Therefore, it is sometimes referred to as O-D (Origin-Destination) connection request. The methods for solving RWA depend on whether it is static or dynamic. In Static RWA, the set of all connection requests are predefined in advance and is well known by the network. On the contrary, requests arrive dynamically at unexpected times in dynamic RWA. In both cases, it is required to allocate suitable non conflicting paths to the different connection requests.

One of the primarily important objectives all of the RWA problem solving algorithms need to take into account is the number of blockings [125, 126]. The number or percentage of failed connection requests or data blockages is defined as the failure to setup a light path to a particular connection request due to lack of network resources such as the unavailability of a free path to setup a connection or the overloading on the path allocated for this particular connection request. The efficiency of a RWA algorithm is dependent to a large extent on the ability of this algorithm to minimise such percentage of blockage.

Another significant factor that measures the performance of a RWA algorithm is the number of wavelengths required to achieve data connectivity with a similar percentage of blocking [125, 126]. Considering the percentage of blocking is fixed, the less the number of wavelengths required, the better is the algorithm’s performance. Many approaches have been proposed to solve the RWA problem. The Ant Colony Optimisation method can be used to solve the RWA problem with both static and dynamic connection requests and arrival modes (ACORWA).

7.2.2 Wavelength Conversion Scenarios

WDM can be graphically represented on an optical network by vertices (nodes) interconnected by optical fibres termed edges with a predefined topology. In Figure 7.14, a WDM optical network is shown with two wavelengths recognised by the colours red and blue.

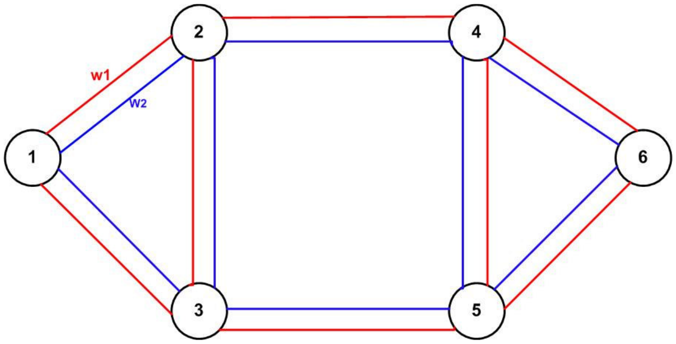


Figure 7.14 WDM with Two Wavelengths

The RWA can be discussed under the following three scenarios, according to the capability of the nodes to convert the wavelength of the received information:

7.2.2.1 RWA with Wavelength Continuation Constraint (WCC)

The network's switches in this scenario have no capability to change the wavelength of the incoming request. In other words, the wavelength of any particular request stays constant during the whole process of requested transmission to the destination. Graphically, in Figure 7.14, if the request is received by any node on a particular colour line (e.g. red) it should be forwarded to the same colour on the outgoing line, otherwise if all these same colour outgoing lines were reserved by other connection requests, request blocking occurs [127].

7.2.2.2 RWA with Full Wavelength Conversion (FWC)

In this case, all the network's nodes are capable of wavelength conversion. Graphically, if a particular node receives a request on any colour input line, it can forward it through any available outgoing line. Such a wavelength conversion can serve to reduce the number of blocking significantly. In addition it can also provide better choice of the routes, but this would be of course at the expense of the hardware complexity accompanied by adding such a facility (wavelength conversion) to the nodes [128].

7.2.2.3 RWA with Partial Wavelength Conversion (PWC)

In such networks, not all the nodes are able to achieve the wavelength conversion, but instead some of them have been fortified with such a capability. This could represent a compromise solution between the hardware complexity of having all nodes facilitated with conversion capabilities and the relatively poor performance of WCC network [129].

7.2.3 Routing and Wavelengths Assignment based on Ant Colony Optimisation (ACORWA)

The Idea of ACO was first introduced by Macro Dorigo [44, 130]. It makes use of the collaborative behaviour of the ant colony to find the shortest path between the source and destination by the request of any connection. ACO was exploited to solve the significant RWA problem in WDM optical networks in [119]. It was introduced as a strong alternative to the previous traditional adaptive centralized RWA algorithms, which needed periodic global link and topology monitoring to track any possible changes in the network topology and link states.

RWA problem can be divided into two sub problems: (i) routing sub problem, which is concerned with choosing the appropriate path to setup a connection for a request, and (ii) wavelength assignment sub problem where any request should be assigned a distinct free wavelength from a set of free wavelengths through its preferred route from the source to the destination. The first sub problem primarily depends on the goodness function which is used to evaluate the different available paths, whereas the second sub problem is mainly constrained by the conversion scenario (see section 7.2.2) being used by the network.

The Multi-Colonies ant routing technique has been used in this section to setup suitable light paths and wavelengths for the different connection requests. In this technique, each node generates ants that belong to different colonies, where each colony corresponds to a wavelength in the WDM optical network. These ants are launched to random destinations across the network tracking the traces of the same colony ants, which had previously passed through the network's links. The mechanism of choosing the preferred route is very similar to that explained in section 7.1, where each ant deposits a trail (pheromone) that is a property of the colony that it belongs to.

Each colony has its own distinct pheromone type. Subsequent ants follow the path of the highest concentration of pheromone of its type, whereas, it neglects the concentration of the other types. The concentration of the colonies' pheromone types is updated on the different routes as soon as a new ant of that colony traverses it according to a particular goodness function that takes into account the length of route and/or some other qualities of the route, such as congestion and security levels. Pheromones evaporate with time to allow for sensing the changes that happen in the network topology or link states.

For static RWA, the set of connection requests is known prior to the arrival of requests and the network is trained for each connection request by a sufficient number of ants to allocate a path and wavelength for this request. As soon as a particular wavelength within a certain route is assigned to a connection request, a flag called "Available" is set to 0 in all the links constructing that route to exclude this link's wavelength from the training of the consequent requests. The ant checks the availability of the wavelength belonging to the link that it wants to choose for the next hop, and if the flag "Available" is 1, then the ant is forwarded to that hop, otherwise if the flag "Available" is 0, then the ant does not go through that hop, but instead, it chooses another way.

Each ant is assigned a wavelength when it is generated, and each link is divided into a number of wavelengths. Depending on the wavelength conversion scenario, the ant of a particular wavelength may either be routed to its destination through a same wavelength throughout all the links that construct the path to the destination, or may change its wavelength, if the wavelength conversion facility is available in the current node.

The algorithms for routing and wavelengths assignments are detailed in sub-sections 7.2.3.1 and 7.2.3.2.

7.2.3.1 ACO based Routing Algorithm

```
Function: Generate_Ant(colony)
repeat
  {
    For each node in the network do
        {
        Select a random destination
        For each ant colony
          {
            Generate_Ant(colony)
            Set (ForwardAnt=true)
            While (ant has not reached the destination)
            {
                If (ForwardAnt=true)
                    {
                    Choose the next hop = Maximum pheromone concentration Link
                    }
                Else
                    {
                    One step back via same path used for the forwarding process
                    Update the pheromone concentration on this link according to the -goodness function
                    }
            }//end while
            If ant reached the destination
                {
                If (ForwardAnt=true)
                    {
                    Calculate the goodness of the whole path to the destination
                    Exchange the source and destination addresses of the ant
                    Set (ForwardAnt=false)
                    One step back via same path used for the forwarding process
                     Update the pheromone concentration on this link according
                     to the- goodness function
                    }
                Else
                    {
                    Kill the ant
                    }
            } //end if
          }//end for
    } until the end of simulation
```

It should be mentioned here that the ants are not allowed to be forwarded to any previously visited node in order to prevent nested loops.

7.2.3.2 ACO based Wavelength Assignment Algorithm

```
Function: Generate_Needle(Wavelength)
For each request (Source, Destination) in the list of connection requests do
    {
    Train the network by launching sufficient number of ants from source node to the random destinations .
    Generate_Needle from the source node
    Set (Forward_Needle=true)
    Assign each colony's pheromone type to a particular distinct network's wavelength
        While (Needle has not reached the destination)
        {
                If (Forward_Needle=true)
                    {
                    Choose the next hop = The Link of maximum pheromone
                    concentration of the type which corresponds to Needle
                    wavelength
                    }
                Else
                    {
                    One step back via same path used for the forwarding process
                    Set the wavelength of this link which is equal to the Needle
                    wavelength as unavailable (Av=0)
                    }
            }//end while
            If Needle reached the destination
                {
                If (Forward_Needle=true)
                    {
                    Exchange the source and destination addresses of the ant
                    Set (Forward_Needlet=false)
                    One step back via same path used for the forwarding process
                    Set the wavelength of this link which is equal to the Needle
                    wavelength as unavailable (Av=0)
                    }
                Else
                    {
                    Discard the Needle
                    }
            } //end if
    } //end for (Connection Requests)
```

Note that when a wavelength of a particular link is reserved by a request, ants will not be allowed to pass through this wavelength of that link in the training phase making its pheromone drop to zero. As a result, this wavelength of the link will not be assigned for any other consequent connection request.

7.2.4 Simulation

The 14 nodes NSF network has been selected again in this chapter to test the algorithm with a wavelength capacity of 40 G bits/sec for all the connecting links, to measure the blocking percentage versus different number of wavelengths. Multi-Colony ant routing has been used here to solve the static RWA over the NSF optical network. Having 14 nodes results in 14^2-14 =182 different (source, destination) requests. The percentage of requests that are blocked varies significantly with the number of wavelengths in the network, supposing that all the network's links have equal number of wavelengths. The network has been simulated under three wavelength conversion scenarios, where (i) no wavelength conversion (wavelength continuity) has been supposed, (ii) partial wavelength conversion with 4 nodes have the wavelength conversion capability and (iii) full wavelength conversion. The percentage of requests that are blocked has been recorded for different number of wavelengths. The result is shown in Figure 7.15. This figure shows that with a wavelength continuity constraint, a minimum of 17 wavelength links should be used to interconnect the network to obtain a fully connected network, i.e. number of requested blockings=0.

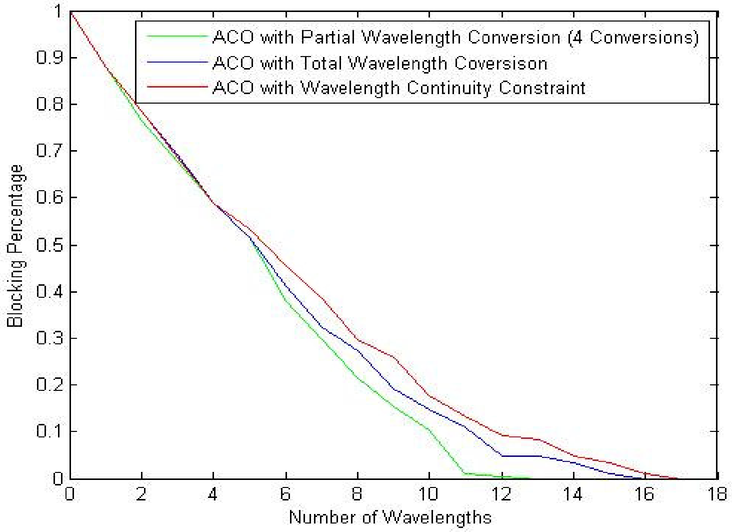


Figure 7.15 Percentage of Blockings Versus the Number of Wavelengths using ACO

On the other hand if wavelength conversion is allowed on all the network's nodes, then the number of wavelengths required for full connection of all requests shrinks to 13. Partial wavelength conversion scenario represents an intermediate stage between the previously mentioned two other scenarios.

7.2.5 Re-Sorting Connection Requests

In sub-section 7.2.4, the requests were allocated paths and wavelengths in a random order. It has been noticed through this simulation that the order in which the requests is served can significantly affect the performance of the network. The best result is obtained when these connection requests are sorted in the order of their distances to destination, where the shorter request is allocated a path and wavelength first. That is because in the case of limited network resources (limited number of wavelengths), connecting the longest path first results in depriving many requests at the expense of connecting this request.

In Figure 7.16, suppose a single wavelength is only used. Node A communicates with B using the link (A-B). If (A) would like to communicate with (C) at the same time, ACO method always try to save the request A-to-C from being blocked, therefore it will reroute this request through the long path (A-H-G-F-E-D-C). Consequently, it will occupy all these links connecting that long path. This will cause blockages for other requests like A-H, H-G, G-F, F-E, E-D, and D-C at the expense of serving a single request. Therefore, it is worthwhile to allocate paths and wavelengths for those requests of short lengths at the beginning, then serve the longer requests with the remaining links and wavelengths.

The distance of the different connection requests can be inspected by propagating ants through the network before deciding which request to serve first. These ants can easily calculate the lengths of the different requests. Figures 7.17 through 7.19 clearly show the blocking percentage reduction gained from re-sorting the requests in order of their distance to their destinations. These Figures show that a less percentage of blocking can be obtained if the requests are ordered according to their distances in all the three wavelength conversion scenarios (no wavelength conversion, full wavelength conversion, and partial wavelength conversion). A drop of about 15% in the percentage of blocking can be gained in full wavelength conversion scenario when 5 wavelengths are used as shown in Figure 7.18.

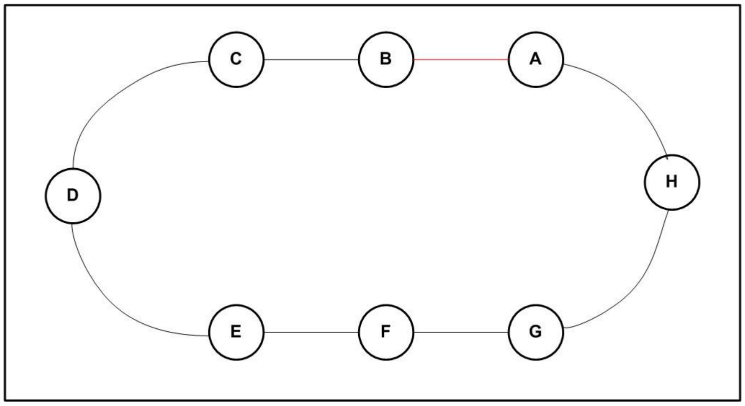


Figure 7.16 Example Network

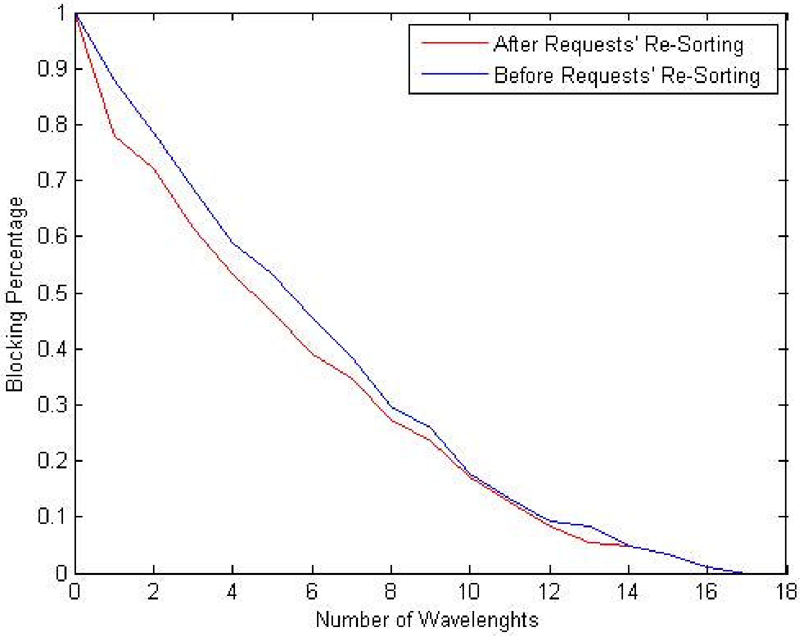


Figure 7.17 Blockings with and without Requests' Re-Sorting in Wavelength Continuity Constraint Scenario

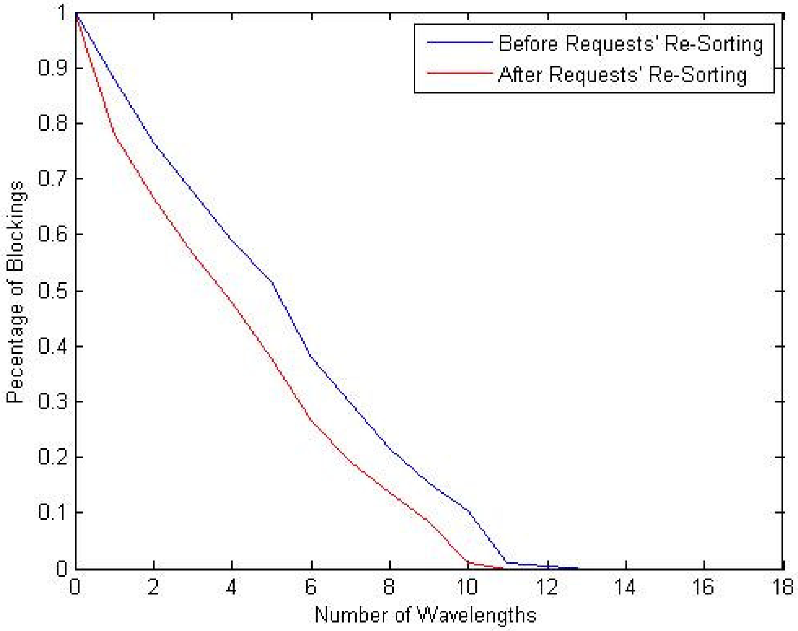


Figure 7.18 Blockings with and without Requests' Re-Sorting in Full Wavelength Conversion Scenario

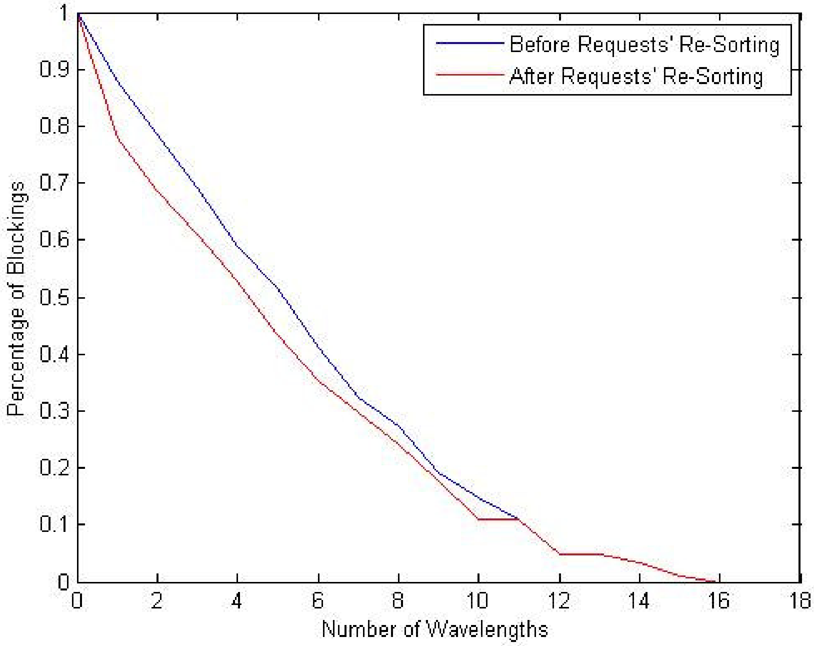


Figure 7.19 Blockings with and without Requests' Re-Sorting in Partial Wavelength Conversion Scenario (4-Conversions)

7.2.6 Accumulative Requests RWA

In this sub-section, we propose a method for improving the performance of RWA in dynamic requests arrival. The improvement will be achieved by reducing the number of requests blockages for a WDM network with a particular number of wavelengths. If the network assigns a path to a request as soon as this request arrives, this will negatively affect the performance of the RWA algorithm since that path may consume too many resources (wavelengths) of the network if the path is long. Therefore, a new proposal is presented, which accumulates a number of requests, re-sorts them then assigns the routes for them in the optimal order so that less requests blockings are achieved. The dynamically arrived connection requests that arrive in a particular time window will be aggregated, sorted in an ascending order of their distances to their destinations, then these requests are allocated paths. The term accumulation sampling time has been used to refer to the time that is used to compute the time when the next allocation which is due.

Our NSF Network has been used again. Requests are exponentially distributed among the nodes with Average rate of λ requests/sec, where λ is set variable to test the network for different loads. Each request is supposed to be accompanied with an extra 10 Mbit/Sec load applied to the network. Accumulation Sampling Time is set at 0.1 μ sec. Figure 7.20 below shows a comparison between the proposed accumulative RWA and the conventional RWA schemes.

One controversy that may arise is whether or not the time required for accumulating the requests cause a substantial amount of delay that may affect the performance of the network. This controversy can be resolved by supposing that the network is huge with too many switching operations required for reaching the destination on average, and more importantly, the connection requests arrive at a very high rate. High connection requests rate may be due to the large number of users in a node, especially if the node represents a whole RAN (Regional Area Network) with hundreds of thousands of or maybe millions of users as it is the case in our network. In this case, even a small delay that only enables the network to accumulate 5 requests per allocation round and resorts them, will come up with a significant reduction in the blocking percentage. Two facts should be taken into account, firstly, more blockings result in either more delay due to requests for retransmissions in TCP communications or loss of data in UDP transmissions, secondly, the time required for accumulation requests is consumed one time per the whole connection, which may be neglected compared with the time required to set up a connection through the many switches in large networks.

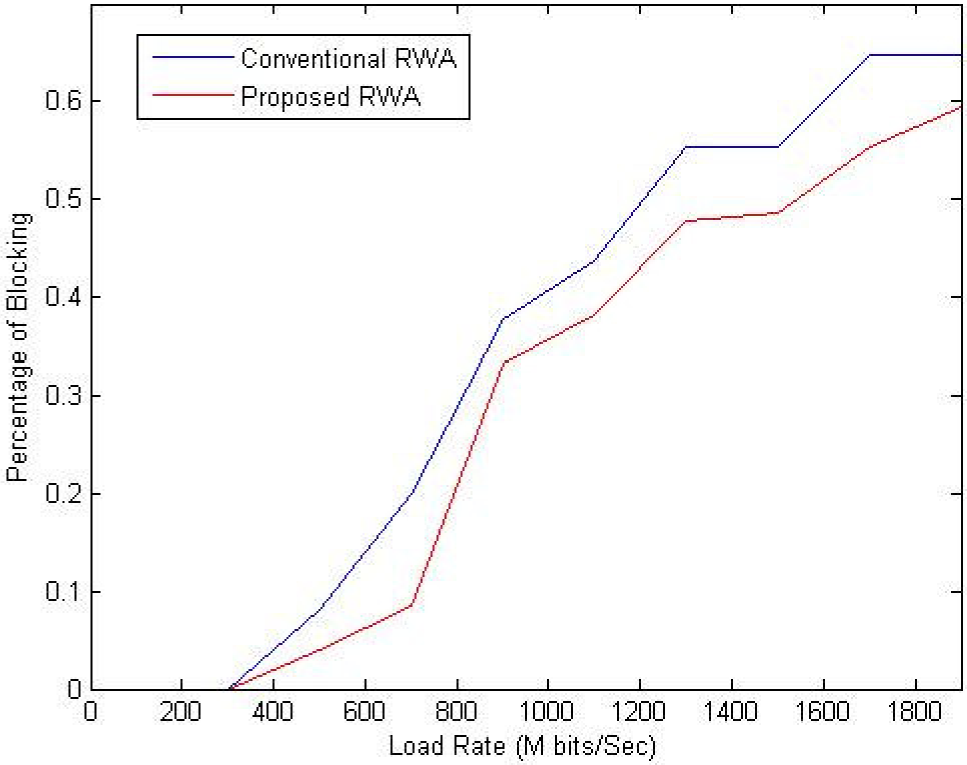


Figure 7.20 Percentage of Blocking Vs. the Applied Load in Conventional Dynamic RWA and Accumulative Dynamic RWA

From Figure 7.19, at load 700 M bits/Sec, which is due to 5 connection requests per node on average (70 requests/14 nodes= 5 requests/ node), the percentage of blocking has been dropped to half when using the proposed RWA. That means waiting to accumulate only 5 requests from each node rather than allocating route immediately will help to drop the percentage of blocking to half its original value. Therefore, it is worthy to wait for a few moments to gain such a drop in the percentage of blocking.

7.3 Summary

Applications here were organised into three categories according to their QoS requirements. Applications in each category require common levels of bandwidth, latency, and security. Oyster Optics security technique has been deployed to secure six bidirectional links out of 20 links aiming to provide secure transmission for private data over the network. Corresponding to these three applications categories, three types of ants were launched over the network's links to test the suitability of the different available paths between each source-destination pair for the different traffic types. Each of these ant types deposits pheromone of a distinct colour (red, green or blue) specialised in estimating the level of security, bandwidth availability, and latency of the path.

Red pheromone was used to test the path's security, whereas green pheromone was used to calculate the amount of free bandwidth over the path. Furthermore, blue pheromone was utilised to check the path's latency. Consequently, unlike the traditional ant routing protocol, which considers only one pheromone type to accommodate for a single mix of QoS requirements for the entire network's traffic, our proposed enhanced ant routing technique finds a way for dealing with the QoS requirements of the network's traffic more precisely, where it offers a different Latency-Bandwidth-Security (LBS) mix for each traffic category to match its QoS requirements.

Results clearly show the merits of our proposed routing protocol in approaching more closely towards satisfying the QoS requirements of the traffics generated due to running the different network's applications. More security was achieved in routing the private information, quicker end to end communication was gained for those applications that needed fast communications, and congestions were avoided in routing the bulky bandwidth consuming applications in order to prevent or minimise the probability of data loss of the traffic belonging to those applications that was bandwidth sensitive as shown in the result section. Moreover, better balance and links' efficiencies have been achieved when applying this enhanced routing approach. Our novel QoS-aware routing technique was compared with the conventional ant routing protocol in order to highlight the merits gained using this proposed routing approach. Results show clear differences in terms of load balancing, end to end delay, and security for the benefit of our proposed routing scheme.

In addition, ACO has been used in this chapter to solve the problem of RWA in WDM optical networks. ACO, as proved by many previous researches, introduces a strong alternative to the other RWA algorithms. Multi-Colony ant routing has been applied in this ACO algorithm, where the ants of each colony is attracted to the pheromone that other ants of the same colony deposit, whereas it is not affected by the pheromones of other colonies.

Three scenarios were simulated and their results compared in this chapter. Firstly, no wavelength conversion is available, i.e. RWA with wavelength continuity constraint. Secondly, full wavelength conversion, where all the nodes are capable of change the wavelength of any incoming request to any available wavelength. Thirdly, partial wavelength conversion, where only some nodes have the wavelength conversion capability.

The two types of RWA, static and dynamic, have been considered in this chapter and a proposal made for each type to improve the network performance in terms of the percentage of blockings. The first proposal is the re-sorting requests techniques to improve the efficiency of the static RWA algorithm. In this technique, the already known connection requests are to be allocated paths in order of their distances to the destinations, where the request of shortest distance is to be allocated a route and wavelength first. An improvement of about15% in terms of dropping the percentage blocking in full wavelength conversion scenario when links of 4 wavelengths are utilised as shown in Figure 7.18. The second RWA-related proposal deals with the dynamic RWA, where it is proposed to accumulate the incoming requests to each node, reorder them and then allocate paths (routes and wavelengths) for them. More than 10% drop in the percentage of blocking has also been achieved for the dynamic RWA at 700 M bits/sec load (see Figure 7.20).

Chapter 8

Conclusion and Future Work

This chapter consists of two sections. The first section concludes the whole thesis, and the second section suggests areas for potential development in future work.

8.1 Conclusion

The main purpose of this thesis was to dimension the traffic on the different networks' links under different scenarios of services resolutions, and to suggest new ideas for routing techniques aiming to improve the overall QoS level being offered to the optical network's end users.

As a first step towards improving the network QoS, the effect of improving the data quality on the network's loading has been studied by creating a scalable software model to simulate the flow of traffic over any fixed topology network. This model is capable of dimensioning the congestion levels on the different network's links, provided that the corresponding network's services user behaviour is available. Basra national optical network has been chosen for studying the loading analysis under different quality of experience scenarios.

A second step was to analyse the network's loading when putting some QoS constraints to the traffic generated by the different applications. The sensitivities of different applications to loss and delay were taken into account to provide different routing choices for the different applications. This work has been broadened then to include a very crucial QoS factor represented by the Security.

Due to the great importance of the privacy for some information, a three-layered QoS routing algorithm has been developed by including security as a third significant QoS requirement together with the bandwidth and the end to end delay. Till now, all the used routing algorithms were considered to be managed in a centralized manner, where a central authority was responsible to provide information about the changes in links connectivity and loadings in order for the different network's nodes to update their routing information.

To avoid the extra amount of traffic overhead caused by the communications of the nodes with the central entity using centralization routing protocols, an artificially intelligent ant based distributed routing algorithm has been developed. The network changes in such a routing protocol is sensed in a distributed manner, and the route is selected within a node without a need to referring to the central party. This routing technique has also been supported with a QoS mechanism to differentiate among the different traffic types by adopting the RGB pheromones technique.

Finally, this ant colony based routing has been deployed to suggest an enhanced version of the solution to the awkward routing and wavelength assignment, which is attendant to the use of WDM in optical networks. This suggested solution is characterised to have less percentage of blockings or less number of required wavelengths to achieve equivalent same performance when compared to the other traditional schemes.

8.2 Future Work

This thesis has focused mainly on three important QoS requirements which are bandwidth, delay, and security. It would be also worthy to include jitter as another QoS parameter. Furthermore the design parameters for the swarm colony based routing, such as β, γ, and P_{noise} was chosen similar to all the other available relevant papers, namely on a trial basis, where they were optimised by changing their values and looking to the performance achieved. It will be very useful if some efforts are targeted to find some optimisation criterion to evaluate these parameters.

Moreover, applications types can be partitioned into smaller types to have a more precise look at the contribution of each particular application into the total network loading. Web browsers for example, can be classified to Internet Explorer, Firefox, Dolphin, Google Chrome, etc. P2P file sharing programs can also be classified to Bittorrent, Limewire, Kazaa, etc. Finding accurate method for estimating the potential amount of data loss and bit error rates can also be good ideas for further work since these factors can largely affect the overall communication QoS.

A possible area for further contributions may include the consideration of the instantaneous links' flow rates which show the accurate variation of flow rates on the network's links. This can be achieved by developing a simulation model that analyse the network in packet basis rather than or in addition to flow basis. Another worthwhile thought for future consideration is to propose a new approach for estimating the network's data loss from the data buffering time, where as long as the target link is busy, data is buffered. If connection requests arrive at the link in a rate greater than the link's processing rate, the traffic is then latched at a buffer that is especially designed for this reason. If the link continues to receive data at this high rate, buffer overflow occurs. This overflow will lead to an amount of traffic is lost to resolve the buffer's overflow problem. This time period during which the data unit is in the buffer can be utilised to speculate the amount of data loss.

Moreover, related to RWA proposed solution, possible ideas for future work may include extensive study on the extra delay which accompanies the process of waiting for the requests needed to be accumulated. Moreover, it will be very interesting if the study incorporates prioritising the connection requests in a manner that the urgent requests are served exceptionally promptly without waiting to accumulate other requests with them. In addition, apart from the quick (urgent) requests, repetition of requests may also be taken into account, where serving the most frequent requests first even if have further distances to the destination may significantly affect the percentage of blocking.

References

[1] Jingjing Wang, Yongli Zhao, Jie Zhang, Yuyao Wu, Wanyi Gu, Dajiang Wang and Xuping Cao, "Centralized and distributed routing and spectrum assignment schemes for bandwidth-variable optical networks," *Communications and Photonics Conference and Exhibition, 2011. ACP. Asia*, pp. 1-6.

[2] Zhan Jing, "Centralized routing and distributed routing protocol for dynamic routing," *World Automation Congress (WAC), 2012*, pp. 1-4.

[3] He Xin, "Introduction of centralized and distributed routing protocols," *Electronics, Communications and Control (ICECC), 2011 International Conference on*, pp. 2698-2701.

[4] J. Fu, P. Sjodin and G. Karlsson, "Convergence of Intra-domain Routing with Centralized Control,", Springer Berlin Heidelberg, Lecture Notes in Computer Science, Volume 4982, 2008, pp 518-529.

[5] Tan Jing, Luo Junzhou, Li Wei and Shan Feng, "Building reliable centralized intra-domain routing in Trustworthy and Controllable Network," *Integrated Network Management (IM), IFIP/IEEE International Symposium on*, *2011,* pp. 462-469.

[6] D.P. Bertsekas and Gallager, "Data Networks,", 2nd edition, Prentice Hall, 1992.

[7] D. Medhi and K. Ramasamy, "Network routing: algorithms, protocols, and architectures,", 1st Edition, Morgan Kaufmann Series in Networking, 2007.

[8] Lydia Parziale, David T. Britt, Chuck Davis, Jason Forrester, Wei Liu, Carolyn Matthews, Nicolas Rosselot, "TCP/IP Tutorial and Technical Overview," IBM International Technical Support Organization, 2006.

[9] U S Patents, "Securing Fiber Optic Communications against Optical Tapping Method*"s, Oyster Optics, Inc*. 2003. Available: www.rootsecure.net/content/downloads/pdf/fiber_optic_taps.pdf [Accessed: 14 February 2012],".

[10] S. Ngo, X. Jiang and S. Horiguchi, "An Ant-Based Approach for Dynamic RWA in Optical WDM Networks," *Photon.Network Commun.*, vol. 11, no. 1, 2005, pp. 39-48.

[11] Royal Pingdom, “World Internet population has doubled in the last 5 years “ royal.pingdom.com. [Online]. Available:
http://royal.pingdom.com/2012/04/19/world-internet-population-has-doubled-in-the-last-5-years/ [Accessed: Sep. 14,2013].

[12] Y. Chen, C. Qiao and X. Yu, “Optical Burst Switching (OBS): A New Area in Optical Networking Research,” *IEEE Network Magazine*, 2004, vol. 18, pp. 16-23.

[13] J.P. Jue and V.M. Vokkarane, “Optical Burst Switched Networks,”, USA: Springer, 2005.

[14] G.I. Papadimitriou, C. Papazoglou and A.S. Pomportsis, “Optical switching: switch fabrics, techniques, and architectures,” *Lightwave Technology, Journal of*, vol. 21, no. 2, 2003, pp. 384-405.

[15] J. Buysse, M. De Leenheer, C. Develder, B. Dhoedt and P. Demeester, “Cost-Effective Burst-Over-Circuit-Switching in a Hybrid Optical Network,” *Networking and Services, ICNS '09. Fifth International Conference on,* 2009, pp. 499-504.

[16] A.G.P. Rahbar and O.W.W. Yang, “Contention avoidance and resolution schemes in bufferless all-optical packet-switched networks: a survey,” *Communications Surveys & Tutorials, IEEE*, vol. 10, no. 4, 2008, pp. 94-107.

[17] C. Liu, Z. Dutton, C.H. Behroozi and L.V. Hau, “Observation of coherent optical information storage in an atomic medium using halted light pulses,” *Nature*, vol. 409, no. 6819, 2001, pp. 490-493.

[18] D. F. Phillips, A. Fleischhauer, A. Mair, R. L. Walsworth, and M. D. Lukin. “Storage of light in atomic vapor “*Physical Review Letters*, 2001, 86(5):783-786.

[19] A. V. Turukhin, V. S. Sudarshanam, M. S. Shahriar, J. A. Musser, B. S. Ham, and P. R. Hemmer, “Observation of ultraslow and stored light pulses in a solid” *Physical Review Letters*”, 88(023602), 2002.

[20] B. Kantarci, S. Oktug, and T. Atmaca, “Analyzing the effects of burst assembly in optical burst switching under self-similar traffic,” *Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop. aict/sapir/elete 2005. proceedings*, 17-20 July 2005, pp. 109-114.

[21] C. Qiao and M. Yoo, “Optical burst switching (OBS) - a new paradigm for an optical Internet,” *J.High Speed Netw.*, vol. 8, no. 1, 1999, pp. 69-84.

[22] K. Dolzer and C. Gauger, “On Burst Assembly in Optical Burst Switching Networks - A Performance Evaluation of Just-Enough-Time,” Proceedings of the 17th International Teletraffic Congress, Salvador, Brazil, September 24-28, 2001, pp. 149-160.

[23] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, “OpenFlow: enabling innovation in campus networks,” *SIGCOMM Comput.Commun.Rev.*, vol. 38, no. 2, March 2008, pp. 69-74.

[24] M. Jarschel, S. Oechsner, D. Schlosser, R. Pries, S. Goll and P. Tran-Gia, “Modeling and performance evaluation of an OpenFlow architecture,” *Teletraffic Congress (ITC), 23rd International*, *2011,* pp. 1-7.

[25] P. Molinero-fernández and N. Mckeown, “The Performance of circuit switching in the Internet,” *OSA Journal of Optical Networking*, 2003, pp. 82-96.

[26] 11.Dr. Farid Farahmand and Dr. Qiong (Jo) Zhang “Circuit Switching” Central Connecticut State University and Arizona State University at West Campus Optical Burst Switching Networks, IEEE Communications Society, (2004).

[27] G.N. Rouskas and L. Xu, “Optical Packet Switching.” Emerging Optical Network Technologies: Architectures, Protocols and Performance”, (Krishna Sivalingam and Suresh Subramaniam, Editors), pp. 111-127, Springer, 2004.

[28] William Stallings, *Data and Computer Communications,* 8th Edition. New Jersey: Pearson Prentice Hall, 2007, p.315.

[29]Tzvetelina Battestilli and Harry Perros, “An Introduction to Optical Burst Switching”, *IEEE Communication Magazine*, vol. 41, no. 8, August, 2003.

[30] Y. Chen, C. Qiao and X. Yu, “Optical burst switching: a new area in optical networking research,” *Network, IEEE*, vol. 18, no. 3, 2004, pp. 16-23.

[31] Pinar Kirci, A. Halim Zaim “ Just-in-time, just-enough-time and horizon signalling protocols on optical burst switches “. Optica Applicata, Vol.36, No.1, 2006, pp. 111-123.

[32] Myungsik Yoo and Chunming Qiao, “Just-Enough-Time (JET): a high speed protocol for bursty traffic in optical networks,” *Vertical-Cavity Lasers, Technologies for a Global Information Infrastructure, WDM Components Technology, Advanced Semiconductor Lasers and Applications, Gallium Nitride Materials, Processing, and Devi*, 1997, pp. 26-27.

[33] P. Kirci and A.H. Zaim, “Comparison of OBS protocols,” *Computer Networks, International Symposium on*, 2006, pp. 158-161.

[34] Jing Teng, George N. Rouskas, "A Detailed Analysis and Performance Comparison of Wavelength Reservation Schemes for Optical Burst Switched Networks." *Photonic Network Communications*, vol. 9, no. 3, May 2005, pp. 311-335.

[35] C. Rotsos, N. Sarrar, S. Uhlig, R. Sherwood and A.W. Moore, "OFLOPS: An Open Framework for OpenFlow Switch Evaluation," Lecture Notes in Computer Science Volume 7192, 2012, pp 85-95.

[36] G. Antichi, A. Di Pietro, S. Giordano, G. Procissi and D. Ficara, "Design and Development of an OpenFlow Compliant Smart Gigabit Switch," *IEEE Global Telecommunications Conference (GLOBECOM 2011),* 2011, pp. 1-5.

[37] A.M. Makowski, "The Binary Bridge Selection Problem: Stochastic Approximations and the Convergence of a Learning Algorithm," Ant Colony Optimization and Swarm Intelligence, Lecture Notes in Computer Science Volume 5217, 2008, pp. 167-178.

[38] G. Di Caro and M. Dorigo, "AntNet: A Mobile Agents Approach to Adaptive Routing," Universite Libre de Bruxelles, Belgium, 1997, Technical Report IRIDIA/97-12.

[39] R. Schoonderwoerd, O. Holland, J. Bruten, L. Rothkrantz, "Ant-based Load Balancing in Telecommunications Networks," Adaptive Behaviour, 5(2):169–207, 1997.

[40] J. Deneubourg and J. Gross, "Collective Patterns in Decision Making," Ethology Ecology & Evolution, Volume 1, Issue 4, 1989, pp. 295-311.

[41] T. White, B. Pagurek and F. Oppacher, "Connection Management using Adaptive Mobile Agents,", International Conference on Parallel and Distributed Processing Techniques and Applications, Las Vegas, NV, USA, 13 - 16 July 1998, pp.802-809.

[42] E. Bonabeau, G. Theraulaz, J. Deneubourg, S. Aron and S. Camazine, "Self-organization in social insects," *Trends in Ecology & Evolution*, vol. 12, no. 5, 5, 1997, pp. 188-193.

[43] M. Dorigo and L.M. Gambardella, "Ant colony system: A cooperative learning approach to the traveling salesman problem," *Evolutionary Computation, IEEE Transactions on*, vol. 1, no. 1, 1997, pp. 53-66.

[44] Colorni, Alberto and Dorigo, Marco and Maniezzo, Vittorio and others, "Distributed optimization by ant colonies," *Proceedings of the first European conference on artificial life*, vol. 142, 1991, pp. 134-142.

[45] M. Dorigo, "Ant Colony Optimization and Swarm Intelligence: 5th International Workshop, ANTS 2006, Brussels, Belgium, September 4-7, 2006, Proceedings,", vol. 4150, 2006.

[46] M. Dorigo and T. Stutzle, “The ant colony optimization metaheuristic: Algorithms, applications, and advances,”, Handbook of Metaheuristics International Series in Operations Research & Management Science, Springer, US, Volume 57, 2003, pp 250-285.

[47] M. Dorigo, G.D. Caro and L.M. Gambardella, “Ant algorithms for discrete optimization,” *Artif.Life*, vol. 5, no. 2, 1999, pp. 137-172.

[48] B. Nazir, J. Ahmed, A. Khan and Azzam-ul-Asar, “Stigmergy of Ants for QoS Provisioning in Dynamic Ad Hoc Networks,” *Emerging Technologies ICET '06, International Conference on*, 2006, pp. 538-543.

[49] Liu Z., “Ant Based Algorithm and Robustness Metric in Spare Capacity Allocation for Survivable Routing”, PhD thesis, University of Canterbury, Christchurch, New Zealand, 2010.

[50] Mesut Günes and Otto Spaniol, “Routing Algorithms for Mobile Multi-Hop Ad-Hoc Networks,” in Network Control and Engineering for QoS, Security and Mobility II, Dominique Gaïti, Ed. Norwell, USA: Kluwer Academic Publishers, 2003, pp.122-137.

[51] M.S. Borella, J.P. Jue, D. Banerjee, B. Ramamurthy and B. Mukherjee, “Optical components for WDM lightwave networks,” *Proceedings of the IEEE*, vol. 85, no. 8, 1997, pp. 1274-1307.

[52] D.N. Payne, “The optical fibre Internet: Where next?” *Transparent Optical Networks (ICTON), 14th International Conference on*, 2012, pp. 1-1.

[53] B.L. Haibo, L.K. Sohraby and C. Wang, “Future internet services and applications,” *Network, IEEE*, vol. 24, no. 4, 2010, pp. 4-5.

[54] Yabin Ye, H. Woesner and I. Chlamtac, “Traffic Grooming Techniques in Optical Networks,” *Broadband Communications, Networks and Systems BROADNETS. 3'rd International Conference on*, 2006, pp. 1-9.

[55] Hequan Wu, “Some thoughts on the transformation of information and communication technologies,” *Technologies Beyond 2020 (TTM), IEEE Technology Time Machine Symposium on*, 2011, pp. 1-1.

[56] Zhenghao Zhang and Yuanyuan Yang, “Optimal scheduling algorithms in WDM optical interconnects with limited range wavelength conversion capability,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 15, no. 11, 2004, pp. 1012-1026.

[57] Jingyi He, S.-.G. Chan and D.H.K. Tsang, “Multicasting in WDM networks,” *Communications Surveys & Tutorials, IEEE*, vol. 4, no. 1, 2002, pp. 2-20.

[58] M. Irshid and M. Kavehrad, “A WDM cross-connected star multihop optical network,” *Communications, ICC '92, Conference record, SUPERCOMM/ICC '92, Discovering a New World of Communications., IEEE International Conference on*, vol.3, 1992, pp. 1451-1455.

[59] L. Wu, H.J. Chao, X.J. Zhao, Y. Zhao, Y. Chai, J.P. Zhang and F.-. Choa, “An FPGA controlled WDM buffer memory,” *Lasers and Electro-Optics (CLEO 2000). Conference on*, 2000, pp. 340-341.

[60] Hussein T. Mouftah, Pin-Han Ho “Optical Networks - Architecture and Survivability” Springer (Sep. 30th, 2002), USA.”.

[61] Cisco. *“Fiber Types in Gigabit Optical Communications,”* cisco.com. [Online]. Available:
http://www.cisco.com/en/US/prod/collateral/modules/ps5455/white_paper_c11-463661.pdf [Accessed: Sep. 18, 2013].

[62] Physicsfacts. *“ Fibre Optics,”* physicsfacts.com. [Online]. Available: http://physicsfacts.com/2013/04/fibre-optics/ [Accessed: Sep. 19, 2013].

[63] Yingjun Gao, P.K.C. Chan, C.C. Chan, W. Jin, Y. Zhou and D.N. Wang, “Optimization of coupling a collimated light beam into a single mode fiber by use of GRIN rod lenses,” *Lasers and Electro-Optics CLEO '01. Technical Digest. Summaries of papers presented at the Conference on*, 2001*,* pp. 464.

[64] W. Eisenhauer and H. Richter, “Light coupling from a semiconductor laser into a polarisation-maintaining single-mode fibre,” *Electronics Letters*, vol. 23, no. 5, 1987, pp. 201-202.

[65] Siemon . “*Optical Fiber Transmission, Media, and Applications,*” siemon.com. [Online]. Available: http://www.siemon.com/us/white_papers/13-07-08-light-it-up.asp [Accessed: Sep. 19, 2013].

[66] Zhang Zihua, Zhong Zhiying and Zhu Na, “SRS effect in DWDM systems,” *Proceedings of the 3rd International Conference on Microwave and Millimeter Wave Technology, ICMMT 2002,* 2002, pp. 1075-1078.

[67] Xiaorui Li, Huaping Gong, Shuhua Li and Jianfeng Wang, “Experimental investigation on pulse light stimulated Brillouin scattering in the optical fiber,” *Communications and Photonics Conference and Exhibition,* 2011. *ACP. Asia*, pp. 1-8.

[68] Y.A. Shpolyanskiy, S.A. Kozlov and V.G. Bespalov, “Stimulated Raman scattering and four wave mixing with self-phase and cross-phase modulation of intense fs laser pulses,” *Quantum Electronics and Laser Science Conference QELS '99. Technical Digest. Summaries of Papers Presented at the*, 1999. pp. 128.

[69] A. Chiba, T. Kawanishi, T. Sakamoto, K. Higuma, K. Takada and M. Izutsu, "Low-Crosstalk Balanced Bridge Interferometric-Type Optical Switch for Optical signal Routing," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. PP, no. 99, 2013, pp. 1-1.

[70] S. V. Kartalopoulos, "Introduction to DWDM Technology", New York, USA: IEEE Press, 2000, pp. 91-96.

[71] S. J. B. Yoo, C. Caneau, R. Bhat, M. A. Koza, A. Rajhel, and Neo Antoniades, "Wavelength conversion by difference frequency generation in AlGaAs waveguides with periodic domain inversion achieved by wafer bonding," *Applied Physics Letters*. 1996.

[72] M. Sato, T. Ishigure and Y. Koike, "Thermally Stable High-Bandwidth Graded-Index Polymer Optical Fiber," *J.Lightwave Technol.*, vol. 18, no. 7, 2000, pp. 952.

[73] Michael Needham, John Harris "Traffic and Network Modeling for Next Generation Applications" IEEE International Symposium on Broadband Multimedia Systems and Broadcasting - Multiple Technologies for Multimedia, March 31 – April 2, Las Vegas, Nevada, USA, 2008, pp. 1 - 18.

[74] John Cosmas, Jonathan Loo, Amar Aggoun, Emmanuel Tsekleves"A Matlab Traffic and Network Flow Model for planning the impact of 3D Applications on Networks" Proceeding of IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, 24-26 March 2010, Shanghai, China, pp.1-7.

[75] United Nations Office for the Coordination of Humanitarian Affairs (OCHA) "Basra Governorate Profile*"*, July 2009*,* www.iauiraq.org/reports/GP-Basrah.pdf.

[76] "The YouTube effect: HTTP traffic now eclipses P2P," http://arstechnica.com/news.ars/post/, 6/19/2007.

[77] Ezilon.com, "VoIP versus regular Phone Service: A Comparison", Ezilon.com Articles, Jan 24, 2006, accessed: July 19, 2010. http://www.ezilon.com/information/article_15582.shtml.

[78] "Global IP Traffic Forecast and Methodology, 20062011" - Cisco Systems – 2007.

[79] Johannes Farber, "Network Game Traffic Modeling," NetGames2002, Braunschweig, Germany, April 16-17, 2002, pp.249-247.

[80] McCreary S., claffy k.: Trends in wide area IP traffic patterns - A view from Ames Internet Exchange, *ITC Spec. Seminar*, 2000.

[81] Wu-chang Feng Francis Chang Wu-chi Feng Jonathan Walpole "A Traffic Characterization of Popular On-line Games" IEEE/ACM Transactions on Networking (TON), Volume 13 , Issue 3, June 2005, Pages: 488 – 500, 2005, ISSN:1063-6692.

[82] David Erman,"BitTorrent Traffic Measurements and Models", Blekinge Institute of Technology , Oct. 2005.

[83] J. Loo, "Traffic and Network Flow Model for Assessing Impact of 3D Applications on Internet, The Sixth International Conference on Wireless and Mobile Communications, September, 2010, Valencia, Spain http://www.iaria.org/conferences2010/filesICWMC10/jonathan_loo_keynote_ICWMC_24_09_2010-1.pdf,".

[84] V.P. Kumar, T.V. Lakshman and D. Stiliadis, "Beyond Best Effort: Router Architectures for the Differentiated Services of Tomorrow's Internet," *IEEE Communications Magazine*, vol. 36, 1998, pp. 152-164.

[85] Xiaolong Yang, Shuheng Zhou, Min Zhang, Xuefei Tang and Jinde Liu, "An efficient QoS routing algorithm based on nonlinear path distance for min-sharing interference and load balancing," *Computer and Information Technology CIT '04. The Fourth International Conference on*, 2004, pp. 380-385.

[86] G. O'Driscoll, "Next Generation IPTV Services and Technologies,", Wiley-Interscience Publishing Co., edition 2008.

[87] A. Mahanti, D.L. Eager, M.K. Vernon and D. Sundaram-Stukel, "Scalable On-Demand Media Streaming with Packet Loss Recovery,", Networking, IEEE/ACM. Transactions on, Volume 11 , Issue 2, 2003, pp. 195-209.

[88] "Improving the Quality of Communications with Packet Loss Concealment" Broadcom, White Paper, September 2008, Irvine,USA.".

[89] Haw-Yun Shin and Feng-Ming Yang, "ATCB: A QoS guarantee mechanism in the optical burst switching internet backbone," *IEEE Region 10 Conference TENCON 2007 -* 2007, pp. 1-4.

[90] C. Chuah, "Providing End-to-End QoS for IP-Based Latency-sensitive Applications," Dissertation Proposal, Department of Electrical Engineering and Computer Science, University of California at Berkeley, US, 2006.

[91] B. Goode, "Voice over Internet protocol (VoIP)," *Proceedings of the IEEE*, vol. 90, no. 9, pp. 2002, 1495-1517.

[92] Moshe Zukerman "Back To The Future", *IEEE Communications Magazine*, Volume 47 Issue 11, November 2009, pp 36-38.

[93] Lawrence G. Roberts, “The Next Generation of IP - Flow Routing”, SSGRR 2003S International Conference, July 29, 2003, L’Aquila Italy.

[94] J. Reed, A. J. Aviv, D. Wagner, A. Haeberlen, B. C. Pierce, J. M. Smith, “Differential Privacy for Collaborative Security”, Proceedings of the Third European Workshop on System Security, EuroSys '10 Fifth EuroSys Conference, Paris, France, April 2010.

[95] Y. Chen, T. Farley, N. Ye, QoS Requirements of Network Applications on the Internet, *Information-Knowledge-Systems Management*, Vol. 4 Issue 1, 2004, pp. 55-76.

[96] Cisco, 2008, “Understanding Delay in Packet Voice Networks”. [online] available at: http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml#standarfordelaylimits [Accessed: 14 February 2012].

[97] A. N. Al-Khwildi, S. Khan, K. K. Loo, H. S. Al-Raweshidy, “Adaptive link-weight routing protocol using cross-layer communication for MANET”, *WSEAS Transactions on Communications,* Vol. 6, Issue 11, 2007, pp.833-839.

[98] V. Vijayalakshmi, T.G. Palanivelu, “Secure Antnet Routing Algorithm for Scalable Adhoc Networks Using Elliptic Curve Cryptography”, *Journal of Computer Science*, Vol. 3, Issue 12, 2007, pp. 939-943.

[99] W. Zhang, J. Tang, C. Wang, S. d. Soysa, “Reliable Adaptive Multipath Provisioning with Bandwidth and Differential Delay Constraints”, *INFOCOM'10 Proceedings of the 29th conference on Information communications,* IEEE Press Piscataway, USA, 2010, pp. 2178-2186.

[100] T. Deng, S. Subramaniam, “Adaptive QoS routing in dynamic wavelength-routed optical networks”, *2nd International Conference on Broadband Networks*, BroadNets 2005. Vol. 1, pp. 184-193.

[101] V. N. Raghavan, M. Venkatesh, T. Labbai, P. D. Prabhu, “Evaluating Performance of Quality-of-Service Routing in Large Networks”,*World Academy of Science, Engineering and Technology, 2007.*
Available: www.waset.org/journals/waset/v26/v26-48.pdf [Accessed: 14 February 2012].

[102] B R. Smith , J.J. Garcia-Luna-Aceves, “Best Effort Quality-of-Service”, *Proceedings of 17th International Conference on Computer Communications and Networks*, US Virgin Islands, 2008, pp. 1-6.

[103] Highteck, "OSI Network Layer," highteck.net. [Online]. Available: http://www.highteck.net/EN/Network/OSI_Network_Layer.html [Accessed: Sep. 16, 2013].

[104] Y. Ito, S. Tasaka and Y. Fukut, "Psychometric analysis of the effect of end-to-end delay on user-level QoS in live audio-video transmission"*, IEEE International Conference on Communications,* Vol. 4, 2004, pp. 2214 – 2220.

[105] T. Eisenbart, S. Kuma, "A Survey of Lightweight Cryptography Implementations", *IEEE Design & Test of Computers*, Vol. 24, Issue 6, 2007, pp. 522 – 533.

[106] Jon Oltsik, "The True Costs of E-mail Encryption", white paper, *Enterprise Strategy Group, Inc.*, June, 2010. http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_true-costs-of-email-encryption_analyst-esg.pdf

[107] C.R. Lin, J.-S. Liu, "QoS routing in ad hoc wireless networks", *IEEE Journal Selected Areas in Communications*, Vol.17, No.8, 1999, pp. 1426-1438.

[108] Blum C., Merkle D. (Eds.),"Swarm Intelligence: Introduction and Applications", Springer, Natural Computing Series, 2008.

[109] Gupta A. K. , Sadawarti H. , Verma A. K. , "MANET routing protocols based on Ant Colony Optimization", *International Journal of Modeling and Optimization*, Vol. 2, No. 1, February 2012, pp 42-49.

[110] Varela G. N., Sinclair M. C., "Ant Colony Optimisation for Virtual-Wavelength-Path Routing and Wavelength Allocation", *Proceedings of the 1999 Congress on Evolutionary Computation,* Volume 3, 1999, pp. 1809-1816.

[111] G. Di Caro and M. Dorigo "AntNet: Distributed Stigmergetic Control for Communications Networks", *Journal of Artificial Intelligence Research*, Volume 9, 1998, pp. 317-365.

[112] Matsuo H. and Mori K., " Accelerated Ants Routing in Dynamic Networks", *2nd International Conf. on Software Engineering, Artificial Intelligence, Networking & Parallel/Distributed Computing*, August 2001, pp.333-339.

[113] Yoo J. H., La R. J., and Makowski A. M., "Convergence of ant routing algorithms – Results for a simple parallel network and perspectives," Technical Report CSHCN 2003-44, Institute for Systems Research, University of Maryland, College Park (MD), 2003.

[114] Purkayastha P. and Baras J. S., "Convergence Results for Ant Routing Algorithms via Stochastic Approximation and Optimization", *Proceedings of the 46th IEEE*

Conference on Decision and Control, New Orleans, LA, USA, Dec. 12-14, 2007, pp. 340-345.

[115] Yan X., Wang L. and Li L., “Ant Agent-Based Multicast Routing with QoS Guarantees”, *1st International Symposium on Pervasive Computing and Applications*, Urumchi, Xinjiang, China, 2006, pp. 279 - 284.

[116] Deepalakshmi P., Radhakrishnan S., “Ant Colony Based QoS Routing Algorithm For Mobile Ad Hoc Networks”, *International Journal of Recent Trends in Engineering*, Vol. 1, No. 1, May 2009, pp. 459-462.

[117] Attia R., Rizk R. and Mariee M., “A hybrid multi-path ant QoS routing algorithm for MANETs”, *IFIP International Conference on Wireless and Optical Communications Networks WOCN '09*, Cairo, 2009, pp. 1-5.

[118] Mohammed Al-Momin, John Cosmas, and Saman Amin “Adaptive Three-Layer Weighted Links Routing Protocol for Secure Transmission over Optical Networks”, WSEAS transactions on communications, Issue 8, Volume 11, August 2012, pp. 287-298.

[119] K. Bhaskaran, J. Triay and V.M. Vokkarane, “Dynamic Anycast Routing and Wavelength Assignment in WDM Networks Using Ant Colony Optimization (ACO),” *Communications (ICC), IEEE International Conference on*, 2011, pp. 1-6.

[120] Z. Na, S. Haijin and Z. Naifu, “Ant Colony Optimization for Dynamic RWA in WDM Networks with Partial Wavelength Conversion,” *Photon.Network Commun.*, vol. 11, no. 2, 2006, pp. 229-236.

[121] J. Triay and C. Cervello-Pastor, “An ant-based algorithm for distributed RWA in optical burst switching,” *Transparent Optical Networks ICTON '09. 11th International Conference on*, 2009, pp. 1-4.

[122] S. Ngo, X. Jiang and S. Horiguchi, “An Ant-Based Approach for Dynamic RWA in Optical WDM Networks,” *Photon.Network Commun.*, vol. 11, no. 1, 2005, pp. 39-48.

[123] K. Khairi, R. Parthiban, C.T. Aijiwati, K.C. Lee and R. Mohamad, “Performance evaluation of the ant-based dynamic RWA on WDM optical network,” *Communications and Photonics Conference and Exhibition (ACP), 2009 Asia*, pp. 1-2.

[124] A. Rubio-Largo, M. Vega-Rodriguez, J. Gomez-Pulido and J. Sanchez-Perez, “Tackling the Static RWA Problem by Using a Multiobjective Artificial Bee Colony Algorithm,”, vol. 6692, 2011, pp. 364-371.

[125] P. Leesutthipornchai, N. Wattanapongsakorn and C. Charnsripinyo, “Multi-objective routing wavelength assignment in WDM network using SPEA2 approach,”

Communications and Information Technology ISCIT2009. 9th International Symposium on, 2009, pp. 1057-1062.

[126] H. Ahn, T. Lee, M. Chung and H. Choo, "RWA on Scheduled Lightpath Demands in WDM Optical Transport Networks with Time Disjoint Paths," *Proceedings of the 2005 international conference on Information Networking: convergence in broadband and mobile networking* , vol. 3391, 2005, pp. 342-351.

[127] P. Gurzi, A. Nowe, W. Colitti and K. Steenhaut, "Maximum flow based Routing and Wavelength Assignment in all-optical networks," *Ultra Modern Telecommunications & Workshops ICUMT '09. International Conference on*, 2009, pp. 1-6.

[128] Xiaowen Chu, Bo Li, K. Sohraby and Zhensheng Zhang, "Routing and wavelength assignment issues in the presence of wavelength conversion for all-optical networks," *IEEE Global Telecommunications Conference, GLOBECOM '02.*, vol. 3, 2002, pp. 2787-2791.

[129] K. Lu, G. Xiao and I. Chlamtac, "Behaviour of Distributed Wavelength Provisioning in Wavelength-Routed Networks With Partial Wavelength Conversion,", *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol.3, 2003, pp. 1816-1825.

[130] M. Dorigo, "Optimization, Learning and Natural Algorithms", PhD thesis, Politecnico di Milano, Italy,1992.