Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Telecom Engineering Postgraduate Program

QoS Performance Evaluation of RWA Algorithms under Different Resilience Mechanisms: in the Case of Ethio-Telecom Backbone Network

A Thesis Submitted to the School of Electrical and Computer Engineering of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Masters of Science in Telecommunication Network Engineering

By: Kedir Yassin

Advisor: Dr. Yalemzewd Negash

December 2019

Addis Ababa, Ethiopia

Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

QoS Performance Evaluation of RWA Algorithms under Different Resilience Mechanisms: in the Case of Ethio-Telecom Backbone Network

By: Kedir Yassin

Approval by Board of Examiners

Dr. Yalemzewd Negash _____
Dean, School of Electrical & Computer Engineering Signature

Committee

Dr. Yalemzewd Negash _____
Advisor Signature

Dr. Dereje H/Mariam _____
Examiner Signature

Dr. Beneyam Haile _____
Examiner Signature

Abstract

For the past decades, data traffic demand considerably increased in volume and quality due to the advent of capable end-user devices and innovative data services. To accommodate the highly increasing data traffic volume and customer demand for service with better quality, an automatic switched optical network (ASON) with different routing and wavelength assignment (RWA) algorithms and resilience mechanisms are used. Previously different researchers evaluated performance of different resilience mechanisms and RWA algorithms separately by considering an ideal highly connected network with ideal uniform traffic demand/connection request. This issue can force telecom operators including Ethio-telecom to implement their backbone network based on vendor recommendation.

In this thesis, first, performance of four adaptive RWA algorithms was evaluated considering blocking probability and average throughput as QoS metrics under different three resilience mechanisms considering a practical Ethio-telecom north circle backbone network topology and its traffic demand scenario. Secondly, performance of the three resilience mechanisms was evaluated under routing algorithm selected from routing algorithm evaluation considering blocking probability, recoverability and average network throughput as QoS performance metrics. Finally, network topology connectivity degree effect on the performance of 1+1 DPP and restoration resilience mechanisms was evaluated by randomly adding 30 unidirectional links to the reference network topology used in the above evaluations. To evaluate the RWA algorithms and resilience mechanisms, Net2Plan simulator is used.

The result of the evaluations shows that, at low connected network topology, restoration with alternate routing has on average 40 % lower blocking probability, higher average throughput and lower recoverability as compared to the other resilience mechanisms combined with alternate routing. An increase in network connectivity by 0.9 decreases the blocking probability and average throughput advantage of restoration by 10%. So considering the possibility of improving the recoverability of the network by preparing a pool of restoration path prior to fault occurrence and its ability to protect against double link failure (DLF), restoration with alternate routing becomes more recommended for low connected network topologies at low traffic load. But for highly connected network topologies with high traffic load using either 1+1 DPP or hybrid becomes more recommended based on the need for DLF protection.

Keywords: Network Resiliency, QoS, Recovery, Resource Utilization, RWA, Survivability.

Declaration

I, the undersigned, declare that this thesis is my original work, has not been presented for a degree in this or any other university, and all sources of materials used for the thesis have been fully acknowledged.

Kedir Yassin

Name Signature

Place: Addis Ababa

Date of Submission: December 2019

This thesis has been submitted for examination with my approval as a university advisor.

Dr. Yalemzewd Negash

Advisor's name Signature

Acknowledgment

First and almost I would like to express my sincere gratitude to almighty ALLAH for giving me wisdom, skill, strength, and patience in my life especially in carrying and pursuing my research work. My special and priceless thanks go to my thesis advisor Dr. Yalemzewd Negash for his endless support and kind encouragement during the entire course. His openness, guidance, and support taught me what kindness and research mean and showed me the right direction of research work and life. I would also like to thank Ethio-telecom for giving me this golden opportunity to pursue my MSc at Addis Ababa University, Addis Ababa Institute of Technology. I would also like to thank Addis Ababa Institute of Technology and all the instructors who have been part of this program.

I wish to express my sincere thanks to Mr. Yohannes Beleyneh, Mr. Wendale Kebede and Mr. Alula Adamu for their valuable and kind support and willingness to provide me the necessary input for this thesis and other courses throughout my MSc program. I would also like to thank Ethio-telecom VSAT department manager and its staff members especially to Mr. Berhanu Habtemariam and Ethio-telecom North region O&M, HR, and finance department staff members (especially Mr. Aklilu Desalegn, Ms. Shemshiya M/Siraj, Mr. Teame Berhane, Mr. Zelalem Alemayoh, Mr. Solomon Yimer, and Mr. Anwar Hussien) for their support in providing me necessary inputs for this thesis and their encouragement through the past Years of the MSc program.

I would also like to acknowledge Mr. Bezuayehu Zerihun, Ms. Aselef Teka and Mr. Nigusse Beyene who were really a good hand for me in the course of my class and this thesis with their valuable encouragements and comments. I would also like to thank and Acknowledge my Mother, Ms. Amina Ali, for her priceless support throughout my life. You are my teacher and example of strong work and patience. I would also like to especially my best friends, Mr. Messued M/salih and Mr. Kald Beshir, for their continued support throughout the past Years of the MSc program.

Finally, I want to express my very profound gratitude to my wife, Ms. Benat, and my brave sons (Abdullah and Amar) for providing me with unfailing support and continuous encouragement throughout my years of study and process of doing this thesis. This accomplishment would not have been possible without them. Thank you so much and glad to have you all.

Table of Contents

Abstract i

Declaration ii

Acknowledgment iii

List of Figures vii

List of Tables vii

Acronyms viii

Chapter 1 1

Introduction 1

1.1. Background and motivation 1

1.2. Problem Statement 2

1.3. Objectives 3

1.3.1. General objective 3

1.3.2. Specific objectives 3

1.4. Methodology 4

1.5. Organization of the thesis 5

Chapter 2 6

A general overview of a backbone network 6

2.1 ASON 6

2.1.1 ASON control plane 8

2.2. GMPLS 11

2.2.1. Diverse Switching capabilities 11

2.2.2. GMPLS protocols and Traffic engineering 12

Chapter 3 15

RWA algorithms and resilience mechanisms of ASON 15

3.1. Routing and Wavelength Assignment of ASON network 15

3.1.1. RWA problem strategies in Optical Networks 16

3.1.2. RWA problem solution approaches 17

3.1.3. Routing Algorithms used in ASON Dynamic Provisioning 18

3.1.4. Wavelength assignment solving approaches in optical network 20

3.2. Resilience Mechanisms 21

3.2.1. Protection 22

3.2.2. Restoration 23

3.2.3. Hybrid resilience mechanism 24

3.5. Literature Review 24

Chapter 4 27

Performance Evaluation of RWA Algorithms and Resilience Mechanisms 27

4.1. Problem Formulation 27

4.1.1. Linear Programming (LP) 28

4.1.2. ILP formulation of RWA algorithms and Resilience mechanism 30

4.2. Performance evaluation methodology 37

4.2.1. Net2Plan simulator 38

4.3. QoS Performance parameters 42

4.3.1. Blocking probability 43

4.3.2. Recoverability 43

4.3.3. Average Network Throughput 43

Chapter 5 44

QoS Performance Evaluation Results and Discussion 44

5.1. Simulation setup and assumption 44

5.1.1. Simulation assumptions 46

5.2. Result and discussion on QoS performance evaluation of RWA algorithms under different resilience mechanisms 47

5.3. Result and discussion on QoS performance evaluation of resilience mechanisms 53

5.4. Result and discussion on network connectivity degree effect on QoS Performance of resilience mechanisms 60

Chapter 6 64

Conclusion and Future Works 64

6.1. Conclusion 64

6.2. Future Works 65

References 66

List of Figures

Figure 2.1. ASON Architecture standardized in G. 8080 7
Figure 4.1. Graph of LP problem with decision variables [51] 28
Figure 4.2. Net2Plan architecture [26], [60]–[62] 41
Figure 5.1. North-circle ethio-telecom ASON backbone reference topology 45
Figure 5.2. Blocking probability under 1+1 DPP 49
Figure 5.3. Blocking probability under restoration 49
Figure 5.4. Blocking probability under hybrid resilience mechanism 50
Figure 5.5. Average Network Throughput under DPP 51
Figure 5.6. Average Network Throughput under Restoration 52
Figure 5.7. Average Network Throughput under Hybrid Resiliency 52
Figure 5.8. Blocking probability under Alternate routing with a unidirectional link failure 55
Figure 5.9. Blocking probability under Alternate routing with Bidirectional link failure 56
Figure 5.10. Recoverability under Alternate routing with a unidirectional link failure 57
Figure 5.11. Recoverability under Alternate routing with Bidirectional link failure 58
Figure 5.12. Average Network throughput under Alternate routing with a unidirectional link failure 59
Figure 5.13. Average Network throughput under Alternate routing with Bidirectional link failure 60
Figure 5.14. Blocking probability of resilience mechanisms for different topology 63
Figure 5.15. Recoverability of resilience mechanisms for different topology 63
Figure 5.16. Average network throughput of resilience mechanisms for different topology 63

List of Tables

Table 4-0-1. input Variables of ILP formulation 30
Table 4-0-2. Decision variables of ILP problem 31
Table 5-0-1. Summary of reference network topology 45
Table 5-0-2. sample of Traffic demand matrix in the case 45800 Gbps offered traffic 46
Table 5-3. Summary of modified network topology(B) 61

Acronyms

3G	3rd Generations
ASON	Automatically Switched Optical Network
DES	Discrete Event Simulation
DLF	Double Link Failure
DWDM	Dense Wavelength Division Multiplexing
FAR	Fixed-Adaptive Routing
FR	Fixed Routing
Gbps	Gigabit per second
GMPLS	Generalized Multiprotocol Label Switching
GSM	Global System for Mobile communication
IETF	Internet Engineering Task Force
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
ITU	International Telecommunication Union
ILP	Integer Linear Programming
LCR	Least Congested Routing
LMP	Link Management Protocol
LSA	Link State Advertisement
LSDB	Link State DataBase
LSP	Label Switched Path
MPLS	Multi-Protocol Label Switching
MTBF	Mean Time Between Failures
MTTF	Mean Time to Fail
MTTR	Mean Time to Repair
NGN	Next Generation Network
NMS	Network Management System
OTN	Optical Transport Network
OXC	Optical cross-connect

PCE	Path Computation Element
OSPF	Open Shortest Path First
QoS	Quality of Service
RSVP-TE	Resource Reservation Protocol with Traffic Engineering Extensions
RWA	Routing and Wavelength Assignment
SDH	Synchronized Digital Hierarchy
SPP	Shared Path Protection
SRG	Shared Risk Group
TDM	Time Division Multiplexer
TE	Traffic Engineering
TED	Traffic Engineering Database
TWDM	Time and Wavelength Division Multiplexing
UNI	User Network Interface
WDM	Wavelength Division Multiplexing

Chapter 1

Introduction

1.1. Background and motivation

In the past three decades, a considerable increase in traffic data volume and demand in service with better quality has been witnessed due to the advancement in communication technologies, devices, and innovation of new service types. This traffic increase requires a transport network with the ability to protect the traffic from loss and delay in addition to high capacity transportation. To fulfill this transportation requirement different transport technologies were developed. Out of the developed transport network technologies, automatic switching optical network (ASON) becomes superior due to its high capacity carrying capability with automatic connection request provisioning and control.

ASON is an optical transport network (OTN) with automatic switching functionality which is defined by international telecommunication union (ITU-T). OTN is a wavelength division multiplexing (WDM) based optical transport network framework with a synchronized digital hierarchy (SDH)/synchroneous optical network (SONET) like frame structure and is defined by ITU-T G.709 recommendation. In addition to its OTN transport network, ASON uses generalized multiprotocol label switching (GMPLS) based control plane to automatically and efficiently provision, manage and control a connection request. The GMPLS based control plane supports traffic engineering (TE) to transport network traffic with diverse quality of service (QoS) requirement.

ASON supports mechanisms such as resilience mechanism and automatic routing and wavelength assignment (RWA) to efficiently provision and transports a connection request. Resilience mechanism is a mechanism used to continue providing a service in the case of network failure either by protection or restoration [1]. In Protection, resilience mechanism is provided by preparing backup path prior to fault occurrence but, in restoration, resilience mechanism is provided by automatically preparing a backup or restoration path after fault occurrence. RWA is a combination of routing and wavelength assignment algorithms and is used to automatically find a route and assign wavelength for connection requests arrived in an ASON network [2].

Different works of literature show that different resilience mechanisms and RWA algorithms have different performance with respect to different QoS metrics such as blocking probability [3], [4], [5]. This performance difference, in turn, affects QoS offered by telecom operators to customers that pass through an ASON network deployed with resilience mechanisms and RWA algorithms. QoS is defined by ITU-T as the collective effect of service performance which determines the degree of satisfaction of a user of the service and is dependent on the capability of a network [6]–[8]. In an internet protocol (IP) based network, QoS can be measured by bandwidth, latency, Bit Error Rate (BER), throughput and Jitter. Even though there are different works of literature that show the effect of different resilience mechanisms and routing algorithms on QoS by considering different QoS metrics separately, these parameters are not thoroughly evaluated considering different topologies and traffic volumes, to the best knowledge of the author, especially dynamic type routing algorithms. Thus, it is important to evaluate the effect of routing algorithms and resilience mechanisms on QoS in order to provide service with the required performance.

1.2. Problem Statement

Customer's demand for services with better quality is increasing from time to time. This increase in demand forces telecom operators to deploy their network with network parameters such as resilience mechanism and routing algorithm that offer better QoS. Even if there are some papers that evaluate the effect of resilience mechanisms and routing algorithms on QoS separately, the result of the paper does not show the exact combined effect of the two parameters, the resilience mechanism and the RWA algorithm, on QoS. This means the papers focus either on the routing algorithm without the use of a resilience mechanism or resilience mechanism without considering the routing algorithm, to the best of the author's knowledge. In addition to this, the research works mainly consider ideal laboratory reference topologies such as the National Science Foundation Network (NSFNET) and European topologies without considering practically used network topologies by network operators across the world. The lack of research work done based on practically used network topologies and traffic demand can force telecom operators to use network parameters such as resilience mechanism and routing algorithm based on vendor recommendation which is not exactly evaluated on their network. In a way, the resource utilization efficiency and quality of services offered by their network can be affected by the use of a network parameter that is not evaluated on their network. Network connectivity effect on resource utilization of a network is shown in research

work [9]. But there is no research work that evaluates a network connectivity effect on the performance of network parameters, to the best of the author's knowledge.

Ethio-telecom deployed an ASON transport network with GMPLS based control plane in 2015 [10], [11]. In deploying the backbone network, Ethio-telecom used a resilience mechanism and RWA algorithm based on vendor recommendation. For example, Ethio-telecom used a 1+1 dedicated path protection (DPP) resilience mechanism based on the vendor recommendation considering the results of research works done on ideal laboratory network topologies. Based on the performance evaluation results done on an ideal network, it is difficult to know the exact performance of the network parameters on the physical network topology.

Considering the above-mentioned cases, lack of research works done based on a practical scenario and the increase in service demand with better QoS, and the current Ethio-telecom backbone network implementation scenario, this thesis answers the following research questions:

- "Which combination of resilience mechanism and routing algorithm offers service with better QoS on low connected backbone network topology? What tradeoff does the combination have?"
- "How network topology connectivity degree affects the QoS performance of different resilience mechanisms?"

1.3. Objectives

1.3.1. General objective

The general objective of this thesis is to evaluate QoS performance of RWA algorithms under different resilience mechanisms using QoS matrices blocking probability, recoverability and average network throughput and propose a combination of routing algorithm and resilience mechanism that better overall performance. The evaluation will take Ethio-telecom north circle GMPLS based ASON backbone network as a case study.

1.3.2. Specific objectives

The following specific objectives are undertaken to achieve the main objective of this thesis:

- Evaluate four adaptive **RWA** algorithms, shared risk group (SRG)-disjoint aware first-fit, least congested routing, Load-sharing, and alternate, under three different **resilience** mechanisms, 1+1 dedicated path protection, Restoration and Hybrid, in Ethio-telecom north-circle GMPLS based ASON backbone network
- Compare the performance of the RWA algorithms and select an RWA algorithm with better blocking probability and average network throughput.
- Evaluate resilience mechanisms, 1+1 dedicated path protection, Restoration and Hybrid, under the RWA algorithm selected by RWA algorithm evaluation.
- Select a resilience mechanism with better blocking probability, recoverability, and average network throughput.
- Evaluate **network topology connectivity degree** effect on performance resilience mechanisms, 1+1 DPP and restoration, under RWA algorithm selected by RWA algorithm evaluation considering two network topologies with different connectivity degree.
- Generalize evaluation result of network topology connectivity degree effect on the performance of resilience mechanism, RWA algorithm and resilience mechanism evaluation.
- Recommend a better resilience mechanism and RWA algorithm combination for topologies with different connectivity degree.

1.4. Methodology

In this thesis, the following methodology is applied to evaluate the performance of RWA algorithms under different resilience mechanisms and select a combination of an RWA algorithm and a resilience mechanism with better overall performance.

- Data collection is done to identify RWA algorithms and resilience mechanisms supported by an ASON network by reviewing related literature, company documents, white papers and equipment manuals. To understand the current implantation scenario, its topology, and traffic demand and identify its gap a brief discussion is done with Ethio-telecom transmission experts.
- Data analysis is done to understand the property of the RWA algorithms and resilience mechanisms collected and select QoS metrics suitable to evaluate the RWA algorithms and resilience mechanisms.

- Problem formulation: the identified RWA algorithms and resilience mechanisms were formulated as integer linear programming (ILP) based on related literature and their property.
- Evaluation: Net2Plan simulator is used to evaluate the RWA algorithms and resilience mechanisms by solving their ILP formulation indirectly. The parameters of the Net2Plan simulation tool is setup based on the property of the RWA algorithms and resilience mechanisms. In the evaluation, Ethio-telecom north circle GMPLS based ASON backbone network topology and its traffic demand scenario are considered. In addition to this, the effect of network topology connectivity degree is evaluated by evaluating the performance of resilience mechanisms using Net2Plan in two network topologies.
- Result analysis and recommendation: the performance result of RWA algorithms and resilience mechanism is analyzed to identify an RWA algorithm and a resilience mechanism with better performance. In addition to this, the operational requirement of the RWA algorithms and resilience mechanism is evaluated to select a combination of RWA algorithm and resilience mechanism with better performance and less operational complexity.

1.5. Organization of the thesis

The remaining part of this thesis is organized as follows. Chapter 2 of this thesis presents a general overview of ASON, GMPLS, and enabling features. Chapter 3 presents a brief discussion of RWA algorithms and resilience mechanisms supported by an ASON network. in addition to this, Chapter 3 gives a review of some related works previously done on resilience mechanisms and RWA algorithms. Chapter 4 gives some basics on ILP and presents a brief discussion on the problem formulation, performance evaluation methodology, QoS performance metrics used in this thesis to evaluate the RWA algorithms and Resilience mechanisms. Chapter 5 briefly discusses simulation assumptions and setup used in this thesis to evaluate the RWA algorithms and resilience mechanisms. In addition to this, chapter 4 gives detail performance evaluation results and discussion on performance evaluation of RWA algorithms and Resilience mechanisms. Chapter 6 presents the conclusion of the research work and discussion on future research work directions.

Chapter 2

A general overview of a backbone network

A backbone network is a name used to represent a telecommunication network segment that interconnects access network elements with the central core network. The main function of a backbone network is to transport aggregate traffic or service between different parts of a network. A backbone network is some times called a core network. Due to the aggregate nature of the traffics carried by the backbone network, implementation of a backbone network is required transport network technologies with high capacity carrying capability. In addition to high capacity carrying capability, a backbone network is required to efficiently and successfully transport the high capacity traffic in case of network failure. To fulfill the requirement of a backbone network, high capacity and protection against failure and delay, different transport network technologies have proposed and developed. ASON is one of the transport network technologies defined by ITU-T and becomes superior due to its automatic switching with high capacity carrying capability [12]–[14]. In addition to ASON, GMPLS based control plane was developed by the international ethernet task force (IETF) to make the backbone network more reliable with the capability of transporting services with diverse QoS [15]. The remaining sections of this chapter give a detail discussion about ASON and GMPLS and their enabling features and functions.

2.1 ASON

ASON is an OTN network with automatic switching capability and is defined by ITU-T in recommendation G.8080 [12], [13], [16]. OTN is a wavelength division multiplexing (WDM) based optical transport technology with SDH/SONET like framing structure. The SDH/SONET like framing structure helps OTN to have superior management with better forward error correction (FEC), fault detection and network monitoring in addition to its high capacity carrying capability. ASON is defined as a three-plane network, management, control, and transport planes, architecture that interacts with each other to successfully and efficiently transport services between different parts of a telecommunication network [17]. Figure 2.1 below shows ASON architecture defined by ITU-T.

The functions of the three planes can be described as follows:

Transport plane (data plane): - is a layered transport plane that represents the functional resources of the network that convey user information between different locations of a network. The transfer of information in this plane is either bi-directional or unidirectional.

Control plane: - performs the call control and connection control functions. It provides network intelligence-based automated functions such as automatic discovery, routing, and signaling.

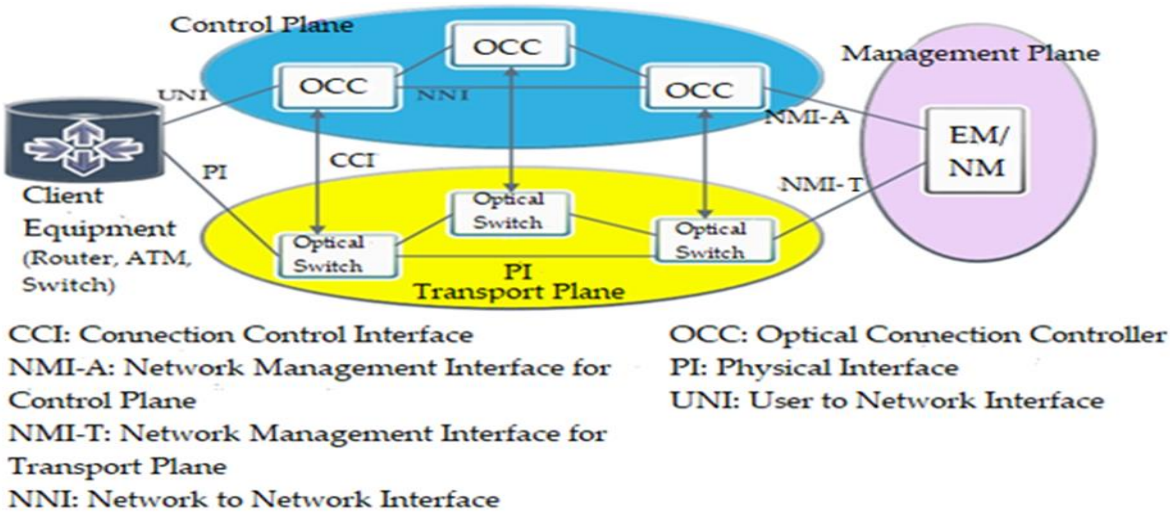

Figure 2.1. ASON Architecture standardized in G. 8080

Management plane: - performs management and coordination functions for the transport plane, the control plane and the system as a whole. The management plane function is less automated than the control plane function.

Even though the three planes of ASON are autonomous, some interactions occur between these planes in operating on a common underlying resource [13]. The interaction between the three planes can be classified into management - transport interaction, control - transport interaction, and management - control interaction. Information presented to a control plane is presented to the management plane but not all information presented to the management plane is presented to the control plane. Even if control plane interfaces used for monitoring, setting policies and affecting internal behavior employed by the management systems, the management plane does not access resources via these resources but manages the components.

The main enabling component of an ASON network is its control plane. An ASON control plane helps the transport network more reliable with no manual interaction. The next subsection gives a brief discussion about an ASON control plane.

2.1.1 ASON control plane

The control plane is a set of communicating entities that are responsible for setting up, maintenance and release of end-to-end connection[12], [17]. Signaling is used to support these capabilities. An ASON control plane is responsible for the call and control connection. A call is an association between endpoints that support an instance of service, while a connection is a transport entity capable of transferring information between its inputs and outputs. The main feature of an ASON control plane is its separation of connection and call control functions. End-to-end session negotiation, call admission control, and call state maintenance are responsibilities of call control. On the other hand, connection control is responsible for the setup and release of connections and connection state maintenance. Due to the separation of call and connection control functions, the connection can be released and re-established while the associated call session is up. In addition to this, this separation reduces call control information at intermediate connection control nodes since call control is provided only at user-network interface (UNI) or (an ingress port) and external network-network interface (E-NNI) or (network boundaries), and not at internal network-network interface (I-NNI).

Authentication of the user and checking the requested service parameters against a service level specification at the starting node is the responsibility of call admission control [12], [13], [16]. In addition to this, call admission control checks if the called user is able to accept the call. On the other hand, the existence of sufficient resources (like wavelength) to admit connection is checked by connection admission control.

Some of the main functions and enabling features of an ASON control plane are discovery, routing, signaling, and survivability. Detail discussion about the main functions and enabling features is given in the following sub-sections.

2.1.1.1. DISCOVERY FUNCTION

ASON control plane provides automatic discovery functions that are used to eliminate explicit manual configuration [12] [17]. This automatic discovery process involves the exchange of identity attribute messages between nodes and uses different relevant protocols in acknowledged or unacknowledged mode. In acknowledged discovery mode, the discovery message contains the attribute of near-end and its acknowledge message contains the attribute of the far end but in unacknowledged mode, both ends send their attribute identity. ASON

control plane provides three automatic groups of discovery functions, neighbor discovery, resource discovery and service discovery.

Neighbor discovery is used to determine the state of local links connecting to all neighbors. This discovery function is used to detect and maintain adjacency of nodes as well as truck adjacent network elements connectivity. Resource discovery is used for the discovery of network topology and its resources by nodes [13] [17]. This discovery function helps for the determination of available network element resources, their capability and level of resource protection. Service discovery, on the other hand, is used for network service capability verification and exchange. The network service capabilities may be defined by administrative domains capability to support a different class of service (CoS), the grade of service (GoS), connection adaptation flexibility and routing.

2.1.1.2. ROUTING FUNCTION

Routing is a process used for path selection in connection establishment through a network[13]. ITU-T Recommendations G. 7715/Y.1706 described ASON routing Architecture and its requirements. ASON routing architecture and its functional components including path selection, routing attributes, abstract messages, and state diagrams are covered in this recommendation. ASON routing architecture supports hierarchical, source-based and step-by-step routing which results in a different distribution of components between nodes and their mutual relationships.

In hierarchical routing, connection controllers have hierarchical relation and each sub-network only knows its own topology [12], [16]. Path selection starts at the top of the hierarchy and the sequence of sub-networks is defined in a lower level through which a path can be found between a given source and destination node. Source-based routing is implemented by the federation of connection and routing controllers and the first controller of a routing area selects the path with the help of route information from different routing controllers in its domain of responsibility. In step-by-step routing, path selection is invoked at each node to obtain the next link of a path to a destination and requires less routing information than the other routing methods.

2.1.1.3. SIGNALING FUNCTIONS

Signaling function involves transporting control messages between all communicating entities of the network's control plane[13]. Signaling protocols are used to create, maintain, restore, and release connections that are essential for enabling fast provisioning and fast recovery after a failure. In addition to this, signaling functions are also used for Automatic discovery and routing functions of an ASON network which gives ASON network the intelligence to replace time-consuming manual tasks such as manual topology updates and path selection. ITU-T Recommendations G.7713/Y.1704 specifies signaling operations for call setup and release.

2.1.1.1.4. SURVIVABILITY MECHANISM OR FUNCTION

Survivability is the capability of a network to continue its function under failure conditions of network elements or links[13]. In an ASON network, survivability is achieved either by protection or restoration mechanism. Protection is implemented by replacing failed network resources such as link or path by pre-assigned standby resource but restoration is implemented by rerouting affected traffic using available spare resources. Restoration action completion takes more time than protection action.

In an ASON network, the survivability function involves all the functional planes[12]. The management plane is responsible for protection configuration of transport plane protection but the transport plane informs control plane about all transport plane resource failures, additions and removals, in order to trigger control plane, supported restoration in case of protection action failure. Both working and protection connections are created by the control plane in the control plane protection mechanism or function. In order to do so, only connection controllers of source and destination are involved. In ASON, with the help of ASON control plane functional elements and its interaction with management and transport planes, three types of connections can be established or provided[13]. The three connection types are permanent, soft permanent and switched optical connections and they differ with each other by their establishment type.

Permanent Optical connection (Provisioned connection): - can be set up by the management system or manual intervention[13]. This connection type is static which lasts relatively for a long period of time and does not involve automatic routing or signaling as well as control plane intervention.

Switched connection: - is established and released on demand using routing and signaling capability of the control plane in communicating endpoints [17]. User-Network Interface (UNI) is required, in this type of connection, in addition to network-to-network interface (NNI) and physical interface (PI) required in the other two connection types. In addition to this, this connection is established either by end-user (client network) or customer equipment. This connection enables the bandwidth-on-demand service.

Soft permanent optical connection: - is established by setting up the switched connections between pre-established edge side permanent connections[12], [16]. To establish this connection type management System Triggers Control Plane (CP) of the head-end node and is called a hybrid connection. This connection type supports traffic engineering or dynamic re-establishing of failed connections and enables the provision of bandwidth-on-demand service.

2.2. GMPLS

GMPLS is a protocol suite with advanced network signaling and routing mechanisms developed by IETF to automate end-to-end connection setup of all types of traffics [15], [18]. This protocol was developed by extending Multi-Protocol Label Switching (MPLS) protocol's Label Switching Router (LSR) function to forward traffic or give switching decisions based on a time slot, wavelength or physical ports [19]. In addition to this, GMPLS extends MPLS protocol to support traffic engineering to dynamically provision different levels of QoS and manage network resources efficiently. Some of the features or functional capabilities supported by GMPLS are the following:

2.2.1. Diverse Switching capabilities

GMPLS defines five layers of switching capable interfaces in both packet and non-packet domains [15]. The defined five layers are Packet Switch Capable (PSC) interfaces, Layer-2 Switch Capable (L2SC) interfaces, Time-Division Multiplex Capable (TDM) interfaces, Lambda Switch Capable (LSC) interfaces, and Fiber-Switch Capable (FSC) interfaces. In order to support the required diverse switching capabilities, GMPLS introduces a new generalized label format that contains the information required for switching decision of the received data. The generalized label may contain wavelength, timeslot, or fiber line information based on the interface switching capability. In addition to this, GMPLS extends MPLS's label distribution that starts from upstream LSR requesting label from downstream LSR to include allowing of

label suggestion by upstream LSR but this suggested label can be overridden by downstream LSR.

In GMPLS, Label Switched Paths (LSP's) are created in the same fashion as that MPLS but the forwarding table of GMPLS includes the labels directly related to the required resource of the network type which is different from that of MPLS forwarding table [15], [20]. In addition to this, LSP of GMPLS may include different LSPs with different switching capabilities (for e.g. packet-switched LSP may include TDM capable LSP in its intermediate link).

2.2.2. GMPLS protocols and Traffic engineering

GMPLS extends two IP/MPLS routing protocols to support traffic engineering. These extended routing protocols, Open Shortest Path First extended for Traffic Engineering (OSPF) and Inter System to Inter System extended for Traffic Engineering (IS-IS), mainly used to Auto-discover network topology and resource availability advertisement [15], [21]. In addition to these two routing protocols, GMPLS extends signaling protocols, resource reservation protocol (RSVP) and constrained label distribution protocol (CR-LDP), to support traffic engineering. On the other hand, GMPLS introduced a new protocol to manage and maintain control and data plane health of neighboring nodes. This protocol is called the Link Management Protocol (LMP). The following Figure 2.2 shows the GMPLS protocol suite.

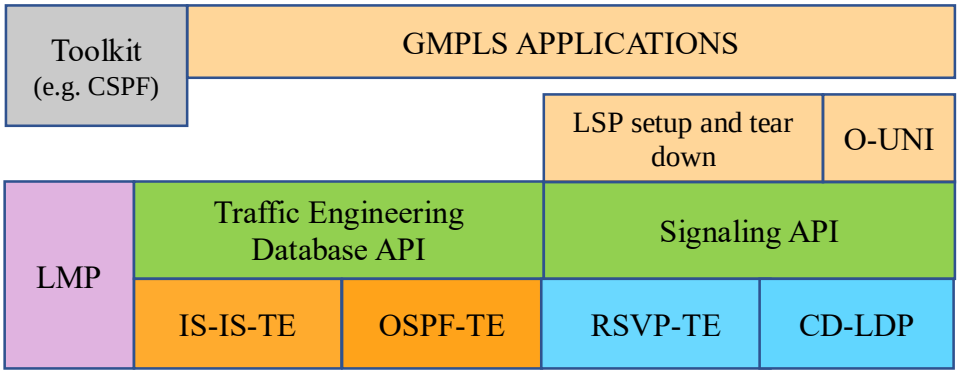

Figure 2.2. GMPLS Protocol Suite [18]

2.2.2.1. GMPLS ROUTING PROTOCOLS

Routing protocols are used to advertise resource availability and Auto-discover network topology. This facilitates end-to-end service provisioning [15], [20], [22]. In GMPLS two routing protocols, OSPF-TE and IS-IS TE, are used to perform this function. In addition to this function, GMPLS routing protocols are enhanced to support the following features:

1. **Support for unnumbered links**: - unnumbered link is a link without IP address that is a link with a combination of unique router ID and link number [20]. In case of unnumbered link advertisement where the advertisement contains local and remote link identifier, the router checks the remote identifier and assign "0" if the remote identifier not identified by the router.

2. **Link protection type**: - this information is used to setup LSP with certain protected characteristics and represents the protection capability of the link [20]. In this message six protection types are supported: extra traffic, unprotected, shared, dedicated 1+1, dedicated 1:1, and enhanced.

3. **Shared Risk Link Group (SRLG)** information: - Shared Risk Link Group is a set of links that share the same resource that may affect all the links and are identified by a 32bit number [20]. This information is used by the path computation algorithm to find a link with disjoint SRLGs in computing path between two LSRs.

2.2.2.2.GMPLS SIGNALING PROTOCOLS

GMPLS signaling protocols are used in the establishment of traffic-engineered LSPs between two nodes or LSRs [15], [20], [22]. GMPLS uses Traffic Engineering extensions of RSVP (Resource Reservation Protocol) and CR-LDP (Constraint-based Routing Label Distribution Protocol0 signaling protocols used in IP/MPLS protocol suites.

2.2.2.3. LINK MANAGEMENT PROTOCOL (LMP)

LMP is an IP-based protocol that includes extensions to the Resource Reservation Protocol-Traffic Engineering (RSVP-TE) and Constraint-Based Label Distribution Protocol (CR-LDP) signaling protocols [21]. This protocol is used to control and maintain the health condition of control and data planes between neighboring nodes or LSRs [15], [20]. The following are the main functions of LMP:

1. **Control channel management:** which is used to establish and maintain connectivity between neighboring nodes. Due to the separation of data and control planes in GMPLS, control-plane neighbors may not be data-plane neighbors.

2. **Link property correlation**: this is used to synchronize TE link properties of local and remote nodes.

3. **Fault localization and notification**: this feature of LMP is used to localize link and channel faults of opaque and transparent optical networks that are independent of the data's encoding scheme and bit rate.

Chapter 3

RWA algorithms and resilience mechanisms of ASON

In Chapter 2 overview of ASON, GMPLS and their enabling features and functions are discussed in detail. To efficiently use ASON functions discussed in chapter 2, different enabling mechanisms and algorithms were developed by different authors. Out of the developed enabling mechanisms and algorithms, resilience mechanisms and RWA algorithms are the main concerns of this thesis. Detail discussion on RWA algorithms and resilience mechanisms supported by an ASON network is given in this chapter. The first section of this chapter gives a brief discussion on what RWA algorithm means, use, classification, and possible solving approach. the second section of this chapter gives a brief discussion on the resilience mechanism, its classification, and its use. The third and fourth section of this chapter discusses ILP and QoS respectively. The final section of this chapter gives a review of previous related research works.

3.1. Routing and Wavelength Assignment of ASON network

In an ASON network, because of its connection-oriented nature, communication between source and destination to exist, a connection needs to be set up from source to destination. The first step before setting up a connection, a path from source to destination should be determined. Then free wavelength will be allocated to the determined path in the optical domain. This all-optical path is called a light-path [2], [5], [23], [24]. The light-path can be allocated a wavelength differently by different intermediate nodes based on the capability of wavelength conversion of the nodes. But the commonly used wavelength allocation is allocating the same wavelength for the whole path which also called wavelength continuity constraint.

As previously stated in describing the functions of GMPLS, the GMPLS control plane was developed with the capability of supporting five different types of switching functions. Switching a signal based on the wavelength of the incoming signal is one of these switching capabilities which is used in an ASON network. This switching function is done by wavelength sensitive switches of intermediate nodes of the path. Due to this capability, ASON is also called a wavelength-routed network [5], [23]–[25]. The phenomenon of path computation and wavelength assignment is called the Routing and Wavelength Assignment (RWA) problem.

The first step in the RWA problem is identifying light-path requests that can be transported on the network with different wavelengths [23]. After light-path request identification, a path with a specific wavelength will be allocated for the accepted light-path requests. In assigning wavelengths for the light-paths, light-paths with disjoint paths can be assigned the same wavelength but light-paths routed in the same path assigned different wavelengths. Light-path requests are blocked if the light-paths cannot be established due to wavelength unavailability. For minimizing the number of light-paths blocked, different RWA problem strategies are followed based on the traffic type handled by the problem.

3.1.1. RWA problem strategies in Optical Networks

Based on the traffic request arrival, RWA problem strategies can be classified as static and dynamic RWA problem strategies [2].

Static RWA

In this RWA strategy, light-paths are statically established between source and destination node pairs due to prior knowledge of light-path requests and its static traffic nature [23]. This type of strategy mainly used in the planning phase of a large transport optical network which can be planned by using aggregate demand factor and its future forecast value. The algorithms proposed for such type of problems are called off-line algorithms. In static RWA strategy, due to the static nature of the traffic, the number of light-path established is unchanged for a long time.

Dynamic RWA

In this RWA strategy, light-paths are established dynamically after traffic arrival due to the dynamic nature of the traffic request with sequential arrival and random holding time of the traffic request [2]. The number of light-paths established in dynamic RWA strategy may vary frequently due to frequent variation of light-path requests. This type of RWA strategy mainly used in the operational phase of an optical network due to the individual light-path routing requirement for efficient network management. The algorithms proposed for such type of problems are called on-line algorithms. Due to the adaptive use of real network status, dynamic RWA algorithms have lower blocking probability as compared with that of Static RWA algorithms.

3.1.2. RWA problem solution approaches

There are different approaches to solve RWA problem strategies [2], [24], [26]. Some approaches solve the RWA problem by partitioning the RWA problem into routing and wavelength assignment sub-problems but others solve the RWA problems as it is either directly by using a direct solving method or by indirect heuristic solving method.

One Step RWA Problem Solution

In this approach, RWA, static and dynamic, problems are solved by jointly considering the routing and wavelength assignment problem [23]. The first step in solving the RWA problem is formulating the problem mathematically with the specific objective function. Some literature formulates an Integer Linear Programming (ILP) as multi-commodity flow with the different objective functions. Some consider an objective function that minimizing blocking probability, others with minimizing a used number of wavelengths or minimization of network congestion. After formulating the RWA problem mathematically, the mathematical formulation can be solved either by using direct solving method using solvers such as CPLEX optimizer and GNU linear programming kit (GLPK) or using heuristic approach by writing an iterating program based on the formulated mathematical model then feed the program to suitable simulator such as java-based Net2Plan simulator. Due to the NP-hard complete nature of the RWA problem, this type of RWA problem-solving approach requires long running time and does not give an optimal solution in polynomial time especially for large networks. One-step RWA problem-solving approach is more suitable for small size networks with static traffic. But due to the lack of prior information about traffic requests in a dynamic RWA problem, this approach does not give an optimal solution for dynamic RWA problem.

Two-Step RWA Problem Solution

In this RWA problem-solving approach, the RWA, static and dynamic, the problem is decomposed into routing and wavelength assignment sub-problems and solve one sub-problem independent of the other. The routing sub-problem is commonly solved using a mathematical problem-solving method after formulating the routing sub-problem mathematically independent of the wavelength assignment sub-problem [27], [23]. On the other hand, the wavelength assignment sub-problem is solved using a graph coloring problem where the nodes of the graph correspond to the demands with links considered as constraints imposed over the

demand based on their possibility of routing over the same link. So, the solution of the routing sub-problem is used for route establishment of a light-path and the solution of the wavelength assignment sub-problem is used for assigning a wavelength to the established light-path. This RWA problem-solving method generates a more optimal solution for large networks with dynamic traffic requests than the one-step RWA solution method. In addition to direct solving of the routing sub-problem, it can be solved by using a heuristic method to minimize the required running time to solve the problem. This heuristic method gives an approximate solution to the routing sub-problem with less running time than the direct solving method and is more suitable for large networks.

3.1.3. Routing Algorithms used in ASON Dynamic Provisioning

ASON network requires routing algorithms with the capability of dynamic connection request provisioning with real-time network state and resource usage detection to minimize connection request blocking probability and maximize resource efficiency of the network. In addition to this, ASON requires routing algorithms that can efficiently handle the additional technologies added to the traditional optical network such as wavelength converters and optical exchanges. GMPLS based control plane helps the ASON network to handle connection requests in a reliable and fast way by frequently updating the network topology and network resource usage [26], [28], [29]. Even though different dynamic routing algorithms like fixed routing and fixed-alternate routing was developed for all-optical OTN network without control plane, the developed dynamic routing algorithms lack intelligence in dynamic congestion minimization and automatic connection request provisioning [26], [30].

With the help of GMPLS based control plane capability, two types of RWA algorithms, hierarchical and source-based, were proposed for ASON network with GMPLS based control plane to efficiently handle its dynamic connection request. ASON specification documents recommend hierarchical based routing for scalability but in a practical scenario, source-based routing is common due to its ability of real network realization by fast and efficient connection request provisioning[26], [28], [29]. In Source routing routes are calculated in source node based on the network information state contained in its database.

Considering the above requirements of an ASON network, different routing algorithms were developed based on the above two specification recommendations [26], [31]. Some of the commonly used adaptive/dynamic routing algorithms developed for dynamic ASON

connection provisioning are SRG-Disjoint Aware First-Fit Routing, Alternate Routing, Least Congested Routing (LCR) and Load Sharing. The above routing algorithms are source-based routing algorithms and the source node of an ASON network establishes a light-path populate routing table by first computing K-shortest alternate routes considering real-time state information of the network.

SRG-Disjoint Aware First-Fit Routing: - in this RWA algorithm, the k-shortest path routing table is populated considering SRG disjointness of the k alternative routes [26], [31], [32]. SRG is a group or set of links with common risk or vulnerability like a group of fibers covered in one conduit. In SRG-disjoint Aware First-Fit routing, the source node maintains a routing table of k SRG disjoint alternative paths by iteratively searching nonSRG overlapping routes out of the possible existing path between specific source-destination pairs. Routes with minimum or no SRG overlap are given high probability in this algorithm. Wavelength assignment used in this algorithm is first-fit as it is indicated in its name. after the populating routing table, this algorithm assigns a wavelength to the connection request considering the availability of wavelength in the alternative paths based on their order of SRG overlap.

Alternate Routing: - in this routing algorithm, the source node computes k alternative path for each source-destination pair and then maintains the computed k routes in its routing table in order prior to the arrival of connection request [26], [31]. when connection request arrives, the source node selects a first available path from the routing table. A connection request is blocked only if there exists no available wavelength in all the k alternative routes computed.

Least Congested Routing: - in this routing algorithm, source node computed k alternative routes considering the congestion level of their path and maintains in its routing table by the order of their congestion level [26], [31], [33]. The congestion level of the routes is measured by the available number of wavelengths. A route with a minimum number of lengths is considered a highly congested route. When a connection request arrives, the source node selects a path with minimum congestion or a path with more number of idle wavelength for the connection request. if two-path exist with the same number of idle wavelength, a path with less number of is selected.

Load Sharing: - in this routing algorithm, the source node selects a path with probability p which is proportional to the traffic carried by the path after computing k shortest paths for each source-destination pair [26], [31]. This algorithm works based on the popular reduced load

approximations algorithm used in loss networks. In this algorithm, a connection request is blocked if there is no wavelength in the selected path without searching for possible alternate paths. Due to this, this algorithm is not common in practical networks.

3.1.4. Wavelength assignment solving approaches in optical network

After the route selection of a connection request by solving the routing sub-problem, the wavelength should be assigned to the connection request from the available wavelength [5], [23], [34], [35]. Different approaches that can be used to solve wavelength assignment sub-problem and effectively assign a wavelength to the previously selected route were developed/proposed in different kinds of literature. The majority of the proposed wavelength assignment approaches consider static connection requests with a variable number of wavelengths and their main objective is minimizing the number of wavelengths used. Out of the proposed wavelength assignment approached that consider static traffic connection, there are also dynamic wavelength assignment approaches that consider the practical dynamic connection request scenario with a constant number of wavelengths. The main objective of the dynamic wavelength assignment approach is minimizing the blocking probability of a connection request. The dynamic wavelength assignment approaches mainly use a heuristic method to solve the wavelength assignment sub-problem. Some of the proposed heuristic-based dynamic wavelength assignment approaches are Random, first-fit, Most-used and Least-used.

Random Wavelength Assignment: - this approach assigns wavelength for a light path dynamically with uniform probability after searching all the available wavelength set for the established route or light-path [35].

First-Fit Wavelength Assignment: - in this approach, the first available wavelength with a lower index number is selected after ordering/indexing the searched available wavelengths [23], [35]. In indexing the wavelengths, the currently used wavelengths are indexed with an upper order index number or packed to the lower end of the wavelength space to give the free available wavelengths with longer paths high probability of selection. This approach does not require global information and has a lower computational cost than random wavelength assignment because the first fit does not search for all the available wavelength sets. In addition to this, the first fit has better blocking probability and fairness as compared to other wavelength assignment approaches. Due to this, this approach is preferred in practice.

Least-Used Wavelength Assignment: - this approach selects least used wavelengths to balance the connection load among the available wavelengths [23], [35]. This approach allows paths that traverse a small number of links to be serviced by the network by quickly breaking the long paths. Least-used have worst performance than random wavelength assignment with higher communication overhead due to its global information required to identify last used wavelength. In addition to this, this approach requires additional storage to store global information and have high computational cost. This approach is not preferred for a practical case.

Most-Used Wavelength Assignment: - in this approach selects the most used wavelength [35]. This approach has better performance than first fit and least used wavelength assignment approaches in packing the connection requests to a minimum number of wavelengths. But due to global information requirements, this approach has higher communication overhead, storage and computational cost than first-fit.

All the above routing algorithms are commonly used with a first-fit wavelength assignment algorithm due to its low computational complexity and overhead in addition to its lower blocking probability and fairness.

3.2. Resilience Mechanisms

Resilience is defined as the ability to provide the required service in the presence of failure [1]. Resilience is sometimes called as survivability or fault-tolerance. Resilience mechanism is a word used to define the mechanisms used for guaranteeing resilience. In an ASON optical network, similar to other WDM based optical networks, the resilience of a network is the main issue due to the large traffic volume carrying capability of the network. In such networks, one link or node failure can cause high traffic loss in its network. As a result of this, a large number of customers can be affected which also affects the revenue of service providers. To minimize or protect the network from such losses, network operators consider the resilience of the network in the planning and operating phase of their network. Different resilience mechanisms differ by their resource allocation and recovery path or link provisioning time. As a general classification, resilience mechanisms are divided into two as protection (proactive) and restoration (reactive) resilience mechanisms based on their recovery path or link provisioning time.

3.2.1. Protection

Protection is a resilience mechanism that provides the resilience of a network by prior planning, computation, and reservation of a redundant resource for protection [36]–[38]. Due to this, this resilience mechanism does not require signaling for topology and resource updates at the time of failure occurrence and has a fast fault recovery time. But the resource requirement of this mechanism is high due to its prior reservation of redundant resources for protection. The priory reserved protection resource can be used to protect single or multiple primary paths based on the type of protection. Protection can either be configured as a dedicated or shared path or link protection based on the usage of the reserved protection resource. In addition to the previously mentioned types of the configuration used in protection mechanism, protection mechanisms configured as reverting or non-reverting type based on the returning possibility of the signal from protection path to primary path after failure maintenance. In the reverting type of protection, the recovered signal returned to the primary path after the maintenance of the failure. But in non-reverting protection, the recovered signal continues in the protection path even if the failed link or path is maintained

Dedicated protection: - dedicated protection is provided by priory assigning protection resources to specific in addition to planning, computation, and reservation of the protection resource [3], [37]–[39]. Dedicated Protection can be configured as dedicated path protection (DPP) which is used to protect single end-to-end path or dedicated link protection which is used to protect a single link. In addition to this, dedicated protection can also be configured as 1+1 or 1:1 based on the possibility of using the dedicated protection resource to carry low priority traffic until a fault happens in its primary path. In 1+1 DPP, the source sends a signal or traffic through both paths, the primary path, and its protection, and the receiver selectively receives from one path with a better quality signal. But in 1:1 DPP, a source node sends a signal or traffic through the primary path only and the protection path can be used to carry low priority traffic as long as the primary path is free of failure. At times of failure, in 1:1 DPP, the protection path is used to carry traffic of the primary path by dropping the low priority traffic. 1:1 DPP requires signaling communication to switch between primary and protection paths but not in 1+1 DPP.

Considering the high traffic carrying capacity of optical network and fault types happen in the network, resilience degree of 1+1 dedicated path protection can be increased or improved by

configuring protection path which is disjoint to its primary path [39]. The protection path can be disjoint by node, link or SRG based on the resilience level required and failure type to be protected. Link-disjoint 1+1 dedicated protection is provided by configuring two link disjoint paths and is used to protect against link failure. Node-disjoint 1+1 DPP is used to protect against node failure in addition to link failure. On the other hand, SRG-disjoint 1+1 DPP is used to protect against SRG failure in addition to link failure. Even though DPP has fast fault recovery time and commonly used in practical networks, it increases the resource requirement of the network by two as compared to the unprotected case due to the parallel transmission of signals through the primary and protection paths.

Shared protection: - in this protection mechanism, the priory planned, computed and reserved protection mechanism is shared among different working or primary paths or links and assigned to specific links or paths at the time of failure [1], [39], [40]. Based on the sharing configuration of the paths, more than one primary path can share one or more than one protection path. In 1: N shared path protection, N working paths share one preplanned, precomputed and pre-reserved protection path. In this case, the N paths should be disjoint or need to be a path with no or minimum possibility of common failure. In M: N (M< N) shared path protection which is a general case of 1: N protection, N primary paths share M protection paths. To configure shared path protection, the primary paths should be disjoint or have no or minimum possibility of common failure among them. Comparing to dedicated path protection, shared path protection has better resource utilization with high signaling overhead and slow fault recovery time.

3.2.2. Restoration

Restoration is a resilience mechanism that provides the resilience of a network by dynamically computing and establishing a restoration path at the time of failure in the primary path [1]. To obtain a new end-to-end restoration path that bypasses the failure in the primary path and obtain network topology updates and resource levels, restoration requires control plane routing and signaling capabilities of an ASON network. In this resilience mechanism, there is no signaling and resource reservation before failure occurrence. In this resilience mechanism, failures are served or restored in a first-come-first-serve manner by using available resources reserved in a pool. So, service recovery is not always guaranteed in this mechanism. The blocking probability of a recovery request is dependent on the size of the resource available in the

resource pool. As the resource pool increases, blocking probability of recovery requests decreases. In addition to this, the recovery time of the restoration mechanism is dependent on the network size of the network. The restoration mechanism has better resource utilization efficiency than protection. But the recovery time of the restoration mechanism is slow as compared to protection.

3.2.3. Hybrid resilience mechanism

In addition to the above two basic types of resilience mechanisms, protection, and restoration, different resilience mechanisms that protect a network against double link failure were proposed by different authors to improve the resilience of a network [41]. The proposed resilience mechanisms were developed based on the two basic resilience mechanisms. One type of resilience mechanism developed to provide the resilience of a network against double link failure is the hybrid resilience mechanism. The hybrid resilience mechanism provides the resilience of a network against double link failure by coordinating the two basic types of resilience mechanisms and was developed with the object of using the advantages of the two resilience mechanisms. The hybrid resilience mechanism uses the two resilience mechanisms in sequence. The common sequence of using the two basic resilience mechanisms is using protection to protect the first failure and restoration to protect the second failure. Due to the computational and operational complexity of shared path protection, a commonly used protection mechanism in a hybrid resilience mechanism is dedicated path protection with different configurations. Some of the configurations of DPP used in the hybrid resilience mechanism are node-disjoint, link-disjoint or SRG-disjoint DPP based on the failure type that needs to be protected.

3.5. Literature Review

Previously different research works that evaluate the performance of different resilience mechanisms and RWA algorithms were conducted. But the previously conducted research works except for research work [26] evaluated the two optical parameters, resilience mechanism and RWA algorithm, separately, to the best knowledge of the author.

Research work [26] evaluated dynamic routing algorithms (Alternate, LCR, SRG-disjoint aware FF, and Load sharing routing) with first-fit wavelength assignment algorithm under 1+1 DPP and restoration resilience mechanisms. The author used QoS performance metrics

blocking probability and availability to evaluate the RWA algorithms. In addition to this, the author proposed and compared hybrid resilience mechanism (DPP + restoration) which is used to protect a network against double link failure (DLF) with the above-mentioned resilience mechanisms, 1+1 DPP and Restoration, under alternate routing with metrics blocking availability, recoverability and network availability. The author considered Ethio-telecom Addis Ababa ASON backbone network topology with 9 nodes and 54 links with uniform traffic demand in the evaluation of RWA and resilience mechanisms. The author used the Net2Plan simulator for evaluation by first formulating the parameters mathematically. The author does not consider the effect of network topology connectivity degree and non-uniformity of traffic demand which is the practical traffic demand scenario of telecom operators including Ethio-telecom on the performance evaluation of the parameters.

Research work [41] proposed and evaluated four resilience mechanisms that can be used to protect a network against DLF. The four resilience mechanisms evaluated by the authors are DPP + Restoration, DPP + Rerouting, DPP + Provisioning + Restoration and DPP (1: 2). The authors evaluated the resilience mechanisms using Java-based discrete event-driven simulator of RedHat Enterprise Linux (RHEL) work station with dual Intel Xeon CPU (4 core per CPU) clocked at 12GHz and 12GB RAM memory. The authors considered cost239 network topology (11 nodes and 50 unidirectional links) for their evaluation.

The authors of the research work [41] considered blocking probability, connection unavailability (ratio of uptime to total time), number of dropped connection, DLF restorability, wavelength resource usage, and connection downtime to evaluate the resilience mechanisms. The authors of the research work did not mention the RWA algorithm and traffic demand-type considered in the evaluation of the resilience mechanisms. In addition to this, the authors evaluated the resilience mechanisms in relatively small network topology with a relatively higher connectivity degree.

Research work [42] developed and compared the Intelligence Water Drop (IWD) based adaptive RWA algorithm that considers load and length status of a network with fixed and adaptive SPR (Shortest Path Routing). The authors of the research work used blocking probability to compare and evaluate the RWA algorithm in java environment simulation. The authors considered two different network topologies, 14 nodes with 21 bidirectional links and 13 nodes with 23 bidirectional links. The authors did not consider the resilience mechanism in

their evaluation. In addition to this, the authors did not mention the nature of the traffic demand considered in the evaluation.

Research work [43] proposed and evaluated an RWA algorithm that can be used in an optical passive star network with non-uniform traffic. The authors used Time and Wavelength Division Multiplexing (TWDM) which is a combination of the TDM and WDM approach to solving the RWA algorithm problem. The authors considered the optical passive star network topology to evaluate the wavelength usage effectiveness of the TWDM based RWA algorithm.

In addition to the above-mentioned research works, there are different works that evaluate resilience mechanisms and RWA algorithms separately. To mention some, research works [36], [37], [44], [45] proposed and evaluated different resilience mechanisms such as Shared Path Protection (SPP) and Segment Path Protection and research works [25], [46]–[49] studied different RWA algorithms using different evaluation methodologies in different network topology environments. On the other hand, research work [50] studied the effect of traffic demand non-uniformity in the Optical Packet Switched (OPS) network. From the above research works, it is possible to see the gap of a research work that evaluate resilience mechanism and RWA algorithms jointly considering the practical non-uniform traffic demand scenario.

Chapter 4

Performance Evaluation of RWA Algorithms and Resilience Mechanisms

ASON network mainly used to carry aggregate traffic of different service types such as voice, data, and video offered by a service provider to its customers. Due to the aggregate nature of the traffic carried by the network, any failure of a network element or a fiber in the network affects a large amount of traffic generated from different customers. In order to protect such cases, service providers use different resilience mechanisms that protect the network from failure. In addition to this, service providers use different RWA algorithms in order to select an optimum transportation path or route for the requested traffics automatically based on their path selection criteria. But, as previously discussed in Chapter 3, different resilience mechanisms and RWA algorithms have different properties with different performance and affect traffic QoS differently. Considering this and the service provider's requirement diversity, different researchers evaluated the performance of resilience mechanisms and RWA algorithms considering different performance metrics using different evaluation approaches.

This chapter discusses in detail the mathematical formulation of RWA algorithms and resilience mechanisms going to be evaluated in this thesis and its problem-solving approach. In addition to this, this chapter gives a detail discussion on performance parameters used to evaluate the RWA and resilience mechanisms in this thesis.

4.1. Problem Formulation

This section discusses the problem formulation of the optical parameters, RWA algorithms and resilience mechanisms, that are evaluated in this thesis. As per the discussion and justification that is given in [31], [51], optical network problems, similar to other communication problems, can be formulated mathematically as multi-commodity flow (MCF) type of integer linear programming (ILP) optimization problem with different constraints related to the optical network problem. Based on this discussion and review of previous works done on the area of consideration, the optical parameters evaluated in this thesis are formulated mathematically as MCF type of ILP optimization problem with objective function and constraints specific to the RWA algorithms and resilience mechanisms under consideration. In this thesis, after

formulating the optical parameters mathematically, the mathematical optimization problem is solved indirectly using Net2Plan simulator to evaluate the performance of the parameters. ILP is an all integer linear programming optimization problem. In the next sub-sections, ILP formulation of the optical parameters is given after highlight discussion on LP, its classification and possible solving methods used to solve the LP optimization problem.

4.1.1. Linear Programming (LP)

Linear programming is a method used to find the optimal solution of mathematical optimization problems with linear objective function by taking linear constraints with equalities and inequalities [52], [53], [54]. The objective function of an LP function can be a maximization or minimization of a linear problem with linear constraints that can be drawn as a linear graph. The general algebraic expression of the LP problem is written as follows:

Objective function: maximize $Z=\sum_i c_i x_i$

Constraint Subject to: $\sum_i a_{ij} xi \leq b_j$ (j=1,2,…,n)

Bound: $x_i \geq 0$ (i=1, 2, …, m)

Where x_i is a decision variable and a_{ij}, b_j and c_i are optimization model parameters. The following figure, Figure 4.1, shows a graph of a linear optimization problem with two decision variables and two constraints.

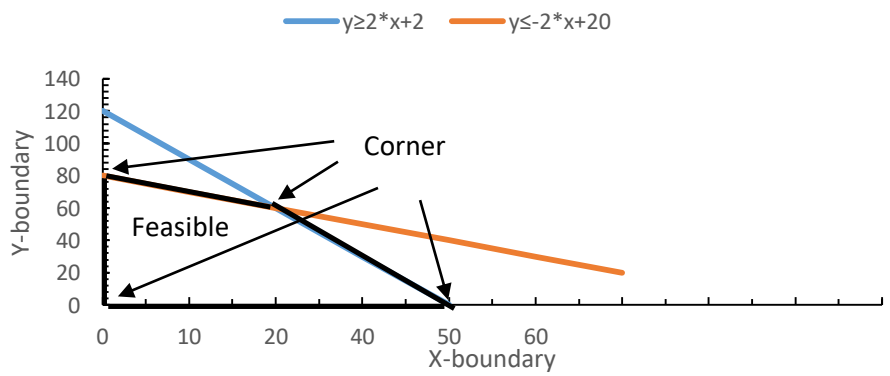

Figure 4.1. Graph of LP problem with decision variables [51]

The feasible region is a region created by the intersection of the constraints and boundary conditions and is a region with possible solutions for the objective function fulfilling the required constraint conditions [51], [54]. The corner points are intersection points of the constraint and boundary conditions. The optimum solution of a linear optimization problem commonly found in one of the corner points, if the linear optimization problem has an optimum solution.

For a linear optimization problem with a small number of decision variables and constraints, it is possible to find an optimum solution by drawing a graph and examining all corner points. But as the number of decision variables and constraints increases, drawing a graph and examining all corner points becomes complex or even impossible. So to solve this type of problem different algorithms or methods were developed. One of the methods is the simplex method. The simplex method is one of the methods used to solve linear programming problems with a large number of decision variables and constrains based on the above assumption of finding the optimum solution in corner points of a feasible region [51], [54]. But this method does not examine all the corner points. In a simplex method, one corner point is selected as a starting point then neighbor points of the corner point along a direction that does not decrease the objective function value (optimum solution found in the corner point), for maximization problem, are examined and vice versa. The corner point is selected as an optimum solution if there is no point along the path that improves the optimum value.

If all decision variables of an LP optimization problem are restricted to an integer value, the LP problem becomes ILP (Integer Linear Programming). On the other hand, if some of the decision variables of an LP optimization problem are allowed to take non-integer value, the ILP becomes MILP (Mixed ILP) [51], [54]. Solving ILP is more complex than that of LP and cannot be solved by evaluating corner points of its graphical expression and simplex method. In general classification of problem complexity, ILP (MILP) is classified as an NP-hard problem. Even if they are complex, to solve practical economic, control and network optimization problems ILP problems are useful. Some of the optimization problems that can be solved using ILP (MILP) is the optimization of RWA algorithms and resilience mechanisms.

The above-mentioned optimization problems are modeled as **single commodity flow problems** with a single type of commodity that flows from one destination to the other [55], [56], [54]. But most practical optimization problems such as transportation and

telecommunication problem contain multiple types of a commodity with a different property that share the same resource. The optimization problem models that deals with such type of property are called the **multi-commodity flow problem**. In the multi-commodity flow problem, a node is used to represent the source and destination of a flow of traffic or commodity and arcs are used to represent transmission links with a specific capacity [54]–[56]. The multi-commodity flow problem mainly addresses the allocation of specific link capacity to multiple commodities flow through it efficiently.

4.1.2. ILP formulation of RWA algorithms and Resilience mechanism

This section will discuss the ILP formulation of RWA algorithms and resilience mechanisms that are going to be evaluated. Similar to other telecommunication optimization problems, ASON optical network optimization problem also considers different types of commodities or constraints with different properties. Due to this, all the RWA algorithms and resilience mechanisms of this thesis are formulated as multi-commodity flow (MCF) with different types of commodities or constraints such as channel capacity, link capacity, traffic demand/request and other constraints that are going to be discussed in detail in the next subsections. The mathematical problem of the RWA and resilience mechanisms is formulated considering a network topology G (V, E) with |V | a number of nodes and |E| a number of links. Input variables and decision variables used in the ILP formulation of the RWA algorithms and resilience mechanisms are given in Table 4.1 and Table 4.2 respectively.

Table 4-1. input Variables of ILP formulation

Notation	Description
G (V, E)	Network topology with a set of V nodes and E links as a directed graph
W	Number of free wavelengths available in a link $(i, j) \in$ E
D	Set of connection requests or demand fed to the ILP
$R_{s,d}$	Traffic demand matrix (number of connection requests from source to destination), $R_{s,d} \in$ D

r	A request r from source s to destination d
h_r	A total volume of the demand matrix
S_w	Maximum capacity per wavelength which is 40Gbps

Table 4-2. Decision variables of ILP problem

Notation	Description
f_{ij}	Number of wavelengths needed to set up a set of light-paths
p_{ij}	Number of wavelengths used by primary paths on a link (i,j)
b_{mn}	Number of wavelengths used by backup paths on a link (m,n)
p_{ij}^r	Equal to 1 if the primary path of a request c from s to d passes through a link (i,j)
b_{mn}^r	Equal to 1 if backup path a of request c from s to d passes through a link (m,n)
f_{ij}^r	Equal to 1 if a request r from s to d passes through the link (i,j)
A_r	Equal to 1 if a request r is successfully provisioned
$S(i,j,g)$	SRG group g where link (i, j) belongs to
λ_r^p	Equal to 1 if light-paths from source s to destination d allocated on wavelength w
f_{ijs}^r	Equal to 1 if a request r from s to d passes through the link $(i,j)$of SRG $S(i,j,g)$

4.1.2.1. ILP formulation of RWA algorithms

ILP formulation of the RWA algorithms considered in this thesis is formulated based on the generic ILP formulation given in different kinds of literature [26], [52], [53], and [31] by adding some additional constraints to make the ILP formulation more practical. The additional constraint is added by considering the route selection property of the RWA algorithms in addition to the ILP formulation given in Net2Plan simulator tool reference documentation. Input variables and decision variables in Table 4.1 and Table 4.2 above are used in formulating the ILP formulation of the RWA algorithms as shown below.

Objective:

$$\boldsymbol{min} \quad (|D| - \sum_{\forall c} A_r) + \sum_{ij\epsilon E} f_{ij} \tag{4.1}$$

Subjected to:

$$\sum_{i:(i,j)\epsilon E} f_{ij}^r - \sum_{k:(j,k)\epsilon E} f_{ji}^r = \begin{cases} -\lambda_r^p, & if\ j = s \\ \lambda_r^p, & if\ j = d \\ 0, & if\ j(! = s,d) \end{cases} \qquad 1 \le s,d,j \le V \tag{4.2}$$

$$\sum_{w=1}^{W} \lambda_r^p = R_{s,d} \qquad 1 \le (s,d) \le V \tag{4.2}$$

$$f_{ij} = \sum_{1\le(s,d)\le V} \sum_{w=1}^{W} f_{ij}^r \qquad \forall (i,j)\epsilon E \tag{4.3}$$

$$f_{ij} \le W \qquad 1 \le (i,j) \le E \tag{4.4}$$

$$\sum_r h_r * f_{ij}^r \le w*S \tag{4.5}$$

$$|E| * S(i,j,g) \ge \sum_{ij\epsilon E} f_{ij} \tag{4.6}$$

$$f_{ij}^r = \begin{cases} 1, & if\ traffic\ r\ from\ s\ to\ d\ pass\ through\ link\ (i,j) \\ 0, & otherwise \end{cases} \tag{4.7}$$

$$\lambda_c^p = \begin{cases} 1, & if\ traffic\ r\ from\ s\ to\ d\ allocated\ wavelength\ w \\ 0, & otherwise \end{cases} \tag{48}$$

The objective function for the ILP formulation given in Equation.4.1 above has two parts. The first part of the objective function is used to minimize the number of blocked connection requests (blocking probability) by calculating the difference between the total number of connection demands or requests |D| and the total number of successfully provisioned

connection requests $\sum_{\forall c} A_r$. The second part of the objective function is used to minimize the total number of wavelengths used to provision arrived connection requests. Equation 4.2 to Equation 4.9 are constraints of the objective function.

Equation 4.2 of the above ILP formulation is flow conservation constraint of the connection requests by maintaining traffic flow conditions at source, destination and intermediate nodes of the network. At the source node, flow conservation constraint maintains the condition of the traffic flow by ensuring the difference between incoming and outgoing traffic to be $-\lambda_r^p$. This condition ensures that, at the source node, there is no incoming traffic. At the destination node, the flow conservation constraint ensures the existence of only incoming traffic by maintaining the difference of incoming and outgoing traffic to be λ_r^p. At intermediate nodes, the difference between incoming and outgoing traffic maintained by flow conservation constraint at 0 to ensure all the incoming traffics is going out of the nodes.

Equation 4.3 is a constraint used to ensure a total number of successfully provisioned and wavelength allocated light-paths to be equal to the number of source-destination pair traffic demands. Equation 4.4 of the above formulation calculates a total number of light-paths traverse links (i, j) for all the provisioned source-destination pair connection requests and is maintained to be within the number of wavelengths supported by the link by Equation 4.5. Equation 4.6 is a wavelength continuity constraint and is used to ensure the non-existence of wavelength conversion or use of the same wavelength for one connection request from source to a destination node. Equation 4.7 ensures SRG-disjoint link selection in provisioning connection requests in the SRG-disjoint aware routing algorithm. Equation 4.8 and equation 4.9 are binary constraints.

4.1.2.2. ILP formulation of resilience mechanisms

ILP formulation of the resilience mechanisms considered in this thesis is formulated based on ILP formulations given in different kinds of literature [26], [31], [41], [51]. Input variables and decision variables in Table 4.1 and Table 4.2 above are used in formulating the ILP formulation of the resilience mechanisms.

ILP formulation of Restoration

ILP formulation restoration type of resilience mechanism is the same as the ILP formulation of generic RWA algorithms. As discussed above, the ILP formulation is formulated using input and decision variables in Table 4.1 and Table 4.2 above and is given below.

Objective:

$$\boldsymbol{min} \quad (|D| - \sum_{\forall c} A_c) + \sum_{ij \epsilon E} p_{ij} \tag{4.9}$$

Subjected to:

$$\sum_{i:(i,j)\epsilon E} p_{ij}^r - \sum_{k:(j,k)\epsilon E} p_{ji}^r = \begin{cases} -\lambda_r^p, & if\ j = s \\ \lambda_r^p, & if\ j = d \\ 0, & if\ j(! = s, d) \end{cases} \quad 1 \le s, d, j \le V \tag{4.10}$$

$$\sum_{w=1}^{W} \lambda_r^p = R_{s,d} \qquad 1 \le (s,d) \le V \tag{4.11}$$

$$p_{ij} = \sum_{1 \le (s,d) \le V} \sum_{w=1}^{W} p_{ij}^r \qquad \forall (i,j) \epsilon E \tag{4.12}$$

$$p_{ij} \le W \qquad 1 \le (i,j) \le E \tag{4.13}$$

$$\sum_r h_r * f_{ij}^r \le w*S \tag{4.14}$$

$$p_{ij}^r = \begin{cases} 1, & if\ traffic\ r\ from\ s\ to\ d\ pass\ through\ link\ (i,j) \\ 0, & otherwise \end{cases} \tag{4.15}$$

$$\lambda_c^p = \begin{cases} 1, & if\ traffic\ r\ from\ s\ to\ d\ allocated\ wavelength\ w \\ 0, & otherwise \end{cases} \tag{4.16}$$

The objective function for the ILP formulation given in Equation 4.10 tries to minimize the number of blocked connection requests (Blocking probability) and the total number of wavelengths used to provision arrived connection requests. Equation 4.11 to Equation 4.17 are constraints of the objective function.

Equation 4.11 of the above ILP formulation is flow conservation constraint of the connection requests by maintaining traffic flow conditions at source, destination and intermediate nodes of the network. Equation 4.12 is a constraint used to ensure a total number of successfully provisioned or restored and wavelength allocated light-paths to be equal to the number of source-destination pair traffic demands. Equation 4.13 of the above formulation calculated a

total number of light-paths traverse links (i, j) for all the provisioned or restored source-destination pair connection requests and is maintained to be within the number of wavelengths supported by the link by Equation 4.14. Equation 4.15 is a wavelength continuity constraint. Equation 4.16 and equation 4.17 are binary constraints.

ILP formulation of Link-disjoint 1+1 DPP

ILP formulation of 1+1 link-disjoint DPP is formulated using input and decision variables given in Table 4.1 and Table 4.2 above based on ILP formulations given in the literature [26], [31], [41], [51]. In addition to this, due to the requirement of traffic flow in both the primary and backup paths in 1+1 DPP, the ILP is formulated considering the traffic demand as double of the original traffic demand requested. The ILP formulation is formulated as shown below.

Objective function:

$$\boldsymbol{min} \quad (|D| - \sum_{\forall c} A_r) + \sum_{ij\epsilon E} p_{ij} + \sum_{mn\epsilon E} b_{mn} \qquad (4.17)$$

Subjected to:

$$\sum_{i:(i,j)\epsilon E} p_{ij}^r - \sum_{k:(j,k)\epsilon E} p_{ji}^r = \begin{cases} -\lambda_r^p, & if\ j = s \\ \lambda_r^p, & if\ j = d \\ 0, & if\ j(! = s, d) \end{cases} \quad 1 \le s, d, j \le V \qquad (4.18)$$

$$\sum_{m:(m,n)\epsilon E} b_{mn}^r - \sum_{k:(n,k)\epsilon E} b_{nm}^r = \begin{cases} -\lambda_r^p, & if\ n = s \\ \lambda_r^p, & if\ j = d \\ 0, & if\ n(! = s, d) \end{cases} \quad 1 \le s, d, n \le V \qquad (4.19)$$

$$\sum_{w=1}^{W} \lambda_r^p = 2 * R_{s,d} \qquad 1 \le (s, d) \le V \qquad (4.20)$$

$$p_{ij} = \sum_{1\le(s,d)\le V} \sum_{w=1}^{W} p_{ij}^r \qquad ; \forall (i,j)\epsilon E \qquad (4.21)$$

$$b_{mn} = \sum_{1\le(s,d)\le V} \sum_{w=1}^{W} b_{mn}^r \qquad ; \forall (m,n)\epsilon E \qquad (4.22)$$

$$p_{ij} + b_{mn} \le W \quad 1 \le (i,j) \le E, 1 \le (m,n) \le E \qquad (4.23)$$

$$\sum_{1\le(s,d)\le V} p_{ij}^r + \sum_{1\le(s,d)\le V} b_{mn}^r \le 1 \quad \forall (i,j),(m,n) \in E\ ; 1 \le w \le W \qquad (4.24)$$

$$p_{ij}^r = \begin{cases} 1, & if\ traffic\ r\ from\ s\ to\ d\ pass\ through\ link\ (i,j) \\ 0, & otherwise \end{cases} \qquad (4.25)$$

$$b_{ij}^{r} = \begin{cases} 1, & if\ traffic\ r\ from\ s\ to\ d\ pass\ through\ link\ (i,j) \\ 0, & otherwise \end{cases} \quad (4.26)$$

$$\lambda_{c}^{p} = \begin{cases} 1, & if\ traffic\ r\ from\ s\ to\ d\ allocated\ wavelength\ w \\ 0, & otherwise \end{cases} \quad (4.27)$$

Objective function 1+1 DPP given in Equation 4.18 has three parts. The first part of the objective function tries to minimize blocked connection requests (blocking probability). The second and third parts of the objective function try to minimize the number of wavelengths used to setup connection requests on primary and secondary (backup) paths respectively. Equations 4.19 to Equation 4.28 are constraints imposed on the objective function.

Equation 4.19 and Equation 4.20 are flow conservation constraints that are used to maintain traffic flow at source, destination and intermediate nodes of primary and secondary paths respectively. Equation 4.21 is a constraint used to ensure the total number of successfully provisioned and wavelength allocated light-paths to be equal to the number of source-destination pair traffic demands which is $2 * R_{s,d}$. Equation 4.22 and Equation 4.23 of the above formulation calculate a total number of light-paths traverse a link (i, j) and link (m, n) for all the provisioned source-destination pair connection requests on primary and backup paths respectively. Equation 4.24 imposes a restriction on a number of wavelengths used on a link to provision a connection request of the primary and secondary path and controls the number to be within the total supported number of wavelengths. Equation 4.25 is a constraint that ensures wavelength continuity and links disjointness usage to provide a connection request on primary and backup paths. Equations 4.26 to Equation 4.28 are binary constraints that express a range of values allowed for the variable.

ILP formulation of Hybrid Resilience Mechanism

As previously discussed in chapter two, the hybrid resilience mechanism is a combination of two different resilience mechanisms. The hybrid resilience mechanism considered in this thesis is 1+1 DPP +Restoration which is a combination of 1+1 link disjoint DPP and restoration resilience mechanisms combined with the aim of protecting a network against double simultaneous link failures. In this hybrid resilience mechanism, 1+1 DPP used to protect against the first failure and the restoration to protect against the second failure. For the hybrid resilience mechanism, the ILP formulations of 1+1 DPP and resilience discussed above are used in sequence.

4.2. Performance evaluation methodology

As previously discussed in Chapter 3, different optical network parameters, RWA algorithms and resilience mechanisms affect the performance of services offered by the network differently. In order to use optical network parameters, such as resilience mechanisms and RWA algorithms, that better suit the topology and requirements of service customers of the network, performance evaluation of these parameters are required. In evaluating these parameters, studying the qualitative behavior of the parameters and their quantitative performance evaluation is required. To evaluate the performance of these parameters, different evaluation approaches can be followed. Some of the approaches or techniques used to evaluate the performance of optical parameters are experimental, emulation-technique, analytical and simulation techniques.

An experimental approach is used to measure the performance of the parameters by building test-bed that include real physical network parameters [26], [57], [58]. Using this approach, it is possible to find accurate performance results of the parameters but it is very expressive to conduct such measurements on large and complex networks. Another type of performance approach is the emulation technique. Emulation technique is a performance evaluation approach that is used to evaluate performance optical network parameters by emulating or replicating the real network functionalities by combining software and hardware. Comparing with the experimental approach, this type of performance evaluation approach is cost-effective but it requires longer execution time and is complex to implement for large and complex networks. In addition to this, this approach yields less accurate results as compared to the experimental approach.

The other performance evaluation approach is analytical modeling [26], [57], [58]. This approach is performed by mathematically, such as ILP, modeling the network parameters and solve the mathematical model using mathematical solvers, such as CPLEX. As previously discussed, ILP optimization formulations of most optical network parameters are NP-complete and are time-consuming or impossible to solve these mathematical formulations for large optical networks. Due to this, this approach can only be used to evaluate the performance of a simple optical network.

The simulation-based performance evaluation approach is another approach that can be used to evaluate performance optical network parameters [26], [57], [58], [59]. Compared to the

previously mentioned performance evaluation approaches, this approach is more suitable for large and complex optical network and resolve the cost, complexity and execution time limitations of the previously mentioned approaches. In addition to this, a simulation-based approach helps to measure performance events that are difficult to measure in other performance approaches. In simulation based performance evaluation approach, it is possible to reproduce performance evaluation results previously generated with low cost and less time configuration of network parameters. Due to the easy of configurability, scalability, cost effectiveness and fast execution time of simulation based approach, it is more preferable for performance evaluation of large and complex optical networks.

Discrete Event Simulation (DES) is the most commonly used simulation-based approach that is used to evaluate performance evaluation optical networks [26], [58], [60]. In DES, network state such as link failure and link recovery change occurs only at discrete time events. There are different types of DES simulation tools that can be used to evaluate the performance of optical network parameters. One of the simulation tools is the Net2Plan simulator which is a Java-based open-source simulation tool.

In this thesis, the **Net2Plan simulator** is used to evaluate the QoS performance of RWA and Resilience mechanisms. This tool is selected due to its ease of operation, traffic demand and optical network parameters configuration in addition to the simplicity of adding additional algorithms using java programming.

4.2.1. Net2Plan simulator

Simulators can be classified into three broad categories based on their accessibility and development objective [26], [60]–[62], [59]. The first category of simulators includes simulators developed by researchers for their self-use and is not able to find their source code documented. In addition to the time-consuming development, the result found by such type of simulators is difficult to investigate or validate by ISPs or network carriers. The second category of simulators include simulators that are developed for commercial use. In such types of simulators, it is difficult to add new algorithms and is developed for mature technologies and algorithms with wide commercial acceptance. An example of such simulators that can be used for optical-based networks is the OPNET simulator. The third and commonly used category of simulators is an open-source simulator which is developed with the objective of fulfilling the requirements academia and industry. It is possible to find a fully documented

source-code of such simulators and is also possible to customize existing algorithms or add new additional algorithms. Net2Plan simulator is one example of open-source simulators which was originally developed as a tool for telecommunication engineering of Technical University of Cartagena (Spain) teaching material by Pablo Pavon and Jose Luis Izquierdo Zaragoza in 2011. Net2Plan is a java-based simulator which can be used for optimization and planning purposes of all network type such as IP, wireless or optical networks.

4.2.1.1. Net2Plan network model

In Net2Plan, Network plan is used to store network design represented by network elements such as nodes, links, traffic demands, SRG, and network layers without depending on specific technology [26], [60]–[62]. Kernel assigns specific information such as Id, Index and working status for each Network element of the network plan. The id is a unique identifier used to identify network elements globally and is unchanged throughout the life of the network plan. Unlike Id, Index only exists as long as network element with that index existed and is numbered in consecutive order. Nodes, which are endpoints of a link, are used to forward traffic targeted to another node in addition to their main use of acting as source and destination of the traffic. Links used to represent elements that connect node of a network plan and are identified by their capacity, link distance, propagation speed, source node, destination node in addition to identifiers that are common to all network elements. In Net2Plan, links with the same source and destination node are not allowed. In Net2Plan, Traffic is modeled as a set of demands represented as unidirectional offered traffic of specific source-destination pair of a network plan. Traffic demand in Net2Plan is identified by source (Ingress) node and destination (Egress) node in addition to ID and Index. In Net2Plan, there are two types of traffic demands, unicast and Multicast traffic demands. Unicast traffic demand represents traffic demand with one source and one destination node. On the other hand, multicast traffic demand has multiple destination nodes.

Net2Plan supports two types of routing, source routing, and hop-by-hoy routing, that represent how the traffic demand of a network plan carried by links [26], [60]–[62]. In source routing, the routing algorithm assigns a sequence of routes from source to a destination node, amount of traffic demand and link capacity consumed prior to data transfer and is suitable to connection-oriented networks such as an optical network. On the other hand, in hop-by-hop routing, each node of a network plan forwards traffic by defines a forwarding rule characterized

by demand, link and a number between 0 and 1 that represents a fraction of the original demand forward through next link. This type of routing is suitable for connectionless networks such as IP networks. Another network element used in a network plan representation of Net2Plan is SRG and is used to represent a set of links or nodes with a common or simultaneous risk of failure. In Net2Plan, SRGs are identified by their MTTR (Mean-Time-To-Repair: the average time required to repair a failure) and MTTF (Mean-Time-To-Fail: average time between consecutive failures) in addition to Id, Index and associated set of links or nodes.

4.2.1.2. Net2Plan Tools

Net2Plan supports two types of user interface mechanisms, GUI (Graphical User Interface) and CLI (Command Line Interface) [26], [60]–[62]. Users can add new network topologies and algorithms in addition to using the existing ones using one of the two user interface mechanisms. In addition to this, Net2Plan provides a tool called kernel that receives a network design composed of network topology, demand, and algorithm to produce an updated version of the network design. Net2Plan provides four different tools, offline network design, online simulation, Automatic report generation, and Traffic matrix generation, that can be used for different purposes. Figure 4.1 Below shows Net2Plan architecture.

Offline Network Design: - this network design tool receives network design as input and returns a modified version of the input topology, capacity or optimizes its routing by executing offline planning algorithms. This tool is mainly used for offline network planning and design purposes. The algorithms used in this tool are constrained based algorithms like ILP and use open-source Java Optimization Modeler library (JOM) to interface with external servers like CPLEX and GLPK. In addition to this, this tool uses the IAlgorithm interface for offline algorithm implementation.

Online Network Design: - this tool is used to visualize the reaction of a network to events generated by built-in or user-defined event generation modules. For example, this simulator can be used to visualize network recovery mechanism reaction to failures by generating failure events. In this tool, two types of modules are used for online simulation of a network, event generator, and processor. The event generator module is used to generate events like failure/repair events, add/removal events and traffic variation events in a network. On the other hand, an event processor is used to process events generated by the event generator and produce a new network state that corresponds to network reaction to the specific event based on the used algorithm.

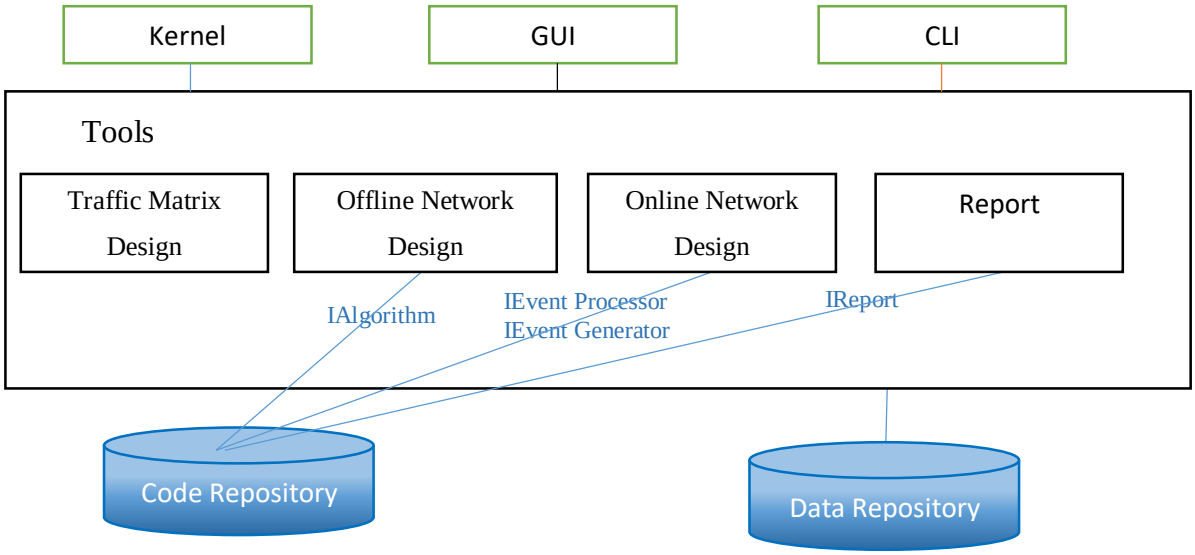

Figure 4.2. Net2Plan architecture [26], [60]–[62]

Traffic Matrix Generator: - this tool is used to generate and normalize traffic demand matrices based on the traffic generation model used such as a uniform traffic model and non-uniform traffic model. In a uniform traffic model, a traffic matrix generator generates a traffic matrix with uniform traffic volume in all source-destination pairs or similar matrix entry values. On the other hand, in a non-uniform traffic model, the traffic matrix generator generates a traffic matrix with non-uniform traffic volume among all source-destination pairs of the network. In Net2Plan, traffic demand is commonly represented as an N*N matrix where N is the number of nodes.

Report Generator: - this Net2Plan tool is used for the generation of network design user-defined or built-in reports.

4.3. QoS Performance parameters

The performance of optical networks can be measured using different parameters that are related to QoS and resource utilization. Quality of service (QoS) is defined differently by different authors based on their technology or service type consideration. QoS is defined by ITU-T as the collective effect of service performance which determines the degree of satisfaction of a user of the service [8]. In other words, QoS is defined by ITU-T as total service characteristics that depend on the ability of a network to deliver satisfying requirements of service users [7], [63]. QoS can be classified as perceived QoS and delivered QoS based on the respective area of consideration [7], [8], [63]. Perceived QoS is used to express the degree of satisfaction of a customer or service quality perceived by a customer and is measured by using qualitative and quantitative opinion ratings of the users. On the other hand, delivered QoS is used to express a level of service quality achieved by the service provider and is used to measure the performance of a network using different network performance metrics that express the ability of a network to serve a network user with required service quality.

Different QoS metrics are standardized and used to measure QoS of the services offered by the specific network based on the technology used and service type offered [6]–[8], [54], [63]. For example, in a mobile network, the most commonly used standard QoS metrics are receiving signal strength, receive signal quality and handover success rate. In an optical network, there are no standard QoS metrics used to measure QoS of the services transported by optical networks. But, due to the aggregate traffic flow in the optical network and its connection-oriented nature, the most commonly used QoS metrics are delay, blocking probability, recoverability, reliability, recovery time delay, and network throughput [64].

Reliability is a main QoS parameter or metric used to measure the performance of a network to provide a service without service outage even if failure happens in the network [65], [6]–[8], [54], [63]. On the other hand, reliability is used to measure the degree of resilience of a network to a failure. Recoverability is another QoS parameter used to measure the performance of a network and is used to determines the degree of failure recovery in a network. On the other hand, blocking probability is a QoS parameter used to determine the probability of connection request block due to resource unavailability. Network throughput is another QoS parameter used to measure the performance of a network by determining the allowed carried traffic volume out of the offered traffic volume.

In this thesis, performance parameters such as blocking probability, recoverability and network throughput are used to evaluate the QoS performance of RWA and resilience mechanisms using the Net2Plan simulator. The performance result of the evaluation is captured using the report generation feature of the Net2Plan simulator. A discussion about the performance parameters is given below.

4.3.1. Blocking probability

Blocking probability is a network performance parameter that expresses the probability of connection request blocking either due to resource unavailability or RWA algorithm failure in a network and is a common metric used to evaluate dynamic light-path establishment in a network [31], [51] and [66]. Blocking probability can be expressed as a ratio of blocked connection requests in a network and total arrived connection requests. As previously discussed in chapter two, in provisioning connection requests dynamically, connection requests can be blocked either by the non-existence of free available resource or unavailability of the same wavelength in all links along a path in a network with wavelength continuity constraint.

4.3.2. Recoverability

Recoverability is a network performance parameter that expresses or represents the degree of network survivability against a network failure [67]. Recoverability can be defined as the ratio connection requests that are successfully recovered by the deployed resilience mechanism to the total connection requests affected by the network failure. On the other hand, recoverability can be defined as a probability of successfully recovering a failed connection request in a network. Network recoverability is used to express the robustness or quality of a deployed resilience mechanism to a network failure.

4.3.3. Average Network Throughput

Network throughput is a network performance metric that expresses the amount of packet or data successfully transmitted in a network [66]. In addition to this, network throughput is used to express the amount of data rate carried between source-destination pairs in a network. Average network throughput expresses the average amount of data carried by a network and is average of the minimum and maximum data rates successfully transmitted between source-destination pairs of a network.

Chapter 5

QoS Performance Evaluation Results and Discussion

The previous chapter, Chapter 4, discusses the performance evaluation approach or methodology of this thesis and presents the mathematical formulation of the RWA algorithms and resilience mechanisms evaluated in this thesis and their solving approach. This chapter discusses the remaining steps of the performance evaluation of the thesis. The first section of this chapter discusses the simulation setup used to evaluate the performance of RWA algorithms and Resilience mechanisms and the assumptions taken. The second section of this chapter presents a brief discussion on the performance evaluation results of RWA algorithms under different resilience mechanisms. The third section of this chapter presents a brief discussion on the performance evaluation of Resilience mechanisms under different RWA algorithms with different failure modes. The last section of this chapter presents a brief discussion on the effect of network topology connectivity on the performance of resilience mechanisms.

5.1. Simulation setup and assumption

In performance evaluation of RWA algorithms and resilience mechanisms, Ethio-telecom North-circle backbone network topology shown in Figure 5.1 is considered as reference topology. This reference topology has 43 ASON enabled nodes with 138 unidirectional links. Each link in the reference topology supports 40 wavelengths and each wavelength supports up to 40Gbps. The summary of the reference network is given in Table 5-1. In the Net2Plan simulator, the reference topology is set up based on this information.

In Net2Plan, as previously discussed in Chapter 4, for topology with N number of nodes, it is possible to generate a uniform traffic demand with uniform N*(N-1) demands and a non-uniform traffic demand up to N*(N-1) non-uniform demands because of the impossibility of self-demand (demand with the same source and destination pair). In this thesis, traffic demand is used to represent a set of connection requests that arrive in a network. In this thesis, non-uniform traffic demand with only 112 number of demands is considered. This non-uniform traffic demand is selected considering the current Ethio-telecom north circle traffic demand matrix. This traffic demand is generated using the Net2Plan traffic generator based on the

offered traffic volume of the Ethio-telecom north circle traffic matrix. An example of the non-uniform traffic demand considered is given in Table 5-2. In addition to this, 69 SRGs are generated considering bidirectional link bundles as one SRG.

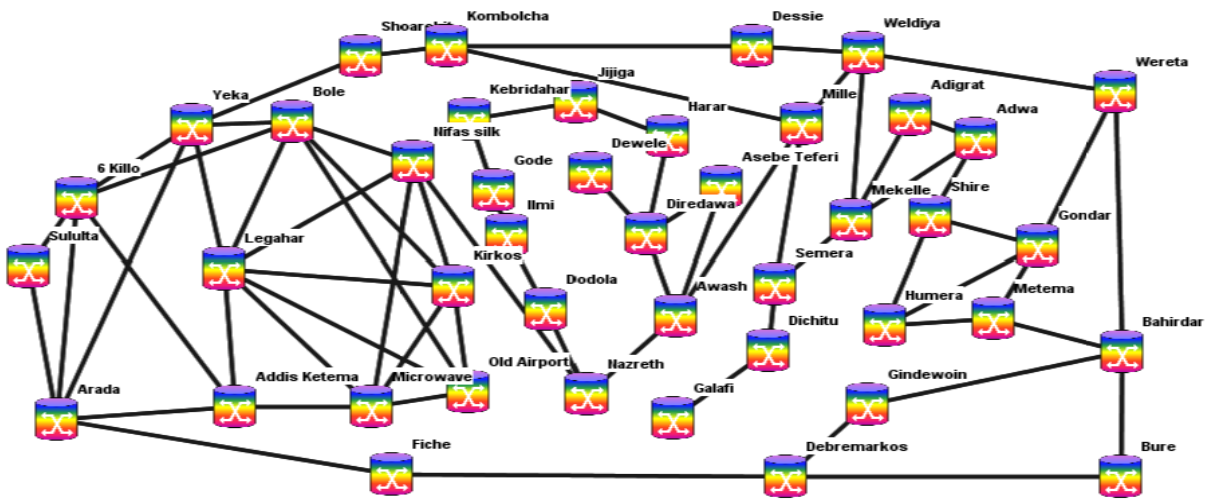

Figure 5.1. North-circle ethio-telecom ASON backbone reference topology

Table 5-1. Summary of reference network topology

Number of Nodes	43
Number of links	138
Node out-degree (max, min, avg)	7, 1, 3.209
Capacity units name	Frequency slots (wavelength)
Capacity installed: total	5520
Capacity installed: average per link	40
Number of demands (s,d node pairs)	112 (non-uniform)
Traffic units name	Gbps
Line Rates Per Light-path (Gbps)	40
Number of SRGs in the network	69
SRG definition characteristic	One SRG per bidirectional link bundle

Table 5-2. sample of Traffic demand matrix in the case 45800 Gbps offered traffic

	Mekelle	Adwa	Adigrat	Semera	Weldya	Shire	Humera	Gondar	Metema	Bahirdar
Mekelle	0	0	200	200	0	200	0	200	0	1000
Adwa	0	0	0	0	0	0	0	0	0	0
Adigrat	200	0	0	0	0	0	0	0	0	0
Semera	200	0	0	0	0	0	0	0	0	0
Weldya	0	0	0	0	0	0	0	0	0	0
Shire	200	0	0	0	0	0	0	0	0	0
Humera	0	0	0	0	0	0	0	0	0	0
Gondar	200	0	0	0	0	0	0	0	0	400
Metema	0	0	0	0	0	0	0	0	0	500
Wereta	0	0	0	0	0	0	0	0	0	0
Bahirdar	1000	0	0	0	0	0	0	400	500	0
Mile	0	0	0	0	0	0	0	0	0	0
Dessie	200	0	0	200	0	0	0	0	0	0
Kombolcha	0	0	0	0	0	0	0	0	0	0
Dichitu	0	0	0	0	0	0	0	0	0	0
Galafi	0	0	0	0	0	0	0	0	0	0
Awash	0	0	0	0	0	0	0	0	0	0
Nazreth	400	0	0	0	0	0	0	0	0	0
Asebeteferi	0	0	0	0	0	0	0	0	0	0

5.1.1. Simulation assumptions

In the evaluation of the RWA algorithms and resilience mechanisms, to analyze network response to event change such as light-path establishment and release at different loads, the event-driven simulation provided by the Net2Plan simulator is considered. In all the performance evaluation simulations, random arrival, departure and holding time of light-path request with exponential distribution (connection request with poison arrival and departure) are considered.

MTTR (Mean Time to Repair) of 6 hours and MTTF (Mean Time to Fair) of 700 hours (one failure in a month) are considered for all the simulations. Even though it is not an exact value, the above MTTF value is considered as the average number of failures per month and the number of links in Ethio-telecom north circle backbone network topology considered. Similarly, the average number of hours elapsed in maintaining a failure in the reference topology is taken as MTTR. These values are taken from failure notification text used by Ethio-telecom to notify failure happening in its network and its resolving time for respective departments and are considered to make the assumptions more practical and consider the frequent failure that happens in the north circle Ethio-telecom backbone network.

In addition to the above assumptions, in all the simulations, a maximum number of candidate paths per demand is considered to be 5 (default value) and the number of events per simulation is considered to be one million (1,000,000) without transitory events in between. Other than the above-mentioned parameters, the default value of all the remaining parameters is taken.

5.2. Result and discussion on QoS performance evaluation of RWA algorithms under different resilience mechanisms

Results of QoS performance evaluation of different RWA algorithms under different resilience mechanisms will be discussed in detail in this section. In this evaluation, four commonly used Dynamic (Adaptive) RWA algorithms, Alternate routing, LCR, Load Sharing, and SRG-disjoint aware FF, are evaluated under three resilience mechanisms, 1+1 DPP, Restoration, and Hybrid. The resilience mechanisms are selected by their wide practical usage and the possibility of their implementation on the current Ethio-telecom backbone network. currently, Ethio-telecom is using a 1+1 DPP resilience mechanism with alternate routing. But due to the optical power debugging problem that exists at the time of optical channel add and drop, the routing is not fully automated. In all the considered RWA algorithms, the first-fit wavelength assignment algorithm is used due to its less complex implementation and better blocking probability performance as previously discussed in Chapter 3. Blocking probability and average network throughput are used to compare the performance of the four RWA algorithms. Net2Plan simulation setup and simulation assumptions mentioned in the previous section of this chapter are used in all the simulations of RWA algorithm evaluation. In the RWA algorithm evaluation a failure scenario, link failure scenario, is considered which is common in the existing optical backbone network.

Blocking probability result and discussion

The graphs of blocking probability versus offered traffic shown in Figures 5.2, 5.3 and 5.4 are generated by running the simulation of the four RWA algorithms, Alternate routing, LCR, Load Sharing, and SRG-disjoint, under different resilience mechanisms with different offered traffic load or volume. In all the simulations, offered traffic load or volume from 1145Gbps to 45800Gbps are considered. In this case, Offered traffic load or volume is used to represent a total load or volume of the traffic demand matrix. The offered traffic load or volume is selected based on the existing traffic volume offered by Ethio-telecom north circle backbone network and its integral multiples. RWA algorithms compute more than one alternate paths for each

connection request arrived based on the criteria of the considered or used type of RWA algorithm and maximum allowed number of alternate paths. In this specific simulation case, allowed alternate paths are set to 5. After the computation of possible alternate paths by the RWA algorithm, resilience mechanisms select and use the required number of path/paths from the computed alternate paths based on the requirement of the considered resilience mechanism. In 1+1 DPP, out of the computed alternate paths two paths are selected for primary and backup paths. But in restoration case, out of the computed alternate paths, only one path is selected to provision arrived connection request or restore connection request affected by a failure. The following three figures, Figures 5.2, 5.3 & 5.4, are drawn offered traffic in Gbps versus Blocking probability in 1+1 DPP, Restoration, and Hybrid resilience mechanisms respectively with unidirectional link failure (link failure) scenario.

Blocking probability of all RWA algorithms increase with the increase in offered traffic, as shown in the following three graphs (Figures 5.2, 5.3 & 5.4) especially in the restoration resilience case. The reason for this increase in blocking probability is the increase in contention for the decreasing available resource that happen by the increase in offered traffic. In restoration, Figure 5.3 shown below, the Load sharing routing algorithm has higher blocking probability than the other three RWA algorithms and the blocking probability difference becomes more significant as offered load increases with the average increase value of 4% at 9160Gbps and 14% at 32060Gbps. This is due to the probabilistic path selection nature of load sharing routing algorithm. As previously discussed, load sharing immediately block a connection request if the randomly selected alternative path is unavailable without trying another path. In addition to this, due to the low connectivity degree of the reference topology and two path selection requirements, primary and secondary paths, of 1+1 DPP and hybrid resilience mechanisms, load sharing does not properly work in the two resilience mechanisms. The low connectivity nature of the network topology makes the probability of finding two paths, primary and backup paths, very low and forces load sharing routing algorithm to fail. Due to this, in the graphs of 1+1 DPP and hybrid resilience mechanism shown in Figures 5.2 & 5.4, only three RWA algorithms are shown.

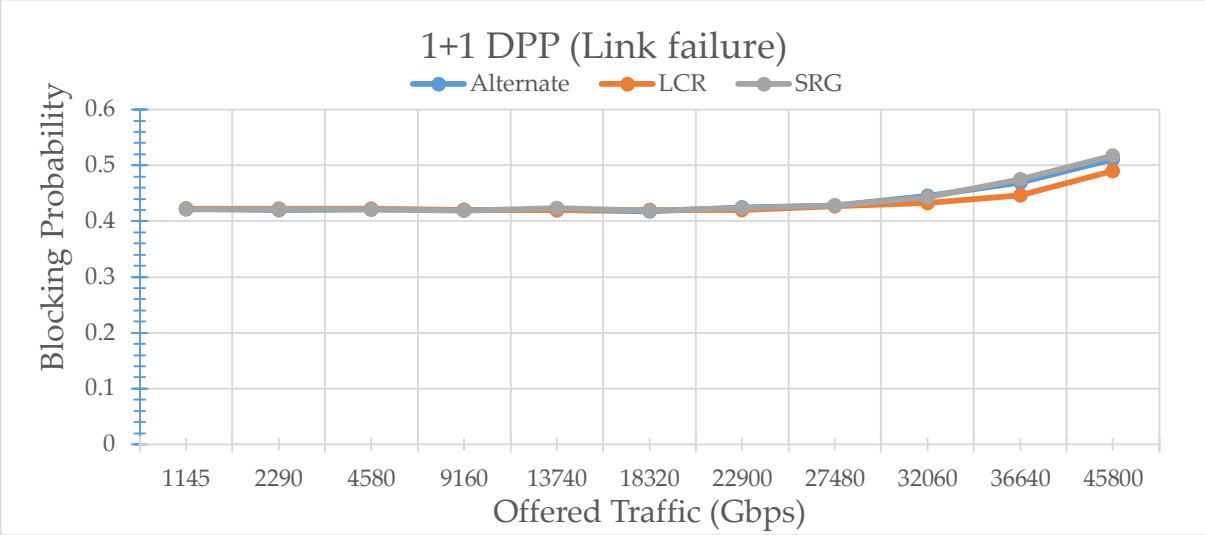

Figure 5.2. Blocking probability under 1+1 DPP

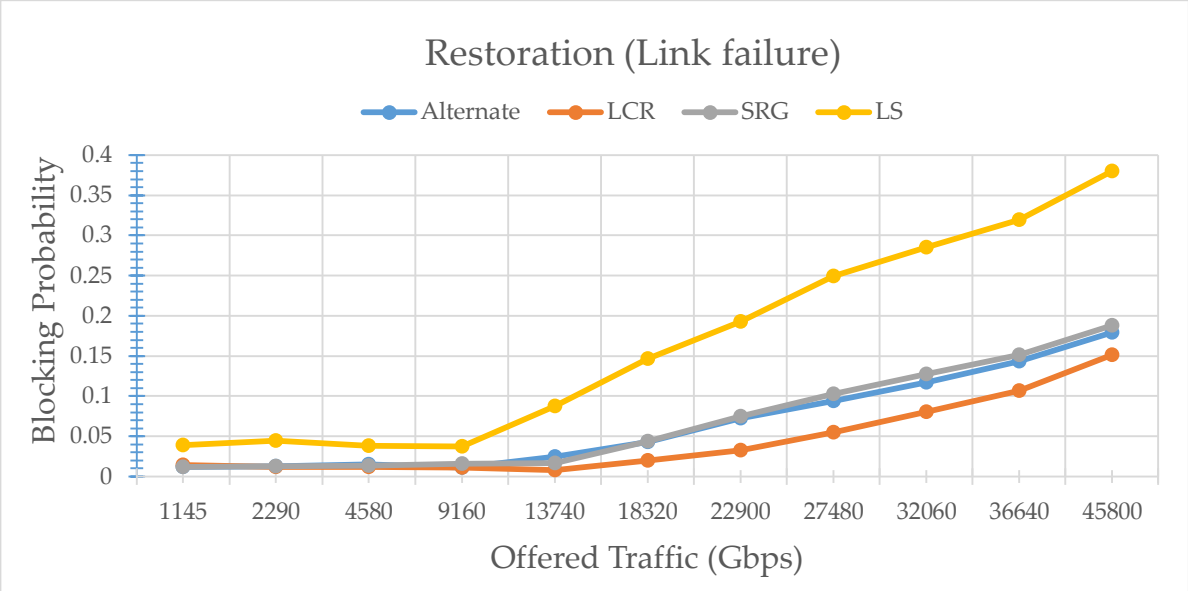

Figure 5.3. Blocking probability under restoration

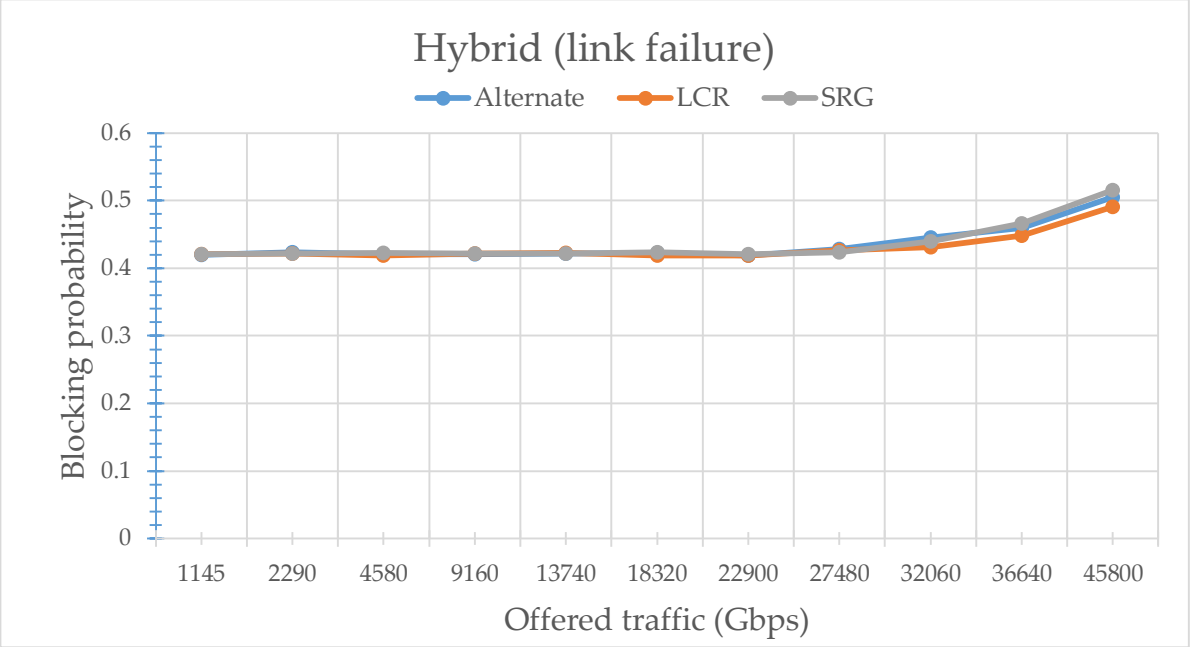

Figure 5.4. Blocking probability under hybrid resilience mechanism

Blocking probability performance of the remaining three RWA algorithms, alternate, LCR, and SRG-disjoint, is comparably the same especially at low traffic load. But as traffic load increases, blocking probability performance of LCR becomes better than alternate and SRG-disjoint especially in restoration resilience mechanism with an average 5% improvement at offered traffic volume 27480Gbps. The reason for the improvement is the congestion-free path selection nature of LCR. On the other hand, SRG-disjoint selects a path with less SRG overlap in addition to path availability and alternate routing only considers path availability. Out of the remaining two RWA algorithms, Alternate and SRG-Disjoint, Alternate routing slightly outperforms SGR-disjoint especially at higher traffic volume with average improvement value of o.6% at 32060 Gbps and 1% at 45800Gbps offered traffic volume.

Average Network Throughput result and discussion

Similar to blocking probability, average network throughput simulation is generated by running the Net2Plan simulator for alternate, Least Congested, SRG-disjoint and Load Sharing RWA algorithms under 1+1 DPP, Restoration and Hybrid resilience mechanisms for different offered traffic loads ranging from 1145Gbps to 45800Gbps. In all the simulations, previously mentioned reference topology (Figure 5.1) and non-uniform traffic demand are considered. From the simulations, the following simulation results are captured using the report generator feature of Net2Plan and graphically expressed using Microsoft Excel.

From the three graphs of average throughput (Gbps) versus offered traffic (Gbps) shown below (Figures 5.5, 5.6 & 5.7), it is clearly seen that average throughput offered by the network increases with an increase in offered traffic volume. In the restoration resilience mechanism, Figure 5.6 below, shows that load sharing offered lowest average throughput as compared to the other three RWA algorithms and the difference in the offered throughput increases with an increase in offered traffic. For instance, the difference in average throughput is 10.63% at offered traffic of 18320Gbps but increased to 15.63% at offered traffic of 32060Gbps. The reason for this is similar to the reason given for the blocking probability and it is due to selection criteria used by load sharing. Load sharing tries to find a path or route of a connection request with probability p considering the possibility of sharing a load and block the connection request if it does not find an available path without trying for another alternative path or route. Due to the low connectivity degree of the selected reference topology, load sharing does not work on 1+1 DPP and hybrid resilience mechanisms.

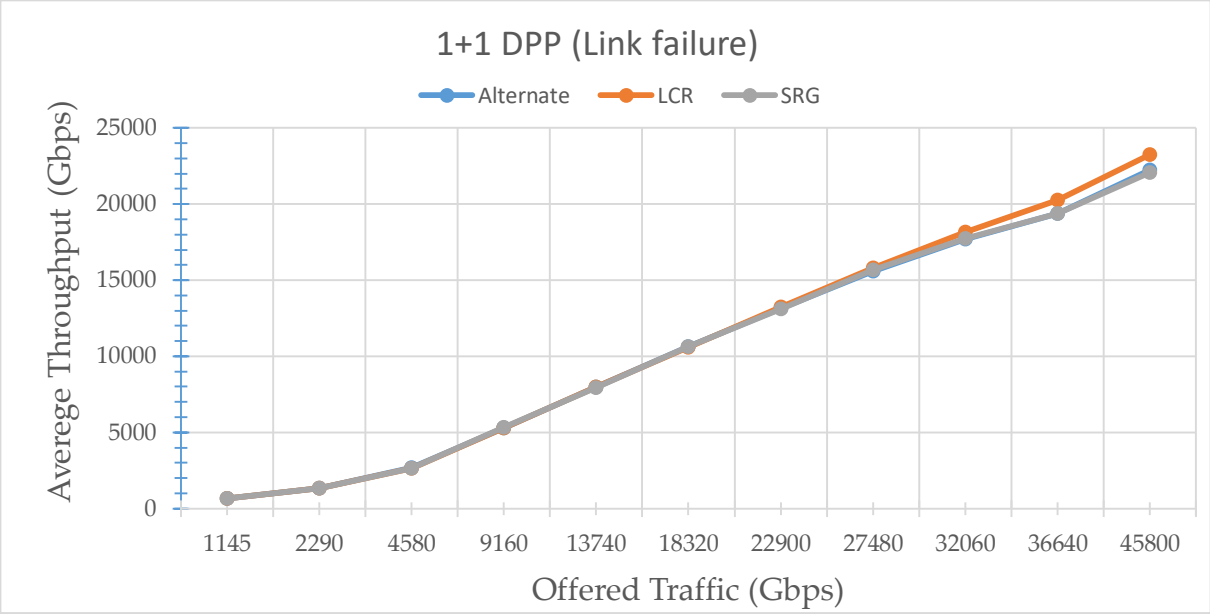

Figure 5.5. Average Network Throughput under DPP

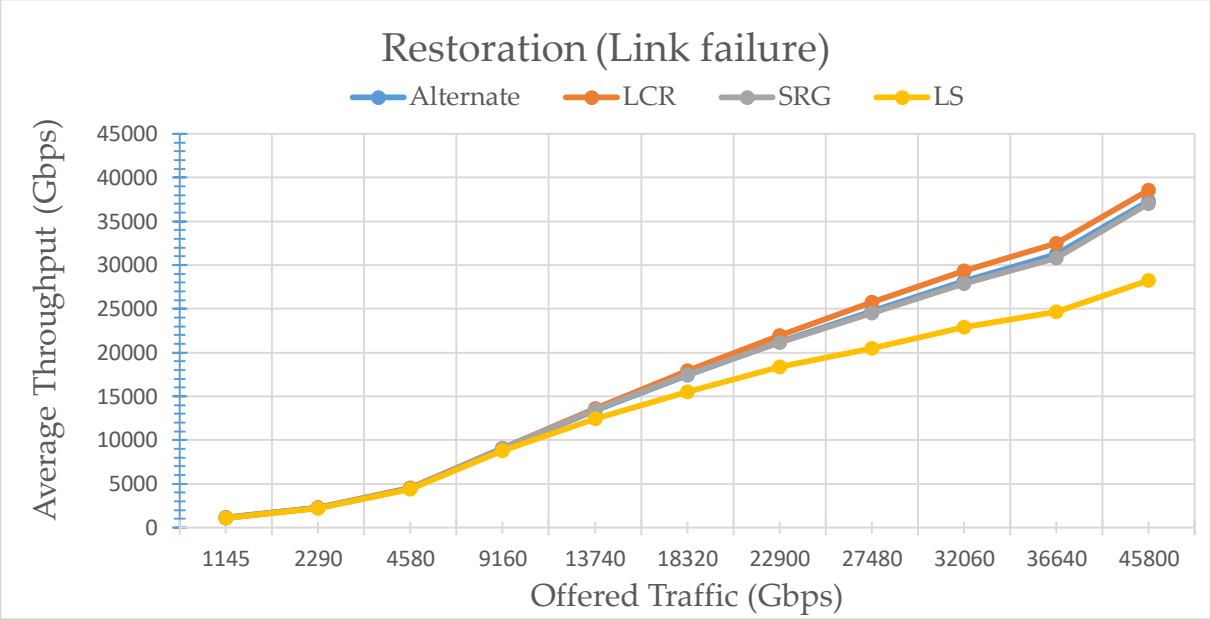

Figure 5.6. Average Network Throughput under Restoration

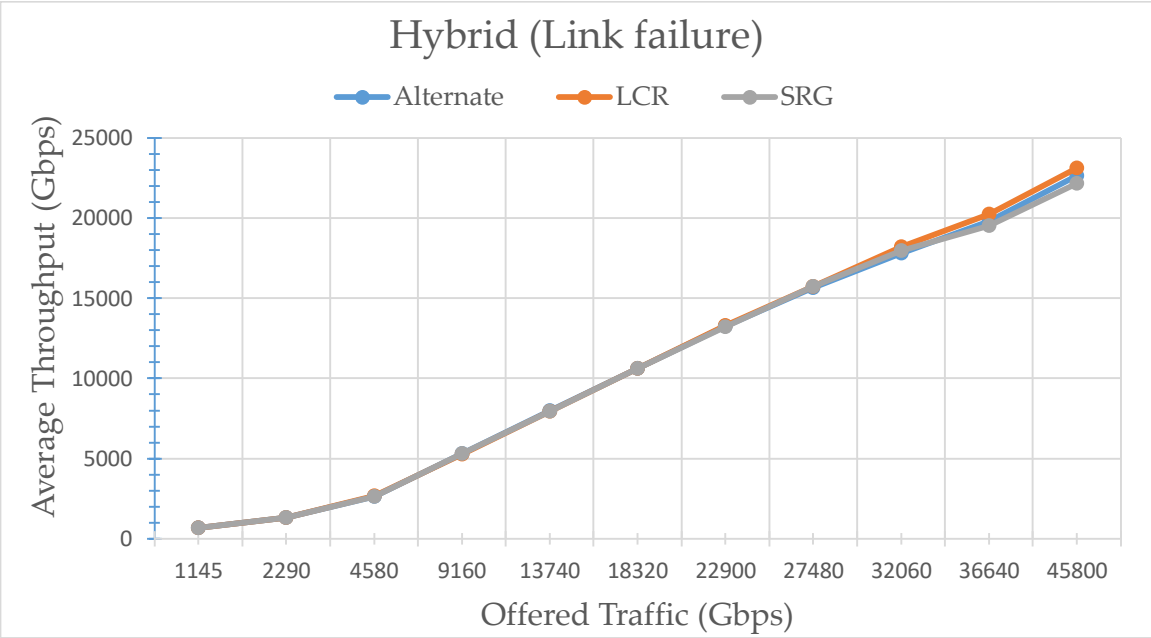

Figure 5.7. Average Network Throughput under Hybrid Resiliency

On the other hand, the remaining three RWA algorithms, Alternate, least congested and SRG-disjoint, have similar performance especially at low offered traffic volume as in the three graphs (Figures 5.5, 5.6 & 5.7). As offered traffic load increases average network throughput offered by least congested routing (LCR) slightly outperforms the other two routing algorithms especially in restoration resilience mechanism. The difference in average network throughput

between LCR and the other two routing algorithms is almost 0.3% at offered traffic volume of 9160Gbps but increased to 3% at offered traffic volume of 366640. The reason for this is the congestion minimization route selection criteria followed by LCR in selecting a route to provide a connection request in a network. On the other hand, alternate routing slightly outperforms SRG-disjoint routing and the performance difference is almost 0.3% at offered traffic volume of 27480Gbps. The reason for this is the route selection criteria followed by alternate routing which is a route or link availability without considering their SRG overlap to provide a connection request in a network.

In general, considering the above performance results of the four RWA algorithms under different resilience mechanisms, LCR outperforms the other three routing algorithms, especially at high offered traffic volume. Considering the path selection complexity of the routing algorithms and their performance difference, at low traffic load, alternate routing becomes more preferable than the other routing algorithms. In addition to this, due to the simplicity of the path selection criteria of alternate routing, the time required to provide a connection request can be minimized by using alternate routing. So, the author of this thesis recommends alternate routing for backbone network topologies with low connectivity degree similar to the considered reference topology and used alternate routing to evaluate resilience mechanisms under different offered traffic loads.

5.3. Result and discussion on QoS performance evaluation of resilience mechanisms

Results of QoS performance evaluation of different Resilience algorithms under the previously proposed RWA algorithm, Alternate Routing with First-Fit Wavelength Assignment will be discussed in detail in this section. In this thesis, three resilience mechanisms, 1+1 DPP, Restoration, and Hybrid resilience mechanisms are evaluated. The resilience mechanisms are selected by their wide practical usage and possibility of implementation on the current backbone networks including Ethio-telcom backbone network.

Blocking probability, recoverability and Average network throughput are used to compare the performance of the three resilience mechanisms. Net2Plan simulation setup and simulation assumptions mentioned in Section 5.1 are used to evaluate the performance of the resilience mechanisms. In evaluating the resilience mechanisms two common failure scenarios, unidirectional link failure and bidirectional link failure scenarios, are considered. A unidirectional link failure is used to represent a failure that happens due to patch cord or

connector problem and bidirectional failure to represent a failure due to fiber cut or SRG failure in a backbone network.

Blocking probability result and discussion

The graphs of blocking probability versus offered traffic (Gbps) shown in Figures 5.8 & 5.9 are generated by running the simulation of the three Resilience mechanisms, 1+1 DPP, Restoration, and Hybrid resilience mechanisms, under Alternate routing with different offered traffic volume. In the simulation, 1145Gbps to 45800Gbps offered traffic volume are considered. The offered traffic volume is selected based on the existing traffic volume offered by Ethio-telecom north circle backbone network. Alternate routing computes more than one alternate paths for each connection request arrived based on the criteria of the routing algorithm which is resource availability and allowed number of alternate paths. In this specific simulation case, allowed alternate paths are set to 5. The resilience mechanisms use the computed alternate paths based on the requirement of the considered type of resilience mechanisms. In 1+1 DPP, out of the computed alternate paths two paths are selected for primary and backup paths. In the restoration case, out of the computed alternate paths, one path is selected to provision a connection request or restore a failed primary path. On the other hand, Hybrid mechanism, which is a combination of 1+1 DPP and restoration, uses two paths out of the computed alternate paths to protect the network against first failure similar to 1+1 DPP and restore the network against second failure similar to Restoration.

The following two figures (Figures 5.8 & 5.9) are drawn offered traffic in Gbps versus Blocking probability in alternate routing for unidirectional and bidirectional link failures respectively. Blocking probability of all the resilience mechanisms increase with an increase in offered traffic as shown from the two graphs or figures (Figures 5.8 & 5.9) especially in the restoration resilience mechanism. The main reason for this increase is the increase in the contention for the decreasing available resources in the network with an increase in offered traffic load. This increase in contention mainly affects restoration due to the automatic restoration of a failed path without prior path provisioning and assignment for protection like 1+1 DPP. Blocking probability increases from 1.1% at 9160Gbps to 11.7% at 32060Gbps in restoration but it increases from 42% at 9160Gbps to 44.5% at 32060Gbps in 1+1 DPP and Hybrid resilience mechanisms. In addition to this, the high blocking probability performance of 1+1 DPP can be seen from results given in [68], [69].

The two graphs (Figures 5.8 & 5.9) show that restoration has better blocking probability as compared to 1+1 DPP and hybrid resilience mechanism in both failure scenarios. At low traffic load, restoration has a very low blocking probability with an average value of 1% but 1+1 DPP and hybrid resilience mechanisms have higher blocking probability with an average value of 42%. As the traffic load increases the difference in blocking probability between restoration and the remaining two resilience mechanisms decreases with the average difference value of 41% at 9160Gbps and 32% at 32060Gbps. On the other hand, the two remaining resilience mechanisms have almost similar blocking probability performance with slight performance differences at some load values. 1+1 DPP has a slightly higher blocking probability than a hybrid resilience mechanism with a performance difference value of 0.8 at higher loads (greater than 32060Gbps).

In addition to this, the two graphs (Figures 5.8 & 5.9) clearly show that the performance of the resilience mechanisms is not greatly affected by the considered failure scenario. The average performance difference that exists between the two failure scenarios is 0.6% in restoration and 0.3% in 1+1 DPP and hybrid. This is due to the fact that resilience mechanisms shift both legs of the affected link to the backup or restoration path even if the failure affects only one unidirectional link.

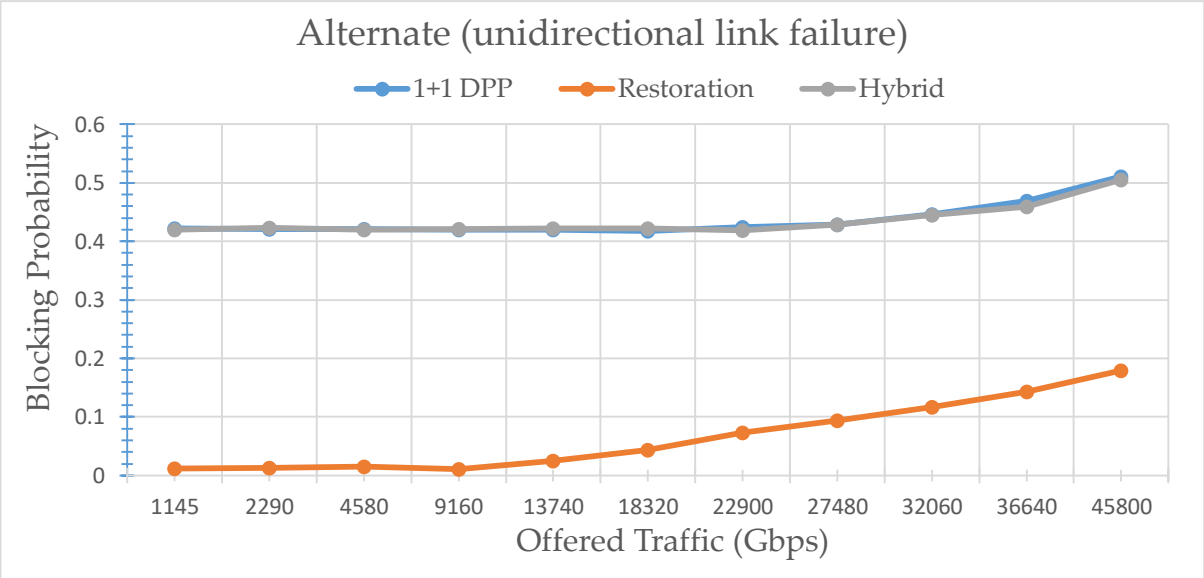

Figure 5.8. Blocking probability under Alternate routing with a unidirectional link failure

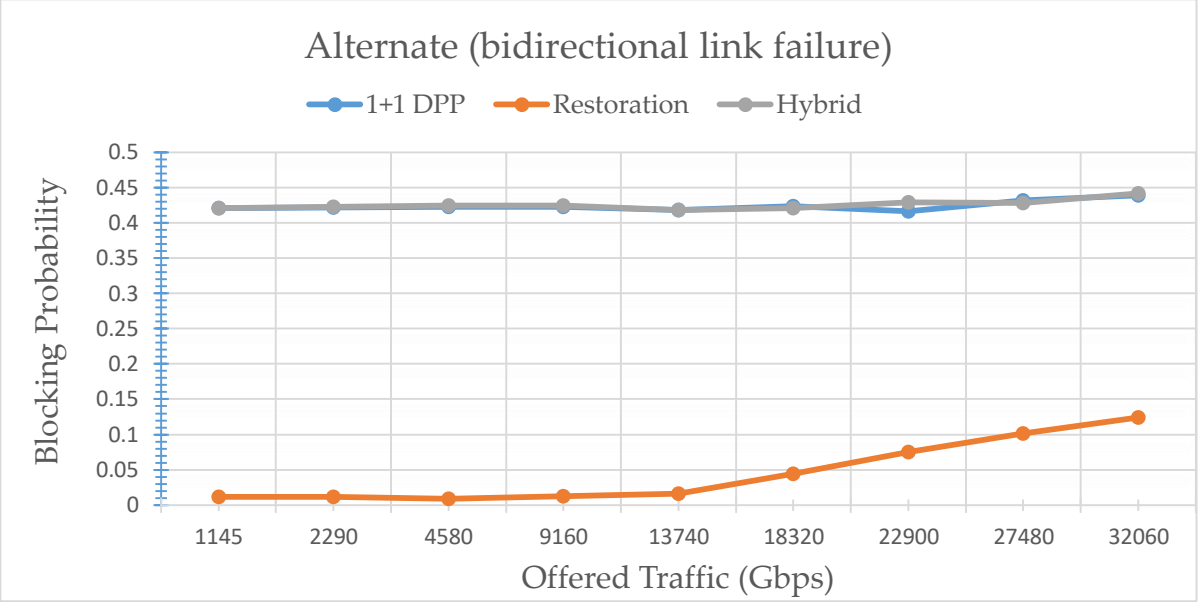

Figure 5.9. Blocking probability under Alternate routing with Bidirectional link failure

As previously discussed in Chapter 4, blocking probability expresses how efficiently network resources utilized. Considering this, from the above blocking probability discussion, it is possible to generalize that restoration better utilizes network resources as compared with the other two resilience mechanisms. In other words, restoration has better network resource utilization efficiency than 1+1 DPP and Hybrid resilience mechanisms.

Recoverability result and discussion

Similar to blocking probability, the graphs of recoverability (recovery probability) versus offered traffic (Gbps) shown in Figures 5.10 & 5.11 are generated by running the simulation of the three Resilience mechanisms, 1+1 DPP, Restoration, and Hybrid resilience mechanisms, under Alternate routing with different offered traffic volume. In the simulation, 1145Gbps to 45800Gbps offered traffic volume is considered. The following two figures (Figures 5.10 & 5.11) are drawn offered traffic in Gbps versus Recoverability in alternate routing for unidirectional and bidirectional link failures respectively.

The following two graphs (Figures 5.10 & 5.11) show that the recoverability performance of all the resilience mechanisms decreases with an increase in offered traffic, especially in restoration. The main reason for the decrease in recoverability is the increase in contention of the decreasing available resource with an increase in offered traffic load. In addition to this, the two graphs show that Restoration has lower recoverability than 1+1 DPP and hybrid

resilience mechanisms with an average recoverability value of 48% in restoration and 99% in 1+1 DPP and hybrid. The main reason for this is the automatic restoration path selection nature of the restoration resilience mechanism. In restoration, the failed link is recovered only if the resilience mechanism automatically finds a restoration path that fulfills the requirement of the service out of the available path in the network after failure occurrence but in 1+1 DPP and hybrid resilience mechanisms there exists one priory allocated backup path to restore a single failed link. From this, it is clear that the recoverability performance of restoration is dependent on the existence of available network resources. Recoverability difference between restoration and the other two resilience mechanisms increases with the increase in offered traffic load. The recoverability difference increases from 47% at 27480Gbps to 66% at 45800Gbps.

The remaining two resilience mechanisms, 1+1 DPP and hybrid, has almost similar recoverability performance with slight performance difference. The maximum performance difference between the two resilience mechanisms is almost 1% that is at some traffic loads 1+1 DPP outperform hybrid by a maximum value of 1% and at other traffic loads hybrid outperforms 1+1 DPP by a maximum value of 1%. In addition to this, the two figures (Figures 5.10 & 5.11) show that the recoverability performance of resilience mechanisms is not greatly affected by the failure scenario considered.

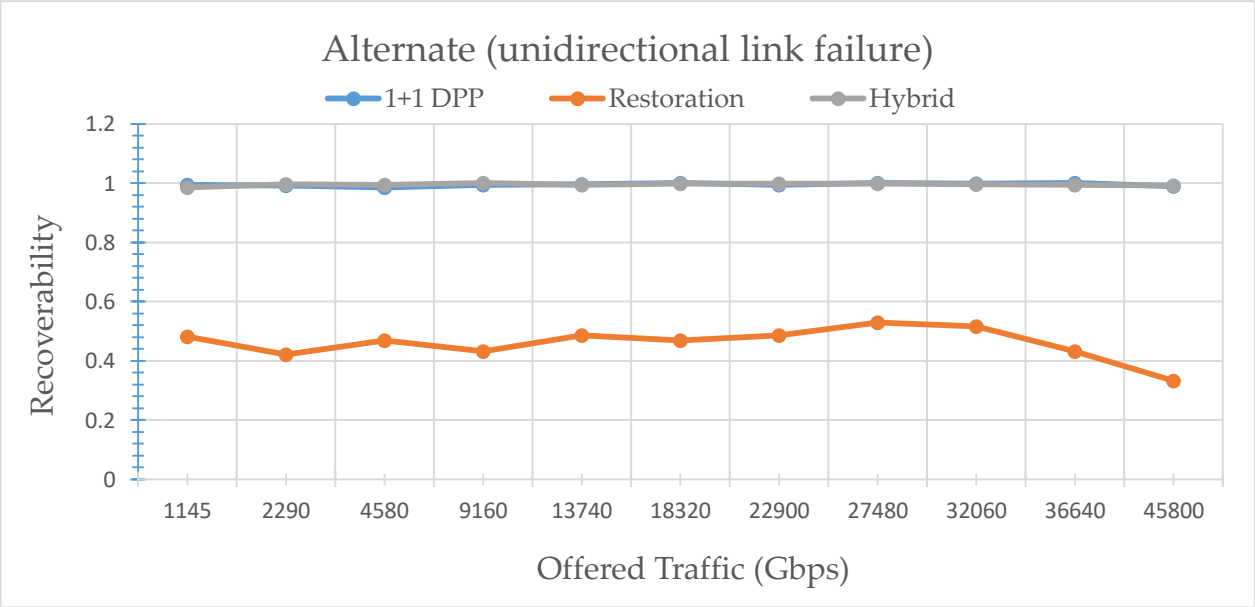

Figure 5.10. Recoverability under Alternate routing with a unidirectional link failure

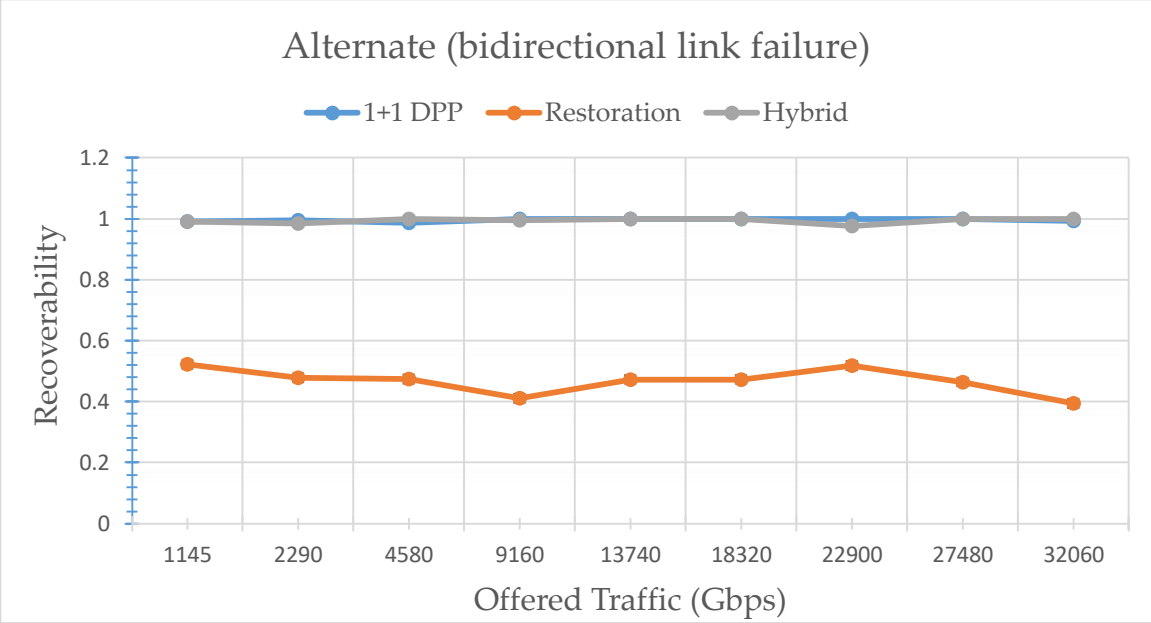

Figure 5.11. Recoverability under Alternate routing with Bidirectional link failure

Average Network Throughput result and discussion

Similar to blocking probability and recoverability, the graphs of average network throughput (Gbps) versus offered traffic (Gbps) shown in Figures 5.12 & 5.13 are generated by running the simulation of the three Resilience mechanisms, 1+1 DPP, Restoration, and Hybrid resilience mechanisms, under Alternate routing with different offered traffic volume. In the simulation, 1145Gbps to 45800Gbps offered traffic volume is considered. The following two figures (Figures 5.12 & 5.13) are drawn offered traffic in Gbps versus average network throughput in Gbps under alternate routing for unidirectional and bidirectional link failures respectively.

The following two figures or graphs (Figures 5.12 & 5.13) show that average network throughput increase with the increase in offered traffic load. The average throughput increase from 9017 Gbps at 9160Gbps to 31242Gbps at 36640Gbps in restoration and it increases from 5304Gbps at 9160Gbps to 19783Gbps at 36640Gbps in 1+1 DPP and hybrid resilience mechanisms. When the ratio of average network throughput to offered traffic is considered, more percentage of the offered traffic is allowed at low traffic load and it decreases with the increase in offered traffic load. In restoration, the percentage value allowed at 9160Gbps is 98.44% and it decreases to 85.27% at 36640Gbps offered traffic load. In 1+1 DPP and hybrid resilience mechanisms, the average value allowed decreases from 57.9% at 9160Gbps to 27%

at 366640Gbps. As previously discussed, the average network throughput value shows how efficiently the network resource is utilized after connection requests successfully provisioned. From these results, it is clear that restoration has a better average throughput than the other resilience mechanisms. In other words, restoration better utilizes network resources as compared to the other two resilience mechanisms. The main reason for this is, in restoration, there is no prior allocation of restoration or backup path. But in 1+1 DPP and hybrid, there is a priory allocated backup path which results in non-efficient network resource utilization.

Out of restoration, the remaining two resilience mechanisms have similar average network throughput performance with a slight difference at some offered traffic load values. In addition to this, the following two graphs (Figures 5.12 & 5.13) show that there is no great performance difference that exists from the failure scenario considered.

Considering the above performance evaluation results, blocking probability, recoverability and average throughput results, of the three resilience mechanisms, 1+1 DPP, Restoration, and Hybrid resilience mechanisms and implementation simplicity of the resilience mechanisms considered, it is possible to generalize that restoration is more suitable for network topologies with low connectivity degree similar to the considered reference topology at low traffic load (traffic load less than 36640Gbps). But as the traffic load increases the performance advantage that can be found from restoration decreases and it is recommended to use either 1+1 DPP or hybrid resilience mechanism based on the need for network protection against double link failure.

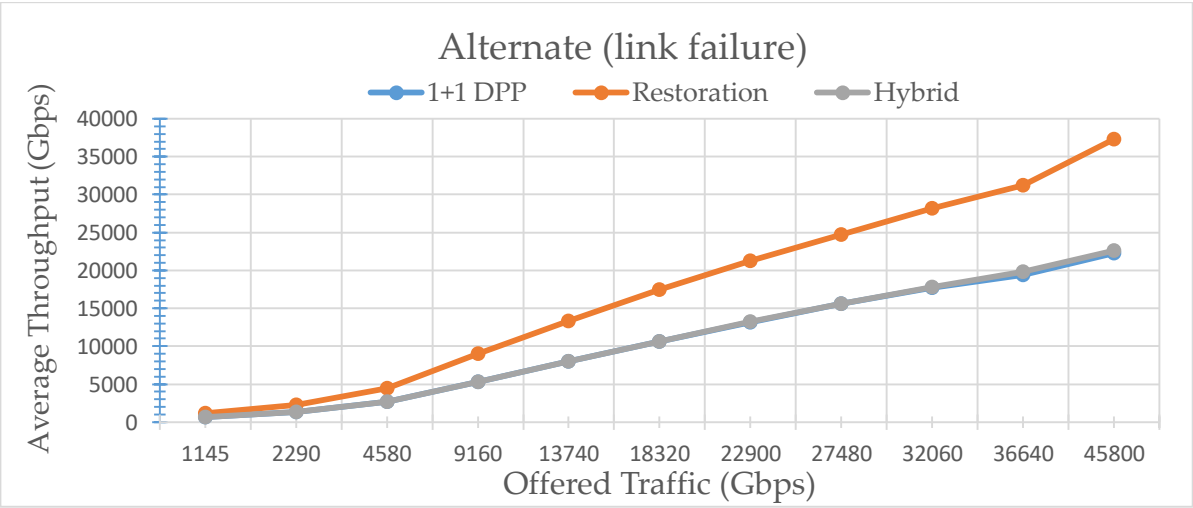

Figure 5.12. Average Network throughput under Alternate routing with a unidirectional link failure

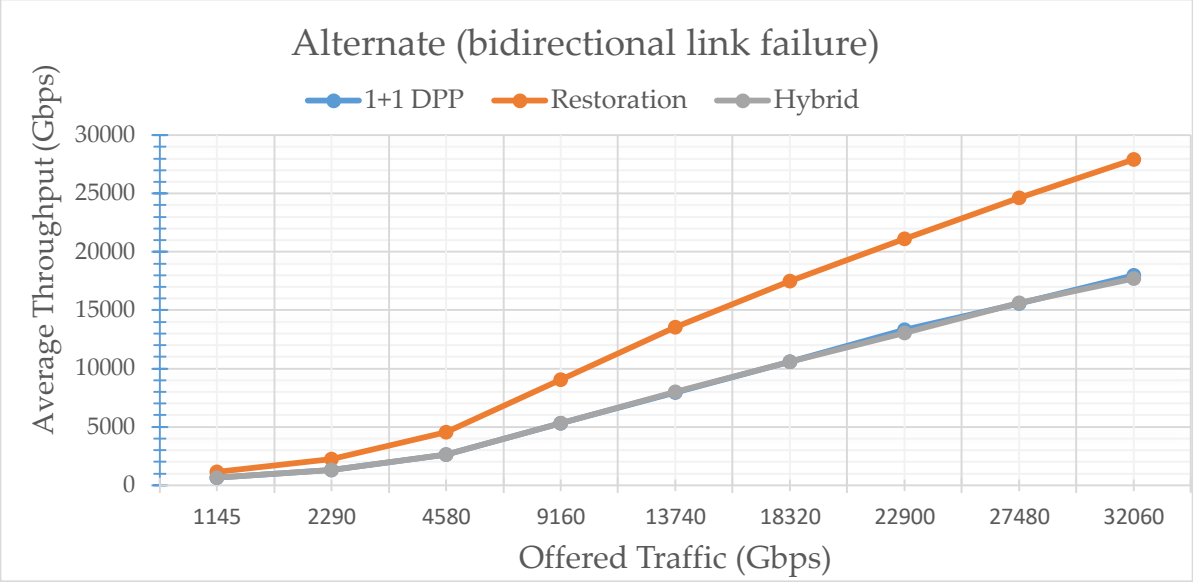

Figure 5.13. Average Network throughput under Alternate routing with Bidirectional link failure

Using restoration on a network topology with low connectivity like the current Ethio-telecom north circle backbone network improves blocking probability and average throughput of the network by about 40%. In using restoration, there is a tradeoff of recoverability and recovery time delay that happens due to the automatic restoration path provisioning at the time fault occurrence especially at high traffic load, as previously discussed in Chapter 3 and performance evaluation discussion above. But this tradeoff can be minimized by priory preparing a pool of restoration paths for each connection request provisioned without path allocation. In addition to this, using restoration, it is possible to protect a network against double link failure without the additional signaling requirement like in a hybrid resilience mechanism. In a hybrid resilience mechanism, additional signaling is required to synchronize the two resilience mechanisms used in addition to the one dedicated backup path requirement used to protect a network against first link failure.

5.4. Result and discussion on network connectivity degree effect on QoS Performance of resilience mechanisms

The network topology connectivity degree effect on the performance of a resilience mechanism will be discussed in this section. This section is added to show the effect of network topology connectivity on the performance of resilience mechanisms and give emphasis to the motivation given in Chapter 1 on the need of exact topology in evaluating the performance of resilience

mechanisms to be used in deploying a backbone network by telecom operators. In this section, two topologies that differ in average topology connectivity degree are used to show the effect of network topology connectivity degree on the performance of resilience mechanisms. In this section, the performance of only restoration and 1+1 DPP will be evaluated. The first topology used in this evaluation is Ethio-telecom north circle backbone network topology with 43 nodes and 138 links, previously used to evaluate the performance of RWA and resilience mechanisms shown in Figure 5.1. The previously used network topology has average connectivity of 3.209. The second topology used is generated by adding 30 unidirectional random links to the topology previously used. The connectivity degree of the second topology is increased to 3.907. The table below, Table 5-3, shows a summary of the second topology used

Table 5-3. Summary of modified network topology(B)

Number of Nodes	43
Number of links	168
Node out-degree (max, min, avg)	7, 1, 3.907
Capacity units name	Frequency slots (Wavelength)
Capacity installed: total	6720
Capacity installed: average per link	40
Number of demands (s,d node pairs)	112 (non-uniform)
Traffic units name	Gbps
Line Rates Per Light-path (Gbps)	40
Number of SRGs in the network	84
SRG definition characteristic	One SRG per bidirectional link bundle

The following three figures or graphs, Figures 5.14, 5.15 & 5.16, are drawn by running the simulation for the two resilience mechanisms, 1+1 DPP and restoration, under alternate routing for different offered traffic volumes. RWA algorithm considered in this evaluation is alternate routing with first-fit wavelength assignment. A failure scenario considered in this evaluation is

a unidirectional link failure. The three graphs, Figures 5.14, 5.15 & 5.16, respectively show blocking probability, recoverability and average network throughput performance of the two resilience mechanisms under the two network topologies. The legend with under bracket "A" represents performance results under the original topology (average connectivity of 3.209) and under bracket "B" represent performance results under the modified topology (average connectivity of 3.907).

As shown from the three graphs, Figures 5.14, 5.15 & 5.16, it is clear that network connectivity affects the performance of resilience mechanisms. Network connectivity degree increase by 0.9 on average decreases blocking probability by 10% and increase average throughput by 10% in the case of 1+1 DPP but it only decrease blocking probability by 1% and increase average throughput by 1% in the case of restoration as shown in Figures 5.14 & 5.16 especially at low traffic load. On the other hand, Network connectivity degree increase by 0.9 on average increases recoverability performance of restoration by 8% but it only increases recoverability performance of 1+1 DPP by less than 1% as shown in Figure 5.15. In 1+1 DPP, the protection path is prepared at the time of connection request provisioning which makes its recoverability independent of topology change. On the other hand, an increase in connectivity degree allows more connection requests to be provisioned by providing more available alternate paths in the network which improves blocking probability and average network throughput of 1+1 DPP. In restoration, there is no prior restoration path preparation and its recoverability is dependent on availability alternate paths on the network which makes its recoverability more dependent on network topology connectivity.

From the three results, Figures 5.14, 5.15 & 5.16, it is possible to generalize that the performance of different resilience mechanisms differs with network topology connectivity degree. In addition to this, the above results show that to select a resilience mechanism for backbone network implementation, network providers must evaluate the performance of the required resilience mechanism in their network topology to efficiently utilize their network resources and provide a service with required quality. Based on the above results, it is recommended to use restoration with alternate routing for low connected network topologies with connectivity degree similar to the considered reference topology at low traffic load. But for highly connected network topologies and low connected network topologies with high traffic load, it is recommended to use either 1+1 DPP or hybrid resilience mechanism with alternate routing based on the need for network protection against double link failure.

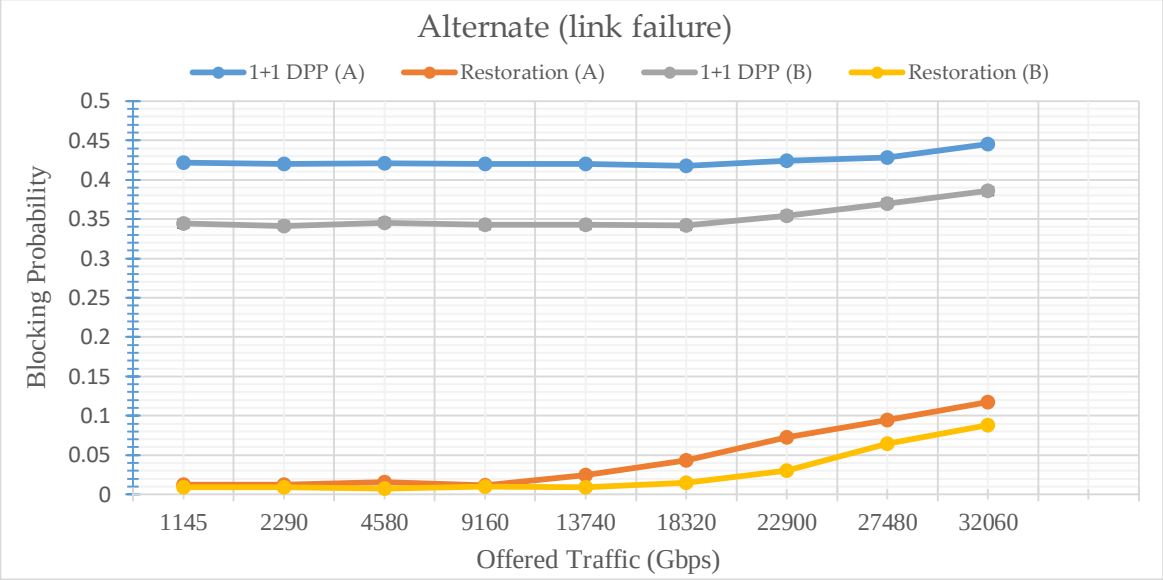

Figure 5.14. Blocking probability of resilience mechanisms for different topology

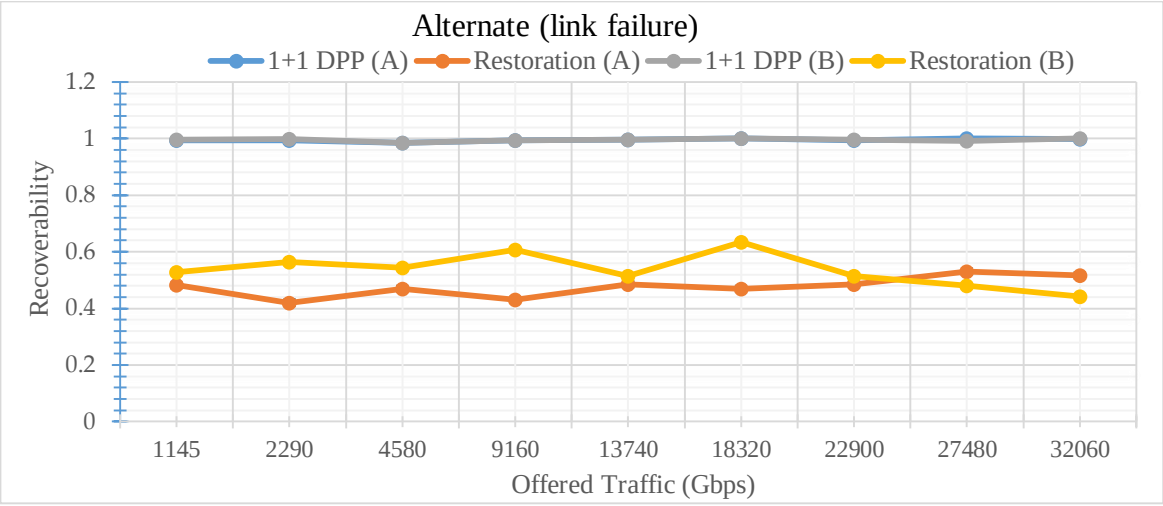

Figure 5.15. Recoverability of resilience mechanisms for different topology

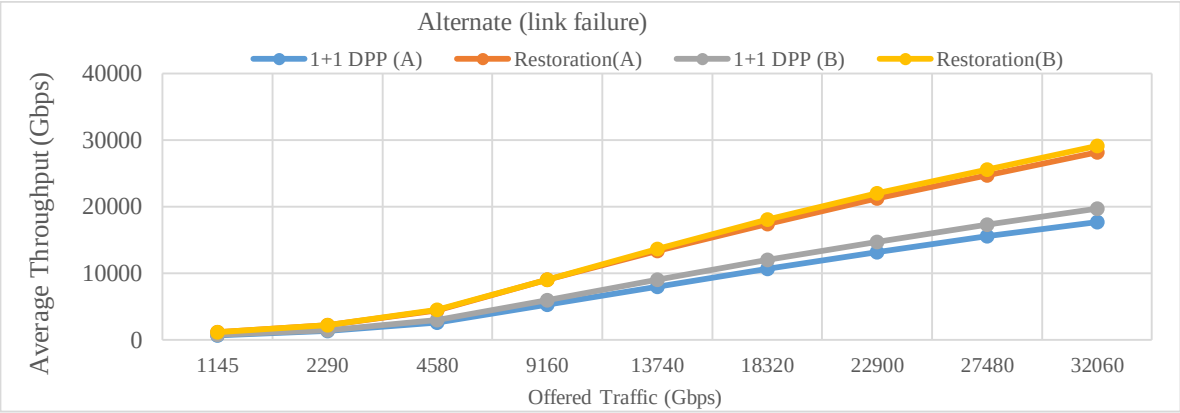

Figure 5.16. Average network throughput of resilience mechanisms for different topology

Chapter 6

Conclusion and Future Works

6.1. Conclusion

From the results of this thesis and review of similar kinds of literature, it is possible to conclude the following points:

- Different RWA algorithms and resilience mechanisms affect QoS of services that pass through ASON backbone network and utilize ASON backbone network resource differently
- Different RWA algorithms have different QoS performance under different resilience mechanism environments
- Load sharing routing algorithm only works under 1+1 DPP and hybrid resilience mechanism if the connectivity degree of the network topology is high (Highly connected network)
- Network topology connectivity degree affects performance of different resilience mechanisms differently
- At low connected network topologies, restoration has better utilizes network resources before and after connection request successful provisioning. But as connectivity degree of the network topology increases QoS performance superiority of restoration over 1+1 DPP decreases.
- For low connected backbone network, it is recommended to use Restoration under Alternate routing with first-fit wavelength assignment for better QoS and network resource utilization.
- For a highly connected backbone network, it is recommended to use a 1+1 DPP or Hybrid resilience mechanism under Alternate routing with first-fit wavelength assignment for better QoS and network resource utilization based on the need for network protection against DLF.

Generally, considering the above cases, it is not recommended and effective to use resilience mechanisms and RWA algorithms proposed for a highly connected network in low connected networks and vice versa. So, it is recommended that telecom operators should evaluate and select RWA algorithms and resilience mechanisms considering their network topology

connectivity degree. In addition to this, telecom operators should implement their backbone network considering the performance of resilience mechanisms on their network topology and allowed performance tradeoff.

6.2. Future Works

The evaluation results of this research work can be used as a starting point to select the RWA algorithm and resilience mechanism in implementing the Ethio-telecom backbone network. But to get the most benefit out of the recommended type of resilience mechanism and make a decision on a possible number of restoration paths to be prepared as a pool, as future work, exact recoverability improvement that exists from preparing a pool of restoration path and its tradeoff needs to be studied. In addition to this, in the future, the effect of physical layer constraints of the network topology on the performance of the resilience mechanisms and RWA algorithm need to be studied to make the evaluation more practical.

As previously mentioned in chapter three, MTTR and MTTF value considered in setting up the evaluation simulations are not the exact value of MTTR and MTTF of the Ethio-telecom north circle backbone network. As future work, MTTR and MTTF of Ethio-telecom should be studied to make future evaluations of the network more practical and know the exact failure behavior of the network. In addition to this, optical power debugging that exist at the time of optical channel add and drop need to be studied. The study of power debugging helps to make the use of RWA algorithms more practical and solve the manual interruption required to minimize service interruption that happens due to optical power difference between channels of the multiplexer and de-multiplexer.

This research considered Ethio-telecom north circle reference topology with 43 nodes and 138 links with non-uniform traffic demand matrix. As future work, the evaluation can be done on the other two circles of the Ethio-telecom backbone network considering their exact network topology failure behavior, physical layer constraint, and traffic matrix. In addition to this, evaluation of the resilience mechanisms with failure scenarios such as node failure can be further studied in future work.

References

[1] L. Wosinska *et al.*, "Network resilience in future optical networks," in *Towards Digital Optical Networks*, vol. 5412 LNCS, 2009, pp. 253–284.

[2] A. E. Ozdaglar and D. P. Bertsekas, "Routing and wavelength assignment in optical networks," *IEEE/ACM Trans. Netw.*, vol. 11, no. 2, pp. 259–272, 2003.

[3] D. A. Schupke, M. Jäger, and R. Hülsermann, "Comparison of resilience mechanisms for dynamic services in intelligent optical networks," *Des. Reliab. Commun. Networks*, pp. 106–113, 2003.

[4] H. Pereira *et al.*, "On the Performance Analysis of Different Link to Path Restoration Schemes for All-Optical Networks," 2012.

[5] G. Karpagarajesh and M. Vijayaraj, "Comparison and Implementation of Routing and Wavelength Assignment Strategies in Wdm Optical Networks Utilizing Without Wavelength Conversion Technique (WWCT)," vol. 9, no. 2, pp. 103–107, 2017.

[6] CCITT, "Quality of Service and Dependability Vocabulary," 1988.

[7] ITU-T, "Quality of experience requirements for IPTV services," 2008.

[8] D. Waturu, "ITU-T Recommendations and other International Standards Relevant to QOS/QOE," Nairobi, Kenya, 2010.

[9] Y. S. Kavian, H. F. Rashvand, M. S. Leeson, W. Ren, E. L. Hines, and M. Naderi, "Network Topology Effect on QoS Delivering in Survivable DWDM Optical Networks," *J. Telecommun. Inf. Technol.*, vol. 1, pp. 68–71, 2009.

[10] E. T. C. (ETC), "Company profile Bulletin," *2008*.

[11] E.-T. Huawei Technologies Ethiopia PLC, "Low-Level Design for LOT-4," Addis Ababa, Ethiopia, 2016.

[12] A. Jajszczyk, "Control Plane for Optical Networks : The ASON Approach," *China Commun.*, no. 113, pp. 113–122, 2004.

[13] A. Jajszczyk, "Automatically Switched Optical Networks: Benefits and Requirements," *IEEE*, no. 0163-6804/05, pp. 10–15, 2005.

[14] L. Velasco, "Recovery mechanisms in ASON / GMPLS networks," Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, 2009.

[15] T. I. E. Consortium, "Generalized Multiprotocol Label Switching (GMPLS) Definition and Overview."

[16] Alcatel-Lucent, "ASON / GMPLS Control Plane : Intelligent Optical Transport," 2009.

[17] R. K. Avadhesh, "Study paper on Automatically Switched Optical Network (ASON), DDG (FA), TEC, New Delhi, 2011."

[18] R. Martinez, R. Munoz, M. Requena, and G. Junyent, "Architecture and implementation

of a resilient control plane for optical networks based on GMPLS OSPF-TE," *9th Eur. Conf. Networks Opt. Commun.*, pp. 1–9, 2004.

[19] S. K. Naik, "QoS Aware data-path routing in DWDM / GMPLS NETWORK," 2011.

[20] G. Deo, "Generalized Multi-Protocol Label Switching (GMPLS) - Multilayer," pp. 1–8, 2003.

[21] C. Systems, "Cisco Segmented Generalized Multiprotocol Label Switching for the IP Next-Generation Network", 2006

[22] S. Tomic, B. Statovci-Halimi, and A. Halimi, "ASON and GMPLS — Overview and Comparison," *Photonic Netw. Commun.*, vol. 7, no. 10.1023/B: PNET.0000012432.77218.10, pp. 111–130, 2004.

[23] O. Brun and S. Baraketi, "Routing and Wavelength Assignment in Optical Networks," no. hal-01062321, pp. 1–41, 2014.

[24] K. Christodoulopoulos, K. Manousakis, and E. Varvarigos, "Comparison of routing and wavelength assignment algorithms in WDM networks," *GLOBECOM - IEEE Glob. Telecommun. Conf.*, pp. 2658–2663, 2008.

[25] R. T. Koganti and D. Sidhu, "Analysis of routing and wavelength assignment in large WDM networks," *Procedia Comput. Sci.*, vol. 34, no. 410, pp. 71–78, 2014.

[26] W. Kebede, "Constraint-Based Hybrid Resiliency Mechanisms for Better Resource Utilization and Service Performance Quality in ASON SLA," Addis Ababa University, 2018.

[27] B. Mukherjee, Hui Zang, and Jason P. Jue, "A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical WDM Networks," *Optical Network Magazine*, pp. 47–60, Jan-1999.

[28] X. Masip-Bruin, S. Sánchez-Lopez, J. Solé-Pareta, J. Domingo-Pascual, and E. Marín-Tordera, "Hierarchical routing with QoS constraints in optical transport networks," in *Third international IFIP-TC6 Networking Conference*, vol. 3042, pp. 662–674, 2004.

[29] S. H. Pei Luo and J. Z. and W. Gu, "Dynamic interdomain wavelength routing based on source routing in ASON," *Netw. Archit. Manag. Appl. IV*, vol. 6354, p. 63543C, 2006.

[30] Z. Na and S. Haijin, "A distributed strategy for dynamic routing and wavelength assignment in ASON network," *Proc. 2005 7th Int. Conf. Transparent Opt. Networks, Ict. 2005*, vol. 1, pp. 201–204, 2005.

[31] P. P. Marino, *Optimization of Computer Networks- Modeling and Algorithms A Hands-on Approach*. 2016.

[32] J. L. Izquierdo-Zaragoza, J. J. Pedreno-Manresa, and P. Pavon-Marino, "Maximizing IP fast rerouting coverage in survivable IP-over-WDM networks," *Eur. Conf. Opt. Commun. ECOC*, vol. 2015-Novem, 2015.

[33] K. man Chan and T. shing P. Yum, "Analysis of least congested path routing in WDM lightwave networks," *Proc. - IEEE INFOCOM*, vol. 2, pp. 962–969, 1994.

[34] A. Wason and R. S. Dr. Kaler, "Wavelength Assignment Problem in Optical WDM Networks," *Int. J. Comput. Sci. Netw. Secur.*, vol. 7, no. 4, pp. 27–31, 2007.

[35] N. Nag and I. Bala, "Comparative Study of Wavelength Assignment Algorithms for WDM Optical Network," vol. 2, no. 10, pp. 1247–1249, 2013.

[36] R. Goscien, K. Walkowiak, M. Klinkowski, and J. Rak, "Protection in elastic optical networks," *IEEE Netw.*, vol. 29, no. 6, pp. 88–96, 2015.

[37] C. M. Machuca, O. Moe, and M. Jäger, "Impact of protection schemes and network component's availability on operational expenditures," *J. Opt. Netw.*, vol. 7, no. 2, pp. 142–150, 2008.

[38] J. Ahmed, "Dynamic Resource Provisioning and Survivability Strategies in Optical Networks," KTH Information and Communication Technology, 2013.

[39] P. H. Ho and H. T. Mouftah, "A novel survivable routing algorithm for shared segment protection in mesh WDM networks with partial wavelength conversion," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 8, pp. 1548–1560, 2004.

[40] M. Jaeger, R. Huelsermann, D. A. Schupke, and R. Sedlak, "Evaluation of Novel Resilience Schemes in Dynamic Optical Transport Networks," *Opt. Netw. II*, vol. 4910, pp. 82–93, 2002.

[41] J. Ahmed, C. Cavdar, P. Monti, and L. Wosinska, "Hybrid Survivability Schemes Achieving High Connection Availability With a Reduced Amount of Backup Resources [Invited]," vol. 5, no. 10, pp. 152–161, 2013.

[42] D. K. Tyagi, "Routing and Wavelength Assignment in WDM Network using IWD based Algorithm," pp. 1424–1429, 2016.

[43] R. Sendag, P. Chuang, and D. H. C. Du, "Routing and Wavelength Assignment in Optical Passive Star Networks with Non-uniform Traffic Load," pp. 1435–1439, 2001.

[44] A. Urra, E. Calle, and J. L. Marzo, "Enhanced protection using shared segment backups in a multiservice GMPLS-based networks," in *Proceedings - IEEE Symposium on Computers and Communications*, 2005, vol. 10, no. 1530–1346/05, pp. 752–757.

[45] A. E. Kamal, "1+N network protection for mesh networks: Network coding-based protection using p-cycles," *IEEE/ACM Trans. Netw.*, vol. 18, no. 1, pp. 67–80, 2010.

[46] U. Mahmud, N. A. Malik, B. Rauf, K. A. Bhatti, and H. Afzal, "QoS Aware Wavelength Assignment in Wavelength Division Multiplexing Based Optical Networks," pp. 23–27, 2015.

[47] W. Halabi, K. Steenhaut, M. Goossens, and T. T. A. Nowé, "Hierarchical routing and traffic grooming in IP / MPLS-based ASON / GMPLS multi-domain networks," pp. 217–229, 2012.

[48] W. Li and L. Kong, "Study on ASON Route Selection Based on Genetic Algorithm," pp. 127–130, 2015.

[49] W. Ramirez *et al.*, "An Hybrid Prediction-based Routing Approach for Reducing

Routing Inaccuracy in Optical Transport Networks i," 2014.

[50] H. Øverby, *Traffic Load Uniformity in Optical Packet Switched Networks*, 2019.

[51] E. Oki, *Linear Programming and Algorithms for Communication Networks*, 2012.

[52] B. Jaumard, C. Meyer, B. Thiongane, and A. L. Formulation, "ILP Formulations and Optimal Solutions for the RWA Problem," pp. 1918–1924, 2004.

[53] Brigitte Jaumard, Christophe Meyer, and Babacar Thiongane "ILP Formulations for the Routing and Wavelength Assignment Problem: Symmetric Systems," in *Handbook of Optimization in Telecommunications*, pp. 637–677, 2006.

[54] Y. Belayneh, "Sleep Mode Operation for Power Consumption Minimization in Optical Networks : a Case Study of Ethio Telecom Backbone Optical Transport Network," Addis Ababa University, 2018.

[55] W. Dai, J. Zhang, and X. Sun, "On solving multi-commodity flow problems : An experimental evaluation," *Chinese J. Aeronaut.*, no. January, 2017.

[56] I. Wang, "Multicommodity Network Flows : A Survey , Part I : Applications and Formulations," *Int. J. Oper. Res.*, vol. 15, no. 10.6886/IJOR.201812_15(4).000, 2019.

[57] D. Hutchison and J. C. Mitchell, *Towards Digital Optical Networks*. 2009.

[58] J. Ahmed and S. Nawaz, "POSE: A New Discrete Event Optical Simulator for the Java Platform," *Natl. Conf. Emerg. Technol.*, pp. 184–188, 2004.

[59] J. Korniak and P. Róycki, "GMPLS - simulation tools," *Tools Inf. Technol.*, pp. 1–6, 2006.

[60] J. I. Zaragoza and P. Pavon-Marino, "Net2Plan : An Open-Source Multilayer Network Planning Tool and In-Operation Simulator (Demo Paper)," pp. 0–3, 2015.

[61] P. Pavon-Marino, "On the Role of Open-Source Optical Network Planning," pp. 2–4, 2014.

[62] P. Pav, "Net2Plan 0.5.0 User's manual," 2017.

[63] ETSI, "Human Factors (HF); Quality of Experience (QoE) requirements for real-time communication services," 2009.

[64] W. Wei, Q. Zeng, Y. Ouyang, and D. Lomone, "DIFFERENTIATED INTEGRATED," no. November, pp. 27–34, 2004.

[65] A. Kavitha, "Performance of Optical Networks : a short survey," vol. 4, no. 02, pp. 600–605, 2012.

[66] G. Karpagarajesh and M. Vijayaraj, "Blocking Probability in All-Optical WDM Network Using IMCA," no. May, pp. 1068–1077, 2016.

[67] Sunil Kumar Kilaka and HIMANSU SAHU, "Performance Analysis of Optical Networks," National Institute of Technology, Rourkela, 2012.

[68] X. Wei, L. Li, H. Yu, and L. Guo, "A heuristic algorithm for priority-based lightpath allocation in survivable WDM mesh networks," in *Proc. SPIE, Network Architectures, Management, and Applications*, vol. 6784, pp. 1–8, 2007.

[69] S. I. Pouremami and B. Bakhshi, "On the trade-off between power-efficiency and blocking probability in fault-tolerant WDM networks," *J. Netw. Comput. Appl.*, vol. 58, no. 1084–8045, pp. 255–266, 2015.