Addis Ababa University

Addis Ababa Institute of Technology

Electrical and Computer Engineering

Telecom Network Engineering Graduate Program

Constraint-Based Hybrid Resiliency Mechanisms for Better Resource Utilization and Service Performance Quality in ASON SLA

Thesis Submitted to the School of Electrical and Computer Engineering in Partial Fulfillment of the Requirements for Master of Science Degree in Telecom Networks Engineering

Wondale Kebede

Advisor: Dr. Yalemzewd Negash

November 2018

Addis Ababa University

Addis Ababa Institute of Technology

Electrical and Computer Engineering

Telecom Network Engineering Graduate Program

Constraint-Based Hybrid Resiliency Mechanisms for Better Resource Utilization and Service Performance Quality in ASON SLA

By**: Wondale Kebede**

Dr. Yalemzewd Negash	____________
Advisor	Signature
______________________________	____________
Evaluator	Signature
______________________________	____________
Evaluator	Signature
______________________________	____________
Evaluator	Signature

Abstract

In optical transport networks, contents of service level agreement (SLA) are not standardized yet. There is a general recommendation to include network resiliency mechanisms in SLA contracts by considering trade-off between resource utilization and service performance quality. This research work proposes two solutions to fulfil these trade-off requirements in network resiliency mechanisms.

The first solution is employing a Routing and Wavelength Assignment (RWA) algorithm that can utilize network resources efficiently in Automatically Switched Optical Network (ASON) service provisioning. The research work conducts blocking probability and network availability comparison simulations for Shared Risk Group (SRG)-Disjoint Aware First-Fit Routing, Alternate Routing, Least Congested Routing and Load Sharing routing algorithms coordinated with First-Fit wavelength assignment algorithm in 1+1 Dedicated Path Protection (DPP) and Restoration schemes. The simulations performed on Net2Plan tool show that Alternate Routing algorithm has best overall results in blocking probability and network availability for both protection and restoration.

The second solution is enhancing service performance qualities by combining protection and restoration. This research work proposes new constraint-based hybrid resiliency mechanisms (1+1 Link-Disjoint + Restoration, 1+1 Node-Disjoint + Restoration and 1+1 SRG-Disjoint + Restoration). The performance of these hybrid resiliency mechanisms is evaluated using Net2plan simulation tool. The results show that the network availability and recoverability performances are improved when it is compared to non-combined counter parts. 1+1 Node-Disjoint + Restoration shows best recoverability at lower traffic loads during link or SRG failures. At higher traffic loads, 1+1 SRG-Disjoint + Restoration performs best in recoverability during SRG failures. For instance, 1+1 SRG-Disjoint + Restoration has on average 16.8% higher recoverability than 1+1 Link-Disjoint + Restoration, at higher traffic loads. These performance enhancements are obtained with cost of relatively higher blocking probability.

Keywords: Alternate Routing, ASON, Availability, blocking probability, DPP, First-Fit, GMPLS, Hybrid Resiliency, Link-Disjoint, Load Sharing, Network Resiliency, Node-Disjoint, Protection, SRG-Disjoint, Recoverability, Recovery, Resource Utilization, Restoration, RWA, SLA, Survivability, SRG-Disjoint Aware.

Acknowledgement

I would like to thank you ethio telecom for praising me this golden opportunity to pursue my Master of Science Degree at Addis Ababa Institute of Technology. It was a great experience for me. My special thanks go to Dr. Yalemzewd Negash, who supervised me during my research. His unreserved and extremely helpful instructions, guidance, encouragements and insightful comments kept me always in the right direction, even in times I felt I was stuck, so that I could finally achieve my goal. I am very grateful to my colleagues in ethio telecom for their valuable support and advice as well as for providing me a great working environment. I need to thank all my friends and individuals for their direct or indirect valuable supports that help me to shape and finalize the thesis. Finally, I would like to thank my family and dear friends for their understanding and patience during my absence in the social life throughout perusing my study. I thank you all for being part of my thesis.

Contents

List of Figures

List of Tables

List of Acronyms/ Abbreviations

AR	Adaptive Routing
ASON	Automatically Switched Optical Network
ATM	Asynchronous Transfer Mode
CR- LDP	Constraint-based Routed Label Distribution Protocol
DES	Discrete Event Simulation
DPP	Dedicated Path Protection
DWDM	Dense Wavelength Division Multiplexing
E-NNI	External Network to Network Interface
FAR	Fixed-Adaptive Routing
FR	Fixed Routing
Gbps	Giga bit per second
GMPLS	Generalized Multi-Protocol Label Switching
IETF	Internet Engineering Task Force
I-NNI	Internal Network to Network Interface
IP	Internet Protocol
ISIS-TE	Inter System to Inter System extended for Traffic Engineering
ITU	International Telecommunication Union
ILP	Integer Linear Programming
ISC	Interface Switching Capability
LCR	Least Congested Routing
LMP	Link Management Protocol
LSA	Link State Advertisement
LSDB	Link State Data Base
LSP	Label Switched Path
LTV	Length Type Variable
MPLS	Multi-Protocol Label Switching
MTBF	Mean Time Between Failures
MTTF	Mean Time to Fail
MTTR	Mean Time to Repair
NMS	Network Management System
OADM	Optical Add-Drop Multiplexer
O-E-O	Optical to Electrical to Optical

OTN	Optical Transport Network
OXC	Optical Cross-Connection
OSPF	Open Shortest Path First
PDH	Plesiochronous Digital Hierarchy
QoS	Quality of Service
RSVP-TE	Resource Reservation Protocol with Traffic Engineering Extensions
RWA	Routing and Wavelength Assignment
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SONET	Synchronous Optical Network
SPP	Shared Path Protection
SRG	Shared Risk Group
Tbps	Tera bit per second
TDM	Time Division Multiplexer
TE	Traffic Engineering
TED	Traffic Engineering Database
UNI	User to Network Interface
WDM	Wavelength Division Multiplexing

Chapter One

1. Introduction

Nowadays, fast-changing technologies and uncertain business tendencies contribute for increasing bandwidth demand [1], [2]. The usual traditional transport technologies, such as Synchronous Digital Hierarchy (SDH) or Synchronous Optical Networking (SONET) and Asynchronous Transfer Mode (ATM) became capacity limited and can no longer fulfill these high bandwidth demands of services emerging currently. These networks are very poor in utilizing full potential of optical fiber medium. Then, Wavelength Division Multiplexing (WDM) technologies are evolved to increase the bandwidth of optical fiber medium and to effectively utilize this bandwidth. In such networks, multiple signals can be transmitted through the same fiber with different wavelengths. It is possible to achieve higher optical link capacities in order of Tera bit per second (Tbps) .

The outcomes in WDM technologies further encouraged developments of wide range of circuit switching devices, such as Optical Cross-Connection (OXCs) and Optical Add-Drop Multiplexers (OADMs) [2]. Then, International Telecommunication Union (ITU-T) established Optical Transport Network (OTN) standard to accommodate coexistence of traditional SDH/SONET networks, WDM-based networks and Internet Protocol (IP) over WDM networks as a layered architecture.

The main objective of OTN was to offer high volume of different service traffic to various clients with different performance requirements in a single network [3], [4]. However, the central Network Management System (NMS) used to carryout out fault management, configuration management and service provisioning has significant limitations. It often cannot allocate available resources properly due to the inflexibility of manually provisioned nature of large-scale optical networks. The provisioning system from NMS requires large amount of manual configuration and human communication. Since this NMS service provisioning is usually error prone and slow, it initiates a higher demand for fast end-to-end connections that can be provisioned automatically and dynamically.

In order to fulfil this dynamic provisioning demand ITU-T proposed Automatically Switched Optical Network (ASON) architecture which enhances the OTN with dynamic connection capability [3], [5]. This capability is accomplished by means of control plane entity enabled with Generalized Multi-Protocol Label Switching (GMPLS) protocols, which is responsible for the establishment, maintenance, and release of connections over optical transport plane. GMPLS control plane provides the required automation and intelligence to configure and manage fast end-to-end connections that are provisioned automatically and dynamically to eliminate human manual intervention. GMPLS is a set of protocols standardized by the IETF which provides functions like routing, signaling and link management.

1.1 Problem Statement

In optical communication, there is an increasing demand for services with better performance quality from customers [10], [11]. These requirements are usually stipulated in Service Level Agreement (SLA) contracts. On the other hand, there is also a demand from service providers side to offer such services with a reasonably better network resource utilization. In optical networks there is always a tradeoff between resource utilization and service performance quality. However, there is no defined standard for the contents of SLA in optical networks. IEFT provides a general recommendation for service providers to implement resiliency mechanisms in their service offers by considering this tradeoff. Protection and restoration schemes are used to implement network resiliency.

There are two obvious ways of solutions to fulfill these requirements in the resiliency mechanisms. The first solution is employing a better Routing and Wavelength Assignment (RWA) algorithm for the resiliency mechanisms. Since the connection paths in resiliency mechanisms are established with the help of RWA algorithms implemented in the network, this solution specifically requires to evaluate effect of RWA algorithms on performance of resiliency mechanisms. Even if performance of resiliency mechanisms and RWA algorithms are studied separately, to the best knowledge of the author, effects of dynamic type RWA algorithms on performance of resiliency mechanisms are not yet studied. Hence, it makes difficult to decide which RWA algorithm has to be implemented in resiliency mechanisms.

The second solution is combining protection and restoration schemes to improve service performance quality in times of multiple failures. Different formats of hybrid resiliency mechanisms are thoroughly studied. But, these hybrid resiliency mechanisms are usually inefficient in times of multiple failures of SRGs. One type of hybrid resiliency mechanism that can be considered in ASON dynamic service provisioning to solve such problems is constraint-based hybrid resiliency mechanism. It can be synthesized by combining different flavors of 1+1 Dedicated Path Protection (DPP) scheme (Link-Disjoint, Node-Disjoint or SRG-Disjoint) with restoration scheme. To the best knowledge the author, constraint-based hybrid resiliency mechanisms for ASON dynamic service provisioning in times of multiple failures are not also studied yet. This research work will address these two most important subjects of solutions for fulfilling requirements of better service performance quality and resource utilization.

1.2 Objective of the Thesis

1.2.1 Main Objective

The main objectives of this research work are:

- To identify and suggest an efficient RWA algorithm, in blocking probability and network Availability, for ASON resiliency mechanisms during dynamic service provisioning.
- To improve service performance quality, such as Network Availability and Recoverability in ASON resiliency mechanisms.

1.2.2 Specific Objectives

The specific objectives of this research work are:

- To evaluate effects of widely used RWA algorithms, such as SRG-Disjoint Aware First-Fit Routing, Alternate Routing, Least Congested Routing and Load Sharing Routing algorithm coordinated with First-Fit wavelength assignment algorithm on performance of 1+1 DPP and Restoration resiliency mechanisms.
- To propose constrained-based hybrid resiliency mechanisms for multiple failures based on the RWA algorithms that perform better.
- To evaluate performances of this proposed resiliency mechanisms in terms of blocking probability, recoverability and network availability.

1.3 Methodology

To accomplish the objectives of the research work, the following methodology will be followed:

- Identify RWA algorithms suitable for dynamic ASON service provisioning
    - SRG-Disjoint Aware First-Fit
    - Alternate Routing

  - Least Congested Routing (LCR)
  - Load Sharing
- Identify target resiliency mechanism relevant to the study.
  - 1+1 Link-Disjoint DPP
  - 1+1 Node-Disjoint DPP
  - 1+1 SRG-Disjoint DPP
  - Restoration
- Asses and formulate ILPs for RWA problem and resiliency mechanisms.
- Net2Plan Simulation setup for the identified resiliency mechanisms and RWA based on Addis Ababa metro OTN backbone network of ethio telecom reference topology.
- Simulate and compare performances of RWA algorithms in 1+1 Link-Disjoint DPP and restoration schemes in terms of blocking probability and network availability.
- Identify an RWA algorithm that perform better in both resiliency Mechanisms.
- Combine the identified 1+1 DPP resiliency Mechanisms with Restoration.
- Net2Plan Simulation Setup for Combined hybrid resiliency mechanisms.
- Simulate and Compare performances of each resiliency mechanisms in terms of blocking probabilities, recoverability and Network Availability.

1.4 Scope and Limitation of the Study

To achieve the objective of this research work in intended time frame, scope and limitations of the study are specified in this section. This research work is intended to compare the identified RWA algorithms in ASON resiliency mechanisms. Performance evaluation will depend on 1+1 Link-Disjoint DPP and Restoration resiliency mechanisms since they are widely used and easy to implement, even if many options of resiliency mechanisms are available. Similarly, among many types of RWA algorithms SRG-Disjoint Aware First-Fit Routing, Alternate Routing, Least Congested Routing and Load Sharing that cooperate with the First-Fit Wavelength Assignment are the choices of this research work, because they are widely used in practice. Performance of the network is measured in terms of resource utilization and service performance quality parameters, such as blocking probability and network availability, respectively.

This research work also proposes three constraint-based hybrid resiliency mechanisms which are, 1+1 Link-Disjoint + Restoration, 1+1 Node-Disjoint + Restoration and 1+1 SRG-Disjoint + Restoration for ASON dynamic service provisioning. It considers a recovery format in which restoration will only be triggered when 1+1 DPP cannot recover the affected path. It will not consider other options, such as restoration will be triggered when either of primary or backup paths fail. The research work considers only link and SRG failure models in performance evaluation of proposed hybrid resiliency mechanisms. Link and SRG failures are dominant failure scenarios in current optical networks. Node failures are less common and relatively rare to happen. Hence, the research work assumes that the chances of node failure are neglected. It will utilize blocking probability, recoverability and availability metrics for performance evaluation of the hybrid resiliency mechanisms.

This research work will be conducted on Addis Ababa Metro OTN Backbone network of ethio telecom as a reference topology. This reference topology is selected since it has mesh interconnection of nodes which makes it suitable for studying resiliency mechanisms. The data rates of light-paths, capacity of each links and distance between each node is directly adopted from the real network topology. Since the RWA algorithms and resiliency mechanism algorithms which are the choice of this research are not distance dependent, the research will not consider the main backbone bone network of ethio telecom. The simulations of the research work are conducted on Net2Plan planning and design simulation tool.

1.5 Outcomes and Contribution of the Thesis

This research work will have three major outcomes and contributions for ASON resiliency mechanisms in dynamic service provisioning. First, the research work will assess and analyze all necessary state of the arts and its basic components that are related to ASON resiliency mechanisms and RWA algorithms involved in provisioning process. Then in its second part, the research work evaluates effects of RWA algorithm usage on performance of resiliency mechanisms. The research work contributes to identify an appropriate RWA (among the widely used one) to be used in protection and restoration resiliency mechanism under different loads of total offered traffic. It will also clearly show how the RWA algorithms play their role on resource utilization and availability of resiliency mechanisms during dynamic ASON service provisioning.

Finally, the research work will propose new constraint-based hybrid resiliency mechanisms which will be very suitable for ASON dynamic service provisioning against multiple link or SRG failures. These hybrid resiliency mechanisms will enhance recoverability and availability of the network in times of link or SRG failure risks. Hence, the research will contribute better and competent ASON resiliency mechanism options that can be stipulated in SLA contracts. In current practice, in academics and industry, the resiliency mechanisms are based on link-disjoint DPP and restoration schemes. However, this research work will propose two additional constraint-based hybrid resiliency mechanisms which are based on Node-disjoint and SRG-disjoint 1+1 DPP, and restoration schemes.

1.6 Organization of the Thesis

This thesis is organized in to six chapters. Chapter 1 describes the basic entities of the research work, such as problem statement, objective, methodology, scope and limitation, and outcomes and contribution of the research work. Chapter 2 is about literature reviews on the basic state of the arts required in this study, such as overview of ASON, RWA problem and its solutions in optical networks. Chapter 3 is about network resiliency mechanisms in ASON. It describes fault recovery schemes used to implement network resiliency mechanisms with their ILP formulations. It also presents the newly proposed constraint-based hybrid resiliency mechanisms.

Chapter 4 discusses performance evaluation methodology which is going to be used in evaluating performance of the RWA algorithms in ASON resiliency mechanisms and the proposed hybrid resiliency mechanisms. It discusses Net2Plan planning and design simulation tool, and its performance parameters that can be used in performance evaluations of the research work. Chapter 5 provides detailed performance results and discussions for performance evaluation of the RWA algorithms in ASON resiliency mechanisms and the proposed resiliency mechanisms. Finally, Chapter 6 sums up this research work. It also discusses future research directions on optical network field, specifically in the field of ASON.

Chapter Two

2. State of the Arts

This chapter provides an overview for all related concepts of ASON technology and RWA problems, on which this thesis is based. First the general concepts of ASON and its functionalities are discussed. Then, the issues related with routing and wavelength assignment problems are presented. The adaptive type RWA algorithms in ASON service provisioning, which are considered in the thesis, are presented in this chapter.

2.1 Overview of Automatically Switched Optical Network (ASON)

2.1.1 ASON Architecture

ASON architecture is defined by ITU-T G.8080 and composed of three well separated planes [6], [7]. Transport plane is a layered plane (also called data plane) and represents functional resources of a network which transport user information, control and management information from one location to another. Transport network represents a layered network, such as IP, SDH/SONET, DWDM, ATM, OTN. Control plane performs call control and connection control functions. It provides automated network intelligence which includes automatic discovery, routing and signaling. Management plane manages transport plane, control plane and the system as a whole. It also coordinates operation of all planes. The management functions provided by management plane are related to network elements, networks and services. This plane is usually less automated than control plane.

Even if each of these three planes are separate and autonomous, some interactions occur on a common underlying resource [6], [7]. Management-Transport interaction, Control-Transport interaction, and Management-Control interaction can be occurred. Management plane operations and control plane operations are autonomous to each other, that is both planes are unaware of existence of each other's plane, they see only the resource behavior. The information presented to both management and control planes is similar. Control plane information overlaps some management plane information, not all management information.

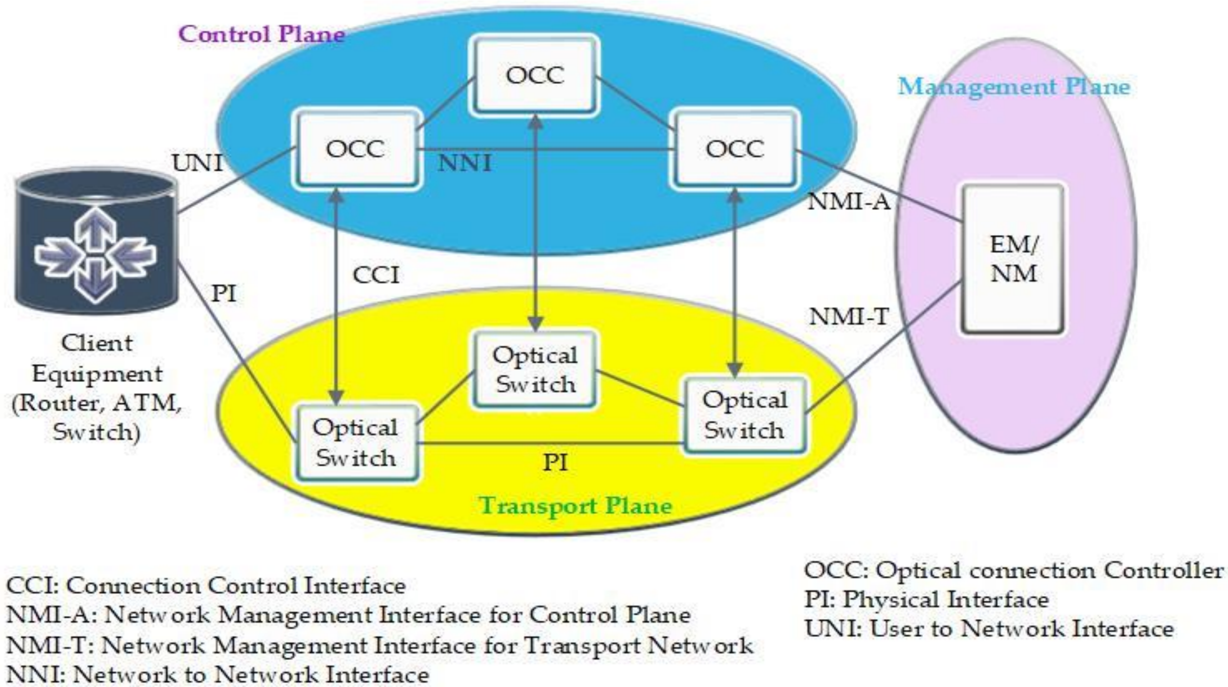

Figure 1: ASON Architecture [6]

Optical Connections

In optical transport networks, control of connectivity is important [3], [7]. Optical transport network can be described as a set of layered networks in which associations between each node are created and removed. This associations are called optical connections. ASON provides three kinds of connections based on connection establishment type.

- **Permanent connection:** It is also referred to as provisioned connection. It can be setup by management system or manual intervention. It doesn't require the control plane support and doesn't need automatic routing and signaling. It is usually static connection that could last relatively longer time, for months or years.
- **Switched connection:** it is on demand established connection. It is established by communicating end points using routing and signaling capabilities of control plane. It follows signaled connection set up. It may be accomplished by end user.
- **Soft permanent connection:** it is a hybrid connection type which is established by specifying two permanent connections at edge of a network and then setting up a switched connection between them. Here, connections are established via network generated signaling and routing protocols.

ASON control plane can support either switched connection or soft permanent connection capability in transport networks [7]. These connection capabilities can be unidirectional or bidirectional and even asymmetric types.

ASON Control Plane

The control plane of ASON is a set of communicating entities responsible for end-to-end connection set up, release and maintenance [6], [7]. It provides call and connection control. An association between end points that can support an instance of service is called call. Connection is a transport entity that can transfer information between input and output end points. Connection set up, release and maintenance are the responsibilities of connection control. Call control is used to maintain association between parties and a call may utilize any number of connections at any instant of time. The call admission function is responsible for authentication of users and checking the requested service parameters against service level specifications at beginning node. At terminating node the user will be checked if it is entitled to accept the call. Connection admission control checks for availability of sufficient resources (like wavelength, TDM channels) to admit a connection. Control plane is a key entity in ASON architecture which provides the necessary intelligence to the whole network. It offers the following functions.

Discovery Function

It provides automatic discovery of transport entities to eliminate explicit configuration activities [6], [8]. This function is proposed in ITU-T Recommendation G.7714. The discovery process involves exchange of identity attribute messages which require operation of relevant protocols. It offers neighbor, resource and service discovery functions. Neighbor discovery determines the state of local links connected to neighbors. It is useful in detecting and maintaining node adjacency as well as it is essential to track connectivity between neighbor network elements. It avoids manual interconnection configuration in NMS, except initial manual configurations.

Routing Functions

Routing is the process of selecting paths for establishment of connections in a network [6], [9]. ITU-T Recommendation G. 7715/Y.1706 specifies requirements and architecture of routing functions for establishment of connections in ASON framework. ASON routing architecture supports hierarchical, step-by-step and source-based routing paradigms, which result in different distribution of components between nodes and their interactions.

In hierarchical routing, a node contains a routing controller, connection controller and link resource manager in a routing area hierarchy [6], [9]. It involves a hierarchical relation in connection controllers of different subnetworks or routing areas in which each subnetwork has only its own topology but no knowledge about topology of other subnetworks at any hierarchical level below or above its hierarchy. Path selection starts at the top of the hierarchy and defines a sequence of subnetworks in a lower level to find a path between source and destination. The connection control process in source routing is implemented by a federation of distributed connection and routing controllers. The first connection controller in a routing area is responsible for path selection which is supported by routing controller to provide routes in routing area. The amount of routing information in step-by-step routing nodes is less when it is compared to the other routing architectures. Here, path selection is invoked at each node to obtain next link on a path to destination.

Signaling Function

It involves transport of control plane messages between ASON components [6]. Signaling protocols are required to create, maintain, restore and release connections which are essential to enable fast provisioning and recovery of services. Automatic discovery and routing functions supported by signaling schemes provide ASON network with intelligence which relieves management system from time consuming tasks concerned with manual topology updates and path selection.

Survivability Function

Survivability is a capability of a network to continue its normal operation in times of fault occurrences [6]. All three ASON functional planes are involved in survivability schemes. In transport plane protection, management plane configures protection and inform control plane about failures on transport resources as well as addition and removal of resources. In control plane protection, both working and protection are configured by control plane where source and destination controllers are only involved. The control plane functions defined by ITU-T are implemented by GMPLS protocol set which is defined by IETF.

2.1.2 Generalized Multi-Protocol Label Switching (GMPLS)

GMPLS is concerned with merging different transport networks with Multi-Protocol Label Switching (MPLS) enabled data forwarding technologies [6], [10]. Its objective is to apply a uniform control plane to any transport technologies that are based on non-packet forwarding technology. GMPLS is built on MPLS protocols on which traffic engineering is applied and implemented.

Requirements of GMPLS

Label: In GMPLS a label is a tag that identifies a switchable data stream corresponding to physical resource [11]. Therefore, in lambda switching networks (WDM) a label identifies specific wavelength and in TDM network a label identifies a specific time slot.

Multiple Types of Switching: GMPLS supports multiple types of switching that makes nodes support both packet and non-packet forwarding schemes, where switching decision is based on packet/cell, time slot, wavelength, or physical ports [10]. Hence, interfaces on GMPLS nodes can be classified in to Packet Switch Capable (PSC) interfaces, Layer-2 Switch Capable (L2SC) interfaces, TDM interfaces, Lambda Switch Capable (LSC) interfaces, Fiber-Switch Capable (FSC) interfaces.

Label switched path (LSP): It is a contiguous series of cross-connected resources (time slot, lambda, and so on) which are directly associated to labels, and capable of delivering traffic from incoming resource to outgoing resource [11]. In establishment of LSPs (sometimes called circuit, trail or light-path), end points are not necessarily points of service delivery, they could be intermediate switches needed to be connected for service delivery. It is not actually a service, it just provides service full or partial connectivity.

Bandwidth: In GMPLS transport networks, LSP is directly related to physical and switchable resources and in turn the bandwidth can only be divided up according to switching device capabilities [11].

Bidirectional of Transport Connections: Services in optical transport networks require bidirectional connectivity that can offer equal connectivity and data transfer capabilities in both directions [11].

LSP Tunneling and Hierarchies: In non-packet transport networks, since a label is associated with physical resource, GMPLS uses a natural hierarchy of switching based on granularity [11]. It allows to nest lambdas in a fiber, time slots in a lambda, packets in time slots. GMPLS LSP hierarchy allows aggregation of tunnels which can offer scalable traffic engineering and efficient bandwidth utilization in core transport networks.

Traffic Engineering (TE) Link and its Attributes: In GMPLS, the network resources available for traffic engineering path computation are modeled as TE links [10], [11]. TE link concept can be extended to cover bundles of links between two nodes, and even to LSP. TE link is the routing protocols Link State Advertisement (LSA) representation between two GMPLS nodes. It is also used in Links State Database (LSDB) to represent certain physical resources and their properties. Control plane uses TE links to establish LSP through its signaling and routing procedures. Since TE links are advertised as link ends, nodes at end are responsible for advertising attributes of TE links from their own side as they see it. TE link will not be completed and available for use until both ends are advertised and correlated. Traffic Engineering Database (TED) is a database of all TE Links and associated information which is processed by path computation algorithm to compute traffic engineered path. GMPLS TE link attributes, which are standardized for constrained-based path computation, are traffic engineering metric, administrative group, link protection type, Shared Risk Link Group (SRLG), and Interface Switching Capability (ISC) descriptor.

2.1.3 GMPLS Protocols

The building blocks of GMPLS control plane are based on the well-known signaling and routing protocols that are extended to support the operation of GMPLS [7]. The only new special protocol is a signaling protocol for link management, called Link Management Protocol (LMP).

GMPLS Signaling Protocols

GMPLS signaling protocols are used to exchange messages in control plane to establish Label Switched Paths (LSPs) within transport plane [10], [13]. Originally, there are two signaling protocols specified for GMPLS: RSVP-TE (Resource Reservation Protocol with Traffic Engineering Extensions) and CR-LDP (Constraint-based Routed Label Distribution Protocol). GMPLS doesn't specify which one of protocols has to be used, it is left to manufacturers and operators to evaluate and implement based on their interest. Further development work on the CR-LDP protocol has been halted by the IETF because it is known that only one signaling protocol is necessary.

GMPLS signaling extends MPLS-TE signaling procedures and abstract messages to cover different types of switching applications, such as TDM, wavelength switching, etc. GMPLS signaling messages (RSVP-TE messages) are encapsulated in IP datagrams addressed to next switching nodes. Since here IP transport mechanism is used without transport protocol, the signaling protocol (RSVP-TE) should handle the unreliable nature of IP data delivery. The RSVP-TE is responsible for LSP establishment, maintenance and teardown in entire ASON network.

GMPLS Routing Protocols

GMPLS routing is distribution of information that can be used for path computation to determine how LSPs will be placed in a network [10]. GMPLS extends two traditional intra-domain link state routing protocols: OSPF-TE (Open Shortest Path First extended for Traffic Engineering) and IS-IS-TE (Inter System to Inter System extended for Traffic Engineering).

OSPF-TE Routing Protocol

OSPF-TE was introduced in MPLS and then it is extended to support GMPLS because the amount of LSA information was still not enough to support non-packet transport networks [11]. GMPLS extended OSPF-TE LSA information are made to incorporate various TE link attributes for constrained-based route computation. OSPF-TE uses OSPF opaque LSA option of type 10 in which TE related advertisements are encapsulated. The OSPF is now transport mechanism to distribute TE LSAs which are flooded within the LSA source routing area. Then, TE LSAs are delivered to every OSPF-TE capable nodes in TE layer of the routing area. TE layer builds and manages TE database (TED) and produces network TE graph (switching nodes as vertex and TE links as edges). TE graph is then used to compute LSP paths.

ISIS-TE Routing Protocol

ISIS-TE GMPLS routing protocol is extended from IS-IS traditional routing protocol by adding TE features as that of OSPF-TE [11]. The main reasons for enhancement are very similar to that of OSPF-TE and their purpose is also identical. Here in IS-IS, the basic unit of information transfer is a routing information LTV (Label, Type, Value), whereas it is LSA in OSPF. Multiple LTVs can be collected together in Link State Protocol Data Units for distribution between nodes. In GMPLS, ISIS-TE information distribution is achieved through new LTVs defined for this purpose to carry the same information to that of OSPF-TE. ISIS-TE capable nodes use Link State Protocol Data Units to advertise their information in a network.

GMPLS Link Management Protocol (LMP)

GMPLS link management protocol (LMP) is defined by IETF, which runs between transport plane adjacent nodes to manage TE links [10], [16]. It specifically provides mechanisms to maintain control channel connectivity, verify physical connectivity of data links, correlate link property information, and manage and localize link failures for protection/restoration purposes in optical transport networks. Link management protocol has several distinct functional procedures defined for GMPLS control planes of ASON-enabled networks, such as control channel management, Link Property Correlation, Verifying Link Connectivity and Fault Management.

2.2 Routing and Wavelength Assignment (RWA) in ASON

According to ITU-T recommendations, ASON has two transport layers: optical layer and electrical layer [1], [17]. A common example for electrical layer path is SDH/SONET path, which is used to access SDH/SONET services and it can be groomed to optical layer. ASON optical layer consists of switching nodes or optical cross-connect (OXC) connected by WDM optical fiber links that route a signal based on wavelength of incoming signal. Since it employs wavelength routing service, ASON optical layer can be referred to as wavelength routed network. Source and sink switching nodes provide electronic-to-optical-to-Electrical conversion and vice versa (O-E-O) to connect the optical network to electronic stations. Wavelength routing enables the network with ability to identify and localize traffic flow, reusing the same wavelength in spatially disjoint network segment.

A connection needs to be set up at optical layer just like the case in circuit-switched networks, to transfer data from one source node to another destination node [1], [17]. This is performed by determining a path connection from source node to destination node and allocating single free wavelength on all traversing fiber links in the path. This all optical path is referred as light-path. The intermediate switching nodes in the path, route the light-paths using wavelength sensitive switches in optical domain. The main constraints for such wavelength routed networks are light-paths traversing the same fiber link must be on different wavelengths and absence of intermediate O-E-O conversion. The absence of intermediate O-E-O conversion constraint enables a network to accommodate rapidly increasing bandwidth, to improve reliability of the network and to simplify network management independent from modulation format and bit rate.

Effective establishment and usage of light-paths are very important since they are basic switched entities in wavelength switched optical networks [1]. Hence, efficient algorithms should be chosen to compute routes for service connections and to assign wavelengths along selected route. This phenomenon is referred to as routing and wavelength assignment (RWA) problem. RWA problem considers networks where light-path requests can be transported on different wavelengths throughout the network. Each accepted request is allocated a path with specific wavelength from source to sink. Light-paths with disjoint paths will use the same wavelength, whereas light-paths routed over the same path will be allocated to different wavelengths. The light-paths that cannot be established due to constraint on wavelength availability are called blocked.

2.2.1 Strategies of RWA in Optical Networks

The main aim of RWA algorithms is minimizing blocking probability of the network to improve network performance [18]. RWA problem strategies can be classified as static and dynamic RWA based on traffic arrivals.

Static RWA

In static strategy of RWA problem, static light-path is established between source-destination node pairs [1], [19]. Here, the traffic is static and set of connection requests are known in advance. This strategy is the case for large transport networks in which planning is made based on aggregate demand factor and future forecast value. In this case, individual requests are accommodated based on planning phase provisioned routes. In static RWA scheme, the number of light-paths will remain fixed overtime with slow traffic requirement changing time. The algorithms proposed for this static RWA problem are known as off-line algorithms.

Dynamic RWA

In this strategy, dynamic light-path is established [1], [19]. Connection requests arrive sequentially, one by one at random times with random holding time. That means light-paths are established on demand. In this dynamic scheme, light-path requirements may vary frequently overtime. So, routing is done individually for each light-path. It can be used in operational phase of a network which needs to be managed efficiently. The algorithms proposed for dynamic RWA problem are referred to as on-line algorithms. Dynamic RWA is more efficient than static in terms of blocking probability performance. It adaptively uses real time network status in route computation process.

2.2.2 Solutions of RWA Problem

There are some practical approaches that try to solve the RWA problem by partitioning the problem in to several smaller subproblems [22]. These subproblems can be solved independently using approximation techniques like multicommodity flow formulation. The multicommodity flow formulation can be combined with randomized rounding to compute routes for light-paths. Then, graph coloring techniques can be deployed for wavelength assignments. The more practicable and tractable approach is partitioning the RWA problem in to two subproblems: routing subproblem and wavelength assignment subproblem. These two subproblems can be solved either jointly in one step or separately in two steps.

2.2.2.1 One Step RWA Problem Solution

This approach tries to find optimal solution for routing and wavelength subproblems jointly [22], [27], [28]. It formulates Integer Linear Programming (ILP) model as multicommodity flow with integer flows in each link. This approach is suitable for static RWA in which light-path requests are known in advance and routing and wavelength assignment operations are performed off-line.

The generic ILP for RWA problem is formulated based on formulations which are already developed in literatures [22], [27], [28]. Assume a given network topology with a set of V nodes and E links as directed graph is denoted as $G(V, E)$, W denotes a set of wavelengths available in each link $(i, j) \in E$, D is a set of connection requests fed to the ILP, $C_{s,d} \in D$ denotes static traffic demand matrix (number of connection requests from source to destination) and $S=\{g\}$ denotes a set of shared risk group (SRG) which is identified by SRG number g. Assume α is a parameter that can be assigned highest value to maximize the number of provisioned/restored connections, and β is a parameter that can be assigned low value to minimize the required wavelength resources.

Let f_{ij} denotes the number of wavelengths needed to set up a certain set of light-paths for a given topology, and f_{ij}^{c} denotes the traffic in number of connection requests (light-path request c) from source to destination on a link (i, j) and wavelength w which takes a value of 1 if the traffic passes through the link, otherwise it will take a value of 0. Let A_c denotes the traffic request c successfully provisioned or restored from source to destination and takes a value of 1. Let λ_c^p denotes the traffic in number of primary light-path requests c between any source destination pair to set up primary paths allocated on wavelength w. Let $S(i,j,g)$ denotes SRG g where a link (i,j) belongs to. The generic ILP formulation for RWA, which can be used to drive ILPs of recovery mechanisms is written as follows:

Objective:

$$\boldsymbol{min} \quad \alpha \cdot \left(|D| - \sum_{\forall c} A_c \right) + \beta \cdot \sum_{ij \epsilon E} f_{ij} \tag{2.1}$$

Subjected to:

$$f_{ij} = \sum_{1 \le (s,d) \le V} \sum_{w=1}^{W} f_{ij}^c \qquad ; \forall (i,j) \epsilon E \tag{2.2}$$

$$f_{ij} \le W \qquad ; 1 \le (i,j) \le E \tag{2.3}$$

$$\sum_{i:(i,j)\epsilon E} f_{ij}^c - \sum_{k:(j,k)\epsilon E} f_{ji}^c = \begin{cases} \lambda_c^p, & if\ j = s \\ -\lambda_c^p, & if\ j = d \\ 0, & if\ j(! = s, d) \end{cases} \qquad 1 \le s, d, j \le V \tag{2.4}$$

$$\sum_{w=1}^{W} \lambda_c^p = \ C_{s,d} \qquad 1 \le (s,d) \le V \tag{2.5}$$

$$\sum_{1 \le (s,d) \le V} f_{ij}^c \le \ \lambda_c^p \quad , \forall (i,j) \in E \ ; 1 \le w \le W \tag{2.6}$$

$$f_{ij}^c = \begin{cases} 1, & if\ traffic\ \ c\ from\ s\ to\ d\ passes\ through\ a\ link\ (i,j) \\ 0, & otherwise \end{cases} \tag{2.7}$$

$$\lambda_c^p = \begin{cases} 1, & if\ traffic\ \ c\ from\ s\ to\ d\ allocated\ on\ wavelength\ w \\ 0, & otherwise \end{cases} \tag{2.8}$$

The objective function expressed in equation (2.1) in its first term tries to minimize the number of failed attempts of connection requests (blocking of requests) or maximize the number of successfully provisioned connection requests. The second term tries to minimize the number of wavelengths required to set up connection requests. Equation (2.2) computes load or number of light paths traversing a link (i,j) for provisioned connections which should not be exceeded the number of available wavelengths W in link (i, j) as shown in eq. (2.3). Eq. (2.4) is flow conservation constraint for connection requests. The flow conservation constraint tries to maintain the condition of traffic flows at the source node, which ensures the outgoing traffic volume from source node is equal to the incoming traffic volume, λ_c^p. It also maintains the condition of traffic flows at intermediate nodes, which ensures all the traffic coming in is always coming out (not dropped at the node). The flow conservation also maintains the traffic flow at destination nodes, which ensures the outgoing traffic is equal to the incoming traffic, $-\lambda_c^p$. Eq. (2.5) is a constraint that satisfies the requirement of the total number of traffic demands between source destination pairs should be equal to the total number of light-path requests which are successfully provisioned and allocated on wavelengths, λ_c^p. Eq. (2.6) is a wavelength continuity constraint which ensures a wavelength can be assigned to only one light-path in the links that traverses from source to destination. That means, the wavelength used at the source node should be the same to that of the wavelength used at the destination node and there is no wavelength conversion in between. Equations (2.7) and (2.8) are binary constraints.

ILP formulation for static RWA problem is usually solved by feeding it to optimization software (such as CPLEX and GLPK) [22], [27], [28]. However, the solution is NP-complete and it is difficult to find optimal solutions in polynomial times for large scale networks. Hence, ILP based RWA problems are used for relatively small scaled networks where time is not critical issue. In dynamic RWA problem, traffic demand is not known in advance and it makes it impossible to find optimal solution for RWA problem.

2.2.2.2 Two Steps RWA Problem Solution

Light-path connection request in ASON requires establishment of a route and then allocation of wavelength [19], [20]. RWA of light-paths in optical networks are usually done in two steps in order to minimize complexity of RWA problem. In the first step, it tries to find a route between source-destination node pairs and in the second step, wavelength assignment for route links is performed.

Routing Subproblem in Optical Networks

Routing problems in optical networks now are solved roughly by three approaches [20]. **Fixed Routing (FR):** It always selects a fixed and precomputed route for a source-destination node connection request [21] [22]. Even if FR routing is simple to implement and has lower computational complexity, it can result in high blocking probability. Here, a simple example is fixed shortest path approach which uses standard shortest path algorithms, such as Dijktra's algorithm or Bellman-Ford algorithm, where any connection between nodes is established in predetermined route. A connection can be blocked when there is no available wavelength in any of the shortest path links or when there is no common wavelength on all links of the shortest path.

Fixed-Alternate Routing (FAR): it considers maintaining a routing table on each node that contains ordered list of multiple fixed routes to their destination node [21], [22]. The routes may be listed as first shortest path route, second shortest path route, third shortest path route and so on. Each listed route is statically computed and should be edge-disjoint (link-disjoint) to improve fault tolerance. For every connection request, the source node tries to establish a connection on each of routes in the routing table in sequence until valid route is found. If a valid route cannot be found in the routing table, the connection request will be blocked and lost. FAR simplifies control of light-path setting up and tearing down with some degree of fault tolerance up on link failures. When a link fails, an alternative route can be used to recover the service. It also significantly reduces connection blocking probability when compared to fixed routing.

Adaptive Routing (AR): In this scheme, a route from a source node to destination node is selected dynamically according to network state [22]. The set of all connections that currently in progress determine the network state. Route selection is based on current network state information and path selection policies, such as least-cost path first (Shortest path first) or least congested path first (LCP). Adaptive least cost path is a form of adaptive routing in which the least cost path between source-destination pair is selected for a connection request. If multiple paths exist with the same cost, one of them will be chosen randomly. If there is no route between source and destination, the connection request will be blocked. AR has lowest blocking probability when compared to FR and FAR. Adaptive routing requires extensive support from management and control plane protocols to regularly update its routing table. Least congested path routing is another form of adaptive routing which requires a sequence of routes to be preselected between source and destination. One of these predetermined routes will be selected for connection requests. The congestion of a link can be measured by the number of available wavelengths on links. Links with fewer number of wavelengths considered as congested.

Wavelength Assignment Subproblem

For dynamic traffic in which light-paths are arrived one at a time, heuristic method must be used to assign wavelengths to light-paths [22]. In such methods, the number of wavelengths is assumed to be fixed which is a practical scenario. A large number of heuristics are proposed for wavelength assignment problem which can be combined with different routing mechanisms. Among these first fit, random, least used and most used wavelength assignments are more commonly used algorithms.

Random Wavelength Assignment: It searches for available set of all wavelengths randomly on each link of selected route and assigns one of the available wavelengths with uniform probability [22]. Such type of algorithm does not require the global network information.

First-Fit Wavelength Assignment: In this approach all wavelengths are ordered in index of numbers [21], [22]. The lower indexed wavelength will be considered before the higher indexed one, in searching for available wavelengths. The first available wavelength is then selected. It doesn't require the global network information. The computation cost is lower than that of random wavelength assignment because it doesn’t search for all available wavelengths on each link. It is based on the idea of packing all in-use wavelengths to lower end of wavelength space in order to make continuous longer paths available towards higher end of wavelength space. It is preferred in practice, since it performs well in terms of blocking probability and fairness, and it has low complexity and small computational overhead.

Least-Used Wavelength Assignment: in this algorithm, wavelengths that are least used in a network are selected [21], [22]. Its purpose is to balance load over all wavelengths. This algorithm will break long wavelength paths and allows only connection requests that traverse small number of links to be established in the network. Since it requires the global network state information to compute least used wavelengths, it introduces additional signaling overhead. It has worse performance than random wavelength assignment. It also needs additional storage and computational cost, that makes it not preferred in practice.

Most-Used Wavelength Assignment: it selects the most used wavelength in a network [21], [22]. It also needs the global network state information to compute wavelengths which are most used. Even if communication overhead, storage and computational cost are similar to least used wavelength assignment, it performs better than least used. It also slightly outperforms first-fit wavelength assignment since it packs connections into fewer wavelengths to save less used wavelengths spare capacity.

2.2.3 RWA Algorithms for ASON Dynamic Provisioning

ASON needs intelligent dynamic RWA algorithm to improve its practicability to perform its dynamic provisioning requirement [23]. In RWA algorithms of ASON, the status of the whole network should be detected in real-time, network resources should be assigned in more reasonable manner and network load should be balanced efficiently. This in turn improves network blocking probability and resource utilization. Since ASON involves application of new technologies, such as wavelength conversion and optical exchange, the route computation environment in ASON is more complicated than the usual optical transport networks. Hence, RWA algorithms designed for traditional optical networks may not work efficiently for ASON due to their limitations in reasonable resource assignment and sufficient algorithm flexibility.

GMPLS control plane provides light-path control mechanisms to efficiently set up and tear down light-paths [24], [25]. The routing protocols of control plane must include flexible, fast and reliable mechanisms to disseminate and update the topology and available resource information throughout the network. ASON specifications specifically recommend hierarchical routing for implementation of routing protocols and algorithms which guarantees network scalability. But, source routing is the most commonly used in which routes are calculated on source nodes based on routing information contained in their network state database. It is due to its ability of fast and efficient set up of optical connections and its convenient realization in practical optical networks.

Accordingly, it is possible to produce different types of routing algorithms based on the routing approaches described above [29]. Some of widely used adaptive routing algorithms in ASON are SRG-Disjoint Aware First-Fit Routing, Alternate Routing, Least Congested Routing (LCR) and Load Sharing. All of these routing algorithms are based on source-based k-shortest path routing which computes k number of alternate routes for each connection request. That means, k alternative shortest paths are computed and populated in source node as a routing table for each connection requests based on current state of the network. These algorithms deploy some criteria to select a route among these k alternative routes.

2.2.3.1 SRG-Disjoint Aware First-Fit Routing Algorithm

Shared Risk Group (SRG) can be defined as a risk or vulnerability that makes a set of links or nodes to fail simultaneously [29], [30]. For example, if the risk is fiber conduit cut, all fibers in the conduit will be cut simultaneously together with light-paths traversing. For a given set of SRGs defined in a network, SRG-Disjoint Aware First-Fit routing computes k shortest alternate paths on source node and populate them as a routing table. Then, the algorithm computes iteratively the number of SRG-route pairs that the route overlaps with respect to already existing light-paths. That means the decision criteria to select a path among the lists is minimum number of SRG overlaps which is obtained by iterating over all SRGs on light-paths traversing between the same source-destination pairs. So, the first available path with minimum number of SRG overlaps will be chosen. If there is no available resource (wavelength) on selected route, the next route with minimum SRG overlaps will be searched in the lists of alternative paths.

2.2.3.2 Alternate Routing Algorithm

Alternate routing algorithm also computes k-shortest paths for each source-destination pair demands in the network [29]. Here, each demand has a precomputed and ordered list of k-shortest paths. When a demand arrives at source node, the first available path among the k-shortest path lists will be selected. If selected route is not available the next available path will be searched in the list. A request is blocked only if all listed paths are unavailable.

2.2.3.3 Least Congested Routing (LCR) Algorithm

LCR computes k-shortest paths for each source-destination connection requests on source node and produces a list of paths (not ordered) as routing table [29], [31]. In this algorithm, choosing a path for a connection request depends on current network state called congestion level of the path. LCR measures congestion level for each admissible path. Path congestion is a measure of idle capacity or number of free wavelengths in traversed links. The larger the number of free wavelengths (idle capacity) the lower congested is the path. On the arrival of connection request, congestion level (number of free wavelengths) of all links along the path are collected first. Then, connection request is established on the path with lower congestion (larger number of free wavelengths). If two paths have the same level of congestion, a path with smaller hop count is selected. In the case of paths with the same congestion level and number of hop counts, one of the paths will be selected arbitrary.

2.2.3.4 Load Sharing Routing Algorithm

This routing algorithm is based on popular approximation techniques in loss networks called reduced load approximations [29]. Load Sharing routing algorithm computes k-shortest paths for each source-destination connection requests. The algorithm selects one of these listed paths randomly with probability p proportional with carried traffic. The drawback of this algorithm is, if selected path is not available, the connection request will be just dropped immediately. The other alternative paths will not be searched even if the paths are free and available. Hence, pure load sharing is not used in practical networks other than theoretical interests. LCR is one of improvements of load sharing model by considering current network state.

All of these routing algorithms work with First-Fit wavelength assignment algorithm. It is preferred in practice, since it performs well in terms of blocking probability and fairness, and it has low complexity and small computational overhead.

Chapter Three

3. Network Resilience Mechanisms in ASON Service Level Agreement

Today, there is an increasing QoS requirement in Internet world [32]. Telephone customers served on high reliable networks expect the same level of reliability for their critical and prioritized Internet traffic services. For instance, IP network can be used to deliver bundled services that include performance sensitive applications, such as voice and video, as well as best effort data services. In order to provide a QoS in such multi-service environment, service differentiation is necessary. Differentiated Service (DiffServ) is a QoS implementation of IP network. It provides differentiated and assured delay, jitter and loss commitments for different Class of Services (CoS) on the same IP network. Even if the GMPLS control plane of ASON is IP based, the massive traffic increment and flexibility introduced by GMPLS control plane and optical transport plane have made IP layer QoS control mechanisms insufficient. Hence, it is required to implement new integrated techniques which can satisfy communication quality on both transport plane and control plane. Resiliency of a service is one of the issues needed to be defined strictly on Service Level Agreement (SLA) of the GMPLS enabled OTN or ASON networks.

3.1 SLA in Optical Networks

Service Level Agreement (SLA) is an official contract between service provider and its customer [4], [10]. It contains both technical and non-technical terms and conditions. The detailed technical specification about the services to be delivered are called Service Level Specifications (SLS). SLS contains parameters with corresponding values to define characteristics of traffic flow and nature of services to be offered in a network. The contents of the SLA are not yet standardized, but some interesting proposals are published as Internet drafts by IETF for IP networks. Even though there are no defined SLA standards that can be adapted to specific needs of optical networks, service providers are expected to offer a variety of service levels by considering the tradeoff between network utilization (cost) and service interruption time. Hence, service providers have started to include service resilience or survivability mechanism in their SLAs for customers served on ASON networks. For this purpose, a new definition of service traffic in terms of recovery mechanisms based on protection and restoration levels is needed.

3.2 Network Resiliency Strategy in Optical Networks

Network resiliency or survivability is defined as the ability of a network to continue providing services, even after failure occurrence [33], [34]. A complete survivability mechanism includes fault detection, localization, notification and migration or recovery steps. In order to perform recovery mechanisms, first fault has to be detected by the layer or node closest to the failure. Then, network nodes communicate each other to localize the fault on nodes or links and notify other nodes about the failure. Then, fault recovery mechanisms will be adopted to release failed node or link. Fault recovery is the most important issue in survivability strategy.

3.2.1 Fault Recovery Mechanisms

The concept of recovery refers to those actions executed in order to recover traffic affected by failures in a network [33], [35]. Depending on the time scale where spare capacity is allocated, there are two types of fault recovery mechanisms: protection and restoration.

3.2.1.1 Protection Schemes

In protection, redundant backup network resources (routes and wavelengths) are preplanned, precomputed and reserved in advance [34], [36]. That means, protection schemes do not need any information update on network topology and resources after a failure has occurred. This mechanism can switch the traffic from primary path to a backup path as soon as possible. The protection switching time is fast, usually less than 50ms, in which impact of the failure can be ignored. But, resource utilization in protection scheme is inefficient since it requires pre-allocated resources for its backup path. Protection schemes can be dedicated or shared path depending on configuration of backup resources.

Dedicated Path Protection (DPP) Schemes

In dedicated path protection, a primary path and an end-to-end backup path is established, and resources are assigned at connection set up time [35], [36]. DPP can be configured in two types: 1+1 DPP and 1:1 DPP. 1+1 DPP employs precomputed and pre-allocated dedicated backup path to certain primary path. The two paths are used in parallel, that is traffic is sent along both paths simultaneously and receiving node selects the traffic from only one of the paths based on some selection criteria. 1:1 DPP also uses pre-allocated and precomputed dedicated backup path protection for a certain primary path. But in 1:1 DPP, the traffic on primary path is sent along backup path only when the primary path fails. That means, traffic on primary path is switched to backup path after occurrence of a failure.

Shared Path Protection (SPP) Schemes

In shared path protection schemes, backup paths are precomputed and sufficient resources for single link failure are pre-allocated [35], [37]. These backup paths are assigned to specific shared protection paths only after occurrence of failure. One or more backup paths may be shared by many primary paths depending on the configuration requirement. There are many different ways of sharing backup path resources.

In 1: N SPP scheme, N primary and 1 backup resource paths are preassigned. That means, there is only one shared backup protection path for N primary working paths along overlapping links. If any of primary paths fail, the traffic will be switched to backup path with some coordination mechanisms. M:N SPP ($M < N$) is a general case of 1:N protection, where M shared backup paths are predefined to protect N primary working paths. Since several working paths are protected by shared backup systems, it is better in efficiency of network resource utilization. However, this improved resource utilization leads to high signaling overhead and in turn increased recovery time (usually over 100ms).

Generally, 1+1 DPP is usually employed in practice by network operators [35], [37]. This is due to the fact that 1+1 protection is easy to implement and it has low recovery time. Since it deploys dual simultaneous transmission of traffic over primary and backup paths, it has fastest recovery time. On the contrary, when it is compared to unprotected path, it requires 100% redundancy of resources (twice the amount of network resource). This protection scheme is being widely used in automatic protection switching for high availability of real-time services.

Disjoint Path Techniques in 1+1 DPP

In practice, fiber bandwidth and node capacity are increasing rapidly [29], [38]. A single failure on a fiber link will cause the interruption of many services of customers. Hence, service providers are considering disjoint path techniques in their 1+1 DPP to enhance survivability of network that can minimize communication loss. This technique requires primary and backup paths to be set up without sharing the same links or SRGs or even nodes between source and destination nodes.

1+1 DPP can be configured in different disjoint forms depending on constraints employed in a path. It can be Link-Disjoint, Node-Disjoint or SRG-Disjoint 1+1 DPP. In 1+1 Link-Disjoint DPP, primary path doesn't share any common link with backup path from source to destination. In 1+1 Node Disjoint DPP, primary path doesn't share any common node from source to destination. Similarly, in 1+1 SRG-Disjoint DPP, primary path will not share any common SRG from source to destination. Here, it is obvious that a set of link-disjoint paths is a subset of node-disjoint paths. The set of link-disjoint paths is also a subset of SRG-disjoint paths. That means, if primary and backup paths in 1+1 DPP configuration are node-disjoint or SRG-disjoint, they are also link-disjoint.

3.2.1.2 Restoration Schemes

Restoration is a mechanism of fault recovery which computes and establishes backup paths dynamically after occurrence of failure, it doesn't use pre-allocated backup resources [10], [34]. It uses GMPLS control plane routing algorithm to obtain a new end-to-end backup path to bypass failed nodes or links. In this scheme, the real-time network topology and resource state information are required to compute the required backup paths. In restoration schemes, primary paths are set up without additional protection configuration. Restoration mechanism is relied on signaling protocols to coordinate switching actions during recovery.

In restoration scheme, there will not be any signaling and restoration bandwidth reservation before failure [8], [10], [35]. The available spare resource or capacity is reserved as resource pool. This resource pool is used in a first-come-first-served manner which implies service recovery is not directly guaranteed. There is always a tradeoff between available spare resource and blocking probability of recovered services. Resource utilization of restoration is better than that of protection schemes, since it doesn't require pre-allocated backup resources for each working path. Since restoration requires more signaling and network state update information to compute backup paths in time of failures, switching time is longer than that of protection. The switching time for restoration mechanism will take several hundred milliseconds (usually over 200ms), depending on size of network topology.

3.2.2 ILP Formulation of Recovery Mechanisms

In practice, recovery routes for static or dynamic connection requests are computed and resources (wavelengths) are assigned with the help of RWA algorithms [22], [27], [28], [38]. Hence, it is possible to drive the ILP formulations of resiliency mechanisms from ILP formulation of RWA by incorporating necessary constraints.

ILP formulations of recovery schemes are based on formulations which are already developed in literatures [22], [27], [28], [38]. Assume a given network topology with a set of V nodes and E links as directed graph is denoted as $G\ (V,\ E)$, W denotes a set of wavelengths available in each link $(i,j)\ \in E$, D is a set of connection requests fed to the ILP, $C_{s,d} \in D$ denotes static traffic demand matrix (number of connection requests from source to destination) and S={g} denotes a set of shared risk group (SRG) which is identified by SRG number g. Assume α is a parameter that can be assigned highest value to maximize the number of provisioned/restored connections, and $\beta,\ \gamma$ are parameters that can be assigned low value to minimize the required wavelength resources in primary and backup paths respectively.

Let $p_{ij}\ and\ b_{mn}$ denote the number of wavelengths needed to set up primary and backup light-paths respectively for a given topology, and $p_{ij}^{c}\ and\ b_{mn}^{c}$ denote the primary and backup traffic in number of connection requests (light-path request c) from source to destination on a link $(i,j)\ or\ (m,n)$ respectively, and wavelength w which takes a value of 1 if the traffic passes through the link, otherwise it will take a value of 0. Let A_c denotes the traffic c successfully provisioned or restored from source to destination and takes a value of 1. Let λ_c^p denotes the traffic in number of light-path requests c between any source-destination pair to set up paths allocated on wavelength w. It represents the number of light paths which are successfully provisioned and assigned on a wavelength w. Let $S(i,j,g)$ denotes SRG g where a link (i,j) belongs to.

ILP Formulation for Dedicated Path Protection

In 1+1 DPP, it is required to route two light-paths (2*$C_{s,d}$) between source-destination pairs (s,d), since traffic is sent on both protection and primary paths. ILP formulations for different flavors of 1+1 DPP (Link-Disjoint, Node-Disjoint and SRG-Disjoint) are very similar, the only difference is the application of constraints in formulations.

ILP for 1+1 Link-Disjoint DPP

Objective:

$$min \quad \alpha \cdot \left(|D| - \sum_{\forall c} A_c \right) + \beta \cdot \sum_{ij\epsilon E} p_{ij} + \gamma . \sum_{mn\epsilon E} b_{mn} \tag{3.1}$$

Subjected to:

$$\sum_{i:(i,j)\epsilon E} p_{ij}^{c} - \sum_{k:(j,k)\epsilon E} p_{ji}^{c} = \begin{cases} \lambda_c^p, \ if\ j = s \\ -\lambda_c^p, \quad if\ j = d \\ 0, \ if\ j(! = s, d) \end{cases} \quad 1 \le s, d, j \le V \tag{3.2}$$

$$\sum_{m:(m,n)\epsilon E} b_{mn}^{c} - \sum_{k:(n,k)\epsilon E} b_{nm}^{c} = \begin{cases} \lambda_c^p, \ if\ n = s \\ -\lambda_c^p, \ if\ j = d \\ 0, \ if\ n(! = s, d) \end{cases} \quad 1 \le s, d, n \le V \tag{3.3}$$

$$\sum_{w=1}^{W} \lambda_c^p = 2 * C_{s,d} \qquad 1 \le (s, d) \le V \tag{3.4}$$

$$p_{ij} + b_{mn} \le W \quad 1 \le (i, j) \le E, 1 \le (m, n) \le E \tag{3.5}$$

$$p_{ij} = \sum_{1 \le (s,d) \le V} \sum_{w=1}^{W} p_{ij}^{c} \qquad ; \forall (i, j)\epsilon E \tag{4.6}$$

$$b_{mn} = \sum_{1 \le (s,d) \le V} \sum_{w=1}^{W} b_{mn}^{c} \qquad ; \forall (m, n)\epsilon E \tag{3.7}$$

$$\sum_{1 \le (s,d) \le V} p_{ij}^{c} + \sum_{1 \le (s,d) \le V} b_{mn}^{c} \le \lambda_c^p \quad \forall (i, j), (m, n) \in E\ ; 1 \le w \le W \tag{3.8}$$

$$p_{ij}^{c} = \{0,1\} \qquad \forall (i, j) \in E, \quad 1 \le (s, d) \le V \tag{3.9}$$

$$b_{mn}^{c} = \{0,1\} \qquad \forall (m, n) \in E, \quad 1 \le (s, d) \le V \tag{3.10}$$

$$\lambda_c^p = \{0,1\} \qquad \forall (i, j), (m, n) \in E; \ 1 \le (s, d) \le V; \ 1 \le w \le W \tag{3.11}$$

Eq. (3.1) is objective function which tries to minimize number of failed attempts of connection requests (blocking of requests) or maximize number of successfully provisioned connection requests in its first term. The second term tries to minimize number of wavelengths required to set up connection requests on primary path. The third term tries to minimize number of wavelengths required to set up connection requests on backup path. Eqs. (3.2) – (3.11) are constraints applied to objective function.

Eq. (3.2) and eq. (3.3) are flow conservation constraints on primary and backup paths. These equations maintain traffic flow at source node, the difference between the incoming traffic volume and outgoing traffic volume is λ_c^p. The outgoing traffic volume on source node is λ_c^p. The equation also maintains traffic flow on intermediate nodes. Outgoing traffic volume and incoming traffic volume is equal on intermediate nodes. The flow conservation constraint tries to maintain the condition of traffic flow at destination node. The difference between incoming traffic volume and outgoing traffic volume is $-\lambda_c^p$, which is incoming traffic volume at destination node.

Eq. (3.4) is a constraint that satisfies the requirement of the total number of light-paths that are successfully provisioned and allocated on a wavelength, λ_c^p which should be equal to twice the total number of traffic demands between source-destination pairs ($2 * C_{s,d}$). Eq. (3.6) and eq. (3.7) compute load in number of wavelengths traversing links (i, j) and (m, n) to set up primary and backup paths, respectively. Eq. (3.5) restricts the total number of wavelengths used to provision primary and backup paths not to exceed the total number of available wavelengths, W in the respective links. Eq. (3.8) ensures wavelength continuity as well as link-disjoint requirement of primary and backup paths. A wavelength can be assigned to only one light-path in links that it traverses from source to destination, no wavelength conversion in between. This constraint can also prohibit primary and backup paths not to exist on the same links from source to destination at the same time, only one path can exist on a link. Eqs. (3.9) – (3.11) express range of values to the respective variables, which are binary.

ILP for 1+1 Node-Disjoint DPP

ILP formulation for 1+1 Node-Disjoint DPP is the same as that of 1+1 Link-Disjoint DPP. Their difference is the inclusion of the following node-disjoint constraints at the end of 1+1 Link-Disjoint ILP formulation to produce 1+1 Node-Disjoint ILP.

$$\sum_{1 \le (s,d) \le V} p_{kj}^c + \sum_{1 \le (s,d) \le V} b_{kn}^c \le \lambda_c^p \;\; \forall k(\, != s), j, n \in V \tag{3.12}$$

$$\sum_{1 \le (s,d) \le V} p_{ik}^c + \sum_{1 \le (s,d) \le V} b_{mk}^c \le \lambda_c^p \;\; \forall k(\, != d), i, m \in V \tag{3.13}$$

Eq. (3.12) and eq. (3.13) ensure node-disjoint requirement of primary and back up paths. The equations express primary and backup paths are expected to be node-disjoint (should not share the same nodes) from source to destination, except at source and destination nodes which are common points for end-to-end path set up.

ILP for 1+1 SRG-Disjoint DPP

ILP formulation for 1+1 SRG-Disjoint DPP protection contains all equations in 1+1 Link-Disjoint DPP ILP, from eq. (3.1) to eq. (3.11). And the following SRG-Disjoint constraint is added at the end.

$$S(i,j,g) + S(m,n,g) \leq 1 \qquad \forall (i,j)! = (m,n) \in E \tag{3.14}$$

Eq. (3.14) ensures SRG-disjoint requirement of primary and back up paths. The equation expresses primary and backup paths are expected to be SRG-disjoint (should not share the same SRGs) from source to destination.

ILP Formulation for Restoration

The formulation of ILP for restoration resiliency mechanisms is the same as that of the RWA ILP. It can be formulated as follows, based on formulations which are already developed in literatures [22], [27], [28], [38].

Objective:

$$min \quad \alpha \cdot \left(|D| - \sum_{\forall c} A_c \right) + \beta \cdot \sum_{ij\epsilon E} p_{ij} \tag{3.15}$$

Subjected to:

$$\sum_{i:(i,j)\epsilon E} p_{ij}^{c} - \sum_{k:(j,k)\epsilon E} p_{ji}^{c} = \begin{cases} \lambda_c^p, \ if\ j = s \\ -\lambda_c^p, \quad if\ j = d \\ 0, \ if\ j(! = s,d) \end{cases} \quad 1 \leq s,d,j \leq V \tag{3.16}$$

$$\sum_{w=1}^{W} \lambda_c^p = C_{s,d} \qquad 1 \leq (s,d) \leq V \tag{3.17}$$

$$p_{ij} \leq W \quad 1 \leq (i,j) \leq E \tag{3.18}$$

$$p_{ij} = \sum_{1 \leq (s,d) \leq V} \sum_{w=1}^{W} p_{ij}^{c} \qquad ; \forall (i,j)\epsilon E \tag{3.19}$$

$$\sum_{1 \leq (s,d) \leq V} p_{ij}^{c} \ \leq \lambda_c^p \quad \forall (i,j) \in E\, ; 1 \leq w \leq W \tag{3.20}$$

$$p_{ij}^{c} = \{0,1\} \qquad \forall (i,j) \in E, \quad 1 \le (s,d) \le V \tag{3.21}$$

$$\lambda_{c}^{p} = \{0,1\} \qquad \forall (i,j),(m,n) \in E; \;\; 1 \le (s,d) \le V; \; 1 \le w \le W \tag{3.22}$$

Eq. (3.15) is the objective function which tries to minimize the number of failed attempts of connection requests in its first term. The second term tries to minimize the number of wavelengths required to set up connection requests on primary path. Eqs. (3.16) – (3.22) are constraints applied to the objective function.

Eq. (3.16) is flow conservation constraints on primary paths. Eq. (3.17) satisfies the requirement of traffic demand and light-paths provisioned on specific wavelengths between source-destination pairs. Eq. (3.19) computes the number of wavelengths used to set up primary paths. Eq. (3.18) ensures the number of wavelengths used in primary paths not to exceed the total number of available wavelengths in a link. Eq. (3.20) is for wavelength continuity in primary paths. Eq. (3.21) and eq. (3.22) express range of values of the respective variables, which are binary.

ILP formulation for resiliency mechanisms in static traffic is usually solved by feeding it to optimization software (such as CPLEX and GLPK) [22], [27], [28], [38]. However, the solution is NP-complete and it is difficult to find optimal solutions for large scale networks. Since the traffic is unknown in advance in dynamic traffic, it is impossible to find optimal solution for ILPs of resiliency mechanisms. Hence, in practice (either static or dynamic traffic) heuristic type algorithms are usually used, which try to solve the problems iteratively.

3.3 Effect of RWA Algorithms on the Performance of Resiliency Mechanisms

The research works conducted till now focus on performance of resiliency mechanisms and RWA algorithms separately, at least to the best knowledge of the author. Protection and restoration resiliency mechanisms are thoroughly studied in different research works like [34]-[38], as discussed in this chapter. The research works claim that 1+1 DPP has fastest recovery, but highest blocking probability, and restoration has lower blocking probability, but longer recovery time.

There are also some researches that specifically study RWA algorithms in optical networks. The research work in [17] analyzes performance of LCR rule in WDM mesh networks with and without wavelength convertors. The research work compares blocking probability in LCR with or without the availability of wavelength converters in the service route. The research uses a fully connected WDM mesh network with 7 nodes, 30 wavelengths in each link. The result shows that blocking probability in both cases increases as traffic load increases. The network with wavelength converter capability shows lower blocking probability when it is compared to that of non-wavelength converting capability.

The research work in [18] proposes adaptive Alternate Routing for WDM networks with presence of wavelength converters. It also analyzes performance the proposed routing with regard to factors, such as number of converters, load conditions, traffic patterns, network topologies, and number of alternate paths. The result shows that at lower load, there is significant performance gain when number of k-shortest alternative paths increased instead of employing more wavelength converters. At moderate to high loads, employing some wavelength converters is beneficial instead of deploying all of nodes with wavelength converters. It also shows that using small number of k alternative paths is better than deploying all nodes with wavelength converters and fewer alternative routes together.

The research work in [22] compares wavelength assignment algorithms in fixed routing algorithm. The result shows that Most-Used wavelength assignment has best blocking performance at low loads and Mean-Sum wavelength assignment has best blocking performance at higher loads. The result also shows that other wavelength assignment algorithms are not too far from the performance of Most-Used and Mean-Sum. It also compares computational complexity of wavelength assignment algorithms which shows First-Fit and Random wavelength assignments are simplest. The research work also compares blocking probability of adaptive routing and fixed routing algorithms that use First-Fit wavelength assignment algorithm. The result shows that adaptive routing algorithms performs better than that of fixed routing.

Researches about effect of RWA algorithms usage on performance of resiliency mechanisms are not available yet, to the best knowledge of the author. However, the criteria employed in RWA algorithms to select the best route among computed k-shortest routes have their own influence on resource utilization and availability of resiliency mechanisms in ASON dynamic service provisioning. Hence, this research work will evaluate the effect of the RWA algorithms on performance of the resiliency mechanisms.

3.4 Hybrid Resiliency Mechanisms for ASON Dynamic Provisioning

Protection and restoration mechanism are not mutually exclusive, they can coexist jointly [10], [35]. The choice of protection and restoration schemes for different level of services can be based on criteria, such as robustness, recovery time and resource sharing. When multiple failures occur simultaneously that can affect both working and protection paths, protection scheme cannot recover the service. In this case, restoration scheme is needed to compute restoration path to recover the service. Hence, it is required to combine advantages of restoration and protection schemes to obtain better service performance quality with fair network resource utilization.

Reverting/Non-Reverting Characteristics of Protection Schemes

Protection schemes can be configured as reverting or non-reverting modes [22]. In both reverting and non-reverting modes, if a failure occurs on a primary path, traffic will be switched to backup path automatically. In reverting mode, traffic is switched back to its original primary path after failure on primary path is repaired. In non-reverting mode, traffic stays on backup path until it fails even if the fault on primary path is cleared. The effect of reverting/non-reverting characteristics is very visible in shared path protection (SPP) techniques. Since backup path is shared among multiple primary paths, backup paths have to be released as soon as failure on primary path is repaired to make it usable for protecting other primary paths in case another failure will occur.

Reverting mode interrupts traffic twice, interruption of traffic when traffic is switched to backup path when a failure occur and another interruption when switching the traffic back to its original primary path after the fault is repaired [22]. These interruption times are longer in SPP schemes. DPP schemes can also be configured as reverting or non-reverting modes. The only disadvantage of configuring DPP schemes as reverting mode is traffic will be interrupted twice. But, this interruption time is very short when it is compared to that of SPP schemes. Since reverting mode in DPP schemes helps the network to restore to its initial and original state after fault is cleared, reverting mode enables network operators to simplify network control and management.

Double Failure Recovery

Failure recovery mechanisms discussed in Section 3.2.1 are specifically designed to recover connection paths against single failures, except restoration scheme. Even if single failure (link or SRG failure) are most common failures on optical networks, it is becoming very necessary to consider multiple failures (at least double failures) in design of resilience mechanisms to enhance availability of a network. Double failure refers to occurrence of a second failure on another link or SRG while first failure on a link or SRG is under maintenance.

Protection resiliency mechanisms will not guarantee full protection against double failures. There will be a high probability of a second failure to affect the momentarily unprotected path. Various research works propose solutions for complete or 100% recoverability in the cases of simultaneous dual failures. The research in [40] extends protection resiliency mechanism against single failures to a mechanism that can fully recover dual simultaneous link failures. This proposed design requires triple spare capacity when it is compared to single failure-based mechanisms. Even if the design can provide a complete recovery from dual failures, its resource utilization is very poor. Simultaneous dual link failures can occur in a network at any time, but the probability of occurrence is not as frequent as single link failures. Hence, it is required to recover the second failure when it happens rather than dedicating protection path all the time.

A best solution to achieve recovering against double failures is combining protection and restoration schemes together. The combination of protection and restoration resiliency mechanisms can be referred to as hybrid resiliency mechanism. Many research works are proposed about hybrid resiliency mechanisms against dual failures. The research work in [41] claims that dual link failures can be recovered using restoration mechanism alone. Restoration resource utilization is better than that of protection schemes, but its ability to prove 100% recoverability against dual failures is very low at higher network loads. Therefore, the research proposes a hybrid resiliency mechanism which aims to recover the first failure with protection schemes and the second failure with restoration schemes. It proposes SPP scheme combined with restoration scheme.

In practice, the most commonly used hybrid resiliency mechanism is the combination of DPP and Restoration. In this approach, paths established for DPP are expected to be link-disjoint. The main concern here is, to be able to proceed restoration mechanism when protection is unable to recover the fault. Hybrid resiliency mechanisms based on link-disjoint DPP and restoration are thoroughly studied in different research works. The research work in [39] conducts a research on resiliency mechanisms based on link-disjoint 1+1 DPP and Restoration in different formats, which are already deployed on practical ASON devices of Alcatel-Lucent. It also considers link-disjoint 1+1 DPP and restoration separately as formats of resiliency mechanisms. The hybrid resiliency mechanism named as Protection and Restoration Combined (PRC) uses link-disjoint 1+1 DPP and restoration in combined manner. Here, restoration is triggered whenever a primary or backup path fails. The research simulates and records recovery times of these resiliency mechanisms to compare their performance for different point of link failures using the company's planning and design tool.

The research in [14] identifies four recovery mechanisms for double link failures (DLF) in a network. Among them, two of the resiliency mechanisms are hybrid based on 1:1 link-disjoint DPP and Rerouting combined together. In the first mechanism, rerouting is triggered if both of working and primary paths are failed. In the second mechanism, rerouting will be triggered if either of primary or backup path fails. The research work evaluates the performances of the resiliency mechanisms on modified version of NSFNet topology. Performance parameters considered here are blocking probability, unavailability and Double Link Failure Restorability.

According to the efforts that have been done and to the best knowledge of the author, the research works on hybrid resiliency mechanisms that consider node-disjoint and SRG-disjoint DPP for ASON dynamic provisioning are not found. However, it is also possible to consider different options of constraints in addition to link-disjoint constraint to produce constraint-based hybrid resiliency mechanism that can enhance performance of a network. The constraints that can be used for hybrid resiliency mechanism are Link-Disjoint, Node-Disjoint and SRG-Disjoint. Based on this idea, a new research work can be conducted to propose constraint-based hybrid resiliency mechanisms. The constraint-based hybrid resiliency mechanisms proposed by this research work are combinations of Link-Disjoint, Node-Disjoint or SRG-Disjoint 1+1 DPP and Restoration schemes.

3.5 Proposed Constraint-Based Hybrid Resiliency Mechanisms

The constraint-based hybrid resiliency mechanisms proposed for ASON utilize reverting mode 1+1 DPP schemes for dynamic provisioning process. This constraint-based resiliency mechanisms initiate Restoration to recompute backup paths in times of dual failures which cannot be recovered by the protection schemes. These proposed reverting mode constraint-based hybrid resiliency mechanisms are: 1+1 Link-Disjoint DPP + Restoration, 1+1 Node-Disjoint DPP + Restoration and 1+1 SRG-Disjoint DPP + Restoration. ILP formulations involved in these schemes are already discussed in Section 3.2.2.

3.5.1 1+1 Link-Disjoint DPP + Restoration Scheme

In this scheme, link-disjoint primary and backup paths, which do not share the same links from source to destination, are established for each connection requests. Restoration will be used when 1+1 link-disjoint DPP is unable to recover faults that can be occurred on links. If a fault occurred on primary path, the traffic on primary path will be switched to backup path. If backup path is also unavailable or a second failure affects it while primary path is being repaired, restoration will be triggered immediately to recover the traffic. If a failure occurs on backup path while primary path is working in normal condition, nothing will be done. In this condition the traffic is carried along primary path and there will be neither traffic switching nor path restoration as long as primary path is in its normal condition. Restoration is executed only when primary and backup paths are affected by failures. If the failure on primary path is repaired, the traffic will be switched back to the original primary path automatically. Since it is specifically designed for link-disjoint primary and backup paths, a single SRG failure may affect both primary and backup paths simultaneously. SRG failure in this scheme will reduce the probability of successfully recovering connection when it is compared to that of link failures.

3.5.2 1+1 SRG-Disjoint DPP + Restoration Scheme

In this scheme, SRG-disjoint primary and backup paths, which do not share the same SRGs from source to destination, are established for each connection requests. Restoration will be used when SRG-disjoint 1+1 DPP is unable to recover faults that can occur on links or SRGs. If primary and backup paths are SRG-disjoint, they are also link-disjoint. So, it can be said that link-disjoint is subset of SRG-disjoint. If a fault (link or SRG) occurs on primary path, and backup path is available, the traffic will be automatically switched to backup path. If a second fault occurs on backup path while primary path is being repaired, restoration will be initiated to recompute a backup path dynamically. If the first fault is on backup path while primary path is carrying the traffic, there will be neither traffic switching nor path recomputing (restoration). If the failure on primary path is repaired, the traffic will be switched back to primary path automatically. Since 1+1 SRG-Disjoint DPP + Restoration scheme utilizes SRG-disjoint 1+1 DPP for dynamic provisioning, it will enhance recoverability of connection requests in times of SRG failures. This performance enhancement comes with cost of slightly higher blocking probability which consumes more network resources.

3.5.3 1+1 Node-Disjoint DPP + Restoration Scheme

In this scheme, Node-disjoint primary and backup paths, which do not share the same nodes from source to destination, are established for each connection requests. The restoration will be used when node-disjoint 1+1 DPP is unable to recover faults that occurred on links or SRGs. Node-Disjoint 1+1 DPP helps to bypass nodes with frequent faults including link and SRG faults. If primary and backup paths are node-disjoint they are also link-disjoint. That means link-disjoint is subset of node-disjoint. But, node-disjoint paths may not be SRG-disjoint and link-disjoint paths may not be node disjoint. The traffic switching and path computation in times of failure risks is very similar to that of link-disjoint and SRG-disjoint based hybrid resiliency mechanisms. It also follows revertive mode operation. This hybrid resiliency scheme helps to improve recoverability of connection requests with cost of slightly higher network resource usage.

Chapter Four

4. Performance Evaluation Methodology

Performance evaluation of optical communication networks is one of key responsibilities of engineering study [42], [43]. It requires to understand behavior of a system and provide quantitative results. It can be conducted in several ways. Some of the options that can be used in performance evaluation of optical networks are experimental measurement, emulation-techniques, analytical modeling and simulation techniques which help to generate the required quantitative results. Measurement techniques require real physical network to deploy the system, protocol or algorithms under investigation. The other approaches are based on simplified model of the system in question which helps to work with virtual situations easily.

Experimental measurement demands to build a test-bed composed of real physical network components to measure the performance based on real network state [42], [43]. Even if experimental measurement in real networks can yield best accurate results, conducting such measurements in large and complex networks is very expensive. To solve this critical issue, modeling techniques which are simplified and scaled down versions of real networks can be considered in performance evaluation. However, the results that can be gathered from this modeling techniques are less accurate than that of experimental measurement technique. One of these modeling is emulation technique which tries to emulate or replicate functionalities of real system using software and hardware combinations. Even if it is cost effective compared to that of experimental measurement, it is complex to develop and requires longer execution time. Hence, it is still difficult to evaluate lager and complex networks.

The other modeling technique that can be used as an option to avoid cost and effort constraints associated with building trail test-beds is analytical modeling [42]. Analytical modeling can be used to evaluate performance of simple optical networks, but it is still complicated and difficult to model moderate and large size realistic networks. Solving these analytical models, such as ILPs using optimization software is time consuming and rather NP-complete for moderate and large size networks.

The other important option that can resolve all the composite constraints, such as cost, complexity and time consumption, measurability, configurability, and reproducibility is simulation-based technique [42], [43]. Simulation-based approach is cost effective since it doesn't involve real network components. This approach also removes error prone and time-consuming configuration that are dominant in real networks. It also makes possible to configure, change parameters and simulate multiple tasks in parallel simultaneously in a single network model. It is very suitable to complex systems and reasonably large networks to assess them easily. Simulation technique helps to measure effect of events which are very rare to happen in real networks and difficult to measure in time. It has also increased configurability which makes it possible to change distinct real network properties with lower cost and time. In simulation technique, it is possible to reproduce the same results of previous results in times of non-real random events which is impossible in experimental measurements due to measurement errors.

In general, simulation-based performance evaluation method is preferable for complex systems [42]. This method is very scalable and can be used to evaluate large scale networks in relatively easy way. Its cost effectiveness and faster execution time makes it preferable than the other models. In simulation approach, it is easier to configure different system parameters and evaluate performance under different network conditions. In specific, communication networks such as optical communication networks are commonly modeled using Discrete Event Simulation (DES). DES involves a predefined number of network states to model a behavior of a network. In DES, state transitions from one state to another occur at a particular moment when a specific event happens.

4.1 Discrete Event Simulation (DES)

Discrete event simulation is a model in which network states change only at discrete time occurrence of events [42], [44]. The actual time taken for an event to happen is assumed to be zero. That means, it is assumed that nothing interesting could happen between consecutive events, and there is no state change in a network between events. Thus, DES allows a simulation to jump in time directly from one event to another event. Powerful DES based simulation tools and frameworks are available for packet switched networks (IP/MPLS). Some of these dominantly used simulation tools are NS2, NS3, OPNET and OMNeT++. However, when it comes to optical communication networks the available options are very limited. They could be custom tailored or self-developed by academic institutions, commercial tools developed by industries, or open source.

The custom-tailored simulation tools are usually developed by academia for their own specific purpose which are not available for public use [44]. Hence, anyone who wants to conduct a research on optical communication system needs to develop his own simulation tool, in this aspect. But, it is always time consuming. The other option is relying on commercial tools, like OPNET. Commercial tools are designed for well matured technologies and algorithms which are already widely accepted in market. In this scenario, there will not be enough flexibility to integrate and test new algorithms. The other option which can meet both the requirements of academia and industry is open source simulation tool.

Open source simulation tools allow users to modify and add new features to meet their specific demands [42], [44], [45]. It also saves cost since its source code is openly available for everyone needs to modify and use it for free. However, most of the available open source options for optical communication are very limited. Some are limited in set of features, some are difficult and cumbersome to use and some have slow simulation speeds. For example, the GMPLS Lightwave Agile Switching Simulator (GLASS) is a java-based open source network simulation tool which can support the complete suite of GMPLS protocols with highly flexible QoS and resiliency mechanisms. However, it is quite difficult and complex to implement new algorithms and protocols. GLASS is also unstable and its update is halted in 2003. It has also slow simulation speed. The other simulation software which is widely used for conducting researches on optical networks is Optical WDM Network Simulator (OWNS). OWNS is an extension of NS-2 with bulk and monolithic code base which makes it slow in execution and complicated for implementing new algorithms and protocols. The other option that can resolve the problems raised in the open source simulation tools, and fill the gap between academia and industry is Net2Plan simulation tool.

4.2 Net2Plan Simulation Tool

Net2Plan is a Java-based open-source network optimization and planning tool [44], [46]. This tool has its origins during preparation of teaching materials for telecommunication engineering courses at Technical University of Cartagena (Spain), in 2011. It is developed by Pablo Pavon and Jose Luis Izquierdo Zaragoza. In the field of communication networks, planning and optimization tools use a range of platforms, system languages, applications and functionalities. Some of these tools are targeted to industry and some other are developed for education and research purpose in academia. Net2Plan is designed to overcome the barriers imposed by existing network planning tools. In Net2Plan, users are allowed to integrate their own algorithms applicable to any network types in addition to built-in algorithms.

Net2Plan Network Model

Net2Plan defines a network representation, named as network plan, based on abstract and technology agnostic concepts, such as nodes, links, traffic demands, routes, resources, shared risk groups and network layers [46]. Net2Plan provides the required flexibility to model any network technology, such as IP, Wireless and Optical networks. Nodes are basic entities of network design which can be end point of links or source and destination of traffic demand. Nodes can also forward traffic demands that are not intended to them. Nodes in a network plan have their own specific information, such as Id, Name, Index and up/down state of the node. The unique identifier (Id) of the node is assigned by kernel and will never be changed in life time of the network plan. Index of a node is a consecutive numbered (starting from 0) identifier assigned by kernel, but it will be renumbered when a node is removed. Up/down state represents working/failed states of nodes. In failed states of nodes, there will not be traffic forwarding, and the links originated from the node also will not carry any traffic.

Links are unidirectional elements connecting nodes and carrying traffic between nodes [46]. A link always starts in one node and ends on another nodes; loops or self-links are not allowed. It is possible to connect two nodes with zero, one or more links. Each link in the network plan is characterized by specific information, like Id, Index, origin node, destination node, capacity, length, propagation speed and up/down state. Traffic in Net2Plan is modeled with a set of commodities called demands. In this model, each demand represents a unidirectional end-to-end offered traffic flow between specific source and destination nodes. Here, a traffic cannot be originated and ended on the same node; self-demand is not allowed. A source-destination pair of nodes in a network can have zero, one or more traffic demands between them. Demand in a network is represented by specific information, such as, Id, index, ingress (source) node, egress (destination) node and offered traffic.

Routing in network plan represents how traffic demand is carried on links [46]. Net2Plan provides two forms of routing: source-routing and hop-by-hop routing. Source-routing involves assigning a set of routes between source and destination for each traffic demand.

Sequence of traversed links, amount of traffic demand and amount of capacity consumed in each link will be defined by the route. Since source-routing is the characteristics of connection-oriented networks, it is suitable to represent routing in optical networks. Hop-by-hop routing form defines routing using forwarding rules, which is the characteristic of connectionless network technologies, such as Ethernet and IP. In source-routing, a route can be assigned to only one demand, but a demand may have zero, one or more routes. Each route in a network is represented by characteristic information, such as Id, index, Associated demand, Sequence of links, Carried traffic and Occupied link capacities.

Shred Risk Group (SRG) represents risk of failures that could create simultaneous failures on specific set of links in a given network [46]. SRGs are represented by information which are characterized as Id, index, average time between two consecutive failures called Mean Time to Fail (MTTF), average time takes to repair a failure called Mean Time to Repair (MTTR), Associated set of links which contain links that can be failed simultaneously when a risk associated with the SRG occurs.

Net2Plan Design and Architecture

Net2Plan tool has two main parts: user interface and kernel [46], [47]. The user interface is provided with Graphical User Interface (GUI) and Command Line Interface (CLI) options. The kernel receives algorithms and current network design composed of network topology and traffic demands, and then produces updated version of the network design. User interface and kernel process the new network design to check its validity (correct topology format, current status of links like oversubscription and so on), to display the design graphically, and to compute some reports and performance results.

Net2Plan tool has different features that can be used for Optical network technologies [46], [47]. GUI of Net2Plan tool has four features of interfaces: offline network design, online simulation, Automatic report generation and Traffic matrix generation. These features implement the respective algorithm interfaces designed for specific purposes.

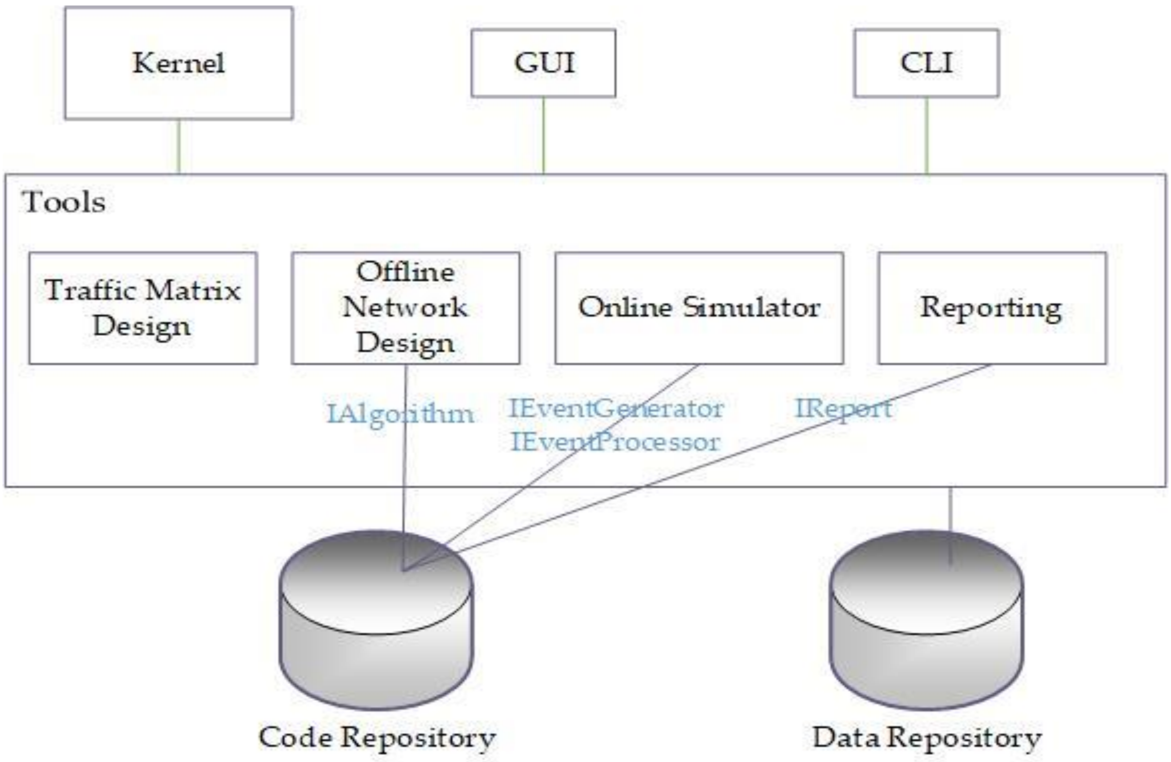

Figure 2: Net2Plan Architecture [47]

Offline Network Design: This Net2Plan feature helps to process offline network design and planning [46], [47]. It involves execution of user-defined or built-in algorithms which receive a network design (including traffic demand and network topology) and try to optimize it in a form of traffic routing or capacities on links to produce a new network design. The algorithms used here are based on constrained optimization formulations, like ILP.

Online Network Simulation: It allows building simulations for online algorithms that facilitate the reaction of a network for different events generated by user-developed or built-in event generator modules [46], [47]. It can be used to evaluate network recovery schemes that react to failure and repairs. It is based on DES paradigm and governed by two module objects: Event Generator and Event Processor which can be user-defined or built-in.

Event generator is a code that can generate external events, such as traffic variation, failure/repairs and demand add/remove events to a network. Even if event generator can send and receive events, it cannot change current network state by itself alone. Event processor consumes events generated by event generator and produce a new network state change according to events it received.

Traffic Matrix Design: In network design each demand is characterized by an ingress and egress node, and traffic volume [46], [47]. Traffic volume may contain one demand for each source-destination node pair, that is no two traffic demands with the same ingress and egress nodes. In such scenario it is possible to represent a demand set with compact matrix known as traffic matrix. Traffic matrix of a network with N nodes is $N \times N$ matrix with zeros on diagonal (to avoid self-demands). The traffic matrix design feature allows to generate user-defined traffic demand matrices for different models of traffic.

Report Generation: This feature allows to generate built-in or user-defined reports from any network design.

4.3 Performance Parameters

Performance of optical communication network designs can be measured in terms of resource utilization and survivability related metrics. Resource utilization of resiliency mechanisms together with usage of RWA algorithms in optical networks is measured using blocking probability of a connection request. Survivability of a network or a given service, which is the main part of SLA contracts that ensures service performance quality, can be measured in terms of availability and recoverability metrics. Hence, usage of RWA algorithms in resiliency mechanisms can be evaluated with blocking probability parameter results collected from Net2Plan online simulation tool. It is also possible to investigate effect of RWA algorithms on survivability of the resiliency mechanisms by measuring availability of a network using Ne2Plan report generating feature. The performance of proposed constraint-based resiliency mechanism is evaluated in terms of blocking probability, recoverability and availability provided by Net2Plan.

4.3.1 Blocking Probability

Blocking probability is a basic performance metric in dynamic light-path establishment [28], [29]. It represents the ratio of total number of blocked connections and total number of connection requests during entire life time of simulation. In other words, blocking probability is the probability of a connection request being blocked or denied due to failures in RWA or resource contention along targeted route. In dynamic light-path provisioning, a connection request will be blocked if a route with sufficient free capacity cannot be found between source to destination. In wavelength continuity constrained optical networks, if the same wavelength cannot be found in all links, a request will be blocked even if free capacity is available on each link along a path.

4.3.2 Availability

Availability is one of major network resiliency metrics that are stipulated in SLA contracts of service providers [29], [46]. Service availability can be defined as the percentage of time in which the service should be operative during observation time. Availability can be also defined as asymptotic probability that a network will be in its operative state at random times in future. Availability of a network can be computed statistically based on frequency of failure and failure repairing rate of network components (links and nodes). Availability of these network components is extracted from Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR) separate estimations. Hence, availability of a network component can be expressed as a function of these two estimates as follows:

$$A = \frac{MTBF - MTTR}{MTBF}$$

However, successful provisioning of services in actual networks involves multiple resources which can suffer individual or multiple risk of failures. This coordinated process will result in a sever degradation of availability level of a network. Hence, in order to guarantee minimum level of availability of a network, availability estimation model based on SRG definition in a network is provided. Risks are possible causes of failures in a network, and SRG f can be defined for each associated risk. Let F denote all possible risks or SRGs in a network, and SRG is composed of one or more links/nodes. For a particular risk f the corresponding availability, MTBF an MTTR values are denoted as $A_f, MTBF_f\ and\ MTTR_f$ respectively. Let S be possible set of network states. A network state $s \in S$ is defined by $down(s)$, which is a set of risks in failure. The set $up(s) = F - down(s)$, represent set of risks which are not in failure. The s_0 denotes no failure state in situation of no SRG is down. The probability of a network to be in state s by assuming statistical independence of SRGs is given by:

$$\pi_s = \prod_{f \in up(s)} A_f \prod_{f \in down(s)} (1 - A_f)$$

The fraction of the time in which the network can be in no failure state is:

$$\pi_{s_0} = \prod_{f \in F} A_f$$

For a given network state s, $h_d(s)$ denotes the amount of carried traffic (surviving traffic) of demand d by assuming a network started with no failure state and SRGs become in $down(s)$ state in any particular order. All the traffic will be carried in no failure state, that means $h_d(s_0) = h_d$. The values of $h_d(s)$ can be computed by tracking resiliency mechanisms deployed in the network. The availability of a demand d which is the fraction of time in which all traffic of a demand is carried, is given by:

$$A_d = \sum_{s:\, h_d(s) = h_d} \pi_s$$

The network availability, which is the fraction of the time in which all traffic of the network is carried, is given by:

$$A = \sum_{s:\, h_d(s) = h_d, \forall \mathrm{d} \in \mathrm{D}} \pi_s$$

4.3.3 Recoverability

Recoverability is a network wide parameter that represents the capability of a network to survive against failures [28], [46]. Hence, Network recoverability can be defined as the fraction of total number of failed connection requests that can be recovered by deploying resiliency mechanisms in a network. Recoverability is the probability of successfully recovering a connection in times of failure occurrences in a given network. It is the ratio of total number of successfully recovered connection requests and the total number of connection request that attempt to recover. Network recoverability can be used to evaluate the robustness of resiliency mechanisms in times failures in a network.

Chapter Five

5. Performance Results and Discussion

This chapter has two sections. The first section is results and discussions about performance evaluation of RWA algorithms in ASON resiliency mechanisms. It tries to show which RWA algorithm is suitable for protection and restoration resiliency mechanisms in terms of blocking probability and availability. The second section is about performance evaluation of the newly proposed constraint-based hybrid resiliency mechanisms based on an RWA algorithm that performs better in the first section. It considers blocking probability, network availability and recoverability performance metrics.

Network availability and recoverability metrics are evaluated by considering link and SRG failure models. Link and SRG failures are dominant failure scenarios in current optical networks. Node failures are less common and relatively rare to happen. But, the disruption will be very severe when a node failure happens, since it can cause failure of all links that are connected to the node. The performance evaluations that consider node failure scenarios are not feasible for networks with small number of nodes. Hence, this research work assumes that the chances of node failure are neglected and only link and SRG failures are considered.

5.1 Performance Evaluation of RWA Algorithms in ASON Resiliency Mechanisms

This specific simulation involves 1+1 DPP (1+1 Link-Disjoint DPP, to be specific) and Restoration resiliency mechanisms. These resiliency mechanisms are selected since they are widely used in practice and easy to implement, as discussed in Section 3.2.1. The connection requests in these resiliency mechanisms are provisioned with the help of RWA algorithms. Four types routing algorithms, SRG Disjoint Aware Routing, Alternate Routing, Least Congested Routing and Load Sharing, are considered for this particular simulation since they are widely used adaptive routing algorithms in practice, as discussed in Section 2.2.3. The type of wavelength assignment that work with these routing algorithms is First-Fit wavelength algorithm. First-Fit wavelength assignment is also preferred in practice since it performs well in blocking performance and has low complexity, as discussed in Section 2.2.2. In this simulation, effect of RWA algorithms usage on performance of resiliency mechanisms will be investigated. These effects will be compared in terms blocking probability and network availability performance results using Net2Plan Simulation tool. Different simulation setup and assumptions are used for blocking probability and network availability. For network availability measurement, the connection requests are expected to be deterministic. It utilizes offline algorithm to estimate availability of a given network. Blocking probability simulation is based on online algorithms in which connection requests are dynamic and non-deterministic.

5.1.1 Simulation Setup

Addis Ababa Metro OTN Backbone Network of ethio telecom is used as a reference topology for blocking probability and availability simulations. It has 10 ASON enabled nodes and 48 unidirectional links. Each link has a capacity of 80 wavelengths with 40Gbps traffic capacity per each wavelength. The reference network topology is setup on Net2Plan simulation tool as shown below.

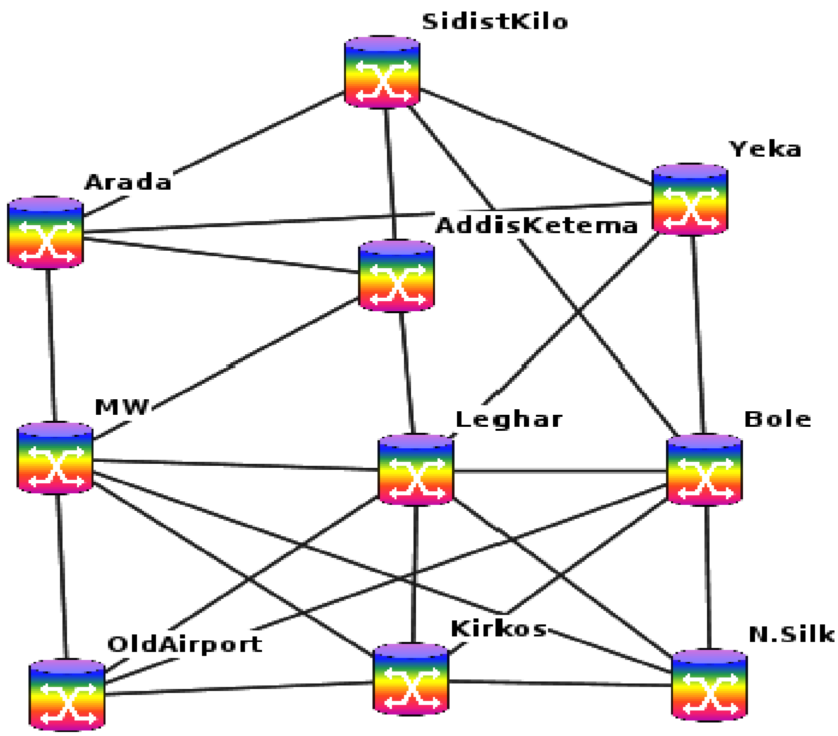

Figure 3: Addis Ababa Metro OTN Reference Topology [48]

The reference network topology is prepared by assuming there are traffic demands between each node in the network. Each demand represents an end-to-end unidirectional traffic flow offered to the network between different particular nodes. That means, there are traffic demands originated from a node and terminated to the remaining nodes, and there will not be traffic flow originated and terminated on the same node (self -demands are not allowed). Therefore, for N number of interconnected nodes of a network it is possible to have N(N-1) possible source-destination pairs of nodes for end-to-end traffic flows. Hence, with 10 nodes it is possible to have 90 source-destination pairs (end-to -end traffic flows, called demands). For this specific simulation, 90 traffic demands are generated using traffic demand matrix generator tool of Net2Plan. The traffic demand generation assumes that the capacity of each demand is equal. In addition to that 24 Shared Risk Groups (SRGs) are defined in the reference topology. The SRG model is one SRG per bidirectional link bundles that connect two nodes. In this reference topology there is no wavelength conversion and regeneration (O-E-O conversion) between source-destination pairs of nodes.

Table 1: Refence Topology Design Summary

Number of Nodes	10
Number of links	48
Node out-degree (max, min, avg)	7, 4, 5.2
Is connected? (# connected components)	Yes
All links are bidirectional (yes/no)	Yes
Layer diameter (hops, km, ms)	2, 20.1, 0.101
Capacity units name	Frequency slots (wavelengths)
Capacity installed: total	3840
Capacity installed: average per link	80
Number of demands (node pairs)	90
Traffic units name	Gbps
Line Rates Per Light-path (Gbps)	40
Number of SRGs in the network	24
SRG Definition Characteristic	One SRG per bidirectional link bundle

5.1.2 Blocking Probability Simulation

Resource utilization of the RWA algorithms in each ASON resiliency mechanisms is compared using blocking probability performance parameter. This simulation will show effects of the RWA algorithms usage on protection and restoration schemes resource utilization.

Simulation Assumptions

Blocking probability simulation uses event-driven simulation which is provided by Net2Plan simulation tool. Event-driven simulation helps to analyze the response of a network to changes, like establishment and release of light-paths in different loads offered to a network. This simulation assumes light-path request events arrive and depart randomly with exponential distribution (Poisson arrival). The connection requests holding time (duration) is also assumed to be random and exponentially distributed. This blocking probability simulation is conducted by assuming the presence of relatively low link failure rates (non-intensive failures) to minimize the number of multiple failures on a path. Accordingly, the simulation assumes exponentially distributed (Poisson arrival) and average normalized values of 192 and 1 unites of time for mean time to failure and mean time to repair the faults occurred in the network, respectively. The simulation generates a million events and among them 10% (100,000) of them are transitory events. Transitory events are number of events for transitory period. So, in every of these transitory events, the kernel will update internal variables of the network design (update current state of the network) to compute current statistics that may exist, before proceeding to next events.

Simulation Result and Discussion

Blocking probability simulation is run for different total offered traffic values, starting from 10.6Tbps to 86.4Tbps in steps of 10.8Tbps for both restoration and protection schemes. In the case of restoration scheme, up to k=10 number of alternative shortest paths are computed for each connection requests at source node. Then, only one primary path (no backup path) for each connection request is selected among computed paths based on criteria deployed in RWA algorithms. Simulating the given reference network topology under specified assumptions for restoration yields the following result, as depicted in Figure 4.

In protection case, up to k=10 link-disjoint alternative shortest paths are computed for each connection request and two best routes (one for primary path and the other one for backup path) are selected and resources are assigned based on the criteria deployed in RWA algorithms. Simulating the given reference network topology under specified assumptions for 1+1 Link-Disjoint DPP yields the following result, as depicted in Figure 5.

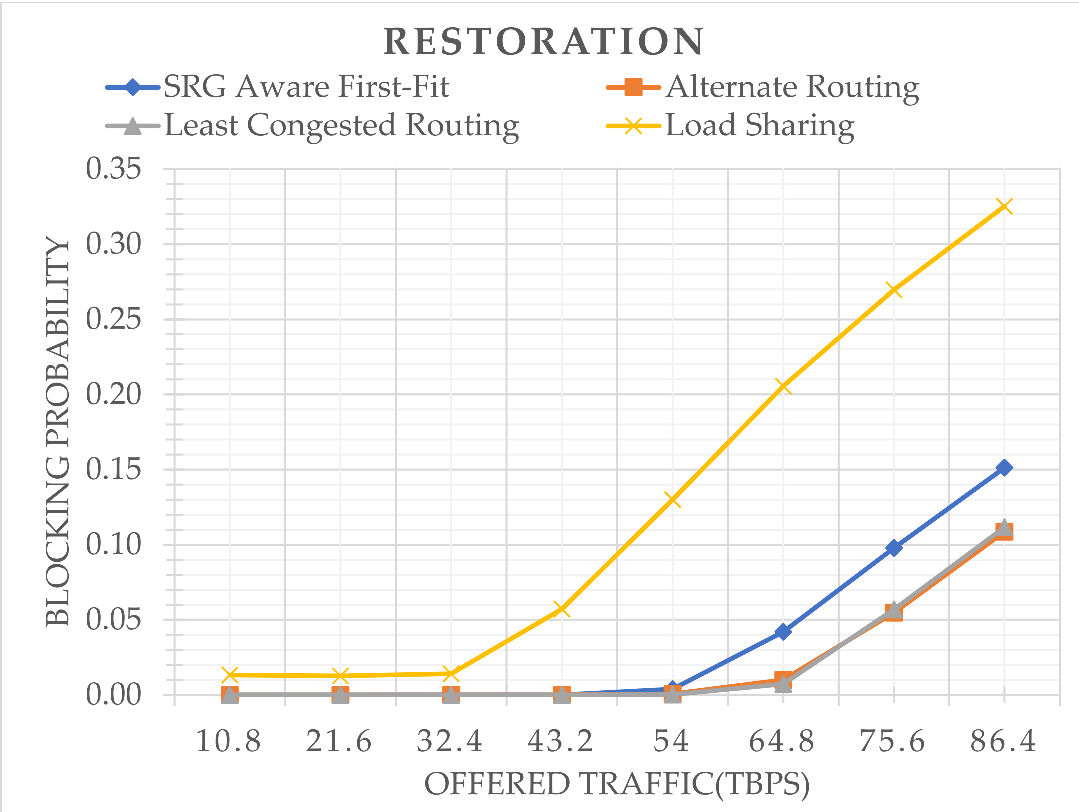

Figure 4: Blocking Probability in Restoration

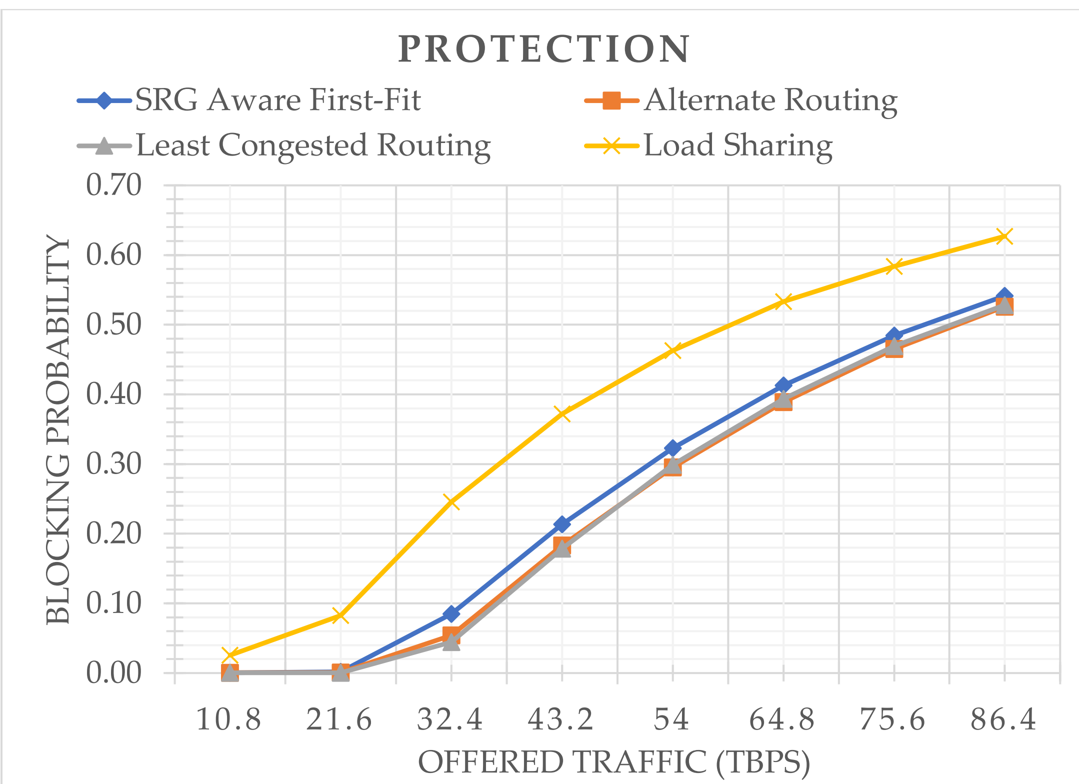

Figure 5: Blocking Probability in Protection

From the above results depicted in Figure 4 and Figure 5, it is clear to see that blocking probability of all RWA algorithms in both restoration and protection schemes is increased as total offered traffic increases. This is due to the fact that the available spare network resources are depleting and the contention for resources becomes higher as traffic demand between source-destination pairs increases. In both restoration and protection schemes, Load Sharing routing algorithm has shown larger values of blocking probability when it is compared to other algorithms. This value is on average 18.8% and 13% higher at higher offered traffic greater than 43.2Tbps in restoration and protection, respectively. This high blocking probability of Load Sharing algorithm is due to distinct property of the algorithm in making decision to select a path from k alternative paths. Load Sharing routing select paths from alternative paths randomly, and the connection will be immediately blocked if selected path is unavailable or if it has no enough spare resources, without retrial in other paths. Since the routing algorithms, other than Load Sharing, perform searching for available path with enough resources in case of selection failure in first trail, they have lower blocking probability.

Alternative Routing and Least Congested Routing algorithms show competently lower blocking probability than that of SRG-Disjoint Aware Routing algorithm in both resiliency mechanisms. These routing algorithms have on average 3% and 2% lower blocking probability than SRG-Disjoint Aware routing at traffic offers higher than 43.2Tbps in restoration and protection, respectively. Since SRG-Disjoint Aware routing uses SRG counts as a criterion to select a path among alternative paths in addition to the availability of the path and resources on the path, its resource utilization becomes poor while it tries to make the RWA process less SRG-overlap. Least Congested Routing performs lowest blocking probability at lower traffic loads, even slightly better than Alternate routing. The best choice at higher loads is always Alternate routing since its criteria to select a path is only availability of the path and resources. Least Congested Routing path selection is based on congestion level of the routes, it chooses a path with lowest congestion. Hence, at lower loads both Alternate routing and Least Congested routes can be considered for better resource utilization requirements of restoration and protection schemes. From the two results of protection and restoration blocking probability, it is possible to understand that RWA algorithms in restoration have lower blocking probability than that of protection. This is due to the nature of path establishment in connection set up time. Unlike protection, restoration doesn’t demand establishment of redundant backup paths for each connection request which makes it better in blocking performance.

5.1.3 Availability Measurement

The effect of RWA algorithms usage in resiliency mechanisms is not limited to resource utilization, it has its own significant effect on availability of the network. Availability is very relevant when it comes to customer satisfaction so that it is a very important service level specification (SLS) in SLA contracts. This part of simulation estimates availability of the given network provisioned with protection and restoration resiliency mechanisms under link and SRG failure occurrences.

Simulation Assumptions

Network availability simulation uses availability estimation report provided by Net2Plan tool. This report receives a network design (reference topology with traffic demand matrix), resiliency mechanisms and network risk (failure models), and estimates availability of a network using enumerative process. Since this report is based on the offline algorithms, the connection requests are expected to be deterministic. The network should be provisioned with these deterministic connection requests according to their recovery types using RWA algorithms. The simulation assumes that provisioning process is accomplished without blocking any connection request. That means, no connection request is blocked in no failure states (normal condition) of the network. The report also assumes failures occur per link or per SRG in the network randomly with exponential distribution according to conservative values of MTBF = 8748hrs and MTTR = 12hrs, which are defined on the respective links or SRGs. That means, per link or per SRG failures in the network will occur on average once in a year and can be repaired in half a day.

Mean Time Between Failures (MTBF) is the average time between two consecutive link or SRG failures, and Mean Time to Repair (MTTR) is the average time needed to repair the failure. Estimation of MTBF and MTTR values is obtained from a specific risk assessment study of failure risks that threaten a network. However, these specific data are not available for the network considered in this research work. Hence, to simplify the process of network availability analysis, conservative generic standard figures of MTTR and MTBF are used, as suggested in [44]. These conservative figures are cautious estimates to avoid excess and exaggerated failure rate estimations. The failure rate indicated by the conservative values is most likely lower than actual estimates of risk assessment studies. This network availability estimate simulation considers no failure, single failure and double failure network states together in the enumeration process. It also assumes that no multiple failures more than dual failures will occur, and if they occur traffic will be interrupted.

Simulation Results and Discussion

Network availability simulation is run for different offered traffic values starting from 3.6Tbps to 21.6Tbps with a range of 3.6Tbps. This offered traffic range is selected in order to fulfil the requirement of no traffic is blocked in normal condition of the network during provisioning process. The simulation results shown below compare availability of the network with protection or restoration recovery mechanism provisioned with SRG-Disjoint Aware Routing, Alternate Routing, Least Congested Routing and Load Sharing Routing algorithms, which are coordinated with First-Fit wavelength assignment algorithm, subjected to different failure risks (link or SRG failures).

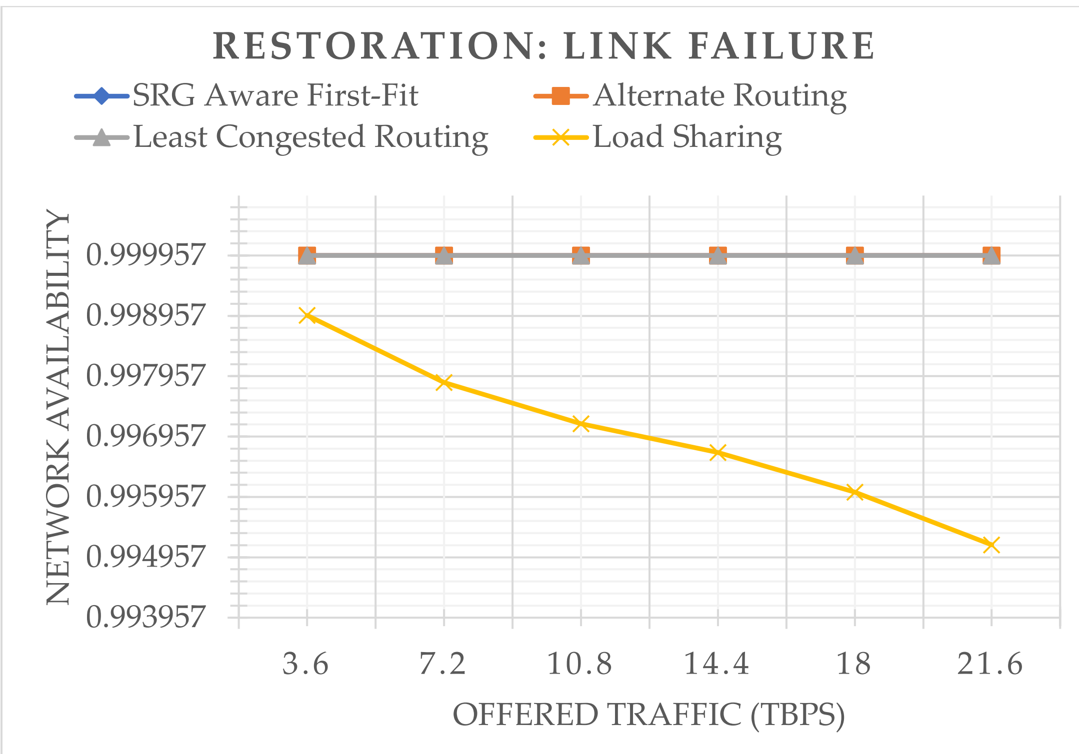

Figure 6: Availability of Restoration in Link Failure

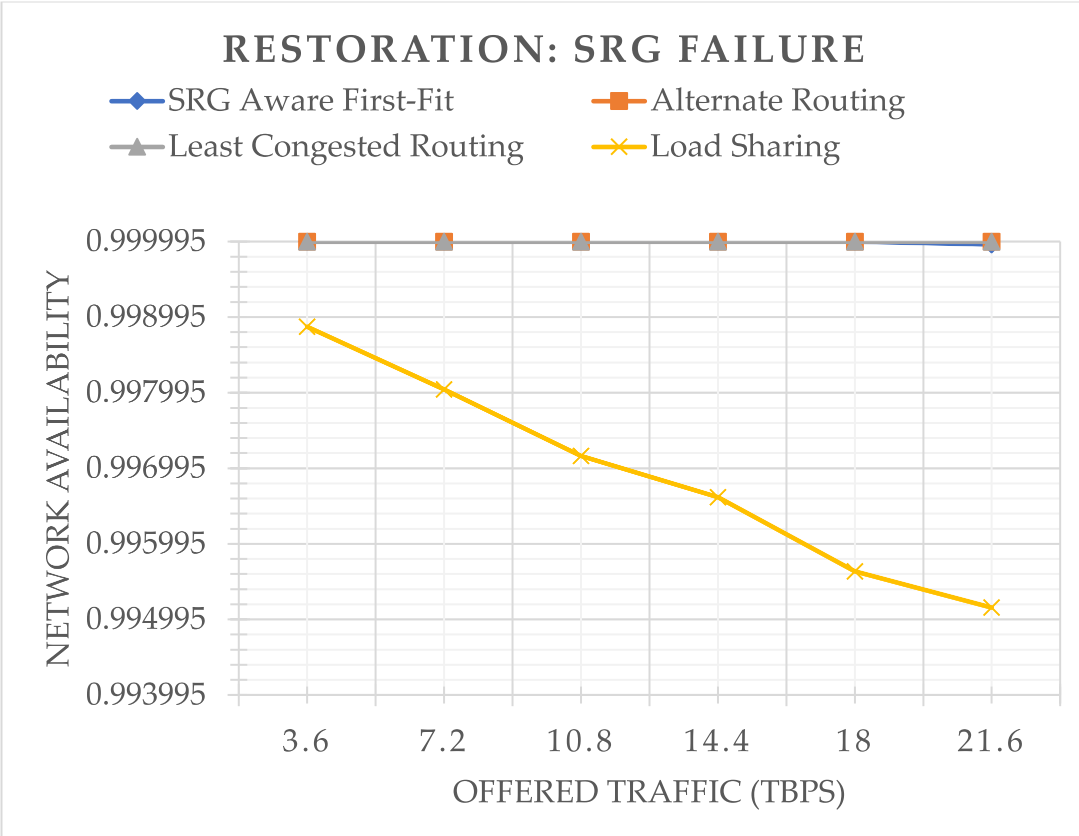

Figure 7: Availability of Restoration in SRG Failure

The results depicted in the above two figures, in Figure 6 and Figure 7, show that availability of the routing and wavelength assignment algorithms (except load sharing) in restoration during link and SRG failures is constant, which is equal to 0.999957 during link failures and 0.999995 during SRG failures, throughout simulation time. The results indicate that availability of the network with restoration recovery will be at highest values in times of link or SRG failures as long as the network has enough spare capacity resources. The network is designed with excess number of spare resources in order to fulfil the requirement of no connection drops in the provisioning process. However, this claim doesn't work for the network provisioned with Load Sharing algorithm since it doesn't perform retrial for path selection in alternative routes in the case of resource and path unavailability on the first route selected randomly. Hence, availability of the network provisioned with Load Sharing decreases rapidly as total offered traffic increases.

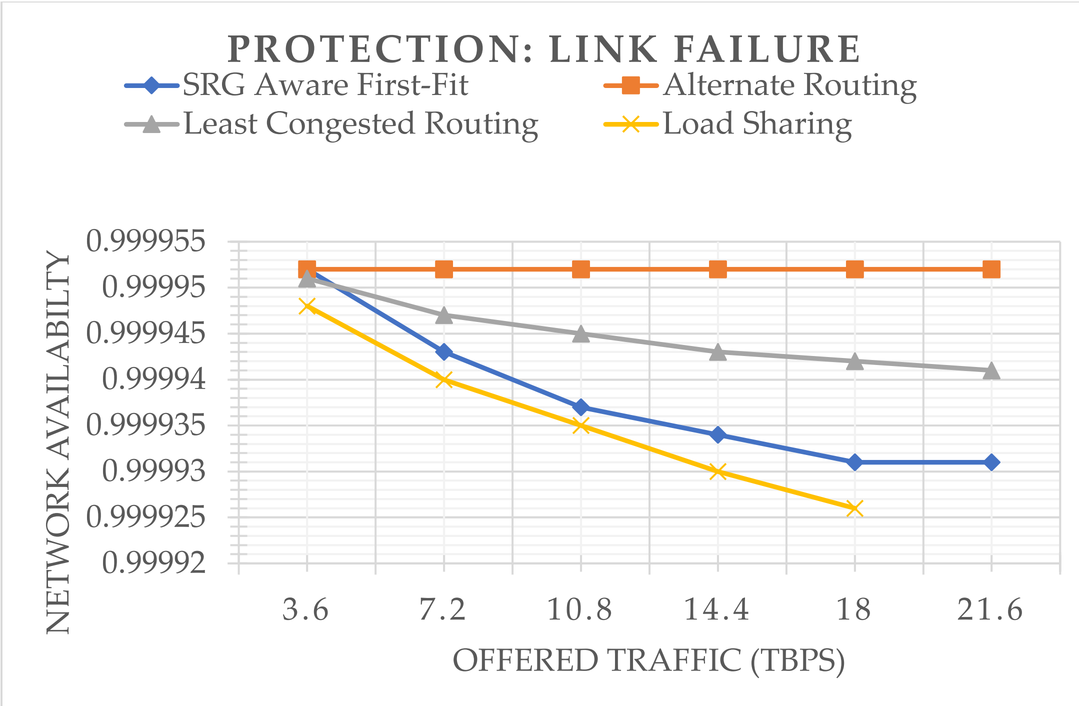

Figure 8: Availability of Protection in Link Failure

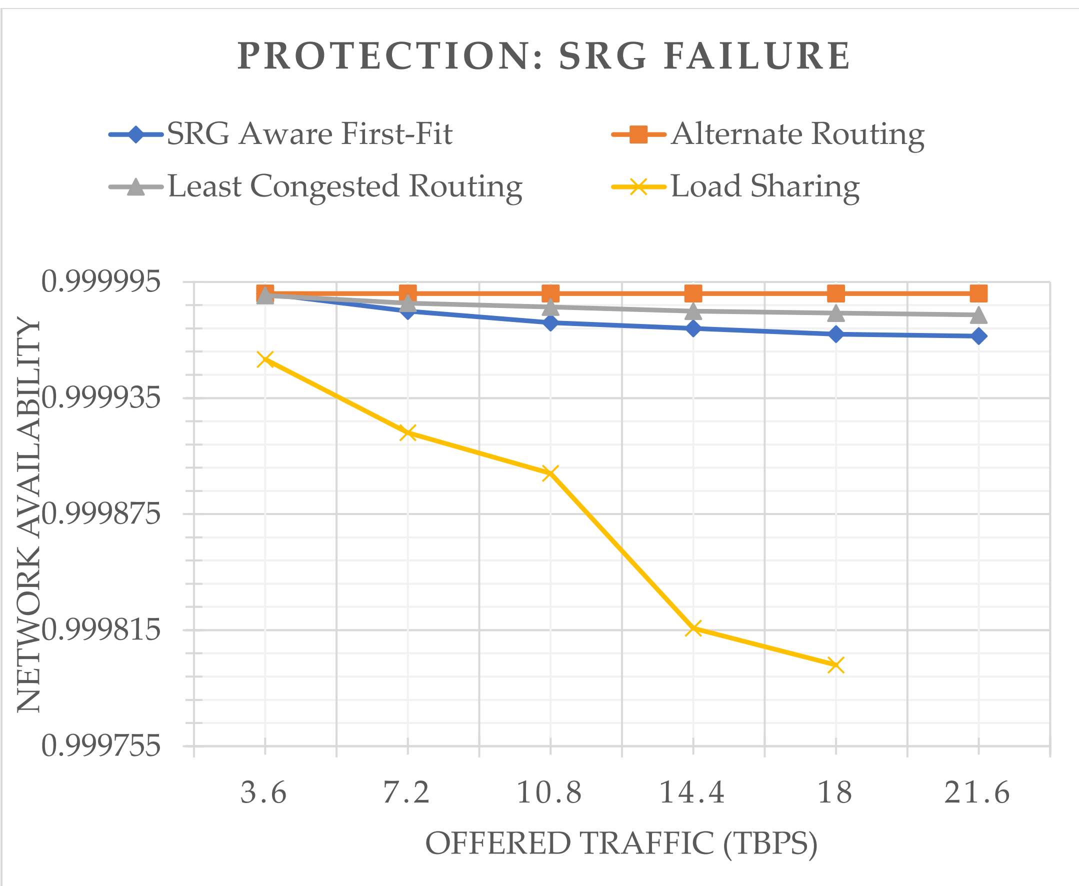

Figure 9: Availability of Protection in SRG Failure

The results shown above on Figure 8 and Figure 9 are Network Availability simulation results for the network that has protection scheme and provisioned with the routing and wavelength assignment algorithms (as mentioned before) subjected to link or SRG failure situations. According to path selection criteria used in each RWA algorithms connection provisioning, availability of the network with protection scheme provisioned with Alternate routing, Least Congested Routing, SRG-Disjoint Aware routing and Load Sharing are found in their order in both cases of failures. Availability of the network provisioned with Alternate routing has a constant and highest value, 0.999952 in link failures and 0.999989 in SRG failures, throughout simulation period and offered traffic values. The other availability values, except the network with Alternate Routing, decreases as the offered traffic increases depending on their resource utilization to set up the connections and recover the faults.

From network availability simulation results of protection and restoration schemes based on RWA algorithm usage, it is possible to understand that RWA algorithms deployed in restoration show better availability than that of protection. As mentioned in simulation assumptions, the availability estimate considers double failures in addition to single and no failure network states. However, protection is designed against single failure risks whereas restoration can mitigate the induced double failures. Hence, the double failures considered in the network will severely affect availability performance of the network provisioned with protection scheme.

As it can be seen from the above network availability simulation results, the Alternate Routing algorithm can contribute higher network availability values in both recovery schemes during link as well as SRG failures. The blocking probability simulation also show that resource utilization of Alternate Routing and Least Congested routing are better than the other algorithms. Hence, both blocking probability and availability simulations confirm that using Alternate routing and Least Congested routing in connection provisioning contribute better resource utilization with better performance quality. However, the overall results of blocking probability and network availability show that Alternate Routing is even a better choice to be used in both protection and restoration resiliency mechanisms.

5.2 Performance Evaluation of Constraint-based Hybrid Resiliency Mechanisms

The hybrid resiliency mechanisms proposed and considered in this simulation are 1+1 Link-Disjoint DPP + Restoration, 1+1 Node-Disjoint DPP + Restoration and 1+1 SRG-Disjoint DPP + Restoration. The Alternative Routing algorithm coordinated with First-Fit wavelength assignment is preferred based on the performance evaluation performed in previous section, Section 5.1.

5.2.1 Simulation Setup

Performance evaluation of the newly proposed constraint-based resiliency mechanisms is performed on Net2Plan simulation tool. Modified version of Addis Ababa OTN Metro Backbone Network of ethio telecom is used as a reference topology for this simulation scenario. This reference network topology is composed of 10 ASON enabled nodes which are interconnected to each other with 54 unidirectional links. Each of these links have 80 wavelengths and each wavelength has a capacity of producing 40Gbps light-paths.

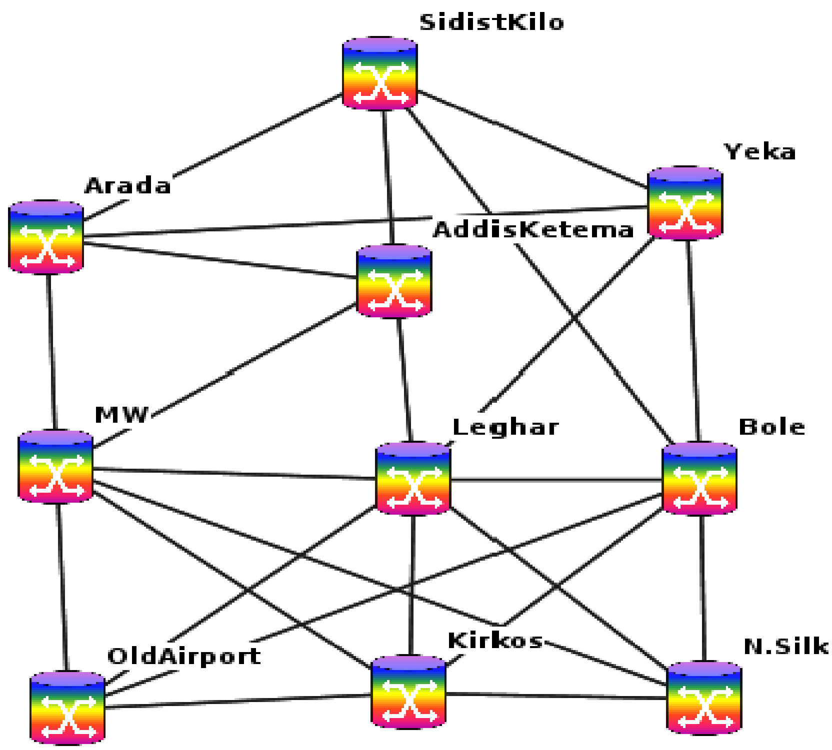

Figure 10: Modified Addis Ababa Metro OTN Reference Topology [48]

The only difference of this reference network topology with the previously used network topology in performance evaluation of RWA algorithms usage (in section 5.1) is the number of links deployed in the network. In this modified network topology, 6 additional unidirectional links (two on each span) are installed on spans of Arada--Yeka, MW--NefasSilk and OldAirport--Bole to make the definition of SRGs more realistic. In this case, the number of member links in the SRG will be more than two, to be specific four, in one

SRG per bidirectional bundle model of SRG definition on mentioned spans. Hence, 24 SRGs are defined in this reference network topology too. Similarly, 90 traffic demands are generated with the help of traffic demand matrix generator of Net2Plan tool. It is also assumed that all traffic demands between source destination pairs have equal capacity. There will not be wavelength conversion and regeneration (O-E-O conversion) between any source-destination pairs of demands.

Table 2: Modified Refence Topology Design Summary

Number of Nodes	10
Number of links	54
Node out-degree (max, min, avg)	7, 4, 5.4
Layer diameter (hops, km, ms)	2, 20, 0.1
Capacity units name	Frequency slots (Wavelengths)
Capacity installed: total	3840
Capacity installed: average per link	80
Number of demands (node pairs)	90
Traffic units name	Gbps
Line Rates Per Light-path (Gbps)	40
Number of SRGs in the network	24
SRG definition characteristic	One SRG per bidirectional link bundle

5.2.2 Blocking Probability and Recoverability Simulation

The simulation for blocking probability and recoverability is used to show resource utilization and service performance quality of the newly proposed hybrid resiliency mechanisms, for this particular scenario. Recoverability and blocking probability share the same assumptions and can be conducted jointly on Net2Plan to collect the respective results. Network availability is also one of the parameters to measure service performance quality of a network, but it requires different assumptions and can't be conducted with recoverability and blocking probability. The availability simulation considered in this research work is based on offline algorithms designed for deterministic connection requests. Hence, blocking probability and recoverability simulation is considered first. The simulation is conducted based on the network setup described above and the following simulation assumptions.

Simulation Assumptions

In blocking probability and recoverability simulation of hybrid resiliency mechanisms, joint event driven simulation feature of Net2Plan is used. In this joint simulation, the connection requests arrival/departure and failure/repair events are assumed to occur in the network during simulation time. Joint event driven simulation helps to analyze how a network reacts to changes due to connection request set up/release in conjunction with failure/repair events. The simulation assumes connection requests (light-path requests) are arrived and departed randomly with exponential distribution (which can be termed as Poisson arrival). It also assumes interarrival and holding time of connection requests are exponentially distributed and independent (Poisson arrival). The simulation assumes link or SRG failure/ repair events occur randomly with exponential distribution. Hence, exponentially distributed mean time to failure and to repair average normalized values of 0.9 and 0.1 units of time, respectively are assumed. These two values show that the failure arrival rate in the network is chosen to be more aggressive than in reality, which helps to test the robustness of resiliency mechanisms and to obtain descent performance results within a reasonable period of simulation. This simulation generates one million events together with 100,000 transitory events.

Simulation Results and Discussion

The joint event driven simulation for blocking probability and recoverability is run for different total offered traffic values from 10.6Tbps to 86.4Tbps in steps of 10.8Tbps for each hybrid resiliency mechanisms exposed to per link and per SRG failures. In 1+1 Link-Disjoint + Restoration resiliency mechanism, first up to 10 link-disjoint candidate shortest paths are computed for each traffic demands. Similarly, in 1+1 Node-Disjoint DPP + Restoration and 1+1 SRG-Disjoint DPP + Restoration, first up to 10 Node-Disjoint and SRG-Disjoint shortest alternative paths are computed for each traffic demands, respectively. Then the first available shortest path is selected and established as primary path and the second one as backup path.

If a failure (link or SRG failure) occurs on primary path, the traffic will be automatically switch to backup path. If another failure occurs on current working path (previous backup path) before primary path is repaired, restoration will be triggered to recover the traffic. Restoration mechanism applied here can recover against multiple failures that could affect current working paths established by restoration as long as enough spare capacity is available in the network. The traffic will be reverted back to its original primary path as soon as failure is repaired. Simulating the given modified reference network topology under specified assumptions and failure models (link and SRG failure) yields the respective blocking probability and recoverability results.

This section first produces blocking probability and recoverability simulation results for non-hybrid resiliency mechanisms under each link and SRG failure situations. Then, the results are compared with hybrid resiliency mechanisms. Finally, the performance results of the proposed hybrid resiliency mechanisms will be compared.

Blocking Probability of Non-hybrid Resiliency Mechanisms

This simulation compares blocking probabilities of 1+1 Link-Disjoint DPP, 1+1 Node-Disjoint DPP, 1+1 SRG-Disjoint DPP and Restoration non-hybrid resiliency mechanisms under link and SRG failures. The results shown below, in Figure 11 and Figure 12 indicate blocking probability of non-hybrid resiliency mechanisms exposed to link and SRG failure risks, respectively.

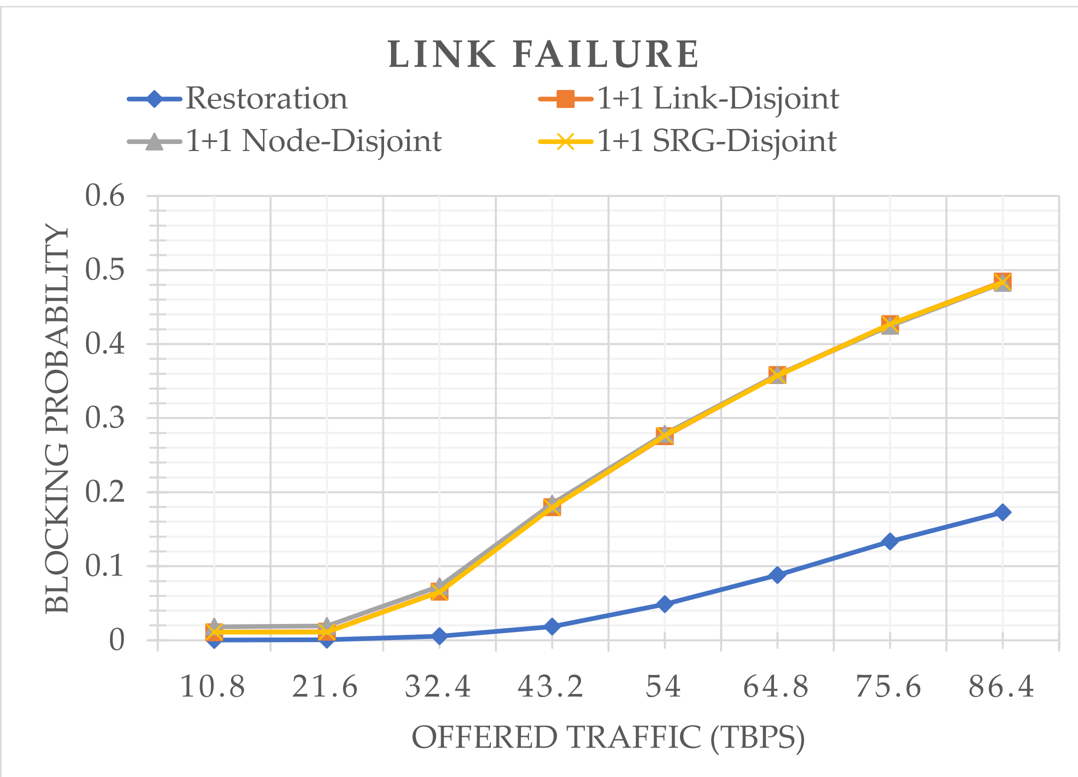

Figure 11: Blocking Probability of Non-hybrid Resiliency Mechanisms during Link failure

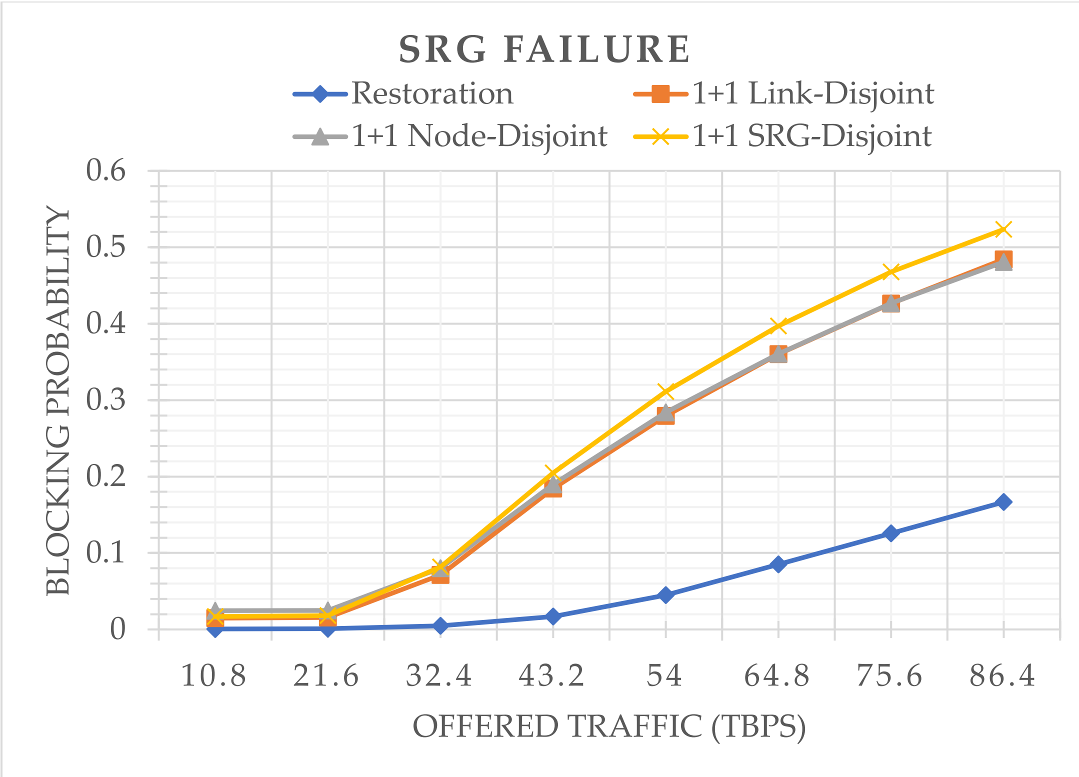

Figure 12: Blocking Probability of Non-hybrid Resiliency Mechanisms under SRG failure

As shown in the above figures (Figure 11 and Figure 12), blocking probability of Restoration is lowest in both link and SRG failure scenarios, since it doesn't require reservation of resources as backup paths. 1+1 Node-Disjoint resiliency mechanism has relatively higher blocking probability at lower traffic loads in both link and SRG failures, which indicates that network resources that are required to set up node-disjoint paths are not used efficiently at lower loads of network traffic. In link failures (shown on Figure 11), resource utilization of 1+1 Link-Disjoint and 1+1 SRG-Disjoint resiliency mechanisms is becoming slightly as poor as that of 1+1 Node-Disjoint when traffic load is increasing. Since link-disjoint is a subset of node disjoint and SRG disjoint, protection schemes perform slightly the same in times of link failures at higher traffic loads.

In SRG failures (Figure 12), even if 1+1 SRG-Disjoint shows lower blocking probability at lower traffic loads, when it is compared to 1+1 Node-Disjoint, it shows highest blocking probability at higher loads. This shows that it is difficult to find SRG-disjoint paths for each request in times of SRG failures. Even though 1+1 Link-Disjoint out performs other protection schemes in resource utilization performance for wide range of offered traffic loads, 1+1 Node-Disjoint competes with it at higher traffic loads.

Blocking Probability Comparison of Hybrid and Non-hybrid Resiliency Mechanisms

The results presented here compare resource utilization of non-hybrid and hybrid resiliency mechanisms. Hence, 1+1 Link-Disjoint + Restoration blocking probability will be compared with 1+1 Link-Disjoint and Restoration resiliency mechanisms (Figure 13 &14), 1+1 Node-Disjoint + Restoration with 1+1 Node-disjoint and Restoration (Figure 15&16), and 1+1 SRG-Disjoint + Restoration with 1+1 SRG-Disjoint and Restoration (Figure 17&18) that are exposed to link and SRG failures.

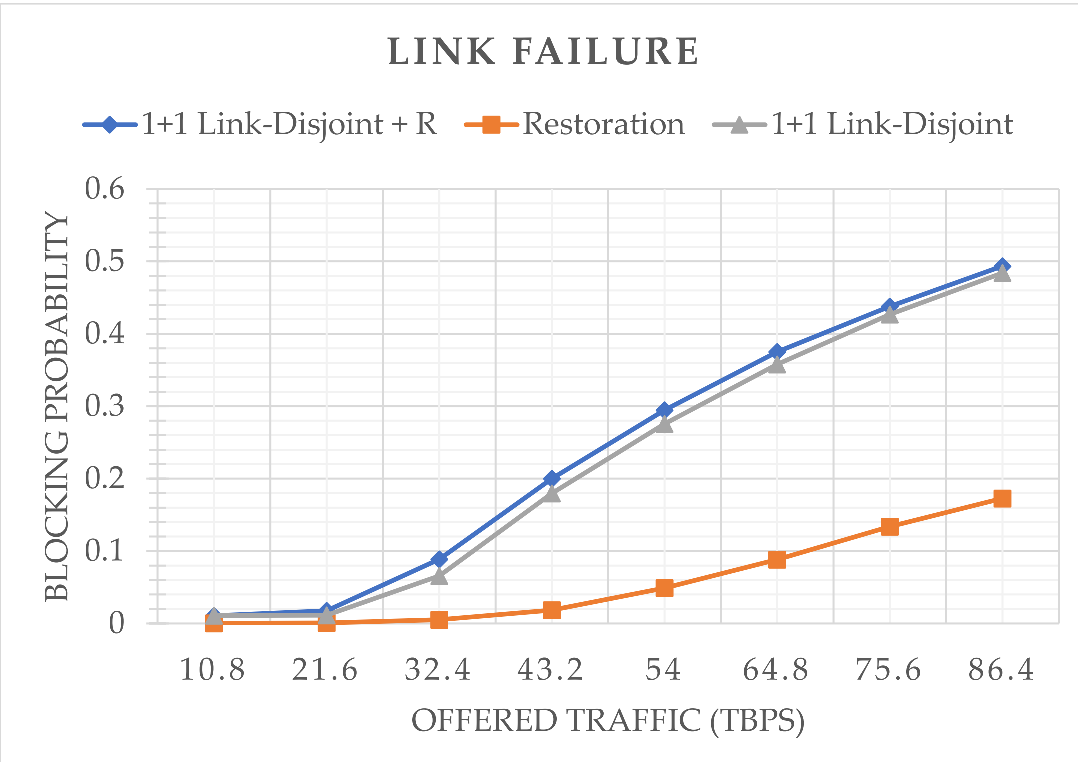

Figure 13: Link-Disjoint Protection and Restoration Blocking Probability in Link Failure

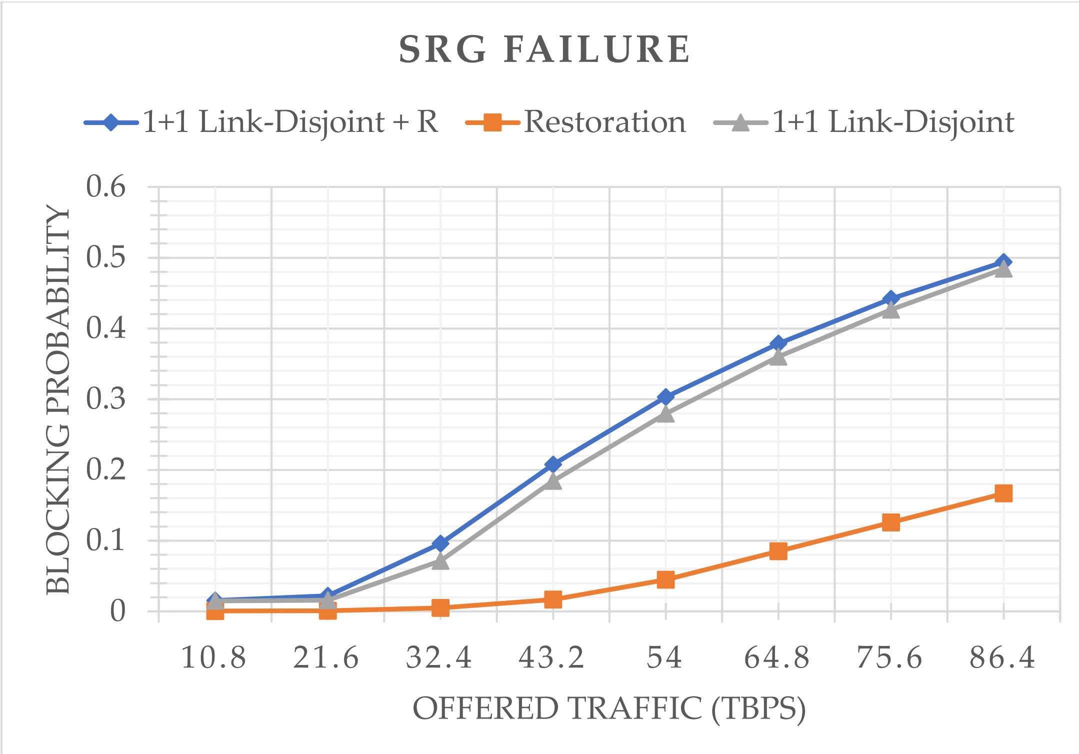

Figure 14: Link-Disjoint Protection and Restoration Blocking Probability in SRG Failure

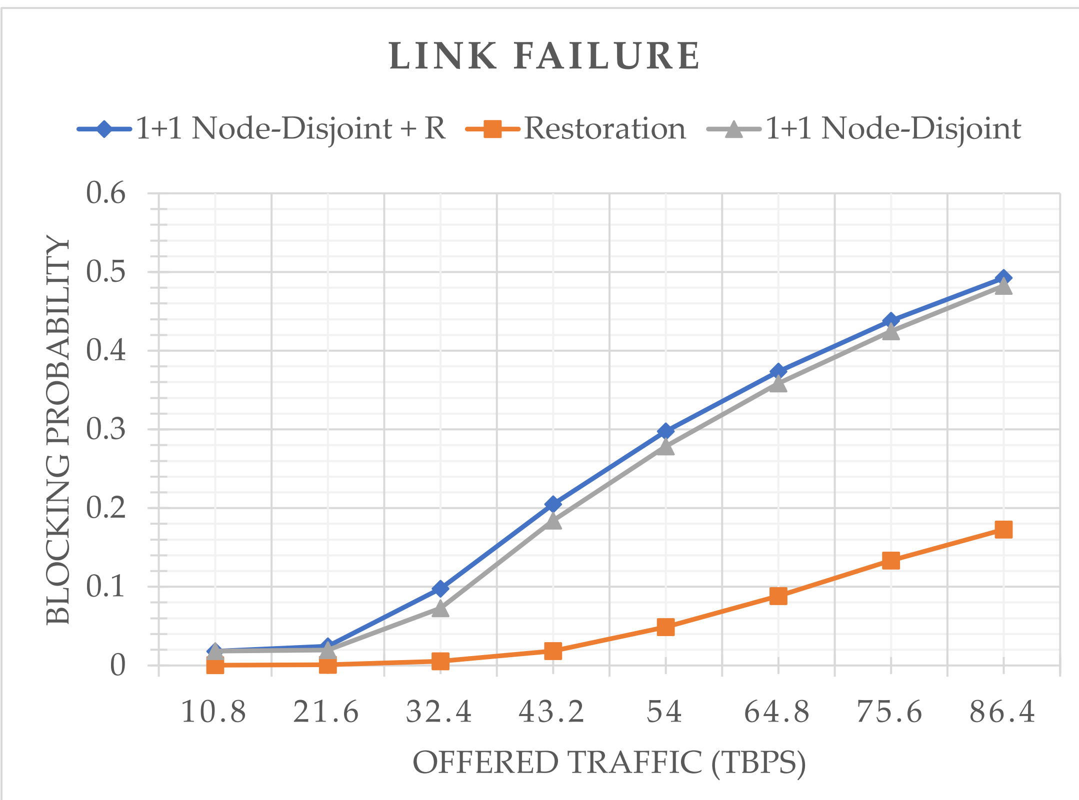

Figure 15: Node-Disjoint Protection and Restoration Blocking Probability in Link Failure

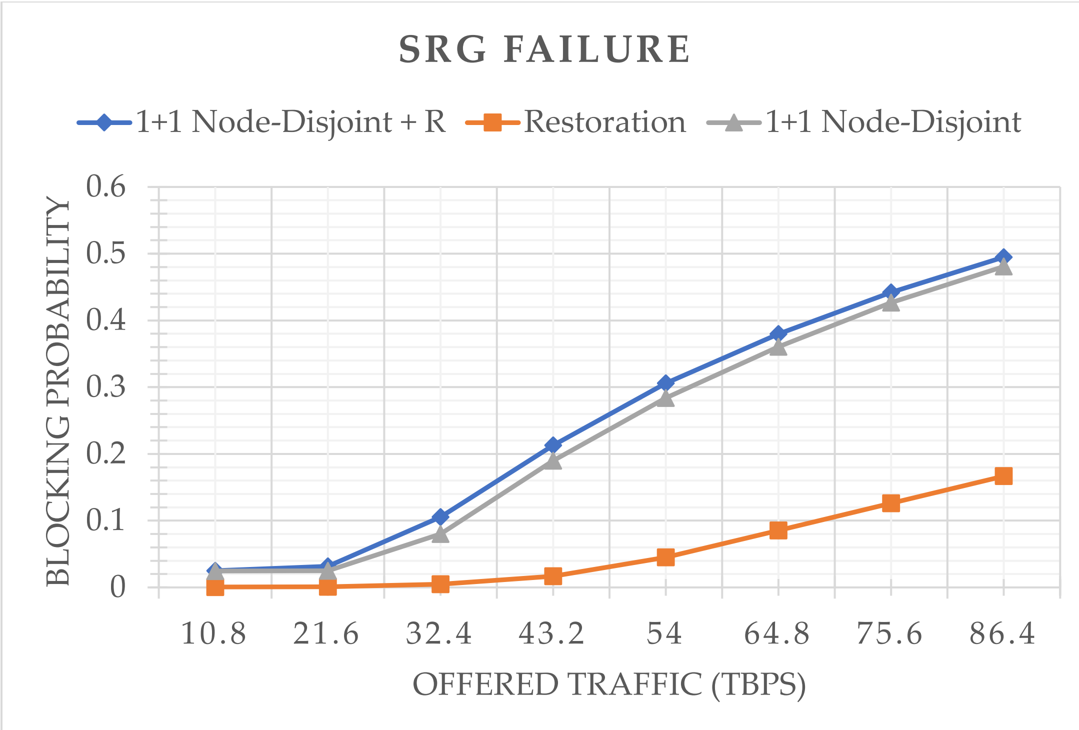

Figure 16: Node-Disjoint Protection and Restoration Blocking Probability in SRG Failure

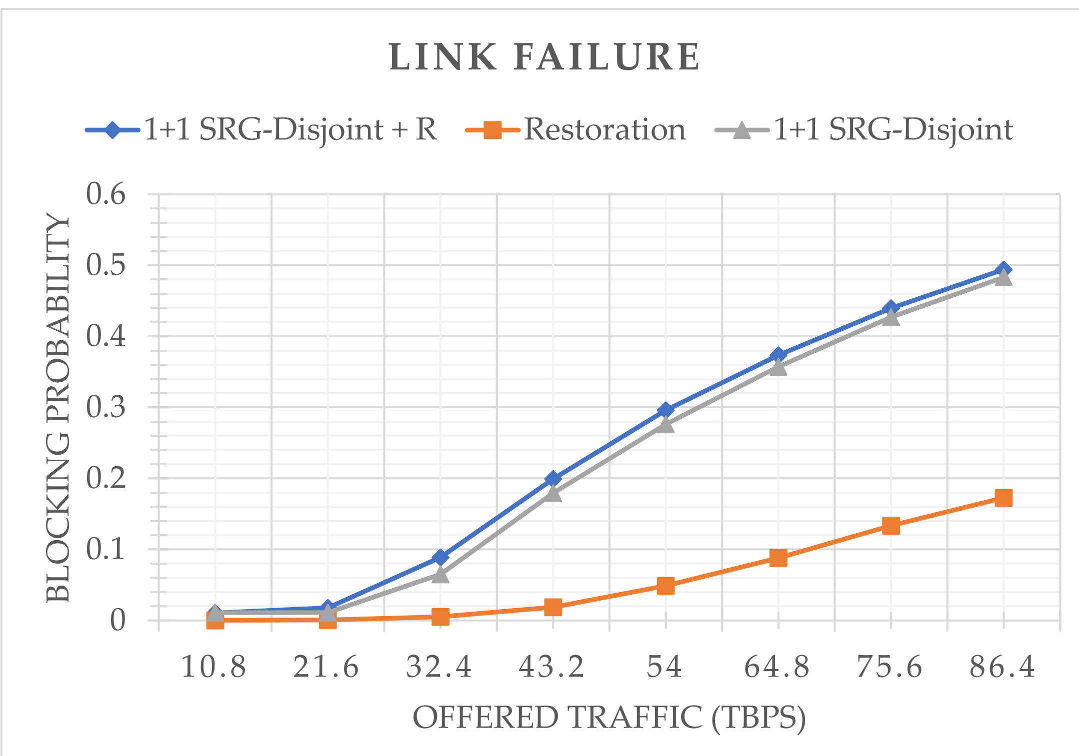

Figure 17: SRG-Disjoint Protection and Restoration Blocking Probability in Link Failure

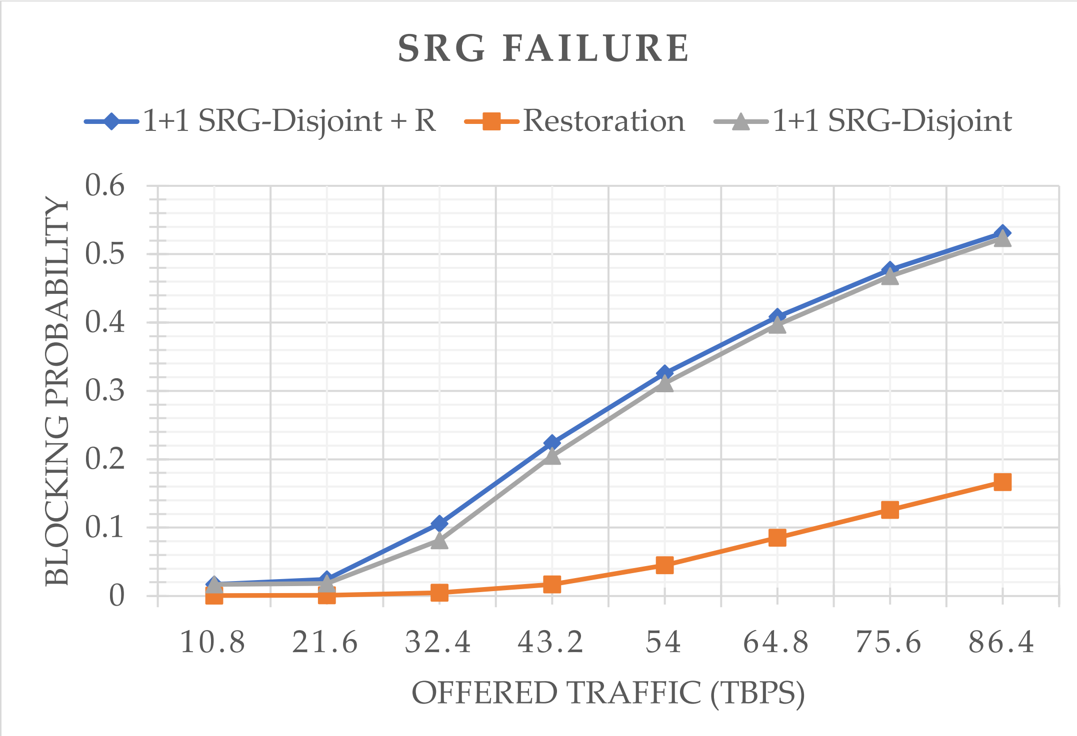

Figure 18: SRG-Disjoint Protection and Restoration Blocking Probability in SRG Failure

As shown in the above results, resource utilization of the hybrid resiliency mechanisms is compared with resource utilization of non-hybrid protection and Restoration schemes (before combination) in times of link and SRG failures. The results indicate that the hybrid resiliency mechanisms have higher blocking probabilities than that of non-hybrid counter parts. This is due to the fact that combining Protection and Restoration schemes requires more resources than they used in their separate form, and the resource contention for recovering the faults increases. These higher resource requirement (cumulative effect of protection and restoration resource usage) and higher resource contention for resources in times of failures induce higher blocking probability in the network provisioned with hybrid resiliency mechanisms.

Blocking Probability Comparison of Proposed Hybrid Resiliency Mechanisms

This part of simulation compares blocking probability of the proposed constraint-based hybrid resiliency mechanism in link and SRG failure occurrences. Hence, blocking probability of 1+1 Link-Disjoint + Restoration, 1+1 Node-Disjoint + Restoration and 1+1 SRG-Disjoint + Restoration are compared. As it can be seen on Figure 19 below, blocking probability of 1+1 Node-Disjoint + Restoration during link failures is on average 3% higher than that of 1+1 Link-Disjoint + Restoration at lower offered traffic loads less than 43.2Tbps. It is due to the presence of node-disjoint requirement of primary and backup paths to be provisioned. Since this node-disjoint constraint excludes all links connected to the node in question, it makes the connection provisioning to take more network resources. In this case the resources which are not node-disjoint cannot be used in the provisioning of primary and backup paths.

Figure 19 also shows that 1+1 Link-Disjoint + Restoration and 1+1 SRG-Disjoint + Restoration have slightly the same blocking probability at entire offered traffic loads, this is due to the fact that link-disjoint is the subset of SRG-disjoint. That means, since primary and backup links in resiliency mechanisms that involve SRG-Disjoint constraint are also link-disjoint, effect of link failures on both resiliency mechanisms resource utilization is very similar.

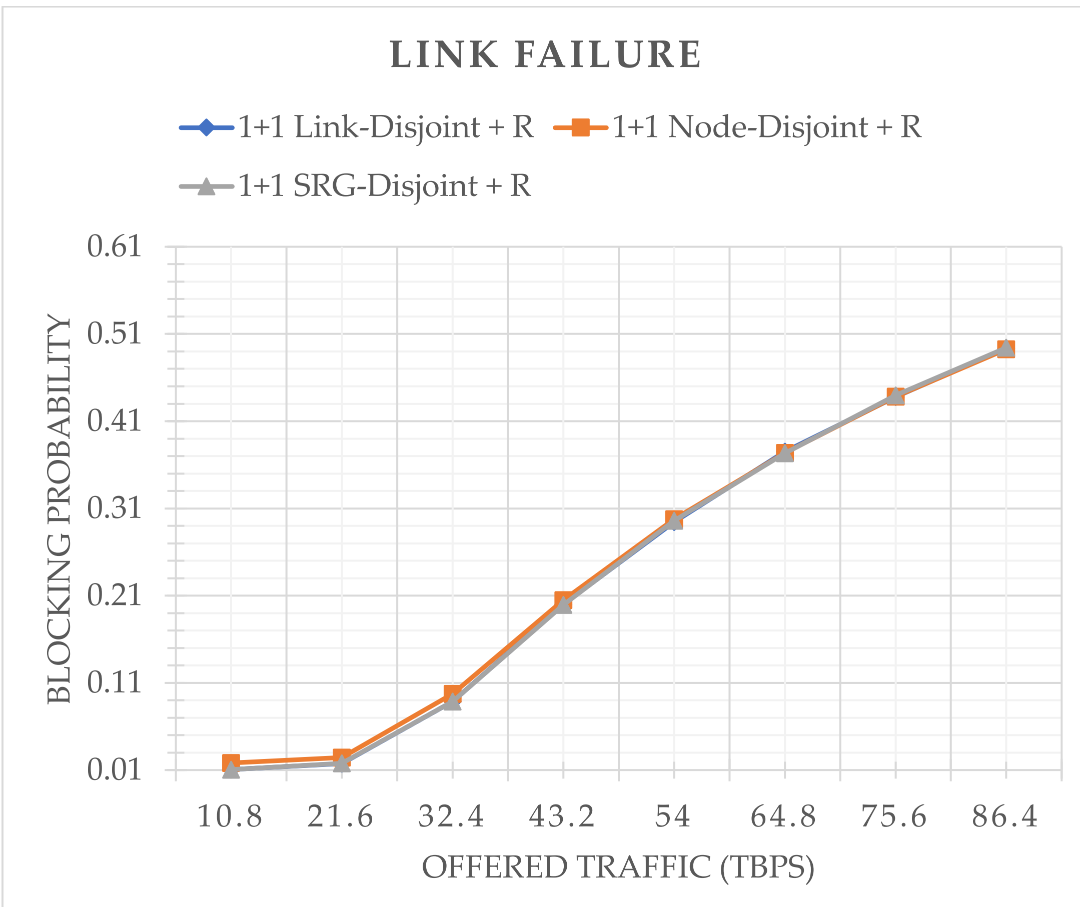

Figure 19: Blocking Probability of Hybrid Resiliency Mechanisms in link failure

Figure 20 as shown below, presents resource utilization of the hybrid resiliency mechanisms in the case of SRG failures. The result shows that 1+1 Node-Disjoint + Restoration has on average 0.9% higher blocking probability at lower loads less than 43.2Tbps and 1+1 SRG-Disjoint + Restoration has on average 14% higher blocking probability at higher offered traffic loads greater than 43.2Tbps when they are compared to 1+1 Link-Disjoint + Restoration. The higher blocking probability in 1+1 SRG-Disjoint + Restoration in SRG failures is due to involvement of SRG-Disjoint constraint which tries to exclude a group of links affected by failure in provisioning process of incoming connections. In SRG failures, resource utilization in 1+1 Node-Disjoint + Restoration is competent with 1+1 Link-Disjoint + Restoration at higher offered traffic loads. Hence, it is becoming difficult to find SRG-Disjoint paths while offered traffic is increased and SRG failure is introduced.

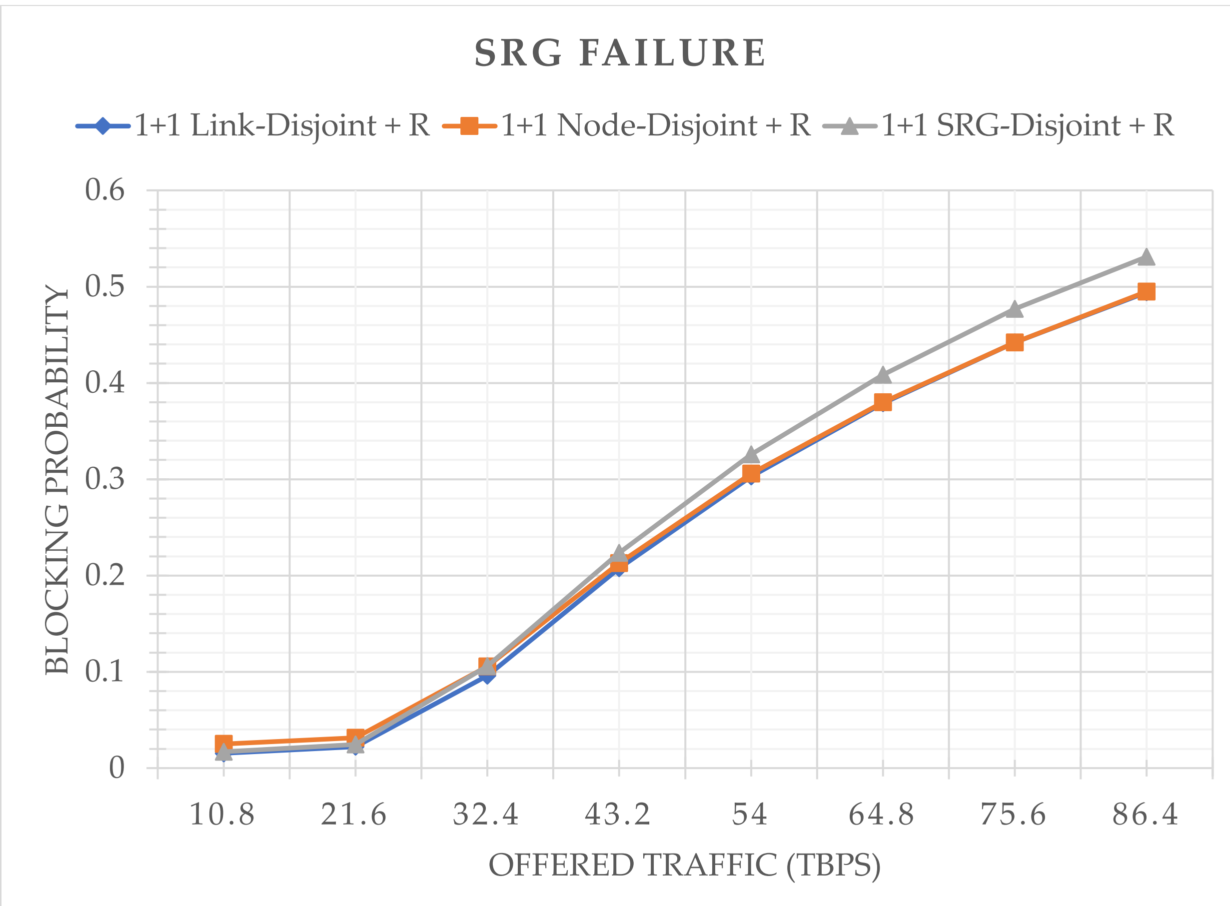

Figure 20: Blocking Probability of Hybrid Resiliency Mechanisms in SRG failure

Recoverability of Non-hybrid Resiliency Mechanisms

The simulation results presented in this section compare the probability of successfully recovering a connection, which can be referred to as recoverability, in non-hybrid resiliency mechanisms in times of link and SRG failures. As it can be noticed on Figure 21 and Figure 22, recoverability of restoration in both link and SRG failures is better than protection resiliency mechanisms at lower traffic loads. However, recoverability of restoration decreases gradually as offered traffic increases since the resource is becoming saturated. In protection schemes (1+1 Link-Disjoint, 1+1 Node-Disjoint and 1+1 SRG-Disjoint) backup resources are reserved which help to recover link and SRG failures in consistent performance.

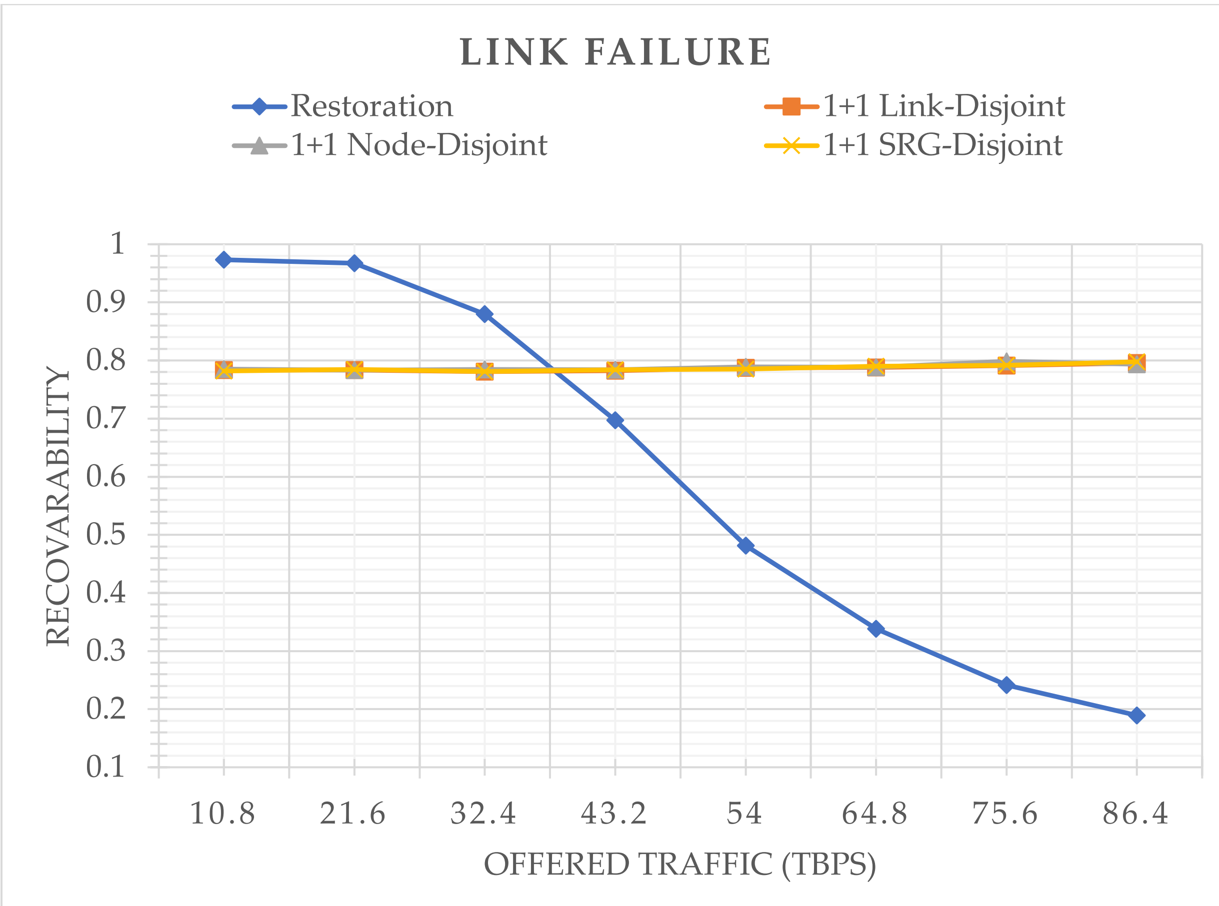

Figure 21: Recoverability of Protection and Restoration in Link Failure

As shown on figure 21 above, about 80% of the connection requests, which are affected by link failure, are successfully recovered in all protection schemes. Recoverability performances of protection schemes are nearly equal, because primary and backup paths are guaranteed to be link-disjoint in all protection schemes which helps them to recover link failures efficiently.

Figure 22 shown below, indicates that recoverability performances of 1+1 SRG-Disjoint, 1+1 Node-Disjoint and 1+1 Link-Disjoint protection schemes in their orders in the case of SRG failure. The result indicates that SRG-Disjoint scheme can bypass SRG failures more effectively than other protection schemes. SRG-Disjoint can recover about 76% of connection recovery attempts due to SRG failures. Similarly, Node-Disjoint and Link-

Disjoint 1+1 Protection schemes can recover about 73% and 70% of the recovery attempts of connections failed due to SRG failure, respectively.

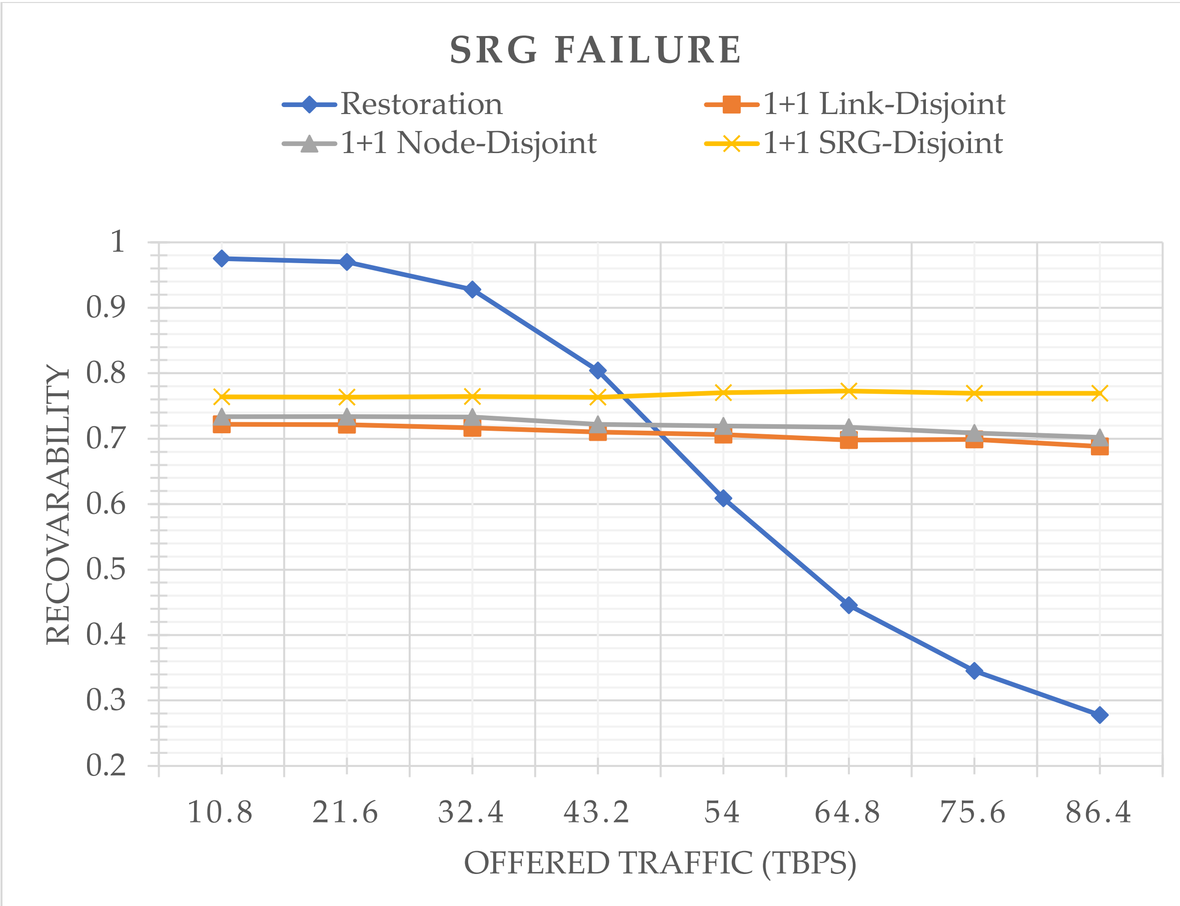

Figure 22: Recoverability of Protection and Restoration in SRG Failure

Recoverability Comparison of Hybrid and Non-hybrid Resiliency Mechanisms

The recoverability simulation results collected for hybrid and non-hybrid resiliency mechanisms which are exposed to link and SRG failures are presented in this subsection. The results depicted on the following figures, show that hybrid resiliency mechanisms perform better in recoverability than that of their non-combined counter parts. That means, 1+1 Link-Disjoint + Restoration recoverability is enhanced by combining 1+1 Link-Disjoint and Restoration (Figures 23&24), 1+1 Node-Disjoint + Restoration recoverability performance is enhanced by combining 1+1 Node-Disjoint and Restoration (Figures 25&26), and 1+1 SRG-Disjoint + Restoration recoverability is enhanced by combining 1+1 SRG-Disjoint and Restoration (Figures 27&28) in both link and SRG failure risks. These hybrid resiliency mechanisms exploit the advantages of restoration and protection. The protection schemes guarantee the recovery of the first single failures and restoration tries to recover incoming multiple failures proportional to available spare network resources.

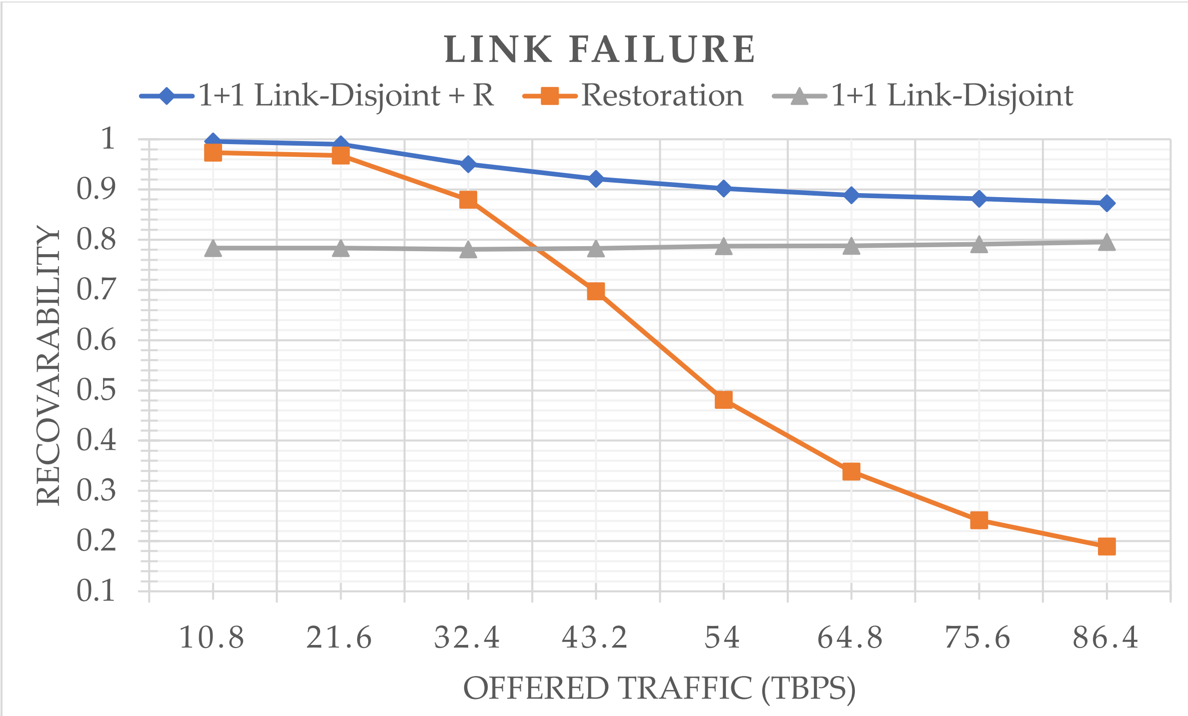

Figure 23: Link-Disjoint Protection and Restoration Recoverability in Link Failure

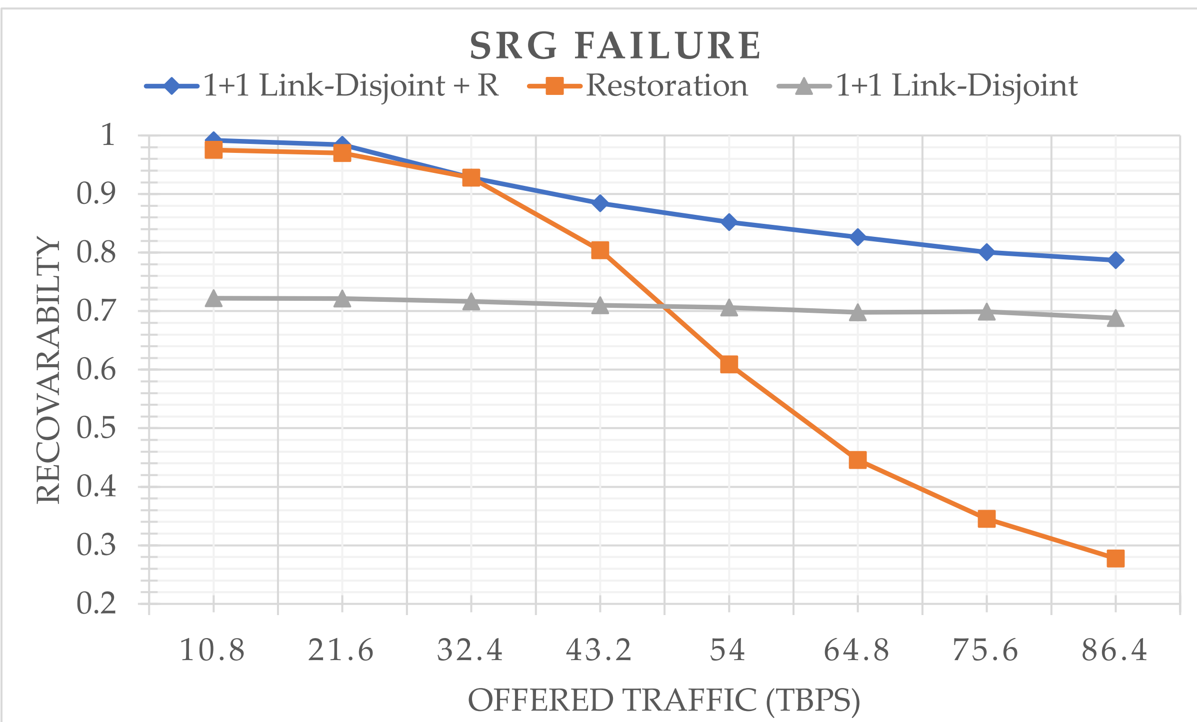

Figure 24: Link-Disjoint Protection and Restoration Recoverability in SRG Failure

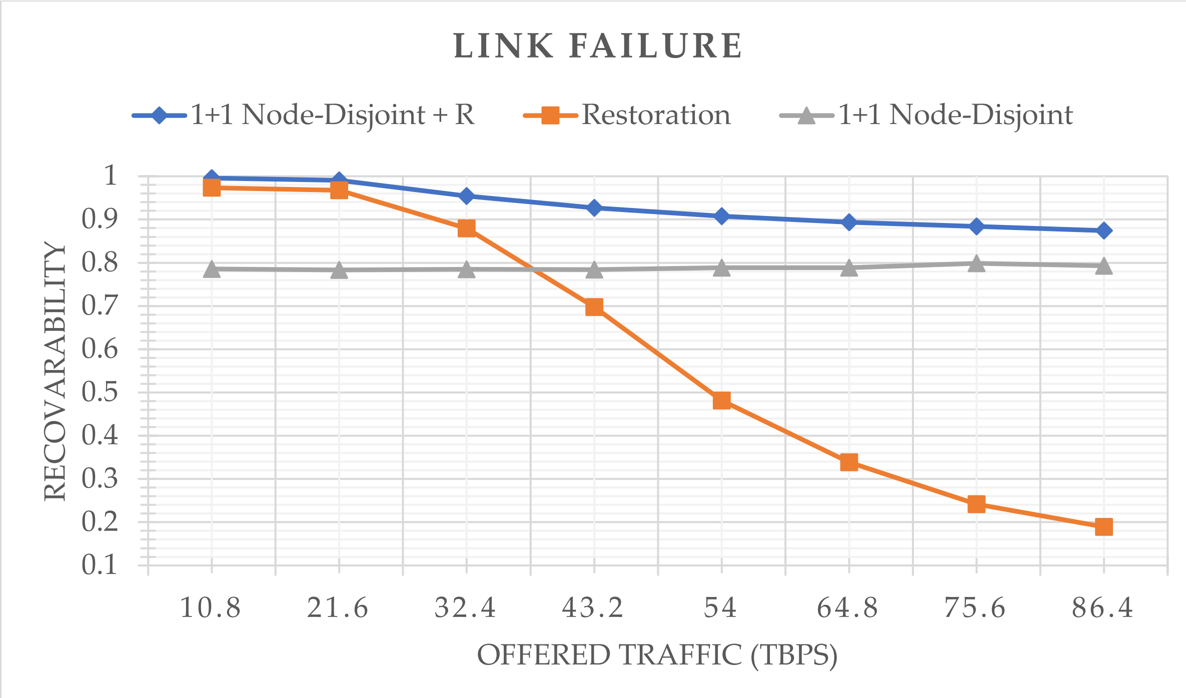

Figure 25: Node-Disjoint Protection and Restoration Recoverability in Link Failure

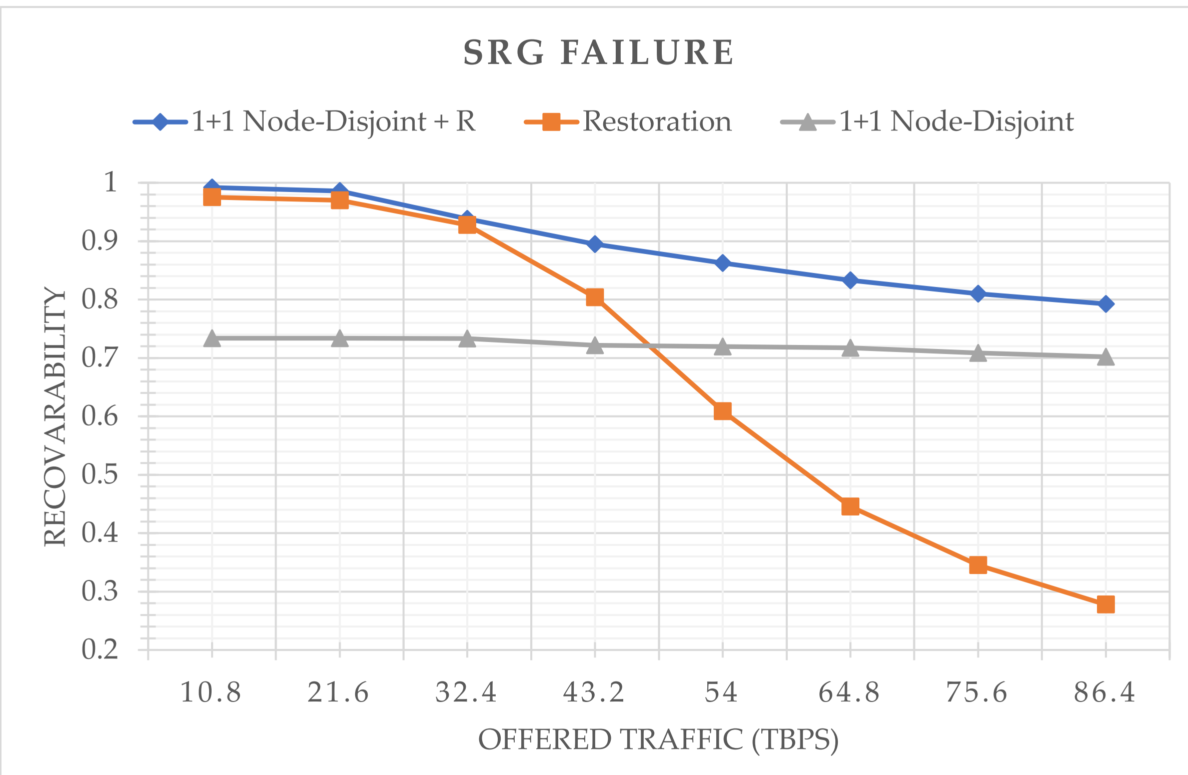

Figure 26: Node-Disjoint Protection and Restoration Recoverability in SRG Failure

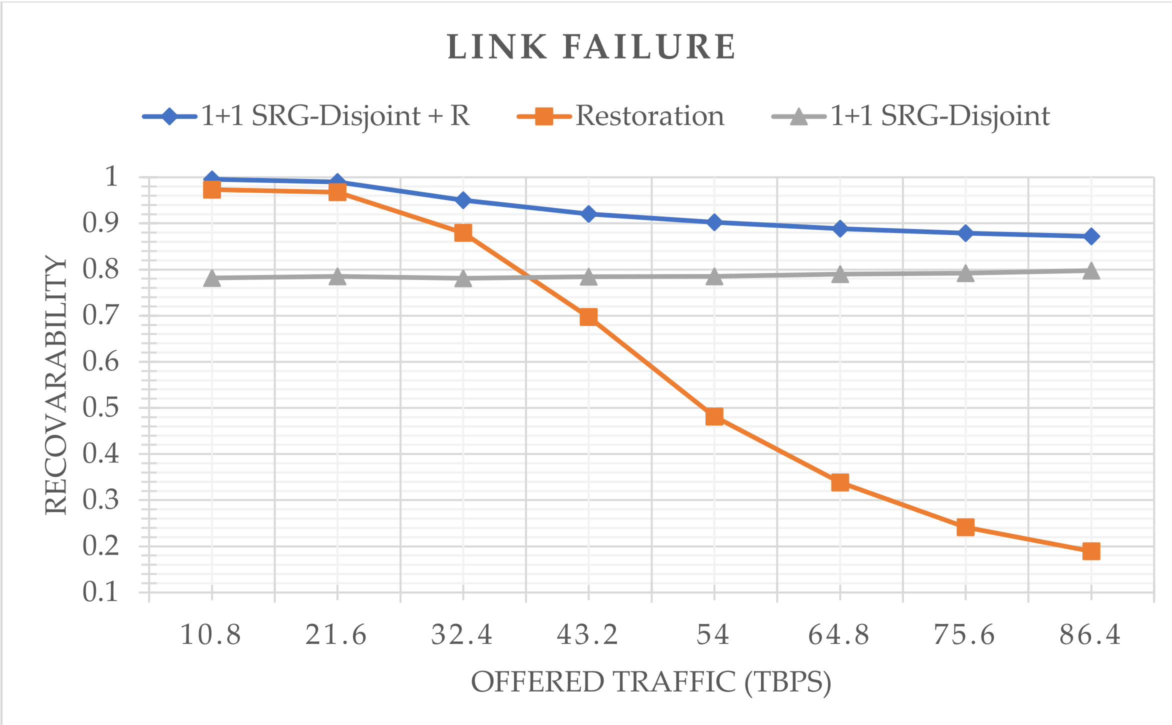

Figure 27: SRG-Disjoint Protection and Restoration Recoverability in Link Failure

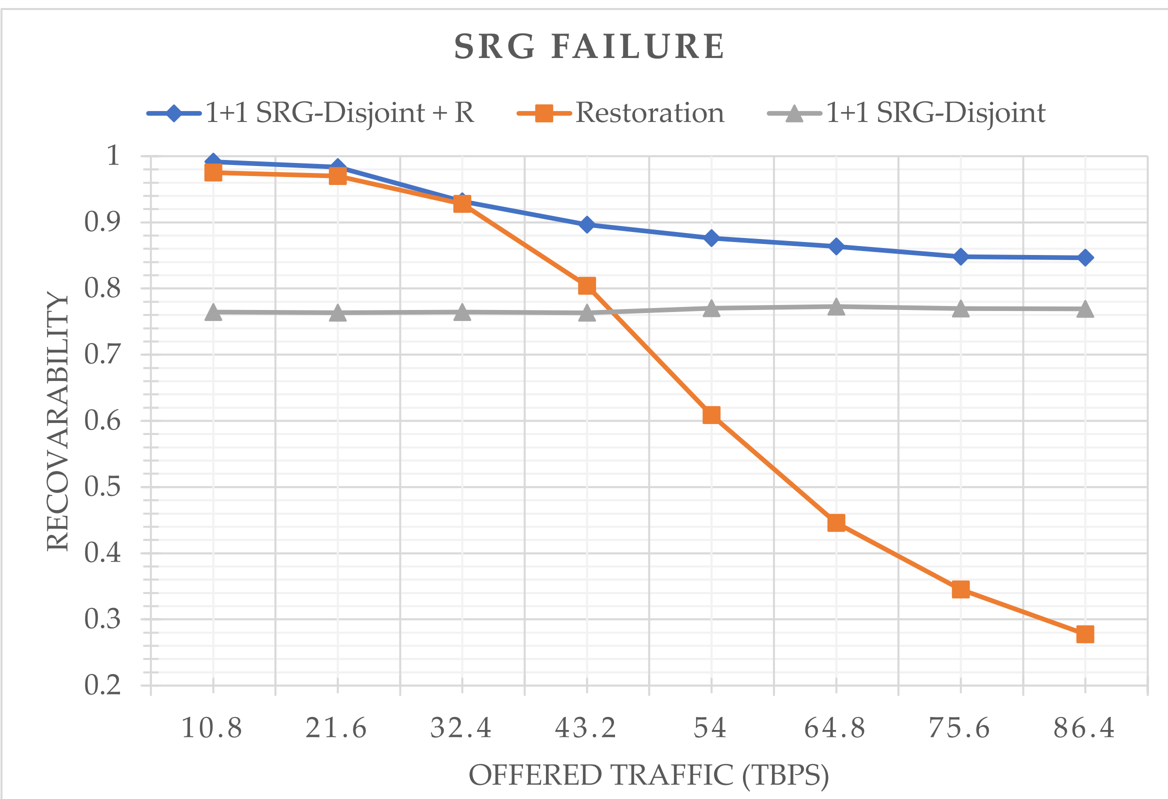

Figure 28: SRG-Disjoint Protection and Restoration Recoverability in SRG Failure

Recoverability Comparison of Hybrid Resiliency Mechanisms

The results plotted on the following figures describe recoverability performance of the newly proposed constraint-based hybrid resiliency mechanisms. The recoverability of 1+1 Link-Disjoint + Restoration, 1+1 Node-Disjoint + Restoration and 1+1 SRG-Disjoint + Restoration against link and SRG failures as a function of total offered traffic is presented here. As depicted on Figure 29, recoverability of 1+1 Node-Disjoin + Restoration is the best and 1+1 SRG-Disjoint + Restoration is fairly competent with 1+1 Link-Disjoin + Restoration in almost all offered traffic values during link failures. 1+1 Node-Disjoint + Restoration has on average 0.5% higher recoverability than that of 1+1 Link-Disjoint + Restoration.

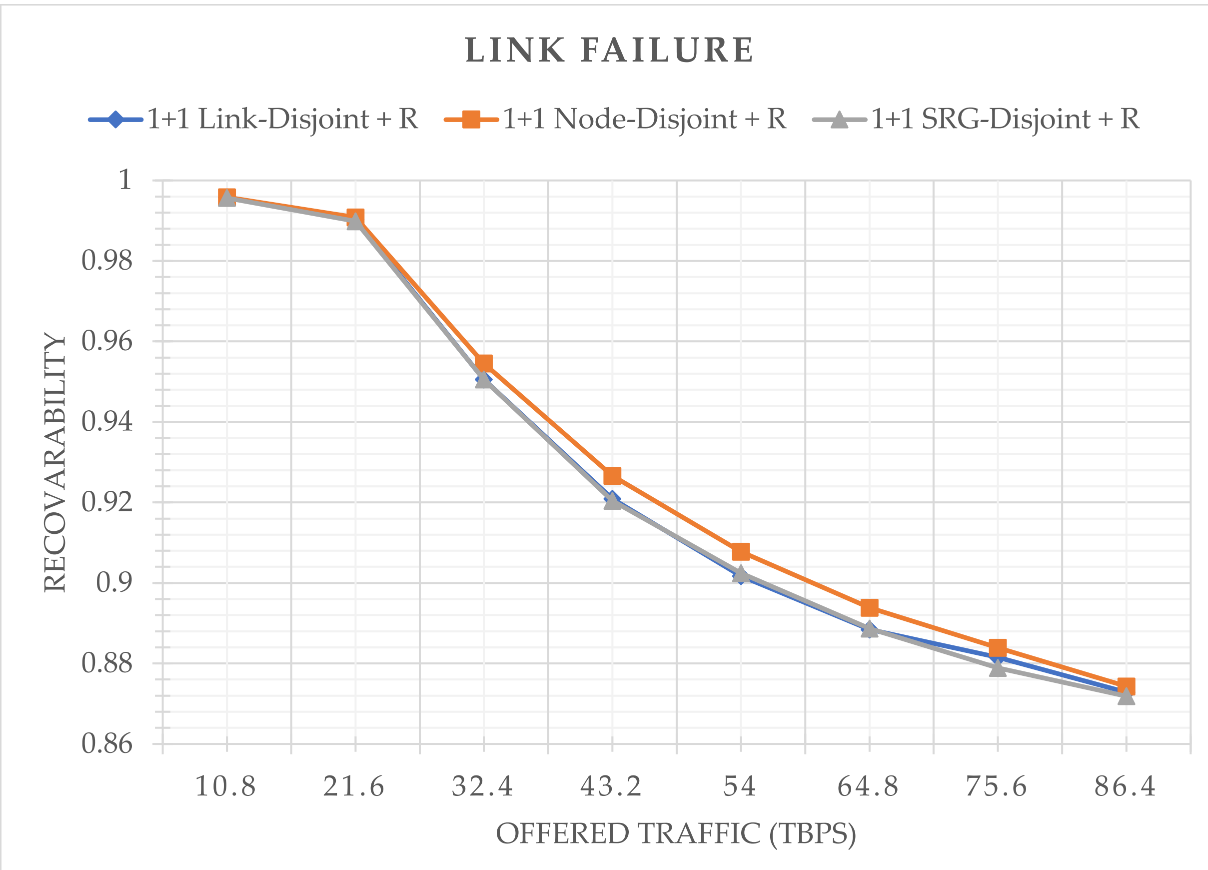

Figure 29: Recoverability in Hybrid Resiliency Mechanisms in Link Failure

The result plotted on Figure 30 shows that the performance of successfully recovering from SRG failures is highest in 1+1 Node-Disjoint + Restoration at lower offered traffic loads, and in 1+1 SRG-Disjoint + Restoration at higher loads. 1+1 Node-Disjoint + Restoration and 1+1 Link-Disjoint + Restoration show lower recoverability performance in their order at higher traffic loads. 1+1 Node-Disjoint + Restoration has on average

0.56% higher recoverability than 1+1 Link-Disjoint + Restoration at lower offered traffic less than 43.2Tbps. 1+1 SRG-Disjoint + Restoration also has on average 16.8% higher recoverability than 1+1 Link-Disjoint + Restoration at higher offered traffic greater than 43.2Tbps. As it is shown in both figures, recoverability of the resiliency mechanisms against link and SRG failures is decreasing as offered traffic load increases. It is due to the resource saturation in the network.

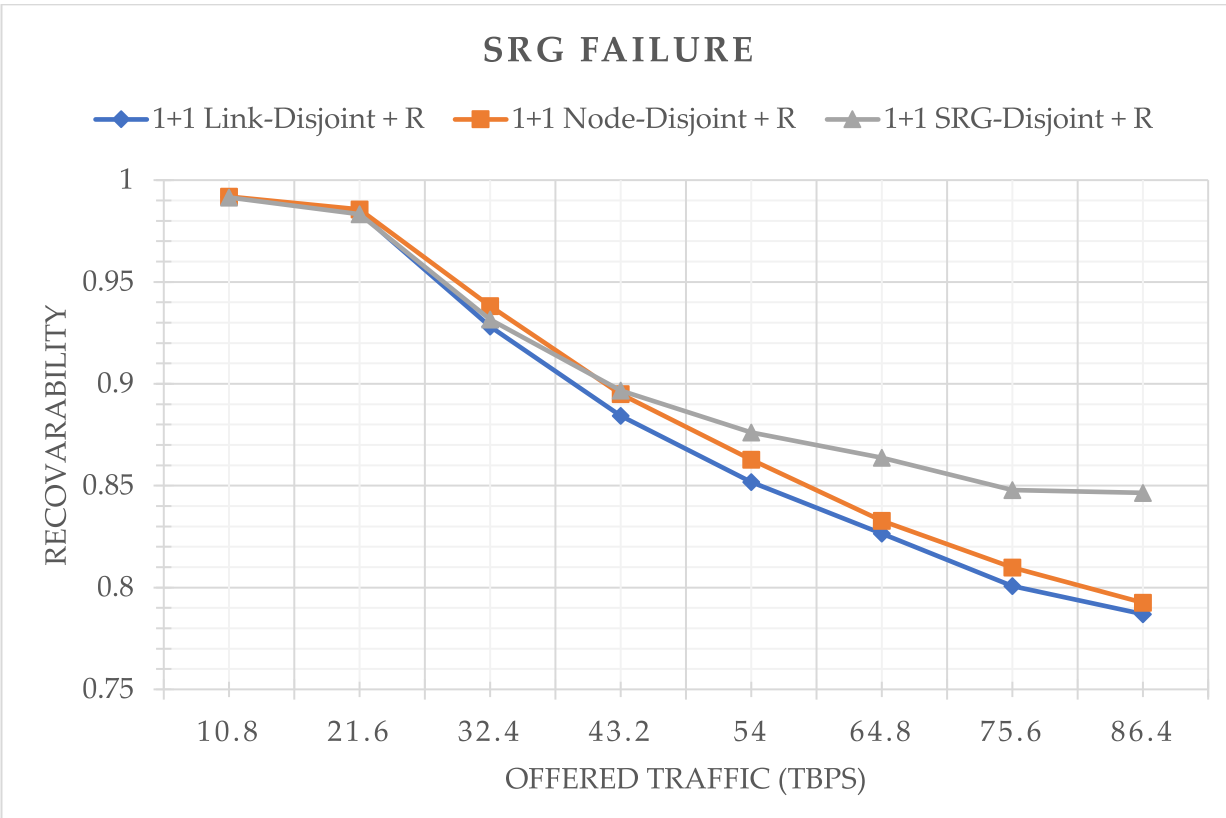

Figure 30: Recoverability of Hybrid Resiliency Mechanisms in SRG Failure

5.2.3 Availability Simulation

Availability measurement of the proposed resiliency mechanisms is conducted based on the simulation setup and simulation assumptions which are considered in simulation of RWA algorithm usage, as discussed in Section 5.1. This section will estimate availability of the proposed hybrid resiliency mechanisms for the given network under link and SRG failures. Then, availability results of the hybrid resiliency mechanisms will be compared with availability results of non-hybrid resiliency mechanisms based on the same network design and assumptions.

Simulation Assumptions

For this simulation Addis Ababa Metro OTN Backbone network is used as a reference topology. As mentioned in section 5.1, this reference topology has 10 ASON enabled nodes and 48 unidirectional links. Each link has 80 wavelengths and each wavelength has a traffic capacity of 40Gbps. Then, 90 equal traffic demands are generated by assuming there is traffic demand between each node pairs, except self-demands. Additionally, 24 SRG are defined in the reference topology. It is also assumed that there is no wavelength conversion and regeneration (O-E-O conversion) between source-destination pairs of nodes.

The reference network is provisioned with deterministic connection requests according to their recovery types. The simulation also assumes that the network is provisioned accordingly without blocking any connection requests. In this simulation, no connection request is blocked in no failure states when the network is in its normal condition. Then, the simulation assumes link or SRG failures occur in the network randomly with exponential distribution. Link or SRG failures will occur according to conservative values of MTBF=8748hrs and MTTR=12hrs, which means per link or SRG failure will occur on average once in a year and it will be repaired in half a day. This simulation considers no failure, single failure and double failure network states together in the network to estimate the availability. It also assumes that no multiple failures more than dual failures will occur and if they occur traffic will be interrupted.

Simulation Results and Discussion

Network availability simulation is run for different offered traffic values starting from 3.6Tbps to 21.6Tbps with a range of 3.6Tbps. This offered traffic range is selected in order to fulfil that no traffic is blocked in normal condition of the network during provisioning process.

Network Availability Comparison of Resiliency Mechanisms

The following two figures, Figure (31&32), compare network availability of the hybrid and non-hybrid resiliency mechanisms during SRG and link failures. The results on the figures shows that availability of protection schemes (1+1 Link-Disjoint, 1+1 Node-Disjoint and 1+1 SRG-Disjoint) is about 0.999989 in SRG failures and 0.999952 in times of link failures. The availability of restoration and hybrid resiliency mechanisms (1+1 Link-

Disjoint + Restoration, 1+1 Node-Disjoint + Restoration, and 1+1 SRG-Disjoint + Restoration) is 0.999995 in SRG failures and 0.999957 in link failures.

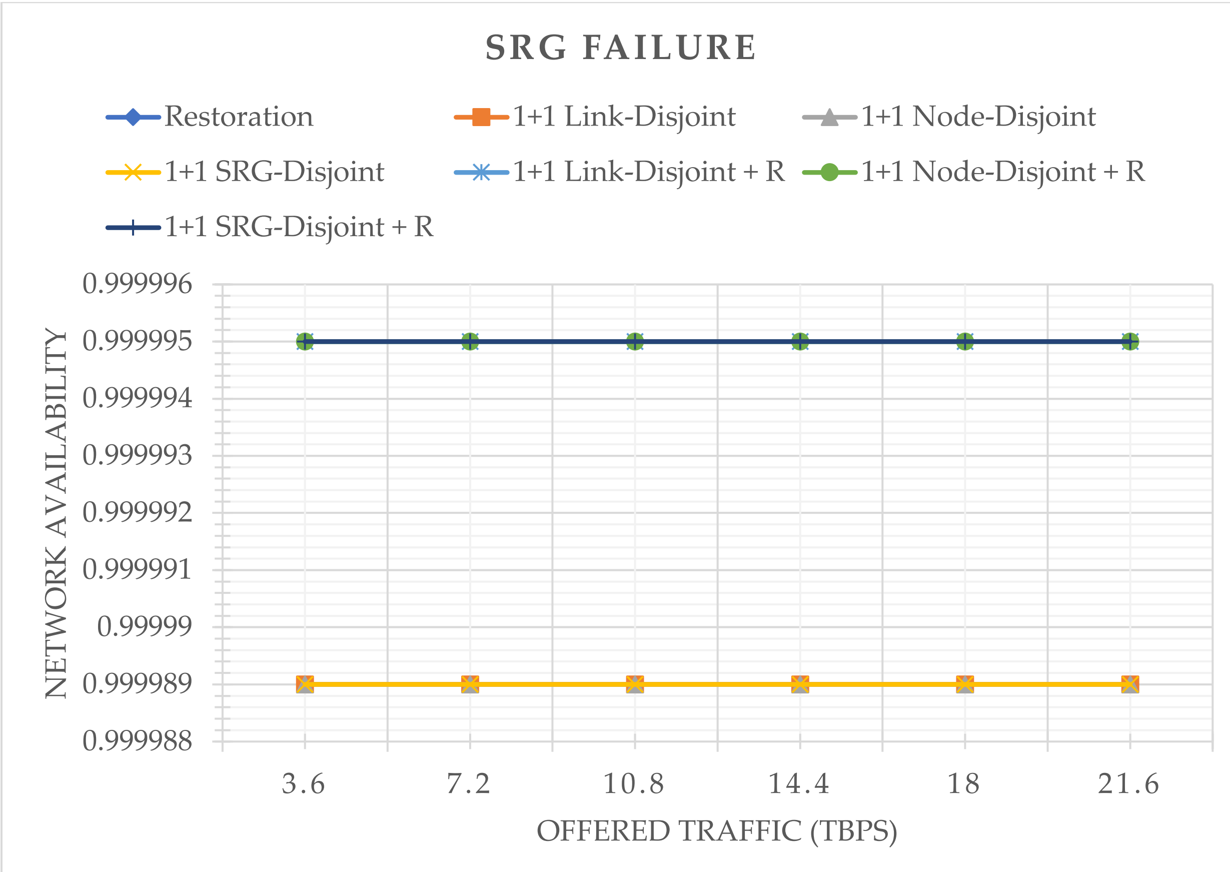

Figure 31: Availability of Resiliency Mechanisms in link failure

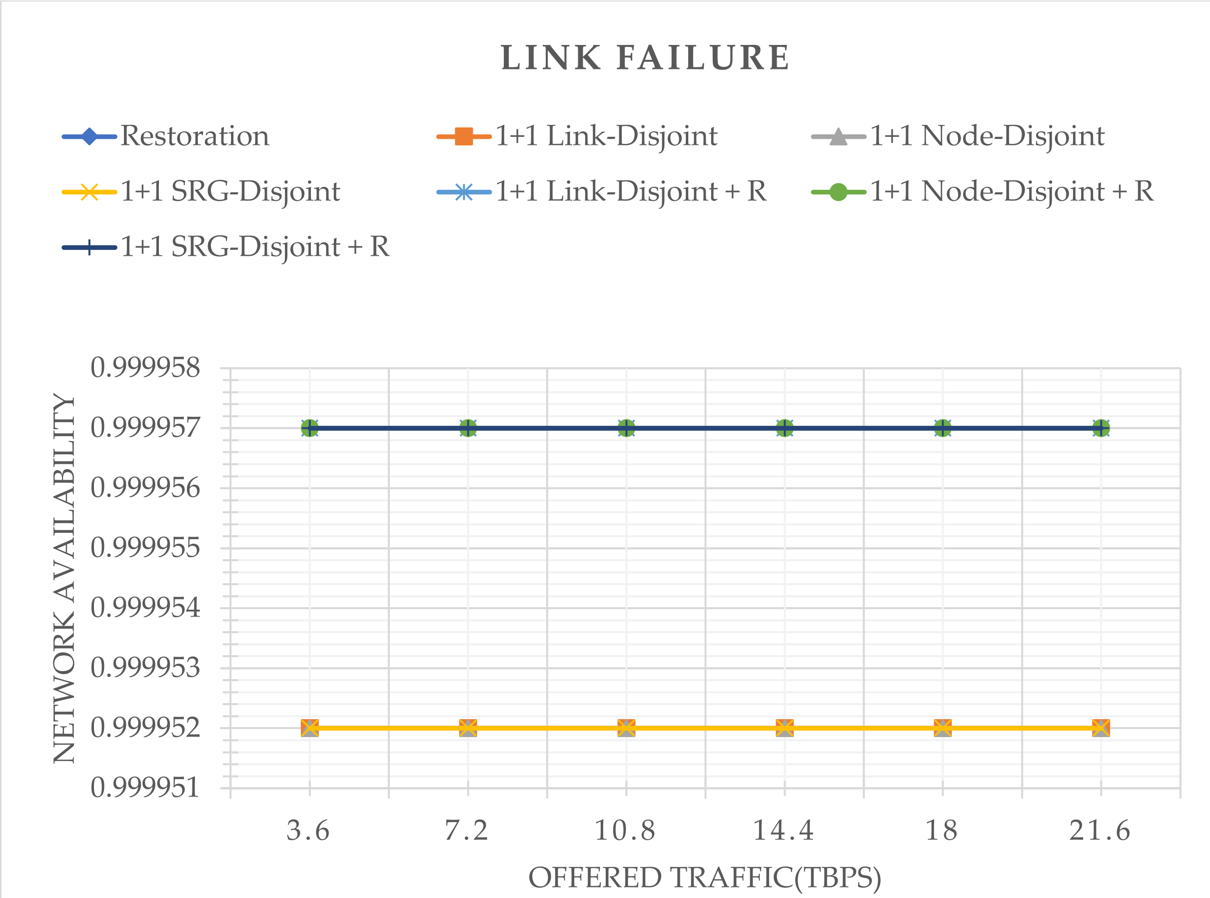

Figure 32: Availability of Resiliency Mechanisms in SRG failure

These results indicate that the network availability in the resiliency mechanisms is highly dependent on the available spare network resources which is utilized by the restoration schemes in times of dual failures. Hence, the availability of the network is enhanced to a value proportional to the available spare resource in the network. Since the network which is used in this simulation is designed to have excess spare resources to avoid blocking of connection requests during connection provisioning, the availability of restoration becomes higher and so the hybrid resiliency mechanisms too.

Chapter Six

6. Conclusion and Future Work

This chapter is about the conclusion, future works and recommendations of the research work. The research work covers the performance evaluation of the RWA algorithms in ASON resiliency mechanisms (in protection and restoration specifically). It also proposes new constraint-based hybrid resiliency mechanisms based on the performance results obtained from the RWA performance evaluation. Then, the research work evaluates the performances of the proposed resiliency mechanisms in terms resource utilization and service performance quality. Resource utilization is measured in terms of blocking probability, and service performance quality is measured in terms of recoverability and network availability in times of link and SRG failure risks. The overall results, the future works and recommendations are summarized as follows.

6.1 Conclusion

This research work proposes two options to fulfil requirement of providing better quality services with minimum network resources. The first solution is using an RWA algorithm that utilizes network resources as low as possible in resiliency mechanisms for dynamic ASON service provisioning. This can be accomplished by comparing resource utilization of the widely used RWA algorithms in protection and restoration resiliency mechanisms. The second solution to enhance service performance qualities is combining protection and restoration resiliency mechanisms which helps to exploit advantages of both schemes in times of multiple failures. 1+1 DPP and Restoration are widely used resiliency mechanisms in ASON service provisioning.

Even if DPP has faster recovery time, its resource utilization is very poor since it reserves backup resources for each connection requests. The way how primary and backup paths are established in a network has also its own effect. The paths in protection and restoration schemes of ASON dynamic service provisioning are established with the help of RWA algorithms. Hence, it is vital issue to employ appropriate RWA algorithms to avoid further resource wastage. Based on this objective, the research work considers four adaptive source-based k-shortest path routing algorithms coordinated with First-Fit wavelength assignment algorithm, which are widely used in ASON dynamic service provisioning. The routing algorithms first compute k alternative shortest paths and then use certain criteria to select one route among them and assign available resources. The routing algorithms considered for this research work are Shared Risk Group (SRG) Disjoint Aware First-Fit routing, Alternate Routing, Least Congested Routing (LCR) and Load Sharing.

In this research work, Integer Linear Programming (ILP) is formulated for RWA algorithms and resiliency mechanisms. However, these analytical models are NP-complete and difficult to solve, simulation models (in Net2Plan) which are based on iterative algorithms are used in this research work. The research work shows, in its performance evaluation, that Least congested routing and Alternate routing have better performance in terms of blocking probability and network availability. Hence, the results of the research show that alternate routing and Least congested routing can be used at lower loads, and alternate routing is a best choice to use in higher offered loads even if Least Congested Routing is still a better competent. From the overall performance results, it can be concluded that Alternate Routing is a better choice for both protection and restoration schemes.

Then, based on performance evaluation results of RWA algorithms in protection and restoration resiliency mechanisms, the research work proposes new constraint-based hybrid resiliency mechanisms. These hybrid resiliency mechanisms are combination of different constraint flavors of 1+1 DPP and restoration. 1+1 Link-Disjoint, 1+1 Node-Disjoint and 1+1 SRG-Disjoint flavors of 1+1 DPP resiliency mechanisms are combined with the restoration scheme to produce the hybrid resiliency mechanisms. This option enhances service quality performance (availability and recoverability) of the network with a cost of relatively higher blocking probability. The research work also formulates ILPs for constraint-based 1+1 DPP and restoration resiliency mechanisms. However, the ILP models are NP-complete and difficult to solve. Hence, Net2Paln simulation model is used in which iterative algorithms are deployed to combine and evaluate their performances.

The results of these research work show that proposed constraint-based hybrid resiliency mechanisms have better recoverability with relatively higher blocking probability than that of non-combined counter parts. Blocking probability of 1+1 Node-Disjoint + Restoration is noticed to be higher at lower offered traffic values for both link and SRG failures. 1+1 SRG-Disjoint + Restoration shows highest resource usage at higher offered traffic loads. This research work also compares recoverability of the hybrid resiliency mechanisms which shows 1+1 Node-Disjoint + Restoration has highest recoverability in times of link failures and at lower traffic loads of SRG failures. 1+1 SRG-Disjoint + Restoration, 1+1 Node-Disjoint + Restoration and 1+1 Link-Disjoint + Restoration perform recoverability in their order at higher offered traffic loads. This research results also show that network availability of the proposed resiliency mechanisms is enhanced when it is compared to separate and non-combined protection schemes.

6.2 Recommendations

Based on the results found on simulations, Least Congested Routing is preferable to be used at lower offered traffic up to 75.6Tbps and 43.2Tbps in Restoration and Protection, respectively. Alternate Routing is a good choice to use at higher offered traffic for both schemes. If the primary concern in the SLA contracts is network availability, it is recommended to use Alternate Routing algorithm, especially in services provisioned with 1+1 DPP schemes.

According to the results from performance evaluation of hybrid resiliency mechanisms, 1+1 Node-Disjoint + Restoration can be recommended for services that require best recoverability against multiple link failure risks in the network. But, in times of multiple SRG failure risks it is better to provision services with 1+1 SRG-Disjoint + Restoration when the offered traffic load is greater than 43.2Tbps. 1+1 Node-Disjoint + Restoration can be used for services that demand higher recoverability against SRG failure risks at lower offered traffic loads below 43.2Tbps.

6.3 Future Works

As future work, SPP can be considered in the hybrid resiliency mechanisms instead of DPP even if management and the implementation of SPP is quite complicated. SPP can contribute significant importance in dynamic service provisioning with lower blocking probability. Different variants of constraint-based resiliency mechanisms can also be included in future works. These variant of constraint-based resiliency mechanisms may use the same constraints, protection and restoration schemes. Their difference is on how restoration is triggered in times of failure occurrences. For instance, it is possible to produce a resiliency mechanism which always keeps the 1+1 DPP as long as there are enough spare network resources. In these resiliency mechanisms, whether it is link-disjoint, node-disjoint or SRG-disjoint, restoration is triggered every time when primary or backup paths fail, so that it creates permanent 1+1 protection.

It is also important to consider additional RWA algorithms to provide variety of options that could meet demands of service providers and customers in provisioning process. Impairment-aware RWA algorithms, like OSNR-Aware RWA can be considered to study effect of physical layer impairments on resource utilization and service performance quality in ASON resiliency mechanisms. The other future work that needs attention is, risk assessment study on optical networks. In this research study, MTTR and MTTF values, that are used to estimate availability of network, are taken with a conservative assumption. However, such type of performance estimations requires a specific risk assessment study to obtain representative values of MTTF and MTTR for a specific network.

The simulations in this research work depend on Addis Ababa Metro OTN backbone network which has only 10 ASON enabled nodes. As a future work, the same study can be conducted for main backbone networks by incorporating node failure risks in addition to link/SRG failures and impairment aware RWA algorithms. Such research studies which are based on node failure risk model and impairment aware RWA algorithm will be more feasible on main backbone networks with a greater number of nodes, links and longer distances between nodes. In this research work, light-paths used for connection request set up are single line rate (40Gbps) which are uniformly used in each traffic demand of the network. However, effect of using mixed line rates of light paths (10Gbps, 40Gbps and 100Gbps) on the performance of resiliency mechanisms as well as on performance of the entire network can be further studied.

References

[1]. O. Brun and S. Baraketi, "Routing and Wavelength Assignment in Optical Networks," Tech. Report. hal-01062321, September 2014.

[2]. S. Yang et al, "Study on Strategy of Dynamic Joint Routing and Resource Allocation in Layered Optical Transport Networks," *Journal of Electronics (China),* vol. 25, March 2008.

[3]. S. Tomic, "ASON and GMPLS-Overview and Comparison," *Photonic Network Commun.*, vol. 7, no. 2, pp. 111-130, 2004.

[4]. W. Fawaz, "Service Level Agreement and Provisioning in Optical Networks," *IEEE Commun. Mag*., vol. 42, no. 1, pp. 36-43, January 2004.

[5]. W. Colitti et al, "Multilayer quality and grade of service support for high speed GMPLS IP/DWDM networks," *International Conference on Network-Based Information Systems (NBiS),* 2007, pp. 187–196.

[6]. A. Jajszczyk, "Control Plane for Optical Networks: The ASON approach," *China Commun. Mag*, vol. 1, no. 1, pp.113-122, December 2004.

[7]. ITU-T Recommendation G.8080/Y.1304, "Architecture for the Automatically Switched Optical Networks," Amendment 1, March 2003.

[8]. ITU-T Recommendation G.7714/Y.1705, "Generalized Automatic Discovery Techniques", November 2001.

[9]. ITU-T Recommendation G.7715/Y.1706, "Architecture and Requirements for Routing in the Automatically Switched Optical Networks," June 2002.

[10]. E. Mannie (ed.), "Generalized Multi-Protocol Label Switching Architecture," *IETF RFC 3945*, 2004.

[11]. A. Farrel and I. Bryskin, *GMPLS: Architecture and Applications.* Morgan Kauffman, 2005.

[12]. M. Maier, *Optical Switching Networks.* New York, USA: Cambridge University Press, 2008.

[13]. L. Andersson and G. Swallow (eds.), "The multiprotocol label switching (MPLS) working group decision on MPLS signaling protocols," *IETF RFC 3468*, February 2003.

[14]. M. N. Ellanti et al, *Next generation transport networks: data, management, and control planes.* 1st ed., Springer, 2005.

[15]. R. Alnuweri, et al, "Performance of New Link State Advertisement Mechanisms in Routing Protocols with Traffic Engineering Extensions," *IEEE Communications Magazine,* vol. 42, No. 5, pp. 151-162, May 2004.

[16]. J. Lang (ed.), "Link Management Protocol (LMP)," *IETF RFC 4204*, October 2005.

[17]. X. M. Bruin et al., "The Routing Inaccuracy Problem in OTN," Tech. Rep. UPC-DAC-RR-CBA-2006-2, February 2006.

[18]. D. K. Tyagi et al., "Routing and Wavelength Assignment in WDM Network using IWD based Algorithm," *International Conference on Computing, Communication and Automation (ICCCA)*, April 2016

[19]. M. Shadab et al, "Simulation and Analysis of Blocking Probability Using RWA Algorithm for All-Optical Networks," *International Journal of Innovative Research in Computer and Communication Engineering*, Issue 5, May 2014

[20]. P. Wang et al., "A Better ACA for Routing and Wavelength Assignment in ASON with Supporting Different SLA of Services and 10Pbps Network Capacity," *Applied Mechanics and Materials,* vols. 687-691, pp. 4148-4152, 2014

[21]. X. M. Bruin et al, "An Adaptive Routing Mechanism for reducing the Routing Inaccuracy Effects in an ASON," in *Proc. ONDM'03,* Budapest, Hungary, February 2003, pp.333–349.

[22]. H. Zang, J. P. Jue and B. Mukherjee, "A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks," *Optical Network Mag*., vol. 1, no. 1, pp. 47-60, January 2000.

[23]. Z. Na and S. Jaijin, "A Distributed Strategy for Dynamic Routing and Wavelength Assignment in ASON Network," *International Conference on Transparent Optical Networks,* 2005, pp. 201–204.

[24]. X. Bruin, et al, "Hierarchical Routing with QoS Constraints in Optical Transport Networks," *3 IFIP-TC6 Networking Conference*, Athens, Greece, May 2004.

[25]. P. Luo et al, "Dynamic Inter-domain Wavelength Routing Based on Source Routing in ASON," in *Proc. of APOC*, 2006, pp. 44-51.

[26]. S. R. Ehsani, V. Ghorbani and S.A. Shahkooh, "Hierarchical Routing in Optical Networks," *Proc. of IEEE Information and Communication Technologies ICTTA,* 3rd International Conference, 2008, pp. 1-5.

[27]. J. Ahmed et al, "Hybrid Survivability Schemes Achieving High Connection Availability with a Reduced Amount of Backup Resources," J. *Opt. Commun. Netw.,* vol. 5, no. 10, October 2013.

[28]. B. Mukherjee, *Optical Communication Networks*. New York, NY: McGraw-Hill, 1997.

[29]. P. P. Marino, *Network optimization: modeling and algorithms. A hands-on approach*. Wiley, May 2016.

[30]. J. L. I- Zaragoza, J. J. P- Manresa and P. P- Marino, "Maximizing IP Fast Rerouting Coverage in Survivable IP-Over-WDM Networks," *European Conference on Optical Communication (ECOC)*, 2015.

[31]. K. Chan and T. P. Yum, "Analysis of Least Congested Path Routing in WDM Lightwave Networks," *Proceedings of INFOCOM '94 Conference on Computer Communications*, vol.2, Toronto, Ontario, Canada, 1994, pp. 962-969.

[32]. A. Urra, E. Calle and J. L. Marzo, "Enhanced Protection using Shared Segment Backups in a Multiservice GMPLS-based Networks," in *Proc. of IEEE ISCC*, June 2005.

[33]. Y. Qin and K. C. How, "Comparison studies on recovery schemes of combining protection and restoration at different layers in IP over WDM networks," *10th IEEE International Conference on Communication systems (ICCS)*, Singapore, 2006, pp. 1-5.

[34]. J. Shen and Z. Mi, "Service-based survivability scheme in Intelligent Optical Networks," *IEEE 12th International Conference on Communication Technology*, Nanjing, 2010, pp. 784-787.

[35]. W. Ramirez et al, "Managing resilience in carrier grade networks: Survey open issues and trends," *Computer Communications*, vol. 61, pp. 1-16, 2015.

[36]. D. A. Schupke, M. Jager and R. Hulsermann, "Comparison of resilience mechanisms for dynamic services in intelligent optical networks," *Fourth International Workshop on Design of Reliable Communication Networks (DRCN) Proceedings.*, 2003, pp. 106-113.

[37]. A. Haider and R. Harris, "Recovery techniques in next generation networks," in *IEEE Communications Surveys & Tutorials*, vol. 9, no. 3, pp. 2-17, Third Quarter 2007.

[38]. E. Oki, *Linear Programming and Algorithms for Communication Networks: A Practical Guide to Network Design, Control, and Management*, CRC Press, Boca Raton, 2013.

[39]. Q. Zhang and L. Xu, "Research on the Different Protection and Restoration Mechanism of ASON," *International Conference on Computer and Electrical Engineering (ICCEE)*, Singapore, 2010.

[40]. M. Clouqueur and W. Grover, "Mesh-restorable networks with enhanced dual-failure restorability properties," in *Proc. SPIE OPTICOMM*, Boston, July 2002.

[41]. R. Shenai and K. Sivalingam, "Hybrid Survivability Approaches for Optical WDM Mesh Networks," *Journal of Lightwave Technology*, Vol. 23, No. 10, October 2005.

[42]. J. Ahmed, and S. Nawaz "POSE: A new discrete event optical simulator for the Java platform," *National Conference on Emerging Technologies (NCET)*, Karachi, Pakistan, December 2004.

[43]. I. Tomkos et al. (Eds.), "COST 291 – Towards Digital Optical Networks," in *Lecture Notes in Computer Science (LNCS) 5412*, Springer Berlin / Heidelberg, 2009, pp. 331–364.

[44]. P. P- Marino, J.L. I- Zaragoza, "Net2plan: an open source network planning tool for bridging the gap between academia and industry," *IEEE Network*, vol. 29, no. 5, pp. 90-96, November 2015.

[45]. J. Korniak and P. Rózycki, "Gmpls - simulation tools," in *Proceedings of the 1st Conference Tools of Information Technology*, September 2006, pp. 20-25.

[46]. Net2Plan – The open-source network planner, http://www.net2plan.com/ [Last accessed: July 2018].

[47]. J. I- Zaragoza and P. P- Marino, "Educational and Research Tools for Network Optimization," *ICTON*, Universidad Politécnica de Cartagena, 2013.

[48]. Ethio telecom, *Huawei U2000 Network Management System*, 2018.