Availability-Aware Spare Capacity Allocation with Partially Protected Rings

by

Mohammad Zulhasnine

A thesis

presented to the University of Waterloo

in fulfillment of the

thesis requirements for the degree of

Master of Applied Science

in

Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2008

Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

This thesis work focuses on designing a survivable IP-core network with the minimal investment of spare capacity. A span-oriented spare capacity allocation (SCA) scheme is proposed to satisfy customers' availability requirements in the end-to-end (E2E) sense. The novelty of the proposed SCA scheme is that it meets the E2E availability requirements despite the lack of knowledge of E2E bandwidth by employing protection rings covering all links in the network. Different ring selection methods are presented and also compared from the aspect of network redundancy and LP feasibility which provide more flexibility to the design. The proposed SCA algorithm further minimizes total cost of spare capacity by incorporating partial protection within the proposed architecture. The simulation results show that it can significantly reduce the spare capacity consumption depending on the availability. The proposed SCA scheme also performs better in terms of redundancy than that of two other dominant methods available these days.

Acknowledgements

I wish to express my deepest gratitude to Prof. Pin-Han Ho and Prof. Xuemin (Sherman) Shen, my supervisors, for their many suggestions and constant supports during this thesis work. I would have been lost without them.

I would also like to thank my thesis readers Prof. Manoj Sachdev and Prof. Sagar Naik for their time and invaluable comments.

I wish to extend my warmest thanks to the entire broadband communication research group for detailed discussions and encouragements. I have particularly benefited from many discussions with Anwar Haque and Qi Guo.

I would also like to thank all my friends in Waterloo for their encouragements and companionship. Finally, and most importantly, I wish to thank my parents, to them I dedicate this thesis.

Dedication

To my beloved parents.

Contents

List of Tables

List of Figures

Abbreviations

DiR	Differentiated Reliability
E2E	End-to-End
FCC	Federal Communications Commission
FD	Failure Dependent
FID	Failure Indpendent
FIT	Failure in Time
IETF	Internet Engineering Task Force
GMPLS	Generalized MPLS
HAR	Highest Availability Ring
LP	Linear Programming
MNR	Minimal Number Ring
MPLS	Multiprotocol Label Switching
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
MPET	Measurement/Performance Evaluation Tool
SBPP	Shared Backup Path Protection
SCA	Spare Capacity Allocation
SLA	Service Level Agreement

SPR	Shortest Path Ring
SSR	Successive Survivable Routing
ST	Simulation Tool
TET	Traffic Engineering Tool
QoP	Quality of Protection
QoS	Quality of Service
WDM	Wavelength Division Multiplexing

Chapter 1

Introduction

With the advent of numerous network-oriented applications, the world is becoming more and more dependent on IP-based networks. IP core network is the nerve center of the network, which provides end-to-end (E2E) quality of service (QoS), service security and reliance, and performs optimization and adjustment according to the changes in service. However, there is a critical concern about the devastating impacts of network failures as the core network carries a large amount of traffic. Despite best-efforts for physical protections; failures usually occur as the result of human action (dig-ups, vehicle, human error, terrorism, hacker attacks) or as the result of natural disasters (flooding, hurricanes) or even by unintentional failures in software or control systems. Hence, survivability in the face of failures has become an essential requirement to avoid losing large volumes of traffic data due to a failure of a node or single/multiple cable cuts. Multiprotocol Label Switching (MPLS), introduced by Internet Engineering Task Force (IETF), has emerged as potential solution for addressing traffic engineering and providing survivability for IP networks. An impor-

tant feature of MPLS is its capability to set up multiple label switched paths between a source and destination. It integrates Layer 2 information such as bandwidth, latency, and utilization into Layer 3 (IP) aiming to improve IP-packet exchange. Hence, MPLS provides flexibility in diverting and routing traffic around link failures, congestion, and bottlenecks. On the other hand, with wavelength division multiplexing (WDM) technology; one single strand of fiber can provide huge bandwidth (in the range of terabits per second). In order to meet the current huge demands, current backbone data networks are converging towards a two-layer architecture of IP/MPLS or generalized MPLS (GMPLS) over an optical transport layer [1]. Fig. 1.1 shows a

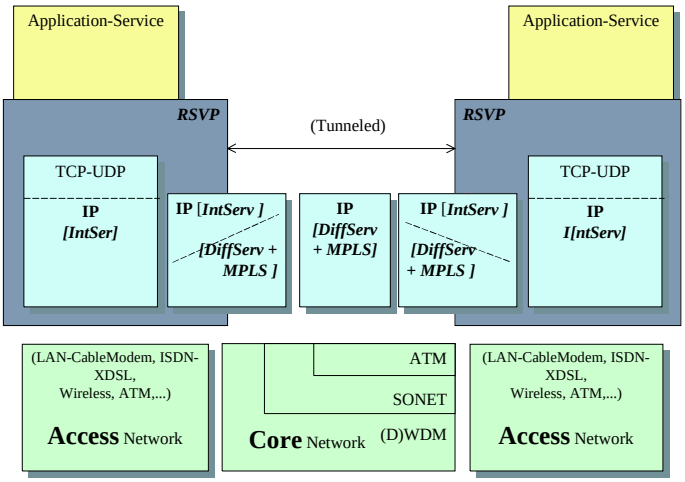


Figure 1.1: Structural layer diagram of the IP-core network.

structural layer diagram of the IP-core network with a possible distribution of protocols and technologies. The IP level is the cornerstone, the linkage between upper levels with E2E relationship and lower levels with many different physical transports. This is not an undisputable structure, many aspects relating MPLS, differential service, internal servers, are still in modification. The focus of this work is obviously on

IP/MPLS framework. With the migration in network architecture, service survivability, as one of the indispensable requirements for IP-core network, has received a lot of attentions in recent years. Survivable network design finds out the backup paths and pre-plans the spare-capacity to protect given working paths from a set of failure scenarios. The survivability requirements are usually mentioned in the Service Level Agreement (SLA) which is a contact between provider and customers that stipulates certain QoS guarantees. In case of non-fulfillment of SLA contract, service provider has to pay a penalty to the customers. With the expansion of network capacity and increasing concentration of services in backbone networks, designing survivable networks that meets the requirements in SLA becomes increasingly important.

1.1 Objective

The objective of this thesis work is to develop a survivable technique that optimizes the backup resource allocation while still satisfying the client application availability requirement. Given a IP-core network, where current working bandwidth of each link is known and no information on E2E bandwidth requirements are available, we try to find out appropriate level of spare capacity in order to have a survivable network that meets the requirements specified in SLA.

1.2 Literature Review

A number of existent survivability techniques, as well as models and algorithms for general survivable network design are reviewed in this section. Survivability schemes

are of two types: Restoration and protection scheme. When backup resources (routes and wavelengths) are pre-computed and reserved in advance, it is called a *protection* scheme. On the other hand, when a failure occurs, if another route and a free wavelength have to be discovered dynamically for each interrupted connection, it is called a *restoration* scheme. Apparently, dynamic restoration schemes are more efficient in utilizing network capacity because they do not allocate spare capacity in advance and provide resilience against different kinds of failures including multiple failures [2]. On the contrary, protection schemes have faster recovery time and can guarantee recovery at the event of service disruption. Restoration scheme also cannot provide provide recovery guarantee [3].

Depending on shareability, protection schemes can be dedicated or shared. In *dedicated protection* (i.e., $1+1$ or $1:1$) there is no sharing between backup resources. Although dedication protection has faster recovery time; the redundancy (i.e., the ratio of the total spare capacity over the total working capacity) usually reaches 100% [4]. With $1+1$ dedicated protection, for one working system there is completely another reserved back up system. Both signal paths are launched with a copy of data transmitted between a source-destination pair during the normal operation. On the other hand, in $1:1$ dedicated protection, only the working path is launched with data traffic while the capacity reserved by the protection path is not in use allowing other users for protection channel when not needed. In [5], two grooming algorithms were proposed aiming to provide availability guaranteed connections based on per-connection requirements. It was suggested to employ less-efficient dedicated protection for connections with extremely high availability requirements. In *shared protection* backup capacity can be shared on some links as long as their protected

segments are disjoint. In case of share shared protection, the spare capacity taken by the protection paths is shared by some other protection paths. Although, the recovery time in shared protection is longer but its resource utilization is better than dedicated protection [6]. The development of shared protection schemes is generally complicated as its implementation required one more disjointness.

According to the initialization locations of the rerouting process, the SCA schemes are subdivided of into two categories: the path-oriented and span-oriented. In *path protection*, the end nodes whose traffic is traversing the failed link initiate the rerouting process. Path protection leads to efficient utilization of backup resources and lower E2E propagation delay for the recovered route, whereas path protection provides shorter protection switching time. A number of path-protection schemes have been proposed and extensively investigated in the past, such as shared backup path protection (SBPP) [8]-[10], [24], [32], shared segment protection (SSP) and [11]-[12]. The design goal of these schemes is to achieve restorability at the minimal investment of spare capacity subject to different constraints and failure scenarios, such as a recovery time constraint, survivability guarantee under one or two simultaneous failures, or availability constraint etc. SBPP with a single backup path for each working path is a type of widely adopted protection scenario for achieving dynamic GMPLS-based recovery due to its generality, simplicity, and dynamicity. Compared with $1+1$ dedicated protection, SBPP has been considered as a more advanced SCA strategy that can significantly reduce the required spare capacity by allowing spare resource sharing among different backup LSPs. The SBPP method, in [10], is named as sharing with partial information, where the information available to the routing algorithm is slightly more than that in the no information scenario. The additional

information in this scenario is that for each link total bandwidth used by active paths and total bandwidth used by backup paths is known.

In *span protection*, the scheme considers the working capacity along each link and protects the working capacity through a set of detouring paths of the end nodes of the failed span. In this type of protection, the nodes adjacent to a failed link are responsible for rerouting the affected traffic flows. Thus it only patches the failed link in the original path. There are many possible approaches to implement span-protection scheme [12], [13]-[19]. The work in [13] presented a span protection scheme to minimize the total cost of spare capacity for required levels of network restoration through hop-limited protection route following a single link failure. This scheme takes into account all eligible restoration routes of the network within the hop limit. In [14], a protection method was proposed to analyze and quantify availability in mesh restorable networks upon dual-failure scenario. It was claimed that span-restorable mesh networks could be extremely robust under dual-failure events even though they were designed against all single span failures. Pre-configure cycle (or p-cycle) is a fairly recent addition to the set of approaches for span-oriented SCA [15]-[17]. This method can be thought of an extension Ring-Cover. p-cycles act ring-like way for on-cycle span failures but also protect against *straddling span* failures. The straddling span is not part of the p-cycle but it can bear twice the working bandwidths for each protection bandwidth on the p-cycle which it straddles. And straddling span itself bear no protection capacity. Unlike rings, p-cycles are formed solely in the spare-capacity of a network and do not constrain the routing of working paths to coincide with the layout of the cycles themselves. Thus p-cycles achieves ring-like speed with mesh-like capacity efficiency. The spare capacity for the working capacities on differ-

ent patterns never share each other which makes the p-cycle protection scheme less efficient than the path-oriented protection scheme. Recently, a simplified framework for dynamic provisioning of survivable services known as Protected Working Capacity Envelope (PWCE) method was proposed as an alternative of the SBPP method [18], [19]. Given a demand matrix, and a routing of demands over the graph, a set of working capacity requirements on each span can is obtained and a set of corresponding spare capacity allocations that guarantee restorability for any span failure at a time is designed. Once, the design is performed for a specific static demand matrix, the set of working channels on each span can support many different demand patterns, not only the one exemplar to which it was designed. Any demand matrix, which is fully routable under the working capacities present, is inherently also survivable under the particular partitioning of total installed capacity into working and spare. Moreover, the set of working channels defines a protected operational envelope within which any number of demand patterns can come and go as long as the resultant instantaneous demand combination lies within the envelope. An important property is that actions of any type related to ensuring protection occur only on the time-scale of the statistical evolution of the network load pattern itself, not on the time-scale of individual connections. Thus, any need for network management actions or state change dissemination is far less dynamic than the traffic itself. The protected envelope requirement is, however, very slowly changing or static over long periods of time. In [19], PWCE is implemented in the context of a network based on span-protecting p-cycles for survivability.

Widely scattered users of the network usually do not care about the network topology and implementation; rather they care about E2E availability specified in SLA.

The analysis of service path availability has recently been performed in some depth [20]-[24]. The work, in [20], first analyzed availability for different protection schemes in WDM mesh networks; and then provided a cost-effective appropriate protection using the availability analysis. However, it only considered static traffic and unprotected or dedicated-path-protected services. The study in [21] proposed a rigorous methodology to quantify availability under several protection scheme. The study in [22] addressed the problem of availability analysis in mesh restorable networks under dual-failure situations, including the cases where the optimization on availability of each connection subject to a capacity constraint, and the minimization of total spare capacity subject to an availability constraint. It is found that a span-restorable mesh network can be extremely robust under dual-failure events against which they are not specifically designed. In [23], the availability of a WDM network was evaluated, where an availability-aware link-state packet is devised and disseminated to facilitate routing under the availability constraint. Few publications have addressed the issue of provisioning connections with guaranteed availability in SBPP as well. Reference [24] presented a method for provisioning connections of different classes with guaranteed availability in the SBPP network. However, this method, which relies on the matrix-based approach for connection unavailability estimation, offers accurate results only for networks of national dimensions and is strongly limited in networks of continental dimensions. In [25], a theory was proposed to estimate a suitable "safety factor" for SLA availability guarantee depending on the term period. In [26], it was clearly stated that although there is linkage between network availability and availability specified in SLA, they are not the same. A method was also suggested to estimate availability to be guaranteed on SLA contact and to control the associated non-complying risk.

Recently, extensive research efforts have been addressed on the topic of spare capacity reconfiguration/reallocation [27]-[30]. The study in [27] proposed a matrix approach in calculating the minimum spare capacity along each link to achieve 100% restorability for any single failure. The proposed Successive Survivable Routing (SSR) approach can effectively solve the spare capacity reconfiguration by sequentially rerouting the backup path of each connection. However, the availability and the inference by double simultaneous failures have not been considered. The work, in [28], investigated how to improve the dual-failure restorability with p-cycle which was originally designed for achieving 100% restorability for any single failure under both static and dynamic situations. Since the amount of resource consumption of p-cycle is similar to or even more that by link protection, the performance can be improved by using SBPP or SSP. In [29], inter-arrival spare capacity reconfiguration is performed by investigating into the computation efficiency and grouping policies of network traffic, where each lightpath is prepared with backup path segments for achieving 100% restorability in the single failure scenario. In [30], a new link-state metric in rerouting each backup path through a wavelength channel was proposed. The proposed approach reallocates spare capacity without disrupting working services and can operate in the context of shared-path protection (with backup multiplexing). Unlike previous spare capacity reallocation approaches which aim at minimizing total spare capacity, the proposed load-balancing approach minimizes the network load vector in order to achieve uniform load distribution.

Most of the previously reported studies focused on improving E2E availability with a restoration granularity in terms of the number of simultaneous failures that can be handled for achieving 100% restorability, in which the source nodes switch

100% of the working bandwidth over to the backup LSPs. The assumptions on uniform and indivisible bandwidth of each connection have been seen to address much unnecessary limitation on the applicability of the developed models in different network environments, where the possibilities of further reducing the spare capacity by partially restoring the working LSPs have been excluded. In fact, in IP-core network, a LSP could be composed of numerous independent service sessions under the framework of GMPLS-based recovery. This structure provides the feasibility of having partial restoration for a LSP based on divisibility of the LSP in the restoration phase. In this case, the source node has the capability of randomly dropping some service sessions of the LSP while restoration is performed. In other words, the source node partially restores a working LSP by switching over a specific proportion of the working bandwidth to the backup LSP while the rest of the bandwidth is dropped. It is necessary to have an approach that can precisely evaluate the E2E availability for the SBPP connections considering a more general network environment and design scope. The work, in [31], introduced a novel dynamic availability-aware survivable routing architecture, which employs partial protection for a working path. The proposed scheme achieved much finer design granularity and significantly reduced the required redundancy in the effort of achieving a specific availability constraint for each connection request. In [32], a policy-based model was proposed to evaluate the E2E availability and to reconfigure the spare capacity allocation (SCA) for dynamic provisioning of SBPP connections. Partial protection was employed in both failure-dependent (FD) and failure-independent (FID) policy-based architecture. Several research efforts have been dedicated to the study of differentiated survivability mechanisms to employ partial protection [33]-[36]. In [33], a modified shared path

protection switching scheme with differentiated reliability (DiR) in WDM mesh networks was proposed. In the scheme, client demands and circuits are differentiated based on their requested individual degree of reliability in a cost-effective way. The cost reduction is inversely proportional to the reliability degree required by the client circuit. In [34], the DiR concept is applied to support QoS where partial protection is adopted. As only a fraction of bandwidth protected in the backup path, this scheme outperforms 1 : 1 protection with respect to blocking probability and resources reserved for backups. The study in [35], presented various methods for providing service differentiation in survivable WDM networks and discusses their performance. Such methods are broadly classified under various paradigms such as DiR, quality of protection (QoP), and quality of recovery. However, most of these works were proposed for WDM networks and do not consider service availability.

1.3 Contributions

The design of survivable networks that can reduce redundancy and achieve a specific availability constraint is a long-lasting challenge. Very few publications have addressed the issue of provisioning connections with guaranteed availability. Any span-protection scheme which can guarantee availability requirements in the E2E sense is yet to be found. The main contribution of this thesis is the development availability-aware SCA algorithm in a network scenario where bandwidth requirement of any connection is unknown.

In the proposed SCA scheme, the network is covered with sufficient rings such that each link is essentially a part of at least one ring. When any link fails it has a

protection path through the other part of the ring. This obviously a span-oriented ring-covered protection. The selection of rings for each link is done based on many different strategies which gives more flexibility to the design. The proposed multi-constraint optimization problem or the SCA problem is formulated using Linear Programming (LP). Thus the proposed SCA scheme provisions connections that achieve the E2E availability higher than while as close as possible to that defined in the SLA at the minimal investment of backup resources. Two other prominent methods of SCA are also implemented for comparison purpose.

Partial protection is also incorporated in the proposed SCA scheme for better utilization of resource allocation which is also unique in case of span protection compared to other span protection schemes available these days. Different ring selection methods are also compared from the aspect of network redundancy and LP feasibility required for measuring spare capacity.

1.4 Thesis Overview

The reminder of the thesis is organized as follows. Chapter 2 discusses the causes of network failures and denotes the impact of outage. This chapter also depicts few basic concepts and techniques on network survivability management that are useful in the following thesis paper. At the end, it formulates the problem. Chapter 3 describes the proposed availability-aware SCA scheme employing partially protected rings in details. Chapter 4 first presents the test networks and experimental conditions and then analyzes the simulation results along with figures and remarks. Chapter 5 concludes the work and suggests future work.

Chapter 2

Causes of Failure, Survivability Measures and Problem Statement

This chapter ascertains the causes of network failures and denotes the impact of outage. This chapter also formulates the problem and discusses a number of possible schemes to solve the problem.

2.1 Causes of Network Failure and Impacts of Outage

Current backbone data networks are converging towards a two-layer architecture of IP/MPLS over an optical transport layer as shown in Fig. 1.1. No matter how advanced today's widespread IP-core network, despite best-efforts with physical protections it could be damaged as it is in a cable. Internet search engine returns hundreds of cable cut related network outage notifications. For example, on $100,000$ installed

route miles of networks it implies more than one disruption *per day* on average [18]. The authors, in [38], highlight that according to Federal Communications Commission (FCC) 2002 report, metro networks annually experience 13 cuts for every 1000 miles of fiber and, long haul networks experience 3 cuts for 1000 miles of fibers. The annual number of cable cuts has also risen with the increased growth of the Internet. It is to be noted that these frequencies of cable cut events are hundreds of times higher than corresponding reports of transport layer node failures. This is why network survivability designed is primarily focused on recovery from span or link failures from cable cuts.

There are several ways in which cables can be cut, and the causes of cable damage can be classified as human error, accidental, or malicious. Cable dig-ups is by far the most common cause of cable damage and failure. In fact, a comprehensive survey on the frequency and causes of cable cut finds that almost 60% of all cuts were caused by cable dig-ups. The vast majority of those were due to digging errors or inadequate notification to cable location authorities prior to digging. Accidents are one of the major causes of cable cuts. Vehicles running into aerial poles, fires, fallen trees and floods can disrupt the networks. Animals have also been implicated in cable cuts. For example, the rat can chew cable, which is very common in Ontario. Deer, gophers, squirrels, and even sharks are believed to be responsible for a number of cable outages. Vandalism and sabotage are also responsible for cable cuts. Terrorist attacks on fiber cable may be a great concern in the near future to the information security community.

Cable cuts impact the network users in a variety of ways. Revenue losses to business and negative publicity from outages are inevitable consequences at the event

of network failures. An outage, that lasts for half an hour or more and affects $30,000$ or more subscribers are obliged for reporting to the FCC. According to FCC report, each cable cut affected over $105,000$ customers for over 4 hours on average. One survey estimates US enterprizes lost more than \$500/year in potential revenue due to network failures that affect critical business functions. Web-based e-commerce services suffer from bankruptcies from an hour or more of outage. Mission critical Internet service providers quote $\$100,000$/minute or more revenue loss from failure of network. Depending on which services are affected, cable cuts can have disastrous consequences. Most of the cases, service providers have to pay rebates to customers based on the numbers or outage duration. Even though statistics on smaller outages are not tracked, it is evident that cable cuts have huge financial impact on businesses that depend on the communication network.

2.2 Survivability Measures

Survivability is the ability of a network to maintain or restore an acceptable level of performance during network failures by applying various restoration techniques. The term is an inherent attribute of the network design regardless of if, or how often, failures actually occur. It gauges the ability of a network of being able to keep on functioning in the presence of various failure scenarios. Some quantitative measures of survivability are: restorability, restoration time, reliability, and availability.

Restorability is design-oriented parameter reflecting the capability of a network to survive a specific failure scenario. In this class of measurements, each relevant failure scenario is first postulated to have occurred, then an assessment of survivability is

made.

Restoration time defines the exact disruption holding time, which should be minimized as much as possible.

In general, *reliability* is a qualitative perception of the network being predictable and usually available. Technically, it is the probability that a system will provide its intended service uninterrupted for a period of time. Let λ is failure rate per member of the group given that the member has already survived until time t. Then the probability of a unit surviving to time t (i.e., not failing in $[0, t]$) is expressed as [18]:

$$R(t) = e^{-\int_0^t \lambda(u) \cdot du} \tag{2.1}$$

Reliability is thus always a non-increasing function of time with $R(t = 0) = 1$ and $R(t = \infty) = 0$. This survivability metric takes into account the probability of failure onset as well as the survivability response or capability of the network. Here assumption that failures can be characterized by random variables with given probability distribution functions. With the increasing growth of mission-critical Internet applications customers are requiring highly-reliable network services. Depending on the service, a number of different ways in which the reliability of a network or service can be measured. Some relevant measures of reliability are availability, throughput, delay, probability of graph disconnection, dial-tone delay, service establishment times, cell-loss rate, error-rate, and so on [22]. To the users of IP-core network, the E2E availability is of supreme concern. The concept of availability is focused next.

Reliability is only concerned with how likely a system stay in operation for a certain time without a service-affecting failure occurring. Hence, another survivability

metric is needed to asses continuously operating systems which are subject to repair when failures occur. The probability of finding a system available can be high even if failures are frequent and promptly repaired. *Availability* is the probability that a system undergoing repair after each failure is found in the "operating" state at any random time in the future. The steady state availability is defined as:

$$A \equiv \lim_{T \to \infty} \left\{ \frac{Uptime}{T_{obs}} \right\} \tag{2.2}$$

where T_{obs} is a total observation time. *Availability* depends on the Mean Time to Failure (MTTF), which is the expected time between failures, and the Mean Time to Repair (MTTR) which is the expected time to next failure. Fig. 2.1 shows the failure and repair cycle of a repairable maintained system. In particular:

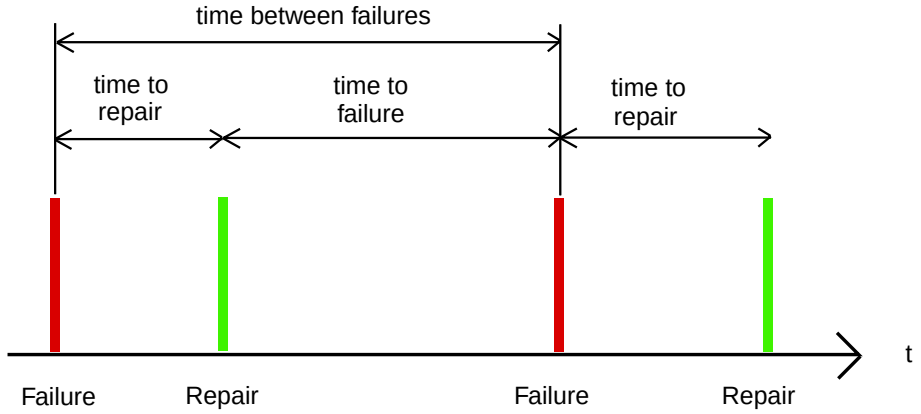


Figure 2.1: Failure and repair cycle of a repairable maintained system

$$A = \frac{Uptime}{T_{obs}} = \frac{MTTF}{MTTF + MTTR} \tag{2.3}$$

In availability analysis, it is usually easier to work with unavailability quantities

because of some simplifications that can be done on the unavailability of elements in series and in parallel. The *unavailability* U is the probabilistic complement of availability A and defined as:

$$U = 1 - A = \frac{MTTR}{MTTF + MTTR} \tag{2.4}$$

Assuming $MTTF \gg MTTR$ for the many practical cases of interest, Eq. 2.4 can be approximated as:

$$U \approx \frac{MTTR}{MTTF} = \lambda \cdot MTTR \tag{2.5}$$

Thus *unavailability* approximately represents simply the repair time times the frequency of failure, or the failure rate in the approximate inverse-time units.

The internationally used unit for measuring or specifying failure rates is failures in time (FIT). Conventionally a period of 10^9 hours is used as a time scale to quantify the failure rates:

$$\text{a failure rate of 1 failure in } 10^9 \text{ hours} = 1 \text{ “FIT”} \tag{2.6}$$

Hence, MTTF in hours can be expressed as:

$$\text{MTTF } = 10^9/\text{FITs} \tag{2.7}$$

1 failure/year is equal to $114,155$ FITs and conversely 1 FIT is equal to 1 failure in $114,155$ years. Also, it is rather common to express unavailability as the average

outage time referred to this reference period:

$$\text{U} = (\text{MTTR} * \text{FITs})/10^9 \tag{2.8}$$

For instance, "Three nines availability" is equivalent 8.76 hours of outage per year and "Five nines availability" is equivalent 5.26 minutes of outage per year.

2.3 Two Basic Concepts

In this section two basic concepts that are necessary for complete understanding of the work presented are described.

2.3.1 Partial Restorability

In case of partial restoration, the amount of bandwidth required for the backup path is only a fraction of the working path's bandwidth. Let the working and protection pathes be denoted as W and P, respectively. The physical availability of W and P are A_w and A_p, respectively. The protection level is θ. Since P is $\theta-$restorative to W, only θ of the working bandwidth is protected by P while the rest $1-\theta$ of working bandwidth is not protected. The availability in the former θ of working bandwidth is

$$A_\theta = 1 - (1 - A_w)(1 - A_p)$$

The availability is in the latter $1 - \theta$ bandwidth

$$A_{1-\theta} = A_w$$

Therefore, the overall E2E availability is

$$\begin{aligned} A_{wp} &= A_\theta \cdot \theta + A_{1-\theta} \cdot (1-\theta) \\ &= [1-(1-A_w)(1-A_p)] \cdot \theta + A_w \cdot (1-\theta) \\ &= 1-(1-A_w)(1-\theta \cdot A_p) \end{aligned} \tag{2.9}$$

This scheme thus outperforms 1 : 1 protection in terms of blocking probability and resources reserved for backups.

2.3.2 E2E Availability

Let A_w and A_p denote the E2E physical availability of W and P, respectively. As links can fail independently to each other, the physical availability of W and P can be expressed as:

$$A_w = \prod_{i \in W} a_i = \prod_{i \in W} (1-u_i)$$
$$A_p = \prod_{j \in P} a_j = \prod_{j \in P} (1-u_j)$$

where a_i and u_i is the physical availability and unavailability of link i. A_w can be numerically approximated as:

$$A_w = \prod_{i \in W} (1-u_i) \approx 1 - \sum_{i \in W} u_i \tag{2.10}$$

As the physical unavailability is very small ($u_i << 1$), the higher order terms of u_i are ignored. A_p can also be reformulated using Similar approach. The physical

unavailability of W and P can now be expressed as:

$$U_w = 1 - A_w \approx 1 - \left(1 - \sum_{i \in W} u_i\right) = \sum_{i \in W} u_i$$
$$U_p = 1 - A_p \approx 1 - \left(1 - \sum_{j \in P} u_j\right) = \sum_{j \in P} u_j$$

These are approximations but quite accurate and simplified for $u_i << 1$. For example,

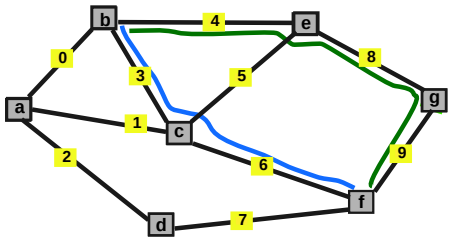


Figure 2.2: E2E availability of two parallel paths.

in Fig. 2.2, the E2E availability of the working path [b-c-f], $A_w = 1 - \sum(u_3 + u_6)$ and that of the protection path [b-e-g-f], $A_p = 1 - \sum(u_4 + u_8 + u_9)$. As availability multiplies for parallel path, the E2E availability between node b and f, $A = A_w \times A_p$.

2.4 Problem Statement

In general, the network topology is composed of links and nodes in constant peril of being interrupted. Let this original network topology be represented by a graph $G(V, E)$, where V is the set of nodes and E is the set of links. The working capacity of each link j is known; while the bandwidth requirement of each connection c is unknown. Availability requirements of all connections specified in SLA and physical availability of all links are given. A protection scheme has to be designed which

ensures E2E availability specified in SLA for all connection c. Let S_j and C_j are the amount of spare capacity and the cost of unit spare capacity corresponding to link j. The design objective is to minimize the allocation of spare capacity on the network while guaranteed the availability required. Total allocated spare capacity is the sum of allocated spare capacity over all links; hence the objective function for the problem is:

$$Min \quad \Big\{ \sum_{j \in E} C_j \cdot S_j \Big\}$$

To make the protection scheme more cost-efficient; partial protection could be adopted instead of 100% restoration while still satisfying the client application availability requirement.

One possible method to solve the above stated problem is to employ span protection scheme that uses hop-limited multiple protection routes [13]. The spare capacity assignment task of this scheme in the form of LP is presented in the following way:

$$Min \quad \Big\{ \sum_{j \in E} C_j \cdot S_j \Big\}$$

Subject to the constraints:

$$\sum_{p \in P_i} f_{i,p} \geq q_i \cdot X_i \qquad \forall i \in E$$

$$S_j - \sum_{p \in P_i} \delta_{i,p}^{j} \cdot f_{i,p} \geq 0 \quad \forall i, j \in E, \text{ and } i \neq j$$

$$f_{i,p} \geq 0, \quad \forall i \in E, \ p \in P_i$$

In the above formulation, P_i is the set of eligible protection routes for link i within the hop limit; q_i is the protection level required for link i, $f_{i,p}$ is the "restoration flow" through the p-th restoration route of link i; $\delta_{i,p}^{j}$ is a binary indicator which takes the value of 1 if the protection route p of link i traverses link j and "0" otherwise. This scheme can solve for SCA when E2E bandwidth requirements are unknown. q_i in the above formulation also allows the scheme to employ partial protection. However, this scheme cannot guarantee E2E availability requirements specified in SLA.

p-Cycle is another possible candidate to solve the above formulation [15]-[17]. The LP formulation for p-cycle is presented below:

$$Min \quad \Big\{ \sum_{j \in E} C_j \cdot S_j \Big\}$$

Subject to the constraints:

$$S_j = \sum_{i \in N_p} \delta_{i,j} \cdot n_i \quad \forall j \in E$$

$$\Big(\sum_{i \in N_p} \xi_{i,j} \cdot n_i \Big) - r_j \geq w_j \quad \forall j \in E$$

$$\delta_{i,j} = \begin{cases} 1 & \text{if link } j \text{ traversed by pattern } i \\ 0 & \text{otherwise} \end{cases}$$

$$\xi_{i,j} = \begin{cases} 1 & \text{if link } j \text{ is on-cycle or straddling with pattern } i \\ 0 & \text{if either one or both nodes of link } j \text{ not on pattern } i \end{cases}$$

In the above formulation, w_j is working capacity on link j; r_j is the spare capacity excess of those required of link j; N_p is the set of candidate patterns (i.e., uni-

directional elementary cycles); n_i is the number of copies of pattern i. There is no provision for employing partial protection in this scheme. This scheme also fails to guarantee E2E availability requirement.

Policy-based (FD/FID) SBPP method that employs partial protection could be another possible candidate to solve the problem [32].

$$Min \quad \sum_{j \in E} S_j$$

Subject to (with FID policy):

$$\begin{aligned}
S_j &= \max Q_{j,r_m} \quad \forall j \in E \\
Q_{j,r_m} &= \sum_{\forall c | m \in W_c, j \in P_c} b_c \cdot \theta_c \quad \forall j \in E, r_m \in R, m \neq j \\
A_c &= 1 - \sum_{r \in R^c_{\overline{wp}}} \pi_r - \sum_{r \in (R^c_{\overline{w1}p} \cup R^c_{\overline{w2}p})} (1 - \theta_c) \cdot \pi_r \quad \forall c \in C \\
A_c &\geq A_{c,SLA} \quad \forall c \in C \\
0 &\geq \theta_c \geq 1 \quad \forall c \in C
\end{aligned}$$

Subject to (with FD policy):

$$
\begin{aligned}
S_j &= \max Q_{j,r} \quad \forall j \in E \\
Q_{j,r} &= \sum_{\forall c | j \in P_c, r \in (R^c_{\overline{w_1}p} \cup R^c_{\overline{w_2}p})} b_c \cdot \theta_{c,r} \quad \forall j \in E, r \in R \\
A_c &= 1 - \sum_{r \in R^c_{\overline{wp}}} \pi_r - \sum_{r \in (R^c_{\overline{w_1}p} \cup R^c_{\overline{w_2}p})} (1 - \theta_{c,r}) \cdot \pi_r \quad \forall c \in C \\
A_c &\geq A_{c,SLA} \quad \forall c \in C \\
0 &\geq \theta_{c,r} \geq 1 \quad \forall c \in C, r \in (R^c_{\overline{w_1}p} \cup R^c_{\overline{w_2}p})
\end{aligned}
$$

In the above formulation, $Q_{j,r}$ denotes the total amount of spare capacity required to be allocated on link j with failure pattern r; C is the set of connections; W_c and P_c are the set of links along working path and protection path of connection c; b_c is the bandwidth requirement of connection c; $\theta_{c,r}$ is the protection level of connection c with failure pattern r; A_c and $A_{c,SLA}$ are the availability requirements without and with SLA, respectively and π_r is the stationary probability of failure pattern r. In all cases, $R^c_{\overline{wp}}$ is the set of failure patterns which interrupted both working and protection path of connection c; $R^c_{\overline{w1}p}$ is the set of failure patterns whose first failure disrupts working path of connection c and second failure doesn't affect protection path of c; $R^c_{\overline{w2}p}$ is the set of failure patterns whose first failure doesn't affect the protection path of connection c and second failure disrupts the working path of c.

This method can guarantee E2E bandwidth requirements and save significant spare capacity employing partial protection. However, this method cannot solve the problem as the the information of b_c, W_c and P_c for all connections are unknown. This method is implemented latter to compare the performance of the proposed scheme.

Chapter 3

Availability-Aware Spare Capacity Allocation

In this chapter the proposed availability-aware spare capacity allocation scheme is presented. Methods of employing different ring selection strategies are briefly described. An example showing how the proposed protection scheme works is addressed at the end.

3.1 System Model

The system model is shown in Fig. 3.1. The main focus is on the GMPLS-enabled IP-core survivable networks. The GMPLS control plane relies on a peer model in which all network elements (MPLS routers and optical cross connects) share the same control and signaling plane. The central server is equipped with traffic engineering tool (TET) that is supported by two tools: simulation tool (ST) and measurement/performance

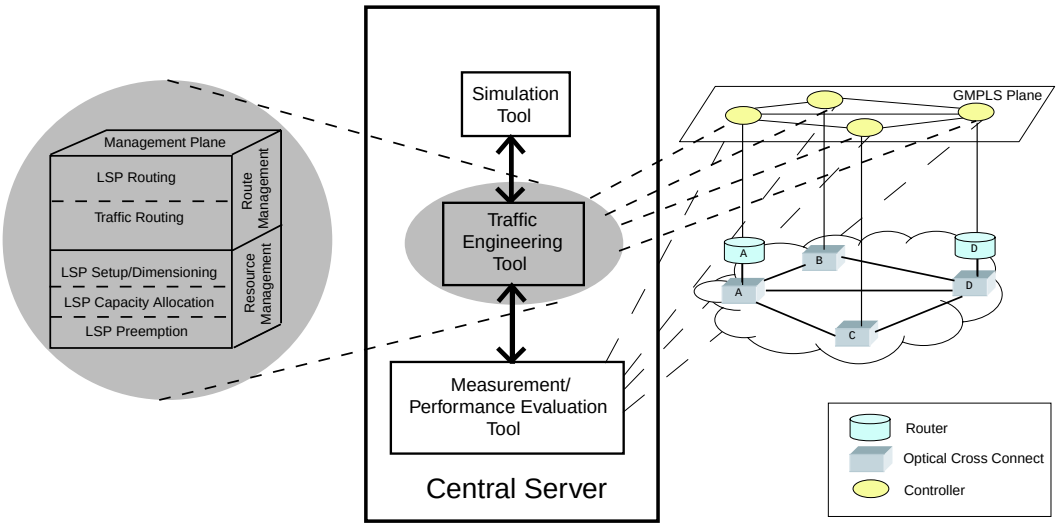


Figure 3.1: The system model and functionalities.

evaluation tool (MPET). The TET and the MPET will interact with the GMPLS plane. The MPET will provide a measure of the various parameters of the network and routers like the link current bandwidth, overall delay, jitter, queue lengths, in the routers, etc. This information will be input to the TET. Based on this measured state of the network, along with information on physical availability and availability specified on SLA the TET will interact with the ST. The ST will simulate a network with the current state of the managed network and apply the decision of the TET to verify the achieved performance. The TET management tasks include resource management (LSP setup/dimensioning, LSP preemption, LSP capacity allocation) and route management (LSP routing), as shown in Fig. 3.1.

The network is denoted as $G(V, E)$ with V set of nodes and E set of edges as stated earlier. To make the analysis straightforward, each node in the original network is replaced by two vertices with an additional link connecting the twin vertices with the node splitting technique [39]. Such a graph yields the desired character-

istic where each vertex has a perfect availability, while only links may fail. Failure on a node in the original network is now simply translated into a failure event on the corresponding links in the transferred graph and the rest of the thesis will only consider the availability of each link in the transferred graph. It is assumed that only the IP/MPLS layer provides protection for each working LSP for availability enhancement. IP routers are usually located at the city and high redundancy and extremely short recovery time can be achieved. Therefore, only failures on each IP link are considered whereas each IP router is taken as perfect. To simply the analysis, the E2E unavailability is calculated by adding link unavailabilities. Let the network be launched with a set of connections denoted as C. Each connection c is associated with a tuple $\left\langle s_c, d_c, A_c^{SLA}, b_c \right\rangle$ and follows a single physical route connecting from the source vertex s_c and the terminating vertex d_c along with the required bandwidth b_c and availability constraint A_c^{SLA}. Notice that although working bandwidth v_j on each link j is known; b_c is unknown for all connection c.

3.2 The Availability Aware SCA Scheme

As IP-core network has moved towards mission-critical infrastructure, availability of some connection-oriented multimedia applications such as VoIP, real-time video streaming becomes increasingly important. Network availability is evaluated as the average availability of connections in the network. Although there is a close link between the network connection availability and the availability specified in SLA, they are not the same [37]. In fact, over a fixed observation time, actual connections' availability is varied around the average availability, i.e. some connections behave

better and others behave worse in terms of availability requirements. As a consequence, setting the availability in SLA at the value of the average availability, the network operator has to comply with the associate risks of paying refunds to those customers whose connections behave worse than average. Very few publications have addressed the issue of provisioning connections with guaranteed availability. Any span-protection scheme which can guarantee availability requirements in the E2E sense is yet to be found.

In this thesis work, a new algorithm for availability-aware spare-capacity assignment in survivable networks is presented, which attempts to optimize network resource utilization. The novelty of the proposed scheme is that it meets the E2E availability requirements despite the lack of knowledge of E2E bandwidth by employing protection rings covering all links in the network. The proposed SCA algorithm further minimizes total cost of spare capacity by incorporating partial protection within the proposed architecture. Only a percentage of the working bandwidth is restored by protection path once the working path is interrupted. The proposed protection scheme consists of two steps. The first step is network specific and executed only once, during the network planning phase. The second step is connection specific and executed online, whenever the unavailability of connection has to be assessed. The flowchart in Fig. 3.2 shows the steps involved in the availability-aware SCA scheme employing partially protected rings. The following two subsections describe the different strategies for protection ring selection and the proposed LP formulation for SCA.

The derivations of the proposed protection scheme are based on the following assumptions:

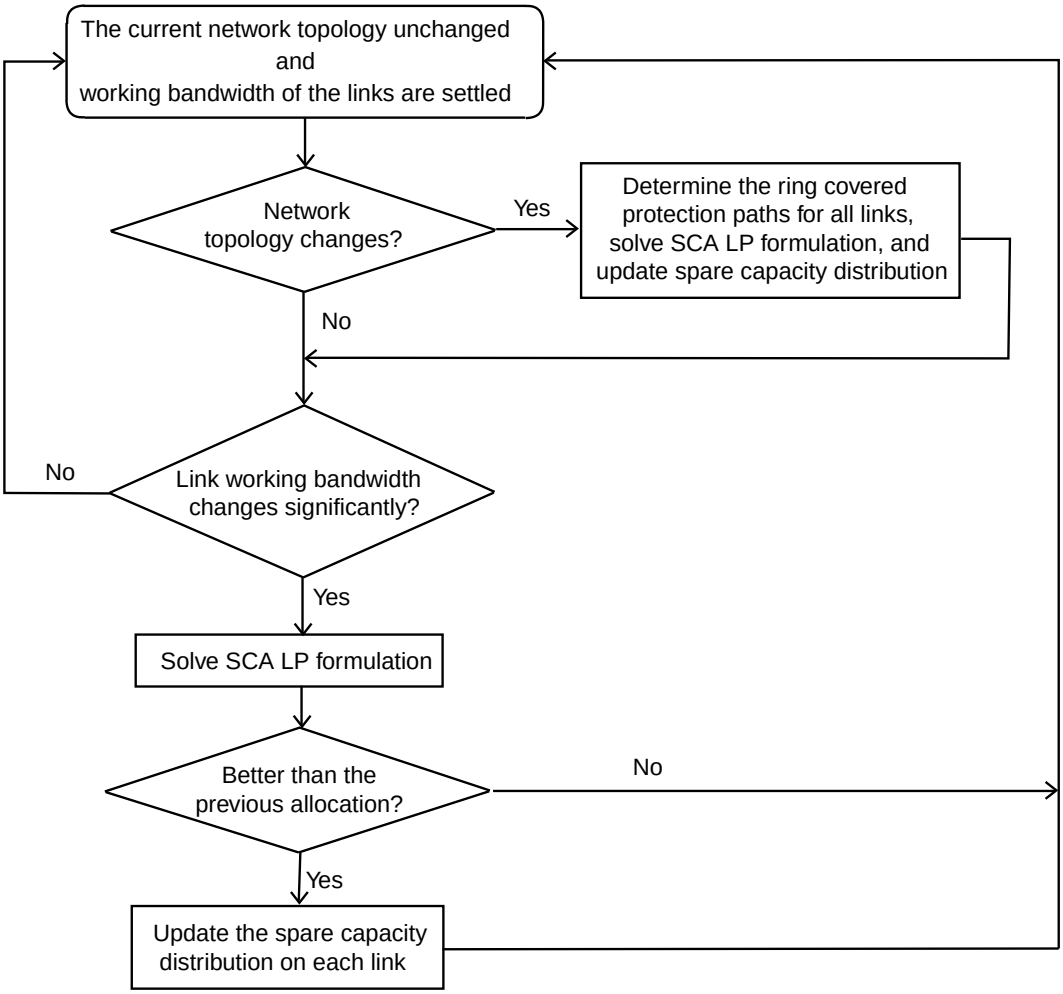


Figure 3.2: Flowchart of the steps involved in the availability-aware SCA scheme employing partially protected rings.

- All IP-core links have two-state "working" or "failed";
- All IP-core links fail independently;
- The repair time and the time to fail of a fiber link are memoryless, exponentially distributed random processes with constant means MTTR and MTTF;
- At most two fiber links can simultaneously fail in the network;

- A working path and its corresponding protection path are always link-disjointly routed.

3.2.1 Protection Ring Selection Methods

The network is covered with sufficient rings such that each link is essentially a part of at least one ring. When any link fails it has a protection path through the other part of the ring. This is obviously a span-oriented ring-covered protection. The protection paths do not carry any demand until a failure occurs. Hence, they can be rearranged and rerouted as the working bandwidth of links or the network conditions change. There are many possible rings for each link. The selection of rings for each link can be done based on many different strategies which gives more flexibility to the design. The ring selection methods can be named as:

i) Highest availability rings.

ii) Minimal number rings.

iii) Shortest path rings.

iv) LP based load balancing rings.

v) Most efficient network management rings.

The first three approaches are part of the proposed availability-aware protection scheme. Here is the brief discussion on first three strategies of protection ring selection.

[i] ***Highest Availability Rings (HARs):*** In this case, for each link a ring is selected such that it has the highest availability in its protection routes. For each link, all possible routes between the the end nodes are found first. Among them the route with highest availability is selected as protection ring for that link. Since for larger network, the number of all possible routes between the end nodes of that link can be very large; the search is limited by the number of hop-count. Finding all possible routes between end nodes of a link is little bit tricky; here is the Pseudo code for HARs selection method.

Pseudo Code for HAR Selection Method:

Notations:

$G(V, E)$: a network G, with set of V nodes and E edges

i, j, k : loop index

$n1, n2$: end nodes of an edges

$PossPaths_i$: a set of nodes of all possible paths between the end nodes of edge i

$HopLimit$: a constant to avoid flooding of possible paths in a large network

Inputs: $G(V, E)$

Outputs: HARs

for$(i = 0; i < E; i++)$

add $n1$ to $PossPaths_i$

for$(j = 0; j < HopLimit; j++)$

for all paths listed in $PossPaths_i$

find neighboring nodes of the last added node in $PossPaths_i$

add that node, if it is not already in that path

end for

end for

for all paths listed in $PossPaths_i$ // checking for path validity

if the end node is other than $n2$; remove paths from $PossPaths_i$

end for

find the path with highest availability from $PossPaths_i$

form ring for link i between link i and the highest availability path

end for

Although this method could result in highest execution time, this method is expected to have feasible result even at lower U_{SLA}. The number of rings is obviously equal to the number of links in the network.

[ii] ***Minimal Number Rings (MNRs):*** In this ring selection strategy, rings are formed in such way that the number of rings covering all links is minimized. The motivation for employing MNRs comes from the expectation that minimal number protection rings will minimize the spare capacity. The steps involved in creating

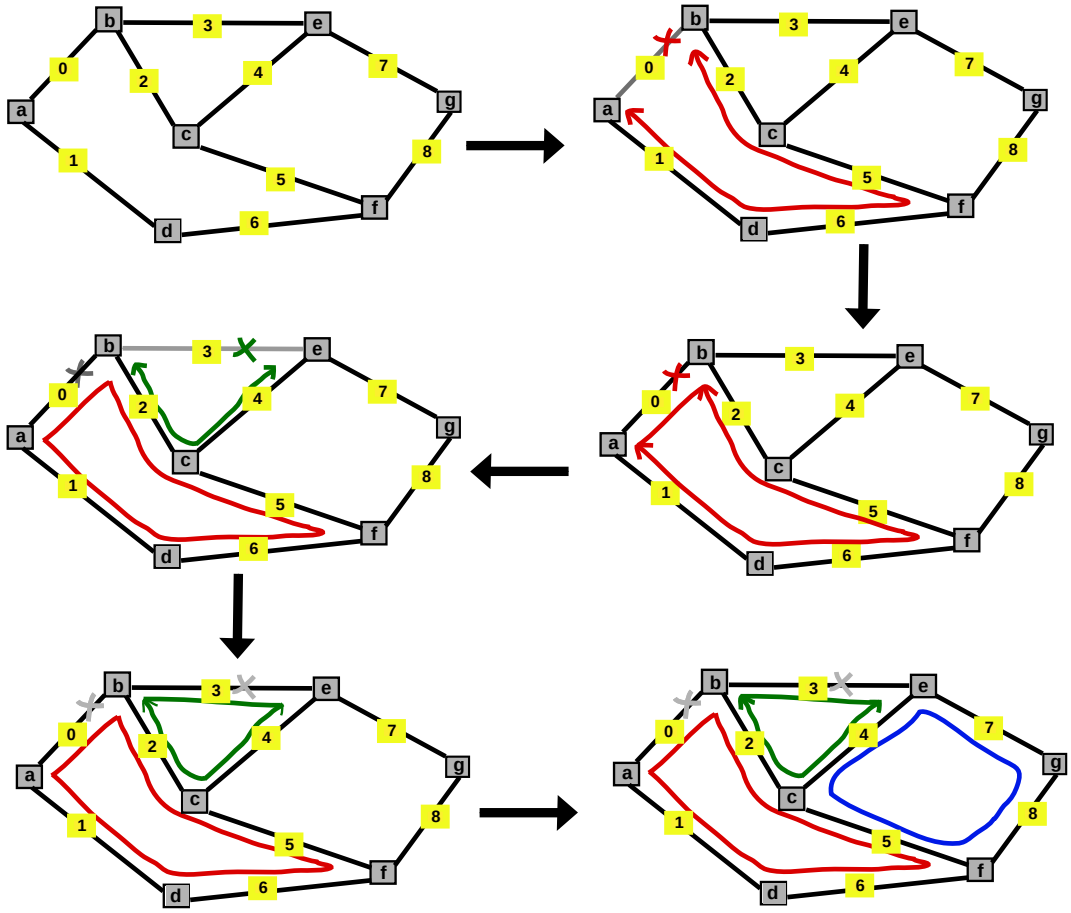


Figure 3.3: The operation of minimal number ring selection method.

MNRs are:

- *Step* 1: A link is chosen arbitrary and then deleted temporally. The shortest distance between the end nodes of the chosen ring is found out over the network;
- *Step* 2: A ring is formed for that link. Links part of this ring are considered to have the same protection ring;
- *Step* 3: Another link which is not already a part of any rings is chosen and a ring is formed in a similar way for that link;
- *Step* 4: The steps are repeated until all links are covered with at least one ring.

Fig. 3.3 illustrates the step-by-step procedure for creating MNRs on a small network with 7 nodes and 9 links. The number of rings in other two methods is equal to the number of links in the network, whereas in this method the number of rings is reduced considerably. For example, there are only 3 rings cover all 9 links. If any link has more than one ring; ring with shortest hop count is considered its protection ring. Here link 2 has two rings (ring 1 with links $0, 2, 5, 6, 1$ and ring 2 with links $2, 3, 4$); ring 2 is selected for link 2 as its protection ring.

[iii] ***Shortest Path Rings (SPRs):*** For both HAR and MNR methods, some links may have long protection rings. SPRs are formed such that all links have rings with shortest path in terms of hop count. In this case, for each link, the route with shortest distance between the end nodes of link is found over the network excluding that link. A protection ring is then formed with that link and the shortest path for that link. The proposed protection scheme, employing SPR, usually has fast restoration time as less network elements are involved and fewer messages are sent and acknowledged during the restoration procedures. This method also finds out

Table 3.1: Notation

C	The set of all connections.
s_c	Source node of connection c.
d_c	Destination node of connection c.
b_c	Bandwidth requirement of connection c.
w_c	The working path of connection c.
W_c	The set of links along w_c.
A_c^{SLA}	Availability requirement of connection c specified in the SLA.
U_c^{SLA}	Corresponding unavailability to A_c^{SLA}
a_j	Availability of link j.
$a_{r\setminus j}$	Availability of the protection path of link j.
v_j	The working capacity of link j.
θ_j	The restoration level required for link j.
S_j	Amount of spare capacity on link j.
C_j	Cost of a spare channel corresponding to link j.
δ_i^j	Binary indicator, of value equals to 1 if the protection route of link i uses the link j and 0 otherwise.

protection ring with minimum execution time. The number of rings is equal to the number of links in the network.

3.2.2 The LP Formulation for Availability-Aware Spare Capacity Allocation

Consider the notation in Table 3.1. In this section, a LP is formulated to determine S_j for $j \in E$ such that E2E availability is high enough to fulfill the SLA with the minimal amount of spare capacity. The target function of the LP is to minimize $\left\{ \sum_{j \in E} C_j \cdot S_j \right\}$. The E2E bandwidth requirements are unknown; however the working capacity of each link is the summation of bandwidth requirements for all connections

passing through that link, hence

$$v_j = \sum_{\forall c | j \in W_c} b_c \tag{3.1}$$

The unavailability of link j is $1 - a_j$. Since the protection level for link j is θ_j and its protection path's availability is $a_{r\backslash j}$, the unavailability of the protection path of link j is $1 - \theta_j a_{r\backslash j}$. Unavailability multiplies for parallel connection; thus the unavailability of link j with ring cover protection is:

$$u_j^r = (1 - a_j)(1 - \theta_j a_{r\backslash j})$$

The unavailability for each connection with ring protection should be less than the unavailability specified in SLA for that connection. Thus, for all c in C, the following constraint should be valid.

$$\begin{aligned} U_c^{SLA} &\geq u_c^r \\ &\geq \sum_{\forall j \in W_c} u_j^r \\ &\geq \sum_{\forall j \in W_c} (1 - a_j)(1 - \theta_j a_{r\backslash j}) \end{aligned}$$

where, u_c^r and u_j^r are the unavailability of connection c and link j, respectively, with ring cover protection. The total cost for allocating spare capacity has to be minimized.

$$Min \quad \Big\{ \sum_{j \in E} C_j \cdot S_j \Big\}$$

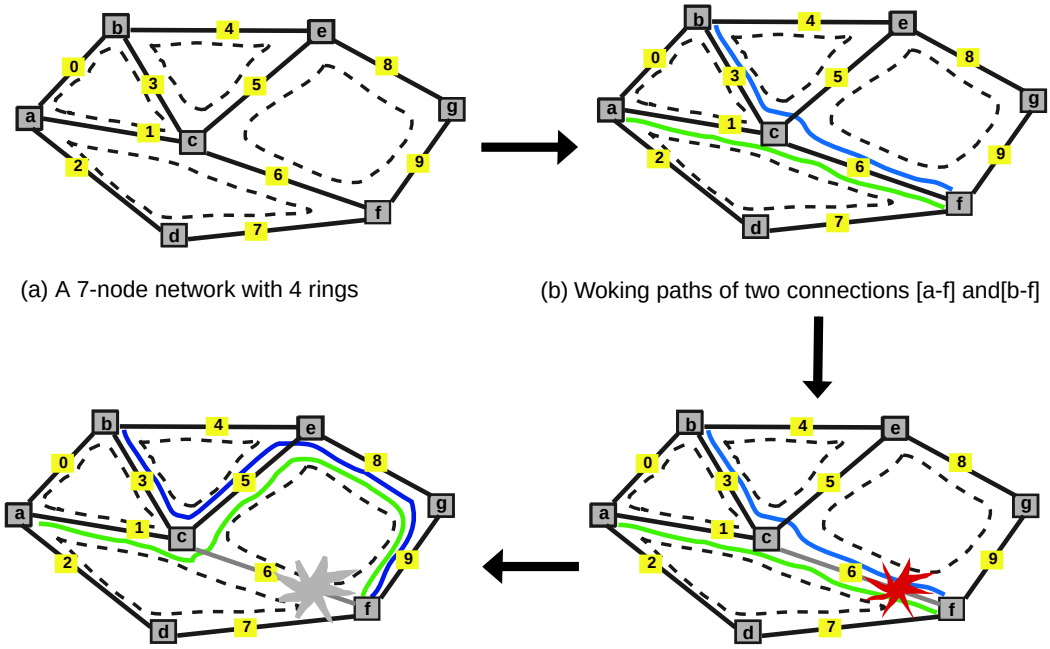
Subject to:

$$S_j \geq \delta_i^j \cdot \theta_i \cdot v_i, \qquad \forall i, j \in E \quad \text{and} \quad i \neq j \tag{3.2}$$

$$U_c^{SLA} \geq \sum_{\forall j \in W_c} (1 - a_j)(1 - \theta_j a_{r \setminus j}), \qquad \forall c \in C \tag{3.3}$$

$$0 \leq \theta_j \leq 1, \qquad \forall j \in E \tag{3.4}$$

Constraints in (3.2) ensure that link j provides enough spare capacity if protection route of link i uses that link. Constraints in (3.3), ensures that the E2E availability requirement of each connection specified in the SLA is met. Constraints in (3.4) restricts that the predefined restoration attempt can store only a part of the interrupted bandwidth. For link j, θ_j of the working bandwidth is protected by the protection path of that link while the rest $1 - \theta_j$ of working bandwidth is not protected. The variables are to be solved are θ_j and S_j for all $j \in E$. The number of variables grows on the order of $O\Big(2 \times |E|\Big)$ and the number of constraints grows on the order of $O(|E| \times |E - 1| + |C|)$. Fig. 3.4 illustrates how the working bandwidth of a link can be restored at the event of a failure while still satisfying the E2E availability requirements.



(a) A 7-node network with 4 rings

(b) Woking paths of two connections [a-f] and[b-f]

(c) Both connections disrupts due to failure on link 6

(d) Both paths restored through corrsponding ring

Figure 3.4: Illustration of how a link can be resorted at the event of a failure while still satisfying the E2E availability requirements.

Chapter 4

Simulation Results and Discussions

Simulation results are presented comparing the performance of different ring selection strategies used in the proposed scheme. The chapter concludes with some remarks.

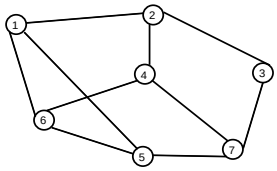
4.1 Network Topology and Simulation Parameters

The simulation program is developed using C++ and executed on a LINUX server with dual-core 2.8 GHz CPU and 1 GB memory. The LP formulation is solved using CPLEX 10.0 optimization packages [40]. Five network topologies are used as representative of typical IP-core network to asses the proposed scheme. The networks have average nodal degrees $\bar{d}$ ranged from 2.86 to 8.45 as given in Table 4.1. Network topologies are also shown in Fig. 4.1 excluding Bell Canada network which is too large to be shown. Without loss of generality, the following assumptions are made: (a) traffic demands between any node pairs are unknown; (b) the network has symmetrical working bandwidths on any links without loss of generality; (c) each node can serve

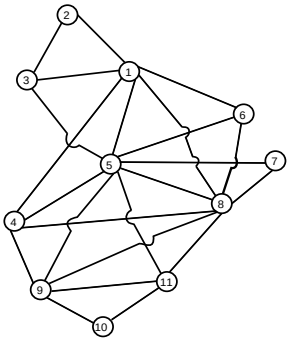
Table 4.1: Network information

Network	TestNet1	TestNet2	GerNet	EuroNet	BellNet
V	7	11	17	37	88
E	10	23	26	58	372
$\bar{d}$	2.86	4.18	3.06	3.13	8.45

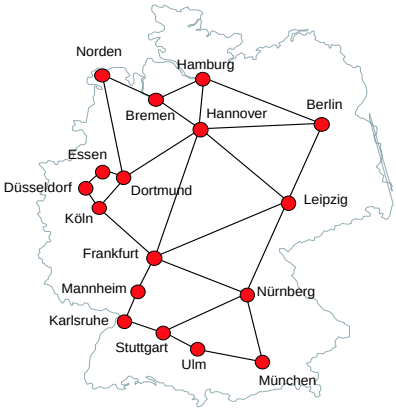
The number of links E here is the number of undirected links



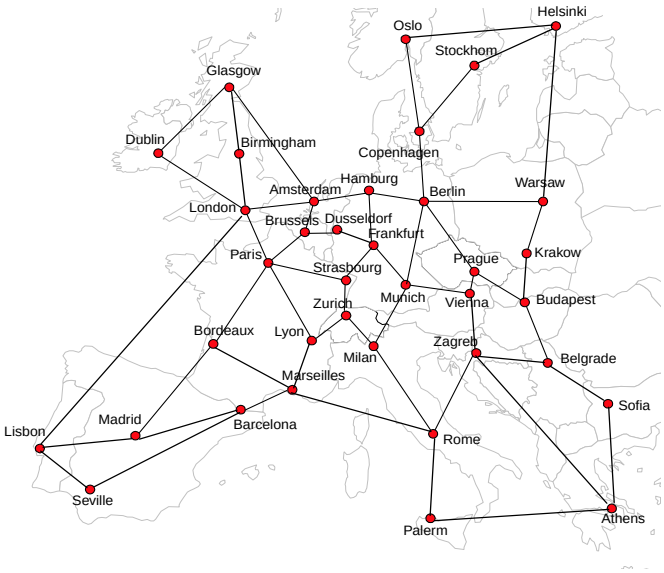
(a) 7 node test network (TesNet1)



(b) 11 node test network (TestNet2)



(c) 17 node German network (GerNet)



(d) 37 node European network (EuroNet)

Figure 4.1: Network topologies

Table 4.2: Performance comparison between different ring selection strategies in terms of redundancy for all networks.

U_{SLA}	10^{-3}			10^{-4}			5×10^{-4}			10^{-5}		
Ring Selection Strategy	M1*	M2⋆	M3§	M1	M2	M3	M1	M2	M3	M1	M2	M3
TestNet1	41	21	21	79	71	71	82	74	74	84	Inf †	Inf
TestNet2	55	38	26	86	82	78	87	85	82	90	Inf	Inf
GerNet	27	22	17	39	31	25	59	51	47	95	Inf	Inf
EuroNet	17	14	11	22	19	15	38	32	25	87	Inf	Inf
BellNet	9	5	4	24	11	10	31	13	12	Inf	Inf	Inf

*HARs; ⋆MNRs; §SPRs; †Infeasible

as a ingress or egress node of the network; and (d) link failure is proportional to link length, and the average failure rate is 1/MTTF per km. normalized in the unit of FIT. Outage time limit or the unavailability specified in the SLA is taken same for all possible connection pairs to simplify the simulation. To compare the proposed scheme which employs different ring selection methods, the performance metrics taken are network redundancy, number of connections for which LP become infeasible and execution time.

4.2 Network Redundancy

The network redundancy is measured by the ratio of the total spare capacity over the total working capacity. The redundancy in percent required by the proposed SCA scheme employing different ring selection strategies for all network topologies are listed in Table 4.2 as found from the simulation. Figs. 4.2 and 4.3 show the redundancy required by the proposed SCA scheme employing different ring selection strategies with U_{SLA} for the network BellNet and TestNet2, respectively. The varia-

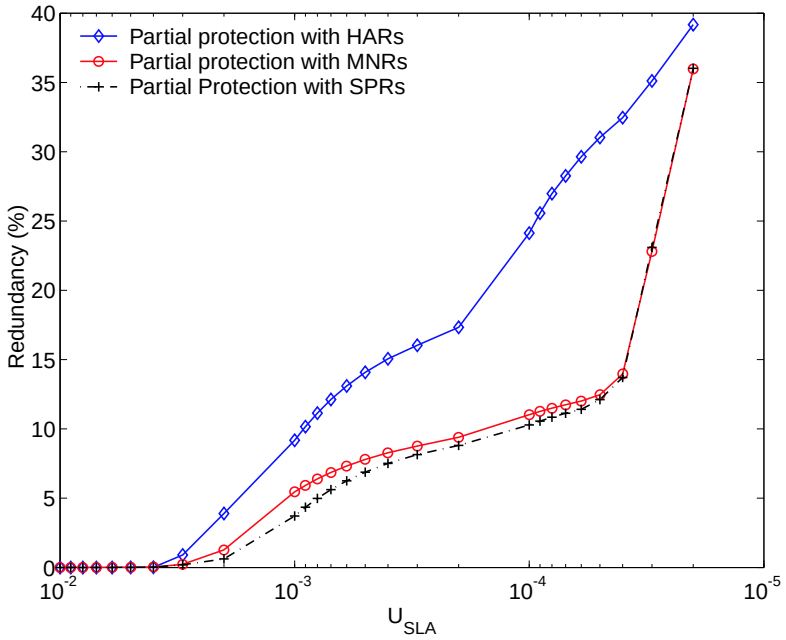


Figure 4.2: Performance comparison between different ring selection strategies in terms of redundancy for Bell Canada network.

tions in redundancy for other networks are also found similar to these two networks. For all ring selection strategies, redundancy increases as the U_{SLA} or the outage time limit specified in SLA is reduced. Nonetheless, network resources can be saved depending on the unavailability stated in the SLA. As for example, in case of BellNet when employs HARs as its protection route, the required redundancies are 9% and 24% at $U_{SLA} = 10^{-3}$ and $U_{SLA} = 10^{-4}$, respectively. Whereas, in case of TestNet2 employing HARs as its protection route, the required redundancies are 55% and 86% at $U_{SLA} = 10^{-3}$ and $U_{SLA} = 10^{-4}$, respectively. When the proposed SCA scheme employs other ring selection strategies (MNRs and SPRs), the variation in redundancy for other networks are also found similar to that of HARs selection strategy.

Thus it is clear that redundancy increases as the U_{SLA} or the outage time limit

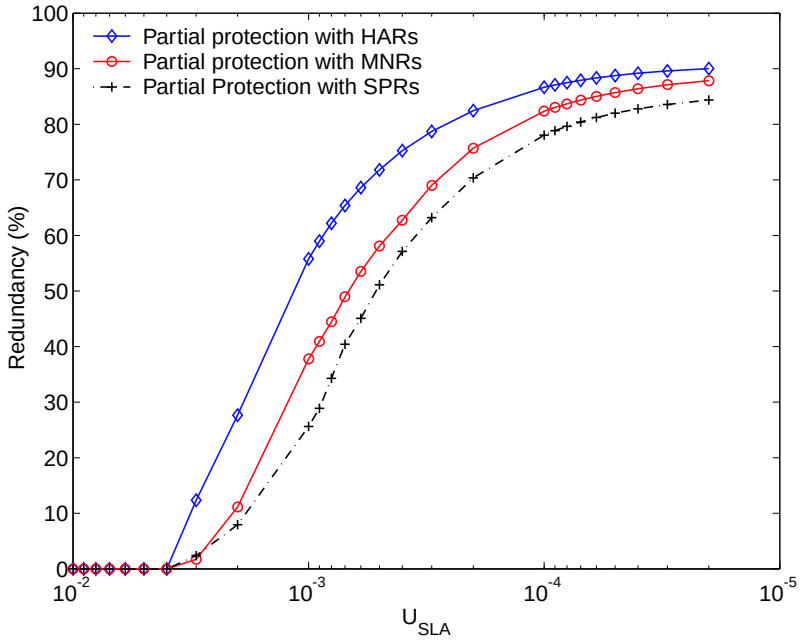


Figure 4.3: Performance comparison between different ring selection strategies in terms of redundancy for 11-node test network.

specified in SLA is reduced. Inversely, network resources can be saved if lower availability is offered in the SLA. Note also that when the availability requirement is above 0.9999 (unavailability specified in SLA is lower than 10^{-4}), the redundancy increases sharply. This is because high availability requirement can only be met with protection level close to 100%. Also large and dense network (BellNet) tends to require less redundancy than the small and sparse network (TestNet2) at specific U_{SLA}.

Different ring selection strategies are now compared in terms of redundancy. As can be seen, for the network BellNet, the require redundancy by the protection scheme when employing HARs, MNRs and SPRs, are 24%, 11%, and 10%, respectively at specific $U_{SLA} = 10^{-4}$. Also for the network TestNet1, the require redundancy by the protection scheme when employing HARs, MNRs and SPRs, are 79%, 71%, and 71%,

Table 4.3: Performance comparison between different ring selection strategies in terms of LP feasibility for all networks.

U_{SLA}	5×10^{-4}			10^{-5}			5×10^{-5}			10^{-6}		
Ring Selection Strategy	M1*	M2⋆	M3§	M1	M2	M3	M1	M2	M3	M1	M2	M3
TestNet1	0	0	0	0	7	7	0	19	19	40	71	71
TestNet2	0	0	0	0	8	8	0	38	37	55	79	79
GerNet	0	0	0	0	3	3	0	17	18	25	71	72
EuroNet	0	0	0	0	6	7	0	22	23	23	84	85
BellNet	0	0	0	0.1	1	0.9	3	7	7	33	42	42

*HARs; ⋆MNRs; §SPRs

respectively at specific $U_{SLA} = 10^{-4}$. As expected, the SCA scheme when employs HARs requires more redundancy than the other two ring selection strategies as the former method resulted in longer routes in some of its protection rings in order to get highest availability. There is not that much visible gap between the protection schemes that employ MNRs and SPRs in their protection paths. It is also to be noted that although the proposed SCA when employs HARs accrues highest redundancy when compared to other ring selection strategy at lower U_{SLA}, this method can give feasible results where other methods fail in doing so. For example, at $U_{SLA} = 10^{-5}$, the scheme employing HARs still results in feasibility where other two methods gives infeasible results for all network topologies except BellNet.

4.3 LP Feasibility

The second objective measure is the number of connections for which LP becomes infeasible. Numerical results are summarized in Table 4.3. For BellNet and TestNet2, the number of connections in percent for which LP becomes infeasible versus

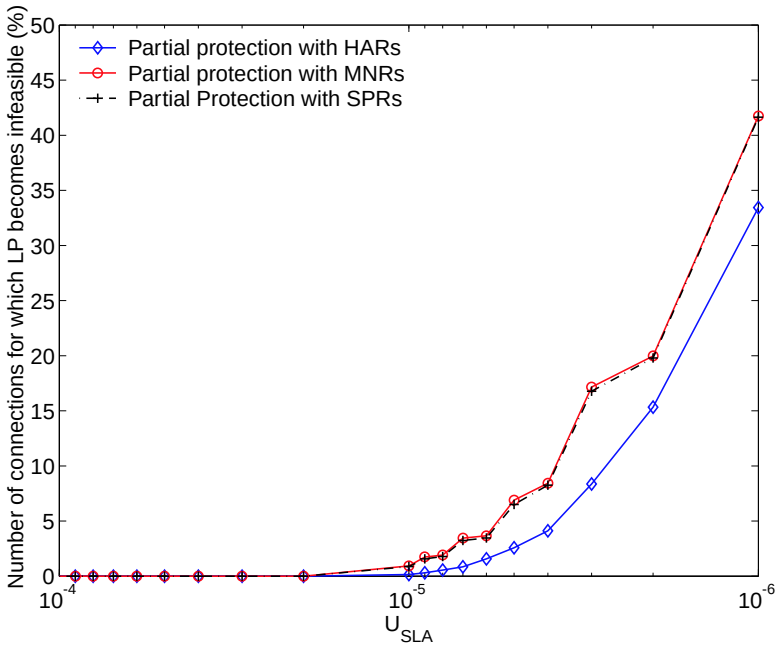


Figure 4.4: Performance comparison between different ring selection strategies in terms of LP feasibility for Bell Canada network.

U_{SLA} are plotted in Fig. 4.4 and Fig. 4.5, respectively. Similar trends are found for other networks too. In case of BellNet when employs MNRs as its protection route, the numbers of connections for which LP becomes infeasible are 1% and 7% at $U_{SLA} = 10^{-5}$ and $U_{SLA} = 5 \times 10^{-5}$, respectively. Whereas, in case of TestNet2 employing MNRs as its protection route, the number of connections for which LP become infeasible are 8% and 38% at $U_{SLA} = 10^{-5}$ and $U_{SLA} = 5 \times 10^{-5}$, respectively. It is clear that the number of connections for which LP becomes infeasible increases as the availability requirement tightens or U_{SLA} is reduced.

Different ring selection strategies are now compared in terms of LP feasibility. In case of the network EuroNet, when the SCA scheme employs HARs, MNRs and SPRs, the number of connections for which LP become infeasible are 0%, 6%, and

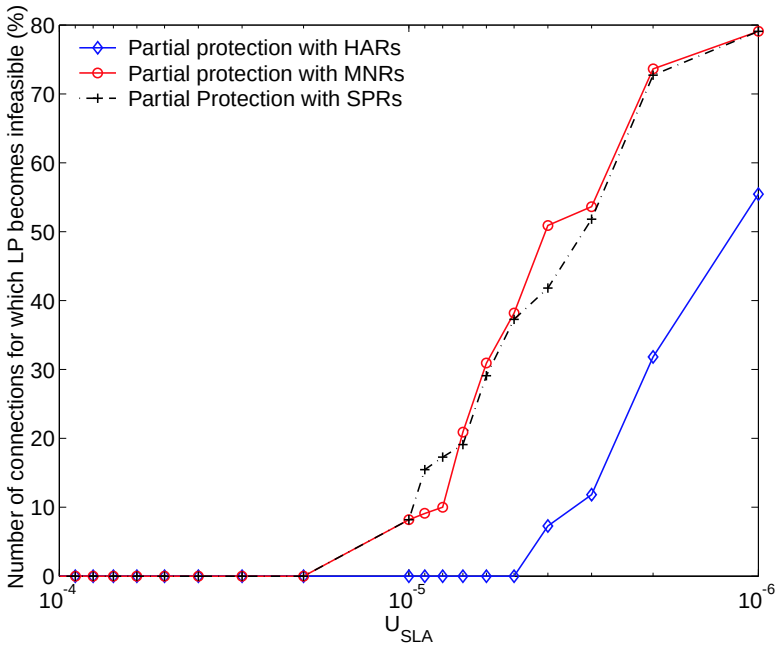


Figure 4.5: Performance comparison between different ring selection strategies in terms of LP feasibility for 11-node test network.

7%, respectively at specific $U_{SLA} = 10^{-5}$. Also for the network TestNet2, when the SCA scheme employs HARs, MNRs and SPRs, the numbers of connections for which LP becomes infeasible are 0%, 8%, and 8%, respectively at specific $U_{SLA} = 10^{-5}$. As expected, the SCA scheme employing HARs performs better than others. The number of connections for which LP becomes infeasible is lower for HARs than that of other two methods (MNRs and SPRs). When the availability requirement is high, the scheme employing HARs still results in feasibility where other two methods gives infeasible results. This gives valid reason to employ rather complex HAR selection method in order to obtain feasible results.

Table 4.4: Execution time of different ring formation schemes.

Test Network	TestNet1	TestNet2	GerNet	EuroNet	BellNet
HARs	≤ 1 ms	2 s	3 s	5 s	23 s
MNRs	≤ 1 ms	≤ 1 ms	≤ 1 s	2 s	4 s
SPRs	≤ 1 ms	≤ 1 ms	≤ 1 s	≤ 1 s	≤ 1 s

4.4 Execution Time

The third objective measure is program execution time. Numerical results are summarized in Table 4.4. Once the rings are selected, the program execution time to solve the LP formulation is same for all different ring selection methods. However, execution time to select rings is different for different ring selection algorithms. The number of rings formed in MNRs is less than the number of links in the network; as links share the rings among them. While the number of rings to be formed is equal to the number of rings for other two methods (HARs and SPRs). Thus MNR selection method is the most efficient as it requires the least time. On the other hand, HARs method is the least efficient in terms time consuming as this method requires to find all possible routes in search of protection route of highest availability.

4.5 Comparisons with other methods

In this section, simulation results are compared with other conventional schemes. The other methods implemented for comparison purpose are Herzberg and Bye's hop-limited span protection (HerzByeHopLim) [13] and (FD/FID) policy based availability-aware SBPP methods (SBPP-FD and SBPP-FID) [32]. As SBPP-FD/FID methods require E2E bandwidth; for comparison purpose, it is assumed that this infor-

Table 4.5: Performance comparison with other existence methods in terms of redundancy for all networks

Protection Level	$\theta = 0.4$						$\theta = 0.8$					
Method	M1*	M2*	M3§	M4$^{\natural}$	M5†	M6‡	M1*	M2*	M3§	M4$^{\natural}$	M5†	M6‡
TestNet1	25.3	18.1	18.0	51.3	54.0	47.2	65.0	61.3	63.5	72.0	75.6	70.1
TestNet2	24.1	14.9	13.5	56.3	51.3	46.2	61.3	55.2	55.0	69.1	71.2	64.0
GerNet	17.2	10.1	9.2	48.1	55	37.5	52.6	43.1	43.8	62.5	68.0	57.2
EuroNet	17.1	10.4	10.6	43.6	45.7	36.0	57.3	55.1	54.9	64.1	62.1	59.1
BellNet	23	12.8	12.1	43.3	55.3	38.6	42.8	40.2	40.0	64.2	70.1	68.1

Proposed schemes with *HARs, *MNRs, §SPRs; $^{\natural}$SBPP-FD scheme; †SBPP-FID scheme; ‡HerzBye Hop limited scheme

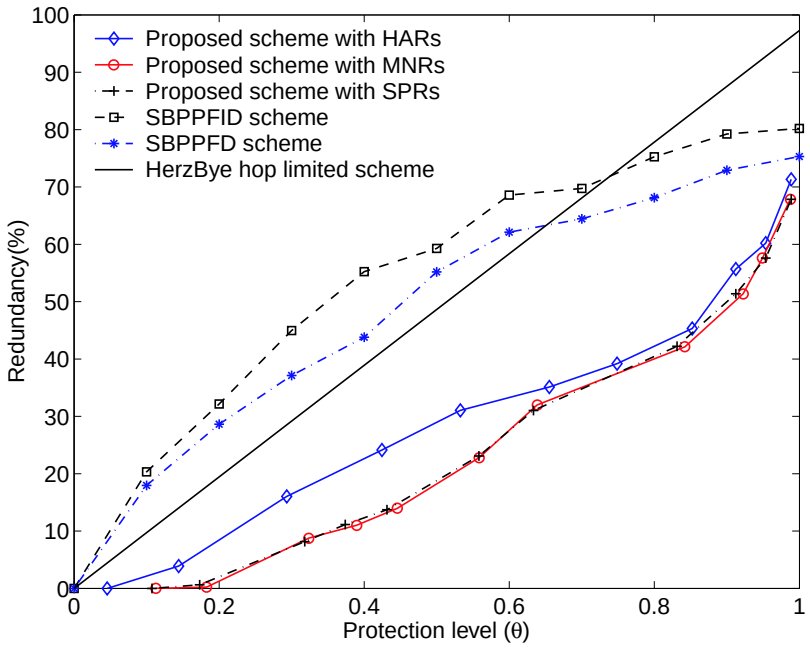


Figure 4.6: Performance comparison with other existence methods in terms of redundancy for Bell Canada network.

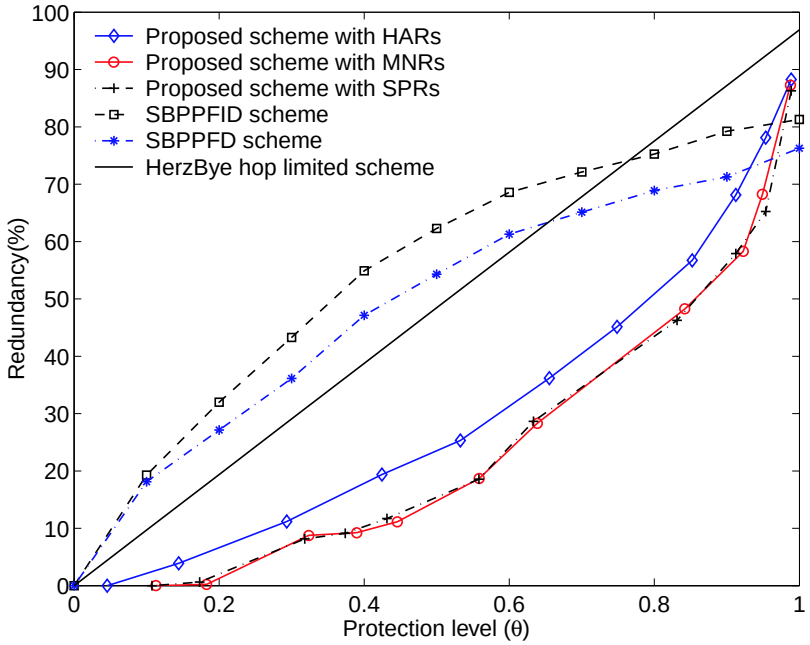


Figure 4.7: Performance comparison with other existence methods in terms of redundancy for German network.

mation is available with working bandwidths remain the same. Table 4.5 summarizes the numerical results for all methods. Figs. 4.6 and 4.7 show the variations of required redundancy in percent with protection level for all methods over BellNet and GerNet, respectively. The variations found for other networks are similar to these two networks. In all cases, the proposed SCA scheme performs better in terms of redundancy required for protection. For example, in case of BellNet, with $\theta = 0.4$, the redundancy required for proposed SCA scheme (employing HARs/MNRs/SPRs) is less than 23%, whereas the redundancy required by other schemes (HerzByeHopLim/SBPP-FD/SBPP-FID) is greater than 38.6%. Again, in case of GerNet, with $\theta = 0.8$, the redundancy required for proposed SCA scheme (employing HARs/MNRs/SPRs) is less than 52.6%, whereas the redundancy required by

other schemes (HerzByeHopLim/SBPP-FD/SBPP-FID) is greater than 57.2%. The proposed SCA scheme includes E2E the availability constraints in the LP formulation and allocates only that amount spare capacity just to meet the E2E availability. The HerzByeHopLim doesn't consider E2E availability, thus it fails to reduce redundancy unlike the proposed scheme. The SBPP-FD/FID methods allocates spare capacity through its E2E protection path for all connections. Some of the E2E protection paths are quite long where as in case of proposed scheme all of its protection routes are quite short. Hence, the redundancy required for the proposed scheme is less than the other methods.

Chapter 5

Conclusions and Future Plan

In this thesis work, a new algorithm for availability-aware spare-capacity assignment in survivable networks has been proposed, which attempts to optimize network resource utilization. The proposed SCA scheme ensures that it meets the E2E availability requirements by employing protection rings covering all links in a network scenario where E2E bandwidth requirement of any connection is unknown. Simulation results show that the proposed SCA scheme saves network resources significantly depending on the availability requirement stated in SLA. Different ring selection methods are also presented and compared from the aspect of network redundancy and LP feasibility. The SCA scheme, that employs HARs as its protection routes, requires more redundancy than the other two ring selection strategies as the former method resulted in longer routes in some of its protection rings in order to get highest availability. However, the SCA scheme employing HARs performs better in terms of LP feasibility. When the availability requirement is high; the scheme employing HARs still results in feasibility where other two methods give infeasible results. This gives valid reason

to employ rather complex ring selection method HARs in order to have feasible results. Incorporation of partial protection within the proposed architecture has also provided a significant performance improvement by reducing the allocation of spare capacity. The proposed SCA scheme, which utilizes different ring selection strategies, has a significant performance improvement over other popular SCA schemes in terms resource allocation.

A number of additional extensions to the proposed protection scheme would be interesting. In this thesis work, for simplified availability analysis, each link is protected with single ring. When the availability requirement is too tight the LP fails to give feasible result. This is due to the fact that some of links with lower physical availability require protection level higher than 1. This indicates those links need to be protected by at least one more ring to meet the availability constraint. The LP formulation can be modified adding multiple protection rings in this scenario.

Partial protection is adopted based on the fact that on divisibility of the LSP in the restoration phase, where the source node has the capability of randomly dropping some service sessions of the LSP while restoration is performed. Hence, the restoration factors (θ) derived in solving the LP for each connection are the lower bound and should be discrete instead of continuous. The LP formulation can be modified for discrete solution of restoration factors to support dropping granularity.

Bibliography

[1] J. Marzo, P. Maryni and P. Vil, "Towards QoS in IP-based Core Networks; A Survey on Performance Management, MPLS Case", in *Proc. of Int. Symposium on Performance Evaluation of Computer and Telecommunication Systems*, pp. 1-7, 2001.

[2] J. Zhang and B. Mukherjee, "A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges," *IEEE J. on Network*, vol. 18, no. 2, pp. 41-48, Apr. 2004.

[3] C. Metz, "IP Protection and Restoration," *IEEE Internet Computing*, vol. 4, no. 2, pp. 97-102, Mar. 2000.

[4] G. Birkan, J. Kennington, E. Olinick, A. Ortynski, and G. Spiride, "Design Strategies for Meeting Unavailability Targets Using Dedicated Protection in DWDM Networks Birkan", *J. of Lightwave Tech.,* vol. 25, no. 5, pp. 1120-1129, 2007.

[5] W. Yao and B. Ramamurthy, "Survivable Traffic Grooming with Differentiated End-to-End Availability Guarantees in WDM Mesh Networks", in *proc. IEEE LANMAN'04*, pp. 86-90, 2004.

[6] P. -H. Ho, and T. Mouftah, "Shared Protection in Mesh WDM Networks," *IEEE Commun. Mag.,* vol. 42, no. 1, pp. 70-76, Jan. 2004.

[7] P. -H. Ho, J. Tapolcai, and H. T. Mouftah, "On Optimal Diverse Routing for Shared Protection in Mesh WDM Networks," *IEEE Trans. on Reliability*, vol. 53, no. 6, pp. 216-225, June 2004.

[8] J. Doucette, M. Clouqueur, and W. D. Grover, "On the Availability and Capacity Requirements of Shared Backup Path-Protected Mesh Networks", *SPIE Optical Network Mag.,* pp. 29-44, 2003.

[9] G. Shen, and W. D. Grover, "Survey and Performance Comparison of Dynamic Provisioning Methods for Optical Shared Backup Path Protection," *IEEE INFOCOM'05*, pp. 387-396, 2005.

[10] D. Xu, C. Qiao, and Y. Xiong, "An Ultra-fast Shared Path Protection Scheme-Distributed Partial Information Management, Part II", *ICNP'02*, pp. 344-353, 2002.

[11] P. -H. Ho, J. Tapolcai, and T. Cinkler, "Segment Shared Protection in Mesh Communications Networks with Bandwidth Guaranteed Tunnels", *IEEE/ACM Trans. on Networking*, vol. 12, no. 6, Dec. 2004.

[12] G. Shen and W. D. Grover, "Extending the p-Cycle Concept to Path-Segment Protection for Span and Node Failure Recovery," *IEEE JSAC*, vol. 21, no. 8, pp. 1306-1319, Oct. 2003.

[13] M. Herzberg and S. Bye, "An Optimal Spare-Capacity Assignment Model for

Survivable Networks With Hop Limits," in *Proc. IEEE GLOBECOM'94*, pp. 1601-1607, 1994.

[14] M. Clouqueur, and W. D. Grover, "Availability Analysis of Span-Restorable Mesh Networks", *IEEE J. on Selected Areas in Commun.*, vol. 20, no. 4, pp. 810-820, May 2002.

[15] W. D. Grover, and D. Stamatelakis, "Cycle-Oriented Distributed Preconfiguration: Ring-Like Speed with Mesh-Like Capacity for Self-Planning Network Restoration," *ICC'98*, pp. 537-543.

[16] W. D. Grover, and D. Stamatelakis, "Bridging the Ring-Mesh Dichotomy with p-cycles," *DRCN'00*, pp. 92-104.

[17] W. D. Grover, J. Doucette, "Advances in Optical Network Design With p-Cycles: Joint Optimization and Pre-Selection of Candidate p-Cycles," *IEEE LEOS Summer Topicals,* pp. 49-50, 2000.

[18] W. D. Grover, *"Mesh Based Survivable Networks: Options and Strategies for Optical, MPLS, SONET, And ATM Networking"*, Prentice Hall, 2004.

[19] W. D. Grover, "The Protected Working Capacity Envelope Concept: An Alternate Paradigm for Automated Service Provisioning," *IEEE Commun. Magazine,* vol. 42, no. 1, pp. 62-69, Jan. 2004.

[20] J. Zhang, H. Zang, and B. Mukherjee, "A New Provisioning Framework to Provide Availability-Guaranteed Service in WDM Mesh Networks", in *Proc. ICC'03*, pp. 1484-1488.

[21] D. Arci, D. Petecchi, G. Maier, A. Pattavina, and M. Tornatore, "Availability Models for Protection Techniques in WDM Networks", in *Proc. of DRCN'03,* pp. 158-166, 2003.

[22] M. Clouqueur and W. D. Grover, "Availibility Analysis of Span-Restorable Mesh Networks," *IEEE J. Select. Areas of Commun.,* vol. 20, no. 4, pp. 810-821, May 2002.

[23] Y. Huang, W. Wen, J. P. Heritage, and B. Mukherjee, "A Generalized Protection Framework Using a New Link-State Availability Model for Reliable Optical Networks", *IEEE/OSA J. of Lightwave Tech.*, pp. 2536-2547, vol. 22, no. 11, Nov. 2004.

[24] D. A. A. Mello, J. U. Pelegrini, R. P. Ribeiro, D. A. Schupke, and H. Waldman, "Dynamic Provisioning Of Shared-Backup Path Protected Connections With Guaranteed Availability Requirements", in *Proc. of 2nd International Conf. on Broadband Networks*, pp. 397-404, 2005.

[25] L. Zhou and W.D. Grover, "A Theory for Setting the "Safety Margin" on Availability Guarantees in an SLA", in *Proc. of Design of Reliable Communication Networks*", pp. 403-409, Oct. 2005.

[26] R. Clemente, M. Bartoli, M. C. Bossi, G. D'Orazio, and G. Cosmo, "Risk Management in Availability SLA", in *Proc. of Design of Reliable Commun. Networks*, pp. 411-418, Oct. 2005.

[27] Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating Optimal Spare

Capacity Allocation by Successive Survivable Routing", *IEEE/ACM Trans. on Networking,* vol. 13, no. 1, pp. 198-211, 2005.

[28] D. A. Schupke, W. D. Grover, and M. Clouqueur, "Strategies for Enhanced Dual Failure Restorability with Static or Reconfigurable p-cycle networks," in *Proc. of ICC'04,* pp. 1628-1633, June 2004.

[29] P. -H. Ho and H. T. Mouftah, "Reconfiguration of Spare Capacity for MPLS-based Recovery for the Internet Backbone Networks", *IEEE/ACM Trans. on Networking,* vol. 12, no. 1, pp. 73-85, Feb. 2004.

[30] L. Shen, X. Yang, and B. Ramamurthy, "A Load-balancing Spare Capacity Reallocation Approach in Service-rich SONET Metro Mesh Networks", in *Proc. of IEEE Broadnet'04*, pp. 269-278, 2004.

[31] P.-H. Ho, et. al., "A Novel Dynamic Availability-Aware Survivable Routing Architecture with Partial Restorability," in *Proc of 23rd Biennial Symposium on Commun.,* pp. 360-363, 2006.

[32] Q. Guo, P. -H. Ho, A. Haque, and H. T. Mouftah, "Availability-Constrained Shared Backup Path Protection (SBPP) for GMPLS-Based Spare Capacity Reconfiguration", in *Proc. of ICC'07.*

[33] M. Tacca, A. Fumagalli, A. Paradisi, F. Unghvry, K. Gadhiraju, S. Lakshmanan, S. M. Rossi, A. C. Sachs, and D. S. Shah, "Differentiated Reliability in Optical Networks: Theoretical and Pratical Results," *J. Lightwave Tech.*, vol. 21, no. 11, pp. 2576-2586, Nov. 2003.

[34] Y. Yinghua, C. Assi, S. Dixit, and M. A. Ali, "A Simple Dynamic Integrated Provisioning/Protection Scheme in IP Over WDM Networks" *IEEE Commun. Magazine*, vol. 39, no. 11, pp. 174-182, Nov. 2001

[35] C. V. Saradhi, M. Gurusamy, and L. Zhou, "Differentiated QoS for Survivable WDM Optical Networks," *IEEE Commun. Mag.*, pp. S8-S14, May 2004.

[36] R. Jo. Gibbens, S. K. Sargood, F. P. Kelly, H. Azmoodeh, R. MacFadyen, and N. MacFadyen, "An Approach to Service Level Agreements for IP Networks with Differentiated Services" *Philosophical Trans: Mathematical, Physical and Engineering Sciences*, vol. 358, no. 1773, pp. 2165-2182, 2000.

[37] R. Clemente, M. Bartoli, M. C. Bossi, G. D'Orazio and G. Cosmo, "Risk Management in Availability SLA," in *Proc. of Design of Reliable Communication Networks*, pp. 411-418, 2005.

[38] A. J. Vermon, J. D. Portier, "Protection of Optical Channels in All-Optical Networks," *National Fiber Optic Engineers Conference*, pp. 1696-1706, 2002.

[39] Y. Perl and Y. Shiloach, "Finding Two Disjoint Paths Between Two Pairs of Vertices in a Graph," *J. of the ACM,* vol. 25, no. 1, pp. 1-9, Mar. 25, 1978.

[40] CPLEX: An optimizer by ILOG Inc, url : www.ilog.com