A Distributed Probability-Based Backup Resource Allocation Algorithm for Network Reliability

by

Minzhe Li, B.Eng.

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfillment of
the requirements for the degree of

Master of Applied Science

Ottawa-Carleton Institute for Electrical and Computer Engineering
Department of Systems and Computer Engineering
Carleton University
Ottawa, Canada

August, 2004

© Copyright 2004, Minzhe Li

Library and
Archives Canada

Bibliothèque et
Archives Canada

Published Heritage
Branch

Direction du
Patrimoine de l'édition

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

ISBN: 0-612-97421-9

Our file Notre référence

ISBN: 0-612-97421-9

The author has granted a non-exclusive license allowing the Library and Archives Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

PAGINATION ERROR.

TEXT COMPLETE.

ERREUR DE PAGINATION.

LE TEXTE EST COMPLET.

ABSTRACT

With the rapid development of the Internet technology, it is essential to handle network failures such that communication reliability is guaranteed. In this thesis, a new distributed backup resource allocation algorithm is proposed to tackle the issue of bandwidth efficiency as well as to support guaranteed network reliability in path-oriented protection schemes. This feature is achieved by analyzing the relationship between the amount of allocated backup resource and the link failure probability, therefore this algorithm works consistently against multiple-failures. The proposed algorithm can be implemented in a distributed manner ensuring the network overhead within acceptable bounds. Furthermore, the “Shared Risk Link Group (SRLG) protection” concept and the reliability distribution policies are incorporated into this scheme efficiently. A modification to the current signaling mechanisms is also discussed. Joint consideration of these features is supposed to achieve a better performance in terms of Call Acceptance Rate and Total Bandwidth Consumption in a large scale network which has also been verified by the mathematical analysis and by performing a set of simulations during the research.

ACKNOWLEDGMENTS

I would like to express my deepest appreciation to my supervisors, Dr. Changcheng Huang and Dr. Anand Srinivasan, for the guidance, encouragement, and feedback they provided me during my research.

NCIT supported me during my research work. I would like to express my sincere gratitude to Dr. Mobammed Zaid and Dr. Robert Crawball who gave me much help and encouragement to complete this research.

I want to thank Dr. Rama Munikoti and Dr. Kalai Chelvan from EION Inc. for their unselfish and stimulating support.

Finally, I take this opportunity to express my gratitude for the constant support, understanding, and love that I received from my wife Shan during the past years.

TABLE OF CONTENTS

	<u>Page</u>
ABSTRACT	iii
ACKNOWLEDGMENTS	iv
TABLE OF CONTENTS.....	v
LIST OF TABLES.....	vii
LIST OF FIGURES	viii
LIST OF NOTATIONS	x
LIST OF ACRONYMS	xiii
CHAPTER 1–INTRODUCTION	1
1.1 Motivation and Background	1
1.2 Thesis Objectives and Contributions	7
1.3 Thesis Organization	9
CHAPTER 2–LITERATURE AND SURVEYS.....	11
2.1 Surveys on Network Failure Recovery Mechanisms.....	11
2.1.1 Network Layer Protection – Rerouting.....	11
2.1.2 Link and Physical Layer Protection – Protection Switching	12
2.1.3 MPLS Failure Recovery Mechanisms	15
2.1.3.1 Path Protection.....	15
2.1.3.2 Link Protection	16
2.1.3.3 Segmented Protection	17
2.1.3.4 Fast Reroute	18
2.2 Surveys on QoS Routing.....	19
2.2.1 QoS Routing Algorithms	19
2.2.2 Joint Path Selection vs. Separate Path Selection	20
2.3 Backup Resource Allocation Algorithms	23
2.4 Failure Recovery in Multiple Failures Model	26
2.5 Probability-based Approach for Network Reliability	28
2.6 Research Summary	31

CHAPTER 3–PROBLEM STATEMENT	32
3.1 Definitions	32
3.2 Related Equations	37
3.3 Some Assumptions.....	42
CHAPTER 4–LFP BASED BACKUP RESOURCE ALLOCATION ALGORITHM.....	46
4.1 General.....	46
4.2 Sharing Blocks Management	48
4.3 Procedure of LFP-First Fit Algorithm	50
4.4 LFP First-Fit vs. LFP Best-Fit	59
4.5 Reliability Constraint Distribution	62
4.6 Extensions to RSVP-TE.....	63
4.7 Summary	64
CHAPTER 5–PERFORMANCE EVALUATION	68
5.1 General.....	68
5.2 Simplified Network Model	69
5.2.1 Description of the Network Model	70
5.2.2 Mathematical Analysis	71
5.2.3 Simulation Results	77
5.3 Call-Acceptance-Rate Test of the Simplified Network Model.....	80
5.3.1 Simulation Model Description.....	80
5.3.2 Mathematical Analysis 1 for Case 1: Fixed Bandwidth Demand.....	81
5.3.3 Simulation Results for Case 1	84
5.3.4 Mathematical Analysis for Case 2: Uniformly Distributed Bandwidth Demand	86
5.3.5 Simulation Results (Case 2).....	89
5.4 Simulation Results in a NSFNET Network	89
CHAPTER 6–CONCLUSIONS AND FUTURE WORK	96
6.1 General.....	96
6.2 Advantages.....	96
6.3 Future Research	98
REFERENCES	100

LIST OF TABLES

<u>Table</u>	<u>page</u>
Table 1: List of calculated working paths in step 1	53
Table 2: List of the calculated working path failure probability in step 2.....	54
Table 3: Some information of the connections in step 3	55
Table 4: Calculated backup path failure probability constraint in step 4	56
Table 5: Calculated backup link constraint in step 5	57
Table 6: Calculated $F_{RB_{mn}^i}(y)$ and $P(RB_{mn}^i = y)$ when $M=2$	74
Table 7: Calculated Values of $\varepsilon(RB_{mn}^i)$ and N_{max} under different value of M	76

LIST OF FIGURES

<u>Figure</u>	<u>page</u>
Figure 1: SONET Two-fiber UPSR Automatic Protection Switching	13
Figure 2: SONET Two-fiber BLSR Automatic Protection Switching	13
Figure 3: MPLS Path Protection.....	16
Figure 4: MPLS Link Protection	16
Figure 5: MPLS Segmented Protection	17
Figure 6: MPLS Protection - Fast Reroute	18
Figure 7: Separate Path Selection Link-disjoint Pair Algorithm	22
Figure 8: Disadvantage of SPS Link-disjoint Pair Algorithm	23
Figure 9: End-to-end Reliability Constraint Distribution	29
Figure 10: Illustration of the Service and the Reserved Bandwidth Allocation	34
Figure 11: Illustration of Two Connections within the Same SRLG	36
Figure 12: The Signaling Process of LFP-FF Algorithm	51
Figure 13: An Illustration of the LFP-FF Algorithm.....	52
Figure 14: Flow Chart of First-Fit Backup Resources Allocation.....	60
Figure 15: Flow Chart of Best-Fit Backup Resources Allocation	61
Figure 16: Improvement of the Backup Bandwidth Block Management (LFP-BF)	62
Figure 17: A Simplified Network Model.....	69

Figure 18: The Distribution Function of the Bandwidth Demand in the Simplified Network Model	73
Figure 19: The Distribution Function of $RB_{mn}^i = \max(B_{c_1}, B_{c_2})$	75
Figure 20: Mathematical Analysis of the Average Maximum Number of Connections in the Simplified Network Model	77
Figure 21: Simplified Network Simulation Result: Average Maximum Number of Connections vs. Network Load.....	79
Figure 22: Plot of the Performance with Error Bars Showing 95% Confidence Intervals	80
Figure 23: An Illustration of M/M/r/r queuing system	82
Figure 24: Mathematical Results: Call Acceptance Rate vs. Network Load in Simplified Network Model	84
Figure 25: Simulation Results: Call Acceptance Rate vs. Network Load in Simplified Network Model in Case 1 (Fixed Bandwidth Demand)	84
Figure 26: Analysis Results: Call Acceptance Rate vs. Network Load in Simplified Network Model in Case 2 (Random Bandwidth Demand).....	88
Figure 27: Simulation Results: Call Acceptance Rate vs. Network Load in Simplified Network Model in Case 2 (Random Bandwidth Demand).....	88
Figure 28: A NSFNet Simulation Model.....	89
Figure 29: NSFNet Simulation Result – Total Bandwidth Consumption vs. Network Load	91
Figure 30: NSFNet Simulation Result – Call Acceptance Rate vs. Network Load.....	93
Figure 31: NSFNet Simulation Result – Ratio of Total Reserved Bandwidth to Total Service Bandwidth vs. Network Load	94

LIST OF NOTATIONS

The following notations are used throughout this thesis:

Sets:

- $G = (V, E)$ is a directed network graph having a set V of nodes and a set E of links
- $V = \{v_1, v_2, \dots, v_N\}$ is a set of nodes in a network where N represents the total number of nodes
- $E = \{e_1, e_2, \dots, e_M\}$ is a set of links in a network where M represents the total number of links
- $C = \{c_1, c_2, \dots, c_K\}$ is a set of connections in a network, where each connection is denoted by a 3-tuple $c_i = (s_i, d_i, x_i)$. $s_i \in V$ is the source node; $d_i \in V$ is the destination node and x_i is the connection identifier
- WP_c is a set of links representing the working path of a connection $c \in C$ such that $WP_{c=(s,d,x)} = \{(s=e_0, e_1), (e_1, e_2), \dots, (e_{z-1}, d=e_z)\}$, $(e_{i-1}, e_i) \in E$
- BP_c is a set of links representing the backup path of a connection $c \in C$ such that $BP_{c=(s,d,x)} = \{(s=e_0, e_1), (e_1, e_2), \dots, (e_{z-1}, d=e_z)\}$, $(e_{i-1}, e_i) \in E$
- $T_{i,j}$ is a set of connections that use the link (i,j) as their backup link:

$$T_{i,j} = \{c_k \mid (i,j) \in BP_{c_k}, c_k \in C\}$$
. $T_{i,j}^n$ is a subset of $T_{i,j}$ representing the set of

connections that share the n^{th} Reserved Bandwidth Block (RBB) of link (i,j) with the allocated bandwidth denoted by $RB_{i,j}^n$.

Variables

- $AB_{i,j}$ denotes the total available (spare) bandwidth on link $(i,j) \in E$
- $SB_{i,j}$ denotes the total service bandwidth on link $(i,j) \in E$ which is being used by the working paths
- $RB_{i,j}$ denotes the total reserved bandwidth on link $(i,j) \in E$ which is being used by the backup paths
- $RB_{i,j}^k$ denotes the reserved bandwidth allocated to the k^{th} Reserved Bandwidth Block (RBB) of link $(i,j) \in E$
- B_c denotes the bandwidth demand requested by a connection $c \in C$
- Q_c denotes the overall reliability demand requested by a connection $c \in C$
- Q_c^{BP} denotes the backup path reliability demand or the residual reliability demand which is used as the reliability criteria for the selection of backup paths after a working path is already determined
- P_c^{Conn} denotes the failure probability of a connection $c \in C$
- $P_{i,j}^L$ denotes the failure probability of link $(i,j) \in E$
- P_c^{Path} denotes the path failure probability
- P_c^{WP} denotes the failure probability of a working path WP_c
- P_c^{BP} denotes the failure probability of a backup path BP_c

- R_c^{Comm} denotes the calculated reliability of a connection $c \in C$
- $R_{i,j}^L$ denotes the reliability of link $(i, j) \in E$
- R_c^{Path} denotes the calculated reliability of a path
- R_c^{WP} denotes the reliability of a working path WP_c
- R_c^{BP} denotes the reliability of a backup path BP_c
- H_c denotes the total number of hops along the backup path BP_c
- β_c^{BP} denotes the calculated backup path failure probability constraint for the backup path BP_c . β_c^{BP} is the complement of the backup path residual reliability, i.e., $\beta_c^{BP} = 1 - Q_c^{BP}$. The selection decision made for the backup path BP_c should satisfy this constraint, so that the overall connection reliability demand Q_c can be satisfied.
- β_c^L denotes the backup link constraint for each link along the backup path BP_c . The constraint β_c^L should be satisfied for each link along the backup path BP_c so that the backup path failure probability constraint β_c^{BP} or the residual reliability demand Q_c^{BP} can be satisfied.

LIST OF ACRONYMS

APS	– Automatic Protection Switching
BLSR	– Bi-directional Link-Switched Rings
CR	– Constrained based Routing
CR-LDP	–Constraint based Label Distribution Protocol
DiR	– Differentiated Reliability services
DPP	– Dedicated Path Protection
FIS	– Failure Indication Signal
IP	– Internetworking Protocol
IPS	– Intelligent Protection Switching
JPS	– Joint Path Selection
LER	– Label Edge Router
LFP	– Link Failure Probability
LFP-BF	– LFP-based Best-Fit algorithm for backup resource allocation
LFP-FF	– LFP-based First-Fit algorithm for backup resource allocation
LSA	– Service Level Agreement / Link-State Advertisement
LSR	– Label Switch Router
MAC	– Media Access Control
MIRR	– Minimum Interference Restorable Routing

MPLS – Multi-Protocol Label Switching

NSFNet – National Science Foundation Network

PML – Path Merging LSR

PSL – Path Switching LSR

QoS – Quality of Service

RBB – Reserved Bandwidth Block

RPR – Resilient Packet Ring

RSVP-TE –Traffic Engineering extensions to Resource ReSerVation Protocol

SONET/SDH – Synchronous Optical Network/Synchronous Digital Hierarchy

SCI – Sharing with Complete routing Information

SPI – Sharing with Partial routing Information

SPP – Shared Path Protection

SPS – Separate Path Selection

SRLG – Shared Risk Link Groups

SRLG-SPP – SRLG based Shared Path Protection

UPSR – Unidirectional Path Switched Rings

CHAPTER 1–INTRODUCTION

1.1 Motivation and Background

In the past, the Internet has provided only the “best-effort” service with no predictable performance. With the rapid increase in the processing power of computers and the bandwidth of high-speed networks, new real-time multimedia applications are emerging, such as Internet Telephony, Video Conferencing and Virtual Private Networks. These applications have traffic characteristics and performance requirements that are significantly different from existing data-oriented applications. Different applications have different Quality of Service (QoS) requirements such as bandwidth, delay, delay jitter, and packet loss. For example, Video Conferencing applications can tolerate moderate end-to-end delay but require high throughput and very low error rate. On the other hand, Internet Telephony requires very low end-to-end delay but needs moderate throughput and accepts a slightly higher error rate.

To receive the required Quality of Service (QoS) for a given communication, the user must be able to negotiate the relevant QoS parameters with the network before any communication starts. Such negotiations can be achieved using signaling. During signaling the user forwards its traffic and QoS parameters and their associated values to

the network and the network provides details of the guaranteed QoS to the user. The communication starts after the QoS negotiation has been completed successfully.

As networks expand with the increasing deployment of optical technology and with the development of ad hoc wireless networks, the consequence of a failure or multiple-failures becomes more pronounced. If the network is unavailable, even for a brief period of time, users or applications may experience unpredictable performance disruption or service disruption that can cause significant loss. Therefore, network reliability is becoming an important element of QoS requirements [5]. Higher availability of the network services has to be considered during the design of the network to minimize the business interruption and the lost revenue caused by network failures.

Network reliability is defined as the ability of a network to maintain or restore an acceptable level of performance during network failures by applying various network failure recovery techniques [5]. In this thesis, the parameter Q_c is being used to denote the reliability requirement. Q_c is simply defined as the probability criteria that enough resources reserved for this connection are functioning properly. Q_c can also be interpreted as the minimum probability demand required by a connection to be operational at any given instant of time [19].

The key objective of network failure recovery mechanisms is to minimize the disruption to data traffic of any failure. Failures may have many causes – for example, Link Failure, Node Failure, Software Failure, etc. as mentioned in [14]. Upon these

failures, network recovers by sending traffic to another part of the network instead of the failed part of the network. Since node failure can be treated as a multiple-links failure problem and software failure is actually a kind of node failure as mentioned in [17], therefore in this thesis, the emphasis is on the Link Failure model [14]. There are mainly two levels of failure recovery mechanisms – Protection Switching and Rerouting. Protection Switching (PS) is a type of failure recovery method where the backup paths are pre-computed while establishing the working paths upon the arrival of connection requests. While for the Rerouting mechanism, the backup paths are assigned dynamically upon failures. Link and Physical layer Protection Switching is capable of achieving a service restoration time within 50 ms, but the scope of the recovery is limited and has no visibility to higher layer operations. On the other hand, IP Layer Rerouting is slower but does not rely on any specific topology; therefore, IP Layer Rerouting provides a much greater flexibility. The detailed classification of network failure recovery mechanisms is further discussed in [3][11][26][31][32][35].

Since Multi-Protocol Label Switching (MPLS) [33] is implemented between the IP and the Link layers, it is the lowest layer with the knowledge of the entire network topology and MPLS failure recovery mechanisms can provide a trade-off between the repair speed and the deployment cost [18][35]. MPLS superimposes a connection-oriented framework over the connectionless IP network to allow resources to be reserved and allow routes to be pre-determined effectively. The Label Switched Path (LSP) can be set up based on the idea of Constraint-based Routing (CR). Therefore, MPLS network is capable of supporting traffic engineering concepts, such as performance optimization,

and capable of providing a certain QoS level. This feature makes it possible to ensure the network reliability by making the backup resource available for rerouting the traffic upon failures [17].

In MPLS networks, failure recovery can be achieved by allocating backup LSPs through which packets can be re-routed in case of working LSPs failures. The structure of the backup LSP and its peering relationship with the working LSP affects how efficiently the network resources can be utilized and how quickly the packets can be re-routed upon failures. Therefore, the design of the backup LSPs must address both the efficiency in resource utilization and the speed in path restoration. Several MPLS failure recovery mechanisms are proposed including Path Protection, Link Protection, Segmented Protection and MPLS Fast Re-Route (FRR).

MPLS Path Protection mechanisms usually achieve better resource utilization compared with other failure recovery schemes. During the design of MPLS Path Protection, an important issue to be addressed is how to find the working-backup path pair given some QoS constraints such as bandwidth, delay, packet loss or reliability, which leads to the problem of QoS routing. The objective of QoS routing is to find a path or multiple paths from the source node to the destination node which has sufficient resource to support the end-to-end QoS requirements. The recent work in QoS routing has been focused on three main directions: Centralized Routing, Source Routing and Distributed Routing. In the Centralized Routing scheme, network topology information is collected to a centralized server where the routes are calculated for every router. In the

Source Routing scheme, each router maintains an image of the global network state, based on which a routing path is centrally computed at the source. In the Distributed Routing scheme, the path is computed by a distributed computation during which the control messages are exchanged among the nodes and the state information kept at each node is collectively used in order to find a path. All of the three schemes require the global link state information to be updated frequently enough to cope with the dynamics of network parameters, which makes the communication overhead excessively high for large scale networks. Considering that QoS routing is typically done on a per-connection basis in MPLS networks, a distributed source-routing framework whose correctness depends only on the local state information is attracting more attentions in recent works.

In terms of backup resource sharing, the following schemes are proposed – Dedicated Path Protection (DPP) and Shared Path Protection (SPP) [21-22]. Dedicated Path Protection, also called 1+1 protection, is used to allocate a link/node-disjoint backup path with the same resource as the working path. The DPP scheme provides higher reliability and fast restoration speed, but is inefficient in resource utilization because it consumes at least twice the amount of required network resources. On the other hand, resource usage efficiency can be improved by using the Shared Path Protection which allows a new backup path to share the resources allocated to some existing backup paths as long as their working paths are not subject to a single point of failure. The SPP scheme is more efficient in terms of spare resource utilization, but may not be as reliable as the DPP scheme. There exist several studies which focus on mesh-based shared-path protection design – for example, Sharing with Partial routing Information (SPI)

protection [21-22], Sharing with Complete routing Information (SCI) protection [21-22], and SRLG-based Shared Path Protection (SRLG-SPP) [40], etc. These schemes also need an extra link state information to be flooded using some IGP routing protocol such as OSPF/ISIS, thus causing a higher network overhead. The scalability problem exists when those schemes are implemented in large scale networks.

Both the legacy DPP and SPP schemes guarantee 100 percent reliability only against single failure event in the network neglecting the possibility of multiple concurrent failures. In the case when the probability of multiple concurrent failures is high, 100 percent reliability is difficult to be satisfied. Therefore, there is a need for providing differentiated reliability of services (DiR) [1][42] in the same network so that different applications require different reliability degree and differ in how much they are willing to pay for the services they get.

Current rates of fiber cuts and links maintenance operations drive network designers' focus toward multi-failure protection schemes [53]. In reality, some links which go different nodes may be in the same conduit. Therefore, if the conduit is cut, many links fail at the same time. This is the case of multiple-link failure. Fire or earthquakes can also damage a large number of nodes causing multiple-node failure; and each node's failure can be treated as multiple-link failures problem. Moreover, multiple-link/multiple-node failure often happens in mobile ad hoc wireless networks. Unlike fixed infrastructure networks where link failures are comparatively rare events, in mobile networks, the rate of link failure is directly related to node mobility and greater mobility

increases the fluctuations in link quality. Therefore, in an ad hoc wireless network, the rate of link failure due to node mobility is the primary obstacle to routing [54] and the restoration algorithm must be able to handle these multi-failure situations.

1.2 Thesis Objectives and Contributions

Since the QoS routing is typically done on a per-connection basis in MPLS networks, a distributed source-routing framework whose correctness depends only on the local state information is preferred for the current multimedia networks. In a mesh-based network, path protection mechanisms usually lead to better resource utilization compared to other schemes like link protection or segmented protection. Today's research in the shared path protection design is mostly based on the single failure model which, in some cases, can not satisfy the customer's reliability requirements especially in an ad hoc wireless network. To guarantee the customer specific network reliability under multiple failures scenario, the following challenges have to be addressed:

- Design a distributed QoS path selection algorithm which does not require the global link state information for the sharing calculation of backup resource; thus, the communication overhead can be reduced for large scale networks.
- Design a failure recovery mechanism which not only guarantees the customer specific network reliability requirement but is also efficient in terms of network resource utilization.

- Design an efficient backup resource sharing algorithm which works consistently against both single failure and multiple failures.
- The modification to the current signaling mechanisms should be done efficiently in order to support the proposed algorithm.

The above goals are achieved as a result of the following accomplishments which are also the main contributions of this thesis:

- Two “Link Failure Probability” (LFP) based backup resource sharing algorithms are proposed, which are “LFP based First-Fit algorithm” (LFP-FF) and “LFP based Best-Fit algorithm” (LFP-BF). Both the legacy DPP and SPP algorithms are special cases of our proposal.
- A new MPLS Path Protection scheme is introduced using an enhanced Separate Path Selection approach. In this new scheme, the working path is selected to tackle the issue of resource optimization problem while one or multiple backup paths are selected based on the reliability constraint.
- An enhancement to RSVP-TE signaling mechanisms is introduced for best supporting the proposed algorithm. We propose signaling protocol extensions to distribute some of the link usage information (i.e., working path failure probability parameter and SRLG constraint) among network nodes. In this distributed signaling framework, the calculation of backup resource is done on each node along the backup path depending only on the local link state

information such that the network overhead is guaranteed within acceptable bounds.

- The performance evaluations on the proposed algorithm were conducted during the research. Simulation results show that our proposal performs better than the conventional Dedicated Path Protection schemes in terms of Call Acceptance Rate and Total Bandwidth Consumption. The performance studies also prove that this scheme achieves some improved features in comparison with other Shared Path Protection schemes such as protection against multiple failures, SRLG protection and reliability distribution policies etc.
- By performing the mathematical analysis for a simplified network model, some insight into the correctness and efficiency of the proposed algorithm is provided.

1.3 Thesis Organization

The remaining part of this thesis is organized as follows. Chapter II provides a survey on various failure recovery schemes and QoS routing algorithms. Chapter III gives the definition of the problem being tackled and some assumptions related to the proposed scheme. This description is followed by the detailed explanation of the proposed LFP-based algorithm in Chapter IV. An example is also given during the explanation of the algorithm. Two schemes – LFP-FF and LFP-BF are introduced in

Chapter IV. In chapter V, the proposed algorithm is validated through the mathematical analysis and a set of simulations. Lastly, a conclusion is provided to summarize this thesis in Chapter VI.

CHAPTER 2–LITERATURE AND SURVEYS

2.1 Surveys on Network Failure Recovery Mechanisms

2.1.1 Network Layer Protection – Rerouting

In the traditional connectionless IP networks, data traffic on a link subjects to a failure is recovered via Layer 3 (network Layer) rerouting. At the network layer, each node maintains its routing tables using the IGP (Interior Gateway Protocol) protocol (such as OSPF, ISIS, RIP) or the BGP (Border Gateway Protocol) protocol. For example, OSPF (Open Shortest Path First protocol) uses Link State Advertisement (LSA) to maintain the routing topology of the network in a distributed fashion. Routing protocols detect the link/node failures, update the routing topology of the network and re-compute the routing tables. Once all the network routing tables are re-computed and have converged, the paths that were using the failed link are rerouted through other links. Since the timer used by the routing protocols to detect link failure is very coarse, the convergence process is very slow. Another issue is that the routing tables have to be re-computed before paths are switched which consumes a lot of switchover time in large networks.

2.1.2 Link and Physical Layer Protection – Protection Switching

With the emergence of commercially important and delay-sensitive applications and with the development of the photonic infrastructure in the backbone networks, not only the restorability of any service interruption must be guaranteed, but the restoration time needs to be within a specific limit. The Link and Physical Layer Protection mechanisms are induced to tackle the issue of protection speed. One example is the self-healing rings.

The self-healing rings are a kind of counter rotating ring networks where all of the nodes are connected in a closed loop. Dual ring architecture adds redundancy to the system where the second ring transmits in the direction opposite to that of the primary ring. Traffic is sent from a source to a destination in one direction only. If a link fails, the other direction is used to reach the destination such that the failed link is avoided. Several Link and Physical Layer failure recovery mechanisms are based on this counter rotating ring topology, for example, SONET UPSR [49] and BLSR [48] Automatic Protection Switching (APS) [45], FDDI protection switching [46], and RPR Intelligent Protection Switching [47].

SONET is a physical layer technology for optical transmission. In SONET, protection with self-healing rings is called “Automatic Protection Switching” (APS [45]). Some studies are based on APS mechanism [12][13][41] which can be further classified into two architectures – UPSR and BLSR.

Figure 1: SONET Two-fiber UPSR Automatic Protection Switching

Figure 2: SONET Two-fiber BLSR Automatic Protection Switching

Unidirectional Path-Switched Ring architecture (UPSR) is actually a 1+1 protection as shown in Figure 1. In UPSR, traffic is transmitted simultaneously over both the working line and the protection line. If there is a failure, the receiver switches to the protection line and takes up the connection. The advantages of UPSR are its low switchover time and low service interruption time allowing it to meet the 50ms goal which is the largest disruption time for voice traffic that can be managed by the human

brain before the jitter effect becomes noticeable. A major disadvantage of the UPSR, however, is the requirement for a large amount of dedicated backup resource since half of the available resource is required to provide full redundancy. Bi-directional Link-Switched Ring architecture (BLSR), achieves 1:1 (one-to-one) protection as shown in Figure 2. In BLSR, every link can carry both regular traffic and backup traffic at the same time and thus, it does not require dedicated backup links. Upon a link failure, the node upstream of the failed link wraps traffic from one ring to another ring in the reverse direction so that traffic still can reach its destination. BLSR is as fast as UPSR and does not waste as many resources.

Fiber Distributed Data Interface (FDDI [46]) is a set of ANSI and ISO standards for data transmission on optical lines in a local area network. The FDDI protocol is based on the SONET BLSR techniques which implements a protection mechanism at the MAC layer. FDDI runs over dual counter rotating rings: one ring is the primary ring and the other ring is for possible backup in case the primary ring fails.

Resilient Packet Ring (RPR) [47] is a more recent MAC protection protocol designed to run on multiple counter-rotating rings. In RPR, the path protection mechanism is called Intelligent Protection Switching (IPS) [47]. IPS can be viewed as an enhanced SONET BLSR mechanism.

The lower layer failure recovery mechanisms are the fastest because the nodes that detect the failure perform the switchover immediately without the notification step.

The recovery time is thus decreased only to the detection time; however, the scope of lower layer recovery is limited and has no visibility to higher layer operations.

2.1.3 MPLS Failure Recovery Mechanisms

MPLS failure recovery mechanism can provide a trade-off between the repair speed and the deployment cost. In MPLS networks, failure recovery can be achieved by allocating backup LSPs through which packets can be routed in case of working LSP failures. The structure of the backup LSP and its peering relationship with the working LSP affects how quickly the packet can be routed through the backup path. Bandwidth efficiency and path restoration speed are two issues to be addressed during the design of the failure recovery mechanisms such as Path Protection, Link Protection, Segmented Protection and MPLS Fast Reroute (FRR), etc.

2.1.3.1 Path Protection

In the Path Protection (or Global Repair) method, an ingress node is responsible for path restoration when the Failure Indication Signal (FIS) arrives. This scheme requires an alternative backup path for each working path. The first router of the backup path is called PSL (Path Switching LSR), and the last router of the backup path is called PML (Path Merging LSR). Path Protection usually achieves better network resource utilization than other schemes like Link Protection or Segmented Protection. Another advantage of Path Protection method is that it is simple to implement because only one

backup path per working path is required and only one LSR (the Ingress LSR) has to be provided with PSL/PML functions (as shown in Figure 3). On the other hand, this method has a high cost, in terms of time, as the FIS is sent to the ingress node. There also exist higher packet losses during the switchover time.

Figure 3: MPLS Path Protection

2.1.3.2 Link Protection

Figure 4: MPLS Link Protection

In the Link Protection (or Local Repair) method, restoration begins at a point much closer to the failure as shown in Figure 4. The Link Protection method offers a

faster restoration time than the Path Protection method, and the packet loss is significantly reduced. On the other hand, every LSR requiring protection has to be provided with a PSL function as well as a PML function. Another drawback is the low resource utilization and increased complexity because different backup path has to be set up for each protected domain. An intermediate solution establishes local backups only for segments with high reliability requirements [7].

2.1.3.3 Segmented Protection

Figure 5: MPLS Segmented Protection

Several segmented protection approaches have been proposed in [15][17][34][36][44]. The main idea of Segmented Protection is to sub-divide a working path into several overlapped segments when the working path is allocated as shown in Figure 5. Each of the segments forms a protection domain and each protection domain has a PSL and a PML, which switches over and merges back to the affected traffic during a failure, respectively. Compared with the global repair method, the restoration time of Segmented Protection can be guaranteed by adjusting the size of the Protection domain

along a working path and the computational complexity of protection paths is simplified. Compared with Link Protection method, Segmented Protection provides the flexibility and the capacity efficiency to yield protection services adaptive to the requirements.

2.1.3.4 Fast Reroute

Several methods have been proposed to fast-reroute (FRR) mechanism in MPLS as in [16][28]. Haskin first proposed the fastest MPLS rerouting mechanism called “MPLS Fast Reroute” [16]. In [28], some slower but less complex mechanisms were introduced.

Figure 6: MPLS Protection - Fast Reroute

The main idea behind the Fast Reroute approach is to reverse traffic at the point of the failure back to the ingress node of the protected LSP and to redirect it via a pre-configured backup LSP. As shown in Figure 6, if link (m,n) fails, the router m , which is the upstream node of link (m,n) , would detect the failure and redirect the packets back to the Ingress router. When the first packet arrives at the PSL, the PSL would know that a

failure has occurred and would subsequently forward (retransmit) the packets on the backup path. MPLS Fast Reroute ensures that no packet is lost after node m detects the failure. The switchover step is instantaneous, as the PSL only needs to start forwarding the packets coming from the Ingress LSR going to the Egress LSR on the backup path instead of the working path. A disadvantage of MPLS Fast Reroute is that some packets may go through a longer distance between the ingress and the egress router during the switchover time. The major advantage of MPLS Fast Reroute is that the recovery is fast and no packet is lost after the failure has been detected.

2.2 Surveys on QoS Routing

2.2.1 QoS Routing Algorithms

Finding the QoS paths that satisfy one or multiple QoS constraints consists of two fundamental tasks [39]: distributing the network state information and computing the paths with the collected network state information. Several QoS routing algorithms based on different combinations of bandwidth, delay, and hop-count were proposed in [25]. Some researchers also addressed the QoS routing issues in the context of bandwidth and delay parameters showing that the feasibility problem under this combination is not NP-complete.

For traffic with only bandwidth guarantees, a natural way to optimize the resource utilization is to select a path with fewer hops. Several routing algorithms that assign

different weight on limiting hop count and balancing the network load have also been proposed in the literature. These suggestions include the widest-shortest path, the shortest-widest path, and the shortest-distance path, etc. The widest-shortest path is a path with the minimum hop count among all feasible paths. If there are several such paths, the one with the maximum reserved bandwidth would be selected. The shortest-widest path, however, is a path with the maximum bandwidth among all the feasible paths. If there are several such paths, the one with the minimum hop count would be selected. The shortest-distance path selects a feasible path based on the shortest distance. In this thesis, the proposed LFP-based backup resource allocation algorithm works well using any of the three bandwidth-guaranteed path selection schemes.

2.2.2 Joint Path Selection vs. Separate Path Selection

In MPLS Path Protection, an important issue which needs to be addressed is how to find a backup path for a working path. Two different approaches exist – Joined Path Selection (JPS) and Separate Path Selection (SPS). The Joined Path Selection method calculates two link/node-disjoint paths at the same time using some specific algorithm. While the Separate Path Selection finds a pair of paths by first calculating the working path, and subsequently calculating the backup path in the same graph, but with the links/nodes of the working path removed from the graph.

Several Joined Path Protection schemes guaranteeing the bandwidth requirement are proposed in the literature. For example in [16], the author proposes a bandwidth

guaranteed dynamic routing algorithm. Another approach mentioned by M. Sridharan [36] for QoS routing is to exploit the dependencies between the QoS parameters and to solve the path selection problem assuming that the specific scheduling schemes are being used at network routers. Other recent scheme, such as MIRR (Minimum-Interference Restorable Routing) [20], develops more complex and effective routing methods. The main objective of MIRR is to offer a protection routing method which maximizes the resource consumption and minimizes the path request rejection ratio.

Joint Path Selection (JPS) is usually implemented to tackle the issue of resource optimization or other single performance metric under single failure scenario, which may guarantee the 100 percent reliability requirement. While considering the joint constraints of resource optimization and network reliability, the Separate Path Selection (SPS) is preferred where two paths are selected based on different constraints – the working path is calculated to be the most resource efficient and the backup path is selected to meet the network reliability requirement. Considering the backup resources are sharable, both the resource optimization and reliability constraints can be satisfied using this enhanced SPS approach.

The conventional SPS link-disjoint path pair algorithm is describe as the following: for a given pair of nodes in the graph $G=(V,E)$, the algorithm finds a pair of paths by first calculating the working path (the optimized path meeting some QoS requirements) and subsequently calculating the backup path (the optimized disjoint path)

in the same graph, but with the links of the first optimized path removed from the graph as shown in Figure 7.

Assuming node A is the source and node Z is the destination, the shortest path is $(ABCDZ)$ and its length is 4 as shown in Figure 7(a). Deleting the links of the shortest path yields the graph in Figure 7(b). The shortest path obtained between node A and Z in this graph is $(AEBFZ)$ of length 8. Thus the link-disjoint pair determined from this algorithm is $(ABCDZ, AEBFZ)$ of length equals to $4+8=12$.

Figure 7: Separate Path Selection Link-disjoint Pair Algorithm

Using the conventional SPS approach, in some cases, the working path may block all the possible global backup paths as shown in Figure 8. Figure 8(a) shows that using the conventional SPS approach, after selecting the working path $(ABCD)$, the link-disjoint backup path is not available. But by jointly selecting the working path and the backup path, the path pair – “ $(AFCE), (ABGD)$ ” can be found as shown in Figure 8(b). In

[21], the author discussed several other algorithms regarding the Joint Path Selection scheme.

Figure 8: Disadvantage of SPS Link-disjoint Pair Algorithm

Different from traditional SPS approaches, the proposed scheme selects a working path based on the resource optimization constraint while one or multiple backup paths are selected to meet the reliability constraint. In addition, since some working path properties (with respect to the failure probabilities, the SRLG constraint, etc.) have to be considered in order to select the backup path with the optimum protection requirements, the enhanced Separate Path Selection approach is best suited for the proposed algorithm.

2.3 Backup Resource Allocation Algorithms

Unlike best effort networks, MPLS QoS networks must make sure that the network is properly dimensioned and that enough communication resources are provided

in order to maintain the negotiated QoS requirement. It may be required to reserve some resources prior to the connection request and release them after the connection ends. The most important network resources that can be reserved are buffer space and link bandwidth. Adequate bandwidth reservation allows maintaining the delay and the jitter constraints during critical calls. Some special schemes such as the resource reservation protocol (RSVP) have been proposed where resources are reserved a priori along the message transmission path from the source to the destination for the duration of a session.

The process of reserving backup link resources is also called the Backup Resources Allocation which can be further classified as link-oriented and path-oriented. A link-oriented method focuses on allocating enough resources for protecting each individual link [17] such as Node Cover, Ring Cover and P-cycle; whereas a path-oriented method uses the end-to-end detouring scheme [18]. Considering the end-to-end path-oriented protection schemes, failure resilience can be achieved by using a link/node disjoint pair of Working Path (WP) and Backup Path (BP) from a source node to a destination node. There are mainly two kinds of protection schemes with regard to the path-oriented allocation of backup resources – Dedicated Path Protection (DPP) and Shared Path Protection (SPP). Dedicated Path Protection, also called 1+1 protection, is used to allocate a link/node-disjoint backup path with the same bandwidth as the working path. The DPP scheme provides higher reliability and fast restoration speed, but is resources inefficient because it consumes at least twice the amount of required network resources. On the other hand, resources usage efficiency can be improved by using the Shared Path Protection which allows a new backup path to share the resources allocated

to some existing backup paths as long as their working paths are not subject to a single point of failure. The SPP scheme is more efficient in terms of spare capacity utilization, but may not be as reliable as the DPP scheme. There exists numerous studies focused on mesh-based shared-path protection design [6][21][22][27][43][40]. In [27], an algorithm is developed to dynamically find a link-disjoint working-backup path pair for each connection request with specified failure restoration guarantees. The Separate Path Selection approach is used to find the link-disjoint backup paths. Since the SPS approach cannot guarantee 100 percent success in path selection, in [5], a k-shortest path-ranking algorithm is applied to search for all the possibility of allocating the working-backup path-pair; however, the blocking probability constraint cannot be satisfied. In some other papers [21-22], the bandwidth efficiency is further improved using two similar dynamic survivable routing schemes, called Sharing with Partial routing Information (SPI) and Sharing with Complete routing Information (SCI), which are based on the shortest path first algorithm in finding the protection paths to achieve an approximation of the optimal spare capacity allocation. In the SPI scheme, at the time of routing, the source node has the information of (1) the aggregate bandwidth used on each link by the working paths; (2) the aggregate bandwidth used on each link by the backup paths; and (3) the available bandwidth of each link. With this information, some sharing of the backup paths is possible, but extra link state updates are required to be flooded using some IGP routing protocol such as OSPF/ISIS. In SCI scheme, at the time of routing, the source node has complete information: it knows the routes for the working paths and backup paths of all the connections currently in the network. This is too much information to be flooded for SCI and SPI in large scale networks. In [43], an Integer Linear Programming (ILP)

formulation is presented for both the SCI and SPI schemes. In [23], the author develops an analytical model for GMPLS-based recovery in $M:N$ protection groups using both the recovery time and the recovery failure probability. In [10], the author proposes a survivable routing scheme that can explore a pool based backup sharing to dynamically find the least-cost backup path for a given working path. Recently, the authors in [40] propose a new scheme called SRLG-based Shared Path Protection (SRLG-SPP). In SRLG-SPP, unlike SPP, an SRLG constraint is imposed, which means if two working paths are using at least one common link, their backup paths would not share any link. But in [40], the authors only give a centralized implementation for this algorithm. In this thesis, the proposed LFP-based algorithm implements the SRLG-SPP concept using a distributed method to obtain a better performance of resource utilization.

2.4 Failure Recovery in Multiple Failures Model

Both the legacy DPP and SPP schemes guarantee 100 percent reliability only against single failure event in the network [38]. When the single failure assumption is not acceptable in the case where some failures affect the working path of a connection and some other failures affect the backup path of the same connection, neither DPP nor SPP can satisfy the reliability requirements. In addition, the SPP scheme also fails if two or more failures affect some distinct working paths whose corresponding backup paths share some protection resource [38]. In this case, multiple failures can be tolerated only if the backup paths do not interfere [38]. Since multiple concurrent failures are very possible especially in ad hoc wireless networks due to node mobility, several papers have

studied the issues of protection against multiple failures [9][38][42]. For example, Fumagalli and Unghvary introduced the Maximum Downtime Ratio [38] which must be satisfied regardless of the network topology and location of the source and the destination.

To guarantee network reliability when taking into consideration multiple failures, one approach is to introduce the concept of Differentiated Reliability (DiR) [1][7][42] to provide multiple degrees of reliability in protection schemes that provision spare resources. Connections across the network may require different reliability degrees. For example, for some critical and higher-priority applications that require higher reliability, a backup path is crucial to meet the requirements. On the other hand, some non-critical applications may not need a backup path because their reliability constraints are not so stringent. Traffic classes, such as Diffserv classes (EF, AF, BE), can be described based on the QoS and protection parameters. Using MPLS-based recovery with its strong functionality in traffic engineering and service differentiation, network resources could be managed such that the connections with a high-quality restoration requirement are allocated with fast and prioritized restoration services, while the connections with lower restoration requirements are equipped with slower restoration services. During the design and implementation stages of this research, the Differentiated Reliability (DiR) concept is used so that each traffic class is assigned with a unique reliability requirement to further improve the bandwidth efficiency.

2.5 Probability-based Approach for Network Reliability

To address the problem of guaranteeing reliability requirement under multiple failures scenario, an efficient approach is to tackle the issue of the link (path) failure probability. There are several probability-based routing schemes discussed in [8][30][50].

In [30], three different policies are proposed concerning the end-to-end reliability constraint distribution across multiple ISP networks – the least-effort policy, the most-effort policy and the equal-distribution policy. The least-effort policy is to allow each network to determine its level of responsibility for the reliability constraint independently. For example, given a network in Figure 9, a request arrives at *ISP A* requesting for a connection between *s* and *d* with a minimum service reliability of 99%. *ISP A* grants the 99.4% path despite two other paths with higher availability. *ISP A* then forwards the provisioning request to *ISP B* with the reliability constraint being modified to $\frac{99}{99.4} = 99.6\%$. *ISP B* selects the 99.9% path to satisfy this constraint and subsequently forwards the request to *ISP C* with the remaining availability constraint equals to $\frac{99.6}{99.9} = 99.7\%$. *ISP C* could select the 99.9% path (with the closest availability to meet the constraint) for the available constraint 99.7%. However, such decision may cause unnecessary demand rejections. The most-effort policy is to force each network to accept the highest available level of responsibility. This policy would make *ISP A* to

choose the 99.99% path, *ISP B* to choose the 99.1% path and *ISP C* to choose any path that meets the constraint. This policy is capable of accepting most of the requests, but it is highly inefficient. A more practical solution is the equal-distribution policy where the level of responsibility is allocated equally among the ISPs along the path. This method sets a limit on the least-effort policy while keeping the resource usage in each ISP at a reasonable level. For example, the equal threshold for *ISP A*, *B*, *C* becomes $\sqrt[3]{99\%} = 99.67\%$. Each of the IPS is able to grant the best fit path concurrently which is 99.99%.

Figure 9: End-to-end Reliability Constraint Distribution

The above-mentioned approaches are proposed for inter-domain applications only. Given the customer specific reliability criteria, it is possible to satisfy this QoS constraint by distributing this reliability constraint to each link along the working path and the backup path within a domain so that when each link satisfies its own link failure requirement, the overall connection's reliability can be satisfied. This is also one of the

main issues addressed in this thesis. The detailed algorithm is described in the next chapter.

In [50], the author proposes a distributed scheme for establishing reliability-constrained least-cost paths by choosing the reliability of the path to satisfy the level of fault-tolerance required by the connection request. However, since the occurrence of link/node failure is extremely rare, selecting paths based on the reliability constraint may not lead to bandwidth efficient solutions compared to the traditional bandwidth-optimization methods. As an improvement over the scheme in [50], the proposed LFP based scheme in this thesis uses the traditional Separate Path Selection approach for selecting a working path and a backup path. Nevertheless, different from other schemes using the SPS approach, the proposed scheme selects a resource-constrained working path and a reliability-constrained backup path so that both the reliability and resource optimization criteria can be satisfied. Furthermore, to allow a better usage of the resources, we allow multiple connections sharing the same backup resource under the condition that reliability requirements are satisfied.

In [8], an analysis of the effect of link failure probability with respect to the selection of failure recovery mechanisms is presented. The author proposes a new scheme to develop and to evaluate protection strategies considering both the Failure Sensibility Degree (failure probability) and the Failure Impact Degree (packet loss and recovery time). Since each path has its own unique link failure probability and a unique sequence of links to cross, by assigning a binary value – Link Protection Requirements,

to each link, thus it is possible to know whenever a link should be protected and it is possible to define different failure recovery strategies. This scheme gives an approximation of the reliability constraints and a higher protection levels can be achieved. However this scheme only gives a coarse assignment of protection strategies. The quantitative analysis of the relationship between the Link Failure Probability and the allocated backup resources is not further discussed. Since the knowledge of each link's LFP value is very important for selecting the paths to satisfy the reliability constraint, in this thesis, a theoretical analysis of the relationship between the LFP and the allocated backup resources is one of the goals targeted by the proposed algorithm.

2.6 Research Summary

The focus of this research is on the issue of shared backup resource optimization under multiple failures scenario to guarantee the customer specific reliability criteria. Moreover, it is also of interest to work out a new path selection algorithm which computes the backup bandwidth by analyzing the effects of each link's LFP value along both the working path and the backup path. Compared to other Shared Path Protection schemes, this approach should achieve the following advantages: Firstly, this algorithm should work consistently under both single and multiple failures scenarios. Secondly, this approach does not require the global link state information for the calculation of backup resource and thus can be implemented in a distributed manner. Thirdly, the proposed algorithm is not only bandwidth efficient but also satisfies the reliability requirements.

CHAPTER 3–PROBLEM STATEMENT

3.1 Definitions

The **Link Failure Probability** (LFP) – $P_{i,j}^L$ is defined as the probability of link (i,j) fails. These values are usually very small – for example, less than 0.01%. In a real network, several technologies coexist such as different physical layers and different type of nodes. The actual failure probability of an element in the network is significantly different from any of the others. Although it is impossible in practice to determine which particular segment in a network will fail, the probability of failure can be calculated by applying prediction techniques based fault statistics. The mechanisms and methods for computing all the failure probabilities in a network are beyond the scope of this work. In this thesis, we assume that knowledge of these probabilities is already known or readily available. Moreover, although their values may vary in time, this information is assumed to be stable in this thesis and the LFP value is assumed to be statistically independent of each other.

The **Path Failure Probability** – P_c^{Path} is defined as the probability of any single link or a combination of the links along the path $(P_{c=(s,d,x)}^{Path} = \{(s = e_0, e_1), (e_1, e_2), \dots, (e_{z-1}, d = e_z)\}, (e_{i-1}, e_i) \in E)$ fails. In this thesis, the

failure of a path is assumed to be only affected by a link breakdown (e.g., due to inadvertent fiber cable cut). Since node failure can be considered as a special case of multiple link failures [17], the proposed algorithm can be also applied to any node failure models which could be the future research direction.

The **Residual Reliability** - Q_c^{BP} is defined as the remaining reliability demand for the selection of backup paths after a working path is determined. Assuming a working path is already selected with the failure probability of $P_c^{WP} = 1 - R_c^{WP}$ and the overall connection reliability demand is Q_c , the residual reliability Q_c^{BP} can be calculated as:

$$Q_c^{BP} = Q_c / (1 - P_c^{WP}) = Q_c / R_c^{WP}.$$

A **Connection** is defined as a combination of a working path and one or multiple backup paths if the backup paths are required to satisfy the reliability requirement. The implementation of the proposed algorithm requires a consistent connection ID assignment. A possible solution is to provide a globally unique connection *ID* using a 3-tuple consisting of the source node s , the destination node d and the connection identifier x to identify each individual connection.

An operational connection may refer to a single working path or may consist of both a working path and one or multiple backup paths. In the case that a connection consists of one working path and one backup path, the **Connection Reliability** R_c^{Conn} is

defined as the probability that either the working path or the backup path or both paths remain operational.

Figure 10: Illustration of the Service and the Reserved Bandwidth Allocation

As illustrated in Figure 10, the bandwidth capacity on link (i,j) can be divided into three parts: the total service bandwidth denoted by SB_{ij} , the total reserved bandwidth denoted by RB_{ij} , and the total available bandwidth denoted by AB_{ij} . The service bandwidth is allocated for different working paths with each allocated working path's bandwidth equals to its bandwidth demand. The total reserved bandwidth can be dynamically divided into multiple parts called **Reserved Bandwidth Blocks (RBBs)** so that the allocated bandwidth on each of the RBBs can be shared by multiple connections as their backup resource as long as the reliability constraints are satisfied.

The allocated reserved bandwidth in the k^{th} RBB of link (i,j) is denoted by $RB_{i,j}^k$.

The total reserved bandwidth on link (i,j) is obtained from the sum of each individual reserved bandwidth as defined in Equation 1 where K is the total number of RBBs on link (i,j) .

$$RB_{i,j} = \sum_{k=1}^K RB_{i,j}^k \quad \text{_____} (1)$$

Two different Reserved Bandwidth Blocks management algorithms are proposed in this study – the First Fit algorithm and the Best Fit algorithm which are explained in next chapter.

The ***Shared Risk Link Group (SRLG)*** constraint defines the availability of the protection resources to a working path, which requires that any two working paths sharing the same risk of failure cannot share the same protection resource. Paths that have a common link are said to be in the same SRLG group. In other words, two paths are said to be SRLG-diverse if no link on one path has a common risk with any link on the other path. When two connections are in the same SRLG group because their working paths interfere at some common link and when their corresponding backup paths use some other common link as their backup link, they can not share the same RBB thus different sharing block has to be assigned. Consequently, the SRLG constraint can be denoted by an array of connections whose working paths share some common link risk.

Figure 11: Illustration of Two Connections within the Same SRLG

An example of the SRLG constraint connections is shown in Figure 11 where two connection requests are being set up. The working paths $(ABCD)$ and $(EBCI)$ share the link (B,C) ; therefore, connection c_1 and connection c_2 are in the same *SRLG* group and this *SRLG* constraint will prevent them from sharing the same RBB under the same link – link (F,G) and link (G,H) .

During the request signaling stage of the backup path, it is necessary for the source node to have the knowledge of the working paths within the same *SRLG* group. To achieve this, the signaling procedure must be modified and the extra *SRLG* constraint information must be recorded along the working path when the working path is being set up. The advantage of this signaling approach is that the source node obtains the *SRLG* constraint information through signaling, thus the global link state update of *SRLG* constraint is not required and the load of the network can be significantly reduced. The

distributed feature of this approach is also the main difference from the centralized SRLG-routing algorithm first mentioned by Y. Wang [40].

3.2 Related Equations

Some theorems and equations related to the proposed algorithm are provided and proven as follows:

Theorem 1: The path failure probability can be calculated using Equation 2, where $P_{i,j}^L$ is the Link Failure Probability of each link (i,j) along the path – $Path_c$ ($P_{c=(s,d,x)}^{Path} = \{(s = e_0, e_1), (e_1, e_2), \dots, (e_{z-1}, d = e_z)\}, (e_{i-1}, e_i) \in E$).

$$P_c^{Path} = 1 - \prod_{(i,j) \in E, (i,j) \in Path_c} (1 - P_{i,j}^L) \quad \text{_____} (2)$$

Accordingly, the working path failure probability P_c^{WP} and the backup path failure probability P_c^{BP} can be calculated using Equation 3 and Equation 4:

$$P_c^{WP} = 1 - \prod_{(i,j) \in E, (i,j) \in WP_c} (1 - P_{i,j}^L) \quad \text{_____} (3)$$

$$P_c^{BP} = 1 - \prod_{(i,j) \in E, (i,j) \in BP_c} (1 - P_{i,j}^L) \quad \text{_____} (4)$$

Proof: Since the path failure probability can be expressed as the complement of the probability that all the links involved work fine, or the complement of the reliability

probability R_c^{Path} of the path, and since the path reliability – R_c^{Path} can be calculated by the multiplicative of each link's reliability – $R_{i,j}^L$ along this path, we have:

$$\begin{aligned}
P_c^{Path} &= 1 - R_c^{Path} \\
&= 1 - \prod_{(i,j) \in E, (i,j) \in Path_c} R_{i,j}^L \quad (\text{Since the reliability constraint is multiplicative}) \\
&= 1 - \prod_{(i,j) \in E, (i,j) \in Path_c} (1 - P_{i,j}^L) \quad (\text{Since each link's reliability and link failure probability are inversely related, i.e. } R_{i,j}^L = 1 - P_{i,j}^L)
\end{aligned}$$

■

Theorem 2: If a connection consists of one working path (denoted by WP) and one backup path (denoted by BP), the connection reliability constraint Q_c should be satisfied by Equation 5 for the connection being operational, where P_c^{WP} is the working path failure probability and P_c^{BP} is the backup path failure probability.

$$R_c^{Conn} = 1 - P_c^{Conn} = 1 - P_c^{WP} \times P_c^{BP} \geq Q_c \quad \text{_____} (5)$$

Proof: Since the connection reliability R_c^{Conn} is defined as the probability that either the working path or the backup path or both the working path and the backup path remain operational. It is inversely correlated to its failure probability – the probability that both the working path and the backup path fail, i.e., $P_c^{Conn} = P_c^{WP} \times P_c^{BP}$. Thus

$$R_c^{Conn} = 1 - P_c^{Conn} = 1 - P_c^{WP} \times P_c^{BP}$$

Since the reliability constraint Q_c is the minimum probability requirement that the connection remains operational, we have

$$Q_c \leq R_c^{Conn} = 1 - P_c^{WP} \times P_c^{BP}$$

■

Theorem 3: The Backup Path Failure Probability Requirement (or the complement of the residual reliability requirement) is calculated by:

$$\beta_c^{BP} = (1 - Q_c) / P_c^{WP} = 1 - Q_c^{BP} \quad \text{_____ (6)}$$

Proof: From Equation 5: $Q_c \leq 1 - P_c^{WP} \times P_c^{BP}$. For the reliability constraint Q_c to be satisfied, the backup path failure probability P_c^{BP} should satisfy the following constraint $P_c^{BP} \leq (1 - Q_c) / P_c^{WP}$. Since the Backup Path Failure Probability Constraint β_c^{BP} is defined as the maximum failure probability requirement for the backup path keeps operational. Thus

$$\beta_c^{BP} = \max(P_c^{BP}) = (1 - Q_c) / P_c^{WP}$$

■

Theorem 4: Given the number of hops H_c of the backup path, the Backup Link Constraint (assuming Equal-Distribution policy is being used) is calculated by:

$$\beta_c^L = 1 - (1 - \beta_c^{BP})^{1/H_c} = 1 - (Q_c^{BP})^{1/H_c} \quad \text{_____ (7)}$$

Proof: Since the Equal-Distribution policy discussed in [30] is being used for the residual reliability constraint distribution along the backup path and since the reliability

constraint is multiplicative, given the length H_c of the backup path, the $(H_c)^{th}$ root of the reliability constraint is assigned to each node as its reliability threshold. Thus each link's reliability constraint is calculated by $Q_c^L = (Q_c^{BP})^{1/H_c}$, where Q_c^{BP} is the residual reliability requirement for the backup path which can be expressed by $Q_c^{BP} = 1 - \beta_c^{BP}$. Therefore each link's failure probability constraint can be calculated by:

$$\beta_c^L = 1 - Q_c^L = 1 - (Q_c^{BP})^{1/H_c} = 1 - (1 - \beta_c^{BP})^{1/H_c}$$

■

Theorem 5: Assuming $T_{i,j}^n$ is the set of connections which use link (i,j) as their backup link and which are sharing the same RBB (RBB #n) with allocated bandwidth capacity denoted by $RB_{i,j}^n$, the set of Backup Link constraints shown as in Equation 8 should be satisfied for any connection $c_k \in T_{i,j}^n$, so that the overall reliability requirement Q_{c_k} could be satisfied.

$$1 - (1 - P_{i,j}^L) * \prod_{\forall c_m \in T_{i,j}^n, m \neq k} (1 - P_{c_m}^{WP}) \leq \beta_{c_k}^L, \forall c_k \in T_{i,j}^n \quad \text{_____} (8)$$

Equation 8 can also be expressed as a matrix of K equations as shown in Equation 9, where K is the total number of connections in the set $T_{i,j}^n$.

$$\left\{ \begin{array}{l} 1 - (1 - P_{i,j}^L) * \prod_{\forall c_m \in T_{i,j}^n, m \neq 1} (1 - P_{c_m}^{WP}) \leq \beta_{c_1}^L \\ 1 - (1 - P_{i,j}^L) * \prod_{\forall c_m \in T_{i,j}^n, m \neq 2} (1 - P_{c_m}^{WP}) \leq \beta_{c_2}^L \\ \dots \\ 1 - (1 - P_{i,j}^L) * \prod_{\forall c_m \in T_{i,j}^n, m \neq K} (1 - P_{c_m}^{WP}) \leq \beta_{c_K}^L \end{array} \right. \quad (9)$$

Proof: For any connection $c_k \in T_{i,j}^n$, to satisfy the requirement that enough resource on the n^{th} RBB is available to recover this connection's working path's failure, the following two conditions have to be satisfied:

Condition A_1 : The link (i,j) is operational;

Condition A_2 : None of the other connections except for c_k in set $T_{i,j}^n$ are occupying the resource of this RBB – i.e., all of the other connections' working paths work fine.

Satisfying the Backup Link Failure Constraint (β_c^L) means that the probability of either of the above two conditions failure should never exceed the constraint β_c^L , i.e.,

$$P(\overline{A_1} \cup \overline{A_2}) \leq \beta_c^L \quad (10)$$

$$\begin{aligned} \text{Since } P(\overline{A_1} \cup \overline{A_2}) &= P(\overline{A_1 \cap A_2}) \quad (\text{according to de Morgan's laws}) \\ &= 1 - P(A_1 \cap A_2) \\ &= 1 - P(A_1)P(A_2) \quad (\text{Since the link failures are independent}) \\ &= 1 - [1 - P(\overline{A_1})] * [P(A_2)] \end{aligned} \quad (11)$$

$P(\overline{A_1})$ is the link failure probability, i.e. $P_{i,j}^L$, and $P(A_2)$ is the probability that all other connections' working path works fine. Thus

$$P(\overline{A_1}) = P_{i,j}^L \quad \text{_____} \quad (12)$$

$$P(A_2) = \prod_{\forall c_m \in T_{i,j}^n, m \neq k} (1 - P_{c_m}^{WP}) \quad \text{_____} \quad (13)$$

From Equation (10), (11), (12), and (13), we have

$$1 - (1 - P_{i,j}^L) * \prod_{\forall c_m \in T_{i,j}^n, m \neq k} (1 - P_{c_m}^{WP}) \leq \beta_{c_k}^L, \forall c_k \in T_{i,j}^n$$

■

Corollary 1: For the n^{th} RBB on link (i,j) , the following bandwidth constraint must be satisfied for the connection being operational.

$$RB_{i,j}^n + AB_{i,j} \geq B_c, \forall n = \{1, 2, \dots, N\} \text{ (N is the total number of RBBs)} \quad \text{—} \quad (14)$$

The left side of Equation 14, $RB_{i,j}^n + AB_{i,j}$, is the maximum available bandwidth capacity to be allocated for the new connection request when checking the n_{th} RBB on link (i,j) . Its value should be greater than or equal to the bandwidth requirement B_c .

■

3.3 Some Assumptions

In this thesis, it is assumed that the connection requests arrive sequentially. Each connection request has the following parameters: a source node s , a destination node d , a bandwidth demand B_c and a reliability demand Q_c . The objective of the routing

algorithm is to compute a working path and one or multiple backup paths for each request. If the available network resource (in terms of bandwidth) is not sufficient to set up either the working path or the backup paths or if the reliability demand can not be satisfied, then the connection request would be rejected. It is also assumed in this thesis that each link's LFP value is known or is readily available either through network measurement or other methods and they are independent of each other. The scenario being considered in this thesis consists of a network of N nodes and M links with restorable connection requests arriving at each node randomly. All the links are duplex and the explicit routes for both the working and backup paths are computed at the source node. The actual path setup is done using the RSVP-TE signaling mechanism in a MPLS network.

Since finding the optimized path between a given pair of nodes in a graph $G=(V,E)$ is the first and foremost step of the disjoint path problem, Dijkstra algorithm is being used during the research. Its efficiency is proven to be $O(|V|^2)$. Other options also exist such as the Fort-Bellmann algorithm, the Modified Dijkstra algorithms and the breadth-first-search algorithm which can also be applied to the proposed algorithm.

As a restorable connection request arrives at a source node, the source node begins to search for an optimized path to the destination as the working path. After a working path is selected, the reliability constraint is checked. If the reliability constraint can not be satisfied using the working path alone, one or multiple backup paths become mandatory. There are two approaches for finding the backup paths. The first approach is

that the source node would subsequently search for a second link-disjoint optimized path to the destination as the backup path. If the joint reliability of the backup path and the working path still can not satisfy the reliability constraint, a second backup path would be selected. This process should continue until the reliability constraint is satisfied or the connection request is rejected due to the lack of resources. A second approach is that only one backup path is selected according to the reliability constraint. If no single backup path exists in the network to satisfy the reliability constraint, then the connection request is rejected. The first option shows a higher chance to meet the reliability constraint, but the implementation is more complex. Without loss of generality, it is assumed that one backup path is enough in the following discussions.

The goal of this research is to answer the following two questions regarding the backup bandwidth allocation:

- How much bandwidth should be allocated for each backup link considering the Link Failure Probability?
- What kind of information is required and must be collected to perform accurately and concisely the request signaling and the bandwidth allocation?

The objective of this thesis is to develop an algorithm for allocating the backup link bandwidth such that both the bandwidth constraint and the reliability constraint are satisfied. The algorithm is explained in detail in the following chapters. Two LFP-based algorithms are proposed which are LFP based First-Fit backup resource sharing (LFP-FF)

and LFP based Best Fit backup resource sharing (LFP-BF). LFP-BF is an improvement of LFP-FF regarding the detail process of the RBBs management. Both LFP-FF and LFP-BF are based on the Shared Path Protection scheme with the analysis of the Link Failure Probability. The generic no sharing scheme used in this thesis for the performance comparison actually implements a Dedicated Path Protection.

CHAPTER 4–LFP BASED BACKUP RESOURCE ALLOCATION ALGORITHM

4.1 General

The LFP-based backup resource allocation algorithm is implemented as follows:

When a restorable connection request c arrives with the following parameters (the source s , the destination d , the bandwidth demand B_c and the reliability demand Q_c), the source node s first searches for an optimized path to the destination node d as the working path denoted by WP_c . During the signaling process of the working path, the source node performs the data collection and subsequently calculates the following parameters – the *Working Path Failure Probability* (P_c^{WP}) (calculated using Equation 3) and *SRLG constraint* (explained in section 3.1). If the calculated reliability of the working path alone can not satisfy the reliability requirement, i.e. $R_c^{WP} = 1 - P_c^{WP} < Q_c$, then the residual reliability is calculated and a backup path becomes mandatory for this connection request. A link-disjoint second optimized path is calculated by the source node s as the backup path BP_c . The source node then calculates the *Backup Path Failure Probability Constraint* (β_c^{BP}) using Equation 6 and the *Backup Link Constraint* (β_c^L) using Equation 7 knowing the number of hops H_c of the backup path. The Equal-Distribution policy discussed in [30] is assumed in this thesis to distribute the reliability constraint to each

individual link along the backup path when calculating β_c^L as in Equation 7. The backup path bandwidth allocation is done link by link with signaling. Each link (i,j) along the backup path first checks if the existing RBBs can be shared for this new backup path request. For the n^{th} RBB with bandwidth capacity $RB_{i,j}^n$, if sharing this RBB can still meet the set of *Backup Link Constraint* ($\beta_{c_k}^L \mid c_k \in T_{i,j}^n$) (as in Equation 8 and 9) and the *Bandwidth Constraint* (B_c) (as in Equation 14), and if the new connection is not in the same SRLG group with other connections in the set $T_{i,j}^n$, then sharing this RBB is granted and the bandwidth capacity allocated to this RBB is updated as $RB_{i,j}^n = \max(RB_{i,j}^n, B_c)$. If all the existing RBBs are not sharable, then a new RBB is allocated for this connection request as long as the bandwidth is not at its full capacity.

The set of *Backup Link Constraints* in Equation 8 is defined as follows: $T_{i,j}^n$ is the set of connections which use link (i,j) as their backup link and which are sharing the same RBB with allocated bandwidth denoted by $RB_{i,j}^n$. The new connection request is also included in the set $T_{i,j}^n$. For any connection $c_k \in T_{i,j}^n$, the left side of Equation 8 is the probability that either the link (i,j) fails or at least one of the working paths of the connections except for c_k in the set $T_{i,j}^n$ fails. This failure probability value should not exceed the *Backup Link Constraint* $\beta_{c_k}^L$ so that the residual reliability requirement $Q_{c_k}^{BP}$ and the overall reliability requirement Q_{c_k} could be satisfied.

The *Bandwidth Constraints* (Equation 14) is defined as follows: $RB_{i,j}^n$ is the allocated bandwidth to the n^{th} RBB on link (i,j) . $AB_{i,j}$ is the total available bandwidth on link (i,j) . The left side of Equation 14 – $(RB_{i,j}^n + AB_{i,j})$ is the maximum available bandwidth capacity for the new connection request when checking the n^{th} RBB on link (i,j) . Its value should be greater than or equal to the bandwidth requirement B_c for the new connection to be operational.

4.2 Sharing Blocks Management

The concept of *Multiple Reserved Bandwidth Blocks* (RBB) is used to manage the bandwidth sharing. If the current RBB is not available for sharing, a new RBB can be created dynamically, provided extra bandwidth is available on the link according to either one of the three scenarios described below.

Scenario 1: Assume that no previous connection is using the link (i,j) as its backup link ($RB_{i,j} = 0$) and the first request for backup path arrives with the parameters Q_{c_1} , B_{c_1} , $P_{c_1}^{WP}$, and $\beta_{c_1}^L$, the first task is to check the following two constraints: (1) the bandwidth constraint such that $AB_{i,j} \geq B_{c_1}$, and (2) the reliability constraint such that $P_{i,j}^L \leq \beta_{c_1}^L$. If both constraints are satisfied, then B_{c_1} unit bandwidth can be allocated for the first RBB – RBB #1 as $RB_{i,j}^1 = B_{c_1}$. The total Reserved Bandwidth becomes

$RB_{i,j} = RB_{i,j}^1 = B_{c_1}$. At the same time, the working path failure probability $P_{c_1}^{WP}$ and the backup link constraint $\beta_{c_1}^L$ are recorded to the local database.

Scenario 2: A second request for a backup path arrives at link (i,j) , with the constraint parameters Q_{c_2} , B_{c_2} , $P_{c_2}^{WP}$, and $\beta_{c_2}^L$, then the following constraints should be checked: (1) the bandwidth constraint such that $AB_{i,j} + RB_{i,j}^1 \geq B_{c_2}$, (2) the reliability constraints such that: $1 - (1 - P_{i,j}^L) \times (1 - P_{c_1}^{WP}) \leq \beta_{c_2}^L$ and $1 - (1 - P_{i,j}^L) \times (1 - P_{c_2}^{WP}) \leq \beta_{c_1}^L$. Both reliability constraints should be checked because adding a new backup path to the RBB may degrade the reliability of the existing connections. (3) The *SRLG constraint* such that if the working path of the first connection and the working path of the second connection are in the same *SRLG* group, they cannot share the same RBB. If all three constraints are satisfied, then the resource on the first RBB can be shared by this new connection request. Consequently, the bandwidth allocated to the first RBB ($RB_{i,j}^1$) is updated to $RB_{i,j}^1 = \max(RB_{i,j}^1, B_{c_2})$. In addition, $P_{c_2}^{WP}$ and $\beta_{c_2}^L$ need to be recorded to the local database for future sharing calculation. If RBB #1 cannot be shared by this new connection, either because there is no more bandwidth available or because the current reliability constraints or the *SRLG* constraint cannot be satisfied, a second RBB has to be allocated which is denoted by RBB #2. Suppose $AB_{i,j} \geq B_{c_2}$ and $RB_{i,j}^2 = B_{c_2}$, the total reserved bandwidth is the sum of the reserved bandwidth of the two individual bandwidth blocks – $RB_{i,j} = RB_{i,j}^1 + RB_{i,j}^2$.

Scenario 3: In general, if a connection request for backup path (c_k) arrives with the parameters Q_{c_k} , B_{c_k} , $P_{c_k}^{WP}$ and $\beta_{c_k}^L$, the existing RBBs are searched similarly to scenario 2. If the current RBB can not be shared, the subsequent RBB needs to be checked. If there is no available RBB that can be shared, then a new sharing block is created as described in scenario 2.

4.3 Procedure of LFP-First Fit Algorithm

In this section, the detail process of setting up a connection and the signaling procedure are described. Figure 12 shows the work flow of the signaling process related to the LFP-FF scheme.

Figure 12: The Signaling Process of LFP-FF Algorithm

Figure 13 shows a simple network $G=(V,E)$ with nine nodes and eleven links to illustrate the detail procedure of our proposal. Each link has an administrative weight of

1, so that finding the optimized path means finding a minimum hop-count path. The link capacity, in terms of bandwidth units, and the LFP value of each link are shown in Figure 13. For example, the capacity of the link (1,2) is 100 and its link failure probability is $P_{1,2}^L = 1 * 10^{-3}$. Suppose three consecutive connection requests c_1 , c_2 , and c_3 arrive at node 1, node 4, and node 9. Request c_1 asks for a restorable connection from node 1 to node 3 with a reliability constraint of $Q_{c1}=99.99\%$ and a bandwidth constraint of $B_{c1}=5$. Request c_2 asks for a connection from node 4 to node 6 with $Q_{c2}=99.98\%$ and $B_{c2}=10$. Request c_3 asks for a connection from node 9 to node 6 with $Q_{c3}=99.97\%$ and $B_{c3}=4$.

Figure 13: An Illustration of the LFP-FF Algorithm

The following steps illustrate the detailed procedure to set up the working path and/or the backup path.

STEP 1: When a request for setting up a restorable connection arrives at the source node, the source node computes the optimized path to the destination node as the working path using the Dijkstra shortest path algorithm.

In the example network, the working paths found for the three connections are $WP_{c_1} = \{(1,2), (2,3)\}$, $WP_{c_2} = \{(4,5), (5,6)\}$, and $WP_{c_3} = \{(9,5), (5,6)\}$ as listed in Table 1.

Table 1: List of calculated working paths in step 1

Connection	Bandwidth Demand	Reliability Demand	Calculated Working Path
c_1	5	99.99%	$\{(1,2), (2,3)\}$
c_2	10	99.98%	$\{(4,5), (5,6)\}$
c_3	4	99.97%	$\{(9,5), (5,6)\}$

STEP 2: An RSVP *PATH* message is sent along WP_c to signal the working path. When each node along the working path receives this *PATH* message, it calculates the aggregated *Working Path Failure Probability* P_c^{WP} from the source to the current node using the equation $P_c^{WP} = 1 - (1 - P_c^{WP}) * (1 - P_{i,j}^L)$, where link (i,j) is the current link and $P_{i,j}^L$ is the *Link Failure Probability*. This information is carried and transmitted with the *PATH* message to the subsequent node and being updated by the following node. The available bandwidth is also checked on each node along the working path to guarantee the bandwidth requirement ($AB_{ij} \geq B_c$). If the available bandwidth AB_{ij} is not sufficient to allocate the B_c bandwidth demand, then a failure acknowledgement message is sent to

the source node and the connection request is rejected. When the *PATH* message arrives at the destination node, an *RESV* message is created containing the calculated *working path failure probability*

$$P_c^{WP} = 1 - \prod_{(i,j) \in WP_c} (1 - P_{i,j}^L).$$

In the example, node 1 sends a *PATH* message along the path $WP_{c_1} = \{(1,2), (2,3)\}$.

The available bandwidth on the link $(1,2)$ and the link $(2,3)$ are checked. Since $AB_{12}=AB_{23}>B_1$, the bandwidth requirement is satisfied. When node 3 receives the *PATH* message, it also knows the information concerning the *working path failure probability* which is $P_{c_1}^{WP} = 1 - (1 - P_{1,2}^L)(1 - P_{2,3}^L) = 1.999 \times 10^{-3}$. Following the same process, the calculated working path failure probabilities for all three connections are listed in Table_2.

Table 2: List of the calculated working path failure probability in step 2

Connection	Working Path Failure Probability	Working Path
c_1	1.999×10^{-3}	$\{(1,2), (2,3)\}$
c_2	1.999×10^{-3}	$\{(4,5), (5,6)\}$
c_3	1.999×10^{-3}	$\{(9,5), (5,6)\}$

STEP 3: The *RESV* message is sent back to the source node along the reverse of the working path carrying the *working path failure probability* P_c^{WP} and the *SRLG* constraint. The destination node initializes the elements of the *SRLG* array to zero. As the *RESV* message is being processed by the transit node, the *SRLG* array is updated

accordingly – all the information regarding the connections that are using the current link as their working link is added to the *SRLG* array. This can be achieved because it is assumed that each node maintains its own state table on a local database and stores the connection information whenever a new working path is being setup. The *SRLG* constraint array is updated at each node and forwarded to the next node with the *RESV* message.

In the example, since connection c_1 is the only connection that uses link $(1,2)$ and link $(2,3)$ as its working link, the *SRLG* array is empty and sets to NULL. Since both connection c_2 and c_3 use the link $(5,6)$ as their working link, these two connections are in the same *SRLG* constraint. When the *RESV* message of the working path WP_{c_3} arrives at node 5, node 5 inserts the information regarding the connection c_2 to the *SRLG* array of the *RESV* message. Once the source nodes receive the *RESV* message, they extract the *working path failure probability* constraint and the *SRLG* constraint from the *RESV* message and record them to their local databases shown in Table 3.

Table 3: Some information of the connections in step 3

Connection	Working Path Failure Probability	SRLG constraint
C_1	$1.999 \cdot 10^{-3}$	NULL
C_2	$1.999 \cdot 10^{-3}$	NULL
C_3	$1.999 \cdot 10^{-3}$	$\{c_2\}$

STEP 4: When the source node receives the working path *RESV* message, it first checks the reliability constraint: $(1 - P_c^{WP}) \geq Q_c$, where Q_c is the reliability requirement. If this constraint is satisfied, connection setup is completed successfully and no backup path is required. If $(1 - P_c^{WP}) < Q_c$, a backup path is required to satisfy the reliability requirement and the source node then calculates the expected *backup path failure probability constraint* β_c^{BP} which is the complement of the residual reliability (refer to Equation 6). The source node also extracts the *SRLG* constraint from the working path *RESV* message and records it to its local database.

Table 4: Calculated backup path failure probability constraint in step 4

Connection	$(1 - P_c^{WP}) \geq Q_c ?$	Backup Path is needed?	β_c^{BP}
C ₁	No	Yes	0.05
C ₂	No	Yes	0.1
C ₃	No	Yes	0.15

STEP 5: The source node searches for a second optimized path to the destination as the backup path which is link-disjoint from the working path. The source node then calculates the *Backup Link constraint* β_c^L , according to Equation 7, knowing the number of hops which is a constraint for each link along the backup path.

Table 5: Calculated backup link constraint in step 5

Connection	Backup Path BP_c	β_c^{BP}	H_c	β_c^L
c_1	$\{(1,7),(7,8),(8,3)\}$	0.05	3	0.017
c_2	$\{(4,7),(7,8),(8,6)\}$	0.1	3	0.035
c_3	$\{(9,7),(7,8),(8,6)\}$	0.15	3	0.053

STEP 6: The source node generates a *PATH* message, which consists of the bandwidth constraint B_c , the Backup Link constraint β_c^L , and the working path failure probability P_c^{WP} for signaling the backup path BP_c . The *SRLG* constraint is also transmitted with this *PATH* message. The *PATH* message is forwarded along the backup path. As each link along the backup path receives the backup *PATH* message, it checks whether the resources on the existing RBBs of this link are sharable by this new connection. If sharing the path still meets the reliability constraint, the bandwidth constraint and the *SRLG* constraint of each connection using this link as the backup link (refer to Equation (8)-(10)), then sharing the bandwidth is granted. If at least one of the constraints cannot be satisfied, then a new RBB is allocated unless there is no bandwidth available. If the bandwidth allocation is successful, the *PATH* message is forwarded to the downstream node; otherwise, a failure notification message is returned to the source node.

In the example network, the behavior of link (7,8) is explained in detail below because all three connections use this link as their backup link. When the first request for the backup path arrives at link (7,8) with the parameters Q_{c_1} , B_{c_1} , $P_{c_1}^{WP}$, and $\beta_{c_1}^L$, since no previous connection is using the link (7,8) as its backup link ($RB_{7,8} = 0$), the following

two constraints should be checked – the Bandwidth Constraint: $AB_{7,8} \geq B_{c_1}$ and the Reliability Constraint: $P_{7,8}^L \leq \beta_{c_1}^L$. Since both constraints are satisfied, B_{c_1} unit bandwidth would be allocated to the first RBB ($RB_{7,8}^1 = B_{c_1}$). The total reserved bandwidth becomes $RB_{7,8} = RB_{7,8}^1 = B_{c_1}$. At the same time, the following information is recorded in the local state database: the *working path failure probability* $P_{c_1}^{WP}$ and the *backup link constraint* $\beta_{c_1}^L$.

When the second request c_2 for a backup path arrives at link (7,8), with the constraint parameters Q_{c_2} , B_{c_2} , $P_{c_2}^{WP}$, and $\beta_{c_2}^L$, the following constraints should be checked for RBB#1 on link (7,8) – the Bandwidth Constraint: $AB_{7,8} + RB_{7,8}^1 \geq B_{c_2}$, the Reliability Constraint: $1 - (1 - P_{7,8}^L) \times (1 - P_{c_1}^{WP}) \leq \beta_{c_2}^L$ and $1 - (1 - P_{7,8}^L) \times (1 - P_{c_2}^{WP}) \leq \beta_{c_1}^L$ and the *SRLG constraint*. Since WP_{c_1} and WP_{c_2} do not share any link, the SRLG constraint is satisfied. Because all these constraints are satisfied, which means the RBB #1 is sharable by this new request, the bandwidth allocated to RBB #1 becomes: $RB_{7,8}^1 = \max(RB_{7,8}^1, B_{c_2}) = \max(5, 10) = 10$. The $P_{c_2}^{WP}$ and the $\beta_{c_2}^L$ values are subsequently recorded in the local database for future reference and sharing calculations.

When the third request for backup path arrives at the link (7,8) with the parameters Q_{c_3} , B_{c_3} , $P_{c_3}^{WP}$, and $\beta_{c_3}^L$, the existing reserved bandwidth blocks are checked to see if any bandwidth blocks can be shared. By analyzing the *SRLG* array from *PATH* message, it is known that connection c_3 is in the same *SRLG* group with connection c_2 .

Therefore connection c_3 cannot share the same RBB with c_2 . RBB#2 is created such that $RB_{7,8}^2 = B_{c_2} = 4$. The total reserved bandwidth on the link $(7,8)$ is now the sum of the two sharing blocks: $RB_{7,8} = RB_{7,8}^1 + RB_{7,8}^2 = 10 + 4 = 14$.

STEP 7: When the destination node receives this *backup PATH* message, it sends back a *RESV* acknowledgement to the source node. When the source node receives the *RESV* message, the connection is completed successfully.

4.4 LFP First-Fit vs. LFP Best-Fit

In the First-Fit backup resource allocation scheme, when a new connection request arrives, each node along the backup path checks the existing RBBs on the link sequentially. Once the first suitable RBB satisfies the reliability constraint, the sharing feature is granted and the bandwidth of this RBB is updated to be the maximum value of all requests. If all the existing RBBs can not be shared with this new request, then a new RBB is allocated. The flow process of this algorithm is illustrated in Figure 14.

Figure 14: Flow Chart of First-Fit Backup Resources Allocation

A limitation of the LFP-FF algorithm is the fact that it does not consider each individual connection's bandwidth requirement separately. In the case that a bandwidth block is being shared by connections with very different bandwidth requirements, the resource utilization may not be efficient. An improvement over LFP-FF algorithm is proposed called LFP Best-Fit (LFP-BF). In LFP-BF algorithm, the sharing blocks are reordered by the value of the allocated bandwidth each time when a new connection is set up successfully. When a new connection request arrives, each node along the backup path first finds the most suitable RBB and then checks the reliability constraint. If the current RBB is not sharable, the node then checks a second suitable RBB until a good fit is found. The main idea behind Best-Fit approach is to group the connections with similar bandwidth requirements into the same sharing block as illustrated in Figure 15.

Figure 15: Flow Chart of Best-Fit Backup Resources Allocation

As shown in Figure 16, different from the LFP-FF scheme, the LFP-BF scheme groups the connections with similar bandwidth requirements into the same sharing block. The overall bandwidth reserved is therefore reduced from 28 to 23.

Figure 16: Improvement of the Backup Bandwidth Block Management (LFP-BF)

4.5 Reliability Constraint Distribution

The equal-distribution policy discussed in [30] is incorporated to our proposal to distribute the residual reliability constraints.

Suppose there are n nodes along the backup path. Each node will be responsible for a fraction of the total threshold. Since the reliability constraints are multiplicative, the n^{th} root of the threshold is assigned to each node as its responsibility threshold. Although the other two schemes discussed in [30] – the least-effort policy and the best-effort policy may also be used for our algorithm, the equal allocation of responsibility is the most suitable because of its simpler implementation. In this case, the source node does not need to know each link's failure probability value before signaling the backup

path. Consequently, this method can be implemented through a distributed method, and the implementation complexity is greatly reduced.

4.6 Extensions to RSVP-TE

In this thesis, it is assumed that the *RSVP Traffic Engineering (RSVP-TE)* extensions [5] are used which allow signaling messages to be explicitly routed from the source to the destination node. Similar extensions are required for the constraint-based routing label distribution protocol (*CR-LDP*).

The LSP creation involves an initial signaling message from the source node to the destination node to set up the working path. An acknowledgement is returned from the destination node to the source node in order to finish the working path establishment. The acknowledgement signaling message collects the information of the *SRLG* array and the working path failure probability. The *SRLG* array is simply an array consisting of all connection IDs whose working paths are in the same *SRLG* with the current working path. After the backup path is selected, the source node then issues another signaling message to the destination node over the backup path to reserve the backup resource. Generally, only one working path and one backup path are to be setup by signaling in this proposal – no extra round trip messages are needed.

In a network $G=(V,E)$, we assume the network diameter is R , where R is defined as the maximum inter-node distance or the maximum number of links that must be traversed to send a message to any node. We also assume that an average of N^{WP} working paths go through a link in the network, an average of N^{BP} backup paths share the same sharing block and the average total number of sharing blocks in a link is assumed to be K . Then an upper bound of the extra size S of the signaling message carrying such information is estimated by $S=N^{WP}*R$, which is linearly increased depending on how many links on each path and how many working paths go through each link. At each node along the backup path, the computation complexity of the reliability constraint is $O((N^{BP})^2*K)$ depending on how many backup paths sharing each link. If such information is to be flooded to each node in the network using conventional routing protocol, the network overhead will be very huge in a large network. Assuming reasonable network diameter and an efficient encoding of the message, we do not anticipate a significant problem with the message size in our proposal.

4.7 Summary

In this chapter, an LFP based backup resource allocation algorithms – LFP-FF and LFP-BF, are explained in detail. The main ideas behind the algorithms are introduced which is followed by the detailed signaling procedure. The potential performance improvement over LFP-FF is also discussed called LFP-BF. And a brief

introduction to the residual reliability distribution scheme and the extensions to RSVP-TE signaling mechanisms are given which have been applied during this research.

In Chapter II, it is discussed that the legacy SPP algorithms guarantee 100% reliability only against single failure event in the network. Under those schemes, the resources on the backup link can be shared by different backup paths as long as their corresponding connections do not belong to the same SRLG. However when the single failure assumption is not acceptable in the case where the probability of multiple concurrent failures is high, the legacy SPP algorithms may not guarantee the stringent customer's reliability requirements. The DPP algorithms try to solve this problem by allocating dedicated bandwidth for each backup path. However there exist two immediate problems with this approach. First, the bandwidth utilization will be low because backup paths are typically idle most of the time. Secondly, the DPP scheme may also fail to satisfy the customer's reliability requirement if the probability that both the working path and the backup path fail at the same time is high. The proposed solution addresses multiple failure scenarios by directly taking the customer's reliability requirement into account. The probability of multiple failures is incorporated through Equation 2 to Equation 9 under the assumption that all failures are statistically independent. Under single failure scenario, if the reliability of the working path itself cannot satisfy the reliability requirement, the proposed algorithm will be similar to the legacy SPP algorithms by setting up a sharable backup path. Therefore, the legacy SPP algorithms are a special case of the proposed algorithm. On the other hand, if the backup path happens to use a new sharing block on each of the links it traverses due to the

reliability constraint of Equation 8, the proposed algorithm will be similar to the DPP algorithms. Therefore, the DPP algorithms are also a special case of the proposed algorithm.

Since the proposed backup resource sharing algorithms are based on the analysis of each link's LFP value along the working paths and the backup paths, not only the reliability requirement of the current connection can be satisfied but the potential effects of the current connection on the reliability of other connections are also considered. Therefore the reliability constraints are satisfied concisely and correctly over all connections in the network.

Since both the LFP parameter and SRLG parameter are collected by signaling message – not by the flooding of some global link state updates, and since the backup resource allocation is done on each node along the backup path depending only on the local state information, thus this distributed source-routing framework can be implemented in large scalable network ensuring the network overhead is minimized.

Using the Separate Path Selection scheme, the resource utilization is optimized by selecting the most bandwidth-efficient working path and by sharing the backup resources efficiently. The reliability constraint is guaranteed by applying the equal-distribution policy to distribute the residual reliability responsibility equally to each link along the backup paths.

In summary, the proposed algorithms incorporate various features such as multiple failures, SRLG issues, network scalability, resources efficiency, the guaranteed reliability and reliability distribution policy issues etc. Joined consideration of these issues is supposed to achieve a better performance in terms of Call Acceptance Rate and Total Bandwidth Consumption in a large network which has been proven by performing a set of simulations during the research. In the next chapter, the simulation model is described and the numerical results are analyzed for the performance verification of the proposed algorithm.

CHAPTER 5–PERFORMANCE EVALUATION

5.1 General

During this research, a discrete event-driven simulation model is built using C++. First, a simplified network model is introduced and analyzed. By comparing the simulation results and the mathematical analysis for the simplified model, we provide some insight into the correctness and efficiency of the proposed algorithm. Then the proposed algorithm is evaluated in a more realistic network model – NSFNet backbone model. Two performance metrics – Call Acceptance Rate and Total Bandwidth Consumption, are investigated. Both sets of simulation results are compared with the performance of Dedicated Path Protection (DPP) scheme. The reason that DPP is being compared instead of other SPP schemes is because the conventional SPP schemes have different goals with the proposed algorithm. As discussed in Chapter II, most of the SPP schemes are based on the algorithms of bandwidth efficiency under single failure model guaranteeing 100% reliability. Those algorithms will fail when multiple concurrent failures occur in the network. Therefore the performances – Bandwidth Utilization and Call Acceptance Rate of those schemes are not comparable with the proposed algorithm. While the DPP algorithm can provide the same level of reliability as our proposed algorithm under the condition that the probability of a concurrent failure of the working

and backup paths is low, therefore we compare the performance of our proposal with DPP scheme.

5.2 Simplified Network Model

For the best understanding of this LFP-based algorithm and assuring that the simulation model is built correctly, a simplified network model is introduced and analyzed as shown in Figure 17. Although this network model is simpler and might not reflect a real system, it still gives us an insight about the impacts of different factors on the performance of the proposed algorithms.

Figure 17: A Simplified Network Model

5.2.1 Description of the Network Model

The goal of this simulation is to analyze the impacts of different factors on the performance evaluation. These factors include the effects of the correlated working paths (SRLG) that happen to share the same backup link and the effects of the reliability constraints on the calculation of backup resource sharing. Figure 17 shows an example with only three source-destination pairs, i.e. pair (1,2), pair (3,4) and pair (5,6). For this set of experiments, the number of source-destination pairs M was incremented from 1 to 100 to simulate different correlation levels of the working paths. The link capacities along the working paths (e.g. links along the path (1,2), the path (3,4) and the path (5,6) etc.) are set to infinity. Because all connections' backup paths go through the same link (m,n) , the bandwidth capacity of link (m,n) is the bottleneck for setting up connections. If no available bandwidth on link (m,n) can be shared, then the connection request is rejected. The working paths of connections with the same source-destination pair go through the same set of links; therefore, they belong to the same *SRLG*. For example, both the working path of connection c_1 (WP_{c_1}) and the working path of connection c_2 (WP_{c_2}) belong to the same *SRLG* because they share the common links between the source node 1 and the destination node 2. Requests asking for restorable connections arrive at each source node (*node 1, node 3, node 5, etc, for example.*) with the corresponding destination node (*node 2, node 4, node 6, etc*) according to a Poisson process with an average rate of $\lambda=1/50$. The average inter-arrival time of the requests is set to 50 hours. The holding time of each connection is set to infinity. All connections

can be restored with the same reliability demand $Q_c = 99.99\%$. The bandwidth demand of each connection request is governed by a discrete uniform distribution between 1 and 10 bandwidth units. All the working paths have the same failure probability of $P_c^{WP} = 0.1\%$. The failures of different working paths are statistically independent – i.e. any working path's failure does not affect other paths. The failure probability of the backup link (m,n) is set to $P_{m,n}^L = 0.1\%$ and the capacity of the link (m,n) is 50 bandwidth units. Each link has an administrative weight of 1 unit.

The performance metrics used in this simulation is to estimate the maximum number of connections in the network (denoted by N_{max}) given the number of source-destination pairs M . In the following sections, a mathematical analysis of N_{max} is explained, which is followed by the simulation results.

5.2.2 Mathematical Analysis

Since the link (m,n) is the only bottleneck when determining N_{max} , the major task is to calculate the number of backup paths that the link (m,n) can accommodate.

Assuming that the total available bandwidth (AB_{mn}) on the link (m,n) can be maximally divided into K blocks ($K > 0$) with each block's average size equals to $E(RB_{mn}^i)$, ($i=1,2,\dots,K$), we have $K = \lfloor AB_{mn} / E(RB_{mn}^i) \rfloor$ where the notation $\lfloor x \rfloor$ represents

the largest integer that is less than or equal to x . It is also assumed that the reliability constraint can always be satisfied no matter how many backup paths share this RBB as long as they are not subject to the same risk of failure. Given the number of source-destination pairs M or the maximum number of backup paths which can share the same RBB denoted by $N'_{\max} = M$, the maximum number of connections $N_{\max}$ can be calculated using Equation 15.

$$N_{\max} = M * K = M * \lfloor AB_{mn} / E(RB_{mn}^i) \rfloor \quad \text{_____ (15)}$$

For estimating the average size of each sharing block $E(RB_{mn}^i)$, we have:

$$E(RB_{mn}^i) = E(\max\{B_{c_j} \mid c_j \in T_{mn}^i\}) \quad \text{_____ (16)}$$

In Equation 16, $\{B_{c_j} \mid c_j \in T_{mn}^i\}$ is the set of bandwidth demands of those connections whose backup paths share this RBB. Since the bandwidth demand of each connection is assumed to be governed by a discrete uniform distribution between 1 and 10 bandwidth units, the distribution function can be approximated as shown in Figure 18. It can be proved that the value RB_{mn}^i is also a discrete random variable between 1 and 10. The following proves the property of the distribution function of RB_{mn}^i .

Figure 18: The Distribution Function of the Bandwidth Demand in the Simplified Network Model

Lemma 1: Let $X_1, X_2, \dots, X_N$ be a set of independent random variables having the distribution functions $F_{X_1}, F_{X_2}, \dots, F_{X_N}$ respectively. Define $Y_N = \max(X_1, X_2, \dots, X_N)$ to be the largest of those random variables. Then the probability distributions function $F_{Y_N}(y)$ can be calculated by $F_{Y_N}(y) = F_{X_1}(y)F_{X_2}(y) \cdots F_{X_N}(y)$ for all y .

Proof: From the definition of the probability distribution function:

$$\begin{aligned}
 F_{Y_N}(y) &= P(Y \leq y) \\
 &= P(\max(X_1, X_2, \dots, X_N) \leq y) \\
 &= P(X_1 \leq y \text{ and } X_2 \leq y \text{ and } \dots X_N \leq y) \\
 &= P(X_1 \leq y) * P(X_2 \leq y) * \dots * P(X_N \leq y) \quad (\text{Since independent}) \\
 &= F_{X_1}(y)F_{X_2}(y) \cdots F_{X_N}(y)
 \end{aligned}$$

■

From Lemma 1, assuming that each connection is randomly assigned to a RBB, the distribution function of RB_{mn}^i can be calculated by:

$$F_{RB_{mn}^i}(y) = \prod_{c_j \in T_{mn}^i} [F_{B_{c_j}}(y)] = [F_{B_{c_j}}(y)]^{N_{\max}^i} \quad (17)$$

Thus the mean value of RB_{mn}^i is calculated by:

$$E(RB_{mn}^i) = \sum_{j=1}^{10} j * P(RB_{mn}^i = j) = \sum_{j=1}^{10} j * (F_{RB_{mn}^i}(j) - F_{RB_{mn}^i}(j-1)) \quad (18)$$

For example, if M equals 2, the calculated values of $F_{RB_{mn}^i}(y)$ and $P(RB_{mn}^i = y)$ are obtained as shown in Table 6. We calculate $E(RB_{mn}^i) = 7.15$. The variable y ranges from 1 to 10. Figure 19 shows the distribution function of $RB_{mn}^i = \max(B_{c_1}, B_{c_2})$.

Table 6: Calculated $F_{RB_{mn}^i}(y)$ and $P(RB_{mn}^i = y)$ when $M=2$

Y	1	2	3	4	5	6	7	8	9	10	
$F_{RB_{mn}^i}(y)$	0.01	0.04	0.09	0.16	0.25	0.36	0.49	0.64	0.81	1	
$P(RB_{mn}^i = y)$	1%	3%	5%	7%	9%	11%	13%	15%	17%	19%	$E(RB_{mn}^i) = 7.15$

Figure 19: The Distribution Function of $RB_{mn}^i = \max(B_{c_1}, B_{c_2})$

Since the bandwidth capacity of the link (m,n) is set to 50 and this bandwidth capacity is only reserved for the backup paths, in the case when $M=2$, the maximum number of connections can be estimated as: $N_{max} = (50/7.15) * 2 \cong 14$.

In general, the maximum number of connections N_{max} can be calculated by:

$$\begin{aligned}
 N_{\max} &= \frac{50}{E(RB_{mn}^i)} * M \\
 &= \frac{50}{\sum_{i=1}^{10} \left\{ i * \left[\left(\frac{i}{10} \right)^{N'_{\max}} - \left(\frac{i-1}{10} \right)^{N'_{\max}} \right] \right\}} * M \\
 &= \frac{50 * M}{10 - 0.1^M - 0.2^M - \dots - 0.9^M} \\
 &= \frac{50 * M}{10 - \sum_{i=1}^9 \left(\frac{i}{10} \right)^M} \approx 5 * M \quad \left(\text{Since } \sum_{i=1}^{10} \left(\frac{i}{10} \right)^M \ll 10 \right)
 \end{aligned}$$

When M is incremented from 1 to 100, the calculated values of $E(RB_{mn}^i)$ and N_{max} are listed in Table 7.

Table 7: Calculated Values of $\varepsilon(RB_{mn}^i)$ and N_{max} under different value of M

M	1	2	3	4	5	6	7	8	...
$\varepsilon(RB_{mn}^i)$	5.5	7.15	7.975	8.467	8.792	9.022	9.192	9.323	...
N_{max}	9.09	13.99	18.81	23.62	28.44	33.25	38.08	42.91	...

From Table 7, it appears that N_{max} increases almost linearly with respect to M without considering the reliability constraints. When the reliability constraints are taken into account, the N_{max} value cannot be increased indefinitely. In reality, the total number of connections whose backup paths share the same RBB is restricted by the reliability constraints. When an increasing number of connections join the sharing group, the reliability of each connection decreases; thus, at some point, the total number of connections will approach to a limit when the number of source-destination pair is increased to some large number M_{max} .

Since each working path failure probability $P_{c_i}^{WP} = 0.001$, the link failure probability of link (m,n) is $P_{mn}^L = 0.001$ and the reliability demand for each connection request is $Q_{c_i} = 99.99\%$. For each RBB, the maximum number of connections N'_{max} should satisfy the following constraint (refer to the analysis through Chapter II to Chapter IV):

$$(1 - P_{c_i}^{WP})^{N'_{max}-1} * (1 - P_{mn}^L) \geq [1 - (1 - Q_{c_i}) / P_{c_i}^{WP}]^{1/3} \quad \text{_____} (19)$$

From Equation 19, we have $N'_{max}=34$, thus $N_{max}=34*5\cong 170$. The actual curve of N_{max} is drawn on Figure 20 as a dotted line. From the figure, it is possible to observe that the actual curve of N_{max} increases almost linearly with the increase of the source-destination pairs. When the number of source-destination pairs exceeds 34, N_{max} approaches to a fix number of 170. The line of $y = 5x$ is also drawn on Figure 20 as the blue line.

Figure 20: Mathematical Analysis of the Average Maximum Number of Connections in the Simplified Network Model

5.2.3 Simulation Results

The performance metric is quantified in terms of the average maximum number of connections the network can accommodate. The value is obtained by running the

simulation until five consecutive connection requests are rejected. Sometimes, when a request happens to be rejected, there is still potential to accommodate future requests. Therefore, there might be some minor difference between the analysis results and the simulation results, however, since the simulation runs for 20 replications and the final result is an averaged approximation, the difference is acceptable and can be minimized with an increase in the number of replications. If there is only 1 source-destination pair, obviously, the behavior of all three schemes (*LFP-FF*, *LFP-BF* and *DPP*) should be the same since all the connections use the same set of links for their working paths and backup paths. In this case, they belong to the same SRLG (backup bandwidth blocks are not sharable). With an increase in the number of source-destination pairs, the total number of successful connections using the *LFP-FF* scheme and the *LFP-BF* scheme will increase almost linearly at first. When the number of source-destination pairs reaches some larger number, the main factor that affects the connections will no longer consist of the *SRLG* constraint. Instead, it is the reliability constraint that will determine the bandwidth sharing likelihood.

Figure 21: Simplified Network Simulation Result: Average Maximum Number of Connections vs. Network Load

Figure 21 shows the simulation results of the simplified network model. The Y-axis depicts the maximum number of connections $E(N_{max})$ in the network and the X-axis shows the number of the source-destination pairs M . This figure also illustrates that both the LFP-FF and the LFP-BF schemes perform better than the DPP scheme in terms of maximum number of connections. When the number of the source-destination pairs reaches a large number, the value of N_{max} from the LFP-FF and the LFP-BF schemes approaches to an asymptote around 160 and 190. The LFP-BF performs better than the LFP-FF scheme as predicted. It is not a surprise that the analytical results sit between the LFP-FF and LFP-BF because it is actually a Random Fit algorithm rather than First Fit or Best Fit. In the case when the number of source-destination pairs equals 1, all three schemes have the same value of around 10. The fact that the curves of the LFP-FF and LFP-BF scheme are very much similar to the mathematical analysis shows that their

performance are indeed limited by the SRLG constraint and the reliability constraint as discussed in the Chapter IV. Figure 22 is a plot of the performance with error bars showing 95% confidence intervals.

Figure 22: Plot of the Performance with Error Bars Showing 95% Confidence Intervals

5.3 Call-Acceptance-Rate Test of the Simplified Network Model

5.3.1 Simulation Model Description

The network model used in this set of experiments is similar to that of the first simulation model as shown in Figure 17. Instead of changing M , we fix M as $M=40$. Furthermore, we assume the holding time of each connection request follow an

exponential distribution with mean values $1/\mu$ incremented from 10 to 2000 to simulate the different loads on the network. This is different from the scenario discussed in previous section where the holding time is infinite. The performance metric used in this simulation is the Call Acceptance Rate (the complement of the Call Loss Rate) which is the ratio of the number of successful connections over the total number of connection requests denoted by

$$R = \frac{\text{Total_Number_of_Successful_Connections}}{\text{Total_Number_of_Connections}} \quad \text{_____} \quad (20)$$

Two cases are analyzed. In Case 1, the bandwidth demand is fixed to $B=5$, and in Case 2, the bandwidth demand is a random variable governed by a discrete uniform distribution between 1 and 10 which is the same case as the NSFNet simulation scenario discussed later.

5.3.2 Mathematical Analysis 1 for Case 1: Fixed Bandwidth Demand

First, we consider the case that the bandwidth demand by each connection request is fixed to $B = 5$ bandwidth units instead of the uniform distribution as in the previous simulation. Since connection requests arrive at each source node according to a Poisson process with an average rate of $\lambda=1/50$ and the holding time is exponentially distributed with mean value of $1/\mu$, this telecommunication system can be modeled as an $M/M/r/r$ queuing system. Here, the “bandwidth capacity” is the servers with the service rate μ , the connection holding time can be the service time, and the connection requests are actually the customers which arrive at rate λ .

Figure 23: An Illustration of M/M/r/r queueing system

Figure 23 shows a schematic diagram for the $M/M/r/r$ queueing system. In an $M/M/r/r$ queueing system, the arrival process and the service process follow a Poisson distribution with mean arrival rate λ and mean service rate μ respectively. There are r servers and no waiting queue in the system so that the system capacity equals the number of parallel servers. Therefore in such a system, an arriving customer finding all servers busy will not enter the system and is considered lost. For the DPP scheme, the number of servers r is estimated as $r = E(N) = \frac{C}{B} = \frac{50}{5} = 10$, where C is the bandwidth capacity of link (m,n) and B is the bandwidth demand for each request. For the LFP-FF or LFP-BF algorithms, similar to the analysis of the previous simulation model, the average number of connections in the system in the case of $M=40$ can be estimated by $E(N) = N'_{\max} * E(K) = 34 * 10 = 340$, where $N'_{\max} = 34$, calculated by Equation 19, is the maximum number of connections for each RBB on link (m,n) and $E(K) = 10$ is the average number of RBBs on link (m,n) . Since the capacity C of link (m,n) is 50 bandwidth units and each connection requests 5 bandwidth units, we have $K=50/5=10$.

Therefore, the number of servers in LFP-FF and LFP-BF is estimated as $r = E(N) = 340$.

The long run proportion of time that the system is full or the probability that all servers are busy is given by Equation 21:

$$E(r, \rho) = \frac{\frac{\rho^r}{r!}}{\sum_{i=0}^r \frac{\rho^i}{i!}} \quad (21)$$

Equation 21 is known as Erlang B Loss formula [51]. $\rho = \frac{\lambda}{\mu}$ denotes the traffic offered load, whose units are Erlangs. $E(r, \rho)$ denotes the blocking probability or the complement of call acceptance rate. It is useful to note that the recursive form for the Erlang B formula, which simplifies the numerical evaluation, is given as follows [51]:

$$E(r, \rho) = \frac{\rho E(r-1, \rho)}{r + \rho E(r-1, \rho)} \quad (22)$$

Using Equation 22, we calculate the mathematical results of Call Acceptance Rate under different network load shown as in Figure 24. The green dotted curve is the mathematical result of DPP scheme (the number of servers $r=10$) and the blue curve is the result of LFP-FF or LFP-BF ($r=340$). Since the bandwidth demand is a fixed value, not a random variable, both LFP-FF and LFP-BF schemes should achieve the same performance.

Figure 24: Mathematical Results: Call Acceptance Rate vs. Network Load in Simplified Network Model

5.3.3 Simulation Results for Case 1

Figure 25: Simulation Results: Call Acceptance Rate vs. Network Load in Simplified Network Model in Case 1 (Fixed Bandwidth Demand)

The simulation results shown on Figure 25 demonstrate that both the LFP-FF and the LFP-BF schemes perform much better than the DPP scheme in terms of the Call Acceptance Rate in this simplified network model. There is no difference between the performance of LFP-BF and LFP-FF for the given scenario because the bandwidth demands are a fixed value. With an increase in the network load, the Call Acceptance Rates of all three schemes decrease, but the DPP scheme diminishes more quickly than the other two schemes. Figure 25 also shows that the simulation results are very much similar to the mathematical analysis. There is a minor difference between the simulation results and the theoretical results of LFP-FF/LFP-BF under low network load. The reason of the difference is because that during the mathematical analysis, we neglect the correlation of the working paths – it was assumed that all connections' working paths do not share any link. While during the simulation, there exists the shared risk issue which has to be considered, for example, two connections with the same source-destination pair will have the same shared risk thus can not share the same bandwidth block. The sharing contentions between the correlated working paths can block some potential connections, thus causing the capacity of system decreased. For the DPP scheme, the sharing feature is not implemented and the contention between the correlated working paths does not exist, therefore the curve of the simulation results of DPP scheme matches the analysis results very well.

5.3.4 Mathematical Analysis for Case 2: Uniformly Distributed Bandwidth Demand

In this section, we consider a more common case that the bandwidth demand by each connection request is uniformly distributed between 1 and 10 bandwidth units.

For DPP algorithm, this system can be modeled as another kind of multi-service loss system called Stochastic Knapsack System [52]. The classical stochastic knapsack problem involves a “knapsack” of capacity C resource units and K classes of objects, with class- k objects having size b_k . Objects may be placed into the “knapsack” as long as the sum of their sizes does not exceed the knapsack capacity. This problem aims to place the objects into the “knapsack” so as to maximize the long run number of objects admitted by the system. In our case, the capacity of link (m,n) is set as $C=50$. The total number of classes is $K=10$ with the request of each class- k denoted by $b_k=k$ ($k=1,2,\dots,10$).

Class- k objects arrive at the system according to a Poisson process with rate $\lambda = \lambda' * \frac{M}{K}$;

where $\lambda' = \frac{1}{50}$ is the arrival rate of each connection request for each source-destination pair and $M=40$ is the total number of source-destination pair. If an arriving class- k object is admitted into the system, it takes b_k resource units for a holding time that is exponentially distributed with mean $1/\mu$. In [52], an expression is given for calculating the class- k objects blocking probability B_k as in Equation 23.

$$B_k = 1 - \frac{\sum_{n \in S_k} \prod_{j=1}^K \rho_j^{n_j} / n_j!}{\sum_{n \in S} \prod_{j=1}^K \rho_j^{n_j} / n_j!} \quad \text{_____} (23)$$

In Equation 23, S is the set of all possible states in the system and S_k is the subset of states in which the “knapsack” admits an arriving class- k object. A more efficient recursive algorithm is also presented in [52] which does not involve brute-force summation. Using this recursive algorithm, we draw the mathematical result of DPP scheme shown as the blue curve in Figure 26.

For LFP-FF and LFP-BF algorithms, the system is still an $M/M/r/r$ queuing system as discussed in Case 1 except that the server number r has to be recalculated due to the fact that each block size is variable now. From Lemma 1, assuming that each connection is randomly assigned to a RBB, the mean value of RB_{mn}^i can be calculated by:

$$\begin{aligned}
E(RB_{mn}^i) &= \sum_{j=1}^{10} j * P(RB_{mn}^i = j) \\
&= \sum_{i=1}^{10} \left\{ i * \left[\left(\frac{i}{10} \right)^{N'_{\max}} - \left(\frac{i-1}{10} \right)^{N'_{\max}} \right] \right\} \\
&= 10 - \sum_{i=1}^9 \left(\frac{i}{10} \right)^{N'_{\max}} \approx 10
\end{aligned}$$

Therefore $r = E(N) = N'_{\max} * E(K) = 34 * \frac{50}{10} = 170$. Using Equation 22, we can calculate the blocking probability or call acceptance rate for LFP-based Random Fit scheme under Case 2. The analysis result is shown as the green dotted curve in Figure 26.

Figure 26: Analysis Results: Call Acceptance Rate vs. Network Load in Simplified Network Model in Case 2 (Random Bandwidth Demand)

Figure 27: Simulation Results: Call Acceptance Rate vs. Network Load in Simplified Network Model in Case 2 (Random Bandwidth Demand)

5.3.5 Simulation Results (Case 2)

The simulation results shown on Figure 27 demonstrate that the performance of LFP-BF is better than LFP-FF for this scenario but there is very little difference between the curves. Figure 27 also shows that the simulation results of DPP are very much similar to the analysis results. There is some minor difference between the simulation results and the analysis results of LFP-FF/LFP-BF for this given scenario.

Once again, the correctness of the simulation model is proved. Some configuration parameters are being used in the NSFNet simulation scenario whose correctness is based on this analysis.

5.4 Simulation Results in a NSFNET Network

To further investigate the proposed scheme, a simulation is performed using the *NSFNet* backbone as shown in Figure 28.

Two measurements are investigated in the simulations to evaluate the performance of this backup resource allocation algorithm. The first measurement is the

$$\text{Average Call Acceptance Rate (R), } R = \frac{\text{Total_Number_of_Successful_Connections}}{\text{Total_Number_of_Connections}}.$$

The Average Call Acceptance Rate R is very important as it measures the call throughput. The second measurement is the Total Bandwidth Consumption –

$\sum_{(i,j) \in E} (SB_{ij} + RB_{ij})$, where SB_{ij} is the total service bandwidth used by the working paths on link (i,j) , and RB_{ij} is the total reserved bandwidth used by the backup paths on link (i,j) .

$\sum_{(i,j) \in E} (SB_{ij} + RB_{ij})$ is the sum of the total consumed bandwidth over all the links in the network. The goal of this metric is to measure the capability of accommodating traffic from these three algorithms.

The topology used in this simulation is the backbone NSFNET – short for National Science Foundation’s network. NSFNET is a series of networks devoted for research and educational communication purposes. The example shown in Figure 28 has 16 nodes and 25 links. The total capacities of the links are of 120 (shown as thin lines) and 480 (shown as bolded lines) bandwidth units. The links are bi-directional. Figure 28 also illustrates the link weight (labeled in blue characters) and the link failure probability

(labeled in red characters). Uniform traffic is used, in which an arrival will choose one out of all possible source and destination pairs with equal probability. The connection requests arrive randomly at the same average rate for all source-destination pairs. Requests arrive at each source-destination pair according to a Poisson distribution with an average rate λ , and the holding times are exponentially distributed with a mean $1/\mu$. The simulations are run over a period of 10,000 hours. 30% of these requests are non-protected traffic and 70% of these requests are protected traffic. All the protected traffic connections are setup by the above-mentioned algorithms. Among the protected traffic connections, 30% are protected with the reliability requirement of 99.95%, 30% with the reliability of 99.97% and the other 40% are protected with the reliability of 99.99%. The allocated bandwidth for each LSP is uniformly distributed between 1 and 10 bandwidth units.

Figure 29: NSFNet Simulation Result – Total Bandwidth Consumption vs. Network Load

In Figure 29, the Total Bandwidth Consumption is plotted as a function of the Network Load for the NSFNet network. LFP-BF has the least total consumed bandwidth, and the DPP scheme has the most total consumed bandwidth. The curve of the LFP-FF scheme lies between the LFP-BF and the DPP scheme, and it is very close to the LFP-BF. With the increase of the traffic load, the Total Bandwidth Consumptions for those three protection schemes also increase. The performance of the LFP-FF and the LFP-BF is very close because many constraints will affect the final determination of the backup resource allocation, e.g. the bandwidth constraint, the reliability constraint and the SRLG constraint. The LFP-BF performs better than the LFP-FF by only improving the method of the backup resource allocation considering the bandwidth issue, not the reliability and the SRLG constraints. Therefore in some cases, the LFP-BF performs better than the LFP-FF if the bandwidth is the main criteria, such as in the Simplified Network Model; whereas in some other cases, the LFP-BF performs only slightly better than the LFP-FF. In this network model, the bandwidth sharing feature between the LFP-FF and the LFP-BF is not particularly distinguishable.

Figure 30: NSFNet Simulation Result – Call Acceptance Rate vs. Network Load

Figure 30 shows the Call Acceptance Rate under different network loads. The figure shows that both the LFP-FF and the LFP-BF perform better than the DPP scheme in terms of the Call Acceptance Rate (or connection rejection rate). There is little difference between LFP-FF and LFP-BF with this particular network topology.

Another metric used in this simulation is the restoration overbuilds denoted by

$$\delta = \frac{\sum_{(i,j) \in E} RB_{ij}}{\sum_{(i,j) \in E} SB_{ij}} \text{ as mentioned by G. Li [24]. } \sum_{(i,j) \in E} SB_{ij} \text{ is the sum of service bandwidth over}$$

all links in the network and $\sum_{(i,j) \in E} RB_{ij}$ is the sum of reserved bandwidth over all links in

the network. The metric $\delta = \frac{\sum_{(i,j) \in E} RB_{ij}}{\sum_{(i,j) \in E} SB_{ij}}$ calculates the extra bandwidth that is needed to

meet the network restoration objective.

Figure 31: NSFNet Simulation Result – Ratio of Total Reserved Bandwidth to Total Service Bandwidth vs. Network Load

Figure 31 shows that the LFP-FF scheme and the LFP-BF scheme have a better bandwidth usage than the DPP scheme under a heavy network load. LFP-BF performs better than LFP-FF, but there is not much difference between the two schemes because of this specific network topology. Figure 31 also shows that the DPP scheme has a much flatter shape than the LFP-FF or LFP-BF. The reason that DPP scheme has a flat performance is because DPP scheme actually achieves a 1+1 protection. In DPP scheme, a backup path always corresponds to a working path. Therefore, the ratio of the total reserved bandwidth over the total service bandwidth should be a fix value which does not

depend on the network load. While for LFP-FF or LFP-BF scheme, multiple working paths share the same backup resource; therefore, with the increase of the network load, the increase of the total reserved bandwidth would be much slower than the increase of the total service bandwidth, thus causing a decrease of the performance.

CHAPTER 6—CONCLUSIONS AND FUTURE WORK

6.1 General

This thesis proposes a distributed probability-based backup resource allocation algorithm, which by simulation and mathematical analysis is shown to be more reliable and more bandwidth-efficient than conventional DPP and SPP schemes. This algorithm is based on the relationship between the allocated backup bandwidth and the link failure probability. Essentially, the algorithm first probes for a working path based on an optimized path and then checks that the bandwidth constraint and reliability constraint are met. If the reliability constraints are not satisfied, then another probe is sent to set up the backup path based on the reliability constraint. The algorithm also checks whether two working path subject to the same failure risk shares the same backup resource which is referred as SRLG protection.

6.2 Advantages

This proposed algorithm achieves the following better features.

First, two LFP-based backup resource sharing algorithms are proposed, which are LFP-FF and LFP-BF. By analyzing the relationship between the allocated backup resources and the failure probability of each link in the network, these algorithms can achieve better backup resource utilization compared to the traditional Dedicated Path Protection method. Both the conventional DPP and SPP algorithms are special cases of the proposed LFP-based algorithm.

Secondly, we design a new MPLS Path Protection scheme where enhanced Separate Path Selection approach is applied. In this new scheme, the working path is selected to tackle the issue of resource optimization problem while one or multiple backup paths are selected subsequently based on the reliability constraint. Therefore, both the resources optimization constraint and the reliability constraint are satisfied effectively using this scheme.

Thirdly, an enhancement to RSVP-TE signaling mechanisms is introduced for best supporting the proposed algorithms. Both the Working Path Failure Probability parameter and the SRLG parameter are carried by the signaling message. Each node along the backup path needs such information to determine whether the backup resources can be shared and to decide how much resources should be allocated. Therefore, in this distributed source-routing framework, the backup resource allocation is done on each node along the backup path depending only on the local state information. The global state information of LFP and SRLG is not required to be flooded throughout the network such that the network overhead is minimized. Assuming reasonable network diameter

and an efficient encoding of the message, we do not anticipate a significant problem with the message size in our proposal.

Lastly, the simulation results show that this new algorithm performs better than the conventional Dedicated Path Protection schemes in terms of Call Acceptance Rate and Total Bandwidth Consumption. The performance studies also prove that this scheme achieves the following improved features in comparison with other SPP schemes:

- This algorithm works consistently under multiple link/node failures scenario.
- This algorithm is scalable due to its distributed nature.
- The Equal-Distribution policy is applied to the proposed algorithm to effectively distribute the reliability constraint to each link along the backup path so that the overall connection reliability constraint can be satisfied.
- This algorithm optimizes the network resource utilization by maximizing the sharing of the backup resources.

By performing the mathematical analysis for a simplified network model, some insight into the correctness and efficiency of the proposed algorithm is also provided.

6.3 Future Research

This research can be used to guide many other future researches. One such research direction is to test the proposed algorithm in a more scalable network topology to further test the algorithm's performance. Another area of future research is to generalize the utilization of the proposed algorithm and to apply the algorithm to other

protection schemes such as the Local Repair or the Segmented Repair. Future work will also need to focus on the improvement of the sharing blocks management algorithms to further improve the performance considering the improvement of not only the bandwidth constraint issue but also the reliability constraint and the SRLG constraint issues.

REFERENCES

- [1] A. Autenrieth and A. Kirstadter, "Engineering end-to-end IP resilience using resilience-differentiated QoS", *Communications Magazine*, IEEE, Volume 40, No. 1, January 2002, Pages 50-57
- [2] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP tunnels", IETF RFC 3209, December. 2001
- [3] S. Ayandeh, "Convergence of protection and restoration in telecommunication networks", *Photonic Network Communications*, Volume 4, July 2002, Pages 237-250
- [4] R. Bartos and M. Raman, "A heuristic approach to service restoration in MPLS networks", ICC 2001, IEEE International Conference on, Volume 1, June 2001, Pages 117-121
- [5] R. Bhandari, "Survivable networks – algorithms for diverse routing", Kluwer Academic Publishers, Norwell, MA, 1999
- [6] E. Bouillet, J. Labourdette, G. Ellinas, R. Ramamurthy and S. Chaudhuri, "Stochastic approaches to compute shared mesh restored lightpaths in optical network architectures", *Proceedings, IEEE INFOCOM 2002*, Volume 2, June 2002, Pages 801-807
- [7] E. Calle, J.L. Marzo, A. Urrea and P. Vila, "Enhancing MPLS QoS routing algorithms by using the Network Protection Degree paradigm", *Proceedings, IEEE GLOBECOM 2003*, Volume 6, Dec. 2003, Pages 3053-3057
- [8] E. Calle, J.L. Marzo and A. Urrea, "Evaluating the probability and the impact of a failure in GMPLS based networks", *Proceedings, DRCN 2003*, October 2003, Pages 114-122
- [9] H. Choi, S. Subramariam and H-Ah Choi, "On double-link failure recovery in WDM optical networks", *Proceedings, IEEE INFOCOM 2002*, Volume 2, June 2002, Pages 808-816
- [10] S. Datta, S. Sengupta, S. Biswas, and S. Datta, "Efficient channel reservation for backup paths in optical mesh networks", *Proceedings, IEEE GLOBECOM 2001*, Volume 4, November 2001, Pages 2104-2108
- [11] B.T. Doshi, S. Dravida, P. Harshavardhana, O. Hauser and Y. Wang, "Optical network design and restoration", *Bell Labs Technical Journal*, January-March 1999, Pages 58-84
- [12] G. Ellinas and T.E. Stern, "Automatic Protection Switching for Link Failures in Optical Networks with Bi-directional links", *Proceedings IEEE GLOBECOM'96*, Volume 1, Nov. 1996, Pages 152-156
- [13] G. Ellinas, A.G. Hailemariam and T.E. Stern, "Protection Cycles in Mesh WDM Networks", *IEEE Journal on Selected Areas in Communications*, Volume 18, Issue 10, Oct. 2000, Pages 1924-1937
- [14] A. Farrel and B. Miller, "Surviving failures in MPLS networks", Technical report, Data Connection, February 2001

- [15] K.P. Gummadi, M.J. Pradeep and C.S.R. Murthy, "An efficient primary-segmented backup scheme for dependable real-time communication in multihop networks", Networking, IEEE/ACM Transactions on, Volume 11, Feb. 2003, Pages 81-94
- [16] D. Haskin and R. Krishnan, "A method for setting an alternative label switched paths to handle fast reroute", IETF Internet Draft, Nov. 2000
- [17] P.-H. Ho and H.T. Mouftah, "Reconfiguration of spare capacity for MPLS-based recovery in the Internet backbone networks", IEEE/ACM Transaction on Networking, Volume 12, February 2004, Pages 73-84
- [18] C. Huang, V. Sharma, K. Owens and S. Makam, "Building reliable MPLS networks using a path protection mechanism", Communications Magazine, IEEE, Volume 40, No. 3, March 2002, Pages 156-162,
- [19] S. Jha and M. Hassan, "Engineering Internet QoS", Artech House, August 2002, ISBN:1580533418
- [20] K. Kar, M. Kodialam and T.V. Lakshman, "Routing restorable bandwidth guaranteed connections using maximum 2-route flows", Networking, IEEE/ACM Transactions on, Volume 11, Oct. 2003, Pages 772-781
- [21] M. Kodialam and T.V. Lakshman, "Dynamic routing of bandwidth guaranteed tunnels with restoration", Proceedings, IEEE INFOCOM 2000, Volume 2, March 2000, Pages 902-911
- [22] M. Kodialam and T.V. Lakshman, "Dynamic routing of locally restoration bandwidth guaranteed tunnels using aggregated link usage information", Proceedings, IEEE INFOCOM 2001, Volume 1, April 2001, Pages 376-385
- [23] S. Lee, D. Griffith and N-O. Song, "An analytical approach to shared backup path provisioning in GMPLS networks", Proceedings, IEEE MILCOM 2002, Volume 1, October 2002, Pages 75-80
- [24] G. Li, D. Wang, C. Kalmanek and R. Doverspike, "Efficient distributed path selection for shared restoration connections", Proceedings, IEEE INFOCOM 2003, Volume 11, October 2003, Pages 761-771
- [25] Q. Ma and P. Steenkiste, "On path selection for traffic with bandwidth guarantees", Proceedings, IEEE International Conference on Network Protocols, Oct. 1997, Pages 191-202
- [26] G. Mohan, C.S.R. Murthy, "Lightpath restoration in WDM optical networks", Proceedings, IEEE Network, Volume 14, Nov.-Dec. 2000, Pages 24-32
- [27] G. Mohan and A.K. Somani, "Routing dependable connections with specified failure restoration guarantees in WDM networks", Proceedings, IEEE INFOCOM 2000, Volume 3, March 2000, Pages 1761-1770
- [28] K. Owens, S. Makam, V. Sharma, B. MackCrane and C. Huang, "A path protection/restoration mechanism for MPLS networks", IETF Internet Draft, July 2001
- [29] D. Papadimitriou and E. Mannie, "Analysis of Generalized MPLS-based Recovery Mechanisms", Internet Draft, September 2003
- [30] P. Pongpaibool and H.S. Kim, "Guaranteed service level agreements across multiple ISP networks", Proceedings, DRCN 2003, October 2003, Pages 325-332
- [31] S. Ramamurthy, B. Mukherjee, "Survivable WDM mesh networks. Part I- Protection", Proceedings, IEEE INFOCOM '99, Volume 2, March 1999, Pages 774-751

- [32] S. Ramamurthy, B. Mukherjee, "Survivable WDM mesh networks. Part II- Restoration", ICC'99, IEEE International Conference on, Volume 3, June 1999, Pages 2023-2030
- [33] E. Rosen, A. Viswanathan and R. Callon, "Multiprotocol Label Switching Architecture", IETF RFC 3031, Jan. 2001
- [34] L. Ruan and H. Luo, "A fast lightpath restoration method using two backup paths in WDM networks", Proceedings, IEEE International Conference on Parallel Processing Workshops 2002, Aug. 2002, Pages 183-189
- [35] V. Sharma and F. Hellstrand, "Framework for Multi-Protocol Label Switching (MPLS)-based recovery", RFC-3469, Feb. 2003
- [36] M. Sridharan, R. Srinivasan and A.K. Somani, "On improving partial information routing with segmented path protection", Proceedings, IEEE International Conference on Parallel Processing Workshops 2002, Aug. 2002, Pages 193-198
- [37] A. Srinivasan, "Fault-tolerance in limited time available multiprocessing system", TR-DCS-IR-237, University of Victoria, Canada, July 1995
- [38] M. Tacca, A. Fumagalli, F. Unghvary, "Double-Fault shared path protection scheme with constrained connection downtime", Proceedings, DRCN 2003, October 2003, Pages 181-188
- [39] S. Vutukury and J. Garcia-Luna-Aceves, "A simple MPLS-based flow aggregation scheme for providing scalable quality of service", Proceedings of SPIE, Quality of Service over Next-Generation Data Network, Volume 4524, Aug. 2001, Pages 91-98
- [40] Y. Wang, Q. Zeng and H. Zhao, "Dynamic survivability in WDM mesh networks under dynamic traffic", Photonic Network Communications, Volume 6, Issue 1, July 2003, Pages 5-24
- [41] O.J. Wasem, "Optimal Topologies for Survivable Fiber Optic Networks Using SONET Self-healing Rings", Proceedings IEEE GLOBECOM'91, Volume 3, Nov. 1991, Pages 2032-2038
- [42] K. Wu, L. Valcarengi, and A. Fumagalli, "Restoration schemes with differentiated reliability", Communications 2003, ICC 2003. IEEE International Conference on, Volume 3, May 2003, Pages 1968-1972
- [43] Y. Xiong, et al., "Achieving fast and bandwidth-efficient shared-path protection", IEEE Journal of Lightwave Technology, Volume 21, No. 2, February 2003, Pages 365-371
- [44] D. Xu, C. Qiao and Y. Xiong, "Protection with Multi-Segments (PROMISE) in Networks with Shared Risk Link Group (SRLG)", 40th Annual Allerton Conference on Communication, 2002
- [45] Bellcore, SR-NWT-001756, "Automatic Protection Switching for SONET", Issue 1, October 1990
- [46] ANSI, "Fiber Distributed Data Interface (FDDI) – Token Ring Media Access Control (MAC)", ANSI X3.139-1987, 1987
- [47] IEEE 802.17, "Resilient Packet Ring Working Group", <http://www.ieee802.org/17/>.
- [48] Bellcore, GR-1230-Core, "SONET Bidirectional Line-Switched Ring Equipment Generic Criteria", Issue 2, November 1995
- [49] Bellcore, GR-1400-Core, "SONET Dual-Fed Unidirectional Path Switched Ring (UPSR) Equipment Generic Criteria", Issue 1, Revision 1, October 1995

- [50] C.V. Saradhi, M. Gurusamy and L. Zhou, "Reliability-Constrained Least-Cost Routing in Multihop Networks", Proceedings, DRCN-2003, October, 2003, Pages 197-202
- [51] N.C. Hock, "Queueing Modeling Fundamentals", ISBN 0471968196, 1996, Pages 116
- [52] K.W. Ross, "Multiservice Loss Models for Broadband Telecommunication Networks", Springer, 1995, ISBN 3-540-19918-7
- [53] W.D. Grover and M. Clouqueur, "Availability Analysis of Span-restorable Mesh Networks." IEEE Journal in Selected Areas in Communications, May 2002
- [54] A.B. McDonald and T. Znati, "A Mobility Based Framework for Adaptive Clustering in Wireless Ad-Hoc Networks". IEEE Journal in Selected Areas in Communications (JSAC)), 17(8). pp. 1466-1487, August 1999