RISK-BASED SURVIVABLE NETWORK DESIGN

by

Korn Vajanapoom

B.E. in Electrical Engineering, Chulalongkorn University, 1998

M.S. in Telecommunications, University of Maryland at College Park, 2002

Submitted to the Graduate Faculty of

The School of Information Sciences in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

University of Pittsburgh

2008

UNIVERSITY OF PITTSBURGH

SCHOOL OF INFORMATION SCIENCES

This dissertation was presented

by

Korn Vajanapoom

It was defended on

July 17, 2008

and approved by

David Tipper, Ph.D., Associate Professor, School of Information Sciences

Richard Thompson, Ph.D., Professor, School of Information Sciences

Deep Medhi, Ph.D., Professor, CSEE, UMKC

Prashant Krishnamurthy, Ph.D., Associate Professor, School of Information Sciences

Bjorn Jager, Ph.D., Associate Professor, Dept. of Informatics, Molde University

Dissertation Advisor: David Tipper, Ph.D., Associate Professor, School of Information Sciences

RISK-BASED SURVIVABLE NETWORK DESIGN

Korn Vajanapoom, PhD

University of Pittsburgh, 2008

Communication networks are part of the critical infrastructure upon which society and the economy depends; therefore it is crucial for communication networks to survive failures and physical attacks to provide critical services. Survivability techniques are deployed to ensure the functionality of communication networks in the face of failures. The basic approach for designing survivable networks is that given a survivability technique (e.g., link protection, or path protection) the network is designed to survive a set of predefined failures (e.g., all single-link failures) with minimum cost. However, a hidden assumption in this design approach is that the sufficient monetary funds are available to protect all predefined failures, which might not be the case in practice as network operators may have a limited budget for improving network survivability. To overcome this limitation, this dissertation proposed a new approach for designing survivable networks, namely; risk-based survivable network design, which integrates risk analysis techniques into an incremental network design procedure with budget constraints.

In the risk-based design approach, the basic design problem considered is that given a working network and a fixed budget, how best to allocate the budget for deploying a survivability technique in different parts of the network based on the risk. The term risk measures two related quantities: the likelihood of failure or attack, and the amount of damage caused by the failure or attack. Various designs with different risk-based design objectives are

considered, for example, minimizing the expected damage, minimizing the maximum damage, and minimizing a measure of the variability of damage that could occur in the network.

In this dissertation, a design methodology for the proposed risk-based survivable network design approach is presented. The design problems are formulated as Integer Programming (InP) models; and in order to scale the solution of models, some greedy heuristic solution algorithms are developed. Numerical results and analysis illustrating different risk-based designs are presented.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PREFACE

Firstly and most importantly, I would like to express my deepest gratitude to my advisor, Dr. David Tipper. Without his guidance, encouragement, support, and understanding during my entire PhD study, this dissertation would not be possible. His profound comments have guided the direction of my research to stay on the right track until this work is finished. I am also very thankful for his financial supports through numerous research fundings, including the grants from National Science Foundation (NSF), National Institute of Standards (NIST), and Bechtel Bettis.

I would also like to thank the members of my dissertation committee: Dr. Deep Medhi at the University of Missouri at Kansas, Dr. Bjorn Jager at the Molde University in Norway, Dr. Richard Thompson, and Dr. Prashant Krishnanmurthy at the Telecommunications Program, University of Pittsburgh, for their expertise and valuable comments to help improve my research.

I am also obliged to the Telecommunications Program at the University of Pittsburgh for a financial support through a number of graduate student assistantship during my entire PhD study.

I also owe thanks to many colleagues at the Telecommunications Program who have helped me during my study at Pitt, particularly Mr. Tae-Hoon Kim, who has been my office mate over the last few years. I would also like to thank all Thai students in the city of Pittsburgh for their friendship during the time that I am far away from home.

Lastly, I would like to thank all of my family members, my father Mr. Nirach Vajanapoom, my mother Mrs. Ratanasri Vajanapoom, and my only sister Ms. Panpilai Vajanapoom. Their unlimited love, support, and understanding are the biggest factor for my success today. In particular, I would also like to dedicate this dissertation to the memory of my beloved father who passed away while I was pursuing the PhD degree. Now, his will for me to obtain the highest education is completed.

1.0 INTRODUCTION

Communication networks are part of the critical infrastructure upon which society and the economy depend. Therefore, it is crucial for the networks to survive failures and physical attacks, and continue to provide critical services. Survivability techniques are deployed to ensure the functionality of communication networks in the face of failures and physical attacks. A number of survivability techniques have appeared in the literature [1-45] for various network technologies, such as Multi-Protocol Label Switching (MPLS), ATM, SONET, and Wavelength Division Multiplexing (WDM) optical networks.

1.1 SURVIVABILITY TECHNIQUES

A common approach for survivability techniques deployed in communication networks is based on the use of backup paths to carry the affected traffic in the event of network failures. Survivability techniques can be classified into different schemes as presented in Figure 1.1 [1, 4-6]. The classification includes link-based or path-based schemes, protection or restoration schemes, and dedicated-backup or shared-backup protection schemes. The differences among these survivability schemes include their capacity efficiency, and level of resiliency to multiple failures. The classification is explained as follows.

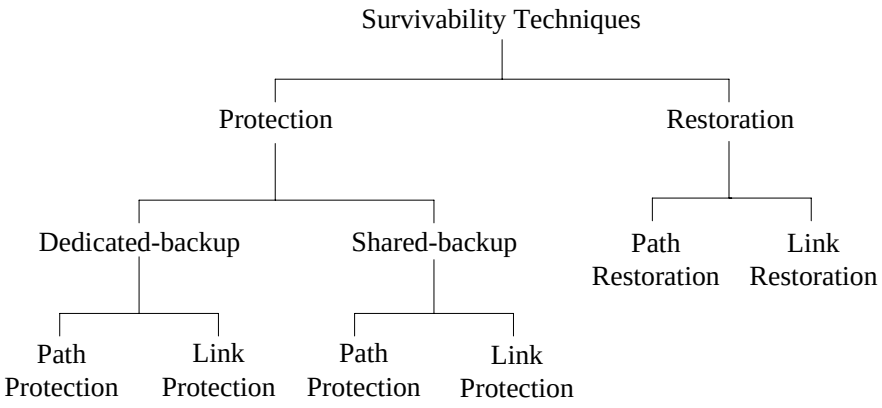


Figure 1.1 Classification of survivability techniques

1.1.1 Link-based and Path-based Schemes

Survivability techniques can be classified into a link-based scheme or a path-based scheme based on the scope of the protected entity (i.e., a link or a path). In the link-based scheme, the backup path (BP) is provided between the two end nodes of the protected link to carry the affected traffic from the protected link in the event of its failure. On the other hand, in the path-based scheme the backup path is provided end-to-end between source and destination nodes of the connection to carry the traffic between two end nodes when the working path (WP) fails. The link-based and the path-based schemes are illustrated in Figure 1.2 (a) and (b), respectively.

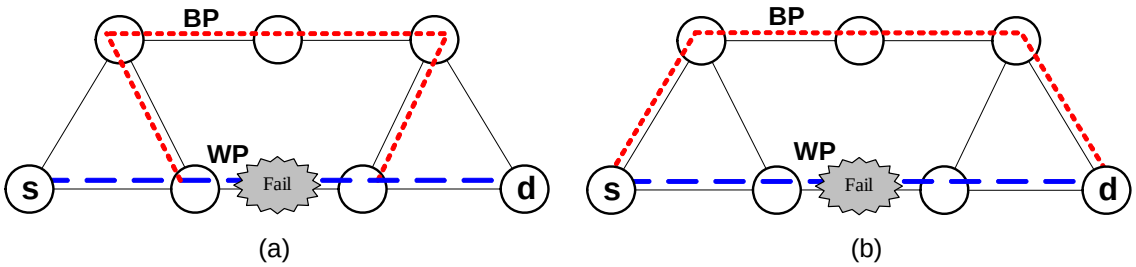


Figure 1.2 (a) link-based scheme and (b) path-based scheme

Typically, the path-based scheme is more spare capacity efficient than the link-based scheme due to its higher flexibility in choosing the backup routes [1, 4, 6-9, 14, 25]. However, the path-based scheme is more susceptible to multiple-link failures because it usually has a longer backup path, and its protected path is also longer than a protected link.

1.1.2 Protection and Restoration Schemes

The survivability techniques can also be classified as a protection or a restoration scheme, depending on when the routes of backup paths are determined. In the protection scheme, the backup routes are predetermined in advance before a failure occurs. To survive any single-link failure, each predetermined backup path must be link-disjoint from its corresponding working path. In contrast, in the restoration scheme the backup routes are computed in real time upon failure notification. The backup paths can utilize any available spare capacity that is left over in the network following the failure. Once the route is computed, the backup path is then established.

The restoration approach is more spare capacity efficient [1, 4, 7], and more flexible to react to different failure scenarios than the protection technique. This is due to its ability to dynamically find backup paths after a failure occurs (i.e., a failure location is known prior to computing the backup routes), and its ability to utilize any available spare capacity in the network, as compared to the predetermined backup routes and pre-assigned spare capacity in the protection scheme.

1.1.3 Dedicated-backup and Shared-backup Protection Schemes

Protection schemes can be further classified as dedicated-backup protection or shared-backup protection, depending on whether spare capacity sharing among backup paths is allowed or not. In dedicated protection, spare capacity allocated along a backup path is dedicated to that backup path only and cannot be used for failure recovery of any other protected links or paths. Whereas in shared-backup protection, backup paths can share spare capacity on a common backup link given that their corresponding protected links or protected paths are not expected to fail at the same time. Spare capacity sharing among backup paths also implies that the backup paths in the shared-backup protection can only be established after a failure.

Figure 1.3 illustrates spare capacity sharing. Since working path 1 (WP1) and working path 2 (WP2) are link and node-disjoint, they are not expected to fail at the same time under a single-link and single-node failure assumption; therefore their backup paths (BP1 and BP2) can share spare capacity on a common link 4-5. Through spare capacity sharing, the amount of spare capacity required on link 4-5 is equal to the maximum value of the spare capacity required by BP1 and BP2, where as in the dedicated-backup protection the amount of spare capacity required on link 4-5 is equal to the sum of spare capacity required by BP1 and BP2.

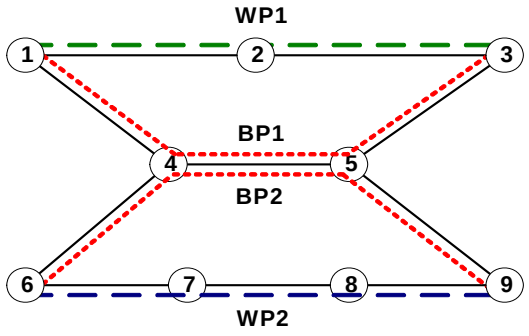


Figure 1.3 Shared-backup protection: spare capacity sharing between BP1 and BP2 on link 4-5

Through spare capacity sharing, the shared-backup protection scheme is more capacity efficient than the dedicated-backup protection scheme [1, 4, 6-7, 16-17, 25]. However, the shared-backup protection is more vulnerable to multiple-link failures in which predetermined backup paths are competing for shared spare capacity which is not sufficiently allocated in the network under a multiple-link failure event [16].

1.2 BASIC APPROACH FOR SURVIVABLE NETWORK DESIGN

The basic approach for designing survivable networks in the literature is that for a given network technology and a given survivability technique (e.g., link protection, shared backup path protection, path restoration, etc.), a network is designed to survive a set of predefined failures, (e.g., all single-link failures), with minimum cost. This basic design approach involves determining an allocation of spare capacity in the network and an assignment of backup routes to minimize the cost. A number of optimization formulations and heuristic algorithms have been proposed for solving minimum-cost survivable network design problems for different network technologies and different survivability techniques [1, 2, 6-25]. However, a limitation of this minimum-cost design approach comes from a hidden assumption that the sufficient monetary funds are available to protect all predefined failures. In practice, many network operators have a very limited budget for improving network survivability, (e.g., a quarterly capital expenditure budget). This is especially true in access networks and edge service providers (e.g., Tier 3 ISPs). Typically, they have to build out the survivable network in pieces in an incremental manner based on a chronological sequence of budgets. In addition, another limitation of the minimum-cost design is that this design approach treats all failures equally without considering the

variability in failure impacts and likelihood. Therefore, these require a new design approach which takes budget limitations and the variability in impacts and likelihood of failures directly into consideration; and this is one of the motivations of this dissertation.

1.3 RISK APPROACH FOR SURVIVABLE NETWORK DESIGN

Due to the limitations of basic survivable network design approach described in Section 1.2, in this dissertation we propose a new approach for designing survivable networks based on integrating risk analysis techniques into an incremental network design procedure with budget constraints. Risk analysis is widely used in engineering, and economics [52-54]. In engineering fields, the term risk accounts not only for a probability of failure but also for a degree of damage resulting from the failure. The risk of a failure is commonly evaluated as the product of the failure probability and the magnitude of damage caused by the failure [52]. In communication networks, potential failures, such as fiber cuts and equipment failures (e.g., router, cross connect, line card, etc.) cause a risk to the network. Different parts of the network are associated with different risk levels. This is due to a variation in an unavailability level of various network components. For example, the rate of cable cuts per km of cable in the United States shows an order of magnitude variation based on the geographic location and population density. The Mean Time To Repair (MTTR) network components also varies across different parts of the network based on the failure location. In addition, failures in some parts of the network cause a higher magnitude of damage than the others. For example, failure of an optical fiber carrying critical supervisory control and data acquisition (SCADA) traffic for the electrical power grid can result in more societal damage than a fiber carrying web or entertainment traffic. Moreover, different

parts of the network require different costs for deploying a survivability technique. For example, some network links may have longer backup paths than the others depending on the network topology, thus requiring a higher spare capacity cost. Observing that the risk level and the survivability cost vary across the network infrastructure, therefore for a given budget, network operators need to carefully determine a budget allocation for deploying network survivability in different parts of the network. This is the design problem we consider in the risk-based survivable network design approach proposed here.

At any capital expenditure investment point, the basic design problem considered is given a working network and a fixed budget, how best to spend the money for deploying a survivability technique in different parts of the network based on the risk. Many different design objectives can be considered in the risk-based design approach, for example minimizing the expected damage value, minimizing the variability of damage, or minimizing the maximum damage that could occur in the network.

The components of the risk-based design approach are a risk assessment and a risk-based investment strategy. The risk assessment is a process of quantifying the risk associated with failures in the network. The assessment is achieved by using probability techniques and understanding of failure relationships in the network. The risk-based investment strategy is used to determine the best budget allocation for deploying a survivability technique in different parts of the network based on the risk criteria.

1.4 PROBLEM STATEMENT

In responding to a need for an approach for incrementally designing survivable networks with budget constraints, a risk-based survivable network design technique is proposed in this dissertation. The basic design problem considered in the risk-based design approach is:

Given a working network and a fixed budget, how best to allocate the budget for deploying a survivability technique in different parts of the network based on the risk?

1.5 CONTRIBUTIONS

The contributions of this dissertation are twofold. First, this dissertation proposes a new design approach which is suited to an incremental design of survivable networks with budget constraints and variability in the damage and likelihood of failures, namely; risk-based survivable network design. Then, based on the proposed risk-based design approach, this dissertation presents solution methods, numerical results, and analysis for different risk-based design formulations. Four risk-based designs are considered in the dissertation: minimum-risk design, min-max damage design, min-max risk design, and minimum-RMS damage design. These design problems are considered for the first time in literature. The Integer Programming (InP) formulations for each design problem with link protection and path protection are presented. However, the minimum-RMS damage design is solved by the proposed greedy heuristic algorithm due to its nonlinearity.

Based on the numerical results, various aspects of the risk-based design approach are disclosed. First, the results exhibit a convexity in the risk curve, and secondly provide

comparison of path protection and link protection based on the risk. The dissertation also presents a cost-benefit analysis which demonstrates whether the cost for providing network survivability is justified by the reduction in risk level, and determines the optimal budget value which maximizes the benefit of an investment in network protection. The dissertation also provides a proof that if the risk curve is convex, there always exists an optimal budget value.

The dissertation shows one advantage of the risk-based design approach over the conventional minimum-cost design approach in that it allows a tradeoff between the survivability cost and the network risk level. In addition, the dissertation shows the ability of the risk-based design approach to provide differential classes of availability or protection to different traffic classes.

Lastly, the dissertation presents the advantages and disadvantages of the four risk-based designs considered based on various measures including the expected damage, the maximum damage, the variability of damage, and the probability distribution of damage.

1.6 ORGANIZATION

The remainder of this dissertation is organized as follows: Chapter 2 provides a literature review on different approaches for survivable network design, along with discussion of their limitations, and comparisons with the proposed risk-based survivable network design approach. Chapter 3 presents the methodology for risk-based survivable network design. The basic risk-based survivable network design approach, namely the minimum-risk survivable network design, is presented in the chapter. Chapter 4 presents and compares various risk-based survivable network design objectives. The min-max damage survivable network design, the min-max risk survivable

network design, and the minimum-root mean square (RMS) damage survivable network design are discussed in this chapter. Lastly, Chapter 5 gives a summary and contributions of this dissertation along with future research directions.

2.0 LITERATURE REVIEW

This chapter presents a literature review on survivable network design. Different survivable network design approaches are discussed, and compared to the proposed risk-based survivable network design. A review of other related literature is also presented.

2.1 MINIMUM-COST SURVIVABLE NETWORK DESIGN

A large amount of literature on survivable network design has appeared in recent years. The basic design approach in the literature is that for a given survivability technique, the network is designed to survive a set of predefined failures (e.g., all single-link failures, or all single-node failures) with minimum cost. This minimum-cost design involves determining an allocation of spare capacity in the network and an assignment of backup routes to minimize the cost. The works in [8, 9] provide Integer Linear Programming (ILP) formulations to determine the minimum-cost capacity allocation and route assignment for a network using link restoration and path restoration to survive all single-link failures. The formulations can be used for minimizing the amount of spare capacity only, or jointly optimizing both working and spare capacity. In [10, 11], the minimum-capacity ILP formulation for a link-restorable network is extended to include dual-link SRLG failures, where SRLG is a group of links that are susceptible to simultaneous failures. The work also shows the effect of the design for dual-link failures on the spare capacity

requirement. Whereas, the minimum-cost link restoration design in [12] also takes the hop limit of backup routes into consideration. In [13], a minimum-capacity design to protect against node failures using path restoration is considered. In addition, some algorithms have been proposed for solving the minimum-capacity link restoration and path restoration design problems, such as in [9, 12, 14].

For networks with Shared-Backup Path Protection (SBPP), the basic minimum-capacity ILP formulations are provided in [15-18]. The formulation is extended for single-node failures in [19], single-duct failures in [24], arbitrary failures in [15], and two-layer networks in [20]. A greedy-based heuristic technique, called Successive Survivable Routing (SSR), to provide good near optimal solutions is proposed in [15]. A simulated annealing heuristic is presented in [21]. For networks with shared-backup link protection, the minimum-cost ILP formulations are presented in [6, 22-23]; and some algorithms are proposed in [22-23].

For a dedicated-backup protection scheme, an ILP formulation to jointly minimize both spare and working capacity is presented in [6, 24]. Alternatively, working and backup routes can be determined by using Bhandari's algorithm [26], which finds a pair of link-disjoint working and backup paths between a source and a destination node with minimum cost.

In all of the above minimum-cost survivable network designs, a common assumption is that the sufficient monetary funds are available to protect all predefined failures. This is fundamentally different from our proposed risk-based survivable network design approach in which the monetary funds are limited, and the network must be designed for a given budget based on the risk consideration.

2.2 AVAILABILITY-BASED SURVIVABLE NETWORK DESIGN

Apart from the capacity cost aspect, a number of studies in literature also consider the failure probability of network components, or an availability aspect of survivable networks.

An availability evaluation of connections in a network with different types of survivability techniques has been considered in the literature. For connections with dedicated protection, a connection availability calculation is similar to an availability calculation of series and parallel systems; and precise closed-form models are available. However, availability evaluations in networks with restoration or shared-backup protection are much more complex, due to spare capacity sharing in both schemes, and flexibility in choosing backup routes in the restoration scheme (i.e., a backup path is not restricted to a predefined route). Therefore, precise closed-form models for connection availability are not available; and a number of approximating models have been proposed in literature (e.g., [27] for link restoration, [28] for path restoration, and [16, 29-30] for Shared-Backup Path Protection (SBPP)). Comparative studies on connection availability for different survivability techniques are also presented in [16, 29-30]. Furthermore, the works in [31-34] present a tradeoff between the minimum cost for providing network survivability and the level of connection availability that can be achieved for different survivability techniques; in order to measure a relationship between the two quantities, a metric called availability gain is proposed in [31, 34] as a ratio between an increase in availability and an increase in backup capacity compared to the unprotected case. In contrast to these works, our work shows a tradeoff in terms of the cost of network survivability and the level of risk reduction. A cost-benefit analysis is considered in our work to show whether the cost for providing network protection is justified by an amount of risk reduction. In addition, in the above literature, an availability evaluation is performed after the networks were designed (e.g., using

the minimum-cost design). This is different from our risk-based design approach in which the failure probability and the availability evaluation are incorporated into the design procedure.

Network design problems which incorporate availability into their design objectives are also considered in some literature. The works in [36, 37] study the maximum-availability network design problems. The design approach in [36] consists of two phases. The first phase determines the routes for each connection with maximum availability using a dedicated path protection with no cost constraint. In the second phase, the design is aimed at minimizing the network cost while keeping the availability level the same, or decreased by a prefixed margin factor. The work in [37] determines maximum-availability routes with no cost constraint for each unprotected or dedicated path protection connection using a modified Dijkstra's algorithm. This work is similar to our risk-based design approach in which a failure probability or an availability is considered as a part of design objective; however the difference is that the risk based design approach considers not only the failure probability, but also the amount of damage resulting from the failure. Also, the risk based design takes into a consideration a budget constraint which imposes a limit on the amount of spare capacity in the network.

In [38-41], an availability-constrained provisioning problem is studied. This problem is to determine the minimum-cost routes for each connection while satisfying the minimum requirement of connection availability by, if necessary, applying a dedicated path protection. This study is similar to our work in which protection is applied only to some connections. However, the difference is that in these studies, cost is an objective function to be minimized, and connection availability is a constraint, whereas in the risk-based design problem the design objective is to minimize the risk function, subject to a budget constraint. Also, the risk-based approach considers the damage of various failure cases in the provisioning of spare resources.

The work in [35] provides an analysis of the survivability cost and the availability that can be achieved for different partially fault-tolerant network configurations. This is similar to our work in that networks are partially protected (i.e., only some network links are protected); however the difference is that in this work, a determination of which network parts to be protected is subjectively given to the analysis without considering a budget constraint; whereas in the risk-based design approach an investment strategy is used to determine which parts of the network to be protected for a given budget and risk-based objective.

2.3 OTHER NETWORK DESIGN APPROACHES

In the risk-based design approach, networks are designed based on a given budget. Other budget-constrained network design problems are also studied in literature [2, 10]. By moving the cost from an objective function in the minimum-cost design to a constraint, it allows the network to be designed according to another objective function. For example, in [2] the network is designed to maximize the network throughput for a given capacity budget. Unlike the risk-based design approach, this design's objective function is not related to a survivability aspect of the networks. The most closely related work to our proposed risk-based design approach is the work in [10], which determines a spare capacity allocation to maximize a restoration level for a given spare capacity budget using link restoration. However, this design approach is different from the risk-based design approach in that its design objective considers only the restoration level, whereas the risk-based design approach considers both the failure probability and the damage caused by the failure.

The proposed risk-based design approach is based on an incremental design in which a Greenfield condition is not assumed, and the network given to the design problem might be partially fault-tolerant. Studies on incremental network design also appear in literature. In [2], the design determines an incremental expansion of network working capacity to support the growth of traffic demands. In contrast, in the risk-based design approach the spare capacity rather than the working capacity is incrementally extended to improve network survivability. The incremental design in [42-43] considers an augmentation of both working and spare capacity to support the future demands. However, the difference from our risk-based design approach is that in the risk-based design, the network is incrementally designed based on a given fixed budget amount rather than the growth of traffic demands, and a risk-based objective function is used.

Lastly, our risk-based design problem is related to the redundancy allocation problem considered in [51] which determines how to allocate a redundancy to different parts of the systems in order to achieve the most effective result for a given budget. Nevertheless, our risk-based design problem is considered specifically in the context of network survivability which is distinctive from other contexts. For example, it includes a routing sub-problem to determine the routes of backup paths which in turn affects the cost of redundancy and the network risk level.

3.0 RISK-BASED SURVIVABLE NETWORK DESIGN

This chapter presents the design methodology for the risk-based survivable network design approach. The risk-based design procedure is presented in Section 3.1, which explains the process, inputs and outputs of the risk-based design. The two components of the risk-based design, namely; a risk assessment and a risk-based investment strategy, are presented in Section 3.2 and 3.3, respectively. The first risk-based survivable network design considered, the minimum-risk survivable network design, is presented in Section 3.4. Two solution approaches for solving the minimum-risk design problem: (1) an Integer Programming (InP) approach, and (2) a heuristic approach, are presented in Section 3.4.1 and 3.4.2, respectively. An extension of the minimum-risk design approach to networks with multiple classes of traffic, and an incremental network design are presented in Section 3.5 and 3.6, respectively. Numerical results illustrating the minimum-risk design approach are presented and discussed in Section 3.7. Lastly, Section 3.8 concludes this chapter.

In this dissertation, we consider two standard survivability techniques: dedicated-backup link protection and dedicated-backup path protection. Also, for ease of presentation the proposed design approach is explained in the context of WDM optical networks with only cable cut failures. However, the methodology is general in nature and can be applied to other connection-oriented network technologies and other failure/attack conditions.

3.1 RISK-BASED DESIGN PROCEDURE

This section explains the design procedure of the risk-based survivable network design approach. Figure 3.1 illustrates a design process along with inputs and outputs of the risk-based design approach. First, a network topology which includes all existing network links and nodes, and an end-to-end traffic demand matrix which indicates the source and destination nodes and the traffic rate for each demand are given to the design. The working network includes the routes for all the traffic demands, which can be based on any design objective, for example, minimizing a cost, minimizing an end-to-end delay, maximizing network utilization [2], shortest hop, etc.

In the design procedure used here, the working network along with a survivability technique, a survivability cost model, and a fixed budget are given to the risk-based survivable network design. In link protection, the risk-based design determines which network links to protect, and the corresponding backup routes for a given budget based on the risk; whereas in path protection, the risk-based design determines which end-to-end paths to protect, and the routes of backup paths for a given budget based on the risk. Various risk-based design objectives are possible in the risk-based design approach. The minimum-risk design, the min-max damage design, the min-max risk design, and the minimum-RMS damage design are discussed in Section 3.4, 4.1, 4.2, and 4.3, respectively. A solution algorithm (e.g., branch and bound algorithm) is then applied to the design problem to determine the survivable network. A risk-based incremental survivable network design can also be applied to the survivable network to further reduce the network risk based on a sequence of budgets as discussed in Sections 3.6, 3.7.5 and 3.7.6.

A design assumption used in this dissertation is that the survivability cost is considered only in term of a spare capacity, and a unit cost of spare capacity on any link is a function of a

cable length (i.e., a unit of spare capacity on a longer cable is more expensive than a unit of spare capacity on a shorter cable). Also, the budget is considered only in term of the maximum spare capacity investment. The spare capacity can only be invested on the existing network links; adding new links to the current network topology in order to support backup paths is not included in the current formulation but it is relatively straightforward to extend the formulation to study this case. In Addition, it is assumed that each OXC has full wavelength conversion capability, so that the wavelength continuity constraint can be ignored.

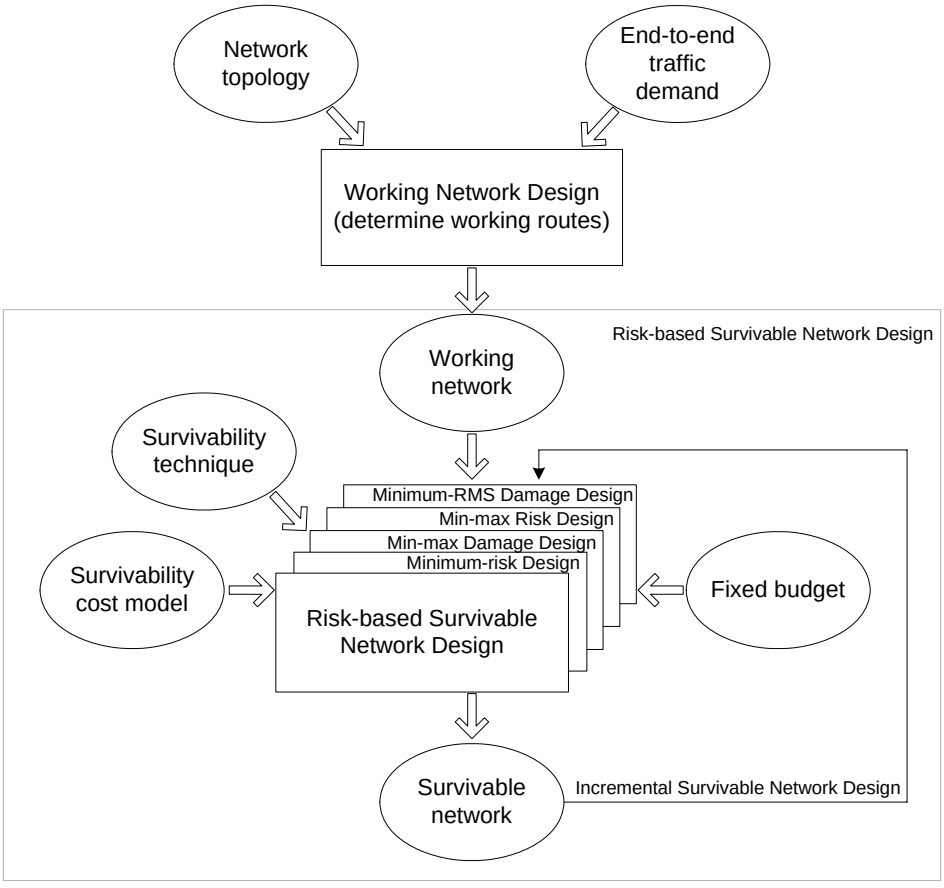


Figure 3.1 Risk-based survivable network design procedure

3.2 RISK ASSESSMENT

As noted earlier, the risk-based survivable network design approach has two components namely: a risk assessment and a risk-based investment strategy. The two components are interrelated since an achievement of the investment's goal is checked by the risk assessment. This section discusses the risk assessment. The notation used in this section is presented in Table 3.1

Table 3.1 Notation used in Section 3.2

L	Set of links or cables
R	Set of lightpaths
S	Set of network states
$\boldsymbol{P} = \{p_{r,i}\}_{\|R\| \times \|L\|}$	$p_{r,i} = 1$ if lightpath r uses link i in its working path, and = 0 otherwise
$\boldsymbol{m} = \{m_r\}_{\|R\|}$	m_r is the data rate (bits/s) of lightpath r
u_i	Unavailability of cable i
$\boldsymbol{STATE} = \{state_{s,i}\}_{\|S\| \times \|L\|}$	$state_{s,i} = 1$ if cable i is cut in network state s, and = 0 otherwise
$\boldsymbol{stateprob} = \{stateprob_s\}_{\|S\|}$	$stateprob_s$ is the probability of network state s
d_r	Damage caused by a failure of lightpath r
$damage_s$	Damage occurring in network state s
$risk_s$	Amount of risk associated with network state s
$totalrisk$	Total risk to the network
$\boldsymbol{1}_{\mathrm{M} \times \mathrm{N}}$	An $\mathrm{M} \times \mathrm{N}$ matrix with only elements "1"
TI	Time Interval over which risk/damage assessed (e.g. 31,536,000 sec/year)

The following notation is used in the link protection case only:	
$\boldsymbol{bp} = \{bp_i\}_{\|L\|}$	bp_i = 1 if link i is protected, and = 0 otherwise
$\boldsymbol{Q} = \{q_{i,j}\}_{\|L\| \times \|L\|}$	$q_{i,j}$ = 1 if link i is protected and its backup path traverses link j, and = 0 otherwise
The following notation is used in the path protection case only:	
$\boldsymbol{bp} = \{bp_r\}_{\|R\|}$	bp_r =1 if lightpath r is protected, and = 0 otherwise
$\boldsymbol{Q} = \{q_{r,j}\}_{\|R\| \times \|L\|}$	$q_{r,j}$ = 1 if lightpath r is protected and its backup path traverses link j, and = 0 otherwise

Risk assessment is a process of quantifying the amount of risk associated with the potential hazards (i.e., failures, attacks, accidents, etc) in the network. Here, the focus is on failures only. Risk measures two quantities related to failures: the probability of failure and the amount of damage resulting from the failure. The risk of failure is defined as the probability of failure times the damage from failure [52]; this is the traditional definition in engineering and IT security. In a network with n failure-prone components, each of which could be in either a failure state or a non-failure state, there are a total of 2^n possible network states. Each network state uniquely identifies a set of components that are in a failure state and a non-failure state. Let S denotes the set of network failure states indexed by s. The risk associated with network state s, denoted by $risk_s$, is equal to a product of the probability of network being in state s, denoted by $stateprob_s$, and the amount of damage occurring in network state s, denoted by $damage_s$, as shown in (3.1).

$$risk_s = stateprob_s \times damage_s \tag{3.1}$$

Since the network states are mutual exclusive to each other (i.e., no two network states can occur at the same time), the total network risk, denoted by *totalrisk*, can be calculated by

summing the risk associated with each network state $risk_s$ for all network states, as in (3.2) and (3.3).

$$totalrisk = \sum_{s \in S} risk_s \tag{3.2}$$

$$totalrisk = \sum_{s \in S} stateprob_s \times damage_s \tag{3.3}$$

It is important to note that the total risk in (3.3) can also be interpreted as an expected damage value across all network states.

In this dissertation, the risk assessment is illustrated in the context of WDM optical networks. A WDM network consists of Optical Cross Connects (OXCs) interconnected by optical fiber links organized in a mesh topology. An end-to-end connection between a source and a destination OXC is called a lightpath (LP). A lightpath occupies a wavelength on each optical fiber link that it traverses. Potential failures, such as fiber cuts and equipment failures (e.g., OXC, amplifier, etc.) cause a risk to the WDM network. The magnitude of risk that these failures pose to the network can be evaluated by (3.3). In WDM networks, the quantity of interest is the damage associated with each lightpath failure due to network component failures. Therefore, the amount of damage occurring in network state *s* is the sum of damages of all failed lightpaths in network state *s*, as shown in (3.4), where d_r is the amount of damage caused by a failure of lightpath *r*.

$$totalrisk = \sum_{s \in S} stateprob_s \Big(\sum_{\substack{\text{all failed lightpaths } r \\ \text{in network state } s}} d_r \Big) \tag{3.4}$$

The amount of damage caused by the failure of lightpath *r*, or d_r, can be measured in many different ways. If knowledge of the higher layer traffic is available, one can construct a damage metric associated with each lightpath that incorporates the societal effects of the loss of

various traffic. For example, a higher damage value would be placed on emergency communications and SCADA for critical infrastructures. One simple damage measure is the traffic loss rate resulting from the lightpath failure. In this case, the amount of damage caused by a failure of lightpath r (i.e., d_r) for the risk calculation in (3.4) is equal to the data rate of lightpath r (i.e., m_r) as shown in (3.5). In other words, the amount of damage in network state s is equal to the sum of the lost traffic rate of all failed lightpaths in that network state.

$$totalrisk = \sum_{s \in S} stateprob_s \Big(\sum_{\substack{\text{all failed lightpaths } r \\ \text{in network state } s}} m_r \Big) \tag{3.5}$$

If the total risk in (3.5) is multiplied by the time interval TI, for example, TI = 365×24×60×60 = 31,536,000 sec/year, the result is equal to the Expected Loss of Traffic (*ELT*) per year in the network as shown in (3.6).

$$ELT = \mathrm{TI} \sum_{s \in S} stateprob_s \Big(\sum_{\substack{\text{all failed lightpaths } r \\ \text{in network state } s}} m_r \Big) \tag{3.6}$$

Note that the risk calculation in (3.3) is very similar to the network failure performability calculation considered in [45-50], where the network performability is defined as a sum of the product of the state probability and the performability measure (e.g., a connection blocking in circuit switched networks, or an average packet delay in packet switched networks) for all network states.

For each network state, a state probability can be obtained by multiplying together appropriated failure probability and working or non-failure probability of all failure-prone network components. If cable cuts are considered as the only source of failures in the network, and the failures are statistically independent of each other, the probability of network state s can be calculated as in (3.7). Note that in (3.7) L denotes a set of cable links; $state_{s,i}$ represents the

network failure states, where $state_{s,i}$ = 1 if cable i is in a failure state in network state s, and $state_{s,i}$ = 0 otherwise; and u_i denotes the unavailability of cable i. Techniques for the calculation of the unavailability of cables due to cable cuts are well known and are discussed in the Appendix A.

$$stateprob_s = \prod_{i \in L} u_i^{state_{s,i}} (1-u_i)^{1-state_{s,i}} \tag{3.7}$$

Note that the calculation of risk in (3.4)–(3.6) requires the determination of the failed lightpaths in each network state. This process must take into account different configurations of survivability techniques being deployed in the network. In this dissertation, a fault tree, which is a well-developed failure-relationship model commonly used in the risk analysis, is utilized for this purpose.

Fault Tree Model

A fault tree [53-54] is a graphical model that depicts the logical interrelationship of failure events in a system. Here, it is used as a failure model for determining the set of failed lightpaths in each network state. The construction of a fault tree starts with identifying the tree's *root* or *top events* which represent failure events of interest (e.g., lightpath failures in WDM networks). Then it proceeds by seeking out the failure events that contribute to an occurrence of the top events, and connecting these events to the top events by logic gates. A variety of logical relationship gates (e.g., AND, OR, NOT, etc.) and specialized gates (e.g., K out N Voting, etc.) are used to construct the tree. Two types of fundamental logic gates used in the fault tree are an AND gate and an OR gate. An AND gate, symbolized by 

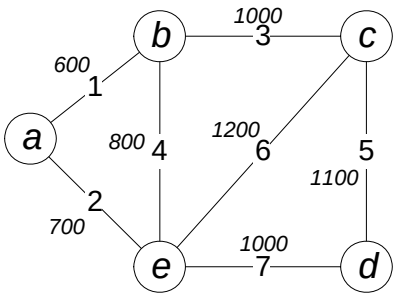
, indicates a situation where the output event occurs if and only if all the input events occur. Whereas, an OR gate, symbolized by 

, is used to indicate that the output event occurs if at least one of the input events occurs. This process repeats until it reaches *basic events*, which are at the lowest level in all branches of the

fault tree, and symbolized by circles. The basic events typically represent initiating failure events (e.g., fiber cuts, and equipment failures) or events that are not further developed in the fault tree model (i.e., underlying failure events that may cause this event to occur are not considered). Once completed, the fault tree provides a failure model, which relates the top events to the basic events via logic gates, and *intermediate events*, represented by rectangles.

Here, the fault tree approach is illustrated by an example using the WDM network in Figure 3.2. For the network in Figure 3.2, we assume that there are 10 bi-directional lightpaths (LPs) between all node pairs in the network. The lightpath routes in the form of a working path link incidence matrix $\boldsymbol{P}$ are given in Figure 3.2, where $\boldsymbol{P} = \{p_{r,i}\}_{|R| \times |L|}$ and $p_{r,i} = 1$ if lightpath r uses link i in its working path, and = 0 otherwise. A fault tree model for a WDM network in Figure 3.2 with link protection on link 1 and link 4 is shown in Figure 3.3. Lightpath failures are defined as the top events of the fault tree. A lightpath fails when at least one of the links that the lightpath traverses fails. For example, the event LP3_fail occurs when either the event Link2_fail or the event Link7_fail occurs, or both events occur. Similarly, each link failure event occurs if a corresponding cable cut event occurs. Here, cable cuts are considered as the only basic events of the fault tree; however, it is straightforward to include other network component failures and attacks (e.g., OXC failures, and optical amplifier failures) into the set of basic events. With link protection, a link is determined to be in a failure state only if both the link itself (i.e., the working link), and its backup path fail. In this example, the backup path of link 1 traverses network links 2, 3 and 6, whereas the backup path of link 4 traverses network links 1 and 2, as illustrated in Figure 3.3. Link protection introduces an additional AND gate located under a failure event of the link being protected, which makes an occurrence of the link failure event less likely. Note that in this protection technique it is assumed that the backup path is not

protected by a link protection mechanism implemented at any links that the backup path traverses.



$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Figure 3.2 Network 1 ($|N| = 5$, $|L| = 7$) and working route matrix ***P***

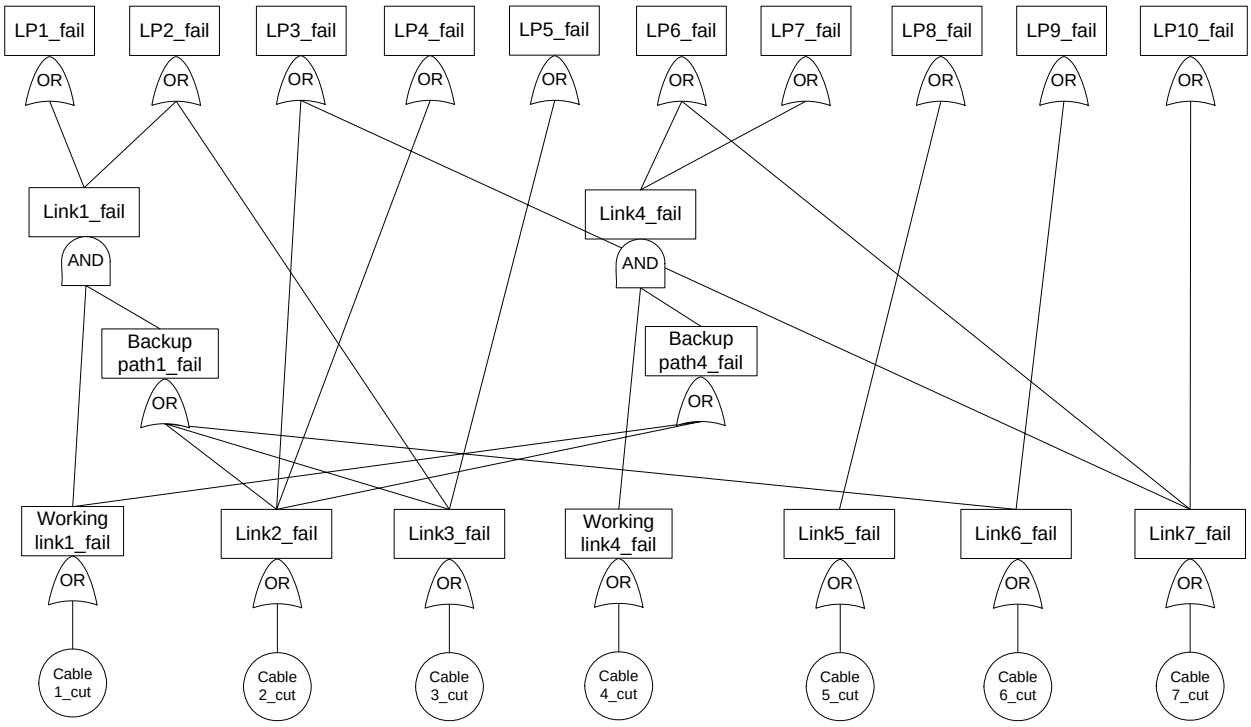


Figure 3.3 Fault tree model for a WDM network in Figure 3.2 with link protection on links 1 and 4.

From the fault tree model, a set of failed lightpaths in each network state can be determined by assigning the corresponding failure states (i.e., occurring or not-occurring) to all basic events in the fault tree, and evaluating the logic of the tree up to the top events.

Combining the fault tree logic with the risk calculation in (3.4), a closed-form formula for determining the amount of network risk in the cases of no protection, link protection, and path protection, can be obtained as given in (3.8), (3.9), and (3.10), respectively. Here, the formulas are in matrix form. Note in these formulas, $\circ$ is a Hadamard (Schur) product, obtained by multiplying together corresponding elements in each matrix [55], and $\odot$ is a binary matrix multiplication operator, which modifies general addition 1+1 = 2 to Boolean addition where 1+1 = 1 [56]. In (3.8)–(3.10), a binary matrix $\boldsymbol{STATE} = \{state_{s,i}\}_{|S| \times |L|}$ is used to list all network states, where $state_{s,i}$= 1 if cable i is in a failure state in network state s, and $state_{s,i}$ = 0 otherwise. A matrix ***STATE*** for the WDM network example in Figure 3.2 is shown in Figure 3.4. In this network example, there are 7 network links, and since cable cuts are considered as the only sources of failures, therefore there are a total of 2^7 = 128 possible network failure states. Moreover, a column vector $\boldsymbol{stateprob} = \{stateprob_s\}_{|S|}$ is used to list network state probabilities, where $stateprob_s$ is the probability of a network state s, which is calculated by (3.7). A vector ***stateprob*** for the WDM network example in Figure 3.2 is also shown in Figure 3.4 (using CC = 450 km and MTTR = 24 hours for u_i calculations as discussed in Appendix A). Column vector $\boldsymbol{d} = \{d_r\}_{|R|}$ represents lightpaths' damage levels, where d_r is the amount of damage caused by the failure of lightpath r. For risk calculation in the link protection case in (3.9), matrix $\boldsymbol{bp} = \{bp_i\}_{|L|}$ indicates which links are being protected, where bp_i = 1 if link i is protected, and = 0 otherwise, whereas backup path link incidence matrix $\boldsymbol{Q} = \{q_{i,j}\}_{|L| \times |L|}$ represents each lightpath's backup route, where $q_{i,j}$ = 1 if link i is protected and uses link j in its backup path, and = 0 otherwise.

Similarly, for risk calculation in the path protection case in (3.10), matrix $\boldsymbol{bp} = \{bp_r\}_{|R|}$ indicates which lightpaths are being protected, where $bp_r = 1$ if lightpath r is protected, and = 0 otherwise, and backup path link incidence matrix $\boldsymbol{Q} = \{q_{r,j}\}_{|R| \times |L|}$ represents the backup routes, where $q_{r,j} = 1$ if lightpath r is protected and uses link j in its backup route, and = 0 otherwise.

Lastly, note that in this work it is assumed that the recovery process is instantaneous (i.e., the down time during the recovery process is negligible), and the network continues to provide service with no disruptions or traffic loss as long as the backup paths are available as in [27].

$$\boldsymbol{STATE} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \vdots & & & & & & \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \qquad \boldsymbol{stateprob} = \begin{bmatrix} 0.96167449 \\ 0.00352585 \\ 0.00411600 \\ 0.00001509 \\ 0.00589081 \\ \vdots \\ 3.2131 \times 10^{-14} \\ 3.7509 \times 10^{-14} \\ 1.3752 \times 10^{-16} \end{bmatrix}$$

Figure 3.4 Matrix ***STATE*** and vector ***stateprob***

$$totalrisk_{no\_protection} = \boldsymbol{stateprob}^T \times \left(\boldsymbol{STATE} \odot \boldsymbol{P}^T \right) \times \boldsymbol{d} \tag{3.8}$$

$$totalrisk_{link\_protection} = \boldsymbol{stateprob}^{\mathrm{T}} \times \left\{ \left\{ \boldsymbol{STATE} \circ \left[\left(\boldsymbol{STATE} \odot \boldsymbol{Q}^{\mathrm{T}} \right) + \left(\boldsymbol{1}_{|S| \times |L|} - \boldsymbol{1}_{|S| \times 1} \times \boldsymbol{bp}^{\mathrm{T}} \right) \right] \right\} \odot \boldsymbol{P}^{\mathrm{T}} \right\} \times \boldsymbol{d} \tag{3.9}$$

$$totalrisk_{path\_protection} = \boldsymbol{stateprob}^{\mathrm{T}} \times \left\{ \left(\boldsymbol{STATE} \odot \boldsymbol{P}^{\mathrm{T}} \right) \circ \left[\left(\boldsymbol{STATE} \odot \boldsymbol{Q}^{\mathrm{T}} \right) + \left(\boldsymbol{1}_{|S| \times |R|} - \boldsymbol{1}_{|S| \times 1} \times \boldsymbol{bp}^{\mathrm{T}} \right) \right] \right\} \times \boldsymbol{d} \tag{3.10}$$

3.3 RISK-BASED INVESTMENT STRATEGY

Once the risk have been identified and assessed, the next component in the design approach is a risk-based investment strategy. The risk-based investment strategy is used to manage or reduce the network risk by deploying risk-reduction techniques in the network, subjected to a budget limit. Various techniques for reducing the risk of failures exist. These techniques can be categorized as prevention and recovery techniques and are discussed in turn below.

The prevention techniques seek to reduce the probability of network component failure. In communications networks, this can be achieved by for example, using more reliable network equipments (e.g., more reliable OXCs), backup power supplies, etc. However, improving network components' reliability is sometimes infeasible, or in some situations, even if the most reliable network components are deployed, the desired level of network risk still may not be achieved. Therefore, the recovery techniques are also considered.

Recovery techniques perform a corrective action upon a failure. In other words, these techniques aim at reducing the amount of damage resulting from a failure, rather than reducing the failure probability of network components as do the prevention techniques. In communications networks, these techniques are the same as the survivability techniques discussed in Section 1.1. Typically, in survivability techniques the corrective actions are achieved by providing backup paths to carry the affected traffic in the event of network component failure. Various survivability techniques are also discussed in Section 1.1.

For a given budget, the risk-based investment strategy is used to determine the best budget allocation for deploying risk-reduction techniques in different parts of the network. In this dissertation, the focus is on survivability techniques only, specifically the link and path protection techniques. In the link protection case, an investment strategy is used to determine

which network links to protect and their corresponding backup routes for a given budget; whereas in the path protection case an investment strategy is used to determine which lightpaths to protect and their corresponding backup routes subjected to a budget limit.

3.4 MINIMUM-RISK SURVIVABLE NETWORK DESIGN

The first risk-based design considered in this dissertation is the minimum-risk survivable network design. In this design problem, the working network (i.e., working capacity and working routes of all lightpaths) is given, and the design objective is to minimize the total risk for a given budget by deploying a survivability technique in different parts of the network. The minimum-risk link protection design problem is to determine which network links to protect, and their corresponding backup routes; whereas the minimum-risk path protection design problem is to determine which lightpaths to protect, and their corresponding backup routes.

Two approaches for solving the minimum-risk survivable network design problem are considered in this dissertation. One is based on an Integer Programming (InP) optimization problem formulation, which provides optimal solutions; however its computational time does not scale well with the problem size. Therefore, a heuristic approach, which can approximate the optimal solution in a reasonable time, is also considered.

3.4.1 Integer Programming (InP) Approach

In this section, the minimum-risk survivable network design problems are formulated as 0-1 InP models. In general, there are two different ways to formulate InP models for network-flow

optimization problems; one is based on a node-link model (also known as a node-arc model), and the other one is based on a link-path model (also known as an arc-flow model and an arc-path model) [1-2].

For the minimum-risk design problems, the node-link model determines candidate backup routes through the flow conservation constraints defined in the problem formulation. It considers all eligible routes in the network as candidate routes for each backup path, and does not require a set of pre-computed backup routes. Therefore, the node-link model provides a true optimal solution in a sense that all eligible routes are considered in the optimization problem. On the other hand, the link-path model requires a set of pre-computed routes as candidate backup routes for each backup path. Therefore, solving a link-path InP model provides an optimal solution for a given set of pre-computed backup routes, which is only guaranteed to be the true optimal solution if the set of all possible backup routes is used. The advantage of the link-path model over the node-link model is that one can scale down the number of backup routes considered in the problem, thereby reducing the size of the solution space. As a result, the complexity of the problem and the computational time for solving the problem is reduced. Another advantage of the link-path model is that the set of pre-computed backup routes can be selected in a way that only pre-qualified backup routes are considered in the problem. This is especially important in communications networks such as WDM optical networks where the signal quality is an important factor, and thus the backup path can take only on some specific routes in the network (e.g., limited by distance, signal quality, and latency).

The node-link model and the link-path model for the minimum-risk survivable network design problem are presented in Section 3.4.1.1 and 3.4.1.2 respectively.

3.4.1.1 Node-Link InP Formulations

In this section, the node-link InP formulations for the minimum-risk link protection design problem and the minimum-risk path protection design problem are presented. The notation used in the node-link InP formulations is presented in Table 3.2.

Table 3.2 Notation used in node-link InP formulations

Given:	
N	Set of nodes
L	Set of links or cables
R	Set of ligthpaths
S	Set of network states
$p_{r,i}$	$p_{r,i}$ = 1 if lightpath r uses link i in its working path, and = 0 otherwise
m_r	Data rate (bits/s) of lightpath r
w_i	Amount of working capacity on link i, calculated by $w_i = \sum_{r \in R} p_{r,i} m_r$
$b_{n,i}$	$b_{n,i}$ = 1 if node n is the origin or destination of link i, and = 0 otherwise
$d_{r,n}$	$d_{r,n}$ = 1 if node n is the source or destination of lightpath r, and = 0 otherwise
$state_{s,i}$	$state_{s,i}$= 1 if cable i is cut in network state s, and = 0 otherwise
$stateprob_s$	$stateprob_s$ is the probability of network state s
d_r	Damage caused by a failure of lightpath r
c_i	The unit cost of spare capacity on link i
budget	The budget
K	A large constant used for bounding

$g_{s,r}$	$g_{s,r} > 0$ if a working path for lightpath r fails in network state s, and = 0 otherwise (i.e., $g_{s,r} = \sum_{i \in L} state_{s,i} p_{r,i}$)

Variables:

$damage_s$	Damage occurring in network state s
$totalrisk$	Total risk to the network
$y_{s,r}$	$y_{s,r} > 0$ if lightpath r fails in network state s, and = 0 otherwise
$z_{s,r}$	$z_{s,r} = 1$ if lightpath r fails in network state s, and = 0 otherwise

The following notation is used in the link protection case only:

bp_i	$bp_i = 1$ if link i is protected, and = 0 otherwise
$q_{i,j}$	$q_{i,j} = 1$ if link i is protected and its backup path traverses link j, and = 0 otherwise
$h_{s,i}$	$h_{s,i} > 0$ if a backup path for link i is not available (either link i is not protected, or the backup path fails) in network state s, and = 0 otherwise
$e_{s,i}$	$e_{s,i} > 0$ if link i fails (both working link fails and backup path is not available) in network state s, and = 0 otherwise

The following notation is used in the path protection case only:

bp_r	$bp_r = 1$ if lightpath r is protected, and = 0 otherwise
$q_{r,j}$	$q_{r,j} = 1$ if lightpath r is protected and its backup path traverses link j, and = 0 otherwise
$h_{s,r}$	$h_{s,r} > 0$ if a backup path for lightpath r is not available (either lightpath r is not protected, or the backup path fails) in network state s, and = 0 otherwise

The node-link InP formulation for the minimum-risk link protection design problem is presented in (3.11)–(3.21). The set of decision variables to be determined are the binary variables bp_i, which determines a set of links to be protected, where $bp_i = 1$ if link i is protected and $bp_i =$

0 otherwise, and the binary variables $q_{i,j}$, which specifies the route of the backup path protecting link i, where $q_{i,j} = 1$ if link i is protected and uses link j in its backup path and $q_{i,j} = 0$ otherwise. The objective (3.11) is to minimize the total network risk. Constraint set (3.12) is the flow conservation constraints for backup paths. Constraints (3.13)–(3.16) are the failure state relationships which determine whether lightpath r will fail in network state s, while also taking the link protection being deployed in the network into account. More specifically, constraint set (3.13) determines whether or not the backup path for link i is available in network state s. The backup path for link i might not be available in network state s (i.e., $h_{s,i} > 0$) for two reasons: either the backup path fails due to a cable cut in that network state (i.e., $\sum_{j \in L} state_{s,j} q_{i,j} > 0$), or link i is not protected (i.e., $bp_i = 0$, or $1\text{-}bp_i > 0$). Constraint set (3.14) indicates that link i fails in network state s (i.e., $e_{s,i} > 0$) if and only if both the working link fails (i.e., $state_{s,i} > 0$) and its backup path is not available in that network state (i.e., $h_{s,i} > 0$). Constraint set (3.15) indicates that lightpath r fails in network state s ($y_{s,r} > 0$) if and only if at least one of the links that it traverses fails (i.e., $\sum_{i \in L} e_{s,i} p_{r,i} > 0$). Constraint set (3.16) relates variable $y_{s,r}$ to binary variable $z_{s,r}$. Constraints (3.17)–(3.18) are for the calculation of the risk as in (3.4). That is, constraint set (3.17) calculates the amount of damage in each network state as the sum of damages of all failed lightpaths in that network state; and constraint (3.18) calculates the total network risk as the sum of the product of the state damage and state probability for all network states. Constraint (3.19) is the budget constraint which limits the total spare capacity investment, where c_j is the unit cost of spare capacity on link j, and w_i is the amount of working capacity on link i. Lastly, constraint sets (3.20) and (3.21) express the binary nature of the design and failure variables.

Minimum-risk link protection design problem (Node-link model)

$$\text{Objective: } \min_{bp_i, q_{i,j}} totalrisk \tag{3.11}$$

$$\text{s.t. } \sum_{j \in L} q_{i,j} b_{n,j} = b_{n,i} bp_i \pmod 2, \quad \forall i \in L, \forall n \in N \tag{3.12}$$

$$h_{s,i} = \sum_{j \in L} state_{s,j} q_{i,j} + 1 - bp_i, \quad \forall s \in S, \forall i \in L \tag{3.13}$$

$$e_{s,i} = state_{s,i} h_{s,i}, \quad \forall s \in S, \forall i \in L \tag{3.14}$$

$$y_{s,r} = \sum_{i \in L} e_{s,i} p_{r,i}, \quad \forall s \in S, \forall r \in R \tag{3.15}$$

$$z_{s,r} \mathrm{K} \geq y_{s,r}, \quad \forall s \in S, \forall r \in R \tag{3.16}$$

$$damage_s = \sum_{r \in R} z_{s,r} d_r, \quad \forall s \in S \tag{3.17}$$

$$totalrisk = \sum_{s \in S} stateprob_s damage_s, \quad \forall s \in S \tag{3.18}$$

$$\sum_{i \in L} \sum_{j \in L} c_j w_i q_{i,j} \leq budget \tag{3.19}$$

$$q_{i,j}, bp_i : binary, \quad \forall i \in L, \forall j \in L \tag{3.20}$$

$$z_{s,r} : binary, \quad \forall s \in S, \forall r \in R \tag{3.21}$$

The node-link InP formulation for the minimum-risk path protection problem is presented in (3.22)–(3.32). The two sets of decision variables to be determined are binary variables bp_r, which determines whether to protect lightpath r, where $bp_r = 1$ if lightpath r is protected and $bp_r = 0$ otherwise, and binary variables $q_{r,j}$, which specifies a backup route for lightpath r, where $q_{r,j} = 1$ if ligthpath r is protected and uses link j in its backup path and $q_{r,j} = 0$ otherwise. The objective (3.22) is to minimize the total network risk. Constraint set (3.23) is the flow conservation constraints for backup paths. Constraints (3.24)–(3.26) are the failure state

relationships which determine whether lightpath *r* will fail in network state *s*, while also taking the path protection being deployed in the network into consideration. More specifically, constraint set (3.24) determines whether or not the backup path for lightpath *r* is available in network state *s*. The backup path for lightpath *r* might not be available in network state *s* (i.e., $h_{s,r} > 0$) for two reasons: either the backup path fails due to a cable cut in that network state (i.e., $\sum_{j \in L} state_{s,j} q_{r,j} > 0$), or lightpath *r* is not protected (i.e., $bp_r = 0$, or $1\text{-}bp_r > 0$). Constraint set (3.25) indicates that lightpath *r* fails in network state *s* (i.e., $y_{s,r} > 0$) if and only if both its working path fails (i.e., $g_{s,r} > 0$) and its backup path is not available in that network state (i.e., $h_{s,r} > 0$). Constraint set (3.26) relates integer variable $y_{s,r}$ to binary variable $z_{s,r}$. Constraints (3.27)–(3.28) are for the calculation of the risk as (3.17)–(3.18) in the link protection case. Constraint (3.29) is the budget constraint. Constraint set (3.30) guarantees that each backup path is link-disjoint from its working path. Lastly, constraint sets (3.31) and (3.32) express the binary nature of the decision and failure variables.

Minimum-risk path protection design problem (Node-link model)

Objective: $\min_{bp_r, q_{r,j}} totalrisk$ (3.22)

s.t. $\sum_{j \in L} q_{r,j} b_{n,j} = d_{r,n} bp_r \pmod 2, \quad \forall r \in R, \forall n \in N$ (3.23)

$$h_{s,r} = \sum_{j \in L} state_{s,j} q_{r,j} + 1 - bp_r, \quad \forall s \in S, \forall r \in R \tag{3.24}$$

$$y_{s,r} = g_{s,r} h_{s,r}, \quad \forall s \in S, \forall r \in R \tag{3.25}$$

$$z_{s,r} \mathrm{K} \geq y_{s,r}, \quad \forall s \in S, \forall r \in R \tag{3.26}$$

$$damage_s = \sum_{r \in R} z_{s,r} d_r, \quad \forall s \in S \tag{3.27}$$

$$totalrisk = \sum_{s \in S} stateprob_s damage_s, \quad \forall s \in S \tag{3.28}$$

$$\sum_{r \in R} \sum_{j \in L} c_j q_{r,j} m_r \leq budget \tag{3.29}$$

$$p_{r,j} + q_{r,j} \leq 1, \quad \forall r \in R, \forall j \in L \tag{3.30}$$

$$q_{r,j}, bp_r : binary, \quad \forall r \in R, \forall j \in L \tag{3.31}$$

$$z_{s,r} : binary, \quad \forall s \in S, \forall r \in R \tag{3.32}$$

3.4.1.2 Link-Path InP Formulations

In this section, the minimum-risk survivable network design problems are formulated as link-path InP models for both link protection and path protection cases. The notation used in the link-path formulations is presented in Table 3.3.

Table 3.3 Notation used in link-path InP formulations

Given:	
N	Set of nodes
L	Set of links or cables
R	Set of ligthpaths
S	Set of network states
$p_{r,i}$	$p_{r,i}$ = 1 if lightpath r uses link i in its working path, and = 0 otherwise
m_r	Data rate (bits/s) of lightpath r
w_i	Amount of working capacity on link i, calculated by $w_i = \sum_{r \in R} p_{r,i} m_r$

$state_{s,i}$	$state_{s,i}$ = 1 if cable i is cut in network state s, and = 0 otherwise
$stateprob_s$	$stateprob_s$ is the probability of network state s
d_r	Damage caused by a failure of lightpath r
c_i	The unit cost of spare capacity on link i
budget	The budget
K	A large constant used for bounding

The following notation is used in the link protection case only:

Q_i	Set of eligible backup routes for link i
$\delta_{i,j}^q$	$\delta_{i,j}^q$ = 1 if the q^{th} eligible backup route for link i in the set Q_i includes link j, and = 0 otherwise
$\zeta_{s,i}^q$	$\zeta_{s,i}^q$ = 1 if the q^{th} backup route for link i in the set Q_i fails in network state s, and = 0 otherwise

The following notation is used in the path protection case only:

Q_r	Set of eligible backup routes for lightpath r
$\delta_{r,j}^q$	$\delta_{r,j}^q$ = 1 if the q^{th} eligible backup route for lightpath r in the set Q_r includes link j, and = 0 otherwise
$\zeta_{s,r}^q$	$\zeta_{s,r}^q$ = 1 if the q^{th} backup route for lightpath r in the set Q_r fails in network state s, and = 0 otherwise
$g_{s,r}$	$g_{s,r} > 0$ if a working path for lightpath r fails in network state s, and = 0 otherwise (i.e., $g_{s,r} = \sum_{i \in L} state_{s,i} p_{r,i}$)

Variables:

$damage_s$	Damage occurring in network state s
totalrisk	Total risk to the network
$y_{s,r}$	$y_{s,r} > 0$ if lightpath r fails in network state s, and = 0 otherwise

$z_{s,r}$	$z_{s,r}$ = 1 if lightpath r fails in network state s, and = 0 otherwise

The following notation is used in the link protection case only:

bp_i	bp_i = 1 if link i is protected, and = 0 otherwise
f_i^q	f_i^q = 1 if link i is protected and uses the q^{th} route in the backup route set Q_i for its backup path, and = 0 otherwise
$h_{s,i}$	$h_{s,i}$ = 1 if a backup path for link i is not available (either link i is not protected, or the backup path fails) in network state s, and = 0 otherwise
$e_{s,i}$	$e_{s,i}$ = 1 if link i fails (both working link fails and backup path is not available) in network state s, and = 0 otherwise

The following notation is used in the path protection case only:

bp_r	bp_r =1 if lightpath r is protected, and = 0 otherwise
f_r^q	f_r^q = 1 if lightpath r is protected and uses the q^{th} route in the backup route set Q_r for its backup path, and = 0 otherwise
$h_{s,r}$	$h_{s,r}$ = 1 if a backup path for lightpath r is not available (either lightpath r is not protected, or the backup path fails) in network state s, and = 0 otherwise

The link-path formulation for the minimum-risk link protection design problem is presented in (3.33)–(3.43). The sets of decision variables are the binary variables bp_i, which determines which links to be protected, where bp_i = 1 if link i is protected and bp_i = 0 otherwise, and the binary variables f_i^q which specifies the backup route for link i, where f_i^q = 1 if link i is protected and uses the q^{th} route in the backup route set Q_i for its backup path, and = 0 otherwise. The objective (3.33) is to minimize the total network risk. Constraint set (3.34) indicates that if link i is protected, there must exist one backup path, for which the route is selected from a set of eligible backup routes Q_i. Constraints (3.35)–(3.38) are the failure state relationships which

determine whether or not lightpath r fails in network state s, taking into account the link protection being deployed in the network. More specifically, constraint set (3.35) determines whether or not the backup path for link i is available in network state s. The backup path for link i might not be available in network state s (i.e., $h_{s,i} = 1$) for two reasons: either the backup path exists but fails due to a cable cut in that network state (i.e., $\sum_{q \in Q_i} f_i^q \zeta_{s,i}^q = 1$), or link i is not protected (i.e., $bp_i = 0$, or $1\text{-}bp_i = 1$). Constraint set (3.36) indicates that link i fails in network state s (i.e., $e_{s,i} = 1$) if and only if both the working link fails (i.e., $state_{s,i} = 1$) and its backup path is not available (i.e., $h_{s,i} = 1$) in that network state. Constraint set (3.37) indicates that lightpath r fails in network state s ($y_{s,r} > 0$) if and only if at least one of the links that it traverses fails (i.e., $\sum_{i \in L} e_{s,i} p_{r,i} > 0$). Constraint set (3.38) relates variable $y_{s,r}$ to binary variable $z_{s,r}$. Constraints (3.39–(3.40) are for the calculation of the risk as in (3.4). That is, constraint set (3.39) calculates the amount of damage for each network state as the sum of damages of all failed lightpaths in that network state; and constraint (3.40) calculates the total network risk as the sum of the products of the state damage and the state probability for all network states. Constraint (3.41) is the budget constraint which limits the total spare capacity investment, where c_j is the unit cost of spare capacity on link j, w_i is the amount of working capacity on link i, and parameter $\delta_{i,j}^q = 1$ if q^{th} eligible backup route for link i in the set Q_i includes link j, and = 0 otherwise. Lastly, constraints (3.42) and (3.43) express the binary nature of the design and failure variables.

Minimum-risk link protection design problem (Link-path model)

$$\text{Objective: } \min_{bp_i,\, f_i^q} totalrisk \tag{3.33}$$

$$\sum_{q\in Q_i} f_i^q = bp_i, \quad \forall i \in L \tag{3.34}$$

$$h_{s,i} = \sum_{q\in Q_i} f_i^q \zeta_{s,i}^q + 1 - bp_i, \quad s \in S, i \in L \tag{3.35}$$

$$e_{s,i} = state_{s,i} h_{s,i}, \quad s \in S, i \in L \tag{3.36}$$

$$y_{s,r} = \sum_{i\in L} e_{s,i} p_{r,i}, \quad s \in S, r \in R \tag{3.37}$$

$$z_{s,r}\mathrm{K} \geq y_{s,r}, \quad s \in S, r \in R \tag{3.38}$$

$$damage_s = \sum_{r\in R} z_{s,r} d_r, \quad \forall s \in S \tag{3.39}$$

$$totalrisk = \sum_{s\in S} stateprob_s damage_s \tag{3.40}$$

$$\sum_{i\in L}\sum_{q\in Q_i}\sum_{j\in L} c_j w_i f_i^q \delta_{i,j}^q \leq budget \tag{3.41}$$

$$bp_i,\ f_i^q : binary, \quad \forall i \in L, \forall q \in Q_i \tag{3.42}$$

$$z_{s,r} : binary, \quad \forall s \in S, \forall r \in R \tag{3.43}$$

For the minimum-risk path protection design problem, the link-path formulation is presented in (3.44)–(3.53). The set of decision variables to be determined are binary variables bp_r, which determines a set of lightpaths to be protected, where bp_r = 1 if lightpath r is protected and bp_r = 0 otherwise, and the binary variables f_r^q, which specifies the backup route for lightpath r, where f_r^q = 1 if lightpath r is protected and uses the q^{th} route in the backup route set Q_r for its backup path, and = 0 otherwise. The objective (3.44) is to minimize the total network risk.

Constraint set (3.45) indicates that if lightpath r is protected, there must exist one backup path, whose route is selected from a set of eligible backup routes Q_r. Constraints (3.46)–(3.48) are the failure state relationships which determine whether or not lightpath r will fail in network state s, taking into account the path protection being deployed in the network. More specifically, constraint set (3.46) determines whether or not the backup path for lightpath r is available in network state s. The backup path for lightpath r might not be available in network state s (i.e., $h_{s,r}$ = 1) for two reasons: either the backup path exists but fails due to a cable cut in that network state (i.e., $\sum_{q \in Q_r} f_r^q \zeta_{s,r}^q$ =1), or lightpath r is not protected (i.e., bp_r = 0, or 1-bp_r = 1). Constraint set (3.47) indicates that lightpath r fails in network state s (i.e., $y_{s,r} > 0$) if and only if both its working path fails (i.e., $g_{s,r} > 0$) and its backup path is not available in that network state (i.e., $h_{s,r}$ = 1). Constraint set (3.48) relates variable $y_{s,r}$ to binary variable $z_{s,r}$. Constraints (3.49)–(3.50) are for the calculation of the risk. Constraint (3.51) is the budget constraint. Lastly, constraints (3.52) and (3.53) express the binary nature of the design and failure variables.

Minimum-risk path protection design problem (Link-path model)

Objective: $\min_{bp_r,\, f_r^q} totalrisk$ (3.44)

$$\sum_{q \in Q_r} f_r^q = bp_r, \quad \forall r \in R \tag{3.45}$$

$$h_{s,r} = \sum_{q \in Q_r} f_r^q \zeta_{s,r}^q + 1 - bp_r, \quad s \in S, r \in R \tag{3.46}$$

$$y_{s,r} = g_{s,r} h_{s,r}, \quad s \in S, r \in R \tag{3.47}$$

$$z_{s,r} \mathrm{K} \geq y_{s,r}, \quad s \in S, r \in R \tag{3.48}$$

$$damage_s = \sum_{r \in R} z_{s,r} d_r, \quad \forall s \in S \tag{3.49}$$

$$totalrisk = \sum_{s \in S} state_s damage_s \tag{3.50}$$

$$\sum_{r \in R} \sum_{q \in Q_r} \sum_{j \in L} c_j m_r f_r^q \delta_{r,j}^q \leq budget \tag{3.51}$$

$$bp_r, f_r^q : binary, \quad \forall r \in R, \forall q \in Q_r \tag{3.52}$$

$$z_{s,r} : binary, \quad \forall s \in S, \forall r \in R \tag{3.53}$$

3.4.2 Heuristic Approach

In the heuristic approach, a set of eligible link-disjoint backup routes is pre-computed and given to the problem. Our heuristics are based on a greedy method, which repeatedly selects the best link (in the link protection case), or the best lightpath (in the path protection case), to be protected along with its corresponding backup route one at a time based on a risk-reduction criteria. Here, three greedy heuristic algorithms are proposed.

Heuristic 1: Greedy heuristic with greatest risk reduction

The basic idea of this greedy heuristic is that at each step, the algorithm chooses to protect the link (in the link protection case) or the lightpath (in the path protection case) using one of the backup routes in the pre-computed route set, where the protection produces the greatest risk reduction and does not violate the budget limit. The process repeats until no more links/lightpaths can be selected due to the budget constraint, or all the links/lightpaths have been protected. The flow chart of the greedy heuristic algorithm with greatest risk reduction is presented in Figure 3.5.

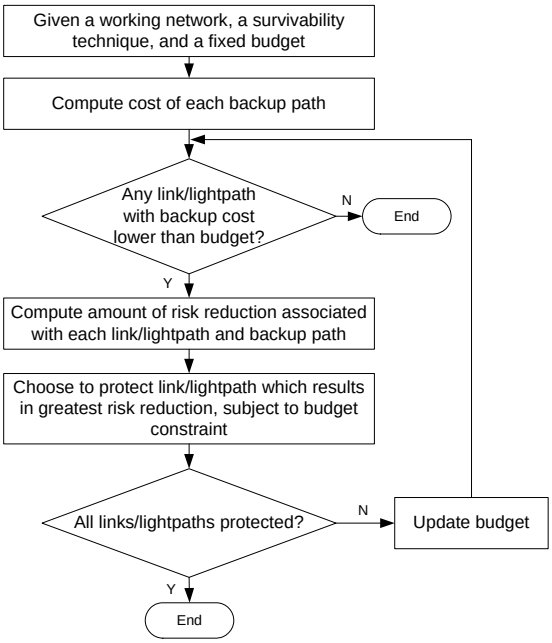


Figure 3.5 Flow chart of the greedy heuristic algorithm with greatest risk reduction

Heuristic 2: Greedy heuristic with greatest risk reduction/cost ratio

This heuristic is similar to Heuristic 1 except that at each step, the algorithm chooses to protect the link (in the link protection case) or the lightpath (in the path protection case) using one of the backup routes in the pre-computed route set, where the protection produces the greatest ratio of risk reduction to backup path cost while not violating the budget limit. The flow chart of the heuristic algorithm with greatest risk reduction/cost ratio is presented in Figure 3.6.

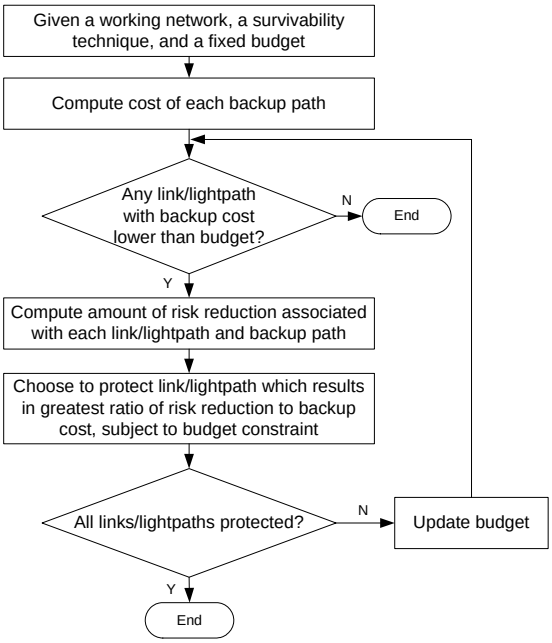


Figure 3.6 Flow chart of the greedy heuristic algorithm with greatest risk reduction/cost ratio

Heuristic 3: Iterative greedy heuristic

This heuristic algorithm consists of two steps. The first step is the same as Heuristic 2. Since the first step may not yield an optimal solution, an iterative process in the second step is deployed to improve the solution. The second step is based on an idea that it is possible to improve the current solution by iteratively selecting a protected link/lightpath then removing the protection from the protected link/lightpath in the current solution, followed by updating the budget, and then choosing to protect the unprotected links/lightpaths that could produce the greatest risk reduction. The iterative process keeps reducing the amount of total network risk; and terminates when the current solution cannot be improved further, or a predefined number of iterations is reached. The flow chart of the iterative greedy heuristic algorithm is presented in Figure 3.7.

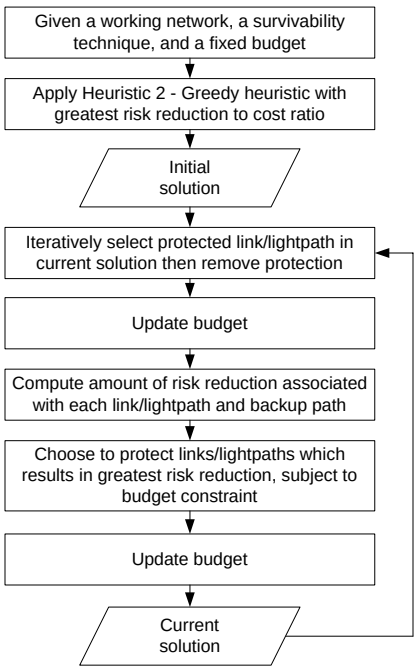


Figure 3.7 Flow chart of the iterative greedy heuristic algorithm

3.5 MINIMUM-RISK SURVIVABLE NETWORK DESIGN FOR NETWORKS WITH MULTIPLE CLASSES OF TRAFFIC

This section extends the minimum-risk survivable network design to networks supporting multiple classes of traffic with different levels of protection. Three different classes of traffic are defined for traffic flows (i.e., lightpaths): bronze, silver and gold, each associated with a different level of damage upon failure. The gold class represents the traffic flows that cause the highest damage level when they fail, for example, the traffic flows with the highest availability requirement and associated violation penalty defined in a Service Level Agreement (SLA). On the other hand, the bronze class represents the traffic flows with the lowest damage level.

The notation used in the minimum-risk survivable network design for networks with multiple classes of traffic is presented in Table 3.4.

Table 3.4 Notation used in minimum-risk design formulations for networks with multiple classes of traffic

Given:

N	Set of nodes
L	Set of links or cables
R^B, R^S, R^G	Set of bronze, silver, and gold-class ligthpaths respectively
S	Set of network states
$p_{r,i}^B$	$p_{r,i}^B$ = 1 if bronze-class lightpath *r* uses link *i* in its working path, and = 0 otherwise
$p_{r,i}^S$	$p_{r,i}^S$ = 1 if silver-class lightpath *r* uses link *i* in its working path, and = 0 otherwise
$p_{r,i}^G$	$p_{r,i}^G$ = 1 if gold-class lightpath *r* uses link *i* in its working path, and = 0 otherwise
m_r^B, m_r^S, m_r^G	Data rate (bits/s) of bronze, silver and gold-class lightpath *r*, respectively
w_i	Amount of working capacity on link *i*, calculated by $w_i = \sum_{r \in R^B} p_{r,i}^B m_r^B + \sum_{r \in R^S} p_{r,i}^S m_r^S + \sum_{r \in R^G} p_{r,i}^G m_r^G$
$state_{s,i}$	$state_{s,i}$ = 1 if cable *i* is cut in network state *s*, and = 0 otherwise
$stateprob_s$	$stateprob_s$ is the probability of network state *s*
d_r^B, d_r^S, d_r^G	Damage caused by a failure of bronze, silver, and gold-class lightpath *r*, respectively
c_i	The unit cost of spare capacity on link *i*
budget	The budget
K	A large constant used for bounding

The following notation is used in the link protection case only:

Q_i	Set of eligible backup routes for link *i*
$\delta_{i,j}^q$	$\delta_{i,j}^q$ = 1 if the q^{th} eligible backup route for link *i* in the set Q_i includes link *j*, and = 0 otherwise

$\zeta_{s,i}^{q}$	$\zeta_{s,i}^{q}$ = 1 if the q^{th} backup route for link i in the set Q_i fails in network state s, and = 0 otherwise

The following notation is used in the path protection case only:

Q_r^B	Set of eligible backup routes for bronze-class lightpath r
Q_r^S	Set of eligible backup routes for silver-class lightpath r
Q_r^G	Set of eligible backup routes for gold-class lightpath r
$\delta_{r,j}^{B,q}$	$\delta_{r,j}^{B,q}$ = 1 if the q^{th} eligible backup route for bronze-class lightpath r in the set Q_r^B includes link j, and = 0 otherwise
$\delta_{r,j}^{S,q}$	$\delta_{r,j}^{S,q}$ = 1 if the q^{th} eligible backup route for silver-class lightpath r in the set Q_r^S includes link j, and = 0 otherwise
$\delta_{r,j}^{G,q}$	$\delta_{r,j}^{G,q}$ = 1 if the q^{th} eligible backup route for gold-class lightpath r in the set Q_r^G includes link j, and = 0 otherwise
$\zeta_{s,r}^{B,q}$	$\zeta_{s,r}^{B,q}$ = 1 if the q^{th} backup route for bronze-class lightpath r in the set Q_r^B fails in network state s, and = 0 otherwise
$\zeta_{s,r}^{S,q}$	$\zeta_{s,r}^{S,q}$ = 1 if the q^{th} backup route for silver-class lightpath r in the set Q_r^S fails in network state s, and = 0 otherwise
$\zeta_{s,r}^{G,q}$	$\zeta_{s,r}^{G,q}$ = 1 if the q^{th} backup route for gold-class lightpath r in the set Q_r^G fails in network state s, and = 0 otherwise
$g_{s,r}^{B}$	$g_{s,r}^{B} > 0$ if a working path for bronze-class lightpath r fails in network state s, and = 0 otherwise (i.e., $g_{s,r}^{B} = \sum_{i \in L} state_{s,i}\, p_{r,i}^{B}$)
$g_{s,r}^{S}$	$g_{s,r}^{S} > 0$ if a working path for silver-class lightpath r fails in network state s, and = 0 otherwise (i.e., $g_{s,r}^{S} = \sum_{i \in L} state_{s,i}\, p_{r,i}^{S}$)
$g_{s,r}^{G}$	$g_{s,r}^{G} > 0$ if a working path for gold-class lightpath r fails in network state s, and = 0 otherwise (i.e., $g_{s,r}^{G} = \sum_{i \in L} state_{s,i}\, p_{r,i}^{G}$)

Variables:

$damage_s$	Damage occurring in network state s
$totalrisk$	Total risk to the network
$y_{s,r}^B$	$y_{s,r}^B > 0$ if bronze-class lightpath r fails in network state s, and = 0 otherwise
$y_{s,r}^S$	$y_{s,r}^S > 0$ if silver-class lightpath r fails in network state s, and = 0 otherwise
$y_{s,r}^G$	$y_{s,r}^G > 0$ if gold-class lightpath r fails in network state s, and = 0 otherwise
$z_{s,r}^B$	$z_{s,r}^B = 1$ if bronze-class lightpath r fails in network state s, and = 0 otherwise
$z_{s,r}^S$	$z_{s,r}^S = 1$ if silver-class lightpath r fails in network state s, and = 0 otherwise
$z_{s,r}^G$	$z_{s,r}^G = 1$ if gold-class lightpath r fails in network state s, and = 0 otherwise

The following notation is used in the link protection case only:

bp_i	$bp_i = 1$ if link i is protected, and = 0 otherwise
f_i^q	$f_i^q = 1$ if link i is protected and uses the q^{th} route in the backup route set Q_i for its backup path, and = 0 otherwise
$h_{s,i}$	$h_{s,i} = 1$ if a backup path for link i is not available (either link i is not protected, or the backup path fails) in network state s, and = 0 otherwise
$e_{s,i}$	$e_{s,i} = 1$ if link i fails (both working link fails and backup path is not available) in network state s, and = 0 otherwise

The following notation is used in the path protection case only:

bp_r^B	bp_r^B =1 if bronze-class lightpath r is protected, and = 0 otherwise
bp_r^S	bp_r^S =1 if silver-class lightpath r is protected, and = 0 otherwise
bp_r^G	bp_r^G =1 if gold-class lightpath r is protected, and = 0 otherwise

$f_r^{B,q}$	$f_r^{B,q}$ = 1 if bronze-class lightpath *r* is protected and uses the q^{th} route in the backup route set Q_r^B for its backup path, and = 0 otherwise
$f_r^{S,q}$	$f_r^{S,q}$ = 1 if silver-class lightpath *r* is protected and uses the q^{th} route in the backup route set Q_r^S for its backup path, and = 0 otherwise
$f_r^{G,q}$	$f_r^{G,q}$ = 1 if gold-class lightpath *r* is protected and uses the q^{th} route in the backup route set Q_r^G for its backup path, and = 0 otherwise
$h_{s,r}^B$	$h_{s,r}^B$ = 1 if a backup path for bronze-class lightpath *r* is not available (either bronze-class lightpath *r* is not protected, or the backup path fails) in network state *s*, and = 0 otherwise
$h_{s,r}^S$	$h_{s,r}^S$ = 1 if a backup path for silver-class lightpath *r* is not available (either silver-class lightpath *r* is not protected, or the backup path fails) in network state *s*, and = 0 otherwise
$h_{s,r}^G$	$h_{s,r}^G$ = 1 if a backup path for gold-class lightpath *r* is not available (either gold-class lightpath *r* is not protected, or the backup path fails) in network state *s*, and = 0 otherwise

The link-path formulation for the minimum-risk link protection design for networks with multiple classes of traffic is presented in (3.54)–(3.70). Two sets of decision variables are used. First set are the binary variables bp_i, which determine which links to be protected, where $bp_i = 1$ if link *i* is protected and $bp_i = 0$ otherwise. The second set are the binary variables f_i^q which specifies the backup route for link *i*, where $f_i^q = 1$ if link *i* is protected and uses the q^{th} route in the backup route set Q_i for its backup path, and = 0 otherwise. The design objective in (3.54) is to minimize the total network risk. Constraint set (3.55) indicates that if link *i* is protected, there must exist one backup path, for which the route is selected from a set of eligible backup routes

Q_i. Constraints (3.56)–(3.63) are the failure state relationships which determine which lightpaths in each traffic class fail in each network state, taking into account the link protection being deployed in the network. More specifically, constraint set (3.56) determines whether or not the backup path for link *i* is available in network state *s*. The backup path for link *i* might not be available in network state *s* (i.e., $h_{s,i} = 1$) for two reasons: either the backup path exists but fails due to a cable cut in that network state (i.e., $\sum_{q \in Q_i} f_i^q \zeta_{s,i}^q = 1$), or link *i* is not protected (i.e., $bp_i = 0$, or $1\text{-}bp_i = 1$). Constraint set (3.57) indicates that link *i* fails in network state *s* (i.e., $e_{s,i} = 1$) if and only if both the working link fails (i.e., $state_{s,i} = 1$) and its backup path is not available (i.e., $h_{s,i} = 1$) in that network state. Constraint sets (3.58)–(3.60) are similar to the constraint set (3.15) in the design for networks with single class of traffic, except that they determine which lightpaths fail in network state s for each traffic class separately. For example, constraint set (3.58) indicates that bronze-class lightpath *r* fails in network state *s* (i.e., $y_{s,r}^B > 0$) if and only if at least one of the links that it traverses fails (i.e., $\sum_{i \in L} e_{s,i} p_{r,i}^B > 0$). Constraint sets (3.61)–(3.63) relate variables $y_{s,r}^B$, $y_{s,r}^S$, and $y_{s,r}^G$ to binary variables $z_{s,r}^B$, $z_{s,r}^S$, and $z_{s,r}^G$ for bronze, silver and gold-class traffic, respectively. Constraint (3.64) calculates the damage in network state *s* as the sum of the damage resulting from failed lightpaths of all traffic classes in network state *s*, where d_r^B, d_r^S, and d_r^G denote the damage caused by a failure of bronze, silver, and gold-class lightpath *r*, respectively. Constraint (3.65) is the calculation of the total network risk as the sum of the product of the state damage and the state probability for all network states. Constraint (3.66) is the budget constraint which limits the total spare capacity investment, where c_j is the unit cost of spare capacity on link *j*, w_i is the amount of working capacity on link *i*, and parameter $\delta_{i,j}^q = 1$ if the q^{th} eligible

backup route for link i in the set Q_i includes link j, and = 0 otherwise. Lastly, constraints (3.67)–(3.70) express the binary nature of the design and failure variables.

Minimum-risk link protection design problem for networks with multiple classes of traffic

Objective: $\min_{bp_i,\, f_i^q} totalrisk$ (3.54)

$$\sum_{q \in Q_i} f_i^q = bp_i, \quad \forall i \in L \tag{3.55}$$

$$h_{s,i} = \sum_{q \in Q_i} f_i^q \zeta_{s,i}^q + 1 - bp_i, \quad s \in S, i \in L \tag{3.56}$$

$$e_{s,i} = state_{s,i} h_{s,i}, \quad s \in S, i \in L \tag{3.57}$$

$$y_{s,r}^B = \sum_{i \in L} e_{s,i} p_{r,i}^B, \quad s \in S, r \in R^B \tag{3.58}$$

$$y_{s,r}^S = \sum_{i \in L} e_{s,i} p_{r,i}^S, \quad s \in S, r \in R^S \tag{3.59}$$

$$y_{s,r}^G = \sum_{i \in L} e_{s,i} p_{r,i}^G, \quad s \in S, r \in R^G \tag{3.60}$$

$$z_{s,r}^B \mathrm{K} \geq y_{s,r}^B, \quad s \in S, r \in R^B \tag{3.61}$$

$$z_{s,r}^S \mathrm{K} \geq y_{s,r}^S, \quad s \in S, r \in R^S \tag{3.62}$$

$$z_{s,r}^G \mathrm{K} \geq y_{s,r}^G, \quad s \in S, r \in R^G \tag{3.63}$$

$$damage_s = \sum_{r \in R^B} z_{s,r}^B d_r^B + \sum_{r \in R^S} z_{s,r}^S d_r^S + \sum_{r \in R^G} z_{s,r}^G d_r^G, \quad \forall s \in S \tag{3.64}$$

$$totalrisk = \sum_{s \in S} stateprob_s damage_s \tag{3.65}$$

$$\sum_{i \in L} \sum_{q \in Q_i} \sum_{j \in L} c_j w_i f_i^q \delta_{i,j}^q \leq budget \tag{3.66}$$

$$bp_i,\ f_i^q : binary, \quad \forall i \in L, \forall q \in Q_i \tag{3.67}$$

$$z_{s,r}^{B} : binary, \quad \forall s \in S, \forall r \in R^{B} \tag{3.68}$$

$$z_{s,r}^{S} : binary, \quad \forall s \in S, \forall r \in R^{S} \tag{3.69}$$

$$z_{s,r}^{G} : binary, \quad \forall s \in S, \forall r \in R^{G} \tag{3.70}$$

For the minimum-risk path protection design problem for networks with multiple classes of traffic, the link-path formulation is presented in (3.71)–(3.92). The formulation is very similar to the minimum-risk path protection design formulation for the single class of traffic case in (3.22)–(3.32) except that it considers each traffic class separately.

The design objective in (3.71) is to minimize the total risk. The set of decision variables to be determined are binary variables bp_r^B, bp_r^S, and bp_r^G which determine a set of bronze, silver and gold-class lightpaths to be protected, respectively, and the binary variables $f_r^{B,q}$, $f_r^{S,q}$, and $f_r^{G,q}$ which specifies the backup route for each lightpath of the bronze, silver and gold traffic class, respectively. Constraint sets (3.72)–(3.74) determine the backup route for each protected lightpath of the bronze, silver and gold traffic class, respectively. For example, constraint set (3.72) indicates that if bronze class lightpath *r* is protected, there must exist one backup path, whose route is selected from a set of eligible backup routes Q_r^B. Constraints (3.75)–(3.83) are the failure state relationships which determine which lightpaths of each traffic class fail in each network state, taking into account the path protection being deployed in the network. More specifically, constraint sets (3.75)–(3.77) determine whether or not the backup path for each lightpath of the bronze, silver and gold traffic class is available in each network state. For example in (3.75), the backup path for bronze lightpath *r* might not be available in network state *s* (i.e., $h_{s,r}^B = 1$) for two reasons: either the backup path exists but fails due to a cable cut in that

network state (i.e., $\sum_{q \in Q_r^B} f_r^{B,q} \zeta_{s,r}^{B,q} = 1$), or lightpath *r* is not protected (i.e., $bp_r^B = 0$, or $1\text{-}bp_r^B = 1$). Constraint sets (3.78)–(3.80) determine which lightpaths of the bronze, silver, and gold traffic classes, respectively, fail in each network state. For example, constraint set (3.78) indicates that bronze-class lightpath *r* fails in network state *s* (i.e., $y_{s,r}^B > 0$) if and only if both its working path fails (i.e., $g_{s,r}^B > 0$) and its backup path is not available in that network state (i.e., $h_{s,r}^B = 1$). Constraint sets (3.81)–(3.83) relate variables $y_{s,r}^B$, $y_{s,r}^S$, and $y_{s,r}^G$ to binary variables $z_{s,r}^B$, $z_{s,r}^S$, and $z_{s,r}^G$, for the bronze, silver and gold traffic classes, respectively. Constraints (3.84) calculates the damage in network state *s* as the sum of the damage resulting from failed lightpaths of all traffic classes in network state *s*, where d_r^B, d_r^S, and d_r^G denote the damage caused by a failure of bronze, silver, and gold-class lightpath *r*, respectively. Constraint (3.85) is the calculation of the total network risk as the sum of the product of the state damage and the state probability for all network states. Constraint (3.86) is the budget constraint. Lastly, constraints (3.87)–(3.92) express the binary nature of the design and failure variables.

Minimum-risk path protection design problem for networks with multiple classes of traffic

Objective: $$\min_{bp_r^B, bp_r^S, bp_r^G, f_r^{B,q}, f_r^{S,q}, f_r^{G,q}} totalrisk \tag{3.71}$$

$$\sum_{q \in Q_r^B} f_r^{B,q} = bp_r^B, \quad \forall r \in R^B \tag{3.72}$$

$$\sum_{q \in Q_r^S} f_r^{S,q} = bp_r^S, \quad \forall r \in R^S \tag{3.73}$$

$$\sum_{q \in Q_r^G} f_r^{G,q} = bp_r^G, \quad \forall r \in R^G \tag{3.74}$$

$$h_{s,r}^B = \sum_{q \in Q_r^B} f_r^{B,q} \zeta_{s,r}^{B,q} + 1 - bp_r^B, \quad s \in S, r \in R^B \tag{3.75}$$

$$h_{s,r}^{S} = \sum_{q \in Q_r^S} f_r^{S,q} \zeta_{s,r}^{S,q} + 1 - bp_r^S, \quad s \in S, r \in R^S \tag{3.76}$$

$$h_{s,r}^{G} = \sum_{q \in Q_r^G} f_r^{G,q} \zeta_{s,r}^{G,q} + 1 - bp_r^G, \quad s \in S, r \in R^G \tag{3.77}$$

$$y_{s,r}^{B} = g_{s,r}^{B} h_{s,r}^{B}, \quad s \in S, r \in R^B \tag{3.78}$$

$$y_{s,r}^{S} = g_{s,r}^{S} h_{s,r}^{S}, \quad s \in S, r \in R^S \tag{3.79}$$

$$y_{s,r}^{G} = g_{s,r}^{G} h_{s,r}^{G}, \quad s \in S, r \in R^G \tag{3.80}$$

$$z_{s,r}^{B} \mathrm{K} \geq y_{s,r}^{B}, \quad s \in S, r \in R^B \tag{3.81}$$

$$z_{s,r}^{S} \mathrm{K} \geq y_{s,r}^{S}, \quad s \in S, r \in R^S \tag{3.82}$$

$$z_{s,r}^{G} \mathrm{K} \geq y_{s,r}^{G}, \quad s \in S, r \in R^G \tag{3.83}$$

$$damage_s = \sum_{r \in R^B} z_{s,r}^{B} d_r^{B} + \sum_{r \in R^S} z_{s,r}^{S} d_r^{S} + \sum_{r \in R^G} z_{s,r}^{G} d_r^{G}, \quad \forall s \in S \tag{3.84}$$

$$totalrisk = \sum_{s \in S} state_s damage_s \tag{3.85}$$

$$\sum_{r \in R^B} \sum_{q \in Q_r^B} \sum_{j \in L} c_j m_r^B f_r^{B,q} \delta_{r,j}^{B,q} + \sum_{r \in R^S} \sum_{q \in Q_r^S} \sum_{j \in L} c_j m_r^S f_r^{S,q} \delta_{r,j}^{S,q} + \sum_{r \in R^G} \sum_{q \in Q_r^G} \sum_{j \in L} c_j m_r^G f_r^{G,q} \delta_{r,j}^{G,q} \leq budget \tag{3.86}$$

$$bp_r^B, f_r^{B,q} : binary, \quad \forall r \in R^B, \forall q \in Q_r^B \tag{3.87}$$

$$bp_r^S, f_r^{S,q} : binary, \quad \forall r \in R^S, \forall q \in Q_r^S \tag{3.88}$$

$$bp_r^G, f_r^{G,q} : binary, \quad \forall r \in R^G, \forall q \in Q_r^G \tag{3.89}$$

$$z_{s,r}^{B} : binary, \quad \forall s \in S, \forall r \in R^B \tag{3.90}$$

$$z_{s,r}^{S} : binary, \quad \forall s \in S, \forall r \in R^S \tag{3.91}$$

$$z_{s,r}^{G} : binary, \quad \forall s \in S, \forall r \in R^G \tag{3.92}$$

3.6 INCREMENTAL MINIMUM-RISK DESIGH WITH DUAL PROTECTION

As communication services require a higher level of network availability, network operators may consider protecting the network using dual protection (i.e., protected by two backup paths). By deploying dual protection, it ensures that the network will survive any dual-link failure, given that the protected link (in link protection) or the protected path (in path protection) and the two backup paths are link-disjoint. However, the deployment of dual protection requires a much higher capital investment than the protection with single backup paths; this is due to the fact that the second link-disjoint backup path is typically longer than the first backup path, especially in sparse networks. In this situation, network operators may not have sufficient monetary funds to deploy dual protection for the whole network, and therefore have to determine in which parts of the network to deploy dual protection based on a fixed budget.

In this section, we consider an incremental minimum-risk survivable network design problem in which the given network was designed to protect against all single-link failures using single backup paths (i.e., all the working routes and the backup routes are given), then the design problem considered is to determine how best to spend a given budget for deploying dual protection (i.e., deploying second backup paths) in different parts of the network such that the total network risk is minimized.

In link protection, the design problem is to determine for which links to deploy the dual protection second backup paths, and their corresponding routes for a given budget. Whereas, in path protection, the design problem is to determine for which lightpaths to deploy the dual protection second backup paths, and their corresponding backup routes.

The incremental minimum-risk design problems with dual protection are formulated as node-link Integer Programming (InP) models. The notation used in this section is presented in Table 3.5.

Table 3.5 Notation used in incremental minimum-risk design with dual protection formulations

Given:	
N	Set of nodes
L	Set of links or cables
R	Set of ligthpaths
S	Set of network states
$p_{r,i}$	$p_{r,i}$ = 1 if lightpath r uses link i in its working path, and = 0 otherwise
m_r	Data rate (bits/s) of lightpath r
w_i	Amount of working capacity on link i, calculated by $w_i = \sum_{r \in R} p_{r,i} m_r$
$b_{n,i}$	$b_{n,i}$ = 1 if node n is the origin or destination of link i, and = 0 otherwise
$d_{r,n}$	$d_{r,n}$ = 1 if node n is the source or destination of lightpath r, and = 0 otherwise
$state_{s,i}$	$state_{s,i}$= 1 if cable i is cut in network state s, and = 0 otherwise
$stateprob_s$	$stateprob_s$ is the probability of network state s
d_r	Damage caused by a failure of lightpath r
c_i	The unit cost of spare capacity on link i
budget	The budget
K	A large constant used for bounding

The following notation is used in the link protection case only:

$q_{i,j}$	$q_{i,j}$ = 1 if the first backup path for link i traverses link j, and = 0 otherwise
$h_{s,i}$	$h_{s,i}$ = 1 if the first backup path for link i fails in network state s, and = 0 otherwise (i.e., $h_{s,i} = 1$ if $\sum_{j \in L} state_{s,j} q_{i,j} > 0$, and = 0 otherwise)

The following notation is used in the path protection case only:

$q_{r,j}$	$q_{r,j}$ = 1 if the first backup path of lightpath r traverses link j, and = 0 otherwise
$h_{s,r}$	$h_{s,r}$ = 1 if the first backup path for lightpath r fails in network state s, and = 0 otherwise (i.e., $h_{s,r} = 1$ if $\sum_{j \in L} state_{s,j} q_{r,j} > 0$, and = 0 otherwise)
$g_{s,r}$	$g_{s,r}$ = 1 if a working path for lightpath r fails in network state s, and = 0 otherwise (i.e., $g_{s,r} = 1$ if $\sum_{j \in L} state_{s,j} p_{r,j} > 0$, and = 0 otherwise)

Variables:

$damage_s$	Damage occurring in network state s
$totalrisk$	Total risk to the network
$z_{s,r}$	$z_{s,r}$ = 1 if lightpath r fails in network state s, and = 0 otherwise

The following notation is used in the link protection case only:

bp_i^2	bp_i^2 = 1 if link i is dual protected, and = 0 otherwise
$q_{i,j}^2$	$q_{i,j}^2$ = 1 if link i is dual protected and its second backup path traverses link j, and = 0 otherwise
$h_{s,i}^2$	$h_{s,i}^2$ = 1 if the second backup path for link i is not available (either link i is not dual-protected, or the second backup path fails) in network state s, and = 0 otherwise
$e_{s,i}$	$e_{s,i}$ = 1 if link i fails (both working link and first backup path fail and second backup path is not available) in network state s, and = 0 otherwise
$y_{s,r}$	$y_{s,r} > 0$ if lightpath r fails in network state s, and = 0 otherwise

The following notation is used in the path protection case only:

bp_r^2	bp_r^2 =1 if lightpath *r* is dual protected, and = 0 otherwise
$q_{r,j}^2$	$q_{r,j}^2$ = 1 if lightpath *r* is dual protected and its second backup path traverses link *j*, and = 0 otherwise
$h_{s,r}^2$	$h_{s,r}^2$ = 1 if the second backup path for lightpath *r* is not available (either lightpath *r* is not dual-protected, or the second backup path fails) in network state *s*, and = 0 otherwise

The node-link InP formulation for the incremental minimum-risk dual link protection design problem is presented in (3.93)–(3.105). The set of decision variables to be determined are the binary variables bp_i^2, which determines a set of links which have dual protection, where bp_i^2 = 1 if link *i* is dual protected, and bp_i^2 = 0 otherwise, and the binary variables $q_{i,j}^2$, which specifies the route of the dual-protection second backup path protecting link *i*, where $q_{i,j}^2$ = 1 if link *i* is dual protected, and its second backup path uses link *j*, and $q_{i,j}^2$ = 0 otherwise. The objective (3.93) is to minimize the total network risk. Constraint set (3.94) is the flow conservation constraints for second backup paths. Constraints (3.95)–(3.98) are the failure state relationships which determine whether lightpath *r* will fail in network state *s*, while also taking the link protection being deployed in the network into account. More specifically, constraint set (3.95) determines whether or not the second backup path for link *i* is available in network state *s*. The second backup path for link *i* might not be available in network state *s* (i.e., $h_{s,i}^2$ = 1) for two reasons: either the second backup path fails due to a cable cut in that network state (i.e., $\sum_{j \in L} state_{s,j} q_{i,j}^2 > 0$), or link *i* is not dual protected (i.e., bp_i^2 = 0, or 1-bp_i^2 > 0). Constraint set (3.96) indicates that link *i* fails in network state *s* (i.e., $e_{s,i}$ = 1) if and only if all of these events

occur: the working link fails (i.e., $state_{s,i} = 1$), the first backup path fails (i.e., $h_{s,i} = 1$), and the second backup path is not available (i.e., $h^2_{s,i} = 1$) in that network state. Constraint set (3.97) indicates that lightpath r fails in network state s ($y_{s,r} > 0$) if and only if at least one of the links that it traverses fails (i.e., $\sum_{i \in L} e_{s,i} p_{r,i} > 0$). Constraint set (3.98) relates variable $y_{s,r}$ to binary variable $z_{s,r}$. Constraints (3.99)–(3.100) are for the calculation of the risk as in (3.4). That is, constraint set (3.99) calculates the amount of damage in each network state as the sum of the damages of all failed lightpaths in that network state; and constraint (3.100) calculates the total network risk as the sum of the product of the state damage and the state probability for all network states. Constraint (3.101) is the budget constraint which limits the total spare capacity investment in dual protection backup paths, where c_j is the unit cost of spare capacity on link j, and w_i is the amount of working capacity on link i. Constraint set (3.102) ensures that each second backup path is link-disjoint from the corresponding first backup path. If the second link-disjoint backup path cannot be found in the network, the link is only protected by one backup path. Lastly, constraint sets (3.103)–(3.105) express the binary nature of the design and failure variables.

Incremental minimum-risk dual link protection design problem (Node-link model)

Objective: $\min_{bp^2_i, q^2_{i,j}} totalrisk$ (3.93)

s.t. $\sum_{j \in L} q^2_{i,j} b_{n,j} = b_{n,i} bp^2_i \pmod 2, \quad \forall i \in L, \forall n \in N$ (3.94)

$h^2_{s,i} \, \mathrm{K} \geq \sum_{j \in L} state_{s,j} q^2_{i,j} + 1 - bp^2_i, \quad \forall s \in S, \forall i \in L$ (3.95)

$e_{s,i} \geq state_{s,i} + h_{s,i} + h^2_{s,i} - 2, \quad \forall s \in S, \forall i \in L$ (3.96)

$$y_{s,r} = \sum_{i \in L} e_{s,i} p_{r,i}, \quad \forall s \in S, \forall r \in R \tag{3.97}$$

$$z_{s,r} \mathrm{K} \geq y_{s,r}, \quad \forall s \in S, \forall r \in R \tag{3.98}$$

$$damage_s = \sum_{r \in R} z_{s,r} d_r, \quad \forall s \in S \tag{3.99}$$

$$totalrisk = \sum_{s \in S} stateprob_s damage_s, \quad \forall s \in S \tag{3.100}$$

$$\sum_{i \in L} \sum_{j \in L} c_j w_i q_{i,j}^2 \leq budget \tag{3.101}$$

$$q_{i,j} + q_{i,j}^2 \leq 1, \quad \forall i \in L, \forall j \in L \tag{3.102}$$

$$q_{i,j}^2, bp_i^2 : \ binary, \quad \forall i \in L, \forall j \in L \tag{3.103}$$

$$h_{s,i}^2, e_{s,i} : binary, \quad \forall s \in S, \forall i \in L \tag{3.104}$$

$$z_{s,r} : binary, \quad \forall s \in S, \forall r \in R \tag{3.105}$$

The node-link InP formulation for the incremental minimum-risk dual path protection design problem is presented in (3.106)–(3.117). The two sets of decision variables to be determined are the binary variables bp_r^2, which determines a set of lightpaths which have dual protection, where bp_r^2 = 1 if lightpath *r* is dual protected and bp_r^2 = 0 otherwise, and the binary variables $q_{r,j}^2$, which specifies the route of the dual-protection second backup path for lightpath *r*, where $q_{r,j}^2$ = 1 if ligthpath *r* is dual protected and uses link *j* in its second backup path, and $q_{r,j}^2$ = 0 otherwise. The objective (3.106) is to minimize the total network risk. Constraint set (3.107) is the flow conservation constraints for second backup backup paths. Constraints (3.108)–(3.109) are the failure state relationships which determine whether lightpath *r* will fail in network state *s*, while also taking the path protection being deployed in the network into

consideration. More specifically, constraint set (3.108) determines whether or not the second backup path for lightpath *r* is available in network state *s*. The second backup path for lightpath *r* might not be available in network state *s* (i.e., $h^2_{s,r} = 1$) for two reasons: either the backup path fails due to a cable cut in that network state (i.e., $\sum_{j \in L} state_{s,j} q^2_{r,j} > 0$), or lightpath *r* is not dual protected (i.e., $bp^2_r = 0$, or $1 - bp^2_r > 0$). Constraint set (3.109) indicates that lightpath *r* fails in network state *s* (i.e., $z_{s,r} = 1$) if and only if all of these events occur: the working path fails (i.e., $g_{s,r} = 1$), the first backup path fails (i.e., $h_{s,r} = 1$), and the second backup path is not available (i.e., $h^2_{s,r} = 1$) in that network state. Constraints (3.110)–(3.111) are for the calculation of the risk as (3.99)–(3.100) in the link protection case. Constraint (3.112) is the budget constraint which limits the total spare capacity investment in dual protection backup paths. Constraint sets (3.113)–(3.114) ensure that each second backup path is link-disjoint from the corresponding working path, and the corresponding first backup path, respectively. If the second link-disjoint backup path cannot be found in the network, the lightpath is only protected by one backup path. Lastly, constraint sets (3.115)–(3.117) express the binary nature of the decision and failure variables.

Incremental minimum-risk dual path protection design problem (Node-link model)

Objective: $\min_{bp^2_r, q^2_{r,j}} totalrisk$ (3.106)

s.t. $\sum_{j \in L} q^2_{r,j} b_{n,j} = d_{r,n} bp^2_r \pmod 2, \quad \forall r \in R, \forall n \in N$ (3.107)

$h^2_{s,r} \, \mathrm{K} \geq \sum_{j \in L} state_{s,j} q^2_{r,j} + 1 - bp^2_r, \quad \forall s \in S, \forall r \in R$ (3.108)

$$z_{s,r} \geq g_{s,r} + h_{s,r} + h_{s,r}^2 - 2, \quad \forall s \in S, \forall r \in R \tag{3.109}$$

$$damage_s = \sum_{r \in R} z_{s,r} d_r, \quad \forall s \in S \tag{3.110}$$

$$totalrisk = \sum_{s \in S} stateprob_s damage_s, \quad \forall s \in S \tag{3.111}$$

$$\sum_{r \in R} \sum_{j \in L} c_j q_{r,j}^2 m_r \leq budget \tag{3.112}$$

$$p_{r,j} + q_{r,j}^2 \leq 1, \quad \forall r \in R, \forall j \in L \tag{3.113}$$

$$q_{r,j} + q_{r,j}^2 \leq 1, \quad \forall r \in R, \forall j \in L \tag{3.114}$$

$$q_{r,j}^2, bp_r^2 : binary, \quad \forall r \in R, \forall j \in L \tag{3.115}$$

$$h_{s,r}^2 : binary, \quad \forall s \in S, \forall r \in R \tag{3.116}$$

$$z_{s,r} : binary, \quad \forall s \in S, \forall r \in R \tag{3.117}$$

3.7 NUMERICAL RESULTS

This section presents the numerical results for the proposed minimum-risk survivable network design. Three networks are used in the experiments: Network 1, Network 2, and Network 3, as shown in Figure 3.2, Figure 3.8, and Figure 3.9, respectively. The cable lengths (km), and the Cable Cut (CC) metric, which is the average cable length (km) that results in a single cable cut per year, if not specified otherwise, are indicated in the figures. All the cables have the same Mean Time To Repair (MTTR) of 24 hours. For each network, a full mesh of lightpath demands between all node pairs are assumed, each of which carries the same data rate of 10 Gbps. The working path of each lightpath is routed along the shortest path based on the hop count, and

given to the design problem. The spare capacity cost is defined as 1 budget unit per 10 Gbps per 1000 km. Also, the amount of damage for the risk calculation is measured as the traffic loss rate resulting from failed lightpaths.

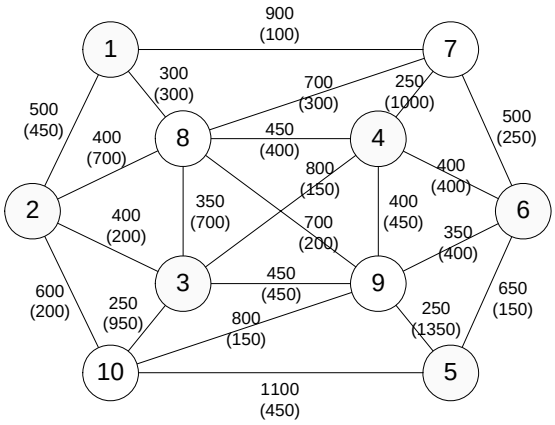


Figure 3.8 Network 2 (|*N*| = 10, |*L*| = 22) with cable length (km) and Cable Cut (CC) metric (km) within parentheses

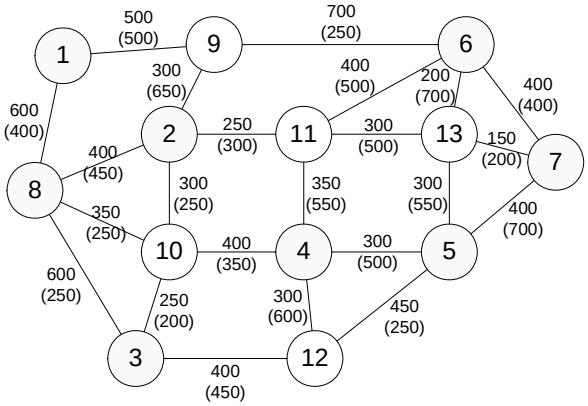


Figure 3.9 Network 3 (|*N*| = 13, |*L*| = 23) with cable length (km) and Cable Cut (CC) metric (km) within parentheses

Several numerical cases were studied. First, the minimum-risk curves (i.e., risk vs budget) for link protection and path protection are compared and discussed. Based on the risk curves, a cost-benefit analysis can show whether an investment in network survivability is justified by the reduction in risk level, and can show an optimal budget value for investing in

network protection, which maximizes the investment benefit. Then, the proposed heuristic algorithms and the InP approach are evaluated in terms of the optimality of results and the computational time. Lastly, results from an extension of the minimum-risk design approach to networks with multiple classes of traffic, and an incremental survivable network design are presented.

3.7.1 Minimum-risk curves

In the first set of experiments, a budget in term of the maximum spare capacity investment is given for each problem instance. The minimum-risk design problem as formulated in the InP models of Section 3.4.1 was solved for each budget value using the AMPL/CPLEX solver. For Network 1, we consider budget values ranging from 0 to 30 units in 0.5 increments. The minimum-risk curves (risk vs budget) for Network 1 with link protection and path protection and a fixed CC value of 450 km for all network links are shown in Figure 3.10. In addition, Table 3.6 shows the results of which links and lightpaths are being protected for some specific budget values.

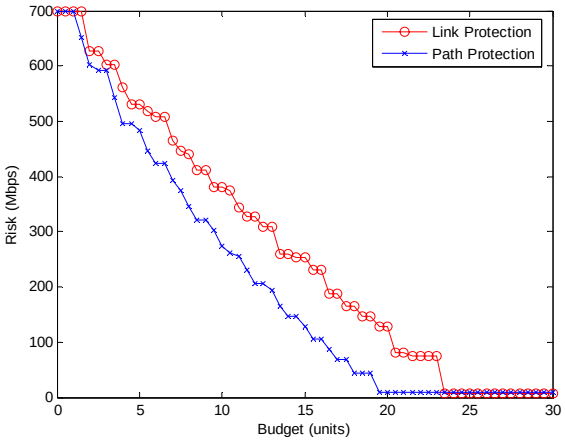


Figure 3.10 Minimum-risk curves (risk vs budget) for link protection and path protection on Network 1

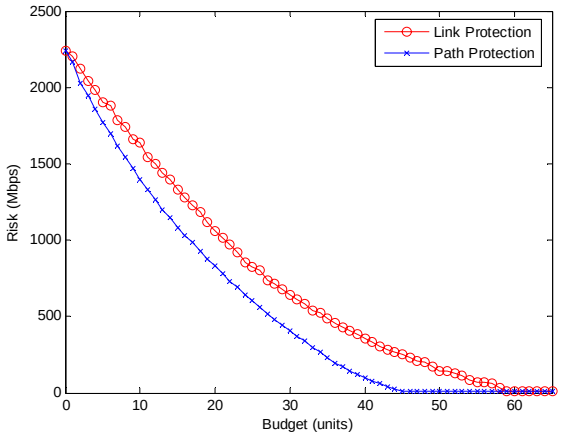
Table 3.6 Investment strategy results indicating which links or lighpaths (LPs) being protected for some specific budget values

Budget	Link Protection	Path Protection
	Protected Links	**Protected LPs**
1.5	None	LP 7
2	Link 6	LP 2
2.5	Link 6	LP 6
3	Link 4	LP 6
7	Link 4, 5 and 6	LP 2, 3, and 6
8	Link 3, 5 and 6	LP 2, 3, 6 and 7
19.5	Links 1, 2, 4, 5, 6 and 7	ALL LPs
23.5	All links	All LPs

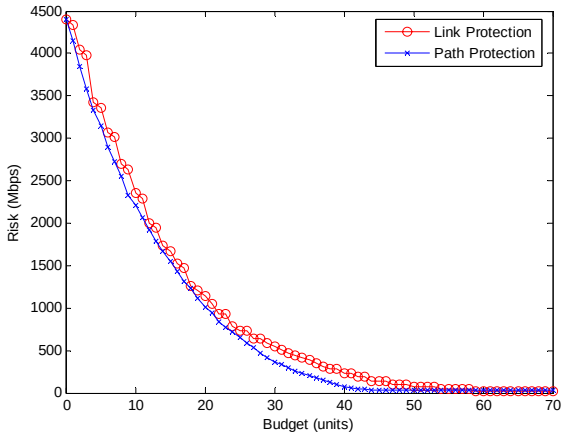
Without any protection in the network, the amount of risk to the network or the expected traffic loss rate is 699.37 Mbps. As the budget increases, the set of protected links and the set of protected lilghtpaths which yield the minimum-risk level vary as illustrated in Table 3.6, and the risk level is continually decreasing as shown in Figure 3.10. For most budget values, the path-protected network has a lower risk level than the link-protected network. This is understandable because path protection is more capacity efficient than link protection due to its higher flexibility in choosing the backup routes; and therefore requiring a lower cost to protect the same amount of traffic (i.e., path protection can protect more traffic for a given budget). For example, path protection requires only 19.5 units of budget to protect all the lightpaths in the network, whereas link protection requires 23.5 units to protect all the network links. Nevertheless, path-protected connections are more vulnerable to multiple-links failures, which can fail the working and backup paths at the same time. This can be seen by, for example, when all the links and all the lightpaths are protected, the total network risk with path protection is 8.56 Mbps, higher than in the network with link protection, which is only 7.88 Mbps.

For Network 2 and Network 3, we run the experiments with two different sets of Cable Cut (CC) values: a fixed CC value of 450 km for all links, and varied CC values as indicated in Figure 3.8 and Figure 3.9 for Network 2 and Network 3, respectively. The minimum-risk curves for network 2 with a fixed CC value of 450 km, and varied CC values are shown in Figure 3.11 (a), and Figure 3.11 (b), respectively. Whereas, the minimum-risk curves for network 3 with a fixed CC value of 450 km, and varied CC values are shown in Figure 3.12 (a), and Figure 3.12 (b), respectively.

In the experiments for Network 2 and Network 3, in order to reduce the number of network states in the risk calculation, we consider only network states with at most two simultaneous failures, rather than all possible network states. This reduces the number of network states considered from $2^{|L|}$ to $1 + |L|(|L|+1)/2$, but this underestimates the risk level. However, it still gives a very close approximation of the overall risk level because most of the probability mass is in the network states with a small number of simultaneous failures (e.g., in Network 3 with CC of 450 km, the network states with at most two simultaneous failures constitute the total state probability of .99958). This type of assumption is very common in the network survivability literature which considers only single and dual failures in their analysis [10, 27, 44]. In addition, the work in [46] shows that by considering only *m* most probable states, a good approximation of a performance measure can be obtained with the proper choice of *m* without having to analyze all possible states. In short, considering all possible network states is not necessary in the risk calculation.

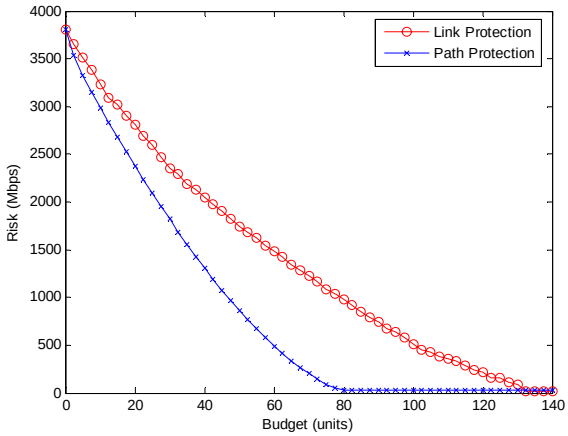


(a)

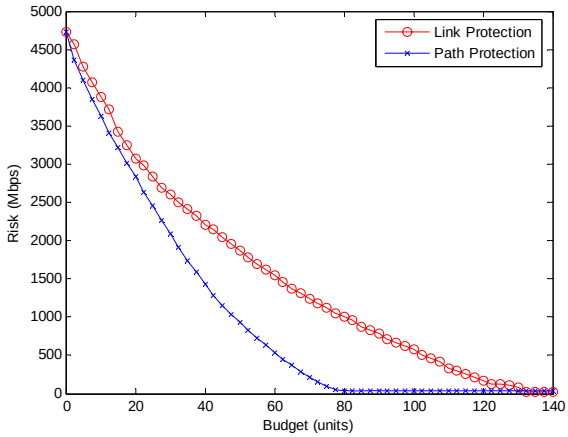


(b)

Figure 3.11 Minimum-risk curves (risk vs budget) for link protection and path protection on Network 2 with (a) a fixed Cable Cut (CC) value of 450 km, and (b) varied Cable Cut (CC) values as indicated in Figure 3.8



(a)



(b)

Figure 3.12 Minimum-risk curves (risk vs budget) for link protection and path protection on Network 3 with (a) a fixed Cable Cut (CC) value of 450 km, and (b) varied Cable Cut (CC) values as indicated in Figure 3.9

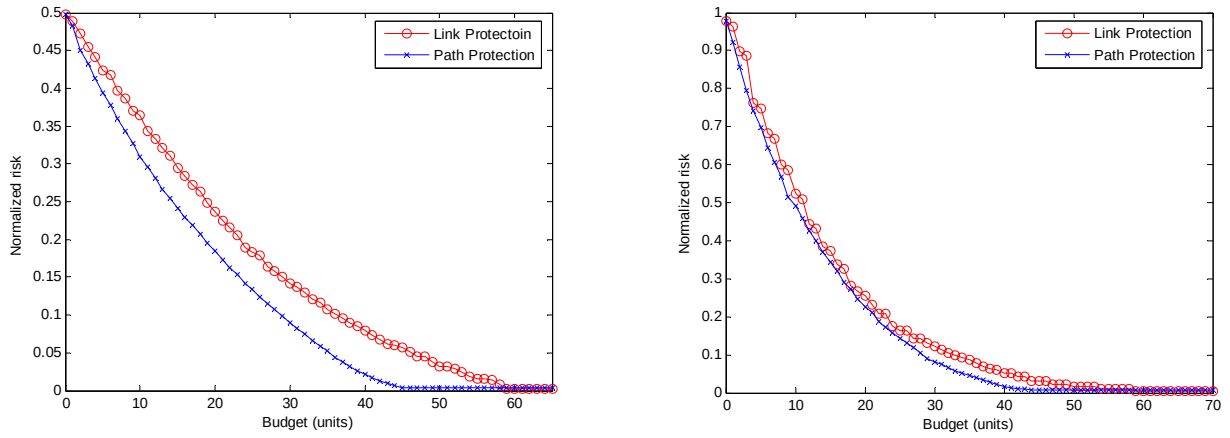
From Figures 3.11 and 3.12, we observe that the minimum-risk curves for both link protection and path protection have a convex shape (i.e., the slope of the risk curve increases, or becomes less negative, as the budget increases), which means that the amount of risk reduction per unit of budget decreases as the budget increases. This is because different parts of the

network are associated with different risk levels; and for a given budget the minimum-risk design seeks to protect a set of links/lightpaths which results in the maximum risk reduction (e.g., more-critical links/lightpaths). Hence, as the budget increases, more links/lightpaths that are relatively less-critical are protected, resulting in a lower risk reduction per unit cost.

The convexity of the risk curve is more apparent in the network with a higher variability of risk level across different parts of the network. For example, the risk curve for Network 2 and Network 3 with varied CC values shown in Figure 3.11 (b) and Figure 3.12 (b) is more convex than the risk curve for the same network with the fixed CC value shown in Figure 3.11 (a) and Figure 3.12 (a), respectively. Note that in Figure 3.10 it is not obvious that the risk curve has a convex shape since Network 1 is too small, in which there are not many selections of links/lightpaths to be protected; and thus the shape of the risk curve is heavily affected by the granularity of backup cost.

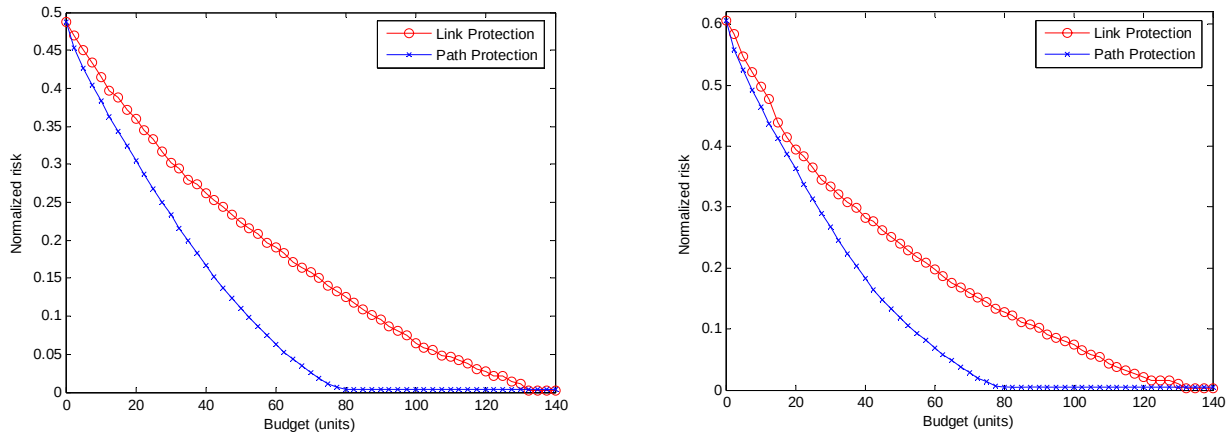
The amount of risk in the risk curves in Figures 3.10–3.12 is presented as a value of risk (i.e., in Mbps of traffic loss rate). However, for a comparison of risk levels across different networks, a normalized risk level should be considered instead. In this experiment, the normalized risk is equal to the value of risk in Mbps of traffic loss rate divided by the total working traffic rate in the network (i.e., $\sum_{r \in R} m_r$) multiplied by a hundred. The minimum-risk curves based on the normalized risk for network 2 with a fixed CC value, and varied CC values are shown in Figure 3.13 (a), and Figure 3.13 (b), respectively. Whereas, the minimum-risk curves based on the normalized risk for network 3 with a fixed CC value, and varied CC values are shown in Figure 3.14 (a), and Figure 3.14 (b), respectively. The results show that the initial normalized risk level of Network 2 with varied CC values in Figure 3.13 (b) is higher than other

networks. This is mainly because on average Network 2 with varied CC values has a higher cable cut rate per km than other networks.



(a) (b)

Figure 3.13 Minimum-risk curves (normalized risk vs budget) for link protection and path protection on Network 2 with (a) a fixed Cable Cut (CC) value of 450 km, and (b) varied Cable Cut (CC) values as indicated in Figure 3.8



(a) (b)

Figure 3.14 Minimum-risk curves (normalized risk vs budget) for link protection and path protection on Network 3 with (a) a fixed Cable Cut (CC) value of 450 km, and (b) varied Cable Cut (CC) values as indicated in Figure 3.9

3.7.2 Cost-benefit analysis

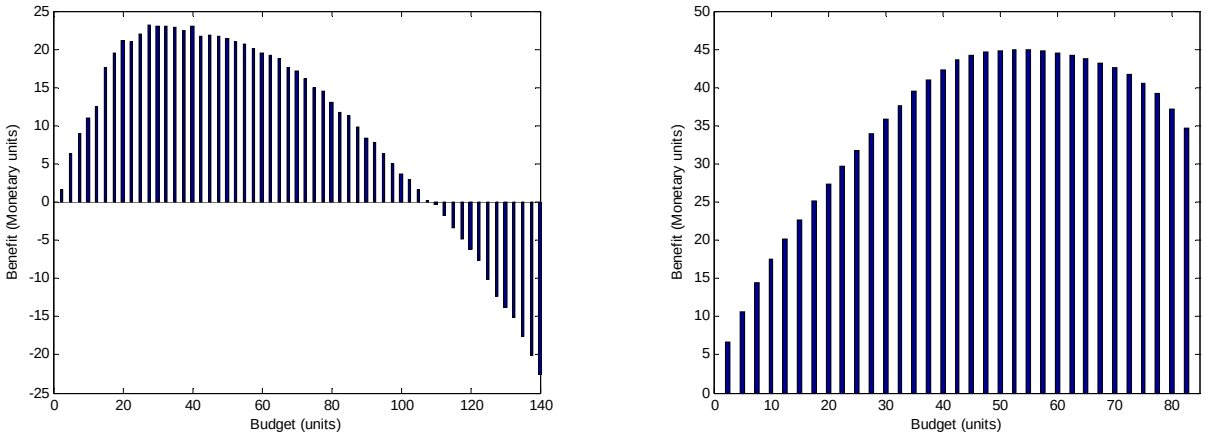
Based on the minimum-risk curves, if information is available, one can convert the amount of risk reduction into a monetary unit; then calculate an investment benefit, which is defined as the reduction in the risk level (in a monetary unit) subtracted by the cost of deploying the survivability technique (i.e., a budget), as shown in (3.118).

$$\text{Investment Benefit (\$)} = \text{Risk Reduction (\$)} - \text{Survivability Cost (\$)} \quad (3.118)$$

The purpose of the cost-benefit analysis here is to demonstrate whether the cost of providing network survivability can be economically justified by the reduction in the risk level. The investment is justified only if the benefit is positive.

For the risk curve of Network 3 in Figure 3.12 (b), if we assume that the reduction in risk level (i.e., expected traffic loss rate) of 40 Mbps is equivalent to one monetary unit, the benefit plot (i.e., benefit vs budget) for link protection, and path protection can be determined as in Figure 3.15 (a), and 3.15 (b), respectively. The benefit plot for link protection in Figure 3.15 (a) shows that the cost of deploying link protection is justified by the reduction in the risk level when the cost is less than or equal to 107.5 units, and it is not justified to invest in link protection for more than or equal to 110 units. In other words, it is not justified to protect all the network links (i.e., it requires 140 budget units to protect all the network links where the benefit is negative), but only some links in the network (i.e., critical links). The benefit plot also suggests that by investing only 27.5 budget units in link protection it results in the maximum benefit. In Appendix B, we give a proof that if the risk curve is convex, there always exists an optimal budget value which maximizes the investment benefit.

Unlike the link protection case, the benefit plot for path protection on the same network in Figure 3.15 (b) suggests that an investment in path protection is justified for all budget values. This can be explained as a result of the higher capacity efficiency of path protection. Since for each budget value, path protection results in a higher risk reduction than link protection as shown in the risk curve in Figure 3.12 (b), and this higher amount of risk reduction can always overcome the cost of path protection in the network. Thus the investment benefit is always positive. The benefit plot for path protection also shows that the optimal budget value, which maximizes the investment benefit, is equal to 52.5 units.

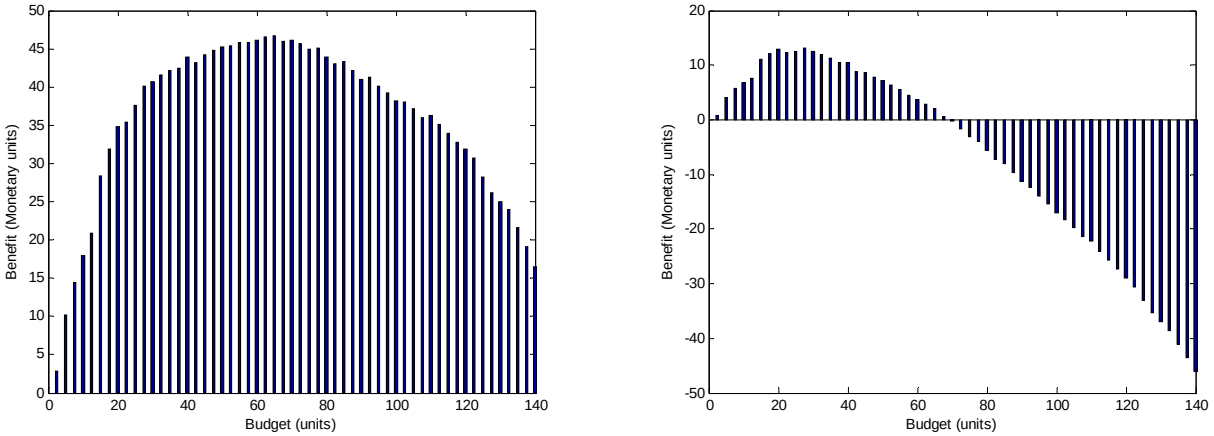


(a) (b)

Figure 3.15 Benefit Plot (benefit vs budget) for (a) link protection, and (b) path protection on Network 3 with varied CC values (assuming a risk reduction of 40 Mbps = 1 monetary unit)

Note that the shape of a benefit plot is greatly affected by the equivalent monetary value of a unit of risk reduction. If the equivalent monetary value of a unit of risk reduction is larger, the benefit plot will tend to shift toward the right, indicating it is more beneficial to invest more in network protection. For example, Figure 3.16 (a) shows the benefit plot for link protection on Network 3, assuming that the reduction in risk level of 30 Mbps is worth one monetary unit. The

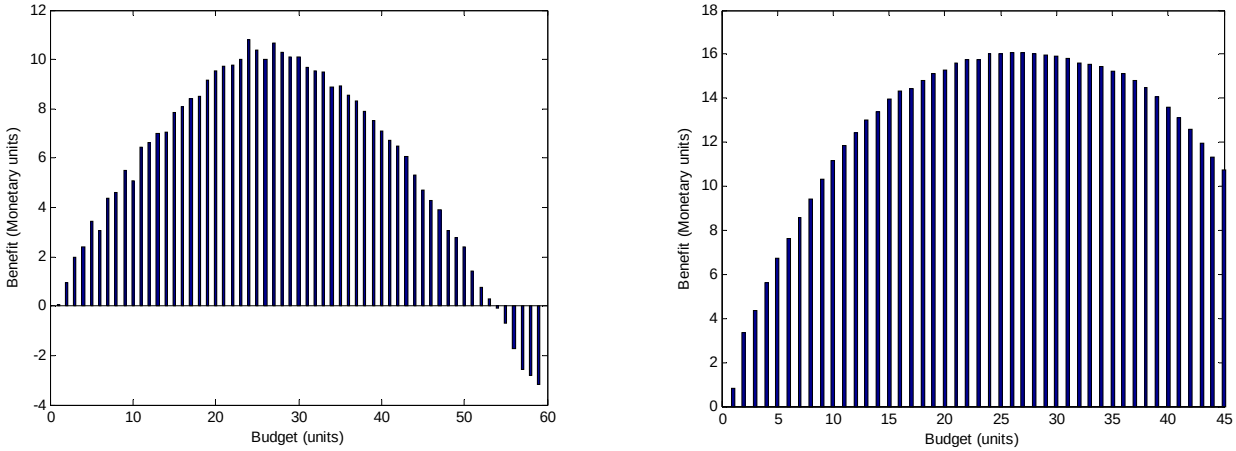
plot indicates that it is justified to invest in a full protection (as compared to the partial protection in Figure 3.15 (a)), and the optimal budget value is now 65 units (as compared to 27.5 units in Figure 3.15 (a)). On the other hand, if the equivalent monetary value for a unit of risk reduction is smaller, the benefit plot will tend to shift toward the left, indicating it is more beneficial to decrease the budget for investing in network protection. For example, Figure 3.16 (b) shows the benefit plot for link protection on Network 3 assuming the reduction in risk level of 50 Mbps is equivalent to one monetary unit. The plot indicates that an investment is only justified when the budget is less than or equal to 67.5 budget units (as compared to 107.5 budget units in Figure 3.15 (a)).



(a) (b)

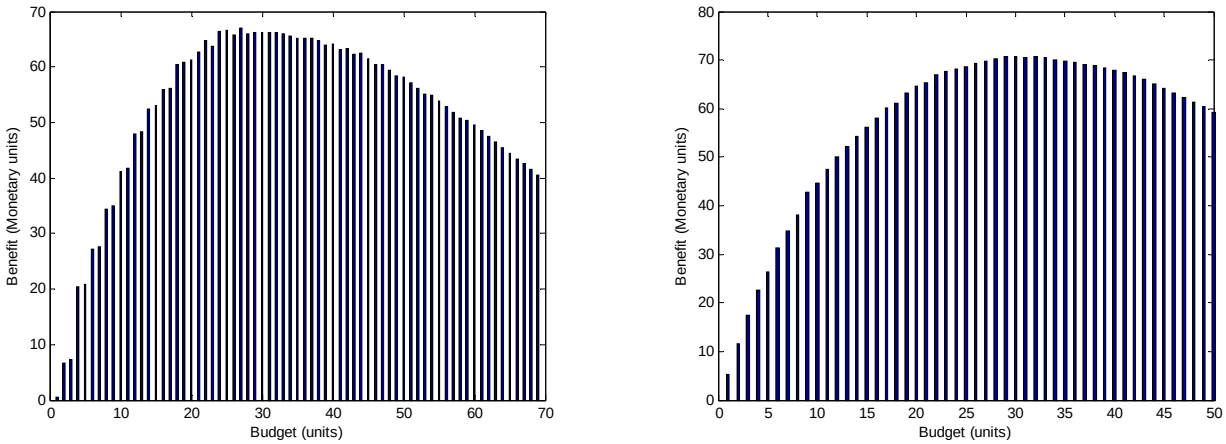
Figure 3.16 Benefit plot (benefit vs budget) for link protection on Network 3 with varied CC values assuming (a) a risk reduction 30 Mbps = 1 monetary unit, and (b) a risk reduction of 50 Mbps = 1 monetary unit

The benefit plots for link protection and path protection on Network 2 with a fixed CC value of 450 km, and varied CC values are shown in Figures 3.17, and 3.18, respectively; whereas the benefit plots for link protection and path protection on Network 3 with a fixed CC value of 450 km are shown in Figures 3.19. These plots assume that the reduction in risk level of 40 Mbps is equal to one monetary unit.



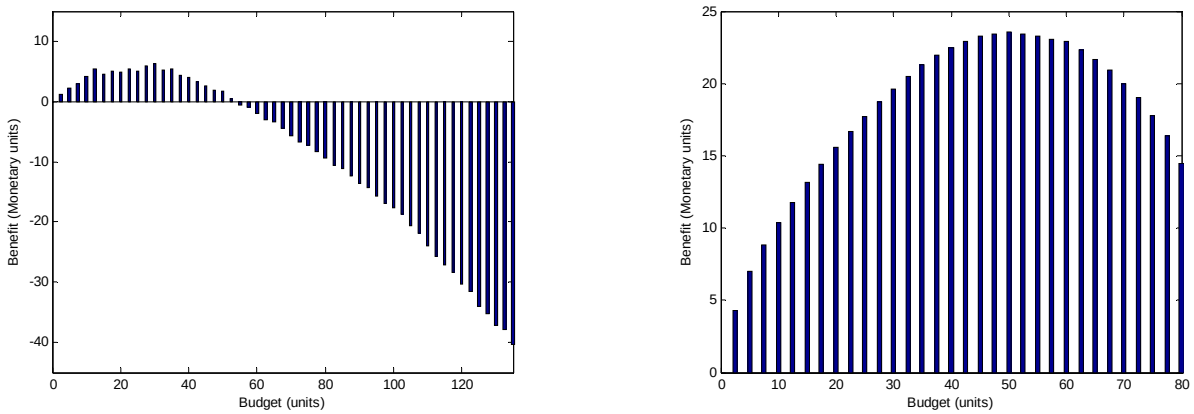
(a) (b)

Figure 3.17 Benefit plot (benefit vs budget) for (a) link protection and (b) path protection on Network 2 with a fixed CC value of 450 km (assuming a risk reduction of 40 Mbps = 1 monetary unit)



(a) (b)

Figure 3.18 Benefit plot (benefit vs budget) for (a) link protection and (b) path protection on Network 2 with varied CC values (assuming a risk reduction of 40 Mbps = 1 monetary unit)



(a) (b)

Figure 3.19 Benefit plot (benefit vs budget) for (a) link protection and (b) path protection on Network 3 with a fixed CC value of 450 km (assuming a risk reduction of 40 Mbps = 1 monetary unit)

3.7.3 Comparison of heuristic and InP approaches

In this section, the heuristic solution algorithms and the InP approach are evaluated and compared both in terms of the optimality and the computational times. For link-path InP models, all possible routes within two hops from the shortest backup route are used as the set of pre-computed backup routes. These pre-computed backup routes are link-disjoint from their corresponding working entity. The numbers of pre-computed routes used in the experiments for each network and each protection technique are summarized in Table 3.7, as the average number, the minimum number, and the maximum number.

Table 3.7 The number of pre-computed backup routes used in link-path InP models

	Network 1		**Network 2**		**Network 3**	
	Link protection	**Path protection**	**Link protection**	**Path protection**	**Link protection**	**Path protection**
Average	3.1	2.8	16.5	21.3	5.9	10.7
[Min,Max]	[3, 4]	[2, 4]	[10, 28]	[10, 53]	[3, 17]	[1, 53]

The results on Network 1, Network 2 and Network 3 with link protection and path protection show that the link-path InP formulation with all possible routes within two hops from the shortest backup route as a set of pre-computed backup routes always yields the same optimal results as the node-link formulation. This proves that for our sample networks a set of pre-computed routes is large enough to include the optimal backup routes.

For the heuristic approach, a link-disjoint route with minimum path unavailability is used as a pre-computed backup route for each protected link and protected lightpath. Since there is only one candidate backup route available, the design problem does not need to determine which backup route to use, but only to determine which links to protect in the link protection case, and which lightpaths to protect in the path protection case. Table 3.8 and Table 3.9 present, for each heuristic algorithm, an average error from the optimal result obtained from the InP approach over a number of problem instances on Network 2 and Network 3 with a fixed CC value of 450 km. Note, that only the problem instances with budget values that result in partial protection are used in the calculation of average errors, since for all other budget values, the InP and heuristic approaches produce the same results (i.e., not protecting at all, or protecting all links/lightpaths).

Table 3.8 Average error of heuristics for link protection and path protection on Network 2

	Average error (%) from Optimal Solutions	
	Link Protection	**Path Protection**
Heuristic 1	18.97	7.78
Heuristic 2	6.97	1.36
Heuristic 3	1.99	0.29

Table 3.9 Average error of heuristics for link protection and path protection on Network 3

	Average Error (%) from Optimal Solutions	
	Link Protection	**Path Protection**
Heuristic 1	27.42	7.72
Heuristic 2	19.63	1.53
Heuristic 3	3.70	0.53

On average, Heuristic 2 outperforms Heuristic 1. This is because Heuristic 2 takes the cost of the backup path into consideration when making decisions (i.e., the amount of risk reduction per unit cost is used as the selection criteria rather than the amount of risk reduction alone). Furthermore, Heuristic 3 always outperforms Heuristic 2 since it uses the result from Heuristic 2 as an initial solution upon which it iteratively improves to produce a better solution.

The computational times of Heuristic 3, node-link InP approach, and link-path InP approach for link protection and path protection on Network 2 are compared in Figure 3.20 (a) and Figure 3.20 (b), respectively; whereas the computational times for link protection and path protection on Network 3 are shown in Figure 3.21 (a), and Figure 3.21 (b), respectively. The computational times of Heuristic 1 and Heuristic 2 are not shown because they are shorter than the computational time of Heuristic 3.

The results show that the node-link InP model cannot guarantee to produce an optimal solution within a reasonable time. For example in Figure 3.21 (a) there are many problem instances where the computational time is longer than 3 hours, and two problem instances where the node-link model cannot find an optimal solution in 3 days (represented by 7×10^4 sec in the figure). The results also show that the link-path InP model can provide an optimal solution with a much faster time than the node-link model, i.e., for our network examples an optimal solution can be found within 1 minute for each problem instance. This is understandable because the link-

path InP model limits the number of candidate backup routes considered, thereby reducing the size of the searching space for the optimization problem. However, in general as in any InP approach, the link-path model cannot guarantee a scalable computational time since it is well known that InP problems are NP-hard. This is one of the motivations why the heuristic approach is necessary. Another motivation for considering the heuristic approach is that it can be applied to a problem with a non-linear objective function, which cannot be solved by the InP approach (note that one of the risk-based design problems with non-linear objective function, namely the minimum-RMS damage design, is considered in Chapter 4). For our network examples, the results show that Heuristic 3 could provide good near-optimal solutions within a reasonable time, i.e., a few ten seconds for most of problem instances, and less than 5 minutes for all problem instances.

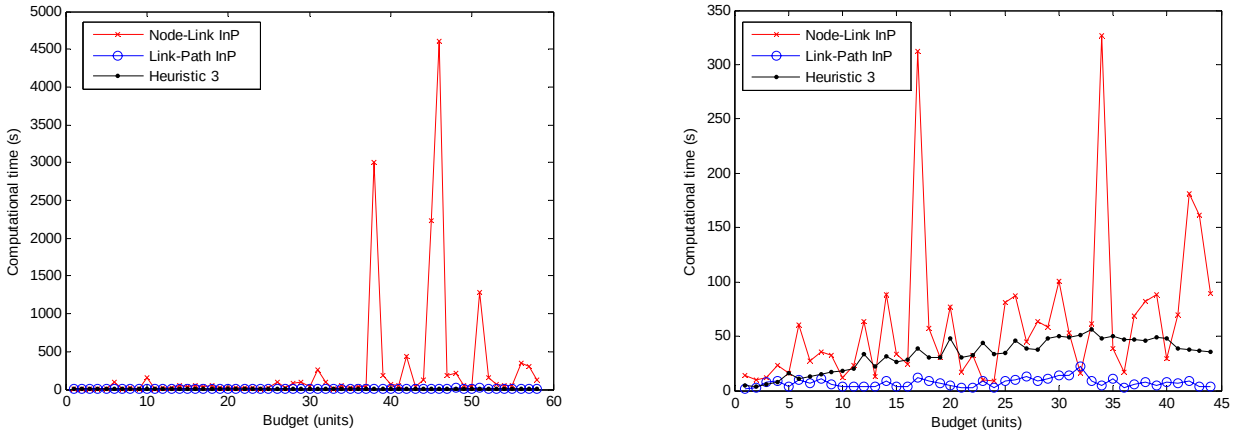


Figure 3.20 Computational times of InP approach and Heuristic 3 for (a) link protection, and (b) path protection on Network 2 with a fixed CC value of 450 km

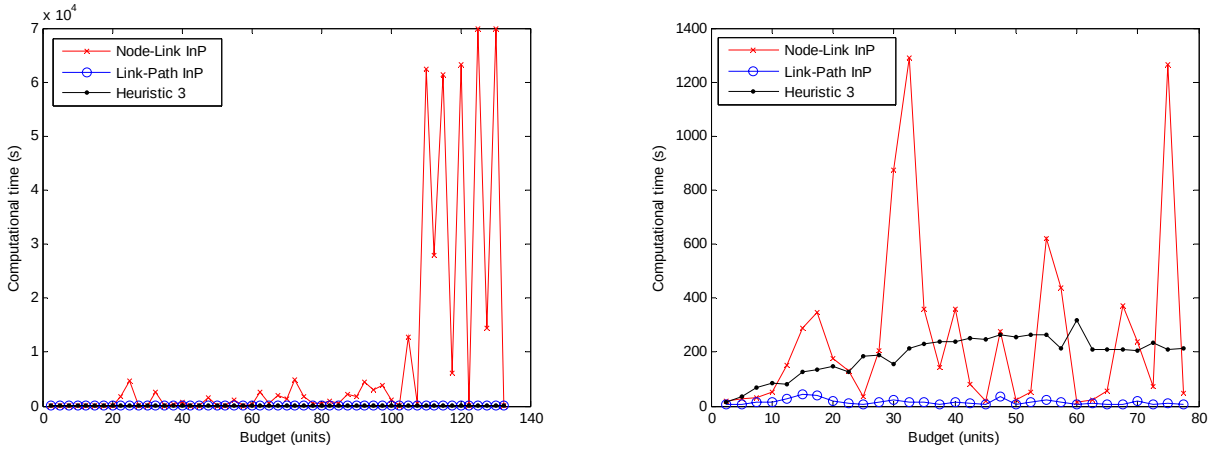


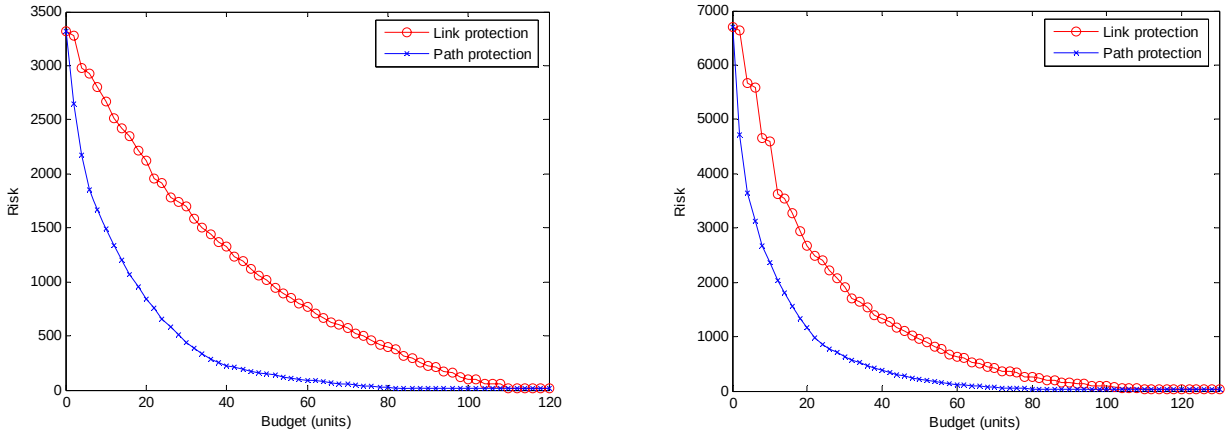
Figure 3.21 Computational times of InP approach and Heuristic 3 for (a) link protection, and (b) path protection on Network 3 with a fixed CC value of 450 km

3.7.4 Minimum-risk survivable network design for networks with multiple classes of traffic

This section presents the results from the minimum-risk survivable network design for networks with multiple classes of traffic. The design problems as formulated in the Integer Programming (InP) models of Section 3.5 were solved using a commercial AMPL/CPLEX solver. In the experiments, we define the damage level caused by a failure of a bronze, silver, and gold traffic flow as 1,000, 10,000, and 50,000 units, respectively (i.e., d_r^B=1,000, d_r^S=10,000, and d_r^G=50,000). For bronze traffic, full-mesh lightpath demands between all node-pairs are assumed; whereas for silver and gold traffics, partial-mesh lightpath demands (i.e., between some node-pairs) are assumed in each network. Each lightpath carries the same data rate of 10 Gbps. In Network 2, the bronze, silver, and gold traffic flows are account for 53.79%, 38.64%, and 7.57% of the total network working capacity; whereas in network 3, the bronze, silver, and gold traffic flows are account for 56.16%, 35.62%, and 8.22% of the total network working

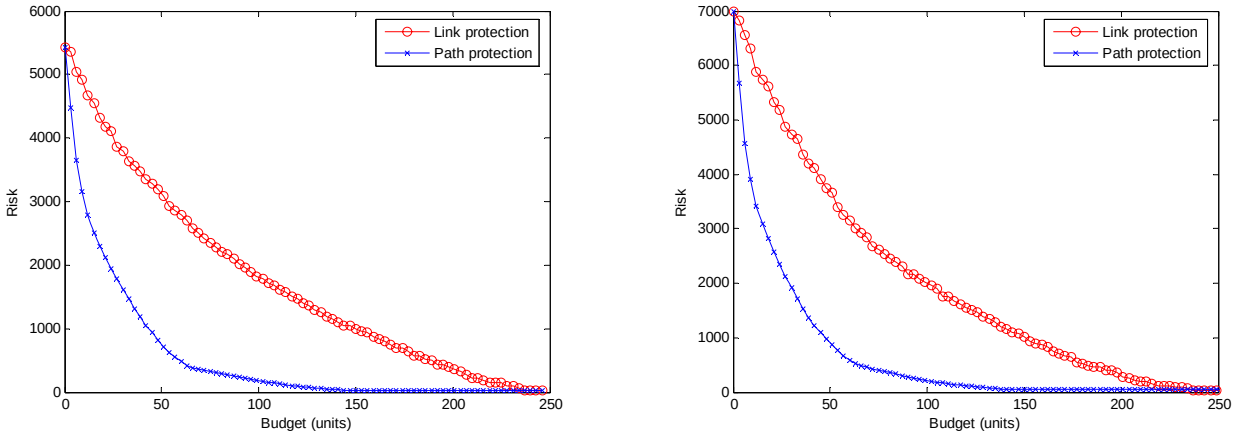
capacity, respectively. In addition, only network states with at most two simultaneous failures are considered in the risk calculation.

The minimum-risk curve for Network 2 with multiple classes of traffic and a fixed CC value of 450 km is shown in Figure 3.22 (a), and with varied CC values in Figure 3.22 (b). Whereas, the minimum-risk curve for Network 3 with multiple classes of traffic and a fixed CC value of 450 km is shown in Figure 3.23 (a), and with varied CC values in Figure 3.23 (b). The results show that in networks with multiple classes of traffic, the path protection technique results in the higher rate of risk reduction than the link protection at low budget values. This is understandable because at low budget values the path protection technique can choose to protect only the traffic flows associated with higher damage levels (e.g., gold traffic flows only), whereas the link protection technique when protecting a link has to protect all of the traffic on the link regardless of class.



(a) (b)

Figure 3.22 Minimum-risk curves (risk vs budget) for Network 2 with multiple classes of traffics and (a) fixed CC values of 450 km, and (b) varied CC values

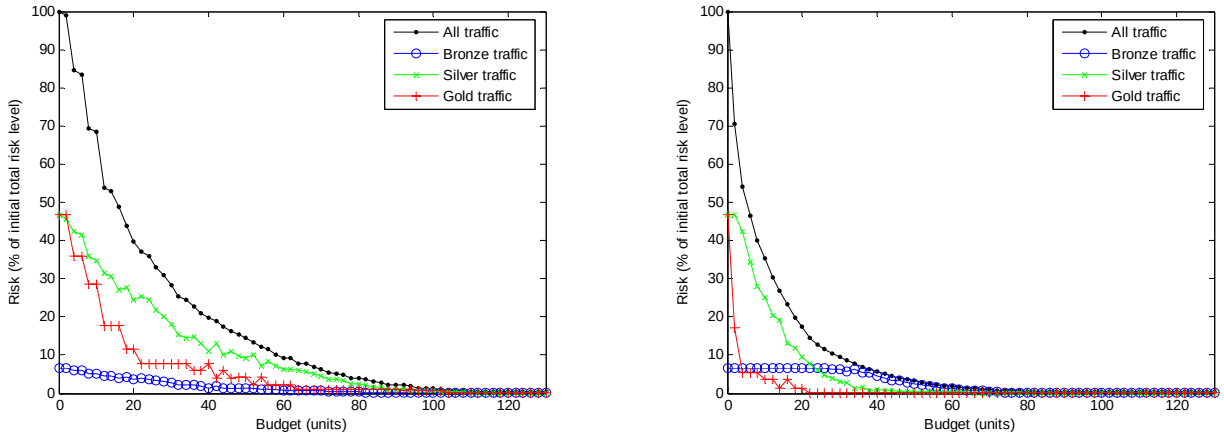


(a) (b)

Figure 3.23 Minimum-risk curves (risk vs budget) for Network 3 with multiple classes of traffics and (a) fixed CC value of 450 km, (b) varied CC values

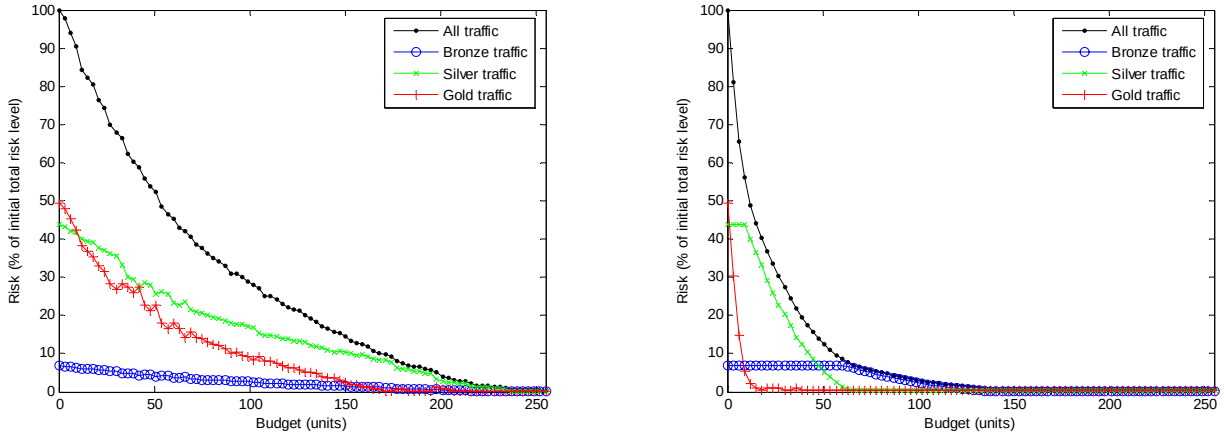
Figures 3.22–3.23 show the risk curves as the total risk level of all traffic in the network regardless of traffic class. In contrast, the risk curves for different classes of traffic are presented in Figures 3.24–3.27. The risk curves in Figures 3.24 and 3.25 show the risk levels of different traffic classes that constitute the total risk level in Network 2 and Network 3, respectively. In these figures, the risk is presented as a percentage of the initial total risk level in the network. Whereas, the risk curves in Figures 3.26 and 3.27 show the risk level as a percentage of the initial risk level of its own traffic class and all traffic in Network 2 and Network 3, respectively.

The results in Figures 3.24–3.27 show that the gold traffic class has the highest rate of risk reduction; whereas the bronze traffic class has the lowest rate of risk reduction. The differentiation in the rate of risk reduction among traffic classes is more apparent in the path protection case in which the protection technique can choose to protect only specific traffic flows based on the class. Note that the risk levels of different traffic classes as presented in Figures 3.24 and 3.25 also depend on the amount of traffic, and the damage level caused by the failure of a lightpath in each traffic class.



(a) (b)

Figure 3.24 Risk curves (a percentage of the initial total risk level) for different classes of traffic in Network 2 with varied CC values and (a) link protection, and (b) path protection



(a) (b)

Figure 3.25 Risk curves (a percentage of the initial total risk level) for different classes of traffic in Network 3 with varied CC values and (a) link protection, and (b) path protection

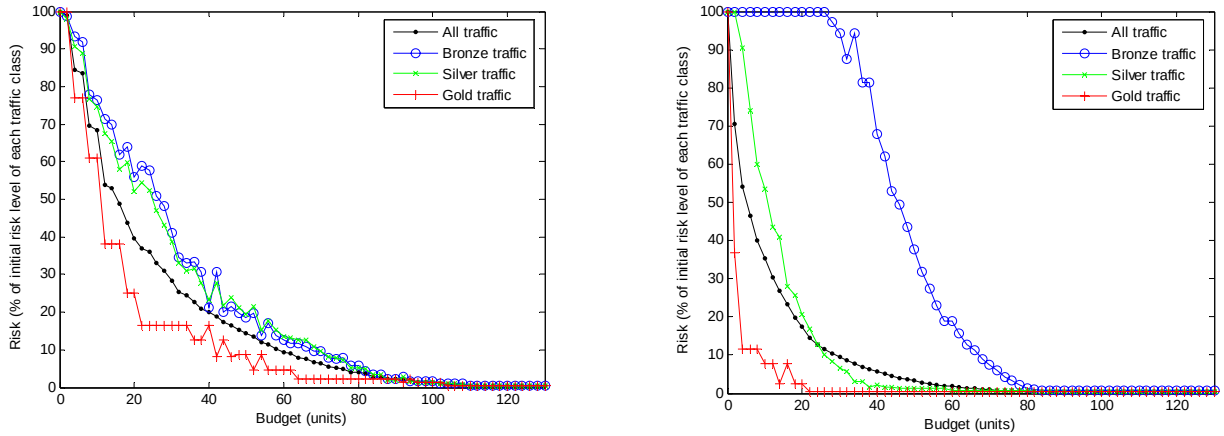


Figure 3.26 Risk curves (a percentage of the initial risk level of each traffic class) in Network 2 with varied CC values and (a) link protection, and (b) path protection

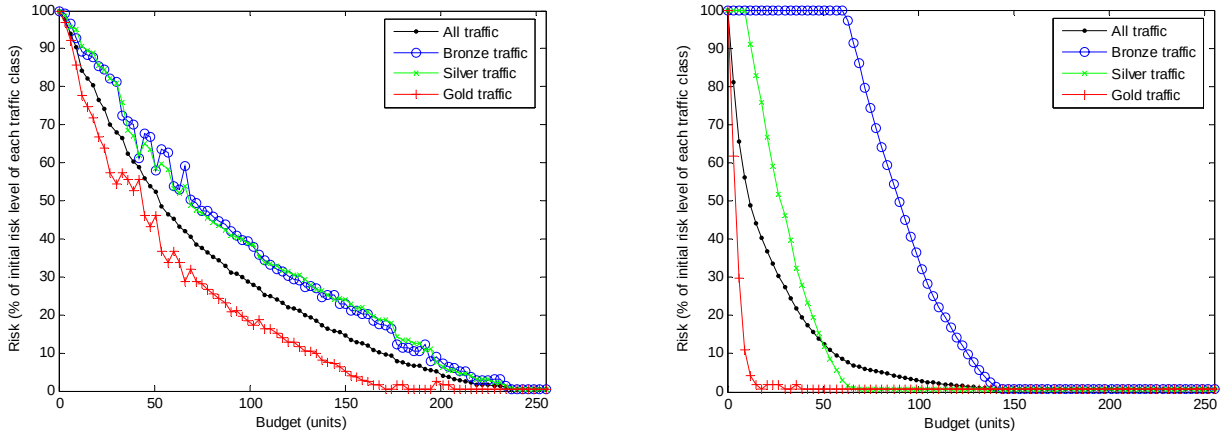


Figure 3.27 Risk curves (percentage of the initial risk level of each traffic class) in Network 3 with varied CC values and (a) link protection, and (b) path protection

The minimum-risk network design is also compared with the minimum-cost network design in terms of the total risk, and the survivability cost. Table 3.10–3.13 show the remaining risk level in the network, and the corresponding required budget for both the minimum-risk design and the minimum-cost design, with link protection and path protection on Network 2, and Network 3 supporting multiple classes of traffic, respectively. In these tables, the remaining risk level is presented as a percentage of the initial risk level in the network given to the current design (i.e., in this case, it is the amount of total risk when the network is not protected), whereas the budget is presented as a percentage of the cost required by the minimum-cost design to survive all single-link failures. The results show a tradeoff between the remaining risk level in the network, and the amount of budget saving that can be achieved in the minimum-risk network design. For example, Table 3.11 shows that by allowing the remaining risk level of 5% in the network, the protection requires only 53.11% of the cost required by the minimum-cost design; thereby we can achieve a budget saving of 46.89%. Moreover, if the same network is designed to have the remaining risk level of about 2% and 1%, we can achieve a budget saving of 30% and 15.51%, respectively.

Note that the minimum-risk design can achieve the lower risk level than the minimum-cost design, but possibly requiring a higher cost. For example in Table 3.11, the minimum-risk design requires a budget of 103.80% of the minimum cost to achieve the lowest risk level at 0.50 %; whereas the minimum-cost design results in a remaining risk level of 0.59%. In this case both designs protect all the links or all the lightpaths in the network; however the difference is that the minimum-risk design chooses the backup routes that have a lower risk, but require higher costs than the minimum-cost design.

Table 3.10 Risk and budget comparisons between minimum-risk design and minimum-cost design for Network 2 with link protection and varied CC values

Remaining Risk Level (% of initial risk level)	**Budget** (% of cost required by minimum-cost design)
Minimum-risk design	
50%	14.58%
25%	30.98%
10%	54.67%
5%	69.25%
2%	85.65%
0.74%	94.76%
0.44% (minimum risk level)	112.98%
Minimum-cost design	
0.57%	100%

Table 3.11 Risk and budget comparisons between minimum-risk design and minimum-cost design for Network 2 with path protection and varied CC values

Remaining Risk Level (% of initial risk level)	**Budget** (% of cost required by minimum-cost design)
Minimum-risk design	
50%	7.24%
25%	19.31%
10%	36.21%
5%	53.11%
2%	70.00%
0.97%	84.49%
0.50% (minimum risk level)	103.80%
Minimum-cost design	
0.59%	100%

Table 3.12 Risk and budget comparisons between minimum-risk design and minimum-cost design for Network 3 with link protection and varied CC values

Remaining Risk Level (% of initial risk level)	**Budget** (% of cost required by minimum-cost design)
Minimum-risk design	
50%	22.80%
25%	48.14%
10%	72.21%
5%	84.88%
2%	92.48%
0.99%	98.82%
0.51% (minimum risk level)	113.89%
Minimum-cost design	
0.54%	100%

Table 3.13 Risk and budget comparisons between minimum-risk design and minimum-cost design for Network 3 with path protection and varied CC values

Remaining Risk Level (% of initial risk level)	**Budget** (% of cost required by minimum-cost design)
Minimum-risk design	
50%	8.42%
25%	23.14%
10%	39.97%
5%	56.80%
2%	79.94%
0.95%	94.67%
0.72% (minimum risk level)	100.98%
Minimum-cost design	
0.76%	100%

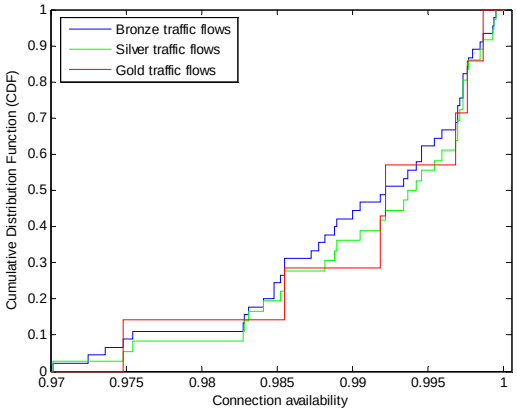
Lastly, the results from the minimum-risk design are presented in term of the connection availability. Unlike the total network risk presented earlier which is a measure for the whole network, the connection availability presented here is a measure for each traffic flow. Figures 3.28 and 3.29 present the Cumulative Distribution Function (CDF) of connection availability across all connections in each traffic class in Network 2, and Network 3 with varied CC values, respectively. The given budget values used in the experiments for link protection, and path protection are the same, which are 28 units and 48 units for Network 2 and Network 3, respectively. The given budget of 28 units is about one fourth of the minimum cost required for protecting all the links, and about one third of the minimum cost required for protecting all the end-to-end paths in Network 2. Whereas, the given budget of 48 units is about one fifth of the minimum cost required for protecting all the links, and about one third of the minimum cost required for protecting all the end-to-end paths in Network 3.

Figures 3.28 (a) and 3.29 (a) show that when the networks are not protected, the connection availability for all traffic classes are roughly the same. In the link protection case, the results in Figures 3.28 (b) and 3.29 (b) show that for the given budget the connection availability for all traffic classes are improved; the gold-class traffic flows have the highest connection availability, followed by the silver-class traffic flows which have a slightly higher connection availability than the bronze-class traffic flows.

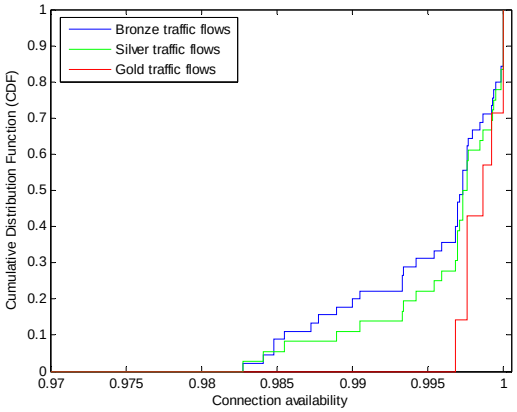
In path protection, for the given budget the results in Figure 3.28 (c) and Figure 3.29 (c) show that the minimum-risk design could improve the connection availability for the gold-class traffic flows significantly; whereas the connection availability for the silver traffic class is improved moderately, and the connection availability for the bronze-class traffic flows is unchanged. This is understandable because in this example the minimum-risk design allocates

the fixed budget to protect all the traffic flows in the gold class, and then allocate the remaining budget to protect the silver-class traffic flows such that the total network risk is minimized.

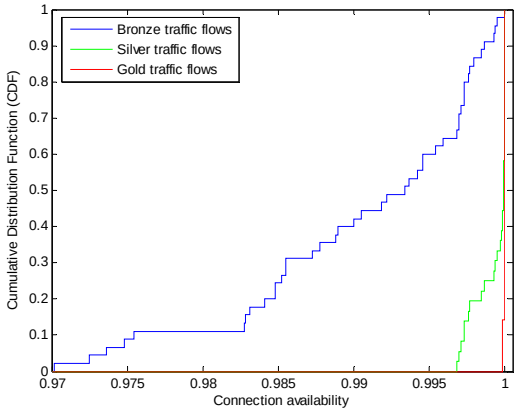
In conclusion, the above results show that path protection has a better differentiation among traffic classes than link protection, and the minimum-risk design approach can be used to provide differential classes of availability or protection to traffic in accordance with the different availability requirements of different traffic classes (e.g., as defined in SLA).



(a)



(b)



(c)

Figure 3.28 Cumulative Distribution Function (CDF) of connection availability across all connections in each traffic class for (a) no protection, (b) link protection with a budget of 28 units, and (c) path protection with a budget of 28 units, on Network 2 with varied CC values.

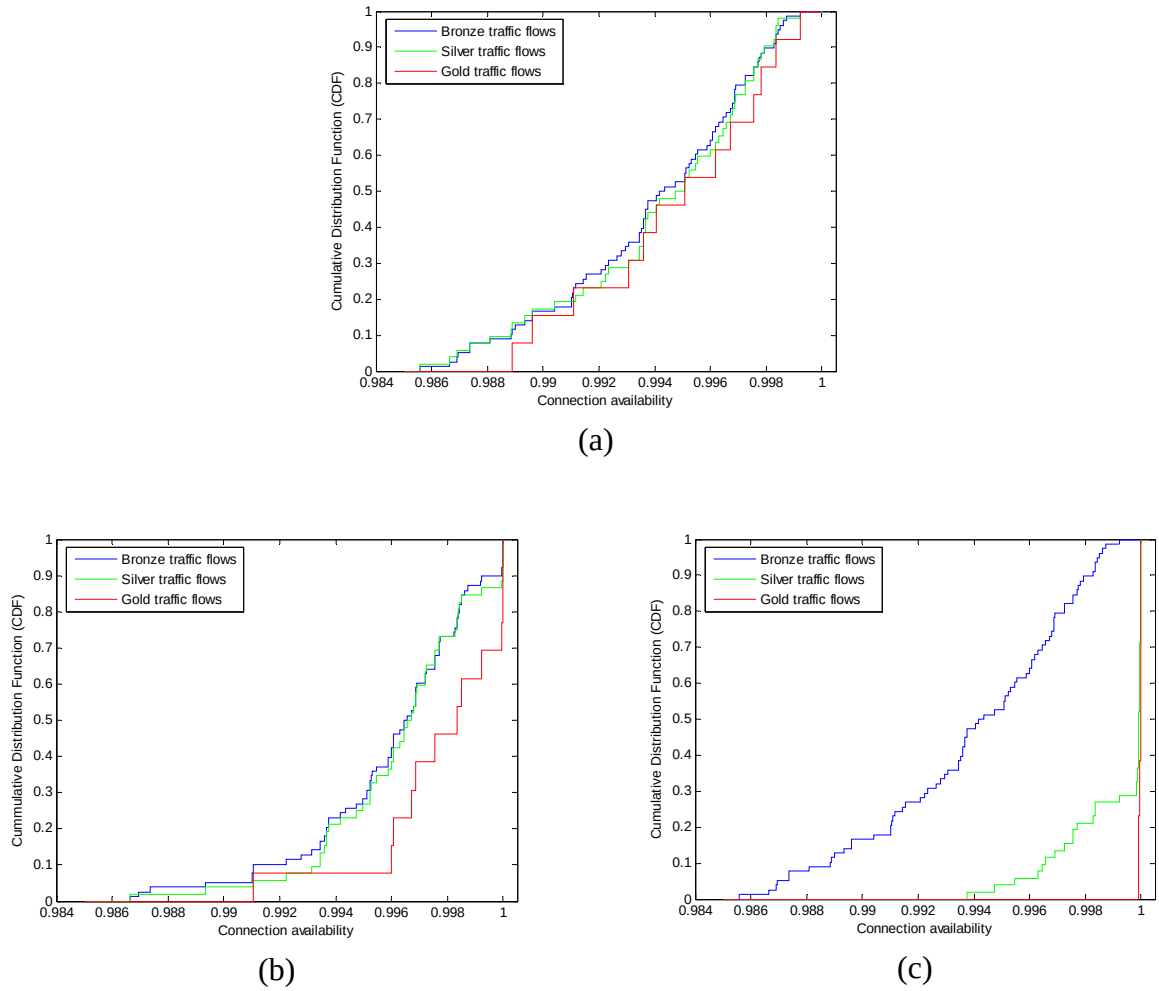


Figure 3.29 Cumulative Distribution Function (CDF) of connection availability across all traffic connections in each traffic class for (a) no protection, (b) link protection with a budget of 48 units, and (c) path protection with a budget of 48 units, on Network 3 with varied CC values.

3.7.5 Sequence of incremental minimum-risk designs

The risk-based survivable network design approach does not assume a Greenfield network condition. In fact, it is well suit to an incremental design approach where the risk is reduced through a series of incremental designs (e.g., quarterly, semi-annual, etc.). A network given to the design problem might be partially fault-tolerant, in which a survivability technique can be

incrementally deployed to further reduce the network risk. For each design increment, the design problem is to determine in which parts of the network to deploy a survivability technique as an addition to the existing survivability mechanisms already in the network in order to minimize the total network risk, while subject to a budget constraint. Typically, it is also assumed that a reconfiguration of existing survivability mechanisms is not possible.

Note, that in general the InP formulations for incremental survivable network design require sets of constraints to fix the values of decision variables corresponding to all protected links (in the link protection case), or all protected lightpaths (in the path protection case), and their backup routes at the values from the previous design. Thus the design problem is to optimize over the remaining variables only. Furthermore, a budget constraint must calculate the spare capacity cost that occurs only in the current incremental design.

In this section, different incremental investment alternatives are compared on the basis of risk. In the experiment, each incremental investment alternative is given the same capital expenditure, but invested at different times. Three incremental investment alternatives are considered: annual, semi-annual, and quarterly investments, representing one-time investment, two consecutive investments, and four consecutive investments, respectively. For each incremental investment alternative the amount of capital expenditure is divided equally over the investments (i.e., uniform series of investments). Due to a modular cost of a backup path, a portion of budget might be left uninvested from each investment. This remaining budget is made available to the subsequent investment for a fair comparison.

For Network 2 and Network 3, the given capital expenditure is 40 units and 50 units, respectively. Table 3.14 and Table 3.15 show the resulting risk after each incremental investment for three different investment alternatives using link protection on Network 2 and Network 3,

with a fixed CC value of 450 km. The result shows that, after all investments, the quarterly investment results in a higher risk remaining to the network (e.g., 381.96 Mbps in Network 2, and 1,809.37 Mbps in Network 3) than the other two investment alternatives (e.g., 357.80 Mbps in Network 2, and 1,737.21 Mbps in Network 3). This is understandable because the quarterly investment has a smaller available budget per investment; therefore it may select to protect links that are not a part of optimal set of protected links selected by the investment alternatives with a larger budget per investment.

Table 3.14 Risk results from three different incremental minimum-risk investment alternatives for link protection on Network 2, and a given capital expenditure of 40 units

	Risk result from each investment (Mbps)			
	Quarter 1	Quarter 2	Quarter 3	Quarter 4
Annual Investment	357.80			
Semi-annual Investment	1061.85		357.80	
Quarterly Investment	1638.86	1092.56	654.09	381.96

Table 3.15 Risk results from three different incremental minimum-risk investment alternatives for link protection on Network 3, and a given capital expenditure of 50 units

	Risk result from each investment (Mbps)			
	Quarter 1	Quarter 2	Quarter 3	Quarter 4
Annual Investment	1737.21			
Semi-annual Investment	2598.51		1737.21	
Quarterly Investment	3090.42	2604.73	2135.92	1809.37

The results in Table 3.14 and Table 3.15 also show that, in incremental investments the prior investment always results in a higher level of risk reduction than each subsequent investment. For example, the semi-annually incremental investments in Table 3.15 show that the first investment which invests half of the capital expenditure results in an amount of risk reduction of 3,803.54 – 2,598.51 = 1,205.03 Mbps (3,803.54 Mbps is an amount of risk in Network 3 with no protection deployed as shown in Figure 3.12 (a)), whereas the second investment which invest the other half of the capital expenditure results in a lower amount of risk reduction, which is only 2,598.51 – 1,737.21 = 861.30 Mbps. These observations can be explained based on the fact that different links in the network are associated with different risk levels; and each incremental investment tries to protect a set of links that are associated with the maximum risk reduction, and thus leaves a set of links that only result in a lower risk reduction per investment to be protected in subsequent investments.

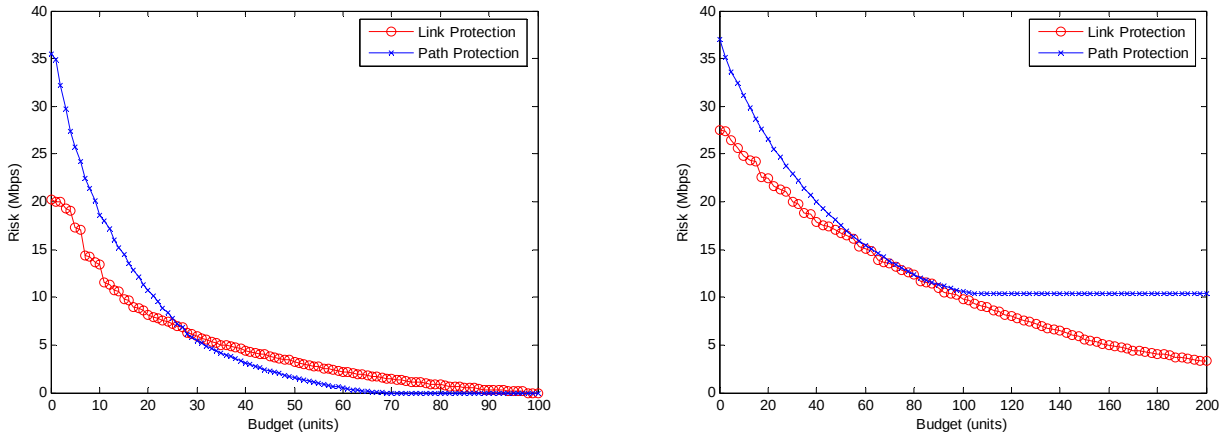
3.7.6 Incremental minimum-risk design with dual protection

In the numerical experiments, the incremental minimum-risk design problems with dual protection as formulated in the Integer Programming (InP) models of Section 3.6 were solved using a commercial AMPL/CPLEX solver. A network given to the problem was designed using the minimum-cost design approach to protect all single-link failures. In addition, only network states with at most two simultaneous failures are considered in the risk calculation.

The minimum-risk curves for dual protection on Network 2, and Network 3 are shown in Figure 3.30 (a) and Figure 3.30 (b), respectively. In these figures, a budget represents the spare capacity cost for the second backup paths only, not including the cost for the first backup paths.

The results show that the initial risk level (i.e., the risk level when budget = 0) in the path-protected network is higher than in the link-protected network. This is because in the networks which are designed to survive any single-link failure, path protection is more susceptible to dual-link failures which can fail the working and backup paths at the same time than the link protection since it has a longer backup path, and the protected path is also longer than a protected link. As the budget increases, path protection results in a higher rate of risk reduction than the link protection due to its higher spare capacity efficiency; therefore there is a point where the two risk curves intersect as shown in the figures. In addition, the risk curves for Network 2 in Figure 3.30 (a) also shows that when the budget is sufficiently enough to protect all the links, or all the lightpaths with dual backup paths, the total risk is reduced to zero, as the network could survive any single-link and dual-link failure. On the other hand, the risk curves for Network 3 in Figure 3.30 (b) show that the risk can never be reduced to zero as the budget increases. This is understandable because node 1 in Network 3 has a nodal degree of two, therefore there are some links and lighpaths in the network (e.g., any links and any lightpaths that has node 1 as an end node such as link 1-8 and link 1-9) for which two link-disjoint backup paths cannot be found, and thus the network is still susceptible to some dual-link failures.

The results also show that the minimum-risk curves for an investment in the second backup paths also have a convex shape similar to the risk curves for investing in the single backup paths in Section 3.7.1. Therefore, we can conclude that there always exists an optimal budget value which maximizes the benefit of an investment in the second backup paths.



(a) (b)

Figure 3.30 Minimum-risk curves (risk vs budget) for deploying the second backup paths in (a) Network 2, and (b) Network 3 with varied CC values

3.8 CONCLUSIONS

In this chapter, the methodology for the proposed risk-based design approach is presented. The design approach consists of two components: a risk assessment and a risk-based investment strategy. The risk assessment is a process of quantifying the risk associated with failures in the network. A fault tree model is used as a failure-relationship model to determine a set of failed lightpaths in each network state. Closed-form formulas for the risk calculation for link-protected networks and path-protected networks are determined. The risk-based investment strategy is used to determine how best to spend a fixed budget for deploying a survivability technique in different parts of the network based on the risk.

The basic risk-based survivable network design approach, namely; the minimum-risk survivable network design, is presented in the chapter. The minimum-risk link protection design

problem and the minimum-risk path protection design problem are formulated as Integer Programming (InP) models. Both the node-link model and the link-path model are provided for each design problem. However, since the InP approach is not scalable to large problems and cannot guarantee to provide an optimal solution within a reasonable time, a set of greedy-based heuristic algorithms are proposed as a method to approximate an optimal solution within a reasonable time.

Through numerical results, various aspects of the minimum-risk survivable network design are disclosed. First, for a given budget, the minimum-risk path protection design provides a lower total network risk than the minimum-risk link protection design due to its higher capacity efficiency. Moreover, the minimum-risk curves (risk vs budget) have a convex shape, which reflects the fact that different parts of the network are associated with different risk levels; therefore the risk reduction rate is not a constant, but a decreasing function of budget. The results also show that the degree of risk curves' convexity varies according to a variation in risk levels associated with different parts of the network. Based on the risk curve, a cost-benefit analysis can be conducted to determine whether an investment in network protection is economically justified by the amount of risk reduction, and one can determine the optimal budget value which maximizes the benefit of an investment. A proof in Appendix B shows that if the risk curve is convex, there always exists an optimal budget value.

In term of the performance of the risk-based network design solution methods, the results show that for the network examples considered, the link-path InP model could provide the same optimal solutions as the node-link InP models with much shorter computational times. Also, the third proposed greedy algorithm (i.e., the iterative greedy heuristic) could provide good near-optimal solutions within scalable times.

The extension of the minimum-risk design to networks with multiple classes of traffic was also presented. For our network examples, the results show that we can achieve a substantial budget saving by allowing a slightly higher risk level in the network. This shows one advantage of the risk-based design over the conventional minimum-cost design in that it allows a tradeoff between the budget and the reduction in risk level in the network. In addition, the results indicate that the minimum-risk design approach can be used to provide differential classes of availability or protection to traffic in accordance with the different availability requirements of different traffic classes defined in Service Level Agreements (SLA); and that path protection has a better differentiation among traffic classes than link protection.

Another extension considered is the incremental minimum-risk design. Two different scenarios for the incremental minimum-risk design are considered: a sequence of minimum-risk investments, and an incremental minimum-risk design with dual protection. The results from the sequence of incremental minimum-risk investments show a disadvantage of the quarterly investments which results in a higher risk level as compared to the annual investment or semi-annual investments. The results from the incremental minimum-risk investment with dual protection show that its risk curves also have a convex shape.

4.0 ALTERNATIVE RISK-BASED SURVIVABLE NETWORK DESIGNS

The minimum-risk survivable network design presented in Chapter 3 is aimed at minimizing the total risk, or equivalently the expected damage value across network failure states. This design objective focuses only on the mean aspect of the risk, while ignoring other aspects related to the risk such as the variation in the damage and failure probabilities across the network failure states, and the amount of damage that could occur in the worst-case failure scenario.

This chapter presents alternative risk-based survivable network designs which take into account different aspects of risk in the design objectives. First, the min-max damage survivable network design is considered in Section 4.1. This design approach considers the minimization of the maximum damage that could occur in the network in the design objective. Section 4.2 presents the min-max risk survivable network design, which takes into consideration a minimization of the maximum risk that could occur in the network. Next, the minimum-root mean square (RMS) damage survivable network design is presented in Section 4.3. In contrast to the minimum-risk survivable network design which minimizes the expected damage value, the minimum-RMS damage design is aimed at minimizing the square root of the expected damage-squared value across all network failure states. The numerical results illustrating various risk-based survivable network designs are presented in Section 4.4. Lastly, Section 4.5 concludes the chapter.

The notation used in this chapter is summarized in Table 4.1.

Table 4.1 Notation used in Chapter 4

Given:

N	Set of nodes
L	Set of links or cables
R	Set of lightpaths
S	Set of network states
$p_{r,i}$	$p_{r,i} = 1$ if lightpath r uses link i in its working path, and = 0 otherwise
m_r	Data rate (bits/s) of lightpath r
w_i	Amount of working capacity on link i, calculated by $w_i = \sum_{r \in R} p_{r,i} m_r$
$state_{s,i}$	$state_{s,i} = 1$ if cable i is cut in network state s, and = 0 otherwise
$stateprob_s$	Probability of network state s
d_r	Damage caused by a failure of lightpath r
c_i	The unit cost of spare capacity on link i
budget	The budget
K	A large constant used for bounding

The following notation is used in the link protection case only:

Q_i	Set of eligible backup routes for link i
$\delta_{i,j}^q$	$\delta_{i,j}^q = 1$ if the q^{th} eligible backup route for link i in the set Q_i includes link j, and = 0 otherwise
$\zeta_{s,i}^q$	$\zeta_{s,i}^q = 1$ if the q^{th} backup route for link i in the set Q_i fails in network state s, and = 0 otherwise

The following notation is used in the path protection case only:

Q_r	Set of eligible backup routes for lightpath r
$\delta_{r,j}^{q}$	$\delta_{r,j}^{q}$ = 1 if the q^{th} eligible backup route for lightpath r in the set Q_r includes link j, and = 0 otherwise
$\zeta_{s,r}^{q}$	$\zeta_{s,r}^{q}$ = 1 if the q^{th} backup route for lightpath r in the set Q_r fails in network state s, and = 0 otherwise
$g_{s,r}$	$g_{s,r} > 0$ if a working path for lightpath r fails in network state s, and = 0 otherwise (i.e., $g_{s,r} = \sum_{i \in L} state_{s,i} p_{r,i}$)

Variables:

$damage_s$	Damage occurring in network state s
$maxdamage$	Maximum damage that could occur in the network in any network state
$risk_s$	Amount of risk in the network in network state s
$maxrisk$	Maximum amount of risk that could occur in the network from any network state
$totalrisk$	Total risk to the network
$y_{s,r}$	$y_{s,r} > 0$ if lightpath r fails in network state s, and = 0 otherwise
$z_{s,r}$	$z_{s,r}$ = 1 if lightpath r fails in network state s, and = 0 otherwise

The following notation is used in the link protection case only:

bp_i	bp_i = 1 if link i is protected, and = 0 otherwise
f_i^q	f_i^q = 1 if link i is protected and uses the q^{th} route in the backup route set Q_i for its backup path, and = 0 otherwise
$h_{s,i}$	$h_{s,i}$ = 1 if a backup path for link i is not available (either link i is not protected, or the backup path fails) in network state s, and = 0 otherwise
$e_{s,i}$	$e_{s,i}$ = 1 if link i fails (both working link fails and backup path is not available) in network state s, and = 0 otherwise

The following notation is used in the path protection case only:

bp_r	bp_r =1 if lightpath r is protected, and = 0 otherwise
f_r^q	f_r^q = 1 if lightpath r is protected and uses the q^{th} route in the backup route set Q_r for its backup path, and = 0 otherwise
$h_{s,r}$	$h_{s,r}$ = 1 if a backup path for lightpath r is not available (either lightpath r is not protected, or the backup path fails) in network state s, and = 0 otherwise

4.1 MIN-MAX DAMAGE SURVIVABLE NETWORK DESIGN

In the risk-based design approach of Chapter 3, the goal is to minimize the total network risk, or the expected damage value across all network states. However, by focusing only on the expected value, the amount of damage that could occur in the worst-case failure scenario might be too high and unacceptable to the network operators, or society. Therefore, in designing survivable networks an alternative approach is to minimize the maximum amount of damage that could occur in the network in addition to the expected damage. In this section, the min-max damage survivable network design is presented. The objective of this design is to minimize a multi-objective function: $k1 \times totalrisk + k2 \times maxdamage$, or a linear summation of the total network risk, denoted by *totalrisk*, and the maximum amount of damage that could occur in any network state, denoted by *maxdamage*, where $k1$ and $k2$ are design parameters. By varying the values of *k1* and *k2*, different survivable network designs are obtained. In the extreme cases, when $k1 = 0$, the design is aimed at minimizing the maximum damage only, whereas when $k2 = 0$, the minimum-risk survivable network design is obtained.

The link-path InP formulation for the min-max damage link protection design is presented in (4.1)–(4.12). The decision variables are the binary variables bp_i, which determines which links to be protected, where $bp_i = 1$ if link i is protected and $bp_i = 0$ otherwise, and the binary variables f_i^q which specifies the backup route for link i, where $f_i^q = 1$ if link i is protected and uses the q^{th} route in the backup route set Q_i for its backup path, and = 0 otherwise. The design objective in (4.1) is to minimize a linear summation of the total risk and the maximum damage that could occur in any network state. The constraint sets (4.2)–(4.12) are similar to the constraints (3.34)–(3.43) in the minimum-risk link protection design except for constraint set (4.8) which determines the maximum amount of damage that could occur in the network.

Constraint set (4.2) indicates that if link i is protected, there must exist one backup path, for which the route is selected from a set of eligible backup routes Q_i. Constraints (4.3)–(4.6) are the failure state relationships which determine whether or not lightpath r fails in network state s, taking into account the link protection being deployed in the network. More specifically, constraint set (4.3) determines whether or not the backup path for link i is available in network state s. The backup path for link i might not be available in network state s (i.e., $h_{s,i} = 1$) for two reasons: either the backup path exists but fails due to a cable cut in that network state (i.e., $\sum_{q \in Q_i} f_i^q \zeta_{s,i}^q = 1$), or link i is not protected (i.e., $bp_i = 0$, or $1\text{-}bp_i = 1$). Constraint set (4.4) indicates that link i fails in network state s (i.e., $e_{s,i} = 1$) if and only if both the working link fails (i.e., $state_{s,i} = 1$) and its backup path is not available (i.e., $h_{s,i} = 1$) in that network state. Constraint set (4.5) indicates that lightpath r fails in network state s ($y_{s,r} > 0$) if and only if at least one of the links that it traverses fails (i.e., $\sum_{i \in L} e_{s,i} p_{r,i} > 0$). Constraint set (4.6) relates variable $y_{s,r}$ to binary variable $z_{s,r}$. Constraint set (4.7) calculates the amount of damage for each network state as the

sum of damages for all failed lightpaths in that network state. Constraint set (4.8) determines an amount of maximum damage that could occur in the network. Constraint (4.9) calculates the total network risk as the sum of the product of the state damage and the state probability for all network states. Constraint (4.10) is the budget constraint which limits the total spare capacity investment, where c_j is the unit cost of spare capacity on link j, w_i is the amount of working capacity on link i, and parameter $\delta_{i,j}^{q}$ = 1 if the q^{th} eligible backup route for link i in the set Q_i includes link j, and = 0 otherwise. Lastly, constraint sets (4.11) and (4.12) express the binary nature of the design and failure variables.

Min-max damage link protection design problem (Link-path model)

Objective: $\min_{bp_i,\, f_i^q} k1 \times totalrisk + k2 \times maxdamage$ (4.1)

$$\sum_{q \in Q_i} f_i^q = bp_i, \quad \forall i \in L \tag{4.2}$$

$$h_{s,i} = \sum_{q \in Q_i} f_i^q \zeta_{s,i}^q + 1 - bp_i, \quad s \in S, i \in L \tag{4.3}$$

$$e_{s,i} = state_{s,i} h_{s,i}, \quad s \in S, i \in L \tag{4.4}$$

$$y_{s,r} = \sum_{i \in L} e_{s,i} p_{r,i}, \quad s \in S, r \in R \tag{4.5}$$

$$z_{s,r} K \geq y_{s,r}, \quad s \in S, r \in R \tag{4.6}$$

$$damage_s = \sum_{r \in R} z_{s,r} d_r, \quad \forall s \in S \tag{4.7}$$

$$maxdamage \geq damage_s, \quad \forall s \in S \tag{4.8}$$

$$totalrisk = \sum_{s \in S} stateprob_s damage_s \tag{4.9}$$

$$\sum_{i\in L}\sum_{q\in Q_i}\sum_{j\in L} c_j w_i f_i^q \delta_{i,j}^q \le budget \tag{4.10}$$

$$bp_i, f_i^q : binary, \quad \forall i \in L, \forall q \in Q_i \tag{4.11}$$

$$z_{s,r} : binary, \quad \forall s \in S, \forall r \in R \tag{4.12}$$

The link-path InP formulation for the min-max damage path protection design is presented in (4.13)–(4.23). The decision variables to be determined are binary variables bp_r, which determines a set of lightpaths to be protected, where $bp_r = 1$ if lightpath r is protected, and $bp_r = 0$ otherwise, and the binary variables f_r^q, which specifies the backup route for lightpath r, where $f_r^q = 1$ if lightpath r is protected and uses the q^{th} route in the backup route set Q_r for its backup path, and = 0 otherwise. The design objective in (4.13) is to minimize a linear summation of the total risk and the maximum damage that could occur in the network. The constraint sets (4.14)–(4.23) are similar to the constraints (3.45)–(3.53) in the minimum-risk path protection design except for constraint set (4.19) which determines the maximum amount of damage.

Constraint set (4.14) indicates that if lightpath r is protected, there must exist one backup path, whose route is selected from a set of eligible backup routes Q_r. Constraints (4.15)–(4.18) are the failure state relationships which determine whether or not lightpath r will fail in network state s, taking into account the path protection being deployed in the network. More specifically, constraint set (4.15) determines whether or not the backup path for lightpath r is available in network state s. The backup path for lightpath r might not be available in network state s (i.e., $h_{s,r} = 1$) for two reasons: either the backup path exists but fails due to a cable cut in that network state (i.e., $\sum_{q\in Q_r} f_r^q \zeta_{s,r}^q = 1$), or lightpath r is not protected (i.e., $bp_r = 0$, or $1\text{-}bp_r = 1$). Constraint set (4.16) indicates that lightpath r fails in network state s (i.e., $y_{s,r} > 0$) if and only if both its

working path fails (i.e., $g_{s,r} > 0$) and its backup path is not available in that network state (i.e., $h_{s,r} = 1$). Constraint set (4.17) relates variable $y_{s,r}$ to binary variable $z_{s,r}$. Constraints (4.18)–(4.20) are for the calculation of the total risk and the maximum damage as in the link protection case. Constraint (4.21) is the budget constraint. Lastly, constraint sets (4.22) and (4.23) express the binary nature of the design and failure variables.

Min-max damage path protection design problem (Link-path model)

$$\text{Objective: } \min_{bp_r,\, f_r^q} \mathrm{k1} \times totalrisk + \mathrm{k2} \times maxdamage \tag{4.13}$$

$$\sum_{q \in Q_r} f_r^q = bp_r, \quad \forall r \in R \tag{4.14}$$

$$h_{s,r} = \sum_{q \in Q_r} f_r^q \zeta_{s,r}^q + 1 - bp_r, \quad s \in S, r \in R \tag{4.15}$$

$$y_{s,r} = g_{s,r} h_{s,r}, \quad s \in S, r \in R \tag{4.16}$$

$$z_{s,r} \mathrm{K} \geq y_{s,r}, \quad s \in S, r \in R \tag{4.17}$$

$$damage_s = \sum_{r \in R} z_{s,r} d_r, \quad \forall s \in S \tag{4.18}$$

$$maxdamage \geq damage_s, \quad \forall s \in S \tag{4.19}$$

$$totalrisk = \sum_{s \in S} stateprob_s damage_s \tag{4.20}$$

$$\sum_{r \in R} \sum_{q \in Q_r} \sum_{j \in L} c_j m_r f_r^q \delta_{r,j}^q \leq budget \tag{4.21}$$

$$bp_r,\ f_r^q : binary, \quad \forall r \in R, \forall q \in Q_r \tag{4.22}$$

$$z_{s,r} : binary, \quad \forall s \in S, \forall r \in R \tag{4.23}$$

4.2 MIN-MAX RISK SURVIVABLE NETWORK DESIGN

The min-max damage survivable network design presented in Section 4.1 considers the maximum amount of damage that could occur in the network, while ignoring the occurrence probability of that failure. Therefore, the network might be designed to protect against failure scenarios that have a high damage level, but are unlikely to occur (e.g., multiple-link failures). In this section, the min-max risk survivable network design is presented. This design approach takes into account the maximum risk that could occur in any network state, where the risk associated with each network state is defined as the product of the amount of damage in that network state and the state probability. The design objective is to minimize a multi-objective function: $k1 \times totalrisk + k2 \times maxrisk$, which is a linear summation of the total risk, and the maximum risk that could occur in any network state, denoted by *maxrisk*, where $k1$ and $k2$ are design parameters. By varying the values of $k1$ and $k2$, different survivable network designs can be obtained. In the extreme cases, when $k1 = 0$, the design is aimed at minimizing the maximum risk only, whereas when $k2 = 0$, the design is aimed at minimizing the total risk.

The link-path InP formulation for the min-max risk link protection design is presented in (4.24)–(4.36). Two sets of decision variables are the binary variables bp_i, which determines which links to be protected, where $bp_i = 1$ if link i is protected and $bp_i = 0$ otherwise, and the binary variable f_i^q which specifies the backup route for link i, where $f_i^q = 1$ if link i is protected and uses the q^{th} route in the backup route set Q_i for its backup path, and = 0 otherwise. The design objective in (4.24) is to minimize a linear summation of the total risk and the maximum risk that could occur in any network state. The constraint sets (4.25)–(4.36) are similar to the

constraints (3.34)–(3.43) in the minimum-risk link protection design except for constraint sets (4.31)–(4.32) which calculate the maximum risk that could occur in any network state.

Constraint set (4.25) indicates that if link i is protected, there must exist one backup path, for which the route is selected from a set of eligible backup routes Q_i. Constraints (4.26)–(4.29) are the failure state relationships which determine whether or not lightpath r fails in network state s, taking into account the link protection being deployed in the network. More specifically, constraint set (4.26) determines whether or not the backup path for link i is available in network state s. The backup path for link i might not be available in network state s (i.e., $h_{s,i} = 1$) for two reasons: either the backup path exists but fails due to a cable cut in that network state (i.e., $\sum_{q \in Q_i} f_i^q \zeta_{s,i}^q = 1$), or link i is not protected (i.e., $bp_i = 0$, or $1\text{-}bp_i = 1$). Constraint set (4.27) indicates that link i fails in network state s (i.e., $e_{s,i} = 1$) if and only if both the working link fails (i.e., $state_{s,i} = 1$) and its backup path is not available (i.e., $h_{s,i} = 1$) in that network state. Constraint set (4.28) indicates that lightpath r fails in network state s ($y_{s,r} > 0$) if and only if at least one of the links that it traverses fails (i.e., $\sum_{i \in L} e_{s,i} p_{r,i} > 0$). Constraint set (4.29) relates variable $y_{s,r}$ to binary variable $z_{s,r}$. Constraint set (4.30) calculates the damage for each network state as the sum of the damage from all failed lighpaths in that network state. Constraint set (4.31) calculates the risk for each network state as the product of the damage and the probability of that network state. Constraint set (4.32) determines the maximum amount of risk that could occur in the network from any network state. Constraint (4.33) calculates the total network risk as the sum of the risk from all network states. Constraint (4.34) is the budget constraint which limits the total spare capacity investment, where c_j is the unit cost of spare capacity on link j, w_i is the amount of working capacity on link i, and parameter $\delta_{i,j}^q = 1$ if the q^{th} eligible backup route for link i in the

set Q_i includes link j, and = 0 otherwise. Lastly, constraint sets (4.35) and (4.36) express the binary nature of the design and failure variables.

Min-max risk link protection design problem (Link-path model)

Objective: $\min_{bp_i,\, f_i^q} k1 \times totalrisk + k2 \times maxrisk$ (4.24)

$$\sum_{q \in Q_i} f_i^q = bp_i, \quad \forall i \in L \tag{4.25}$$

$$h_{s,i} = \sum_{q \in Q_i} f_i^q \zeta_{s,i}^q + 1 - bp_i, \quad s \in S, i \in L \tag{4.26}$$

$$e_{s,i} = state_{s,i} h_{s,i}, \quad s \in S, i \in L \tag{4.27}$$

$$y_{s,r} = \sum_{i \in L} e_{s,i} p_{r,i}, \quad s \in S, r \in R \tag{4.28}$$

$$z_{s,r} \mathrm{K} \geq y_{s,r}, \quad s \in S, r \in R \tag{4.29}$$

$$damage_s = \sum_{r \in R} z_{s,r} d_r, \quad \forall s \in S \tag{4.30}$$

$$risk_s = damage_s stateprob_s, \quad \forall s \in S \tag{4.31}$$

$$maxrisk \geq risk_s, \quad \forall s \in S \tag{4.32}$$

$$totalrisk = \sum_{s \in S} risk_s \tag{4.33}$$

$$\sum_{i \in L} \sum_{q \in Q_i} \sum_{j \in L} c_j w_i f_i^q \delta_{i,j}^q \leq budget \tag{4.34}$$

$$bp_i, f_i^q : binary, \quad \forall i \in L, \forall q \in Q_i \tag{4.35}$$

$$z_{s,r} : binary, \quad \forall s \in S, \forall r \in R \tag{4.36}$$

The link-path InP formulation for the min-max risk path protection design is presented in (4.37)–(4.48). The decision variables to be determined are binary variables bp_r, which determines a set of lightpaths to be protected, where $bp_r = 1$ if lightpath r is protected, and $bp_r = 0$ otherwise, and the binary variables f_r^q, which specifies the backup route for lightpath r, where $f_r^q = 1$ if lightpath r is protected and uses the q^{th} route in the backup route set Q_r for its backup path, and = 0 otherwise. The design objective in (4.37) is to minimize a linear summation of the total risk and the maximum risk that could occur in any network state. The constraint sets (4.38)–(4.48) are similar to the constraints (3.45)–(3.53) in the minimum-risk path protection design except for constraint sets (4.43)–(4.44) which calculate the maximum risk.

Constraint set (4.38) indicates that if lightpath r is protected, there must exist one backup path, whose route is selected from a set of eligible backup routes Q_r. Constraints (4.39)–(4.41) are the failure state relationships which determine whether or not lightpath r will fail in network state s, taking into account the path protection mechanism being deployed in the network. More specifically, Constraint set (4.39) determines whether or not the backup path for lightpath r is available in network state s. The backup path for lightpath r might not be available in network state s (i.e., $h_{s,r} = 1$) for two reasons: either the backup path exists but fails due to a cable cut in that network state (i.e., $\sum_{q \in Q_r} f_r^q \zeta_{s,r}^q = 1$), or lightpath r is not protected (i.e., $bp_r = 0$, or $1\text{-}bp_r = 1$). Constraint set (4.40) indicates that lightpath r fails in network state s (i.e., $y_{s,r} > 0$) if and only if both its working path fails (i.e., $g_{s,r} > 0$) and its backup path is not available in that network state (i.e., $h_{s,r} = 1$). Constraint set (4.41) relates variable $y_{s,r}$ to binary variable $z_{s,r}$. Constraints (4.42)–(4.45) are for the calculation of the total risk and the maximum risk as in the link protection case. Constraint (4.46) is the budget constraint. Lastly, constraint sets (4.47) and (4.48) express the binary nature of the design and failure variables.

Min-max risk path protection design problem (Link-path model)

$$\text{Objective: } \min_{bp_r,\, f_r^q} k1 \times totalrisk + k2 \times maxrisk \tag{4.37}$$

$$\sum_{q \in Q_r} f_r^q = bp_r, \quad \forall r \in R \tag{4.38}$$

$$h_{s,r} = \sum_{q \in Q_r} f_r^q \zeta_{s,r}^q + 1 - bp_r, \quad s \in S, r \in R \tag{4.39}$$

$$y_{s,r} = g_{s,r} h_{s,r}, \quad s \in S, r \in R \tag{4.40}$$

$$z_{s,r} \mathrm{K} \geq y_{s,r}, \quad s \in S, r \in R \tag{4.41}$$

$$damage_s = \sum_{r \in R} z_{s,r} d_r, \quad \forall s \in S \tag{4.42}$$

$$risk_s = damage_s stateprob_s, \quad \forall s \in S \tag{4.43}$$

$$maxrisk \geq risk_s, \quad \forall s \in S \tag{4.44}$$

$$totalrisk = \sum_{s \in S} risk_s \tag{4.45}$$

$$\sum_{r \in R} \sum_{q \in Q_r} \sum_{j \in L} c_j m_r f_r^q \delta_{r,j}^q \leq budget \tag{4.46}$$

$$bp_r, f_r^q : binary, \quad \forall r \in R, \forall q \in Q_r \tag{4.47}$$

$$z_{s,r} : binary, \quad \forall s \in S, \forall r \in R \tag{4.48}$$

4.3 MINIMUM-RMS DAMAGE SURVIVABLE NETWORK DESIGN

In this section, the minimum Root-Mean-Squared (RMS) damage survivable network design is presented. This design approach can avoid some drawbacks of other design approaches. In the minimum-risk design approach, the design only focuses on the minimization of the expected

damage value, while ignoring how low or high the damage from each failure scenario could be or the variability of damage across the failure scenarios, as long as the expected value is minimized. In addition, the min-max damage design and the min-max risk design are only concerned about the expected damage value and the worst-case values (i.e., the maximum damage, and the maximum risk), while not directly considering the variability of damage or the probability distribution of damage that could occur in the network.

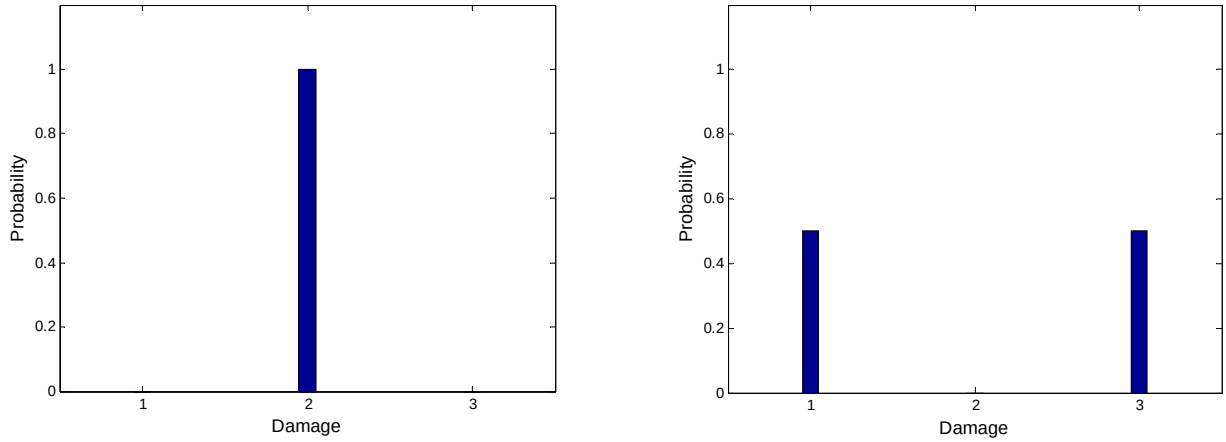
In contrast, the minimum-RMS damage design takes into account how small or large the damage from each network state could be by minimizing the variability of damage that could occur in the network. The objective of this design is to minimize the square root of the expected damage-squared value across all network states, or the RMS of damage, as calculated in (4.49).

$$RMS \text{ of } damage = \sqrt{\sum_{s \in S} stateprob_s damage_s^{\,2}} \tag{4.49}$$

By squaring the damage level of each network failure state, the damage in the network states with higher damage levels is increased to a greater extent than the damage in the network states with lower damage levels, thus encouraging the design to protect against failures with higher damage levels.

Figure 4.1 illustrates a difference between the minimum-RMS damage survivable network design and the minimum-risk survivable network design. In the figure, two probability distributions of damage are shown. The damage distribution in Figure 4.1 (b) has both low and high damage levels, but the same expected damage value as the one in Figure 4.1 (a) (i.e., 2). However the damage distribution in (b) has a higher RMS value of damage (i.e., $\sqrt{5}$) than the one in (a) (i.e., 2), and therefore the minimum-RMS damage design prefers the damage

distribution in Figure 4.1(a) to the distribution in Figure 4.1(b). This example shows that the minimum-RMS damage design tends to protect the network from high damage values.



(a) (b)

Figure 4.1 Two probability distributions of damage illustrating a difference between the minimum-RMS damage design and the minimum-risk design

Since the objective function of the minimum-RMS damage design is non-linear, the design problem cannot be solved using an InP approach. Here, a greedy heuristic algorithm similar to Heuristic 3 in Section 3.4.2 is proposed for solving the minimum-RMS damage design. The flow chart of this iterative greedy heuristic algorithm is presented in Figure 4.2.

This heuristic algorithm consists of two steps. In the first step, the algorithm chooses to protect a link (in the link protection case) or a lightpath (in the path protection case) one at a time using one of the backup routes in the pre-computed route set, where the protection produces the greatest ratio of the reduction in RMS of damage to the backup path cost, and does not violate the budget limit. The process repeats until no more links or lightpaths can be selected due to the budget constraint, or all the links or lightpaths have been protected. Since the first step might not yield an optimal solution, an iterative process in the second step is deployed to improve the

solution. The second step is based on an idea that it is possible to improve the current solution by iteratively removing the protection from a protected link or lightpath in the current solution, followed by updating the budget, and then choosing to protect other unprotected links or lightpaths using one of the pre-computed backup routes that could produce a greater reduction in RMS of damage. The iterative process keeps reducing the amount of RMS of damage, and terminates when the current solution cannot be improved further, or a predefined number of iterations is reached.

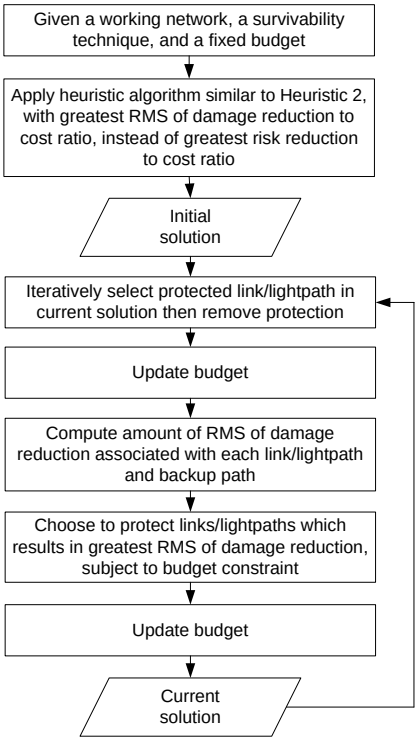


Figure 4.2 Flow chart of the iterative greedy heuristic algorithm for solving the minimum-RMS damage design problem

4.4 NUMERICAL RESULTS

The numerical results from the min-max damage survivable network design, and the min-max risk survivable network design with different values of design parameters $k1$ and $k2$, are presented in Section 4.4.1, and 4.4.2, respectively. Then, a numerical comparison of different risk-based survivable network designs for networks with single class of traffic is presented in Section 4.4.3; and a comparison for networks supporting multiple classes of traffic is presented in Section 4.4.4.

In the experiments, the minimum-risk design problems, the min-max damage design problems, and the min-max risk design problems as formulated in the InP models of Sections 3.4.1, 4.1, and 4.2 were solved using the commercial CPLEX/AMPL solver with all possible routes within two hops from the shortest backup route used as a set of pre-computed backup routes. Whereas the minimum-RMS damage design problems were solved using the heuristic algorithm explained in Section 4.3 with the same set of pre-computed backup routes. Also, the damage is measured as the traffic loss rate caused by lightpath failures; and only network states with at most two simultaneous link failures are considered in the risk calculation.

Network 2 shown in Figure 3.8, with cable lengths and Cable Cut (CC) metrics indicated in the figure, is used as a network example. All the cables have the same Mean Time To Repair (MTTR) of 24 hours. For each network, a full mesh of lightpath demands between all node pairs are assumed, each of which carries the same data rate of 10 Gbps. The working path of each lightpath is routed along the shortest path based on the hop count, and given to the design problem. Also, the spare capacity cost is defined as 1 budget unit per 10 Gbps per 1000 km.

The numerical results are only presented for some particular budget values. For link protection on Network 2, budget values of 15, 30, and 45 units are considered, which represents

approximately about 25%, 50%, and 75% of the minimum cost required for protecting all the network links, respectively. Whereas for path protection on Network 2, budget values of 10, 20, and 30 units are considered, which represents approximately about 25%, 50%, and 75% of the minimum cost required for protecting all the lightpaths in the network, respectively.

4.4.1 Min-max damage survivable network design

Table 4.2 shows a list of all network states in Network 2 which have the highest damage level (i.e., 100 Gbps) and the second highest damage level (i.e., 90 Gbps), when the network is not protected. Each network state is represented as the failed links in that network state and the corresponding damage level. As shown in Table 4.2, the network states which have the highest damage levels are those among the dual-link failure states.

Table 4.2 A list of all network states in Network 2 which have the two highest damage levels

Network state (shown as failed links)	Damage level (Gbps)	Network state (shown as failed links)	Damage level (Gbps)
3-4, 5-9	100	2-10, 8-9	90
3-4, 8-9	100	3-4, 6-7	90
1-7, 3-4	90	3-10, 5-9	90
1-7, 5-9	90	3-10, 8-9	90
1-7, 8-9	90	4-7, 5-9	90
1-8, 3-4	90	4-7, 8-9	90
2-10, 3-4	90	5-9, 6-7	90
2-10, 5-9	90	6-7, 8-9	90

Table 4.3 presents the results from the min-max damage link protection designs on Network 2 with a budget of 30 units (about 50% of the minimum cost for protecting all network links); whereas Table 4.4 presents the results for the path protection case with a budget of 20

units (about 50% of the minimum cost for protecting all lightpaths). The results are presented in terms of the set of protected links or lightpaths, the total risk or the expected damage, and the maximum damage for different values of design parameters $k1$, and $k2$.

In the link protection case, the results in Table 4.3 show that the min-max damage design with $k1=0$ and $k2=1$, which minimizes the maximum damage only, provides the lowest maximum damage level, i.e., 80 Gbps. This design could avoid the high damage levels (i.e., 100 Gbps and 90 Gbps) from occurring in the network by choosing to protect at least one of the two failed links in each of the network states listed in Table 4.2, and deploying the backup route for each protected link that does not traverse the other failed link in that network state. Note that the design with $k1=0$ and $k2=1$ is only considered as to provide the lowest value of maximum damage. However, this design could result in a very high risk level, because a minimization of total risk is not a part of the design objective. Thus the design might not spend any money for protecting the network to reduce the total risk level, or might choose backup routes that do not result in the minimum risk level.

For the min-max damage design with $k1=1$ and $k2=1$, since the maximum damage value is typically much larger than the total risk value (i.e., the expected damage value), therefore this design puts a higher priority on minimizing the maximum damage level than minimizing the total risk level. The results in Table 4.3 show that the design with $k1=1$ and $k2=1$ chooses to protect at least one of the two failed links in each network state listed in Table 4.2 (i.e., links 1-7, 2-10, 3-4, 5-9, and 8-9) in order to minimize the maximum damage, which results in the lowest maximum damage level (i.e., 80 Gbps), and protect some additional links (i.e., links 2-3, 5-6, 5-10, 6-7, 7-8, and 9-10) in order to reduce the total risk level as much as possible, which results in a total risk that is 28.56% higher than the lowest total risk level. In contrast, the design with $k1=1$

and $k2$=0, or the minimum-risk design, yields the lowest total risk level, but results in a maximum damage level that is 12.5% higher than the lowest possible value. For this network example the experiments reveal that there is no other values of design parameters $k1$ and $k2$ that could provide other results than those shown in Table 4.3.

In the path protection case, the results in Table 4.4 show that the min-max damage design with $k1$=1 and $k2$=1, which put a higher priority on minimizing the maximum damage than minimizing the total risk, can achieve the lowest maximum damage level (i.e., 50 Gbps), but results in the total risk that is 81.38% larger than the smallest total risk level. On the other hand, the design with $k1$=1 and $k2$=0, or the minimum-risk path protection design, could provide the smallest total risk level, but a maximum damage that is 60% higher than the lowest possible value. Whereas, the design with $k1$=20 and $k2$=1 provides a compromise between the minimum-risk design ($k1$=1 and $k2$=0) and the min-max damage design with $k1$=1 and $k2$=1. Even though this design cannot achieve the smallest total risk level or the smallest maximum damage level, it yields the total risk that is only 17.45% larger than the smallest total risk level, and the maximum damage that is only 20% larger than the minimum possible value.

Table 4.3 Results from min-max damage link protection design on Network 2 for a given budget of 30 units

Metric	$k1$=1, $k2$=0	$k1$=1, $k2$=1	$k1$=0, $k2$=1
Protected links	1-2, 1-7, 2-3, 2-10, 3-4, 4-8, 5-6, 5-10, 6-7, 7-8, 8-9, 9-10	1-7, 2-3, 2-10, 3-4, 5-6, 5-9, 5-10, 6-7, 7-8, 8-9, 9-10	1-7, 2-10, 3-4, 3-10, 5-9, 8-9
Total Risk (Mbps)	549.53 (0%)	706.63 (+28.56%)	1852.90 (+237.18%)
Maximum Damage (Gbps)	90 (+12.5%)	80 (0%)	80 (0%)

Table 4.4 Results from min-max damage path protection design on Network 2 for a given budget of 20 units

Metric	$k1$=1, $k2$=0	$k1$=20, $k2$=1	$k1$=1, $k2$=1	$k1$=0, $k2$=1
Protected lightpaths	1-4, 1-6, 1-7, 1-10, 2-5, 2-6, 2-7, 2-9, 2-10, 3-4, 3-6, 3-7, 4-10, 5-6, 5-7, 6-10, 7-8, 7-9, 7-10, 8-9, 9-10	1-4, 1-5, 1-6, 1-7, 2-5, 2-6, 2-7, 2-9, 2-10, 3-4, 3-6, 3-7, 4-5, 4-10, 5-6, 5-7, 6-10, 7-9, 8-9, 9-10	1-3, 1-4, 1-5, 1-6, 1-7, 2-5, 2-6, 2-7, 2-9, 3-5, 3-7, 4-10, 5-8, 5-9, 7-9, 7-10, 9-10	1-2, 1-3, 1-5, 1-6, 2-5, 2-6, 2-7, 2-9, 3-5, 3-7, 4-10, 5-8, 5-9, 7-9, 7-10
Total Risk (Mbps)	1,013.69 (0%)	1,190.54 (+17.45%)	1,838.67 (+81.38%)	2,448.11 (+141.51%)
Maximum Damage (Gbps)	80 (+60%)	60 (+20%)	50 (0%)	50 (0%)

4.4.2 Min-max risk survivable network design

Table 4.5 lists the ten network states in Network 2 that have the highest risk levels in decreasing order, when the network is not protected. Each of the network states is represented by the failed links in that network state. We observe that the network states that have the highest risk levels are those among the single-link failure states. This is because the single-link failure states have a much higher state probability than the dual-link failure states, despite their lower damage level.

Table 4.5 A list of ten network states in Network 2 with the highest risk levels in decreasing order

Network state (shown as failed links)	Risk level (Mbps)	Network state (shown as failed links)	Risk level (Mbps)
1-7	1,771.64	9-10	519.58
3-4	1,298.95	6-7	386.10
8-9	848.11	5-10	354.36
5-6	631.48	1-8	192.52
2-10	580.76	4-8	162.50

Table 4.6 presents the results from the min-max risk link protection designs on Network 2 with a budget of 30 units; whereas Table 4.7 presents the results for the path protection case with a budget of 20 units. The results are presented in terms of the set of protected links/lightpaths, the total risk, and the maximum risk for different values of design parameters $k1$, and $k2$. The results from the design with $k1=1$ and $k2=0$ which yields the minimum total risk level, and the design with $k1=0$ and $k2=1$ which gives the minimum maximum risk level are also provided as references.

The results for the min-max risk link protection case in Table 4.6 show that for the given budget the min-max risk design tends to protect those high-risk links listed in Table 4.5, especially when $k2$ is large relative to $k1$ (i.e., when the design puts a higher priority on minimizing the maximum risk). The results show that the design with $k1=1$, $k2=100$ achieves the smallest value for the maximum risk, and results in the total risk that is 18.21% higher than the minimum value. In contrast, the design with $k1=1$ and $k2=0$, or the minimum-risk design, yields the lowest total risk level, but results a maximum risk level that is 19.97% higher than the lowest value. Whereas, the design with $k1=1$ and $k2=5$ provides a compromise between the minimum-risk design and the min-max risk design with $k=1$ and $k2=100$. Even though this design does not achieve the lowest possible values for the total risk and the maximum risk, it yields the total risk that is only 4.55% higher than the minimum total risk level, and the maximum risk that is only 1.26% higher than the lowest value.

Similarly, the results for the path protection case in Table 4.7 show that the min-max risk design with $k1=1$ and $k2=100$, which puts a higher priority on minimizing the maximum risk rather than the total risk, can achieve the lowest possible value for the maximum risk, but results in a high total risk that is 14.83% larger than the minimum total risk level. In contrast, the design

with $k1$=1 and $k2$=0 or the minimum-risk design yields the lowest total risk level, but results in a maximum risk that is 141.75% larger than the minimum maximum risk level. Whereas the design with $k1$=1 and $k2$=1 provides a compromise between the minimum-risk design and the min-max risk design with $k1$=1 and $k2$=100.

Note that the design with $k1$=0 yields a higher total risk level than other design alternatives. This is understandable because when $k1$=0 the minimization of the total risk is not a part of the design objective, therefore the design might not choose the backup routes that result in the lowest total risk level, or not spend any budget for protecting the network to reduce the total risk level, as long as it could achieve the smallest maximum risk level.

Table 4.6 Results from the min-max risk link protection design on Network 2 for a given budget of 30 units

Metric	$k1$=1, $k2$=0	$k1$=1, $k2$=5	$k1$=1, $k2$=100	$k1$=0, $k2$=1
Protected links	1-2, 1-7, 2-3, 2-10, 3-4, 4-8, 5-6, 5-10, 6-7, 7-8, 8-9, 9-10	1-7, 1-8, 2-3, 2-10, 3-4, 4-9, 5-6, 5-10, 6-7, 7-8, 8-9, 9-10	1-7, 1-8, 2-10, 3-4, 5-6, 5-10, 6-7, 8-9, 9-10	1-7, 1-8, 2-10, 3-4, 5-6, 5-10, 6-7, 8-9, 9-10
Total Risk (Mbps)	549.53 (0%)	574.53 (+4.55%)	649.58 (+18.21%)	651.62 (+18.58%)
Maximum Risk (Mbps)	96.26 (+19.97%)	81.25 (+1.26%)	80.24 (0%)	80.24 (0%)

Table 4.7 Results from the min-max risk path protection design on Network 2 for a given budget of 20 units

Metric	$k1$=1, $k2$=0	$k1$=1, $k2$=1	$k1$=1, $k2$=100	$k1$=0, $k2$=1
Protected lightpaths	1-4, 1-6, 1-7, 1-10, 2-5, 2-6, 2-7, 2-9, 2-10, 3-4, 3-6, 3-7, 4-10, 5-6, 5-7, 6-10, 7-8, 7-9, 7-10, 8-9, 9-10	1-4, 1-6, 1-7, 1-9, 1-10, 2-5, 2-6, 2-7, 2-9, 2-10, 3-4, 3-6, 3-7, 4-10, 5-6, 5-7, 6-10, 7-10, 8-9, 9-10	1-4, 1-6, 1-7, 1-9, 2-5, 2-6, 2-7, 2-9, 2-10, 3-4, 3-6, 3-7, 4-10, 5-7, 5-8, 6-10, 7-10, 8-9, 9-10	1-4, 1-6, 1-7, 1-9, 2-5, 2-6, 2-7, 2-9, 2-10, 3-4, 3-6, 3-7, 4-10, 5-7, 5-8, 6-10, 7-10, 8-9, 9-10
Total Risk (Mbps)	1,013.69 (0%)	1,033.85 (1.99%)	1,164.04 (14.83%)	1,164.63 (14.89%)
Maximum Risk (Mbps)	254.43 (141.75%)	169.62 (61.17%)	105.25 (0%)	105.25 (0%)

4.4.3 Comparisons of different risk-based survivable network designs

This section compares and analyzes the results from the different proposed risk-based survivable network design alternatives: the minimum-risk design, the min-max damage design, the min-max risk design, and the minimum-RMS damage design. For the min-max damage design, the design parameters: $k1$=1 and $k2$=1, are used; whereas for the min-max risk design, the parameters: $k1$=1 and $k2$=100, are used. These parameter values are chosen such that the min-max damage design puts a higher priority on minimizing the maximum damage than minimizing the total risk; and the min-max risk design puts a higher priority on minimizing the maximum risk than minimizing the total risk.

The comparisons are made based on the following measures: the probability of no damage which is the probability that the network is in the states that have a zero-damage level taking into account the protection deployed in the network, the total risk (i.e., the expected damage value), the maximum damage, the maximum risk, the RMS of damage, the standard deviation of damage, the sum of the expected damage value and the standard deviation of damage, and lastly the probability distribution of damage.

Tables 4.8–4.10 presents the results from different risk-based link protection designs on Network 2 for a budget of 15, 30, and 45 units, which are approximately about 25%, 50%, and 75% of the minimum cost for protecting all the network links, respectively. Whereas, Table 4.11–4.13 presents the results from different risk-based designs using path protection on Network 2 for a budget of 10, 20, and 30 units, which are approximately about 25%, 50%, and 75% of the minimum cost for protecting all the lightpaths in the network, respectively. In these tables, each number in the parenthesis represents the percentage difference of the metric of interest from the smallest value that can be achieved from any design being considered.

Table 4.8 Comparison of different risk-based link protection designs on Network 2 for a budget of 15 units

Metric	Design's objective function			
	Total Risk	Total Risk + MaxDamage	Total Risk + 100×MaxRisk	RMS Damage
Probability of no Damage	0.9499	0.9088	0.9373	0.9372
Total Risk (Mbps)	1,675.09 (0%)	2,826.26 (+68.72%)	1,814.05 (+8.30%)	1,817.03 (+8.47%)
Maximum Damage (Gbps)	90 (+12.5%)	80 (0%)	90 (+12.5%)	90 (+12.5%)
Maximum Risk (Mbps)	424.06 (+46.04%)	885.82 (+205.06%)	290.38 (0%)	290.38 (0%)
RMS Damage (Mbps)	8,054.61 (+3.80%)	10,074.28 (+29.82%)	7,767.15 (+0.09%)	7,759.97 (0%)
Std. of Damage (Mbps)	7,707.46 (+5.06%)	9,286.65 (+26.59%)	7,345.24 (+0.12%)	7,336.25 (0%)
Expected Damage + Std. of Damage (Mbps)	9,382.54 (+2.50%)	12,112.91 (+32.33%)	9,159.29 (+0.07%)	9,153.27 (0%)

Table 4.9 Comparison of different risk-based link protection designs on Network 2 for a budget of 30 units

Metric	Design's objective function			
	Total Risk	Total Risk + MaxDamage	Total Risk + 100×MaxRisk	RMS Damage
Probability of no Damage	0.9819	0.9765	0.9701	0.9762
Total Risk (Mbps)	549.53 (0%)	706.63 (+28.59%)	649.58 (+18.21%)	589.58 (+7.29%)
Maximum Damage (Gbps)	90 (+12.5%)	80 (0%)	90 (+12.5%)	90 (+12.5%)
Maximum Risk (Mbps)	96.26 (+19.96%)	96.26 (+19.96%)	80.24 (0%)	81.25 (+1.25%)
RMS Damage (Mbps)	4,312.29 (+2.85%)	4,814.95 (+14.84%)	4,264.56 (+1.71%)	4,192.67 (0%)
Std. of Damage (Mbps)	4,242.32 (+3.22%)	4,711.34 (+14.63%)	4,165.94 (+1.36%)	4,109.92 (0%)
Expected Damage + Std. of Damage (Mbps)	4,791.84 (+1.96%)	5,417.97 (+15.29%)	4,815.53 (+2.47%)	4,699.50 (0%)

Table 4.10 Comparison of different risk-based link protection designs on Network 2 for a budget of 45 units

Metric	Design's objective function			
	Total Risk	Total Risk + MaxDamage	Total Risk + 100×MaxRisk	RMS Damage
Probability of no Damage	0.9961	0.9507	0.9961	0.9947
Total Risk (Mbps)	140.22 (0%)	1,101.73 (+685.73%)	140.22 (0%)	154.94 (+10.50%)
Maximum Damage (Gbps)	90 (+28.57%)	70 (0%)	90 (+28.57)	90 (+28.57)
Maximum Risk (Mbps)	36.05 (0%)	259.79 (+620.67%)	36.05 (0%)	48.13 (+33.52%)
RMS Damage (Mbps)	2,390.79 (+1.43%)	5,417.21 (+129.82%)	2,390.79 (+1.43%)	2,357.16 (0%)
Std. of Damage (Mbps)	2,382.57 (+1.52%)	5,194.04 (+121.31%)	2,382.57 (+1.52%)	2,346.98 (0%)
Expected Damage + Std. of Damage (Mbps)	2,522.79 (+0.83%)	6,295.77 (+151.64%)	2,522.79 (+0.83%)	2,501.93 (0%)

Table 4.11 Comparison of different risk-based path protection designs on Network 2 for a budget of 10 units

Metric	Design's objective function			
	Total Risk	Total Risk + MaxDamage	Total Risk + 100×MaxRisk	RMS Damage
Probability of no Damage	0.9089	0.8981	0.8865	0.8760
Total Risk (Mbps)	2,210.96 (0%)	2,550.38 (+15.35%)	2,355.91 (+6.56%)	2,462.35 (+11.37%)
Maximum Damage (Gbps)	90 (+28.57%)	70 (0%)	90 (+28.57%)	90 (+28.57%)
Maximum Risk (Mbps)	424.06 (+63.23%)	389.68 (+50%)	259.79 (0%)	259.79 (0%)
RMS Damage (Mbps)	8,408.52 (+8.90%)	8,609.02 (+11.50%)	7,721.01 (0%)	7,752.86 (+0.41%)
Std. of Damage (Mbps)	7,833.94 (+12.22%)	7,859.21 (+12.58%)	7,010.13 (0.42%)	6,980.76 (0%)
Expected Damage + Std. of Damage (Mbps)	10,044.89 (+7.25%)	10,409.59 (+11.14%)	9,366.04 (0%)	9,443.10 (+0.82%)

Table 4.12 Comparison of different risk-based path protection designs on Network 2 for a budget of 20 units

Metric	Design's objective function			
	Total Risk	Total Risk + MaxDamage	Total Risk + 100×MaxRisk	RMS Damage
Probability of no Damage	0.9496	0.8981	0.9248	0.9164
Total Risk (Mbps)	1,013.69 (0%)	1,838.67 (+81.38%)	1,164.04 (+14.83%)	1,180.75 (+16.48%)
Maximum Damage (Gbps)	80 (+60%)	50 (0%)	80 (+60%)	80 (+60%)
Maximum Risk (Mbps)	254.43 (+141.75%)	259.79 (+146.78%)	105.25 (0%)	169.62 (+61.17%)
RMS Damage (Mbps)	5,164.57 (13.76%)	6,216.14 (36.92%)	4,806.33 (5.86%)	4,540.08 (0%)
Std. of Damage (Mbps)	4,966.81 (+17.26%)	5,676.48 (+34.02%)	4,526.86 (+6.88%)	4,235.57 (0%)
Expected Damage + Std. of Damage (Mbps)	5,980.49 (+10.42%)	7,515.15 (+38.75%)	5,690.90 (+5.07%)	5,416.32 (0%)

Table 4.13 Comparison of different risk-based path protection designs on Network 2 for a budget of 30 units

Metric	Design's objective function			
	Total Risk	Total Risk + MaxDamage	Total Risk + 100×MaxRisk	RMS Damage
Probability of no Damage	0.9782	0.8986	0.9781	0.9633
Total Risk (Mbps)	367.36 (0%)	1,163.61 (+216.75%)	378.18 (+2.95%)	447.85 (+21.91%)
Maximum Damage (Gbps)	70 (+75%)	40 (0%)	70 (+75%)	60 (+50%)
Maximum Risk (Mbps)	54.17 (+12.54%)	129.89 (+169.88%)	48.13 (0%)	59.06 (+22.71%)
RMS Damage (Mbps)	2,712.28 (+5.68%)	3,927.99 (+53.04%)	2,819.78 (+9.86%)	2,566.61 (0%)
Std. of Damage (Mbps)	2,662.60 (+6.99%)	3,585.82 (+44.08%)	2,769.15 (+11.27%)	2,488.70 (0%)
Expected Damage + Std. of Damage (Mbps)	3,029.96 (+3.18%)	4,749.43 (+61.73%)	3,147.33 (+7.18%)	2,936.56 (0%)

The results show the tradeoffs among different risk-based survivable network designs. First, a comparison in term of the total risk or the average damage level is considered. The results show that the minimum-risk design always yields the smallest total risk level. Whereas, the min-max risk design (with $k1$=1, $k2$=100) and the minimum-RMS damage design have the comparable total risk levels; The min-max damage design (with $k1$=1, $k2$=1) results in the highest total risk level, much larger than the other designs (e.g., 68.72%, and 216.75% higher than the smallest possible value in Table 4.8, and Table 4.13, respectively). This is understandable because when the min-max damage design minimizes the maximum damage level, it does not take the probability of failure into a consideration. Therefore, the design might protect the network against failure scenarios which have high damage levels but a small probability of occurring, which results in a small risk reduction. Another reason is that in order for the min-max damage design to reduce the damage occurring in a dual-link failure state, the design must select the backup route for each failed link (in link protection) and each failed lightpath (in path protection) such that it does not traverse the other failed link in that dual-link failure state. As a result, the backup paths in the min-max damage design might take longer routes, and therefore require a higher spare capacity cost.

Next, we compare different risk-based designs in term of the maximum damage that could occur in the network from any network state. The results show that the min-max damage design provides the lowest maximum damage level; whereas all other designs result in the comparable maximum damage levels. For example, in the link protection case in Table 4.10, the min-max damage design results in a maximum damage of 70 Gbps, whereas other designs result in the same maximum damage level of 90 Gbps. Also, in the path protection case in Table 4.12,

the min-max damage design results in a maximum damage of 50 Gbps, whereas other designs result in the same maximum damage level of 80 Gbps.

We also compare the different risk-based designs in term of the maximum risk that could occur from any network state. The results show that the min-max risk design provides the lowest maximum risk level. Whereas, in most cases the min-max damage design results in the highest maximum risk level, which is significantly larger than the smallest maximum risk level (e.g., about 3 times higher in Tables 4.8 and 4.13)

Then, different risk-based designs are compared in term of the variability of damage that could occur in the network. The variability of damage is an important measure because the expected damage value seems to be the most appropriate measure only when an observation of damage level is made over an infinite period of time; however, in reality we are interested in the measures which are observed over a finite-time period, such as the loss of traffic per year, or the down time per year as defined in the Service Level Agreement (SLA). Over a finite period of time, the actual damage level that occurs could vary significantly and might be different from the expected value; therefore in this case the expected damage value is no longer the best measure, and the variability of damage should be considered.

Two measures of the variability of damage are presented here: the RMS of damage and the one-side standard deviation (Std.) of damage. The one-side standard deviation of damage is defined as $\sqrt{\sum_{s\in S: damage_s > \text{expected damage value}} stateprob_s (damage_s - \text{expected damage value})^2}$, where only the network states with the damage level greater than the expected damage value are included in the variability calculation since it makes sense to be only concerned about the variability of damage that is worse than the expected damage value. The RMS of damage measures the variability of damage above the zero-damage level, whereas the Std. of damage

measures the variability of damage above an expected damage value. In fact, the RMS damage can be viewed as the Std. of damage with zero expected damage value.

The results show that, among the risk-based designs being considered, the minimum-RMS damage design yields the lowest RMS value of damage, and the lowest one-side Std. of damage. Nevertheless, there is one case in Table 4.11 where the minimum-RMS damage design did not provide the lowest value for RMS damage level. This is understandable because the minimum-RMS damage design problem is solved by a heuristic approach which sometimes might not yield the optimal solution. The results also show that in most cases, the min-max risk design yields a lower RMS value of damage, and lower Std. of damage than the minimum-risk design. This is understandable because the min-max risk design includes a minimization of the maximum risk in its design objective, which tends to result in the lower variability of damage level. Whereas, the min-max damage design results in the highest values for both RMS of damage and Std. of damage. In fact, all of the above results show that the minimization of the maximum damage is a very costly design in terms of the total risk, the maximum risk, and the variability of damage.

We also compare different risk-based designs in term of a linear summation of the expected damage value (i.e., the total risk) and the one-side Std. of damage. This measure takes into account together the expected value and the variability of damage above the expected value. This is a common approach for comparing different investments in financial industry (i.e., an expected value and a variance of the portfolio's return). Based on this measure, we can say that one design is preferred to another design when it has a lower expected damage value and a lower Std. of damage than the other design; otherwise, a tradeoff between the minimization of the expected damage and the minimization of the variability of damage must be considered. This

tradeoff can be achieved through assigning the weight to each quantity indicating its relative importance according to the preference toward the expected value or the Std. of damage (i.e., risk-averse or risk-seeking). Here, we assume that the weights for both the expected damage and the variation of damage are equal to one.

From the results we observe that even though the minimum-risk design could provide the lowest expected damage value, it does not yield the lowest value for the sum of the expected damage and the one-side standard deviation of damage, due to its high Std. of damage value. The results show that in most cases the minimum-RMS damage design provides the lowest value for the sum of the expected damage and the one-side standard deviation of damage. The results also show that in most cases, the min-max risk design provides the value that is slightly higher than that from the minimum-RMS damage design; whereas the min-max damage design results in the highest value. Based on the results, by considering together the expected damage and the variability of damage, network operators may choose the minimum-RMS damage design and the min-max risk design as preferred design alternatives to the minimum-risk design approach, which is aimed at minimizing the expected damage value only.

Lastly, we compare different risk-based designs based on the probability distribution of damage. The damage distribution plots provide complete information about the damage levels and their associated probability. The probability distribution of damage in Network2 with no protection is shown in Figure 4.3. The probability distribution of damage for different risk-based link protection designs on Network 2 with a budget of 30 units are presented in Figure 4.4 (a)–(d); whereas the probability distributions of damage for the risk-based path protection designs on Network 2 with a budget of 20 units are presented in Figures 4.5 (a)–(d). Note that the probability associated with zero-damage level is not shown in the damage distribution plots due

to its higher value which cannot fit well with other probability value in the same plot, but are presented in Tables 4.9 and 4.12.

These damage distribution plots in Figures 4.4–4.5 show how the different risk-based designs reduce the failure probability associated with each damage level from the initial value in Figure 4.3. The results show the advantage of the minimum-RMS damage design over other design alternatives in that it results in lower probabilities for the higher damage levels. The minimum-RMS damage design, which aims at minimizing the variability of damage above zero damage, protects the network in a way that the network tends to have lower likelihood of high damage levels, at the expense of higher probabilities for the smaller damage levels, as compared to other design approaches. This can be illustrated by considering, for example, the results in the link protection case from the minimum-risk design in Figures 4.4 (a) and the minimum-RMS damage design in Figure 4.4 (d). The minimum-RMS damage design results in higher or comparable probabilities for the low damage levels (i.e., traffic loss rate of 10, 20, and 30 Gbps) than the minimum-risk design, but smaller or comparable probabilities for the larger damage levels (i.e., traffic loss rate of 40 Gbps and above). Another example is to compare the results from the minimum-risk path protection design in Figure 4.5 (a) and the minimum-RMS damage path protection design in Figure 4.5 (d). The minimum-RMS damage design results in higher probabilities for the low damage levels (i.e., traffic loss rate of 10 and 20 Gbps) than the minimum-risk design, but smaller or comparable probabilities for the larger damage levels (i.e., traffic loss rate of 30 Gbps and above).

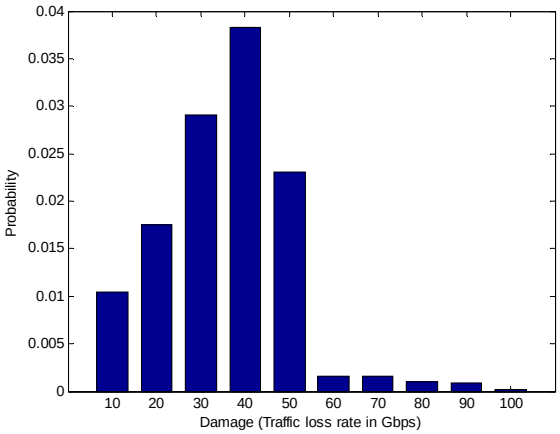


Figure 4.3 Probability distribution of damage in Network 2 with no protection deployed

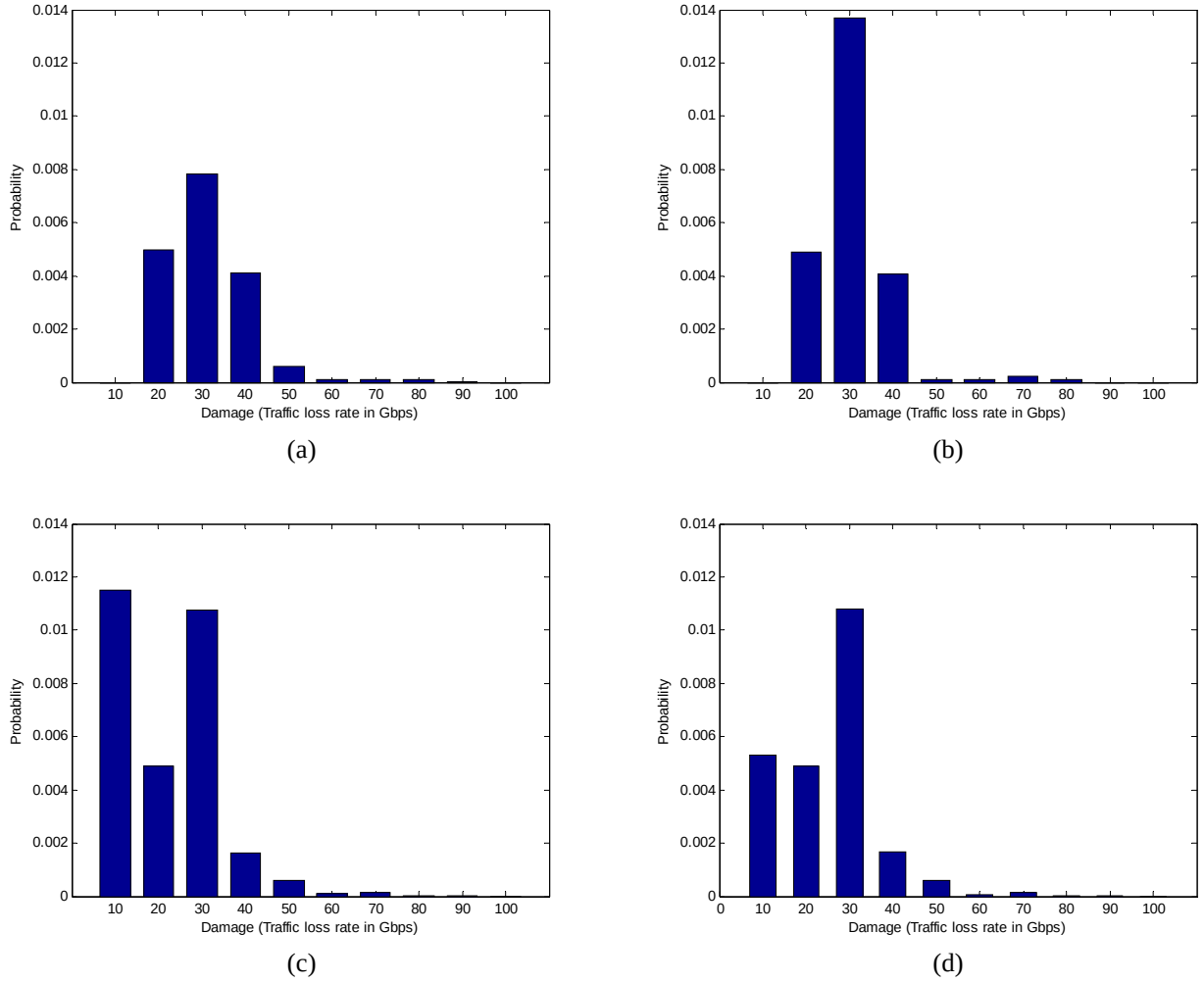


Figure 4.4 Probability distribution of damage in Network 2 with link protection using (a) minimum-risk design, (b) min-max damage design, (c) min-max risk design, and (d) minimum-RMS damage design for a budget of 30 units

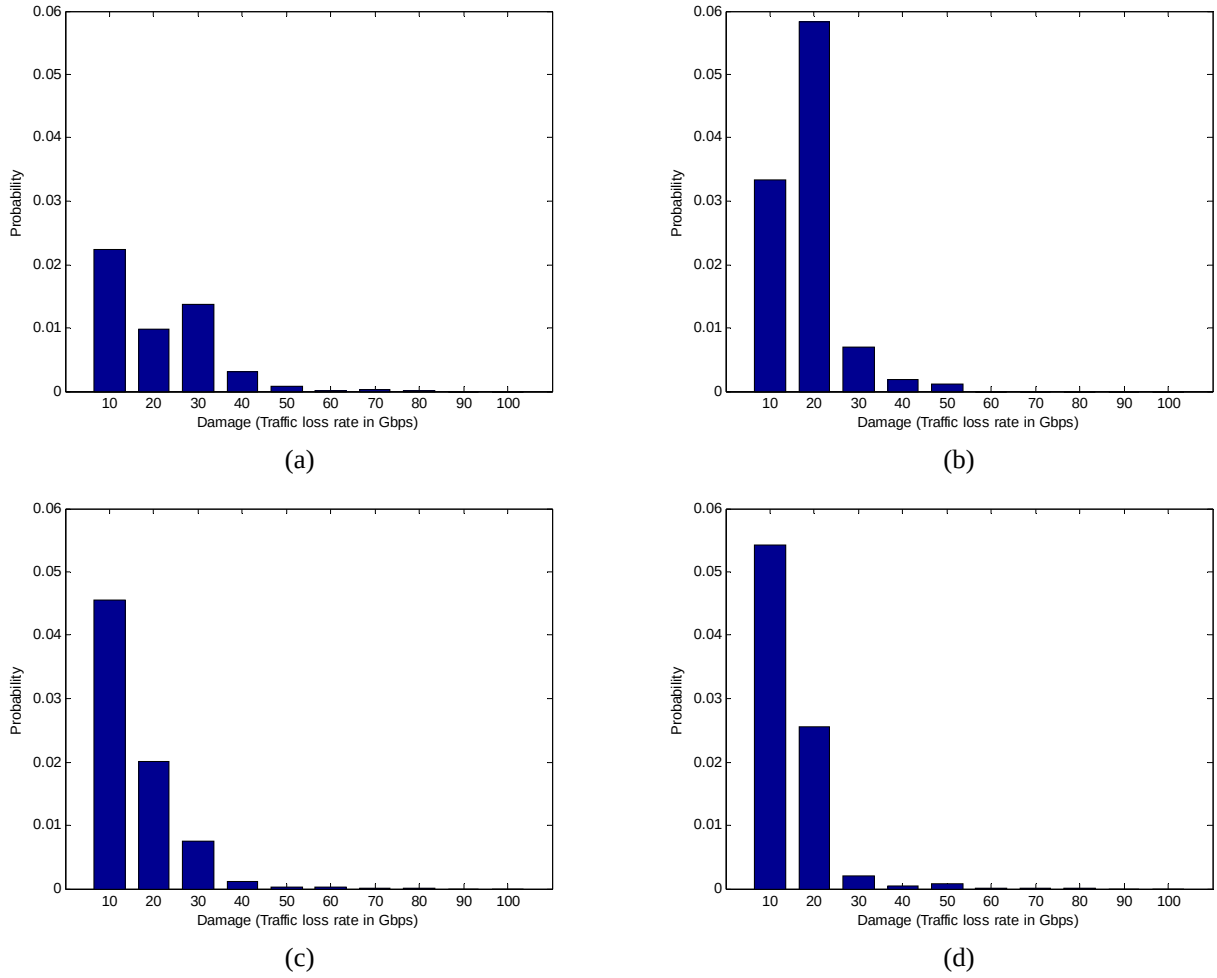


Figure 4.5 Probability distribution of damage in Network 2 with path protection using (a) minimum-risk design, (b) min-max damage design, (c) min-max risk design, and (d) minimum-RMS damage design for a budget of 20 units

4.4.4 Comparisons of different risk-based survivable network designs for networks with multiple classes of traffic

The results from different risk-based designs for networks supporting multiple classes of traffic are presented in this section. Three classes of traffic are defined for traffic flows (i.e., lightpaths): bronze, silver and gold, each associated with a different level of damage upon failure. In the experiments, we define the damage level caused by a failure of a bronze, silver, and gold traffic

flow as 1,000, 10,000, and 50,000 units, respectively. For the bronze traffic, a full-mesh of lightpath demands between all node-pairs are assumed; whereas for the silver and gold traffics, partial-mesh lightpath demands (i.e., between some node-pairs) are assumed in each network. Each lightpath carries the same data rate of 10 Gbps. In Network 2, the bronze, silver, and gold traffic are account for 53.79%, 38.64%, and 7.57% of the total network working capacity, respectively.

Table 4.14 compares the results from different risk-based link protection designs on Network 2 for a given budget of 54 units, which is about 50% of the minimum cost required to protect all the network links; whereas Table 4.15 compares the results from different risk-based path protection designs on the same network for a given budget of 40 units, which is about 50% of the minimum cost required to protect all the connections. Figure 4.6 shows the probability distribution of damage in Network2 with no protection; where as the probability distributions of damage in the same network with link protection, and path protection are given in Figures 4.7 (a)–(d), and Figures 4.8 (a)–(d), respectively.

We observe that the results presented here for networks supporting multiple classes of traffic are very consistent with the results for networks with single class of traffic in Section 4.4.3. The different risk-based deigns exhibit the same advantages and disadvantages as described in Section 4.4.3. That is, the minimum-risk design yields the smallest total risk level or average damage level. Whereas, the min-max risk design (with $k1$=1 and $k2$=100) and the minimum-RMS damage design have the comparable total risk levels; The min-max damage design (with $k1$=1 and $k2$=1) results in the highest total risk level, much larger than the other designs (e.g., 107.46% and 169.56% higher than the smallest possible value in Table 4.14, and Table 4.15, respectively). The result also shows that the min-max damage design provides the

lowest maximum damage level; whereas all other designs result in the comparable maximum damage levels. Moreover, the min-max risk design provides the lowest maximum risk level. Whereas, the min-max damage design results in the highest maximum risk level. Also, the minimum-RMS damage design yields the lowest value for RMS of damage, the lowest one-side Std. of damage, and the lowest value for the sum of the expected damage and the one-side standard deviation of damage. Whereas, the min-max damage design results in the highest values for the RMS of damage, the Std. of damage, and the sum of the expected damage and the one-side standard deviation of damage. Lastly, the result for the probability distribution of damage shows that the minimum-RMS damage design tends to have lower likelihood of high damage levels, at the expense of higher probabilities for the smaller damage levels, as compared to other design approaches.

Table 4.14 Comparison of different risk-based link protection designs on Network 2 with multiple classes of traffic for a budget of 54 units

Metric	Design's objective function			
	Total Risk	Total Risk + MaxDamage	Total Risk + 100×MaxRisk	RMS Damage
Probability of no Damage	0.9807	0.9415	0.9715	0.9688
Total Risk (units)	814.79 (0%)	1690.39 (+107.46%)	832.67 (+2.19%)	911.90 (+11.92%)
Maximum Damage (units)	169,000 (+40.83%)	120,000 (0%)	169,000 (+40.83%)	169,000 (+40.83%)
Maximum Risk (units)	173.27 (+27.55%)	454.63 (+234.68%)	135.84 (0%)	212.03 (+56.09%)
RMS Damage (units)	6,739.90 (+16.87%)	7,968.75 (+38.18%)	5,936.28 (+2.94%)	5,766.85 (0%)
Std. of Damage (units)	6,641.62 (18.11%)	7,612.66 (+35.38%)	5,819.99 (+3.50%)	5,623.09 (0%)
Expected Damage + Std. of Damage (units)	7,456.40 (+14.10%)	9,303.05 (+42.36%)	6,652.67 (+1.80%)	6,534.90 (0%)

Table 4.15 Comparison of different risk-based path protection designs on Network 2 with multiple classes of traffic for a budget of 40 units

Metric	Design's objective function			
	Total Risk	Total Risk + MaxDamage	Total Risk + 100×MaxRisk	RMS Damage
Probability of no Damage	0.8981	0.8760	0.8760	0.8760
Total Risk (units)	380.31 (0%)	1,025.15 (+169.56%)	424.54 (+11.63%)	417.77 (+9.85%)
Maximum Damage (units)	135,000 (+132.76%)	58,000 (0%)	145,000 (+150%)	135,000 (+132.76%)
Maximum Risk (units)	51.96 (+79.92%)	212.03 (634.18%)	28.88 (0%)	51.96 (+79.92%)
RMS Damage (units)	2,048.29 (+8.45%)	4,493.77 (+137.94%)	2,354.43 (+24.66)	1,888.61 (0%)
Std. of Damage (units)	1,980.13 (+10.02%)	4,268.75 (+137.18%)	2,281.49 (+26.76%)	1,799.83 (0%)
Expected Damage + Std. of Damage (units)	2,360.44 (+6.44%)	5,293.89 (+138.72%)	2,706.03 (+22.03%)	2,217.60 (0%)

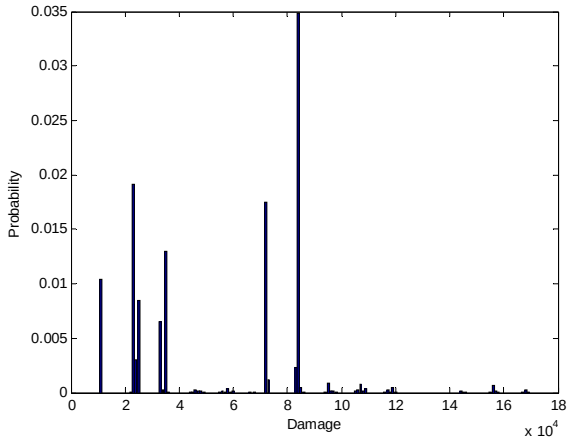


Figure 4.6 Probability distribution of damage in Network 2 with multiple classes of traffic with no protection

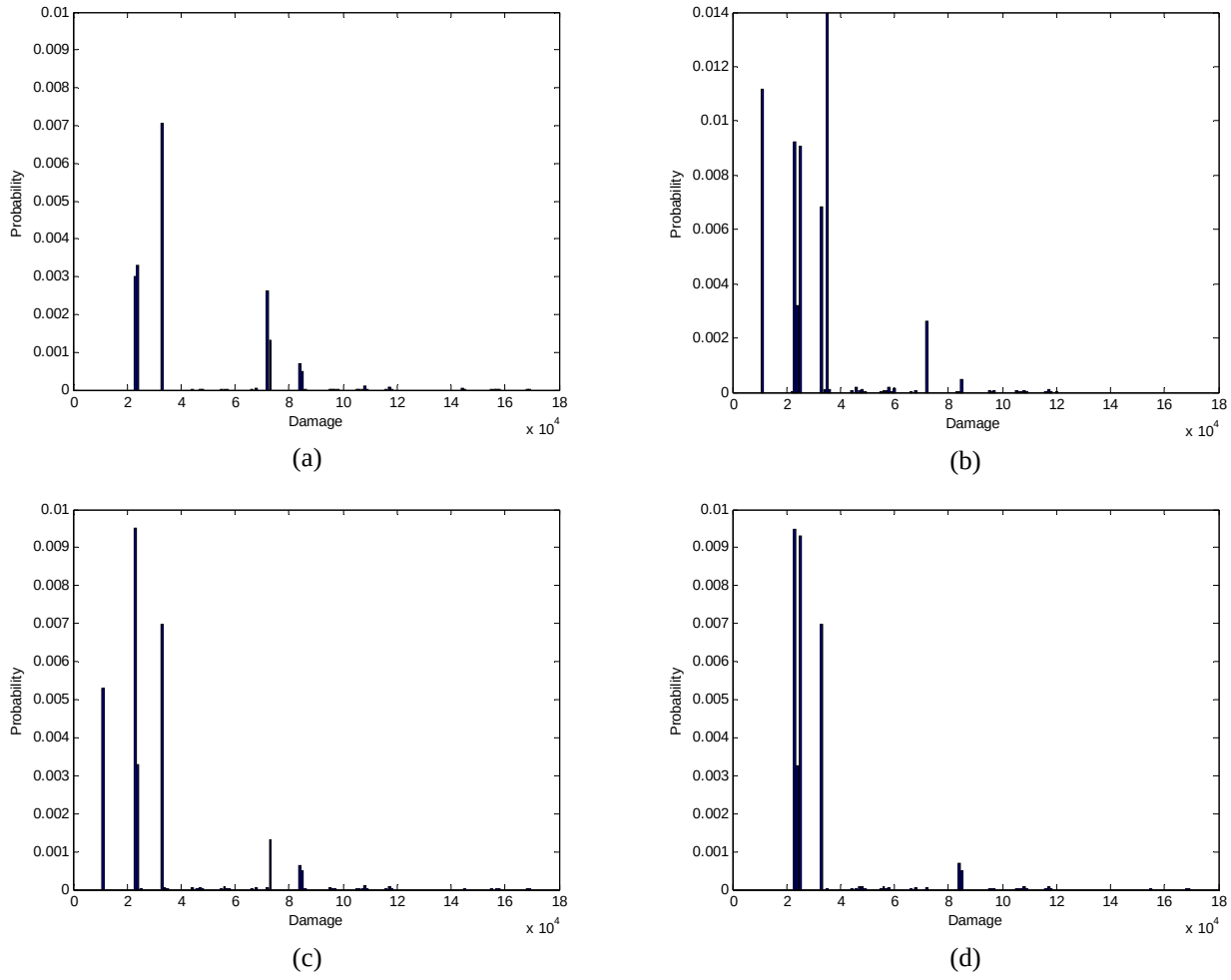


Figure 4.7 Probability distribution of damage in Network 2 supporting multiple classes of traffic with link protection using (a) minimum-risk design, (b) min-max damage design, (c) min-max risk design, and (d) minimum-RMS damage design for a budget of 54 units

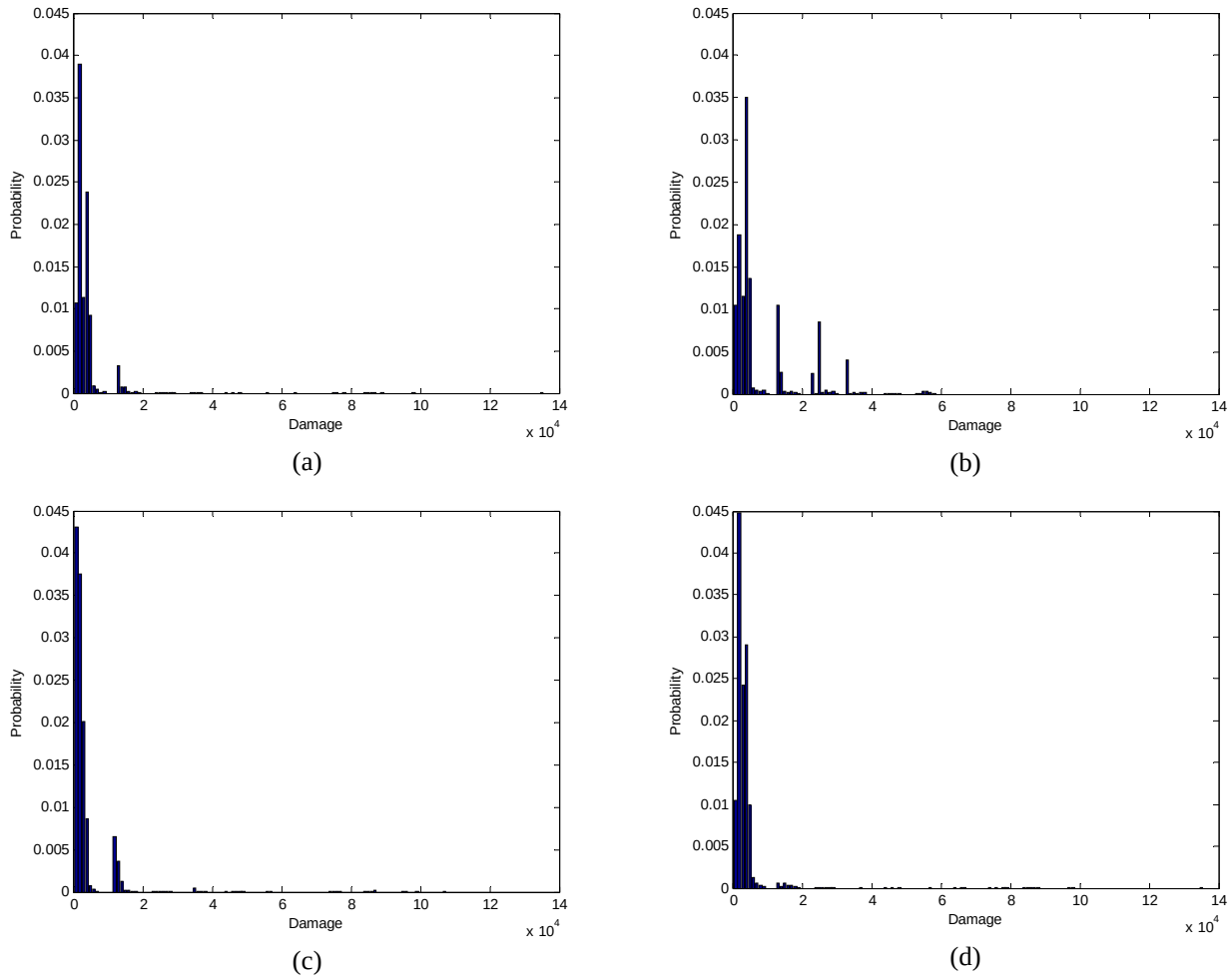


Figure 4.8 Probability distribution of damage in Network 2 supporting multiple classes of traffic with path protection using (a) minimum-risk design, (b) min-max damage design, (c) min-max risk design, and (d) minimum-RMS damage design for a budget of 40 units

4.5 CONCLUSIONS

Various risk-based survivable network designs are presented in this chapter. The min-max damage survivable network design, and the min-max risk survivable network design are formulated as Integer Programming (InP) models; where as the minimum-route mean square

(RMS) damage survivable network design is solved by a heuristic algorithm due to its non-linear objective function.

The advantages and disadvantages of different risk-based designs are illustrated through numerical results. If the total network risk or equivalently the expected value of damage is the only measure under consideration, the minimum-risk design is a preferred design alternative as it provides the minimum average damage level (i.e., total risk). However, if the expected value and the variability of damage are considered together, the minimum-risk design might not be the most preferred design, since it results in a higher variability than the minimum-RMS damage design. Determining which design is better depends on a preference toward the expected value or the variability of the damage. The results show that the minimum-RMS damage design could provide the lowest value for the sum of the expected damage and the standard deviation of damage. Also, the plots of probability distribution of damage also show an advantage of the minimum-RMS damage design in that the design results in smaller probabilities for the high damage levels, at the expense of higher probabilities for the smaller damage levels, when compared to other designs.

The results also show that minimizing the maximum damage that could occur in the network is a very expensive design approach. The min-max damage design is the most conservative design which tries to minimize the worst damage from failures, but it results in a much higher value of the expected damage and the variability of damage (i.e., RMS of damage, and Std. of damage) than other designs in most cases.

5.0 CONTRIBUTIONS AND SUMMARY

The contributions of this dissertation are twofold. First, this dissertation proposes a new approach for designing survivable networks, namely; risk-based survivable network design, which integrates risk analysis techniques into an incremental network design procedure with budget constraints. This design approach takes into account the network survivability aspects, as well as the economic aspects of an investment in network survivability. Then, based on the proposed risk-based design approach, this dissertation presents the solution methods, results, and analysis for different risk-based designs. Four risk-based designs are considered in the dissertation: the minimum-risk design, the min-max damage design, the min-max risk design, and the minimum-RMS damage design. These design problems are considered for the first time. The Integer Programming (InP) formulations for each design problem with link protection and path protection are also presented; whereas the minimum-RMS damage design is solved by the proposed greedy heuristic algorithm due to its nonlinearity.

Based on the numerical results, interesting observations about the risk-based design approach are made. First, the results reveal that the minimum-risk curves have a convex shape. Then, based on the minimum-risk curves, a cost-benefit analysis is presented. Network operators can use the cost-benefit analysis to determine whether an investment in network survivability is justified by the amount of risk reduction, and determine the optimal budget value which

maximizes the benefit of an investment. The proof in Apendix B shows that if the risk curve is convex, an optimal budget value always exists.

One advantage of the risk-based design approach is that it allows a tradeoff between the survivability cost saving and the amount of risk reduction in the network. The results show that network operators can achieve a substantial budget savings by allowing a slightly higher risk level in the network.

The minimum-risk design for networks with multiple classes of traffic is also presented. The results show that network operators can use the minimum-risk design approach to design the networks in accordance with different availability requirements for different traffic classes as defined in the Service Level Agreement (SLA).

As communication services require a higher level of network availability, network operators may consider protecting their network with dual protection. This dissertation also presents the incremental minimum-risk design for dual-protected networks, which can be used to determine in which parts of the networks to deploy the additional protection for a given budget. The results show that the risk curves for an investment in dual protection also have a convex shape, which indicates the existence of an optimal budget value for investing.

The results from different risk-based designs are also compared. If only the total network risk or expected damage value is considered, the minimum-risk design is the most preferred design as it could provide the minimum value. However, if the expected value and the variability of damage are considered together, the minimum-risk design might not be the best design, since other designs such as the min-max risk design, and especially the minimum-RMS damage design provide lower variability in the damage. Different network operators may choose different design alternatives based on their preferences toward the expected value or the variability of

damage. In addition, if the maximum damage that could occur in the network is the major concern for network operators, the min-max damage design should be considered as this conservative design approach provides the smallest maximum damage level. However, this design approach results in a very high expected damage level, and a high variability in the damage.

Additional future research works on risk-based survivable network design approaches are possible. The simplest extension is to consider other survivability techniques, such as link restoration, and path restoration. Unlike the dedicated protection techniques, the risk-based design for restorable networks is to determine how to allocate spare capacity to different parts of the network without specifying which links or connections to protect, because spare capacity is shared and can be used for failure recovery of any failed links or failed connections in the network. Another possible extension is to consider the risk-based designs for multi-layer networks. The cost model used in the risk-based designs can also be improved as the current model only considers the spare capacity cost. Lastly, another future research direction is to incorporate connection availability requirements along with the associated violation penalties as defined in Service Level Agreements (SLA), directly into the risk-based design approach. This may provide an answer to questions, such as, how should network operators set the required availability level and the associated penalty value in the SLA so that an investment in network survivability is justified.

APPENDIX A

UNAVAILABILITY CALCULATION OF CABLE LINK

Unavailability (U) is defined as the probability that the component will be found in the failure state at a random time in the future. In repairable systems in which failed components are replaced or repaired after a failure occurs, the unavailability of a component is

$$U = \frac{MTTR}{MTTF + MTTR} = \frac{MTTR}{MTBF}, \tag{A.1}$$

where MTTR denotes Mean Time To Repair, and MTTF denotes Mean Time To Failure. Note that, the Mean Time Between Failure (MTBF) is given by MTBF = MTTR+MTTF. For fiber optic cables, the MTBF is typically represented by a Cable Cut (CC) metric [4], which is the average cable length (km) that results in a single cable cut per year. For a given CC, MTBF of a fiber optic cable can be calculated by (A.2), where 365×24 is the amount of time in hours per year.

$$MTBF_{cable}(hour) = \frac{CC \times 365 \times 24}{cable\ length\ (km)} \tag{A.2}$$

APPENDIX B

PROOF OF EXSISTENCE OF OPTIMAL BUDGET VALUE

This appendix provides a proof that if the risk curve is convex, there always exists an optimal budget value which maximizes the benefit of an investment in network protection.

The notation used in this section is shown in Table B.1

Table B.1 Notation used in APPENDIX B

x	A variable denoting the budget (monetary unit)
$B(x)$	The benefit (monetary unit) as a function of variable x
I	A constant representing an initial risk level (risk unit) in the network
$R(x)$	Amount of risk (risk unit) in the network as a function of variable x (i.e., a minimum-risk curve)
M	A constant representing an equivalent monetary value per unit of risk reduction (monetary/risk unit)

The benefit (monetary unit) of an investment in network protection is defined as the amount of risk reduction (monetary unit) subtracted by the budget or the protection cost (monetary unit) as shown in (3.118). Based on the notation in Table B.1, the investment benefit equation can be written as in (B.1), where $B(x)$ and $R(x)$ are defined over a budget range $[a, b]$.

$$B(x) = \mathrm{M}\left(\mathrm{I} - R(x)\right) - x, \quad \text{for } a \le x \le b \tag{B.1}$$

Taking the second derivative of the right hand side of (B.1) with respect to *x*, we have

$$\frac{d^2}{dx^2}\left(\mathrm{M}\left(\mathrm{I} - R(x)\right) - x\right) = -\frac{d^2}{dx^2} R(x).$$

Since $R(x)$ is a convex function over a budget range [*a*, *b*], thus $\frac{d^2}{dx^2} R(x) \ge 0$ over the range [*a*, *b*].

Therefore,

$$\frac{d^2}{dx^2} B(x) \le 0, \quad \text{for } a \le x \le b.$$

Since the second derivative of the benefit $B(x)$ is less than or equal to zero, the benefit $B(x)$ is a concave function. Therefore, there always exists a value of *x* which gives a maximum value of $B(x)$. The optimal budget value $x_{optimal}$ is the value of *x* which gives the first derivative of the benefit function equal to zero as in (B.2) or (B.3).

$$\frac{d}{dx}\left(\mathrm{M}\left(\mathrm{I} - R(x)\right) - x\right) = 0 \tag{B.2}$$

$$\frac{d}{dx} R(x) = -\frac{1}{\mathrm{M}} \tag{B.3}$$

If there is no value of *x* in the range of [*a*, *b*] that satisfies (B.2) or (B.3), the optimal budget value still exists and equals to the budget value at the edge of the budget range, i.e., either at $x_{optimal} = a$ or $x_{optimal} = b$.

The example below illustrates that the optimal budget value obtained from the analytical approach in (B.3) is equal to the optimal budget value from the experiment. Figure B.1 shows the minimum-risk curves for link protection and path protection on Network 3. Assuming that the

risk reduction of 40 Mbps is equal to one monetary unit (i.e., M = 1/40), from (B.3) the optimal budget value from the analytical approach is the budget value at which a slope of the risk curve is equal to -40. In Figure B.1, the straight lines with a slope -40 are also shown, which can identify the point at which the slope of each risk curve equals to -40. As shown in Figure B.1, the optimal budget value from an analytical approach is 27.5 units, and 52.5 units in the link protection case and the path protection case respectively. These optimal budget values are equal to the optimal budget values obtained from the experiment which maximize the benefit as shown in Figure B.2 (a) and (b) for the link protection and path protection cases, respectively.

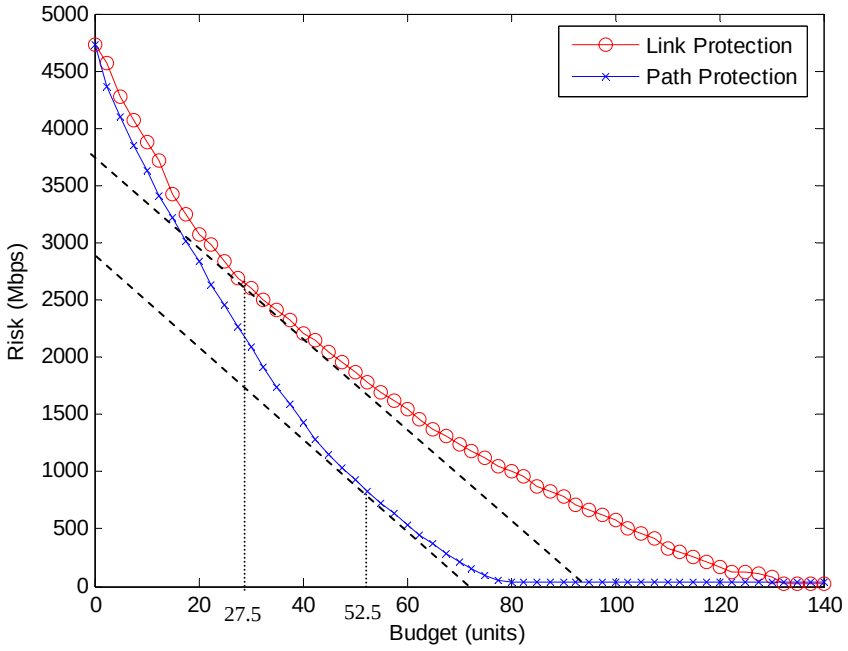
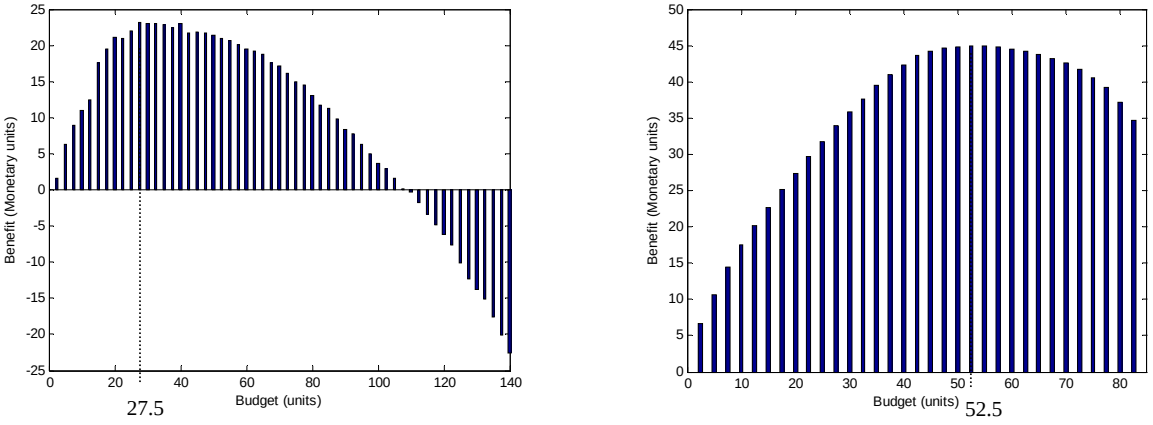


Figure B.1 Minimum-risk curves (Risk vs Budget) for link protection and path protection on Network 3 and optimal budget values obtained from analytical approach



(a) (b)

Figure B.2 Benefit plots for (a) link protection, and (b) path protection on Network 3 showing the optimal budget value of 27.5 units, and 52.5 units, respectively.

BIBLIOGRAPHY

[1] W. D. Grover, *Mesh-based Survivable Networks: Options and Strategies for Optical, MPLS, and ATM Networking*. New Jersey: Prentice Hall PTR, 2003.

[2] M. Pioro and D. Medhi, *Routing, Flow, and Capacity Design in Communication and Computer Network*. San Francisco, CA: Morgan Kauffman Publishers, 2004.

[3] H. Mouftah and P.-H Ho, *Optical Networks: Architecture and Survivability*. Norwell, MA: Kluwer Academic Publisher, 2003.

[4] J. Vasseur, M. Pickavet, and P. Demeester, *Network Recovery*. Morgan Kaufmann Publishers, 2004.

[5] G. Maier, S. De Patre, A. Pattavina, and M. Martinelli, "Optical network survivability: protection techniques in the WDM layer," *Photonic Networks Communications*, vol. 4, no. 3-4, Jul.-Dec. 2002.

[6] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," *Journal of Lightwave Technology*, vol. 21, issue 4, pp. 870 – 883, April 2003.

[7] J. Doucette and W.D. Grover, "Comparison of mesh protection and restoration schemes and the dependency on graph connectivity," in *Proc. Of the 3rd International Workshop on Design of Reliable Communication Networks (DRCN 2001)*, Budapest, Hungry, Oct. 2001, pp. 121-128.

[8] R.R. Iraschko, M.H. MacGregor, and W.D.Grover, "Optimal capacity placement for path restoration in STM or ATM mesh-survivable networks," *IEEE/ACM Transactions on Networking*, vol. 6, issue 3, pp. 325 – 336, Jun. 1998.

[9] Y. Xiong and L.G. Mason, "Restoration strategies and spare capacity requirements in self-healing ATM networks," *IEEE/ACM Transactions on Networking*, vol. 7, issue 1, pp. 98 – 110, Feb. 1999.

[10] M. Clouqueur and W. D. Grover, "Mesh restorable networks with enhanced dual failure restorability properties," *Photonic Network Communications*, vol. 9, no. 1, pp. 7-18, Jan. 2005.

[11] J. Doucette and W. D. Grover, "Shared-risk logical span Groups in span-restorable optical networks: analysis and capacity planning model," *Photonic Network Communications*, vol. 9, no. 1, pp. 35-53, Jan. 2005.

[12] M. Herzberg and S. J. Bye, "An optimal spare-capacity assignment model for survivable networks with hop limits," in *Proc. of IEEE Global Telecommunications Conference*, vol. 3, Nov. 28 – Dec. 2, 1994, pp. 1601 – 1606.

[13] G. Shen and W. Grover, "Capacity requirements for network recovery from node failure with dynamic path restoration," in *Proc. of Optical Fiber Communications Conference 2003 (OFC 2003)*, vol. 2, 23-28 Mar. 2003, pp. 775- 777.

[14] K. Murakami and H.S. Kim, "Optimal capacity and flow assignment for self-healing ATM networks based on line and end-to-end restoration," *IEEE Transaction on Networking*, vol 6, issue 2, pp. 207-221, Apr. 1998.

[15] Yu Liu, D. Tipper, and P. Siripongwutikorn, "Approximating optimal spare capacity allocation by successive survivable routing," *IEEE/ACM Transactions on Networking*, vol. 13, no. 1, pp. 198-211, Feb. 2005.

[16] J. Doucette, M. Clouqueur, and W. D. Grover, "On the availability and capacity requirements of shared backup path-protected mesh networks," *Optical Networks Magazine*: *Special issue on engineering the next generation optical Internet*, vol. 4, no. 6, pp. 29-44, Nov./Dec. 2003.

[17] R. Ramamurthy, Z. Bogdanowicz, S. Samieian, D. Saha, B. Rajagopalan, S. Sengupta, S. Chaudhuri, and K. Bala, "Capacity performance of dynamic provisioning in optical networks," *Journal of Lightwave Technology*, vol. 19, issue 1, pp. 40 – 48, Jan. 2001.

[18] M. S. Kodialam and T. V. Lakshman, "Dynamic routing of restorable bandwidth-guaranteed tunnels using aggregated network resource usage information," *IEEE/ACM Transactions on Networking*, vol. 11, no. 3, pp. 399-410, Jun. 2003.

[19] Yu Liu, and David Tipper, "Successive survivable routing for node failures," in *Proc. of IEEE Global Telecommunications Conference (GLOBECOM 2001)*, vol. 4, San Antonio, TX, Nov. 25-29, 2001, pp. 2093-2097.

[20] Y. Liu, D. Tipper, and K. Vajanapoom, "Spare capacity allocation in two-layer networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, issue 5, pp. 974-986, Jun. 2007.

[21] Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating optimal spare capacity allocation by successive survivable routing," in *Proc. of the Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2001)*, vol. 2, Apr. 22-26, 2001, pp. 699 – 708.

[22] C. Chekuri, A. Gupta, A. Kumar, J. Naor, and D. Raz, "Building edge-failure resilient networks," in *Proc. of the 9th International Conference on Integer Programming and Combinatorial Optimization (IPCO)*, May 27-29, 2002, pp.439-456.

[23] M. Alicherry and R. Bhatia, "Pre-provisioning networks to support fast restoration with minimum over-build, in *Proc. of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004)*, vol. 1, Mar. 7-11, 2004, pp.- 164.

[24] H. Zang and B. Mukherjee, "Path-protection routing and wavelength-assignment (RWA) in WDM mesh networks under duct-Layer constraints," *IEEE/ACM Transactions on Networking*, vol. 11, no. 2, Apr. 2003.

[25] M. Tornatore, G. Maier, and A. Pattavina, "Cost and benefits of survivability in an optical transport network," in *Telektronikk*, Feb. 2005.

[26] R. Bhandari, "Optimal diverse routing in telecommunication fiber networks," in *Proc. of IEEE INFOCOM 94*, vol. 3, Toronto, Ontario, Canada, Jun. 1994, pp. 1498–1508.

[27] M. Clouqueur, and W.D. Grover, "Availability analysis of span-restorable mesh networks, *IEEE Journal on Selected Areas in Communications*, vol. 20, issue 4, pp. 810 – 821, May 2002.

[28] R. Clemente, L. Serra, G. D'Orazio, and G.Cosmo, "A framework for class of service definition in GMPLS-based meshed ASTN," in *Proc of the 4th International Workshop on Design of Reliable Communication Networks 2003 (DRCN 2003)*, Oct. 19-22, 2003, pp. 93 – 100.

[29] D. Arci, G. Maier, A. Pattavina, D. Petecchi, and M. Tornatore, "Availability models for protection techniques in WDM networks," in *Proc. of the 4th International Workshop on Design of Reliable Communication Networks 2003 (DRCN 2003)*, Oct. 19-22, 2003, pp. 158 – 166.

[30] B.T. Doshi, D.R. Jeske, N. Raman, and A. Sampath, "Reliability and capacity efficiency of restoration strategies for telecommunication networks," in *Proc. of the 4th International Workshop on Design of Reliable Communication Networks 2003 (DRCN 2003)*, Oct. 19-22, 2003, pp.440 – 447.

[31] R. Hülsermann, M. Jäger, A. M. C. A. Koster, S. Orlowski, R. Wessäly, and A. Zymolka, "Availability and cost based evaluation of demand-wise shared protection," in *Proc. of the 7th ITG-Workshop on Photonic Networks*, Leipzig, Germany, pp. 161-168.

[32] A. Di Giglio, G. Di Giorgio, and M. Quagliotti, "Cost and reliability comparison of some static and dynamic multilayer resilience schemes," in *Proc. of the 5th International Workshop on Design of Reliable Communication Network 2005. (DRCN 2005)*, Oct. 16-19, 2005.

[33] G. Willems, P. Arijs, W. Van Parys, and P. Demeester, "Capacity versus availability trade-offs in mesh-restorable WDM networks," in *Proc. of the 3rd International Workshop on Design of reliable Communications Networks (DRCN 01)*, Budapest, Hungary, Oct. 2001, pp. 107-112.

[34] S. Verbrugge, D. Colle, P. Demeester, R. Huelsermann, and M. Jaeger, "General availability model for multilayer transport networks," in *Proc. of 5th IEEE Int. Workshop on Design of Reliable Communication Networks (DRCN 2005)*, Ischia, Italy, Oct. 16-19, 2005.

[35] R. Clemente, A. del Pistoia, M. Bartoli, Dapos, G. Orazio, and B. Pennestri, "Short term strategies for a carrier-class IP over optics network," in *Proc. of the 5th International Workshop on Design of Reliable Communication Networks 2005 (DRCN 2005)*, Ischia, Italy, Oct. 16-19, 2005.

[36] M. Tornatore, G. Maier, and A. Pattavina, "Availability design of optical transport networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, issue 8, pp. 1520-1532, Aug. 2005.

[37] P. Pongpaibool and H. S. Kim, "Novel algorithms for dynamic connection provisioning with guaranteed service level agreements in IP-over-optical networks," in *Proc. of IEEE Global Telecommunications Conference (Globecom 2003)*, vol. 5, Dec. 2003, pp. 2643-2648.

[38] J. Zhang, K. Zhu, H. Zang, and B. Mukherjee, "A new provisioning framework to provide availability-guaranteed service in WDM mesh networks," in *Proc. of IEEE International Conference on Communications 2003 (ICC'03)*, vol. 2, May 11-15, 2003, pp. 1484 – 1488.

[39] J. Zhang, K. Zhu, H. Zang, and B. Mukherjee, "Service provisioning to provide per-connection-based availability guarantee in WDM mesh networks," in *Proc. of Optical Fiber Communications Conference 2003 (OFC 2003)*, vol.2, Mar. 23-28, 2003, pp. 622 – 624.

[40] D.A. Schupke, and F. Rambach, "A link-flow model for dedicated path protection with approximative availability constraints", *IEEE Communications Letters*, vol. 10, issue 9, pp. 679 – 681, Sep. 2006.

[41] D.A. Schupke, "Guaranteeing service availability in optical network design," presented at the Asia-Pacific Optical Communications Conference (APOC), Shanghai, China, Nov. 6-10, 2005.

[42] M. Clouqueur, W.D. Grover, "Availability analysis and enhanced availability design in *p*-cycle-based networks," *Photonic Network Communications*, vol. 10, no. 1, pp. 55-71, Jul. 2005.

[43] D. Leung, W.D. Grover, "Capacity planning of survivable mesh-based transport networks under demand uncertainty," *Photonic Network Communications*, vol. 10, no. 2, pp. 123-140, Sep. 2005.

[44] D. Medhi, A unified approach to network survivability for teletraffic networks: models, algorithms and analysis, *IEEE Transactions on Communications*, vol. 42, issue 234, pp. 534-548, Feb/Mar/Apr. 1994.

[45] D. Medhi, "Network reliability and fault tolerance", *Wiley Encyclopedia of Electrical Electronics Engineering*, vol. 14, pp. 213-218, 1999.

[46] V. O. K. Li and J. A. Silvester, "Performance analysis of networks with unreliable components," *IEEE Transactions on Communications*, vol. 32, issue 10, pp. 1105-1110, Oct. 1984.

[47] P. Kubat, "Reliability analysis for integrated networks with application to burst switching," *IEEE Transaction on Communications*, vol. 34, issue 6, pp. 564-568, Jun. 1986.

[48] P. Kubat, "Assessing throughput and reliability in communication and computer networks," *IEEE Transactions on Reliability*, vol. 37, issue 3, pp. 208-211, Aug. 1988.

[49] B. Sansó, F. Soumis, and M. Gendreau, "On the evaluation of telecommunications network reliability using routing models," *IEEE Transactions on Communications*, vol. 39, issue 10, pp. 1494-1501, Oct. 1991.

[50] B. Sansó and F. Soumis, "Communication & transportation network reliability using routing models," *IEEE Transaction on Reliability*, vol. 40, issue 1, Apr. 1991.

[51] B. B.M. Shao, "Optimal redundancy allocation for information technology disaster recovery in the network economy," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, issue 3, pp. 262-267, Jul. 2005.

[52] B. M. Ayyub, *Risk Analysis in Engineering and Economics*. Chapman and Hall/CRC Press, 2003.

[53] H. Kumamoto and E. Henley, *Probabilistic Risk Assessment for Engineers and Scientists*. New York: IEEE Press, 1996.

[54] N. H. Roberts, W.E EG-0492. Vesely, D.F. Haasl, and F. F., Goldberg, *Fault Tree Handbook*. Washington, DC: NURm U.S. Nuclear Regulatory Commission, 1981.

[55] S. Barnett, *Matrices: Methods and Applications*. Oxford University Press, 1990, pp. 29-32.

[56] B. Kolman, R. C. Busby, and S. Ross, *Discrete Mathematical Structures*. New York: Prentice-Hall, 1996.