Telecommun Syst
DOI 10.1007/s11235-011-9578-1

Risk based resilient network design

Korn Vajanapoom · David Tipper · Sira Akavipat

Abstract This paper presents a risk-based approach to resilient network design. 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 managing 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. A design methodology for the proposed risk-based survivable network design approach is presented within an optimization model framework. Numerical results and analysis illustrating the different risk based designs and the tradeoffs among the schemes are presented.

Keywords Risk · Survivable networks · Fault tolerance · Incremental design

1 Introduction

Communication networks are one of the critical infrastructures upon which society depends [1, 2]. Recognition of this has led to a body of work on designing survivable networks with a focus on wired backbone networks [3–6]. The basic approach for survivable network design is for a given network technology (e.g., WDM) and a given survivability technique (e.g., link protection, path protection, shared backup path protection, p-cycles etc.), a network is designed to survive a set of predefined failures, (e.g., all single link failures), with minimum cost [3–6]. This basic design approach involves determining an allocation of spare capacity in the network and an assignment of backup routes to minimize the cost.

However, a limitation of this minimum-cost design approach is that it treats all failures equally without considering the variability in failure impacts and likelihood of failures. Several, recent studies have noted that failure rates and repair rates are geographically correlated [1, 7, 8] due to a number of factors. Examples of factors are variations in: weather, workforce capabilities, exposure to natural disasters (e.g., earthquakes, hurricanes, ice storms, etc.), local regulations (e.g., call before dig penalties), and power supply reliability. An additional major drawback of the minimum-cost design approach is the hidden assumption that sufficient monetary funds are available to protect all the predefined failure scenarios. 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). Often operators have to build out the survivable network in pieces in an incremental manner based on a chronological sequence of budgets. Even in a situation that the network operators have sufficient monetary funds to protect the networks against any set of failures, they may prefer to reduce their capital expenditures in network survivability by choosing to protect only some parts of the networks based on a cost-benefit analysis. This situation

K. Vajanapoom · D. Tipper (✉) · S. Akavipat
Graduate Telecommunications and Networking Program, University of Pittsburgh, Pittsburgh, PA 15260, USA
e-mail: tipper@tele.pitt.edu

K. Vajanapoom
e-mail: korn.v@samtel.samartcorp.com

S. Akavipat
e-mail: sia10@pitt.edu

Published online: 25 August 2011

cannot directly be addressed in the minimum-cost design approach.

Here, we propose a different approach based on the adoption of risk management techniques. Risk management has been advocated for critical infrastructure protection as the method of choice in allocating scarce/spare resources for guarding against failure, accidents and attacks [2, 9, 10]. Risk analysis is widely used in aerospace and civil engineering, IT security and economics [1, 11, 12]. 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 defined as the product of the failure probability and the magnitude of damage caused by the failure [11]. In communication networks, potential failures, such as fiber cuts and equipment failures (e.g., router, cross connect, etc.) cause a risk to the network. Typically, different parts of the network are associated with different risk levels. For example, the rate of cable cuts per km of cable in the United States shows a large variation based on the geographic location and population density. In addition, failures in some parts of the network could result in 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 data traffic. Also, the cost for deploying a survivability technique varies across different parts of the network. For example, some network links may have longer backup paths than others, based on the network topology (and the routing policy of backup paths) and thus require a higher spare capacity cost.

Observing that the risk level and the survivability cost vary across the network infrastructure, therefore in the case where network operators have a fixed budget for improving network survivability, they need to have careful planning to determine the best budget allocation for deploying network survivability in different parts of the network based on managing the risk (i.e., failure impacts and likelihood of failures). This is the design problem we consider in the risk based resilient network design approach proposed here. Note, that different risk metrics can be used in the resilient network design problem. The typical metric is to minimize the average network risk. However, in many fields (e.g., finance, civil engineering, etc.) one often considers different risk based metrics such as the maximum risk or maximum damage that occurs for the failure scenarios considered or a metric that considers both the mean risk and its variability. Here, we formulate four risk management resilient network design techniques using link protection or path protection to provide survivability. The first approach minimizes the average network risk. The second formulation is a linear combination of the mean network risk and the maximum damage from the worst case failure scenario. The third model minimizes a linear combination of the mean network risk and the maximum risk case. Lastly, we consider minimizing the variability of risk across all failure scenarios using a minimum root mean squared damage metric. Additionally, solution methods for the optimization formulations, along with numerical results and analysis illustrating the different risk based designs and the tradeoffs among them are presented.

The remainder of the paper is organized as follows. Section 2 introduces the risk approach for resilient network design. The proposed risk management based resilient network design techniques are presented in Sect. 3. Section 4 reports numerical results and a comparative evaluation of the different risk management survivable network designs. Lastly, Sect. 5 summarizes our conclusions.

2 A risk based approach

The risk-based design approach proposed here integrates risk analysis techniques into an incremental network design procedure with budget constraints. In engineering fields, the term risk measures two quantities related to failures: the likelihood of failure and the amount of damage resulting from the failure. The risk of a failure is commonly defined as the product of the failure probability and the magnitude of damage caused by the failure [11]. In communication networks, potential failures, such as fiber cuts and equipment failures (e.g., router, line card, etc.) cause a risk to the network. As noted above, different geographic parts of the network have different risk levels. Furthermore, network failures result in different levels of damage depending on the type of traffic carried. These factors can be incorporated into a risk metric as discussed below.

Risk assessment is a process of quantifying the amount of risk associated with failures in the network. The risk of failure is defined as the probability of failure times the damage from failure [11]; 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 (i.e., failure scenarios). Each network state uniquely identifies a set of failed components and working components in that state. Let S denote the set of network failure states, or failure scenarios, indexed by s. The risk associated with network state s, denoted by $risk_s$, is equal to the product of the probability of the 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 (1).

$$risk_s = stateprob_s \times damage_s \tag{1}$$

By definition all network states are mutually exclusive to each other. Thus the network risk, denoted by *Netrisk*, can be calculated by summing the risk associated with each network state over all states, as in (2). In fact, the total network

risk in (2) can be interpreted as the mean or expected damage level across all network states.

$$Netrisk = \sum_{s \in S} stateprob_s \times damage_s \tag{2}$$

For each network state, the state probability can be calculated by multiplying together the appropriate failure probability (i.e., unavailability) and availability of all network components. If link failures (e.g., cable cuts in optical networks) 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 obtained as in (3). Note that L denotes a set of links; $state_{s,i}$ represents the network failure states, where $state_{s,i} = 1$ if link i fails in network state s, and $state_{s,i} = 0$ otherwise; and u_i denotes the unavailability of cable i.

$$stateprob_s = \prod_{i \in L} u_i^{state_{s,i}} (1 - u_i)^{1 - state_{s,i}} \tag{3}$$

The amount of damage that occurs in each network state or failure scenario can be measured in different ways. However, in connection-oriented networks, such as WDM, and MPLS, it is natural to consider the amount of damage associated with the loss of each end-to-end connection (e.g., lightpaths in WDM, LSPs in MPLS) due to network failures. Hence, the amount of damage that occurs in network state s is the sum of damages of all failed connections in network state s, as shown in (4), where dam_r is the amount of damage caused by a failure of connection r.

$$Netrisk = \sum_{s \in S} stateprob_s \left(\sum_{\substack{\text{all failed connections } r \\ \text{in network state } s}} dam_r \right) \tag{4}$$

Note that if information on the traffic is available, one can construct a damage metric associated with each end-to-end connection that incorporates the societal or monetary effects of the loss. Here the amount of damage caused by a failure of connection r is equal to the data rate of connection r itself (i.e., $dam_r = m_r$).

Once the risk has been identified and assessed, the next component in the design approach is a risk management investment strategy. The task of a risk management investment strategy is to determine how to allocate a fixed budget for deploying resources in the network in order to reduce or manage the network risk. These techniques can be categorized as prevention, and survivability techniques.

Prevention techniques seek to reduce the failure probability or increase the reliability of network components. In communications networks, this can be achieved by using more reliable network equipment, backup power supplies, etc. However, improving network components' reliability is sometimes technically infeasible. Even if the most reliable network components are deployed, the desired level of network risk may still not be achieved. Therefore, survivability techniques are also employed. Survivability techniques perform a corrective action upon 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.

Various techniques for reducing the risk of failures in communication networks exist (e.g., p-cycles, $1 + 1$ protection, etc). In this paper, we study both link protection and path protection schemes [3, 5, 6]. In link protection, a backup path that reconnects the end points of the protected link is determined with appropriate spare capacity allocated to the backup path in order to recover all the working capacity on the protected link.

In path protection, one sets up an end-to-end backup path with appropriate spare capacity for a protected connection (e.g., LSP in MPLS, end to end lightpath in WDM). In the link protection case, the task of risk management design is to determine which network links to protect and their corresponding backup routes for a given budget to achieve a risk-based objective. Whereas in path protection, the risk based design is used to determine which end-to-end connections to protect and their corresponding backup routes based on the risk criteria subject to a budget constraint.

Different design objectives can be considered in the risk based design approach. For example the basic design objective is to minimize the network risk as in (4). Alternative design objectives include minimizing the maximum damage that could occur in the network from any failure scenario, minimizing the maximum risk that could occur in the network for any failure scenario or minimizing the variability of damage across network states as determined by the root mean square (RMS) of the damage.

Figure 1 illustrates the overall design process along with inputs and outputs of the risk-based design. First, the working network, which includes a network topology, and working routes of all end-to-end connections, is given to the risk-based survivable network design problem. The given working network may have been designed based on any design objective, such as minimizing the cost, minimizing the delay or hop counts, maximizing network utilization [3], etc.

A survivability cost model and a fixed budget are also given to the risk based design problem. In the design procedure used here, an assumption 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 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

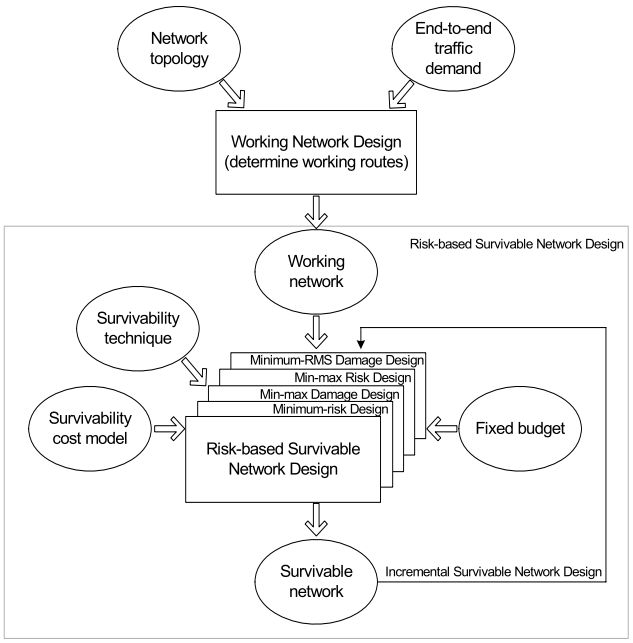

Fig. 1 Risk based Resilient Network Design Procedure

not (included in the current formulation) permissible in this study but it is relatively straightforward to extend the formulation to study this case.

Note that the design approach can be applied in a sequential fashion to improve the network resilience based on a sequence of budgets as detailed in [13]. The notation adopted in the paper is summarized in Table 1 for the link protection case, with additional variables for the path protection case given in the text.

3 Resilient network design based on risk

In this section we present the risk based design model formulations. We start with the basic minimum risk survivable network design which aims at minimizing the total network risk, or equivalently the expected damage across all network states. This is followed by the other risk based design objective formulations, presented as extensions to the minimum risk design.

3.1 Minimum risk survivable network design

The minimum risk survivable network design can be formulated as an Integer Programming (InP) optimization problem for both the link protection and path protection cases. The formulation is based on a link-path model (also known as an arc-flow model [3, 13, 14]), which requires a set of precomputed routes as candidate backup routes for each backup path. The InP formulation for the minimum risk link protection design is presented as Problem (P1) below.

The decision variables are the binary variables bp_i, which determine a set of network 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 determine the backup routes for protected links where $f_i^q = 1$ if link i is protected and uses the qth route in the backup route set Q_i for its backup path, and $f_i^q = 0$ otherwise. The design objective in (5) is to minimize the total network risk. Constraint set (6) 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 (7)–(10) are the failure state relationships, which determine whether or not end-to-end connection r fails in network state s, taking into account the link protection to be deployed in the network. More specifically, constraint set (7) 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 link failure 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., 1-$bp_i = 1$). Constraint set (8) 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 (9) indicates that connection 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 (10) connects variable $y_{s,r}$ to binary variable $z_{s,r}$ so that $z_{s,r} = 1$ if $y_{s,r} > 0$, and $z_{s,r} = 0$ otherwise. Constraint set (11) calculates the amount of damage for each network state as the sum of damages associated with all failed connections in that network state. Constraint set (12) calculates the total network risk as the sum of the product of the state damage and the state probability for all network states. Constraint (13) 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 qth eligible backup route for link i in the set Q_i includes link j, and $\delta_{i,j}^q = 0$ otherwise. Lastly, constraint sets (14) and (15) express the binary nature of the design and failure variables.

Problem (P1) Minimum risk link protection design problem

$$\min_{bp_i, f_i^q} \; Netrisk \tag{5}$$

$$\sum_{q \in Q_i} f_i^q = bp_i, \quad \forall i \in L \tag{6}$$

$$h_{s,i} = \sum_{q \in Q_i} f_i^q \zeta_{s,i}^q + 1 - bp_i, \quad s \in S,\ i \in L \tag{7}$$

$$e_{s,i} = state_{s,i} h_{s,i}, \quad s \in S,\ i \in L \tag{8}$$

$$y_{s,r} = \sum_{i \in L} e_{s,i}\, p_{r,i}, \quad s \in S,\ r \in R \tag{9}$$

Table 1 Notation

N, L, R, S	Set of nodes, links or cables, lightpaths, and 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
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
$\boldsymbol{STATE} = \{state_{s,i}\}_{\|S\|\times\|L\|}$	$state_{s,i} = 1$ 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
dam_r	Damage caused by a failure of lightpath r
$damage_s$	Damage occurring in network state s
c_i	The unit cost of spare capacity on link i
$budget$	The budget
K	A large constant used for bounding
$risk_s$	Amount of risk associated with network state s
$Netrisk$	Total risk to the network
$g_{s,r}$	$g_{s,r} > 0$ if a working path for lightpath r fails 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
$z_{s,r}$	$z_{s,r} = 1$ if lightpath r fails in network state s, and $= 0$ otherwise
$\mathbf{1}_{M\times N}$	An $M \times N$ matrix with only elements "1"
TI	Time Interval over which risk/damage assessed (e.g. 31,536,000 sec/year)
$\boldsymbol{bp} = \{bp_i\}_{\|L\|}$	$bp_i = 1$ 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
$h_{s,i}$	$h_{s,i} > 0$ 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
Q_i	Set of eligible backup routes for link i
$\delta^q_{i,j}$	$\delta^q_{i,j} = 1$ if the qth eligible backup route for link i in the set Q_i includes link j, and $= 0$ otherwise
$\zeta^q_{s,i}$	$\zeta^q_{s,i} = 1$ if the qth backup route for link i in the set Q_i fails in network state s, and $= 0$ otherwise
f^q_i	$f^q_i = 1$ if link i is protected and uses the qth route in the backup route set Q_i for its backup path, and $= 0$ otherwise

$$z_{s,r} K \geq y_{s,r}, \quad s \in S, r \in R \tag{10}$$

$$damage_s = \sum_{r\in R} z_{s,r} dam_r, \quad \forall s \in S \tag{11}$$

$$Netrisk = \sum_{s\in S} stateprob_s \times damage_s \tag{12}$$

$$\sum_{i\in L}\sum_{q\in Q_i}\sum_{j\in L} c_j w_i f^q_i \delta^q_{i,j} \leq budget \tag{13}$$

$$bp_i, f^q_i : binary, \quad \forall i \in L, \ \forall q \in Q_i \tag{14}$$

$$z_{s,r} : binary, \quad \forall s \in S, \ \forall r \in R \tag{15}$$

For the path protection case, the minimum-risk survivable network design formulation (P2) is presented in (16)–(25). The set of decision variables are binary variables bp_r, which determine a set of end-to-end connections to be protected, where $bp_r = 1$ if connection r is protected and $bp_r = 0$ otherwise, and the binary variables f_r^q, which determine the backup routes for protected connections, where $f_r^q = 1$ if connection r is protected and uses the qth route in the backup route set Q_r for its backup path, and $= 0$ otherwise. The objective (16) is to minimize the total network risk. Constraint set (17) indicates that if connection r is protected, there must exist one backup path, whose route is selected from a set of eligible backup routes Q_r. Constraints (18)–(20) are the failure state relationships which determine whether or not connection r will fail in network state s, taking into account path protection to be deployed in the network. More specifically, constraint set (18) determines whether or not the backup path for connection r is available in network state s. The backup path for connection 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 link failure in that network state (i.e., $\sum_{q \in Q_r} f_r^q \zeta_{s,r}^q = 1$), or connection r is not protected (i.e., $bp_r = 0$, or 1-$bp_r = 1$). Constraint set (19) indicates that end-to-end connection 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 (20) relates variable $y_{s,r}$ to binary variable $z_{s,r}$ (i.e., $z_{s,r} = 1$ if $y_{s,r} > 0$, and $z_{s,r} = 0$ otherwise). Constraints (21)–(22) are for the calculation of the risk as in (4). Constraint (23) is the budget constraint which limits the total capacity investment on the end-to-end backup paths. Lastly, constraints (24) and (25) express the binary nature of the design and failure variables.

Problem (P2) Minimum risk path protection design problem

$$\min_{bp_r, f_r^q} \; Netrisk \tag{16}$$

$$\sum_{q \in Q_r} f_r^q = bp_r, \quad \forall r \in R \tag{17}$$

$$h_{s,r} = \sum_{q \in Q_r} f_r^q \zeta_{s,r}^q + 1 - bp_r, \quad s \in S,\ r \in R \tag{18}$$

$$y_{s,r} = g_{s,r} h_{s,r}, \quad s \in S,\ r \in R \tag{19}$$

$$z_{s,r} \mathrm{K} \geq y_{s,r}, \quad s \in S,\ r \in R \tag{20}$$

$$damage_s = \sum_{r \in R} z_{s,r} d_r, \quad \forall s \in S \tag{21}$$

$$Netrisk = \sum_{s \in S} stateprob_s \times damage_s \tag{22}$$

$$\sum_{r \in R} \sum_{q \in Q_r} \sum_{j \in L} c_j m_r f_r^q \delta_{r,j}^q \leq budget \tag{23}$$

$$bp_r,\ f_r^q : binary, \quad \forall r \in R,\ \forall q \in Q_r \tag{24}$$

$$z_{s,r} : binary, \quad \forall s \in S,\ \forall r \in R \tag{25}$$

The optimization Problems (P1) and (P2) are binary integer programming problems and can be solved by standard techniques such as the branch and bound method. Note that the minimum-risk survivable network design aims at minimizing the total network risk, or equivalently the expected damage across all network states. This design objective focuses only on the mean aspect of the relationship between the damage level and the failure likelihood, while ignoring other aspects of the probabilistic distribution, such as the variability of damage and failure probabilities across the network states, and the amount of damage that could occur in the network in the worst-case failure scenario. In the following subsections, alternative risk-based survivable network designs which consider different aspects of the probabilistic distribution of damage, other than the expected value, are considered.

3.2 Minimum-maximum damage survivable network design

One approach is to minimize the maximum amount of damage that could occur in the network in addition to the expected damage. This results in the objective of the design being to minimize: $k1 \times Netrisk + k2 \times maxdamage$, where *Netrisk* denotes the total network risk; *maxdamage* denotes the maximum amount of damage that could occur in the network in any failure scenario; and $k1$ 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 if $k2 = 0$, the design minimizes the total network risk. The minimum-maximum damage survivable network design can be formulated as an Integer Programming (InP) optimization Problem (P3) similar to Problem (P1) above with the modifications given below. The design objective (26) in (P3) is to minimize a linear summation of the total network risk and the maximum damage that could occur in any network state. The constraint sets (6)–(11) are taken from (P1) and serve the same purpose here. Constraint set (27) determines the maximum damage that could occur in the network. Lastly constraints (12)–(15) are taken from Problem (P1) to express the budgetary limits and the binary nature of the design variables.

Problem (P3) Min-max damage link protection design problem

$$\min_{bp_i, f_i^q} \; k1 \times Netrisk + k2 \times maxdamage \tag{26}$$

Constraints (6)–(11) from (P1)

$$maxdamage \geq damage_s, \quad \forall s \in S \tag{27}$$

Constraints (12)–(15) from (P1)

The minimum maximum damage path protection design problem can be formulated following Problem (P2) and (P3) above with the result given below as Problem (P4). The design objective (28) in (P4) is to minimize a linear summation of the total network risk and the maximum damage that could occur in any network state. The constraint sets (17)–(21) are taken from (P2) and serve the same functional relationship here. Constraint set (29) determines the maximum damage that could occur in the network. Constraints (22)–(25) are taken from Problem (P2) to express the total network risk, the budget constraints and the binary nature of the design and failure variables.

Problem (P4) Min-max damage path protection design problem

$$\min_{bp_r, f_r^q} k1 \times Netrisk + k2 \times maxdamage \tag{28}$$

Constraints (17)–(21) from (P2)

$$maxdamage \geq damage_s, \quad \forall s \in S \tag{29}$$

Constraints (22)–(25) from (P2)

As in the minimum risk design case, problems (P3) and (P4) are binary integer programming problems and can be solved using the branch and bound algorithm.

3.3 Minimum-maximum risk survivable network design

The min-max damage survivable network design presented above 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). An alternative to this is to minimize 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. Thus the design objective is to minimize the function: $k1 \times Netrisk + k2 \times maxrisk$, which is a linear summation of the total risk, and the maximum risk that could occur in any network state, denoted by *maxrisk*. The terms $k1$ 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. This can be formulated as an InP Problem (P5) which is similar to (P1) above which some modifications as given below. The design objective (30) in (P5) is to minimize a linear summation of the total risk and the maximum risk that could occur in any network state. The constraint sets (6)–(11) are taken from (P1) and serve the same purpose here. Constraint sets (31)–(33) are particular to this problem and calculate the maximum risk that could occur in any network state. Lastly constraints (13)–(15) are take form Problem (P1) to express the budget limitations and the binary nature of the design variables.

Problem (P5) Min-max risk link protection design problem

$$\min_{bp_i, f_i^q} k1 \times Netrisk + k2 \times maxrisk \tag{30}$$

Constraints (6)–(11) from (P1)

$$risk_s = damage_s stateprob_s, \quad \forall s \in S \tag{31}$$

$$maxrisk \geq risk_s, \quad \forall s \in S \tag{32}$$

$$Netrisk = \sum_{s \in S} risk_s \tag{33}$$

Constraints (13)–(15) from (P1)

In a like fashion, the minimum maximum risk path protection design problem can be formulated following Problem (P2) and (P5) above with the result given below as problem (P6). The objective function (34) is the weight sum of the network risk and the maximum risk. The constraint sets (17)–(21) are taken from (P2) and serve the same function here. Constraint sets (35)–(37) are specific to this problem and determine the maximum risk that could occur in any network state. Constraints (22)–(25) are take from Problem (P2) to determine the total network risk, the limit on the budget and the binary nature of the design and failure variables.

Problem (P6) Min-max risk path protection design problem

$$\min_{bp_r, f_r^q} k1 \times Netrisk + k2 \times maxrisk \tag{34}$$

Constraints (17)–(21) from (P2)

$$risk_s = damage_s stateprob_s, \quad \forall s \in S \tag{35}$$

$$maxrisk \geq risk_s, \quad \forall s \in S \tag{36}$$

$$Netrisk = \sum_{s \in S} risk_s \tag{37}$$

Constraints (22)–(25) from (P2). Similar to problems (P1)–(P4), problems (P5) and (P6) are binary integer programming problems and can be solved using the branch and bound algorithm.

3.4 Minimum-RMS damage survivable network design

In contrast to the risk based designs above, the objective of the minimum Root Mean Squared (RMS) damage design is to minimize the variability of damage across all failure scenarios. The variability of the damage is measured by the square root of the expected damage-squared value across all network states as calculated in (38). By squaring the damage value of each network state, the values in the network states with higher damage levels are increased to a greater extent than the values in the network states with lower damage levels. Hence, this objective function encourages the design to protect against failures with higher damage levels as compared to the minimum risk design.

$$\text{RMS of } damage = \sqrt{\sum_{s \in S} stateprob_s \times damage_s^2} \tag{38}$$

The amount of damage in each network state is a function of design variables (i.e., which links/end-to-end connections to protect, and the routes of all backup paths), therefore the RMS of the damage is non-linear. Since the objective function of the minimum RMS damage design is non-linear, the design problem cannot be solved using a straightforward InP approach. Here, a simple iterative greedy heuristic algorithm is proposed for solving the design problem for both link and path protection. A flow chart of the heuristic is shown in Fig. 2. Given a working network topology, a pre-computed set of possible backup routes and a fixed budget, the algorithm finds a feasible initial solution as follows. First the cost of each possible backup route is computed. Then for each link/end-to-end lightpath with backup routes whose cost is less than the budget, the amount of reduction in the RMS-damage of using a backup path to protect the link/lightpath is computed. The link whose ratio of RMS-damage reduction/backup path cost is largest is selected for implementing link protection. The process repeats until no more links can be protected due to the budget limit, or all the links have been protected. Since the result from the initial solution might not be an optimal, an iterative process is used to improve the solution. The iterative step is based on the idea that it may be possible to improve the current solution by randomly removing the protection from a protected link/lightpath in the current solution, followed by updating the budget, and then choosing to protect other unprotected links/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.

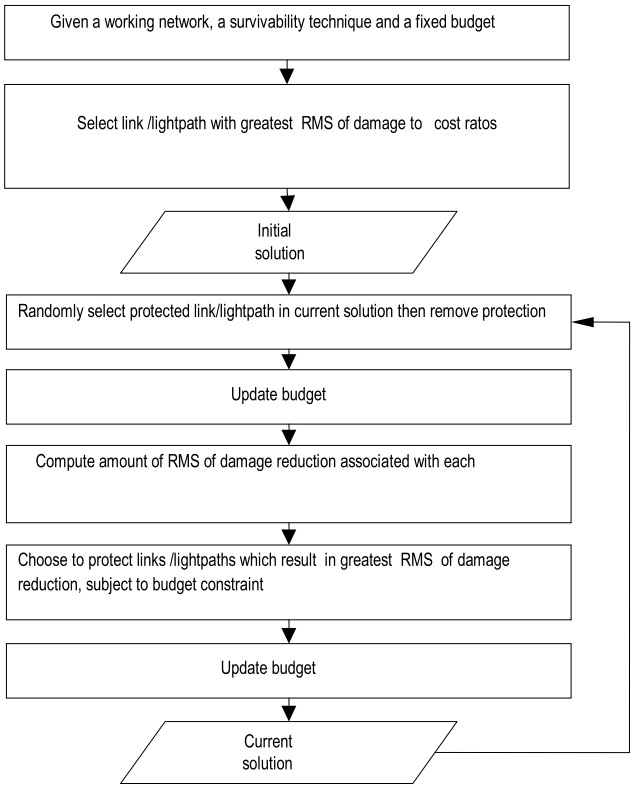

Fig. 2 Flowchart of greedy heuristic for Minimum RMS damage design

4 Numerical results

This section presents numerical results and analysis of the proposed risk based resilient network designs. The numerical experiments were carried out in the context of an Optical Transport Network (OTN). An OTN consists of Optical Cross Connects (OXCs) interconnected by WDM optical fiber links organized in a mesh topology. An end-to-end connection between a source and a destination OXC is called a lightpath. A lightpath occupies a wavelength on each optical fiber link that it traverses. Figure 3 shows the network topology used in the experiments. The cable lengths in kilometers are given next to each link in the figure, along with the Cable Cut (CC) metric in parentheses. The CC is the average cable length in kilometers that results in a single cable cut per year and is used to determine the unavailability of the links as in [3, 16]. All the cables have the same Mean Time To Repair (MTTR) of 24 hours. A full mesh of lightpath demands between all node pairs is 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/1000 km. In addition, it is assumed that each OXC has full wavelength conversion capability, so that the wavelength continuity constraint can be ignored.

In the risk calculation, the damage is measured as the traffic loss rate resulting from failed lightpaths. Also, we consider only the network states with at most two simultaneous failures, rather than all possible states. This significantly reduces the number of states considered from $2^{|L|}$ to $1 + |L|(|L| + 1)/2$, but still gives a close approximation of the overall risk, since most of the probability mass is in the network states with a small number of simultaneous failures. [11, 15, 16].

In the experiments, the minimum risk, minimum-maximum damage and minimum-maximum risk design InP models of Sect. 3 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 possible backup routes. Whereas the minimum-RMS damage design problems were solved using the heuristic algorithm explained in Sect. 3 with the same set of pre-computed backup routes used in the InP models. Numerical results are shown only for a few budget values with additional results given in [13, 14].

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 network risk; and the min-max risk design puts a higher priority on minimizing the maximum risk than minimizing the total network risk.

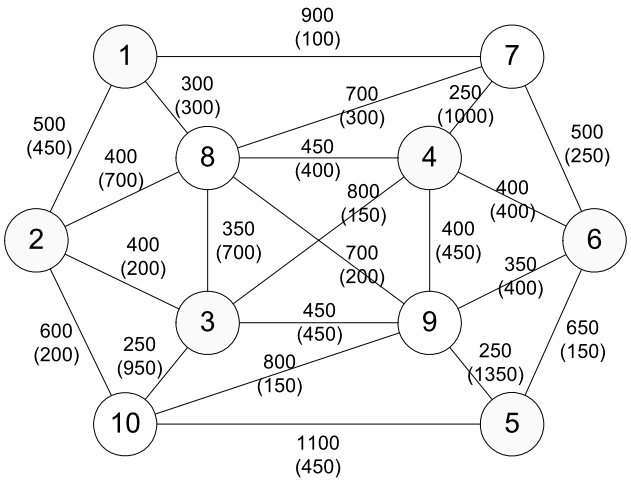

Fig. 3 Network ($|N| = 10$, $|L| = 22$) with cable length (km) and Cable Cut (CC) metric within parentheses

Comparisons are made based on the following measures: the probability of no damage which is the probability that the network is in states that have a zero-damage level taking into account the protection deployed in the network, the total network risk, the maximum damage, the maximum risk, the RMS of damage, the standard deviation of damage and lastly the probability distribution of damage.

Table 2 shows typical results for each design scheme using *link protecti*on. Table 2 is for the case of maximum budget of 30 units which is approximately 50% of the minimum cost required to protect every link in the network. From the table, one can see that the min-max risk design has the largest probability of no damage. However, the difference with the other schemes is small $<1.25\%$). As expected the minimum-risk design has the smallest total risk level. Whereas, the min-max risk design and the minimum-RMS damage design have comparable total risk levels. The min-max damage design, results in the highest total risk level, much larger than the other designs. This is understandable because the min-max damage design 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. In terms 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, with all other designs resulting in similar maximum damage levels. Comparing the different designs in term of the maximum risk that could occur, the results show that the min-max risk design provides the lowest maximum risk level. Notice that both the minimum risk design and the min-max damage design results in the highest maximum risk level. Lastly, we

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

Metric	Design's objective function			
	Min risk	Min-max damage	Min-max risk	Min RMS damage
Probability of no damage	0.9819 (+1.22%)	0.9765 (+.66%)	0.9701 (0%)	0.9762 (+.63%)
Total network 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 + Std. of damage	4,791.84 (+1.96%)	5,417.97 (+15.29%)	4,815.53 (+2.47%)	4,699.50 (0%)

compare the different risk-based designs in terms of the variability of damage that could occur in the network. 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:

$$\sqrt{\sum_{s\in S: damage_s > expected\ damage\ value} stateprob_s (damage_s - expected\ damage\ value)^2}$$

where only the network states with the damage level greater than the expected damage value are included in the calculation. The Table 2 results show that, among the risk-based designs considered, the minimum-RMS damage design yields the lowest RMS value and the smallest one-side Std. of damage. The min-max risk design yields a lower RMS value of damage, and lower Std. of damage than the minimum- network risk design. Notice that the min-max risk design has variability metrics that are close to minimum-RMS. Whereas, the min-max damage design results in the highest values for both RMS of damage and Std. of damage.

We also compare the 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 both the expected value and the variability of damage above the expected value. This is a common approach for comparing different investments in the financial industry (i.e., expected value and 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. The results in Table 2 show that the minimum-RMS damage design has the smallest value.

The probability distribution of damage in the network is shown in Fig. 4. The probability distribution of damage with no protection deployed is shown in Fig. 4(a). In addition, the four different risk-based designs for a budget of 30 units are presented in Fig. 4(b)–(e). These damage distribution plots in Fig. 4 show how the different risk-based designs reduce the failure probability associated with each damage levels from the initial values in Fig. 4(a). The results show the advantage of the minimum-RMS damage design (Fig. 4(e)) 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. For example, 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).

Table 3 shows representative results for each design scheme using path protection. Table 3 is for the case of maximum budget of 30 units, which is about 75% of the minimum cost required for protecting all the lightpaths in the network. Note that as discussed in the literature [3–6] path protection needs a smaller cost to protect all lightpaths

Table 3 Comparison of different risk-based path protection designs for a budget of 30 units

Metric	Design's objective function			
	Min risk	Min-max damage	Min-max risk	Min RMS damage
Probability of no damage	0.9782 (+8.86%)	0.8986 (0%)	0.9781 (+8.85%)	0.9633 (+7.2%)
Total network 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)	2,662.6 (+6.99%)	3,585.82 (+44.08%)	2,769.15 (+11.27%)	2,488.7 (0%)
Expected + Std. of damage	3,029.96 (+3.18%)	4,749.43 (+61.73%)	3,147.33 (+7.18%)	2,936.56 (0%)

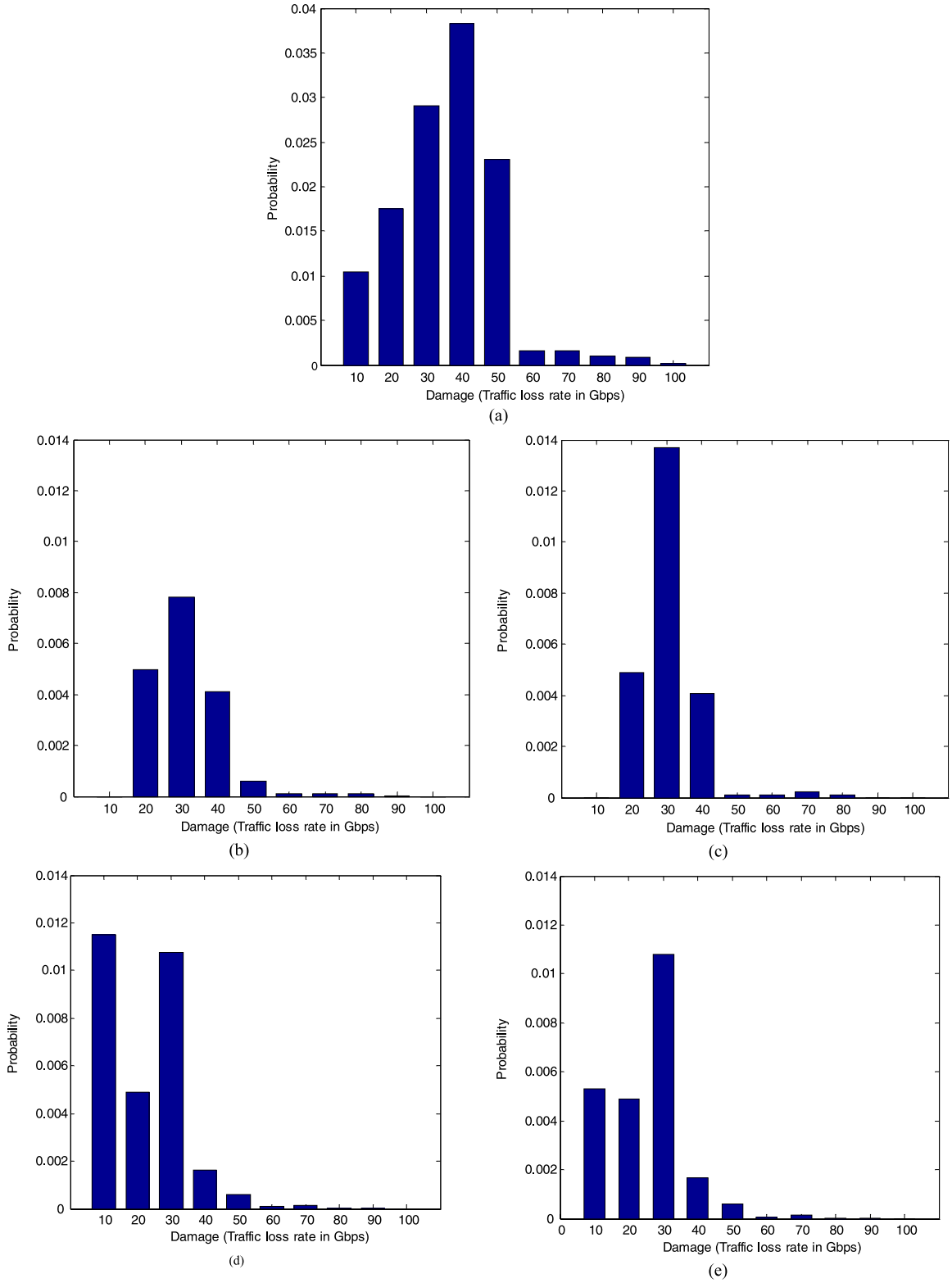

Fig. 4 Probability distribution of damage with (**a**) no protection deployed, (**b**) minimum-risk design, (**c**) min-max damage design, (**d**) min-max risk design, and (**e**) minimum-RMS damage design

then link protection to protect all links. In the table, one can see that the min-max damage has the smallest probability of no damage which is unlike the link protection case.

In terms of the total risk, the minimum risk design has the smallest value with the min-max risk design yielding a relatively close value. As in the link protection case the min-max damage design, results in the highest total risk level, much larger than the other designs. This is because the min-max damage design minimizes the maximum damage level, protecting the network against failure scenarios which have high damage levels but a small probability of occurring, which results in a small risk reduction. Here, the min-max damage design guards against some dual failure scenarios, which results in the backup paths taking long routes, therefore requiring a higher spare capacity cost.

Next, we compare the different 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 Table 3, the min-max damage design results in a maximum damage of 40 Gbps, whereas other designs result in maximum damage levels of 60–70 Gbps. The results are similar in the link protection case of Table 2.

Considering the maximum risk, that could occur in any network state, the results in Table 3 show the min-max risk design has the lowest maximum risk. The min-max damage design results in the highest maximum risk level, which is significantly larger than the smallest maximum risk level and the maximum risk levels from other designs.

Comparing the designs based on the variability of damage that could occur in the network. The results in Table 3 show that the minimum-RMS damage design yields the lowest RMS value of damage, and the lowest one-side Std. of damage. This is expected since the minimum-RMS design seeks to reduce the variability of the damage in the design objective. Note, that the minimum risk design yields the next smallest variability values. 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.

Considering the designs based on the summation of the expected damage and the standard deviation of the damage in Table 3, one can see that the minimum-RMS design has the lowest value just as in the link protection case. Based on the results in Tables 2 and 3, 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.

5 Conclusions

In this paper, we developed a new approach to resilient network design based on managing the risk. Four risk management based approaches for survivable network design were proposed. Specifically, we present minimum risk, minimum-maximum damage, minimum-maximum risk and minimum-RMS damage survivable network design models. Numerical results for a sample network show that all approaches can reduce the risk from the initial value. The numerical comparisons show the advantage of the minimum-RMS damage design over other the design alternatives in that it only slightly increases the average network risk while greatly reducing the variability in the damage.

References

1. Lewis, T. (2006). *Critical infrastructure protection in homeland security*. New York: Wiley-Interscience.
2. Department of Homeland Security (2009). National infrastructure protection plan. USA Government Printing Office. Available online at http://www.dhs.gov.
3. Grover, W. D. (2003). *Mesh-based survivable networks: options and strategies for optical, MPLS, and ATM networking*. Englewood Cliffs: Prentice Hall PTR.
4. Pioro, M., & Medhi, D. (2004). *Routing, flow, and capacity design in communication and computer network*. San Francisco: Morgan Kauffman.
5. Vasseur, J.-P., Pickavet, M., & Demeester, P. (2004). *Network recovery: protection and restoration of optical, SONET-SDH, IP, and MPLS*. San Mateo: Morgan Kaufmann.
6. Mouftah, H., & Ho, P.-H. (2003). *Optical networks: architecture and survivability*. Norwell: Kluwer Academic.
7. Neumayer, S., Zussman, G., Cohen, R., & Modiano, E. (2009). Assessing the vulnerability of the fiber infrastructure to disasters. In *Proceedings of IEEE Infocom 2009*, Rio de Janeiro, Brazil, 19–25 April.
8. González, M., Andrés, J., Helvik, B., Hellan, J., & Kuusele, P. (2010). Analysis of dependencies between failures in the UNINETT IP backbone network. In *IEEE 16th Pacific Rim international symposium on dependable computing [PRDC2010]*, December.
9. Department of Homeland Security (2010). *Communications sector specific plan*. USA Government Printing Office. Available online at http://www.dhs.gov.
10. Department of Homeland Security (2010). *Information technology sector specific plan. USA Government Printing Office*. Available on-line at http://www.dhs.gov.
11. Ayyub, B. M. (2003). *Risk analysis in engineering and economics*. London: Chapman and Hall/CRC Press.
12. Aven, T. (2003). *Foundations of risk analysis: a knowledge and decision-oriented perspective*. New York: Wiley.
13. Vajanapoom, K. (2008). *Risk-based survivable network design*. Ph.D. dissertation, School of Information Sciences, University of Pittsburgh.

14. Vajanapoom, K., & Tipper, D. (2007). Risk based incremental survivable network design. In *Sixth international workshop on design of reliable communication networks (DRCN)*, 7–10 October.
15. Clouqueur, M., & Grover, W. D. (2005). Mesh restorable networks with enhanced dual failure restorability properties. *Photonic Network Communications*, *9*(1), 7–18.
16. Clouqueur, M., & Grover, W. D. (2002). Availability analysis of span restorable mesh networks. *IEEE Journal on Selected Areas in Communications*, *20*(4), 810–821.

Korn Vajanapoom graduated with a B.E. in Electrical Engineering from Chulalongkorn University, a M.S. Telecommunications from the University of Maryland, and a Ph.D. in Telecommunications from the University of Pittsburgh. Currently Dr. Vajanapoom is a Senior Consultant at Samart Comtech, Bangkok, Thailand.
His research interests are wired and wireless network design.

David Tipper is an Associate Professor and Director of the Graduate Telecommunications and Networking Program at the University of Pittsburgh. He is a graduate of the University of Arizona (Ph.D. E.E., M.S.S.I.E.) and Virginia Tech (B.S.E.E.). His current research focuses on network design, energy efficiency, information assurance techniques, time varying network performance analysis and control.

Sira Akavipat received the B.E. degree in Electrical Engineering from Chulalongkorn University, Thailand, in 2003, and the M.S. degree in Telecommunications from the University of Pittsburgh, Pittsburgh, PA, in 2008. He is currently working toward the Ph.D. degree in Telecommunications at the University of Pittsburgh. From 2003 to 2006, he was an engineer at Department of Network Planning, TOT Public Company Limited, Bangkok, Thailand. His research interests include incremental survivable network design, multi-layer network survivability and energy savings in cellular network.