A Risk Management Approach to Resilient Network Design

Korn Vajananopoom, David Tipper, and Sira Akavipat
Graduate Telecommunications and Networking Program
University of Pittsburgh, Pittsburgh, PA 15260 USA
Email:korn.v@samtel.samartcorp.com, tipper@tele.pitt.edu, sia10@pitt.edu

Abstract—This paper considers the problem of where a survivability technique should be deployed in a network based on managing risk given a limited financial budget. We formulate three novel risk management resilient network design techniques: (1) minimize the maximum damage that could occur in the network, (2) minimize the maximum risk in the network and (3) minimize the root mean squared damage. The first two approaches try to minimize the damage/risk from the worst case failure scenario, whereas the third technique minimizes the variability of damage across all failure scenarios. Numerical results for a sample network show the tradeoffs among the schemes.

I. INTRODUCTION

Communication networks are part of the critical infrastructure upon which society depends. Recognition of this has led to a body of work on designing survivable networks with a focus on wired backbone networks [1-3]. 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, etc.), a network is designed to survive a set of predefined failures, (e.g., all single link failures), with minimum cost [1-3]. 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 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). Even in a situation where network operators have sufficient monetary resources to protect the networks against a set of failures, they may prefer to reduce their capital expenditures by choosing to protect only some parts of the network based on a cost-benefit analysis. Another limitation of the minimum-cost design approach is that it treats all failures equally without considering the variability in failure impacts and likelihood of failures. However, it has been noted that failure/attack rates and repair rates are geographically correlated [4,5] 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.

Due to the limitations of the minimum cost design approach, we proposed a risk-based approach to survivable network design in [6] where the minimum risk survivable design optimization problem for a network using link protection was given. Note that minimum risk-based design focuses on minimizing the average risk. In other 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 three novel risk management resilient network design techniques using link protection to provide survivability. The first approach minimizes a linear combination of the network risk and the maximum damage from the worst case failure scenario. The second technique minimizes a linear combination of the 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.

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

II. A RISK BASED APPROACH

The risk-based design approach is based on integrating 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 [7].

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. As noted above, different geographic parts of the network have different risk levels. For example, the rate of cable cuts per km of cable and the Mean Time To Repair (MTTR) of network components in the United States show variations depending on the geographic location. Furthermore, network failures result in different levels of damage depending on the type of traffic carried. For instance, 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. These factors can be incorporated into a risk metric as discussed below. The notation used in the paper is summarized in Table I.

**TABLE I**

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N, L, R, S$</td>
<td>Set of nodes, links or cables, lightpaths, and network states</td>
</tr>
<tr>
<td>$P = {p_{ri}}_{i \times i}$</td>
<td>$p_{ri} = 1$ if lightpath $r$ uses link $i$ in its working path, and $= 0$ otherwise</td>
</tr>
<tr>
<td>$m = {m_{ri}}_{i \times i}$</td>
<td>$m_{ri}$ is the data rate (bits/s) of lightpath $r$</td>
</tr>
<tr>
<td>$u_i$</td>
<td>Amount of working capacity on link $i$, calculated by $w_i = \sum_{r \in R} p_{ri} m_{ri}$</td>
</tr>
<tr>
<td>$w_i$</td>
<td>The unit cost of spare capacity on link $i$.</td>
</tr>
<tr>
<td>$b_{si}$</td>
<td>$b_{si} = 1$ if node $s$ is the origin or destination of link $i$, and $= 0$ otherwise</td>
</tr>
<tr>
<td>$d_{si}$</td>
<td>$d_{si} = 1$ if node $s$ is the source or destination of lightpath $r$, and $= 0$ otherwise</td>
</tr>
<tr>
<td>$STATE = {state_{ij}}_{i \times j}$</td>
<td>Stateprob$_{ij}$ is the probability of network state $s$</td>
</tr>
<tr>
<td>$stateprob = {stateprob_{ij}}_{i \times j}$</td>
<td>Damage caused by a failure of lightpath $r$</td>
</tr>
<tr>
<td>$dam_{r,s}$</td>
<td>Damage occurring in network state $s$</td>
</tr>
<tr>
<td>$c_i$</td>
<td>The unit cost of spare capacity on link $i$.</td>
</tr>
<tr>
<td>$K$</td>
<td>A large constant used for bounding</td>
</tr>
<tr>
<td>$risk_s$</td>
<td>Amount of risk associated with network state $s$</td>
</tr>
<tr>
<td>$Netrisk$</td>
<td>Total risk to the network</td>
</tr>
<tr>
<td>$g_{r,s}$</td>
<td>$g_{r,s} &gt; 0$ if a working path for lightpath $r$ fails in network state $s$, and $= 0$ otherwise</td>
</tr>
<tr>
<td>$y_{r,s}$</td>
<td>$y_{r,s} &gt; 0$ if lightpath $r$ fails in network state $s$, and $= 0$ otherwise</td>
</tr>
<tr>
<td>$z_{r,s}$</td>
<td>$z_{r,s} = 1$ if lightpath $r$ fails in network state $s$, and $= 0$ otherwise</td>
</tr>
<tr>
<td>$I_M \times N$</td>
<td>An $M \times N$ matrix with only elements “1”</td>
</tr>
<tr>
<td>$T_i$</td>
<td>Time Interval over which risk/damage is assessed (e.g., 31,536,000 sec/year)</td>
</tr>
<tr>
<td>$bp = {bp_{ij}}_{i \times j}$</td>
<td>$bp_{ij} = 1$ if link $i$ is protected, and $= 0$ otherwise</td>
</tr>
<tr>
<td>$Q = {Q_{ij}}_{i \times j}$</td>
<td>$Q_{ij}$ is the probability of network state $s$</td>
</tr>
<tr>
<td>$h_{ij}$</td>
<td>$h_{ij} &gt; 0$ 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</td>
</tr>
<tr>
<td>$e_{ij}$</td>
<td>$e_{ij} &gt; 0$ if link $i$ fails (both working link fails and backup path is not available) in network state $s$, and $= 0$ otherwise</td>
</tr>
<tr>
<td>$Q_{ij}$</td>
<td>Set of eligible backup routes for link $i$</td>
</tr>
<tr>
<td>$\delta_{ij}^{q}$</td>
<td>$\delta_{ij}^{q} = 1$ if the $q$th eligible backup route for link $i$</td>
</tr>
<tr>
<td>$\xi_{ij}^{q}$</td>
<td>$\xi_{ij}^{q} = 1$ if the $q$th backup route for link $i$</td>
</tr>
<tr>
<td>$\zeta_{s,j}^{q}$</td>
<td>$\zeta_{s,j}^{q} = 1$ if $Q_{ij}$ fails in network state $s$, and $= 0$ otherwise</td>
</tr>
<tr>
<td>$f_{i}^{q}$</td>
<td>Route in the backup route set $Q_{ij}$ for its backup path, and $= 0$ otherwise</td>
</tr>
</tbody>
</table>

The risk of failure is defined as the probability of failure times the damage from failure [7]; 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).

$$risk_s = stateprob_s \times damage_s$$ (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.

$$Netrisk = \sum_{s \in S} stateprob_s \times damage_s$$ (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$_{ij}$ represents the network failure states, where state$_{ij} = 1$ if link $i$ fails in network state $s$, and state$_{ij} = 0$ otherwise; and $u_i$ denotes the unavailability of cable $i$.

$$stateprob_{ij} = \prod_{i \in L} u_i \text{state}_{ij} (1 - u_i)^{1 - \text{state}_{ij}}$$ (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 $dam_{r,s}$ is the amount of damage caused by a failure of connection $r$.

$$Netrisk = \sum_{s \in S} stateprob_s (\sum_{r \in \text{all failed connections}} dam_{r,s})$$ (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., $dam_{r,s} = m_r$).

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. Various techniques for
reducing the risk of failures in communication networks exist (e.g., p-cycles, 1+1 protection, etc). In this paper, we utilize the link protection scheme [1]. 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 the design procedure used here, an assumption is that the survivability cost is considered only in terms 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 not included in the current formulation but it is relatively straightforward to extend the formulation to study this case.

III. RESILIENT NETWORK DESIGN BASED ON RISK

Minimum risk survivable network design [6,8] aims at minimizing the total network risk, or equivalently the expected damage across all network states. However, if the amount of damage in each network state is not properly considered, the maximum damage that occurs in the network might be unacceptable to network operators or society. Therefore, we consider alternative risk related design objectives.

A. 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 (IP) optimization problem. The formulation is based on a link-path model (also known as an arc-flow model [1,2]), which requires a set of pre-computed routes as candidate backup routes for each backup path. The IP formulation for the min-max damage link protection design is presented as problem (P1) below.

The decision variables are the binary variables \( bpi \), which determine a set of network links to be protected, where \( bpi = 1 \) if link \( i \) is protected and \( bpi = 0 \) otherwise, and the binary variables \( fqi \) which determine the backup routes for protected links where \( fqi = 1 \) if link \( i \) is protected and uses the \( q^{th} \) route in the backup route set \( Q \), for its backup path, and \( fqi = 0 \) otherwise. The design objective in (5) is to minimize a linear summation of the expected network risk and the maximum damage that could occur.

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 \( Q \). 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., \( h_{si} = 1 \) for two reasons: either the backup path exists but fails due to a link failure in that network state (i.e., \( \sum fqi q^q s,i = 1 \)), or link \( i \) is not protected (i.e., \( 1-bpi = 1 \)).

Constraint set (8) indicates that link \( i \) fails in network state \( s \) (i.e., \( e_{si} = 1 \) if and only if both the working link fails (i.e., \( state_{si} = 1 \) and its backup path is not available (i.e., \( h_{si} = 1 \) in that network state. Constraint set (9) indicates that connection \( r \) fails in network state \( s \) (\( y_{sr} > 0 \)) if and only if at least one of the links that it traverses fails (i.e., \( \sum e_{si} p_{ri} > 0 \)). Constraint set (10) connects variable \( y_{sr} \) to binary variable \( z_{sr} \), so that \( z_{sr} = 1 \) if \( y_{sr} > 0 \), and \( z_{sr} = 0 \) 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) determines a maximum spare capacity investment. The spare capacity on link \( i \) and parameter \( \delta_{ij} = 1 \) if the q^{th} eligible backup route for link \( i \) in the set \( Q \) includes link \( j \), and \( \delta_{ij} = 0 \) otherwise. Lastly, constraint sets (15) and (16) express the binary nature of the design and failure variables.

(P1) Min-max damage link protection design problem

\[
\min k1 \times Netrisk + k2 \times maxdamage
\]

\[
\sum fqi = bpi, \quad \forall i \in L
\]

\[
h_{si} = \sum fqi q^q s,i + 1-bpi, \quad s \in S, i \in L
\]

\[
e_{si} = state_{si} h_{si}, \quad s \in S, i \in L
\]

\[
y_{sr} = \sum e_{si} p_{ri}, \quad s \in S, r \in R
\]

\[
z_{sr} K \geq y_{sr}, \quad s \in S, r \in R
\]

\[
damage_{s} = \sum z_{sr} damage, \quad \forall s \in S
\]
The optimization problem (P1) is a binary integer programming problem and can be solved by standard techniques such as the branch and bound method.

B. 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: \( \min \frac{k_1}{k_2} \sum_{s \in S} \text{stateprob}_s \times \text{damage}_s \), which is a linear summation of the total risk, and the maximum risk that could occur in any network state, denoted by \( \text{maxrisk} \). The terms \( k_1 \) and \( k_2 \) are design parameters. By varying the values of \( k_1 \) and \( k_2 \), different survivable network designs can be obtained. In the extreme cases, when \( k_1 = 0 \), the design is aimed at minimizing the maximum risk only, whereas when \( k_2 = 0 \), the design is aimed at minimizing the total risk. This can be formulated as an InP problem (P2) which is similar to (P1) above which some modifications as given below. The design objective (17) in (P2) 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 (18)–(20) are particular to this problem and calculate the maximum risk that could occur in any network state. Lastly constraints (14) – (16) are take form problem (P1) to express the budget limitations and the binary nature of the design variables.

\[
\text{(P2) Min-max risk link protection design problem}
\begin{align*}
\min & \quad k_1 \times \text{Netrisk} + k_2 \times \text{maxrisk} \\
\text{subject to} & \quad \text{Constraints (6) – (11) from (P1)} \\
& \quad \text{risk}_s = \text{damage}_s \times \text{stateprob}_s, \quad \forall s \in S \\
& \quad \text{maxrisk} \geq \text{risk}_s, \quad \forall s \in S \\
& \quad \text{Netrisk} = \sum_{s \in S} \text{risk}_s \\
& \quad \text{Constraints (14) – (16) from (P1)}
\end{align*}
\]

C. Minimum-RMS damage survivable network design

In the minimum-risk design approach [6], the design only focuses on minimizing the expected damage value across all failure scenarios, while ignoring how low or high the damage in each failure scenario could be, as long as the expected value is minimized. In contrast to this and the two 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, which is measured by the square root of the expected damage-squared value across all network states as calculated in (21). 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.

\[
\text{RMS of damage} = \sqrt{\sum_{s \in S} \text{stateprob}_s \times \text{damage}_s^2} \tag{21}
\]

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 this design problem. Given a working network topology, a pre-computed set of backup routes and a fixed budget, the algorithm finds a feasible initial solution as follows. First the cost of each backup route is computed. Then for each link 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 is computed. The link whose ratio of RMS-damage reduction/breakup 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 removing the protection from a protected link in the current solution, followed by updating the budget, and then choosing to protect other unprotected links 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.

IV. NUMERICAL RESULTS

This section presents the numerical results and analysis of the proposed risk-based survivable network designs. The experiments were carried out in the context of an Optical Transport Network (OTN). An OTN consists of Optical Cross Connects (OXC)s 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. Fig. 1 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 [1]. 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 10Gbps/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 $2^{k_1 + k_2}$ 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. [8-10]

In the experiments, the min-max damage and min-max risk design InP models of Section III 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 III with the same set of pre-computed backup routes used in the InP models. The numerical results are shown only for a budget value of 30 units (i.e., approximately 50% of the min cost required for protecting all the network links), additional results are in [8].

For the min-max damage design, the design parameters: $k_1=1$ and $k_2=1$, are used; whereas for the min-max risk design, the parameters: $k_1=1$ and $k_2=100$, 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.

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 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 II shows the basic results for each design scheme. One can see that the minimum-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 the 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 compare the different risk-based designs in terms of the variability of damage that could occur in the

<table>
<thead>
<tr>
<th>Metric</th>
<th>Design’s objective function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of no Damage</td>
<td>Min Risk</td>
</tr>
<tr>
<td>Total Network Risk (Mbps)</td>
<td>549.53 (0%)</td>
</tr>
<tr>
<td>Maximum Damage (Gbps)</td>
<td>90 (+12.5%)</td>
</tr>
<tr>
<td>Maximum Risk (Mbps)</td>
<td>96.26 (+19.96%)</td>
</tr>
<tr>
<td>RMS Damage (Mbps)</td>
<td>4,312.29 (+2.85%)</td>
</tr>
<tr>
<td>Std. of Damage (Mbps)</td>
<td>4,242.32 (+3.22%)</td>
</tr>
</tbody>
</table>
are presented in Fig. 2 (b)–(e). These damage distribution plots in Fig. 2 show how the different risk-based designs reduce the failure probability associated with each damage level from the initial values in Fig. 2 (a). The results show the advantage of the minimum-RMS damage design (Fig. 2 (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).

V. CONCLUSIONS

In this paper, three new risk management based approaches for survivable network design are proposed. Specifically, we present minimum-maximum damage survivable network design, minimum maximum risk survivable network design and minimum-RMS damage survivable network design. Numerical results show that all approaches can reduce failure probability associated with each damage level from the initial value. The numerical comparisons show the advantage of the minimum-RMS damage design over other design alternatives in that it slightly increases the average network risk while greatly reducing the variability.

REFERENCES