Risk Based Incremental Survivable Network Design

Korn Vajanapoom and David Tipper
Graduate Program in Telecommunications and Networking
University of Pittsburgh, Pittsburgh, PA 15260, USA
Email: kornv@mail.sis.pitt.edu, dtipper@mail.sis.pitt.edu

Abstract—**This paper presents a new approach for incremental survivable network design based on the use of risk analysis techniques. The objective of the design approach is: given a fixed budget, determine how to incrementally improve the network survivability in order to reduce the risk from network failures. Risk is defined as the product of the failure probability and the damage resulting from the failure. The design approach consists of two parts: a risk assessment and a risk reduction investment strategy. Fault tree models, which depict causal relationships among failure events in the network are used for the risk assessment. The risk-reduction investment strategy is used to determine an allocation of budget for implementing a survivability technique (e.g., link protection) in different parts of the network to minimize the network risk. Mixed Integer Linear Programming (MILP) formulations and greedy-based heuristics are proposed for solving the minimum-risk design problems. Numerical results illustrating the investment strategy for link and path protections, using an MILP approach and proposed heuristic algorithms, along with the comparisons of different capital investment alternatives on the basis of risk consideration are presented and discussed.**

I. INTRODUCTION

Communication networks are part of the critical infrastructure upon which society depends. It is thus 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. A number of survivability techniques have appeared in the literature [1]-[4], for various network technologies, such as Multi-Protocol Label Switching (MPLS) networks, ATM, SONET networks, and Wavelength Division Multiplexing (WDM) optical networks.

The basic approach for designing survivable networks in the current literature is that for a given network technology and a given survivability technique (e.g., link protection, shared backup path protection, p-cycles, etcetera), 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 [1]-[4] in different technologies with different survivability techniques. A limitation of this minimum-cost design approach comes from the hidden assumption that the sufficient monetary funds are available to protect all predefined failures. However, 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 their network in *pieces* in an *incremental* manner based on a chronological sequence of budgets. This requires a design approach, which takes budget limitations directly into consideration.

Here, we propose a different approach for survivable network design based on integrating risk analysis techniques into an incremental network design procedure with budget constraints. Risk analysis is widely used in engineering, and economics [5]-[7]. 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 [5]. 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. 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 an order of magnitude 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 or entertainment traffic. Therefore, for a given budget, it is desirable to determine which parts of the network to apply a survivability technique so that the overall risk from network failures is minimized.

The objective of the design approach proposed here is to minimize the risk of failures to the network for a given budget. At any capital expenditure investment point the basic problem considered is given a working network and a fixed budget, how best to spend the money in order to reduce the network risk from failures. The components of the design approach are a risk assessment and a risk-reduction 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-reduction investment strategy is used to determine how to allocate a fixed budget for implementing a survivability technique in different parts of the network to minimize the overall network risk. In this work, we consider two standard survivability techniques: dedicated-backup link protection and dedicated-backup path protection. For each survivability technique, the risk reduction investment strategy is formulated as a Mixed Integer Linear Programming (MILP) optimization problem. Due to the complexity of solving MILPs we propose a set of greedy heuristic solution algorithms for the optimization problems. Numerical results illustrating our approach and evaluating the quality of the heuristics are given. In this paper, 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 network technologies and other failure/attack conditions.

The remainder of this paper is organized as follows: Section II presents our proposed risk-based survivable network design approach. The risk assessment procedure is presented in Section II.A, and the risk-reduction investment strategy is presented in Section II.B. Section III presents the extension to incremental survivable network design. Section IV presents and discusses the numerical results and lastly Section V summarizes the paper and our conclusions.

II. RISK BASED SURVIVABLE NETWORK DESIGN

As noted above, our risk based survivable network design approach has two components namely: a risk assessment and a risk-reduction investment strategy. We discuss each in turn below. Note, that the two components are interrelated since an achievement of the investment's goal, i.e., minimizing the network risk, is checked by the risk calculation process considered in the risk assessment. The notation used in this paper is presented in Table I.

A. Risk Assessment

We define the risk of failure i as the probability of failure i times the damage from failure $i.$ The network risk of all failures can then be calculated as a sum of risks of all individual failures. Let F denote the set of failures considered. Then the risk can be determined as

$$Risk = \sum_{i \in F} \text{probability of failure}_i \times \text{damage from failure}_i \, . \qquad (1)$$

In order to quantify the risk one needs to measure the two quantities associated with the risk: the probability of failures and the damages resulting from the failures. Here we utilize a fault tree and truth table approach to evaluate the failure probabilities of interest. We illustrate our approach within 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 destination OXC in WDM networks is called a lightpath (LP). A lightpath occupies a wavelength on each optical fiber link that it traverses. We assume that each OXC has a full wavelength conversion capability. The potential failures of network components, (e.g., fiber cuts, OXC failures, etc.) pose a risk to the network. The magnitude of risk that these failures pose to the network can be evaluated by (1). Here the set of failure events considered F are lightpath failures in the network due to fiber cuts. Thus, the probability of failure event i is the probability of lightpath failure, or the lightpath unavailability. The damage in this case is simply the damage resulting from the lightpath failure, which can be measured in many different ways. If knowledge of the higher layer traffic is available, one can construct a damage metric that incorporates the societal effects of the loss of various traffics. For example a higher damage value would be place on emergency communications and SCADA for critical infrastructures. Here we use a simple damage measure, namely, the data rate of the failed lightpath. Therefore, the risk to the WDM network can be calculated as in (2), where R is a set of all lightpaths in the network, ulp_r is the unavailability of lightpath r, and m_r is the data rate of lightpath r.

TABLE I
NOTATION

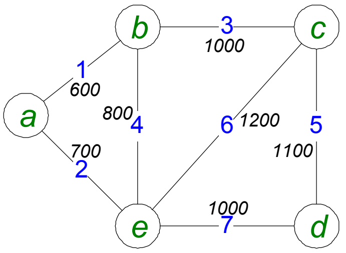
N, R, S	A set of nodes, lightpaths, and network states respectively
L	A set of links or cables
F	A set of failures considered
$\boldsymbol{P} = \{p_{rl}\}_{\lvert R\rvert \times \lvert L\rvert}$	$p_{r,l}$= 1 if lightpath r uses link l in its working path, and = 0 otherwise
$\boldsymbol{m} = \{m_r\}_{\lvert R\rvert}$	m_r is a data rate (bits/s) of lightpath r
$\boldsymbol{B} = \{b_{nl}\}_{\lvert N\rvert \times \lvert L\rvert}$	b_{nl} = 1 if node n is an origin or destination of link l, and = 0 otherwise
$\boldsymbol{D} = \{d_{rn}\}_{\lvert R\rvert \times \lvert N\rvert}$	d_{rn} = 1 if node n is a source or destination of lightpath r, and = 0 otherwise
u_l	Unavailability of cable l
$\boldsymbol{STATE} = \{state_{sl}\}_{\lvert S\rvert \times \lvert L\rvert}$	$state_{sl}$ = 1 if cable l is cut under network state s, and = 0 otherwise
$\boldsymbol{stateprob} = \{stateprob_s\}_{\lvert S\rvert}$	$stateprob_s$ probability of network state s
$\boldsymbol{1}_{\mathrm{M} \times \mathrm{N}}$	An M × N matrix with only elements "1"
w_l	Amount of working capacity on link l, calculated by $w_l = \sum_{r \in R} p_{rl} m_r$
y_{sr}	$y_{sr} > 0$ if lightpath r fails under network state s, and = 0 otherwise
z_{sr}	z_{sr} = 1 if lightpath r fails under network state s, and = 0 otherwise
ulp_r	Unavailability of lightpath r
c_l	The unit cost of spare capacity on link l
budget	The budget
K	A sufficiently large number used for bounding
TY	The amount of time per year (i.e., 31,536,000 s)
The following notation is used in the link protection case only:	
$\boldsymbol{bp} = \{bp_i\}_{\lvert L\rvert}$	bp_i = 1 if link i is protected, and = 0 otherwise
$\boldsymbol{Q} = \{q_{ij}\}_{\lvert L\rvert \times \lvert L\rvert}$	q_{ij} = 1 if link i is protected and its backup path traverses link j, and = 0 otherwise
h_{si}	$h_{si} > 0$ if a backup path for link i is not available (either link i is not protected, or the backup path fails) under network state s, and = 0 otherwise
e_{si}	$e_{si} > 0$ if link i fails (both working link fails and backup path is not available) under network state s, and = 0 otherwise
The following notation is used in the path protection case only:	
$\boldsymbol{bp} = \{bp_r\}_{\lvert R\rvert}$	bp_r =1 if lightpath r is protected, and = 0 otherwise
$\boldsymbol{Q} = \{q_{rl}\}_{\lvert R\rvert \times \lvert L\rvert}$	q_{rl} = 1 if lightpath r is protected and its backup path traverses link l, and = 0 otherwise
h_{sr}	$h_{sr} > 0$ if a backup path for lightpath r is not available (either lightpath r is not protected, or the backup path fails) under network state s, and = 0 otherwise
g_{sr}	$g_{sr} > 0$ if a working path for lightpath r fails under network state s, and = 0 otherwise

$$Risk = \sum_{r \in R} ulp_r . m_r \qquad (2)$$

The risk in (2), when multiplied by the amount of time per year TY, (TY = 365×24×60×60 = 31536000 sec), is equal to the Expected annual Lost of Traffic (ELT) in the network, or

$$ELT = \mathrm{TY} \sum_{r \in R} ulp_r . m_r \ . \qquad (3)$$

In this paper, the quantitative measure of risk, as ELT, in (3) will be used as a criterion for evaluating and comparing alternate survivable network designs. The risk calculation in (3) requires a method for evaluating lightpath unavailability, especially when different configurations of survivability technique are applied in the network. A well-developed analytical method for evaluating failure probabilities is the fault tree method. The fault tree is a failure-relationship model, which together with the truth table quantification technique can be used to evaluate the occurrence probability of failure events in a systematic way.



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

Figure 1. Network 1 ($|N| = 5$, $|L| = 7$) and Matrix $\boldsymbol{P}$ (working routes)

1) Fault Tree Models

A fault tree [6] is a graphical model that depicts the logical interrelationship of events that cause the occurrence of the failure of interest, referred to as the *root* or *top events* of the fault tree. Construction of a fault tree starts with identifying the tree's top/root events (e.g., lightpath failures), then proceeds by seeking out the 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 AND, indicates a situation where the output event occurs if and only if all the input events occur. Whereas, an OR gate, symbolized by OR, 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 each branch 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. The occurrences of basic events should be statistically independent to each other. 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.

An example of a fault tree model for a WDM network in Fig. 1 with link protection on link 1 and link 4 is shown in Fig. 2. For the network in Fig. 1, we assume that there are 10 bi-directional lightpaths (LPs) between all node pairs in the network. The lightpath routes in the form of matrix $\boldsymbol{P}$ are also given in Fig. 1, where $\boldsymbol{P} = \{p_{rl}\}_{|R| \times |L|}$ and $p_{rl} = 1$ if lightpath r uses link l in its working path, and = 0 otherwise. 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, in Fig. 2 the event LP3_fail occurs when either the event Link2_fail or the event Link7_fail or both events occurs. Similarly, each link failure event occurs if a corresponding cable cut event occurs. In this paper, 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 into the set of basic events. Note in Fig. 2, link protection is provided for links 1 and 4. 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. This is illustrated in Fig 2. 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. Link protection

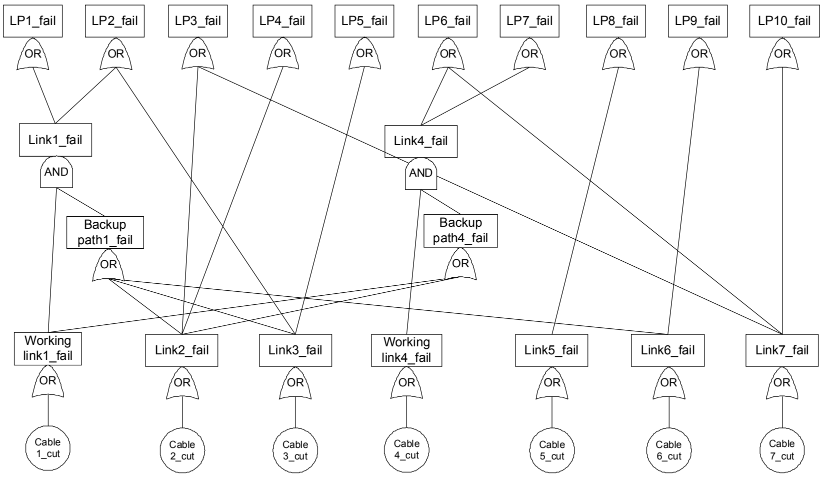


Figure 2. Fault tree for a WDM network in Fig. 1 with link protection on links 1 and 4.

introduces an additional AND gate located under a failure event of the link being protected. This makes the failure probability of the link in the end-to-end path of the lightpath lower. Note that in this network it is assumed that the backup path is not protected by a link protection mechanism implemented at any links that the backup path traverses.

From a fault tree, a logical expression of a top event in term of basic events can be obtained and evaluated quantitatively. In a quantitative evaluation, the probability of basic events must be given, and then combined together to calculate the probability of the top events. Simple rules exist for combining probabilities through logic gates. Assume that there are n statistically independent input events to a logic gate. Let E_{out} and E_i denote an output event and an input event i, whose probability of occurrence is $P(E_{out})$ and $P(E_i)$, $\forall i \in \{1,2,...,n\}$, respectively. For an AND gate, the probability of an output event is

$$P(E_{out}) = P(E_1 \text{ AND } E_2 \text{ AND ... AND } E_n) = \prod_{i=1}^{n} P(E_i)\,. \qquad (4)$$

For an OR gate, the probability of an output event is

$$P(E_{out}) = P(E_1 \text{ OR } E_2 \text{ OR ... OR } E_n) = 1 - \prod_{i=1}^{n}\left(1 - P(E_i)\right). \quad (5)$$

However, in Fig. 2, consider the probability calculation of the top event LP2_fail (i.e., the unavailability of LP2), which is given by

$$P(LP2\_fail) = P((Cable1\_cut \text{ AND } (Cable2\_cut \text{ OR } Cable3\_cut \text{ OR } Cable6\_cut)) \text{ OR } Cable3\_cut).$$

This example shows a situation where the probability calculation is not straightforward as elements in the expression are not independent (i.e., duplicated elements of *Cable3_cut*). Therefore, rules in (4) and (5) cannot be readily applied; otherwise it will produce erroneous results. One approach to solve this problem is to apply rules of Boolean algebra to simplify the expression into a form that contains no duplicated elements. In this example, by applying a distributive law, followed by an absorption law, the expression can be simplified into

$$P(LP2\_fail) = P((Cable1\_cut \text{ AND } (Cable2\_cut \text{ OR } Cable6\_cut)) \text{ OR } Cable3\_cut),$$

from which, (4) and (5) can be directly applied to obtain the unavailability of LP2, which is

$$P(LP2\_fail) = 1 - \{1 - u_l[1 - (1 - u_2)(1 - u_6)]\}(1 - u_3),$$

where u_l denotes the unavailability of cable l. Techniques for the calculation of the unavailability of cables u_l due to cable cuts are well known and are discussed in the Appendix. Note, that the process of calculating the probability of the top events in a fault tree as explained above is tedious especially in a large complex fault tree (e.g., a fault tree for multi-layer networks), where the expression may contain several duplicate terms. Furthermore, simplification has to be done on a case-by-case basis. Therefore, in this paper, another method, namely a truth table, which can calculate the probability of the top events in a fault tree in a systematic way, is used.

A truth table [7] is a systematic quantification technique, which can be applied to a fault tree or any other failure models to calculate the probability of failure events. One advantage of using the truth table method is that it eliminates the difficulty in probability calculation associated with duplicated terms in failure event's expressions. Another benefit is that it could provide exact results without using any approximation. The basic idea of the truth table method is to enumerate all network states with respect to the occurrence or non-occurrence of the fault tree's basic events, and then analyze the tree to determine the effect of each network state on the top events of the fault tree. Since all network states are mutual exclusive, the probability of a top event can be obtained by summing probabilities of all network states that cause an occurrence of the top event. The number of network states is determined by the number of basic events in the fault tree. For a fault tree with n basic events, each of which is alternatively occurring or not occurring, the number of all possible mutual exclusive network states, $|S|$, is equal to 2^n.

In the WDM network example of Fig. 1, since we consider cable cuts as the only basic events, therefore there are 7 basic events, and $2^7 = 128$ mutual exclusive network states. We use a binary matrix ***STATE*** = $\{state_{sl}\}_{|S|\times|L|}$, as a matrix form of a truth table, to list all network states, where $state_{sl} = 1$ if cable l is in a failure state under network state s, and $state_{sl} = 0$ otherwise. The matrix ***STATE*** for the WDM network of Fig. 1 is shown in Fig. 3. We also use a column vector ***stateprob*** = $\{stateprob_s\}_{|S|}$ to represent network state probabilities, where $stateprob_s$ is the probability of a network state s, which is calculated by

$$stateprob_s = \prod_{l\in L} u_l^{\,state_{sl}} (1 - u_l)^{1-state_{sl}}. \qquad (6)$$

The vector ***stateprob*** for our sample WDM network is also shown in Fig. 3 (using CC = 450 km and MTTR = 24 hours for u_l calculations as discussed in the Appendix). For each network state, we can determine whether or not a lightpath is in a failure state by assigning corresponding failure states (i.e., occurring or not-occurring) to all basic events in the fault tree, and evaluating the logic of the tree. The failure probability of the lightpath can be calculated by summing the probability of all network states that result in a failure of the lightpath being considered, or

$$ulp_i = \sum_{\substack{s\in S \text{ that results} \\ \text{in LP}_i \text{ failure}}} stateprob_s. \qquad (7)$$

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

Figure 3. Matrix ***STATE*** and vector ***stateprob***

$$ELT_{no\_protection} = \boldsymbol{stateprob}^{T} \times \left(\boldsymbol{STATE} \odot \boldsymbol{P}^{T}\right) \times \boldsymbol{m}.\mathrm{TY} \tag{8}$$

$$ELT_{link\_protection} = \boldsymbol{stateprob}^{\mathrm{T}} \times \left\{\left\{\boldsymbol{STATE} \circ \left[\left(\boldsymbol{STATE} \odot \boldsymbol{Q}^{\mathrm{T}}\right) + \left(\boldsymbol{1}_{|S|\times|L|} - \boldsymbol{1}_{|S|\times 1} \times \boldsymbol{bp}^{\mathrm{T}}\right)\right]\right]\right\} \odot \boldsymbol{P}^{\mathrm{T}}\right\} \times \boldsymbol{m}.TY \tag{9}$$

$$ELT_{path\_protection} = \boldsymbol{stateprob}^{\mathrm{T}} \times \left\{\left(\boldsymbol{STATE} \odot \boldsymbol{P}^{\mathrm{T}}\right) \circ \left[\left(\boldsymbol{STATE} \odot \boldsymbol{Q}^{\mathrm{T}}\right) + \left(\boldsymbol{1}_{|S|\times|R|} - \boldsymbol{1}_{|S|\times 1} \times \boldsymbol{bp}^{\mathrm{T}}\right)\right]\right]\right\} \times \boldsymbol{m}.\mathrm{TY} \tag{10}$$

Based on the fault tree logic and the truth table method, we also provide closed-form formulas for computing ELT for a network with three different protection scenarios: no protection, link protection, and path protection, as shown in (8), (9), and (10) respectively. For the ELT calculation in (9) and (10), matrix ***bp*** indicates which links or lightpaths respectively are currently protected, whereas matrix ***Q*** indicates the backup routes. In these formulas, $\circ$ is a Hadamard (Schur) product, obtained by multiplying together corresponding elements in each matrix [8], and $\odot$ is a binary matrix multiplication operator, which modifies general addition 1+1 = 2 to Boolean addition where 1+1 = 1 [9].

B. Risk-reduction Investment Strategy

An investment strategy is used to determine the best allocation of budget for implementing a survivability technique in different parts of the network to minimize the risk. In the link (path) protection case, an investment strategy determines which network links (paths) to be protected and their corresponding backup routes, subject to a budget limit, such that the network ELT is minimized. Here we present two approaches for solving the investment strategy problem. One is based on the Mixed Integer Linear Programming (MILP), 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 presented.

1) MILP Approach

In this section, we formulate the risk-reduction investment strategy as an MILP optimization problem for both link protection and path protection cases. The formulation is based on an arc-flow approach, in which a set of pre-computed backup paths is not required. Also, the formulation is based on the fault tree logic and the truth table method for the risk calculation, which allows the network ELT to be expressed as a linear function of decision variables ***bp*** and ***Q***. As a result, our investment strategy problem can be formulated as an MILP rather than a non-linear programming problem which would be the case if (4) and (5) are used for the unavailability calculation.

The MILP formulation for the link protection case is presented in (11)-(21). Two sets of decision variables to be determined are binary variables bp_i, which determines whether or not to protect link *i*, and binary variables q_{ij}, which determines the route of the backup path protecting link *i*. The objective (11) is to minimize the network ELT. Constraint set (12) is the flow balance constraints for backup paths. Constraints (13)-(16) are failure state relationships which determine whether or not lightpath *r* will fail under network state *s*. More specifically, constraint set (13) determines whether or not the backup path for link *i* is available under network state *s*. The backup path for link *i* might not be available under network state *s* (i.e., $h_{si} > 0$) for two reasons: either the backup path fails due to a cable cut under that network state (i.e., $\sum_{j\in L} state_{sj}q_{ij} > 0$), or link *i* is not protected (i.e., $bp_i = 0$, or $1\text{-}bp_i > 0$). Constraint set (14) indicates that link *i* fails under network state *s* (i.e., $e_{si} > 0$) if and only if both the working link fails (i.e., $state_{si} > 0$) and its backup path is not available under that network state. Constraint set (15) indicates that lightpath *r* fails under network state *s* ($y_{sr} > 0$) if and only if at least one of the links that it traverses fails (i.e., $\sum_{i\in L} e_{si}p_{ri} > 0$). Constraint set (16) relates variable y_{sr} to binary variable z_{sr}. Constraints (17)-(18) are for a risk calculation. That is, constraint set (17) calculates unavailability of lightpath *r* (ulp_r) by summing probabilities of all network states that results in a failure of that lightpath as in (7); and constraint (18) calculates a network ELT, as in (3). Constraint (19) is a budget constraint which limits the total spare capacity investment, where c_j is a unit cost of spare capacity on link *j*, and w_i is an amount of working capacity on link *i*.

MINIMUM-RISK LINK PROTECTION DESIGN FORMULATION

$$\text{Objective: } \min_{bp,q} ELT \tag{11}$$

$$\text{s.t. } \sum_{j\in L} q_{ij}b_{nj} = b_{ni}bp_i (\mathrm{mod}\ 2), \quad \forall i \in L, \forall n \in N \tag{12}$$

$$h_{si} = \sum_{j\in L} state_{sj}q_{ij} + 1 + bp_i, \quad \forall s \in S, \forall i \in L \tag{13}$$

$$e_{si} = state_{si}h_{si}, \quad \forall s \in S, \forall i \in L \tag{14}$$

$$y_{sr} = \sum_{i\in L} e_{si}p_{ri}, \quad \forall s \in S, \forall r \in R \tag{15}$$

$$z_{sr}\mathrm{K} \ge y_{sr}, \quad \forall s \in S, \forall r \in R \tag{16}$$

$$ulp_r = \sum_{s\in S} z_{sr}stateprob_s, \quad \forall r \in R \tag{17}$$

$$ELT = \mathrm{TY}\sum_{r\in R} ulp_r m_r \tag{18}$$

$$\sum_{i\in L}\sum_{j\in L} c_j w_i q_{ij} \le budget \tag{19}$$

$$q_{ij}, bp_i : \ binary, \quad \forall i \in L, \forall j \in L \tag{20}$$

$$z_{sr} : binary, \quad \forall s \in S, \forall r \in R \tag{21}$$

For the path protection case, the MILP formulation is presented in (22)-(33). Two sets of decision variables to be determined are binary variables bp_r, which determines whether or not to protect lightpath r, and binary variables q_{rj}, which determines a backup route for lightpath r. The objective (22) is to minimize the network ELT. Constraint set (23) is the flow balance constraints for backup paths. Constraints (24)-(27) are failure state relationships which determine whether or not lightpath r will fail under network state s. More specifically, constraint set (24) determines whether or not the backup path for lightpath r is available under network state s. The backup path for lightpath r might not be available under network state s (i.e., $h_{sr} > 0$) for two reasons: either the backup path fails due to a cable cut under that network state (i.e., $\sum_{j \in L} state_{sj} q_{rj} > 0$), or lightpath r is not protected (i.e., bp_r = 0, or 1-bp_r > 0). Constraint set (25) indicates that the working path of lightpath r fails under network state s (i.e., $g_{sr} > 0$) if and only if at least one of the links in the end-to-end path fails under that network state (i.e., $\sum_{j \in L} state_{sj} p_{rj} > 0$). Constraint set (26) indicates that lightpath r fails under network state s (i.e., $y_{sr} > 0$) if and only if both its working path fails and its backup path is not available under that network state (i.e., $g_{sr}h_{sr} > 0$). Constraint set (27) relates variable y_{sr} to binary variable z_{sr}. Constraints (28)-(29) are for a risk calculation same as (17)-(18) in the link protection case. Constraint (30) is a budget constraint. Constraint set (31) guarantees that each backup path is link-disjoint from its working path.

MINIMUM-RISK PATH PROTECTION DESIGN FORMULATION

$$\text{Objective: } \min_{bp,q} ELT \quad (22)$$

$$\text{s.t. } \sum_{j \in L} q_{rj} b_{nj} = d_{rn} bp_r (\text{mod } 2), \quad \forall r \in R, \forall n \in N \quad (23)$$

$$h_{sr} = \sum_{j \in L} state_{sj} q_{rj} + 1 - bp_r, \quad \forall s \in S, \forall r \in R \quad (24)$$

$$g_{sr} = \sum_{j \in L} state_{sj} p_{rj}, \quad \forall s \in S, \forall r \in R \quad (25)$$

$$y_{sr} = g_{sr} h_{sr}, \quad \forall s \in S, \forall r \in R \quad (26)$$

$$z_{sr} \mathrm{K} \geq y_{sr}, \quad \forall s \in S, \forall r \in R \quad (27)$$

$$ulp_r = \sum_{s \in S} z_{sr} stateprob_s, \quad \forall r \in R \quad (28)$$

$$ELT = \mathrm{TY} \sum_{r \in R} ulp_r m_r \quad (29)$$

$$\sum_{r \in R} \sum_{j \in L} c_j q_{rl} m_r \leq budget \quad (30)$$

$$p_{rj} + q_{rj} \leq 1, \quad \forall r \in R, \forall j \in L \quad (31)$$

$$q_{rj}, bp_r : binary, \quad \forall r \in R, \forall j \in L \quad (32)$$

$$z_{sr} : binary, \quad \forall s \in S, \forall r \in R \quad (33)$$

2) *Heuristic Approach*

In the heuristic approach for solving the minimum-risk design problems, the backup routes are pre-computed and given to the problem. Each backup route is selected as a link-disjoint route from the working link (in link protection) or the working path (in path protection) with the minimum path unavailability. As a result, the investment strategy only needs to determine which links/lightpaths in the network to be protected for a given budget. These problems are equivalent to a well-known 0-1 Knapsack problem [10]. We note that, 0-1 Knapsack problems are often solved using greedy heuristics and here we propose three greedy heuristic algorithms.

Heuristic 1: Greedy heuristic with greatest risk reduction

The basic idea of this greedy heuristic is that at each step, protection is applied to a link (in a link protection case) or a lightpath (in a path protection case) where the protection produces the greatest risk reduction and does not violate the budget limit. The amount of risk reduction associated with each link and lightpath can be calculated using (9), and (10) respectively with appropriated settings of ***bp*** and ***Q*** values. The process repeats until no more protection can be applied due to the budget limit, or all the links/lightpaths have been protected.

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

This heuristic is similar to Heuristic 1 except that at each step, the protection is applied to the link/lightpath where the protection produces the greatest ratio of risk reduction to backup path cost while not violating the budget limit.

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 current solution. The second step is based on an idea that it is possible to improve the solution by iteratively removing the protection from a protected link/lightpath in the current solution and then reinvesting in other unprotected links/lightpaths that could produce a greater risk reduction. The iterative process keeps reducing the amount of risk; and terminates when the current solution cannot be further improved, or the predefined number of iterations is reached.

III. INCREMENTAL SURVIVABLE NETWORK DESIGN

The proposed risk-based survivable network design approach does not assume a Greenfield condition. The given network to the design problem could be partially fault-tolerant, where a survivability improvement can be incrementally applied to the network to reduce the network risk. For each increment, the design seeks to determine in which parts of the network to implement a survivability technique as an addition to the existing survivability mechanisms in the network to minimize the total network risk, while not exceeding the given budget. It is typically assumed that a reconfiguration of existing survivability mechanisms is not possible.

The MILP formulations for incremental survivable network design requires two additional sets of constraints in order to fix decision variables bp_i and q_{ij}, for all existing protected links/lightpaths in the network, at their values from the previous design. Consequently, the problem will only optimize over the remaining variables. Furthermore, a budget constraint must be modified as a sum of spare capacity costs occurring only in the current incremental design.

IV. Experimental Design and Numerical Results

This section presents the experimental results of the proposed risk-based survivable network design. Two networks are used in the experiments: Network 1, and Network 2 as shown in Fig.1, and Fig. 4 respectively. The cable lengths (km) are also indicated in the figures. All the cables have the same metric CC of 450 km and the same MTTR of 24 hours, except for link 2 in Network 1, which has a CC of 30 km. For each network, full mesh 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 hop count. Also, the spare capacity cost is defined as 1 budget unit per 10 Gbps per 1000 km.

Several numerical cases were studied. First, the risk curves (i.e., risk vs budget) for link protection and path protection are compared and discussed. Then, the cost benefit analysis can show whether the investment in network survivability is justified by the reduction in the risk level, and also show an optimal budget value for investing in the network survivability. Secondly, the results from MILP approach and proposed heuristic algorithms are compared. Lastly, different incremental investment alternatives are compared.

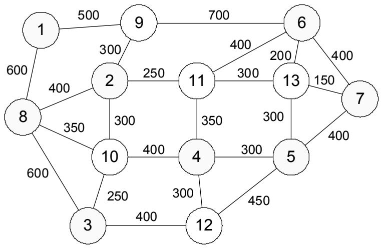


Figure 4. Network 2 ($|\boldsymbol{N}| = 13$, $|\boldsymbol{L}| = 23$)

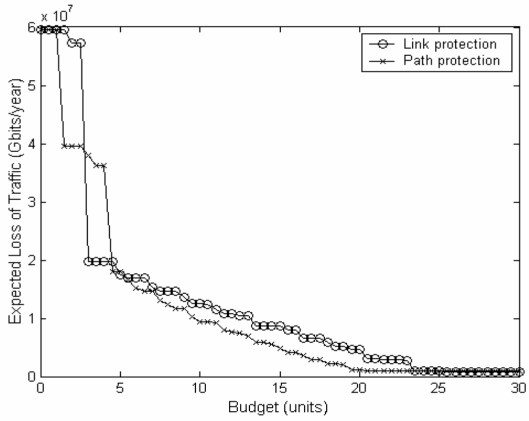


Figure 5. ELT vs Budget for link and path protection on Network 1

TABLE II
INVESTMENT STRATEGY RESULTS INDICATING WHICH LINKS OR LPS ARE PROTECTED FOR SOME BUDGET VALUES

Budget	Link Protection	Path Protection
1.5	None	LP 4 (critical LP)
2	Link 6 (cheapest link to be protected)	LP 4 (critical LP)
3	Link 2 (critical link)	LP 3 (critical LP)
4.5	Link 2 (critical link)	LP 3, and 4 (critical LPs)
12	Link 2, 3, 4, and 6	LP 2, 3, 4, 5, 6, and 9
20.5	Link 2, 3, 4, 5, 6 and 7	All LPs
25.5	All links	All LPs

In the first set of experiments, a budget in term of spare capacity investment is given for each problem instance. For Network 1, we consider budget values ranging from 0 to 30 units by 0.5 increments. The investment strategy problem was solved for each budget value to optimality using the CPLEX solver. The results from the investment strategy in term of network ELT for both link protection and path protection cases for various budget values are shown in Fig. 5. In addition, Table II shows the results of which links and lightpaths are being protected for some specific budget values.

In Network 1, link 2 is considered as the most critical link since it is most vulnerable to cable cuts as indicated by its extremely low CC value. Similarly, LP3 and LP 4, whose working path are routed via link 2, are also considered as the most critical lightpaths. The results in Fig. 5 and Table II show that, the risk based design tries to protect the most critical links/lightpaths first whenever the budget is sufficient. For example, when the budget is equal to 3 units (i.e., the lowest budget value sufficient for protecting link 2), link 2 is protected, which results in a significant reduction in the network risk (i.e., ELT) down to 19,717,544 Gbits (shown as the biggest down step in the link protection risk curve). For most budget values, the ELT in the network with path protection is lower than in the network with link protection. This is understandable because the path protection is more capacity efficient due to its higher flexibility in choosing the backup routes; and therefore cheaper to implement. For example, the link protection requires 25.5 units of budget to protect all the network links, whereas the path protection requires only 20.5 units to protect all the lightpaths in the network. Nevertheless, a connection with the path protection is more vulnerable to multiple failures, which can damage the working and backup paths simultaneously. This can be seen by, for example, when all links and lightpaths are protected, the network ELT in the path protection case (994,203 Gbits) is higher than in the link protection case (722,008 Gbits).

For Network 2, the risk curve is shown in Fig. 6, with budget values ranging from 0 to 150 units by 2.5 increments. However, in our experiment for Network 2, we consider only network states with at most two simultaneous failures, rather than all possible network states, which results in a reduction of number of network states in the truth table from $2^{|L|}$ to $1 + |L|(|L|+1)/2$. This, in turn, underestimates the risk level; however it gives a very close approximation because most of the probability mass is in the network states with a small number of simultaneous failures (e.g., in Network 2, it constitutes the total state probability of .99958).

From the results, we observe that the 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 for an additional unit of budget decreases as the budget increases. This is understandable because for a given budget the investment strategy tries to protect a set of links/lightpaths that results in the maximum risk reduction (e.g., critical links/lightpaths). As the budget increases, more and more critical links/lightpaths have been protected, and only

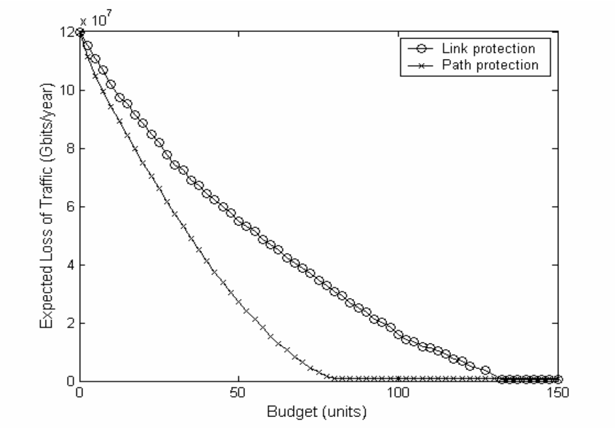


Figure 6. ELT vs Budget for link and path protections on Network 2

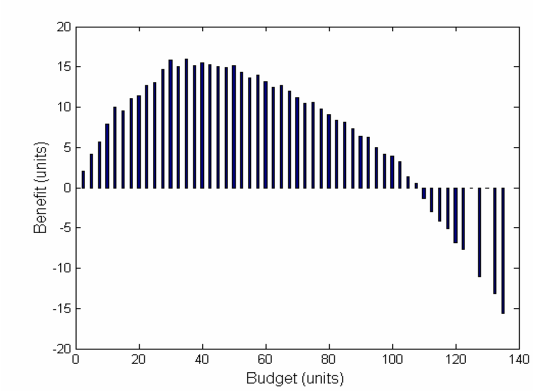


Figure 7. Benefit vs Budget for link protection on Network 2

relatively less-critical links/lightpaths remain for protection, resulting in a lower risk reduction for an additional budget unit. Note that the risk curve in Fig. 5 is not obvious to be convex 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.

If information is available, one can convert the reduction in the risk level into a monetary unit; then, calculate an investment benefit, defined as the reduction in the risk level (in a monetary unit) subtracted by the cost of implementing the survivability technique (i.e., a budget). The purpose of the cost benefit analysis here is to demonstrate whether or not the cost of implementing the survivability technique can be justified by the reduction in the risk level. The survivability investment is economically justified only if the benefit is positive.

From the results in Fig. 6, if we assume that the reduction in 10^6 Gbits traffic loss per year is equivalent to one monetary unit, the plot of the benefit against the budget for the link protection case can be shown in Fig 7. The benefit plot for the path protection case also has a similar shape, but due to the space limit it is not presented here. The benefit plot in Fig. 7 shows that the cost of implementing the survivability technique is justified by the reduction in the risk level for investments with a budget less than or equal to 107.5 units, but it is not justified to invest in the network survivability for more than or equal to110 units. In other words, it is not justified to protect all the network links, but only some links in the network (i.e., critical links). The benefit plot also shows the optimal budget value for investing in the network survivability, which yields the highest benefit, i.e., at 35 budget units in Fig. 7. Note that the shape of a benefit plot is greatly affected by the assumption on the monetary value per unit of risk reduction. If the monetary value per unit of risk reduction is assumed higher, the optimal budget value will move to the right, indicating it is more beneficial to increase the budget for investing in the network survivability. On the other hand, if the monetary value per unit of risk reduction is assumed lower, the optimal budget value will move to the left, indicating to invest less in the network survivability.

Next, the performance of heuristic algorithms are presented and compared. Table III presents, for each heuristic algorithm, an average error from the optimal result obtained from the MILP approach over all problem instances, on Network 2. Only the problem instances with budget values that result in the partial protection are used in the calculation of average errors, since for all other budget values, the MILP and heuristic approaches always produce the same results (i.e., not protecting at all, or protecting all links/lightpaths). 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., an amount of risk reduction per unit cost is used as a selecting criterion rather than an 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 the iterative greedy heuristic algorithm and MILP approach for the link protection case on Network 2 are also compared if Fig. 8. Due to a space limit, the computational time of the other two heuristics, which are shorter, and for the path protection case, are not presented here. The results show that the MILP approach cannot guarantee that

TABLE III

AVERAGE ERROR OF HEURISTICS FOR LINK PROTECTION AND PATH PROTECTION ON NETWORK 2

	Link Protection	Path Protection
	Average Error (%)	**Average Error (%)**
Heu.1	28.45	7.72
Heu.2	18.85	1.53
Heu.3	3.84	0.53

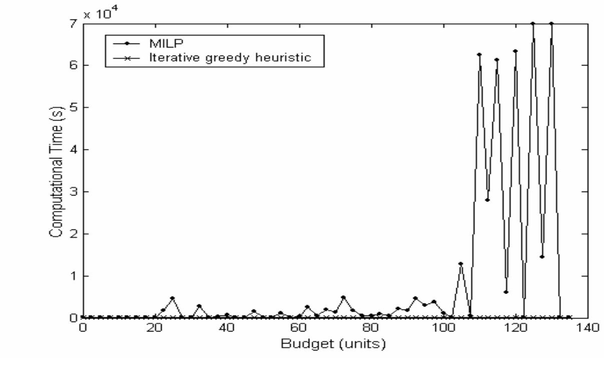


Figure 8. Computational times for MILP and Iterative greedy heuristic on Network 2 with link protection

TABLE IV

ELT RESULTS FROM THREE DIFFERENT INVESTMENT ALTERNATIVES

	ELT result from each investment (Gbits per year)			
	Quarter1	Quarter2	Quarter3	Quarter4
Annual Investment	54,784,566			
Semi-annual Investment	81,946,580		54,784,566	
Quarterly Investment	97,459,612	82,142,699	67,358,274	57,060,430

an optimal solution can be obtained in a reasonable time. For example, in Fig. 8, there are many problem instances where the computational times is larger than 3 hours, and especially two instances where the optimal solution cannot be found after 3 days (represented by 7×10^4 sec in the figure), whereas the iterative greedy heuristic could provide near-optimal solutions in less than 3 minutes for all problem instances.

Lastly, different incremental investment alternatives are compared on the basis of risk. In our experiments, 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. 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. Table IV shows the ELT result from each incremental investment for the three investment alternatives using link protection on Network 2. The given capital expenditure is 50 units. The result shows that, after all investments, the quarterly investment results in a higher risk remaining to the network (i.e., 57,060,430 Gbits) than the other two investment alternatives (i.e., 54,784,566 Gbits). This is because the quarterly investment has a smaller available budget per investment; therefore it may select a set of links to be protected that is only suboptimal to the set of protected links selected by the investment alternatives with a larger budget per investment.

V. SUMMARY

This paper shows a proof of concept for a risk-based approach to incremental survivable network design. The new design approach is proposed to determine how to incrementally implement a survivability technique in different parts of the network for a given budget to minimize the risk from network failures. The minimum-risk design problems for link and path protections are formulated in MILP models, and solved for optimal solutions. Greedy heuristic algorithms are also considered as scalable solution techniques. The truth table is used as a systematic quantification method to provide an exact calculation of failure probability, and enable the minimum-risk design problems to be formulated in MILP models.

The numerical results showed that for most budget values the path protection scheme results in a lower risk (i.e., ELT) than the link protection. Moreover, the results showed that the risk curves (i.e., risk vs budget) have the convex shape. This emphasizes the fact that different parts of the network are associated with different risk levels. Therefore, the amount of risk reduction for an additional unit of budget decreases as the budget increases. Also, the cost benefit analysis demonstrated that it might not be economically justified to protect all the links or lightpaths in the network. The analysis could show the range of budgets in which the cost of implementing the survivability technique is justified by the reduction in the risk level. Furthermore, it could show the optimal budget value for investing in the network survivability. The results from heuristic approach showed that the iterative greedy heuristic algorithm could provide good near-optimal solutions with scalable computational time.

VI. APPENDIX

The unavailability of fiber optic cables due to cable cuts has been studied in the literature and can be determined as follows. 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, unavailability of a component is

$$U = \frac{MTTR}{MTTF + MTTR} = \frac{MTTR}{MTBF}, \tag{34}$$

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, MTBF is typically represented by a Cable Cut (CC) metric, 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 (35).

$$MTBF_{cable}(hour) = \frac{CC\times 365\times 24}{cable\ length(km)} \tag{35}$$

REFERENCES

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

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

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

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

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

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

[7] H. Kumamoto, E. Henley, Probabilistic Risk Assessment for Engineers and Scientists, second edition, IEEE Press, New York, 1996.

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

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

[10] S. Martello, and P. Toth, Knapsack Problem: Algorithms and Computer Implementation, John Wiley & Sons, New York, 1990.