Risk Reduction Based Survivable WDM Network Design

Korn Vajanapoom and David Tipper
Department of Information Science and Telecommunications
University of Pittsburgh, Pittsburgh, PA 15260, USA
email: kov2@pitt.edu, tipper@tele.pitt.edu

***Abstract*— This paper presents an investment strategy to reduce the risk associated with failures in Wavelength Division Multiplexing (WDM) optical networks. The investment strategy determines how to allocate a fixed budget for implementing survivability techniques in different parts of the network such that the Expected Loss of Traffic (ELT) is minimized. Two survivability schemes are considered in this paper: dedicated link protection and dedicated path protection. Two analytical techniques for evaluating network unavailability and ELT are presented in this paper: a fault tree analysis and an event tree. Based on the event tree approach, we propose a novel Mixed Integer Linear Programming (MILP) formulation for the investment strategy problem. Numerical results illustrating the investment strategy for both link and path protection are presented and discussed.**

I. INTRODUCTION

Backbone wide area and metro networks have been steadily moving to optical technology based on Wavelength Division Multiplexing (WDM). A WDM network is comprised 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. Nowadays, a lightpath can carry a data rate up to 40Gbs and a higher rate is expected in the future. Obviously, the failure of a lightpath will result in enormous traffic loss. Since network components, such as OXCs, optical fibers, optical amplifiers, and WDM (de)multiplexers, have non-zero probabilities of failure, WDM networks should be designed with fault tolerant properties.

A number of techniques for designing survivable WDM optical networks have appeared in the literature [1]-[7]. The focus of much of the current literature is to provide a full recovery against a set of predefined failures, such as all single network failures, with a minimum additional cost. However, in reality, a WDM network service provider may have a limited budget for improving its network (e.g., quarterly capital expenditure budget). Here we propose a different approach to the survivable network design problem, aimed at reducing risk associated with network failures for a given budget. In this paper, we present an optimization based investment strategy to reduce the network risk as measured by an Expected Loss of Traffic (ELT).

A. Risk Reduction Techniques

Various techniques to reduce the risk associated with network failures exist. These techniques can be categorized as prevention/avoidance and recovery schemes.

1) Prevention/avoidance schemes.

The prevention/avoidance techniques seek to reduce the probability of network component failure. This can be achieved by, for example, using more reliable network equipments (e.g., more reliable OXCs). Improving the reliability of constituent network components can reduce the network's ELT. However, in some situations, even if the most reliable network components are deployed, the desired level of network downtime or ELT may not be achieved. Therefore, the network should be designed with spare capacity and a traffic recovery technique is needed.

2) Recovery schemes.

Recovery techniques, also called as survivability techniques, perform a correction action after a failure occurs. Typically, this can be achieved by providing backup network components (e.g., backup nodes or paths) so that in the event of a component failure, a backup component can immediately take its place. In WDM networks, the most common recovery technique is based on the use of backup paths to carry the affected traffic in the event of network's component failure. Two preplanned recovery techniques are considered in this paper: dedicated link protection and dedicated path protection [4], [5] (or link and path protection in short). Other recovery techniques such as a shared protection [6]-[8], and dynamic restoration [9], [10] are not considered in this paper. For both link protection and path protection techniques, backup paths are established in advance before a failure occurs. Each backup path is dedicated to a single protected link (in the link protection case), or a single protected lightpath (in the path protection case), and cannot be used by any other links/lightpaths for failure recovery. However, the difference between the two techniques relies on the scope of the backup path. In the link protection, the backup path is provided between two adjacent OXCs of a protected link, whereas, in the path protection, the backup path (i.e., a backup lightpath)

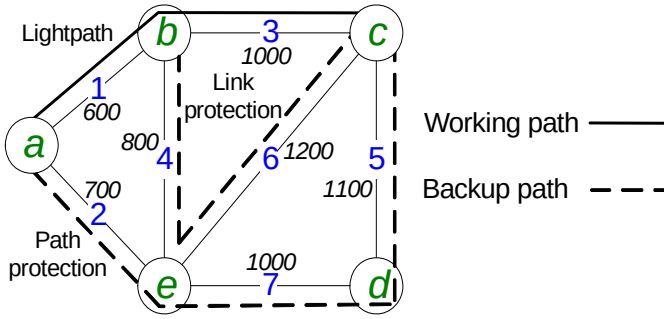

Fig. 1. WDM optical network with 5 nodes and 7 bi-directional links with cable lengths (*km*) as indicated, and illustration of link protection and path protection techniques

is provided end-to-end between a source and destination OXCs of a protected lightpath. In the link protection, we assume that all the lightpaths that traverse the failed link are recovered using the same backup path i.e., recovered at the optical multiplex section (OMS) layer [4][5]. Fig. 1 illustrates the link protection and the path protection techniques.

In this paper, we assume that the recovery process is instantaneous, and that the network continues to provide service with no disruptions as long as the backup paths are available, (i.e., the down time during the recovery process is negligible), and does not cause a traffic loss in our consideration.

For a given budget to implement a link protection in a WDM network, an investment strategy is used to determine which network links to be protected along with their corresponding backup routes such that the network's ELT is minimized. Similarly, for a path protection, an investment strategy is used to determine which lightpaths to be protected, and their corresponding backup routes such that the network's ELT is minimized. To our best knowledge, this problem is considered for the first time. We also proposed a novel Mixed Integer Linear Programming (MILP) formulation for the investment strategy problem. Although in this paper we discuss the problem in the context of WDM networks, the general concept and the proposed formulation can be applied to any connection-oriented networks, such as ATM and MPLS networks.

The notation used in this paper is summarized in Table I. The remainder of this paper is organized as follows. Section II presents a basic unavailability calculation. Section III discusses a fault tree analysis for evaluating network unavailability. Section IV discusses an event tree approach for evaluating network unavailability, and presents matrix-based formulations for calculating network's ELT. A risk based incremental investment strategy problem and its MILP formulations are presented in section V. Section VI presents and discusses the results from our proposed investment strategy. And section VII concludes the paper.

TABLE I
NOTATION

N, R, S	A set of nodes, lightpaths, and network states respectively
L	A set of links or a set of cables
$\boldsymbol{P} = \{p_{rl}\}_{\lvert R\rvert \times \lvert L\rvert}$	$p_{r,l} = 1$ if lightpath r uses link l in its working path, and = 0 otherwise
$\boldsymbol{m} = \{m_r\}$	m_r is a data rate of lightpath r (bits/s)
$\boldsymbol{B} = \{b_{nl}\}_{\lvert N\rvert \times \lvert L\rvert}$	$b_{nl} = 1$ 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	The unavailability of cable l
$\boldsymbol{F} = \{f_{sl}\}_{\lvert S\rvert \times \lvert L\rvert}$	$f_{sl} = 1$ if cable l fails under network state s, and = 0 otherwise
$\boldsymbol{stateprob} = \{stateprob_s\}_{\lvert S\rvert}$	$stateprob_s$ is a probability of occurrence of network state s
$\boldsymbol{1}_{\mathrm{M}\times\mathrm{N}}$	An M × N matrix with only elements "1"
w_l	An amount of working capacity on link l, calculated by $w_l = \sum_{r \in R} p_{rl} m_r$
lpf_{sr}	$lpf_{sr} > 0$ if lightpath r (both working and backup if exists) fails under network state s, and = 0 otherwise
$lpfbinary_{sr}$	$lpfbin_{sr} = 1$ if lightpath r (both working and backup if exists) fails under network state s, and = 0 otherwise
ulp_r	The unavailability of lightpath r
c_l	The unit cost of spare capacity on link l
budget	The budget
K	A sufficiently large number
The following notation is used in the link protection case only:	
$\boldsymbol{bp} = \{bp_l\}_{\lvert L\rvert}$	$bp_l = 1$ if there exists a backup path protecting link l, and = 0 otherwise
$\boldsymbol{Q} = \{q_{ij}\}_{\lvert L\rvert \times \lvert L\rvert}$	$q_{ij} = 1$ if link i uses link j in its backup path, and = 0 otherwise
bpf_{sl}	$bpf_{sl} > 0$ if a backup path for link l is not available (either not existd, or failed) under network state s, and = 0 otherwise
$linkf_{sl}$	$linkf_{sl} > 0$ if link l (both working and backup if exists) fails 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 there exists a backup path protecting lightpath r, and = 0 otherwise
$\boldsymbol{Q} = \{q_{rl}\}_{\lvert R\rvert \times \lvert L\rvert}$	$q_{rl} = 1$ if lightpath r uses link l in its backup path, and = 0 otherwise
bpf_{sr}	$bpf_{sr} > 0$ if a backup path for lightpath r is not available (either not existed, or failed) under network state s, = 0 otherwise
wpf_{sr}	$wf_{sr} > 0$ if a working path for lightpath r fails under network state s, and = 0 otherwise

II. Basic Unavailability Calculation

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

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

where MTTR denotes Mean Time To Repair, and MTTF denotes Mean Time To Failure which indicates a reliability of a component. Another related term is Mean Time Between Failure (MTBF), where MTBF = MTTR+MTTF. Availability (A) is a complement of unavailability or $A = 1 - U$, and is defined as the probability that component will be found in the

working state at a random time in the future.

Validated data on MTTR and MTTF for many network equipments can be found in literatures [11]. For optical fiber cables, MTBF can be calculated from a cable length, and a Cable Cut (CC) metric, which is the average cable length (km) that results in a single cable cut per year, or

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

In WDM networks, we are interested in evaluating lightpaths' unavailability. Two techniques for evaluating the unavailability of lightpaths are discussed in this paper: a fault tree analysis (section III) and an event tree (section IV).

An unavailability of a lightpath can also be expressed using a metric *downtime per year*, which typically gives a better illustration of differences in unavailability. A downtime per year (min) is calculated by multiplying lightpath unavailability with minutes per year, or

$$\text{downtime per year (min)} = U \times 365 \times 24 \times 60. \quad (3)$$

Another important metric is a lightpath's Expected Loss of Traffic (ELT). It is a traffic-weighted lightpath unavailability, obtained by multiplying a lightpath downtime per year with a connection data rate, or

$$\text{lightpath's ELT} = \text{lightpath's downtime per year} \times \text{data rate}. \quad (4)$$

A network's ELT is obtained by summing lightpath's ELT of all lightpaths in the network, or $\sum_{\text{all LP}} \text{ELT}_{\text{LP}}$.

III. Fault tree Analysis

This section explains the use of fault tree analysis as a method for evaluating unavailability of a network. The fault tree is a graphical model that depicts the logical interrelationship of fault events that cause the occurrence of the predefined undesired failure events of the network, called top events of the fault tree. A fault tree consists of the following elements [12].

Basic events: Basic events are the fault events that are not further developed (i.e., underlying fault events that may cause this event to occur are not considered). These events are at the lowest level in each branch of the fault tree and symbolized by circles. The probability of occurrence of these events must be provided if the fault tree is to be used for computing a probability of top events.

Logic gates: A logic gate indicates a relationship of lower-level events (i.e., inputs to the gate) that can cause an occurrence of higher-level event (i.e., output of the gate). Two fundamental logic gates for fault tree structure are an AND gate and an OR gate. An AND gate, symbolized by  , indicates a situation where the output event occurs if and only if all the input events occur. Whereas, an OR gate, symbolized by  , is used to indicate that the output event occurs if at least one of the input events occurs.

Intermediate events: Intermediate events are the fault events whose occurrences result from a logical combination of lower-level events through logic gates. All intermediate events are represented by rectangles.

A fault tree model can be evaluated quantitatively, i.e., to calculate an occurrence probability of fault events of interest, e.g., top events of the fault tree. In such a case, a probability of occurrence of basic fault events must be given, and then combined together using the logic of the tree to give the probability of fault events of interest. There are two basic rules for combining probabilities of occurrence through logic gates: one for AND gates, and the other one for OR gates. Assume that there are n statistically independent input events to a logic gate. Let E_{out} and E_i represent 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 occurrence of an output event is

$$\begin{aligned} P(E_{out}) &= P(E_1 \text{ AND } E_2 \text{ AND } ... \text{ AND } E_n) \\ &= \prod_{i=1}^{n} P(E_i). \end{aligned} \quad (5)$$

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

$$\begin{aligned} P(E_{out}) &= P(E_1 \text{ OR } E_2 \text{ OR } ... \text{ OR } E_n) \\ &= 1 - \prod_{i=1}^{n} \left(1 - P(E_i)\right). \end{aligned} \quad (6)$$

A. A WDM network with no protection

Consider the WDM network in Fig. 1, we assume that there are 10 bi-directional lightpaths between all node pairs in the network. The lightpath routes in the form of matrix ***P*** are given in Fig. 2. The corresponding fault tree for this WDM network is shown in Fig. 3. Since we are interested in computing lightpath unavailability and ELT, lightpath failures are defined as the top events of the fault tree. A lightpath is in a failure state when at least one of the links that the lightpath traverses is in a failure state. For example, an event LP2_fail occurs when either an event Link1_fail or an event Link2_fail or both events occurs. Similarly, each link failure event occurs if a corresponding cable cut event occurs. In this analysis, cable cuts are considered as the only basic events of a fault tree; however, it is straightforward to include other network component failures into a set of basic events, such as OXC failures and optical amplifier failures.

From a fault tree, a Boolean expression of a top event in term of basic events can be obtained. Then, the probability of

occurrence of a top event, i.e., a lightpath unavailability, can be calculated using the two basic probability's rules in (5) and (6). For example, an unavailability of LP2 is

$$\begin{aligned} P(LP2\_\ fail) &= P(Link1\_\ fail \text{ OR } Link3\_\ fail) \\ &= P(Cable1\_cut \text{ OR } Cable3\_cut) \\ &= 1-\big(1-P(Cable1\_cut)\big)\big(1-P(Calbe3\_cut)\big) \\ &= 1-(1-u_1)(1-u_3). \end{aligned}$$

After calculating unavailabilities for all lightpaths, we can compute a network's ELT as explained in section II.

The WDM network modeled by a fault tree in Fig. 3 does not incorporate any recovery techniques. When a survivability technique such as link protection or path protection is applied to a network, the fault tree model structure must be modified accordingly to reflect the existence of backup paths. These are discussed below.

B. A WDM network with link protection

With link protection, a link is determined to be in a failure state only if both the link itself, so called a working link, and its backup path fail. This is illustrated in a fault tree in Fig. 4, where link protection is applied to links 1 and 4. The backup path of link 1 traverses network links 2, 3 and 6, whereas a backup path of link 4 traverses network links 1 and 2. The link protection introduces an additional AND gate located under a link failure event being protected. This makes the probability of failure of the link in the end-to-end path of the lightpath lower. Note that in this model we assume that the backup path is not protected by a link protection mechanism implemented on any links that it traverses. From the fault tree model in Fig. 4, an expression of lightpath unavailability can be obtained. For example, the unavailability of LP2 is given by

$$\begin{aligned} P(LP2\_\ fail) = P((&Cable1\_cut \text{ AND } (Cable2\_cut \text{ OR} \\ &Cable3\_cut \text{ OR } Cable6\_cut)) \text{ OR } Cable3\_cut). \end{aligned}$$

The probability calculation in this example requires careful thought, as elements in the expression are not independent, i.e., there exist duplicated basic events of Cable3_cut. In such a case, rules for combining probabilities in (5) and (6) cannot be readily applied; otherwise it will produce erroneous results. Some methods exist for solving this problem, for example, we can apply rules of Boolean algebra [13] to simplify the expression into a form that contains only independent elements (i.e., to eliminate duplicated elements), from which we can apply (5) and (6) to calculate the occurrence probability. In this example, without showing details, we have

$$\begin{array}{c} \\ LP1 \\ LP2 \\ LP3 \\ LP4 \\ LP5 \\ LP6 \\ LP7 \\ LP8 \\ LP9 \\ LP10 \end{array} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Fig. 2. Lightpath routing matrix $\boldsymbol{P} = \{p_{ri}\}_{R \times L}$

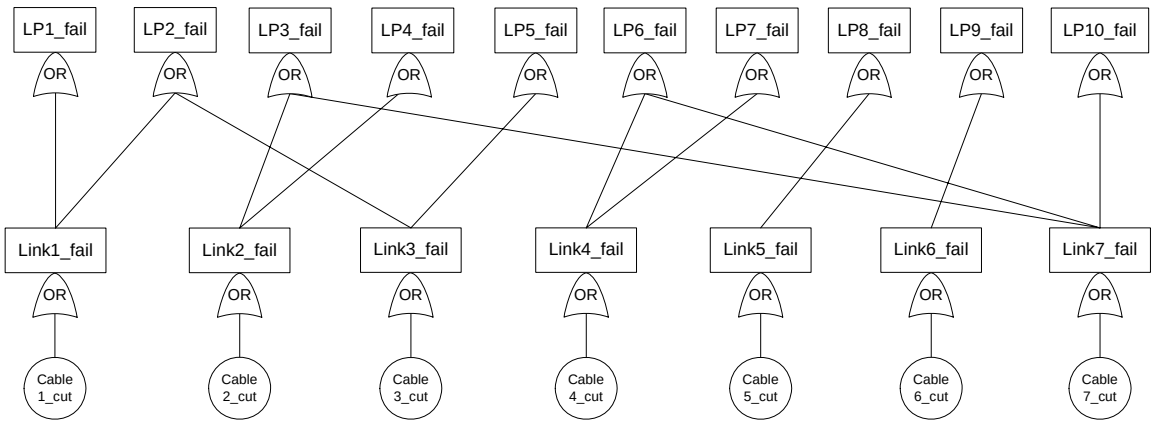

Fig. 3. A fault tree model of a WDM network with no protection

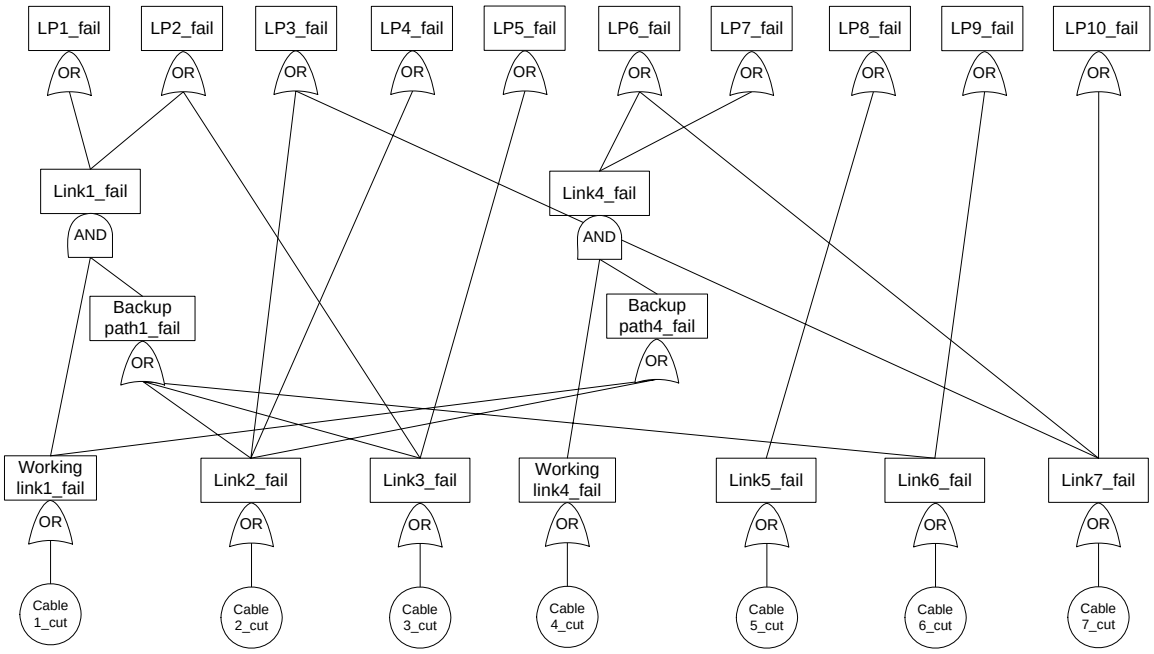

Fig. 4. A fault tree model of a WDM network with a link protection applied to link 1 and link 4

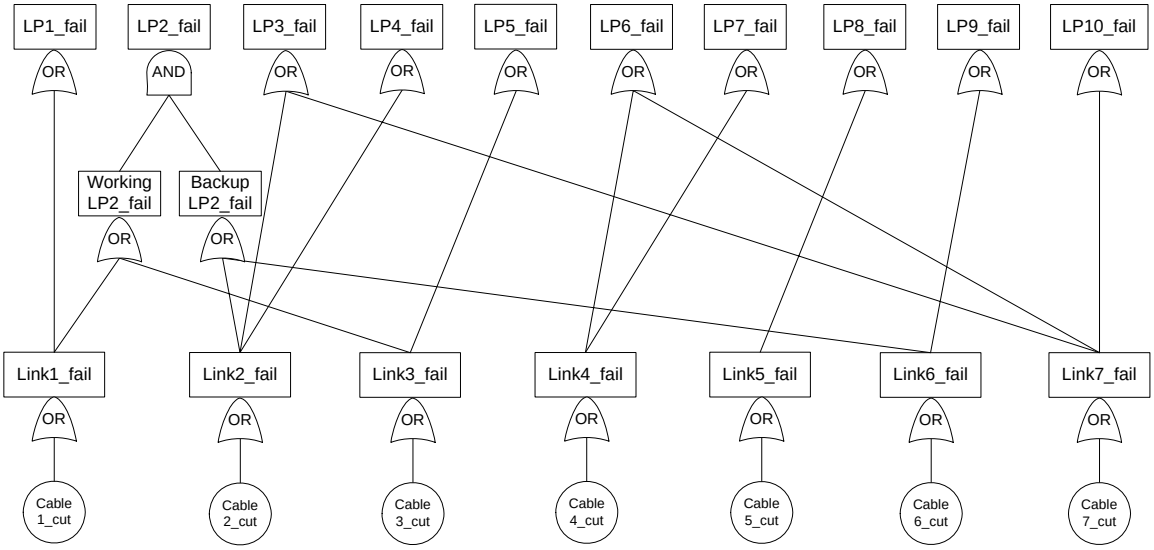

Fig. 5. A fault tree model of a WDM network with a path protection for LP2

$$P(LP2\_fail) = P((Cable1\_cut \text{ AND } (Cable2\_cut \text{ OR } Cable6\_cut)) \text{ OR } Cable3\_cut)$$
$$= 1 - \left\{1 - u_1.\left[1 - (1-u_2)(1-u_6)\right]\right\}.(1-u_3).$$

C. A WDM network with path protection

With path protection, a lightpath is determined to be in a failure state only if both the working path and backup path fail. Fig. 5 illustrates a fault tree model of a WDM network with a path protection applied to the lightpath 2. In this example, the backup lightpath is routed on links 2 and 6. The path protection introduces an additional AND gate located under a failure event of a lightpath being protected. This makes the probability of failure of the lightpath being protected lower.

IV. Event Tree

An event tree is another approach for evaluating network unavailability. The basic idea of an event tree is to enumerate all mutual exclusive network states, and then analyze the tree to determine the effect of each network state on the fault events of interest (e.g., top events of the fault tree model). The probability of the fault event of interest can be obtained by summing probabilities of all network states that cause an occurrence of the fault event. The number of network states is determined by the number of basic events in the fault tree

model of the network. For a tree with n basic events, each of which could be either in one of two states: occur or not occur, the number of all possible mutual exclusive states is equal to 2^n. If all basic events are independent of each other, the probability of occurrence of a network state is obtained by multiplying the appropriate probabilities of the basic events, (i.e., probability of occurrence or non-occurrence) constituting the network state.

In our WDM network example, as we confine the problem to a situation where cable cuts are considered as the only basic events, therefore there are 7 basic events, and 2^7 or 128 mutual exclusive network states. We use a binary matrix $\boldsymbol{FAIL} = \{fail_{sl}\}_{|S|\times|L|}$, as an equivalent matrix form of an event tree, to represent all network states information, where $fail_{sl}$ = 1 if a cable l (consequently a link l) is in a failure state under the network state s, and $fail_{sl}$ = 0 otherwise. A matrix ***FAIL*** for our sample WDM network is shown in Fig. 6. We also use a column matrix $\boldsymbol{stateprob} = \{stateprob_s\}_{|S|}$ to represent network state probabilities, where $stateprob_s$ is the occurrence probability of a network state s, which is calculated by

$$stateprob_s = \prod_{l\in L} u_l^{\,fail_{sl}} \left(1-u_l\right)^{1-fail_{sl}}. \tag{7}$$

The matrix ***stateprob*** for our sample WDM network is also shown in Fig. 6 (using CC = 450 km and MTTR = 24 hours for cable unavailability calculation).

For each network state, we can determine whether or not a lightpath is in a failure state by assigning corresponding event states (i.e., occur or not occur) under that network state to basic events, and evaluating the logic gates up the tree to determine a failure state of the lightpath under consideration. Since all network states are mutual exclusive, we can calculate the probability of a lightpath to be in a failure state by summing the probability of all network states that result in a failure of the lightpath being considered. Specifically,

$$\text{unavailability of LP}_i = \sum_{\substack{s\in \boldsymbol{S} \text{ that results} \\ \text{in a LP}_i \text{ failure}}} stateprob_s. \tag{8}$$

Base on an event tree approach, we propose a matrix-based formula for computing a network's ELT in bits per year for the case of no protection, link protection, and path protection, as shown in (9), (10), and (11) respectively. In these formulas, ∘ is a Hadamard (Schur) product, obtained by multiplying together corresponding elements in each matrix [14], and □ is a binary matrix multiplication operator which modifies the general addition in 1+1 = 2 to Boolean addition in 1+1 = 1 [15]. The notation used in (9)-(11) is explained in Table I.

FAIL =

$$\begin{bmatrix} 0&0&0&0&0&0&0\\ 1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 1&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ \vdots&&&&&&\\ 1&0&1&1&1&1&1\\ 0&1&1&1&1&1&1\\ 1&1&1&1&1&1&1 \end{bmatrix}$$

state =

$$\begin{bmatrix} 0.96167449\\ 0.00352585\\ 0.00411600\\ 0.00001509\\ 0.00589081\\ \vdots\\ 3.2131\times10^{-14}\\ 3.7509\times10^{-14}\\ 1.3752\times10^{-16} \end{bmatrix}$$

Fig. 6. Examples of network states and their probabilities of occurrence

One advantage of using an event tree method is that the difficulty in combining probabilities of dependent events, which exists when calculating occurrence probabilities in a fault tree method as shown in section III.B, can be avoided. In an event tree method, the probability calculation simply involves a summation of appropriated network states probabilities as in (8). Another advantage is that based on the event tree method, the network's ELT can be expressed as a linear function of the backup path routing (***Q*** and ***bp***). As a result, our investment strategy problem (discussed in section V.) can be formulated as a Mixed Integer Linear Programming (MILP) rather than a non-linear programming.

V. Investment Strategy

An investment strategy is used for determining which parts of the network, i.e., links or lightpaths, we should apply a protection technique for a given budget such that the network's ELT is minimized. In this section, we formulate the investment strategy as an optimization problem and present novel MILP formulations for both link protection and path protection cases. The formulation is based on an event tree approach, which allows the network's ELT to be expressed as a linear function of the decision variables. The MILP formulation for the link protection case is presented in (12)-(22). The decision variables of interest are binary variables bp_l, which determines whether of not there exists a backup path protecting link l, and q_{ij}, which determines backup routes. The objective function (12) is to minimize the network's ELT.

$$ELT_{no\_protection} = \boldsymbol{stateprob}^T \times \left(\boldsymbol{FAIL} \square\ \boldsymbol{P}^T\right) \times (365\times 24\times 3600\times \boldsymbol{m}) \tag{9}$$

$$ELT_{link\_protection} = \boldsymbol{stateprob}^T \times \left\{ \left\{ \boldsymbol{FAIL} \circ \left[\left(\boldsymbol{FAIL} \square\ \boldsymbol{Q}^T\right) + \left(\boldsymbol{1}_{|S|\times|L|} - \boldsymbol{1}_{|S|\times 1} \times \boldsymbol{bp}^T\right) \right] \right\} \square\ \boldsymbol{P}^T \right\} \times (365\times 24\times 3600\times \boldsymbol{m}) \tag{10}$$

$$ELT_{path\_protection} = \boldsymbol{stateprob}^T \times \left\{ \left(\boldsymbol{FAIL} \square\ \boldsymbol{P}^T\right) \circ \left[\left(\boldsymbol{FAIL} \square\ \boldsymbol{Q}^T\right) + \left(\boldsymbol{1}_{|S|\times|R|} - \boldsymbol{1}_{|S|\times 1} \times \boldsymbol{bp}^T\right) \right] \right\} \times (365\times 24\times 3600\times \boldsymbol{m}) \tag{11}$$

Constraint set (13) is flow balance constraints for backup paths. Constraints (14)-(19) are for calculating network's ELT as defined in (9). More specifically, constraint set (14) determines whether or not the backup path for link *i* is available under network state *s*. The backup path might not be available (i.e., bpf_{si} >0) for two reasons: either the backup path failure (i.e., $\sum_{j\in L} fail_{sj}.q_{ij} > 0$), or no link protection scheme implemented for that link (i.e., $1-bp_i$ >0). Constraint set (15) indicates that a link *l* fails under network state *s* if and only if both the working link fails and its backup path is not available under that network state. Constraint set (16) indicates that a lightpath *r* fails under network state *s* if and only if at least one of the links that it traverses fails. Constraint set (17) relates a variable lpf_{sr} to a binary variable $lpfbinary_{sr}$. Constraint set (18) calculates lightpath unavailability by summing state probabilities of all network states that cause a failure of that lightpath. And, constraint (19) calculates a network's ELT. Constraint (20) is a budget constraint which limits the total spare capacity investment.

$$\text{Objective: } \min_{bp,q} ELT \tag{12}$$

$$\text{s.t. } \sum_{j\in L} q_{ij}b_{nj} = b_{ni}bp_i \,(\text{mod } 2), \quad \forall i \in L,\ \forall n \in N \tag{13}$$

$$bpf_{si} = \sum_{j\in L} fail_{sj}q_{ij} + 1 - bp_i, \quad \forall s \in S, \forall i \in L \tag{14}$$

$$linkf_{sl} = fail_{sl}bpf_{sl}, \quad \forall s \in S, \forall l \in L \tag{15}$$

$$lpf_{sr} = \sum_{l\in L} linkf_{sl}\,p_{rl}, \quad \forall s \in S, \forall r \in R \tag{16}$$

$$lpfbinary_{sr}\mathrm{K} \geq lpf_{sr}, \quad \forall s \in S, \forall r \in R \tag{17}$$

$$ulp_r = \sum_{s\in S} lpfbinary_{sr}stateprob_s, \quad \forall r \in R \tag{18}$$

$$ELT = \sum_{r\in R} ulp_r\,(365\times 24\times 3600)m_r \tag{19}$$

$$\sum_{i\in L}\sum_{j\in L} c_j w_i q_{ij} \leq budget \tag{20}$$

$$q_{ij},\ bp_i : binary, \quad \forall i \in L,\ \forall j \in L \tag{21}$$

$$lpfbinary_{sr} : binary, \quad \forall s \in S, \forall r \in R \tag{22}$$

For the path protection case, the MILP formulation is presented in (23)-(33). The decision variables of interest are binary variables bp_r, which determines whether or not there exists a backup path protecting lightpath *r*, and q_{rl}, which determines backup routes. The objective function (23) is the same as before. Constraint set (24) is flow balance constraints for backup paths. Constraints (25)-(30) are for calculating network's ELT as defined in (10) for the path protection case. More specifically, constraint set (25) determines whether or not the backup path for lightpath *r* is available under network state *s*. The backup path might not be available (i.e., $bpf_{sr} > 0$) for two reasons: either the backup path failure (i.e., $\sum_{l\in L} fail_{sl}q_{rl}$ >0), or no path protection scheme implemented for that lightpath (i.e., $1-bp_r$ >0). Constraint set (26) indicates that the working path of lightpath *r* fails under network state *s* if and only if at least one of the links in the end-to-end path fails under that network state. Constraint set (27) indicates that a lightpath fails if and only if both its working path fails and its backup path is not available. Constraints (28)-(30) are the same as (17)-(19) in the link protection case. Constraint (31) is a budget constraint.

$$\text{Objective: } \min_{bp,q} ELT \tag{23}$$

$$\text{s.t. } \sum_{l\in L} q_{rl}b_{nl} = d_{rn}bp_r \,(\text{mod } 2), \quad \forall r \in R,\ \forall n \in N \tag{24}$$

$$bpf_{sr} = \sum_{l\in L} fail_{sl}q_{rl} + 1 - bp_r, \quad \forall s \in S, \forall r \in R \tag{25}$$

$$wpf_{sr} = \sum_{l\in L} fail_{sl}\,p_{rl}, \ \forall s \in S, \ \forall r \in R \tag{26}$$

$$lpf_{sr} = wpf_{sr}bpf_{sr}, \quad \forall s \in S, \forall r \in R \tag{27}$$

$$lpfbinary_{sr}\mathrm{K} \geq lpf_{sr}, \quad \forall s \in S, \forall r \in R \tag{28}$$

$$ulp_r = \sum_{s\in S} lpfbinary_{sr}stateprob_s, \quad \forall r \in R \tag{29}$$

$$ELT = \sum_{r\in R} ulp_r\,(365\times 24\times 3600)m_r \tag{30}$$

$$\sum_{r\in R}\sum_{l\in L} c_l q_{rl} m_r \leq budget \tag{31}$$

$$q_{rl},\ bp_r : binary, \quad \forall r \in R,\ \forall l \in L \tag{32}$$

$$lpfbinary_{sr} : binary, \quad \forall s \in S, \forall r \in R \tag{33}$$

Note that in the formulations above, the link-disjoint primary and backup paths are not constrained.

VI. Numerical results

The WDM network in Fig. 1 is used as a sample network for our proposed investment strategy. The length of each cable (km) is indicated in the figure. We assume that all cables have the same metric CC of 450 km and the same MTTR of 24 hours. There are 10 bi-directional lightpaths between all node pairs, each of which carries the same data rate of 10Gb/s. The lightpath routes are given as in Fig. 2. The cost of spare capacity on link *l*, c_l, is defined as 1 unit per 10Gb/s per 1000 km. The budget in term of spare capacity investment is given. We consider various values of the budget ranging from 0 to 30 units by 0.5 increments. The MILP problems for both link and path protection were solved using AMPL and the associated branch and bound solver in CPLEX. The results from the investment strategy in term of network's ELT for both the link protection case and the path protection case for different budget values are shown in Fig. 7. Also, Table II shows the results of which links and lightpaths are being protected for some specific budget values.

When the budget is not large enough to implement a protection mechanism (i.e., ≤1.5 units for a link protection, and ≤ 1 unit for a path protection), the network's ELT is

equal to 22,055,452 Gbits per year for both cases. For a budget of 2 units, link protection can be implemented in the network for the first time, in which link 6 is protected. Similarly, for a budget of 1.5 units, path protection can be applied for the first time, in which LP 2 is protected. Note that, the network's ELT is lower for a given budget with path protection than the link protection counterpart. This is mainly because the path protection scheme is more capacity efficient than the link protection scheme, and therefore cheaper to implement. For example, to protect all the links in the network, the link protection scheme requires 23.5 units of budget, which can reduce the network's ELT to 248,460 Gbits per year; whereas, the path protection scheme requires 19.5 units of budget to protect all the lightpaths in the network, and results in 270,061 Gbits per year.

An interesting observation is that even though all the links or all the lightpaths in the network are protected, the network's ELT still cannot be reduced to zero. This is due to the possible multiple-link failures which can bring down the working link/path and the backup path at the same time, resulting in a traffic loss. The minimum network's ELT that can be achieved by the link protection scheme is lower than that by the path protection scheme. The reason for this is that the link protection scheme has a shorter working path, strictly at one-hop length, i.e., a working link, and typically has a shorter backup path, thus it is less vulnerable to the multiple-links failures that can damage both working and backup paths at the same time. Also note that the investment strategy result such as in Fig. 7 also helps transport network providers to determine how much investment budget is required to achieve a desired level of ELT for each protection scheme.

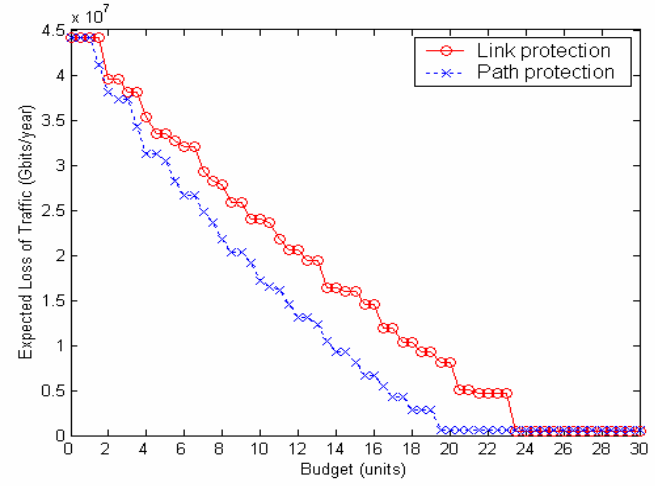

Fig. 7. ELT versus Budget

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

Budget	Link Protection	Path Protection
2	Link 6	LP 2
2.5	Link 6	LP 6
3	Link 4	LP 6
7	Link 4, 5, and 6	LP 2, 3, and 6
8	Link 3, 5, and 6	LP 2, 3, 6, and 7
19.5	Link 1, 2, 4, 5, 6 and 7	All LPs
23.5	All links	All LPs

VII. CONCLUSION

This paper presents an investment strategy to reduce the risk associated with failures in WDM networks. The investment strategy determines how to allocate a fixed budget for implementing survivability techniques in different parts of the network such that the Expected Loss of Traffic (ELT) is minimized. Based on an event tree unavailability model approach, we propose a novel Mixed Integer Linear Programming (MILP) optimization problem formulation for the investment strategy problem. Formulations for dedicated link protection and dedicated lightpath protection are given. Numerical results illustrating the investment strategy for both link and path protection are presented. Future work looks at the scalability of the approach and incorporating additional threats/risk into the design model

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

[6] Pin-Han Ho, H.T. Mouftah, "Shared protection in mesh WDM networks", IEEE Communications Magazine, vol. 42, issue 1, Jan 2004, pp. 70-76.

[7] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, Part II – Restoration," in *Proc. ICC*, Vancouver, BC, Canada, Jun. 1999.

[8] Yu Liu, D. Tipper, and P. Siripongwutikorn, ``Approximating Optimal Spare Capacity Allocation by Successive Survivable Routing," *ACM/IEEE Transactions on Networking*, Vol. 13., No. 1, pp. 198-211, Feb., 2005

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

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

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

[12] R. Billinton and R. N. Allan, *Reliability Evaluation of Engineering Systems*, 2 ed: Plenum Press, 1992.

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

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