An efficient hybrid protection scheme with shared/dedicated backup paths on elastic optical networks

Nogbou G. Anoh\(^{a,b,c,*}\), Michel Babri\(^{d}\), Ahmed D. Kora\(^{c,d}\), Roger M. Faye\(^{c}\), Boko Aka\(^{a}\), Claude Lishou\(^{c}\)

\(^{a}\) LMI, Université Nangui Abrogoua, Abidjan, Cote d’Ivoire
\(^{b}\) LTI, Institut National Polytechnique Félix Houphouët Boigny, Abidjan, Cote d’Ivoire
\(^{c}\) CIETI, Ecole Supérieure Polytechnique, Université Cheikh Anta Diop, Dakar, Senegal
\(^{d}\) Ecole Supérieure Multinationale des Télécommunications, Dakar, Senegal

ABSTRACT

Fast recovery and minimum utilization of resources are the two main criteria for determining the protection scheme quality. We address the problem of providing a hybrid protection approach on elastic optical networks under contiguity and continuity of available spectrum constraints. Two main hypotheses are used in this paper for backup paths computation. In the first case, it is assumed that backup paths resources are dedicated. In the second case, the assumption is that backup paths resources are available shared resources. The objective of the study is to minimize spectrum utilization to reduce blocking probability on a network. For this purpose, an efficient survivable Hybrid Protection Lightpath (HybPL) algorithm is proposed for providing shared or dedicated backup path protection based on the efficient energy calculation and resource availability. Traditional First-Fit and Best-Fit schemes are employed to search and assign the available spectrum resources. The simulation results show that HybPL presents better performance in terms of blocking probability, compared with the Minimum Resources Utilization Dedicated Protection (MRU-DP) algorithm which offers better performance than the Dedicated Protection (DP) algorithm.

1. Introduction

New services such as video-conferencing, online games, telemedicine, social networks and peer to peer traffic constitute most of the Internet traffic today. The development of such services requires new modulation formats in telecommunication networks. Current optical transport networks are based on Wavelength Division Multiplexing (WDM) technologies. In these networks, the total optical spectrum is divided into a set of wavelength channels with a fixed frequency grid defined by the International Telecommunication Union—Telecommunication (ITU-T). The introduction of flexibility in bandwidth allocation and high efficiency of spectrum utilization with the advent of elastic optical networks named Spectrum-Sliced Elastic optical path network (SLICE) [1–5], have revolutionized optical transport networks. SLICE architecture employs Optical-Orthogonal Frequency Division Multiplexing technology (O-OFDM) to allocate a variable number of spectrum blocks for variable-bandwidth channels in order to increase spectral efficiency [6]. Compared with conventional WDM networks, SLICE is able to provide arbitrary contiguous spectrum slots thanks to its flexible allocation of spectrum resources. These networks are also confronted with networks connectivity problems with nodes, links, or channels. For some critical applications, this problem disrupts transactions, causing enormous data loss or damage to network service users. Survivability of such optical systems is implemented with two different approaches. These approaches are considered as complementary: protection [7] and restoration [8]. Restoration is a reactive scheme in which a backup path is determined and established after a failure occurs on the primary path. However, protection is a proactive scheme in which the backup path is pre-reserved when the primary path is found to establish a connection request on the network.

The protection problem remains a very important research domain in SLICE networks including path-based protection and link-based protection. In link based protection, for each primary path link, a backup path is determined and established after a failure occurs on the primary path. However, protection is a proactive scheme in which the backup path is pre-reserved when the primary path is found to establish a connection request on the network.
and path-based protection. In recent years, the question of Routing and Spectrum Assignment (RSA) has been the focus of extensive research efforts in elastic optical networks [13–17]. The different variants of the RSA problem are classified into two approaches, dynamic and static RSA. SLICE networks introduce some novelties in survivability schemes in order to solve protection or restoration problems [18–23]. In [18], the authors presented a survivable algorithm, named as Dynamic Load Balancing Shared-Path Protection (DLBSPP). One of the key ideas of the DLBSPP algorithm is to consider the links with many available contiguous resources in path computation. A link cost function for primary path computation has been defined in this paper combining the number of free frequency slots on each link and the basic cost of a link. Similarly, for shared backup path computation, the link cost function is defined with the number of free frequency slots, and the number of backup frequency slots consumed on each backup link and the basic cost of a link. To compute the shortest path, the Dijkstra algorithm is adopted for each connection request. For spectrum assignment, the traditional assignment schemes First-Fit and Random-Fit are used under spectral continuity and contiguous frequency constraints. DLBSPP adopts a restoration strategy to recover from the simultaneous failure of multiple links. The key idea of the restoration scheme is the affected traffic that will be classified by priority. In [19], the authors formulated an off-line genetic algorithm for solving the routing and spectrum allocation problem with dedicated path protection under static connection requests and subject to a single-link failure. The primary path and backup path are computed subject to the following constraints: spectrum continuity, spectrum continuity and same subset of slices for both paths where the objective is to minimize the spectral width required on the network. In [20], the same problem as in the [19] was formulated as an Integer Linear Programming formulation. Taboo search algorithms have been developed to provide an optimal solution to the previous algorithm for the routing problem. Three different methods are proposed to solve the problem of free resources and working-backup paths allocation: First Assign, Random and Sorted allocation. In First Assign (FA) allocation, for each demand, the first candidate working-backup path pair and their candidate channel are used for allocation. However, the candidate channel is the one which has the free spectrum with the lowest index. Random allocation is similar to FA allocation. However, candidate working-backup path pair is chosen randomly. In sorted allocation, the demands are sorted according to the decreasing value of their sizes. The candidate working-backup path pair is the one which has the free spectrum channel with the lowest index. In [21], the authors proposed a heuristic algorithm for protection schemes in different networks technologies (WDM and SLICE) and compared them in terms of energy efficiency and cost under dedicated (1+1 or 1:1) and Shared Protection (SP). The Optical Cross-Connect (OXC) power consumption is defined from each node degree and add/drop degree. Each path metric candidate based on the end-to-end lightpath power consumption is calculated as in [16], considering the transponder power consumption and approximate consumption from the EDFA amplifiers and Optical Cross-Connects (OXC) along the path. For an established connection, the total power consumption metric is calculated with the contribution of working and backup paths power metric. The working-backup path combination which has the most efficient energy is chosen for transmission and protection. The candidate pair of working-backup paths for each connection was computed using the k-shortest path algorithm. The author in [22], developed an integer linear programming model considering shared backup path protection in comparison with dedicated (1+1) path protection for elastic optical networks. In this protection technique, two transponder models were considered: i) full tunable transponder and ii) non-tunable transponder. With the non-tunable transponder, the same set of contiguous frequency slots is required to be used for both working and backup paths. In this case, if the primary path uses slots 5, 6 and 7, its backup path also uses slots 5, 6 and 7. Now with the full tunable transponder, working and backup paths can use different sets of contiguous frequency slots. For example, if the primary path uses slots 5, 6 and 7, its backup path can use slots 1, 2, 3 and 4. When failures occur on the network, a Bandwidth Squeezing Restoration (BSR) scheme is applied to obtain maximum restoration levels for the affected connections. The static survivable p-cycle RSA problem was studied in [23]. The authors developed an Integer Linear Programming formulation to solve the SC-RSA problem. As the ILP model cannot be solved in real time for a large scale network, the authors proposed a heuristic algorithm called Elastic p-cycle protection (ECP) to tolerate the single-fiber link failure, to minimize the maximum number of sub-channels on a fiber.

However, all protection schemes developed consider that backup path resources are being shared or dedicated. In this paper a hybrid protection scheme with shared and dedicated backup paths resources is proposed. The objective of this study is to minimize spectrum utilization to reduce blocking probability.

The rest of the present study is organized as follows. In Section 2, we describe: i) the network model, and ii) the resource allocation model. Section 3 describes our hybrid protection algorithm which employs shared and dedicated backup paths. Section 4 shows the simulation and analysis. The paper is concluded in Section 5.

2. Problem statement

2.1. Network model

The network topology is defined as a graph $G = (N, L, fs, C)$, where

- $N$ is the set of bandwidth variable nodes;
- $L = \{(i, j) \mid i, j \in N \land i \neq j\}$ is the set of fiber links;
- $fs = \{f_1, f_2, \ldots, f_n\}$ is the set of frequency slots of each fiber link;
- $CR = \{c_{11}, c_{12}, \ldots, c_{1m}\}$ is the set of connection requests on the network.

Each connection request $id$ is associated with a bit rate $w_{id}(Gb/s)$ with $1 \leq id \leq n$ which corresponds to a specific number of frequency slots. A connection $c_{id}$ between source node $s_d$ and destination node $d_d$ is represented by expression $c_{id} = (s_{id}, d_{id}, w_{id})$.

Frequency slot $k$ on fiber link $(i, j)$ can be in one of the following cases:

$f_{k}^{(i,j)} = \begin{cases} f_k & \text{if slot } k \text{ is not used on link} (i, j) \\ 0 & \text{if slot } k \text{ is used as dedicated on link} (i, j) \\ -1 & \text{if slot } k \text{ is used as backup on link} (i, j) \end{cases}$

The number of frequency slots of a connection $c_{id}$ on path $P$, $Nf_{is}(P(c_{id}))$, is calculated as in [24]:

$Nf_{is}(P(c_{id})) = \left\lfloor \frac{w_{id}}{M(P(c_{id})) \times w_{slot}} \right\rfloor + Ngb$  \hspace{1cm} (1)

where $w_{slot}$ is a signal speed for one frequency slot, $M(P(c_{id}))$ corresponds to a modulation format of connection $c_{id}$ and its transparent reach defined in [24] and $Ngb$ is the number of guard bands. The symbol $\left\lfloor \cdot \right\rfloor$ represents rounding up to the higher integer. To compute primary and backup paths, contiguity and continuity constraints are used.

For each modulation format, the maximum optical signal reach with an acceptable quality without needing to regenerate the signal is represented in Table 1, where the propagation speed of each frequency slot and the power consumed by each frequency slot are represented. Each line of the table shows the ability of a frequency slot and the maximum distance without regeneration of an optical signal for each modulation format.

The modulation format for each connection request is determined with its path length as follows:

$M(P(c_{id})) = \text{Modform}(\sum_{i,j \in P} l_{i,j})$ where Modform(.) returns the appro-
private number of spectrum efficiency corresponding to the modulation format between 1 and 6 that a transmission distance can support, and \( l_{ij} \) is the length of link \((i, j)\) on path \( P \). For BPSK, QPSK, 8QAM, 16QAM, 32QAM, 64QAM, the corresponding numbers returned by \( \text{Modform}() \) are 1, 2, 3, 4, 5 and 6 bits/s/Hz, respectively.

### 2.1.1. Power consumption cost of lightpath

The optical path power consumption cost is calculated considering the cost of: i) the power consumption of a single subcarrier, ii) the power consumption of a EDFA amplifier and iii) the power consumption of an optical cross-connect along the path. The cost of the path \( P \) power consumption for connection \( c_{rd} \) is defined by the following expression using (1) and based on the power consumption metric in [16]:

\[
\text{CostPC}(c_{rd}) = \left( \text{Nfs}(c_{rd}) - Ngb \right) \times \text{CostSABC} \times \text{PCSABC} + \sum_{(i,j) \in P} \text{Costamp} \times \rho_{ij} \times \text{PCamp} + \sum_{\text{OXC} \in P} \text{CostOXC} \times \text{POXC}
\]  

(2)

where

- \( l_{ij} \) is the length of link \((i, j)\) on path \( P \);
- \( d_{amp} \) is the amplification distance;
- \( \rho_{ij} = \begin{cases} 0 & \text{if } \frac{l_{ij}}{d_{amp}} \leq 1 \\ \frac{l_{ij}}{d_{amp}} & \text{otherwise} \end{cases} \)
- \( PC_{amp} \) is the power consumption of a single EDFA amplifier;
- \( \text{Costamp} \) is the cost of a single amplifier power consumption;
- \( PC_{SABC} \) is the power consumption of a single subcarrier for corresponding modulation format;
- \( \text{CostSABC} \) is the cost of a single subcarrier power consumption;
- \( PC_{OXC} \) is the cost of a single optical cross-connect power consumption;
- \( \text{CostOXC} \) is a single optical cross-connect power consumption;
- TotalFS is a fiber link capacity;
- \( \lfloor . \rfloor \) represents rounding to the lower integer.

A longer optical path generally requires more slots, amplifiers and nodes. It will consume more energy than a shorter path with fewer nodes, amplifiers and slots. Thereby, the expression (2) will be used to select the paths which consume less energy during the routing phase.

### 2.1.2. Resources availability cost on lightpath

Expression (3) makes it possible to choose the appropriate path which has available resources to establish the request. The path which has minimum spectrum blocks and a lot of available resources is chosen by using the following expression:

\[
\text{CostRss}(P(c_{rd})) = \begin{cases} \frac{1}{\eta} \times \frac{1}{\sum_{b \in B(P)} T_b} \times \sum_{(i,j) \in P} \phi_{ij} \times [\text{Nfs}(P(c_{rd})) - \theta_{ij}] & \text{if } \eta \neq 0 \land \exists b \in B(P), T_b \geq Nfs(P) \\ \infty & \text{if } \eta = 0 \end{cases}
\]

(3)

where

- \( B(P) \) is the set of available spectrum blocks of path \( P \);
- \( b \) is an available spectrum block on path \( P \);
- \( T_b \) is the size of spectrum block \( b \);
- \( \eta \) is the number of available spectrum blocks on the path \( P \).

#### 2.1.3. Path cost

The metric for calculating the cost of a path is defined according to multi-criteria conventional optimization methods from (2) and (3) as follows:

\[
\text{Cost}(P(c_{rd})) = \begin{cases} \text{CostPC}(P(c_{rd})) + \text{CostRss}(P(c_{rd})) & \text{if } \eta \neq 0 \\ \infty & \text{if } \eta = 0 \end{cases}
\]

(4)

### 2.2. Resource allocation model

To establish a connection request \( c_{rd} \), the set of k-shortest paths are determined between the source and the destination. The cost of each path is calculated with (4) when there are available resources for satisfying a connection request. To determine the primary path \( P_{c} \) of a connection request, the two paths with minimum cost \( (P_{c}(c_{rd}) \text{ and } P_{b}(c_{rd})) \) with \( i \neq j \in \mathbb{N} \) with available resources must be selected to determine the primary path of the connection request \( c_{rd} \). For each path \( P_{c}(c_{rd}) \text{ and } P_{b}(c_{rd}) \), the k-shortest link-disjoint backup paths \( P_{b} \) are determined. The cost of each backup path is calculated and then the backup path with the minimum cost is selected for every primary path. If we assume that \( P_{c}(c_{rd}) \text{ and } P_{b}(c_{rd}) \) with \( i \neq j \in \mathbb{N} \) are backup paths, the path pair \( (P_{c}(c_{rd}), P_{b}(c_{rd})) \) or \( (P_{b}(c_{rd}), P_{b}(c_{rd})) \) which minimizes the number of resources used is selected for the establishment and protection of the connection request. The conventional First-Fit approach is used for resource allocation in the present approach. When there are no resources determined for a backup or primary path the connection request is blocked.

For each backup frequency slot, the maximum number of connections that are used is fixed by a threshold. To determine the utilization cost of each frequency slot of a backup path \( P_{b}(c_{rd}) \), the following expression is defined:

\[
\text{costrssat}(\phi_{k,m}) = \sum_{P_b \in PB} \eta_{k,P_b}^{(m, n)}
\]

(5)

where

- \( \eta_{(n,m)}^{(k,P_b)} = \begin{cases} 1 & \text{if slot } k \text{ is used on link } (n, m) \text{ by the path } P_b \\ 0 & \text{otherwise} \end{cases} \)
- \( PB \) is the set of paths which uses slot \( k \) on link \((n, m)\).

The total cost of the resources used by a primary-backup path pair is defined by the following expression:

\[
\text{CTRss}(P_{c}(c_{rd}), P_{b}(c_{rd})) = h(c_{rd}) \times \text{Cost}(P_{c}(c_{rd})) + \sum_{(i,j) \in P_{b}} \phi_{ij} \times [\text{Nfs}(P_{b}(c_{rd})) - \theta_{ij}] + \sum_{(i,j) \in P_{c}} \phi_{ij} \times [\text{Nfs}(P_{c}(c_{rd})) - \theta_{ij}]
\]

(6)

where

- \( h(c_{rd}) \) returns the number of primary path links.
- \( \phi_{ij} = \begin{cases} 0 & \text{if resources are shared on link } (i, j) \\ 1 & \text{otherwise} \end{cases} \)
- \( \theta_{ij} = \begin{cases} 0 & \text{if backup resources are dedicated on link } (i, j) \\ c & \text{if resources are shared on link } (i, j) \end{cases} \)
Two possibilities are considered, in the case where the backup resources do not have a utilization threshold and the case where there is a threshold for resource utilization.

3. Hybrid protection algorithm

To satisfy a set of connection requests that enters the network at a given time, the hybrid protection algorithm sorts connection requests by decreasing order (higher demand first) and applications are processed one by one. To establish a connection between a source and a destination, all K-shortest primary paths (in terms of distance) are determined. When the primary paths with available resources are obtained, we select two paths with the minimum cost. For each primary path, we determine their corresponding candidate backup paths (K-shortest link-disjoint paths). When the backup paths with available spectrum are obtained, we determine the pair of primary-backup paths which have available resources. Next, the pair of primary-backup paths which minimize resource utilization for each connection request is chosen. In our study, for resources allocation, we assume that primary path and backup path use different frequency slots. The set of connections requests are generated randomly (for a random source and destination), as shown in Fig. 1.

The flowchart of the protection approach is presented by the following figure:

Phase 1 is used to determine the set of primary paths for the connection requests. If Phase 1 makes it possible to find primary paths with enough resources, phase 2 is responsible for determining the backup paths for each connection to be established on the network.

The procedure for determining backup resources is defined as follows:

**PROCEDURE 1 - Determination of backup resources**
**Input:** backup path \( P_b \)
**Output:** backup resources of \( P_b \)

1. **IF** dedicated backup path **THEN**
   - DETERMINE appropriate modulation format
   - DETERMINE available free slot blocks of backup path \( P_b \)
2. **ELSE**
   - DETERMINE appropriate modulation format
   - DETERMINE available non-free slot blocks of backup path \( P_b \)
3. **ENDIF**

4. **IF** slot blocks are found **THEN**
   - **FOR** each slot block \( b_i \) of backup path \( P_b \) which is found **DO**
     - **IF** \( |b_i| \geq Nfs(P_b) \) **THEN**
       - **SAVE** block \( b_i \) in BACKUPBLOCS
       - **BREAK**
   - **ENDFOR**

5. **ENDIF**

6. **IF** BACKUPBLOCS is not empty **THEN**
   - **EXTRACT** the first \( Nfs \) slots of backup block
   - **SAVE** necessary resources for request
   - **ENDIF**

**ENDIF**

The determination of backup paths is detailed in the following procedure:

**PROCEDURE 2 – Determination of backup paths**
**Input:** path \( P_r \)
**Output:** BACKUPPATHS \((c_{rid})\)

1. **IF** backup paths found **THEN**
   - **FOR** each path \( P_r \) found **DO**
     - **CALCULATE** total cost of resources for Path pair \( (P_r, P_b) \) with (5) and choose pair with minimum cost
     - **UPDATE** performance measurement
   - **ELSE**
     - Request is BLOCKED
     - **UPDATE** information of request \( c_{rid} \)
   - **ENDIF**

2. **ENDFOR**

3. **ELSE** request is BLOCKED
   - **ENDIF**

4. **ENDFOR**

5. **REMOVE** request \( c_{rid} \)

**ENDIF**

**ENDWHILE**

4. Simulation results and analysis

The NSFNET (National Science Foundation network) topology (nodes 14, links 22) is used, as shown in Fig. 2, to evaluate the performance of the network using the protection algorithm proposed for elastic optical networks. It is assumed that each link is bidirectional. The bandwidth required for each connection request is a function of the modulation format which is proportional to the transmission length and the bandwidth of one subcarrier and the connection speed required.
Fig. 1. The flowchart of the protection approach.

Fig. 2. NSFNET topology.
In the first scenario: i) 250 frequency slots per link, ii) a guard band fixed to 1, iii) primary and backup paths are determined by a k-shortest path algorithm, iv) the required bandwidth of each demand varies between 30 and 150 Gb/s.

The performance indicators used are the blocking probability and the total number of resources used. The blocking probability is the ratio between the number of blocked requests and the total number of connection requests on the network. The number of resources used for a connection is the total number of frequency slots used by its primary path and backup path, as determined by (6). To evaluate our approach, Heuristic algorithm for routing and resource allocation with Protection (DP) [21] and our HybPL, MRU-DP approaches were implemented with Java in Eclipse under Windows 10. Simulation is run on Intel core i3 CPU, 2.4 GHz with 4 GB of RAM. In the first case, the connections requests are not generated randomly, we have chosen fifty (55) requests with 80 slots per link and the simulation results are presented in Fig. 3. With MRU-DP, and HybPL, more connections are established than with DP; which justifies that the blocking probability is lower with MRU-DP and HybPL than with DP.

Considering the threshold of backup resource utilization is equal to 2, 4 and 6, we notice that when the threshold is low, the blocking probability is high (Fig. 4) and therefore the number of resources used in the network increases (Fig. 5).

In Fig. 6, we observe that the blocking probability of the HybPL algorithm is lower than the MRU-DP and DP algorithms when the link capacity increases in the network. And MRU-DP also establishes more connections than DP.

In the second case of the simulation, each step is repeated two thousand times. Connections requests are generated randomly in each step. We assume that in this simulation, when the request is accepted, its light path remains indefinitely on the network. Two resources allocation approaches were used in this simulation: First-Fit and Best-Fit approaches. In the first part of the simulation, we analyzed the impact of the k-shortest paths number on the blocking probability. With Dedicated Protection DP [21] and MRU-DP protection approaches when the k-shortest paths increases, the average blocking probability is practically the same as shown in Fig. 7. However, the average blocking probability increases when the number of connections increases in the network with an error rate of 0.002.
In the hybrid protection approach (HybPL), the $k$-shortest paths increase, the blocking probability decreases as shown in Fig. 8 contrary to dedicated protection approaches. In this simulation part, we assume that $k$ is equal to 2 because it is when $k=2$, that the proposed hybrid approach (HybPL) has a higher blocking probability. The hybrid approach has better performance compared to the dedicated approaches MRU-DP (Minimum Resources Utilization Dedicated Protection) and DP when we apply the first-fit technique or best-fit technique as shown in Figs. 9 and 10. When comparing the DP and DP-MRU approaches, it appears that MRU-DP has a low blocking probability compared to DP. In fact, in the DP algorithm, where the $k$-shortest primary paths are determined, automatically $k$-shortest backup paths (disjoint of $k$-shortest primary paths) are determined.

In MRU-DP, for each primary path, $k$-shortest disjoint backup paths are determined. This increases the possibility of finding a backup path for establishing a request. In addition to these results, we compared the hybrid approach to fixed routing SBPP (Shared Backup Path Protection) approach [26] and the results show that the HybPL approach presents better performance than SBPP, as shown in Fig. 11.

5. Conclusions

In this paper, the focus was put on the protection problem in elastic optical networks with the objectives of minimizing the resources used on the network with a low blocking probability. Two approaches were proposed for connection protection: the first one with dedicated and the other one with sharing backup resource. For primary and backup path computation, paths that use less power consumption and have more resources were selected. For the resource allocation, the traditional mechanisms "First Fit or Best Fit" were used to identify and select the available resources under the constraint of spectrum contiguity and continuity. In addition, the blocking probability of HybPL was compared to the Shared Backup Path Protection SBPP-FR approach. The network performance was evaluated with the present HybPL, MRU-DP and the DP algorithms. The evaluation results show that our HybPL approach provides a lower blocking probability and better resource utilization on the network.

References


