IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 13, 2019, accepted January 1, 2020, date of publication January 20, 2020, date of current version February 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2967751

A Fault-Tolerance Solution to Any Set of Failure Scenarios on Dynamic WDM Optical Networks With Wavelength Continuity Constraints

NICOLÁS JARA[1], HERMANN PEMPELFORT[1], GERARDO RUBINO[2], AND REINALDO VALLEJOS[1]

[1]Department of Electronics, Universidad Técnica Federico Santa María, Valparaíso 2391206, Chile
[2]National Institute for Research in Digital Science and Technology (INRIA), 35042 Rennes, France

Corresponding author: Nicolás Jara (nicolas.jara@usm.cl)

This work was supported in part by FONDEF ID14I20129, CONICYT, in part by STICAMSUD 19STIC-01 ACCON and in part by INRIA.

ABSTRACT Survivability of internet services is a significant and crucial challenge in designing optical networks. A robust infrastructure and transmission protocols are needed to maintain communication, despite the existence of one or more failed components on the system. Here, we present a generalized approach to tolerate any set of failure scenarios to the extent network users can still communicate with the remaining components, where a scenario is an arbitrary set of links in a non-operational state. We propose a joint solution to assess the survivability problem. The issues to be solve simultaneously are as follows: the set of primary routes, a collection of alternate routes associated with each failure scenario, and the capacity required on the network to allow communication between all users, in spite of any considered failure scenario, while satisfying for each user a specific predefined quality of service threshold, defined in the Service Level Agreement (SLA). Numerical results show that the proposed approach not only enjoys the advantages of low complexity and ease of implementation, but it is also able to achieve significant resource savings compared to existing methods. The savings are higher than 30% on single link failures and more than 100% on two simultaneous link failures cases or in more complex failure scenarios.

INDEX TERMS Network capacity, optical networks, quality of service, routing, survivability.

I. INTRODUCTION

A remarkable issue to be solved when designing WDM (Wavelength Division Multiplexing) optical networks is to ensure that the network will still be able to provide transmission services after the failure of one or more of its links. The solution to this problem consists in providing the necessary infrastructure to rapidly re-establish communications between all source-destination pair of nodes affected by these link failures. This type of mechanism is known as ''Fault Tolerance''.

The frequency of link failure occurrences is significant. For instance, [1], [2] report measures that, for example, in a 26,000 km-long network such as NSFNet [3], there is an average of one fiber cut every 5 days. This failure frequency explains why failures on links may significantly impact the performance of optical networks. Moreover, the frequency with which two simultaneous links failures occur is high enough to be considered in the design process. In fact, Schupke [2] reported that in a network like NSFNet there is a downtime of about 24 hours per year, on average, which in addition to the high transmission rate of this kind of networks, means an unacceptable data loss.

The previous elements justify the need to provide an efficient methodology for multiple fault tolerance, which should ensure (with a certain probabilistic guarantee) successful communications among all network users, despite the occurrence of failures in some of the links, and at the lowest possible cost regarding the network infrastructure. Note that node failure may be modeled as the failure of all the links connected to the node, so the general problem can be modeled as a set of link failures only.

The fault tolerance methods proposed so far have been generally devoted to finding alternative paths considering single link failures (consider a bidirectional link), affecting all the users with routes passing through

The associate editor coordinating the review of this manuscript and approving it for publication was Yi Zhang.

the failed link in both directions. Then, the number of wavelengths in the network is dimensioned to tolerate this situation [2], [4]–[8]. However, as already pointed out, the probability of occurrence of two or more simultaneous failures is high enough, meaning that it is necessary to consider this kind of event in the design process. Some studies have focused on this 2-failures scenario [9]–[12]. Also, some studies have considered more complex cases of failures, such as Disaster risk constraints and Shared-Risk-Group scenarios. Disaster risk constraints [13]–[15] considers the possible service disruptions as a consequence of a natural disaster or a targeted attack, in which case the failures affect various links simultaneously. The case of Shared-Risk-Group (SRG) [16], [17] considers cases where some fibers are placed physically together, even if they are connecting different optical nodes. This situation makes those fibers liable to the same physical event since they can be cut together at the same time.

The previous discussion supports the need to produce an adequate strategy concerning multiple fault tolerance scenarios, which should ensure (with a certain probabilistic guarantee) successful communications among all network users, notwithstanding the existence of failures in some of the links, with the lowest cost regarding the network infrastructure.

In this paper we propose a new fault-tolerance scheme, which we call the ''Cheapest Shared Alternate Paths'' method (*CSAP*). In our approach, we go one step further concerning previous works, and we take into account the case of arbitrary sets of links failures scenarios, where a failure scenario is composed of a set of links in failure state. This means that we solve the fault-tolerance problem in a very general case.

The method also evaluates the number of wavelengths for each link of the network, ensuring that the blocking probability of any user request is lower than a given corresponding predefined threshold β_c, despite the possible occurrence of those simultaneous link failures. This dimensioning problem is specially tricky when the network has wavelength continuity constraint (the case analyzed here). This constraint means that when a user wants to transmit, the same wavelength has to be available on every link belonging to the given user route (end-to-end). The value of β_c is defined on the Service Level Agreement (SLA), signed by the service providers and their clients, which defines the minimum quality of service (QoS) acceptable for each user, measured here as a probabilistic guarantee. The definition of these bounds is obtained considering objective criteria, such as taking into account different quality of service requirements [18]–[20] or considering subjective decisions, for instance network scalability requirements. Based on these QoS agreements, engineers must design the network fulfilling said QoS requirements. Thus, we assume that the β_c values are given and acknowledged by the users and the network service providers.

The remainder of this paper is as follows. In Section II, we summarize the state of art of fault tolerance strategies. In Section III, we present the proposed method. In Section IV we compare some results obtained by the proposed algorithm with those obtained with the current best techniques in a set of different scenarios. Finally, some conclusions of our work are given in Section V.

II. STATE OF ART

Next, we briefly describe the most common methods currently used to provide fault tolerance in optical networks with wavelength continuity constraints.

One of the most frequent ways used to address single and double fault tolerance, called ''*1+1*'', can be found in [5], [21], [22]. In this technique, a secondary route is associated with each primary one (with the restriction that they do not share any link), and the information is transmitted simultaneously through both of them, avoiding restoration delays in case of a failure. To dimension the number of wavelengths of each link -a task usually done by simulation-, each secondary route is considered as just another network route with a load equal to the load of the corresponding primary one. The 1+1 method is also scalable to provide tolerance to $K \geq 1$ simultaneous failures. In this case, for each user, $K + 1$ supplementary disjoint routes must be found, one as the primary route and the remaining K as secondary routes. Observe that a necessary and sufficient condition that allows this scheme to work is that the graph defined by the set of nodes and links is $(K + 1)$-connected.

Another fault tolerance strategy is known as ''*Shared Path Protection*'' (SPP) [12], [23]–[25]. In this scheme, the extra resources (wavelengths) assigned to the secondary routes can be shared by different users, and are assigned only when a fault occurs. The SPP can be executed in two different ways. The first one consists of running the algorithm off-line, which means that the routes are calculated prior to the operation of the network (off-line SPP). The second way is the on-line implementation (on-line SPP). In this last case, the primary routes are computed before the network is operating, however, it must be executed again every time that one or more simultaneous failures occur, to compute alternate paths to the affected communications. For this reason, it is said that this is a proactive and reactive approach at the same time.

In [9], [10], [26]–[28] another method of fault tolerance called ''*p-cycle*'' is discussed, which provides survivability through fixed secondary routes that have a cyclic form. These cyclic routes are shared between several primary routes. One problem associated with this approach is that its applicability is very dependent on the size of the network, because it may introduce an excessive additional delay for a user in protection state on large networks. Also, to perform multiple fault tolerance, it requires a large number of cycles (e.g., hundreds of cycles for the 11 nodes pan-European COST 239 network [26]), which is impractical from various points of view.

III. THE PROPOSED FAULT TOLERANCE METHOD

We present first the model used and the associated assumptions. Then, we describe the main sub-procedures

necessary to our technique. Last, we present the algorithm we propose to solve the fault-tolerance problem.

A. MODEL

The network topology is represented by a graph $\mathcal{G} = (\mathcal{N}, \mathcal{L})$, where $\mathcal{N}$ is the set of network nodes or vertices and $\mathcal{L}$ is the set of unidirectional links (the arcs in $\mathcal{G}$), with respective cardinalities $|\mathcal{N}| = N$ and $|\mathcal{L}| = L$. The set of users $\mathcal{X}$, with cardinality $|\mathcal{X}| = X$, is composed by all the source-destination pairs with communication between them.

We use an ON-OFF model (as in [29]–[32]) to represent the traffic between a given source-destination pair. Consider user c. During any of its ON periods, whose average length is $t_{ON\,c}$, the source transmits at a constant rate (which is the rate associated with the wavelength, that is, a technological constant in our model). During an OFF period, with average length $t_{OFF\,c}$, the source refrains from transmitting data. Observe that we address here the general case where the load can be different for each user, the so-called heterogeneous situation.

The used technology determines the constant transmission rate during the ON periods, but to simplify the presentation, it is our rate unity. Consequently, the traffic load of user c, denoted by ϱ_c, is given by:

$$\varrho_c = \frac{t_{ON\,c}}{t_{ON\,c} + t_{OFF\,c}}. \tag{1}$$

Remark that we model the users traffic load which in turn together with the users path leads to the links traffic load.

Let $\mathcal{R} = \{r_c \mid c \in \mathcal{X}\}$ be the set of routes that enable communications among the different users, where r_c is the route associated with user $c \in \mathcal{X}$. The set $\mathcal{R}$ is known as the set of *primary* routes, since this set alone does not offer any fault tolerance to the possible failure of network links.

Let $\mathcal{W} = \{W_\ell \mid \ell \in \mathcal{L}\}$ be the set containing the number of wavelengths of each unidirectional network link, where W_ℓ, with $\ell \in \mathcal{L}$, is the number of wavelengths on link ℓ. The value W_ℓ, for every $\ell \in \mathcal{L}$, must be evaluated so that the blocking probability BP_c of each user $c \in \mathcal{X}$ is less than or equal to the given pre-specified threshold β_c, and the total number of available network wavelengths is as small as possible (saving resources).

Remark that the pre-defined threshold value β_c can be different for each network user, which means that we treat the general case where there are classes of users with different quality of services (QoS).

As in several works [31], [33], [34], in this proposal the total network cost C_{net} is defined as the sum of the total number of wavelengths of all network links, that is, $C_{net} = \sum_{\ell \in \mathcal{L}} W_\ell$. Because we are considering fault tolerance capabilities, this cost must includes all the additional wavelengths needed to provide tolerance to the desired failures scenarios.

Let Ω be the set of every possible failure scenarios, where each scenario is a subset $\mathcal{F}$, with $\mathcal{F} \subset \mathcal{L}$, a set of links in failure state. The method explained below can be applied to any possible set of failure scenarios: for example, to every possible single failure case ($|\mathcal{F}| = 1$), to every possible double link failure scenario ($|\mathcal{F}| = 2$), to the case when a node failure makes that all the links connected to that node are considered non-operational, in disaster risk situations [35], [36] where all the links affected by the disaster are considered non-operational, in the Shared-Risk-Group (SRG) [37] case where $\mathcal{F}$ is composed by every link that can be affected by the same physical cut, etc. Note that the previous examples consider all kinds of failure scenarios already treated in the literature. However, the method proposed here is applicable to any set of failure scenarios, with the condition that the network remains connected after any of the failure scenarios considered, which implies that the method can provide alternative routes for all affected users.

B. DEFINITIONS AND SUB-PROCEDURES NEEDED BY OUR METHOD

Since the graph representing the network topology and the set of users are fixed data, as well as the upper bounds β_c, for all $c \in \mathcal{X}$ (the maximum acceptable blocking probabilities of the users), we omit them in the list of the parameters of the procedures. For simplicity, when we refer to the network capacity, we write C_{net}, because we must change the capacities of the links many times during the computational process.

Some definitions required for the explanation of the method are presented in the following list:

- $\mathcal{G}_{-\mathcal{F}} = (\mathcal{N}, \mathcal{L}\backslash\mathcal{F})$, is the partial graph of $\mathcal{G}$ (same nodes, part of the edges), containing only the non-failed links, where $\mathcal{F}$ contains the set of failed links;
- $\mathcal{X}_\mathcal{F} = \{c \in \mathcal{X} \mid r_c \cap \mathcal{F} \neq \phi\}$, is the set of users c affected by the failures of all the links in $\mathcal{F}$;
- $\mathcal{A}_\mathcal{F} = \{r_c \in \mathcal{R} \mid r_c \cap \mathcal{F} \neq \phi\}$, is the subset of the routes in $\mathcal{R}$ disabled because of the failures of all the links in $\mathcal{F}$;
- $\mathcal{R}_\mathcal{F}$ is a set of routes that replace those in $\mathcal{A}_\mathcal{F}$ when all links in $\mathcal{F}$ are failed;
- $\mathcal{S}_\mathcal{F}$ is the total set of routes guaranteeing fault tolerance to the failure event "all links in $\mathcal{F}$ fail". That is, the set defined by $\mathcal{S}_\mathcal{F} = \left(\mathcal{R} \setminus \mathcal{A}_\mathcal{F}\right) \cup \mathcal{R}_\mathcal{F}$;
- $\mathcal{C}_\mathcal{F} = \{\mathcal{C}_\ell \mid \text{ for all } \mathcal{L} \setminus \mathcal{F}\}$ is the costs (to be defined later) of each link non-affected by the failure $\mathcal{F}$.

The method also needs a few sub-procedures to work. They are described next.

- *PrimaryRoutes*(). A procedure that computes a set of primary routes. The selection of the routes can be made by any available technique, e.g., Dijkstra's algorithm [38]. To represent the execution of this sub-procedure, let us symbolically write $\mathcal{R} :=$ *PrimaryRoutes*()
- *SecondaryRoutes*(). Considering that we have a set of failed links $\mathcal{F}$, the set of costs $\mathcal{C}_\mathcal{F}$ (see below), and a set of users $\mathcal{X}_\mathcal{F}$ affected by the failures of the links in $\mathcal{F}$, the procedure finds a new set of routes allowing to connect each user in $\mathcal{X}_\mathcal{F}$ despite the failure scenario $\mathcal{F}$, while still satisfying the QoS required by each user.
  The search for the new routes is done as follows. We run Dijkstra's algorithms looking, for each user $c \in \mathcal{X}$,

```
function Dimensioning(L, R, β_c)
1    Q := φ;
2    foreach link ℓ
3        W_ℓ := 1;
4    do
5        BP_c := Blocking(G, R);
6        foreach user c ∉ Q
7            if BP_c ≤ β_c
8                Q := Q ∪ {c};
9        if Q ≢ X
10           for all ℓ ∈ L
11               W_ℓ := W_ℓ + 1;
12   until Q ≡ X
13 return W
```

FIGURE 1. Dimensioning procedure to compute the number of wavelengths on the network.

for the cheapest route to be used by c, where the link costs are now given by the link costs in $\mathcal{C}_{\mathcal{F}}$ (explained later, in the algorithm). This procedure creates a new set of routes, that we denote by $\mathcal{R}_{\mathcal{F}}$.
Symbolically, the execution of this sub-procedure is written $\mathcal{R}_{\mathcal{F}} := SecondaryRoutes(\mathcal{F}, \mathcal{X}_{\mathcal{F}}, \mathcal{C}_{\mathcal{F}})$.

- *Dimensioning*(). This procedure consists in finding, for each link $\ell \in \mathcal{L}$, a capacity W_ℓ such that the end-to-end blocking probability BP_c of every user $c \in \mathcal{X}$ passing through the link ℓ is less than the given threshold β_c. For different reasons, the usual dimensioning procedures consider homogeneity in the links' capacities, that is, look for the minimum capacity $\mathcal{W}$, the same on all links, such that the performance objective is reached [39]–[41]. We will then follow here the same approach, because this facilitates comparisons with existing methods. But remember that our method deals with the general case as well.
  The idea is simple: we are given the operational links of the network, the set of routes $\mathcal{R}$ and the set of quality of service bounds β_c. We then initialize the network links capacities W_ℓ by value 1 and we evaluate the blocking probabilities per user (computed by calling *Blocking*()); then, we check if the blocking probability of each user is less than the one defined on the SLA. If the condition is satisfied, we stop the algorithm. If not, we increase W_ℓ values by 1 and we repeat the procedure.
  Let us define $\mathcal{Q} \subseteq \mathcal{X}$, as the set of users with their QoS constraint satisfied (maximum acceptable blocking probability). Then, symbolically we call the dimensioning sub-procedure by writing $\mathcal{W} = Dimensioning(\mathcal{L}, \mathcal{R})$. Remember that $\mathcal{W}$ is the set composed by all the network links capacities W_ℓ. Figure 1 contains in pseudo-algorithmic form the procedure just described.

C. Fault Tolerance method

Figure 2 contains a diagram with the inputs required, the condition to be guaranteed, and the outputs obtained by the execution of our method.

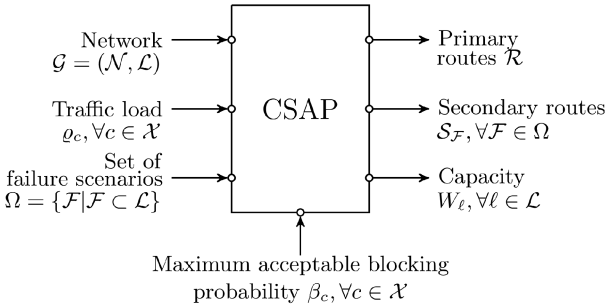


FIGURE 2. Diagram showing the inputs required to run the CSAP method, the condition to be guaranteed, and the outputs delivered to solve the four problems jointly.

The inputs are: the network topology $\mathcal{G} = (\mathcal{N}, \mathcal{L})$, which can be arbitrary, the traffic load ϱ_c of user c, for all $c \in \mathcal{X}$ (notice that the value ϱ_c of each user c can be different) and the set $\Omega = \{\mathcal{F} | \mathcal{F} \subset \mathcal{L}\}$ composed of all the link failure scenarios to be considered by our procedure.

The constraint to be satisfied by the method is to guarantee that the blocking probability of each network user c is less than the upper bound β_c predefined on the Service Level Agreement (SLA).

The method's outputs are the set of primary routes $\mathcal{R}$, allowing to provide communication to each network user c, for all $c \in \mathcal{X}$, under the condition of no link failure; the set of alternative routes $\mathcal{S}_{\mathcal{F}}$, for each failure scenarios $\mathcal{F} \in \Omega$, which allow communicating in spite of the fact that links in $\mathcal{F}$ are not operational, and the number of wavelengths W_ℓ necessary on each network link ℓ, for all $\ell \in \mathcal{L}$ (considering every possible failure scenario in Ω), thus fulfilling the QoS constraints to each user despite of the failure occurrence of any scenario in Ω.

We use our LIBPE method [30] to compute the users' blocking probabilities necessary to evaluate the quality of service offered to each user c. This procedure is an accurate and fast technique to evaluate the blocking probability of each user, on networks with wavelength continuity constraints. Note that a fast evaluation of the QoS is significant, since solving the previously listed problems (the routing of the primary and secondary paths, with the corresponding dimensioning of each failure scenario), it is necessary to compute the blocking probability a lot of times (hundreds) considering all failure cases of the set Ω, and in each of these cases to execute the dimensioning procedure. Therefore, simulation techniques are not a possibility due to the time-consuming task involved.

Additionally, the method depends of the wavelength assignment scheme used during the network operation. This problem refers to the procedure used to search for an available wavelength during network operation [33], [42]. The wavelength assignment problem has been widely covered in the literature [33], [41]–[43], and First-Fit is the most popular method currently used, because it performs better in terms of blocking probabilities than its competitors, and with low complexity. As a consequence, on our research we use this procedure to allocate the wavelengths.

```
function CSAP()
// --- input: the graph (the network), the users,
//     the bounds on the blocking probabilities,
//     and the set Ω of links failure scenarios,
//     where at most one of the events 'all links in F ∈ Ω
//     fail simultaneously' occurs, all seen as global variables
// --- output: the primary routes, the secondary routes
//     and the number of wavelengths per link

// first compute the primary routes
1   R := PrimaryRoutes();

// then, calculate the secondary paths in all failure scenarios
2   foreach F in Ω
3       for all links ℓ ∈ L \ F
4           ϱ_ℓ := Σ_{c:c∈X\X_F ∧ ℓ∈r_c} ϱ_c; // non-affected routes
5       ϱ̄ := (Σ_{ℓ∈L\F} ϱ_ℓ) / L;
6       for all links ℓ ∈ L \ F
7           C_ℓ := e^{ϱ_ℓ − ϱ̄};
8       R_F := SecondaryRoutes(F, X_F, C_F); // compute alternative routes
9       S_F := (R \ A_F) ∪ R_F;
10      W_F := Dimensioning(L \ F, S_F);

// Set the final wavelength dimensioning
11  for all links ℓ ∈ L
12      W_ℓ := max(W_{ℓ,1}, ..., W_{ℓ,|Ω|})
13  return (R, S, W)
```

FIGURE 3. Algorithm for solving the fault tolerance problem, providing alternative routes to any failure scenario in Ω.

In algorithmic form, the CSAP method is presented in Figure 3.

In **line 1**, by calling the sub-procedure *PrimaryRoutes*, we use Dijkstra's algorithm [38] to obtain an initial set of primary routes $\mathcal{R}$. However, it must be noted that the fault-tolerance mechanism presented here is not associated with any particular routing decision, thus any routing method can be applied to obtain the primary routes.

Then in **line 2**, we include all possible failure scenarios stored in Ω, where each of these scenarios is a subset $\mathcal{F}$ of failed network links. To explain how the procedure works, assume that initially the only possible failure scenario is the simultaneous failures of all links in a specific subset $\mathcal{F}$ of $\mathcal{L}$. In **lines** 3 **to 7**, we first start by finding replacement routes in case of the failure of all links in the subset of links $\mathcal{F}$. If a route r_c does not use any link of $\mathcal{F}$, it is not changed. However, for all users c whose route $r_c \in \mathcal{R}$ uses at least one link of $\mathcal{F}$ (that is, for all $c \in \mathcal{X}_\mathcal{F}$), we must find a new route that avoids the links of $\mathcal{F}$. To this end, for every link $\ell \in \mathcal{L} \setminus \mathcal{F}$, we define its cost $\mathcal{C}_\ell$ through the expression

$$\mathcal{C}_\ell = \mathrm{e}^{\varrho_\ell - \overline{\varrho}}, \tag{2}$$

where ϱ_ℓ is the traffic load offered to the link ℓ by the users non-affected by the failed links, and $\overline{\varrho}$ is the mean traffic load on all the links ℓ, such that $\ell \in \mathcal{L} \setminus \mathcal{F}$ (the non affected links). Cost function ($\mathcal{C}_\ell$) stands for one of many ways to represent how much unbalanced is the traffic load on the network, therefore seeking to balance the network traffic load, since balancing the network load may achieve remarkable savings by using network resources as even as possible [44], [45]. Then, with these $\mathcal{C}_\ell$ values as weights, in **line 8** we run Dijkstra's algorithm to find the cheapest route for each user $c \in \mathcal{X}_\mathcal{F}$. The set of all these routes is denoted by $\mathcal{R}_\mathcal{F}$. Symbolically, we execute the call $\mathcal{R}_\mathcal{F} := \mathit{SecondaryRoutes}(\mathcal{X}_\mathcal{F}, \mathcal{F}, \mathcal{C}_\mathcal{F})$. After that, **line 9** defines the set of routes $\mathcal{S}_\mathcal{F}$:

$$\mathcal{S}_\mathcal{F} = \left(\mathcal{R} \setminus \mathcal{A}_\mathcal{F}\right) \cup \mathcal{R}_\mathcal{F}.$$

In words, $\mathcal{S}_\mathcal{F}$ is the set of routes to be used when all links in $\mathcal{F}$ are failed. Under this condition, we must dimension the links again, because we must always respect the QoS constraints. For this purpose, we restrict the analysis to the graph $\mathcal{G}^{-\mathcal{F}}$, that is, we remove the links in $\mathcal{F}$ from $\mathcal{L}$. Then in **line 10**, we run a dimensioning phase. In pseudo-algorithmic form, we execute the function call $\mathcal{W}_\mathcal{F} := \mathit{Dimensioning}(\mathcal{L} \setminus \mathcal{F}, \mathcal{S}_\mathcal{F}, \{\beta_c, \forall c \in \mathcal{X}\})$.

Repeating the steps explained above for each different failure scenario (**lines 2 to 9**), we obtain a set of secondary routes for each failure scenario $\mathcal{F}$ of Ω, and the corresponding links dimensioning for each failure scenario.

To finish, in **lines 11 to 12**, we compare each $W_{\mathcal{F},\ell}$, the number of wavelengths of link ℓ under each failure scenario $\mathcal{F}$, for all $\ell \in \mathcal{L}$, and the procedure determines the capacity of the link ℓ as the maximum between them. Formally, we add a procedure max() that performs this task. We symbolically write $W_\ell := \max(\mathcal{W}_{\ell,1}, \ldots, \mathcal{W}_{\ell,|\Omega|})$, where $\mathcal{W}_{\ell,\mathcal{F}}$ is the capacity of link ℓ under failure scenario $\mathcal{F}$. Each final link capacity W_ℓ, $\ell \in \mathcal{L}$ conform the final dimensioning set $\mathcal{W}$.

IV. Numerical Results

To quantify the quality of the CSAP method, the proposed solution should be compared against the current optimal solution. However, it is known that the Routing and Wavelength Dimensioning (RWD) problem belongs to the NP-complete class [46]. In fact, those who solved this problem optimally only have been able to achieve it in the case of very small networks (networks with less than 10 nodes) [47], [48]. Consequently, for typical existing topologies (networks with dozens to hundreds of nodes), the fault-tolerance problem cannot be optimally solved (recall that the RWD problem must be solved multiple times). Given this situation, our best alternative was to compare the CSAP method with those methods considered as the most competitive ones at this moment.

In order to make a comparison, the most important metrics on the survivability problem are the capacity of the network, and the delay in the restoration procedure in case of the occurrence of failures. Next, we analyze which are the most suitable alternative methods to be compared with.

As mentioned in the introduction, there are several types of fault tolerance algorithms proposed so far, such as Shared Path Protection, p-Cycle, and 1+1. Hereafter, we discuss the pertinence in comparing CSAP with each of these different types of algorithms.

Shared Path Protection (SPP) Method: As discussed in this paper's introduction, this strategy provides tolerance to multiple network links failures. There are two methods for implementing this algorithm (on-line and off-line). Both methods require between 40 to 80% of additional wavelengths (compared to the case without fault tolerance) to provide single link fault tolerance capability [23]. Another aspect that must be considered is that the SPP off-line method has the additional weakness that the percentage of restoration obtained (percentage of users that remain connected in case of a link failure) is deficient (80% to 90% [23]), which means that it does not provide complete fault-tolerance to the network. Therefore, it is not a possible competitor to the method proposed in this work, which ensures that the blocking probability pre-established by the network designer is satisfied. On the other hand, the implementation of the SPP-online method requires to run on demand a route search algorithm (whenever one or more links fail) to find an alternative route to each affected user. Evidently, this on-line strategy causes a slow re-routing. Added to the fact that many of the applications that use computer networks require swift on-line responses in case of failures [49], this implies that this type of method does not represent a practical fault-tolerant mechanism for most applications. Due to the facts just commented, the SPP method was not considered for comparison.

The p-Cycle Method: As discussed earlier, to provide tolerance to multiple failures the p-cycle method requires a large number of cycles (which implies a high cost when defining secondary routes), so it is not scalable for multiple faults. Given the fact that in this paper, we also consider the multiple fault-tolerant cases, it is unreasonable to compare our method with the p-cycle one.

Method 1+1: This method provides tolerance to multiple failures, using as many disjoint routes as simultaneous link failures considered. It solves the problem of primary and secondary routes before the network dimensioning (off-line) sub-task. Then, the number of wavelengths is computed, having as a constraint to provide enough resources to all routes, and sufficient information to re-route each user in case of failure. Consequently, 1+1 is a suitable fault-tolerance method to be compared with our algorithm.

In summary, the most appropriate method for a comparative study and positioning of our proposal is the 1+1 for the fault-tolerance mechanism. Additionally, reviewing current methods of Routing we notice that the algorithms most commonly referenced today, and considered the best so far, use the shortest path, together with a First Fit wavelength assignment scheme. This is SP-FF (Shortest Path with First-Fit allocation scheme) [31], [33], [41], [43], [50]. Therefore, the routing strategy used with the 1+1 fault-tolerance method in this section is naturally SPFF. Both methods together are denoted SPFF1+1 in the text.

To assess the blocking probabilities in both SPFF1+1 and CSAP strategies we use the mathematical method called LIBPE [30], and the final results are validated by simulation.

As previously discussed, the Wavelength Dimensioning method most commonly used nowadays is the homogeneous dimensioning, that is, all links have the same amount of wavelengths. Consequently, we consider a homogeneous dimensioning strategy on both fault-tolerance mechanisms. Remark that we restrict our method to obtain an homogeneous dimensioning to have a fair comparison with literature solutions, but our strategy can easily compute a different amount of wavelengths to each network link.

To evaluate the performance of the methods under different scenarios, the algorithms were executed for different real network topologies, having different sizes and different degrees of connection d, where d is the average number of neighbors of a node in the network. Some of the selected topologies and their respective parameters N, L and d are shown in Figure 4.

The total network capacity C_{net} is one of the metrics chosen to compare the algorithms, which, we recall, is given by the total number of wavelengths necessary to satisfy the users QoS constraints, including the primary and secondary routes needed on each different failure scenario $\mathcal{F} \in \Omega$. In Figure 5 we show the total cost C_{net} obtained by the CSAP and SPFF1+1 methods for the case of a single link failure,

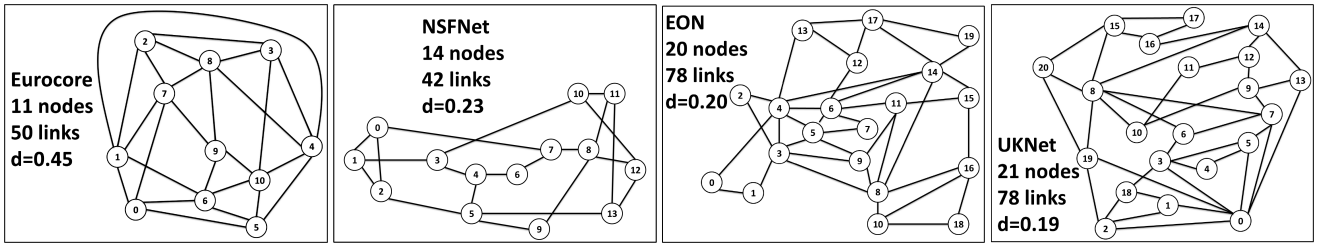


FIGURE 4. Some of the mesh networks evaluated. The number of links is the number of bi-directional arcs, that is, of edges. For instance, the picture shows the EON network topology with 39 edges, which corresponds to 78 arcs. The parameter d is a measure of density: if the graph has a arcs (twice the number of edges) and n nodes, $d = a/(n(n-1))$.

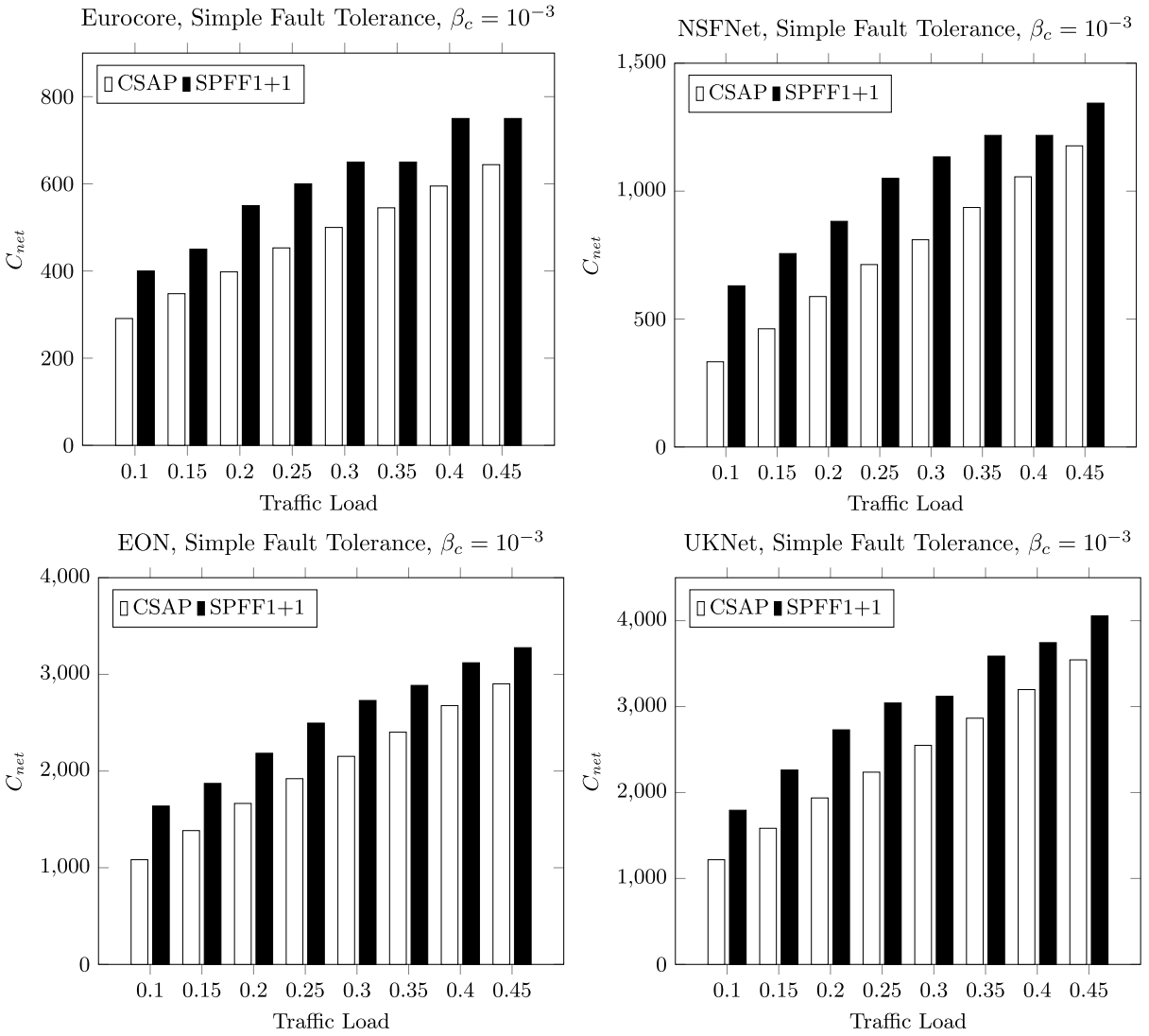


FIGURE 5. Total number of wavelengths C_{net} obtained with our method (CSAP) and with SPFF1+1 on Eurocore, NSFNet, EON and UKNet real mesh network topologies, for different connection traffic loads, with a blocking probability threshold β_c equal to 10^{-3} in the single fault tolerance case.

as a function of the traffic load, for different network topologies, and a maximum acceptable blocking user of 10^{-3}. In Figure 6 we show the C_{net} value for the same methods, but in the case of double-link failures (i.e., any pair of simultaneous link failure possible). We show only single and double link failure scenarios, in particular to be able to perform meaningful comparisons with well-known techniques, but recall that the algorithm developed can quickly evaluate any fault tolerance scenario. In addition, in this failure scenarios the amount of path computed by our method are 2 per user on case of single link failure ($2N(N-1)$ paths), and 3 per user on double link failure scenario ($3N(N-1)$ routes).

Note that in all the scenarios evaluated in our experiments for the case of a single link failure, the SPFF1+1 method

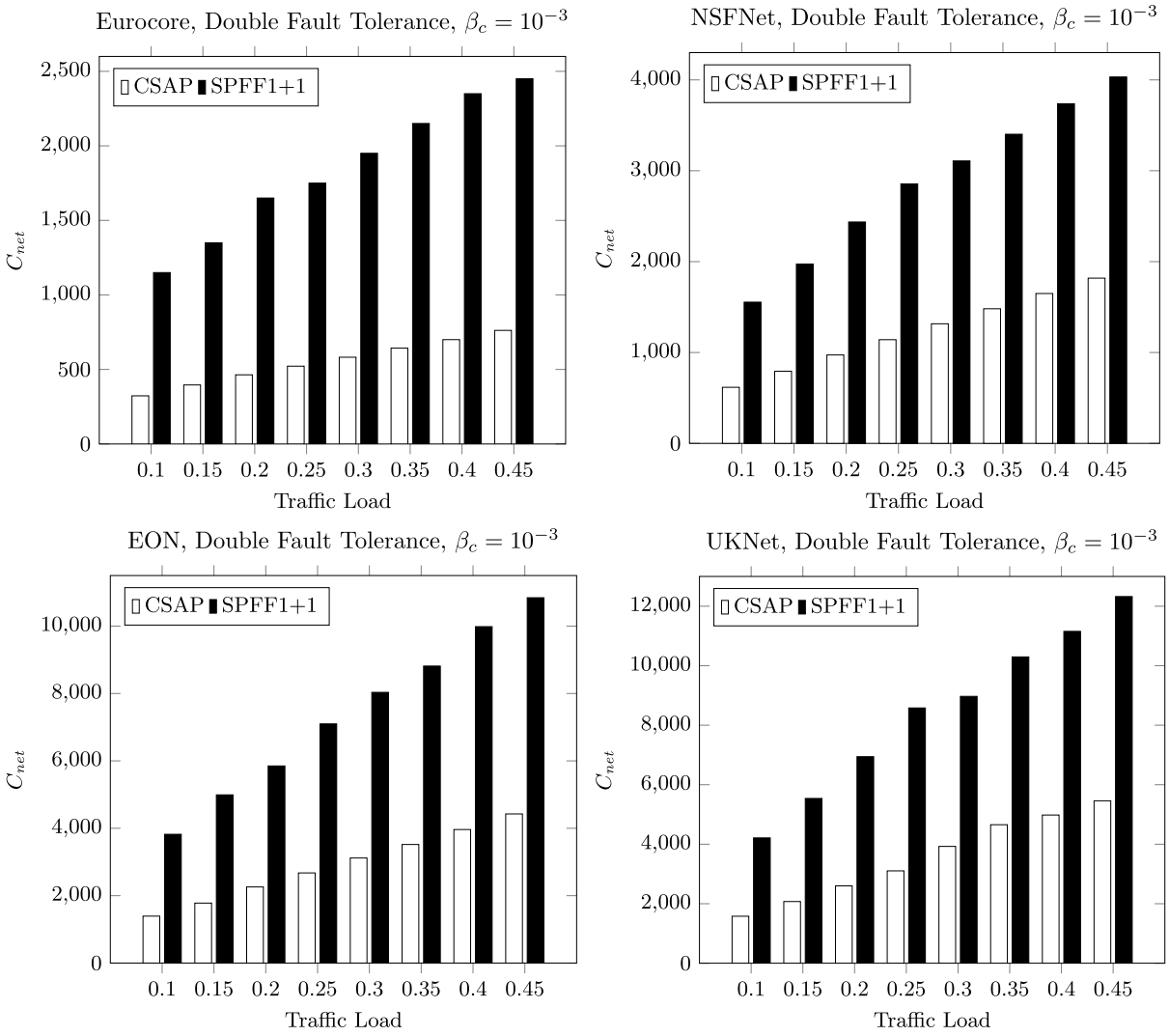


FIGURE 6. Total number of wavelengths C_{net} obtained with our method (CSAP) and with SPFF1+1 on Eurocore, NSFNet, EON and UKNet real mesh network topologies, for different connection traffic loads, with a blocking probability threshold β_c equal to 10^{-3} in the simultaneous double fault tolerance case.

requires in general 30% more wavelengths (for $\varrho = 0.3$, which is a representative network load [49]) than our proposal. Moreover, in the case of tolerance to two simultaneous failures of links (Figure 6), the CSAP method also outperforms significantly the SPFF1+1 technique: the latter requires in the order of 160% more wavelengths (always for $\varrho = 0.3$ [49]) than CSAP.

Remark that for each scenario analyzed herein, both compared methods achieve to connect the same users with the same QoS requirements (maximum acceptable blocking probability), but our proposal requires significantly fewer resources than SPFF1+1 to do so.

To provide a more in-depth discussion of the results obtained by CSAP, we present the computation complexity analysis of our proposal, and, next, an analysis about the memory size the methods need, and the time required for memory access during network operation (Sub-Sections IV-B and IV-C respectively).

A. COMPLEXITY ANALYSIS

The total computational complexity of the CSAP method depends on the wavelength dimensioning algorithm used to compute the network links capacities, which in turn depends on the blocking probability evaluation techniques used. This dependency is critical since the dimensioning procedure is executed as many times as failure scenarios considered in the set Ω. Even more, the dimensioning algorithm executes several times the blocking probability computation procedure to calculate the network capacity. Therefore, the computational complexity of the proposed strategy is calculated in three stages: the blocking probability evaluation, the wavelength dimensioning solution, and the survivability solution.

Blocking Probability As mentioned in this work, we used the method LIBPE [30] to compute the blocking probability of each network user for a given network capacity W. Let the value I be the number of iterations that the method executes to converge and $\bar{r}$ be the mean length of all the

users' paths. Then, the iterative solution executes the following steps sequentially (Algorithm 1 in [30]):

- an update of the t_{OFF} values of all the network users $c \in \mathcal{X}$ (complexity $\mathcal{O}(X)$);
- the method evaluates the blocking probability per network link $\ell \in \mathcal{L}$ ($\mathcal{O}(L)$) by means of the computation of the stationary distribution of a Markov chain covering all the users passing through the given link. The complexity of the Markov chain evaluation bounded by a quantity proportional to the mean number of user per link, that is, $\mathcal{O}(\frac{X\bar{r}}{L})$. Then, the stage complexity is given by $\mathcal{O}(X\bar{r})$;
- finally, the method evaluates the blocking probability for all the users $c \in \mathcal{X}$, with complexity $\mathcal{O}(X\bar{r})$.

In a nutshell, the blocking probability then iterates I times executing the 3 sequential stages on all the wavelengths W, thus with a complexity $\mathcal{O}(IW(X + X\bar{r} + X\bar{r}))$. This leads to a computational complexity of $\mathcal{O}(IWX\bar{r})$.

Wavelength Dimensioning the computational complexity of the algorithm displayed in Algorithm in Figure 1 is as follows. From lines 2 to 3 the complexity is $\mathcal{O}(L)$. Then, the iterative section (lines 4 to 12) solves for the blocking probability (complexity $\mathcal{O}(IWX\bar{r})$; then, for each user it is checked if its blocking probability is less than its blocking threshold, in $\mathcal{O}(X)$; and finally, the algorithm updates the links capacities, in ($\mathcal{O}(L)$). The iterative section is executed until the wavelength dimensioning is computed, thus W times. Consequently, the total computational complexity is $\mathcal{O}(W(X + IWX\bar{r} + L))$, leading to a final computational complexity of $\mathcal{O}(W^2IX\bar{r})$.

CSAP method the computational complexity of this method (shown in Algorithm in Figure 3) is then presented.

- In line 1, the primary routing problem is solved using Floyd-Warshall's (or Dijkstra's) algorithm, known to have an $\mathcal{O}(N^3)$ computational complexity;
- from lines 2 to 9, the secondary paths are computed. Let Z denote the number of failure scenarios in Ω, and F the maximum number of simultaneous links in the failure state on a given scenario in Ω. We iterate for all the Z failure scenarios considered (line 2), computing the cost of all the operational links (lines 3 to 6), with complexity $\mathcal{O}(L\frac{X\bar{r}}{L})$ (lines 3 to 4), in $\mathcal{O}(L)$ in line 5, and $\mathcal{O}(L)$ in lines 6 to 7. Later, the secondary routes are computed, executing Dijkstra ($\mathcal{O}(N^2)$) for each user affected by the failure scenario ($O(F\frac{X\bar{r}}{L})$). Finally, in line 9 the dimensioning is executed with the previously calculated complexity $\mathcal{O}(W^2IX\bar{r})$.
- The last stage (lines 10 to 11) computes the final wavelength dimensioning, comparing the dimensioning obtained on all Z scenarios in Ω, then with complexity is $\mathcal{O}(LZ)$.

Summarizing, the complexity is given by the sum of the complexities of the 3 stages. Consequently, the final computational complexity of the complete CSAP procedure is $\mathcal{O}\left(N^3 + ZF\frac{X\bar{r}}{L}N^2 + ZW^2IX\bar{r}\right)$. It is important to notice the most complex procedures are the primary route computation (first term in the computational complexity), the secondary route calculation (the second one), and the wavelength dimensioning procedure (the last one).

B. MEMORY SIZE

Other aspects that influence the network performance are the storage size used by the routing tables, and the delay imposed by the routing procedure when each user attempts to transmit over a path.

The routing tables storage size depends on how many routes are computed for each user by the implemented procedure. If the 1+1 method provides fault tolerance to a single link failure, it computes only one secondary path for each user. Likewise, to offer fault tolerance to simultaneous double link failures, the 1+1 technique provides two secondary routes per user. Therefore, the number of entries stored on the routing tables are two and three times the number of users in $\mathcal{X}$, to provide single and double fault tolerance, respectively (with centralized management).

On our method, the number of paths computed changes based on the different failure scenarios and the network topology (size and node degree). This occurs because, on each failure case, our method searches a new route to each user affected by the failed links on that scenario. In the executed experiments, our method required a similar number of alternate paths to provide single and fault tolerance than 1+1. For example, on the Eurocore network topology, to provide single and double fault tolerance, our method computed the same number of alternate paths than 1+1. Moreover, on a bigger network such as Arpanet, our methods required, on average, three and four paths per user to provide single and double fault tolerance, respectively.

C. ROUTING DELAY

During network operation, there is a delay incurred by the routing procedure, due to the time required to find the corresponding path and to transmit by it successfully, or to be finally blocked. We denote this delay as $\tau(A)$, where A is the algorithm considered (SPFF1+1 or CSAP). Since both methods compared in this work use fixed predefined routes, the delay is mainly composed by the time needed to access the routing table and the corresponding transmission. Since an access needs a constant time T, then, $\tau(A)$ measures how many times it is required to access the routing tables to have a successful communication, or to be blocked, using the routing scheme obtained by method A.

Note that both methods store the alternate paths in routing tables, but the technique to route each user on every communication request differs. The 1+1 fault tolerance scheme sends the information on each alternate path every time the user attempts to transmit; thus, the access to routing tables requires to read two routes per user on single fault tolerance and three routes per user on simultaneous double fault tolerance. On the other hand, our method has only one route per link failure case; thus, it requires to read only one entry on the routing table on each attempt of transmission.

In a nutshell, the $\tau(A)$ value per method is:

- $\tau(SPFF1+1) = 2\ T$, considering tolerance to single link failure.
- $\tau(SPFF1+1) = 3\ T$, considering tolerance to simultaneous double link failure.
- $\tau(CSAP) = T$, for any link failure scenario.

showing the advantage of the CSAP method with respect to the routing delay.

V. CONCLUSION

A novel method was proposed to solve the fault-tolerance problem for any possible set of scenarios, where each scenario is defined by a specific set of link failures.

The method differs considerably from those published so far, obtaining better results in terms of the necessary number of wavelengths and the associated delays. Additionally, the dimensioning method does not make any distinction between primary and alternative routes, with the constraint that it only evaluates scenarios that may happen during the network operation (for each user, it considers either a primary or a secondary route, not both simultaneously). Consequently, the method allows sharing the resources between all the secondary routes, while guaranteeing a pre-specified upper bound on the blocking probability of each network user.

The proposed fault tolerance technique is scalable to any set of simultaneous link failures, as long as the network topology allows re-connection via the links that remain operational. This scheme is executed before the network operation, typically requiring just a few seconds of execution time. This fast execution also allows to quickly solve any link failure scenario during network operation if needed (think, for instance, of the case of important traffic load variations). Additionally, the network operation based on our approach is fast and straightforward, since the routes (both primary and secondary) are stored in routing tables and consulted only on demand.

As a final remark, Elastic Optical Networks (EON) are an essential and current topic to address. A fast and accurate mathematical method to evaluate the users blocking probability is imperative to assess all the scenarios in a fault-tolerance context on EON architectures. We are currently working to achieve this model, since to the best of our knowledge, there is not a proper one. In future work, we will assess the survibability problem including this new model on the flexible optical network architectures.

REFERENCES

[1] M. To and P. Neusy, "Unavailability analysis of long-haul networks," *IEEE J. Sel. Areas Commun.*, vol. 12, no. 1, pp. 100–109, Jan. 1994.

[2] D. A. Schupke, A. Autenrieth, and T. Fischer, "Survivability of multiple fiber duct failures," in *Proc. 3rd Int. Workshop Design Reliable Commun. Netw. (DRCN)*, 2001, pp. 7–10.

[3] R. Ramaswami and K. N. Sivarajan, "Design of logical topologies for wavelength-routed all-optical networks," in *Proc. 14th Annu. Joint Conf. IEEE Comput. Commun. Societies (INFOCOM)*, vol. 3, Apr. 1995, pp. 1316–1325.

[4] S. Ahuja, S. Ramasubramanian, and M. Krunz, "Single-link failure detection in all-optical networks using monitoring cycles and paths," *IEEE/ACM Trans. Netw.*, vol. 17, no. 4, pp. 1080–1093, Aug. 2009.

[5] H. Singh, J. Prakash, D. Arora, and A. Wason, "Fault tolerant congestion based algorithms in OBS network," *Int. J. Eng.*, vol. 5, no. 5, pp. 350–359, 2011.

[6] M. F. Habib, M. Tornatore, M. De Leenheer, F. Dikbiyik, and B. Mukherjee, "Design of disaster-resilient optical datacenter networks," *J. Lightw. Technol.*, vol. 30, no. 16, pp. 2563–2573, Aug. 15, 2012.

[7] F. S. H. Souza, D. L. Guidoni, and G. R. Mateus, "A column generation-based heuristic for the GRWA with protection and QoS in WDM optical networks," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2013, pp. 922–927.

[8] C. Y. Chu, K. Xi, M. Luo, and H. J. Chao, "Congestion-aware single link failure recovery in hybrid SDN networks," in *Proc. IEEE INFOCOM*, Apr. 2015, pp. 1086–1094.

[9] D. S. Mukherjee, C. Assi, and A. Agarwal, "Alternate strategies for dual failure restoration using p-cycles," in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 6, Jun. 2006, pp. 2477–2482.

[10] R. Yadav, R. S. Yadav, and H. M. Singh, "Intercycle switching (ICS)-based dynamic reconfiguration of p-cycle for dual-failure survivability of WDM networks," *Photon. Netw. Commun.*, vol. 24, no. 2, pp. 160–165, Oct. 2012.

[11] D. S. Yadav, S. Rana, and S. Prakash, "A mixed connection recovery strategy for surviving dual link failure in WDM networks," *Opt. Fiber Technol.*, vol. 19, no. 2, pp. 154–161, Mar. 2013.

[12] M. Jinno, T. Takagi, and Y. Uemura, "Enhanced survivability of translucent elastic optical network employing shared protection with fallback," in *Proc. Opt. Fiber Commun. Conf. Exhibit. (OFC)*, Mar. 2017, pp. 1–3.

[13] D. Serre and C. Heinzlef, "Assessing and mapping urban resilience to floods with respect to cascading effects through critical infrastructure networks," *Int. J. Disaster Risk Reduction*, vol. 30, pp. 235–243, Sep. 2018.

[14] F. Dikbiyik, M. Tornatore, and B. Mukherjee, "Minimizing the risk from disaster failures in optical backbone networks," *J. Lightw. Technol.*, vol. 32, no. 18, pp. 3175–3183, Sep. 15, 2014.

[15] S. Ferdousi, F. Dikbiyik, M. F. Habib, M. Tornatore, and B. Mukherjee, "Disaster-aware dynamic content placement in optical cloud networks," in *Conf. Opt. Fiber Commun., Tech. Dig. Ser.*, 2014, pp. 1–3.

[16] X. Shao, Y. Bai, X. Cheng, Y.-K. Yeo, L. Zhou, and L. H. Ngoh, "Best effort SRLG failure protection for optical WDM networks," *J. Opt. Commun. Netw.*, vol. 3, no. 9, p. 739, Sep. 2011.

[17] P. Babarczi, J. Tapolcai, P. H. Ho, and M. Médard, "Optimal dedicated protection approach to shared risk link group failures using network coding," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2012, pp. 3051–3055.

[18] W. Liao and C.-H. Loi, "Providing service differentiation for optical-burst-switched networks," *J. Lightw. Technol.*, vol. 22, no. 7, pp. 1651–1660, Jul. 2004.

[19] D. H. Hailu, G. G. Lema, E. A. Yekun, and S. H. Kebede, "Unified study of quality of service (QoS) in OPS/OBS networks," *Opt. Fiber Technol.*, vol. 36, pp. 394–402, Jul. 2017.

[20] S. M. Sam, S. M. Daud, K. Kamardin, and N. Maarop, "Study of QoS performance in optical burst switched networks (OBS)," *Indian J. Sci. Technol.*, vol. 9, Dec. 2016. [Online]. Available: [Online]. Available: http://www.indjst.org/index.php/indjst/article/view/99269

[21] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," *J. Lightw. Technol.*, vol. 21, no. 4, pp. 870–883, Apr. 2003.

[22] M. Wang, S. Li, E. W. M. Wong, and M. Zukerman, "Performance analysis of circuit switched multi-service multi-rate networks with alternative routing," *J. Lightw. Technol.*, vol. 32, no. 2, pp. 179–200, Jan. 15, 2014.

[23] D. A. Schupke and R. G. Prinz, "Capacity efficiency and restorability of path protection and rerouting in WDM networks subject to dual failures," *Photon. Netw. Commun.*, vol. 8, no. 2, pp. 191–207, Sep. 2004.

[24] A. Wason and R. Kaler, "Fault-tolerant routing and wavelength assignment algorithm for multiple link failures in wavelength-routed all-optical WDM networks," *Optik*, vol. 122, no. 2, pp. 110–113, Jan. 2011.

[25] D. Pereira and M. C. Penna, "A new algorithm for dimensioning resilient optical networks for shared-mesh protection against multiple link failures," *Opt. Switching Netw.*, vol. 13, pp. 158–172, Jul. 2014.

[26] D. A. Schupke, "Multiple failure survivability in WDM networks with p-cycles," in *Proc. Int. Symp. Circuits Syst. (ISCAS)*, vol. 3, May 2003, pp. III-866–III-869.

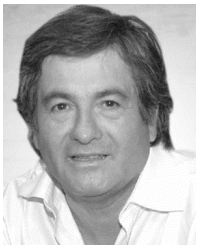
[27] L. Tang, M. Cai, B. Li, and R. Wu, "A novel multi-link fault-tolerant algorithm for survivability in multi-domain optical networks," *Photon. Netw. Commun.*, vol. 24, no. 2, pp. 77–85, Oct. 2012.

[28] F. Ji, X. Chen, W. Lu, J. J. Rodrigues, and Z. Zhu, "Dynamic p-cycle configuration in spectrum-sliced elastic optical networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2013, pp. 2170–2175.
[29] N. Jara, H. Pempelfort, G. Rubino, and R. Vallejos, "How much the wavelength dimensioning methods and a tightened QoS provision impact on the dynamic WDM optical networks capacity?" *Opt. Switching Netw.*, vol. 35, Jan. 2020, Art. no. 100540.
[30] N. Jara, R. Vallejos, and G. Rubino, "Blocking evaluation and wavelength dimensioning of dynamic WDM networks without wavelength conversion," *J. Opt. Commun. Netw.*, vol. 9, no. 8, pp. 625–634, Aug. 2017.
[31] A. Zapata-Beghelli and P. Bayvel, "Dynamic versus static wavelength-routed optical networks," *J. Lightw. Technol.*, vol. 26, no. 20, pp. 3403–3415, Oct. 2008.
[32] M. Zukerman, E. W. M. Wong, Z. Rosberg, G. M. Lee, and H. Le Vu, "On teletraffic applications to OBS," *IEEE Commun. Lett.*, vol. 8, no. 2, pp. 116–118, Feb. 2004.
[33] R. Ramaswami, K. Sivarajan, and G. Sasaki, *Optical Networks: A Practical Perspective*, 3rd ed. San Francisco, CA, USA: Morgan Kaufmann Publishers, 2009.
[34] N. Jara, R. Vallejos, and G. Rubino, "A method for joint routing, wavelength dimensioning and fault tolerance for any set of simultaneous failures on dynamic WDM optical networks," *Opt. Fiber Technol.*, vol. 38, pp. 30–40, Nov. 2017.
[35] F. Dikbiyik, A. S. Reaz, M. De Leenheer, and B. Mukherjee, "Minimizing the disaster risk in optical telecom networks," in *Proc. OFC/NFOEC*, Los Angeles, CA, USA, 2012, pp. 1–3.
[36] S. Ferdousi, F. Dikhiyik, M. F. Habib, and B. Mukherjee, "Disaster-aware data-center and content placement in cloud networks," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2013, pp. 1–3.
[37] H. Zang, C. Ou, and B. Mukherjee, "Path-protection routing and wavelength assignment in WDM mesh networks under shared-risk-group constraints," *Proc. SPIE*, vol. 4585, pp. 49–60, Oct. 2001.
[38] E. W. Dijkstra, "A note on two problems in connexion with graphs," *Numer. Math.*, vol. 1, no. 1, pp. 269–271, Dec. 1959.
[39] X. J. Zhang, S.-I. Kim, and S. S. Lumetta, "Dimensioning WDM networks for dynamic routing of evolving traffic," *J. Opt. Commun. Netw.*, vol. 2, no. 9, p. 730, Sep. 2010.
[40] L. Tan, Q. Yang, J. Ma, and S. Jiang, "Wavelength dimensioning of optical transport networks over nongeosychronous satellite constellations," *J. Opt. Commun. Netw.*, vol. 2, no. 4, p. 166, Apr. 2010.
[41] R. T. Koganti and D. Sidhu, "Analysis of routing and wavelength assignment in large WDM networks," *Procedia Comput. Sci.*, vol. 34, pp. 71–78, 2014.
[42] B. Mukherjee, *Optical WDM Networks*, vol. 26. Boston, MA, USA: Springer, 2006.
[43] B. Chatterjee, P. Sahu, and N. Sarma, "Review and performance analysis on routing and wavelength assignment approaches for optical networks," *IETE Tech. Rev.*, vol. 30, no. 1, pp. 12–23, 2013.
[44] A. A. Neghabi, N. J. Navimipour, M. Hosseinzadeh, and A. Rezaee, "Load balancing mechanisms in the software defined networks: A systematic and comprehensive review of the literature," *IEEE Access*, vol. 6, pp. 14159–14178, 2018.
[45] R. Vallejos and N. Jara, "Join routing and dimensioning heuristic for dynamic WDM optical mesh networks with wavelength conversion," *Opt. Fiber Technol.*, vol. 20, no. 3, pp. 217–223, Jun. 2014.
[46] V. López and L. Velasco, Eds., *Elastic Optical Networks*. Cham, Switzerland: Springer, 2016.
[47] C. Meza, N. Jara, V. M. Albornoz, and R. Vallejos, "Routing and spectrum assignment for elastic, static, and without conversion optical networks with ring topology," in *Proc. 35th Int. Conf. Chilean Comput. Sci. Soc. (SCCC)*, Oct. 2016, pp. 1–8.
[48] R. Vallejos, A. Zapata-Beghelli, V. Albornoz, and M. Tarifeño, "Joint routing and dimensioning of optical burst switching networks," *Photon. Netw. Commun.*, vol. 17, no. 3, pp. 266–276, Jun. 2009.
[49] A. Saleh and J. Simmons, "Technology and architecture to enable the explosive growth of the Internet," *IEEE Commun. Mag.*, vol. 49, no. 1, pp. 126–132, Jan. 2011.
[50] N. Charbonneau and V. M. Vokkarane, "A survey of advance reservation routing and wavelength assignment in wavelength-routed WDM networks," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 1037–1064, 4th Quart., 2012.

NICOLÁS JARA received the B.Sc. and M.Sc. degrees in telematics engineering from Universidad Técnica Federico Santa María (UTFSM), Chile, in 2010, and the Ph.D. degree on a double graduation program from the Université de Rennes I, France, and UTFSM, in 2017 and 2018, respectively. He is currently an Assistant Professor with the Department of Electronics Enginering, UTFSM. His current research interests include optical networks design, networks performability, and simulation techniques.

HERMANN PEMPELFORT received the B.Sc. degree in computer science from the Universidad de Valparaíso (UV), Chile, in 2011. He is currently an Assistant Researcher with the Department of Electronics Enginering, Universidad Técnica Federico Santa María (UTFSM), Chile. His current research interests include software development and research on optical networks design, networks performability, and simulation techniques.

GERARDO RUBINO is a Senior Researcher with the French National Institute for Research in Computer Science and Control (INRIA), where he leads the DIONYSOS Group that works on the analysis and design of networking technologies. He is also a board member of the media and networks cluster in Brittany, France. He is interested in quantitative analysis of complex systems using probabilistic models, networking, and other engineering areas. He is the author of more than 200 scientific works in applied mathematics and computer science. He currently works on performance and dependability analysis, optical architectures, the perceptual quality assessment of audio and video applications and services built on top of the Internet, AI applications to networking, and rare event analysis. He is a member of the Steering Committee of RESIM, the only workshop dedicated to his research topics.



REINALDO VALLEJOS received the B.Eng. degree in electronic engineering from Universidad Técnica Federico Santa María (UTFSM), Valparaiso, Chile, in 1975, and the M.Sc. degree in computer science from the Pontificia Universidade Católica do Río de Janeiro, Brazil, in 1991, and the Ph.D. degree in computer science from the Universidade Federal do Río de Janeiro, Brazil, in 1993. He is currently a Professor with the Department of Electronics Engineering, UTFSM. He has received the Professional title of Electronic Engineer from Universidad Técnica Federico Santa Maria (UTFSM), Valparaiso, in 1976.