Optical Switching and Networking 42 (2021) 100633

Contents lists available at ScienceDirect

Optical Switching and Networking

journal homepage: www.elsevier.com/locate/osn

RMSA algorithms resilient to multiple node failures in dynamic EONs

Fábio Barbosa [a], Amaro de Sousa [a,*], Agostinho Agra [a,b], Krzysztof Walkowiak [c], Róża Goścień [c]

[a] Instituto de Telecomunicações, DETI, Universidade de Aveiro, Portugal
[b] CIDMA, Dept. de Matemática, Universidade de Aveiro, Portugal
[c] Department of Systems and Computer Networks, Faculty of Electronics, Wrocław University of Science and Technology, Wrocław, Poland

ARTICLE INFO

Keywords:
Elastic optical networks
RMSA
Multiple node failures
Disaster resilience
Simulation

ABSTRACT

In Elastic Optical Networks (EONs), the way different service demands are supported in the network is ruled by the Routing, Modulation and Spectrum Assignment (RMSA) algorithm, which decides how the spectrum resources of the optical network are assigned to each service demand. In a dynamic EON, demand requests arrive randomly one at a time and the accepted demands last in the network for a random time duration. So, one important goal of the RMSA algorithm is the efficient use of the spectrum resources to maximize the acceptance probability of future demand requests. On the other hand, multiple failure events are becoming a concern to network operators as such events are becoming more frequent in time. In this work, we consider the case of multiple node failure events caused by malicious attacks against network nodes. In order to obtain RMSA algorithms resilient to such events, a path disaster availability metric was recently proposed which takes into account the probability of each path not being disrupted by an attack. This metric was proposed in the offline variant of the RMSA problem where all demands are assumed to be known at the beginning. Here, we exploit the use of the path disaster availability metric in the RMSA of dynamic EONs. In particular, we propose RMSA algorithms combining the path disaster availability metric with spectrum usage metrics in a dynamic way based on the network load level. The aim is that the efficient use of the resources is relaxed for improved resilience to multiple node failures when the EON is lightly loaded, while it becomes the most important goal when the EON becomes heavily loaded. We present simulation results considering a mix of unicast and anycast services in 3 well-known topologies. The results show that the RMSA algorithms combining the path disaster availability metric with spectrum usage metrics are the best trade-off between spectrum usage efficiency and resilience to multiple node failures.

1. Introduction

The support of different service demands in Elastic Optical Networks (EONs) is ruled by the Routing, Modulation and Spectrum Assignment (RMSA) algorithm, which decides how the network resources are assigned to each service demand. In a dynamic EON, demand requests arrive randomly one at a time and the accepted demands last in the network for a random time duration.

One of the main goals of the RMSA algorithm is to use the resources in an efficient way, i.e., by keeping the spectrum resources usage low so that future demands can be accommodated with higher probability [1–5]. However, other goals are also important due to the continuous advances of EONs in terms of node architectures and transceiver characteristics (bit-rate and transmission reach). This is particularly important in the RMSA offline problem where all demands to be supported by the EON are estimated at the beginning and the RMSA efficient use of the network resource also considers other goals as the minimization of transceiver costs or of the network power consumption [6–8].

On the other hand, large-scale failure events are becoming a concern to network operators as such events are becoming more frequent in time [9]. Large-scale failure events can have different causes, as natural disasters [10] or human malicious activities [11], which might involve a significant number of simultaneous failures. Network resilience to failure events is, broadly speaking, the ability of the network to keep supporting the service demands after a failure event and many works have addressed this problem for single link (or single node) failures considering protection mechanisms to guarantee that all demands can be maintained after the failure event [12–14]. However, the guarantee that all demands are maintained in a large-scale failure event involving multiple failures is infeasible in practice as the required network

* Corresponding author.
E-mail address: asou@ua.pt (A. de Sousa).

https://doi.org/10.1016/j.osn.2021.100633
Received 15 July 2020; Received in revised form 3 April 2021; Accepted 5 July 2021
Available online 21 July 2021

resources become too costly. In this case, the aim becomes to improve the network preparedness to large-scale failure events as much as possible by maximizing the amount of demand that can still be maintained in face of such events.

In this work, we consider the case of multiple node failure events caused by human malicious attacks against network nodes. In terrorist attacks, although node shutdowns are harder to realize than link cuts, they are the most rewarding in the attackers' perspective since the shutdown of a node also shuts down all its fiber links. So, we deal with multiple node failures as they are the most harmful case. The topology design of optical networks resilient to multiple node failures was addressed in Refs. [15,16]. In those works, though, the RMSA is not considered and the resilience of the network topology is evaluated by the impact of the simultaneous failure of its critical nodes, i.e., the nodes with the highest impact on the connectivity of the network.

Meanwhile, a family of RMSA algorithms resilient to multiple node failures caused by attacks against multiple nodes has been recently proposed for EONs in Ref. [17] assuming that the attacker "discovers" with some probability a set of nodes to be attacked. The proposed algorithms use a metric, named *path disaster availability*, in the RMSA decision which takes into account the probability that each path is not disrupted by the attack. While the work in Ref. [17] considers the offline version of the RMSA problem (i.e., all service demands are assumed to be known at the beginning), we exploit in this work the use of the path disaster availability metric in the RMSA of dynamic EONs. In particular, we propose RMSA algorithms combining the path disaster availability metric with spectrum usage metrics in a dynamic way based on the network load level. The aim is that the efficient use of the resources is relaxed for improved resilience to multiple node failures when the EON is lightly loaded, while it becomes the most important goal when the EON is heavily loaded.

To evaluate the proposed RMSA algorithms, we have developed an event-driven simulator (in this type of simulation, only the time instants at which the state of the system changes need to be simulated, i.e., the system is modeled as a series of time instants when a state-change occurs, called *events* [18]). The simulator is used to estimate the spectrum usage efficiency of each RMSA algorithm (assessed by the bit-rate amount of all requests that are blocked due to insufficient free spectrum resources) and the network resilience to multiple node failures. In the latter case, the resiliency is evaluated by 2 parameters: the average non-disrupted demand (the bit-rate percentage that is not disrupted after a failure, averaged over all failures) and the average surviving demand (the bit-rate percentage that is supported after a failure, averaged over all failures). Both resiliency parameters are important in practice. On one hand, higher average surviving demand values are important for non-critical services as they are less penalized by short-term disruptions. On the other hand, higher average non-disrupted demand values are important for critical services (which require high availability) and for minimizing the number of disrupted lightpaths requiring reconfiguration.

We present a set of computational results considering a mix of unicast and anycast services in 3 well-known topologies. All algorithms are evaluated through simulation considering a restoration mechanism where, upon a multiple node failure event, the non-affected lightpaths remain unchanged and the demands of the affected lightpaths are reassigned as much as possible with new lightpaths in the spectrum resources of the surviving network. The results show that the RMSA algorithms combining the path disaster availability metric with spectrum usage metrics are the best trade-off between spectrum usage efficiency and resilience to multiple node failures.

The paper is organized as follows. Section 2 describes how the malicious node attacks are modeled and how the path disaster availability metric is computed based on the attack model. Section 3 describes the RMSA algorithms in the regular state and in the failure state. Section 4 describes the simulation procedure used to assess the different RMSA algorithms. The computational results are presented and discussed in Section 5. Finally, Section 6 draws the main conclusions of the work.

2. Modeling node attacks and path disaster availability

In this work, a malicious attack against multiple nodes corresponds to the case when a malicious organization discovers some nodes that it is able to attack. By shutting down these nodes, the organization aims to disrupt as much as possible the services supported by the network.

In general, different levels of public information exist related to the location of each network node. For example, the location of Data Centers is usually publicly known and most likely a network node is nearby, which results in a higher probability of such nodes being discovered by malicious organizations. Moreover, the set of nodes discovered by a malicious organization depends on its resources (human cells and geographical base locations) and operational capabilities. However, different malicious organizations might exist, each one with its own resources and capabilities. So, from the perspective of the network operator, since it does not know which organization is planning an attack on its network (or how nodes are discovered by the organization), any set of uncorrelated nodes can be attacked. In modeling terms, it is similar to multiple unintended failures with the difference that single failures are much more likely than multiple failures in unintended failure events, while the failure of multiple nodes is more likely in malicious attacks.

Following these assumptions, we describe in separate subsections, first, how a malicious node attack is modeled and, then, how the path disaster availability metric is computed for each routing path based on the attack model. In both subsections, we consider an EON topology defined by a graph $G = (N, E)$, with a set of $n = |N|$ nodes and a set of $|E|$ undirected links.

2.1. Modeling a malicious node attack

We consider the following malicious node attack model. An attacker discovers with a given probability a set of nodes that can be attacked (almost) simultaneously. Each node $i \in N$ has an associated positive weight w_i proportional to the probability of the node being discovered by the attacker and, as discussed before, there is no correlation between discovered nodes. The number s of discovered nodes is between a minimum number s_m below which its destructive impact in the network is considered not worthy by the attacker and a maximum number s_M above which the probability of such number of nodes being attacked is negligible. Moreover, we assume that the effort required to attack s nodes is proportional to the number of nodes and, therefore, the probability P_s of s nodes being attacked, with $s_m \leq s \leq s_M$, is inversely proportional to the number of attacked nodes, i.e.:

$$P_s = \frac{\frac{1}{s}}{\sum_{t=s_m}^{s_M} \frac{1}{t}}, \quad s = s_m, \ldots, s_M \tag{1}$$

2.2. Computing the path disaster availability

Consider a given path p on graph $G = (N, E)$ defined by its set of nodes $i \in p$ (including source and destination nodes). The path disaster availability a_p of path p is the probability that p is available (i.e., not disrupted) after an attack. Due to the assumption of no correlation between attacked nodes, the path disaster availability a_p is given by:

$$a_p = \prod_{i \in p} (1 - \pi_i) \tag{2}$$

where π_i is the probability of node $i \in N$ to be attacked when an attack is realized. Then, π_i is given by:

$$\pi_i = \sum_{s=s_m}^{s_M} \pi_i^s \times P_s \tag{3}$$

where π_i^s is the probability of node i being attacked on an attack to s nodes and P_s, previously defined in (1), is the probability of an attack to s nodes. Finally, probability π_i^s is computed by the sum of the probabilities of all sequences without repetitions of s nodes out of n ($= |N|$) nodes that include node i in one of its positions, given by:

$$\pi_i^s = \frac{w_i}{W_N} + \sum_{j \in N \setminus \{i\}} \frac{w_j}{W_N} \times \frac{w_i}{W_{N \setminus \{j\}}} + \sum_{j \in N \setminus \{i\}} \frac{w_j}{W_N} \left(\sum_{k \in N \setminus \{i,j\}} \frac{w_k}{W_{N \setminus \{j\}}} \times \frac{w_i}{W_{N \setminus \{j,k\}}} \right) + \ldots \quad (4)$$

where W_M denotes the sum of the node weights of a set $M \subseteq N$, i.e., $W_M = \sum_{i \in M} w_i$. The first term $\frac{w_i}{W_N}$ in (4) is the probability of all sequences such that i is the first node of the sequence. The second term $\sum_{j \in N \setminus \{i\}} \frac{w_j}{W_N} \times \frac{w_i}{W_{N \setminus \{j\}}}$ is the probability of all sequences such that i is the second node of the sequence, i.e., all sequences composed by a node $j \in N \setminus \{i\}$ in the first position and node i in the second position. The third term is the generalization of the previous term for the sequences such that i is the third node of the sequence.

The probability π_i^s defined in (4) has s terms and can be computed recursively as follows. For a given set of nodes N and associated weights $w = \{w_i, i \in N\}$, a given number of attacked nodes s and a given node i, the probability π_i^s is computed as:

$$\pi_i^s = prob(N, w, i, 0, s) \quad (5)$$

where *prob*() is the recursive function defined in Algorithm 1. The input parameters of Algorithm 1 are a set of nodes *M* which were still not selected (in the first call in (5), this parameter is the complete node set *N*), the set *w* of node weights, the node *i* whose probability we want to compute, the number *z* of already selected nodes (in the first call in (5), this parameter is $z = 0$) and the number of attacked nodes *s*.

Algorithm 1
Recursive function to compute π_i^s

```
1: function π = prob(M, w, i, z, s)
2: z ← z + 1
3: W_M ← Σ_{j ∈ M} w_j
4: π ← w_i / W_M
5: if z < s then
6:   for all j ∈ M\{i} do
7:     π ← π + (w_j / W_M) × prob(M\{j}, w, i, z, s)
8:   end for
9: end if
10: return π
```

For illustration purposes, consider the example of graph $G = (N, E)$ presented in Fig. 1, with $n = 12$ nodes and $|E| = 18$ edges and assume that the nodes highlighted in gray are 10 times more probable of being discovered than the other nodes. Therefore, $w_i = 10$ for nodes $i \in \{2, 5, 11\}$ and $w_i = 1$ for all other nodes. Note that the probabilities π_i^s given by (4) are equal for nodes with equal weight values w_i. In this example, since there are only two different weight values, all probabilities of nodes $i \in \{2, 5, 11\}$ are equal and all probabilities of the other nodes are also equal. Table 1 presents the probability values of this example computed by Algorithm 1 for a number of attacked nodes s from 2 up to 6. As expected, these results show that the more the attacked nodes s are, the higher the probabilities π_i^s of all nodes become. Moreover, for all values of s, the nodes i with the highest weight value $w_i = 10$ have always a higher probability of being attacked than the other nodes.

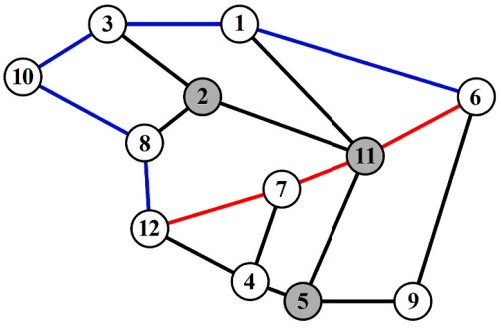

Fig. 1. Polska network topology [19].

Then, for a given range $[s_m, s_M]$ in the number of attacked nodes, the probability π_i of each node i to be attacked when an attack is realized is given by (3). Table 2 presents the probability values π_i of all nodes (third and fourth columns) for different $[s_m, s_M]$ ranges (first and second columns) assuming a constant minimum number of attacked nodes $s_m = 2$ an increasing maximum number of attacked nodes $s_M = 3$, 4, 5 and 6. Again, an increasing average number of attacked nodes increases the probability values π_i of all nodes and the probability values of the nodes with the highest weight value are always higher than the probability values of the nodes with the lowest weight values.

Now consider in the example of Fig. 1 the end-nodes $s = 6$ and $t = 12$ and the following two candidate paths: $p_1 = \{6\text{–}11\text{–}7\text{–}12\}$ (highlighted in red) and $p_2 = \{6\text{–}1\text{–}3\text{–}10\text{–}8\text{–}12\}$ (highlighted in blue). The path disaster availability of these two candidate paths is given by (2), whose values are presented in Table 2 (fifth and sixth columns) for the different considered $[s_m, s_M]$ ranges. For any of the considered ranges, although path p_1 is shorter (in number of links), its probability of not being affected by an attack (i.e., its path disaster availability) is lower than the probability of p_2 not being affected by an attack. This is because p_1 includes one of the nodes (node 11) with higher probability of being discovered while p_2 does not include any of such nodes.

Note that the values of π_i^s computed with Algorithm 1 and π_i computed with (3) only depend on the EON topology and on the parameters defining the malicious node attack model. So, they are computed once (in advance) and, then, the path disaster availability a_p of each candidate path p considered by the RMSA algorithms is efficiently computed with (2).

3. RMSA algorithms

In a dynamic EON, demand requests arrive one at a time in the regular state. When a new request arrives, there is a set of lightpaths already established in the network (occupying some spectrum on the different fiber links) and the RMSA algorithm decision is either to assign a lightpath to the incoming request or to block it if there are not enough spectrum resources in the network. On the other hand, in a failure state (caused by an attack to multiple nodes), we consider a restoration mechanism where the non-affected lightpaths remain unchanged and the RMSA algorithm has to assign as much as possible new lightpaths to the affected demands in the available resources of the surviving network (i.e., the network without the attacked nodes). Next, we address the regular state and the failure state in separate subsections.

Table 1
Probability value π_i^s of each node $i \in N$ for each s in the example.

s	2	3	4	5	6
π_i^s ($w_i = 10$)	0.494	0.700	0.845	0.929	0.971
π_i^s ($w_i = 1$)	0.058	0.100	0.163	0.246	0.343

Table 2
Probability value π_i of each node $i \in N$ and path disaster availability of p_1 and p_2 for different $[s_m, s_M]$ ranges.

s_m	s_M	π_i ($w_i = 10$)	π_i ($w_i = 1$)	a_{p_1}	a_{p_2}
2	3	0.577	0.074	0.336	0.628
2	4	0.638	0.095	0.268	0.550
2	5	0.684	0.118	0.217	0.469
2	6	0.717	0.144	0.178	0.393

3.1. RMSA algorithm in the regular state

Recall that we consider an EON topology defined by a graph $G = (N, E)$, with a set of $n = |N|$ nodes and a set of $|E|$ undirected links. Consider also $F = \{1, 2, \ldots, |F|\}$ as the ordered set of Frequency Slots (FSs) available on each fiber link to be assigned to lightpaths. In the regular state, a set of lightpaths is already established and there is a request d for a new demand to be accepted.

The type of request d can be either unicast or anycast. An unicast request d is characterized by a pair of end-nodes (s_d, t_d) and its required bit-rate b_d. In anycast requests, the network supports a set R of services and each anycast service $r \in R$ is provided by a set of Data Centers (DCs) located in nodes $C_r \subseteq N$. Then, an anycast request d is characterized by a source node s_d, an anycast service $r_d \in R$ and a required bit-rate b_d (the anycast request d can be satisfied by any of the DCs in C_{r_d}).

Consider $\mathcal{P}_d$ as the set of candidate paths that can be selected for request d. If d is of unicast type, $\mathcal{P}_d$ is a set of different routing paths between s_d and t_d. If d is of anycast type, $\mathcal{P}_d$ is a set of different routing paths between s_d and one of the nodes in C_{r_d}. When the incoming request d is accepted, the RMSA decision is the specification of a lightpath to support d, which is defined by a routing path p selected from $\mathcal{P}_d$, a modulation format (MF) for electrical-optical-electrical conversion on the end-nodes of the lightpath and a set of contiguous FSs occupied by the lightpath in all fiber links of the selected routing path p.

In all RMSA algorithms, a set of parameters is associated to each candidate path $p \in \mathcal{P}_d$ and the path of the lightpath is selected as the candidate path with the best parameter values. One of the associated parameters is a_p indicating the path disaster availability of each candidate path $p \in \mathcal{P}_d$ as already defined in (2) of section 2.2.

Note that each MF has an associated transmission reach, which specifies an optical length threshold above which the lightpath does not work. So, another parameter associated to each candidate path $p \in \mathcal{P}_d$ is n_p indicating the number of FSs of the most efficient MF (the one requiring less FSs able to support the bit-rate b_d of request d) whose transmission reach is not lower than the optical length of p. We consider the optical length of each candidate path $p \in \mathcal{P}_d$ as the sum of its link lengths plus a given length value Δ per intermediate node (modeling the optical degradation suffered by a lightpath while traversing an intermediate optical switch).

Finally, based on the required number of FSs, given by the value of parameter n_p, and on the free FSs in all the links of each candidate path $p \in \mathcal{P}_d$ at the time instant of request d, another associated parameter is f_p indicating the highest FS index of the lowest set of n_p free contiguous FSs available in path p (this parameter is only considered in the candidate paths $p \in \mathcal{P}_d$ with enough available resources, i.e., with at least one set of n_p free contiguous FSs).

First, we describe three basic RMSA algorithms where the first two (FF and LFS) are well-known algorithms and the third one aims to obtain the best resilience to multiple node failures.

First-Fit (FF): Request d is routed in the first path $p \in \mathcal{P}_d$ with enough available resources and assigned with the lowest set of n_p free contiguous FSs (in this algorithm, $\mathcal{P}_d$ is ordered from the shortest to the longest optical length).

Lowest Frequency Slot (LFS): Among the paths $p \in \mathcal{P}_d$ with enough available resources, request d is routed in the path p with lowest f_p and assigned with the set of n_p free contiguous FSs whose highest FS index is f_p. If multiple paths have the same value of f_p, the path among them with the shortest optical length is selected.

Path Disaster Availability (PDA): Among the paths $p \in \mathcal{P}_d$ with enough available resources, request d is routed in the path p with the highest path disaster availability a_p and assigned with the lowest set of n_p free contiguous FSs. If multiple paths have the same value of a_p, one of them is selected with the **LFS** rule.

In [17], one of the main findings (in the offline variant of the RMSA problem) is that **LFS** is the best RMSA in terms of spectrum usage efficiency (as it keeps a larger portion of the highest spectrum completely free) and **PDA** is the best RMSA in terms of resilience to multiple node failures (as it avoids the selection of paths involving the nodes with higher probability of being attacked).

In general, the best trade-off between spectrum usage efficiency and resilience to multiple node failures depends on the load level of the network: (i) when the EON is lightly loaded, there are plenty of free resources and the spectrum usage efficiency can be relaxed to reach a better resilience to multiple node failures; (ii) when the EON is heavily loaded, the spectrum must be used in the most efficient way to maximize the acceptance probability of future demand requests.

In order to reach the best trade-off between these two aims in a dynamic EON (where, typically, the network oscillates over time between different load levels), we also propose RMSA algorithms combining the path disaster availability metric with two spectrum usage metrics in three different possible options. In all three options, we compute an additional parameter m_p for each path $p \in \mathcal{P}_d$ with enough available resources and the aim is to select the path p with the highest value of m_p.

The way parameter m_p is computed in each option is as follows. In the first option, parameter m_p is given by:

$$m_p = \left(1 - \frac{H}{|F|}\right) a_p + \frac{H}{|F|}\left(1 - \frac{f_p}{|F|}\right) \tag{6}$$

where H is the current highest FS occupied in at least one fiber link (which is used as a measure of the current network load). In this option, we combine the maximization of the path disaster availability a_p with the minimization of the spectrum usage metric given by f_p. Note that a higher value of $\left(1 - \frac{f_p}{|F|}\right)$ represents a lower value of f_p as desired by maximizing the combined parameter m_p. Moreover, both a_p and $\left(1 - \frac{f_p}{|F|}\right)$ terms are normalized as both values are between 0 and 1. So, when H is lower, the path disaster availability a_p has a higher weight in the determination of m_p, while when H is higher, the FS index f_p has a higher weight in the determination of m_p. In the second option, parameter m_p is given by:

$$m_p = \left(1 - \frac{H}{|F|}\right) a_p + \frac{H}{|F|} \frac{1}{\log_{\beta}(\alpha_p)} \tag{7}$$

where α_p is total number of FSs occupied by the lightpath to support request d in candidate path p (i.e., α_p is given by n_p multiplied by the number of fiber links of path p). In this second option, the spectrum usage metric α_p aims to give preference to paths using less spectrum resources so that more resources remain free for future requests. Again, a higher value of $\frac{1}{\log_{\beta}(\alpha_p)}$ represents a lower value of α_p as desired by maximizing the combined parameter m_p. In order to normalize the term $\frac{1}{\log_{\beta}(\alpha_p)}$ between 0 and 1, we consider β as the minimum number of FSs that can be required by any lightpath in any candidate path. Finally, in the third option, parameter m_p is given by:

$$m_p = \left(1 - \frac{H}{|F|}\right) a_p + \frac{H}{|F|}\left(\frac{1}{2}\left(1 - \frac{f_p}{|F|}\right) + \frac{1}{2}\frac{1}{\log_{\beta}(\alpha_p)}\right) \tag{8}$$

where the two previous spectrum usage metrics (the minimization of the highest FS index f_d used in (6) and minimization of the total number of required FSs α_p used in (7)) are combined with equal weight in the second term of (8). The resulting combined RMSA algorithms are as follows.

Mixed RMSA: Among the paths $p \in \mathcal{P}_d$ with enough available resources, request d is routed in the path p with the highest m_p and assigned with the lowest set of n_p free contiguous FSs. If multiple paths have the same value of m_p, the path among them with the shortest optical length is selected. Depending on the option to compute the values m_p, we obtain three different variants – Variant 1, 2 and 3 – of the **Mixed RMSA**, using eqs. (6)–(8), respectively.

Assuming that the set of candidate paths is computed in advance for all possible demand requests (which is possible as the network topology does not change over time in the regular state), all algorithms require in the worst case the computation of the different parameters for all candidate paths and the processing of each parameter is linear with the number of nodes included in each candidate path (which is at most n). So, the complexity of all RMSA algorithms is $\mathcal{O}(n \times |\mathcal{P}_d|)$. Note that the **FF** algorithm has lower complexity when compared with all other algorithms as it needs to run up to the first candidate path that can be used to assign the lightpath while all the others require the computation of all candidate paths.

3.2. RMSA algorithm in a failure state

In a failure state caused by an attack to multiple nodes, the non-affected lightpaths remain unchanged and the RMSA algorithm tries to assign as much as possible new lightpaths to the affected demands in the available resources of the surviving EON, i.e., the network without the attacked nodes.

In this case, the resilience to node failures is not a priority and the RMSA must have the lowest possible complexity as it has to assign lightpaths not for a single request but for all affected demands. So, we consider the **FF** algorithm adapted to the failure cases. The complete algorithm has 3 phases.

First phase: the algorithm computes the FSs occupied by the non-affected lightpaths and runs a k-shortest paths algorithm for each affected demand to compute its set of candidate paths in the surviving network.

Second phase: the set of affected demands d with a non-empty set of candidate paths (i.e., the ones such that the k-shortest path has returned at least one candidate path) is ordered following the next three hierarchical orders (from the most important to the least important):

1. decreasing order of its bit-rate b_d;
2. decreasing order of the number of links of the shortest optical length path;
3. decreasing order of the optical length of the shortest optical length path.

Third phase: starting with the FSs occupied by the non-affected lightpaths (computed in first phase), the algorithm tries to assign iteratively a lightpath to each demand by the order computed in second phase and using the **FF** algorithm; at each iteration, when a new lightpath is assigned to a demand, the set of occupied FSs is updated before the next iteration.

The hierarchical order used in the second phase was shown in our preliminary tests to provide the best performance in terms of total surviving demand. Note that, in a failure state, it is no longer possible to compute in advance the set of candidate paths as the set of failing nodes cannot be predicted. The complexity of the algorithm is mainly imposed by the first phase where a k-shortest paths algorithm must be run between many node pairs and its complexity is $\mathcal{O}(kn(|E| + n\log(n)))$ for each pair of nodes [20] when using Yen's algorithm [21].

4. Simulation description

An event-driven simulator was developed to evaluate the spectrum usage efficiency and the resilience to multiple node failures of the different RMSA algorithms in dynamic EONs. The spectrum usage efficiency is assessed by the bit-rate amount of all requests that are blocked in the regular state due to insufficient free spectrum resources. The resilience to multiple node failures is evaluated by the average non-disrupted demand (the average bit-rate percentage that is not disrupted after a multiple node failure) and the average surviving demand (the average bit-rate percentage that is supported after a multiple node failure) among all failure events of each simulation.

A simulation is composed by two modules, one simulating the regular state and another simulating the failures states, which are described separately in the next subsections.

4.1. Simulation of the regular state

In the regular state, events are associated with time instants when the EON has either to assign a lightpath to a new request or to tear down a previously assigned lightpath. In each simulation, λ is the arriving request rate (per time unit) at the end of the simulation and the lightpath duration is exponentially distributed with an average duration of one time unit.

Each simulation runs a total number of events given by $\mathcal{E}$ and the arriving request rate is $\frac{e}{\mathcal{E}} \times \lambda$, where $e = 1, 2, \ldots, \mathcal{E}$ is the current event number. In this way, a single run simulates all network load values from a very lightly loaded network (at the beginning of the simulation) up to a heavily loaded network (at the end of the simulation). Parameter λ is tuned for each network case so that the blocking probability at the end of the simulation is around 10 % for the worst RMSA algorithm.

Each unicast request d has its end-nodes (s_d, t_d) randomly generated with a uniform distribution among all node pairs and its bit-rate b_d (in Gbps) randomly generated with a uniform distribution in the set {50, 100, 150, 200} resulting in an average bit-rate request of 125 Gbps. On the other hand, each anycast request d has its source node s_d randomly generated with a uniform distribution among all nodes, its anycast service r_d randomly generated with a uniform distribution among all anycast services and its bit-rate b_d (in Gbps) randomly generated with a uniform distribution in the set $\{50 \times \omega : \omega \in \mathbb{N},\ \omega \leq 20\} = \{50, 100, \ldots, 1000\}$ resulting in an average bit-rate request of 525 Gbps.

At each request event, first the request type is randomly selected between unicast with probability p_{uni} or anycast (with probability $1 - p_{uni}$). Then, the request of each type is randomly generated as described before. In all simulations, we have considered that the total generated bit-rate is equally split between unicast and anycast services. Since the average bit-rate request is 125 Gbps for unicast and 525 Gbps for anycast, p_{uni} was set to:

$$p_{uni} = \frac{525}{125 + 525} = \frac{21}{26}$$

.

In the simulations reported in the computational results, we have set $\mathcal{E} = 10^5$ events. Moreover, for a fair evaluation between the different RMSA algorithms, we have randomly generated all parameters associated with request events once for each network, and used the same values when simulating the different RMSA algorithms for the same network.

4.2. Simulation of the failure states

When the regular state reaches the event numbers in set $\mathcal{E}_f$, the failure state simulation module is launched and, when this module ends, the regular state simulation continues from the state it was before. The simulation of a failure state has the following 3 steps:

1. generate a random multiple node failure event;
2. run the RMSA algorithm (as described in section 3.2) taking into account the regular state at the moment of the failure event and the set of failure nodes;
3. compute the resulting total non-disrupted bit-rate and surviving bit-rate of the current failure event.

The random generation of a multiple node failure event in step 1 follows the attack model described in section 2.1. First, the number of attacked nodes s is randomly generated between s_m and s_M with the probabilities given by (1). Then, a set of s nodes is randomly selected (without replacement) with a probability of each node $i \in N$ being selected proportional to its weight w_i.

At the end of the regular state simulation, the average non-disrupted demand and the average surviving demand performance parameters are computed based on the values obtained on all failure events run in the set $\mathcal{E}_f$ of event numbers.

In the simulations reported in the computational results, we have considered set $\mathcal{E}_f$ composed by the event numbers multiple of 100 in the range $10^3 < e \leq \mathcal{E}(= 10^5)$, which gives a total of 990 multiple node failure events per simulation. The aim was to select the set $\mathcal{E}_f$ uniformly from a minimum number (below which the network load is very low) until $\mathcal{E}$ so that the resilience performance parameters are assessed over the whole range of network loads. Again, for a fair evaluation between the different RMSA algorithms, we have randomly generated all multiple node failure events once for each network and used the same node failures when simulating the different RMSA algorithms for the same network.

5. Computational results

The computational results presented in this section are based on 3 network topologies with public available information [19] and shown in Fig. 2: Germany50, Cost266 and Janos-US. Table 3 presents their topology characteristics in terms of number of nodes n and fiber links $|E|$, average node degree $\overline{\delta}$, average link length $\overline{l}$ (in Km) and diameter D, i.e., the highest optical length (in Km) among all shortest paths adding Δ per intermediate node (the length Δ modeling the degradation suffered by a lightpath on each intermediate node was set to 60 km).

In each network, we have considered a set of five anycast services ($|R| = 5$) and each service $r \in R$ is run on five randomly selected DC nodes. We restricted the possible DC locations of each anycast service to set $C \subset N$ (highlighted in large circles in Fig. 2) which was selected among the nodes with largest node degree (the number of such nodes is also provided in the last column of Table 3). Then, the DC node locations (set C_r) providing each anycast service $r \in R$ were randomly selected with a uniform distribution among the nodes in C.

In the regular state, the set of candidate paths associated to each incoming unicast request d was computed with a k-shortest paths algorithm (considering $k = 30$) and the same set was used for all RMSA algorithms. In anycast requests, we have considered the union of the sets of the $k = 30$ shortest paths from the source node s_d to each DC node of its anycast service r_d, and then excluded from the union set the paths that have intermediate DC nodes of the same service. In each failure state, we have considered up to $k = 5$ shortest paths as the candidate paths in the surviving topology. Notice that, in both states, if the number of feasible paths is lower than k, we consider all possible paths as the set of

Table 3
Topology characteristics of each network.

Network	$n = \|N\|$	$\|E\|$	$\overline{\delta}$	$\overline{l}$ (Km)	D (Km)	$\|C\|$
Germany50	50	88	3.52	100.7	1417	11
Cost266	37	57	3.08	438.1	4574	9
Janos-US	26	42	3.23	600.6	5094	7

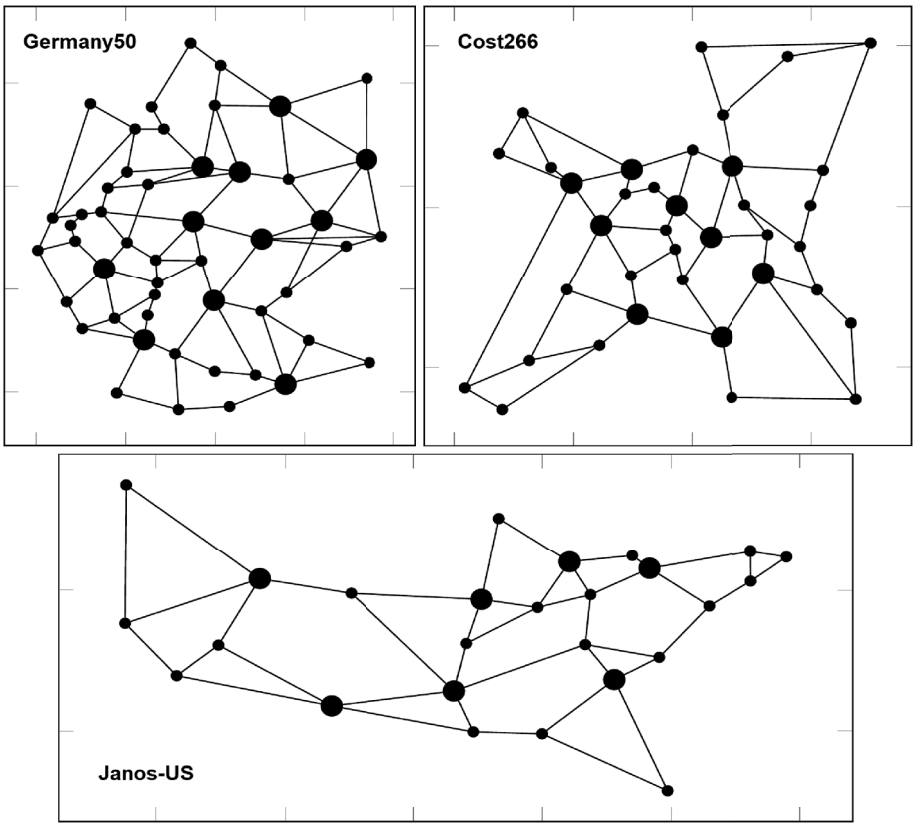

Fig. 2. Network topologies.

candidate paths.

We have considered a capacity of $|F| = 320$ FSs on all fiber links of the network, which corresponds to a spectral grid of granularity 12.5 GHz. We have assumed 4 available MFs whose transmission reach and bit-rate capacity are presented in Table 4 (transceiver model based on [22] and transmission reaches based on [23]).

The number n_p of FSs required by each candidate path $p \in \mathcal{P}_d$ for a request d requiring a bit-rate b_d is computed based on the distance-adaptive transmission (DAT) rule as follows. We first select the highest bit-rate MF whose transmission reach is not lower than the optical length of p (the assumptions are that transceivers support polarization division multiplexing, operate at a fixed baud rate of 28 Gbaud, and transmit/receive on an optical channel occupying 37.5 GHz). If the bit-rate b_d of request d is not higher than the selected MF bit-rate, one single transceiver is required. Otherwise, multiple optical channels (each one used by one transceiver with the previous selected MF) are grouped in a single spectral super-channel (SCh). We assume that lightpaths require a 12.5 GHz guard-band and, so, the required number of contiguous FSs is $n_d = 3t + 1$, where t denotes the minimum number of transceivers with a total bit-rate not lower than b_d. Consequently, we set $\beta = 4$ in expressions (7) and (8) of the Mixed RMSA algorithm as $n_d = 3t + 1$ has a minimum of 4 when $t = 1$.

As explained in Section 4.1, parameter λ was tuned for each network case so that the blocking probability at the end of the simulation is around 10 % for the worst RMSA algorithm. After preliminary tests with each topology, we have considered $\lambda = 1200$ for Germany50, $\lambda = 550$ for Cost266 and $\lambda = 500$ for Janos-US.

Concerning the multiple node attacks, we have considered that the number of attacked nodes s is between $s_m = 2$ and $s_M = 6$ (we have excluded $s = 1$ since typical topologies are already resilient to single node failures). Moreover, the node weights (defining the probability of each node being discovered by the attacker) were assumed to be $w_i = 10$ for the DC nodes (set C) and $w_i = 1$ for all other nodes (set $N \backslash C$).

Concerning the obtained simulation results, Table 5 presents for each network the total rejected bit-rate obtained by each RMSA algorithm, i.e., the sum of the bit-rate values of all requests that were blocked in the regular state (the best values are highlighted in bold for each network). In this table (and in the following ones), Mv1, Mv2 and Mv3 refers to the Mixed RMSA Variants 1, 2 and 3, respectively, as described in section 3.1.

The results in Table 5 clearly show that the Mixed RMSA Variant 3 algorithm is the best alternative in terms of spectrum usage efficiency. Note that it is even better than the LFS algorithm which does not use the path disaster availability metric and selects the path only based on assigning the FSs on the lowest possible spectrum. Recall that the Mixed RMSA Variant 3 algorithm combines with equal weights two spectrum usage metrics (the minimization of the highest assigned FS and the minimization of the total number of assigned FSs). Moreover, the rejected bit-rates happen when the network is heavily loaded. In these cases, the weight of the spectrum usage metrics becomes close to 1 (and the weight of the path disaster availability metric becomes close to 0) in the Mixed RMSA algorithms. So, the results in Table 5 show that the combination of the two spectrum usage metrics with equal weights (of the Mixed RMSA Variant 3 algorithm) uses more efficiently the spectrum resources than considering only the minimization of the highest assigned FS (of the LFS algorithm).

On the other hand, both FF (which uses the basic first-fit approach) and PDA (which uses the path disaster availability metric as the first criterion) algorithms are the ones that, overall, are the least efficient in terms of spectrum usage. Finally, the other RMSA algorithms present intermediate results.

Table 4
Transmission reach and bit-rate capacity of each MF.

Modulation Format (MF)	BPSK	QPSK	8-QAM	16-QAM
Transmission reach (km)	6300	3500	1200	600
Bit-rate capacity (Gbps)	50	100	150	200

Table 5
Total rejected bit-rate (in Gbps) results.

Network	FF	LFS	PDA	Mv1	Mv2	Mv3
Germany50	46800	2600	49150	3650	35100	**1700**
Cost266	43900	19350	36500	18700	33950	**14350**
Janos-US	35250	19900	42600	18700	33500	**12400**

Concerning the resilience to multiple node failures, Table 6 presents for each network the average non-disrupted demand, in percentage, obtained by each RMSA algorithm, i.e., the average bit-rate percentage that is not disrupted after a multiple node failure (again, best values highlighted in bold). As expected, the PDA algorithm is the best RMSA algorithm since, by using the path disaster availability metric, minimizes the probability of the selected routing paths to be affected by the multiple node failures. On the other hand, the FF and LFS algorithms are worst, on average, than the PDA algorithm.

Concerning the Mixed RMSA algorithms (which combine the path disaster availability metric with spectrum usage metrics), they do not seem to be as good as the PDA algorithm. Nevertheless, these values represent percentages over the total bit-rate accepted in the network at the time instant of each failure event. Recall from the previous Table 5 that the Mixed RMSA Variant 3 has a much smaller total rejected demand. So, for this RMSA algorithm, the percentage values in Table 6 represent absolute non-disrupted demands which are closer to the ones of the best PDA algorithm.

Finally, Table 7 presents for each network the average surviving demand, in percentage, obtained by each RMSA algorithm, i.e., the average bit-rate percentage that is supported after a multiple node failure (again, best values highlighted in bold). In this case, the Mixed RMSA Variant 3 is the best, on average, although for each network the results are very close between the different RMSA algorithms. This is due to the fact that in a multiple node failure, many of the affected lightpaths have end-nodes which become disconnected in the surviving network. Like in the previous table, the values of Table 7 represent percentages over the total bit-rate accepted in the network at the time instant of each multiple node failure. So, since the Mixed RMSA Variant 3 has a much smaller total rejected demand (seen in Table 5), we reach the conclusion that the Mixed RMSA Variant 3 is the best algorithm concerning the average surviving demand parameter.

In overall, the best algorithm among all tested ones is the Mixed RMSA Variant 3 as it is the most efficient in terms of spectrum usage (reaching the lowest level of rejected bit-rate) and, concerning the resiliency to multiple node failures, it is the most efficient in terms of average surviving demand and almost as efficient as the PDA algorithm in terms of average non-disrupted demand.

Note that, upon a multiple node failure event, there are demands that cannot survive in the surviving network whatever RMSA is adopted. The obvious ones are the demands such that at least one of their end-nodes has failed. Moreover, if the multiple node failure event splits the network in different components: (i) unicast demands cannot survive if their end-nodes are in different components and (ii) anycast demands cannot survive if their source nodes are in a network component without any of the DC nodes of their anycast service.

In the results of both Tables 6 and 7, the performance values obtained by all RMSA algorithms are always better for Germany50,

Table 6
Average non-disrupted demand (%) results.

Network	FF	LFS	PDA	Mv1	Mv2	Mv3
Germany50	67.61	64.96	**70.98**	67.88	69.24	68.86
Cost266	58.71	57.17	**62.10**	59.85	60.76	60.46
Janos-US	53.86	50.97	**55.03**	53.01	54.81	53.88

Table 7
Average surviving demand (%) results.

Network	FF	LFS	PDA	Mv1	Mv2	Mv3
Germany50	89.46	89.70	89.31	89.70	89.48	**89.74**
Cost266	83.56	83.58	83.40	83.58	83.57	**83.59**
Janos-US	**75.17**	75.12	74.82	75.14	75.04	75.15

intermediate for Cost266 and worst for Janos-US. In order to better understand these results, we have also analyzed the type of surviving networks that were imposed by all failure events on each network. In graph theory, a disconnected network is a graph that does not contain a path for at least one of its node pairs. Moreover, a 1-connected network is a graph such that the minimum number of elements (nodes and edges) whose removal makes the network disconnected is 1. Finally, a 2-connected network is a graph such that the minimum number of elements whose removal makes the network disconnected is 2. Table 8 presents, for each network, the relative frequency (in percentage) of each type of surviving network among all 990 simulated failure events.

Note that a 2-connected surviving network is more likely to have enough resources to assign lightpaths to the affected demands than a 1-connected surviving network. In Table 8, although most of the surviving networks are 1-connected for all networks, the network with the best resilience to multiple node failures (i.e., Germany50) is the one with the lowest percentage of disconnected surviving networks and the highest percentage of 2-connected surviving networks. On the other hand, the network with the worst resilience to multiple node failures (i.e., Janus-US) is the one with the highest percentage of disconnected surviving networks and the lowest percentage of 2-connected surviving networks.

Next, we present different visualizations of the conducted simulations to further analyze the reasons for the best performance of the Mixed RMSA Variant 3 algorithm. The different simulations are visualized comparing this algorithm with the LFS (whose decision aims only the best spectrum usage efficiency) and with the PDA (whose decision aims primarily the best resiliency to multiple node failures).

Using the highest allocated FS (parameter H in section 3.1) as a measure of the network load, Fig. 3 visualizes the evolution of the highest allocated FS as a function of the event number for the three RMSA algorithms on each of the three networks (in each plot, the plotted value on each event number is the average value of H in the last 1000 events).

Fig. 3 shows that, for all networks, the spectrum usage is the lowest in most of the events with LFS reaching the highest load values only at the events very close to the end of the simulation. On the other hand, the spectrum usage is the highest in all events with PDA reaching the highest load values much sooner than LFS (the reason why the PDA algorithm has a poor performance in terms of total rejected bit-rate). Finally, the Mixed RMSA Variant 3 algorithm is similar to PDA at the lower network load values (when there are plenty of free resources and the spectrum usage efficiency can be relaxed to reach a better multiple node failure resiliency) and gets slightly lower (i.e., better), on average, than LFA as the network load becomes very high (when the free spectrum resources become very scarce and the spectrum resources must be efficiently used).

As already discussed, there are affected demands that cannot survive whatever RMSA is adopted. In the simulations, we have also computed the total bit-rate that can survive in terms of connectivity on each failure event. Next figures visualize the evolution of the non-disrupted demand (Fig. 4) and the surviving demand (Fig. 5) as a function of the consecutive failure events for the three RMSA algorithms on each of the three networks. Both non-disrupted and surviving demands are computed as the ratio (in percentage) between their absolute bit-rate values and the total bit-rate that can survive at each failure event (in each plot, the plotted value on each failure event is the average value over the last 100 failure events).

As expected, the visualizations in Fig. 4 show that PDA is always the best and LFS is always the worst algorithm concerning the non-disrupted demand. Moreover, the Mixed RMSA Variant 3 algorithm is as good as the best in the initial failure events (as it gives a higher weight to the path disaster availability metric when the network load is low) and becomes worse than the best PDA algorithm but still always better than the LFS algorithm (as it keeps using the path disaster availability metric on its decision although with a lower weight).

Regarding the surviving demand, the visualizations in Fig. 5 show that all RMSA algorithms are able to maintain 100 % of all survivable bit-rate for the lower values of network load. This is not surprising as there is plenty of the resources in the surviving network in these cases and this is the reason why the average surviving demand results shown in Table 6 are so close between the different RMSA algorithms. Then, when failure events happen in higher network load values, only part of the survivable bit-rate can survive and the Mixed RMSA Variant 3 becomes consistently better than the two other algorithms.

Concerning simulation running times, Table 9 presents the total running time of each simulation, including the regular state and all failure states. Recall that we have considered the same number of events (both in terms of request and failure events) for all simulations of all networks. However, the runtime values in Table 9 increase with the size of the network. The reason for this increase is a combination of two factors. One in that bigger networks accommodate more lightpaths and so, in multiple node failure events, the RMSA algorithm has to deal with more affected demands, on average. The other is that the k-shortest paths algorithm which is run in every RMSA decision takes longer runtime in bigger networks.

Moreover, there are some noticeable differences between the runtime values of the different RMSA algorithms for the same network. The reason for these differences is again a combination of two factors. One is the complexity of each RMSA decision: FF is clearly the less complex algorithm while the Mixed RMSA variants are the more complex ones. The second is the performance of each algorithm in terms of non-disrupted demand: the most efficient algorithms minimize the number of disrupted lightpaths and the required RMSA decision in the failure state becomes quicker as it involves a smaller number of affected demands.

As a final note, recall that the node weights defining the probability of each node being discovered by the attacker were assumed to be $w_i = 10$ for the DC nodes and $w_i = 1$ for all other nodes. Some additional simulation tests were conducted (not reported here) with different weight sets. The conclusions between the different proposed RMSA algorithms are similar to the ones reported here as long as the ratio between the highest weight and the lowest weight is significant. When this ratio is small, the probability of each node being attacked (when an attack is realized) becomes similar among all nodes and the path disaster availability of candidate paths becomes inversely proportional to the number of links of the path. In this case, the maximization of the path disaster availability tends to select the same paths as the minimization of the number of assigned FSs in all links of the path (the second considered spectrum usage metric used in the Mixed RMSA Variant 3) as the number of links of the path becomes the main optimization factor of both metrics. Again the Mixed RMSA Variant 3 is the best overall algorithm but the difference between its performance and the performance of the other RMSA algorithms becomes smaller than the ones reported here. In particular, the FF algorithm becomes better as it selects the first path with enough available spectrum resources considering the paths ordered from the shortest to the longest optical length and there is

Table 8
Relative frequency (in %) of each type of surviving network.

Network	Disconnected	1-connected	2-connected
Germany50	4.24	60.51	35.25
Cost266	17.07	72.12	10.81
Janos-US	40.61	55.15	4.24

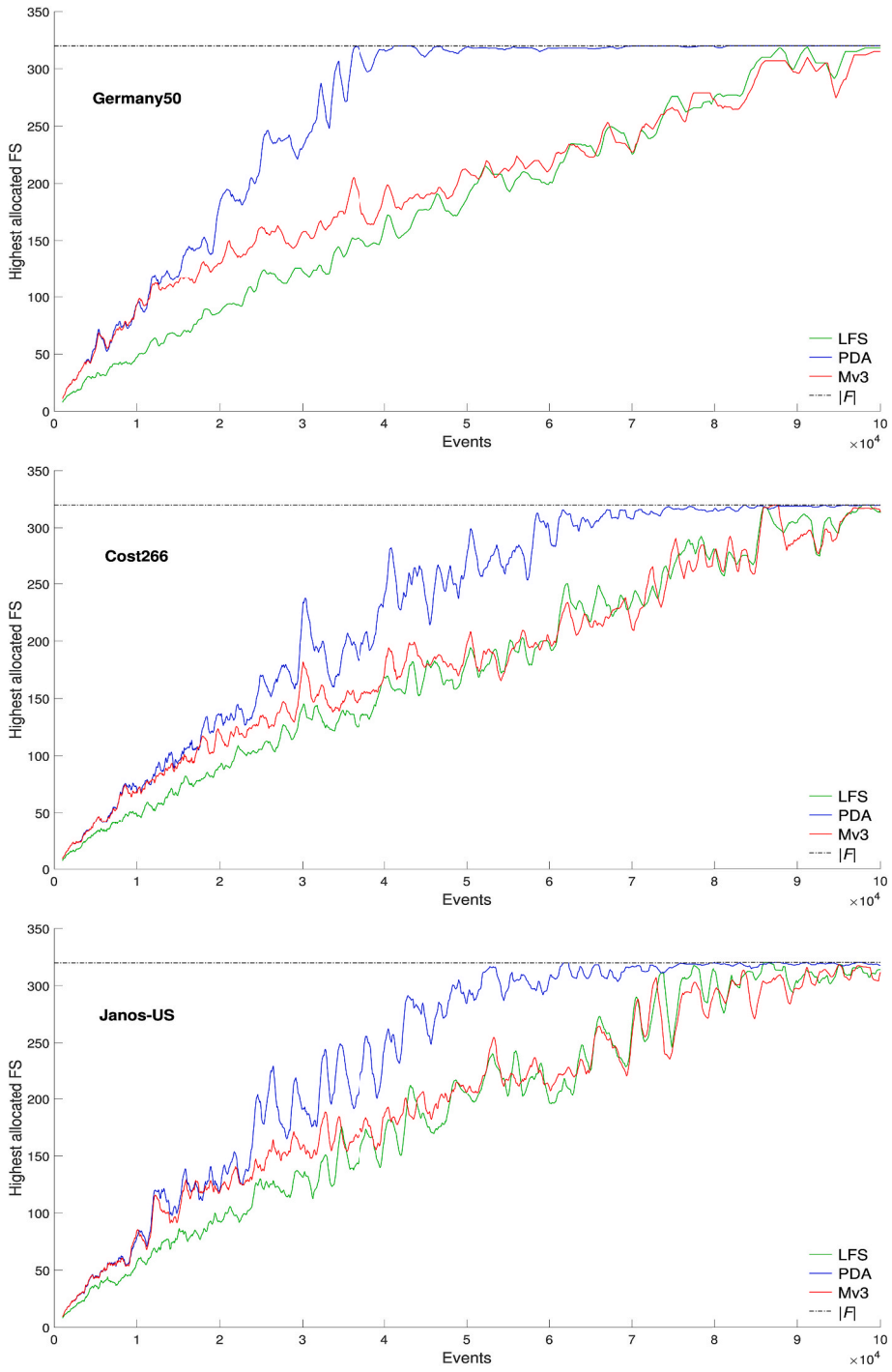

Fig. 3. Evolution of the highest allocated FS as a function of the event number in the regular state ($|F|$ is the number of FSs on each fiber link).

a strong positive correlation between the optical length of a path and its number of links.

6. Conclusions

In EONs, the RMSA algorithm rules the way the optical spectrum of the EON is assigned to each service demand with the primary goal of using the spectrum resources in an efficient way. Then, other goals can also be addressed as long as the spectrum usage efficiency is not jeopardized. One such goal is the resilience of the EON to large-scale failures and one source of such failures is malicious human activities. In terrorist attacks, although node shutdowns are harder to realize than link cuts, they are the most rewarding in the attackers' perspective since the shutdown of one node also shuts down all its fiber links.

In a previous work, a path disaster availability metric was proposed for the RMSA decision which takes into account the probability of each path not being disrupted by a multiple node failure. Here, we have proposed a set of RMSA algorithms that make use of the path disaster availability metric for dynamic EONs where requests arrive randomly one at a time and the accepted ones last in the network for a random time duration.

To evaluate the proposed RMSA algorithms, we have developed an event-driven simulator able to assess the spectrum usage efficiency of the different RMSA algorithms and also their resilience to multiple node

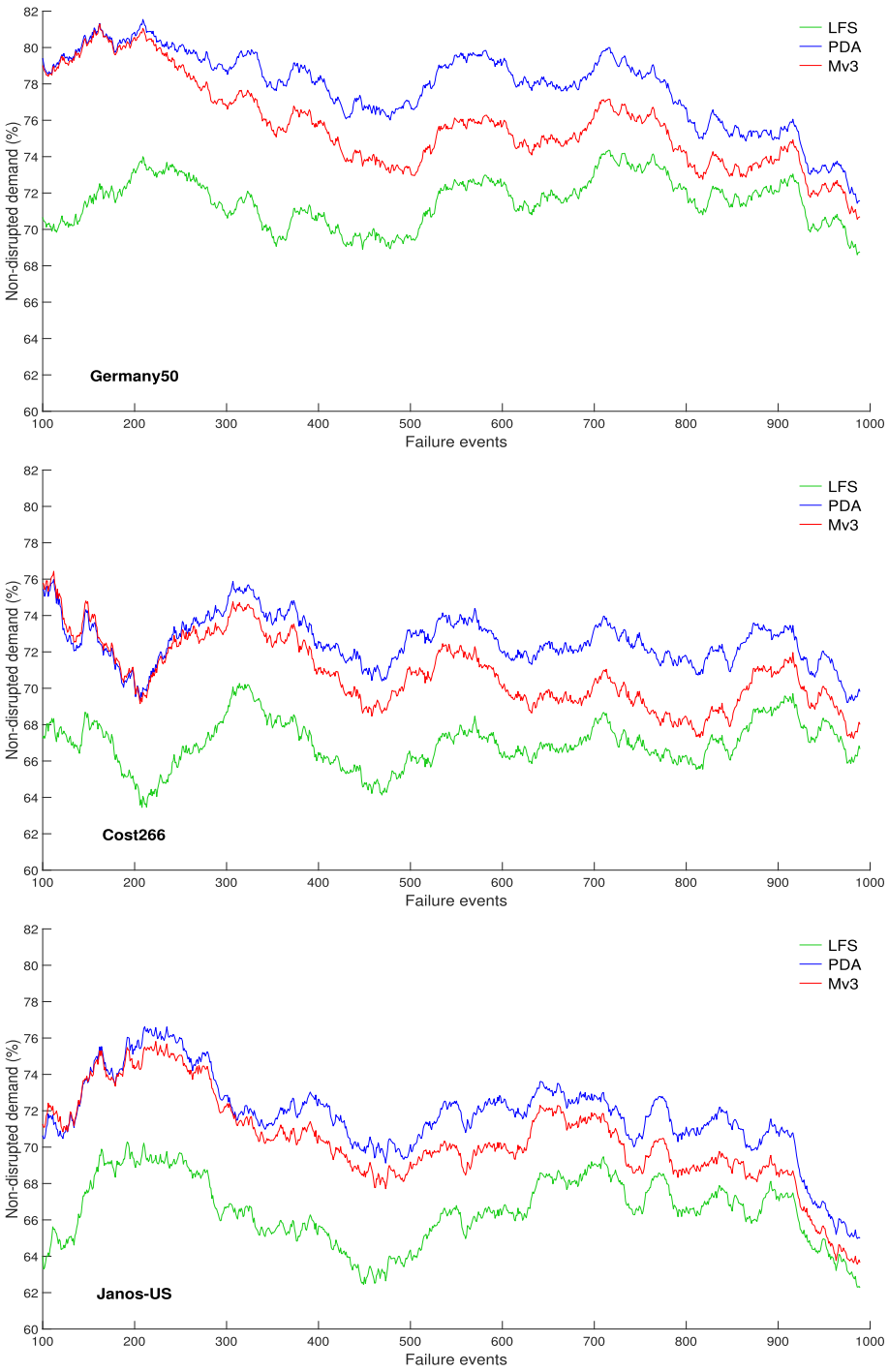

Fig. 4. Evolution of the non-disrupted demand, in percentage, as a function of the consecutive failure events.

failures assessed by 2 parameters: the average non-disrupted demand and the average surviving demand. All algorithms were evaluated through simulation considering a mix of unicast and anycast services in 3 well-known topologies and, in the failure cases, a restoration mechanism where the non-affected lightpaths remain unchanged and the demands of the affected lightpaths are reassigned as much as possible in the spectrum resources of the surviving network.

In the simulations, we have compared two commonly used RMSA algorithms (FF and LFS) with different proposed RMSA algorithms using the path disaster availability metric: the PDA algorithm and the 3 variants of the Mixed RMSA algorithm. PDA uses the path disaster availability metric as its primary criterion. The 3 variants of the Mixed RMSA combine in three different ways the path disaster availability metric with 2 spectrum usage metrics: the lowest assigned frequency slot and the number of assigned frequency slots. Moreover, the combination takes into consideration the current load of the EON so that the resilience to multiple node failures has a higher weight in the RMSA decision when the EON is lightly loaded while the spectrum usage metrics have a higher weight in the RMSA decision when the EON is heavily loaded.

The simulation results have shown that the RMSA algorithm that combines the path disaster availability with the two spectrum usage metrics (named Mixed RMSA Variant 3 algorithm) is the best trade-off between the spectrum usage efficiency and the resilience of the EON to multiple node failures: this algorithm is the most efficient in terms of

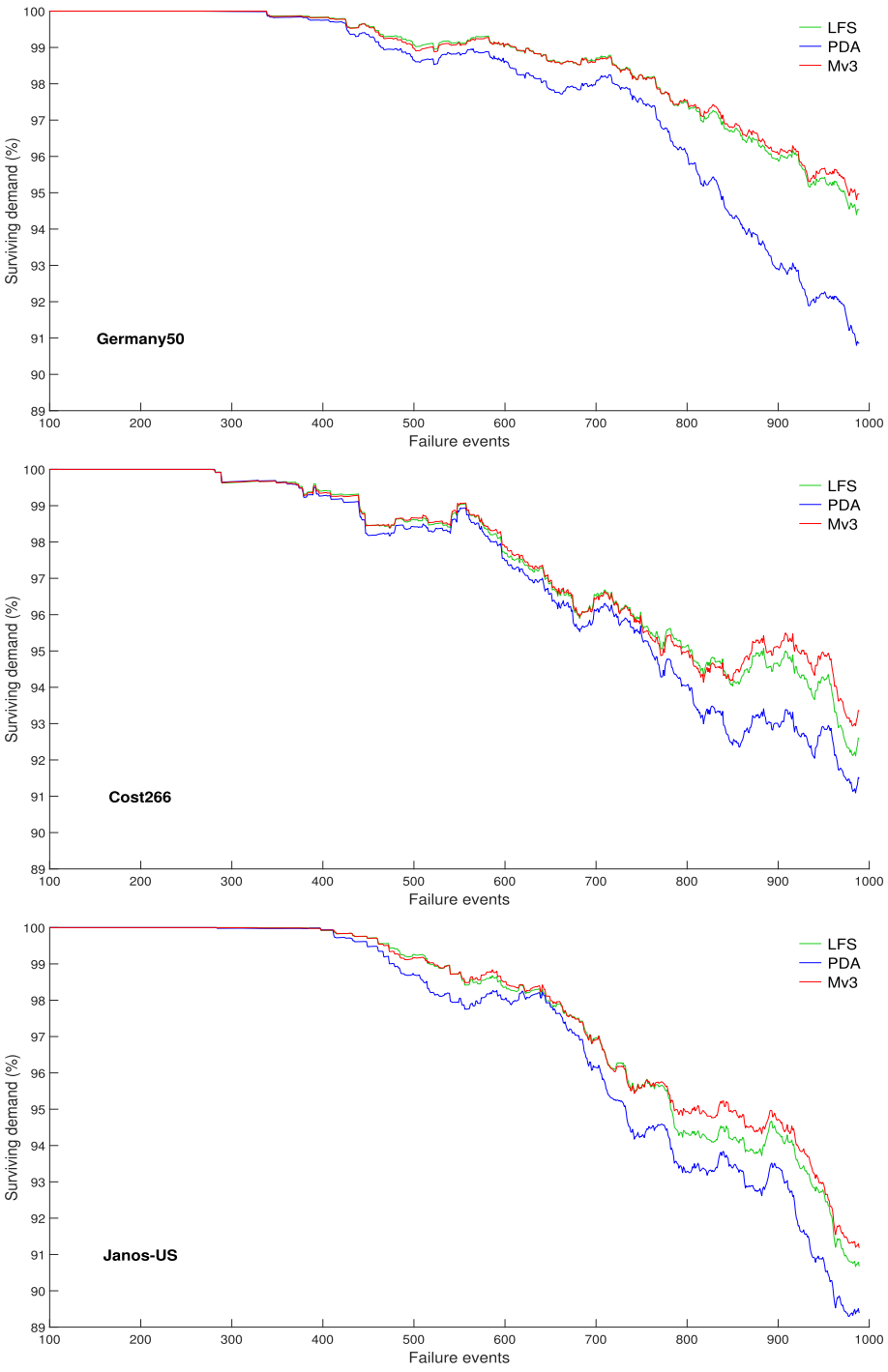

Fig. 5. Evolution of the surviving demand, in percentage, as a function of the consecutive failure events.

Table 9
Total running time (in the format H:MM:SS) of each simulation.

Network	FF	LFS	PDA	Mv1	Mv2	Mv3
Germany50	1:00:33	1:08:51	0:52:10	1:04:27	0:59:11	1:04:44
Cost266	0:20:11	0:22:57	0:18:52	0:22:04	0:20:23	0:21:43
Janos-US	0:06:17	0:08:10	0:06:56	0:07:57	0:07:06	0:07:47

spectrum usage (reaching the lowest level of rejected bit-rate) and, concerning the resiliency to multiple node failures, it is the most efficient in terms of average surviving demand and almost as efficient as the PDA algorithm in terms of average non-disrupted demand.

Authors statement

The authors declare that have seen and approved the final version of the manuscript being submitted. They warrant that the article is the authors' original work, hasn't received prior publication and isn't under consideration for publication elsewhere.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by FEDER Funds and National Funds through FCT, Portugal, under the project ResNeD CENTRO-01-0145-FEDER-029312. F. Barbosa was also supported by FCT, Portugal, under the PhD Grant SFRH/BD/132650/2017. K. Walkowiak and R. Goścień were also supported by the National Science Centre, Poland, under Grant No. 2017/27/B/ST7/00888. R. Goścień was also partially supported by the Foundation for Polish Science (FNP).

References

[1] K. Christodoulopoulos, I. Tomkos, E.A. Varvarigos, Elastic bandwidth allocation in flexible ofdm-based optical networks, J. Lightwave Technol. 29 (9) (2011) 1354–1366, https://doi.org/10.1109/JLT.2011.2125777.

[2] M. Klinkowski, K. Walkowiak, Routing and spectrum assignment in spectrum sliced elastic optical path network, IEEE Commun. Lett. 15 (8) (2011) 884–886, https://doi.org/10.1109/LCOMM.2011.060811.110281.

[3] K. Walkowiak, M. Klinkowski, Joint anycast and unicast routing for elastic optical networks: modeling and optimization, in: 2013 IEEE International Conference on Communications (ICC), 2013, pp. 3909–3914, https://doi.org/10.1109/ICC.2013.6655168.

[4] S. Talebi, G.N. Rouskas, On distance-adaptive routing and spectrum assignment in mesh elastic optical networks, IEEE/OSA Journal of Optical Communications and Networking 9 (5) (2017) 456–465, https://doi.org/10.1364/JOCN.9.000456.

[5] F.S. Abkenar, A.G. Rahbar, Study and analysis of routing and spectrum allocation (rsa) and routing, modulation and spectrum allocation (rmsa) algorithms in elastic optical networks (eons), Opt. Switch. Netw. 23 (2017) 5–39, https://doi.org/10.1016/j.osn.2016.08.003.

[6] E. Palkopoulou, M. Angelou, D. Klonidis, K. Christodoulopoulos, A. Klekamp, F. Buchali, E. Varvarigos, I. Tomkos, Quantifying spectrum, cost, and energy efficiency in fixed-grid and flex-grid networks [invited], IEEE/OSA Journal of Optical Communications and Networking 4 (11) (2012) B42–B51, https://doi.org/10.1364/JOCN.4.000B42.

[7] B.C. Chatterjee, N. Sarma, E. Oki, Routing and spectrum allocation in elastic optical networks: a tutorial, IEEE Communications Surveys Tutorials 17 (3) (2015) 1776–1800, https://doi.org/10.1109/COMST.2015.2431731.

[8] R. Goścień, K. Walkowiak, M. Klinkowski, Tabu search algorithm for routing, modulation and spectrum allocation in elastic optical network with anycast and unicast traffic, Comput. Network. 79 (2015) 148–165, https://doi.org/10.1016/j.comnet.2014.12.004.

[9] J. Rak, D. Hutchison (Eds.), Guide to Disaster-Resilient Communication Networks, Computer Communications and Networks, Springer, 2020, https://doi.org/10.1007/978-3-030-44685-7.

[10] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P.O. Ugalde, A. Pašić, D. Pezaros, S. Jouet, S. Secci, M. Tornatore, A survey of strategies for communication networks to protect against large-scale natural disasters, in: 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), 2016, pp. 11–22, https://doi.org/10.1109/RNDM.2016.7608263.

[11] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, J.L. Marzo, An overview of security challenges in communication networks, in: 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), 2016, pp. 43–50, https://doi.org/10.1109/RNDM.2016.7608266.

[12] X. Chen, S. Zhu, L. Jiang, Z. Zhu, On spectrum efficient failure-independent path protection p-cycle design in elastic optical networks, J. Lightwave Technol. 33 (17) (2015) 3719–3729, https://doi.org/10.1109/JLT.2015.2456052.

[13] J. Wu, Z. Ning, L. Guo, Energy-efficient survivable grooming in software-defined elastic optical networks, IEEE Access 5 (2017) 6454–6463, https://doi.org/10.1109/ACCESS.2017.2674963.

[14] R. Goścień, M. Kucharzak, On the efficient optimization of unicast, anycast and multicast flows in survivable elastic optical networks, Opt. Switch. Netw. 31 (2019) 114–126, https://doi.org/10.1016/j.osn.2018.10.010.

[15] F. Barbosa, A. de Sousa, A. Agra, Topology design of transparent optical networks resilient to multiple node failures, in: 2018 10th International Workshop on Resilient Networks Design and Modeling (RNDM), 2018, pp. 1–8, https://doi.org/10.1109/RNDM.2018.8489825.

[16] F. Barbosa, A. de Sousa, A. Agra, Design/upgrade of a transparent optical network topology resilient to the simultaneous failure of its critical nodes, Networks 75 (4) (2020) 356–373, https://doi.org/10.1002/net.21933.

[17] F. Barbosa, A. de Sousa, A. Agra, K. Walkowiak, R. Goścień, A rmsa algorithm resilient to multiple node failures on elastic optical networks, in: 2019 11th International Workshop on Resilient Networks Design and Modeling (RNDM), 2019, pp. 1–8, https://doi.org/10.1109/RNDM48015.2019.8949141.

[18] S. Robinson, Simulation: the Practice of Model Development and Use, John Wiley & Sons, Inc., Hoboken, NJ, USA, 2004.

[19] S. Orlowski, R. Wessäly, M. Pióro, A. Tomaszewski, SNDlib 1.0 - survivable network design library, Networks 55 (3) (2010) 276–286, https://doi.org/10.1002/NET.V55:3.

[20] E. Bouille, G. Ellinas, J.-F. Labourdette, R. Ramamurthy (Eds.), Path Routing in Mesh Optical Networks, Wiley, 2007, https://doi.org/10.1002/9780470032985.

[21] J. Yen, Finding the k shortest loopless paths in a network, Manag. Sci. 17 (11) (1971) 712–716, https://doi.org/10.1287/mnsc.17.11.712.

[22] C. Rottondi, P. Boffi, P. Martelli, M. Tornatore, Routing, modulation format, baud rate and spectrum allocation in optical metro rings with flexible grid and few-mode transmission, J. Lightwave Technol. 35 (1) (2017) 61–70, https://doi.org/10.1109/JLT.2016.2627618.

[23] P.S. Khodashenas, J.M. Rivas-Moscoso, D. Siracusa, F. Pederzolli, B. Shariati, D. Klonidis, E. Salvadori, I. Tomkos, Comparison of spectral and spatial super-channel allocation schemes for sdm networks, J. Lightwave Technol. 34 (11) (2016) 2710–2716, https://doi.org/10.1109/JLT.2016.2551299.