A RMSA Algorithm Resilient to Multiple Node Failures on Elastic Optical Networks

Fábio Barbosa, Amaro de Sousa,
Instituto de Telecomunicações
Universidade de Aveiro
3810-193 Aveiro, Portugal
{fabiobarbosa, asou}@ua.pt

Agostinho Agra,
CIDMA / IT, Dept. Matemática
Universidade de Aveiro
3810-193 Aveiro, Portugal
aagra@ua.pt

Krzysztof Walkowiak, Róża Goścień,
Department of Systems and Computer Networks
Faculty of Electronics,
Wrocław University of Science and Technology
Wrocław, Poland
{krzysztof.walkowiak, roza.goscien}@pwr.edu.pl

***Abstract*—An Elastic Optical Network (EON) provides a lot of flexibility on the way an optical network supports the demands of multiple services. This flexibility is given by the Routing, Modulation and Spectrum Assignment (RMSA) algorithm whose primary goal is to use the spectrum resources of the network in an efficient way. Recently, large-scale failures are becoming a concern 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 connected links. In order to obtain a RMSA algorithm resilient to multiple node failures, we propose the use of a path disaster availability metric which measures the probability of each path not being affected by a multiple node failure. We present computational results considering a mix of unicast and anycast services in 3 well-known topologies. We assess the trade-off between spectrum usage efficiency and resilience to multiple node failures of our proposal against other previous known algorithms. The results show that the RMSA decision is always better when the disaster path availability metric is used. Moreover, the best way to use the path disaster availability metric in the RMSA decision depends on the traffic load of the EON.**

***Index Terms*—Elastic Optical Networks, RMSA, Multiple Node Failures, Disaster Resilience**

I. Introduction

An Elastic Optical Network (EON) provides a lot of flexibility on the way an optical network can support the demands of multiple services. This flexibility is given by the Routing, Modulation and Spectrum Assignment (RMSA) of each demand and is used, in practice, to make the most out of the available spectrum resources of the optical network.

The primary goal of the RMSA 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 as much as possible [1]–[5]. Then, other goals can also be considered as transceiver costs or power consumption [6]–[8].

One of the most relevant goals is the network resilience to failures. Network resilience is, broadly speaking, the ability of the network to keep supporting the service demands in case of network failures. Many works address this problem considering protection mechanisms to guarantee that all demands can be maintained after any single link or node failure [9]–[11].

Recently, large-scale failures are becoming a concern to network operators due to different causes, as natural disasters [12] or human malicious activities [13], which might involve a significant number of simultaneous failures. The guarantee that all demands are maintained in a large-scale failure is infeasible in practice as the required resources become too costly. In this case, the aim is to improve the network preparedness to large-scale failures by maximizing the amount of demand that can still be maintained in face of such failures. 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 connected links. So, in this work, we deal with the multiple node failures as they are the most harmful case.

The topology design of optical networks resilient to multiple node failures was recently addressed in [14]. In that work, the resilience is evaluated by the impact of the simultaneous failure of the critical nodes, i.e., the nodes with the highest impact on the connectivity of the network. Here, we propose a family of RMSA algorithms resilient to multiple node failures assuming that an attacker "discovers" with some probability a set of nodes to be attacked. The algorithms use a path metric, which we name *path disaster availability*, in the RMSA decision of each demand. This metric measures the probability of the path not being affected by the attacked nodes. Although the concept of path availability is commonly used to characterize the availability of networking services to unintended failures, as far as we are aware, it has never been exploited in the context of multiple node failures.

We present a set of computational results considering a mix of unicast and anycast services in 3 well-known topologies and compare the proposed RMSA algorithms with the first-fit algorithm, used in many works due to its simplicity, and with a RMSA algorithm recently used in [15] and adapted from [2]. All algorithms are evaluated through simulation considering a restoration mechanism where, when a multiple node failure happens, the non-affected lightpaths remain unchanged and the demands of the affected lightpaths are reassigned as much as possible in the surviving network resources.

The different RMSA algorithms are compared in terms of spectrum usage efficiency and resiliency to multiple node failures. In the latter case, the resiliency is evaluated by 2 parameters: the average non-disrupted demand (the average demand percentage that is not disrupted after a failure) and the average surviving demand (the average demand percentage

that is supported after a failure). Both parameters are important in practice. Higher surviving demands are important for non-critical services as they are less penalized by short-term disruptions. Higher non-disrupted demands are important for critical services (requiring high availability) and because a lower number of lightpaths required to be reassigned minimizes the instability impact of the simultaneous reconfiguration of many lightpaths.

The paper is organized as follows. In Section II, the path disaster availability metric is presented, together with its determination method. Section III describes the RMSA methods considered in this work. The computational results are presented and discussed in Section IV. Finally, Section V draws the main conclusions of the work.

II. Modeling Path Disaster Availability for Multiple Node Attacks

Consider an EON topology defined by a graph $G = (N, E)$, with a set of $|N|$ nodes and a set of $|E|$ undirected links. Consider the following attack model: an attacker "discovers" with some probability a set of nodes and plans to attack them (almost) simultaneously.

Since public information might exist related to the location of each node (for example, the location of Data Centers is usually publicly known and most likely a network node is nearby), we assume that each node $i \in N$ is associated with a positive weight w_i proportional to the probability of the node being discovered by an attacker. We assume that there is no correlation between discovered nodes as, if exists, it is related to attacker's organizational issues which require insight information usually not available to the network operator. Moreover, we assume that the number of attacked nodes s is between a minimum number s_m and a maximum number s_M. Finally, we assume that the effort to attack s nodes is proportional to the number of nodes and, therefore, the probability of s nodes being attacked, with $s_m \leq s \leq s_M$, is inversely proportional to the number of attacked nodes $1/s$.

First, the path disaster availability a_p of a given path p defined by its set of nodes $i \in p$ (including the source and destination nodes) is:

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

i.e., the probability that path p is available in the surviving network. In expression (1), p_i is the probability of node $i \in N$ to be attacked when a multiple node attack is realized and, by the adopted attack model, it is independent of the other attacked nodes.

Then, the probability p_i of node $i \in N$ being attacked is:

$$p_i = \frac{1}{\sigma} \sum_{s=s_m}^{s_M} p_i^s \times \frac{1}{s} \tag{2}$$

where $\sigma = \sum_{s=s_m}^{s_M} \frac{1}{s}$ and p_i^s is the probability of node i being attacked on an attack to s nodes.

Finally, the probability p_i^s of node i being attacked on an attack to s nodes is the sum of the probabilities of all sequences (without repetitions) of s out of n nodes that include node i, given by:

$$\begin{aligned} p_i^s = & \frac{w_i}{W_N} + \sum_{j \in N \backslash \{i\}} \frac{w_j}{W_N} \times \frac{w_i}{W_{N \backslash \{j\}}} \\ & + \sum_{j \in N \backslash \{i\}} \frac{w_j}{W_N} \left(\sum_{k \in N \backslash \{i,j\}} \frac{w_k}{W_{N \backslash \{j\}}} \times \frac{w_i}{W_{N \backslash \{j,k\}}} \right) + ... \end{aligned} \tag{3}$$

where W_R denotes the sum of the weights of the nodes in set R, with $R \subset N$, i.e., $W_R = \sum_{i \in R} w_i$.

The first term $\frac{w_i}{W_N}$ in expression (3) is the probability of all sequences such that node i is the first node of the sequence. The second term $\sum_{j \in N \backslash \{i\}} \frac{w_j}{W_N} \times \frac{w_i}{W_{N \backslash \{j\}}}$ is the probability of all sequences such that node i is the second node of the sequence, i.e., all sequences composed by a node $j \in N \backslash \{i\}$ 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 node i is the third node of the sequence.

The probability p_i^s given by expression (3) has s terms and can be computed recursively as follows. For a given set N of nodes and associated weights $w = \{w_i, i \in N\}$, a given number of attacked nodes s and a given node i, the probability p_i^s is computed as:

$$p_i^s = prob(N, w, i, 0, s) \tag{4}$$

where $prob()$ is a recursive function defined in Algorithm 1. The input parameters (Line 1) are a set of nodes R which were still not selected (in the first call in (4), 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 (4), this parameter is $z = 0$) and the number s of nodes to be selected.

Algorithm 1 Recursive function to compute p_i^s

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

III. RMSA Algorithms

Consider a given EON topology defined by graph $G = (N, E)$ and a given set D of estimated traffic demands. Each demand $d \in D$ can be of either unicast or anycast service type. In unicast services, each demand is characterized by a pair of end-nodes (s_d, t_d) and its required bit-rate b_d. In anycast services, a set S of services is provided by a set $C \subset N$ of existing Data Centers (DCs) and each anycast service $r \in S$ is provided by a DC subset $C_r \subseteq C$. Then, each anycast demand

is characterized by a source node s_d, an anycast service $r_d \in S$ and a bit-rate b_d. In this case, the anycast demand can be satisfied by any of the DCs in C_{r_d}.

The RMSA algorithm determines the way lightpaths are assigned both in the regular state and in any failure state. To model the RMSA, we need additional sets and parameters. Set $F = \{1, 2, ..., |F|\}$ is the ordered set of Frequency Slots (FSs) available on each fiber link to be assigned to lightpaths. Set P_d is the set of candidate paths associated with demand $d \in D$, ordered from the shortest to the longest optical length.

The optical length of a path is the sum of its link lengths plus a given length value Δ per intermediate node (which models the optical degradation suffered by a lightpath while traversing an intermediate optical switch). Each $p \in P_d$ is defined by:

- the binary parameters α_e^p which are equal to 1 if link $e \in E$ is in p, or equal to 0 otherwise;
- the integer parameter n_p indicating the number of FSs of the most efficient modulation format whose transmission range is not lower than the optical length of p.

A. First-Fit RMSA Algorithm

In the First-Fit (FF) RMSA algorithm, each demand d is routed in the first candidate path with available resources. Starting from an empty network, this task is conducted for each demand by some order. Many works assume the order of the demands given by the input data file. However, the best results are obtained if we consider first the demands that require more network resources. For fairness reasons when comparing the different RMSA algorithms, in this work, we consider this "more sophisticated" FF approach.

Initially, the set of demands $d \in D$ is ordered based on the properties of the shortest path of its set of candidate paths, i.e., the first path in P_d. This order follows the next 3 hierarchical orders (from the most important to the least important):

1. decreasing order of the number of hops of the optical shortest path between the source s_d and either the destination t_d (for unicast demands) or the closest DC (for anycast demands);
2. decreasing order of the demand bit-rate b_d;
3. decreasing order of the optical shortest path length between the source s_d and either the destination t_d (for unicast demands) or the closest DC (for anycast demands).

This ordering strategy was adopted after some preliminary computational tests. Then, for each $d \in D$ (and by this order), we compute the highest FS f of the lowest set of n_p contiguous FSs that can be assigned on the shortest path $p \in P_d$ without overlap with previous assignments. If $f \in F$, a lightpath is assigned to demand d on path p and on FSs from $f - n_p + 1$ to f. Otherwise, the process is repeated for the next shortest path $p \in P_d$ until a lightpath can be assigned to demand d or all paths in P_d have been computed (in the latter case, the demand is not assigned).

B. Resilient RMSA Algorithms

Recall that the required number of FSs n_p depends on the candidate path $p \in P_d$. First, consider for each demand d the parameter n_d with the minimum number of FSs required by any of its candidate paths $p \in P_d$, i.e., $n_d = \min_{p \in P_d} n_p$. Consider also P_e as the set of candidate paths of all demands that include link $e \in E$.

A RMSA algorithm for the regular state of the network is defined in Algorithm 2, following the general approach proposed in [2]. In a nutshell, Algorithm 2 is a greedy algorithm that starts with an empty network (i.e., all FSs are free in all links) and, iteratively, assigns to a demand $d \in D$, a lightpath $p \in P_d$ and a set of n_p contiguous FSs.

Algorithm 2 starts by computing the maximum value n among the n_d values of all demands (Line 1) and initializes set $\bar{D}$ with all demands such that $n_d = n$ (Line 3). Then, for all candidate paths of all demands in $\bar{D}$ (Line 6), the algorithm computes the lowest set of n_p contiguous FSs that can be assigned without overlapping with previous assignments (Lines 7–11) and, among all, it selects the one according to a given *best assignment condition* (Lines 8–10), explained later. The selected path and associated set of FSs are used to assign the lightpath to the corresponding demand (Line 12) and the demand is removed from set $\bar{D}$ (Line 13). When $\bar{D}$ becomes empty, n is decremented (Line 15) and the algorithm continues until n reaches 0.

Algorithm 2 Robust RMSA

```
1: Initialize n ← max_{d∈D} n_d
2: while n ≥ 1 do
3:    D̄ ← {d ∈ D : n_d = n}
4:    while D̄ ≠ ∅ do
5:       f̄ ← ∞, l̄ ← ∞, d̄ ← {}, p̄ ← {} and ā ← 0
6:       for all p ∈ P_d, d ∈ D̄ do
7:          f ← highest FS index of the lowest set of n_p
            contiguous FSs that can be assigned on p to d
            without overlap with previous assignments
8:          if [best assignment condition] then
9:             f̄ ← f, p̄ ← p, d̄ ← d, l̄ ← l_p and ā ← a_p
10:         end if
11:      end for
12:      Assign to demand d̄ a lightpath on the candidate path
         p̄ and on the FSs from f̄ − n_p̄ + 1 to f̄
13:      D̄ ← D̄\d̄
14:   end while
15:   n ← n − 1
16: end while
```

The *best assignment condition* (Line 8) is the step where the RMSA can be tuned according to different lightpath assignment criteria. In [2], a collision metric c_e is proposed for each link $e \in E$ given by $c_e = \sum_{d \in D} \sum_{p \in (P_d \cap P_e)} n_p$. Then, each candidate path $p \in \cup_{d \in D} P_d$ has an associated path collision length metric $l_p = \sum_{e \in E} \alpha_e^p c_e$ which is used in the RMSA when selecting candidate paths.

Here, we investigate how both metrics (the path collision length and the path disaster availability, as defined in (1)) can be combined to reach a RMSA algorithm which is more resilient to multiple node failures.

Note that in Lines 5–11 of Algorithm 2, the selected path $\bar{p}$ is initialized empty (Line 5) and is updated (Line 9) when a new best candidate path p is found (Line 8). So, the *best assignment condition* in Line 8 is a comparison between the best path already found $\bar{p}$ (associated with demand $\bar{d}$ with the highest FS $\bar{f}$, collision length $\bar{l}$ and disaster availability $\bar{a}$) and the current candidate path p (associated with demand d with the highest FS f, collision length l_p and disaster availability a_p).

To define different *best assignment conditions*, we consider 3 measures: the best FS ("S"), the best path disaster availability ("P") and the best path collision length ("C"). Then, the following 4 different *best assignment conditions* were investigated:

SC: p is better than $\bar{p}$ if its highest FS is better ($f < \bar{f}$), or if $f = \bar{f}$ and its collision length is better ($l_p < \bar{l}$). This condition represents the strategy proposed in [2] where it is shown to be more efficient than other RSMA algorithms in terms of spectrum usage efficiency.

SPC: p is better than $\bar{p}$ if its highest FS is better ($f < \bar{f}$), or if $f = \bar{f}$ and its disaster availability is better ($a_p > \bar{a}$), or if $f = \bar{f}$ and $a_p = \bar{a}$ and its collision length is better ($l_p < \bar{l}$). The first preference is still to assign the lowest spectrum but, as a tie-breaker, the path disaster availability is used aiming to improve the resilience to multiple node attacks (the collision length is only used as a tie-breaker of the path disaster availability).

PSC: p is better than $\bar{p}$ if its disaster availability is better ($a_p > \bar{a}$), or $a_p = \bar{a}$ and its highest FS is better ($f < \bar{f}$), or if $a_p = \bar{a}$ and $f = \bar{f}$ and its collision length is better ($l_p < \bar{l}$). Now, the first preference is the path disaster availability even if p requires higher spectrum than $\bar{p}$ (i.e., the aim is to improve the resilience to multiple node attacks at the possible cost of a lower spectrum usage efficiency).

Mix: it is defined as **PSC** if $f \leq H$, or as **SPC** if $f > H$, where H is the highest FS already assigned to all previous lightpaths. It is a combination of the two previous cases: if the highest FS f of path p does not increase H, the first preference is to improve the disaster resilience; otherwise, the first preference is to assign the lowest spectrum.

Algorithm 2 with the SC *best assignment condition* was recently used in [15] in the design of EONs resilient to multiple node failures. Like in here, a restoration mechanism is considered in [15] where, when a multiple node failure happens, the non-affected lightpaths remain unchanged and the affected demands are reassigned as much as possible in the surviving network. Following [15], we consider for the failure state (i.e., when multiple nodes fail), a RMSA algorithm slightly different than the RMSA algorithm used in the regular state (as presented in Algorithm 2). The algorithm starts with the FSs occupied by the non-affected lightpaths (i.e., with a fragmented spectrum occupation). Then, the RMSA considers the demands in increasing order of their n_d values (as opposed to the decreasing order used in Algorithm 2) as the increasing order performs better, on average (lightpaths requiring less number of FSs can better fit in the initial fragmented spectrum). Finally, the SC *best assignment condition* is used as in a failure state the aim is to reassign as much as possible the affected demands (spectrum usage efficiency is the most important aim).

IV. Computational Results

The computational results presented in this section are based on 3 network topologies with public available information [16]: Germany50, Cost266 and Janos-US. Table I presents their topology characteristics in terms of number of nodes $|N|$ and fiber links $|E|$, average node degree $\bar{\delta}$, average link length $\bar{l}$ and diameter, i.e., the highest length 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). The last column presents the number of DC nodes considered on each topology. The network topologies are shown in Fig. 1 with DC node locations (highlighted in large circles) selected among the nodes with largest node degree.

TABLE I: Topology characteristics of each network.

Network	$\|N\|$	$\|E\|$	$\bar{\delta}$	$\bar{l}$	Diameter	$\|C\|$
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

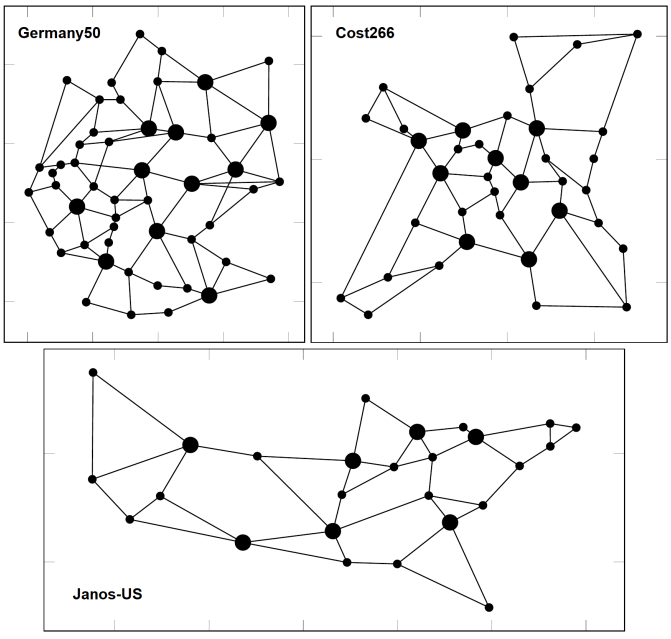

Fig. 1: Network topologies.

The candidate paths associated to each demand were computed with a k-shortest path algorithm considering $k = 5$ in

all cases. For anycast demands, we have considered 5 shortest paths between the source node and each DC node of its anycast service, and then excluded the paths that have DC nodes of the same service as intermediate nodes.

For each fiber, we have considered a capacity of $|F| = 320$ FSs which corresponds to a spectral grid of granularity 12.5 GHz. The number of FSs n_p required by each candidate path $p \in P_d$ of each demand d was computed as follows. Based on the distance-adaptive transmission (DAT) rule, 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 demand 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. 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. The transmission reach and bit-rate of all considered MFs are presented in Table II (transceiver model based on [17] and transmission reaches based on [18]).

TABLE II: Transmission reach and bit-rate of each MF.

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

Concerning the estimated demand set D, we have considered 5 sets for each topology with an increasing amount of traffic where each set considers the traffic equally divided into unicast and anycast traffic.

Regarding the unicast traffic, each unicast demand $d \in D$ has its end-nodes (s_d, t_d) randomly generated without replacement (with a uniform distribution among all nodes) and its bit-rate b_d (in Gbps) randomly generated with a uniform distribution in the set $\{50, 100, 150, 200\}$.

Regarding the anycast traffic, a set of five anycast services ($|S| = 5$) is considered in all cases and each service $r \in S$ is served by five randomly selected DCs from C (i.e., the DC subset C_r of anycast service $r \in S$ is randomly selected with a uniform distribution from the set of all DC nodes C). Then, each anycast demand $d \in D$ has its source node s_d randomly generated with a uniform distribution among all nodes, its anycast service $r_d \in S$ randomly generated with a uniform distribution between all services and its bit-rate b_d (in Gbps) randomly generated with a uniform distribution in the set $\{50k : k \in \mathbb{N},\ 1 \leq k \leq 20\} = \{50, 100, ..., 1000\}$. The s_d and r_d values are generated without repetition (i.e., we guarantee at most one demand from each source node s_d to each anycast service $r \in S$).

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 the nodes being discovered by the attacker), were assumed to be $w_i = 5$ for the DC nodes (set C) and $w_i = 1$ for all other nodes (set $N \backslash C$).

Recall that the aim is to determine the trade-off between spectrum usage efficiency and resiliency to multiple node failures among the different RMSA algorithms. Note that all RMSA algorithms described in section III assign lightpaths in the lowest possible spectrum available in the routing path selected to each demand. So, the spectrum usage efficiency can be evaluated by the highest FS allocated at the end of the algorithm and a better algorithm is one whose highest allocated FS is lower.

Table III presents the highest allocated FS obtained by each RMSA algorithm on each problem instance in the regular state (T is the total bit-rate, in Tbps, of the instance, i.e., $T = \sum_{d \in D} b_d$). The lowest value among all algorithms is highlighted in bold for each problem instance and the absence of a value means that the RMSA algorithm was not able to assign lightpaths to all demands.

TABLE III: Highest FS allocated by each RMSA method.

Network	T (Tbps)	FF	SC	SPC	PSC	Mix
Germany50	20	90	**62**	65	108	72
	45	177	119	**113**	199	146
	70	282	**172**	179	318	235
	95	320	227	**221**	–	304
	135	–	320	**319**	–	–
Cost266	15	122	65	**64**	91	83
	30	218	138	**133**	199	171
	45	275	**181**	185	258	238
	60	320	**250**	251	–	292
	80	–	**300**	310	–	–
Janos-US	15	113	**73**	76	89	80
	30	226	**155**	156	191	175
	45	317	**211**	214	276	258
	55	–	254	**248**	–	299
	65	–	294	**288**	–	–

Table III results show that, concerning spectrum usage efficiency, both SC and SPC based RMSA algorithms present very similar results and are much more efficient than the others. This is a direct consequence of both using the highest FS as the first measure in the *best assignment condition*. The PSC based RMSA strongly penalizes the spectrum usage efficiency (even worst than FF in the Germany50) while the Mix (being a combination of the SPC and PSC) presents intermediate penalty results.

In order to assess the resilience of each RMSA algorithm to multiple node attacks, we have generated 500 random attacks for each problem instance (after some preliminary testing, this value was shown to be good enough as larger values do not significantly change the average results).

Each attack was implemented as follows. First, the number of attacked nodes s is randomly generated in $\{s_m, ..., s_M\}$ with probabilities proportional to $1/s$. Then, s network nodes

are randomly sampled without repetition with probabilities proportional to the weights w_i. For each attack, we run the RMSA algorithm variant for the failure state and we compute the total non-disrupted demand (the sum of the demands whose lightpaths were not disrupted) and the total surviving demand (the sum of the demands whose lightpaths were not disrupted plus the sum of the demands that were assigned with new lightpaths). Finally, the resiliency of each RSMA algorithm is evaluated by 2 parameters: the Average Non-Disrupted Demand (the average bit-rate percentage that is not disrupted among all 500 attacks) and the Average Surviving Demand (the average bit-rate percentage that is supported after the attack among all 500 attacks).

Table IV presents the average results of the resilience evaluation of each RSMA algorithm on each problem instance (once again, best values among all RMSA algorithms highlighted in bold for each problem instance).

First, note that when multiple nodes are shut down, there are some demands that cannot survive whatever RMSA is adopted. The obvious ones are the demands such that at least one of its end-nodes is a shutdown node. Then, in multiple node shutdowns that separate the network in different components: (i) unicast demands with end-nodes in different components cannot survive and (ii) anycast demands whose source node is in a network component without any of the DC nodes of its anycast service also cannot survive. So, on each random attack, the total demand that can survive is also computed and both evaluation parameters are determined as percentages of this total survivable demand. The last column "Survivable Demand" of Table IV presents the average total bit-rate that can survive among all 500 random attacks.

Regarding the Average Non-Disrupted Demand, the best results are provided, on average, by the PSC based RMSA (i.e., using the path disaster availability metric as the first measure in the *best assignment condition*). However, due to its low spectrum usage efficiency (already seen in the results of Table III), it can be used in practice only for light to medium loaded EONs. The Mix based RMSA is, on average, the second best algorithm and, as it can accommodate more total traffic demand, it becomes the best algorithm for the demand sets D that cannot be accommodated by the previous PSC based RMSA. Finally, for the demand sets D with the highest traffic, the SPC based RMSA provides the best results although closely followed by the SC based RMSA. Note that there is no case where either the FF or the SC based RMSA algorithms are better than all RMSA algorithms using the path disaster availability metric.

Regarding the Average Surviving Demand, all RSMA algorithms present similar results for the demand sets D of lower traffic (in fact, for the smallest traffic values considered in each topology, all RMSA algorithms were able to maintain 100% of all survivable demand). When the total demand becomes higher, then the SPC based RMSA becomes the best, on average, although closely followed by the SC based RMSA. Again, there is no case where the FF RMSA is better than all other algorithms.

Finally, it should be pointed out that, for a given problem instance, the percentage difference across all RMSA algorithms is never higher than 3% in Table IV. The next tables show the resilient evaluation of the different RMSA algorithms in a different way by presenting the number (in percentage) of the 500 random attacks such that each RMSA algorithm (excluding the FF based RMSA) has provided the best resiliency value. Table V presents the results for the Average Non-Disrupted Demand while Table VI presents the results for the Average Surviving Demand. In both cases, when a best value is given by multiple algorithms, it is accounted in the percentage of all of them (once again, best values highlighted in bold).

Regarding the Average Non-Disrupted Demand, the results in Table V highlight the conclusions taken from Table IV. For the three lowest traffic instances of all topologies, the PSC based RMSA is the best algorithm on 52.3% of the attacks (among 4 algorithms); then, for the fourth traffic instance of all topologies, the Mix based RMSA becomes the best algorithm on 73.1% of the attacks (among 3 algorithms); finally, for the highest traffic instance of all topologies, the SPC based RMSA is the best algorithm on 66.1% of the attacks (among 2 algorithms).

Regarding the Average Surviving Demand, again the results in Table VI confirm the conclusions taken from Table IV. For the lowest traffic instance of each topology, all RSMA algorithms were able to maintain 100% of all demand that can survive. For the problem instances with growing traffic demand, the SPC based RMSA becomes the best, on average, and the SC based RMSA becomes the second best algorithm.

In the overall, the trade-off analysis between spectrum usage efficiency (Table III) and resiliency to multiple node failures (Tables IV, V and VI) among the different RMSA algorithms is as follows. First, the FF RMSA is worst than all other algorithms, on average, as it is one of the algorithms with the lowest spectrum usage efficiency and, for all cases, it never provides the best resilience to multiple node failures. This comes without surprise, although we have adopted a "more sophisticated" variant, as described in Section III.

Then, comparing the RMSA algorithms using the disaster path availability metric (SPC, PSC and Mix) with the previously known SC based RMSA, we can conclude that the 3 alternatives provide 3 different trade-offs. The PSC alternative provides significant better resiliency at the cost of a significantly lower spectrum usage efficiency. The SPC alternative provides slightly better resiliency with the same spectrum usage efficiency. Finally, the Mix alternative is a trade-off between the two previous ones providing an intermediate level of resiliency gain at the cost of an intermediate penalty of spectrum usage efficiency.

As a consequence, the best RMSA algorithm depends on the traffic load of the EON. For lightly loaded networks, since spectrum resources are abundant, the PSC based RMSA is the best alternative as an higher percentage of non-disrupted demand can be provided. For medium loaded networks, the Mix based RMSA is the best alternative for the cases such that

TABLE IV: Resilience evaluation results.

N.	T	Average Non-Disrupted Demand (%)					Average Surviving Demand (%)					Survivable Demand
		FF	SC	SPC	PSC	Mix	FF	SC	SPC	PSC	Mix	
Germany50	20	75.444	74.503	75.884	**77.491**	76.827	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	18.2
	45	76.520	75.149	75.867	**78.230**	77.320	99.694	99.790	**99.794**	99.751	99.780	40.7
	70	76.193	73.953	75.134	**78.014**	77.324	97.776	**98.626**	98.608	97.696	98.374	63.4
	95	75.360	74.217	75.273	–	**76.895**	93.972	95.614	**95.807**	–	94.344	85.9
	135	–	73.847	**74.689**	–	–	–	87.118	**87.205**	–	–	121.9
Cost266	15	71.751	72.998	73.309	73.829	**74.032**	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	12.6
	30	71.135	71.335	71.361	**73.494**	73.180	97.657	**97.778**	97.758	97.568	97.690	25.3
	45	71.780	72.359	71.229	**73.801**	73.690	94.264	**95.035**	94.958	94.447	94.530	38.1
	60	71.193	71.520	71.695	–	**72.984**	89.430	89.684	**90.161**	–	89.279	50.9
	80	–	71.696	**71.903**	–	–	–	84.925	**85.063**	–	–	67.8
Janos-US	15	72.650	72.034	72.862	**73.945**	73.452	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	11.6
	30	70.973	69.104	69.611	**71.929**	71.187	98.538	**98.650**	98.516	98.346	98.496	23.3
	45	70.517	68.928	68.797	**71.562**	71.106	91.457	91.488	**91.726**	91.318	91.125	35.1
	55	–	68.988	69.376	–	**71.183**	–	88.086	**88.668**	–	88.011	43.0
	65	–	68.444	**69.458**	–	–	–	84.613	**85.306**	–	–	50.5

TABLE V: Percentage no. of attacks such that each RMSA provides the best Average Non-Disrupted Demand value.

Network	T	SC	SPC	PSC	Mix
Germany50	20	22.8	13.0	**56.6**	17.0
	45	11.0	10.6	**54.4**	27.4
	70	10.4	2.8	**57.2**	31.6
	95	13.8	6.0	–	**81.0**
	135	27.4	**73.4**	–	–
Cost266	15	17.8	23.8	**43.6**	32.8
	30	26.4	9.2	**49.2**	22.8
	45	28.2	7.6	**43.0**	23.8
	60	25.6	11.0	–	**65.4**
	80	48.2	**52.8**	–	–
Janos-US	15	27.0	9.6	**54.0**	24.8
	30	7.6	20.0	**53.8**	26.6
	45	11.0	5.2	**58.6**	34.8
	55	18.4	13.0	–	**72.8**
	65	30.0	**72.2**	–	–

TABLE VI: Percentage no. of attacks such that each RMSA provides the best Average Surviving Demand value.

Network	T	SC	SPC	PSC	Mix
Germany50	20	**100.0**	**100.0**	**100.0**	**100.0**
	45	**98.2**	98.0	96.2	97.0
	70	**89.8**	87.2	58.6	75.8
	95	64.0	**74.8**	–	21.4
	135	27.4	**73.4**	–	–
Cost266	15	**100.0**	**100.0**	**100.0**	**100.0**
	30	**89.0**	**89.0**	82.6	86.2
	45	**78.4**	73.2	58.2	59.4
	60	46.4	**58.2**	–	27.4
	80	52.0	**54.0**	–	–
Janos-US	15	**100.0**	**100.0**	**100.0**	**100.0**
	30	**93.4**	90.4	83.6	86.2
	45	51.0	**61.0**	45.6	37.4
	55	40.6	**65.4**	–	33.4
	65	40.4	**73.2**	–	–

TABLE VII: Running time (in seconds) of each RMSA algorithm in the regular state.

Network	T	k-SP	FF	SC	SPC	PSC	Mix
Germany50	70	14.7	1.2	0.8	0.9	0.9	0.9
Cost266	45	4.9	0.5	0.2	0.2	0.3	0.3
Janos-US	45	1.7	0.5	0.2	0.2	0.2	0.2

the previous algorithm cannot accommodate all the traffic. For heavily loaded networks, the SPC based RMSA is still better than the previous known SC based RMSA as it has the same spectrum usage efficiency and it is better (at least slightly) in both the non-disrupted demand percentage and surviving demand percentage.

Table VII presents the total running time, in seconds, of the k-shortest paths algorithm (column "k-SP"), which is common to all algorithms, and of each RSMA algorithm on the highest demand problem instance of each network such that the algorithm has accommodated all the traffic (i.e, the RMSA algorithm was able to assign lightpaths to all demands). For each algorithm, the total running time is the sum of its runtime with the k-shortest paths algorithm runtime.

Table VII shows that the pre-computation of the set of candidate paths for all demands is much more time-consuming than the RMSA itself. Moreover, because the FF strategy requires ordering the set of demands, it presents a higher runtime than all other RMSA algorithms. Finally, and more importantly, the disaster path availability metric does not impose any runtime penalty in the RMSA decision, when compared with the previously known SC based RMSA algorithm.

Finally, Table VIII presents the average running time per attack (among all 500 attacks), in seconds, of each RSMA algorithm on the same problem instances used in the previous

table. In this case, the values include the computation of the k-shortest paths for all demands with disrupted lightpaths as these demand sets vary between the different cases.

TABLE VIII: Average running time (in seconds) of each RMSA algorithm per attack.

Network	T	FF	SC	SPC	PSC	Mix
Germany50	70	4.237	4.644	4.361	3.958	3.991
Cost266	45	1.598	1.624	1.645	1.527	1.538
Janos-US	45	0.548	0.568	0.572	0.531	0.537

Table VIII shows that the running times are very similar among all algorithms but the RMSA algorithms that prioritize the path disaster availability metric (PSC and Mix) are slightly faster, on average, than the others. Since these algorithms provide better average non-disrupted demand, the total number of demands whose lightpaths are disrupted is lower, on average, and so these RMSA algorithms have a lower number of demands for lightpath reassignment.

V. Conclusions

In this work, we have proposed a family of RMSA algorithms resilient to multiple node failures due to malicious human activities. First, we have assumed that an attacker "discovers" with some estimated probabilities a set of nodes to be attacked and we have proposed a path disaster availability metric that measures the probability of each path not being affected by the attacked nodes. Then, the path disaster availability metric was included in the RMSA decision in three different alternative ways (SPC, PSC and Mix).

The resulting algorithms were compared with the simplest first-fit algorithm and with a previously known RMSA algorithm in terms of spectrum usage efficiency, average non-disrupted demand and the average surviving demand.

The results have shown that the RMSA decision is always better when the disaster path availability metric is included but the best algorithm depends on the traffic load of the EON. For lightly loaded networks, the PSC based RMSA is the best alternative as an higher percentage of non-disrupted demand can be provided. For medium loaded networks, the Mix based RMSA is the best alternative for the cases such that the previous algorithm cannot accommodate all the traffic. For heavily loaded networks, the SPC based RMSA is still better than the previous known algorithm as it has the same spectrum usage efficiency and it is better (at least slightly) in both the non-disrupted demand percentage and surviving demand percentage.

Finally, the computational results have also shown that the use of the disaster path availability metric in the RMSA decision does not impose any runtime penalty in any of the 3 proposed alternatives.

Acknowledgements

This paper is based upon work from COST Action CA15127 ("Resilient communication services protecting end-user applications from disaster-based failures – RECODIS") supported by COST (European Cooperation in Science and Technology). First author was supported by FCT through PhD grant SFRH/BD/132650/2017. The work of F. Barbosa, A. de Sousa and A. Agra was supported by FCT, Portugal, through project ResNeD CENTRO-01-0145-FEDER-029312. The work of K. Walkowiak and R. Goścień was supported by statutory funds of the Dep. of Systems and Computer Networks, Wroclaw University of Science and Technology.

References

[1] K. Christodoulopoulos, I. Tomkos, E. A. Varvarigos. *Elastic Bandwidth Allocation in Flexible OFDM-Based Optical Networks*. *IEEE/OSA J. of Lightwave Technology*, vol. 29, no. 9, 1354–1366, 2011.

[2] M. Klinkowski and K. Walkowiak. *Routing and Spectrum Assignment in Spectrum Sliced Elastic Optical Path Network*. *IEEE Communications Letters*, vol. 15, no. 8, 884—886, August 2011.

[3] K. Walkowiak, M. Klinkowski. *Joint anycast and unicast routing for elastic optical networks: Modeling and optimization*. in *proc. IEEE ICC*, Budapest, Hungary, 3909–3914, 2013.

[4] S. Talebi, G. N. Rouskas. *On distance-adaptive routing and spectrum assignment in mesh elastic optical networks*. *IEEE/OSA J. of Optical Communications and Networking*, vol. 9, no. 5, 456–465, 2017.

[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)*. *Optical Switching and Networking*, vol. 23, part 1, 5–39, 2017.

[6] E. Palkopoulou, et al. *Quantifying spectrum, cost, and energy efficiency in fixed-grid and flex-grid networks [Invited]*. *IEEE/OSA J. of Optical Communications and Networking*, vol. 4, no. 11, B42–B51, 2012.

[7] B. C. Chatterjee, N. Sarma, E. Oki. *Routing and Spectrum Allocation in Elastic Optical Networks: A Tutorial*. *IEEE Communication Surveys & Tutorials*, vol. 17, no. 3, 1776–1800, 2015.

[8] R. Goscien, K. Walkowiak, M. Klinkowski. *Tabu search algorithm for routing, modulation and spectrum allocation in elastic optical network with anycast and unicast traffic*. *Computer Networks*, vol. 79, 148–165, 2015.

[9] X. Chen, S. Zhu, L. Jiang, Z. Zhu. *On Spectrum Efficient Failure-Independent Path Protection p-Cycle Design in Elastic Optical Networks*. *IEEE/OSA J. of Lightwave Technology*, vol. 33, no. 17, 3719–3729, 2015.

[10] J. Wu, Z. Nin, L. Guo. *Energy-Efficient Survivable Grooming in Software-Defined Elastic Optical Networks*. *IEEE Access*, vol. 5, 6454–6463, 2017.

[11] R. Goscien, M. Kucharzak. *On the efficient optimization of unicast, anycast and multicast flows in survivable elastic optical networks*. *Optical Switching and Networking*, vol. 31, 114–126, 2019.

[12] T. Gomes, et al. *A survey of strategies for communication networks to protect against large-scale natural disasters*. in *proc. RNDM*, Halmstad, Sweden, 11–22, 2016.

[13] M. Furdek, et al. *An overview of security challenges in communication networks*. in *proc. RNDM*, Halmstad, Sweden, 43–50, 2016.

[14] F. Barbosa, A. de Sousa, A. Agra. *Topology Design of Transparent Optical Networks Resilient to Multiple Node Failures*. in *proc. RNDM*, Longyearbyen, Norway, 1–8, 2018.

[15] F. Barbosa, A. de Sousa, A. Agra. *Evaluation and Design of Elastic Optical Networks Resilient to Multiple Node Failures*. in *proc. DRCN*, Coimbra, Portugal, 154–161, 2019.

[16] S. Orlowski, R. Wessaly, M. Pioro, A. Tomaszewski. *SNDlib 1.0 — Survivable Network Design Library*. *Networks*, vol. 55, no. 3, 276–286, 2010.

[17] P. S. Khodashenas, et al. *Comparison of spectral and spatial super-channel allocation schemes for SDM networks*. *IEEE Journal of Lightwave Technology*, vol. 34, no. 11, 2710–2716, 2016.

[18] C. Rottondi, et al. *Routing, modulation format, baud rate and spectrum allocation in optical metro rings with flexible grid and few-mode transmission*. *IEEE/OSA J. of Lightwave Technology*, vol. 35, no. 1, 61–70, 2017.