Offline Routing and Spectrum Allocation Algorithms for Elastic Optical Networks with Survivability and Multicasting

Rana Alaskar, Anwar Alyatama, Imtiaz Ahmad
Computer Engineering Department
Kuwait University, P.O. Box 5969, Safat 13060, Kuwait
Email: rana.alaskar@hotmail.com, a.yatama@ku.edu.kw, imtiaz.ahmad@ku.edu.kw

Abstract—**Elastic Optical Network (EON) is an emerging and a promising solution for future high-speed networks, because of its ability to efficiently manage network resources and provide better spectrum utilization. The intractable routing and spectrum allocation (RSA) problem and the eventually imposed survivability and/or multicast constraints play key roles in the effective design and control of EONs. In this work, we investigate priority allocation algorithms designed to solve the offline RSA problem in protection- and/or multicast-based EONs. Our objective is to minimize the total amount of spectrum needed to serve the traffic demand, when the demand includes unicast unprotected, unicast protected, multicast unprotected, and multicast protected requests. The proposed priority allocation algorithms are based on the compact scheduling algorithm and the ordering obtained with two different metrics, both of which consider the frequency slot and required number of links of the requests presented to the network. We evaluate the performance and efficiency of the proposed algorithms across a range of demand frequency slot distributions and a set of different scenarios, in two mesh topologies, the National Science Foundation network (NSFNET) and United Kingdom (UK) Backbone. A comparative analysis of the obtained experimental results reveals that the proposed algorithms improved the results by 2% - 10% in terms of spectrum utilization compared with existing reference algorithms.**

Keywords-elastic optical networks; spectrum allocation; survivability; multicasting; spectrum utilization.

I. INTRODUCTION

Elastic Optical Network (EON) [1]-[4] is an emerging solution for the increased demand of multimedia streaming services and cloud computing applications, because it can efficiently manage network resources and provide better spectrum utilization. Many challenges have been faced by EON researchers concerning hardware development, and spectrum management. Routing and spectrum allocation (RSA) [5] is one of the key challenges to be faced. RSA includes two main functions: assigning a suitable physical path between the source and destination(s), and allocating contiguous, continuous, and non-overlapping parts of the spectrum to meet traffic demand, while minimizing the total amount of spectrum needed to serve it. RSA is considered to be an NP-hard problem, because of the continuity constraint [5]. It can be divided into offline and online RSA. In the offline RSA, the demand is known in advance, and traffic variations occur over a long period of time, whereas in the online, the traffic arrives in a random manner.

Data transmitted through the network can be of critical nature (e.g., military, medical, or financial information). Protecting the paths followed by those data is crucial, to ensure a continuous transfer of data. Survivability is an important design criterion for traditional networks in general and optical networks in particular, including EONs [6][7][8]; it describes the ability to continue providing services in the presence of a single failure, which could be caused by fiber cuts, active component failure inside the network equipment, or node failure [9][10]. Networks serve two types of requests: protected and unprotected. Protected requests are designed to overcome a single network failure, most commonly by assigning a disjoint backup path (optical path, in the context) for each working path. The commonly used protection techniques can be divided into dedicated path protection (DPP) and shared path protection (SPP) techniques. Dedicated path protection means that each working path is assigned its own dedicated backup path, to which it can switch in case of a failure. On the other hand, shared path protection means that backup spectrum subcarriers can be shared on some links, as long as their protected segments (links, subpaths, paths) are mutually disjoint. Two different channel allocation policies can be applied with the aforesaid protection schemes. The first one is a same channel (SC) policy, where the working path and the backup path share the same central frequency. The second is the different channel (DC) policy, where both the working path and the backup path can utilize any available central frequency [11].

Multicast is an important and fundamental communication style, which addresses how to distribute the data from one or many sources to a group of destinations simultaneously. Multicast instead of usual unicast can reduce the traffic sent by the sources and thus save bandwidth significantly. A wide range of applications such as file distribution, multiplayer games, and software updates, require multicast connections and can transfer petabyte-scale data [12]. Multicasting is the most effective communication technique, because it helps increasing throughput, enhancing network's performance, and saving network's resources. The high criticality and wide popularity of the applications supporting multicast services require developing effective survivable multicasting techniques in EONs, to protect critical multicast sessions from either node or link failures. Protecting multicast sessions is more sophisticated than protecting unicast sessions in both WDM and OFDM networks [13]. As reported in the literature, two different path-based protection techniques are used to protect multicast trees, self-sharing and cross-sharing. In the self-sharing, each primary path (i.e., source destination pair) in a multicast tree is protected by a link-disjoint backup path. The backup edges of a backup path can be shared with other primary or backup paths of the given multicast tree, however, they cannot be shared with its corresponding primary path. Links sharing between different multicast trees is not allowed in the self-sharing technique. In the cross-sharing, backup edges, which are not shared with any edges of the corresponding multicast tree, can be shared with other multicast trees, in addition to self-sharing with the paths of the corresponding tree. In other words, both self-sharing within a tree and cross-sharing with different trees are allowed in the cross-sharing protection technique [14][15].

As mentioned above, in the multicast tree, requests are transmitted to the leaf nodes (i.e., destination nodes). Requests passing through a non-leaf destination node are dropped locally, but a copy of the request is transmitted downstream to the next node. The multicast tree need to be protected in order to assure the delivery of the request to all destination nodes. Considering survivability in multicast trees requires taking into consideration both the primary and backup links while solving the RSA problem; in contrast with our previous work [2], which considers only the primary links. In this paper, we extend our priority allocation algorithms [1][2] to handle survivability and/or multicast in EONs with the goal of minimizing the total amount of spectrum needed to serve the traffic demand. Protecting multicast connections from a single link failure, and handling demands with different types of traffic are the contributions of this paper. In the previous work [1], we considered unicast unprotected and unicast protected requests, while in this work, we study the behavior of the priority allocation algorithms when the traffic demand includes unicast unprotected, unicast protected, multicast unprotected, and multicast protected requests. The protection technique used in this work is dedicated path protection with same channel (RSA/DPP/SC), while the multicast protection technique is path-pair protection. We consider spectrum usage as a performance metric, to show the effectiveness of the proposed algorithms.

The rest of the paper is structured as follows. Section II sheds light on the research efforts related to the problem. Section III formulates the problem. Section IV reviews the proposed algorithms, with working examples. Section V discusses the experimental results. We present our conclusions with some ideas for future work in the last section.

II. PELATED WORK

In this section, we briefly present research efforts that have been proposed to handle offline RSA problem, survivability, multicasting, and survivability in multicasting for EONs. A significant amount of research has been conducted addressing the offline RSA problem [2][16]-[18]. For more details about the spectrum management techniques in EONs, readers are referred to the recent excellent surveys in [19][20].

Previous investigations have been carried out to study the issue of survivability in EONs. Some of these research efforts have been directed to the online RSA problem [21][22], whereas others considered the offline RSA problem in survivable EONs, considering the different protection techniques mentioned above. In particular, the use of DPP in EONs has been addressed in [1][11][18][23]-[26]. Alaskar et al. [1] addressed offline RSA with dedicated path protection in EONs with same channel (RSA/DPP/SC). They proposed different priority allocation mechanisms to enhance requests allocation in the network. Ruan et al. [26] studied the offline survivable multi-path RSA problem with DPP in EONs. They formulated the problem as an integer linear programming (ILP) problem, and proposed a heuristic algorithm for the static multipath routing and spectrum allocation (SM-RSA) problem. The RSA problem in EONs with DPP with static traffic demand has also been addressed in another work presented by Klinkowski [18], where the author used genetic algorithms to develop an efficient algorithm, which performs better than other reference algorithms. Concurrently, the use of SPP in EONs has been studied by many researchers [12][27]-[30]. Walkowiak et al. [29] addressed the offline RSA problem in EONs with SPP, formulating it also as an ILP problem. Another work presented by Liu et al. [31] handled spectrum fragmentation and low sharing degree in survivable EONs, by proposing an algorithm called shared path protection by reconstructing sharable bandwidth based on spectrum segmentation (SPP-RSB-SS). The aim of the algorithm was to minimize spectrum fragmentation and utilization. Recently, Goscien et al. [32] studied the survivability of EONs when the traffic demands include unicast and anycast requests, by applying multipath routing. They formulated the problem as an ILP, and proposed an algorithm called survivable multipath allocation (SMA). The problem of spectrum-aware survivable strategies with failure probability constraints has been addressed by Chen et al. [33]. They considered both dedicated and shared path protection by developing ILP models, with the goal of minimizing resource consumption. More details about the use of protection techniques in EONs can be found in [34][35], recent surveys of the topic.

Many algorithms have been introduced to solve the multicast tree problem in EONs. Kmiecik et al. [36] studied a two-layer optimization problem that combines both multicasting optimization in the application layer and the optimization of lightpaths in EONs, considering different survivability scenarios. In another work, Goscien et al. [37] addressed the routing, modulation, and spectrum allocation problem in EONs. They formulated the problem as an ILP covering both unicast and anycast traffic demands. Their proposed method is based on the standard tabu search approach. Liu et al. [38] have designed integrated multicast-capable routing and spectrum assignment (MC-RSA) algorithms by incorporating a layered approach with the aim of efficient serving of multicast requests in EONs.

Much research has been conducted to provide protection to the multicast sessions in EONs. The authors in [15] proposed a cross-sharing approach, which provides an optimal backup resources sharing between multiple multicast sessions. Their solution maximizes the sharing between multiple multicast sessions by using a link vector model. Another work proposed by Gong et al. [39] handled the problem of protecting multicast requests by proposing two ILP models. In the same context, Cai et al. [14] have evaluated both self- and cross-sharing protection schemes for distance-adaptive for multicast RSA in EONs, by formulating the problem as a mixed integer linear programming (MILP) problem. A general load balancing technique (LBT) has been proposed by Constantinou et al. [40] to be combined with any survivable multicasting approach, with the goal of balancing the distribution of the network load. The aforementioned works formulated the problem as an ILP, which is complicated, as compared with our proposed algorithms. The proposed heuristics provide a good quality solution since they are fast, and scalable.

III. PROBLEM FORMULATION

In this section, we present and explain the offline RSA problem in protection/multicasting-based EONs, with an example that will be used in the priority allocation algorithms section.

A. Problem Statement

The problem to be addressed can be formulated as follows: Given: a) A directed graph $G(V, E)$, where G denotes the physical topology of an EON, V denotes the set of nodes, and E denotes the set of bidirectional optical links. b) A set of frequency slices (i.e., subcarriers) in each optical link, of cardinality *sc*. c) A set of requests between source-destination pairs $(s, d)_i$ of request size (i.e., the number of frequency slices needed to serve a request) *sz*, where $i \in I$ represents the request type. Our aim is to minimize the total amount of spectrum needed to serve the traffic demand—which includes different types of requests to the mesh network—under the following constraints:

1) Spectrum contiguity constraint: Each request should be assigned to a contiguous portion of the spectrum.

2) Spectrum continuity constraint: Each request should be assigned to a similar portion of spectrum for all the corresponding links.

3) Non-overlapping spectrum constraint: Requests that need to use similar links should be assigned to non-overlapping portions of the spectrum.

4) Same channel (applies only to RSA/DPP/SC): For each unicast protected request, the working and backup paths should be assigned to similar portions of the spectrum.

In this paper, we consider four types of requests, $I = \{1, 2, 3, 4\}$. A request can be unicast unprotected ($i = 1$), unicast protected ($i = 2$), multicast unprotected ($i = 3$), or multicast protected ($i = 4$). When the demand includes a unicast unprotected request $(s, d)_1$ from s to d, the request will be served by contiguous subcarriers on all optical links belonging to the predetermined fixed working path from s to d. However, when the demand includes a unicast protected request $(s, d)_2$ from s to d, the request will be served by contiguous subcarriers on all optical links belonging to both the predetermined fixed working and backup paths from s to d. When the demand includes a multicast unprotected request $(s, d_n)_3$ from s to $\{d_1, d_2, d_3, \ldots, d_n\}$, the request will be served by contiguous subcarriers on all optical links belonging to the predetermined subgraph $G(s, d_n)_3$. When the demand includes a multicast protected request $(s, d_n)_4$ from s to $\{d_1, d_2, d_3, \ldots, d_n\}$, the request will be served by contiguous subcarriers on all optical links belonging to both the predetermined fixed working and backup subgraphs.

B. Example

To exemplify the problem, consider the mesh network illustrated in Figure 1, with 11 nodes and 16 bidirectional links. Table I shows the requests made to the mesh network, their type (unicast protected or multicast protected), size (4, 40, or 100), and the nodes traversed by the working and backup paths.

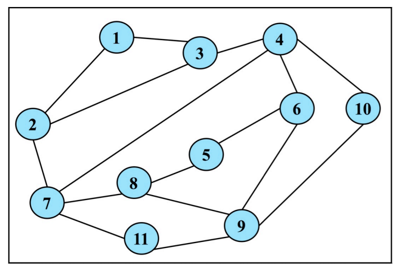


Figure 1. Mesh network with 11 nodes.

TABLE I. REQUESTS MADE TO THE MESH NETWORK

Requests	Type of request	Size (sz)	Working links	Backup links
τ_1 $(8 \rightarrow 5)_2$	Unicast protected	100	8-5	8-9 9-6 6-5
τ_2 $(6 \rightarrow 5)_2$	Unicast protected	100	6-5	6-9 9-8 8-5
τ_3 $(3 \rightarrow 2)_2$	Unicast protected	4	3-2	3-1 1-2
τ_4 $(1 \rightarrow 2, 3, 4, 6)_4$	Multicast protected	40	1-2 1-3 3-4 4-6	2-3 3-2 2-7 7-4 | 9-6 4-10 10-9
τ_5 $(1 \rightarrow 2, 3)_4$	Multicast protected	100	1-2 1-3	3-2 2-3
τ_6 $(4 \rightarrow 1, 2)_4$	Multicast protected	4	4-3 3-1 3-2	1-2 2-1 7-2 4-7
τ_7 $(6 \rightarrow 11)_2$	Unicast protected	4	6-9 9-11	6-4 4-7 7-11
τ_8 $(7 \rightarrow 9)_2$	Unicast protected	4	7-8 8-9	7-11 11-9

For the unicast protected requests, the working path is fixed and arbitrarily selected from the set of shortest paths computed with Dijkstra's algorithm; likewise, the backup path is fixed and arbitrarily selected from the set of shortest paths computed by Dijkstra's algorithm, after removing all edges belonging to the working path. For the multicast protected requests, a multicast tree is fixed and arbitrarily selected based on the minimum total number of links belonging to a rooted tree at the source s to the set of destination nodes $\{d_1, d_2, d_3, \ldots, d_n\}$. Each link in the working tree is protected separately (rather than the entire tree).

Those requests will be sorted based on the selected sorting mechanism, and the sorted list of requests will be used as an input to the compact scheduling algorithm [9]. The proposed priority allocation algorithms aim to optimize the mapping of requests to spectral resources, and minimize the total amount of spectrum needed to serve the traffic demand without violating the above-mentioned constraints.

IV. PRIORITY ALLOCATION ALGORITHMS

In this section, we evaluate the extended version of the proposed algorithms [1][2] as a solution to the offline RSA problem in survivable and/or multicast OFDM optical networks; the objective is to minimize the amount of spectrum needed to serve traffic demand when it includes unicast protected, and multicast protected requests. The RSA problem has two different dimensions: the spectrum (or bandwidth) and the links. The combination of these two dimensions plays a key role in improving the process of spectrum allocation. Therefore, the proposed solution is based on combining them in multiple ways. First, we introduce the compact scheduling algorithm [17], which has been used to show the effectiveness of the proposed algorithms. We then review the priority allocation algorithms; specifically, the sorting mechanisms. Finally, we show a working example, to demonstrate the performance of the algorithms when compared with the existing algorithms.

A. Compact Scheduling Algorithm

The proposed algorithms are based on an existing algorithm, the compact scheduling algorithm, proposed by Talebi et al. [17]. The compact scheduling algorithm is a typical list scheduling algorithm, where the quality of the solution is very sensitive to the order of requests in the list. It has a complexity of $O(n^2)$, where n is the number of requests in the list.

The input to the compact scheduling algorithm is a sorted list of requests to the mesh network. Figure 2 represents the flowchart of the compact scheduling algorithm, where L is the list of requests, id is the request location in the list, and t is the current execution time. The compact scheduling algorithm is constituted by the following steps:

1) Select the first request in the list and assign it to a set of consecutive links.
2) Delete the executed request from the list, and update the status (idle or busy) of the corresponding links.
3) Scan the list at the same scheduling instant to select requests that can be executed simultaneously with the currently executed requests.
4) Continue scanning the list until there are no other requests that can be executed at that scheduling instant or no available links.
5) Advance the scheduling time based on the earliest finishing request, and add the available links to the set of free links.
6) Repeat the aforementioned steps until all the requests have been satisfied.

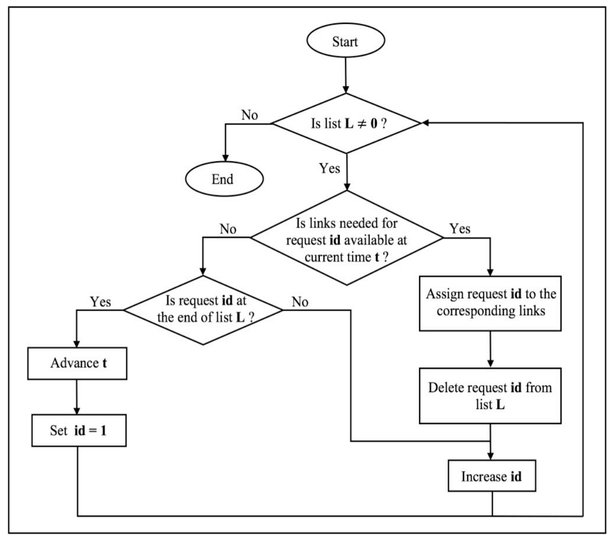


Figure 2. Compact schedulling algorithm flowchart.

B. Sorting Mechanisms

The proposed algorithms consider both dimensions of the problem: the links and the spectrum (or bandwidth). It is worth mentioning that in the present paper the link dimension is represented by the number of links used by the working path in the case of unicast unprotected requests, and by the number of links used by both the working and backup paths in the case of unicast protected requests. Similarly, in the case of multicast unprotected requests, it consists of the number of links in the working multicast tree, and the number of links in both working and backup multicast trees in the case multicast protected requests. On the other hand, in our previous work [2], the link dimension was represented by the number of links used by only the working path, because only unicast unprotected requests were being considered there. The complexity of the proposed algorithms is the same as of compact scheduling algorithm, which is $O(n^2)$, where n is the number of requests in the list. The proposed algorithms only sort the requests based on the selected criterion and pass them to the compact scheduling algorithm. The complexity of sorting algorithm is O(nlogn). Therefore, the running time of the algorithms is bounded by the complexity of the compact scheduling algorithm. The sorting mechanisms, the longest then widest compact algorithm (LWC) and the area compact algorithm (AC), are described below.

1) Longest then Widest Compact Algorithm (LWC): In the first proposed algorithm, we consider both dimensions of the problem, the links and spectrum (or bandwidth), using two levels (a primary and a secondary sorting mechanisms) to sort the requests in the demand. In the primary sorting mechanism, requests are sorted based on the amount of needed spectrum or bandwidth, from higher to lower. Then, in the secondary sorting mechanism, requests with equal bandwidth are sorted based on the required number of links from higher to lower.

2) Area Compact Algorithm (AC): In the second proposed algorithm, we also consider both dimensions of the problem, but in a different way. The amount of spectrum needed for a request and the required number of links are multiplied, thus providing a shape area. This area captures both dimensions of the problem and constitutes a better ordering metric. In this mechanism, the areas are used to sort the requests in the list, from higher to lower.

C. Working Example

In this subsection, we discuss the behavior of the above-mentioned algorithms, and show how different sorting mechanisms can affect the amount of spectrum needed to satisfy the demand, when it includes both unicast protected and multicast protected requests. As mentioned previously, existing algorithms [17] considered one dimension of the problem (i.e., either the bandwidth or the links), while our proposed algorithms consider both dimensions of the problem. As a result, the process of spectrum allocation is improved, and the number of needed subcarriers is decreased greatly while using our algorithms. Note that the request lists presented below are based on the demand shown in Table I in the problem formulation section.

1) Existing Algorithms:

The longest first compact algorithm (LFC) [17], sorts the requests based on the required amount of spectrum, from higher to lower. The sorted list of requests that will be used as input to the compact scheduling algorithm after applying the LFC algorithm is shown below:

$$\{\tau_2, \tau_5, \tau_1, \tau_4, \tau_3, \tau_6, \tau_7, \tau_8\}$$

Running the compact scheduling algorithm with LFC shows that 240 subcarriers are needed to serve the considered demand (which includes both unicast and multicast protected requests).

The widest first compact algorithm (WFC) [17], sorts the requests based on the required number of links used by the working and/or backup paths, from higher to lower. The sorted list of requests that will be used as input to the compact scheduling algorithm after applying the WFC algorithm is shown below:

$$\{\tau_4, \tau_6, \tau_7, \tau_8, \tau_1, \tau_2, \tau_5, \tau_3\}$$

Running the compact scheduling algorithm with WFC shows that 204 subcarriers are needed to serve the considered demand. The number of required subcarriers using WFC is therefore lower than when using LFC.

2) Proposed Algorithms (LWC):

The sorted list of requests that will be used as input to the compact scheduling algorithm after applying the LWC algorithm is shown below:

$$\{\tau_5, \tau_1, \tau_2, \tau_4, \tau_6, \tau_7, \tau_8, \tau_3\}$$

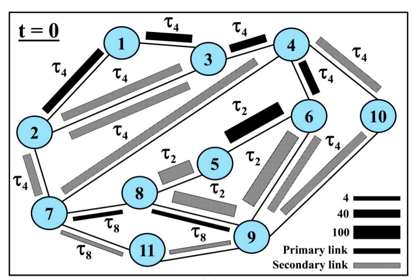
Running the compact scheduling algorithm with LWC shows that only 200 subcarriers are needed to serve the same demand. The number of subcarriers needed with LWC is therefore lower than if either LFC or WFC are used (240 and 204, respectively).

3) Proposed Algorithms (AC):

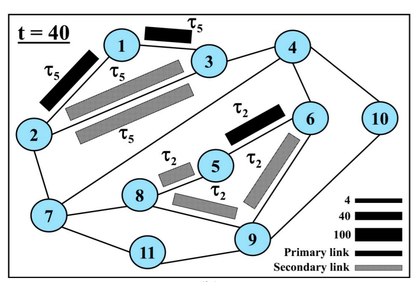
The sorted list of requests that will be used as input to the compact scheduling algorithm after applying the AC algorithm is shown below:

$$\{\tau_4, \tau_5, \tau_1, \tau_2, \tau_6, \tau_7, \tau_8, \tau_3\}$$

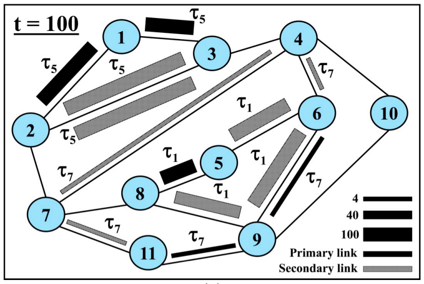
In Figure 3 (a), request 4 is assigned at t = 0, and it occupies 40 subcarriers from the following links: 1-2, 1-3, 3-4, 4-6, 2-3, 3-2, 2-7, 7-4, 9-6, 4-10, and10-9. Then, request 2 is assigned, and it occupies 100 subcarriers from the following links: 6-5, 6-9, 9-8, and 8-5. Last request that will be assigned at t = 0 is request 8, and it occupies 4 subcarriers from the following links: 7-8, 8-9, 7-11, and 11-9. After that, the time is advanced to t = 40, and the request list is scanned again. Figure 3 shows the spectrum utilization as time proceeds, using the AC algorithm. Running the compact scheduling algorithm with AC shows that 200 subcarriers are required for the considered demand.



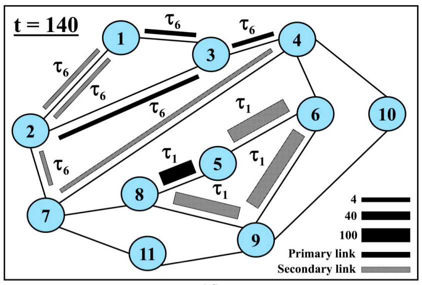
(a)



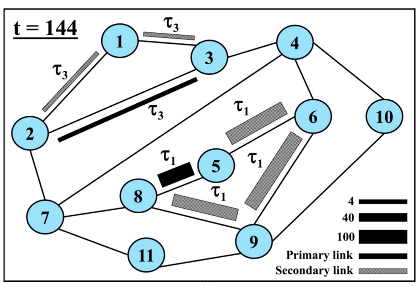
(b)



(c)



(d)



(e)

Figure 3. Area compact algorithm progression. (a) Step 1. (b) Step 2. (c) Step 3. (d) Step 4. (e) Step 5.

As obviously seen in the example, the number of subcarriers needed for the proposed algorithms (i.e., AC, and LWC) is lower than the numbers needed for the existing algorithms (LFC, and WFC (240 and 204, respectively)). Thus, both AC, and LWC strongly achieve the goal of the paper (i.e., minimize the total amount of spectrum needed to serve the traffic demand when it includes different types of requests).

Although both LWC and AC in the example require the same number of subcarriers (i.e., 200 subcarriers) to serve the demand, their behaviors are quite different. They have different request ordering mechanisms and different request allocation orders. The performance difference between them will be discussed in the experimental results and analysis section.

V. EPERIMENTAL RESULTS AND ANALYSIS

In this section, we start by presenting the comparison metric used for performance evaluation, along with the simulation environment. We examine different scenarios by varying the percentage of unicast unprotected, unicast protected, multicast unprotected, and multicast protected requests. We present a comparative evaluation between our algorithms (i.e., LWC and AC) and the heuristics recently proposed in [17] (i.e., LFC and WFC) with three traffic frequency slot distributions (discrete uniform, discrete high, and discrete low). Finally, we present the performance and analysis results. It is worth mentioning that both LFC and WFC were developed in the context of the RSA problem without additional survivability and multicasting constraints in the mesh network. Therefore, we modified the aforesaid existing algorithms to address the new constraints resulting from the use of protection and multicast.

A. Comparison Metric

We consider spectrum usage as the goal metric to evaluate the performance of our proposed algorithms. Spectrum usage is defined here as the number of subcarriers needed to serve a traffic demand including the four different types of requests (i.e., unicast unprotected, unicast protected, multicast unprotected, and multicast protected requests).

B. Simulation Setup

To test our priority allocation algorithms in terms of survivability and/or multicast EONs, we use two mesh topologies, the 14-node NSFNET and the 21-node UK Backbone as shown in Figures 4, and 5, respectively. In the case of unicast unprotected or unicast protected with dedicated path protection requests, the routing algorithm assumes an arbitrary fixed working path, selected from the set of shortest paths computed with Dijkstra's algorithm. The backup path in the unicast protected request is selected from the set of shortest paths computed with Dijkstra's algorithm, after removing all edges belonging to the working path.

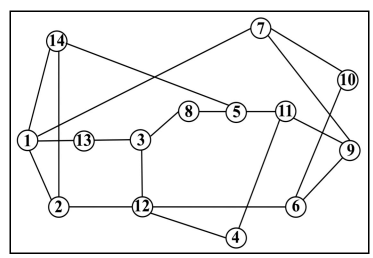


Figure 4. NSFNET-like topology.

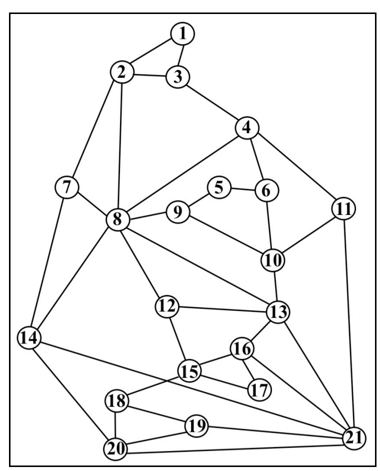


Figure 5. UK topology.

For multicast unprotected and protected requests, a multicast tree is fixed and arbitrarily selected based on the minimum total number of links belonging to a rooted tree at the source s to the set of destination nodes $\{d_1, d_2, d_3, \ldots, d_n\}$, where the number of destinations is randomly selected from 1 to 13 in the NSFNET network, and 1 to 20 in the UK Backbone. In the NSFNET network, we arbitrarily selected 182 trees with the number of links in each tree ranging from 1 to 13. The multicast traffic is uniformly distributed between the 182 trees. In the UK Backbone, we arbitrarily selected 420 trees with the number of links in each tree ranging from 1 to 21. The multicast traffic is uniformly distributed between the 420 trees. We protect the multicast tree with path-pair protection by utilizing both the links in the working tree and a set of sharable backup links to protect from single fiber failure [41]. The sharable backup links are the outcomes of computing a backup segment for each link belonging to the working tree. That is, each link on the tree is protected by a backup segment starting at the tail node and finishing at the head node of the link it protects [42]. Therefore, we protect each link in the working tree separately (rather than the entire tree) and allow these backup segments to share links with other existing working and backup segments. Backup links are only sharable within a tree and selected based on the minimum total number of sharable backup links.

We use a distance-adaptive spectrum allocation strategy to allocate the spectrum for each traffic demand based on its needed frequency slots and the length of its path as reported in [16][17]. We assume an elastic optical network with five different types of request sizes. Each demand requests 10, 40, 100, 400, and 1000 frequency units. The size of the traffic demand is generated using three different types of frequency slot distributions. In the discrete uniform distribution case, all frequency slots have the same probability, whereas in the discrete high distribution higher frequency slots have higher probabilities, and in the discrete low distribution higher frequency slots have lower probabilities. The details of these three distributions and their frequency slot selection probabilities are listed in Table II.

We consider three scenarios to evaluate our algorithms, with different traffic demand generation patterns. These scenarios are presented below:

1) In the first scenario, the traffic demand includes both unicast unprotected and unicast protected requests; the ratio of unicast protected to unicast unprotected requests varies from 0 % to 50 %, in increments of 10 %. In the first demand type, (i.e., the first data point in the graphs), all the requests are unicast unprotected, while in the last demand type half the requests are unicast unprotected, and half are unicast protected [1].

2) In the second scenario, the traffic demand includes unicast unprotected, unicast protected, and multicast unprotected requests; the ratio of unicast protected plus multicast unprotected to unicast unprotected requests varies from 0 % to 50 %, in increments of 10 %. In the first demand, (i.e., the first data point in the graphs), all the requests are unicast unprotected, while in the last demand half the requests are unicast unprotected, one quarter are unicast protected, and one quarter are multicast unprotected.

3) In the third and last scenario, the traffic demand includes both unicast protected and multicast protected requests; the number of multicast protected to unicast protected requests varies from 0 % to 50 %, in increments of 10 %. In the first demand type, (i.e., the first data point in the graphs), all the requests are unicast protected, while in the last demand half the requests are unicast protected, and half are multicast protected.

Tables III, IV, and V present the number of unicast unprotected, unicast protected, multicast unprotected, and multicast protected requests in the above mentioned scenarios.

Our proposed algorithms are implemented in C++ using Xcode (version 8.3.2) on a MacBook Pro with macOS Sierra (version 10.12.4), a 2.2-GHz Intel Core i7 processor, and 16 GB of memory.

TABLE II. DETAILS OF THE USED TRAFFIC FREQUENCY SLOTS DISTRIBUTION

Frequency slot	**Discrete uniform**	**Discrete high**	**Discrete low**
10	0.2	0.1	0.3
40	0.2	0.15	0.25
100	0.2	0.2	0.2
400	0.2	0.25	0.15
1000	0.2	0.3	0.1

TABLE III. NUMBER OF REQUESTS IN THE FIRST SCENARIO

Percentage (%)	**Number of requests**			
	Unicast unprotected	***Unicast protected***	***Multicast unprotected***	***Multicast protected***
0	182	0	0	0
10	164	18	0	0
20	146	36	0	0
30	128	54	0	0
40	110	72	0	0
50	91	91	0	0

TABLE IV. NUMBER OF REQUESTS IN THE SECOND SCENARIO

Percentage (%)	**Number of requests**			
	Unicast unprotected	***Unicast protected***	***Multicast unprotected***	***Multicast protected***
0	182	0	0	0
10	164	9	9	0
20	146	18	18	0
30	128	27	27	0
40	110	36	36	0
50	91	45	46	0

TABLE V. NUMBER OF REQUESTS IN THE THIRD SCENARIO

Percentage (%)	Number of requests			
	Unicast unprotected	*Unicast protected*	*Multicast unprotected*	*Multicast protected*
0	0	420	0	0
10	0	378	0	42
20	0	336	0	84
30	0	294	0	126
40	0	252	0	168
50	0	210	0	210

C. Performance Analysis and Results

In this subsection, we determine the average percentual improvement in the number of needed subcarriers in the scenarios, to evaluate the performances of our proposed algorithms (LWC and AC) when compared with the two existing algorithms (LFC and WFC) [17]. For each data point in our experiment, a large number of random problem instances (up to 8000) were executed, and only the resulting average values are being reported in this research. The averaged results were obtained with 99 % confidence, with a confidence interval smaller than 1 % of the average value.

1) First Scenario:

The topology used to evaluate the first scenario, where the demand includes unicast unprotected and unicast protected requests, is 14-node NSFNET. Figures 6, 7, and 8 show the average number of needed subcarriers versus the percentage of unicast protected requests, both for our proposed algorithms (LWC and AC) and the existing LFC and WFC algorithms. Table VI presents the performance improvements of our proposed algorithms when compared to LFC and WFC, for different frequency slot distributions. As shown in Figures 6, 7 and 8, the proposed algorithms performed better than both the LFC and WFC algorithms. In other words, the number of needed subcarriers with our algorithms was less than the number of needed subcarriers with either LFC or WFC. In particular, in the case of a discrete high distribution of the requested frequency slots, LWC and AC improved the results obtained with LFC by 9.5 %, and 9.6 %, respectively; when compared with WFC, improvements of 7.1 % and 7.2 % were respectively obtained.

TABLE VI. AVERAGE PERCENTUAL IMPROVEMENTS IN THE FIRST SCENARIO

Distribution	LWC		AC	
	LFC	*WFC*	*LFC*	*WFC*
Uniform	8.5 %	6.9 %	8.5 %	6.9 %
Discrete high	9.5 %	7.1 %	9.6 %	7.2 %
Discrete low	6.3 %	6.1 %	6.3 %	6.1 %

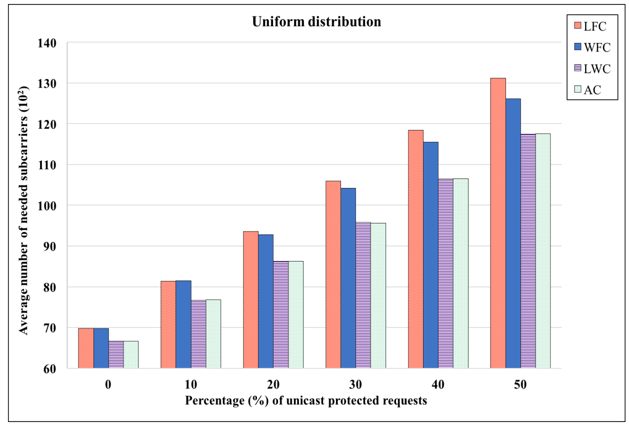


Figure 6. Average number of subcarriers as a function of the percentage of unicast protected requests; uniform frequency slot distribution.

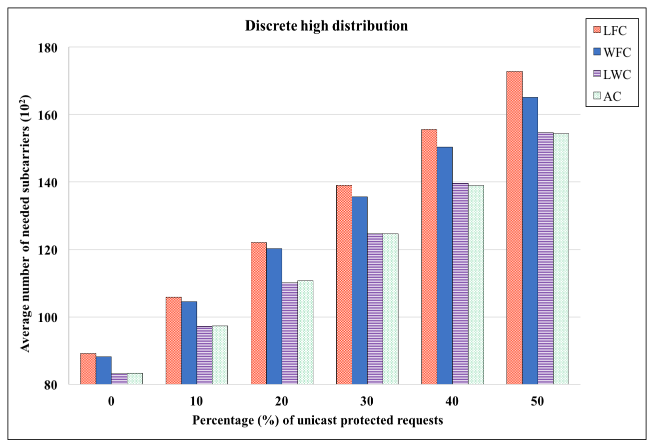


Figure 7. Average number of subcarriers as a function of the percentage of unicast protected requests; discrete high frequency slot distribution.

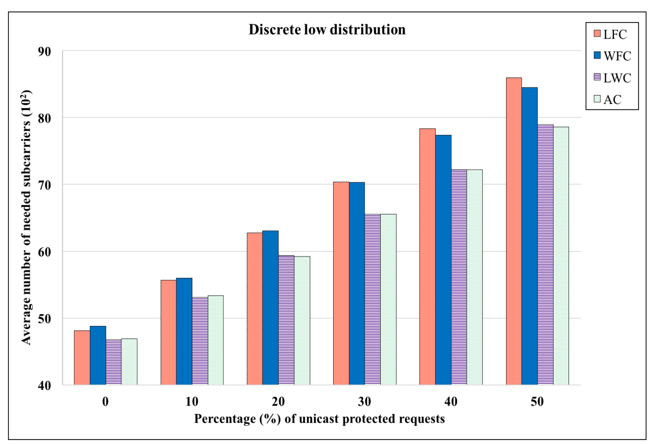


Figure 8. Average number of subcarriers as a function of the percentage of unicast protected requests; discrete low frequency slot distribution.

2) Second Scenario:

The second scenario, which has been simulated in 14-node NSFNET, considers a more varied demand, with unicast unprotected, unicast protected, and multicast unprotected requests. Figures 9, 10, and 11 show the average number of needed subcarriers versus the percentage of the sum of unicast protected and multicast unprotected requests for both our proposed algorithms (LWC and AC) and the existing LFC and WFC algorithms. Table VII presents the performance improvements of our proposed algorithms when compared to LFC and WFC, for different distributions. As shown in Figures 9, 10, and 11, both proposed algorithms perform better than either the LFC or WFC algorithms. In particular, in the case of a discrete high frequency slot distribution, LWC and AC improved the results obtained with LFC by 10.6 % and 10.7 %, respectively; when compared with WFC, improvements of 7.2 % and 7.1 % were respectively obtained.

TABLE VII. AVERAGE PERCENTUAL IMPROVEMENTS IN THE SECOND SCENARIO

Distribution	LWC		AC	
	LFC	*WFC*	*LFC*	*WFC*
Uniform	10.1 %	7.3 %	10.1 %	7.5 %
Discrete high	10.6 %	7.2 %	10.7 %	7.1 %
Discrete low	8.2 %	6.1 %	8.1 %	6.1 %

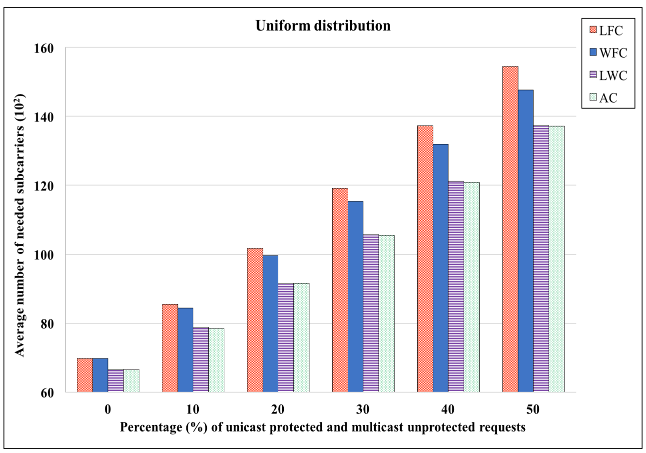


Figure 9. Average number of subcarriers as a function of the percentage of unicast protected and multicast unprotected requests; uniform frequency slot distribution.

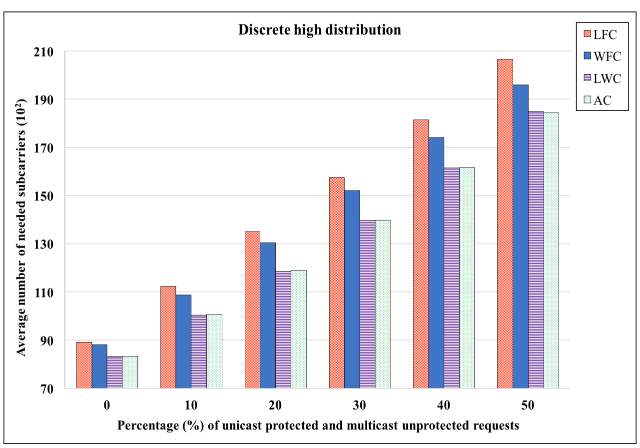


Figure 10. Average number of subcarriers as a function of the percentage of unicast protected and multicast unprotected requests; discrete high frequency slot distribution.

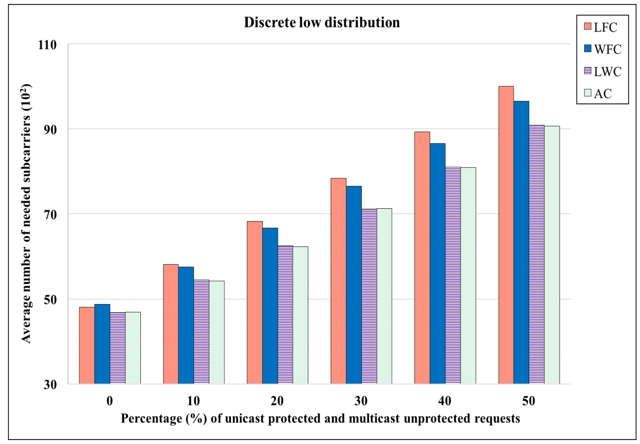


Figure 11. Average number of subcarriers as a function of the percentage of unicast protected and multicast unprotected requests; discrete low frequency slot distribution.

3) Third Scenario:

For the third and last scenario, where the demand includes unicast protected and multicast protected requests, the simulation is performed for the 21-node UK backbone. Figures 12, 13, and 14 show the average number of needed subcarriers versus the percentage of multicast protected requests for both our proposed algorithms (LWC and AC) and the existing LFC and WFC algorithms. Table VIII presents the performance improvements of our proposed algorithms when compared to LFC and WFC, for different frequency slot distributions. It can be observed that considering multicast protected requests along with unicast protected requests noticeably increases the number of needed subcarriers, especially in the discrete high distribution case. Spectrum consumption therefore increases when the traffic demand includes multicast protected requests. As shown in Figures 12, 13, and 14, both proposed algorithms performed better than either the LFC or WFC algorithms. In particular, in the case of a discrete high distribution of the requested frequency slots, LWC and AC improved the results obtained with WFC by 6.1 % and 6.3 %, respectively; when compared with LFC, even higher improvements of 4.6 % and 4.8 % were respectively obtained.

As mentioned previously, considering both dimensions; the amount of spectrum and the number of links (both primary and backup links); while sorting the requests, affects the number of subcarriers needed to serve the traffic demand. Therefore, the proposed sorting mechanisms outperform the existing mechanisms, and require less number of subcarriers.

TABLE VIII. AVERAGE PERCENTUAL IMPROVEMENTS IN THE THIRD SCENARIO

Distribution	LWC		AC	
	LFC	*WFC*	*LFC*	*WFC*
Uniform	4.5 %	5.5 %	4.6 %	5.6 %
Discrete high	4.6 %	6.1 %	4.8 %	6.3 %
Discrete low	2.8 %	3.8 %	2.8 %	3.7 %

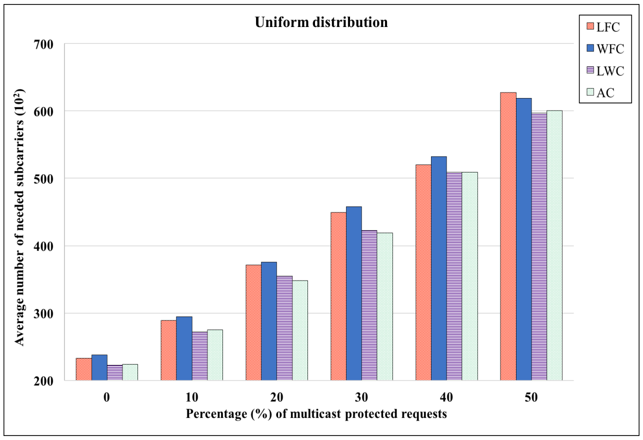


Figure 12. Average number of subcarriers as a function of the percentage of multicast protected requests; uniform frequency slot distribution.

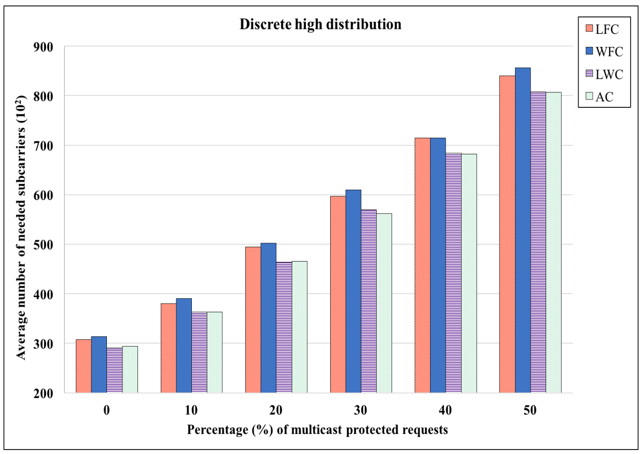


Figure 13. Average number of subcarriers as a function of the percentage of multicast protected requests; discrete high frequency slot distribution.

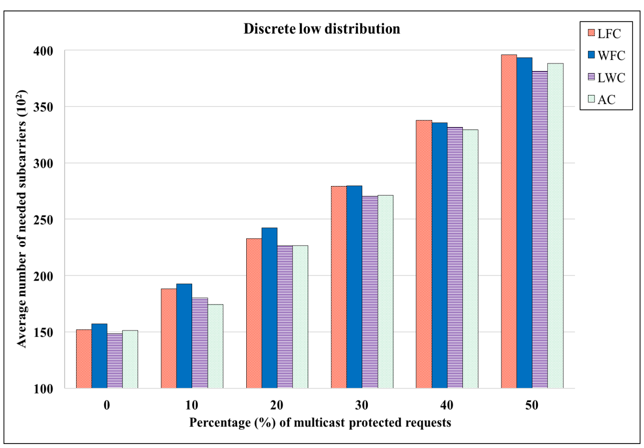


Figure 14. Average number of subcarriers as a function of the percentage of multicast protected requests; discrete low frequency slot distribution.

Overall, the simulation results demonstrate the viability and effectiveness of the proposed algorithms in serving different traffic demands (i.e., with different fractions of unicast unprotected, unicast protected, multicast unprotected, and multicast protected requests) using a smaller number of subcarriers than the existing algorithms, across a range of demand frequency slot distributions.

VI. CONCLUSION AND FUTURE WORK

In this paper, we addressed the intractable offline RSA problem in protection- and/or multicast-based EONs, with the objective of minimizing the total amount of spectrum needed to serve traffic demand when this demand includes unicast unprotected, unicast protected, multicast unprotected, and multicast protected requests. We investigated the efficiency of priority allocation algorithms based on the compact scheduling algorithm and the ordering obtained with two different metrics, both of which consider the frequency slot and required number of links of the requests presented to the network, albeit in slightly different ways. We evaluated the performance of the algorithms across a range of demand frequency slot distributions, and for a set of different demand composition scenarios, in two mesh topologies, the 14-node NSFNET and the 21-node UK backbones. The obtained experimental results have shown that the proposed algorithms outperformed other reference algorithms in term of spectrum utilization. The proposed algorithms are robust, and can be used in EONs with different setups.

This work can be extended in several interesting directions. For instance, it would be enlightening to investigate the online RSA problem in protection- and/or multicast-based EONs, in what concerns the reduction of blocking and/or fragmentation obtainable by combining multiple bin packing algorithms (e.g., first fit, best fit, and worst fit). Moreover, the algorithms can be extended to achieve the power saving in the survivable EONs with an energy-efficient hybrid protection scheme (i.e., shared and dedicated) [43], while serving the maximum amount of traffic [44]. Additionally, it would also be very interesting to study the trade-off between the energy consumption and fragmentation [45].

REFERENCES

[1] R. Alaskar, A. Alyatama, and I. Ahmad, "Offline Routing and Spectrum Allocation Algorithms for Elastic Optical Networks with Survivability," *16th Int. Conf. on Networks*, Venice, 2017, pp. 8-14.

[2] R.W. Alaskar, I. Ahmad, and A. Alyatama, "Offline routing and spectrum allocation algorithms for elastic optical networks," *Opt. Switch. Netw.*, vol. 21, pp. 76-92, July 2016.

[3] M. Jinno et al., "Spectrum-efficient and scalable elastic optical path network: architecture, benefits, and enabling technologies," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 66-73, Nov. 2009.

[4] O. Gerstel, M. Jinno, A. Lord, and S.J. Yoo, "Elastic optical networking: a new dawn for the optical layers?," *IEEE Commun. Mag.*, vol. 50, no. 2, pp. s12-s20, Feb. 2012.

[5] M. Klinkowski and K. Walkowiak, "Routing and spectrum assignment in spectrum sliced elastic optical path network," *IEEE Commun. Lett.*, vol. 15, no. 8, pp. 884-886, Aug. 2011.

[6] C. Politi et al., "Dynamic operation of flexi-grid OFDM-based networks," *Optical Fiber Communication Conf. and the Nat. Fiber Optic Engineers Conf.*, Los Anglos, CA, 2012, pp. 1-3.

[7] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, Part I – Protection," *18th Annu. Joint Conf. IEEE Computer and Communications Societies*, New York, 1999, pp. 744-751.

[8] R. Ramaswami, K. Sivarajan, and G. Sasaki, Optical Networks: A Practical Perspective, CA (2001).

[9] L. Ruan and Y. Zheng, "Dynamic survivable multipath routing and spectrum allocation in OFDM-based flexible optical networks," *J. Opt. Commun. Netw.*, vol. 6, no. 1, pp. 77-85, Jan. 2014.

[10] G. Shen and Q. Yang, "From coarse grid to mini-grid to gridless: How much can gridless help contentionless?," *Optical Fiber Communication Conf. and Expo. and the Nat. Fiber Optic Engineers Conf.*, Los Anglos, CA, 2011, pp. 1-3.

[11] M. Klinkowski and K. Walkowiak, "Offline RSA algorithms for elastic optical networks with dedicated path protection consideration," *4th Int. Congress on Ultra-Modern Telecommunications and Control Systems and Workshops*, St. Petersburg, 2012, pp. 670-676.

[12] T. Takagi et al., "Algorithms for maximizing spectrum efficiency in elastic optical path networks that adopt distance adaptive modulation," *13th European Conf. and Exhibition on Optical Communication*, Torino, 2010, pp. 1-3.

[13] D. Din and L. Lai, "Multicast protection problem on elastic optical networks using segment-base protection," *Int. Conf. on Informatics Electronics and Vision*, Fukuoka, 2015, pp. 1-6.

[14] A. Cai, M. Zukerman, R. Lin, and G. Shen, "Survivable multicast routing and spectrum assignment in light-tree-based elastic optical networks," *Asian Communication and Photonics Conf.*, Hong Kong, 2015.

[15] N. Singhal, C. Ou, and B. Mukherjee, "Cross-sharing vs self-sharing trees for protecting multicast sessions in mesh networks," *Comput. Netw.*, vol. 50, no. 2, pp. 200-206, Feb. 2006.

[16] M. Jinno et al., "Distance-adaptive spectrum resource allocation in spectrum-sliced elastic optical path network," *IEEE Commun. Mag.*, vol. 48, no. 8, pp. 138-145, Aug. 2010.

[17] S. Talebi, E. Bampis, G. Lucarelli, I. Katib, and G. Rouskas, "Spectrum assignment in optical networks: a multiprocessor scheduling perspective," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 6, no. 8, pp. 754-763, Aug. 2014.

[18] M. Klinkowski, "A genetic algorithm for solving RSA problem in elastic optical networks with dedicated path protection," *Adv. Intell. Syst. Comput*, vol. 189, pp. 167-176, 2013.

[19] S. Talebi et al., "Spectrum management techniques for elastic optical networks: a survey," *Opt. Switch. Netw.*, vol. 13, pp. 34-48, July 2014.

[20] B. Chatterjee, N. Sarma, and E. Oki, "Routing and spectrum allocation in elastic optical networks: a tutorial," *Commun. Surv. Tuts.*, vol. 17, no. 3, pp. 1776-1800, May 2015.

[21] A. Alyatama, "Dynamic spectrum allocation for orthogonal frequency-division multiplexing optical networks with survivability and multicasting," *J. High Speed Netw.*, vol. 22, no. 1, pp. 1-13, Feb. 2016.

[22] A. Tarhan and C. Cavdar, "Shared path protection for distance adaptive elastic optical networks under dynamic traffic," *5th Int. Congr. on Ultra-Modern Telecommunications and Control Systems and Workshops*, Almaty, 2013, pp. 62-67.

[23] M. Klinkowski, "An evolutionary algorithm approach for dedicated path protection problem in elastic optical networks," *Cybern. Syst.*, vol. 44, no. 6-7, pp. 589-605, Aug. 2013.

[24] K. Walkowiaka, M. Klinkowskib, B. Rabiegaa, and R. Gościeńa, "Routing and spectrum allocation algorithms for elastic optical networks with dedicated path protection," *Opt. Switch. Netw.*, vol. 13, pp. 63-75, July 2014.

[25] J. López, Y. Ye, V. López, and F. Jimenez, "Traffic and power-aware protection scheme in elastic optical networks," *15th Int. Telecommunications Network Strategy and Planning Symposium*, Rome, 2012, pp. 1-6.

[26] S. Shirazipourazad, C. Zhou, and A. Sen, "On routing and spectrum allocation in spectrum-sliced optical networks," *IEEE INFOCOM*, Turin, 2013, pp. 385-389.

[27] C. Yang, N. Hua, and X. Zheng, "Shared Path Protection based on Spectrum Reserved Matrix Model in Bandwidth-Variable Optical Networks," *7th Int. ICST Conf. Communications and Networking in China*, Kun Ming, 2012, pp. 256-261.

[28] M. Liu, M. Tornatore, and B. Tornatore, "Survivable Traffic Grooming in Elastic Optical Networks—Shared Protection," *J. Lightw. Technol.*, vol. 31, no. 6, pp. 903-909, March 2013.

[29] K. Walkowiak and M. Klinkowski, "Shared Backup Path Protection in Elastic Optical Networks: Modeling and Optimization," *9th Int. Conf. Design of Reliable Communication Networks*, Budapest, 2013, pp. 187-194.

[30] B. Chen et al., "Spectrum-block consumption for shared-path protection with joint failure probability in flexible bandwidth optical networks," *Opt. Switch. Netw.*, vol. 13, pp. 49-62, July 2014.

[31] H. Liu, M. Zhang, P. Yi, and Y. Chen, "Shared path protection through reconstructing shareable bandwidth based on spectrum segmentation for elastic optical networks," *Opt. Fiber Technol.*, vol. 32, pp. 88-95, Dec. 2016.

[32] R. Goścień, K. Walkowiak, and M. Tornatore, "Survivable multipath routing of anycast and unicast traffic in elastic optical networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 8, no. 6, pp. 343-355, June 2016.

[33] B. Chen et al., "Spectrum aware survivable strategies with failure probability constraints under static traffic in flexible bandwidth optical networks," *J. Lightw. Technol.*, vol. 32, no. 24, pp. 4823-4836, Dec. 2014.

[34] G. Shen, G. Guo, and S.K. Bose, "Survivable elastic optical networks: survey and perspective," *Photonic Netw. Commun.*, vol. 31, no. 1, pp. 71-87, Feb. 2016.

[35] R. Goscien, K. Walkowiak, M. Klinkowski, and J. Rak, "Protection in elastic optical networks," *IEEE Network*, vol. 29, no. 6, pp. 88-96, Dec. 2015.

[36] W. Kmiecik, R. Goścień, K. Walkowiak, and M. Klinkowski, "Two-layer optimization of survivable overlay multicasting in

elastic optical networks," *Opt. Switch. Netw*., vol. 14, no. 2, pp. 164-178, Aug. 2014.

[37] R. Goscien, K. Walkowiak, and M. Klinkowski, "Tabu search algorithm for routing, modulation, and spectrum allocation in elastic optical network with anycast and unicast traffic," *Comput. Netw.*, vol. 79, pp. 148-165, March 2015.

[38] X. Liu, L. Gong, and Z. Zhu, "Design integrated RSA for multicast in elastic optical networks with a layered approach," *IEEE Global Comuunication Conf.*, Atlanta, 2013, pp. 2346-2351.

[39] L. Gong et al., "Efficient resource allocation for all-optical multicasting over spectrum-sliced elastic optical networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 5, no. 8, pp. 836-847, Aug. 2013.

[40] C. Constrantinou and G. Ellinas, "A load balancing technique for efficient survivable multicasting in mesh optical networks," *Opt. Switch. Netw.*, vol. 22, pp. 1-8, Nov. 2016.

[41] N. K. Singhal, L. H. Sahasrabuddhe, and B. Mukherjee, "Provisioning of survivable multicast sessions against single link failures in optical WDM mesh networks," *J. Lightw. Technol*., vol. 21, no. 11, pp. 2587-2594, Nov. 2003.

[42] L. Long and A. Kamal, "Tree-based protection of multicast services in WDM mesh networks," *IEEE Global Telecomuunication Conf.*, Honolulu, 2009, pp. 1-6.

[43] N. Anoh et al., "An affection hybrid protection scheme with shared/ dedicated backup paths on elastic optical networks," *Digital Commun. and Netw*., vol. 3, no. 1, pp. 11-18, Feb. 2017.

[44] R. Ren et al., "Spectrum and energy-efficient survivable routing algorithm in elastic optical network," *Optik*, vol. 127, no. 20, pp. 8795-8806, Oct. 2016.

[45] J. Vizcaino et al., "Protection in optical transport networks with fixed and flexible grid: cost and energy efficiency evaluation," *Opt. Switch. Netw*., vol. 11, pp. 55-71, Jan. 2014.