BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 71(2), 2023, Article number: e145568
DOI: 10.24425/bpasts.2023.145568

ELECTRONICS, TELECOMMUNICATION AND OPTOELECTRONICS

Handling high- and low-priority traffic in multi-layer networks

Edyta BIERNACKA*, Piotr BORYŁO, Piotr JURKIEWICZ, Robert WÓJCIK, and Jerzy DOMŻAŁ

Institute of Telecommunications, AGH University of Science and Technology, Kraków, Poland

Abstract. In this paper, we propose a novel priority-aware solution named bypass to handle high- and low-priority traffic in multi-layer networks. Our approach assumes diversification of elastic optical spectrum to ensure additional resources reserved for emergency situations. When congestion occurs, the solution dynamically provides new paths, allocating a hidden spectrum to offload traffic from the congested links in the IP layer. Resources for a bypass are selected based on traffic priority. High-priority traffic always gets the shortest bypasses in terms of physical distance, which minimizes delay. Bypasses for low-priority traffic can be established if the utilization of the spectrum along the path is below the assumed threshold. The software-defined networking controller ensures the global view of the network and cooperation between IP and elastic optical layers. Simulation results show that the solution successfully reduces the amount of rejected high-priority traffic when compared to regular bypasses and when no bypasses are used. Also, overall bandwidth blocking probability is lower when our priority-aware bypasses are used.

Key words: elastic optical resources; high-priority traffic; multi-layer networks; priority-aware bypasses.

1. INTRODUCTION

Global network traffic grows rapidly, driven mainly by the number of network users and the increasing popularity of Internet streaming services (e.g., video and game streaming). New services and applications appear one by one, and they require additional bandwidth. To meet the requirements of emerging applications, future networks must transmit traffic with diverse quality of service (QoS) requirements. An important issue is priority awareness of traffic. For traffic fluctuations, the network should be able to handle high-priority traffic without disruptions even under congestion conditions.

The mentioned problem may be approached from the multi-layer network perspective, in which traffic management is performed in various layers. Such an approach has become a popular infrastructure for network operators [1]. An architecture consists of an optical substrate for physical communication, with a virtual (IP) layer on the top. The optical layer is responsible for carrying IP traffic by setting optical connections (lightpaths). Since then, significant efforts have been made to develop a technology that efficiently utilizes spectral resources. Elastic optical networks (EONs) have been proposed as a potential optical technology suitable to overcome tremendous traffic growth [2]. The EON offers efficient utilization of the spectral resources thanks to the flexible grid resources (spectrum is divided into narrow frequency slots denoted as slices) and adaptive transmission rates (utilizing multi-carrier modulation formats). Further, cooperation between virtual and optical layers is needed to balance resource utilization in both layers. Centralized architectures, such as software-defined networking (SDN), are the most promising candidates to meet those requirements [3,4]. In SDN, the principle is that the control plane and data plane are separated. The network control logic resides in the central controller, which instructs all the nodes on how to process forwarded data.

To deal with congestions in SDN-based multi-layer networks, a bypass mechanism was proposed in [5]. The concept of bypasses introduces diversification of optical resources in IP-over-optical networks. Only a selected part of optical resources is revealed to the IP layer which means that it can be used for setting lightpaths abstracted as virtual links. On the other hand, the remaining part of optical resources is denoted as hidden resources, and can be used when needed. The term bypass refers to a lightpath utilizing hidden resources and created on demand. When a request cannot be served in the IP layer due to a lack of resources, a new lightpath (bypass) is established, but a virtual link is not created. For example, bypasses in [5] and [6] handle traffic in IP-over-WDM (Wavelength Division Multiplexing) networks. Optical resources are divided; some wavelengths (lambdas) are available and visible for IP, whereas others are used to build bypasses when congestions occur.

In this paper, we propose a novel priority-aware bypass (PAB) solution aimed at reducing bandwidth-blocking probability (BBP) for high-priority traffic in multi-layer EONs utilizing the SDN concept. We assume high- and low-priority requests generated dynamically. The aim is to handle unexpected high-priority traffic spikes and minimize BBP for it. Our approach assumes two types of EON resources in the multi-layer network [7]. When congestion occurs, the proposed algorithm tries to select and allocate hidden elastic optical resources for

*e-mail: edyta.biernacka@.edu.pl

Manuscript submitted 2023-01-02, revised 2023-03-10, initially accepted for publication 2023-03-20, published in June 2023.

a bypass, depending on the priority of the traffic. While setting bypasses, all routing, modulation format and spectrum allocation (RMSA) constraints are satisfied. The centralized network controller monitors the utilization of resources in the IP and EON layers. The mechanism is implemented and assessed in the OMNeT++ simulator [8]. The proposed solution allows for advanced traffic service and effectively handles unexpected high-priority traffic growth.

The main contributions of this paper can be summarized as follows:

- We study the important problem of handling high-priority traffic in emergency situations.
- We utilize SDN as a promising control plane.
- We consider the newest standard of flex-grid in the optical layer.
- We thoroughly evaluate the performance of the proposed approach using numerical simulations. For a comprehensive and unbiased comparison, we implement agnostic and nonbypass references approaches.
- The proposed approach shows promising results in terms of BBP, especially for high-priority traffic.

The remainder of this paper is organized as follows. The survey of related works is provided in Section 2. Furthermore, we define a dynamic multi-layer problem in Section 3 and present elastic optical resources assumed for bypasses in Section 4. Then, we propose the PAB algorithm in Section 5.1 to solve the problem in a priority-aware manner. The network model used during simulations, as well as assumptions, are presented in Section 6. Numerical results are shown and discussed in Section 7, whereas conclusions are provided in Section 8.

2. RELATED WORK

Several works have already addressed the issue of handling network requests in a priority-aware manner in multi-layer networks. Note that these solutions consider the visibility of all EON resources for IP layer. We also present papers that assume hiding EON resources in multi-layer infrastructures, but in a priority-agnostic way.

Firstly, we present papers investigating multi-layer resources in the context of traffic prioritization. For example, the solution proposed in [9] combines routing in the electric layer and resource allocation in the EON layer according to the traffic priority. When congestion occurs, the number of services for selected requests is lowered to minimize BBP. Solution proposed in [10] also differentiates traffic. Based on the priority, traffic is routed through the network utilizing different paths in the IP layer. Additionally, optimization of the IP layer based on traffic rerouting utilizing existing or potential lightpaths has been introduced for handling requests in a priority-aware manner. However, solutions [9] and [10] assume that all EON resources are available for the IP layer, which is the most important difference in comparison to our work. The aim of our work is to show that traffic prioritization is possible to be used together with bypasses.

An interesting approach to handle high-priority traffic fluctuations has been presented in [11]. The main idea of multi-layer allocation is to split existing lightpaths under congestion conditions. A lightpath is divided into shorter parts to apply more efficient modulation formats. As a result, the capacity of virtual links is increased. Nevertheless, it can be noticed that the number of electric hops for the routing path in the IP layer also increases.

The problem of planning resources in IP-over-EONs to serve multiple classes of traffic is addressed in [12]. Traffic demands are known in advance and divided into two categories according to latency constraints, e.g., maximum end-to-end delay. The proposed algorithm calculates paths to satisfy the requested bandwidth and end-to-end latency for the demands. The latency comprises electronic processing delay in the IP layer and propagation delay in the EON layer. The candidate paths consist of existing virtual links (reusing spare available bandwidth of lightpaths) or new lightpaths. The proposed solution selects the shortest paths for delay-sensitive traffic. After checking all constraints, the spectrum is allocated to that traffic demand along the selected path using the first-fit policy. Nevertheless, all established lightpaths represent virtual links in the IP layer, and the scenario is limited to the planning phase of multi-layer resources rather than considering a dynamic traffic scenario.

All multi-layer solutions presented above assume that all EON resources are available for the IP layer, which is the most important difference in comparison to our work.

Finally, in [7] and [13], elastic optical bypasses are used in IP-over-EONs. Diversification of EON resources is explored to offload traffic fluctuations. In [7], the proposed bypasses reduce bandwidth blocking probability and minimize utilization of resources in the IP and EON layer, whereas in [13], the proposed solution provides a reduction of power consumption for networks. Nevertheless, these solutions are priority agnostic.

To sum up, hidden resources in the context of priority-aware policies remain unexplored. To the best of our knowledge, there are no other works that directly focus on the issues addressed in this paper.

3. DESCRIPTION OF PROBLEM

In this paper, we focus on providing additional resources through bypasses established in a priority-aware manner for traffic growth in multi-layer architectures. The study considers dynamic traffic scenarios where demands arrive and disappear stochastically. Resources to handle requests are allocated dynamically with respect to the current state of the network. We assume a network architecture comprising: virtual (IP) and EON layers [14]. Routers are able to groom traffic in the electric layer. Simultaneously, full flexibility is assumed in a sense that each router port is connected to a sliceable transponder able to groom multiple traffic streams in the optical domain [15]. According to [7] we also introduce two types of spectrum resources in the EON layer, namely: visible (available for IP layer) and hidden (dedicated for bypasses) in multi-layer networks. Figure 1 shows a simple network architecture containing IP and EON layers. This figure explains the difference between lightpaths associated with virtual links and bypasses. Diversification of resources is introduced for each fiber link,

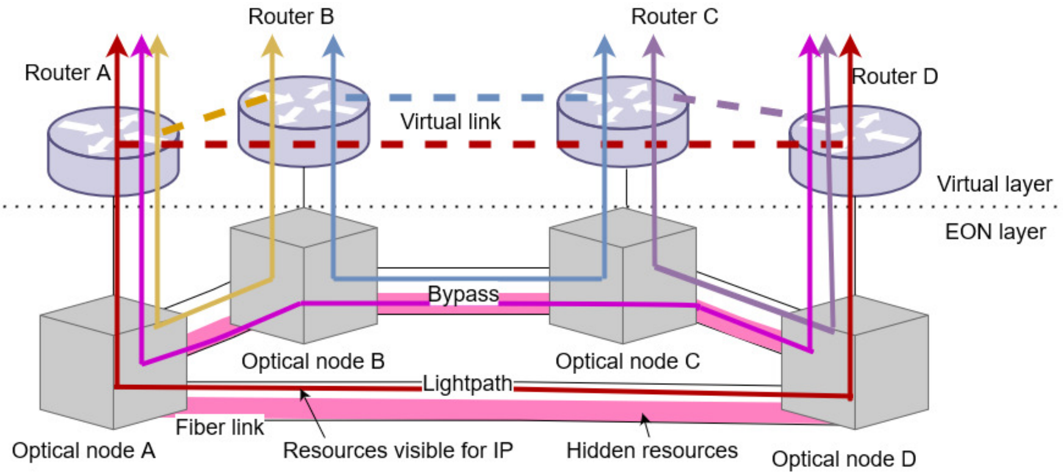

Fig. 1. Example of lightpaths associated with virtual links and bypass

the white color and the pink color of resources denote resources available for IP and hidden resources, respectively. As can be seen, lightpaths utilizing resources visible for IP layer are reported as virtual links between routers, e.g., lightpaths between nodes A–B (solid yellow line), B–C (solid blue line) handle virtual links between routers A–B (dotted yellow line), B–C (dotted blue line), respectively. A lightpath between nodes A-D through B and C (solid pink line) is a bypass since it allocates a hidden spectrum. This bypass is established to offload traffic, but a new virtual link is not reported in the IP layer. When transmission handled by the bypass ends, the lightpath is torn down and resources are released.

In multi-layer networks, the problem of resource allocation can be divided into two sub-problems separately corresponding to each layer. First one is routing over a virtual topology, while the second regards the lightpath setup process. Especially, the lightpath setup process is an important issue when bypasses (elastic lightpaths utilizing hidden resources) need to be dynamically established to omit links congested in the IP layer. This requires Solving a specific problem for the EON layer, namely, the routing and modulation format and spectrum allocation (RMSA) problem [16].

4. ELASTIC OPTICAL RESOURCES FOR BYPASSES

We assume that the EON layer is deployed as an optical layer in multi-layer networks. In the EON, the available optical spectrum is divided into narrow frequency slices of a given granularity (e.g. 6.25 GHz, 12.5 GHz, or 37.5 GHz) [17]. The width of a slice corresponds to the bandwidth of an orthogonal frequency-division multiplexing subcarrier. To solve the problem of allocation of such optical resources (in terms of a number of adjacent slices) along links composing an end-to-end path the RMSA algorithms are introduced [18]. In this context, to set up bypasses the RMSA algorithm is needed since elastic lightpaths need to be established. While setting bypasses the algorithms must satisfy the following RMSA constraints:

- spectrum continuity constraint: the lightpath must allocate the same set of slices along links of an end-to-end path,
- spectrum contiguousness constraint: all slices assigned to a lightpath should be adjacent,
- non-overlapping spectrum constraint: at the same time, at most one lightpath occupies particular slices of the link,
- transmission distance constraint: the length of an end-to-end path, that uses a modulation format, cannot be longer than the maximum transmission distance range for this modulation format,
- guard band constraint: two neighbour lightpaths must be separated by a guard band.

To understand RMSA constraints we provide an example. Figure 2 presents resources of two links. Diversification of optical resources is introduced, i.e., yellow color denotes resources reserved for IP layer. Three different bypasses are already established and occupy hidden spectrum. The arriving request re-

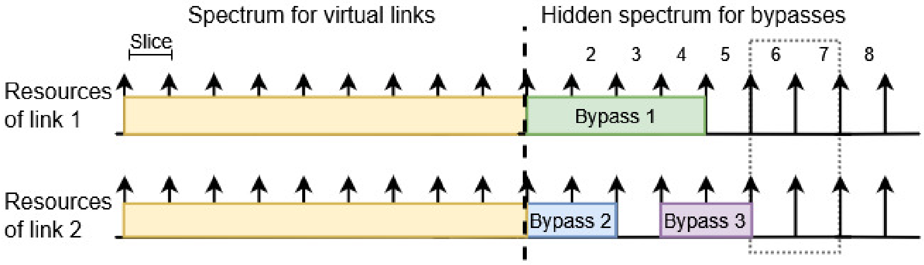

Fig. 2. Example of optical resources

quires 2 slices (including guard band) for the selected modulation format along links 1 and 2. Thus slices 6th and 7th satisfy the continuity, contiguousness, non-overlapping spectrum constraint and can be assigned along links 1 and 2 (dotted line).

In this paper, we apply a two-step strategy [16, 19]. Our algorithm firstly finds a feasible path with determined modulation format. Secondly, it allocates a required number of slices (hidden spectrum) between end nodes.

5. HANDLING TRAFFIC IN MULTI-LAYER NETWORKS

In this section, we describe in details our new concept of priority-aware bypasses (PAB). The goal of PAB is to provide additional resources through bypasses established in a priority-aware manner for emergency situations. Then we explain agnostic bypasses [7] and nonbypass scenario. Note that, all the algorithms handle traffic in the IP layer in the same way. To better understand algorithms, we introduce the notation that will be used further in this paper. Let us assume a request d defined by s, t, BW_{req}, *priority*, where s is the source node and t is the destination node of the request. BW_{req} represents the requested bandwidth between nodes s and t in Gbps, whereas, *priority* defines the priority of the request in terms of low or high. The following sections describe the concept and reference algorithms.

5.1. Priority-aware bypasses

We propose the novel algorithm to establish bypasses in a priority-aware manner. It means that high- and low-priority traffic is handled differently.

In order to manage multi-layer resources, address the dynamic conditions in the infrastructure, and effectively handle incoming network requests, the SDN controller is utilized. When the request arrives, the SDN controller uses information about the current utilization of virtual links from the network devices installed in the IP layer and current utilization of optical links from the network devices installed in the optical layer. Thanks to that, the controller may optimize path establishment process.

Pseudocode for describing the PAB algorithm is shown in Fig. 3. The algorithm starts when a new request arrives. The controller verifies if sufficient resources are available. Firstly, the SDN controller estimates resources in IP, no matter of priority of traffic. To route traffic between s and t, a single shortest path is determined in the IP layer (line 1) using the Open Shortest Path First (OSPF) protocol. If sufficient resources are available on the part of the spectrum available to the IP layer, then traffic is sent using those resources and the algorithm returns true (lines 2-4). If requested bandwidth cannot be guaranteed in IP layer (line 6), then the SDN controller tries to utilize the EON layer.

Algorithm 1 Priority-aware bypasses

Input:New $d(s, t, BW_{req}, priority)$;

```
1:  Estimate resources in IP
2:  if Route in IP is not congested then
3:     Service in IP
4:     return true
5:  end if
6:  if Route in IP is congested then
7:     Utilize EON layer
8:     Determine priority of traffic
9:     if $priority$ of $d$ is high then
10:       for $p \in P(s,t,k)$ in increasing order of length do
11:          Determine number of slices
12:          if Resources exist then
13:             Set bypass along $p$ according to FF policy
14:             return true
15:          end if
16:       end for
17:    end if
18:    if $priority$ of $d$ is low then
19:       for $p \in P(s,t,k)$ in increasing order of length do
20:          Calculate utilization of hidden resources for $p$
21:          if Utilization(p) $<$ Utilization threshold then
22:             Determine number of slices $n_{bypass}$
23:             if Resources exist then
24:                Set bypass along $p$ according to FF policy
25:             end if
26:             return true
27:          end if
28:       end for
29:    end if
30:    return false // blocked request
31: end if
```

Fig. 3. Pseudocode for describing the PAB algorithm

It should be noted that d in the virtual layer denotes requirement for bandwidth, while d for EON is a request for setting lightpaths according to the RSMA problem solution. Any bypass established in the optical layer is composed of slices. The number of adjacent slices further determines the amount of bandwidth provided by that bypass. The number of adjacent slices (n_{bypass}) required to handle bandwidth demand between two nodes (BW_{req}) along a considered physical bypass-path p is calculated according to the following equation [20]:

$$n_{\text{bypass}} = \left\lceil \frac{BW_{\text{req}}}{M * \Delta_{\text{slice}}} \right\rceil + GB, \tag{1}$$

where: BW_{req} [Gbit/s] denotes requested bandwidth; M [bit/s/Hz] is the spectral efficiency of the modulation format utilized on the bypass-path p; Δ_{slice} [GHz] denotes the width of frequency slice; GB is the number of slices for guard-band needed to separate adjacent optical transmissions. To determine modulation format for a particular bypass, the SDN controller compares the expected length of bypass-path and the maximum range of each modulation. The sum of link lengths included in the bypass-path cannot exceed the transmission reach of modulation selected for this path. Therefore, for a particular demand blocked in the upper layer, the width of the bypass depends on the requested bandwidth and modulation format used for transmissions between the end nodes.

The main goal of the EON layer is to minimize the amount of rejected bit-rate that is requested by high-priority traffic. Firstly, priority of traffic is determined (line 8). For the purpose of traffic provisioning, we use the k-shortest path algorithm to calculate candidate paths $P(s,t,k)$. Candidate paths $P(s,t,k)$ are sorted and organized in ascending order based on physical length.

Handling high-priority traffic. To handle high-priority request, the Shortest Path First (SPF) method with First Fit (FF) policy is applied (see Fig. 3, lines 9–17). Candidate paths are examined one by one to find the solution of RMSA. If an unoccupied set of slices n_{bypass} exists, a path is selected to handle the request d. Spectrum (the set of slices) along p is assigned according to the FF policy. If none of the paths meets the condition, the request is blocked and strategy returns false (see Fig. 3, line 30).

Handling low-priority traffic. Handling low-priority traffic in EON layer (see Fig. 3, lines 18–29) we introduce metric whose aim is to offload low-priority traffic and retain more hidden spectrum for high-priority one. Metric denotes utilization ratio calculated as the sum of occupied slices across all links of the path to the sum of the total number of slices across all links of the path. Bypasses for low-priority traffic are allowed along paths that spectrum is utilized below the assumed utilization threshold $utilization\_threshold$. Thus, if utilization for a particular path p is below the threshold assumed for low-priority traffic (line 21) and resources exist (line 23), spectrum along p is allocated according to the FF policy. If none of the paths meets the condition, the request is blocked and strategy returns false (see Fig. 3, line 30).

5.2. Agnostic bypasses

Pseudocode for describing the agnostic bypass algorithm is shown in Fig. 4. Similarly to PAB (see Section 5.1), the algorithm starts when a new request arrives. Note that, the SDN controller estimates resources in IP and in EON, regardless of the priority of traffic. A single shortest path between s and t is determined in the IP layer (line 1) using the OSPF protocol. If sufficient resources are available on the part of the spectrum available to the IP layer, then traffic is sent using those resources and the algorithm returns true (lines 2-4). Otherwise, (line 6), the SDN controller tries to utilize the EON layer (line 7).

Algorithm 2 Agnostic bypasses

Input:New $d(s,t,BW_{req},priority)$;

```
 1: Estimate resources in IP
 2: if Route in IP is not congested then
 3:    Service in IP
 4:    return true
 5: end if
 6: if Route in IP is congested then
 7:    Utilize EON layer
 8:    for $p \in P(s,t,k)$ in increasing order of length do
 9:       Determine the number of slices $n_{bypass}$
10:       if Resources exist then
11:          Set bypass along $p$ according to FF policy
12:          return true
13:       end if
14:    end for
15:    return false // blocked request
16: end if
```

Fig. 4. Pseudocode for describing the agnostic bypass algorithm

Candidate paths $P(s,t,k)$ are sorted and organized in ascending order, based on physical length. The SPF method with FF policy is applied (see Fig. 4, lines 8–17). The number of adjacent slices (n_{bypass}) required to handle requested bandwidth BW_{req} between nodes s and t along a considered physical bypass-path p is calculated according to equation 1. Candidate paths are examined one by one to find the solution of RMSA. If an unoccupied set of slices n_{bypass} exists, a path is selected to handle the request d. The set of slices along p is assigned according to the FF policy. If none of the paths meets the condition, the request is blocked and the strategy returns false (line 15).

5.3. Nonbypass

Optical resources are fully visible for IP layer and bypasses are not utilized at all. Pseudocode for describing the nonbypass algorithm is shown in Fig. 5. The nonbypass algorithm starts when a new request arrives (similarly to PAB and agnostic bypass algorithms, see Sections 5.1 and 5.2). A single shortest path between s and t is determined in IP layer (line 1) using the OSPF protocol. If sufficient resources are available on the part of the spectrum available to the IP layer, then traffic is sent using those resources (lines 2–7) and the algorithm returns true (line 4). Otherwise, (lines 6–8), the algorithm returns false and the request is blocked (line 7).

Algorithm 3 Nonbypass

Input:New $d(s,t,BW_{req},priority)$;

```
1: Estimate resources in IP
2: if Route in IP is not congested then
3:    Service in IP
4:    return true
5: end if
6: if Route in IP is congested then
7:    return false // blocked request
8: end if
```

Fig. 5. Pseudocode for describing the nonbypass algorithm

Efficiency of the proposed PAB is validated through numerous simulations performed for two networks under dynamic traffic scenarios. PAB solution is compared with priority agnostic bypass policy and nonbypass scheme. The following sections contain simulation details as well as present and discuss the results of extensive numerical experiments conducted to assess PAB for prioritized traffic.

6. SIMULATION SETUP

In this section, we provide the simulation setup to evaluate the performance of the proposed PAB. Three utilization thresholds were assumed for the PAB algorithm, namely 0.9 (PAB(0.9)), 0.8 (PAB(0.8)) and 0.7 (PAB(0.7)).

6.1. Reference networks

To assess the proposed algorithms, simulations were performed in two reference networks: NSF15 (15 nodes, 46 directed links) and UBN24 (24 nodes, 86 directed links) [21] shown in Figs. 6 and 7, respectively. Distances between nodes are marked in figures. Table 1 presents parameters for networks investigated in simulations.

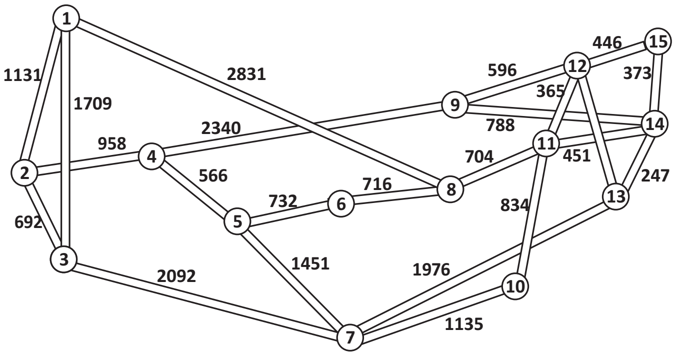

Fig. 6. The NSF15 network used in simulations

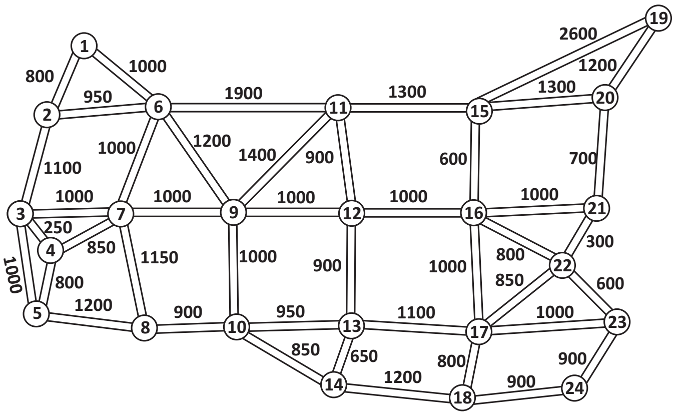

Fig. 7. The UBN24 network used in simulations

6.2. Simulation details

The topology of the IP and EON layers was the same. The optical spectrum was divided into 320 slices each of 12.5 GHz as specified in the ITU-T G.694.1 recommendation [17]. One slice was set as a guard band and introduced between neighbour transmissions.

The proposed PAB solution has been compared with priority agnostic bypass policy (presented in [7]), and reference nonbypass scheme (optical resources fully visible for IP layer and bypass mechanism is not utilized at all). In cases of bypass policies (PAB and priority agnostic) half of optical resources were hidden. In PAB and agnostic bypass each directed virtual link was created by the lightpath, which occupied 160 adjacent slices. Such an assumption is the most efficient, as proved in [7]. The nonbypass utilizes 320 slices in IP layer.

The topology of the virtual layer was established. Each directed virtual link was created by the lightpath that occupied resources visible for IP. Then the capacity of a virtual link c_{VL} [Gbit/s] comprising n_{VL} slices can be calculated using the following equation:

$$c_{VL} = (n_{VL} - GB) * M * \Delta_{\text{slice}}\,, \tag{2}$$

where: GB is the number of slices used for the guard band; M is the spectral efficiency of the modulation format utilized by lightpath; and Δ_{slice} denotes the width of a slice. Particularly, $n_{VL} = 320$ was used for nonbypass and $n_{VL} = 160$ was used for bypasses. Note that, capacities of virtual links are constant and are not changed during network operation.

To achieve elastic spectrum allocation, four modulation formats: BPSK (binary phase-shift keying), QPSK (quadrature phase-shift keying), 8QAM (8-quadrature amplitude modulation), 16QAM (16-quadrature amplitude modulation) were considered. We decided to use the same transmission model as in [22] and [23] assuming bit-rate per 12.5 GHz width slice for each modulation format of 12.5, 25, 37.5 and 50 Gbit/s and a transmission distance of 9600, 4800, 2400 and 1200 km, respectively. Table 2 describes parameters for modulation formats including spectral efficiency, transmission range, and bit rate per slice for each modulation format. The applied transmission distances allow to set up long bypasses without regeneration in the networks. The number of candidate paths considered for bypasses was 10. For a given path length, a usable modulation format with the highest bit-rate was chosen.

Table 1
Parameters for investigated networks

Parameter	NSF15	UBN24
Number of nodes	15	24
Number of links	46	86
Minimum node degree	2	2
Maximum node degree	4	5
Average node degree	3.07	3.58
Average link length	1022 km	997 km

Table 2
Spectral efficiency, transmission range and supported bit rate per slice for various modulation formats [23, 27]

Modulation format	Spectral efficiency	Maximum range	Bit rate
BPSK	1 bit/s/Hz	9600 km	12.5 Gbit/s
QPSK	2 bit/s/Hz	4800 km	25 Gbit/s
8QAM	3 bit/s/Hz	2400 km	37.5 Gbit/s
16QAM	4 bit/s/Hz	1200 km	50 Gbit/s

In addition to the dynamic traffic described below, we also generated long-lived background traffic to utilize resources of virtual links in varying degrees, particularly to create congestions. However, it is not taken under consideration during probability calculation and bandwidth-blocking probability assessment. In our experiments, background traffic is distributed uniformly between each pair of nodes with a bitrate equal to 200 Gbit/s for the NSF15 topology and 80 Gbit/s for the UBN24 topology. This is low-priority traffic. The background traffic is always handled in the virtual layer utilizing OSPF. In the case of non-bypass, background traffic is sent through virtual links associated with lightpaths that allocate 320 slices. In cases of agnostic bypasses and priority-aware bypasses, background traffic is sent through virtual links associated with lightpaths that allocate 160 slices available for the virtual layer. Even if the capacity of virtual links is equal, these links are occupied differently depending on the location in topology and the number of supported flows. The amount of traffic is selected in such a way as to ensure that a link is close to congestion. In cases of bypasses, the most loaded link utilizes 67% of virtual link capacity for NSF15 and UBN24 topologies. This allowed us to analyze bypasses in a near-real environment.

Low- and high-priority requests were generated dynamically between selected nodes in the network. We decided to select 4 nodes in NSF15 and 5 nodes in UBN24. Localization of these nodes generating requests in the network was determined according to values of the shortest path to any other network node [24]. As a result, nodes with indices $V_{sp} = \{12,13,14,15\}$ were selected in the NSF15 network, while nodes with indices $V_{sp} = \{9,10,12,13,16\}$ in the UBN24 network. For each pair of selected nodes, demands were uniformly distributed between 50 Gbit/s and 1 Tbit/s with a 50 Gbit/s step [25]. The high-priority traffic was 20% of dynamic requested bandwidth, while low-priority traffic was 80% of dynamic requested bandwidth.

Dynamic requests arrived one by one to the network with an exponentially distributed inter-arrival time and mean value iat and an exponentially distributed holding time ht. Therefore, the traffic load was computed as ht/iat Erlangs. In order to simulate different network conditions, the mean value of ht was changed in a step manner while iat remained constant. For each value of traffic load, the first 5000 requests were ignored to achieve steady-state. After that, another 10^5 requests were evaluated [26]. The simulations have been performed in OMNeT++ simulator [8].

6.3. Metrics

BBP was selected as a metric to assess the performance of methods. BBP was calculated taking into account solely dynamic requests. The following metrics were selected as a measure of the bypass and nonbypass methods performance:

- BBP for overall traffic is defined as the total bandwidth of all blocked demands divided by the total bandwidth requested by all demands.
- BBP for high-priority traffic is defined as the bandwidth of all blocked high-priority demands divided by the total bandwidth of all high-priority demands.
- BBP for low-priority traffic is defined as the bandwidth of all blocked low-priority demands divided by the total bandwidth of all low-priority demands.

All results presented in the next section are in logarithmic scale.

7. SIMULATION RESULTS

In this section, we present and analyze simulation results. The main objective is to assess the proposed bypass mechanism against reference approaches in terms of BBP. We separately analyze overall traffic as well as high- and low-priority traffic to provide a comprehensive study. The approach with the bypass mechanism disabled is further denoted as nonbypass, the priority agnostic bypass is simply denoted as bypass. To the best of our knowledge, there are no other works that are directly focused on dealing with high- and low-priority traffic utilizing hidden resources in IP-over-EONs; therefore, we select nonbypass and agnostic bypass as reference mechanisms. We believe that this is the best choice to meet our aims. Firstly, we are able to investigate how priority traffic is handled in IP-over-EON architecture by the most generic approaches: nonbypass and bypass. Secondly, we investigate how priority-aware bypasses can improve the performance of IP-over-EON architecture in terms of minimization of BBP. Therefore, as we measured BBP for overall, high-priority and low-priority traffic, we can verify if our proposal is suitable for IP-over-EON networks with heterogeneous traffic.

Firstly, BBP for overall traffic is shown in Figs. 8 and 9 for the NSF15 and UBN24 networks, respectively. Based on the figures, the following conclusions can be drawn for both networks. Nonbypass provides the worst performance in terms of BBP when compared to both approaches introducing bypass mechanism. That is because, in the nonbypass case, only a single path is utilized to handle traffic between a pair of nodes in the IP layer. Thus, there is no possibility to omit congested links. It confirms our findings in [7].

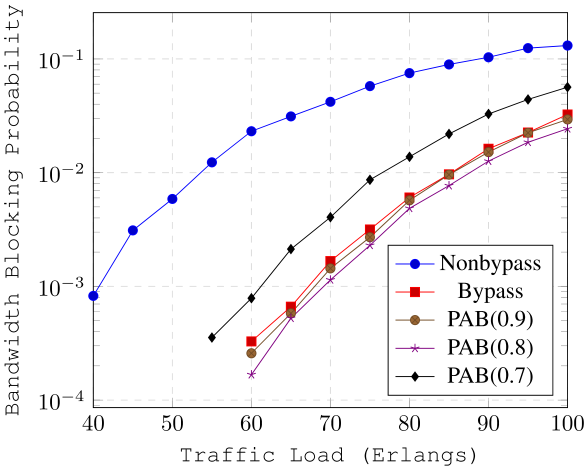

Fig. 8. BBP for overall traffic as a function of the traffic load in the NSF15 network

Furthermore, assuming 0.9 and 0.8 utilization threshold detailed analyses of the results for PAB and the priority agnostic

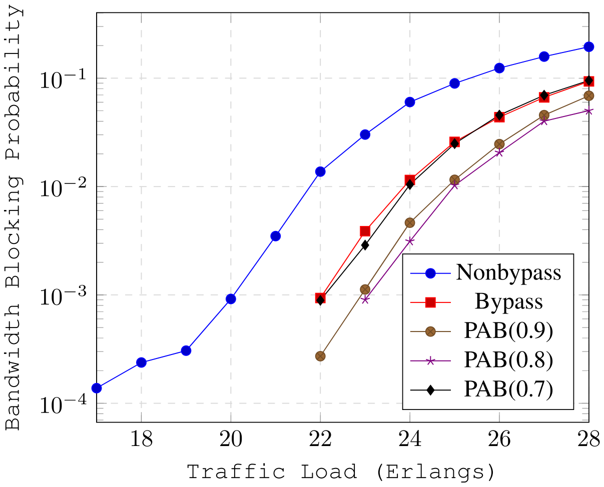

Fig. 9. BBP for overall traffic as a function of the traffic load in the UBN24 network

bypass show that PAB(0.9) and PAB(0.8) provide the level of BBPs not higher than priority agnostic bypass. These threshold values (0.9 and 0.8) allow to effectively distribute low-priority traffic over a network. However, PAB(0.7) deteriorates overall BBP when compared to PAB(0.9) and PAB(0.8). This is because PAB(0.7) reserves too much of the spectrum for high-priority traffic and the remaining resources are insufficient to handle low-priority traffic. As a result, the spectrum tends to become more occupied and the possibility to successfully establish lightpaths is decreased.

Simulation results obtained for high-priority traffic are presented in Figs. 10 and 11 for NSF15 and UBN24 networks, respectively. According to the results, the implementation of PAB reduces BBP for high-priority traffic for both networks. The BBP reduction for high-priority traffic increases with decreasing the value of utilization threshold under a given traffic load. PAB(0.7) provides the best reduction of BBP for high-priority traffic as more spectrum is reserved for it.

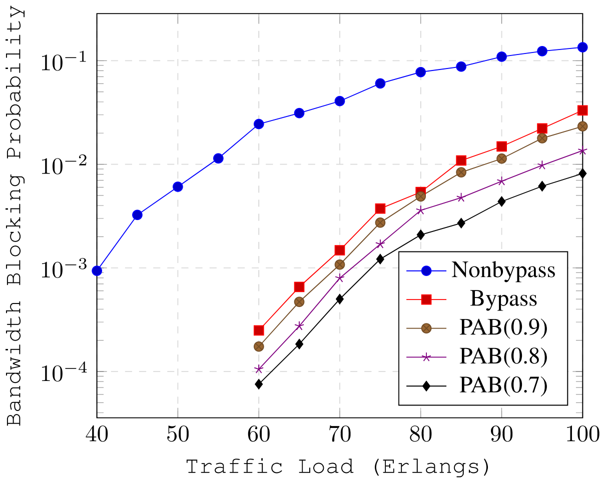

Fig. 10. BBP for high-priority traffic as a function of the traffic load in the NSF15 network

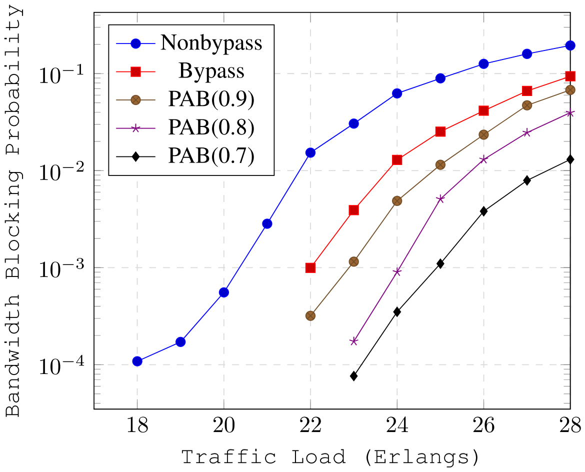

Fig. 11. BBP for high-priority traffic as a function of the traffic load in the UBN24 network

Simultaneously, simulation results obtained for low-priority traffic are shown in Figs. 12 and 13 for the NSF15 network and the UBN24 network, respectively. The BBP observed for low-priority traffic increases with decreasing threshold. Also, it can be seen that nonybass provides the highest BBP for high-priority traffic as well as for low-priority traffic in both networks.

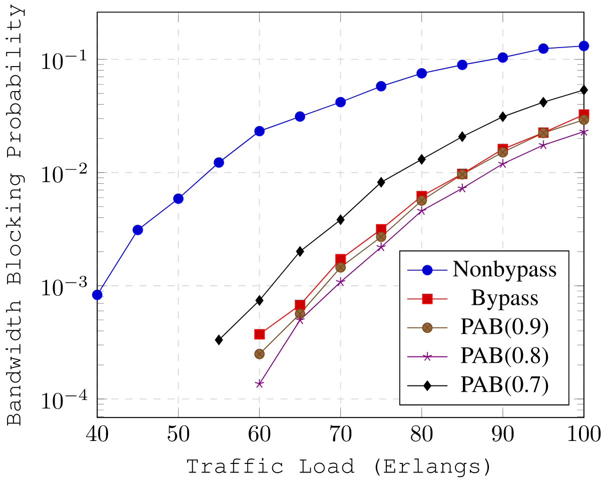

Fig. 12. BBP for low-priority traffic as a function of the traffic load in the NSF15 network

Some additional conclusions are as follows. Comparing results (BBP for overall traffic and for low-priority traffic) obtained in the NSF15 and UBN24 networks, we can notice differences in the relation between the performance of priority agnostic bypass and PAB(0.7). In NSF15, priority agnostic bypass provides lower BBPs for overall traffic and for low-priority when compared to PAB(0.7). Contrary, PAB(0.7) outperforms priority agnostic bypasses in the UBN24 network. It results from the fact that the average UBN24 node degree is higher than the average NSF15 node degree. Thus, PAB(0.7) effectively utilizes more paths without blocking low-priority traffic.

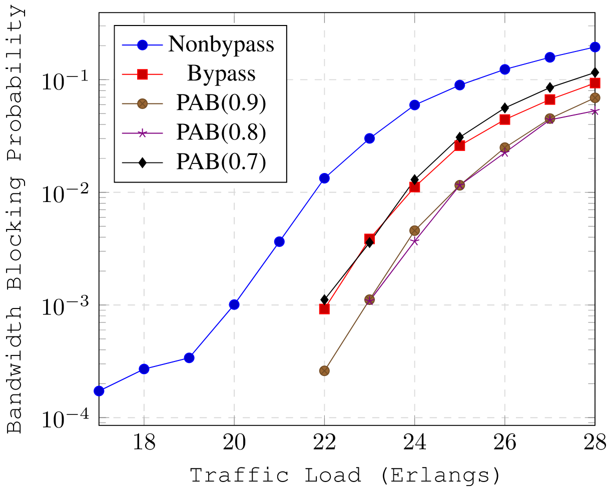

Fig. 13. BBP for low-priority traffic as a function of the traffic load in the UBN24 network

It confirms that the threshold should be carefully adjusted to the network topology.

To sum up, introducing priority awareness improves the performance of the bypass method for high-priority traffic. PAB(0.7) may achieve the lowest BBP for high-priority traffic in both networks. The value 0.8 of threshold ensures the trade-off between BBP reduction for high-priority and deterioration for low-priority, which results in the best BBP reduction for overall traffic. It is because the network load is distributed over the network evenly.

8. CONCLUSIONS

This paper proposes a novel multi-layer bypass algorithm to minimize BBP in a priority-aware manner. We introduced the utilization threshold to reserve spectrum for high-priority traffic. Hence, high-priority traffic is always handled by the shortest bypasses, whereas for low-priority traffic, alternative bypasses may be selected. The performance of the proposed algorithm was evaluated through extensive discrete event simulation studies and compared to the reference scenarios (nonbypass and priority agnostic bypass). Additionally, different utilization thresholds were considered for the PAB.

The analysis of the obtained results showed that priority-aware bypasses reduce BBP for high-priority traffic when compared to priority agnostic bypass and nonbypass scenarios. Moreover, PABs can serve more high-priority traffic until the first blocking event appears in a network. Finally, PABs also provide lower BBPs for overall traffic when compared to the nonbypas approach.

To sum up, it was demonstrated that priority-aware bypasses are suitable for handling unpredictable high-priority traffic growth originating from emerging situations. Since the proposed solution is fully compatible with the SDN concept, it is believed that the bypass approaches can be easily implemented in the SDN control plane. Priority-aware bypasses improve network performance in terms of reduction of BBP, nevertheless, handling traffic is priority agnostic in the virtual layer. In the future, we will focus on handling requests in a priority-aware manner in the virtual layer.

ACKNOWLEDGEMENTS

The research was carried out with the support of the project “Intelligent management of traffic in multi-layer Software-Defined Networks” founded by the Polish National Science Centre under project no. 2017/25/B/ST6/02186.

REFERENCES

[1] S. Fichera, R. Martínez, B. Martini, M. Gharbaoui, R. Casellas, D.R. Vilalta, R. Muñoz, and P. Castoldi, “Latency-aware resource orchestration in sdn-based packet over optical flexi-grid transport networks,” *IEEE/OSA J. Opt. Commun. Netw.*, vol. 11, no. 4, pp. B83–B96, April 2019, doi: 10.1364/JOCN.11.000B83.

[2] M. Jinno, “Elastic optical networking: Roles and benefits in beyond 100-gb/s era,” *J. Lightwave Technol.*, vol. 35, no. 5, pp. 1116–1124, March 2017, doi: 10.1109/JLT.2016.2642480.

[3] V. Lopez, D. Konidis, D. Siracusa, C. Rozic, I. Tomkos, and J.P. Fernandez-Palacios, “On the benefits of multilayer optimization and application awareness,” *J. Lightwave Technol.*, vol. 35, no. 6, pp. 1274–1279, Mar 2017.

[4] M. Kantor, E. Biernacka, P. Boryło, J. Domżał, P. Jurkiewicz, M. Stypiński, and R. Wójcik, “A survey on multi-layer IP and optical Software-Defined Networks,” *Comput. Netw.*, vol. 162, p. 106844, 2019, doi: 10.1016/j.comnet.2019.06.022.

[5] J. Domżał, Z. Duliński, J. Rząsa, P. Gawłowicz, E. Biernacka, and R. Wójcik, “Automatic Hidden Bypasses in Software-Defined Networks,” *J. Netw. Syst. Manag.*, vol. 25, pp. 457–480, 2017, doi: 10.1007/s10922-016-9397-5.

[6] P. Boryło, J. Domżał, and R. Wójcik, “Survivable automatic hidden bypasses in Software-Defined Networks,” *Comput. Netw.*, vol. 133, pp. 73–89, 2018, doi: 10.1016/j.comnet.2018.01.022.

[7] E. Biernacka, P. Boryło, R. Wójcik, and J. Domżał, “Elastic optical bypasses for traffic bursts,” *Comput. Commun.*, vol. 146, pp. 95–102, 2019, doi: 10.1016/j.comcom.2019.07.017.

[8] “Omnet++,” http://www.omnetpp.org.

[9] Z. Zhong, J. Li, N. Hua, G.B. Figueiredo, Y. Li, X. Zheng, and B. Mukherjee, “On qos-assured degraded provisioning in service-differentiated multi-layer elastic optical networks,” in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016, pp. 1–5.

[10] C. Rožić, M. Savi, C. Matrakidis, D. Klonidis, and D. Siracusa, “A dynamic multi-layer resource allocation and optimization framework in application-centric networks,” *J. Lightwave Technol.*, vol. 36, no. 20, pp. 4908–4914, 2018.

[11] Z. Zhong, N. Hua, M. Tornatore, J. Li, Y. Li, X. Zheng, and B. Mukherjee, “Provisioning short-term traffic fluctuations in elastic optical networks,” *IEEE/ACM Trans. Netw.*, vol. 27, no. 4, pp. 1460–1473, 2019.

[12] E. Etezadi, H. Beyranvand, and J.A. Salehi, “Latency-aware service provisioning in survivable multilayer ip-over-elastic optical networks to support multi-class of service transmission,” *Comput. Commun.*, vol. 183, pp. 161–170, 2 2022, doi: 10.1016/j.comcom.2021.12.003.

[13] B. Kadziolka, M. Skala, R. Wojcik, P. Jurkiewicz, and J. Domzal, “Employing FAMTAR and AHB to Achieve an Optical

Resource-Efficient Multilayer IP-Over-EON SDN Network," *IEEE Access*, vol. 10, pp. 94 089–94 099, 2022, doi: 10.1109/ACCESS.2022.3204290.

[14] C.A. Kyriakopoulos, G.I. Papadimitriou, and P. Nicopolitidis, "Towards energy efficiency in virtual topology design of elastic optical networks," *Int. J. Commun. Syst.*, vol. 31, no. 13, pp. 1–16, 2018, doi: 10.1002/dac.3727.

[15] Q. Zhu, X. Yu, Y. Zhao, A. Nag, and J. Zhang, "Auxiliary-graph-based energy-efficient traffic grooming in ip-over-fixed/flex-grid optical networks," *J. Lightwave Technol.*, vol. 39, pp. 3011–3024, 5 2021, doi: 10.1109/JLT.2021.3057389.

[16] B.C. Chatterjee, N. Sarma, and E. Oki, "Routing and Spectrum Allocation in Elastic Optical Networks: A Tutorial," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 3, pp. 1776–1800, 2015, doi: 10.1109/COMST.2015.2431731.

[17] ITU-T, "Spectral grids for WDM applications: DWDM frequency grid," no. G.694.1, February 2012.

[18] K. Christodoulopoulos, I. Tomkos, and E.A. Varvarigos, "Elastic bandwidth allocation in flexible ofdm-based optical networks," *J. Lightwave Technol.*, vol. 29, no. 9, pp. 1354–1366, May 2011, doi: 10.1109/JLT.2011.2125777.

[19] V.A. Vale, R.C. Almeida, and K.D. Assis, "Network-state-dependent routing and route-dependent spectrum assignment for PRMLSA problem in all-optical elastic networks," *Opt. Switch. Netw.*, vol. 43, p. 100646, Feb 2022, doi: 10.1016/j.osn.2021.100646.

[20] X. Luo, C. Shi, X. Chen, L. Wang, and T. Yang, "Global optimization of all-optical hybrid-casting in inter-datacenter elastic optical networks," *IEEE Access*, vol. 6, pp. 36 530–36 543, 2018, doi: 10.1109/ACCESS.2018.2852067.

[21] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski, "Sndlib 1.0–survivable network design library," *Networks*, vol. 55, no. 3, p. 276–286, May 2010.

[22] H. Tode and Y. Hirota, "Routing, spectrum, and core and/or mode assignment on space-division multiplexing optical networks [invited]," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 9, no. 1, pp. A99–A113, 2017.

[23] A. Agrawal, V. Bhatia, and S. Prakash, "Spectrum efficient distance-adaptive paths for fixed and fixed-alternate routing in elastic optical networks," *Opt. Fiber Technol.*, vol. 40, pp. 36–45, 2018, doi: 10.1016/j.yofte.2017.11.001.

[24] R. Goścień and K. Walkowiak, "Comparison of different data center location policies in survivable elastic optical networks," in *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*, Oct 2015, pp. 48–55, doi: 10.1109/RNDM.2015.7324308.

[25] M. Klinkowski and K. Walkowiak, "An Efficient Optimization Framework for Solving RSSA Problems in Spectrally and Spatially Flexible Optical Networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 4, pp. 1474–1486, 2019, doi: 10.1109/tnet.2019.2922761.

[26] M. Aibin, K. Walkowiak, and A. Sen, "Software-defined adaptive survivability for elastic optical networks," *Opt. Switch. Netw.*, vol. 23, pp. 85–96, 2017, doi: 10.1016/j.osn.2016.06.008.

[27] F. Shirin Abkenar and A. Ghaffarpour Rahbar, "Study and Analysis of Routing and Spectrum Allocation (RSA) and Routing, Modulation and Spectrum Allocation (RMSA) Algorithms in Elastic Optical Networks (EONs)," *Opt. Switch. Netw.*, vol. 23, pp. 5–39, 2017, doi: 10.1016/j.osn.2016.08.003.