On Cost-Efficient Integrated Multilayer Protection Planning in IP-over-EONs

Wei Lu, Xiaofu Yin, Xiaobao Cheng, Zuqing Zhu, *Senior Member, IEEE*

***Abstract*—In this work, we investigate the problem of integrated multilayer protection planning in IP over elastic optical networks (IP-over-EONs). We consider a single-failure scenario where either a router outage or a fiber cut would occur in any time period. To protect against a router outage, we formulate the backup router planning problem as a mixed linear programming (MILP) model in which the optical-layer spare capacity can be reused by the IP-layer spare capacity and the total cost consisting of the extra spare capacity and the IP-layer backup lightpaths is to be minimized. According to the time complexity of the weighted set-covering problem, we prove the $\mathcal{NP}$-hardness of the backup router planning problem and therefore propose a heuristic algorithm. To protect against fiber cuts, we employ shared "1 + 1" path protection and propose a lightpath establishment algorithm that can not only clarify the types of the spare capacity but also perform spectrum sharing among them adaptively. Extensive numerical simulations show that our proposed backup router algorithm can achieve 96.88% similar results to the MILP model, and requires about 43.78% less IP-layer lightpaths than the benchmark algorithm based on dedicated backup routers. Meanwhile, our proposed lightpath establishment algorithm can reduce the planned spectrum resources by 35.67%.**

***Index Terms*—IP-over-EONs, Integrated multilayer protection, Router backup, Spare capacity sharing.**

I. Introduction

To meet the unprecedented growth in IP traffic, it is of great importance and necessary to have advanced optical transport networks as the underlying network infrastructure. However, the development of traditional wavelength-division-multiplexing (WDM) optical networks are rapidly running into their bottlenecks of realizing beyond-100-Gb/s channel capacity and improving spectrum efficiency, due to their fixed-grid spectrum management in the optical layer. To address these bottlenecks, elastic optical networks (EONs) have been proposed. Enabled by the advanced technologies in bandwidth-variable transponders (BV-Ts) and bandwidth-variable optical switches (BV-OXCs) [1], EONs have finer bandwidth allocation granularity and can customize any-size of transmission channels as required [2, 3], thus enhancing network capacity and flexibility largely. For this reason, the architecture of IP-over-EONs is envisioned as a promising prototype for building the next-generation backbone networks, and hence it becomes relevant to study the concerned issues in such networks.

Network survivability is one of the most concerned issues in IP-over-EONs. This is because backbone networks are subject to a variety of unplanned failures, *e.g.*, router outages and fiber cuts, as well as planned interruptions during maintenance. It has been reported by network operators that, in contrast to OXC failures, router outages occur more frequently, *i.e.*, IP routers tend to be more unreliable than OXCs. Specifically, router outages can contribute up to 40% of the unplanned failures in today's IP-over-WDM networks, while the remaining unplanned failures are dominated by fiber cuts [4]. Note that, a router outage would cause thousands or even millions of packets to be dropped even though the underlying lightpaths are intact, while a single fiber cut would result in even more data loss since all the clients' packets are aggregated and transmitted in the optical layer. This makes both of these two types of failures non-negligible, and thus we have to address them properly in future IP-over-EONs.

To protect against these failures in IP and optical layers effectively, the first question to ask is "what is the best restoration strategy for each failure case?". To answer it, we should notice the following facts. First, when a fiber cut happens, the restoration can be performed in either IP or optical layer. However, the associated cost and efficiency are essentially different. Specifically, IP layer restoration needs to find new routes and update the forwarding tables on routers to restore the affected traffic flows. Given the large number of affected flows and expensive router ports, IP layer restoration is neither efficient nor inexpensive. By contrast, optical layer restoration can directly switch all the affected flows to a backup lightpath [5, 6] and optical switching is more cost-efficient due to the inexpensive OXC ports [7]. Hence, it is preferable to use optical layer restoration to address a fiber cut [8, 9]. On the other hand, when a router outage occurs, IP layer restoration becomes the only solution to restore the affected traffic. Again, due to the large number of affected flows, they should not be handled individually. Instead, it would be more effective to restore them as a whole and in a local manner. Specifically, each router is assigned with a backup router [10, 11] and when it breaks down, the affected flows are redirected to the backup router, where they will be forwarded toward their destinations. Hence, for IP layer restoration, only the forwarding tables on the backup router and the routers adjacent to the failed router need to be updated.

Keeping the best restoration strategies in mind, we need to ask the next question "how to plan the spare capacity for protecting against those failures in the most efficient way?". Intuitively, the integrated multilayer protection scheme that leverages the spare capacity in both IP and optical layers to address a failure would be much more cost-efficient than the separated one that only handles the failure with the spare capacity in its own layer [12]. Since it is very rare that

W. Lu, X. Yin, X. Cheng and Z. Zhu are with the School of Information Science and Technology, University of Science and Technology of China, Hefei, Anhui 230027, P. R. China (email: zqzhu@ieee.org).

Manuscript received on Feb. 4, 2018.

multiple failures happen simultaneously, we can assume that only one failure (either a router outage or a fiber cut) would occur at a time instant, *i.e.*, only considering the single-failure scenario. By sharing spare capacity between layers, not only the spectrum efficiency can be enhanced, but also the number of BV-Ts on routers for setting up optical-/IP-layer backup paths can be reduced, both of which are relevant to obtain a cost-efficient multilayer protection planning solution. Note that, even though the idea itself is straightforward and it has already been studied for IP-over-WDM networks [12], how to design the integrated multilayer scheme to plan the spare capacity in IP-over-EONs cost-efficiently is still challenging. This is because differently from WDM networks, EONs need to satisfy certain unique constraints when setting up lightpaths [13–16] and the lightpaths in them can have heterogeneous modulation-levels and bandwidth occupations [17–19].

In this work, we investigate integrated multilayer protection planning in an IP-over-EON and try to minimize both the spectrum resources and the number of working/backup lightpaths in the optical layer. First, to protect against a router outage, we formulate an MILP model to solve the backup router planning problem, prove its $\mathcal{NP}$-hardness, and propose a time-efficient heuristic. Then, with an updated traffic matrix, we design a shared "1 + 1" path protection scheme to address single fiber cuts in the optical layer, which can maximize the spectrum resource sharing to protect against different failures and finally achieving cost-efficient integrated multilayer protection.

The rest of this paper is organized as follows. Section II gives a brief survey on the related work. Section III explains the problem of multilayer protection in IP-over-EONs. Then, the idea of using backup routers to protect against router outages in the IP layer is discussed in Section IV, and how to reuse the spare capacity in the optical layer to address the failures in both IP and optical layers is explained in Section V. We use extensive simulations to evaluate our proposals in Section VI. Finally, Section VII summaries the paper.

II. Related Work

Previously, in [12], the authors give an overview of the multilayer protection and recovery strategies in IP over optical transport networks (IP-over-OTNs). Chigan *et al.* [20] propose a joint multilayer protection scheme for IP-over-WDM networks. However, the schemes discussed in [12, 20] still have a few drawbacks. First of all, it would be relatively inefficient and complicated to restore the affected traffic flows, especially when they are in large numbers. Secondly, if we consider not only the router ports used for multilayer protection but also those for traffic de-/re-aggregation, the schemes' advantage would turn into undetermined since the affected flows that are aggregated for saving router ports might need to be de-aggregated and re-aggregated along their routing paths, which would increase the usage of router ports. More importantly, these schemes cannot be applied to IP-over-EONs directly. For example, setting up a direct lightpath right under the failed router would make the newly-established lightpath much longer than the two original ones that use the failed router as an intermediate optical-electrical-optical hop. Hence, its quality-of-transmission (QoT) would be worse, which might result in using a lower modulation-level and thus requiring more optical spectra to support the same capacity.

To overcome a router outage in an IP-over-OTN, the study in [10] proposes a backup router planning scheme. Nevertheless, it does not consider the failures in the optical layer. Considering the single failures due to router outages, fiber cuts, or optical-to-electrical (OE) port failures, Ruiz *et al.* [11] formulate two ILP models to design the separated and integrated multilayer protection schemes for IP-over-WDM networks, respectively. On one hand, the proposed ILP models would become intractable in large-scale networks. On the other hand, the recovery strategies do not differentiate the failures in IP and optical layers, which would complicate the related network control and management (NC&M) operations.

The study in [21] addresses the problem of multilayer planning in IP-over-EONs. However, it only focuses on how to use the fixed/flexible transponders adaptively but does not consider multilayer protection planning. Castro *et al.* [22] study the dynamic restoration in IP-over-EONs and they propose to re-aggregate the affected traffic flows on intact lightpaths to maximize the traffic recovery. To protect the high-priority requests against single fiber cuts, the authors of [23] propose to squeeze the capacity that is originally assigned to the best-effort requests, and compare three network scenarios that use fixed-rate transponders, mixed-line-rate transponders and BV-Ts, respectively. Their results suggest that IP-over-EON is the most cost-efficient network scenario to realize the differentiated traffic restoration. However, the investigations in [22, 23] only consider fiber cuts but do not address the router outages in the IP layer. Concerning the fact that both router outages and fiber cuts contribute to significant parts of the unplanned failures in today's IP-over-optical networks [4], it would be relevant to design the integrated multilayer protection planning scheme to address the failures in both IP and optical layers of an IP-over-EON.

III. Integrated Multilayer Protection Planning in IP-over-EONs

A. Network Architecture and Network Model

As shown in Fig. 1, the architecture of an IP-over-EON consists of an IP layer and an EON layer, which are interconnected by short-reach fibers. For all the incoming packets, an IP router can be either an intermediate hop or the destination node. When an IP router works as an intermediate hop, it transforms passing-by electrical packets into optical signals via the plugged BV-Ts, and sends them to the locally-connected BV-OXC for long-haul transmission in the EON. When it is the destination, the IP router converts the optical signals received from the locally-connected BV-OXC into electrical packets via the plugged BV-Ts, and drops them for further processing.

We model an IP-over-EON as $G(V_i, V_o, E_o)$, where V_i is the router set in the IP layer, and V_o and E_o are the BV-OXC and fiber link sets, respectively, in the EON layer. On each fiber link $e \in E_o$, there are B frequency slots (FS'), each of which takes adaptively modulated optical signal based on QoT and provides a capacity of C_{slot} when the modulation-level M is 1, *i.e.*, BPSK. An IP-over-EON planning request is described

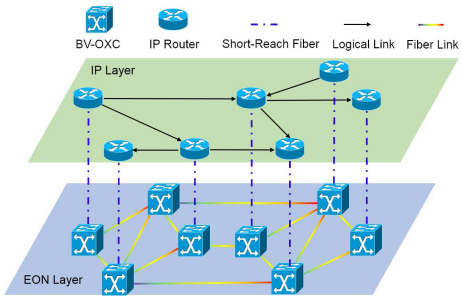


Fig. 1. Architecture of an IP-over-EON.

with a traffic matrix $[C]_{|V_i|\cdot|V_i|}$, in which each element $c_{m,m'}$ represents the working capacity (in Gbps) from router v_i^m to router $v_i^{m'}$, and a non-zero value means that a logical link is required in between the two routers, *e.g.*, a direct solid line in the IP layer of Fig. 1. The network planning needs to not only deploy the logical links in the IP layer by setting up lightpaths in the EON layer, but also plan spare capacity for protecting against single failures due to either router outages or fiber cuts.

B. Integrated Multilayer Protection Planning

We employ the router backup strategy to protect against router outages, since it is relatively simple, fast and port-saving. Note that, even with a backup router, it is still only possible to recover the passing-by traffic, leaving the packets designated to the failed router lost inevitably. To evaluate the complexity of backup router planning, we divide the routers in V_i into: 1) edge routers (ERs) $V_{i,e}$ that have incoming and/or outgoing traffic but do not forward any passing-by traffic, and 2) intermediate routers (IRs) $V_{i,i}$ that however have passing-by traffic to forward. Hence, in IP layer planning, we only need to protect IRs. Note that, in practice, an update on the network design may lead to the transition between IRs and ERs, and ERs can also be connected further on to lower-level networks. Meanwhile, we use the shared "1 + 1" path protection strategy against single fiber cuts in the EON layer.

The objective of integrated multilayer protection planning is to minimize both the spectrum resources and the number of working/backup lightpaths that are needed in the EON layer. Hence, with the single-failure assumption, we try to share the spare capacity in the two layers for failure recovery as much as possible. In backup router planning, we reuse the spare capacity of the backup lightpaths and try to minimize the extra spare capacity and the number of IP-layer backup lightpaths simultaneously. As a result, the spare capacity (in Gbps) can be classified into: 1) the optical-layer spare capacity against single fiber cuts, 2) the IP-layer spare capacity against single router outages, and 3) the multilayer spare capacity against both single fiber cuts and single router outages. In the EON layer, with the objective of minimizing the number of assigned FS', we share the backup FS' assigned for failure recovery in the two layers while satisfying the constraint that every backup FS should not be shared by two backup lightpaths that can be simultaneously enabled to address a failure in either layer. In all, Table I lists the notations used in the network model.

TABLE I
NOTATIONS USED IN THE NETWORK MODEL

Notation	Explanation
IP-over-EON Model:	
V_i	the router set in the IP layer
$V_{i,e}$	the set of edge routers in V_i
$V_{i,i}$	the set of intermediate routers in V_i
V_o	the BV-OXC set in the EON layer
E_o	the fiber link set in the EON layer
B	the number of FS' on each fiber link
M	the indicator of a modulation format
C_{slot}	the transmission capacity of an FS when $M = 1$
v_i^m	the m-th router in V_i
$v_{i,i}^n$	the n-th intermediate router in $V_{i,i}$
A Network Planning Request:	
$[C]_{\|V_i\|\cdot\|V_i\|}$	the traffic matrix of the request
$c_{m,m'}$	the working capacity from router v_i^m to router $v_i^{m'}$

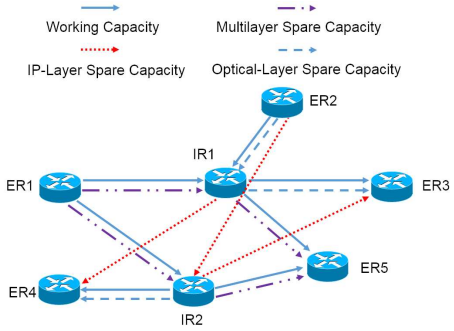


Fig. 2. Example on multilayer spare capacity planning.

IV. Backup Router Planning in IP Layer

Given a network planning request $[C]_{|V_i|\cdot|V_i|}$, we first get an spare capacity matrix $[C]^s_{|V_i|\cdot|V_i|}$ only for path protection in the EON layer as $[C]^s_{|V_i|\cdot|V_i|} = [C]_{|V_i|\cdot|V_i|}$. Then, we plan backup routers in the IP layer, in which in addition to $[C]^s_{|V_i|\cdot|V_i|}$, more spare capacity may still be needed around the selected backup routers to recover the passing-by traffic of the routers that they are protecting, and initialize another spare capacity matrix $[C]^{s'}_{|V_i|\cdot|V_i|}$ as $[C]^{s'}_{|V_i|\cdot|V_i|} = [C]^s_{|V_i|\cdot|V_i|}$. For example, in Fig. 2, there are 5 ERs, *i.e.*, $\{\text{ER1}, \text{ER2}, \cdots, \text{ER5}\}$, and 2 IRs, *i.e.*, $\{\text{IR1}, \text{IR2}\}$. In between any two routers, if there is working capacity, a logical link is plotted as a blue solid line, along with which there is a blue dashed line for the optical-layer spare capacity of the same size. Naturally, IR1 and IR2 are the backup routers of each other.

Around IR1, there are incoming traffic from ER1 and ER2 and outgoing traffic to ER3 and ER5. To protect IR1, IR2 should have IP-layer spare capacity in the directions of ER1→IR2, ER2→IR2, IR2→ER3, and IR2→ER5. Around IR2, since the optical-layer spare capacity in the directions of ER1→IR2 and IR2→ER5 can be reused, they become multilayer spare capacity, *i.e.*, plotted as purple dashed lines in Fig. 2. Note that, if the optical-layer spare capacity is not enough to cover the IP-layer spare capacity in a specific direction, we need to expand the spare capacity in $[C]^{s'}_{|V_i|\cdot|V_i|}$ to the maximum IP-layer spare capacity required in the direction and turn the blue dashed line into a purple one. Besides, in

the directions of ER2→IR2 and IR2→ER3, there is no optical-layer spare capacity to be shared and thus dedicated IP-layer spare capacity should be prepared to recover the traffic from ER2 and to ER3, which are plotted as red dashed lines in Fig. 2 and also need to be updated in $[C]^{s'}_{|V_i|\cdot|V_i|}$.

Similarly, to protect IR2, the optical-layer spare capacity in the directions of ER1→IR1 and IR1→ER5 turn into multilayer spare capacity and dedicated IP-layer spare capacity should be planned in the direction of IR1→ER4. Note that, for these optical-layer/multilayer/IP-layer spare capacity, we need to establish optical-layer/multilayer/IP-layer backup lightpaths in the EON layer accordingly. These backup lightpaths also consume BV-Ts on the source/destination routers, and thus contribute to capital expenditure (CAPEX). For a network planning request $[C]_{|V_i|\cdot|V_i|}$, the number of working lightpaths and optical-layer/multilayer backup lightpaths are determinate, while the number of IP-layer backup lightpaths can change with the backup router planning scheme. Therefore, we aim to optimize the backup router planning scheme for minimizing not only the extra spare capacity of $[C]^{s'}_{|V_i|\cdot|V_i|}$ relative to $[C]^{s}_{|V_i|\cdot|V_i|}$ but also the number of IP-layer backup lightpaths. In the following, we formulate the problem as a mixed integer linear programming model (MILP) and analyze its complexity.

A. Mixed Integer Linear Programming Model (MILP)

Parameters:

- $[C]^{s}_{|V_i|\cdot|V_i|}$: Spare capacity matrix only for path protection in the EON layer, namely the optical-layer spare capacity matrix.
- $[C]^{s'}_{|V_i|\cdot|V_i|}$: Spare capacity matrix for not only path protection in the EON layer but also router protection in the IP layer, namely the two-layer spare capacity matrix.
- $c^{w,f}_{n,m}$: Working capacity between the n-th IR $v^n_{i,i}$ in $V_{i,i}$ and m-th router v^m_i in V_i, if v^m_i is a previous hop of $v^n_{i,i}$.
- $c^{w,b}_{n,m}$: Working capacity between the n-th IR $v^n_{i,i}$ in $V_{i,i}$ and m-th router v^m_i in V_i, if v^m_i is a next hop of $v^n_{i,i}$.
- $c^{s,f}_{n,m}$: Optical-layer spare capacity between the n-th IR $v^n_{i,i}$ in $V_{i,i}$ and m-th router v^m_i in V_i, if v^m_i is a previous hop of $v^n_{i,i}$.
- $c^{s,b}_{n,m}$: Optical-layer spare capacity between the n-th IR $v^n_{i,i}$ in $V_{i,i}$ and m-th router v^m_i in V_i, if v^m_i is a next hop of $v^n_{i,i}$.
- $w_{n,m}$: Spare capacity multiplier between the n-th IR $v^n_{i,i}$ in $V_{i,i}$ and m-th router v^m_i in V_i. The value of $w_{n,m}$ depends on the modulation-levels and optical hop-counts of the backup lightpaths between v^m_i and $v^n_{i,i}$.
- $\{\alpha, \beta\}$: Two constants to balance the optimization in the objective.
- Q: A large positive integer used in the model.

Variables:

- $x_{n,n'}$: Boolean variable that equals 1 if the n'-th IR $v^{n'}_{i,i}$ in $V_{i,i}$ is selected as the backup router of the n-th IR $v^n_{i,i}$ in $V_{i,i}$, and 0 otherwise.
- $a^{s,f}_{n',n,m}$: Real variable that represents the extra spare capacity between the m-th router v^m_i in V_i and n'-th IR $v^{n'}_{i,i}$ in $V_{i,i}$, if $v^{n'}_{i,i}$ is selected as the backup router of the n-th IR $v^n_{i,i}$ in $V_{i,i}$ and v^m_i is a previous hop of $v^n_{i,i}$.
- $a^{s,b}_{n',n,m}$: Real variable that represents the extra spare capacity between the m-th router v^m_i in V_i and n'-th IR $v^{n'}_{i,i}$ in $V_{i,i}$, if $v^{n'}_{i,i}$ is selected as the backup router of the n-th IR $v^n_{i,i}$ in $V_{i,i}$ and v^m_i is a next hop of $v^n_{i,i}$.
- $a^{s,f}_{n',m}$: Real variable that represents the maximum amount of extra spare capacity between the m-th router v^m_i in V_i and n'-th IR $v^{n'}_{i,i}$ in $V_{i,i}$, if $v^{n'}_{i,i}$ is selected as a backup router and v^m_i is a previous hop of any router.
- $a^{s,b}_{n',m}$: Real variable that represents the maximum amount of extra spare capacity between the m-th router v^m_i in V_i and the n'-th IR $v^{n'}_{i,i}$ in $V_{i,i}$, if $v^{n'}_{i,i}$ is selected as a backup router and v^m_i is a next hop of any router.
- a^s_n: Real variable that represents the total amount of extra spare capacity around the n-th IR $v^n_{i,i}$ in $V_{i,i}$, if it is selected as the backup router of other IRs.
- $l^{i,f}_{n',m}$: Boolean variable that equals 1 if an IP-layer backup lightpath needs to be established between the m-th router v^m_i in V_i and n'-th IR $v^{n'}_{i,i}$ in $V_{i,i}$, if $v^{n'}_{i,i}$ is selected as a backup router and v^m_i is a previous hop of any router, and 0 otherwise.
- $l^{i,b}_{n',m}$: Boolean variable that equals 1 if an IP-layer backup lightpath needs to be established between the m-th router v^m_i in V_i and n'-th IR $v^{n'}_{i,i}$ in $V_{i,i}$, if $v^{n'}_{i,i}$ is selected as a backup router and v^m_i is a next hop of any router, and 0 otherwise.
- l^i_n: Integer variable that equals the number of IP-layer backup lightpaths around the n-th IR $v^n_{i,i}$ in $V_{i,i}$, if it is selected as the backup router of other IRs.

Objectives:

$$Minimize \quad \sum_{v^n_{i,i}\in V_{i,i}} \alpha \cdot a^s_n + \beta \cdot l^i_n, \tag{1}$$

which minimizes the extra spare capacity and the number of IP-layer backup lightpaths simultaneously.

Constraints:

$$\sum_{v^{n'}_{i,i}\in V_{i,i}: n'\neq n} x_{n,n'} \geq 1, \quad \forall v^n_{i,i} \in V_{i,i}. \tag{2}$$

Eq. (2) ensures that every IR is protected by at least one IR.

$$a^{s,f}_{n',n,m} \geq \frac{x_{n,n'} \cdot (c^{w,f}_{n,m} - c^{s,f}_{n',m})}{w_{n',m}}, \ \forall v^n_{i,i},\ v^{n'}_{i,i},\ v^m_i,\ n \neq n', \tag{3}$$

$$a^{s,b}_{n',n,m} \geq \frac{x_{n,n'} \cdot (c^{w,b}_{n,m} - c^{s,b}_{n',m})}{w_{n',m}}, \ \forall v^n_{i,i},\ v^{n'}_{i,i},\ v^m_i,\ n \neq n'. \tag{4}$$

Eqs. (3)-(4) determine the lower bounds of $a^{s,f}_{n',n,m}$ and $a^{s,b}_{n',n,m}$, respectively.

$$a^{s,f}_{n',m} \geq a^{s,f}_{n',n,m}, \quad \forall v^n_{i,i},\ v^{n'}_{i,i},\ v^m_i,\ v^n_{i,i} \neq v^m_i. \tag{5}$$

$$a^{s,b}_{n',m} \geq a^{s,b}_{n',n,m}, \quad \forall v^n_{i,i},\ v^{n'}_{i,i},\ v^m_i,\ v^n_{i,i} \neq v^m_i. \tag{6}$$

Eqs. (5)-(6) determine the lower bounds of $a^{s,f}_{n',m}$ and $a^{s,b}_{n',m}$, respectively.

$$a^s_n \geq \sum_{v^m_i\in V_i: v^m_i \neq v^n_{i,i}} a^{s,b}_{n,m} + a^{s,f}_{n,m}, \quad \forall v^n_{i,i}. \tag{7}$$

Eq. (7) determines the lower bounds of a^s_n.

$$l^{i,f}_{n',m} \cdot Q \geq a^{s,f}_{n',m} \cdot (1 - c^{s,f}_{n',m}), \quad \forall v^{n'}_{i,i},\ v^m_i,\ v^{n'}_{i,i} \neq v^m_i. \quad (8)$$

$$l^{i,b}_{n',m} \cdot Q \geq a^{s,b}_{n',m} \cdot (1 - c^{s,b}_{n',m}), \quad \forall v^{n'}_{i,i},\ v^m_i,\ v^{n'}_{i,i} \neq v^m_i. \quad (9)$$

Eqs. (8)-(9) determine the values of $l^{i,f}_{n',m}$ and $l^{i,b}_{n',m}$, respectively, where Q makes sure the trueness of Eqs. (8)-(9) in the cases of $l^{i,f}_{n',m} = 1$ and $l^{i,b}_{n',m} = 1$.

$$l^i_n \geq \sum_{v^m_i \in V_i : v^m_i \neq v^n_{i,i}} l^{i,b}_{n,m} + l^{i,f}_{n,m}, \quad \forall v^n_{i,i}. \quad (10)$$

Eq. (10) determines the lower bounds of l^i_n.

Complexity Analysis: As in the single-failure network scenario a router can protect multiple routers simultaneously, we define a router protection group as a set of routers that share the same backup router, and the cost of it is the extra spare capacity and the number of IP-layer backup lightpaths for the IP-layer protection. Given the IR set $V_{i,i}$, we can include all the possible router protection groups in set $\{PG_j : PG_j \subset V_{i,i}, j \in [1, 2^{|V_{i,i}|} - 1]\}$ and get the corresponding cost set by finding an optimal backup router for each group. Then, the backup router planning problem becomes to find a subset J^* of the minimum cost, which satisfies $\cup(PG_j : j \in J^*) = V_{i,i}$. This, however, is equivalent to the weighted set-covering problem, which is known to be $\mathcal{NP}$-hard [24]. Therefore, the backup router planning problem is $\mathcal{NP}$-hard too. Even though a few greedy heuristics with proved upper-bound have been proposed for the weighted set-covering problem [24, 25], it is still impractical to solve the backup router planning problem with them, especially when the value of $|V_{i,i}|$ is large. This is because the size of set $\{PG_j\}$ increases with $|V_{i,i}|$ exponentially, *i.e.*, $2^{|V_{i,i}|} - 1$, which prevents those heuristics to be polynomial algorithms.

B. Backup Router Planning Algorithm

For better readability, the new notations that are introduced in this subsection are listed as follows:

- PG_{j*}: A protection group that consists of a set of IRs sharing the same backup router, where j^* is its index.
- $v^{n'}_{i,i}$: Optimal backup router that is assumed for a protection group temporarily.
- $V_i(v^n_{i,i}, S)$: Set of previous-/next-hop routers of IR $v^n_{i,i}$ that have an outgoing/incoming degree of one[1], *e.g.*, $\{\text{ER2}, \text{ER3}\}$ of IR1 in Fig. 2.
- $V_i(v^n_{i,i}, M)$: Set of previous-/next-hop routers that have multiple logical links to/from IRs including $v^n_{i,i}$, *e.g.*, $\{\text{ER1}, \text{ER5}\}$ of IR1 in Fig. 2.
- $PG^{max}_{v^n_{i,i}}$: Maximum-sharing protection group of IR $v^n_{i,i}$, satisfying $V_i(v^n_{i,i}, M) \cap V_i(v^{n^*}_{i,i}, M) \neq \emptyset$ for all $v^{n^*}_{i,i} \in PG^{max}_{v^n_{i,i}}$ and $PG^{max}_{v^n_{i,i}}$ has the maximum size out of $V_{i,i}$.
- PG^s_j: A protection group that belongs to the minimum independent protection group set.
- J_s: Number of independent protection groups.

[1]Here, the incoming/outgoing degree only counts the logical links that use an IR as the source/destination.

- $v^{n'(j)}_{i,i}$: Optimal backup router that is assumed for PG^s_j.
- $c_{n'(j)}$: Minimum cost to protect the IRs in PG^s_j.

For a protection group PG_{j^*}, we assume that its optimal backup router is $v^{n'}_{i,i} \in V_{i,i}$. Then, the contribution of each protected router $v^n_{i,i} \in PG_{j^*}$ to the value of $\alpha \cdot a^s_{n'} + \beta \cdot l^i_{n'}$ in Eq. (1) can be calculated as:

$$\begin{aligned}
&\alpha \cdot a^s_{n',n} + \beta \cdot l^s_{n',n} \\
&= \sum_{v^m_i \in V_i(v^n_{i,i}, S)} \left(\alpha \cdot \frac{c^{w,f}_{n,m} + c^{w,b}_{n,m}}{w_{n',m}} + \beta \right) + \\
&\sum_{v^m_i \in V_i(v^n_{i,i}, M)} \left(\alpha \cdot \frac{\max\{c^{w,f}_{n^*,m} - c^{s,f}_{n',m}, c^{w,b}_{n^*,m} - c^{s,b}_{n',m}, 0 : v^{n^*}_{i,i} \in PG_{j^*}\}}{w_{n',m} \cdot |PG_{j^*}|} \right. \\
&\left. + \beta \cdot \frac{l^{i,f}_{n',m} + l^{i,b}_{n',m}}{|PG_{j^*}|} \right),
\end{aligned} \quad (11)$$

Due to the single degree, there is certainly no optical-layer spare capacity between backup router $v^{n'}_{i,i}$ and router $v^m_i \in V_i(v^n_{i,i}, S)$, and thus the first term calculates the dedicated IP-layer spare capacity and the number of IP-layer backup lightpaths for $v^n_{i,i}$. Note that, we divide the components of the first term with the spare capacity multiplexer $w_{n',m}$ for the link between $v^{n'}_{i,i}$ and v^m_i, making it preferable to select backup routers with higher spare capacity multiplexers. Meanwhile, the second term calculates the extra spare capacity and the number of IP-layer lightpaths that are required between backup router $v^{n'}_{i,i}$ and router $v^m_i \in V_i(v^n_{i,i}, M)$, for protecting protection group PG_{j^*}. Note that, we average the components of the second term with not only the spare capacity multiplexer $w_{n',m}$ but also the size of PG_{j^*}. By doing so, the extra spare capacity and the number of IP-layer lightpaths between backup router $v^{n'}_{i,i}$ and router $v^m_i \in V_i(v^n_{i,i}, M)$ would be evenly distributed to all the protected routers in PG_{j^*}, and hence the more the spare capacity is shared in PG_{j^*} the less each group member will contribute to the second term.

The difficulty of finding the optimal protection groups lies in the facts that: 1) for a certain protection group PG_{j^*}, the optimal backup router $v^{n'}_{i,i}$ is determined by all the group members collectively; 2) however, the optimal backup router $v^{n'}_{i,i}$ might not be the optimal one for certain group members. Hence, those group members might leave PG_{j^*} for minimizing their extra spare capacity and IP-layer backup lightpaths, which in turn affects the selection of the optimal backup router of PG_{j^*}; 3) due to this dynamics in protection groups, it could be difficult to find the optimal protection group set.

Therefore, utilizing the principle of dynamic equilibrium, we propose a backup router planning algorithm that can not only maximize spare capacity sharing in the constructed protection groups, but also decide whether a group member leaves or stays in a protection group for further reducing the extra spare capacity and the number of IP-layer backup lightpaths, until no group member is willing to move. We first find a maximum-sharing protection group for each IR $v^n_{i,i} \in V_{i,i}$, denoted as $PG^{max}_{v^n_{i,i}}$. Then, we merge the maximum-sharing protection groups $\{PG^{max}_{v^n_{i,i}} : v^n_{i,i} \in V_{i,i}\}$ into minimum independent protection groups $\{PG^s_j : j \in [1, J_s]\}$.

Algorithm 1 elaborates the detailed procedure of constructing the minimum independent protection groups. *Line* 1 is

for the initialization. *Lines* 3-9 try to merge the maximum-sharing protection group of an unsettled IR into a constructed independent protection group. The merging condition is in *Line* 5, *i.e.*, the maximum-sharing protection group must intersect with the independent protection group. If there is such an independent protection group, we set the *indicator* as 1 in *Line* 6 to indicate that the IR is settled, and *Line* 7 performs the group merging. Otherwise, a new independent protection group is created and initialized as the maximum-sharing protection group of the IR in *Lines* 10-12.

Fig. 3 illustrates an example on constructing the minimum independent protection groups. In Fig. 3(a), we assume that both IR1 and IR3 have incoming traffic from ER1, both IR1 and IR2 have outgoing traffic to ER2 and ER5, both IR1 and IR3 have incoming traffic from ER3, and both IR4 and IR5 have incoming traffic from ER6 and outgoing traffic to ER7. Therefore, the maximum-sharing protection group of IR1 is $\{\text{IR1}, \text{IR2}, \text{IR3}\}$ to share the incoming spare capacity from ER1 and the outgoing spare capacity to ER2 and ER5 with IR2 and IR3. Similarly, we can determine that IR2 and IR3 have the same maximum-sharing protection group of IR1, and IR4 and IR5 have the same maximum-sharing protection group as $\{\text{IR4}, \text{IR5}\}$. In Fig. 3(b), we merge the maximum-sharing protection groups and obtain two independent protection groups, which are $\{\text{IR1}, \text{IR2}, \text{IR3}\}$ and $\{\text{IR4}, \text{IR5}\}$, respectively.

Algorithm 1: Construction of Minimum Independent Protection Groups

Input: $\{PG^{max}_{v^n_{i,i}} : v^n_{i,i} \in V_{i,i}\}$
Output: $\{PG^s_j : j \in [1, J_s]\}$
1 $J_s = 0$, $PG^s_0 = \emptyset$;
2 **for** *each* $v^n_{i,i} \in V_{i,i} / \bigcup_{j=0}^{J_s} PG^s_j$ **do**
3 Indicator = 0;
4 **for** *each* $PG^s_j, j \in [0, J_s]$ **do**
5 **if** $PG^{max}_{v^n_{i,i}} \cap PG^s_j \neq \emptyset$ **then**
6 Indicator = 1;
7 $PG^s_j = PG^s_j \cup PG^{max}_{v^n_{i,i}}$;
8 **end**
9 **end**
10 **if** *Indicator = 0* **then**
11 $J_s = J_s + 1$, $PG^s_{J_s} = PG^{max}_{v^n_{i,i}}$;
12 **end**
13 **end**

Then, for each $PG^s_j, j \in [1, J_s]$, we find the optimal backup router $v^{n'(j)}_{i,i}$ that has the minimum cost $c_{n'(j)} = \alpha \cdot a^s_{n'(j)} + \beta \cdot l^i_{n'(j)}$ to protect the IRs in PG^s_j. *Algorithm* 2 gives the detailed procedure. *Line* 1 is for the initialization. If the size of PG^s_j is smaller than that of $V_{i,i}$ (*Line* 2), there are IRs in $V_{i,i}/PG^s_j$ as the backup router candidates for PG^s_j. Then, for every $v^{n'}_{i,i} \in V_{i,i}/PG^s_j$, we calculate $\alpha \cdot a^s_{n'} + \beta \cdot l^i_{n'}$ with Eq. (11) (*Lines* 3-8), and update $\{v^{n'(j)}_{i,i}, c_{n'(j)}\}$ in the case of $\alpha \cdot a^s_{n'} + \beta \cdot l^i_{n'} < c_{n'(j)}$ (*Lines* 9-11). Otherwise, the optimal backup router $v^{n'(j)}_{i,i}$ cannot be found and the protection group cost $c_{n'(j)}$ is set as ∞.

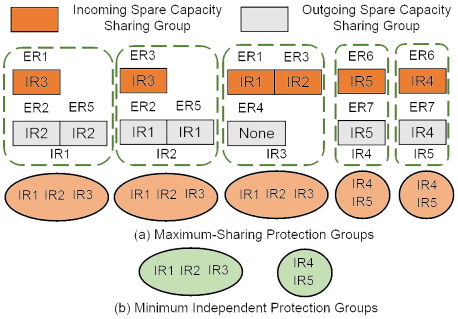


Fig. 3. Example on constructing minimum independent protection groups.

Algorithm 2: Finding the Optimal Backup Router of a Protection Group

Input: $\{PG^s_j : j \in [1, J_s]\}$
Output: $v^{n'(j)}_{i,i}$, $c_{n'(j)}$
1 $v^{n'(j)}_{i,i} = \emptyset$, $c_{n'(j)} = \infty$;
2 **if** $|PG^s_j| < |V_{i,i}|$ **then**
3 **for** *each* $v^{n'}_{i,i} \in V_{i,i}/PG^s_j$ **do**
4 $c_{n'} = 0$;
5 **for** *each* $v^n_{i,i} \in PG^s_j$ **do**
6 calculate $\alpha \cdot a^s_{n',n} + \beta \cdot l^i_{n',n}$ with Eq. (11);
7 $c_{n'} = c_{n'} + (\alpha \cdot a^s_{n',n} + \beta \cdot l^i_{n',n})$;
8 **end**
9 **if** $c_{n'} < c_{n'(j)}$ **then**
10 $v^{n'(j)}_{i,i} = v^{n'}_{i,i}$, $c_{n'(j)} = c_{n'}$;
11 **end**
12 **end**
13 **end**

Finally, based on the principle of dynamic equilibrium, we move the group members in $\{PG^s_j : j \in [1, J_s]\}$ around to further reduce the total cost, especially for those with $c_{n'(j)}$ as ∞. *Algorithm* 3 shows the procedure, and we define several temporary variables as:

- $PG^{s,*}_j$: A variable that has the same meaning with PG^s_j.
- $v^{n'(j),*}_{i,i}$: A variable that has the same meaning with $v^{n'(j)}_{i,i}$.
- $c^*_{n'(j)}$: A variable that has the same meaning with $c_{n'(j)}$.
- Δ_j: Number of additional protection groups from PG^s_j.
- $PG^s_{j,n}$: PG^s_j after removing IR $v^n_{i,i}$.
- $PG^s_{J_s+\Delta_j,n}$: The Δ_j-th additional protection group from PG^s_j that has $v^n_{i,i}$ as the only group member.
- $v^{n'(J_s+\Delta_j,n)}_{i,i}$: The optimal backup router of the additional protection group $PG^s_{J_s+\Delta_j,n}$.
- $c_{n'(J_s+\Delta_j,n)}$: The cost of $v^{n'(J_s+\Delta_j,n)}_{i,i}$ for protecting $PG^s_{J_s+\Delta_j,n}$.

Lines 1, 3, and 5 are for initialization. The for-loop covering *Lines* 2-25 tries to move group members from each protection group for reducing the total cost. Specifically, in each iteration (*Lines* 4-19), we move the IR $v^n_{i,i}$ in PG^s_j, which can reduce the total cost furthest. If the size of PG^s_j

becomes 1 or there is no such a router that can minimize the total cost (*i.e.*, $PG^s_{J_s+\Delta_j} = \emptyset$), we stop the iterations for PG^s_j (*Line* 4). To find the IR that reduces the total cost furthest, we move each IR $v^n_{i,i}$ in PG^s_j alternatively, and get two protection groups as $PG^s_{j,n}$ and $PG^s_{J_s+\Delta_j,n}$, respectively (*Lines* 7-8). Then, we calculate the optimal backup routers and the associated cost of the two protection groups using *Algorithm* 2 (*Lines* 9-10). If the total cost of the two protection groups is smaller than the current cost $c^*_{n'(j)}$ (*Line* 11), we update $\{PG^{s,*}_j, v^{n'(j),*}_{i,i}, c^*_{n'(j)}\}$ and $\{PG^s_{J_s+\Delta_j}, v^{n'(J_s+\Delta_j)}_{i,i}, c_{n'(J_s+\Delta_j)}\}$ (*Lines* 12-15). Finally, $\{PG^s_j, v^{n'(j)}_{i,i}, c_{n'(j)}\}$ are updated as $\{PG^{s,*}_j, v^{n'(j),*}_{i,i}, c^*_{n'(j)}\}$ (*Line* 18), and *Lines* 20-24 update the value of J_s for the additional protection groups from PG^s_j.

Algorithm 3: Dynamic Group Member Removal

Input: $\{PG^s_j, v^{n'(j)}_{i,i}, c_{n'(j)} : j \in [1, J_s]\}$
Output: $\{PG^s_j, v^{n'(j)}_{i,i}, c_{n'(j)} : j \in [1, J_s]\}$
1 $J^0_s = J_s$;
2 **for** *each* $PG^s_j, j \in [1, J^0_s]$) **do**
3 $PG^{s,*}_j = PG^s_j$, $v^{n'(j),*}_{i,i} = v^{n'(j)}_{i,i}$, $c^*_{n'(j)} = c_{n'(j)}$, $\Delta_j = 0$;
4 **while** $|PG^s_j| > 1$ *and* $PG^s_{J_s+\Delta_j} \neq \emptyset$ **do**
5 $\Delta_j = \Delta_j + 1$, $PG^s_{J_s+\Delta_j} = \emptyset$;
6 **for** *each* $v^n_{i,i} \in PG^s_j$ **do**
7 $PG^s_{j,n} = PG^s_j / v^n_{i,i}$;
8 $PG^s_{J_s+\Delta_j,n} = v^n_{i,i}$;
9 find the optimal $\{v^{n'(j,n)}_{i,i}, c_{n'(j,n)}\}$ for $PG^s_{j,n}$ using *Algorithm* 2;
10 find the optimal $\{v^{n'(J_s+\Delta_j,n)}_{i,i}, c_{n'(J_s+\Delta_j,n)}\}$ for $PG^s_{J_s+\Delta_j,n}$ using *Algorithm* 2;
11 **if** $c_{n'(j,n)} + c_{n'(J_s+\Delta_j,n)} < c^*_{n'(j)}$ **then**
12 $PG^{s,*}_j = PG^s_j / v^n_{i,i}$, $PG^s_{J_s+\Delta_j} = v^n_{i,i}$;
13 $v^{n'(j),*}_{i,i} = v^{n'(j,n)}_{i,i}$, $c^*_{n'(j)} = c_{n'(j,n)}$;
14 $v^{n'(J_s+\Delta_j)}_{i,i} = v^{n'(J_s+\Delta_j,n)}_{i,i}$;
15 $c_{n'(J_s+\Delta_j)} = c_{n'(J_s+\Delta_j,n)}$;
16 **end**
17 **end**
18 $PG^s_j = PG^{s,*}_j$, $v^{n'(j)}_{i,i} = v^{n'(j),*}_{i,i}$, $c_{n'(j)} = c^*_{n'(j)}$;
19 **end**
20 **if** $PG^s_{J_s+\Delta_j} \neq \emptyset$ **then**
21 $J_s = J_s + \Delta_j$;
22 **else**
23 $J_s = J_s + \Delta_j - 1$;
24 **end**
25 **end**

Time Complexity: The time complexity of *Algorithm* 1 is $O(|V_{i,i}|)$, the time complexity of *Algorithm* 2 is $O(|V_{i,i}|)$, and the time complexity of *Algorithm* 3 is $O(|V_{i,i}|^3)$. Therefore, the proposed backup router planning algorithm has a complexity of $O(|V_{i,i}|^3)$, and is a polynomial one.

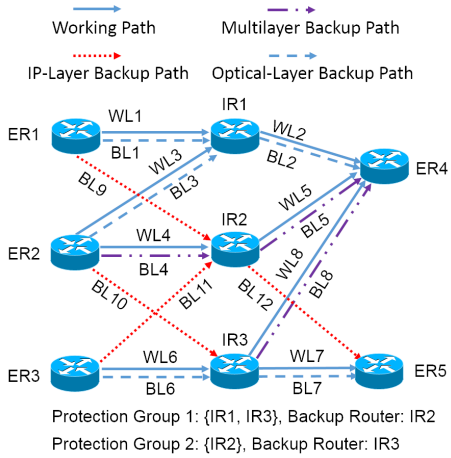


Fig. 4. Example on spectrum sharing among backup lightpaths.

V. Lightpath Establishment in the Optical Layer

A. Spectrum Sharing among Backup Lightpaths

1) Backup Lightpaths for Optical-Layer Protection: Since they are protecting against fiber cuts in the EON layer, they can share FS' with each other if they have link-disjoint working lightpaths. For example, in Fig. 4, the optical-layer backup lightpaths in $\{BL1, BL2, BL3, BL6, BL7\}$ can share FS' with each other on their common links if their working lightpaths in $\{WL1, WL2, WL3, WL6, WL7\}$ are link-disjoint. Similarly, they can share FS' with the multilayer backup lightpaths, *e.g.* $\{BL4, BL5, BL8\}$. They can also share FS' with the IP-layer backup lightpaths (*e.g.*, $\{BL9, BL10, BL11, BL12\}$) unconditionally. This is because they are protecting against failures in different layers, which would not happen simultaneously.

2) Backup Lightpaths for IP-Layer Protection: Since they are protecting against router outage(s) in the IP layer, they can share FS' with each other if they are protecting different routers. For example, in Fig. 4, the IP-layer backup lightpath BL9 can share FS' with the IP-layer backup lightpaths in $\{BL11, BL12\}$, but BL11 and BL12 cannot share FS' with each other. This is because BL9 protects IR1, while BL11 and BL12 work jointly to protect against the outage of IR2. For the same reason, they can share FS' with the multilayer backup lightpaths, *e.g.*, BL9 can share FS' with multilayer backup lightpath BL8, and BL11 and BL12 can share FS' with the multilayer backup lightpaths in $\{BL4, BL5\}$. As explained above, they can share FS' with the optical-layer backup lightpaths (*e.g.*, $\{BL1, BL2, BL3, BL6, BL7\}$) unconditionally. Note that, when an IP-layer backup lightpath only protects one router, it can still share FS' with the working lightpaths around the protected router, *e.g.*, BL9 can share FS' with the working lightpaths $\{WL1, WL2, WL3\}$ around IR1.

3) Backup Lightpaths for Multilayer Protection: Since they are protecting against both fiber cuts and router outages, they can share FS' with each other only if their working lightpaths are link-disjoint and they are protecting different routers. For example, in Fig. 4, the multilayer backup lightpaths BL4 and BL5 cannot share FS' with each other even if their working lightpaths WL4 and WL5 are link-disjoint, since they are

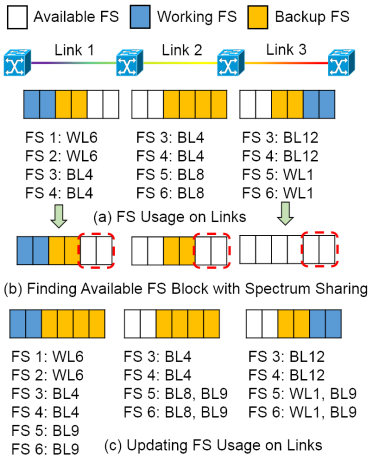


Fig. 5. Example on spectrum assignment with FS sharing.

protecting the same router IR1. However, both of them can share FS' with multilayer backup lightpath BL8 under the condition that working lightpaths WL4 and WL5 are link-disjoint with working lightpath WL8, since BL8 is protecting a different router IR2. For optical-layer backup lightpaths, *e.g.*, $\{\text{BL1}, \text{BL2}, \text{BL3}, \text{BL6}, \text{BL7}\}$, multilayer backup lightpaths can share FS' with them only if they have link-disjoint working lightpaths. Meanwhile, for IP-layer backup lightpaths, multilayer backup lightpaths can share FS' with them only if they are protecting different routers.

B. Lightpath Establishment Algorithm

Based on the analysis above, we establish lightpaths and assign spectrum resources in the EON layer, aiming to minimize the number of assigned FS' by sharing the three types of spare capacity as much as possible. With the network planning request $[C]_{|V_i|\cdot|V_i|}$, the two-layer spare capacity matrix $[C]^{s'}_{|V_i|\cdot|V_i|}$, and the protection groups $\{PG^s_j, v^{n'(j)}_{i,i} : j \in [1, J_s]\}$, we first set up the working lightpaths. Table II lists the notations used in the lightpath establishment. Here, the i-th working lightpath is denoted as $WL_i = \{ws_i, wd_i, wc_i\}$, and when the backup lightpaths have been established, the i-th of them is $BL_i = \{bs_i, bd_i, bc_i\}$. For each BL_i, there is a multilayer protection group pg_i to include all the working lightpaths and routers that it is protecting. Then, we find the proper routing, modulation-level and spectrum assignment (RMSA) schemes for the working and backup lightpaths.

For each working lightpath WL_i, we use the shortest-path routing and first-fit spectrum allocation (SP-FF) algorithm to find its RMSA scheme. On the other hand, for each backup lightpath BL_i, we first use the K-shortest-path routing (KSP) algorithm to find K path candidates. Note that, if there is a working lightpath in its protection group pg_i, the K path candidates should be link-disjoint with the working lightpath. Then, we assign FS' with spectrum sharing. Here, we use the example in Fig. 5 to explain how to find a feasible FS block for maximum spectrum sharing. In Fig. 5, we try to assign FS' for backup lightpath BL9 in Fig. 4 on a path candidate that goes through Link1, Link2, and Link3.

Fig. 5(a) shows the link usage on the three links. Here, the assigned FS' are classified into working and backup FS', and the related working and/or backup lightpaths are collected for each assigned FS, *e.g.*, FS 1 on Link1 is assigned for WL6. If backup lightpath BL9 needs 2 FS', we find that under the spectrum continuity constraint, there will be no available FS block on the selected path candidate without spectrum sharing. However, with spectrum sharing, Fig. 5(b) shows the right FS usages on links for BL9. Specifically, the backup FS' 5 and 6 on Link2 and the working FS' 5 and 6 on Link3 become available for BL9, since the related backup lightpath BL8 and working lightpath WL1 can share FS' with BL9 according to the aforementioned analysis. Therefore, FS' 5 and 6 on the three links can be assigned to BL9 and the FS usages on them are updated in Fig. 5(c), such that BL9 is added to the related lightpath sets of the FS' 5 and 6 on Link1, Link2, and Link3.

TABLE II
NOTATIONS USED IN LIGHTPATH ESTABLISHMENT

Notation	Explanation
The i-th Working Lightpath WL_i:	
ws_i	the source BV-OXC
wd_i	the destination BV-OXC
wc_i	the capacity requirement
wm_i	the selected modulation level
The i-th Backup Lightpath BL_i:	
bs_i	the source BV-OXC
bd_i	the destination BV-OXC
bc_i	the capacity requirement
pg_i	the multilayer protection group
K	the number of path candidates
$bm_{i,k}$	the selected modulation level for the k-th path candidate

Algorithm 4: Lightpath Establishment Algorithm

```
for each WL_i = {ws_i, wd_i, wc_i} do
    find the shortest path between ws_i and wd_i;
    select a proper modulation level wm_i;
    calculate the number of FS' given wm_i and wc_i;
    assign FS' using the first-fit method;
    update the FS usage on the related links;
end
for each BL_i = {bs_i, bd_i, bc_i, pg_i} do
    find K shortest path candidates between bs_i and bd_i;
    for each path candidate do
        select a proper modulation level bm_{i,k};
        calculate the number of FS' given bm_{i,k} and bc_i;
        get the right FS usage on links for BL_i with pg_i;
        find a feasible FS block that shares the most
        assigned FS';
    end
    select the path candidate that has a feasible FS block
    of maximum spectrum sharing;
    assign the feasible FS block of maximum spectrum
    sharing for BL_i;
    update the FS usage on the related links;
end
```

The detailed procedure of the proposed lightpath establish-

ment algorithm is shown in *Algorithm* 4. *Lines* 1-7 find an RMSA scheme for each working lightpath WL_i using the SP-FF algorithm. *Lines* 8-19 find an RMSA scheme for each backup lightpath BL_i. More specifically, *Line* 9 calculates K shortest path candidates for BL_i. Then, for each path candidate, *Lines* 11-14 get the right FS usages on the path using the method explained in Fig. 5, and find a feasible FS block that shares the most assigned FS'. Finally, *Lines* 16-17 select the path candidate that has the FS block of the maximum spectrum sharing, and assign the path and the FS block to BL_i, and *Line* 18 updates the FS usage on the related links.

VI. Performance Evaluation

A. Simulation Parameters

The simulations use the NSFNET and US Backbone topologies [26, 27] in Figs. 6(a) and 6(b), respectively, as the topology of the EON layer. The bandwidth of an FS is set as 12.5 GHz. We assume that the spectrum efficiency of BPSK is 1 bit/s/Hz, and thus the capacity of an FS C_{slot} is 12.5 Gb/s. Fig. 6(c) gives the transmission reaches of BPSK, QPSK, 8-QAM, and 16-QAM signals, according to [28, 29]. Note that, the transmission reach model considered is relatively simple and does not get into propagation details such as fiber non-linearities. However, we also run simulations with different reach values, and the results, which are not reported here for brevity, show a very similar behavior of the proposed algorithms. The simulations test 8 network planning instances as shown in Fig. 6(d). Specifically, we consider four instances for each EON topology. In each instance, we place both the IRs and ERs randomly on the nodes in the EON topology.

When generating the network planning request, we randomly select the adjacent routers for the IRs and ERs, and have the working capacity between them uniformly distributed within $[100, 200]$ Gbps. In this way, we generate 10 working traffic matrixes for each instance and average the results for comparison, which leads to an expected confidence level of 90% [30]. In the backup router planning, the spare capacity multiplexer $w_{n,m}$ is set according to the parameters of the shortest lightpath between IR $v^n_{i,i} \in V_{i,i}$ and router $v^m_i \in V_i$, *i.e.*, as the ratio of its hop-count to its modulation-level. We consider two scenarios, *i.e.*, the major objective of the first one is to minimize the extra spare capacity (with $\alpha = 1$ and $\beta = 1$), while the second one tries to minimize the number of IP-layer backup lightpaths first (with $\alpha = 1$ and $\beta = 5000$). In lightpath establishment, we use the shortest path (*i.e.*, $K = 1$) since our simulations have confirmed that the algorithm's sensitivity to K varying within $[1, 3]$ is very limited. All the simulations use MATLAB R2013a and run on a computer with 2.93 GHz Intel Core i3 CPU and 6 GB RAM.

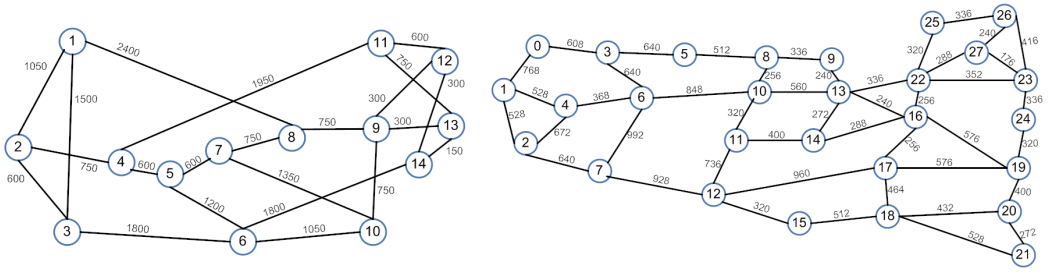
B. Backup Router Planning in IP Layer

Figs. 7(a)-7(c) show the results of backup router planning in the IP layer with $\{\alpha, \beta\} = \{1, 1\}$. Here, we use the dedicated backup router algorithm as the benchmark, which finds a backup router with the minimum cost for each IR individually without considering the protection groups. Fig. 7(a) compares the results on the total amount extra spare capacity, *i.e.*, the value of $\sum a^s_n$ in Eq. (1). We can see that the proposed backup router planning algorithm can achieve very similar results as the MILP model (*i.e.*, with a similarity of 96.88%), and both of them generally require less extra spare capacity than the dedicated backup router algorithm. More promisingly, the advantages of our proposed algorithms over the benchmark become more significant with the increases of the number of IRs and average router degree. These observations verify the effectiveness of the proposed backup router algorithm on reducing the extra spare capacity.

Fig. 7(b) compares the results on the number of IP-layer backup lightpaths, *i.e.*, the value of $\sum l^i_n$ in Eq. (1). It is interesting to notice that in Fig. 7(b), our proposed backup router algorithm requires $\sim 43.78\%$ less IP-layer backup lightpaths than the dedicated backup router algorithm for all the test instances. Fig. 7(c) compares the results on the number of backup routers. As shown in the instances that have a smaller router degree, the dedicated backup router algorithm plans almost twice as many backup routers as those from the proposed backup router algorithm, and hence it would apparently plan much more IP-layer backup lightpaths. It is worth noting that, the proposed MILP model and algorithm achieve similar confidence intervals in Figs. 7(a) and 7(b).

Figs. 8(a)-8(c) show the results of backup router planning in the IP layer with $\{\alpha, \beta\} = \{1, 5000\}$. Here, we can observe similar trends to those in Figs. 7(a)-7(c). However, with the sharp increase of β, all the backup router algorithms set their primary goal as minimizing the number of IP-layer backup lightpaths while making the reduction of extra spare capacity as the secondary goal. Hence, compared with the results in Figs. 7(a) and 7(b), all the backup router algorithms generally require more extra spare capacity in Fig. 8(a) for realizing the reduction of IP-layer backup lightpaths in Fig. 8(b). More specifically, the dedicated backup router algorithm requires $\sim 29.05\%$ more extra spare capacity for a reduction ratio of $\sim 9.92\%$ on the number of IP-layer backup lightpaths, while the proposed backup router algorithm requires $\sim 20.93\%$ more extra spare capacity for a reduction ratio of $\sim 11.47\%$ on the number of IP-layer backup lightpaths. More importantly, for some instances, *e.g.*, the instances $\{1, 6, 8\}$, the dedicated backup router algorithm cannot reduce the IP-layer backup lightpaths even with much more extra spare capacity.

On one hand, these observations verify the effectiveness of the proposed backup router algorithm on reducing the IP-layer backup lightpaths. On the other hand, they also confirm that the proposed backup router algorithm has a relatively good robustness against the changes of optimization parameters. For the confidence intervals, we can see the similar trend in Fig. 8(b) as that in Fig. 7, which verifies the performance robustness of our proposed MILP model and algorithm. Moreover, considering the fact that the numbers of both the working lightpaths and optical-layer/multilayer ones are fixed, we can evaluate the average size of the routers by analyzing the ratio between the number of IP-layer lightpaths and the number of backup routers. Hence, the results in Figs. 7 and 8 also suggest that the proposed MILP model and backup router algorithm can reduce the average size of the routers, when being compared with the dedicated backup router algorithm.



(a) 14-node NSF Network (Link Length in Kilometers)

(b) US Backbone Network (Link Length in Kilometers)

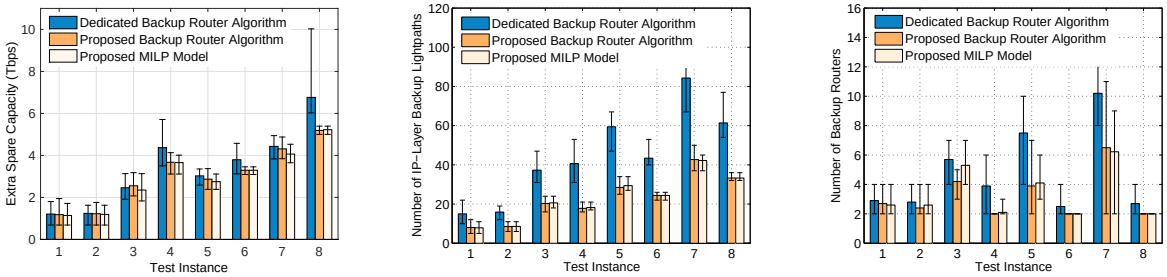
Modulation Level	Transmission Reach (km)
BPSK (M = 1)	4800
QPSK (M = 2)	2400
8-QAM (M = 3)	1200
16-QAM (M = 4)	600

(c) Transmission Reach of Modulation Levels

Network Topology	NSF Network				US Backbone Network			
Number of IRs	5		10		15		20	
Number of ERs	5		4		5		5	
Average Router Degree	2	4	3	6	3	9	4	12
Instance ID	1	2	3	4	5	6	7	8

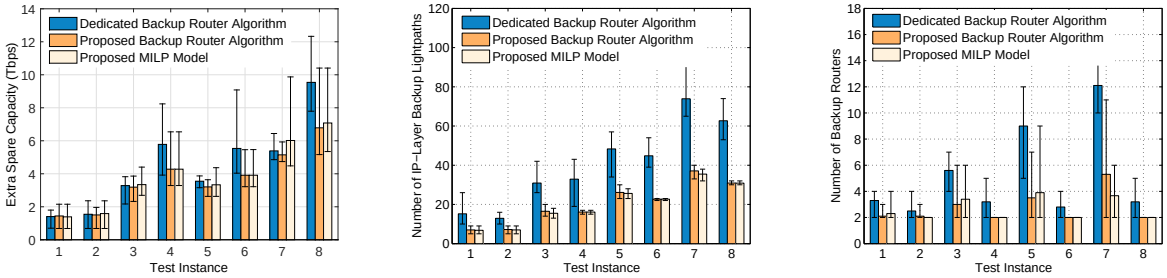
(d) Test Instances

Fig. 6. Simulation setup, (a) NSFNET topology, (b) US Backbone topology, (c) Transmission reaches of modulation-levels, and (d) Test instances.



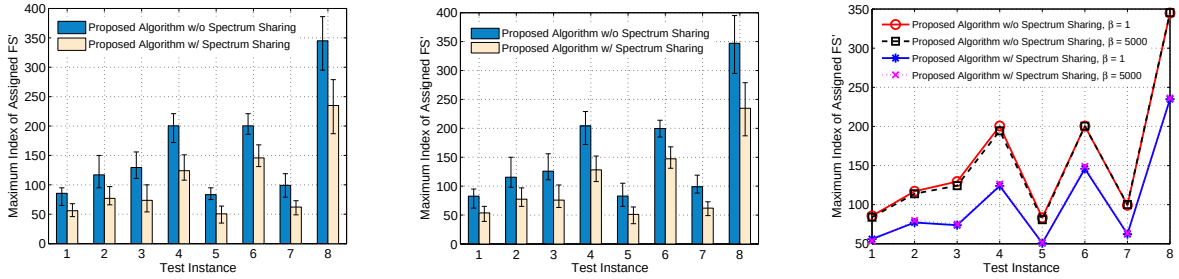
(a) Total amount of extra spare capacity. (b) Number of IP-layer backup lightpaths (c) Number of backup routers

Fig. 7. Results with $\beta = 1$, (a) Total amount of extra spare capacity, (b) Number of IP-layer backup lightpaths, and (c) Number of backup routers.



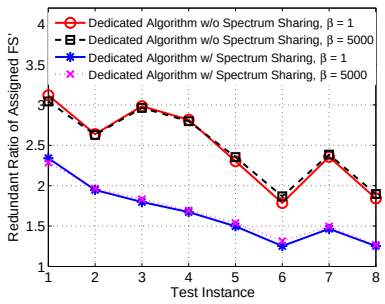
(a) Total amount of extra spare capacity. (b) Number of IP-layer backup lightpaths (c) Number of backup routers

Fig. 8. Results with $\beta = 5000$, (a) Total amount of extra spare capacity, (b) Number of IP-layer backup lightpaths, and (c) Number of backup routers.

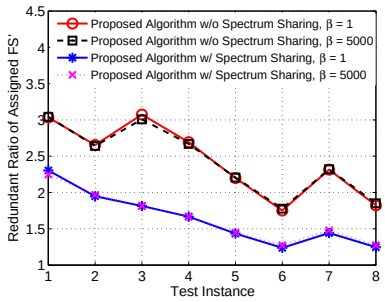


(a) In the scenario of $\beta = 1$ (b) In the scenario of $\beta = 5000$ (c) Comparison of results from two scenarios

Fig. 9. Results on the maximum index of assigned FS' in the EON with the proposed backup router algorithm under the scenarios of $\beta = 1$ and $\beta = 5000$.



(a) Dedicated backup router algorithm



(b) Proposed backup router algorithm

Fig. 10. Results on the redundant ratio of assigned FS', (a) Dedicated backup router algorithm, and (b) Proposed backup router algorithm.

Regarding the time complexity, the running time of the MILP model increases exponentially with the number of IRs, and it takes more than 2 hours to solve the problem of the 8-th test instance. However, the proposed backup router algorithm can always finish the computation with a few milliseconds, and it runs as fast as the dedicated backup router algorithm.

C. Lightpath Establishment in the EON Layer

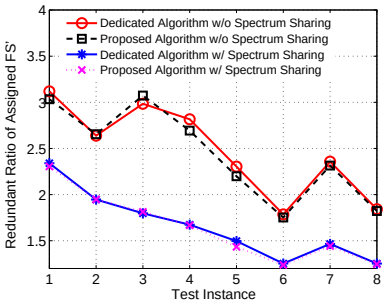
Here, we use the algorithm that considers no spectrum sharing among the lightpaths as the benchmark. Figs. 9(a) and 9(b) compare the results on the maximum index of assigned FS' on fiber links in the EON layer under the scenarios of $\beta = 1$ and $\beta = 5000$, respectively. With the proposed backup router algorithm, the proposed lightpath establishment algorithm can reduce the maximum index of assigned FS' by 35.67% on average. When comparing the results under the two scenarios in Fig. 9(c), we observe overlapped trends in both the lightpath establishment algorithms. This observation indicates that, even though the proposed backup router algorithm requires more extra spare capacity under the scenario of $\beta = 5000$ as shown in Fig. 8(a), it has almost no effect on the maximum index of assigned FS'. This may be because: 1) the amount of increased extra spare capacity is not that significant to make a difference, and 2) the proposed backup router algorithm naturally prefers to plan the extra spare capacity on the optical-layer backup lightpaths, which would not deteriorate the spectrum fragmentation in the EON layer.

Figs. 10(a) and 10(b) show the results on the redundant ratio of assigned FS' in the EON layer using the dedicated backup router algorithm and the proposed backup router algorithm, respectively. Note that, the redundant ratio of assigned FS' is defined as the ratio of the total number of backup FS' to the total number of working FS'. In both figures, under the same scenario of β, the proposed lightpath establishment algorithm can reduce the redundant ratios by 32.84% on average. Moreover, with the dedicated backup router algorithm, the redundant ratios under the scenario of $\beta = 5000$ are generally higher than those under the scenario of $\beta = 1$ by both the lightpath establishment algorithms, but the differences become smaller when using the proposed backup router algorithm.

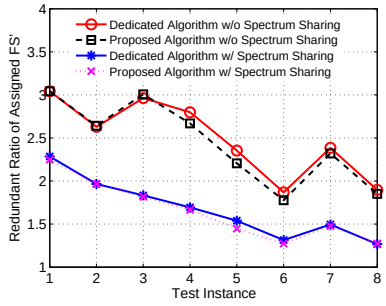
Figs. 11(a) and 11(b) compare the results on the redundant ratio of assigned FS' using the dedicated backup router algorithm and the proposed backup router algorithm under the scenarios of $\beta = 1$ and $\beta = 5000$, respectively. In both figures, when the proposed backup router algorithm is incorporated, both lightpath establishment algorithms generally achieve smaller redundant ratios than those that use the dedicated backup router algorithm. Moreover, when using different backup router algorithms, the lightpath establishment algorithms with spectrum sharing have smaller performance difference than those without. This is because: 1) the proposed lightpath establishment algorithm allows the IP-layer backup lightpaths to share FS' with the working lightpaths, the optical-layer backup lightpaths, and the multilayer backup lightpaths flexibly, resulting in a relatively small number of extra backup FS' even for a large number of IP-layer backup lightpaths, and 2) compared with the multilayer backup lightpaths that have to be link-disjoint with the related working lightpaths, the IP-layer backup lightpaths usually have smaller hop-counts, and thus reduce the number of backup FS' on links. Hence, the proposed lightpath establishment algorithm complements the differences between the dedicated backup router algorithm and the proposed backup router algorithm in terms of spectrum efficiency to some extent. However, we still should notice the remarkable advantages of the proposed backup router algorithm on reducing the CAPEX of network planning and having a good robustness, which make it irreplaceable.

VII. Conclusion

In this work, we focused on solving integrated multilayer protection planning in an IP-over-EON. Considering a single-failure scenario, we employed the router backup strategy to protect against a router outage in the IP layer and the shared "1 + 1" path protection strategy to protect against single fiber cut in the EON layer. First, we formulated the backup router planning problem in the IP layer as an MILP model with an objective of minimizing the extra spare capacity and the number of IP-layer backup lightpaths simultaneously, proved its $\mathcal{NP}$-hardness, and therefore proposed a time-efficient backup router planning algorithm. Simulation results verified that the proposed backup router planning algorithm can achieve 96.88% similar results to the proposed MILP model and required about 43.78% less IP-layer lightpaths than a benchmark algorithm, significantly reducing the CAPEX of network planning. Then, we proposed a lightpath establishment algorithm to maximize multilayer spectrum sharing in the EON layer. Simulation results showed that the proposed algorithm can reduce the planned FS' by 35.67% compared with a benchmark algorithm without spectrum sharing.



(a) $\beta = 1$



(b) $\beta = 5000$

Fig. 11. Results on the redundant ratio of assigned FS' using two backup router algorithms, (a) $\beta = 1$, and (b) $\beta = 5000$.

ACKNOWLEDGMENTS

This work was supported in part by the NSFC Projects 61701472 and 61771445, CAS Key Project (QYZDY-SSW-JSC003), NGBWMCN Key Project (2017ZX03001019-004), China Postdoctoral Science Foundation (2016M602031), and Fundamental Research Funds for the Central Universities (WK2100060021).

REFERENCES

[1] N. Sambo *et al.*, "Next generation sliceable bandwidth variable transponders," *IEEE Commu. Mag.*, vol. 53, pp. 163–171, Feb. 2015.
[2] Z. Zhu, W. Lu, L. Zhang, and N. Ansari, "Dynamic service provisioning in elastic optical networks with hybrid single-/multi-path routing," *J. Lightw. Technol.*, vol. 31, pp. 15–22, Jan. 2013.
[3] P. Lu *et al.*, "Highly-efficient data migration and backup for big data applications in elastic optical inter-datacenter networks," *IEEE Netw.*, vol. 29, pp. 36–42, Sept./Oct. 2015.
[4] M. Ghobadi and R. Mahajan, "Optical layer failures in a large backbone," in *Proc. of ACM IMC 2016*, pp. 461–467, Nov. 2016.
[5] F. Ji *et al.*, "Dynamic p-cycle protection in spectrum-sliced elastic optical networks," *J. Lightw. Technol.*, vol. 32, pp. 1190–1199, Mar. 2014.
[6] X. Chen *et al.*, "Flexible availability-aware differentiated protection in software-defined elastic optical networks," *J. Lightw. Technol.*, vol. 33, pp. 3872–3882, Sept. 2015.
[7] F. Rambach *et al.*, "A multilayer cost model for metro/core networks," *J. Opt. Commun. Netw.*, vol. 5, pp. 210–225, Mar. 2013.
[8] X. Chen, F. Ji, and Z. Zhu, "Service availability oriented p-cycle protection design in elastic optical networks," *J. Opt. Commun. Netw.*, vol. 6, pp. 901–910, Oct. 2014.
[9] X. Chen, S. Zhu, L. Jiang, and Z. Zhu, "On spectrum efficient failure-independent path protection p-cycle design in elastic optical networks," *J. Lightw. Technol.*, vol. 33, pp. 3719–3729, Sept. 2015.
[10] M. Kodialam, T. Lakshman, J. Orlin, and S. Sengupta, "Preconfiguring IP-over-optical networks to handle router failures and unpredictable traffic," *IEEE J. Sel. Areas Commun.*, vol. 25, pp. 934–948, Jun. 2007.
[11] M. Ruiz *et al.*, "Survivable IP/MPLS-over-WSON multilayer network optimization," *J. Opt. Commun. Netw.*, vol. 3, pp. 629–640, Aug. 2011.
[12] M. Pickavet *et al.*, "Recovery in multilayer optical networks," *J. Lightw. Technol.*, vol. 24, pp. 122–134, Jan. 2006.
[13] Y. Yin *et al.*, "Spectral and spatial 2D fragmentation-aware routing and spectrum assignment algorithms in elastic optical networks," *J. Opt. Commun. Netw.*, vol. 5, pp. A100–A106, Oct. 2013.
[14] W. Shi, Z. Zhu, M. Zhang, and N. Ansari, "On the effect of bandwidth fragmentation on blocking probability in elastic optical networks," *IEEE Trans. Commun.*, vol. 61, pp. 2970–2978, Jul. 2013.
[15] L. Gong and Z. Zhu, "Virtual optical network embedding (VONE) over elastic optical networks," *J. Lightw. Technol.*, vol. 32, pp. 450–460, Feb. 2014.
[16] M. Zhang, C. You, H. Jiang, and Z. Zhu, "Dynamic and adaptive bandwidth defragmentation in spectrum-sliced elastic optical networks with time-varying traffic," *J. Lightw. Technol.*, vol. 32, pp. 1014–1023, Mar. 2014.
[17] W. Lu and Z. Zhu, "Dynamic service provisioning of advance reservation requests in elastic optical networks," *J. Lightw. Technol.*, vol. 31, pp. 1621–1627, May 2013.
[18] L. Gong *et al.*, "Efficient resource allocation for all-optical multicasting over spectrum-sliced elastic optical networks," *J. Opt. Commun. Netw.*, vol. 5, pp. 836–847, Aug. 2013.
[19] X. Liu, L. Gong, and Z. Zhu, "On the spectrum-efficient overlay multicast in elastic optical networks built with multicast-incapable switches," *IEEE Commun. Lett.*, vol. 17, pp. 1860–1863, Sept. 2013.
[20] C. Chigan, G. Atkinson, and R. Nagarajan, "Cost effectiveness of joint multilayer protection in packet-over-optical networks," *J. Lightw. Technol.*, vol. 21, pp. 2694–2704, Nov. 2003.
[21] V. Gkamas, K. Christodoulopoulos, and E. Varvarigos, "A joint multi-layer planning algorithm for IP over flexible optical networks," *J. Lightw. Technol.*, vol. 33, pp. 2965–2977, Jul. 2015.
[22] A. Castro, L. Velasco, J. Comellas, and G. Junyent, "Dynamic restoration in multi-layer IP/MPLS-over-flexgrid networks," in *Proc. of DRCN 2013*, pp. 155–162, Mar. 2013.
[23] D. Amar, E. Le Rouzic, N. Brochier, and C. Lepers, "Class-of-service-based multilayer architecture for traffic restoration in elastic optical networks," *J. Opt. Commun. Netw.*, vol. 8, pp. A34–A44, Jul. 2016.
[24] V. Chvatal, "A greedy heuristic for the set-covering problem," *Math. Oper. Res.*, vol. 4, pp. 233–235, Aug. 1979.
[25] P. Slavík, "A tight analysis of the greedy algorithm for set cover," in *Proc. of ACM STOC 1996*, pp. 435–441, Jul. 1996.
[26] W. Lu, Z. Zhu, and B. Mukherjee, "On hybrid IR and AR service provisioning in elastic optical networks," *J. Lightw. Technol.*, vol. 33, pp. 4659–4669, Nov. 2015.
[27] J. Zhu, B. Zhao, and Z. Zhu, "Attack-aware service provisioning to enhance physical-layer security in multi-domain EONs," *J. Lightw. Technol.*, vol. 34, pp. 2645–2655, Jun. 2016.
[28] A. Bocoi *et al.*, "Reach-dependent capacity in optical networks enabled by OFDM," in *Proc. of OFC 2009*, pp. 1–3, Mar. 2009.
[29] L. Gong, X. Zhou, W. Lu, and Z. Zhu, "A two-population based evolutionary approach for optimizing routing, modulation and spectrum assignments (RMSA) in O-OFDM networks," *IEEE Commun. Lett.*, vol. 16, pp. 1520–1523, Sept. 2012.
[30] S. Buckland, "Monte carlo confidence intervals," *Biometrics*, vol. 40, pp. 811–817, Sept. 1984.