# Security-aware Planning of Packet-over-Optical Networks in Consideration of OTN Encryption

Feng Chen, Man Song, Fen Zhou, and Zuqing Zhu, *Senior Member, IEEE*

***Abstract*—The fast development of cloud computing and Big Data applications has promoted virtualization technologies such as network function virtualization (NFV), which in turn dramatically increased the amount of sensitive data being transmitted over the optical networks for datacenter interconnections (DCIs). To ensure the physical-layer security in DCIs, people have developed optical transport network (OTN) encryption technologies, *i.e.*, leveraging high-speed encryption cards (ECs) to encrypt OTN payload frames. Although experimental studies have confirmed the benefits of ECs in terms of line-speed processing, low latency, and small encryption overhead, the problem of how to utilize them to build a secure packet-over-optical network with high cost-effectiveness has not been explored yet. In this paper, we study how to realize cost-effective and security-aware multilayer planning in a packet-over-optical network that covers both trusted and untrusted zones, in consideration of OTN encryption. We first formulate an integer linear programming (ILP) model to minimize the total capital expenditure (CAPEX) of the multilayer planning, which includes the costs of OTN linecards (LCs), ECs, and bandwidth resources, and solve the optimization exactly. Then, we prove the $\mathcal{NP}$-hardness of the multilayer planning, and to reduce the time complexity, we propose a column generation (CG) model and design a more time-efficient approximation algorithm based on it. Our simulation results confirm the performance and advantages of our CG-based proposal, *i.e.*, it is much more time-efficient than solving the ILP directly, and outperform the existing heuristic in terms of total CAPEX and costs of used LCs and ECs.**

***Index Terms*—Multilayer network planning, Optical transport network (OTN), OTN encryption, Physical-layer security, Column generation, Approximation algorithm.**

## I. Introduction

RECENTLY, we have witnessed the proliferation of cloud computing and Big Data applications all over the world, which lead to increasing demands for data processing, data storage and digital communications [1, 2], while the only way to address such demands is to speed up the global deployment of data centers (DCs) and the network infrastructures to interconnect them (*i.e.*, DCIs) [3–5]. This stimulated intensive interests on the research and development (R&D) of optical communications and networking technologies [6–9]. However, it is known that optical transport networks (OTNs) are vulnerable to physical-layer impairments and attacks [10, 11], especially when they have adopted the new technologies to support DCIs better. For instance, elastic optical networks (EONs) [12–14] provide improved spectral efficiency and an agile optical layer to address the high-throughput and highly dynamic traffic in DCIs [15], but as they use much narrower channel spacings than fixed-grid wavelength-division multiplexing (WDM) networks, wire-tapping can be realized in a more efficient and harder-to-detect way [16]. Meanwhile, the wide usages of virtualization technologies (*e.g.*, virtual network slicing [17, 18] and network function virtualization (NFV) [19, 20]) can make sensitive data be transferred frequently in DCIs. Therefore, DCI operators have to find effective ways to protect their networks from the data leakage due to physical-layer vulnerabilities such that their own business and those of their clients can be secured [21].

Previously, people have developed various network planning approaches to protect optical networks against physical-layer attacks [23–28]. They distributed the lightpaths in an optical network in the way that the probability of many lightpaths sharing fiber links and/or switch nodes could be minimized. Nevertheless, even though these approaches can effectively reduce the threats from physical-layer vulnerabilities, physical-layer attacks (*e.g.*, wire-tapping) can still happen. A safer way to protect data transfers in DCIs is to utilize the OTN encryption technologies, which leverage high-speed electronics to encrypt OTN payload frames and have the benefits of line-speed processing, low latency, and small encryption overhead [21]. Specifically, in addition to the well-known OTN linecards (LCs), OTN encryption introduces special encryption cards (ECs) that can work with LCs flexibly.

As suggested by the study in [22], LCs, ECs and OTN switches[1] can be organized in the three typical architectures in Fig. 1 to realize traffic grooming and wavelength routing. Architecture I in Fig. 1(a) maps ECs to LCs in the "one-to-one" scenario and routes each packet flow with an end-to-end lightpath. Architecture II in Fig. 1(b) grooms packet flows first, and maps the groomed traffic to ECs and LCs in sequence, while each packet flow can be routed over multiple lightpaths. With Architecture III in Fig. 1(c), each packet flow is encrypted by an EC before being groomed with others in an LC, and it can also experience multi-hop lightpath routing.

Previous studies have compared the capital expenditure (CAPEX) of the three architectures in Fig. 1 in different network planning scenarios [22, 29]. However, they found that there does not exist a universal winner and the CAPEX can be significantly impacted by the granularity, volume and distribution of the traffic in a packet-over-optical network.

F. Chen, M. Song, 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).

F. Zhou is with IMT Lille Douai, Institute Mines-Tlcom, Univ. Lille, Center for Digital Systems, F59000 Lille, France.

Manuscript received on October 26, 2020.

[1]In this work, we consider the general concept of OTN, which might use a broader range of technologies than those defined in ITU-T G.709.

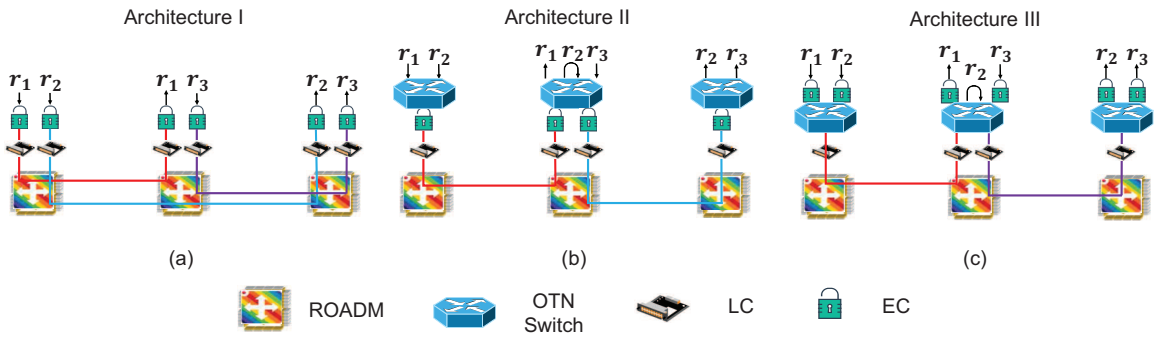


Fig. 1. Network architectures for multilayer planning in consideration of OTN encryption [22].

To this end, the network planning in consideration of OTN encryption should use the three architectures jointly and adaptively to realize the best cost-effectiveness. As it needs to jointly optimize the traffic grooming in the packet layer and the wavelength routing in the optical layer, the network planning is a multilayer one. Nevertheless, this multilayer planning problem is more complex than the existing ones that only consider LCs and OTN switches. This is because in addition to the packet and optical layers, the ECs bring in a new layer (*i.e.*, the encryption layer), and the operation sequence of the packet and encryption layers can be switched back and forth when the three architectures are used simultaneously. Moreover, the problem becomes even more challenging, if we address the generic scenario where the multilayer DCI includes both trusted and untrusted zones, and the packet flows can be either sensitive or non-sensitive. Such a multilayer planning problem still has not been fully explored.

In [30], we conducted a preliminary study on how to realize cost-effective and security-aware multilayer network planning in a DCI, which covers both trusted and untrusted zones, and can choose OTN encryption architectures based on traffic conditions. However, the study has the following issues. Firstly, it was based on the assumption that all the packet flows are sensitive ones and need to be encrypted when passing through untrusted zone(s), which is not practical or at least not generic enough. Secondly and more importantly, the algorithm design in [30] was preliminary, *i.e.*, the integer linear programming (ILP) model is not compact and thus can only be solved for the problems whose sizes are small, and the heuristic based on collapsed auxiliary graphs (CAGs) cannot ensure a bounded performance gap to the exact solution. In this work, we extend the study in [30] with a few major improvements to make the problem-solving more comprehensive:

- We categorize the packet flows considered in the multilayer planning as sensitive and non-sensitive ones, where the non-sensitive flows do not need to be encrypted when passing through untrusted zone(s). Hence, the network model becomes more generic.
- Based on the new network model, we formulate a new ILP, which contains less variables and constraints than that in [30], to minimize the total CAPEX of the multilayer planning. Therefore, the new ILP model is not only more generic but also more compact, and thus it can be solved more time-efficiently.
- We propose a novel approximation algorithm based on column generation (CG) [31], which can solve the multilayer planning with reduced time complexity and guarantee a bounded approximation ratio. This is the most important improvement achieved in this work.
- We conduct extensive simulations to evaluate our proposal and compare it with the CAG-based heuristic developed in [30], and the results confirm its effectiveness.

The rest of the paper is organized as follows. Section II surveys the related work briefly. We describe the network model and the optimization problem in Section III. The ILP model to solve the problem exactly and the complexity analysis of the problem are presented in Section IV. We propose the CG model in Section V. The performance evaluations with numerical simulations are discussed in Section VI. Finally, Section VII summarizes the paper.

## II. Related Work

Considering the traffic characteristics in DCIs, the operators normally build their networks based on the packet-over-optical architecture [21, 32], where the packet layer grooms and routes the packet flows from DC applications, while the optical layer leverages wavelength routing to achieve high-throughput data transmissions among DCs. Hence, given a set of packet flows or an estimated traffic matrix, the multilayer planning for a DCI is to find the way to aggregate the traffic flows from the packet layer, plan lightpaths to carry the groomed traffic, and determine the routing schemes of the lightpaths in the optical layer, such that the total CAPEX including both the equipment cost and the cost of spectrum utilization can be minimized.

To solve the multilayer planning problem, people have considered various optical networking technologies [33, 34] and different types of traffic demands [35–39]. In [35], the authors proposed several genetic algorithms based meta-heuristics to solve the multilayer planning of survivable IP/multi-protocol label switching (MPLS) over WDM networks. The study in [36] considered the multilayer planning in IP-over-EONs, and designed an effective heuristic to jointly optimize the grooming and routing in the IP layer, and the routing, modulation-level and spectrum assignments in the EON layer. Lu *et al.* [37] studied how to plan data-oriented tasks in multilayer DCIs whose optical layers are based on fixed-grid and flexible-grid optical networking. The cost-efficient multilayer restoration schemes to address IP router outages were developed in

[38]. The authors of [39] tackled the problem of multilayer planning to protect IP-over-EONs from failures in both the IP and EON layers. However, since all these studies did not consider physical-layer vulnerabilities, the multilayer planning algorithms developed in them are not security-aware.

The optical layer of a DCI can be affected by anomalies and attacks. To improve the DCI's survivability and availability against random failures and natural disasters, one can resort to either the proactive scheme that utilizes multilayer protection planning (*e.g.*, in [35, 38, 39]), or the reactive scheme that tries to evacuate important data out when service outages happen or are approaching [40, 41]. Nevertheless, none of these schemes can address physical-layer attacks, because most of them are hard-to-detect [11]. For example, a malicious party can achieve wire-tapping easily by bending an optical fiber and collecting the leakage signal [25]. Therefore, the authors of [23] laid out a network security framework to list the potential methods for dealing with physical-layer attacks. The mentioned methods tried to manipulate the routing and spectrum assignment (RSA) schemes of lightpaths such that either the physical-layer attacks become difficult to launch or their adverse effects can be minimized [16, 24–28]. However, as they only mitigate the threats, the possibility of data leakage cannot be eliminated. Furthermore, because the security-aware RSA schemes need to avoid certain fiber links or/and reserve spectral guard-bands frequently, spectrum wastes (*e.g.*, spectrum fragmentation [42, 43]) would be inevitable. Hence, DCI operators also need OTN encryption technologies[2] to protect their sensitive data [21].

The multilayer planning that considers OTN encryption was first formulated in [22], where the authors laid out the three architectures for multilayer planning and compared their CAPEX. Then, in [29], we evaluated the three architectures in the situation where multilayer restoration needs to be invoked to address router outages. These two studies did not optimize the security-aware multilayer planning based on practical assumptions or jointly consider the three architectures. This motivated our preliminary study on the topic in [30]. However, the network model in [30] was still not practical enough, because it assumed that all the packet flows are sensitive and need to be encrypted if being sent through untrusted zone(s). More importantly, we only designed a heuristic whose performance gap to the exact solution is not bounded.

In this work, we leverage CG to design an approximation algorithm for the problem. Note that, CG decomposition is a commonly-used technique to quickly find near-optimal solutions for $\mathcal{NP}$-hard problems. The studies in [46, 47] used CG decomposition to solve the network planning with RSA. We optimized service function chain deployment and readjustment with CG in [48], and Zhou *et al.* [49] proposed a CG-based approach to tackle the multicast provisioning in mixed-line-rate optical networks. However, even though this work shares the general procedure of CG decomposition with the algorithms developed in these studies, the actual CG-based algorithm designs are completely different. This is because for CG, the master and pricing problems need to be specifically designed based on the actual optimization problem [31].

[2]Note that, by when this paper is written, there is no standard OTN encryption scheme per ITU-T, and all the available commercial offerings for OTN encryption are proprietary and cannot inter-operate with each other. Meanwhile, recent research also suggested that DCIs can be architected without the OTN layer [44] and use the Layer-1 encryption schemes (*e.g.*, the one in [45]). This will make the network model different from the one considered in this work, and will be considered in our future work.

## III. Problem Description

In this section, we describe the network model, and explain the problem of multilayer planning that leverages OTN encryption to architect secure packet-over-optical DCIs.

### A. Network Model

We model the physical topology of the optical layer as a graph $G(V, E)$, where $V$ represents the set of switch nodes and $E$ is the set of fiber links. Each switch node $v \in V$ consists of an optical switch built with reconfigurable optical add-drop multiplexers (ROADMs) and packet layer equipment (*i.e.*, LCs, ECs and an OTN switch). Here, we assume that the LCs and ECs can use a few preset capacities [21, 22], and denote the sets of feasible LC and EC capacities as $B^{\text{LC}}$ and $B^{\text{EC}}$, respectively[3]. Meanwhile, considering the fact that each OTN switch may only have a limited number of slots to hold LCs/ECs, we assume that the number of each type of LCs/ECs[4] on a switch node cannot exceed an upper-limit. We denote the upper-limits for the LCs/ECs with the $n$-th feasible LC/EC capacity as $M_n^{\text{LC}}$ and $M_n^{\text{EC}}$, respectively. There are two types of fiber links in $E$, *i.e.*, the trusted and untrusted ones, and the untrusted fiber links refer to those on which wire-tapping can happen. Hence, if one needs to transmit flows containing sensitive data (*i.e.*, sensitive flows) over untrusted fiber links, OTN encryption has to be used, while this is not required if the flows are transmitted over trusted fiber links or they are non-sensitive. The trusted and untrusted fiber links formulate trusted and untrusted zones in $G(V, E)$, respectively.

The multilayer planning needs to serve a set of flows from the packet layer, and we denote the flow set as $\mathcal{R}$. Each flow $r_i \in \mathcal{R}$ can be represented with a tuple $\{s_i, d_i, b_i\}$, where $i$ is its unique index, $s_i$ and $d_i$ denote its source and destination nodes, respectively, and $b_i$ is its bandwidth demand in Gbps. In this work, we consider two types of flows, *i.e.*, the sensitive and non-sensitive ones, and denote their sets as $\mathcal{R}_{\text{S}}$ and $\mathcal{R}_{\text{NS}}$, respectively. We have $\mathcal{R}_{\text{S}} \cap \mathcal{R}_{\text{NS}} = \emptyset$ and $\mathcal{R}_{\text{S}} \cup \mathcal{R}_{\text{NS}} = \mathcal{R}$. The multilayer planning has to let a sensitive flow go through ECs, if the flow will be transmitted over untrusted fiber link(s).

### B. Multilayer Planning with OTN Encryption

Fig. 2 shows an example on the security-aware multilayer planning considered in this work. The physical topology

[3]Note that, in addition to the legacy LCs/ECs considered here, some of the advanced LCs, which are produced recently, have the feature of full-rate line-encryption [50, 51]. However, if the network planning only considers these advanced LCs, it will have two drawbacks. Firstly, its universality becomes limited because operators might still possess legacy LCs/ECs in their existing systems and inventories. Secondly, its flexibility will be restricted because with the full-rate line-encryption, the packet flows going through an advanced LC either all get encrypted or are all transmitted in plaintext. Therefore, a more generic version of the network planning should consider legacy LCs/ECs together with the advanced LCs, which will be studied in our future work.

[4]A type of LCs/ECs refer to the LCs/ECs whose capacities are the same.

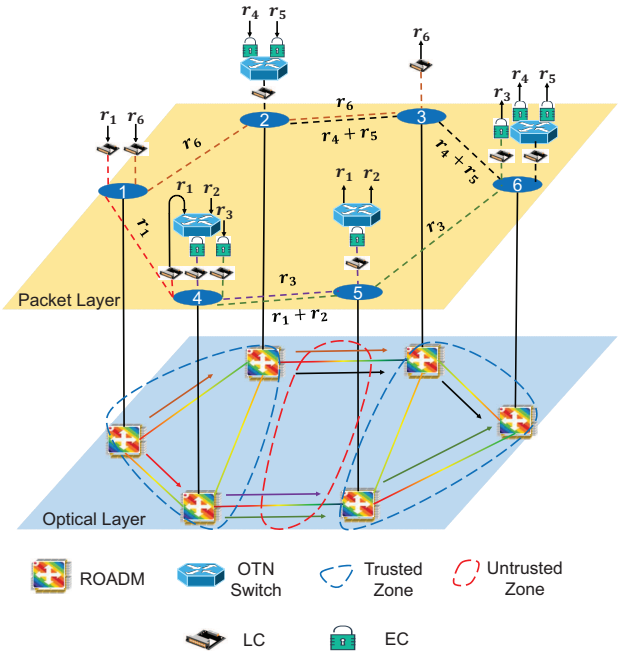


Fig. 2. Example on multilayer planning in consideration of OTN encryption.

consists of 6 switch nodes and 8 fiber links. Among the fiber links, two are untrusted and the remaining ones are trusted. The multilayer planning needs to serve 6 flows, *i.e.*, $\mathcal{R} = \{r_i, i \in [1,6]\}$, where $r_6$ is a non-sensitive flow and the rest of the flows are sensitive. As $r_1$ and $r_2$ are sensitive flows and both of their destinations are *Node* 5, we first send $r_1$ through a lightpath between *Nodes* 1 and 4, then groom it with $r_2$ on *Node* 4 to share the same EC and LC (*i.e.*, using the Architecture II in Fig. 1(b)), and finally transmit encrypted $r_1$ and $r_2$ through a lightpath between *Nodes* 4 and 5 to go across the untrusted zone. We leverage the Architecture I in Fig. 1(a) to serve $r_3$, which means that it gets assigned with dedicated EC and LC pairs and is transmitted from *Node* 4 to *Node* 6 with an end-to-end lightpath. With the Architecture III in Fig. 1(c), $r_4$ and $r_5$ first experience separate ECs, and then are groomed by an LC for being transmitted through the lightpath from *Node* 2 to *Node* 6. Finally, as $r_6$ is non-sensitive, it does not need to use ECs to go across the untrusted zone.

To this end, we can see that the multilayer planning needs to serve sensitive and non-sensitive flows according to their demands, and choose OTN encryption architectures based on traffic conditions. The optimization objective is to minimize the total CAPEX of the multilayer planning. As the multilayer planning does not change the deployments of OTN switches and ROADM-based optical switches in the packet-over-optical network, we consider the total CAPEX as the summation of the costs from used LCs, ECs, and bandwidth resources.

## IV. ILP Formulation

This section formulates an ILP model to solve the security-aware multilayer planning in consideration of OTN encryption.

**Parameters:**

- $G(V, E)$: the physical topology of the optical layer.
- $\mathcal{P}$: the set of feasible routing paths in $G(V, E)$ for establishing lightpaths. For each node pair $u$-$v$, we pre-calculate $K$ shortest paths, and $p_k^{u,v}$ denotes the $k$-th path.
- $\mathcal{P}_{\text{UT}}$: the set of feasible routing paths that contain untrusted fiber links, *i.e.*, $\mathcal{P}_{\text{UT}} \subseteq \mathcal{P}$.
- $h_k^{u,v}$: the hop-count of the $k$-th shortest path for $u$-$v$.
- $\mathcal{R}$: the set of pending flows from the packet layer, where the $i$-th flow is denoted as $r_i(s_i, d_i, b_i)$. Each flow $r_i$ belongs to either the sensitive flow set $\mathcal{R}_{\text{S}}$ or the non-sensitive flow set $\mathcal{R}_{\text{NS}}$, *i.e.*, $\mathcal{R}_{\text{S}} \cup \mathcal{R}_{\text{NS}} = \mathcal{R}$.
- $B^{\text{LC}}$: the set of feasible LC capacities, where $b_n^{\text{LC}} \in B^{\text{LC}}$ in Gbps is the $n$-th feasible LC capacity.
- $B^{\text{EC}}$: the set of feasible EC capacities, where $b_n^{\text{EC}} \in B^{\text{EC}}$ in Gbps is the $n$-th feasible EC capacity.
- $c_n^{\text{LC}}$: the cost of an LC with the $n$-th feasible LC capacity.
- $c_n^{\text{EC}}$: the cost of an EC with the $n$-th feasible EC capacity.
- $M_n^{\text{LC}}$: the largest number of LCs that use the $n$-th feasible LC capacity and can be deployed on a switch node.
- $M_n^{\text{EC}}$: the largest number of ECs that use the $n$-th feasible EC capacity and can be deployed on a switch node.

**Variables:**

- $\gamma_i^{u,v}$: the boolean variable that equals 1 if flow $r_i \in \mathcal{R}$ is routed over a lightpath for $u$-$v$, and 0 otherwise.
- $\vartheta_{i,k}^{u,v}$: the boolean variable that equals 1 if flow $r_i$ uses a lightpath that is routed over the $k$-th shortest path for $u$-$v$, and 0 otherwise.
- $x_{i,j,n}^{u,v}$: the boolean variable that equals 1 if on switch node $u$, flow $r_i$ uses the $j$-th LC, which provides the $n$-th feasible capacity and originates a lightpath for $u$-$v$, and 0 otherwise. We assume that each used LC/EC on a switch node can be referred to with a unique index. For each lightpath, we need to deploy a pair of LCs at its two ends. Here, with this variable, we only consider one end of a lightpath, and thus we will double the total cost of LCs in the optimization objective in Eq. (1).
- $y_{i,j,n}^{u,v}$: the boolean variable that equals 1 if on switch node $u$, flow $r_i$ uses the $j$-th EC, which provides the $n$-th feasible capacity and connects to a lightpath for $u$-$v$, and 0 otherwise. ECs are also deployed in pairs, and their total cost will be doubled in the objective in Eq. (1) too.
- $f_{j,n}^{u,v}$: the boolean variable that equals 1 if the $j$-th LC on switch node $u$ provides the $n$-th feasible capacity and originates a lightpath for $u$-$v$, and 0 otherwise.
- $g_{j,n}^{u,v}$: the boolean variable that equals 1 if the $j$-th EC on switch node $u$ provides the $n$-th feasible capacity and connects to a lightpath for $u$-$v$, and 0 otherwise.
- $z_{i,j,n,j',n'}^{u,v}$: the boolean variable that equals 1 if on switch node $u$, flow $r_i$ uses the $j$-th LC, which provides the $n$-th feasible capacity, and the $j'$-th EC, which provides the $n'$-th feasible capacity, and the LC and EC connect to a lightpath for $u$-$v$, and 0 otherwise.
- $w_{j,n,j',n'}^{u,v}$: the boolean variable that equals 1 if on switch node $u$, one or more flows use the $j$-th LC, which provides the $n$-th feasible capacity, and the $j'$-th EC, which provides the $n'$-th feasible capacity, and the LC and EC connect to a lightpath for $u$-$v$, and 0 otherwise.

**Objective:**

The optimization objective is to minimize the total cost from the used LCs, ECs, and bandwidth resources.

$$\begin{aligned}\text{Minimize}\quad & 2\cdot\sum_{u,v\in V}\left(\sum_{n=1}^{|B^{\mathrm{LC}}|}c_n^{\mathrm{LC}}\cdot\sum_j f_{j,n}^{u,v}+\sum_{n=1}^{|B^{\mathrm{EC}}|}c_n^{\mathrm{EC}}\cdot\sum_j g_{j,n}^{u,v}\right)\\ &+\alpha\cdot\sum_{i=1}^{|\mathcal{R}|}b_i\cdot\left(\sum_{u,v\in V}\sum_{k=1}^{K}\vartheta_{i,k}^{u,v}\cdot h_k^{u,v}\right),\end{aligned}\tag{1}$$

where $\alpha$ is the unit cost of using 1 Gbps per fiber hop.

**Constraints:**

*1) Constraints for Flow Routing over Lightpaths:*

$$\sum_{v\in V}(\gamma_i^{u,v}-\gamma_i^{v,u})=\begin{cases}1, & u=s_i\\ -1, & u=d_i\\ 0, & \text{otherwise}\end{cases},\quad\forall r_i\in\mathcal{R}.\tag{2}$$

Eq. (2) ensures that the routing of each flow $r_i$ over lightpaths in the optical layer satisfies the flow conservation condition.

$$\sum_{k=1}^{K}\vartheta_{i,k}^{u,v}=\gamma_i^{u,v},\quad\forall r_i\in\mathcal{R},\ \forall u,v\in V.\tag{3}$$

Eq. (3) ensures that each flow uses one and only one lightpath when being transmitted between a node pair.

*2) Constraints for LC Deployments:*

$$\sum_{n=1}^{|B^{\mathrm{LC}}|}\sum_j x_{i,j,n}^{u,v}=\gamma_i^{u,v},\quad\forall r_i\in\mathcal{R},\ \forall u,v\in V.\tag{4}$$

Eq. (4) ensures that each flow uses one and only one LC to go through a lightpath.

$$\sum_{i=1}^{|\mathcal{R}|}b_i\cdot x_{i,j,n}^{u,v}\le b_n^{\mathrm{LC}},\quad\forall u,v\in V,\ j,\ n\in[1,|B^{\mathrm{LC}}|].\tag{5}$$

Eq. (5) ensures that total bandwidth demand of the flows using a same LC does not exceed the capacity of the LC.

$$f_{j,n}^{u,v}\le\sum_{i=1}^{|\mathcal{R}|}x_{i,j,n}^{u,v},\quad\forall u,v\in V,\ j,\ n\in[1,|B^{\mathrm{LC}}|],\tag{6}$$

$$f_{j,n}^{u,v}\ge x_{i,j,n}^{u,v},\quad\forall r_i\in\mathcal{R},\ \forall u,v\in V,\ j,\ n\in[1,|B^{\mathrm{LC}}|],\tag{7}$$

$$\sum_j\sum_{u\in V}f_{j,n}^{u,v}\le M_n^{\mathrm{LC}},\quad\forall n\in[1,|B^{\mathrm{LC}}|],\ \{v:v\in V,v\ne u\}.\tag{8}$$

Eqs. (6)-(8) ensure that on each switch node, the number of used LCs, which provides the same feasible capacity, does not exceed the preset upper-limit.

*3) Constraints for EC Deployments:*

$$\sum_{n=1}^{|B^{\mathrm{EC}}|}\sum_j y_{i,j,n}^{u,v}=\sum_{\{k:p_k^{u,v}\in\mathcal{P}_{\mathrm{UT}}\}}\vartheta_{i,k}^{u,v},\quad\forall r_i\in\mathcal{R}_{\mathrm{S}}.\tag{9}$$

Eq. (9) ensures that each sensitive flow uses one and only one EC to go through a lightpath, if the lightpath routes over untrusted fiber link(s).

$$\sum_{i=1}^{|\mathcal{R}|}b_i\cdot y_{i,j,n}^{u,v}\le b_n^{\mathrm{EC}},\quad\forall u,v\in V,\ j,\ n\in[1,|B^{\mathrm{EC}}|].\tag{10}$$

Eq. (10) ensures that total bandwidth demand of the flows using a same EC does not exceed the capacity of the EC.

$$g_{j,n}^{u,v}\le\sum_{i=1}^{|\mathcal{R}|}y_{i,j,n}^{u,v},\quad\forall u,v\in V,\ j,\ n\in[1,|B^{\mathrm{EC}}|],\tag{11}$$

$$g_{j,n}^{u,v}\ge y_{i,j,n}^{u,v},\quad\forall r_i\in\mathcal{R},\ \forall u,v\in V,\ j,\ n\in[1,|B^{\mathrm{EC}}|],\tag{12}$$

$$\sum_j\sum_{u\in V}g_{j,n}^{u,v}\le M_n^{\mathrm{EC}},\ \forall n\in[1,|B^{\mathrm{EC}}|],\ \{v:v\in V,v\ne u\}.\tag{13}$$

Eqs. (11)-(13) ensure that on each switch node, the number of used ECs, which provides the same feasible capacity, does not exceed the preset upper-limit.

*4) Constraints for Mappings among Flows, LCs and ECs:*

$$\begin{aligned}x_{i,j,n}^{u,v}+y_{i,j',n'}^{u,v}-1\le z_{i,j,n,j',n'}^{u,v},\quad&\forall r_i\in\mathcal{R},\ \forall u,v\in V,\\ &\forall j,\ j',\ \forall n\in[1,|B^{\mathrm{LC}}|],\ n'\in[1,|B^{\mathrm{EC}}|],\end{aligned}\tag{14}$$

$$\begin{aligned}z_{i,j,n,j',n'}^{u,v}\le y_{i,j',n'}^{u,v},\quad&\forall r_i\in\mathcal{R},\ \forall u,v\in V,\\ &\forall j,\ j',\ \forall n\in[1,|B^{\mathrm{LC}}|],\ n'\in[1,|B^{\mathrm{EC}}|],\end{aligned}\tag{15}$$

$$\begin{aligned}z_{i,j,n,j',n'}^{u,v}\le x_{i,j,n}^{u,v},\quad&\forall r_i\in\mathcal{R},\ \forall u,v\in V,\\ &\forall j,\ j',\ \forall n\in[1,|B^{\mathrm{LC}}|],\ n'\in[1,|B^{\mathrm{EC}}|].\end{aligned}\tag{16}$$

Eqs. (14)-(16) ensure that each combination of used LC and EC gets assigned to the flows correctly (*i.e.*, according to one of the architectures in Fig. 1).

$$\begin{aligned}w_{j,n,j',n'}^{u,v}\le\sum_{i=1}^{|\mathcal{R}|}z_{i,j,n,j',n'}^{u,v},\quad&\forall u,v\in V,\\ &\forall j,\ j',\ \forall n\in[1,|B^{\mathrm{LC}}|],\ n'\in[1,|B^{\mathrm{EC}}|],\end{aligned}\tag{17}$$

$$\begin{aligned}w_{j,n,j',n'}^{u,v}\ge z_{i,j,n,j',n'}^{u,v},\quad&\forall r_i\in\mathcal{R},\ \forall u,v\in V,\\ &\forall j,\ j',\ \forall n\in[1,|B^{\mathrm{LC}}|],\ n'\in[1,|B^{\mathrm{EC}}|],\end{aligned}\tag{18}$$

$$\sum_{n'=1}^{|B^{\mathrm{EC}}|}\sum_{j'}w_{j,n,j',n'}^{u,v}\cdot b_{n'}^{\mathrm{EC}}\le b_n^{\mathrm{LC}},\ \forall u,v\in V,\ \forall j,\ n\in[1,|B^{\mathrm{LC}}|],\tag{19}$$

$$\sum_{n=1}^{|B^{\mathrm{LC}}|}\sum_j w_{j,n,j',n'}^{u,v}\le 1,\quad\forall u,v\in V,\ j',\ n'\in[1,|B^{\mathrm{EC}}|].\tag{20}$$

Eqs. (17)-(20) ensure that the total capacity of the ECs, which connect to a same LC, does not exceed the capacity of the LC, and if an EC is used by one or more flows (*e.g.*, in Architecture II), these flows have to be assigned to a same LC. This is because the three architectures in Fig. 1 suggest that we cannot map the flows going through an EC to multiple LCs, but the other way around is permitted (*i.e.*, in Architecture III). Note that, the joint considerations of the three architectures in Fig. 1 in the ILP are enforced by the constraints in Eqs. (14)-(20).

**Theorem 1.** *The optimization described by the aforementioned ILP model is $\mathcal{NP}$-hard.*

*Proof:* We prove the $\mathcal{NP}$-hardness of the optimization by restriction, *i.e.*, restricting away several of its aspects until a known $\mathcal{NP}$-hard problem appears [52]. First of all, we apply the restriction to set $\alpha=0$ and $\{c_n^{\mathrm{EC}}=0,\ \forall n\in[1,|B^{\mathrm{EC}}|]\}$, which means that the bandwidth resources and ECs are free when counting the total CAPEX. Hence, the arrangements

related to them become irrelevant to the optimization. Secondly, we restrict the number of feasible LC capacities to be $|B^{\mathrm{LC}}| = 1$. Finally, we restrict the physical topology $G(V, E)$ to only contain two switch nodes and one fiber link between them. Then, the optimization gets transformed into the problem that given a set of pending flows $\mathcal{R}$, how to groom and transmit them with the least number of fixed-capacity LCs? If we treat the flows as items and the LCs as bins, the problem is just the general case of the bin packing problem [53], which is known to be $\mathcal{NP}$-hard. To this end, since a special case of the optimization described by the ILP model is the general case of a known $\mathcal{NP}$-hard problem, we prove that the problem of security-aware multilayer planning in consideration of OTN encryption is $\mathcal{NP}$-hard as well. ■

## V. Column Generation based Approximation Algorithm

In this section, we propose a novel CG model based on the ILP model formulated in the previous section, and leverage it to design an approximation algorithm for solving the optimization time-efficiently and with performance guarantee.

### A. Overall Procedure of CG-based Approach

By checking the variables of the ILP in Section IV, we can see that for each flow, its provisioning scheme actually includes the related deployment of LCs and ECs and its routing scheme over lightpaths. Hence, if we denote a feasible provisioning scheme of a flow as one column $c$ and get the column set $\mathcal{C}_i$ for each flow $r_i \in \mathcal{R}$, we can leverage CG to optimize the selections of columns in iterations to find a near-optimal solution. The overall procedure of our proposed approximation algorithm is shown in *Algorithm* 1. It follows the general principle of CG (*i.e.*, the simplex method [31]).

Specifically, we first decompose the original optimization into a master problem and a pricing problem. Then, the master problem is transformed into a restricted master problem (RMP) whose variables are real and fewer than those in the master problem. As the optimal solution of the RMP might not be the one that we intend to get in the end, we use the pricing problem to check whether by adding the variables, which are in the master problem but not included in the RMP currently, in the RMP can reduce the objective of the RMP (*i.e.*, the original optimization is for minimization). If yes, we add the variables in the RMP, and update the pricing problem accordingly. This procedure is repeated in iterations until we cannot reduce the RMP's objective by adding the variables of the master problem in it. At this moment, the optimal solution of the RMP is just the near-optimal solution of the original optimization [31], with a bounded approximation ratio.

In *Algorithm* 1, *Lines* 1-9 are for the initialization. Here, *Line* 1 defines all the parameters to represent a column $c$, which denotes a feasible provisioning scheme of each flow. In *Lines* 2-4, we decompose the original ILP into a master problem and a pricing problem, and formulate two ILP models for them, respectively. Then, the for-loop that covers *Lines* 5-9 initializes the column set $\{\mathcal{C}_i,\ \forall r_i \in \mathcal{R}\}$. Specifically, for each flow $\forall r_i \in \mathcal{R}$, *Line* 7 uses a heuristic to obtain its initial provisioning scheme for the column construction. Here, we modify the CAG-based heuristic designed in [30] to obtain the heuristic used in *Line* 7. With the initial column set $\{\mathcal{C}_i,\ \forall r_i \in \mathcal{R}\}$, *Line* 10 constructs the RMP, which is actually the linear programming (LP) relaxation of the ILP for the master problem (ILP-MP).

Next, the while loop leverages CG to solve the problem (*Lines* 11-23). *Line* 12 solves the RMP, which can be done in polynomial-time with the ellipsoid algorithm [54]. Then, the for-loop covering *Lines* 13-18 generates a new column for each flow. Here, the ILP for the pricing problem (ILP-PP) is solved for each flow to get an objective value $\mathbb{Q}_i$ (*Line* 15), and we leverage the ILP-PP's solution to generate a new column for the flow (*Line* 16). *Line* 19 updates the RMP with the newly-generated columns, and *Lines* 20-22 check whether the minimum objective value of all the ILP-PPs is larger than or equal to zero. If yes, it means that the CG procedure cannot find a better solution with more iterations, and thus the while-loop of *Lines* 11-23 should be terminated. Finally, with the most updated column set $\{\mathcal{C}_i,\ \forall r_i \in \mathcal{R}\}$, *Lines* 24-25 get a near-optimal solution of the original problem.

### B. Representation of a Column

We introduce the following parameters to represent a column $c$, which is a feasible provisioning scheme of a flow $r_i \in \mathcal{R}$ (*i.e.*, including the related deployment of LCs and ECs and the flow's routing scheme over lightpaths).

**Parameters:**

- $x^{u,v}_{i,c,j,n}$: the boolean that equals 1, if the provisioning scheme in column $c$ shows that on node $u$, flow $r_i \in \mathcal{R}$ uses the $j$-th LC, which provides the $n$-th feasible capacity and originates a lightpath for $u$-$v$, and 0 otherwise.
- $y^{u,v}_{i,c,j,n}$: the boolean that equals 1, if the provisioning scheme in column $c$ shows that on node $u$, flow $r_i$ uses the $j$-th EC, which provides the $n$-th feasible capacity and connects to a lightpath for $u$-$v$, and 0 otherwise.
- $z^{u,v}_{i,c,j,n,j',n'}$: the boolean that equals 1, if column $c$ indicates that on node $u$, flow $r_i$ uses the $j$-th LC, which provides the $n$-th feasible capacity, and the $j'$-th EC, which provides the $n'$-th feasible capacity, and the LC and EC connect to a lightpath for $u$-$v$, and 0 otherwise.
- $b_{i,c}$: the integer that indicates the bandwidth usage of flow $r_i$ with the provisioning scheme in column $c$, in Gbps multiplying fiber hops.

### C. Master Problem

We decompose the original problem in Eqs. (1)-(20) into a master problem and a pricing problem. To reduce the time complexity of the problem-solving, we formulate the ILP model of the master problem (ILP-MP) as follows, to optimize the provisioning schemes of the flows in $\mathcal{R}$ within the solution space that only contains the existing columns ($\{\mathcal{C}_i,\ \forall r_i \in \mathcal{R}\}$).

**Variables:**

- $\lambda_{i,c}$: the boolean variable that equals 1 if flow $r_i$ uses the provisioning scheme depicted by $c \in \mathcal{C}_i$, and 0 otherwise.
- $f^{u,v}_{j,n}$, $g^{u,v}_{j,n}$ and $w^{u,v}_{j,n,j',n'}$: the boolean variables that still bear the definitions in the original ILP.

**Algorithm 1:** CG-based Approximation Algorithm

define the parameters to represent a column $c$;
decompose the ILP model in Eqs. (1)-(20) into a master problem and a pricing problem;
formulate the ILP model for master problem (ILP-MP);
formulate the ILP model for pricing problem (ILP-PP);
**for** each flow $r_i \in \mathcal{R}$ **do**
    $\mathcal{C}_i = \emptyset$;
    obtain a feasible provisioning scheme for $r_i$ with a heuristic, and generate a column $c$ for $r_i$ based on the provisioning scheme;
    insert $c$ into $\mathcal{C}_i$;
**end**
build the LP relaxation of ILP-MP with $\{\mathcal{C}_i,\ \forall r_i \in \mathcal{R}\}$ to get a RMP;
**while** TRUE **do**
    solve the RMP to obtain values of the primal and dual variables;
    **for** each flow $r_i \in \mathcal{R}$ **do**
        update the ILP-PP of $r_i$ based on RMP's solution;
        solve the ILP-PP to get an objective value $\mathbb{Q}_i$;
        generate a new column $c$ with ILP-PP's solution;
        insert $c$ into $\mathcal{C}_i$;
    **end**
    update the RMP with $\{\mathcal{C}_i,\ \forall r_i \in \mathcal{R}\}$;
    **if** $\min_{r_i \in \mathcal{R}}(\mathbb{Q}_i) \geq 0$ **then**
        **break**;
    **end**
**end**
use $\{\mathcal{C}_i,\ \forall r_i \in \mathcal{R}\}$ to build an ILP-MP;
solve the ILP-MP to obtain the final solution;

**Objective:**

The optimization objective is still to minimize the total cost from the used LCs, ECs, and bandwidth resources, but only with the existing columns, *i.e.*, $\{\mathcal{C}_i,\ \forall r_i \in \mathcal{R}\}$.

$$\begin{aligned}\text{Minimize}\quad & 2 \cdot \sum_{u,v \in V} \left( \sum_{n=1}^{|B^{\text{LC}}|} c_n^{\text{LC}} \cdot \sum_j f_{j,n}^{u,v} + \sum_{n=1}^{|B^{\text{EC}}|} c_n^{\text{EC}} \cdot \sum_j g_{j,n}^{u,v} \right) \\ & + \alpha \cdot \sum_{i}^{|\mathcal{R}|} \sum_{c \in \mathcal{C}_i} b_{i,c} \cdot \lambda_{i,c}.\end{aligned} \tag{21}$$

**Constraints:**

The constraints are listed as follows. For the constraints that are directly related to variables $\{\lambda_{i,c}\}$, we define their corresponding dual variables in "()", which provide the reduced cost on the objective in Eq. (21). We define negative dual variables for the constraints whose inequations have the relation of "$\leq$", and thus all the dual variables will not be smaller than 0.

$$\sum_{c \in \mathcal{C}_i} \lambda_{i,c} = 1, \quad \forall r_i \in \mathcal{R}, \quad (\varepsilon_i). \tag{22}$$

Eq. (22) ensures that each flow only uses the provisioning scheme described by one column.

$$\begin{aligned}\sum_{i=1}^{|\mathcal{R}|} \sum_{c \in \mathcal{C}_i} x_{i,c,j,n}^{u,v} \cdot b_i \cdot \lambda_{i,c} \leq b_n^{\text{LC}}, \quad \forall u,v \in V,\ j, \\ \forall n \in [1, |B^{\text{LC}}|], \quad (-\phi_{j,n}^{u,v}).\end{aligned} \tag{23}$$

$$\begin{aligned}\sum_{i=1}^{|\mathcal{R}|} \sum_{c \in \mathcal{C}_i} y_{i,c,j,n}^{u,v} \cdot b_i \cdot \lambda_{i,c} \leq b_n^{\text{EC}}, \quad \forall u,v \in V,\ j, \\ \forall n \in [1, |B^{\text{EC}}|], \quad (-\psi_{j,n}^{u,v}).\end{aligned} \tag{24}$$

Eqs. (23)-(24) ensure that the capacity constraint of each used LC and EC is satisfied.

$$\begin{aligned}\sum_{c \in \mathcal{C}_i} x_{i,c,j,n}^{u,v} \cdot \lambda_{i,c} \leq f_{j,n}^{u,v}, \quad \forall r_i \in \mathcal{R}, \forall u,v \in V,\ j, \\ \forall n \in [1, |B^{\text{LC}}|], \quad (-\chi_{i,j,n}^{u,v}),\end{aligned} \tag{25}$$

$$\sum_{j} \sum_{u \in V} f_{j,n}^{u,v} \leq M_n^{\text{LC}}, \quad \forall n \in [1, |B^{\text{LC}}|],\ \forall v \in V. \tag{26}$$

Eqs. (25)-(26) ensure that on each switch node, the number of used LCs, which provides the same feasible capacity, does not exceed the preset upper-limit.

$$\begin{aligned}\sum_{c \in \mathcal{C}_i} y_{i,c,j,n}^{u,v} \cdot \lambda_{i,c} \leq g_{j,n}^{u,v}, \quad \forall r_i \in \mathcal{R}, \forall u,v \in V,\ j, \\ \forall n \in [1, |B^{\text{EC}}|], \quad (-\varphi_{i,j,n}^{u,v}),\end{aligned} \tag{27}$$

$$\sum_{j} \sum_{u \in V} g_{j,n}^{u,v} \leq M_n^{\text{EC}}, \quad \forall n \in [1, |B^{\text{EC}}|],\ \forall v \in V. \tag{28}$$

Eqs.(27)-(28) ensure that on each switch node, the number of used ECs, which provides the same feasible capacity, does not exceed the preset upper-limit.

$$\begin{aligned}\sum_{i=1}^{|\mathcal{R}|} \sum_{c \in \mathcal{C}_i} z_{i,j,n,j',n'}^{u,v} \cdot \lambda_{i,c} \geq w_{j,n,j',n'}^{u,v}, \quad \forall u,v \in V, \\ \forall j,\ j',\ \forall n \in [1, |B^{\text{LC}}|],\ n' \in [1, |B^{\text{EC}}|], \quad (\tau_{j,n,j',n'}^{u,v}),\end{aligned} \tag{29}$$

$$\begin{aligned}\sum_{c \in \mathcal{C}_i} z_{i,j,n,j',n'}^{u,v} \cdot \lambda_{i,c} \leq w_{j,n,j',n'}^{u,v}, \quad \forall r_i \in \mathcal{R},\ \forall u,v \in V, \\ \forall j,\ j',\ \forall n \in [1, |B^{\text{LC}}|],\ n' \in [1, |B^{\text{EC}}|], \quad (-\xi_{i,j,n,j',n'}^{u,v}),\end{aligned} \tag{30}$$

$$\sum_{n'=1}^{|B^{\text{EC}}|} \sum_{j'} w_{j,n,j',n'}^{u,v} \cdot b_{n'}^{\text{EC}} \leq b_n^{\text{LC}},\ \forall u,v \in V,\ \forall j,\ n \in [1, |B^{\text{LC}}|], \tag{31}$$

$$\sum_{n=1}^{|B^{\text{LC}}|} \sum_{j} w_{j,n,j',n'}^{u,v} \leq 1, \quad \forall u,v \in V,\ j',\ n' \in [1, |B^{\text{EC}}|]. \tag{32}$$

Eqs. (29)-(32) ensure that the total capacity of the ECs, which connect to a same LC, does not exceed the capacity of the LC, and if an EC is used by one or more flows, these flows have to be assigned to a same LC.

### D. Pricing Problem

In *Algorithm* 1, we try to reduce the total cost in Eq. (21) by solving the ILP of the pricing problem (ILP-PP) for each flow. If this can be achieved, there is at least one objective value $\mathbb{Q}_i < 0$. Then, we get $|\mathcal{R}|$ new columns based on the solutions of the ILP-PPs, which will be inserted into the existing columns ($\{\mathcal{C}_i,\ \forall r_i \in \mathcal{R}\}$). Otherwise, the iterations in the CG should be terminated. Based on these considerations, we design the ILP-PP of each flow $r_i \in \mathcal{R}$ as follows.

**Variables:**

- $\gamma_i^{u,v}$, $\vartheta_{i,k}^{u,v}$, $x_{i,j,n}^{u,v}$, $y_{i,j,n}^{u,v}$, and $z_{i,j,n,j',n'}^{u,v}$: the boolean variables that still bear the definitions in the original ILP.

The relations between these variables and the parameters defined to represent a column $c$ (*i.e.*, $x_{i,c,j,n}^{u,v}$, $y_{i,c,j,n}^{u,v}$, $z_{i,c,j,n,j',n'}^{u,v}$, and $b_{i,c}$) are as follows.

$$x_{i,c,j,n}^{u,v} = x_{i,j,n}^{u,v}, \quad \forall r_i \in \mathcal{R},\ u,v \in V,\ j,\ n \in [1, |B^{\text{LC}}|], \tag{33}$$

$$y_{i,c,j,n}^{u,v} = y_{i,j,n}^{u,v}, \quad \forall r_i \in \mathcal{R},\ u,v \in V,\ j,\ n \in [1, |B^{\text{EC}}|], \tag{34}$$

$$\begin{aligned} z_{i,c,j,n,j',n'}^{u,v} = z_{i,j,n,j',n'}^{u,v}, \quad & \forall r_i \in \mathcal{R},\ u,v \in V, \\ & \forall j,\ j',\ \forall n \in [1, |B^{\text{LC}}|],\ n' \in [1, |B^{\text{EC}}|], \end{aligned} \tag{35}$$

Eqs. (33)-(35) ensure that in each iteration of the CG, we only consider one provisioning scheme of each flow $r_i \in \mathcal{R}$.

$$b_{i,c} = \sum_{u,v \in V} \sum_{k=1}^{K} \vartheta_{i,k}^{u,v} \cdot h_k^{u,v} \cdot b_i, \quad \forall r_i \in \mathcal{R}. \tag{36}$$

Eq. (36) gets the bandwidth usage of flow $r_i$ with the provisioning scheme in column $c$, in Gbps multiplying fiber hops.

**Objective:**

Based on the relations between the primal and dual problems, the reduced cost achieved by $\lambda_{i,c}$ for each flow $r_i \in \mathcal{R}$ can be calculated as

$$\begin{aligned} & \alpha \cdot b_{i,c} - \varepsilon_i + \sum_{u,v \in V} \sum_{j,n} \left(\phi_{j,n}^{u,v} \cdot b_i + \chi_{i,j,n}^{u,v}\right) \cdot x_{i,c,j,n}^{u,v} \\ & + \sum_{u,v \in V} \sum_{j,n} \left(\psi_{j,n}^{u,v} \cdot b_i + \varphi_{i,j,n}^{u,v}\right) \cdot y_{i,c,j,n}^{u,v} \\ & + \sum_{u,v \in V} \sum_{j,n} \sum_{j',n'} \left(\xi_{i,j,n,j',n'}^{u,v} - \tau_{j,n,j',n'}^{u,v}\right) \cdot z_{i,c,j,n,j',n,}^{u,v}. \end{aligned} \tag{37}$$

Then, by putting Eqs. (33)-(36) into (37), we can get the objective of the pricing problem as

$$\begin{aligned} \text{Minimize} \quad \mathbb{Q}_i = & \alpha \cdot \sum_{u,v \in V} \sum_{k} \vartheta_{i,k}^{u,v} \cdot h_k^{u,v} \cdot b_i - \varepsilon_i \\ & + \sum_{u,v \in V} \sum_{j,n} \beta_{i,j,n}^{u,v} \cdot x_{i,j,n}^{u,v} + \sum_{u,v \in V} \sum_{j,n} \hat{\beta}_{i,j,n}^{u,v} \cdot y_{i,j,n}^{u,v} \\ & + \sum_{u,v \in V} \sum_{j,n} \sum_{j',n'} \tilde{\beta}_{i,j,n,j',n'}^{u,v} \cdot z_{i,j,n,j',n'}^{u,v}, \end{aligned} \tag{38}$$

where we simplify the expression with the following notations

$$\begin{cases} \beta_{i,j,n}^{u,v} = \phi_{j,n}^{u,v} \cdot b_i + \chi_{i,j,n}^{u,v}, \\ \hat{\beta}_{i,j,n}^{u,v} = \psi_{j,n}^{u,v} \cdot b_i + \varphi_{i,j,n}^{u,v}, \\ \tilde{\beta}_{i,j,n,j',n'}^{u,v} = \xi_{i,j,n,j',n'}^{u,v} - \tau_{j,n,j',n'}^{u,v}. \end{cases} \tag{39}$$

**Constraints:**

The ILP-PP reuses the constraints in Eqs. (2)-(4), (9), and (14)-(16) defined in the original ILP. Additionally, we define the following constraints to ensure that the capacity constraint of each used LC and EC is satisfied.

$$b_i \cdot x_{i,j,n}^{u,v} \le b_n^{\text{LC}}, \quad \forall r_i \in R,\ u,v \in V,\ j,\ n \in [1, |B^{\text{LC}}|], \tag{40}$$

$$b_i \cdot y_{i,j,n}^{u,v} \le b_n^{\text{EC}}, \quad \forall r_i \in R,\ u,v \in V,\ j,\ n \in [1, |B^{\text{EC}}|]. \tag{41}$$

Finally, by double-checking the ILP-PP, we can see that it is essential to find the least-cost lightpath routing scheme for each flow, provided that the LC and EC deployments have been determined in advance. This is equivalent to finding the least-weighted routing path in a weighted graph, which can be solved exactly by leveraging the well-known Dijkstra algorithm with linear time complexity. Therefore, the time complexity of *Algorithm* 1 can be further reduced by using the Dijkstra algorithm to solve the optimization in ILP-PP in *Line* 15, instead of solving the ILP-PP directly.

### E. Complexity Analysis and Approximation Ratio

According to the principle of CG, the maximum number of iterations that the while-loop of *Lines* 11-22 in *Algorithm* 1 needs to run is finite [31], and it can be denoted as $I_{\max}$. Note that, the actual value of $I_{\max}$ is normally two to several hundred, and we will discuss it with the simulations in the next section. Hence, *Lines* 1-23 in *Algorithm* 1 can be accomplished in polynomial-time. This is because all the major steps in it can be finished in polynomial-time. For instance, solving the LP relaxation of ILP-MP in *Line* 12 can be done in polynomial-time [54], and the ILP-PP can be solved exactly by leveraging the Dijkstra algorithm whose time complexity is $O(V^2)$. *Algorithm* 1 needs to solve the ILP-MP in *Line* 24, which is the only part in the algorithm that might not be accomplished in polynomial-time. Nevertheless, compared with the original ILP in Section IV, the ILP-MP is much more compact. Specifically, the original ILP has much more constraints and variables than the ILP-MP, and the differences on constraints and variables are $(4 \cdot |\mathcal{R}| \cdot |V| + (2 + |B^{\text{LC}}| + |B^{\text{EC}}| + |B^{\text{LC}}| \cdot |B^{\text{EC}}|) \cdot |\mathcal{R}| \cdot |V|^2)$ and $((1+K) \cdot |\mathcal{R}| \cdot |V|^2 + (|B^{\text{LC}}| + |B^{\text{EC}}| + |B^{\text{LC}}| \cdot |B^{\text{EC}}|) \cdot |\mathcal{R}| \cdot |V|^2 - |\mathcal{R}| \cdot |\mathcal{C}_i|)$, respectively. These differences make sure that the ILP-MP can be solved much more time-efficiently than the original ILP. In the next section, we will use simulations to further investigate the time-complexity of *Algorithm* 1.

With the final integer solution provided by *Algorithm* 1 and the real number solution of the corresponding LP relaxation, we can calculate the objective values with Eq. (1) and denote them as $\Phi$ and $\Phi_{\text{LP}}$, respectively.

**Theorem 2.** Algorithm *1 is an approximation algorithm for the security-aware multilayer planning problem defined with the ILP in Section IV, and its approximation ratio is upper-bounded by* $\frac{\Phi - \Phi_{LP}}{\Phi_{LP}}$.

*Proof:* We first assume that the objective value calculated with the exact solution of the ILP is $\Phi^*$. As the original problem is for minimization, the objective value from the LP relaxation of ILP-MP (*i.e.*, $\Phi_{\text{LP}}$) provides a lower-bound on $\Phi^*$. Meanwhile, the solution from *Algorithm* 1 is feasible for

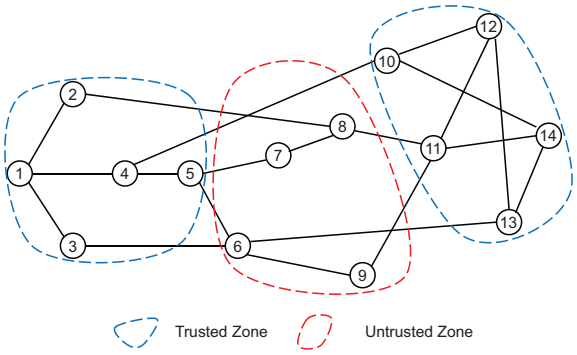


Fig. 3. NSFNET topology considered in simulations.

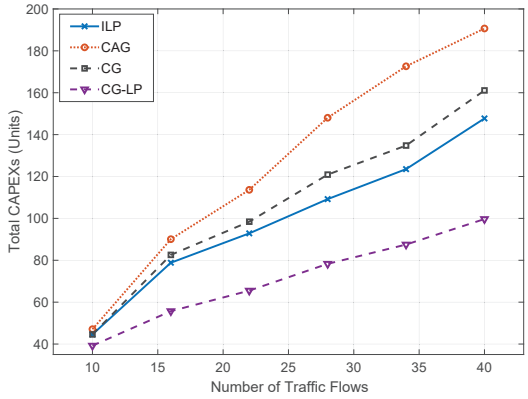


Fig. 4. Results on total CAPEX with six-node topology.

the original problem, and thus $\Phi$ gives an upper-bound on $\Phi^*$. The approximation ratio of *Algorithm* 1 can be computed as

$$\eta = \frac{\Phi - \Phi^*}{\Phi^*} \leq \frac{\Phi - \Phi_{\text{LP}}}{\Phi_{\text{LP}}}, \tag{42}$$

which proves the upper-bound of the approximation ratio. ■

## VI. Performance Evaluations and Discussions

In this section, we use numerical simulations to evaluate the performance of our proposed algorithms.

### A. Simulation Setup

Our simulations consider two physical topologies, *i.e.*, a small six-node one as shown in Fig. 2 and the NSFNET topology in Fig. 3. We evaluate three algorithms, which are 1) the one that directly solves the ILP model in Section IV, 2) the CG-based approximation algorithm, and 3) a heuristic that is developed by modifying the collapsed auxiliary graph (CAG) based algorithm in [30] and making it adapt to the network model of this work. Specifically, the CAG-based heuristic serves flows in descending order of their bandwidth demands, while for each flow, it first builds a CAG based on the current network status, and then based on the CAG, it deploys LCs/ECs for the flow and finalizes the flow's provisioning scheme. All the three algorithms are compared with the small-scale topology, while due to the time complexity of solving the ILP directly, we do not run it with the NSFNET topology.

According to [22], we assume that the feasible capacities of LCs and ECs are $B^{\text{LC}} = B^{\text{EC}} = \{40, 100, 400\}$ Gbps, while the unit costs of corresponding LCs and ECs are $\{1, 2, 4\}$ and $\{2, 4, 8\}$, respectively. The largest numbers of LCs and ECs that can be deployed on each switch node are assumed to be within $[2, 8]$, depending on the traffic conditions. For each flow $r_i$, its source $s_i$ and destination $d_i$ are randomly selected, and bandwidth demand $b_i$ uniformly distributes within $[25, 200]$ Gbps. We set $\alpha = 0.01$ in the objective in Eq. (1) to balance the importance of the cost of LCs and ECs and that of bandwidth resources[5]. To ensure the statistical accuracy of the simulations, we get each data point by averaging the results from 10 independent runs. The simulations are carried out on a computer with 4.00 GHz Intel i7-6700K CPU and 64 GB memory, and we implement the algorithms with C++ and use the Gurobi toolbox [55] to solve the ILP and CG models.

[5]Note that, due to the lack of necessary information, we cannot get the costs of LCs, ECs and bandwidth resources in reality. However, as our optimization only uses them as parameters, its performance will not be affected by them, *i.e.*, it can minimize the total CAPEX of the network planning for an arbitrary setting of the costs. We also hope to point out that in real-world networks, the cost of the service on an LC might depend not only on the service's data-rate but also on the LC's line-rate. However, for simplicity, we assume that the service cost is independent of an LC's line-rate in this work.

### B. Small-scale Tests

The small-scale tests use the six-node topology as the physical topology, where the trusted and untrusted zones are shown in Fig. 2. We randomly select $20\%$ of the flows in $\mathcal{R}$ and mark them as sensitive flows ($R_{\text{S}}$), while the remaining ones are non-sensitive ($R_{\text{NS}}$). Fig. 4 plots the results on total CAPEX from the three algorithms, and there are two curves for the CG, which are "CG" and "CG-LP". Here, CG refers to the final solution from the CG model, while CG-LP stands for the solution of the RMP, *i.e.*, the lower-bound on the optimal solution. We can see that when the number of traffic flows is as small as 10, all the algorithms perform similarly, but when the number of flows increases, CG still outputs the results that can approximate the optimal ones provided by ILP, and has more distinct advantages over CAG. This is because CAG, as a heuristic, can easily be trapped by local optima when the problem's scale becomes larger, and thus cannot follow the trend of ILP as CG does. Because CG-LP only provides a lower-bound on the total CAPEX but its solution is not a feasible one to the original problem, the solution of ILP is always in between those of CG and CG-LP. In other words, the gaps between the results of CG and CG-LP are always larger than those of CG and ILP, which satisfy the approximation ratio derived in Eq. (42). Hence, we can use CG-LP as a baseline to evaluate CG when ILP becomes intractable to solve the optimization in large-scale topologies.

Table I lists the running time of the algorithms. As expected, CAG is the most time-efficient one. It can be seen that the running time of ILP is shorter than CG when the number of flows is 16 or less. This is because the ILP can be directly solved in one shot, while CG runs in iterations to approximate the optimal solution. However, when the number of flows keeps increasing, the running time of ILP increases much faster than that of CG, and becomes more than one magnitude longer when we have $|\mathcal{R}| = 40$ flows to plan.

TABLE I
AVERAGE RUNNING TIME PER FLOW WITH SIX-NODE TOPOLOGY (SECONDS)

| Number of Flows ($\|\mathcal{R}\|$) | CAG | CG-LP | CG | ILP |
|---|---|---|---|---|
| 10 | 0.0035 | 0.1279 | 0.1298 | 0.5025 |
| 16 | 0.0023 | 0.1266 | 0.1311 | 0.7438 |
| 22 | 0.0020 | 0.1483 | 0.1544 | 1.5500 |
| 28 | 0.0019 | 0.1799 | 0.1816 | 6.7366 |
| 34 | 0.0021 | 0.2124 | 0.2607 | 8.4018 |
| 40 | 0.0027 | 0.2278 | 0.2714 | 56.0494 |

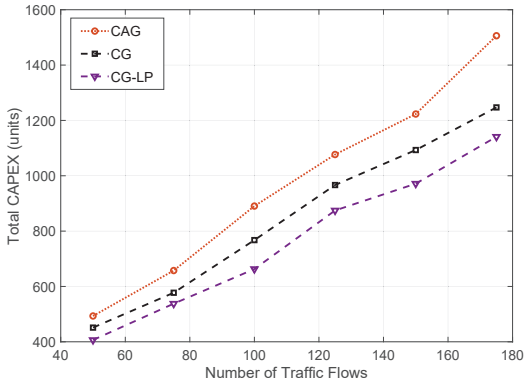


Fig. 5. Results on total CAPEX with NSFNET topology.

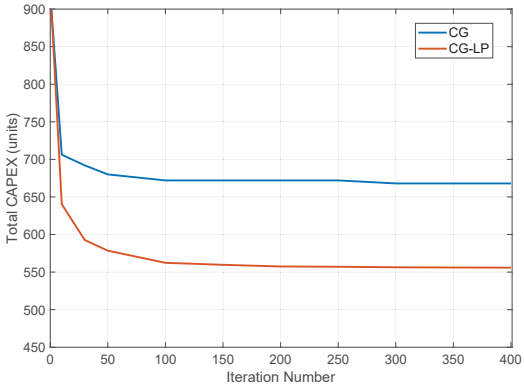


Fig. 6. Convergence performance of CG with NSFNET topology ($\mathcal{R} = 100$).

TABLE II
AVERAGE RUNNING TIME PER FLOW WITH NSFNET TOPOLOGY (SECONDS)

| Number of Flows ($\|\mathcal{R}\|$) | CAG | CG-LP | CG |
|---|---|---|---|
| 50 | 0.108 | 1.272 | 1.282 |
| 75 | 0.122 | 1.837 | 1.896 |
| 100 | 0.105 | 2.355 | 2.684 |
| 125 | 0.106 | 3.840 | 4.596 |
| 150 | 0.104 | 4.677 | 5.486 |
| 175 | 0.102 | 5.215 | 5.623 |

### C. Large-scale Tests

We then use the NSFNET topology in Fig. 3, where the untrusted zone consists of 10 fiber links, to evaluate the algorithms with problems whose sizes are relatively large. The ratio of sensitive flows ($R_{\mathrm{S}}$) in $\mathcal{R}$ is still $20\%$, while the remaining $80\%$ are non-sensitive ones ($R_{\mathrm{NS}}$).

Fig. 5 shows the results on the total CAPEX, which indicates that the results of CG are still always smaller than those of CAG, as the number of flows increases. According to Eq. (42), the upper-bound of the CG's approximation ratio can be obtained by checking the gaps between the results of CG and CG-LP. The convergence performance of CG for the case where there are $|\mathcal{R}| = 100$ flows is shown in Fig. 6, which indicates that CG converges quickly after $\sim$100 iterations and the approximation ratio is $\eta \leq 20\%$.

Meanwhile, we have to admit that the superior performance of CG is obtained at the expense of increased time complexity. Table II lists the running time of the algorithms, and because the scale of the problem becomes much larger in the NSFNET topology, CG takes more time to converge and deliver an approximation solution. Although the running time of CG is longer than that of CAG, it is still relatively short and thus is acceptable for our network planning problem. In the meantime, the results in Fig. 5 indicate that when the scale of the network planning problem increases, CG can still get a reasonably good approximation ratio. Therefore, with the results in Fig. 5 and Table II, we can conclude that our CG-based approximation algorithm has reasonably good scalability.

To further analyze the performance of CG, we plot the total costs of LCs and ECs in Fig. 7. It can be seen that when the number of flows increases, both of the algorithms need to use more LCs and ECs to ensure effective traffic grooming and routing, but CG can always use smaller numbers of LCs and ECs to serve all the flows. We then fix the number of flows as $|\mathcal{R}| = 50$ but change the proportion of sensitive flows in $\mathcal{R}$ to evaluate the algorithms in more aspects. Fig. 8 shows how the total CAPEX and total cost of ECs and LCs change with the proportion of sensitive flows. To plan more sensitive flows, the algorithms need to deploy more ECs and LCs to ensure the security requirements, but CG makes better decisions on traffic grooming and thus can provide smaller costs on them.

Finally, we hope to point out that results on total CAPEX in Fig. 5 already show the gap between CAG and CG increasing with the number of flows to plan. This suggests that as a heuristic, CAG cannot ensure a bounded performance gap to the exact solution. To further verify this claim, we set up simulations to make more flows share the same source-

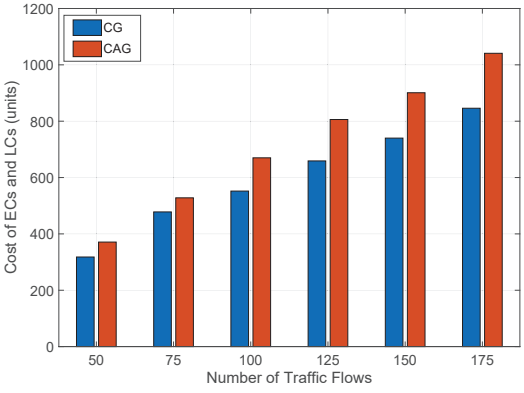


Fig. 7. Results on total cost of ECs and LCs with NSFNET topology.

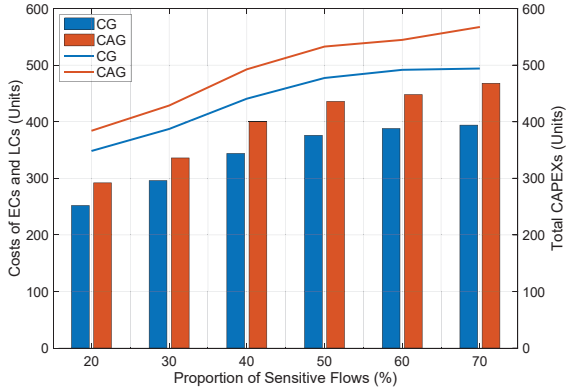


Fig. 8. Results on total CAPEX and cost of ECs and LCs ($|\mathcal{R}| = 50$).

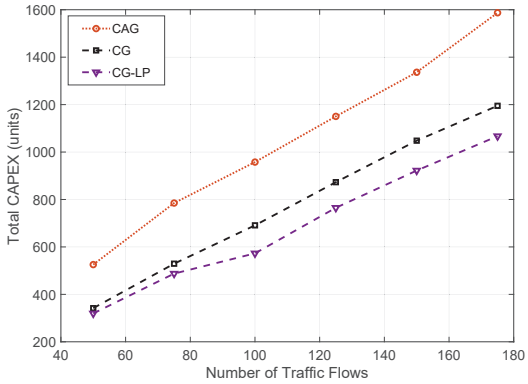


Fig. 9. Results on total CAPEX with NSFNET topology (special spatial distribution of flows).

destination pairs, and plot the results on total CAPEX in Fig. 9. It can be seen that with this special spatial distribution of flows, the gaps between CAG and CG are much larger than those in Fig. 5, while the gaps between CG and CG-LP stay almost unchanged. Therefore, although CAG has the advantage on time complexity, its gap to the exact solution is divergent and thus cannot deliver any performance guarantee. Meanwhile, we hope to point out that the time-efficiency of CG can be further improved if we simplify the formulations of the ILP and CG, which will be considered in our future work.

## VII. Conclusion

In this paper, we studied the problem of security-aware multilayer network planning in consideration of OTN encryption, for architecting secure packet-over-optical networks. We first formulated an ILP model to solve the problem exactly. Then, to reduce the time complexity, we proposed a CG model and developed an approximation algorithm based on it. Simulation results showed that our CG-based approximation algorithm is much more time-efficient than solving the ILP directly, and it also outperforms the existing CAG-based heuristic in terms of total CAPEX and costs of used LCs and ECs.

## Acknowledgments

This work was supported in part by the NSFC projects 61871357, Zhejiang Lab Research Fund 2019LE0AB01, and SPR Program of CAS (XDC02070300).

## References

[1] W. Lu *et al.*, "AI-assisted knowledge-defined network orchestration for energy-efficient data center networks," *IEEE Commun. Mag.*, vol. 58, pp. 86–92, Jan. 2020.

[2] Z. Zhu, S. Li, and X. Chen, "Design QoS-aware multi-path provisioning strategies for efficient cloud-assisted SVC video streaming to heterogeneous clients," *IEEE Trans. Multimedia*, vol. 15, pp. 758–768, Jun. 2013.

[3] P. Lu *et al.*, "Highly efficient data migration and backup for Big Data applications in elastic optical inter-data-center networks," *IEEE Netw.*, vol. 29, pp. 36–42, Sept. 2015.

[4] W. Fang *et al.*, "Joint spectrum and IT resource allocation for efficient vNF service chaining in inter-datacenter elastic optical networks," *IEEE Commun. Lett.*, vol. 20, pp. 1539–1542, Aug. 2016.

[5] L. Paraschis *et al.*, "System innovations in open WDM DCI networks," *Photon. Netw. Commun.*, vol. 40, pp. 269–280, Dec. 2020.

[6] Z. Zhu *et al.*, "Demonstration of cooperative resource allocation in an OpenFlow-controlled multidomain and multinational SD-EON testbed," *J. Lightw. Technol.*, vol. 33, pp. 1508–1514, Apr. 2015.

[7] M. Filer *et al.*, "Low-margin optical networking at cloud scale," *J. Opt. Commun. Netw.*, vol. 11, pp. C94–C108, Oct. 2019.

[8] C. Xie *et al.*, "Open and disaggregated optical transport networks for data center interconnects," *J. Opt. Commun. Netw.*, vol. 12, pp. C12–C22, Jun. 2020.

[9] M. Newland *et al.*, "Open optical communication systems at a hyperscale operator," *J. Opt. Commun. Netw.*, vol. 12, pp. C50–C57, Jun. 2020.

[10] Z. Zhu *et al.*, "Jitter and amplitude noise accumulations in cascaded all-optical regenerators," *J. Lightw. Technol.*, vol. 26, pp. 1640–1652, Jun. 2008.

[11] M. Fok, Z. Wang, Y. Deng, and P. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensic Secur.*, vol. 6, pp. 725–736, Sept. 2011.

[12] 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.

[13] 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.

[14] 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.

[15] B. Li, W. Lu, and Z. Zhu, "Deep-NFVOrch: Leveraging deep reinforcement learning to achieve adaptive vNF service chaining in EON-DCIs," *J. Opt. Commun. Netw.*, vol. 12, pp. A18–A27, Jan. 2020.

[16] 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.

[17] L. Gong and Z. Zhu, "Virtual optical network embedding (VONE) over elastic optical networks," *J. Lightw. Technol.*, vol. 32, pp. 450–460, Feb. 2014.

[18] L. Gong, H. Jiang, Y. Wang, and Z. Zhu, "Novel location-constrained virtual network embedding (LC-VNE) algorithms towards integrated node and link mapping," *IEEE/ACM Trans. Netw.*, vol. 24, pp. 3648–3661, Dec. 2016.

[19] M. Zeng, W. Fang, and Z. Zhu, "Orchestrating tree-type VNF forwarding graphs in inter-DC elastic optical networks," *J. Light. Technol.*, vol. 34, pp. 3330–3341, Jul. 2016.

[20] Y. Wang, P. Lu, W. Lu, and Z. Zhu, "Cost-efficient virtual network function graph (vNFG) provisioning in multidomain elastic optical networks," *J. Lightw. Technol.*, vol. 35, pp. 2712–2723, Jul. 2017.

[21] J. Ceballos, R. DiPasquale, and R. Feldman, "Business continuity and security in datacenter interconnection," *Bell Labs Tech. J.*, vol. 17, pp. 147–155, Dec. 2012.

[22] K. Guan, J. Kakande, and J. Cho, "On deploying encryption solutions to provide secure transport-as-a-service (TaaS) in core and metro networks," in *Proc. of ECOC 2016*, pp. 1–3, Sept. 2016.

[23] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, pp. 110–117, Aug. 2016.

[24] N. Skorin-Kapov, J. Chen, and L. Wosinska, "A new approach to optical networks security: Attack-aware routing and wavelength assignment," *IEEE/ACM Trans. Netw.*, vol. 18, pp. 750–760, Jun. 2010.

[25] M. Furdek, N. Skorin-Kapov, and M. Grbac, "Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation," *J. Opt. Commun. Netw.*, vol. 2, pp. 1000–1009, Nov. 2010.

[26] S. Yuan and D. Stewart, "Protection of optical networks against inter-channel eavesdropping and jamming attacks," in *Proc. of CSCI 2014*, pp. 34–38, Mar. 2014.

[27] J. Zhu, B. Zhao, and Z. Zhu, "Leveraging game theory to achieve efficient attack-aware service provisioning in EONs," *J. Lightw. Technol.*, vol. 35, pp. 1785–1796, May 2017.

[28] J. Zhu and Z. Zhu, "Physical-layer security in MCF-based SDM-EONs: Would crosstalk-aware service provisioning be good enough?" *J. Lightw. Technol.*, vol. 35, pp. 4826–4837, Nov. 2017.

[29] X. Jin, W. Lu, S. Liu, and Z. Zhu, "On multi-layer restoration in optical networks with encryption solution deployment," in *Proc. of OFC 2018*, pp. 1–3, Mar. 2018.

[30] M. Song, J. Zhu, F. Zhou, and Z. Zhu, "On security-aware multilayer planning for IP-over-optical networks with OTN encryption," in *Proc. of ICC 2020*, pp. 1–6, Jun. 2020.

[31] J. Desrosiers and M. Lübbecke, *A primer in column generation*. Springer, 2005.

[32] Z. Pan *et al.*, "Advanced optical-label routing system supporting multicast, optical TTL, and multimedia applications," *J. Lightw. Technol.*, vol. 23, pp. 3270–3281, Oct. 2005.

[33] Z. Zhu *et al.*, "RF photonics signal processing in subcarrier multiplexed optical-label switching communication systems," *J. Lightw. Technol.*, vol. 21, pp. 3155–3166, Dec. 2003.

[34] Z. Pan *et al.*, "Demonstration of variable-length packet contention resolution and packet forwarding in an optical-label switching router," *IEEE Photon. Technol. Lett.*, vol. 16, pp. 1772–1774, Jul. 2004.

[35] M. Ruiz *et al.*, "Survivable IP/MPLS-over-WSON multilayer network optimization," *J. Opt. Commun. Netw.*, vol. 3, pp. 629–640, Aug. 2011.

[36] V. Gkamas, K. Christodoulopoulos, and E. Varvarigos, "A joint multi-layer planning algorithm for IP over flexible optical networks," *J. Light. Technol.*, vol. 33, pp. 2965–2977, Jul. 2015.

[37] P. Lu and Z. Zhu, "Data-oriented task scheduling in fixed- and flexible-grid multilayer inter-DC optical networks: A comparison study," *J. Lightw. Technol.*, vol. 35, pp. 5335–5346, Dec. 2017.

[38] S. Liu, W. Lu, and Z. Zhu, "On the cross-layer orchestration to address IP router outages with cost-efficient multilayer restoration in IP-over-EONs," *J. Opt. Commun. Netw.*, vol. 10, pp. A122–A132, Jan. 2018.

[39] W. Lu, X. Yin, X. Cheng, and Z. Zhu, "On cost-efficient integrated multilayer protection planning in IP-over-EONs," *J. Lightw. Technol.*, vol. 36, pp. 2037–2048, May 2018.

[40] J. Yao, P. Lu, L. Gong, and Z. Zhu, "On fast and coordinated data backup in geo-distributed optical inter-datacenter networks," *J. Lightw. Technol.*, vol. 33, pp. 3005–3015, Jul. 2015.

[41] X. Xie *et al.*, "Evacuate before too late: Distributed backup in inter-DC networks with progressive disasters," *IEEE Trans. Parallel Distrib. Syst.*, 2018.

[42] 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.

[43] 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.

[44] V. Dukic *et al.*, "Beyond the mega-data center: networking multi-data center regions," in *Proc. of SIGCOMM 2020*, pp. 765–781, Aug. 2016.

[45] "Wavelogic encryption," (Accessed on May 11, 2021). [Online]. Available: https://www.ciena.com/products/wavelogic/wavelogic-encryption/.

[46] M. Ruiz *et al.*, "Column generation algorithm for RSA problems in flexgrid optical networks," *Photon. Netw. Commun.*, vol. 26, pp. 53–64, Mar. 2013.

[47] L. Velasco, A. Castro, M. Ruiz, and G. Junyent, "Solving routing and spectrum allocation related optimization problems: From off-line to in-operation flexgrid network planning," *J. Light. Technol.*, vol. 32, pp. 2780–2795, Aug. 2014.

[48] J. Liu *et al.*, "On dynamic service function chain deployment and readjustment," *IEEE Trans. Netw. Serv. Manag.*, vol. 14, no. 3, pp. 543–553, Sept. 2017.

[49] F. Zhou, M. Ju, and A. Ait-Ouahmed, "Joint optimization for multicast provisioning in mixed-line-rate optical networks with a column generation approach," *J. Light. Technol.*, vol. 36, pp. 637–649, Feb. 2018.

[50] "High-capacity wire-speed encryption modules for the 6500 packet-optical platform," (Accessed on Feb. 1, 2021). [Online]. Available: https://www.ciena.com/products/high-capacity-wire-speed-encryption-modules/.

[51] "mTera ODU payload encryption: Wire-speed encryption with the flexibility of universal switching," (Accessed on Feb. 1, 2021). [Online]. Available: https://www.infinera.com/wp-content/uploads/mTera-ODU-Payload-Encryption-0008-AN-RevA-0419.pdf.

[52] M. Garey and D. Johnson, *Computers and Intractability: a Guide to the Theory of NP-Completeness*. W. H. Freeman & Co. New York, 1979.

[53] S. Martello and P. Toth, "Lower bounds and reduction procedures for the bin packing problem," *Discrete Appl. Math.*, vol. 28, pp. 59–70, Jul. 1990.

[54] D. Goldfarb and M. Todd, "Modifications and implementation of the ellipsoid algorithm for linear programming," *Math. Program.*, vol. 23, pp. 1–19, Dec. 1982.

[55] "Gurobi optimizer reference manual," (Accessed on Jul. 1, 2020). [Online]. Available: http://www.gurobi.com.