On Security-aware Multilayer Planning for IP-over-Optical Networks with OTN Encryption

Man Song[1], Jing Zhu[1], Fen Zhou[2], Zuqing Zhu[1,†]
[1]School of Information Science and Technology, University of Science and Technology of China, Hefei, China
[2]LISITE lab, Institut Superieur d'Electronique de Paris, France
[†]Email: {zqzhu}@ieee.org

***Abstract*—We study how to achieve cost-effective and security-aware multilayer planning for an optical transport network (OTN) that covers both trusted and untrusted zones and has the option to choose encryption solution deployment (ESD) architectures based on traffic condition. We first formulate an integer linear programming (ILP) model to solve the optimization exactly, and then propose a novel heuristic based on collapsed auxiliary graphs (CAGs) to have improved time-efficiency.**

***Index Terms*—Multilayer network planning, Optical transport networking (OTN), OTN encryption, Physical-layer security.**

I. Introduction

Nowadays, the rapid development of cloud computing has accelerated global deployment of datacenters (DCs) and their interconnect networks (*i.e.*, DCIs). Consequently, as the only viable physical infrastructure for DCIs, optical networks are undergoing notable changes to address the new challenges [1]. Meanwhile, when laying out a DCI, one should never neglect the vulnerabilities in the optical layer. This is because wire-tapping that is hard to detect can be easily realized by leveraging them [2], while data transferred in DCIs can be sensitive and valuable such that data leakage will cause unimaginable losses to DC operators and their clients [3].

To address the physical-layer vulnerabilities, people have developed OTN encryption technologies that can directly encrypt data in OTN payload frames and achieve low processing latency and small encryption overhead. Moreover, OTN encryption can benefit from the grooming capability of OTN switching fabric, thereby improving the utilization of expensive lines and encryption equipment, and reducing the complexity of key management. Then, three architectures, which organize the OTN switches/linecards (LCs) and encryption cards (ECs) to realize different cross-layer traffic grooming and wavelength routing scenarios, have been evaluated for encryption solution deployment (ESD) [4]. The results from these studies suggested that the architectures' performance on equipment cost and resource utilization can be significantly affected by the volume, granularity and distribution of the traffic in an OTN, and there might not be a universal winner. Hence, security-aware multilayer network planning for OTNs with ESD deserves further investigation to consider the situation where an OTN adaptively uses the three architectures discussed in [4] based on its traffic condition.

Note that, with ESD, the multilayer planning for an OTN (*i.e.*, the cross-layer traffic grooming and wavelength routing) becomes much more complex such that the algorithms designed for conventional OTNs will be inapplicable. This is because ESD adds another layer of operation (as shown in Fig. 1), and the operation sequence (*i.e.*, whether the traffic flows should be groomed before being encrypted or the other way around) would be flexible if the three architectures can be used simultaneously. Also, the security-aware multilayer planning should be further generalized to consider the situation in which the OTN of an DCI covers a relatively large geographical area [5] including both trusted and untrusted zones. However, to the best of our knowledge, such a multilayer planning problem has not been studied in the literature before.

In this paper, we study how to achieve cost-effective and security-aware multilayer planning for an OTN that covers both trusted and untrusted zones and has the option to choose ESD architectures based on traffic condition. Specifically, we first lay out the network model and formulate an integer linear programming (ILP) model to optimize the security-aware multilayer planning exactly, and then propose a novel heuristic based on collapsed auxiliary graphs to solve the problem time-efficiently. Simulation results suggest that our proposed algorithms can achieve cost-effective multilayer planning.

The rest of the paper is organized as follows. Section II gives a brief survey on the related work. We lay out the network model of security-aware multilayer planning for OTNs with ESD and formulate the ILP model to optimize it in Section III. The time-efficient heuristic is described in Section IV, and we discuss the performance evaluation with numerical simulations in Section V. Finally, Section VI summarizes the paper.

II. Related Work

To adapt to its traffic demands, a DCI is normally an "IP-over-OTN" [3]. Therefore, its network planning should groom the traffic flows from the IP layer, plan lightpaths to carry the aggregated traffic, and calculate wavelength routing for the lightpaths. To tackle this problem, previous studies have considered various OTN technologies and traffic demand types [6–8]. Nevertheless, as they did not address physical-layer security or take ESD into consideration, their multilayer planning algorithms are not security-aware.

According to [2], optical networks are vulnerable to physical layer attacks. For instance, eavesdropping can be easily realized by tapping into an optical fiber directly or bending it to collect the leaked optical signal [9]. Previously, people

have proposed a few security-aware planning algorithms to design the routing and spectrum assignment (RSA) schemes of lightpaths such that the adverse impacts of physical-layer vulnerabilities can be minimized [9–11]. However, they only planned the optical layer, and without ESD, their proposals cannot rule out the possibility of data leakage. Moreover, as security-aware RSA has to bypass certain fiber links and/or reserve large spectral guard-bands, unwanted spectrum waste (*e.g.*, spectrum fragmentation [11–13]) would be inevitable. Hence, ESD might be more realistic [3]. The studies in [4, 14] analyzed three ESD architectures, for normal service provisioning and multilayer restoration, respectively. Nevertheless, they did not optimize the security-aware multilayer planning or consider the practical situation in which an OTN covers trusted/untrusted zones and have no flexibility to choose ESD architectures based on traffic condition.

III. Problem Formulation

A. Network Model

Fig. 1 provides an illustrative example on the security-aware multilayer planning in an OTN with ESD. Specifically, the network planning provisions a set of traffic flows (*i.e.*, $\{r_i,\ i \in [1,9]\}$ in Fig. 1) from the IP layer in the OTN with cross-layer traffic grooming and wavelength routing. Here, each flow r_i is modeled with a source-destination pair (*i.e.*, s_i-d_i) corresponding to two nodes in the IP layer and a bandwidth requirement b_i in Gbps. The OTN in the optical layer covers both trusted and untrusted zones. If a flow gets groomed onto a lightpath traversing the untrusted zone, its data needs to be encrypted with ESD to protect it from data leakage, *i.e.*, at least a pair of ECs should be allocated to the flow. Otherwise, the flow can be transmitted as unencrypted. No matter whether a flow is encrypted or not, a pair of OTN LCs should be allocated to it when being groomed onto a lightpath. The data-rate of each lightpath is just the capacity of its two LCs.

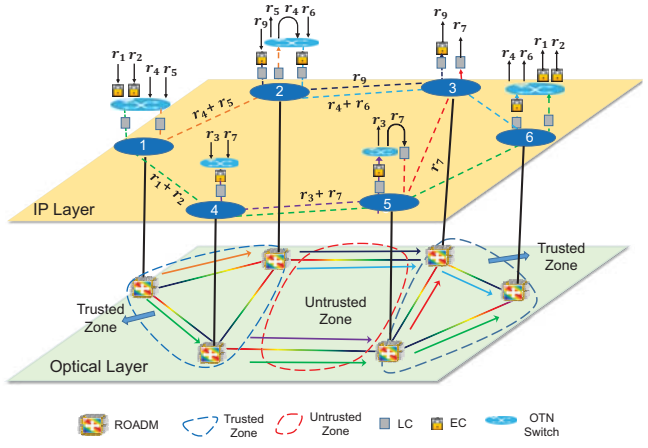


Fig. 1. Security-aware multilayer planning for an OTN with ESD.

In this work, we assume that the cross-layer traffic grooming can use any of the ESD architectures in [4]. For instance, in Fig. 1, *Flow* r_9 is provisioned by using a direct lightpath with dedicated EC and LC pairs (*i.e.*, *Architecture* I in [4]), *Flows* r_3 and r_7 are groomed first and then encrypted before being transmitted on a lightpath (*i.e.*, *Architecture* II in [4]), while *Flows* r_1 and r_2 experience encryption first and then are groomed onto a lightpath (*i.e.*, *Architecture* III in [4]). On the other hand, if its lightpath is routed within the trusted zone, a flow does not need encryption and thus only consumes LCs (*e.g.*, the transmission of *Flows* r_4 and r_5 for 1→2). Note that, we also allow a flow to be routed over multiple lightpaths. For example, in Fig. 1, *Flow* r_7 first shares a lightpath with *Flow* r_3 for 4→5, and then takes a dedicated lightpath for 5→3.

In summary, our security-aware multilayer planning tries to provision all the pending traffic flows in an OTN with ESD, by reasonably routing the flows over lightpaths and arranging the configurations of ECs and LCs for them, so that the total cost from used LCs, ECs and bandwidth resources is minimized.

B. ILP Formulation

We first formulate an ILP model to solve the aforementioned problem of security-aware multilayer planning exactly.

Parameters:

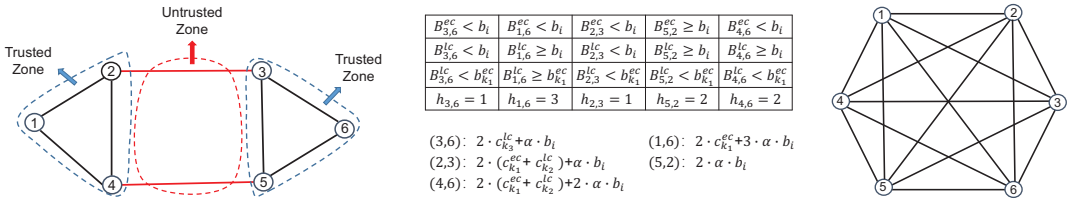
- $G(V, E)$: the OTN's physical topology, where V is the set of switch nodes and E represents the set of fiber links.
- P: the set of feasible routing paths in $G(V, E)$ for setting up lightpaths, where for each node pair u-v, we calculate two feasible paths, *i.e.*, the shortest one and the shortest "safe" one between the node pair[1]. If the two paths are the same, we just put one as $(u, v) \in P$.
- P_{un}: the set of feasible routing paths that use untrusted fiber links[2], *i.e.*, $P_{un} \subset P$.
- $h_{u,v}$: the hop-count of a lightpath (u, v), $u, v \in V$.
- R: the set of pending traffic flows, where each flow $r_i \in R$ associates with a source-destination pair s_i-d_i, and a bandwidth requirement b_i in Gbps.
- LC: the set of feasible LC capacities, where $b_k^{lc} \in LC$ in Gbps is the k-th feasible LC capacity.
- EC: the set of feasible EC capacities, where $b_k^{ec} \in EC$ in Gbps is the k-th feasible EC capacity.
- c_k^{lc}: the cost of an LC with the k-th feasible LC capacity.
- c_k^{el}: the cost of an EC with the k-th feasible EC capacity.
- M: a positive constant that is large enough.
- T_k^{lc}: the upper limit on the number of used LCs with the k-th feasible capacity.
- T_k^{ec}: the upper limit on the number of used ECs with the k-th feasible capacity.

Variables:

- $k_i^{u,v}$: the boolean variable that equals 1 if flow $r_i \in R$ gets routed over a lightpath (u, v), and 0 otherwise.
- $x_{i,j,k}^{u,v}$: the boolean variable that equals 1 if flow r_i uses the j-th LC of those with the k-th feasible capacity for being transmitted over a lightpath (u, v), and 0 otherwise.

[1]Note that, the optical spectra on the fibers are assumed to be always sufficient for supporting lightpaths that carry traffic flows. Hence, the lightpaths' RSA schemes [15–17] become trivial in the multilayer planning, and we can assume that each lightpath is set up with the shortest safe/unsafe paths in the OTN and ignore its spectrum assignment in the ILP model.

[2]Here, we assume that the untrusted zone only consists of fiber links. In other words, all the switch nodes in the OTN are trusted.



(a) Physical topology of OTN (b) Parameters for 5 links in the CAG (c) Topology of CAG

Fig. 2. Example on building a CAG.

- $y^{u,v}_{i,j,k}$: the boolean variable that equals 1 if flow r_i uses the j-th EC of those with the k-th feasible capacity for being transmitted over a lightpath (u, v), and 0 otherwise.
- $N^{lc}_{v,k}$: the integer variable that indicates the number of used LCs with the k-th feasible capacity at node $v \in V$.
- $N^{ec}_{v,k}$: the integer variable that indicates the number of used ECs with the k-th feasible capacity at node $v \in V$.
- $w^{u,v}_{i,i',j,k}$: the boolean variable that equals 1 if flows r_i and $r_{i'}$ share the j-th LC of those with the k-th feasible capacity to go through a lightpath (u, v), and 0 otherwise.
- $z^{u,v}_{i,i',j,k}$: the boolean variable that equals 1 if flows r_i and $r_{i'}$ share the j-th EC of those with the k-th feasible capacity to go through a lightpath (u, v), and 0 otherwise.
- $f^{u,v}_{j,k}$: the boolean variable that equals 1 if the j-th LC of those with the k-th feasible capacity is used for the transmission over a lightpath (u, v), and 0 otherwise.
- $g^{u,v}_{j,k}$: the boolean variable that equals 1 if the j-th EC of those with the k-th feasible capacity is used for the transmission over a lightpath (u, v), and 0 otherwise.
- $Q^{u,v}_{j,k,j',k'}$: the boolean variable that equals 1 if one or more requests use the j'-th EC of those with the k'-th feasible capacity and the j-th LC of those with the k-th feasible capacity over a lightpath (u, v), and 0 otherwise.
- $t^{u,v}_{i,j,k,j',k'}$: the boolean variable that equals 1 if flows r_i uses the j'-th EC of those with the k'-th feasible capacity and the j-th LC of those with the k-th feasible capacity over a lightpath (u, v), and 0 otherwise.

Objective:

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

$$\text{Minimize} \quad 2 \cdot \sum_{v \in V} \left(\sum_{k=1}^{|LC|} c^{lc}_k \cdot N^{lc}_{v,k} + \sum_{k=1}^{|EC|} c^{ec}_k \cdot N^{ec}_{v,k} \right) + \alpha \cdot \sum_{i=1}^{|R|} \sum_{u,v \in V} k^{u,v}_i \cdot h_{u,v} \cdot b_i. \tag{1}$$

We double the first term because LCs and ECs are allocated in pairs, and α is the unit cost of using 1 Gbps per fiber hop.

Constraints:

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

Eq. (2) ensures that the routing scheme of each flow r_i satisfies the flow conservation.

$$\sum_{j,k} x^{u,v}_{i,j,k} = k^{u,v}_i, \quad \forall r_i \in R, \ \forall (u, v) \in P. \tag{3}$$

Eq. (3) ensures that each flow r_i only uses one LC for being sent through a lightpath.

$$\sum_{i=1}^{|R|} x^{u,v}_{i,j,k} \cdot b_i \leq b^{lc}_k, \quad \forall j \in [1, M], \ k \in [1, |LC|], \ (u, v) \in P. \tag{4}$$

Eq. (4) ensures that the capacity of each used LC is not smaller than the total bandwidth demand of the flows assigned to it.

$$\sum_{j,k} y^{u,v}_{i,j,k} = k^{u,v}_i, \quad \forall r_i \in r, \ \forall (u, v) \in P_{un}. \tag{5}$$

Eq. (5) ensures that each flow r_i only uses one EC for being sent through a lightpath, which traverses the untrusted zone.

$$\sum_{i=1}^{|R|} y^{u,v}_{i,j,k} \cdot b_i \leq b^{ec}_k, \ \forall j \in [1, M], \ k \in [1, |EC|], \ (u, v) \in P_{un}. \tag{6}$$

Eq. (6) ensures that the capacity of each used EC is not smaller than the total bandwidth demand of the flows assigned to it.

$$x^{u,v}_{i,j,k} + x^{u,v}_{i',j,k} - 1 \leq w^{u,v}_{i,i',j,k}, \ \{i, i' : i \neq i', \ i, i' \in [1, |R|]\}, \ \forall j \in [1, M], \ k \in [1, |LC|], \ (u, v) \in P. \tag{7}$$

$$y^{u,v}_{i,j,k} + y^{u,v}_{i',j,k} - 1 \leq z^{u,v}_{i,i',j,k}, \ \{i, i' : i \neq i', \ i, i' \in [1, |R|]\}, \ \forall j \in [1, M], \ k \in [1, |EC|], \ (u, v) \in P_{un}. \tag{8}$$

$$z^{u,v}_{i,i',j,k} \leq \sum_{m,l} w^{u,v}_{i,i',m,l}, \ \{i, i' : i \neq i', \ i, i' \in [1, |R|]\}, \ \forall j \in [1, M], \ k \in [1, |LC|], \ (u, v) \in P. \tag{9}$$

$$\sum_{j,k} w^{u,v}_{i,i',j,k} \leq 1, \quad \{i, i' : i \neq i', \ \forall i, i'\}, \ \forall (u, v) \in P. \tag{10}$$

$$\sum_{j,k} z^{u,v}_{i,i',j,k} \leq 1, \ \{i, i' : i \neq i', \ \forall i, i'\}, \ \forall (u, v) \in P. \tag{11}$$

Eqs. (7)-(11) ensure that all the flows using the same EC have to be assigned to the same LC.

$$f^{u,v}_{j,k} \leq \sum_i x^{u,v}_{i,j,k} \leq f^{u,v}_{j,k} \cdot M, \quad \forall j, \ k, \ (u, v) \in P. \tag{12}$$

$$g^{u,v}_{j,k} \leq \sum_i y^{u,v}_{i,j,k} \leq g^{u,v}_{j,k} \cdot M, \quad \forall j, \ k, \ (u, v) \in P. \tag{13}$$

$$\sum_j \sum_{u \in V} f^{u,v}_{j,k} \leq N^{lc}_{v,k}, \quad \forall k, \ v \in V. \tag{14}$$

$$\sum_j \sum_{u \in V} g^{u,v}_{j,k} \leq N^{ec}_{v,k}, \quad \forall k, \ v \in V. \tag{15}$$

Eqs. (12)-(15) ensure that the numbers of LCs and ECs, which are used for data transmission in the OTN, are set correctly.

$$x^{u,v}_{i,j,k} + y^{u,v}_{i,j',k'} - 1 \leq t^{u,v}_{i,j,k,j',k'}, \ \forall r_i \in R, \ j, j' \in [1, M], \ \forall k \in [1, |LC|], \ k' \in [1, |EC|], \ (u, v) \in P_{un}. \tag{16}$$

$$Q^{u,v}_{j,k,j',k'} \leq \sum_i t^{u,v}_{i,j,k,j',k'} \leq Q^{u,v}_{j,k,j',k'} \cdot M, \ \forall r_i \in R \ \forall j, j' \in [1, M], k \in [1, |LC|], k' \in [1, |EC|], (u, v) \in P_{un}. \tag{17}$$

$$\sum_{j',k'} Q^{u,v}_{j,k,j',k'} \cdot b^{ec}_{k'} \le b^{lc}_{k},\ \forall j \in [1,M],\ k \in [1,|LC|], \quad \forall (u,v) \in P_{un}. \tag{18}$$

Eqs. (16)-(18) ensure that the total capacity of all the ECs on an LC cannot exceed the capacity of the LC.

$$2 \cdot \sum_{v \in V} N^{lc}_{v,k} \le T^{lc}_{k}, \quad \forall\ k \in [1,|LC|]. \tag{19}$$

$$2 \cdot \sum_{v \in V} N^{ec}_{v,k} \le T^{ec}_{k}, \quad \forall\ k \in [1,|EC|]. \tag{20}$$

Eqs. (19)-(20) ensure that the numbers of used LCs and ECs can not exceed their corresponding upper limits.

IV. Heuristic Algorithm Design

In this section, we design a novel heuristic to solve the security-aware multilayer planning time-efficiently. As explained above, the multilayer planning for OTNs with ESD becomes much more complex after we introduce the flexibility to choose ESD architectures. Specifically, unlike the one-level grooming (*i.e.*, traffic flows to LCs) in conventional multilayer planning, we need to tackle the hybrid one/two-level grooming (*i.e.*, traffic flows to LCs for the trusted zone, and traffic flows first to ECs and then to LCs for the untrusted zone). Hence, we propose to build collapsed auxiliary graphs (CAGs) and solve the security-aware multilayer planning based on them.

Algorithm 1 shows the overall procedure of our CAG-based security-aware multilayer planning (CAG-Sa-MLP). *Lines* 1-6 is for the initialization. Here, we use $B^{lc}_{u,v}$ and $B^{ec}_{u,v}$ to record the largest available capacities on the ECs and LCs for (u,v), respectively, and they are initialized as 0. we use T^{lc}_{k} and T^{ec}_{k} to represent the upper limit of the number of LCs and the number of ECs with k capacity respectively. We use N^{lc}_{k} and N^{ec}_{k} to record the numbers of used LCs and ECs, which are initialized as 0 and cannot exceed their upper limits (*i.e.*, T^{lc}_{k} and T^{ec}_{k}, respectively). We also introduce another variable $\mathcal{R}_{u,v}$ to store the total bandwidth of unserved flows from u to v. Note that, (u,v) is the logic connection between u-v and it can include a bundle of lightpaths, each of which uses the shortest safe/unsafe path in $G(V,E)$, terminates by a pair of LCs, and has one or more pairs of attached ECs if its physical path traverses the untrusted zone. Next, we use the for-loop that covers *Lines* 7-34 to provision the flows in R in descending order of their bandwidth demands. For each flow r_i, we first get the logic connection(s) that can route it from s_i to d_i based on a CAG (*Lines* 8-9), and then traverse each selected logic connection to finalize the flow's provisioning scheme (*Lines* 10-33). The CAG is built in *Algorithm* 2.

Line 11 checks whether the physical path of (u,v) goes through the untrusted zone. If yes, we either use *Line* 13 to assign r_i to an existing EC, or allocate a new EC (*Lines* 17-18) or both a new EC and a new LC (*Line* 20) for it, depending on whether there is enough EC and LC capacities for it. Here, *Line* 15 determines its proper capacity $\hat{b}$ if a new EC has to be allocated. Specifically, we get $\hat{b}$ based on $\mathcal{R}_{u,v}$ as

$$\hat{b} = \begin{cases} b^{ec}_{k}, & b^{ec}_{k-1} < \mathcal{R}_{u,v} \le b^{ec}_{k},\ N^{ec}_{k} \le T^{ec}_{k}, \\ \max\limits_{b^{ec}_{k} \in EC} (b^{ec}_{k}), & \text{otherwise}, \end{cases} \tag{21}$$

Algorithm 1: CAG-Sa-MLP

```
1  for each node pair u-v in V do
2      calculate the shortest safe/unsafe paths in G(V,E);
3      update h_{u,v}, P and P_un accordingly;
4      B^lc_{u,v} = 0, B^ec_{u,v} = 0, N^lc_k = 0, N^ec_k = 0 ;
5      get R_{u,v} as total bandwidth of flows from u to v;
6  end
7  for each flow r_i ∈ R in descending order of b_i do
8      invoke Algorithm 2 to build a CAG G_a(V_a,E_a) based
       on the current network status;
9      get the shortest path p for s_i→d_i in G_a(V_a,E_a),
       where each link (u,v) ∈ p is a logic connection;
10     for each link (u,v) ∈ p do
11         if (u,v) ∈ P_un then
12             if B^ec_{u,v} ≥ b_i then
13                 assign r_i to a feasible EC with the least
                   available capacity;
14             else
15                 get proper capacity of a new EC as b̂;
16                 if B^lc_{u,v} ≥ b̂ then
17                     allocate a new EC with capacity b̂;
18                     attach the EC to a feasible LC with
                       the least available capacity;
19                 else
20                     allocate a new LC and a new EC (both
                       with capacity b̂) to attach together and
                       the capacity of the new LC cannot be
                       lower than that of the new EC;
21                 end
22                 assign r_i to the new EC;
23             end
24         else
25             if B^lc_{u,v} ≥ b_i then
26                 assign r_i to a feasible LC with the least
                   available capacity;
27             else
28                 allocate a proper new LC for r_i;
29             end
30         end
31         update B^ec_{u,v}, N^lc_k, N^ec_k, B^lc_{u,v}, and R_{u,v};
32         update network status to consider r_i over (u,v);
33     end
34 end
```

to facilitate effective traffic grooming. Following the similar logic of *Lines* 12-23, we assign r_i to an LC if the physical path of (u,v) only uses trusted fiber links. The "a proper new LC" in *Line* 28 refers to an LC whose capacity is also determined based on $\mathcal{R}_{u,v}$ with the similar expression in Eq. (21). Finally, after r_i having been provisioned over (u,v), *Lines* 31-32 update the network status.

We explain the procedure of building a CAG for a flow r_i in *Algorithm* 2. *Lines* 1-3 are for the initialization, where k_1, k_2 and k_3 are the proper indices of feasible EC/LC capacities to use for accommodating b_i in different situations. In *Line* 4, we take all the nodes in V, and build a fully-connected graph over them, which is the topology of the CAG. Here, each node pair in the CAG is connected with one or two links, each of which represents a safe/unsafe shortest path between the node pair in the OTN topology $G(V,E)$. Then, we use the length of each link (u,v) in the CAG to represent the current status of the corresponding logic connection in the OTN $G(V,E)$. *Lines*

5-23 determine the length of each link $(u, v) \in E_a$ based on the fact whether the existing ECs/LCs on the logic connection (u, v) in $G(V, E)$ can be reused to provision r_i. Specifically, the cost of new ECs/LCs will be included in the length of (u, v) if r_i cannot reuse the existing ECs/LCs on it, and *vice versa*. If the total number of LCs or ECs in the network after adding new LC and EC exceeds the upper limit, then the length of (u, v) set to be infinity. Fig. 2 shows an example on building the CAG. With the OTN's physical topology in Fig. 2(a), we obtain the CAG's topology as the 6-node complete graph in Fig. 2(c). Then, for a request $r_i(s_i = 1, d_i = 6, b_i)$, the table in Fig. 2(b) provides the necessary parameters and relations for calculating the lengths of 5 links in the CAG. Next, we can use *Algorithm* 2 to get the lengths of the corresponding links in the CAG as shown in Fig. 2(b).

Complexity Analysis: The overall complexity of *Algorithm* 2 is $O(|V|^2)$. In *Algorithm* 1, the time complexity of sorting the affected flows is $O(|\mathbf{R}| \cdot \log(|\mathbf{R}|))$. The complexity of calculating the shortest path p in an CAG is $O(|\mathbf{R}| \cdot |E| \cdot |V|^2)$. We need to update LCs and ECs information on each link (u, v) in the shortest path p, and thus the complexity of this part is $O(|\mathbf{R}| \cdot |p|)$. Finally, the overall complexity of *Algorithm* 1 is $O(|V|^2 + |\mathbf{R}| \cdot |V|^2 + |\mathbf{R}| \cdot |E| \cdot |V|^2 + |\mathbf{R}| \cdot \log(|\mathbf{R}|) + |\mathbf{R}| \cdot |p|)$.

V. Performance Evaluation

We first consider a small-scale OTN topology, *i.e.*, the six-node topology in Fig. 2(a). We assume that the feasible capacities of LCs and ECs are $LC = EC = \{40, 100, 400\}$ Gbps [4], while the unit costs of the corresponding LCs and ECs are $\{1, 2, 4\}$ and $\{2, 4, 8\}$, respectively. For each request r_i, s_i and d_i are randomly selected, and bandwidth demand b_i uniformly distributes within $[25, 200]$ Gbps. We choose α from $\{0.002, 0.01\}$. We consider two situations: 1) the LCs and ECs are enough such that most of the requests can served with direct lightpaths, and 2) the LCs and ECs are limited such that each request can be frequently groomed on multiple lightpaths from end to end. Table I shows the results. The gap between the results from CAG-Sa-MLP to the exact ones from the ILP is relatively small. When the LCs/ECs are limited, the network planning can require more bandwidths than in the cases where the LCs/ECs are enough. This is because in this case, the requests may need to be groomed with others to take routing paths with larger hop-counts. We also observe that both algorithms optimize the multilayer planning according to α, and CAG-Sa-MLP is much more time-efficient than the ILP.

Next, we consider the large-scale OTN topology in Fig. 3 to further evaluate CAG-Sa-MLP. Here, we introduce a benchmark, *i.e.*, shortest path priority multilayer planning (SPP-MLP) [18]. The total traffic load of flows ranges in $[100, 125]$ Tbps, while the remaining parameters are similar as above. Fig. 4 shows the results on total cost of multilayer planning. For each bar in the plots, the lower part is for total bandwidth cost, while the higher one represents total cost of LCs and ECs. Comparing Fig. 4(a) and Fig. 4(b), we find that CAG-Sa-MLP always provides smaller total costs than SPP-MLP. For different values of α, the gap on bandwidth

Algorithm 2: CAG Construction

Input : a flow r_i, network status, T_k^{lc}, T_k^{ec}, LC, and EC.
output: the CAG $G_a(V_a, E_a)$ for routing r_i.

$k_1 = \text{argmin}\left(\{b_k^{ec} : b_k^{ec} \geq b_i, N_k^{ec} \leq T_k^{ec}, b_k^{ec} \in EC\}\right)$;
$k_2 = \text{argmin}\left(\{b_k^{lc} : b_k^{lc} \geq b_{k_1}^{ec}, N_k^{lc} \leq T_k^{lc}, b_k^{lc} \in LC\}\right)$;
$k_3 = \text{argmin}\left(\{b_k^{lc} : b_k^{lc} \geq b_i, b_k^{lc} \in LC\}\right)$;
$V_a = V$, build a fully-connected graph $G_a(V_a, E_a)$;
for *each link* $(u, v) \in E_a$ **do**
  if $(u, v) \in P_{un}$ **then**
    if $B_{u,v}^{ec} \geq b_i$ **then**
      set length of (u, v) in $G_a(V_a, E_a)$ as $\alpha \cdot h_{u,v} \cdot b_i$;
    else
      if $N_{k_1}^{ec} \leq T_{k_1}^{ec}$ **then**
        if $B_{u,v}^{lc} \geq b_{k_1}^{ec}$ **then**
          set length of (u, v) as $2 \cdot c_{k_1}^{ec} + \alpha \cdot h_{u,v} \cdot b_i$;
        else
          if $N_{k_2}^{lc} \leq T_{k_2}^{lc}$ **then**
            set length of (u, v) as $2 \cdot (c_{k_1}^{ec} + c_{k_2}^{lc}) + \alpha \cdot h_{u,v} \cdot b_i$;
          else
            set length of (u, v) as $+\infty$;
          end
        end
      else
        set length of (u, v) as $+\infty$;
      end
    end
  else
    if $B_{u,v}^{lc} \geq b_i$ **then**
      set length of (u, v) as $\alpha \cdot h_{u,v} \cdot b_i$;
    else
      if $N_{k_3}^{lc} \leq T_{k_3}^{lc}$ **then**
        set length of (u, v) as $2 \cdot c_{k_3}^{lc} + \alpha \cdot h_{u,v} \cdot b_i$;
      else
        set length of (u, v) as $+\infty$;
      end
    end
  end
end
return $G_a(V_a, E_a)$;

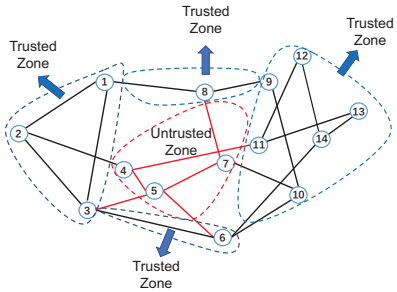


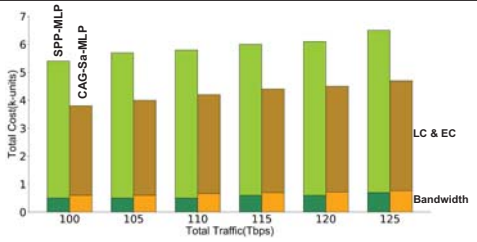
Fig. 3. NSFNET topology

costs from CAG-Sa-MLP and SPP-MLP is relatively small, but compared with SPP-MLP, CAG-Sa-MLP always saves significant numbers of LCs and ECs in its network planning.

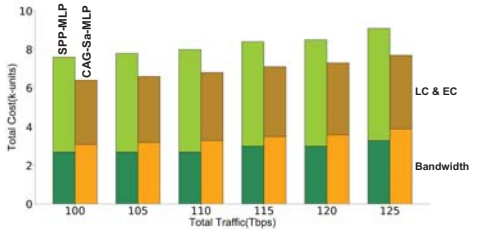
Fig. 5 compares the numbers of LCs/ECs used in the multilayer planning. We notice that to ensure effective traffic grooming, both algorithms use more 400 Gbps LCs/ECs than other types of LCs/ECs. The results also indicates that CAG-Sa-MLP uses smaller numbers of LCs/ECs, especially ECs.

TABLE I
SIMULATION RESULTS WITH SIX-NODE TOPOLOGY

$\|R\|$		3	4	5	6
Total Traffic (Gbps)		320	420	520	610
$\alpha = 0.002$					
ILP/enough	Total Cost	14.64	39.24	43.63	58
	Bandwidth (Gbps)	320	620	815	1000
	EC & LC amount	3	5.5	6	8
CAG-Sa-MLP/enough	Total Cost	14.64	39.24	43.63	58.9
	Bandwidth (Gbps)	320	620	815	1450
	EC & LC amount	3	5.5	6	8
ILP/limited	Total Cost	17.14	41.64	50.05	58.5
	Bandwidth (Gbps)	570	820	1025	1275
	EC & LC amount	2	4	5	6
CAG-Sa-MLP/limited	Total Cost	17.14	41.64	50.05	59.25
	Bandwidth (Gbps)	570	820	1025	1625
	EC & LC amount	2	4	5	6
$\alpha = 0.01$					
ILP/enough	Total Cost	17.2	44.2	50.15	66
	Bandwidth (Gbps)	320	620	815	1000
	EC & LC amount	3	5.5	6	8
CAG-Sa-MLP/enough	Total Cost	17.2	44.2	50.15	70.5
	Bandwidth (Gbps)	320	620	815	1450
	EC & LC amount	3	5.5	6	8
ILP/limited	Total Cost	21.7	48.2	58.25	68.75
	Bandwidth (Gbps)	570	820	1025	1275
	EC & LC amount	2	4	5	6
CAG-Sa-MLP/limited	Total Cost	21.7	48.2	58.25	72.25
	Bandwidth (Gbps)	570	820	1025	1625
	EC & LC amount	2	4	5	6
ILP's Running Time (s)		3	540	1560	6485
CAG-Sa-MLP's Running Time (s)		0.086	0.14	0.2	0.2



(a) $\alpha = 0.002$



(b) $\alpha = 0.01$

Fig. 4. Large-scale simulation results on total cost.

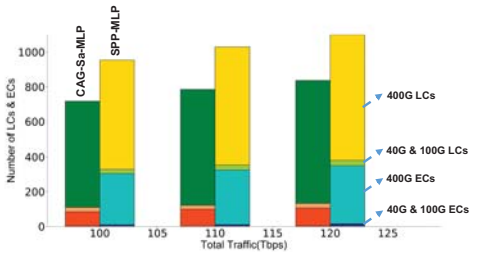
VI. CONCLUSION

We studied how to achieve cost-effective and security-aware multilayer planning for an OTN that covers both trusted and untrusted zones and has the option to choose ESD architectures based on traffic condition. An ILP model was proposed together with a novel heuristic based on CAGs. Simulation results confirmed that our proposed algorithms can achieve cost-effective multilayer planning and outperform benchmark.

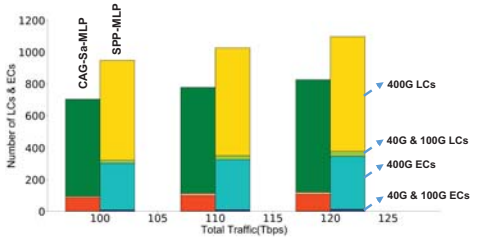
REFERENCES

[1] 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.

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



(a) $\alpha = 0.002$



(b) $\alpha = 0.01$

Fig. 5. Large-scale simulation results on LCs & ECs.

[3] 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.

[4] 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.

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

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

[7] 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.

[8] W. Lu, X. Yin, X. Cheng, and Z. Zhu, "On cost-efficient integrated multilayer protection planning in IP-over-EONs," *J. Lightw. Technol.*, vol. 35, pp. 5335–5346, Dec. 2017.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[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] C. Sommer, "Shortest-path queries in static networks," *ACM Comput. Surveys*, vol. 46, pp. 1–31, Apr. 2014.