Planning Security-aware Filterless Optical Networks
(*Invited Paper*)

Qian Lv and Zuqing Zhu

University of Science and Technology of China, Hefei, Anhui 230027, China, Email: zqzhu@ieee.org

Abstract: We consider to leverage optical transport network (OTN) encryption to enhance the security in filterless optical networks (FONs), and solve the resulting security-aware multilayer planning.

OCIS codes: (060.1155) optical transport network; (060.4251) Networks, assignment and routing algorithms.

1. Introduction

Nowadays, the raising of new data-driven applications has stressed the underlying optical architecture of wide-area networks (WANs) [1–5]. As a promising passive solution, filterless optical network (FON) has been proposed to replace optical switching elements (*e.g.*, reconfigurable optical add-drop multiplexer (ROADM)) in WANs with passive splitters/combiners [6]. Hence, FON can potentially provide a more cost-efficient, and energy-efficient optical architecture for WANs, because it removes or minimizes the need of active optical switching. However, as the transmission in FONs is based on "broadcast-and-select", a malicious party can tap into the communications much more easily. Previously, to overcome the physical-layer vulnerabilities in WANs and backbone networks, people have developed optical transport network (OTN) encryption technologies that can ensure the security of OTN payload frames with high-speed encryption cards (ECs) [7]. Specifically, in such a security-aware OTN, the OTN linecards (LCs)/switches, and ECs can be arranged in three EC deployment (ECD) architectures to facilitate cross-layer traffic grooming and wavelength routing [8]. Hence, it is expected that the security breaches due to broadcast-and-select can be resolved by introducing ECs in FONs, *i.e.*, a malicious party cannot decrypt the OTN payload frames without a proper EC. Nevertheless, to the best of our knowledge, the security-aware planning of FONs has not been studied yet.

Note that, even for a normal OTN with wavelength switching, the security-aware planning that jointly considers LCs and ECs is much more complex than the conventional one that only tries to groom traffic flows with LCs and schedule the wavelength routing of resulting lightpaths [9]. This is because in addition to the packet and optical layers, the ECs introduce a new encryption layer, and the operations of the packet and encryption layers are correlated, especially when the three ECD architectures in [8] can be used simultaneously. Furthermore, because FONs utilize completely different optical architecture than normal OTNs, the security-aware planning for them can be even more challenging. This motivates us to study the security-aware planning in this work. Specifically, we consider the generic case in which the nodes in an FON can either have mutual trustiness or not, and the network planner needs to switch among different ECD architectures to adapt to traffic condition. We formulate an integer linear programming (ILP) model to optimize the cost-effectiveness of the security-aware planning, and design a novel heuristic to solve the problem time-efficiently.

2. Security-aware Multilayer Planning for an FON with ECs

Fig. 1(a) explains the three commonly-used ECD architectures that organize LCs, OTN switches and ECs for multilayer service provisioning [8]. The OTN switches are actually the electrical switches for grooming/de-grooming low-speed traffic flows to/from lightpaths. Hence, they can be incorporated in FONs. *Architecture* I maps each traffic flow to an EC that connects to an LC and sets up an end-to-end lightpath with the LC to transmit the flow, *Architecture* II grooms flows to an LC that connects to an EC and uses multi-hop lightpath routing to transmit the flows, and *Architecture* III uses an EC to encrypt each flow, grooms the encrypted flows to an LC, and also transmits the flows with multi-hop lightpath routing. To incorporate these ECD architectures in an FON, we only need to replace the ROADMs with passive splitters/combiners, while the remaining configurations are the same.

The security-aware planning needs to serve a set of flows from the IP layer (denoted as R). Each flow in R is $r_i(s_i, d_i, b_i)$, where i is its unique index, s_i and d_i represent its source and destination, respectively, and b_i is its bandwidth demand in Gbps. The physical topology of the FON is modeled as a graph $G(V, E)$, where V and E are the sets of nodes and fiber links, respectively. We assume that the nodes in V can either have mutual trustiness or not. As the FON uses broadcast-and-select to realize filterless transmissions, the optical layer should be designed with fiber trees [6], each of which covers a subset of nodes in V. The optical signal from a node can only be broadcasted within its fiber tree, and if the node wants to talk with another one that is not in its fiber tree, it needs to leverage cross-layer traffic de-grooming/re-grooming to send a flow across fiber trees. And if the communication may be received by any node (except the destination) that do not have mutual trustiness with the source node, it should be encrypted with ECs.

Fig. 1(b) gives an example on the security-aware planning for an FON with ECs. The sub-figure on the bottom right shows the planning in the optical layer. Here, we mark the nodes that have mutual trustiness with the same color, and

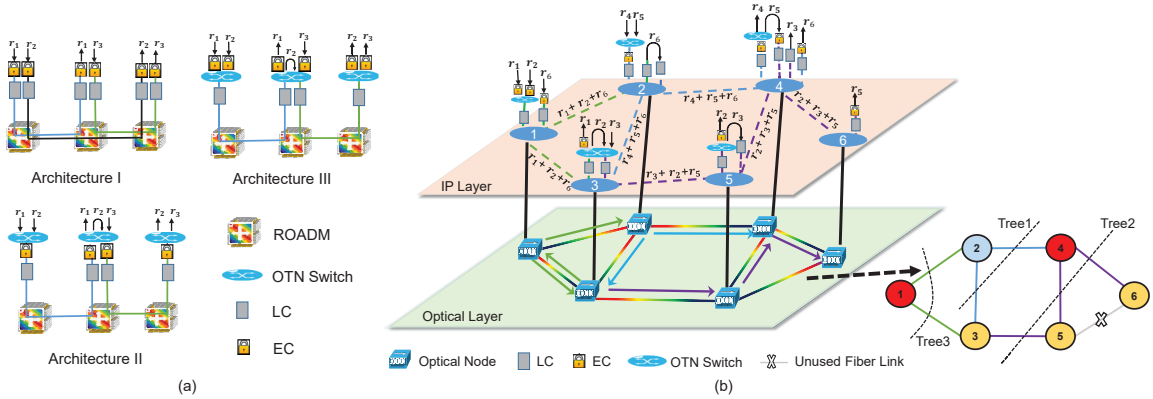


Fig. 1. (a) Three ECD architectures (adapted from [8]), and (b) Security-aware planning in an FON.

the links that belong to the same fiber tree are also in the same color. Hence, we design three fiber trees for the FON, *i.e.*, *Trees* 1-3 cover *Nodes* $\{2,3,4\}$, $\{3,4,5,6\}$ and $\{1,2,3\}$, respectively, and *Link* 5-6 is not included in any fiber tree to avoid loops. The security-aware planning serves the six flows in R. Flow r_6 gets routed across *Trees* 1 and 3, both of which contain nodes that do not have mutual trustiness with *Node* 1. Therefore, we allocate an EC to encrypt r_6 at *Node* 1, and it is not decrypted until reaching its destination (*Node* 4), *i.e.*, r_6 is served with *Architecture* I in Fig. 1(a). Meanwhile, we allocate LCs on *Node* 2 for r_6 to transmit it from *Tree* 3 to *Tree* 1. At *Node* 1, we encrypt r_1 and r_2 with ECs separately and then groom them to a same LC (*Architecture* III in Fig. 1(a)). For r_3, we groom it with r_2 at *Node* 3 using an LC, but do not allocate an EC to encrypt it. This is because r_3 is served with *Tree* 2 only, where all the nodes have mutual trustiness with its source (*Node* 3), except for *Node* 4, which is the destination of r_3.

3. Algorithm Design

To optimize the cost-effectiveness of the security-aware planning, we formulate the ILP model below.

Key Notations:

$t_{u,v}$: equals 1 if nodes u and v have mutual trustiness, and 0 otherwise.

R: set of traffic flows, where the i-the flow is $r_i(s_i,d_i,b_i)$.

B^{Ec}/B^{Lc}: set of EC/LC capacities on a node, and b_n^{Ec}/b_n^{Lc} is the n-th one.

$Z^i_{(u,v)}$: boolean variable that equals 1 if flow $r_i \in R$ is received after link (u,v), and 0 otherwise.

$X^i_{n,v}/Y^i_{m,v}$: boolean variable that equals 1 if flow $r_i \in R$ uses (the n-th EC)/(the m-th LC) on node v, and 0 otherwise.

$Kl^{i,j}_{m,v}/Ke^{i,j}_{n,v}$: boolean variable that equals 1 if flows r_i and r_j use the (m-th LC)/(n-th EC) on node v, and 0 otherwise.

$N^{(1)}_{m,v}/N^{(2)}_{n,v}$: boolean variable that equals 1 if the (m-th LC)/(n-th EC) on node v is used, and 0 otherwise.

$P_{(u,v),k}/T_{u,k}$: boolean variable that equals 1 if (link (u,v))/(node u) belongs to fiber tree k ($k \in [1,|E|]$), and 0 otherwise.

d_k: boolean variable that equals 1 if d_k is a fiber tree, and 0 otherwise.

Objectives:

$$\text{Minimize} \quad 2\cdot\sum_{v\in V}\left(\sum_{m=1}^{|B^{\text{LC}}|}\alpha_{m,v}\cdot N^{(1)}_{m,v}+\sum_{n=1}^{|B^{\text{EC}}|}\beta_{n,v}\cdot N^{(2)}_{n,v}\right). \tag{1}$$

Key Constraints:

$$\sum_{n\in[1,|B^{Ec}|]} X^i_{n,s} \geq Z^i_{(u,v)}\cdot P_{(u,v),k}\cdot T_{p,k}\cdot(1-t_{s,p}),\ \{p: p\in V, p\neq d_i\}, \tag{2}$$

$$\sum_{n\in[1,|B^{Ec}|]} X^j_{n,d_i} \geq \sum_{(d_i,v)\in E} Z^j_{(d_i,v)}\cdot Ke^{i,j}_{n',u}, \forall r_i,r_j\in R, n'\in[1,|B^{Ec}|], \tag{3}$$

$$\sum_{m\in[1,|B^{Lc}|]} Y^i_{m,v} \geq Z^i_{(u,v)}\cdot Z^i_{(v,p)}\cdot P_{(u,v),k}\cdot(1-P_{(v,p),k}),\ \forall(v,p)\in E, \tag{4}$$

$$\sum_{m\in[1,|B^{Lc}|]} Y^j_{m,d_i} \geq \sum_{(d_i,v)\in E} Z^j_{(d_i,v)}\cdot Kl^{i,j}_{m',u}, \forall r_i,r_j\in R, m'\in[1,|B^{Lc}|], \tag{5}$$

$$N^{(1)}_{m,v} \leq \sum_{r_i\in R} Y^i_{m,v} \leq M\cdot N^{(1)}_{m,v},\quad \forall v\in V, m\in[1,|B^{Lc}|], \tag{6}$$

$$N^{(2)}_{n,v} \leq \sum_{r_i\in R} X^i_{n,v} \leq M\cdot N^{(2)}_{n,v},\quad \forall v\in V, n\in[1,|B^{Ec}|], \tag{7}$$

$$\sum_{m\in[1,|B^{Lc}|]} Y^i_{m,s}=1,\quad \forall r_i\in R, \tag{8}$$

$$\sum_{k\in[1,|E|]} T_{v,k}\geq 1,\quad \forall v\in V, \tag{9}$$

$$\sum_{k\in[1,|E|]} P_{(u,v),k}\leq 1,\quad \forall(u,v)\in E, \tag{10}$$

$$\frac{1}{2}\sum_{(u,v)\in E} P_{(u,v),k}=\sum_{p\in V} T_{p,k}-d_k,\quad \forall k, \tag{11}$$

$$\sum_{(u,v)\in E} P_{(u,v),k}\leq M\cdot T_{v,k},\quad \forall v,\ k, \tag{12}$$

$$T_{v,k}\leq \sum_{(u,v)\in E} P_{(u,v),k},\quad \forall v,\ k, \tag{13}$$

The objective in Eq. (1) is to minimize the total cost of deployed LCs/ECs, where $\alpha_{m,v}$ and $\beta_{n,v}$ are the unit costs of corresponding LC and EC, respectively. Eqs. (2)-(8) ensure that the allocations of LCs and ECs are correct in the FON. Eqs. (9)-(13) ensure that the fiber trees are designed properly. Note that, some of the constraints in Eqs. (2)-(13) are not linear. We linearize them with the commonly-used method for processing the multiplication of binary variables [10], while the detailed linearization procedure is omitted due to the page limit.

To improve the time-efficiency of problem solving, we also propose a novel heuristic that solve the security-aware multilayer planning with three steps, *i.e.*, generating the initial fiber trees, provisioning flows in R based on the initial fiber trees and allocating LCs/ECs accordingly, and updating the fiber trees and flow provisioning to reduce the de-

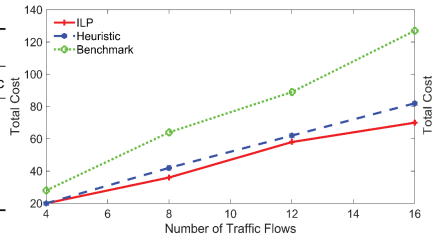
ployed LCs/ECs. In **Step 1**, we divide the nodes in the FON into groups according to their mutual trustiness and the flows in R, calculate a minimum spanning tree for each node group as an initial fiber tree, add the smallest number of links (each link is also treated as an initial fiber tree) to connect the fiber trees, and store all the initial fiber trees in set $\mathscr{T}$. Next, we move to **Step 2**, where the flows in R are first sorted in descending order of their bandwidth demands, and then they are served in the sorted order, based on the fiber trees in $\mathscr{T}$. Specifically, for each flow, we calculate K shortest paths in the FON, find the provisioning scheme on each path that can reuse the most deployed LCs/ECs, and serve the flow with the scheme that results in the smallest incremental cost. Finally, **Step 3** updates the fiber trees and allocations of LCs/ECs in iterations to minimize the cost of deployed LCs/ECs. We first store all the links, which are not included in $\mathscr{T}$, in E'. Then, for each link in E', we insert it in a proper fiber tree in $\mathscr{T}$ or mark it as a new fiber tree, and obtain a new set $\mathscr{T}'$. We apply **Step 2** to $\mathscr{T}'$ to see whether the cost of deployed LCs/ECs can be reduced. If yes, we replace $\mathscr{T}$ with $\mathscr{T}'$. The procedure in **Step 3** is repeated until all the links in E' has been checked.

4. Performance Evaluations

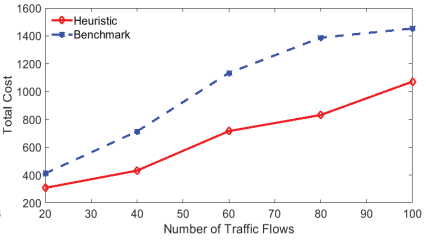
Our simulations consider two physical topologies, which are the six-node one in Fig. 1(b) and the 14-node NSFNET [10]. We assume that the feasible capacities of LCs/ECs are $B^{Ec} = B^{Lc} = \{40, 100, 400\}$ Gbps [8], while the unit costs of the corresponding LCs and ECs are $\{1,2,4\}$ and $\{2,4,6\}$, respectively. The flows in R are randomly generated and their bandwidth demands are within $[25, 200]$ Gbps, and the mutual trustiness among nodes is also randomly determined. In addition to our ILP and heuristic, we also consider a benchmark that first randomly divides the nodes in an FON into groups, and then applies **Step 2** in the heuristic once to get the multilayer planning. The simulations are conducted on a computer with 2.1 GHz Intel CPU and 32 GB memory, and the environment is MATLAB 2019a with Gurobi toolbox. Figs. 2(a) and 2(b) show the results with the small-scale six-node topology. We can see that the total costs from the heuristic are close to the optimal solutions from the ILP, and they are much smaller than those from the benchmark. These results confirm the performance of our heuristic on security-aware multilayer planning. The comparison in Fig. 2(a) explains the performance gap between the ILP and heuristic in Fig. 2(b). Specifically, the ILP plans the flows to use a shorter average path length than the heuristic, *i.e.*, unnecessary detouring and LC/EC usages are eliminated. However, the ILP takes much longer time to run than the heuristic, and it can easily become intractable when the problem size increases. As the ILP becomes intractable when NSFNET is used, Fig. 2(c) only compares the costs from the heuristic and benchmark. The heuristic still performs better to provider much smaller deployment costs.

Number of Traffic Flows	Running Time (s)		Average Path Length (km)	
	ILP	Heuristic	ILP	Heuristic
4	2.89	0.12	85	85
8	188.65	0.26	145	245
12	1262.73	0.30	157	200
16	6624.74	0.41	164	241

(a)



(b)



(c)

Fig. 2. Simulation results.

5. Conclusion

To enhance physical-layer security in FONs, we introduced the ECs for OTN encryption, and obtained a novel problem of security-aware multilayer planning. We formulated an ILP model and design a heuristic to solve the problem.

References

[1] 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./Oct. 2015.

[2] Z. Zhu, W. Lu, L. Zhang, and N. Ansari, "Dynamic service provisioning in elastic optical networks with hybrid single-/multi-path routing," *J. Lightw. Technol.*, vol. 31, pp. 15-22, Jan. 2013.

[3] 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.

[4] 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.

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

[6] E. Archambault *et al.*, "Design and simulation of filterless optical networks: Problem definition and performance evaluation," *J. Opt. Commun. Netw.*, vol. 2, pp. 496-501, Aug. 2010.

[7] J. Ceballos *et al.*, "Business continuity and security in datacenter interconnection," *Bell Labs Tech. J.*, vol. 17, pp. 147-155, Dec. 2012.

[8] K. Guan *et al.*, "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.

[9] M. Song *et al.*, "On security-aware multilayer planning for IP-over-optical networks with OTN encryption," *in Proc. of ICC 2020*, pp. 1-6, Jun. 2020.

[10] Q. Lv *et al.*, "Network planning with bilevel optimization to address attacks to physical infrastructure of SDN," *in Proc. of ICC 2020*, pp. 1-6, Jun. 2020.