Attack-Aware Service Provisioning to Enhance Physical-Layer Security in Multi-Domain EONs

Jing Zhu, Bin Zhao, Wei Lu, and Zuqing Zhu, *Senior Member, IEEE*

***Abstract*—It is known that with the multi-domain scenario, elastic optical networks (EONs) can improve network scalability, extend service coverage, and handle the multi-carrier situation. However, as a malicious client can launch cross-domain attacks in the physical layer, the security issues in multi-domain EONs should not be overlooked. In this paper, we consider how to improve the physical-layer security-level of multi-domain EONs. Specifically, we propose to differentiate the routing and spectrum assignment (RSA) schemes of intra- and inter-domain requests with security considerations. To achieve this, we review the physical-layer vulnerabilities due to different clients (especially trusted and untrusted ones) sharing optical components in EONs, analyze the potential attack scenarios to different RSA arrangements, and quantify the corresponding security threats with an attack factor. Then, we define the problem of multi-domain attack-aware RSA and formulate an integer linear programming model to solve it exactly. To reduce the time complexity, a heuristic algorithm is also proposed. The proposed algorithms are evaluated with extensive simulations using both the offline and online provisioning scenarios, and the simulation results verify its effectiveness.**

***Index Terms*—Attack-aware service provisioning, elastic optical networks (EONs), multi-domain, physical-layer security.**

I. Introduction

OVER the past decade, the traffic in backbone networks has been increasing exponentially due to the emerging applications such as Big Data [1], [2]. This stimulated the research and development on highly efficient and flexible optical networking technologies. Under this circumstance, flexible-grid elastic optical networks (EONs) have been proposed and demonstrated to achieve higher spectral efficiency and more agile bandwidth allocation than the traditional fixed-grid wavelength-division multiplexing (WDM) networks [1]. Specifically, EONs set up lightpaths with bandwidth-variable transponders and switches (BV-WSS') that operate on a series of spectrally-contiguous frequency slots (FS'), each of which has a bandwidth of 12.5 GHz or less.

Meanwhile, considering the geographical span of backbone networks and the heterogeneous technologies of multi-vendor network elements, we can hardly explore the advantages of EONs without addressing the multi-domain scenario [3]. Basically, with the multi-domain scenario, we can accommodate the inter-operability issues when using network elements from different vendors, improve network scalability, extend service coverage, and handle the situation in which network elements are managed by different carriers. Therefore, it is very relevant to study multi-domain service provisioning schemes for EONs. Previously, people have demonstrated a few network architectures to facilitate cross-domain network orchestration in multi-domain EONs [3]–[6]. However, they just used the existing intra-domain provisioning schemes to handle inter-domain lightpath requests, with the only exception that the domain managers had to collaborate to serve inter-domain requests. Note that, in this scenario, they treated intra- and inter-domain requests equally within each domain and overlooked the physical-layer security issues.

It is known that in optical networks, there would be physical-layer vulnerabilities if different clients (especially trusted and untrusted ones) share optical components. For example, a high power jamming attack from the physical-layer can interrupt the high-speed data transmission in optical networks badly, and the adjacent-channel interference can be easily utilized to realize eavesdropping [7]. These threats would become more intimidating in multi-domain EONs, since a super-channel can carry over 400 Gb/s capacity and the channel spacing is much narrower than that in WDM networks. For instance, a malicious client can realize cross-domain attacks by injecting jamming light from a neighbor domain to degrade the quality-of-transmission (QoT) of a supper-channel. Hence, if we do not consider these potential security threats in EON-related multi-domain service provisioning, unimaginable losses might be caused by the attacks.

Note that, the aforementioned security threats can be minimized by strictly enforcing optical-to-electrical-to-optical (O/E/O) conversions in between domains, i.e., building opaque domains. This, however, would increase both the capital expenditure and operational expenditure of multi-domain EONs to an unacceptable level. Hence, it makes much more sense to design an attack-aware service provisioning scheme to address the security threats, under the assumption that the multi-domain EONs are transparent or translucent. Nevertheless, to the best of our knowledge, this problem has not been explored before.

In this paper, based on the idea of minimizing the sharing of optical components among trusted and untrusted clients intelligently, we design attack-aware provisioning schemes to improve the physical-layer security-level of multi-domain EONs effectively. Specifically, we propose to differentiate the routing and

Manuscript received October 26, 2015; revised January 8, 2016 and February 21, 2016; accepted March 11, 2016. Date of publication March 13, 2016; date of current version April 13, 2016. This work was supported in part by the NSFC Project 61371117, the Fundamental Research Funds for Central Universities under Grant WK2100060010, the Natural Science Research Project for Universities in Anhui under Grant KJ2014ZD38, and the Strategic Priority Research Program of the CAS under Grant XDA06011202.

The authors are with the School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China (e-mail: zhujinng@mail.ustc.edu.cn; bbz812@mail.ustc.edu.cn; luwei11@mail.ustc.edu.cn; zqzhu@ieee.org).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JLT.2016.2541779

spectrum assignment (RSA) schemes of intra- and inter-domain requests with security considerations. To achieve this, we review the vulnerabilities of optical components in EONs, analyze the potential attack scenarios to different RSA arrangements, and quantify the corresponding security threats with an attack factor (AF). Then, we develop a multi-domain attack-aware RSA (MDAa-RSA) algorithm to improve the overall security-level of a multi-domain EON, i.e., reducing the average AF in the network. We formulate an integer linear programming (ILP) model to solve the problem exactly, and also propose a heuristic algorithm to reduce the time complexity. The proposed algorithms are evaluated with extensive simulations using both offline and online provisioning scenarios, and the results verify the effectiveness of the algorithms.

The rest of the paper is organized as follows. Section II surveys the related work. The problem description is given in Section III, where we analyze the security threats to different RSA arrangements and define the network model for multi-domain attack-aware service provisioning. In Section IV, we formulate the ILP model to solve the MDAa-RSA problem, and the time-efficient heuristic is discussed in Section V. We describe the performance evaluation with simulations in Section VI. Finally, Section VII summaries the paper.

II. Related Work

From the perspective of improving the security-level of optical networks with hardware assistances, various technologies have been proposed and demonstrated before [8]–[12]. However, as they would require additional hardware elements, they are out of the scope of this work. For WDM networks, the problem of attack-aware routing and wavelength assignment (Aa-RWA) was first formulated in [13], where the authors considered the security threat from the intra-channel crosstalk generated by non-ideal optical switches and designed several heuristics to address the wavelength assignment subproblem in Aa-RWA. Specifically, under the assumption of unlimited attack propagation capability, they tried to assign wavelengths in a way such that the impact of intra-channel crosstalk attacks can be minimized. In [14], they reduced the complexity of the wavelength assignment and made their algorithms more scalable. And the work was further expanded in [15] to consider more security threats, e.g., from inter-channel crosstalk and erbium-doped fiber amplifier (EDFA) gain competition, and to solve the routing subproblem of Aa-RWA with the objective to minimize the maximum lightpath attack radius.

Furdek *et al.* [16] considered the multi-domain scenario of mixed-line-rate WDM networks, and pointed out that the alien wavelengths from other domains could be attacks. Recently, the work in [17] showed some new and interesting results on Aa-RWA. Specifically, the authors tried to optimize the RWA in transparent WDM network planning for minimizing the negative effects from the propagation of high-power jamming signals, where the security threats from both intra-channel and inter-channel crosstalk were considered. However, the work did not address either the EONs or the multi-domain scenario.

Even though our work is inspired by the studies in [13]–[15], the fundamental differences between them are threefold. First of all, the studies in [13]–[15] only addressed one subproblem in Aa-RWA (i.e., routing or wavelength assignment) at a time, while we try to optimize the RSA arrangements jointly to improve the network's physical-layer security-level. Considering the fact that RSA in EONs is already more complex than RWA in WDM networks [18], [19], we can see that our work addresses a more sophisticated problem. Secondly, when defining the maximum lightpath attack radius in [15], Skorin-Kapov *et al.* only considered the security threat due to link-sharing but ignored that from node-sharing, while our work considers both. Specifically, as we will show later in Section III-A, both intra- and inter-channel crosstalk attacks can be launched when two lightpaths only share node(s) but do not share any link. Hence, our network model is more comprehensive. Last and most importantly, the studies in [13]–[15] and [17] still worked on the single-domain scenario and treated all the requests equally in the Aa-RWA, while we try to address the practical situation in multi-domain EONs and propose to differentiate the RSA schemes of intra- and inter-domain requests with security considerations. This, however, to the best of our knowledge, has not been proposed in previous works.

On the other hand, a few RSA schemes have been proposed in literature [20]–[27] to address the service provisioning in single-domain EONs, but they did not include any security consideration. Meanwhile, people tried to leverage the software-defined networking (SDN) scenario [28], [29] to realize efficient network orchestration in multi-domain EONs [3]–[6]. Casellas *et al.* demonstrated to control an EON with an integrated path computation element and SDN controllers in [4]. A multi-broker based hierarchical control plane architecture was proposed in [5] to facilitate market-driven cross-domain orchestration. Meanwhile, in [3] and [6], we also designed the protocols to enable cooperative RSA in multi-domain EONs and demonstrated them experimentally. Nevertheless, the studies in [3]–[6] still treated intra- and inter-domain requests equally within each domain and overlooked the security threats in the physical-layer.

III. Problem Description

In this section, we review the physical-layer vulnerabilities due to trusted and untrusted clients sharing optical components in EONs, analyze the potential attack scenarios to different RSA arrangements, and describe the network model for realizing MDAa-RSA. Here, in order to make the network model generic, we do not specify the actual attack model and optical node architecture, but it should be noted that different optical node architectures may provide different levels of protection against a specific type of attacks, and the negative effects would be different if the attackers' capabilities are different [30]. In our future work, we will address more specific network environments.

A. Vulnerabilities on Optical Components in EONs

It is known that there are mainly three types of physical-layer vulnerabilities due to the sharing of optical components in optical networks, i.e., intra-channel crosstalk, inter-channel crosstalk, and EDFA gain competition [7], [31]. This is also the case in EONs. Specifically, by leveraging one or a combination of them, malicious clients can launch various types of attacks and degrade a multi-domain EON's security-level.

1) *Intra-Channel Crosstalk* is generated in BV-WSS' due to their non-ideality, e.g., the response of the switching fabric and/or the isolation of the ports. Hence, when the lightpaths of an attacker and a legitimate client use overlapped spectrum assignments and pass the same BV-WSS, the attacker can either inject a high-power jamming signal to degrade the client's QoT or utilize the intra-channel crosstalk to gather signal leakage from the client for eavesdropping.

2) *Inter-Channel Crosstalk* can be produced in both fibers and BV-WSS'. On one hand, when two lightpaths share the same fiber and their spectrum assignments are spectrally adjacent, their signals can interfere with each other due to fiber nonlinearity. On the other hand, the non-ideal responses of the wavelength multiplexers/de-multiplexers in a BV-WSS can also make their signals interfere when two lightpaths share it. Therefore, the attacking scenarios described for intra-channel crosstalk can also be applied here.

3) *EDFA Gain Competition* means that different FS' can compete for the gain when being amplified by an EDFA. Hence, an FS channel can manipulate the gains of others by changing its own power, and an attacker can easily degrade other clients' QoT as long as they share the same fiber link(s) (i.e., the EDFAs on the link(s)).

B. *Potential Attack Scenarios to RSA Arrangements*

This work considers how to minimize the security threats due to the vulnerabilities mentioned above by arranging the RSA schemes of intra- and inter-domain requests intelligently. Basically, the relations of the RSA schemes of two arbitrary requests in a multi-domain EON can be categorized into the following three scenarios. Fig. 1 shows intuitive examples on them, in which two requests LR_1 and LR_2 are from a legitimate client and a malicious one, respectively.

1) *Node-disjoint*: In this scenario, as shown in Fig. 1(a), since LR_1 and LR_2 do not share any optical components, none of the vulnerabilities will cause security threats.
2) *Node-joint but Link-disjoint*: In this scenario, as LR_1 and LR_2 share a node (i.e., the BV-WSS in it), there will be security threats. If the spectrum assignments of LR_1 and LR_2 overlap with each other as in Fig. 1(b), there will be both intra- and inter-channel crosstalk. Otherwise, if the spectrum assignments are as those in Fig. 1(c), there will be only inter-channel crosstalk.[1]
3) *Link-joint*: Since LR_1 and LR_2 share not only a node but also a fiber link, both inter-channel crosstalk and EDFA gain competition will present.[2] As illustrated by Fig. 1(d), the inter-channel crosstalk can be suppressed by increasing the spacing between the spectrum assignments of LR_1 and LR_2. However, no matter what is the spectral location that LR_1 and LR_2 take, the security threat from EDFA gain competition always exists.

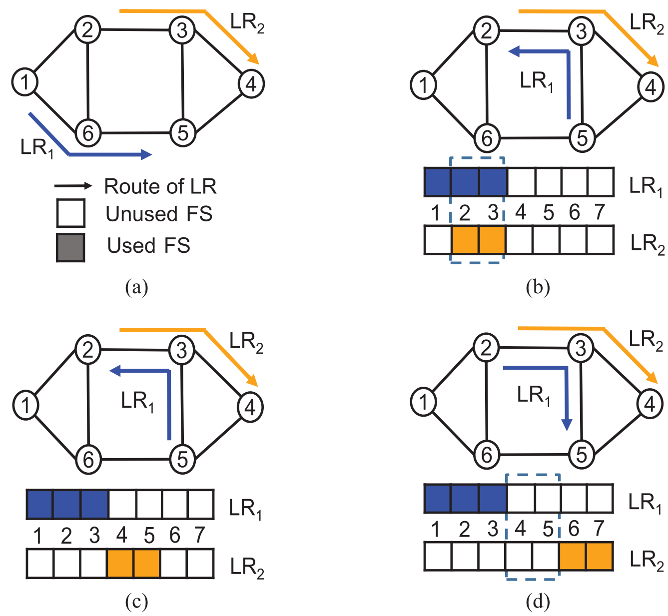

Fig. 1. RSA arrangements in an EON.

Based on the analysis above, we can define an AF to quantify the security threat when LR_1 is from a legitimate client and LR_2 is set up by a malicious one. Specifically, the AFs are α_1, α_2, and α_3 for the node-disjoint, node-joint but link-disjoint, and link-joint scenarios, respectively. Apparently, we should have $\alpha_1 < \alpha_2 < \alpha_3$.

C. *Network Model*

According to the discussions in [3], the domain managers of different domains collaborate to set up an inter-domain lightpath, while each domain manager establish the path segment in its own domain independently. Hence, *w.l.o.g.*, in the rest of the paper, we just analyze the situation in one domain of a multi-domain EON. Basically, we focus on the security issues inside a domain and assume that the cross-domain orchestration can be achieved with the mechanism developed in [3]. We use $G(V, E)$ to represent the topology of one domain in a multi-domain EON, where V and E represent the sets of nodes and fiber links in the domain, respectively. Here, $V_b \subset V$ denotes the set of border nodes, i.e., the ingress/egress points for inter-domain requests. We assume that only the nodes in V_b are equipped with O/E/O converters, and an inter-domain lightpath can change its spectrum assignments on them if necessary. In the mean time, all the signal transmissions inside $G(V, E)$ are established all-optically to save cost and energy. Therefore, we consider translucent domains in this work [32]. There are F FS' on each $e \in E$, and each FS has a bandwidth of 12.5 GHz and provides a capacity of $C_{FS} = 12.5$ Gb/s.

The lightpaths in $G(V, E)$ can be categorized into four types, i.e., LR^{in}, LR^{lv}, LR^{er} and LR^{ps}, respectively. Here, LR^{in}

[1] Note that, inter-channel crosstalk is normally much weaker than intra-channel crosstalk.

[2] Due to the spectrum non-overlapping constraint, LR_1 and LR_2 cannot use overlapped spectrum assignments, and thus there is no intra-channel crosstalk.

is for intra-domain traffic, while LR^{lv}, LR^{er}, and LR^{ps} are all for inter-domain traffic. Specifically, LR^{lv} stands for an inter-domain lightpath that originates from $G(V, E)$, LR^{er} is for the one that ends in $G(V, E)$, and LR^{ps} passes through $G(V, E)$ as an intermediate domain. Then, an LR^{in} can be denoted as $LR_i^{in}(s, d, n)$, where i is its index, $s, d \in V$ are the source and destination, respectively, and n is the bandwidth requirement in FS'. We use $LR_i^{lv}(s, V_b, n)$ to denote an LR^{lv}, since it can use any node in V_b as its egress point to leave $G(V, E)$. Similarly, an LR^{er} and an LR^{ps} have the forms of $LR_i^{er}(V_b, d, n)$ and $LR_i^{ps}(V_b, V_b, n)$, respectively. Here, we do not consider the cross-domain lightpaths that experience O/E/O conversions at the ingress border nodes. This is because one such lightpath can be equivalently treated as either LR^{in} or LR^{lv}, depending on whether its destination is in $G(V, E)$ or not. Basically, the O/E/O conversions eliminate the security threats and the cross-domain lightpaths become trusted ones that originate from the ingress border nodes.

As explained in the previous section, different RSA arrangements bear different security threats, which can be quantified with AF. If an intra-domain lightpath and an inter-domain lightpath are *node-disjoint*, we set AF as $\alpha_1 = 0$, since in this scenario, all the vulnerabilities are avoided. As for the *node-joint but link-disjoint* scenario, we try to make sure that their spectrum assignments do not overlap. Then, we only need to consider the threat from inter-channel crosstalk, and define AF as $\alpha_2 = 1$. When the lightpaths are *link-joint*, we not only ensure that their spectrum assignments do not overlap, but also allocate certain guard-band FS' between them to suppress the threat from inter-channel crosstalk. Therefore, there is only EDFA gain competition left, and we set AF as $\alpha_3 = 3$ since it is the most threatening one.

Basically, in this work, we assume that all the attacks can only be launched from outside of a domain, i.e., all the nodes in the domain are within the trust-zone and can be well maintained by the domain manager to minimize security threats. Then, LR^{er} and LR^{ps} are from untrusted nodes, while LR^{in} and LR^{lv} come from the trust-zone. Since LR^{in} is purely for intra-domain, we should protect it with the highest priority. While for LR^{lv}, we just protect it in the best-effort manner, as it needs to traverse other domains to reach its destination and could also be attacked there (i.e., out of control of this domain). Meanwhile, LR^{er} and LR^{ps} are treated as potential attacks, which need to be quarantined.

In order to improve the overall security-level of the domain, we need to solve the MDAa-RSA problem for both offline and online service provisioning. Specifically, for each LR, we find a feasible RSA scheme to serve it, and minimize the average AF for all the pairs of LR^{in} and LR^{er}/LR^{ps} in the domain. Ideally, the average AF would be zero if we can make sure that all LR^{er} and LR^{ps} are *node-disjoint* with all LR^{in}. However, this is not always feasible, if we consider the constraints from network topology and link capacity. Hence, we need to arrange the RSA schemes of all the lightpaths carefully to ensure that LR^{er}/LR^{ps} and LR^{in} are isolated from each other as much as possible. In offline provisioning, we try to minimize the average AF and spectrum utilization jointly, while in online provisioning, we balance the tradeoff between blocking probability and average AF.

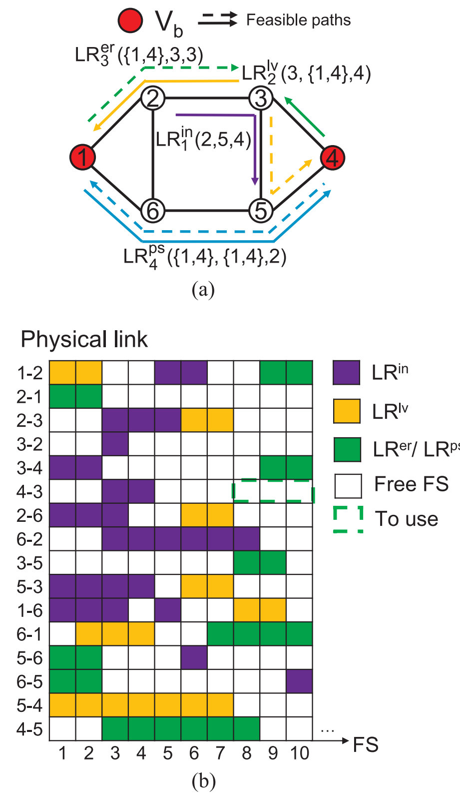

Fig. 2. Example on MDAa-RSA in a domain. (a) Domain topology. (b) Spectrum utilization.

Fig. 2(a) shows an example on $G(V, E)$ with $V_b = \{\text{Node } 1, \text{ Node } 4\}$, which are colored in red. In Fig. 2(a), there are four lightpaths, i.e., $LR_1^{in}(\text{Node } 2, \text{ Node } 5, 4)$, $LR_2^{lv}(\text{Node } 3, \text{ Nodes } \{1,4\}, 4)$, $LR_3^{er}(\text{Nodes } \{1,4\}, \text{ Node } 3, 3)$ and $LR_4^{ps}(\text{Nodes } \{1,4\}, \text{ Nodes } \{1,4\}, 2)$. The feasible routing paths of each lightpath are also marked in Fig. 2(a). For example, LR_3^{er} can use either 4→3 or 1→2→3. If we select 2→3→5 for LR_1^{in}, 4→3 for LR_3^{er} and 1→6→5→4 for LR_4^{ps}, respectively, the network's total AF is 2. Otherwise, if we change the path of LR_3^{er} to 1→2→3 and keep the rest paths unchanged, the network's total AF becomes 4. Therefore, the final paths for the lightpaths are those marked with solid lines in Fig. 2(a). Note that, for LR_2^{lv}, the path 3→5→4 shares *Link* 3→5 with the path 2→3→5 for LR_1^{in}. Hence, for the sake of load-balancing, we select 3→2→1 for LR_2^{lv}.

Fig. 2(b) shows spectrum utilization of the network in Fig. 2(a).[3] Here, in addition to the lightpaths plotted in Fig. 2(a), we consider some background traffics that also occupy FS' on the fiber links. The used FS' are marked with different colors to indicate that they are occupied by different types of lightpaths, i.e., LR^{in}, LR^{lv}, LR^{er}, and LR^{ps}. An example on the spectrum assignment is provided as follows. Since the routing path

[3]Note that, all the topologies considered in this work are assumed to have two bi-directional fibers per link.

of LR_3^{er} is 4→3, we can see in Fig. 2(b) that FS-block $[5, 10]$ on it is available. But in order to isolate LR_3^{er} from all LR^{in}, we cannot use FS-block $[5, 7]$ as FS-block $[3, 4]$ on 4→3 is used by an LR^{in}, assuming that a 3-FS guard-band is needed. Then, we check all the links that is *node-joint* with 4→3 to collect the FS usages on them by LR^{in}, and want to ensure that the spectrum assignment of LR_3^{er} should not overlap with any of these FS usages, for minimizing intra-channel crosstalk. Finally, we select FS-block $[8, 10]$ for LR_3^{er}.

IV. ILP Formulation for MDAa-RSA

In this section, we formulate an ILP model to solve the MDAa-RSA problem exactly. For each node pair in $G(V, E)$, we pre-calculate K shortest paths as the inputs to the ILP.

Parameters:

1) $G(V, E)$: the domain topology.
2) F: the number of FS' on each fiber link.
3) n_i: the bandwidth requirement of LR_i.
4) P_i: the set of feasible routing paths for LR_i.
5) sg: the number of guard-band FS' for request isolation.
6) $\pi_{i,j}$: the boolean indicator that equals 1 if LR_i belongs to LR^{in} and LR_j is an LR^{er} or LR^{ps}, and 0 otherwise.

Variables:

7) x_i^p: the boolean variable that equals 1 if LR_i uses path p in P_i, and 0 otherwise.
8) y_i^e: the boolean variable that equals 1 if LR_i uses link e, and 0 otherwise.
9) w_i^v: the boolean variable that equals 1 if LR_i passes through node v, and 0 otherwise.
10) $z_{i,j}$: the boolean variable that equals 1 if LR_i and LR_j share node(s), and 0 otherwise.
11) $t_{i,j}$: the boolean variable that equals 1 if LR_i and LR_j share node(s) but do not share link(s), and 0 otherwise.
12) $l_{i,j}$: the boolean variable that equals 1 if LR_i and LR_j share link(s), and 0 otherwise.
13) st_i: the integer variable that indicates the start-index of the assigned FS-block for LR_i.
14) ed_i: the integer variable that indicates the end-index of the assigned FS-block for LR_i.
15) $ls_{i,j}$: the boolean variable that equals 1 if st_i is less than st_j, and 0 otherwise.
16) $af_{i,j}$: the integer variable that indicates the corresponding AF of the RSA arrangement for LR_i and LR_j.
17) F_{max}: the integer variable that indicates the maximum index of used FS' on all the fiber links.

Objective:

The objective is to minimize the average AF and the maximum index of used FS' jointly. We define ρ_1 as

$$\rho_1 = \frac{\sum_i \sum_j af_{i,j}}{\sum_i \sum_j \alpha_3}, \qquad \{i, j : \pi_{i,j} = 1\}, \tag{1}$$

which represents the normalized average AF for all the pairs of LR^{in} and LR^{er}/LR^{ps} in the domain, i.e., the overall security-level of the domain decreases with ρ_1, and have ρ_2 as

$$\rho_2 = \frac{F_{max}}{\sum_i n_i} \quad \forall i, \tag{2}$$

which stands for the normalized value of the maximum index of used FS' in the domain, i.e., a smaller ρ_2 indicates that the spectra resources are used in a more compact manner. Then, the optimization objective can be formulated as

$$\text{Minimize} \quad \rho = \eta_1 \cdot \rho_1 + \eta_2 \cdot \rho_2, \tag{3}$$

where η_1 and η_2 are the constants to measure the importance of ρ_1 and ρ_2, respectively. Since both ρ_1 and ρ_2 have been normalized within $[0, 1]$, we set $\eta_1 = \eta_2 = 1$ to make them equally important in the joint optimization.

Constraints:

1) *Routing Constraints:*

$$\sum_{p \in P_i} x_i^p = 1 \quad \forall i. \tag{4}$$

Eq. (4) ensures that there is one and only one path selected for each lightpath

$$y_i^e \geq x_i^p \quad \forall i, \ \{e : e \in p \, \forall p \in P_i\}. \tag{5}$$

Eq. (5) ensures that all the links on path p, which is selected for LR_i, are identified correctly

$$w_i^v \geq x_i^p \quad \forall i, \ \{v : v \in p \quad \forall p \in P_i\}. \tag{6}$$

Eq. (6) ensures that all the nodes on path p, which is selected for LR_i, are identified correctly.

2) *Spectrum Assignment Constraints:*

$$ls_{i,j} + ls_{j,i} \leq 1, \quad \{i, j : i \neq j\}, \tag{7}$$

$$ed_j - st_i + 1 \leq F \cdot (1 + ls_{i,j} - l_{i,j}), \quad \{i, j : i \neq j\}, \tag{8}$$

$$ed_i - st_j + 1 \leq F \cdot (2 - ls_{i,j} - l_{i,j}), \quad \{i, j : i \neq j\}. \tag{9}$$

Eqs. (7)–(9) ensure that the assigned FS' of any two lightpaths satisfy the spectrum non-overlapping constraint if the lightpaths share link(s), and the spectrum assignments also obey the bandwidth capacity constraint

$$\begin{aligned} st_j - ed_i > \quad & sg \cdot \pi_{i,j} \cdot (l_{i,j} + ls_{i,j} - 1) \\ & + F \cdot (ls_{i,j} + l_{i,j} - 2), \quad \{i, j : i \neq j\}, \end{aligned} \tag{10}$$

$$\begin{aligned} st_i - ed_j > \quad & sg \cdot \pi_{i,j} \cdot (l_{i,j} - ls_{i,j}) \\ & + F \cdot (l_{i,j} - ls_{i,j} - 1), \quad \{i, j : i \neq j\}. \end{aligned} \tag{11}$$

Eqs. (10)–(11) ensure that a guard-band of $sg > 0$ FS' can be applied, if LR_i belongs to LR^{in} and LR_j is an LR^{er} or LR^{ps}, and the paths of LR_i and LR_j are *link-joint*

$$st_j - ed_i \geq \pi_{i,j} \cdot (z_{i,j} + ls_{i,j} - 1) + F \cdot (ls_{i,j} + z_{i,j} - 2), \quad \{i, j : i \neq j\}, \tag{12}$$

$$st_i - ed_j \geq \pi_{i,j} \cdot (z_{i,j} - ls_{i,j}) + F \cdot (z_{i,j} - ls_{i,j} - 1), \quad \{i, j : i \neq j\}. \tag{13}$$

Eqs. (12)–(13) ensure that the assigned FS' do not overlap, if LR_i belongs to LR^{in} and LR_j is an LR^{er} or LR^{ps}, and the paths of LR_i and LR_j are *node-joint but link-disjoint*

$$ed_i - st_i + 1 = n_i \quad \forall i, \tag{14}$$

Eq. (14) ensures that each request is offered with enough FS'

$$ed_i, st_i, F_{max}, sg \in (0, F] \quad \forall i, \tag{15}$$

$$ed_i \leq F_{max} \quad \forall i. \tag{16}$$

Eqs. (15) and (16) ensure that the variables are within right ranges and the maximum index of used FS' is obtained correctly.

3) *AF Related Constraints*

$$l_{i,j} \geq y_i^e + y_j^e - 1, \quad \{i, j : i \neq j\} \quad \forall e \in E, \tag{17}$$

$$z_{i,j} \geq w_i^v + w_j^v - 1, \quad \{i, j : i \neq j\} \quad \forall v \in V. \tag{18}$$

Eqs. (17) and (18) ensure that all the common link(s) and common node(s) between LR_i and LR_j are handled

$$t_{i,j} \geq z_{i,j} - l_{i,j}, \quad \{i, j : i \neq j\}, \tag{19}$$

$$af_{i,j} = l_{i,j} \cdot \alpha_3 + t_{i,j} \cdot \alpha_2 + (1 - z_{i,j}) \cdot \alpha_1, \quad \{i, j : i \neq j\}. \tag{20}$$

Eqs. (19) and (20) obtain the AF of any pair of lightpaths.

V. Heuristic Algorithm for MDAa-RSA

Due to its complexity, the ILP model can hardly be applied to solve the MDAa-RSA problem in large-scale networks. Hence, we propose a time-efficient heuristic.

A. Spectrum Assignment

Algorithm 1: Preprocessing for Spectrum Assignment

input : Domain topology $G(V, E)$, request LR_i (for n_i FS'), a selected routing path p for LR_i.
output: Set of available FS-blocks on p Ω.

1 insert all links on p into set L_r^p;
2 **for** *each node* $v \in p$ **do**
3   find all the links in E that starts/ends on v;
4   insert the links in L^p if they are not in L_r^p;
5 **end**
6 get all largest available FS-blocks $\{[w_s, w_e]\}$ on p;
7 $\Omega = \emptyset$, $\mathbf{W} = \{[w_s, w_e]\}$;
8 **for** *each link* $e \in L_r^p$ **do**
9   **for** *each* $[w_s, w_e] \in \mathbf{W}$ **do**
10   **for** $j = 1$ *to* sg **do**
11   **if** $w_s - sg + j - 1$ *is occupied by an incompatible lightpath* **then**
12                 $w_s = w_s + j - 1$;
13   **end**
14   **if** $w_e + sg - j + 1$ *is occupied by an incompatible lightpath* **then**
15                 $w_e = w_e - j + 1$;
16   **end**
17   **end**
18   **if** $w_e - w_s < n_i$ **then**
19   remove $[w_s, w_e]$ from $\mathbf{W}$;
20   **else**
21   insert $[w_s, w_e]$ into Ω;
22   **end**
23   **end**
24 **end**
25 **for** *each link* $e \in L^p$ **do**
26   **for** *each* $[w_s, w_e] \in \Omega$ **do**
27   remove FS' in $[w_s, w_e]$ that are used by incompatible lightpaths on e;
28   transform $[w_s, w_e]$ into feasible FS-blocks for LR_i and use them to replace $[w_s, w_e]$ in Ω;
29   **end**
30 **end**
31 **return** Ω;

Algorithm 1 shows the procedure to preprocess the available FS-blocks on a selected routing path p for a request LR_i. Specifically, to improve the domain's security-level, we purposely block all the spectrum assignment schemes that may lead to security threats and store the rest in Ω as the set of available FS-block on p for LR_i. *Lines* 1–7 are for the initialization. Here, we consider two link sets, i.e., L_r^p stores all the links on p, and L^p includes all the links that are not on p but share one end-node with the link(s) on p. The "largest available FS-blocks" in *Line* 6 means that each of these FS-blocks cannot be expanded further under the spectrum non-overlapping constraint. We denote an FS-block as $[w_s, w_e]$, where w_s and w_e are the start- and end-indices. The for-loop that covers *Lines* 8–24 processes each link in L_r^p to guarantee that a guard-band of sg FS' can be applied if LR_i shares the link with an incompatible lightpath. Here, we say two lightpaths are "incompatible" if one of them is an LR^{in} and the other is an LR^{er} or LR^{ps}, i.e., they should be isolated to avoid security threats. After checking all the links in L_r^p, we store all the feasible FS-blocks on p in Ω. *Lines* 25–30 consider all the links in L^p, and make sure that their spectrum usages will not overlap if LR_i shares node(s) with an incompatible lightpath. Note that, *Line* 28 means that an FS-block can be transformed into a few smaller ones if certain FS' in it have been removed in *Line* 27. In this case, we should ensure that each of the smaller FS-blocks contains at least n_i FS', and then use them to replace the original one (i.e., $[w_s, w_e]$) in Ω.

The complexity of *Lines* 1–7 is $O(|V| \cdot |E|)$. The for-loop covering *Lines* 9–23 will run $F \cdot sg$ times at most, and L_r^p can

Algorithm 2: MDAa-RSA with Partial Comparison

input : Domain topology $G(V, E)$, lightpath request set $\mathbf{LR}$, candidate routing paths $\{P_i\}$.

1 classify requests in $\mathbf{LR}$ as LR^{in}, LR^{lv}, and LR^{er}/LR^{ps} types;
2 sort requests in descending order of bandwidth requirement;
3 **for** $i = 1$ *to* $|\mathbf{LR}|$ **do**
4 $\quad \Lambda = \emptyset$;
5 $\quad$ **for** *each path* p *in* P_i **do**
6 $\quad\quad AF_{tot} = 0$;
7 $\quad\quad$ **if** LR_i *is not an* LR^{lv} **then**
8 $\quad\quad\quad$ **for** *each served request* LR_j *that is incompatible with* LR_i **do**
9 $\quad\quad\quad\quad$ calculate AF of LR_i and LR_j;
10 $\quad\quad\quad\quad AF_{tot} = AF_{tot} + AF$;
11 $\quad\quad\quad$ **end**
12 $\quad\quad\quad$ apply *Algorithm* 1 to get Ω;
13 $\quad\quad\quad$ assign FS' with Ω using first-fit;
14 $\quad\quad$ **else**
15 $\quad\quad\quad$ assign FS' using first-fit;
16 $\quad\quad$ **end**
17 $\quad\quad$ obtain average AF ϖ_t with AF_{tot};
18 $\quad\quad \varpi = \beta \cdot \varpi_t + \gamma \cdot num(p)$;
19 $\quad\quad$ store the RSA scheme and ϖ in Λ;
20 $\quad$ **end**
21 $\quad$ **if** $\Lambda = \emptyset$ **then**
22 $\quad\quad$ mark LR_i as blocked;
23 $\quad$ **else**
24 $\quad\quad$ serve LR_i using RSA with $\min(\varpi)$ in Λ;
25 $\quad\quad$ update network status;
26 $\quad$ **end**
27 **end**

contain $|V| - 1$ links at most. Hence, the complexity of the for-loop that covers *Lines* 8–24 is $O(|V| \cdot F \cdot sg)$. The complexity of *Lines* 25–30 is $O((|E| - |V| + 1) \cdot F)$. Finally, the complexity of *Algorithm* 1 is $O(|V| \cdot |E| + F \cdot (|V| \cdot sg + (|E| - |V|)))$.

B. MDAa-RSA based on Partial Comparison

With the assistance of *Algorithm* 1, we propose an MDAa-RSA algorithm based on partial comparison (MDAa-RSA-PC) and *Algorithm* 2 shows the detailed procedure. *Lines* 1 and 2 are for the initialization. The for-loop that covers *Lines* 3–27 accomplishes the MDAa-RSA procedure. The inner for-loop covering *Lines* 5–20 checks each of its path candidates to find a feasible RSA scheme for LR_i and calculates a weight ϖ with Eq. (21) for the RSA scheme. Specifically, if LR_i is an LR^{in}, LR^{er}, or LR^{ps}, *Lines* 8–13 check each served lightpath that is incompatible with it to obtain the AF between them and update the total AF (i.e., AF_{tot}), otherwise, AF_{tot} stays unchanged. *Line* 17 obtains the average AF ϖ_t by dividing AF_{tot} over the number of served incompatible requests on p. In *Line* 18, we

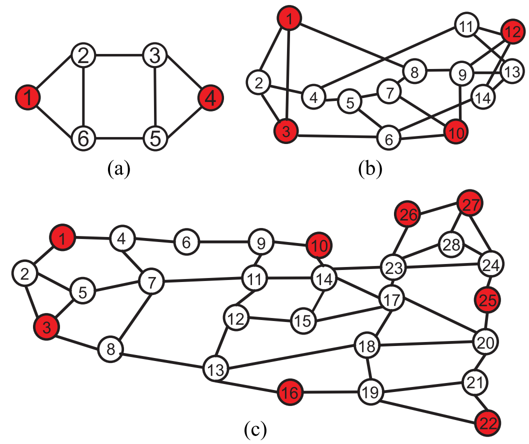

Fig. 3. Domain topologies with border nodes marked as red. (a) Six-node topology. (b) NSFNET topology. (c) US Backbone topology.

assign a weight ϖ to the RSA scheme as

$$\varpi = \beta \cdot \varpi_t + \gamma \cdot num(p), \tag{21}$$

where $num(p)$ returns the number of all the served requests on p, and β and γ are the constants for normalization. Finally, in *Lines* 21–26, we try to provision LR_i using the RSA scheme that has the minimum weight ϖ.

Lines 5–20 will run $K \cdot |V_b|^2 \cdot (|\mathbf{LR}| + |V| \cdot |E| + F \cdot (|V| \cdot sg + (|E| - |V|)))$ times at most, where $|V_b|$ is the number of border nodes, K is the number of routing paths precalculated for each node pair and $|\mathbf{LR}|$ is the total number of lightpaths in the domain. Hence, the overall time complexity of *Algorithm* 2 is $O(|\mathbf{LR}| \cdot K \cdot |V_b|^2 \cdot (|\mathbf{LR}| + |V| \cdot |E| + F \cdot (|V| \cdot sg + (|E| - |V|))))$.

VI. Performance Evaluation

In this section, we evaluate the proposed MDAa-RSA algorithms for both offline and online service provisioning. In order to maintain sufficient statistical accuracy, all the data points discussed in this section are obtained by averaging the results from 50 independent simulations.

A. Offline Service Provisioning

For offline service provisioning, we assume that the link capacity is large enough to accommodate all the lightpaths, which are known in prior. For each request, the source (set) and destination (set) are randomly chosen according to the network model described in Section III-C, and its bandwidth requirement is uniformly distributed within $[1, 20]$ FS'. For the purpose of saving spectrum resources, we set the guard-band as $sg = 3$ FS' for spectral isolation. In a practical multi-domain EON system, a larger sg may be required to suppress inter-channel crosstalk effectively. Basically, there is a performance tradeoff between the efficiency of spectrum utilization and the inter-channel crosstalk suppression. Note that, even though we consider multi-domain service provisioning in this work, we actually focus on improving the physical-layer security-level of a domain where both intra- and inter-domain requests exist. Hence, *w.l.o.g.*, the simu-

TABLE I
RESULTS ON AVERAGE AF ρ_1, MAXIMUM INDEX OF USED FS' F_{max}, AND TOTAL RUNNING TIME (IN SECONDS) IN SIX-NODE TOPOLOGY

# of Requests =	ILP			MDAa-RSA-PC			mSP-FF			mLB-KSP		
$(LR^{in} + LR^{lv} + LR^{er} + LR^{ps})$	ρ_1	F_{max}	Time	ρ_1	F_{max}	Time	ρ_1	F_{max}	Time	ρ_1	F_{max}	Time
$5 = (2 + 1 + 1 + 1)$	0.198	25.6	0.249	0.237	26.8	0.024	0.302	30.3	0.011	0.358	28.6	0.013
$10 = (4 + 3 + 2 + 1)$	0.203	31.7	28.807	0.237	35.3	0.038	0.257	41.0	0.024	0.397	38.5	0.029
$20 = (8 + 6 + 4 + 2)$	0.220	59.7	1701.356	0.253	61.2	0.090	0.262	70.9	0.055	0.395	62.0	0.061

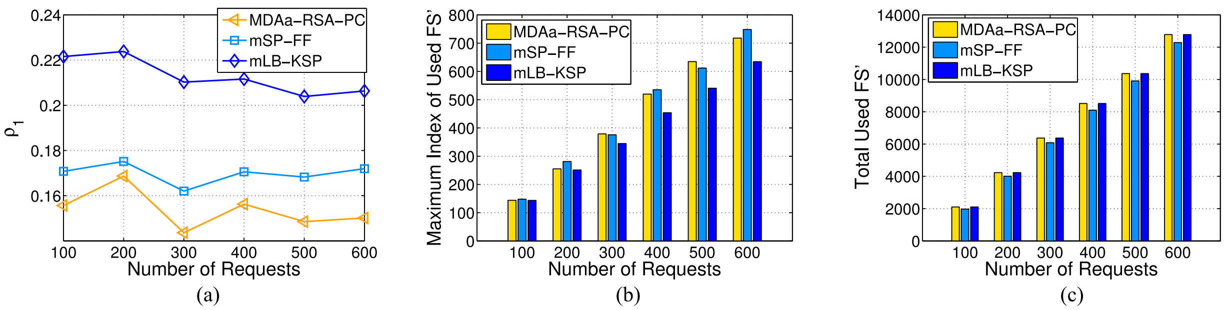

Fig. 4. Offline service provisioning results in NSFNET topology. (a) Average AF ρ_1. (b) Maximum index of used FS' F_{max}. (c) Total used FS'.

TABLE II
RESULTS ON RUNNING TIME PER REQUEST IN NSFNET TOPOLOGY

	Running Time (Seconds)		
# of Requests	MDAa-RSA-PC	mSP-FF	mLB-KSP
100	0.032	0.008	0.008
200	0.039	0.012	0.013
300	0.047	0.017	0.018
400	0.053	0.023	0.025
500	0.060	0.030	0.033
600	0.069	0.037	0.042

lations are still conducted with a single-domain scenario, while a real multi-domain EON can be easily handled by applying the algorithms we develop here to each individual domain in it.

We first use the six-node topology in Fig. 3(a) to compare the performance of the ILP and heuristics. The simulations run on a computer with 3.20 GHz Intel Core i5-4570M CPU and 4 GB RAM. We use Lingo to solve the ILP and implement the heuristics with MATLAB R2011b. We adopt the shortest-path first-fit (SP-FF) in [21] and the load-balanced K shortest-path (LB-KSP) in [20] as benchmarks. Note that, both SP-FF and LB-KSP are not attack-aware, and for fair comparisons, we modify the spectrum assignment mechanisms in them to incorporate certain security considerations. Specifically, if two incompatible lightpaths are *node-joint but link-disjoint*, we guarantee that their spectrum assignments do not overlap, and if they are *link-joint* instead, we make sure that their spectrum usages are separated with a guard-band that includes at least $sg = 3$ FS'. The modified algorithms are referred to as mSP-FF and mLB-KSP in the following discussions.

Table I shows the results, where ρ_1 is the normalized average AF defined in Eq. (1) and F_{max} is the maximum index of used FS' in the EON. As expected, the ILP provides both the smallest ρ_1 and the smallest F_{max} for all the simulation scenarios, and thus solves the optimization in Eq. (3) in the best way. Our proposed attack-aware approach, i.e., MDAa-RSA-PC, follows ILP and performs better than the non-attack-aware benchmarks in terms of balancing ρ_1 and F_{max}. Specifically, it obtains smaller ρ_1 and similar or even smaller F_{max} than mSP-FF and mLB-KSP. Due to its high complexity, ILP takes the longest running time and becomes almost intractable when the number of requests is 20 or more. The heuristics are much more time-efficient than ILP.

We then simulate the heuristics in much larger network topologies with more requests to serve. Here, we use the NSFNET and US Backbone topologies in Fig. 3(b) and (c), and the LR^{in}, LR^{lv}, LR^{er}, and LR^{ps} types of requests are generated according to the ratio of $[6:4:3:1]$, respectively. Fig. 4 shows the results on ρ_1, F_{max}, and total used FS' in the NSFNET topology. In Fig. 4(a), we can see clearly that compared with the non-attack-aware approaches (i.e., mSP-FF and mLB-KSP), our proposed attack-aware algorithm MDAa-RSA-PC always provides smaller average AF ρ_1. This verifies that MDAa-RSA-PC can also provide higher security-levels than benchmarks, when the domain topology becomes larger. Basically, MDAa-RSA-PC considers the potential security threats and try to use the RSA scheme that can minimize AF, while both mSP-FF and mLB-KSP do not address this issue in their RSA scenarios as they treat all the lightpath requests equally. Consequently, mSP-FF and mLB-KSP make intra- and inter-domain requests share more optical components, and thus introduce more potential security threats.

Fig. 4(b) illustrates the results on F_{max} in the NSFNET topology. It is exciting to observe that MDAa-RSA-PC achieves comparable or even smaller results on F_{max}, related to mSP-FF. This attributes to the fact that MDAa-RSA-PC can not only manipulate the RSA arrangements of intra- and inter-domain requests

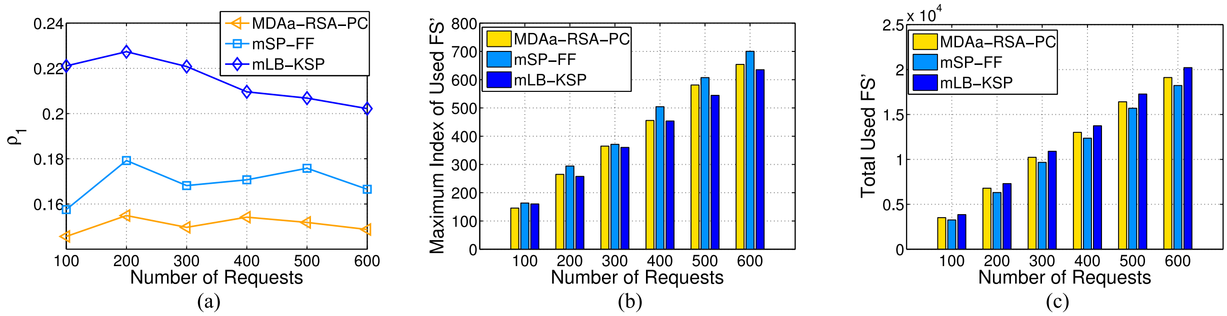

Fig. 5. Offline service provisioning results in US Backbone topology. (a) Average AF ρ_1. (b) Maximum index of used FS' F_{max}. (c) Total used FS'.

for better spectrum isolations, but also load-balance the requests to avoid creating high-load fiber links. Since mLB-KSP considers load-balancing to the largest extent, it provides the smallest F_{max} among all the algorithms. But as it packs the lightpaths in the most compact way, the results on ρ_1 from it are also the largest. In terms of the total used FS', MDAa-RSA-PC and mLB-KSP perform similarly, while mSP-FF uses the least total FS', as shown in Fig. 4(c). This is because mSP-FF always tries to use the shortest path, while MDAa-RSA-PC tries to separate intra- and inter-domain requests and thus may select longer paths. The running time of the algorithms are listed in Table II, which suggests that MDAa-RSA-PC takes more time than the benchmarks, for arranging the RSA schemes intelligently.

We further evaluate the algorithms in an even larger US Backbone topology as shown in Fig. 3(c). Fig. 5 shows the results on ρ_1, F_{max}, and total used FS'. In general, we observe that the results in the US Backbone topology exhibit similar trends as those in the NSFNET topology. However, since the network becomes more connected, MDAa-RSA-PC can load-balance the compatible requests better. This makes it provide smaller F_{max} than mSP-FF and reduce the gap on F_{max} related to mLB-KSP. Also, it is interesting to notice that with regard to the results on total used FS', MDAa-RSA-PC actually performs better than mLB-KSP now. Basically, as the network is more connected, for each request, the possibility of sharing optical components with other incompatible ones increases if it uses a longer path. This motivates MDAa-RSA-PC to choose shorter paths, and hence the total used FS' can be reduced. On the other hand, mLB-KSP does not consider the potential security threats and for the purpose of load-balancing, it may still use relatively long paths. Table III lists the running time of the algorithms. As the topology becomes larger, all the algorithms take longer time to run.

B. *Online Service Provisioning*

The simulations of online service provisioning use the dynamic network scenario, in which the link capacity is limited as $F_{max} = 358$ FS' and the requests can arrive and leave on-the-fly according to the Poisson traffic model. The LR^{in}, LR^{lv}, LR^{er}, and LR^{ps} types of requests are still generated according to the ratio of $[6:4:3:1]$, respectively. Here, we use the K shortest-path (KSP) algorithm in [26] as a benchmark to replace SP-FF, since it is known that KSP can achieve lower blocking probability than SP-FF. Meanwhile, for fair comparisons, we also modify KSP to mKSP to include the attack-aware spectrum assignment mechanisms. We evaluate the performance of online provisioning also with the NSFNET and US Backbone topologies.

TABLE III
RESULTS ON RUNNING TIME PER REQUEST IN US BACKBONE TOPOLOGY

	Running Time (Seconds)		
# of Requests	MDAa-RSA-PC	mSP-FF	mLB-KSP
100	0.074	0.011	0.012
200	0.131	0.019	0.021
300	0.207	0.029	0.032
400	0.296	0.040	0.045
500	0.401	0.054	0.060
600	0.519	0.069	0.077

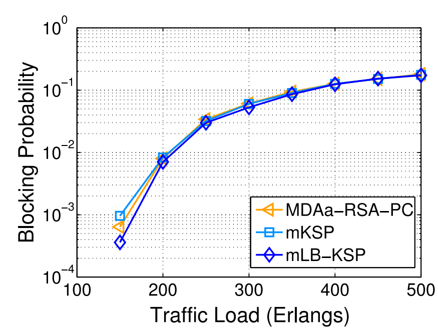

Fig. 6. Blocking probability in NSFNET topology.

Fig. 6 shows the blocking probability in NSFNET topology. We can see that the blocking probability of MDAa-RSA-PC is comparable to those from the non-attack-aware benchmarks (i.e., mLB-KSP and mKSP). Actually, when the traffic load is the lowest as 150 Erlangs, the blocking probability of MDAa-RSA-PC is slightly lower than that of mKSP but higher than that of mLB-KSP. This can be explained as follows. Since mLB-KSP can load-balance the traffic to the largest extent and hence make best use of the spectrum resources, while mKSP always chooses the shortest path that carries enough available spectra and thus can make certain fiber links become congested. Since MDAa-RSA-PC tries to minimize the average AF and to load-balance different types of lightpaths simultaneously, its performance on blocking probability is in between those of mLB-KSP and

TABLE IV
RESULTS ON ρ_1 FOR ONLINE SERVICE PROVISIONING IN NSFNET

	ρ_1		
Traffic Load (Erlangs)	MDAa-RSA-PC	mKSP	mLB-KSP
50	0.149	0.166	0.178
100	0.147	0.167	0.174
150	0.146	0.168	0.173
200	0.151	0.168	0.170
250	0.154	0.171	0.172
300	0.158	0.171	0.172

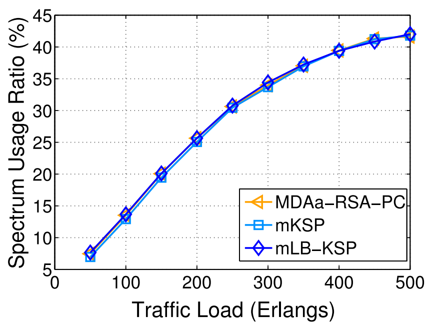

Fig. 7. Spectrum usage ratio in NSFNET topology.

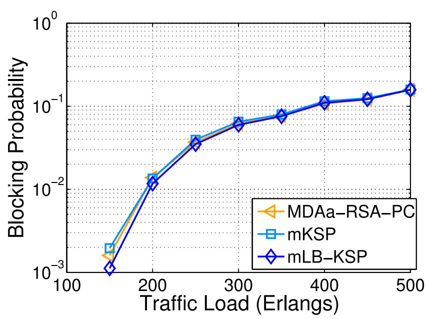

Fig. 8. Blocking probability in US Backbone topology.

mKSP. The results in Table IV verify that MDAa-RSA-PC still provides lower average AF ρ_1 than the benchmarks in online provisioning. In Fig. 7, we show the results on the spectrum usage ratio, which is calculated as the average ratio of used FS' to total FS' in the EON. It can be seen clearly that the results on spectrum usage ratio are almost the same for all the algorithms, which confirms that MDAa-RSA-PC does not use more spectrum resources than the benchmarks.

The results in US Backbone topology are shown in Figs. 8 and 9 and Table V. The results exhibit similar trends as those in NSFNET topology. Note that, the spectrum usage ratio of mKSP is slightly lower than those of MDAa-RSA-PC and mLB-KSP this time. This attributes to the fact that US Backbone topology is more connected, and hence MDAa-RSA-PC and mLB-KSP have more relatively long path candidates to choose from in load-balancing.

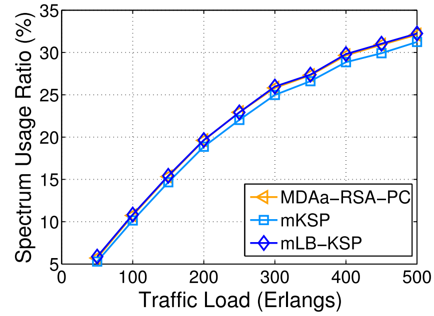

Fig. 9. Spectrum usage ratio in US Backbone topology.

TABLE V
RESULTS ON ρ_1 FOR ONLINE SERVICE PROVISIONING IN US BACKBONE

	ρ_1		
Traffic Load (Erlangs)	MDAa-RSA-PC	mKSP	mLB-KSP
50	0.142	0.164	0.176
100	0.147	0.166	0.172
150	0.146	0.167	0.169
200	0.146	0.167	0.167
250	0.149	0.165	0.165
300	0.146	0.161	0.160

VII. CONCLUSION

This paper investigated the MDAa-RSA problem in multi-domain EONs. We first formulated an ILP model to solve the problem exactly and then designed a time-efficient heuristic. Simulation results of offline provisioning demonstrated that in a small-scale network, the heuristic achieved near-optimal solutions but with much less computation time than the ILP. While in a relatively large-scale network, our algorithm also provided higher security-levels and similar or even better spectrum usage than several existing ones. For online provisioning, simulation results verified that our proposed heuristic could balance the performance tradeoff between request blocking and network security-level well.

REFERENCES

[1] P. Lu, L. Zhang, X. Liu, J. Yao, and Z. Zhu, "Highly-efficient data migration and backup for big data applications in elastic optical inter-datacenter networks," *IEEE Netw.*, vol. 29, no. 5, pp. 36–42, Sep./Oct. 2015.

[2] R. Mao, H. Xu, W. Wu, J. Li, Y. Li, and M. Lu, "Overcoming the challenge of variety: Big Data abstraction, the next evolution of data management for AAL communication systems," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 42–47, Jan. 2015.

[3] Z. Zhu, C. Chen, X. Chen, S. Ma, L. Liu, X. Feng, and S. Yoo, "Demonstration of cooperative resource allocation in an OpenFlow-controlled multidomain and multinational SD-EON testbed," *J. Lightw. Technol.*, vol. 33, no. 8, pp. 1508–1514, Apr. 2015.

[4] R. Casellas, R. Martinez, R. Munoz, R. Vilalta, L. Liu, T. Tsuritani, and I. Morita, "Control and management of flexi-grid optical networks with an integrated stateful path computation element and OpenFlow controller," *J. Opt. Commun. Netw.*, vol. 5, pp. A57–A65, Oct. 2013.

[5] S. Yoo, "Multi-domain cognitive optical software defined networks with market-driven brokers," in *Proc. Eur. Conf. Opt. Commun.*, Sep. 2014, pp. 1–3.

[6] Z. Zhu, X. Chen, C. Chen, S. Ma, M. Zhang, L. Liu, and S. Yoo, "OpenFlow-assisted online defragmentation in single-/multi-domain

software-defined elastic optical networks," *J. Opt. Commun. Netw.*, vol. 7, pp. A7–A15, Jan. 2015.

[7] M. Medard, D. Marquis, R. Barry, and S. Finn, "Security issues in all-optical networks," *IEEE Netw.*, vol. 11, no. 3, pp. 42–48, May 1997.

[8] K. Shaneman and S. Gray, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection prevention," in *Proc. Military Commun. Conf.*, Oct. 2004, pp. 711–716.

[9] R. Rejeb, M. Leeson, and R. Green, "Fault and attack management in all-optical networks," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 79–86, Nov. 2006.

[10] Y. Du, F. Xue, and S. Yoo, "Security enhancement of SPECTS O-CDMA through concealment against upstream DPSK eavesdropping," *J. Lightw. Technol.*, vol. 25, no. 9, pp. 2799–2806, Sep. 2007.

[11] M. Fok, Z. Wang, Y. Deng, and P. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[12] A. Lazzez, "All-optical networks: Security issues analysis," *J. Opt. Commun. Netw.*, vol. 7, pp. 136–145, Mar. 2015.

[13] N. Skorin-Kapov and M. Furdek, "Limiting the propagation of intra-channel crosstalk attacks in optical networks through wavelength assignment," in *Prof. Opt. Fiber Commun. Conf.*, Mar. 2009, pp. 1–3.

[14] 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.

[15] 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, no. 3, pp. 750–760, Jun. 2010.

[16] M. Furdek, N. Skorin-Kapov, S. Zsigmond, and L. Wosinska, "Vulnerabilities and security issues in optical networks," in *Proc. Int. Conf. Transp. Opt. Netw.*, Jul. 2014, pp. 1–4.

[17] K. Manousakis and G. Ellinas, "Attack-aware planning of transparent optical networks," *Opt. Switch. Netw.*, vol. 19, pp. 97–109, Jan. 2016.

[18] 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, no. 7, pp. 2970–2978, Jul. 2013.

[19] 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, no. 5, pp. 1014–1023, Mar. 2014.

[20] Y. Wang, X. Cao, and Y. Pan, "A study of the routing and spectrum allocation in spectrum-sliced elastic optical path networks," in *Proc. INFOCOM*, Apr. 2011, pp. 1503–1511.

[21] K. Christodoulopoulos, I. Tomkos, and E. Varvarigos, "Elastic bandwidth allocation in flexible OFDM-based optical networks," *J. Lightw. Technol.*, vol. 29, no. 9, pp. 1354–1366, May 2011.

[22] L. Gong, X. Zhou, W. Lu, and Z. Zhu, "A two-population based evolutionary approach for optimizing routing, modulation and spectrum assignments (RMSA) in O-OFDM networks," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1520–1523, Sep. 2012.

[23] X. Zhou, W. Lu, L. Gong, and Z. Zhu, "Dynamic RMSA in elastic optical networks with an adaptive genetic algorithm," in *Proc. GLOBECOM*, Dec. 2012, pp. 2912–2917.

[24] W. Lu and Z. Zhu, "Dynamic service provisioning of advance reservation requests in elastic optical networks," *J. Lightw. Technol.*, vol. 31, no. 10, pp. 1621–1627, May 2013.

[25] L. Gong, W. Zhao, Y. Wen, and Z. Zhu, "Dynamic transparent virtual network embedding over elastic optical infrastructures," in *Proc. Int. Conf. Commun.*, Jun. 2013, pp. 3466–3470.

[26] 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, no. 1, pp. 15–22, Jan. 2013.

[27] Y. Yin, M. Zhang, Z. Zhu, and S. Yoo, "Fragmentation-aware routing, modulation and spectrum assignment algorithms in elastic optical networks," in *Proc. Opt. Fiber Commun. Conf.*, Mar. 2013, pp. 1–3.

[28] S. Ma, C. Chen, S. Li, M. Zhang, S. Li, Y. Shao, Z. Zhu, L. Liu, and S. Yoo, "Demonstration of online spectrum defragmentation enabled by OpenFlow in software-defined elastic optical networks," in *Proc. Opt. Fiber Commun. Conf.*, Mar. 2014, pp. 1–3.

[29] C. Chen, X. Chen, M. Zhang, S. Ma, Y. Shao, S. Li, M. Suleiman, and Z. Zhu, "Demonstrations of efficient online spectrum defragmentation in software-defined elastic optical networks," *J. Lightw. Technol.*, vol. 32, no. 24, pp. 4701–4711, Dec. 2014.

[30] N. Skorin-Kapov, M. Furdek, R. Aparicio Pardo, and P. Pavon Marino, "Wavelength assignment for in-band crosstalk attacks in optical networks: ILP formulations and heuristic algorithms," *Eur. J. Oper. Res.*, vol. 222, pp. 418–429, Nov. 2012.

[31] Z. Zhu, M. Funabashi, Z. Pan, B. Xiang, L. Paraschis, and S. Yoo, "Jitter and amplitude noise accumulations in cascaded all-optical regenerators," *J. Lightw. Technol.*, vol. 26, no. 12, pp. 1640–1652, Jun. 2008.

[32] Z. Zhu, X. Chen, F. Ji, L. Zhang, F. Farahmand, and J. Jue, "Energy-efficient translucent optical transport networks with mixed regenerator placement," *J. Lightw. Technol.*, vol. 30, no. 19, pp. 3147–3156, Oct. 2012.

Authors' biographies not available at the time of publication.