Attack-aware Lightpath Provisioning in Elastic Optical Networks with Traffic Demand Variations

Konstantinos Manousakis[1], Tania Panayiotou[1], Panayiotis Kolios[1], Ioannis Tomkos[2] and Georgios Ellinas[1]
[1]*KIOS Research and Innovation Center of Excellence, Department of Electrical and Computer Engineering, University of Cyprus, 1678 Nicosia, Cyprus*
{manouso, panayiotou.tania, pkolios, gellinas}@ucy.ac.cy
[2]*Athens Information Technology, Marousi, 15125 Athens, Greece*
itom@ait.gr

***Abstract*—This work considers lightpath provisioning in elastic optical networks with traffic demand variations while accounting for the impact of jamming attacks. Traffic requests are modeled based on their variation in traffic and a number of network traffic scenarios are pre-computed. Variations in traffic are used in order to design the network with improved resilience to jamming attacks in the general case, without considering a specific traffic matrix. The mathematical formulation and heuristic algorithms proposed in this work jointly consider the routing and spectrum allocation problem for the pre-computed network scenarios, aiming to minimize the required lightpath reallocations and the number of wavelength selective switches (WSSs) placed at specific network nodes/ports so as to minimize the impact of jamming attacks. Performance results demonstrate the benefits of this approach in terms of required lightpath reallocations, number of WSSs, as well as computational time required for dynamically reconfiguring the network when considering traffic demand variations.**

I. Introduction

The ever increasing traffic demand of core networks is expected to be supported by elastic optical networks (EONs), as in EONs the spectrum is more efficiently utilized, using finer slot granularity, compared to wavelength division multiplexed (WDM) networks. In addition to the increasing traffic demands, a big challenge for the network operators is to cope with traffic demand variations and guarantee network availability for the requested connections. For example, traffic demand variations can occur due to several bandwidth consuming applications/services (e.g., 3D video, cloud computing) as well as popular events (e.g., Olympic Games, World Cup) and will necessitate more frequent network reconfigurations so as to satisfy the user demands and manage the network resources more efficiently [1].

Usually, in order to satisfy the network requests, network operators overprovision the network, leading to a waste of resources and increased operational and capital expenditures (opex/capex). For this reason, several other approaches have been proposed in the literature that reconfigure the network so that it closely follows the traffic demand variations [2]–[5]. Generally, proactive network optimization is initially required prior to the demand requests, followed, in real time, by network reconfiguration. With the right network design and real-time support, network operators can handle the expected traffic demand, even during popular events [6].

Further, for establishing a connection in EONs, the routing and spectrum allocation (RSA) problem must be solved, satisfying the spectrum continuity, contiguity, and non-overlapping constraints [7]. In addition to the aforementioned constraints, the crosstalk effect must also be taken into account when provisioning a new connection (both for the new connections as well as the already established ones), since crosstalk not only degrades the signal quality [8] but it can also be used to spread a jamming attack throughout the network [9], [10]. These attacks can have an even more devastating effect during popular events, as they can cause significant service disruption and affect a large part of the telecommunication network.

A. Previous Work

The concept of attack-aware algorithms in WDM networks to solve the routing and wavelength assignment (RWA) problem was presented in [11]–[13] having as an objective the minimization of the impact of high-power jamming attacks. In these works, apart from the attack-aware RWA problem, equalizer placement [14], monitor placement [15], and dedicated path protection [16] were also considered. The concept of jamming attacks in EONs has been considered in [17]–[20]. Authors in [17] address the problem of physical-layer security in multi-domain flexible grid optical networks, proposing to differentiate the routing and spectrum allocation (RSA) schemes of intra- and inter-domain requests with security considerations. Authors in [18] solve the problem of attack-aware service provisioning in one domain of multi-domain EONs to improve network scalability using game theory techniques. Further, authors in [19] propose an Integer Linear Program (ILP) for the crosstalk-aware RSA problem, while in [20], they propose a crosstalk-aware RSA together with a wavelength selective switch (WSS) placement technique to eliminate intra-band crosstalk. In that work, initially, all network nodes (reconfigurable add/drop multiplexers - ROADMs) are assumed to have a broadcast-and-select (BS) architecture, with splitters and WSSs at the input and output ports, respectively. The algorithm decides on the replacement of some of the splitters with WSSs at the input stage of the BS-based architecture in order to compensate for the in-band crosstalk interactions among lightpaths. In fact, the algorithm tries to achieve zero crosstalk interactions and in the cases where it is not possible, WSSs are placed to compensate for these interactions.

In the aforementioned works, the authors assume that the traffic demand is static and that it can be known a priori. Therefore, none of these works considers traffic demand variations and lightpath reallocations that are required for such traffic, while at the same time considering the impact of intra-band jamming attacks, which is precisely the focus of this work.

Further, it is also important to note that there exist several works in the literature that reallocate the lightpaths considering dynamic traffic or variations in traffic [24]–[26]. However, none of these works considers how one network configuration can affect the other configurations, nor do they consider the crosstalk effect, thus, the proposed solutions can result in high network blocking probabilities.

B. Our Contribution

In this work, the attack-aware (Aa)-RSA and WSS placement problems in EONs (with the WSS placement problem following the procedure described above [20]) are solved for satisfying jointly several sets of connection requests (demand scenarios). A demand scenario is defined as a possible demand state that can be found based on traffic demand variations (by considering the stochastic nature of the traffic that varies with time [21], [22]). The proposed algorithms use models that take advantage of the fact that probability distributions governing the traffic demands are known or can be estimated. Therefore, the traffic is modeled in order to precompute a number of possible configurations that have high probability to appear in the network.

The output of the problem solution is a set of network configurations, where a network configuration is a RSA solution and the WSS placement for each demand scenario. The network configurations are computed offline and can be used online for dynamic reconfiguration of the network in order to meet the traffic demand variations. One of the problem objectives is to minimize the required lightpath reallocations between different network configurations. Another objective of the problem is to minimize the number of required WSSs for all the possible demand scenarios in order to compensate for the crosstalk effect and therefore to minimize the impact of jamming attacks.

The novelty of this work is the design of optimization as well as heuristic algorithms that jointly consider the crosstalk-aware RSA problem with WSS placement and the lightpath reallocations between different demand scenarios. Thus, the solutions consider the network configurations jointly in order to avoid lightpath reallocations. In addition, the WSS placement considers the variations in traffic and places the WSSs not only at specific nodes but also decides in which node ports to place the WSSs in order to satisfy jointly the network configurations, for every possible traffic demand scenario.

Consequently, the algorithms reduce both the capex, by minimizing the required number of WSSs, and the opex, by minimizing the number of lightpath reallocations and thus reducing the computational complexity and time required in the path computation element (PCE) for reconfiguring the network upon variations in the traffic demand.

The reader should note that in this work the term reconfiguration is used to denote the change between one configuration of the network to another (in terms of established lightpaths), while the term reallocation is used to denote the tear-down and the setup of a lightpath (leading to service disruption) in order to meet the variation in traffic.

The rest of the paper is organized as follows. Section II presents the traffic demand modeling, while Section III presents the concept of jamming attacks and WSS placement. Section IV provides the mathematical formulation of the problem. Section V presents the proposed attack-aware RSA heuristic algorithms, while performance results are discussed in Section VI. Finally, Section VII offers some concluding remarks and avenues for future work.

II. Modeling Traffic Demands

In this work, without loss of generality, during normal network operation, we assume traffic that is log-normally distributed and each connection is described by its own distribution as described in [21], [22] (note that any other traffic distribution can also be applied in this work). Further, regarding traffic modeling during popular events, we assume that each connection is described by its expected bandwidth demand during the occurrence of the specific event. On this basis, the traffic demand for each connection n during normal network operation is described by $Z_n \sim LN(\mu_n, \sigma_n^2)$ and during popular events is described by a fixed value e_n^i, where e_n^i denotes the expected bandwidth demand of connection n during the occurrence of the i^{th} event.

For normal network operation, we find the distribution describing the probability of the network being at a particular state (demand scenario) $s = \{d_n\}_{n=1}^N$, where N is the number of connections in scenario s, and d_n is the bandwidth demand of connection n. For finding such a distribution, Monte Carlo simulations are performed, by sampling the discretized $\{Z_n\}_{n=1}^N$ distributions. Regarding popular events, the assumption is that these events are known in advance and occur with certainty at particular time intervals. Their related states (demand scenarios) can be easily found by the $\{e_n^i\}_{i=1}^N$ values. Upon the occurrence of such events, the network switches to some pre-computed network configurations.

Finding the discretized distribution allows us to find the possible traffic demand scenarios of the network and accordingly to solve the crosstalk-aware RSA problem for different network configurations. Each distribution is a function of the bandwidth demand that is measured according to the requested number of spectrum slots. Even though the requested number of spectrum slots depends on several factors, such as the transmission distance, the modulation format, and the quality-of-transmission (QoT) requirements, for simplicity, and without loss of generality, we assume that the distributions directly reflect the requested number of spectrum slots; an assumption that does not affect the scope of this work. As the number of possible scenarios may render the crosstalk-aware RSA problem computationally intractable, the scenarios that rarely appear, are not considered while solving this problem. These scenarios, if they appear, can be handled dynamically.

III. Jamming Attacks and WSS Placement in EONs

In-band crosstalk in optical networks is the result of power leakage between two signals on the same wavelength crossing an optical node. In-band crosstalk must be addressed in optical networks, as it not only causes optical signal degradation but it can be potentially used to launch high-power in-band jamming attacks in the network (an attacker injects a high-power signal at an optical node on the same wavelength as the information carrying signal). A high-power jamming signal can cause significant leakage inside the switches between lightpaths that are on the same wavelength as the attacking signal, resulting in lightpath signals that cannot be recovered at their respective receivers. It is further important to note that these affected lightpaths become secondary attackers, affecting other lightpaths on the same wavelength that they encounter at other switching nodes along their path, and so on. Thus, the high-power jamming attack can potentially spread through the network affecting a large number of lightpaths [13]. Several of the works mentioned in Section I tried to address this problem by solving the RWA/RSA problems in WDM/EON networks respectively in such a way that if an attack happens the propagation effect is minimized [11]–[13], [19].

To address such an attack, other works [20] proposed algorithms that initially aim to minimize the crosstalk interactions among lightpaths as much as possible (through crosstalk-aware RSA), trying to achieve zero interactions. If this is not possible, then splitters are replaced by WSSs at the input stage of the ROADMs where there are lightpath interactions through in-band crosstalk (utilizing the minimum required number) in order to further compensate for the crosstalk effect and minimize the impact of a jamming attack. The replacement of a few splitters with WSSs at specific locations of the network will maintain the network cost low while at the same time the crosstalk effect will be decreased with the use of the WSSs. Therefore, the impact of jamming attacks will be minimized.

In this work, the problem of the placement of WSSs is further explored in order to cover a set of demand scenarios. In this case, each of the demand scenarios must be satisfied, while the WSSs must be placed in positions that also satisfy all the different demand scenarios. Thus, the RSA solution of each set must be taken into account by the other demand sets in order for the total number of required WSSs to be minimized.

IV. Attack-Aware RSA and WSS Placement Formulation

A mathematical formulation is presented in this section for the efficient establishment of connections in EONs with traffic demand variations. To capture the uncertainties in the traffic demand, mathematical optimization is employed through scenario construction, where the number of required lightpath reallocations as well as the number of WSSs are minimized for the sum of deterministic equivalent instances. Note that the in-band crosstalk interactions are minimized per scenario, whereas the minimum number and the placement of WSSs are chosen in order to satisfy all demand scenarios.

In particular, the attack-aware RSA and WSS placement problem is solved having as an objective to minimize spectrum utilization, the number of lightpath reallocations, and also the number of required WSSs. The proposed algorithm consists of two phases; in the first phase, k candidate paths are identified for each source-destination pair by employing a k-shortest path algorithm [23], while in the second phase the problem is formulated taking as input the output of the first phase (i.e., the set of k candidate paths). Its parameters, variables, and objective/constraints are shown below:

Parameters:

- $(d, s) \in D_s$: a demand d for scenario s
- $f \in F$: a spectrum slot over the available spectrum slots
- $p \in P$: a candidate path
- $l \in E$: a network link
- F_d^s: required number of slots for demand d of scenario s
- S: set of all scenarios
- P_d: set of candidate paths to serve demand d
- π_s: probability for scenario s to occur
- B, M: large constants that are used to activate/deactivate a constraint, where $M \gg B$

Variables:

- x_{pf}^s: Boolean variable for the s^{th} realization, equal to 1 if path p and frequency slot f are used to serve demand d and equal to 0 otherwise.
- y_{pf} Boolean variable, equal to 1 if frequency slot f is the starting spectrum slot of a contiguous spectrum to serve demand d over path p and equal to 0 otherwise.
- z_l: Boolean variable, equal to 1 if there exists a WSS at the end of link l and equal to 0 otherwise.

Objective: *Minimize* :

$$\sum_s \pi_s \sum_p \sum_f c_1 \cdot x_{pf}^s + \sum_l c_2 \cdot z_l + \sum_p \sum_f c_3 \cdot y_{pf} \quad (1)$$

Subject to the following constraints:

- Demand constraint

$$\sum_{p \in P_d} \sum_f x_{pf}^s = F_d^s, \forall (d, s) \in D_s, \forall s \in S \quad (2)$$

- Contiguity constraint

$$x_{pf}^s - x_{p(f-1)}^s \leq y_{pf}, \forall p \in P, \forall f \in F, \forall s \in S \quad (3)$$

Case: $f = 1$, then, $x_{p(f-1)}^s = 0$, $\forall s \in S$

- Non-overlapping spectrum

$$\sum_{p|l \in p} x_{pf}^s \leq 1, \forall l \in E, \forall f \in F, \forall s \in S \quad (4)$$

- Jamming interactions and WSS placement

$$\sum_{\{p'|m \in p, p'\}} x_{p'f}^s + B \cdot x_{pf}^s - M \cdot z_l \leq B, \quad (5)$$

$\forall l \in p, \forall p \in P, \forall f \in F, \forall s \in S$

The objective function, (Eq. 1) accounts for (i) the number of required frequency slots, (ii) the number of required WSSs, and (iii) the number of required reallocations. Each coefficient c_i ($i = 1, 2, 3$), declares the relative impact of each term of the objective. The frequency slot minimization is considered based on the probability π_s associated with a particular scenario. This means that a scenario that is more probable to happen will have a higher impact on the objective function.

In addition, a number of x^s_{pf} Boolean variables are activated to satisfy the different scenarios. Hence, a number of path-slot pairs are assigned for each source-destination request, that are jointly optimized to minimize the objective function. Note that the assignment for each demand scenario s is decided based on the assignment for every other scenario, thus the path-slot pairs are chosen in such a way so as to minimize the overall cost indicated in the objective function.

Constraint 1 (Eq. 2) ensures that all lightpaths have a total capacity equal to the requested demand for each of the realizations and thus all incoming traffic is satisfied. Constraint 2 (Eq. 3) ensures that each demand is assigned contiguous spectrum on all the fibers of each path. Specifically, this constraint counts the transitions from zero to one. In this way, variable y_{pf} keeps track of the starting frequency slot to serve a demand. Variable y_{pf} is the same for all the different scenario realizations. Therefore, taking into account the objective and this constraint the spectrum and path reallocations are minimized as much as possible. Constraint 3 (Eq. 4) is the non-overlapping spectrum constraint and ensures that each spectrum slot is used at most once on each fiber for each scenario realization. Note that the spectrum continuity constraint (each demand is assigned the same spectrum along all the edges of the path) in this formulation is taken into account via the definition of the x^s_{pf} variable. Finally, Constraint 4 (Eq. 5) is included in order to account for the in-band jamming interactions and to minimize the number of required WSSs. In Constraint 4, B and M are constants (taking large values), where $M \gg B$. The reason for introducing constant B is to take into account only the constraints for the lightpaths that will be used from all the candidate lightpaths (activate/deactivate the constraint). Additionally, the reason for introducing constant M is to account for the replacement of splitters with WSSs (activate/deactivate the constraint). In Constraint 4, $\sum_{\{p'|m \in p,p'\}} x^s_{p'f}$ is the total number of in-band crosstalk interfering sources that affect the signal of lightpath (p, f) at node m for the s^{th} scenario, while variable z_l specifies where to place the required WSSs. Note that node n in Constraint 4 is the end-node of link l. Based on the objective function, the WSSs are placed at specific locations inside the network nodes in order to satisfy all the different scenarios under consideration.

V. Attack-aware Expansion/Reduction RSA Heuristic Algorithm

To solve the problem utilizing an algorithmic approach, we propose the *attack-aware expansion/reduction* RSA (*Aa-ER-RSA*) heuristic algorithm that aims at finding a set of network configurations that (i) supports all possible traffic demand scenarios, (ii) minimizes the number of WSSs required for handling the crosstalk effect, and (iii) minimizes the service interruptions that may occur during switching between sequential (in time) configurations (including configurations that support popular events). To achieve this, the proposed algorithm finds a set of network configurations that are similar (as much as possible) in their lightpaths (routing paths and allocated spectrum) and support the possible future demand when appropriately expanding/reducing [24] the allocated spectrum of each lightpath. By doing so, we aim to reduce the number of WSSs required for supporting all the possible network configurations and minimizing the service disruptions that may occur during switching between sequential (in time) network configurations.

The *Aa-ER-RSA* algorithm is compared to a complete reallocation attack-aware RSA algorithm (*Aa-REC-RSA*) that solves the provisioning problem for each scenario without considering the configurations found in previous scenarios (only the WSSs found from previous network configurations are considered). Thus, a compete lightpath reallocation takes place for each scenario, aiming to minimize the number of WSSs required for supporting all the possible demand scenarios. In general, with the usage of the expansion/reduction policy, traffic interruptions can be avoided [25] but the resources may not be efficiently utilized amongst the established connections. Compared to the expansion/reduction policy, the complete reallocation policy requires higher computational complexity and complex algorithms in the PCE for minimizing traffic interruptions [26]. Both the *Aa-ER-RSA* and *Aa-REC-RSA* heuristics are described in Algorithm 1, while the expansion/reduction (ER) procedure of the *Aa-ER-RSA* heuristic is described in Algorithm 2.

Algorithm 1 Aa-*x*-RSA Heuristic Algorithm

Input: The set $S = \{s_i\}_{i=1}^{D}$, where s_i is a demand scenario with $\pi_{s_i} > p$. Set S is sorted in descending order with the scenario demanding the maximum cumulative spectrum placed first on the list.

Output: The sets W and $\{C_{s_i}\}_{i=1}^{D}$, where W is the set of WSSs and C_{s_i} is the set of established lightpaths for demand scenario s_i.

```
W → ∅
C_{s_i} → ∅ ∀s_i ∈ S
for i = 1 to D do
    if i = 1 OR x = Rec then
        Solve the Aa-REC-RSA problem for all connections in s_i
        Update sets C_{s_i} and W
    else
        Solve Algorithm 2
        Update sets C_{s_i} and W (updates in W may occur only
        from the reallocated connections)
    end if
end for
Return sets C_{s_i} ∀s_i ∈ S, and W
```

In general, both heuristics (Algorithm 1) start from the traffic demand scenario s demanding the maximum cumulative bandwidth and continue to scenario s' with a cumulative

Algorithm 2 ER Algorithm

1: Identify in s_i the connections that remain unchanged, need to be reduced or expanded in their spectrum when compared to their allocated spectrum at $s_{(i-1)}$.
2: From $C_{s_{(i-1)}}$ add in C_{s_i} the lightpaths that remain unchanged or need to be reduced in their spectrum.
3: In C_{s_i} update the information regarding the allocated spectrum of the lightpaths that need to be reduced in their spectrum (by removing the necessary number of slots, starting from the rightmost slot, and shifting the central frequency accordingly).
4: In C_{s_i} add from $C_{s_{(i-1)}}$ the lightpaths where expansion is feasible and update in C_{s_i} information regarding their allocated spectrum (by adding the necessary number of slots, starting from the rightmost slot, and shifting the central frequency accordingly).
5: For each connection in s_i that its expansion is not feasible, solve the Aa-RSA problem (reallocate).

bandwidth that is closer to that of the previous scenario. Specifically, the Aa-*x*-RSA problem is solved for each scenario, s, by taking into account the previous WSS placement. For the first scenario (s) on the sorted list or when reallocation is needed (i.e., when the REC procedure is followed (*x*=REC) or when connection expansion is not feasible in the ER procedure (*x*=ER)), the heuristic solves the Aa-RSA problem as follows: For the routing procedure, it calculates k-shortest paths and for each one of the k paths the spectrum allocation is solved according to the first-fit scheme. Among the candidate lightpaths, the one that yields the minimum *crosstalk penalty* is chosen, where the crosstalk penalty, r_j, for the j^{th} lightpath is defined as the number of nodes the j^{th} lightpath overlaps (on its allocated spectrum) with the already established lightpaths. If the minimum crosstalk penalty is not zero, WSSs are placed at the necessary network nodes' input ports for eliminating the crosstalk effect among the overlapping connections.

The reader should note that as the number of possible scenarios may render the problem computationally intractable, the scenarios that rarely appear are not be considered during *Aa-x-RSA*. Specifically, in this work, the heuristics are solved for all scenarios s with $\pi_s > p$, where p is a probability threshold used so as not to consider the scenarios that rarely occur. These rare scenarios can be handled online given the placement of the WSSs.

VI. Performance Results

To evaluate the performance of the proposed optimization and heuristic algorithms, a small network with 6 nodes and 9 links, and the generic Deutsche Telekom (DT) network with 14 nodes and 23 links (Fig. 1), were considered, and each spectrum slot was assumed to occupy 12.5GHz. For solving the mathematical formulation, the Gurobi library was used [27] and a PC with Core $i5-2400@3.1$GHz and 16GB memory was used for the simulation environment. The proposed algorithms are investigated and compared for different metrics; number of required WSSs, number of lightpath reallocations, and running times. In this work, it is assumed that the network has some traffic demands that vary over time based on a log-normal distribution (other distributions can be considered as well) and some fixed connections, where their bandwidth demand was set to be constant for all the different scenarios (the requested number of slots was chosen uniformly between 0 and 5). For all connections, the source destination pairs were chosen randomly. Further, ten (10) executions corresponding to different traffic instances for each traffic load were performed and for all simulations the network resources were enough to establish all connections (i.e., the blocking probability was set to zero in order to fairly compare all approaches in terms of the investigated metrics). The mathematical formulation and the *Aa-ER-RSA* heuristic algorithm are compared with the *Aa-REC-RSA* heuristic algorithm to illustrate the benefits to network planning and operation when jointly considering the crosstalk-aware RSA problem with WSS placement and the lightpath reallocations between different demand scenarios. It is noted that the coefficients c_i of the objective functions (Eq. 1) were set equal to one ($c_i = 1$), since it is assumed that all the terms equally contribute to the objective function. Different values for these coefficients can be used when the monetary cost of using a spectrum slot, reallocating a connection and the cost of the WSS is determined.

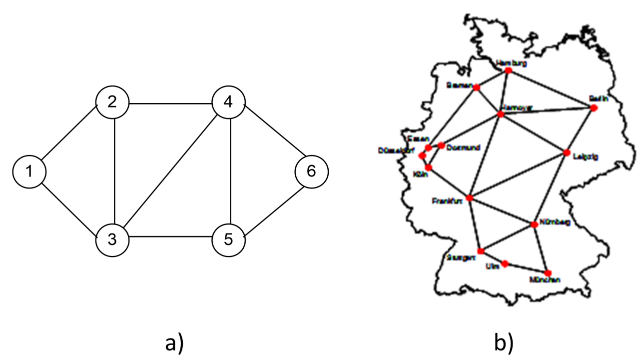

Fig. 1. (a) 6-node network, and (b) DT network topology.

A. Results for the 6-node Network

For the 6-node network, six of the connections follow the log-normal distribution, whereas the rest are set to be static. We assume that the 6-node network supports 30 slots per link. Each connection's bandwidth demand was assumed to take values between 2 and 10 slots (increasing by 2 slots between sequential intervals). Monte Carlo simulations returned 23 scenarios with probability $p \geq 10^{-2}$. The mean numbers of requested slots (static and log-normal) per scenario are shown in Table I. This table depicts a comparison of the proposed mathematical formulation and the heuristic algorithms for the requested connections with respect to the objective performance and the required running time for different mean numbers of requested slots per scenario.

The *Aa-REC-RSA* algorithm is used as a benchmark for lightpath reallocations. In this case, the required number of reallocations is high compared to the rest of the algorithms that have as an objective the minimization of the lightpath reallocations. Specifically, it is shown that the *Aa-ER-RSA* heuristic

TABLE I
6-NODE NETWORK RESULTS (W:NUMBER OF WSSS, R: NUMBER OF REALLOCATIONS,T:RUNNING TIME)

Mean slot requests	Formulation			*Aa-ER-RSA*			*Aa-REC-RSA*		
	W	R	T	W	R	T	W	R	T
33	0	0	2.7m	0	0	0.55s	0	95	10s
47	0	0	25h	5	0	1.86s	6	329	38s
59	0	0	48h	10	0	2.5s	10	380	46s
75	4	0	48h	11	0	2.5s	15	483	53s
85	4	1	48h	11	0	2.55s	18	502	1m
100	7	2	48h	14	0	2.77s	18	512	1m

algorithm requires no lightpath reallocations for all cases under consideration and has better performance compared to the mathematical formulation, since the optimization algorithm requires $1-2$ reallocations for the examined scenarios. However, the mathematical formulation requires less number of WSSs to compensate for the crosstalk-related interactions among lightpaths compared to the *Aa-ER-RSA* heuristic algorithm. This occurs due to the fact that the *Aa-ER-RSA* heuristic algorithm has as a primary objective the minimization of the number of lightpath reallocations and as a secondary objective the minimization of WSSs, whereas the optimization algorithm tries to jointly optimize the number of required frequency slots, the number of lightpath reallocations, as well as the number of required WSSs.

The mathematical formulation found the best bound (optimal solution) for the first two cases in 3 minutes and 25 hours, respectively. For the rest of the cases, the optimal solution cannot be found and the algorithm terminated due to the time limit that was set to 48 hours, as the running time of the mathematical formulation increases exponentially with the traffic load. On the other hand, the *Aa-ER-RSA* heuristic required less than 3 minutes of running time for all the cases under consideration. The reader should note that this time period is just for planning purposes and that the online adaptation can be performed on the order of seconds or even milliseconds [28]. It must also be noted that the performance of crosstalk-unaware algorithms exhibit high number of lightpath interactions irrespective of the number of scenarios considered (one or more scenarios) and thus require a high number of WSSs [20].

B. Results for the DT Network

For the DT network, 10 of the connections follow the log-normal distribution, whereas the rest are set to be static. The DT network is assumed to support 300 slots per link. Each connection's bandwidth demand was assumed to take values between 2 and 10 slots (increasing by 2 slots between sequential intervals). Monte Carlo simulations returned 707 scenarios with probability $p \geq 10^{-2}$. In this scenario, only the heuristics are implemented and compared as the mathematical formulation cannot be implemented due to the large network size.

As can be seen from Figs. 2 - 4, the *Aa-ER-RSA* algorithm significantly outperforms *Aa-REC-RSA* for all metrics considered. Note that due to the high running time (62 hours)

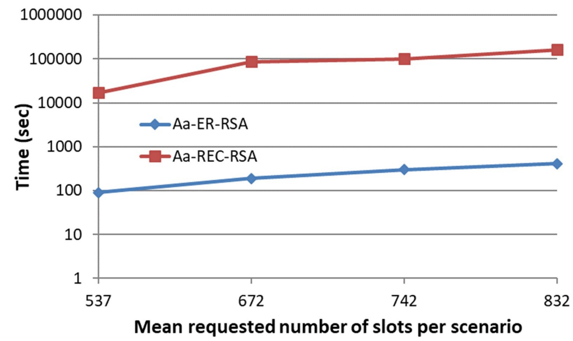

Fig. 2. Running time vs. mean requested number of slots per scenario.

required by *Aa-REC-RSA* for the case of 832 requested slots (Fig. 2), we have chosen not to examine any other scenario requesting a larger number of slots. Also, note that *Aa-ER-RSA*, even for the case of 832 requested slots, ran in only a few minutes, as it does not need to recompute the lightpaths for every scenario and for every connection within each scenario, since it follows an expansion/reduction policy for adjusting the spectrum of the already established connections. On the contrary, *Aa-REC-RSA* recomputes the lightpaths for every scenario and for every connection within each scenario, leading to both an increased computational time (Fig. 2) and an increased number of reallocations (Fig. 4) and as a consequence an increased number of service interruptions.

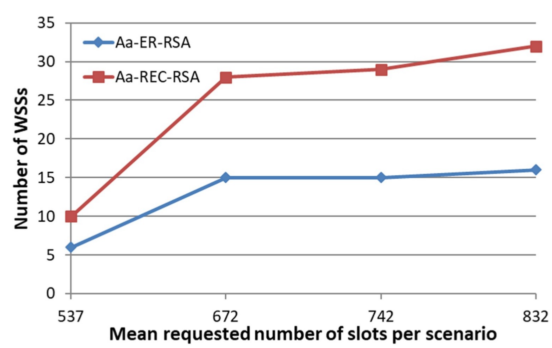

Fig. 3. Number of WSSs vs. mean requested number of slots per scenario.

Regarding the number of WSSs, *Aa-ER-RSA* requires significantly fewer WSSs than *Aa-REC-RSA* as can be seen in Fig. 3. This is due to the fact that *Aa-ER-RSA* finds a set of network configurations that are similar in their computed lightpaths and for which the crosstalk effect can be mitigated by "almost" the same set of WSSs. In contrast, *Aa-REC-RSA* has to find a new network configuration for each scenario without taking into account the WSSs that are already placed in the network.

VII. CONCLUSIONS

This work proposed attack-aware RSA optimization and heuristic algorithms in EONs, that consider a set of different scenarios representing demands with uncertainty that vary

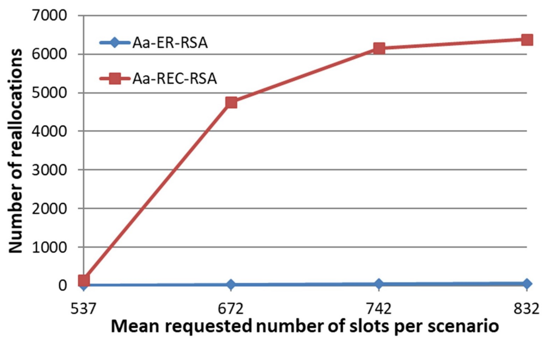

Fig. 4. Number of reallocations vs. mean requested number of slots per scenario.

over time. The aim of these algorithms is to minimize the number of WSSs, placed at the input ports of specific network nodes, required to mitigate the crosstalk effect, and thus the spread of an attack, as well as to minimize the required lightpath reallocations between different traffic scenarios. Thus, the proposed technique reduces both the network capex and opex, by minimizing the required number of WSSs and the number of lightpath reallocations upon variations in the traffic demand. Performance results demonstrate the effectiveness of the heuristic algorithm in terms of computational time, as the proposed heuristic performs close to the results of the mathematical formulation, while outperforming the complete reallocation policy.

Future works will explore decomposition techniques for the mathematical formulation so as to address larger network problems. In addition, online reconfigurability of the network with samples from the distributions of the connections will be examined.

Acknowledgment

This work has been partially supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 739551 (KIOS CoE) and from the Government of the Republic of Cyprus through the Directorate General for European Programmes, Coordination and Development. It was also partially supported by the Cyprus Research and Innovation Foundation under project CULTURE/AWARD-YR/0418/0014. This article is based upon work from COST Action CA15127 (Resilient communication services protecting end-user applications from disaster-based failures RECODIS) supported by COST (European Cooperation in Science and Technology).

References

[1] Cisco white paper, "The Zettabyte Era: Trends and Analysis," 2017.

[2] R. Alvizu, S. Troia, G. Maier and A. Pattavina, "Matheuristic with Machine-learning-based Prediction for Software-defined Mobile Metro-core Networks," *IEEE/OSA Journal of Optical Communications and Networking*, 9(9):19–30, 2017.

[3] F. Morales, M. Ruiz, L. Gifre, L. M. Contreras, V. Lopez and L. Velasco, "Virtual Network Topology Adaptability based on Data Analytics for Traffic Prediction," *IEEE/OSA Journal of Optical Communications and Networking*, 9(1):35–45, 2017.

[4] N. Fernández et al., "Virtual Topology Reconfiguration in Optical Networks by means of Cognition: Evaluation and Experimental Validation," *IEEE/OSA J. of Opt. Commun. Netw.*, 7(1):162–173, 2015.

[5] T. Panayiotou, K. Manousakis, S. P. Chatzis and G. Ellinas, "A Data-Driven Bandwidth Allocation Framework with QoS Considerations for EONs," *IEEE/OSA J. of Lightw. Techn.*, 37(9):1853–1864, May 2019.

[6] Ericsson, "Ericsson Mobility Report", https://www.ericsson.com/en/mobility-report/reports/june-2018, 2018.

[7] K. Christodoulopoulos, I. Tomkos and E. A. Varvarigos, "Elastic Bandwidth Allocation in Flexible OFDM-based Optical Networks," *IEEE/OSA Journal of Lightwave Technology*, 29(9):1354–1366, 2011.

[8] M. Filer and S. Tibuleac, "N-degree ROADM Architecture Comparison: Broadcast-and-select versus Route-and-select in 120 Gb/s DP-QPSK Transmission Systems," *Proc. IEEE/OSA OFC*, San Francisco, CA, 2014.

[9] N. Skorin-Kapov, M. Furdek, S. Zsigmond and L. Wosinska, "Physical-layer Security in Evolving Optical Networks," *IEEE Comm. Magazine*, 54(8):110-117, 2016.

[10] M. Furdek et al., "An Overview of Security Challenges in Communication Networks," *Proc. IEEE International Workshop on Resilient Networks Design and Modeling (RNDM)*, Halmstad, pp. 43-50, 2016.

[11] N. Skorin-Kapov, et al., "A New Approach to Optical Networks Security: Attack-aware Routing and Wavelength Assignment," *IEEE/ACM Transactions on Networking*, 18(3):750760, 2010.

[12] N. Skorin-Kapov, et al., "Wavelength Assignment for Reducing In-band Crosstalk Attack Propagation in Optical Networks: ILP Formulations and Heuristic Algorithms," *Eur. J. of Oper. Res.*, 222(3):418–429, 2012.

[13] K. Manousakis and G. Ellinas, "Attack-aware Planning of Transparent Optical Networks," *Optical Switc. and Netw.*, 19(2):97–109, 2016.

[14] K. Manousakis and G. Ellinas, "Equalizer Placement and Wavelength Selective Switch Architecture for Optical Network Security," *Proc. IEEE Symposium on Computers and Communication (ISCC)*, 2015.

[15] D. Monoyios, K. Manousakis, C. Christodoulou, K. Vlachos, and G. Ellinas, "Attack-aware Resource Planning and Sparse Monitor Placement in Optical Networks", *Optical Switching and Netw.*, 29:46–56, 2018.

[16] M. Furdek, N. Skorin-Kapov and L. Wosinska, "Attack-Aware Dedicated Path Protection in Optical Networks," *IEEE/OSA Journal of Lightwave Technology*, 34(4):1050-1061, 2016.

[17] J. Zhu, B. Zhao, W. Lu, and Z. Zhu, "Attack-Aware Service Provisioning to Enhance Physical-Layer Security in Multi-Domain EONs," *IEEE/OSA Journal of Lightwave Technology*, 34(11):2645-2655, 2016.

[18] J. Zhu, B. Zhao and Z. Zhu, "Leveraging Game Theory to Achieve Efficient Attack-Aware Service Provisioning in EONs," *IEEE/OSA Journal of Lightwave Technology*, 35(10):1785–1796, 2017.

[19] K. Manousakis and G. Ellinas, "Crosstalk-aware Routing and Spectrum Assignment in Flexible Grid Networks," *Proc. IEEE Symposium on Computers and Communication (ISCC)*, Messina, Italy, 2016.

[20] K. Manousakis and G. Ellinas, "Crosstalk-Aware Routing Spectrum Assignment and WSS Placement in Flexible Grid Optical Networks," *IEEE/OSA Journal of Lightwave Technology*, 35(9):1477–1489, 2017.

[21] I. Antoniou, et al., "On the Log-normal Distribution of Network Traffic," *Physica D, Nonlinear Phenomena*, 167(12):72–85, 2002.

[22] M. Kassim, et al., "Statistical Analysis and Modeling of Internet Traffic IP-Based Network for Tele-traffic Engineering," *ARPN J. of Eng. and Applied Sciences*, 10(3):1505–1512, 2015.

[23] J.Y. Yen, "Finding the k Shortest Loopless Paths in a Network," *Management Science*, 17(11):712–716, 1971.

[24] K. Christodoulopoulos, I. Tomkos, and E. Varvarigos, "Time-Varying Spectrum Allocation Policies and Blocking Analysis in Flexible Optical Networks," *IEEE J. on Sel. Areas in Commun.*, 31(1):13–25, 2013.

[25] F. Cugini, et al., "Push-pull Defragmentation without Traffic Disruption in Flexible Grid Optical Networks," *IEEE/OSA Journal of Lightwave Technology*, 31(1):125–133, 2013.

[26] M. Klinkowski, et al., "Elastic Spectrum Allocation for Time-Varying Traffic in FlexGrid Optical Networks," *IEEE J. on Sel. Areas in Commun.*, 31(1):26–38, 2013.

[27] Gurobi Optimization, Inc. "Gurobi Optimizer Reference Manual," 2016, http://www.gurobi.com

[28] Int. Telecommun. Union, "Architecture for the Automatically Switched Optical Network", Rec. ITU-T G.8080, Geneva, Switzerland, 2012.