IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 25, 2021, accepted February 2, 2021, date of publication February 9, 2021, date of current version February 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3058259

High-Power Jamming Attack Mitigation Techniques in Spectrally-Spatially Flexible Optical Networks

GIANNIS SAVVA[1], (Graduate Student Member, IEEE), KONSTANTINOS MANOUSAKIS[1], (Senior Member, IEEE), JACEK RAK[2], (Senior Member, IEEE), IOANNIS TOMKOS[3], (Fellow, IEEE), AND GEORGIOS ELLINAS[1], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering and KIOS Research and Innovation Center of Excellence, University of Cyprus, 1678 Nicosia, Cyprus
[2]Department of Computer Communications, Gdańsk University of Technology, 80-233 Gdańsk, Poland
[3]Department of Electrical and Computer Engineering, University of Patras, 265 04 Patras, Greece

Corresponding author: Giannis Savva (savva.giannis@ucy.ac.cy)

This article is based on 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); *http://www.cost.eu*. 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 (REALFON).

ABSTRACT This work presents efficient connection provisioning techniques mitigating high-power jamming attacks in spectrally-spatially flexible optical networks (SS-FONs) utilizing multicore fibers. High-power jamming attacks are modeled based on their impact on the lightpaths’ quality of transmission (QoT) through inter-core crosstalk. Based on a desired threshold on a lightpath’s QoT, the modulation format used, the length of the path, as well as a set of physical layer characteristics, each lightpath can potentially tolerate a high-power jamming attack. In this paper, an integer linear program is thus formulated, as well as heuristic algorithms to solve the problem of attack-aware routing, spectrum, modulation format, and core allocation in SS-FONs, aiming to both efficiently provision the network in terms of network resources, as well as minimize the impact of high-power jamming attacks on the established lightpaths. Extensive simulation results are obtained for several algorithm variants with different objectives, demonstrating the validity and efficiency of the proposed techniques that can effectively mitigate high-power jamming attacks, by minimizing the number of inter-core interactions, while at the same time establishing connections with high spectral efficiency.

INDEX TERMS Physical layer security, multicore fibers, routing spectrum and core allocation, jamming attacks, quality of transmission, integer linear programming.

I. INTRODUCTION

Elastic optical networks (EONs) that use finer spectrum granularity (frequency slots of 6.25, 12.5, and 25GHz compared to 50GHz of wavelength-division multiplexed (WDM) networks), in addition to transponders that can transmit data in several contiguous slots, have been proposed as a viable technology to address the increasing capacity crunch in optical networks [1]. As the required capacity is expected to further increase with the advent of 5G networks [2], space division multiplexing (SDM) technology is also considered to support the new era of optical networks, as it provides one additional dimension to increase capacity. Networks that combine both the spatial and the spectrum dimensions are called spectrally-spatially flexible optical networks (SS-FONs). In particular, multicore fibers (MCFs), multi-mode fibers (MMFs), few-mode multicore fibers (FM-MCFs), or even bundles of single mode fibers (SMFs) are envisioned to be used in the implementation of SS-FONs [3].

To provision a connection in SS-FONs, the routing, modulation format, spectrum, and core allocation (RMSCA) problem must be solved. This problem includes finding a path,

The associate editor coordinating the review of this manuscript and approving it for publication was Qunbi Zhuge.

the appropriate modulation format, the required spectrum, and the core in the path that can be allocated for a given set of demands [4]. A feasible spectrum allocation solution must satisfy several constraints, namely the spectrum *continuity*, *contiguity*, and *non-overlapping* constraints. In addition, the *core continuity* constraint must be satisfied (i.e., each connection must use the same core from source to destination), as joint switching (J-Sw) is assumed in this work. The reader should note that there also exist other more relaxed core switching architectures, such as independent switching (Ind-Sw), where information on any core can be switched independently to any other core, and fractional joint switching (Fr J-Sw), where information on a core within a group of cores can be directed to any other core within another specific group of cores [5]. Clearly, each switching architecture varies in terms of performance, flexibility, and hardware cost [6]–[8]. However, the Ind-Sw and Fr J-Sw architectures are not considered, as the aim is to keep the switching constraints as strict as possible (i.e., investigate the worst-case scenario).

As in optical networks attacks can compromise a large amount of data, significant effort has been placed on the security of these networks [9], mainly focusing on the prevention of service disruption attacks (high-power jamming attacks) and unauthorized access to information (eavesdropping attacks) [10]–[15]. The focus of this work is on service disruption, via the injection of high-power signals. These high-power signals can directly affect other existing connections through crosstalk interactions (primary attack), as well as spread the attack to other parts of the network, through crosstalk interactions with affected lightpaths that essentially become secondary attackers [14]. Thus, when designing the network, crosstalk interactions must be minimized, so as to consequently minimize the potential spread of a high-power jamming attack.

It should be noted that reconfigurable optical add-drop multiplexers (ROADMs) with variable optical attenuators (VOAs) can be deployed to limit the effects of a high-power jamming attack by regulating the output power of transiting signals. However, in such an architecture, significant effects (e.g., increased induced crosstalk due to spectral broadening effects) can cause signal degradation on co-propagating channels on the link where the jamming signal is inserted [16]. Also, the jamming signal can propagate to other links depending on the power of the signal and the operation region of the associated VOAs [17]. Further, wavelength selective switched (WSS)-based ROADMs could be utilized, with high-port isolation WSSs, to thwart high-power signals. However, with increasing traffic demand (that substantially increases lightpath interactions through the crosstalk effect at the WSSs), WSS isolation must also be increased equivalently [18]. Thus, considering that high-port isolation WSSs are costly, and that the number of WSS ports increases substantially with increased traffic demand, deploying components that achieve sufficient crosstalk isolation in SS-FONs can increase substantially the network deployment cost.

Hence, during the network design phase, different kinds of attack models can be considered, including a jamming attack that affects only the link on which it is inserted (i.e., thwarted at the next node) – requiring, however, a higher deployment cost – or an attack that propagates along the connection (utilizing networks with a lower deployment cost). In this work, the latter attack scenario is assumed, where jamming attacks can affect every lightpath at every point of interaction.

Nevertheless, it is also worth noting here that optimization as to the required crosstalk isolation levels for a particular ROADM architecture and a given network topology and traffic matrix is also possible with our approach, while considering the crosstalk-related performance of the utilized components within the ROADM. The goal would be to identify the ROADM design and associated components' crosstalk specifications that will keep the network performance within acceptable limits. In such a way, unnecessarily high-cost WSSs could be avoided and design flexibility would be allowed, as the chosen solution would be up to the network operator and the budget that has available in order to offer improved quality of service (QoS), in case that this is required by the service level agreements (SLAs). Such an approach, even though outside of the scope of this work, is noted here as a possible avenue for future research work.

To consider the impact of jamming attacks, the quality of transmission (QoT) of all connections is examined, by taking into account the physical-layer impairments (PLIs) during network design, so as to prevent service disruption under jamming attack operation in SS-FONs. Specifically, the main contributions of this work include:

- Addressing the RMSCA problem, taking also into account the impact of high-power jamming attacks on the signal quality of the established lightpaths. To assess this impact, inter-core interactions through the crosstalk effect are modeled using our extended version of the QoT estimator-tool [19].
- Formulating this new problem (attack-aware RMSCA (Aa-RMSCA)) as an integer linear program (ILP), together with efficient techniques for minimizing the search space of the ILP. Specifically, precise models for PLIs affecting the signal are used to measure the QoT of each connection and also PLIs in combination with the input power of the signal are embedded as additional constraints to the Aa-RMSCA problem. The ILP aims to minimize both the impact of high-power jamming attacks on the established lightpaths, as well as the usage of network resources. In this work, during the network design phase, a worst-case attack scenario is assumed, where jamming attacks can affect every lightpath at every point of interaction (i.e., a jamming attack propagates along the connection and/or multiple attacks are simultaneously deployed in the network). It is worth noting that for the ILP formulation proposed in this work, by tuning specific input parameters of the ILP, different node architectures (e.g., WSSs are placed

at specific locations within certain nodes) as well as specific types of jamming attacks (e.g., a jamming attack that only affects the link on which it is inserted) can be considered.
- Proposing jamming-aware heuristic algorithms to handle large scale instances, as well as additional ILPs and heuristics that are used as benchmarks and for comparison purposes, to ascertain the penalty of network operation under jamming attacks in terms of blocking rate, network resources, and running times.

To the best of our knowledge, this is the first time that such an approach is used to explore high-power jamming attacks in SS-FONs, by minimizing their impact during the network design phase, while efficiently using the network's spectrum resources.

The rest of the paper is organized as follows. Section II overviews the related work on SS-FONs, while Section III describes the problem addressed in this work. Section IV presents the security considerations as well as the modeling of jamming attacks in SS-FONs. Section V details the proposed ILP formulation for the Aa-RMSCA problem, while Section VI includes the proposed heuristic algorithms. Performance results are discussed in Section VII, while Section VIII presents some concluding remarks and possible avenues for future research.

II. RELATED WORK

As optical networks are vulnerable to high-power jamming attacks, the research community has investigated various mitigation techniques for such attacks, mostly during the design phase of the network. Most works in the literature address high-power jamming attacks related to WDM networks, where authors solve the problem of routing and wavelength assignment (RWA) with the objective to minimize the crosstalk interactions [14], [20], [21] and as a consequence, to minimize the impact of jamming attacks. Recent works also consider the problem of jamming attack detection using machine learning techniques [22]–[24]. Moreover, other works deal with the problem of jamming attacks in EONs, investigating physical-layer security in multi-domain networks [25], attack-aware RSA in conjunction with wavelength selective switch (WSS) placement algorithms [26], and jamming effects within the physical layer model for a dynamic traffic scenario [27].

Furthermore, considerable research effort has been devoted to the problem of routing, spectrum, and core allocation (RSCA) in SS-FONs. Authors in [4] survey the various resource allocation schemes and algorithms that aim to efficiently and optimally use network resources in SS-FONs, while in [28] authors study a similar problem, namely the baud rate, modulation format, core and spectrum assignment (BMCSA) problem over a single link, considering distance-adaptive reaches for different baud rates, modulation formats, and crosstalk impairments. It is shown that the latter problem is NP-hard even for a single link, and ILPs as well as heuristic approaches are proposed to solve the problem for large traffic instances. In addition, authors in [29]–[34] solve the RSCA problem, while also considering the crosstalk effect, in order to improve the performance of SDM flexible optical networks with MCFs. In a similar vein, authors in [30] propose a core prioritization policy based on the MCF's architecture to reduce crosstalk by avoiding the utilization of adjacent cores. Also, in [35], authors investigate the problem of establishing a lightpath for a connection, such that the inter-core crosstalk between the new lightpath and any existing lightpaths does not degrade the QoT for any lightpath below a set threshold, utilizing either a technique based on static/worst-case crosstalk or one that uses dynamic/precise crosstalk estimation. Moreover, in [36], [37] the authors propose crosstalk-aware spectrum allocation algorithms that focus on spectrum defragmentation in SS-FONs. Additional related works in the literature solve the RSCA problem for SS-FONs operating with MCFs while taking into account physical layer impairments (including crosstalk) having as their objective to increase the spectral efficiency of the network [29], [38]. Finally, the authors in [39] present a methodology to estimate the worst-case transmission reach of the optical signals (at different bit rates and modulation formats) across MCFs given real laboratory crosstalk measurements. They also present an ILP formulation for the design of a flex-grid/SDM optical transport network that makes use of the transmission reach estimations.

A number of works also addresses scalability issues for these problems. For example, to minimize computational complexity for large sets of requests, various solutions are presented such as grouping cores [30] and combining spectrum and spatial dimensions into virtualized resources [40]. Metaheuristic approaches are also a good match for the RSCA problem, since they are able to provide near-optimal solutions for large networks in less time compared to the ILP formulations. For example, in [39] authors propose an effective simulated annealing (SA)-based metaheuristic able to solve large problem instances with reasonable execution times. Further, authors in [41], [42] utilize evolutionary, tabu search, and greedy randomized adaptive search metaheuristic approaches to solve the RSCA problem offering several capabilities (e.g., anycasting and protection) to the connections in the network. Finally, a crosstalk worst-case and a crosstalk-aware ILP formulation for the RSCA problem is proposed in [43], and in [44] the routing, modulation level, space, and spectrum assignment (RMLSSA) problem is formulated as an ILP, while a step-wise greedy heuristic algorithm is proposed when the problem scales to larger sizes.

The effects of high-power jamming attacks in SS-FONs are assessed in [45], where authors investigate the jamming-induced reduction of the signal reach for different bit rates and modulation formats and subsequently use the obtained reach limitations to derive the maximal traffic disruption at the network level during normal network operation. To evaluate the impact of jamming attacks, the authors consider a worst-case attack scenario where

the jamming signal traverses all fiber links in the network. Moreover, authors in [46] propose attack-aware routing, spectrum, and core assignment algorithms that aim to reduce crosstalk-interactions for both static network planning and dynamic network provisioning using ILP and heuristic algorithms.

Clearly, there is a large body of work on mitigating jamming attacks in WDM and elastic optical networks, as well as on RSCA/RMSCA in SS-FONs with and without crosstalk consideration. However, the state-of-the-art on the mitigation of jamming attacks in SS-FONs is limited, and as also previously mentioned in Section I, this work differs from the existing literature, as this is the first time that an Aa-RMSCA algorithm is designed to account for the physical layer jamming attacks by considering analytical models for the PLIs of established connections.

III. PROBLEM DESCRIPTION

In this work, the Aa-RMSCA problem is solved for a given set of static connection requests in MCF-based SS-FONs under a jamming attack scenario. It should be noted that the focus is on in-band jamming attacks, where inter-core crosstalk can affect the connection, while any out-of-band jamming attacks are omitted, as the use of guardbands for each connection is assumed. Specifically, the objectives of the problem are the following:

- Minimize the impact on the QoT of all established lightpaths in the case of high-power jamming attacks.
- Minimize the required spectrum resources in order to establish the set of the connection requests (total used spectrum or the maximum id of the used spectrum).

Due to the formulation utilized, connection blocking because of physical layer impairments (i.e., QoT below a predefined threshold) is also minimized as much as possible. It should be noted though that the blocking rate will depend on the values of the jamming signal power levels, as well as other factors such as the modulation format, the requested bit rate, the number of connections, and the interactions among lightpaths.

In general, three different approaches can be used to establish a set of connections in SS-FONs: (i) **Min-RMSCA**: Minimizes the required spectrum. Jamming attacks and PLIs are not taken into account and the QoT of each lightpath is evaluated after all connections are established in the network (developed as a benchmark). (ii) **MinLI-RMSCA**: Minimizes lightpath interactions (i.e., minimize the number of inter-core interactions) regardless of the impact on the QoT of each lightpath. QoTs are evaluated after all connections are established in the network (developed as a benchmark). (iii) **Aa-RMSCA**: Considers the impact of inter-core lightpath interactions on the QoT of each lightpath (i.e., in some cases, spectrum slots with the same id in adjacent cores can be simultaneously utilized, allowing inter-core interactions based on the impact on the QoT of each lightpath), while minimizing spectrum resources due to PLIs (proposed approach).

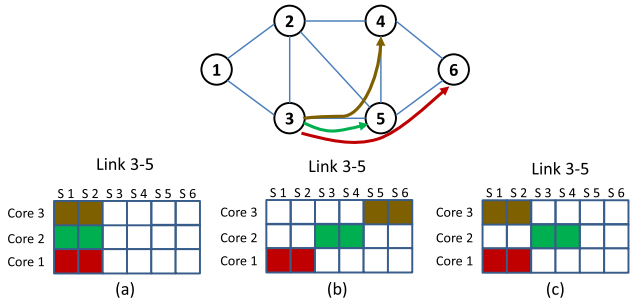

FIGURE 1. Link (3 – 5) slot assignments for the three lightpaths when the three different techniques are utilized: (a) Min-RMSCA, (b) MinLI-RMSCA, and (c) Aa-RMSCA.

Figure 1 illustrates a simple example of the three aforementioned approaches assuming a 6-node network and three connection requests, $\{3-4, 3-5, 3-6\}$. In this example, a 3-core MCF is utilized, with each core adjacent to the rest. Further, for simplicity, it is assumed that each connection requires the same number of spectrum slots, regardless of the path and bit-rate requested. Also, it is assumed that inter-core interaction exists when spectrum slots with the same id are utilized by adjacent cores and that one inter-core interaction between two connections is tolerated, even in the case where one of the connections is a high-power jamming signal. Three different solutions are then illustrated for the spectrum allocation of link $(3-5)$ for the three different approaches considered (i.e., Min-RMSCA, MinLI-RMSCA, and Aa-RMSCA).

In particular, Fig. 1(a) illustrates the Min-RMSCA solution, where the connections are allocated to the first available resources without considering adjacent cores and slots. However, in this case, high-power jamming signals on one connection can affect (through inter-core crosstalk) the other two connections, leading to unacceptable QoT. Figure 1(b) illustrates the MinLI-RMSCA solution, where connections are allocated to spectrum slots such that inter-core interaction between connections is minimized. In this case, high-power jamming signals on one connection cannot affect the rest of the connections. However, in this case, connections must choose spectrum slots without any inter-core interference, moving to slots with higher id. As a result, in more realistic cases, some connections will choose longer paths that require more slots in order to avoid inter-core interference, offering an overall spectrum inefficient solution. Finally, Fig. 1(c) illustrates the Aa-RMSCA solution, demonstrating efficient utilization of the resources, while at the same time ensuring that any high-power jamming attack does not affect the rest of the established connections, since at most one inter-core interaction between two connections is allowed (brown-colored and red-colored connections). It is important to note that both methods (b) and (c) constitute jamming attack-aware approaches, with the latter one (Aa-RMSCA) being a more resource-efficient approach, since it considers the impact of inter-core lightpath interactions on the QoT of each connection in the network, and allows for some inter-core interactions, while examining the effects of a jamming attack.

IV. SECURITY CONSIDERATIONS IN SS-FONs

In this work, instead of minimizing just the interactions of the established lightpaths, analytical models of the PLIs are taken into account in order to specify the connections that are susceptible to jamming attacks. In this way, a more efficient lightpath establishment is achieved without inefficient utilization of resources, as described in the toy example of the previous section. The modeling of the PLIs and the jamming attacks are described next.

A. MODELING PHYSICAL LAYER IMPAIRMENTS

To account for the PLIs, our extended version of the Q-tool estimator proposed in [19] is used. This tool is able to calculate the QoT of new lightpaths to be established in the network, as well as the impact on the existing connections when setting up a new one, by taking into account the analytical models of linear and nonlinear impairments of SS-FONs. The tool input comprises the network topology, spectral windows, link characteristics, signal types (baud rate and modulation format), as well as lightpaths currently established in the network. The impact of the PLIs on each established connection depends on the links of the path, the optical fiber's physical characteristics (e.g., number of adjacent cores and the distance between them), the number of allocated frequency slots operating at the same frequency in adjacent cores, as well as the modulation format used at each frequency slot. Finally, the estimated QoT can be expressed in optical signal-to-noise ratio (OSNR) or bit error rate (BER) per spatial channel.

The OSNR for core r in a homogeneous weakly coupled (WC)-MCF over link l can be expressed as:

$$OSNR^{l}_{MCF,r} = \frac{P_{ch}}{N^{l}_{s} \cdot (G^{l}_{ASE} + G^{l}_{NLI,r}) \cdot B_{ref} + P^{r}_{XT_l}} \quad (1)$$

where P_{ch} is the input channel power, G^{l}_{ASE} is the noise power spectral density (PSD) in the amplifiers, $G^{l}_{NLI,r}$ is the noise PSD from nonlinear impairments of link l and core r, and N^{l}_{s} is the number of spans of link l. Also, B_{ref} is the reference noise bandwidth. Moreover, $P^{r}_{XT_l}$ is equal to

$$P^{r}_{XT_l} \cong N^{l}_{s} \cdot \mu^{r}_{XT_l} \cdot P_{ch} \quad (2)$$

where $\mu^{r}_{XT_l}$ is the crosstalk parameter, given by:

$$\mu^{r}_{XT_l} \cong \sum_{n=1, n\neq r}^{C} \eta^{nr}_{coupl} L_{span} \quad (3)$$

where L_{span} is the span length and η^{nr}_{coupl} is the power coupling coefficient between cores n and r. These equations [19] are used as a starting point to model the effect of jamming attacks in SS-FONs.

B. MODELING JAMMING ATTACKS

In this section, the impact of high-power jamming attacks (through inter-core crosstalk) on the QoT of a lightpath in SS-FONs is calculated. The expression related to crosstalk as presented in Eq. (2) and [19], [47], is valid under the assumption that the lightpaths traversing different cores have the same power. However, when considering high-power jamming attacks, the power of the jamming signal will be much higher than the nominal value. In addition, Eq. (3) is valid under the assumption that all cores of the fiber are active. Equations (2) and (3) do not hold in the case of high-power jamming attacks, since the power of the jammed signal, as well as the different adjacent active cores affecting a signal, impact differently the QoT of an affected lightpath.

To calculate the jamming attack tolerance (i.e., acceptable QoT) for each lightpath m in SS-FONs, the approach described below is used. Let SNR_{thr} be the acceptable threshold for the QoT of a lightpath, i.e.,

$$SNR_m > SNR_{thr} \quad (4)$$

with

$$SNR_m = \frac{1}{\frac{1}{SNR_{XI}} + \sum_{l\in p} \frac{1}{SNR^{l}_{ASE,NLI}}} \quad (5)$$

where SNR_{XI} is the signal-to-noise ratio (SNR) value accounting for the inter-channel crosstalk and the inter-symbol interference in back-to-back measurements for different modulation formats and spectral widths of the signal and $SNR^{l}_{ASE,NLI}$ is the SNR corresponding to the amplified spontaneous emission (ASE) and non-linear interference (NLI) for link l and is equal to:

$$SNR^{l}_{ASE,NLI} = \frac{OSNR^{l}_{MCF,r} \cdot B_{ref}}{N_{pol} \cdot B_{rx}} \quad (6)$$

where N_{pol} and B_{rx} are the number of polarizations and the receiver filter bandwidth, respectively.

Using Eqs. (4) and (5):

$$\sum_{l\in p} SNR^{l}_{ASE,NLI} > \frac{1}{\frac{1}{SNR_{thr}} - \frac{1}{SNR_{XI}}} = SNR_T \quad (7)$$

Also, using Eqs. (1), (6), and (7):

$$\sum_{l\in p} P_{XT_l} \leq [\frac{P_{ch} \cdot B_{ref} \cdot SNR_T}{N_{pol} \cdot B_{rx}} - \\ -(G_{ASE} + G_{NLI,r}) \cdot B_{ref}] = JAM^{p}_{thr} \quad (8)$$

where G_{ASE} over path p is equal to

$$G_{ASE} = \sum_{l\in p} N^{l}_{s} \cdot G^{l}_{ASE} \quad (9)$$

and $G_{NLI,r}$ over path p and core r is equal to

$$G_{NLI,r} = \sum_{l\in p} N^{l}_{s} \cdot G^{l}_{NLI,r} \quad (10)$$

Parameter P_{XT_l} is the resulting power on link l of path p due to inter-core crosstalk by other connections that are under jamming attack. The total power, $\sum_{l\in p} P_{XT_l}$, on path p must be lower than the JAM^{p}_{thr}, to allow connection using path p to have an acceptable QoT.

V. ATTACK-AWARE RMCSA - ILP FORMULATIONS

In this section, ILP formulations are presented for solving the Aa-RMSCA problem. As this problem is computationally intensive, the number of variables and constraints is reduced (i.e., reducing the search space) by applying the path and channel modeling as described below.

A. PATH MODELING

To reduce the search space of the ILP, for each demand d, a set of k shortest paths is calculated instead of searching for the solution amongst all possible paths. Then, to model the candidate path space, each path is evaluated in terms of its QoT (using the QoT estimator tool (Q-tool)) for all modulation formats considered, assuming a network without existing connections, where the only PLIs accounted for are the ones that affect the lightpath itself (e.g., attenuation, dispersion, etc.). Further, the spectrum slots required per link are calculated by:

$$f_{dp} = \left\lceil \frac{B_d}{B_{rate} \cdot MF_p \cdot N_{pol}} \right\rceil \tag{11}$$

where B_d is the bit-rate requested by the connection, B_{rate} is the baud rate of each spectrum slot in the network, MF_p is the modulation format used by the candidate path p (expressed in terms of bits/symbol), and N_{pol} is the number of polarization modes.

Then, parameter JAM^p_{thr} is calculated. To evaluate each connection request, the BER is considered as the QoT metric (with BER threshold set to $T = 1 \times 10^{-3}$ [19]) and the BER of each path is related to the SNR_{thr} (Eq. (7)) as shown in Table 1, where $erfc(x)$ is the complementary error function $erfc(x) = 2/\sqrt{\pi} \int_x^\infty e^{-t^2} dt$.

Subsequently, the set of candidate paths and modulation formats is reduced (i.e., only the paths and modulation formats that achieve a $JAM^p_{thr} > 0$ are selected, since any other path, even without any crosstalk interference, cannot achieve the requested bit-rate with an acceptable QoT). Finally, for each connection, the paths are sorted in ascending order based on the overall number of spectrum slots required to establish that connection (i.e., number of hops required by a connection multiplied by f_{dp}), and the first k' paths are used in the ILP (i.e., they constitute the path space P_d for each demand d). This means that the most efficient paths that can achieve an acceptable QoT are selected for each demand.

B. CHANNEL MODELING

In SS-FONs, by taking into account the contiguity constraint for the spectrum slots of a connection, any available sets of spectrum slots can be modeled together without affecting optimality. Thus, to model the required set of contiguous slots for a given demand, the channel is modeled according to [48], with the differentiation that in this work the modulation format is also accounted for to ascertain the number of spectrum slots required. A set of candidate channels W_{dp} is calculated for each connection request d, where p is a candidate path $p \in P_d$. The set W_{dp} consists of all possible groups of contiguous slots f_{dp} that connection d could be allocated to using path p. Thus, $|W_{dp}| = |F| - f_{dp} + 1$, where F is the set of frequency slots for each fiber. Parameter γ_{wf} is also defined that relates channel w with slot f. This parameter is equal to 1 whenever channel $w \in W_{dp}$ uses slot $f \in F$, and 0 otherwise. Hence, $\forall w \in W_{dp}, \sum_{f \in F} \gamma_{wf} = f_{dp}$.

TABLE 1. SNR to BER [19].

Mod. format	SNR to BER eq.
BPSK	$\frac{1}{2} erfc(\sqrt{SNR})$
QPSK	$\frac{1}{2} erfc(\sqrt{\frac{1}{2} SNR})$
8-QAM	$\frac{2}{3} erfc(\sqrt{\frac{3}{14} SNR})$
16-QAM	$\frac{3}{8} erfc(\sqrt{\frac{1}{10} SNR})$

C. ILP FORMULATION (P1): Aa-RMSCA

The ILP formulation takes as input the defined candidate paths associated with the candidate channels and modulation formats. The solution of the ILP will be the established lightpaths in terms of paths, modulation formats, cores, and spectrum slots per demand that will ensure that the QoT of all established lightpaths will not deteriorate below a set threshold in case of a high-power jamming attack. The following parameters and variables are used to formulate the Aa-RMSCA problem.

1) PARAMETERS

- $d \in D$: a requested connection
- $f \in F$: a spectrum slot over the available spectrum slots
- P: set of all candidate paths
- $p \in P$: a candidate path
- P_d: set of candidate paths to serve connection d, $P_d \subset P$
- $l \in E$: a network link
- $c \in C$: a fiber core
- W_{dp}: set of candidate channels to serve connection d using candidate path p
- $w \in W_{dp}$: a candidate channel from the set of candidate channels that can be used to serve connection d using candidate path p
- f_{dp}: the requested number of slots for demand d when utilizing candidate path p
- γ_{wf}: equal to 1 if channel w uses slot f and 0 otherwise
- $\gamma_{ww'}$: equal to 1 if channel w has at least one common slot with channel w', and 0 otherwise
- $\gamma_{wf^{dp}_{max}}$: the maximum slot f of channel w for path p of demand d
- δ_{pl}: equal to 1 if path p uses link l and 0 otherwise
- $JAM^{MF_p}_{thr}$: threshold to be used for the QoT evaluation of lightpaths using path p and modulation format MF_p under high-power jamming attacks according to Eq. (8)
- XT^{pwc}_l: The effect of inter-core crosstalk interactions of lightpath (p, w, c) on the lightpath under consideration at link l
- A_c: The set of cores which interact with core c
- M: large positive constant

2) VARIABLES

- x_{pwc}: Boolean variable, equal to 1 if path p, channel w, and core c are used to serve connection d; 0 otherwise.
- S^d_{tol}: Integer variable to check whether the QoT of the path and spectrum slots selected for demand d violates the QoT threshold. If $S^d_{tol} > 0$, demand d cannot tolerate jamming attacks.
- F_{max}: The maximum assigned slot id in the network.

3) OBJECTIVE

$$Minimize : \sum_{d} S^d_{tol} + F_{max}$$

Subject to the following constraints:

- Demand satisfaction

$$\sum_{p\in P_d} \sum_{w\in W_{dp}} \sum_{c\in C} x_{pwc} = 1, \quad \forall d \in D \tag{12}$$

- Maximum id of established spectrum slots

$$\gamma_{wf^{dp}_{max}} \cdot x_{pwc} \leq F_{max}, \ \forall d \in D, \forall p \in P_d, \\ \forall w \in W_{dp}, \forall c \in C \tag{13}$$

- Non-overlapping spectrum slots

$$\sum_{d\in D} \sum_{p\in P_d} \sum_{w\in W_{dp}} \gamma_{wf} \cdot \delta_{pl} \cdot x_{pwc} \leq 1, \\ \forall l \in E, \forall f \in F, \forall c \in C \tag{14}$$

- Jamming attack tolerance

$$\sum_{l\in p} \sum_{d'\in D} \sum_{p'|p\neq p', p'\in P_{d'}} \delta_{pl} \cdot \delta_{p'l} \cdot \\ \left(\sum_{w'\in W_{d'p'}} \gamma_{ww'} \cdot \left(\sum_{c'=1, c'\in A_c}^{C} x_{p'w'c'} \cdot XT_l^{p'w'c'} \right) \right) \\ + M \cdot x_{pwc} \leq JAM^{MF_p}_{thr} + S^d_{tol} + M, \\ \forall d \in D, \forall p \in P_d, \forall w \in W_{dp}, \forall c \in C, \tag{15}$$

The objective of the formulation is to minimize any inter-core interactions between connections ($S_{tol} = \sum_d S^d_{tol}$) that set the QoT to a lower value than the required threshold, for any demand d in the network. Also, the id of the maximum used slot F_{max} is minimized to provide a more compact solution, when possible. Constraint (12) ensures that all requested demands are established, constraint (13) is used to define the maximum id of used spectrum slots across all cores (the upper bound of variable F_{max} is equal to the number of slots per core), while constraint (14) is the non-overlapping spectrum constraint. Finally, constraint (15) is used to define the tolerance of each connection to high-power jamming attacks that can spread through inter-core crosstalk. This constraint is used for every path p, channel w, and core c, in order to account for the inter-core crosstalk interactions of adjacent cores through the term:

$$\sum_{l\in p} \sum_{d'\in D} \sum_{p'|p\neq p', p'\in P_{d'}} \delta_{pl} \cdot \delta_{p'l} \cdot \\ \left(\sum_{w'\in W_{d'p'}} \gamma_{ww'} \cdot \left(\sum_{c'=1, c'\in A_c}^{C} x_{p'w'c'} \right) \right)$$

where the set A_c is defined as the set of cores $c' \in C$ which interact with core c. Without loss of generality, in this work a 7-core MCF is used, assuming the interactions between cores shown in Fig. 2 (i.e., nodes correspond to cores and links to the interactions between cores). For example, in this MCF, $A_1 = \{2, 6, 7\}$, $A_2 = \{1, 3, 7\}$ and $A_7 = \{1, \ldots, 6\}$, etc.

Also, the summation above is multiplied by $XT_l^{p'w'c'}$, where

$$XT_l^{p'w'c'} = N^l_s \cdot \eta^{cc'}_{coupl} \cdot L_{span} \cdot P^{p'w'c'}_{jam}$$

that is, the inter-core crosstalk interactions that affect the signal of lightpath (p, w, c) on link l (derived from Eqs. (2) and (3)). Parameter $P^{p'w'c'}_{jam}$ is the jamming power of lightpath (p', w', c') that affects the lightpath under consideration. For planning purposes, it can be assumed that all jamming signals have the same power value, P_{jam} (even though attacks of different power levels can easily be assessed). The effect of inter-core crosstalk for each path p and channel w must be lower than the set threshold $JAM^{MF_p}_{thr}$ for the corresponding lightpath to have acceptable QoT under the condition of high-power jamming attacks. It is important to note that the problem formulation is generic and it is possible to specify different classes of connections based on their required QoT in case of a high-power jamming attack, as well as different types of jamming attacks (e.g., affecting only the link they are inserted on). This can be achieved by proper tuning of the parameters $XT_l^{p'w'c'}$ and $JAM^{MF_p}_{thr}$ of constraint (15).

In this formulation, the spectrum and the core continuity constraints are taken into account implicitly by the definition of the x_{pwc} variable, since this variable uses the same spectrum slots w and core c across all links that constitute a path p.

In order to compare the proposed Aa-RMSCA solution with MinLI-RMSCA and Min-RMSCA as described in Section III, their corresponding ILP formulations are discussed below in brief.

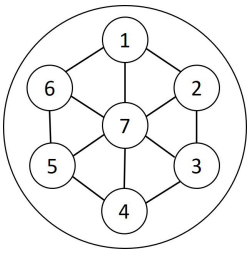

FIGURE 2. Interaction between adjacent cores in 7-core fibers.

D. ILP FORMULATION (P2): MinLI-RMSCA

To minimize the number of inter-core interactions, and hence minimize the impact of high-power jamming attacks, the formulation of the MinLI-RMSCA ILP does not take into account the actual physical layer impairments of the network. To achieve this, constraint (15) is modified as follows:

$$\sum_{l\in p}\sum_{d'\in D}\sum_{p'|p\neq p',p'\in P_{d'}}\delta_{pl}\cdot\delta_{p'l}\cdot\Bigg(\sum_{w'\in W_{d'p'}}\gamma_{ww'}\cdot\Bigg(\sum_{c'=1,c'\in A_c}^{C}x_{p'w'c'}\Bigg)\Bigg)+M\cdot x_{pwc}\leq S^{d}_{tol}+M$$
$$\forall d\in D,\forall p\in P_d,\forall w\in W_{dp},\forall c\in C \quad (16)$$

In this case, this modified ILP takes as input the candidate paths as described in Section V-A, which means that these paths will have an acceptable QoT when there are no interactions in the network. Utilizing this approach, the algorithm will avoid using slots that can cause inter-core crosstalk between lightpaths. Hence, this approach will provide solutions with acceptable QoT in the case of high-power jamming attacks at the expense, however, of additional spectrum resources.

E. ILP FORMULATION (P3): Min-RMSCA

To minimize the required spectrum and establish a set of demands in SS-FONs, the ILP formulation of Section V-C is again used by now completely omitting constraint (15). In addition, the objective of the ILP will contain only the term F_{max}. As this approach does not take into account the QoT of the lightpaths nor the effect of high-power jamming attacks, it is the most resource efficient approach (i.e., in terms of spectrum utilization) compared to Aa-RMSCA and MinLI-RMSCA and is used as a benchmark for the minimum spectrum resources required to establish a set of connections. Again, for comparison purposes, the paths that are used as input to the ILP are the same as in the previous two ILPs.

F. VARIABLES AND CONSTRAINTS

Table 2 lists the number of variables and constraints required in the aforementioned formulations, with $N = |V|$ denoting the number of nodes, $L = |E|$ the number of links, $B = |F|$ the number of frequency slots, $Q = |C|$ the number of cores per fiber link, and D the number of requested connections. $A = \sum_{d\in D}\sum_{p\in P_d}|W_{dp}|$ denotes the total number of candidate channels for all paths and demands, where $|W_{dp}|$ is the number of candidate channels for demand d and path p.

VI. ATTACK-AWARE RMSCA - HEURISTIC ALGORITHMS

Two different heuristic algorithms are also developed for solving the Aa-RMSCA problem, taking into account high-power jamming attacks and physical layer impairments, and following similar principles as for the ILP algorithms.

TABLE 2. Variables and constraints.

Formulation	Variables	Constraints
Aa-RMSCA	$A\cdot Q+D+1$	$D+2\cdot A\cdot Q+L\cdot B\cdot Q$
MinLI-RMSCA	$A\cdot Q+D+1$	$D+2\cdot A\cdot Q+L\cdot B\cdot Q$
Min-RMSCA	$A\cdot Q+1$	$D+A\cdot Q+L\cdot B\cdot Q$

A. JAMMING ATTACK RMSCA (JA-RMSCA) HEURISTIC

A heuristic algorithm for the attack-aware RMSCA problem, denoted as JA-RMSCA, is described in this section, that considers first the routing and modulation format sub-problem, where k-shortest paths are found in combination with H modulation formats to serve a traffic demand and then the spectrum and core allocation sub-problem, where spectrum slots and core resources are allocated to a given demand.

The objective of the heuristic is to minimize the number of blocked connections due to QoT degradation in the case of jamming attacks, and at the same time use the spectrum resources efficiently. Further, a modification of the same algorithm, denoted as impairment-aware RMSCA (IA-RMSCA) is used as a benchmark to provide results for the normal operation of the network (i.e., when the network is not under attack). This way an insight can be gained on the additional resources required to design the network for jamming attack operation.

Specifically, the JA-RMSCA heuristic follows the same process as the *path modeling* pre-processing step of the ILP discussed in Section V-A: Initially, a set of k-shortest paths to serve a traffic demand is found and for these paths, the $JAM_{thr}^{MF_p}$ for all available modulation formats is calculated according to Eq. (8), with only the reduced set of feasible paths considered. Then, for each connection, the paths (and their associated modulation formats) are sorted in ascending order, based on the number of slots required to establish a connection. Subsequently, each connection is established on the first path and modulation format (first-fit approach), with a spectrum and core allocation solution that meets all physical layer criteria. If a feasible solution cannot be found for all candidate paths, the connection is blocked.

It should also be noted that in terms of the SCA problem, again a first-fit policy is used and the first solution that meets the $JAM_{thr}^{MF_p}$ threshold is selected. Specifically, the first available spectrum resources and the first core along all links of the selected path that satisfy the spectrum and core allocation constraints are selected for evaluation. Then, the already established lightpaths that interact through inter-core crosstalk with the new candidate lightpath to be provisioned are found (i.e., they utilize spectrum slots with the same id in neighboring cores). Based on the number of neighboring cores that are active on each link of the path, and P_{XT_l}, $l \in p$, the value of P_{XT} is calculated. If that value is greater than the value of the threshold ($JAM_{thr}^{MF_p}$), the high-power jamming interactions violate the threshold and hence, the connection cannot be provisioned in these spectrum slots. In that case, another core is first selected

Algorithm 1 JA-RMSCA and IA-RMSCA Heuristics

```
loops = 0;
Calculate k shortest paths
Evaluate JAM_thr for each path and modulation format and keep reduced set of feasible candidate paths and modulation formats.
Sort all paths and modulation formats in ascending order based on the number of spectrum slots required.
for all connection requests do
    Select route (p) and modulation format (MF_p) (first-fit)
    Select feasible core and spectrum slots (first-fit) (such that P_XT ≤ JAM_thr^MF_p)
end for
Evaluate QoT (BER): (a) IA, (b) JA
Remove connections with BER > T,
Num_blocked=connections with BER > T
if (Num_blocked > 0 && loops < I) then
    loops = loops + 1
    Go back to For Loop only for connections with BER>T (Step 5)
else
    Calculate spectrum utilization, blocked connections, and QoT of solution
end if
```

prior to considering another set of spectrum slots. It is noted that first the candidate cores are investigated rather than the candidate groups of spectrum slots, so as to utilize all cores of a fiber in lower spectrum slots (when available), thus keeping the maximum slot id as low as possible.

Clearly, using this approach, the QoT of all connections is evaluated based on the state of the network when each new connection is provisioned. Hence, an initially feasible connection may become infeasible when other connections are provisioned. Thus, a feedback approach is introduced after all connections are established in the network, where each connection is evaluated based on the final state of the network. In each stage of QoT evaluation, for the jamming-aware approach (JA-RMSCA), all connections that are served by (even partially) the same spectrum slots in neighboring cores are assumed to be under a high-power signal attack when considering each connection. On the other hand, when considering the impairment-aware approach (IA-RMSCA), all connections with neighboring cores are assumed to use their nominal input power when evaluating each connection. In either case, if a connection achieves a QoT lower than its required threshold, then it is reallocated utilizing another feasible RMSCA solution, if one is found, based on the current state of the network. This process is repeated until all connections are established with an acceptable QoT, or a designated loop threshold I is reached. Algorithm 1 presents the pseudocode of the proposed heuristics.

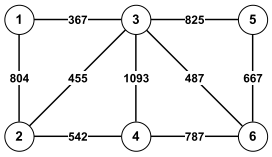

FIGURE 3. 6-node network topology.

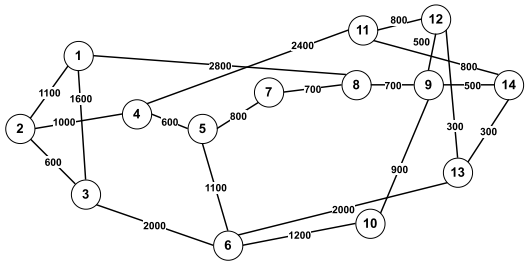

FIGURE 4. NSF network topology.

B. ZERO INTERACTIONS RMSCA (ZI-RMSCA) HEURISTIC

An additional heuristic is introduced, denoted as zero interactions RMSCA (ZI-RMSCA) that does not allow for any inter-core lightpath interactions. The routing and modulation format sub-problem is solved as for the previous heuristics, while for the spectrum and core allocation sub-problem, only the lightpath interactions through inter-core crosstalk are considered, and not the physical layer impairments. This is a stricter approach, since any spectrum allocation solution for a connection allowing for inter-core interactions with other connections is considered as infeasible, regardless of the network state and the QoT of the connections. However, it is included in the performance results section, as a benchmark, providing an upper bound on the resources required when no inter-core interactions occur.

It should be noted that for the implementation of this heuristic, the $JAM_{thr}^{MF_p}$ threshold is not utilized, all established connections will have an acceptable QoT irrespective of the network state (since paths are evaluated during the path modeling step), and hence, the feedback loop step utilized in the previous heuristics is no longer required.

VII. PERFORMANCE RESULTS

To evaluate the proposed algorithms, two different network topologies are used; a 6-node network (Fig. 3), which consists of 6 nodes and 18 directed links, and the NSF network topology (Fig. 4), which consists of 14 nodes and 42 directed links. Each network is assumed to operate with bandwidth-variable transponders (BVTs) and several modulation formats, namely, BPSK, QPSK, 8-QAM, and 16-QAM. Table 3 presents the physical layer characteristics of the networks under consideration.

To evaluate the ILP algorithms, the number of spectrum slots per core is assumed to be equal to $F = 20$, with a baud rate of 16 Gbauds. The bit rate for each connection is randomly generated following a uniform distribution ranging from 10 to 200 Gbps for all demands. The number of shortest paths k is initially equal to 3 and 14 for each

TABLE 3. Network characteristics.

Network topology:	6-node		$N = 6$	$L = 18$
	NSF network		$N = 14$	$L = 42$
Frequency spacing	25 GHz			
Baud rate	16 Gbaud			
Number of slots (F)	20			
Number of cores (C)	7			
Modulation format (d: distance in km)	BPSK d>4600	QPSK 1700<d <4600	8-QAM 800<d <1700	16-QAM d<800
Number of connections (D)	6 - node		40	
	NSF Network		80	
Bit rate required per connection	10-200 Gbps			

TABLE 4. ILP results.

ILP model - network	S_{tol}	F_{max}	Block. rate (%)		Run. times (sec.)	Inter-core intera.
			normal oper.	jam. oper.		
(P1) - 6-node	0	4	0	0	1416	40
(P2) - 6-node	0	5	0	0	4506	0
(P3) - 6-node	-	4	0	27.5	19.5	50
(P1) - NSF	0	8	0	0	25254	123
(P2) - NSF	0	11	0	0	172850*	0
(P3) - NSF	-	8	2.5	42.5	105.5	164

*Exceeded the time limit of 48 hrs.

source-destination pair, for the 6-node and NSF networks, respectively. Then, following the path modeling in both the ILP and heuristic approaches, only the reduced feasible set of paths and modulation formats remains. It is noted that for the ILP case, in all simulations, a server was used with an Intel Xeon CPU E5-2680 with 28 cores and 256 GB RAM. For solving the ILP formulations, the Gurobi library was used [49].

First, the results of the ILP formulations for the three different objectives are presented. The nominal power for each lightpath is assumed to be equal to 0dBm. To evaluate the QoT of the established lightpaths, our modified version of the Q-estimation tool [19] is used. Further, two different scenarios are considered: (i) the case of *normal operation*, where no attacks are present in the network. For this case, to calculate the QoT of a given connection, all connections have an input power equal to 0dBm. (ii) the case of *jamming attack operation*, where all connections, except the one under consideration, are under attack through inter-core crosstalk (i.e., most demanding scenario where all other connections are assumed to be under attack). In this case, the power of the signal under consideration is equal to 0dBm, and all other connections have a signal power equal to 10dBm.

Table 4 presents performance results regarding the maximum spectrum slot id used in the network, the blocking rate due to unacceptable QoT, as well as the computation time required for the ILP to find the optimal solution for the two different scenarios in two different networks. It is shown that the lower bound of spectrum slots to establish all connections is equal to $F_{max} = 4$ and 8, for the 6-node and NSF networks, respectively, which is the optimal solution provided by the Min-RMSCA approach. The same results are achieved by the proposed Aa-RMSCA algorithm in both networks, while on the other hand, the MinLI-RMSCA scheme requires more slots (5 and 11 for the 6-node and NSF networks, respectively) to establish the same set of connections (due to the stricter approach utilized for spectrum slot assignment within a core). Further, the MinLI-RMSCA approach exhibits zero blocking rate for both the normal and jamming-attack operations in both network scenarios. This is to be expected, since each connection is only affected by the path impairments and not by any change in the state of the rest of the (established) connections. This result also presents the lower bound of blocking rate for all cases, since MinLI-RMSCA minimizes the number of inter-core interactions under the case of high-power jamming attacks. The same results are achieved for the proposed Aa-RMSCA algorithm, albeit with a smaller F_{max}, signifying that connections can be utilized in the same frequency slots at neighboring cores, as long as these interactions are tolerated ($S_{tol} = 0$).

Finally, the Min-RMSCA algorithm exhibits a 0% blocking rate for the 6-node network, while it achieves a 2.5% blocking rate for the NSF network under normal operation. This means that for the 6-node network, the interactions have a small impact on the QoT of the connections, while for the NSF network scenario, the interactions result in blocked connections, even without having high-power jamming attacks in the network. In addition, under the worst-case assumption of a jamming-attack operation (i.e., all other neighboring connections are being attacked when evaluating each connection), the blocking rate is exceptionally high (27.5% and 42.5% for 6-node and NSF networks, respectively). Nevertheless, this is not a realistic scenario and is only noted here in order to demonstrate the (worst-case) upper bound in terms of blocking rate. It is also important to note here that even though the Min-RMSCA algorithm is the most resource efficient approach (in terms of spectrum utilization), the blocking that occurs when this approach is utilized is QoT-based (i.e., the QoTs for the lightpaths that are blocked do not achieve the required threshold at the receiver).

It is evident from the aforementioned results that the proposed Aa-RMSCA algorithm can achieve the lower bound for both the required spectrum and the blocking rate. This is achieved with added complexity compared to the algorithm that only minimizes the required spectrum (24 minutes vs 20 seconds for the 6-node network and 7 hours vs 2 minutes for the NSF network). Nevertheless, the Aa-RMSCA algorithm is characterized by much less running time compared to MinLI-RMSCA, that required 75 minutes to find a solution in the 6-node network. Further, for the NSF network topology, the MinLI-RMSCA required two days to achieve the presented results (with no optimal solution found). It is noted that the lower bound provided by Gurobi solver for MinLI-RMSCA was $F_{max} = 10$, thus even in the scenario that this solution can be achieved, it is still higher than the solution found by the attack-aware approach.

Table 5 presents the results for the heuristic algorithms. It has to be noted that the IA-RMSCA algorithm is used as a benchmark, so as to illustrate to what extent the required

TABLE 5. Heuristic results.

Heuristic method	F_{max}	Block. rate (%)	Run. time (sec.)	Inter-core inter.
IA-RMSCA (normal oper.) **6-node network**	4	0	0.088	100
JA-RMSCA (jam. oper.) **6-node network**	6	0	0.472	47
ZI-RMSCA **6-node network**	7	0	0.109	0
IA-RMSCA (normal oper.) **NSF network**	11	0	0.114	346
JA-RMSCA (jam. oper.) **NSF network**	14	0	0.417	181
ZI-RMSCA **NSF network**	16	1.25	0.213	0

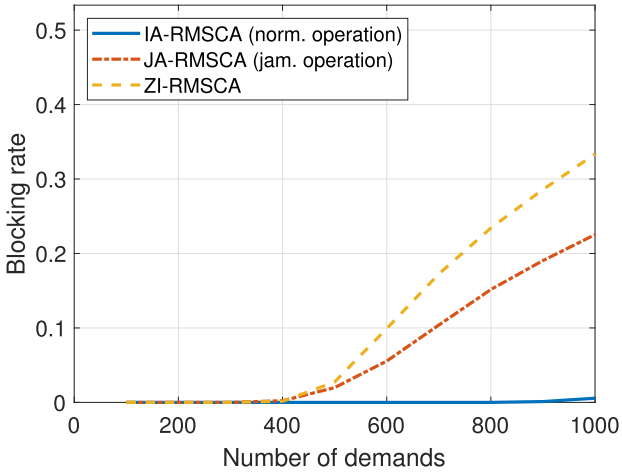

FIGURE 5. Blocking rate results for each heuristic.

spectrum slots and the blocking rate are increased compared to JA-RMSCA (i.e., comparing normal (IA-RMSCA) with jamming-attack operation (JA-RMSCA)). In other words, the IA-RMSCA algorithm considers by design the normal operation, while the JA-RMSCA considers the jamming-attack operation. In contrast, ZI-RMSCA exhibits the same results for both the normal and jamming-attack operations, since the algorithm does not allow for any inter-core interactions. Further, it should be also noted that the JA-RMSCA heuristic considers the same problem as the Aa-RMSCA ILP (P1), the ZI-RMSCA considers the same problem as MinLI-RMSCA ILP (P2), while the IA-RMSCA heuristic is not related to any ILP formulation and serves as a benchmark for the comparison of the heuristic approaches.

As can be seen from this table, the solutions provided by the JA-RMSCA and ZI-RMSCA heuristics correspond to the results obtained by the Aa-RMSCA and MinLI-RMSCA ILPs, respectively. In this case, however, the blocking rate for the ZI-RMSCA approach in the NSF network scenario is due to the lack of resources to provision all connections (since only 20 spectrum slots per core are considered). It is also important to note that the heuristics have only one objective, namely to minimize the blocking rate, without considering F_{max}.

To evaluate the heuristic algorithms for larger size instances, only the NSF network topology is used, but now with 160 spectrum slots for each core in the network and demand size that varies from 100 to 600 Gbps. Each presented result is the average of 10 experiments performed with different generated sets of demands, with the feedback threshold for all cases set to $I = 10$. For these simulations, a PC with a CPU i7-3930K, 6 cores, and 24 GB RAM is used and performance results include the spectrum utilization of the network, the blocking rate of the connections, the number of inter-core interactions, the maximum utilized spectrum slot (F_{max}), as well as the running times of the heuristics.

First, the blocking rate of each approach is presented in Fig. 5. As shown, IA-RMSCA (network under normal operation) achieves the best results, allowing more connections to be established in the network compared to the rest of the heuristics. Heuristic JA-RMSCA achieves a higher blocking rate, since this approach considers the jamming attack scenario and allows for inter-core crosstalk interactions, as long as the BER required is maintained. Finally, ZI-RMSCA achieves the worst results, since now connections are not established at the same spectrum slots in neighboring cores. This leads to a waste of resources, and, in turn, to higher blocking rates.

Next, the spectrum utilization for each approach is presented in Fig. 6, demonstrating that a large number of spectrum slots that could potentially be utilized by JA-RMSCA and ZI-RMSCA is not used. This is the case, since in both approaches, additional considerations regarding jamming attacks restrict some spectrum resources from being utilized. Only IA-RMSCA (that does not consider jamming attacks) utilizes more spectrum slots to establish connections in the network (exhibiting also lower blocking rate). Further, the spectrum utilization of JA-RMSCA is higher than ZI-RMSCA, as in ZI-RMSCA more connections are blocked. Thus, the comparison of both blocking rate and spectrum utilization results for all three heuristics clearly demonstrates the ''penalty'' (in terms of network performance) incurred for providing an RMSCA solution for the jamming attack scenario, as compared with the normal operation. It is noted that the security provided can ensure service without any disruptions and loss of information due to jamming attacks, which is of great importance (as also discussed in Section I). This is the case, as a jamming attack can potentially result in several disrupted connections (resembling a denial of service attack), and if it is not addressed it can cause both tangible and intangible losses for the company that provides the service, as well as for its clients, in terms of revenue, as well as in terms of the credibility and reputation of an organization. Thus, ensuring that the network is protected against such attacks justifies the penalty incurred in terms of network performance. Further, the results shown in this work present the

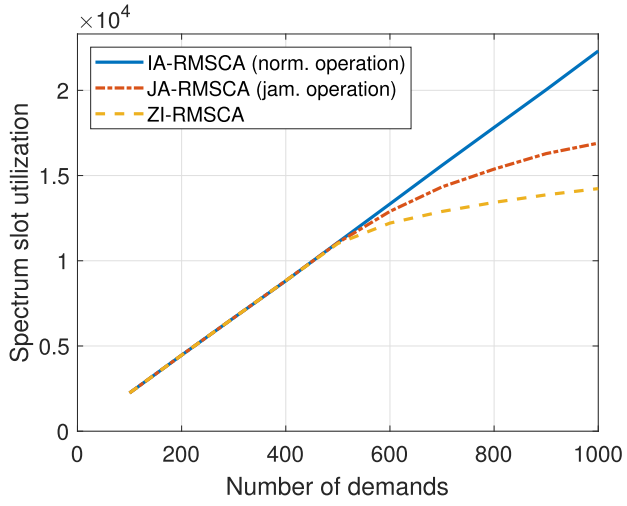

FIGURE 6. Spectrum utilization results for each heuristic.

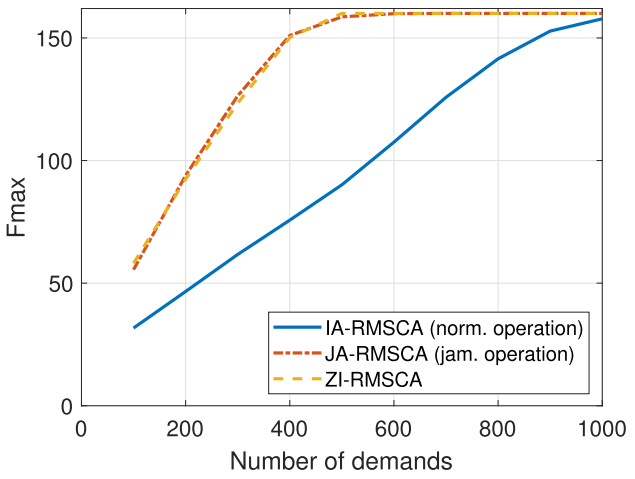

FIGURE 7. Highest frequency slot id utilized in the network for each heuristic.

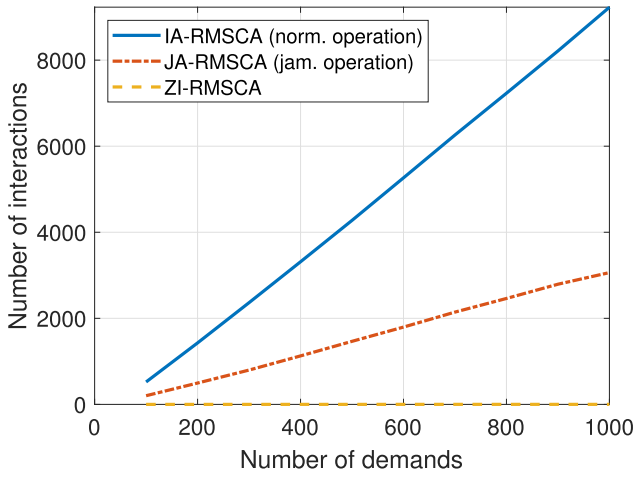

FIGURE 8. Number of inter-core interactions for each heuristic.

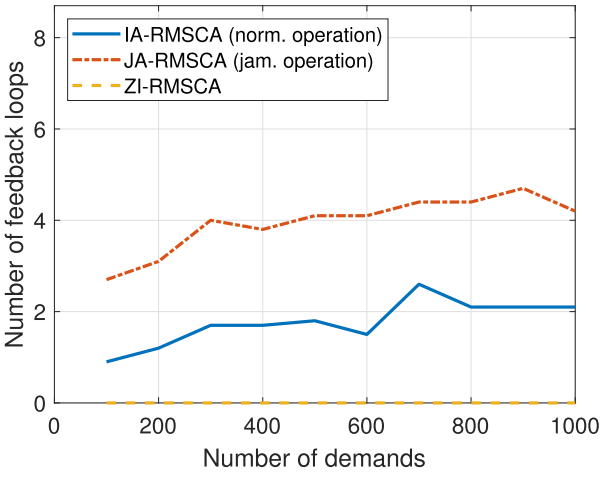

FIGURE 9. Number of feedback loops required for each heuristic.

most demanding scenario, i.e., the case where all connections require protection against jamming attacks. In the case that different connections require different levels of security (e.g., different classes of connections based on their SLAs or QoT requirements), the blocking probability of the network would be significantly reduced.

The same results regarding the spectrum efficiency of the presented approaches can also be seen from Fig. 7, which presents the highest frequency slot id utilized by each approach. As shown, the impairment-aware approach provides a more compact solution, since F_{max} is reached at network states with higher number of demands. This occurs because inter-core crosstalk induced jamming is not considered in this case. On the other hand, ZI-RMSCA provides a more sparse spectrum allocation solution, since F_{max} is increased at lower network loads. Finally, JA-RMSCA follows a similar spectrum allocation to the stricter ZI-RMSCA approach, in order to be able to provision all connections, while also accounting for jamming attacks.

Another important parameter that showcases the different solution that each heuristic approach provides is the total number of inter-core interactions achieved by each approach, presented in Fig. 8. In this case, the IA-RMSCA approach allows for many more inter-core interactions, since jamming attacks are not considered in the evaluation stage. On the other hand, JA-RMSCA results in a much smaller number of specific inter-core interactions, which ensure that any jamming attack will still not compromise any connection in the network, in contrast to ZI-RMSCA that does not allow for any inter-core interactions.

Further, the number of feedback loops required to establish all connections that find available slots is shown in Fig. 9. JA-RMSCA requires up to five loops to establish all connections, compared to the IA-RMSCA approach that converges faster. This is due to the difficulty of JA-RMSCA in finding an assignment that ensures tolerance against any jamming attacks, while also considering that any change in the network state has a higher impact on the QoT of each connection. Also, as previously mentioned, ZI-RMSCA does not require any feedback steps, since a strictly non-inter-core interaction policy is followed, meaning that regardless of the state of the network, the QoT of each connection will solely be affected by its path parameters.

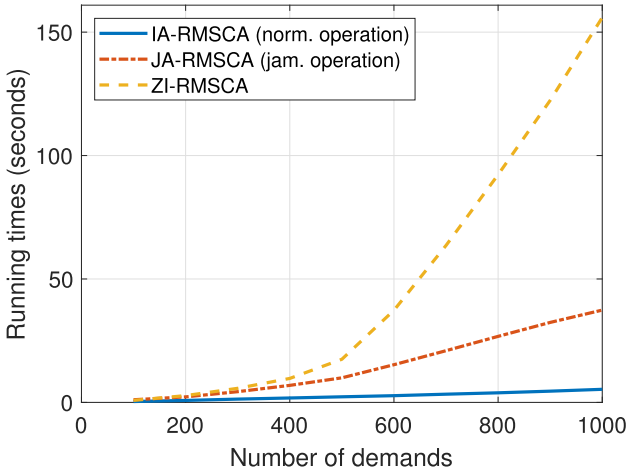

FIGURE 10. Heuristic running times.

Finally, the running times of each approach are presented in Fig. 10. In this case, both IA-RMSCA and JA-RMSCA require similar times to establish all connections in the network. Specifically, JA-RMSCA requires slightly more time compared to IA-RMSCA to establish all connections, due to the increased number of loops performed by the former. On the other hand, the running time of ZI-RMSCA increases exponentially with traffic demand. This is the case, as a larger number of groups of spectrum slots must now be checked to find a solution which ensures that all adjacent cores are empty.

It is clear from the presented results that it is possible to efficiently design the network in terms of spectral resources, while also mitigating high-power jamming attacks. This is demonstrated by both the Aa-RMSCA ILP and the JA-RMSCA heuristic that allow for a much smaller number of interactions compared to the impairment-aware-only policy, with also much less additional resources as compared to a strict non-inter-core interaction policy. This is achieved by including the physical layer impairments during the RMSCA phase and allowing for specific interactions that are tolerant to potential jamming attacks, rather than strictly prohibiting any interactions.

VIII. CONCLUSION

This work formulates an ILP to optimally solve the problem of attack-aware RMSCA in SS-FONs so as to minimize both the impact of high-power jamming attacks as measured by a QoT estimator tool, as well as the required spectrum resources. The ILP's search space is reduced and some constraints are also relaxed, to improve its computational complexity. Specifically, the impact of high-power jamming attacks over a lightpath is analyzed taking into account the physical layer impairments. Based on this analysis, a maximum threshold for jamming attack tolerance is quantified. Then, high-power jamming attacks are modeled and incorporated as additional constraints to the ILP formulation. In addition, two modifications to the ILP formulation (Min-RMSCA and MinLI-RMSCA) are also presented that only minimize the spectrum resources and the number of interactions, respectively, for benchmarking and comparison purposes.

Further, heuristic algorithms are proposed that solve the same problem for larger problem instances. Based on the performance results, it is evident that it is possible to design the network so as to minimize the impact of jamming attacks that can spread through inter-core crosstalk, with lightpaths having acceptable QoT even during jamming-attack operation. This can be achieved without compromising spectrum efficiency.

Future avenues of research include consideration of additional core switching architectures (e.g., Ind-Sw and Fr J-Sw architectures), as well as the joint consideration of in-band and out-of-band jamming attacks.

ACKNOWLEDGMENT

(Giannis Savva and Konstantinos Manousakis are co-first authors.)

REFERENCES

[1] O. Gerstel, M. Jinno, A. Lord, and S. J. Yoo, "Elastic optical networking: A new dawn for the optical layer?" *IEEE Commun. Mag.*, vol. 50, no. 2, pp. s12–s20, Feb. 2012.
[2] *Cisco Annual Internet Report, 2018–2023*, Cisco, San Jose, CA, USA, 2020.
[3] P. J. Winzer, "Spatial multiplexing: The next frontier in network capacity scaling," in *Proc. 39th Eur. Conf. Exhib. Opt. Commun. (ECOC)*, 2013, pp. 372–374.
[4] M. Klinkowski, P. Lechowicz, and K. Walkowiak, "Survey of resource allocation schemes and algorithms in spectrally-spatially flexible optical networking," *Opt. Switching Netw.*, vol. 27, pp. 58–78, Jan. 2018.
[5] B. Shariati, J. M. Rivas-Moscoso, D. M. Marom, S. Ben-Ezra, D. Klonidis, L. Velasco, and I. Tomkos, "Impact of spatial and spectral granularity on the performance of SDM networks based on spatial superchannel switching," *J. Lightw. Technol.*, vol. 35, no. 13, pp. 2559–2568, Jul. 1, 2017.
[6] D. M. Marom and M. Blau, "Switching solutions for WDM-SDM optical networks," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 60–68, Feb. 2015.
[7] M. Yang, Q. Wu, and Y. Zhang, "Joint assignment of spatial granularity, routing, modulation, and spectrum in SDM-EONs: Minimizing the network CAPEX considering spectrum, WSS, and laser resources," *J. Lightw. Technol.*, vol. 36, no. 18, pp. 4153–4166, Sep. 15, 2018.
[8] M. Yang, C. Zhang, Q. Wu, W. Zheng, and Y. Zhang, "Comparison of switching policies in terms of switching cost and network performance in static SDM-EONs," *Opt. Switching Netw.*, vol. 38, Sep. 2020, Art. no. 100573.
[9] M. Furdek, L. Wosinska, R. Goscien, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, and J. L. Marzo, "An overview of security challenges in communication networks," in *Proc. 8th Int. Workshop Resilient Netw. Design Modeling (RNDM)*, Sep. 2016, pp. 43–50.
[10] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2016.
[11] K.-I. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, and A. Takada, "Security in photonic networks: Threats and security enhancement," *J. Lightw. Technol.*, vol. 29, no. 21, pp. 3210–3222, Nov. 2011.
[12] G. Savva, K. Manousakis, and G. Ellinas, "Eavesdropping-aware routing and spectrum/code allocation in OFDM-based EONs using spread spectrum techniques," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 11, no. 7, pp. 409–421, Jul. 2019.
[13] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 725–736, Sep. 2011.
[14] K. Manousakis and G. Ellinas, "Attack-aware planning of transparent optical networks," *Opt. Switching Netw.*, vol. 19, pp. 97–109, Jan. 2016.

[15] G. Savva, K. Manousakis, and G. Ellinas, "Network coding-based routing and spectrum allocation in elastic optical networks for enhanced physical layer security," *Photonic Netw. Commun.*, vol. 40, no. 3, pp. 160–174, Dec. 2020.

[16] T. Xu, B. Karanov, N. Shevchenko, D. Lavery, G. Liga, Z. Li, D. Jia, L. Li, L. Kanthan, R. Killey, and P. Bayvel, "Spectral broadening effects in optical communication networks: Impact and security issue," *Proc. Int. Conf. Adv. Infocomm Technol. (ICAIT)*, 2018, pp. 1–2.

[17] M. Furdek, N. Skorin-Kapov, and L. Wosinska, "Attack-aware dedicated path protection in optical networks," *J. Lightw. Technol.*, vol. 34, no. 4, pp. 1050–1061, Feb. 15, 2016.

[18] P. Roorda, *Critical Issues for the Flexible Spectrum Network*. San Jose, CA, USA: Lumentum, 2015.

[19] B. Shariati, A. Mastropaolo, N.-P. Diamantopoulos, J. M. Rivas-Moscoso, D. Klonidis, and I. Tomkos, "Physical-layer-aware performance evaluation of SDM networks based on SMF bundles, MCFs, and FMFs," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 10, no. 9, pp. 712–722, Sep. 2018.

[20] 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.

[21] K. Manousakis and G. Ellinas, "Equalizer placement and wavelength selective switch architecture for optical network security," *Proc. IEEE ISCC*, Jul. 2015, pp. 918–923.

[22] C. Natalino, M. Schiano, A. Di Giglio, L. Wosinska, and M. Furdek, "Experimental study of machine-learning-based detection and identification of physical-layer attacks in optical networks," *J. Lightw. Technol.*, vol. 37, no. 16, pp. 4173–4182, Aug. 15, 2019.

[23] M. Bensalem, S. K. Singh, and A. Jukan, "On detecting and preventing jamming attacks with machine learning in optical networks," in *Proc. IEEE GLOBECOM*, Dec. 2019, pp. 1–6.

[24] M. Furdek, C. Natalino, A. Di Giglio, and M. Schiano, "Optical network security management: Requirements, architecture, and efficient machine learning models for detection of evolving threats" *J. Opt. Commun. Netw.*, vol. 13, no. 2, p. A144, 2021.

[25] J. Zhu, B. Zhao, W. Lu, and Z. Zhu, "Attack-aware service provisioning to enhance physical-layer security in multi-domain EONs," *J. Lightw. Technol.*, vol. 34, no. 11, pp. 2645–2655, Jun. 1, 2016.

[26] K. Manousakis and G. Ellinas, "Crosstalk-aware routing spectrum assignment and WSS placement in flexible grid optical networks," *J. Lightw. Technol.*, vol. 35, no. 9, pp. 1477–1489, May 1, 2017.

[27] M. Bensalem, I. Brasileiro, A. Drummond, and A. Jukan, "Embedding jamming attacks into physical layer models in optical networks," *Proc. IEEE ONDM*, May 2020, pp. 1–6.

[28] C. Rottondi, P. Martelli, P. Boffi, L. Barletta, and M. Tornatore, "Crosstalk-aware core and spectrum assignment in a multicore optical link with flexible grid," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2144–2156, Mar. 2019.

[29] A. Muhammad, G. Zervas, D. Simeonidou, and R. Forchheimer, "Routing, spectrum and core allocation in flexgrid SDM networks with multi-core fibers," in *Proc. IEEE ONDM*, May 2014, pp. 192–197.

[30] S. Fujii, Y. Hirota, H. Tode, and K. Murakami, "On-demand spectrum and core allocation for reducing crosstalk in multicore fibers in elastic optical networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 6, no. 12, pp. 1059–1071, Dec. 2014.

[31] K. Morita and K. Hirata, "Dynamic spectrum allocation method for reducing crosstalk in multi-core fiber networks," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2017, pp. 686–688.

[32] G. Savva, G. Ellinas, B. Shariati, and I. Tomkos, "Physical layer-aware routing, spectrum, and core allocation in spectrally-spatially flexible optical networks with multicore fibers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[33] F. Yousefi and A. Rahbar, "Novel crosstalk, fragmentation-aware algorithms in space division multiplexed-Elastic Optical Networks (SDM-EON) with considering physical layer security," *Opt. Switching Netw.*, vol. 37, Apr. 2020, Art. no. 100566.

[34] G. Savva, K. Manousakis, B. Shariati, I. Tomkos, and G. Ellinas, "Connection provisioning in spectrally-spatially flexible optical networks with physical layer considerations," in *Proc. 20th Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2018, pp. 1–4.

[35] M. Klinkowski and G. Zalewski, "Dynamic crosstalk-aware light-path provisioning in spectrally-spatially flexible optical networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 11, no. 5, pp. 213–225, May 2019.

[36] Y. Zhao, L. Hu, R. Zhu, X. Yu, X. Wang, and J. Zhang, "Crosstalk-aware spectrum defragmentation based on spectrum compactness in space division multiplexing enabled elastic optical networks with multicore fiber," *IEEE Access*, vol. 6, pp. 15346–15355, 2018.

[37] Y. Zhao, L. Hu, R. Zhu, X. Yu, X. Wang, and J. Zhang, "Crosstalk-aware spectrum defragmentation by re-provisioning advance reservation requests in space division multiplexing enabled elastic optical networks with multi-core fiber," *Opt. Exp.*, vol. 27, pp. 5014–5032, Dec. 2019.

[38] M. N. Dharmaweera, L. Yan, M. Karlsson, and E. Agrell, "Nonlinear impairments and crosstalk-aware resource allocation schemes for multicore-fiber-based flexgrid networks," *Proc. ECOC*, 2016, pp. 1–3.

[39] J. Perelló, J. M. Gené, A. Pagès, J. A. Lazaro, and S. Spadaro, "Flex-grid/SDM backbone network design with inter-core XT-limited transmission reach," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 8, no. 8, pp. 540–552, Aug. 2016.

[40] H. Tode and Y. Hirota, "Routing, spectrum, and core and/or mode assignment on space-division multiplexing optical networks [invited]," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 9, no. 1, pp. A99–A113, Jan. 2017.

[41] M. W. Przewozniczek, P. Lechowicz, and K. Walkowiak, "Metaheuristic algorithms with solution encoding mixing for effective optimization of SDM optical networks," *Eng. Appl. Artif. Intell.*, vol. 95, Oct. 2020, Art. no. 103843.

[42] P. Lechowicz, K. Walkowiak, and M. Klinkowski, "Greedy randomized adaptive search procedure for joint optimization of unicast and anycast traffic in spectrally-spatially flexible optical networks," *Comput. Netw.*, vol. 146, pp. 167–182, Dec. 2018.

[43] M. Yang, Y. Zhang, and Q. Wu, "Routing, spectrum, and core assignment in SDM-EONS with MCF: Node-arc ILP/MILP methods and an efficient XT-aware heuristic algorithm," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 10, no. 3, pp. 195–208, Mar. 2018.

[44] M. Yaghubi-Namaad, A. Ghaffarpour Rahbar, and B. Alizadeh, "Adaptive modulation and flexible resource allocation in space-division-multiplexed elastic optical networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 10, no. 3, pp. 240–251, Mar. 2018.

[45] R. Goscien, C. Natalino, L. Wosinska, and M. Furdek, "Impact of high-power jamming attacks on SDM networks," in *Proc. Int. Conf. Opt. Netw. Design Model. (ONDM)*, May 2018, pp. 77–81.

[46] J. Zhu and Z. Zhu, "Physical-layer security in MCF-based SDM-EONs: Would crosstalk-aware service provisioning be good enough?" *J. Lightw. Technol.*, vol. 35, no. 22, pp. 4826–4837, Nov. 1, 2017.

[47] T. Hayashi, T. Taru, O. Shimakawa, T. Sasaki, and E. Sasaoka, "Uncoupled multi-core fiber enhancing signal-to-noise ratio," *Opt. Exp.*, vol. 20, no. 26, p. B94, 2012.

[48] L. Velasco, M. Klinkowski, M. Ruiz, and J. Comellas, "Modeling the routing and spectrum allocation problem for flexgrid optical networks," *Photonic Netw. Commun.*, vol. 24, no. 3, pp. 177–186, Dec. 2012.

[49] Gurobi Optimization. (2020). *Gurobi Optimizer Reference Manual*. [Online]. Available: http://www.gurobi.com

GIANNIS SAVVA (Graduate Student Member, IEEE) received the B.Sc. degree in electrical engineering from the Department of Electrical and Computer Engineering, University of Cyprus, in 2017, where he is currently pursuing the Ph.D. degree. He is also a Research Assistant with the KIOS Research and Innovation Center of Excellence, University of Cyprus. His research interests include in the areas of telecommunications, resource allocation algorithms in spectrally-spatially flexible optical networks (SS-FONs), network planning, network coding, and physical-layer security in optical networks.

KONSTANTINOS MANOUSAKIS (Senior Member, IEEE) received the Diploma degree in computer engineering and informatics and the M.Sc. and Ph.D. degrees from the University of Patras, Greece, in 2004, 2007, and 2011, respectively. He is currently a Senior Research Fellow with the KIOS Research and Innovation Center of Excellence, University of Cyprus. His research work has been published in more than 55 top tier journals and telecommunications conferences. His research interests include optimization algorithms for high-speed networks, security in optical networks, network coding, protection, restoration techniques, and techno-economic aspects of communication networks. He is a Marie Curie Fellow, having been granted a Marie Curie Career Integration Grant for the period 2014 to 2018. His work has received a number of awards, including the Best Paper Award at CRITIS'2013. He was a recipient of the Cyprus Research Award-Young Researcher 2018 for the thematic area of Physical Sciences and Engineering which is awarded to a young researcher annually that has implemented high quality research work.

JACEK RAK (Senior Member, IEEE) received the M.Sc., Ph.D., and D.Sc. (habilitation) degrees from the Gdańsk University of Technology, Gdańsk, Poland, in 2003, 2009, and 2016, respectively. He is currently an Associate Professor and the Head of the Department of Computer Communications, Gdańsk University of Technology. He has authored more than 100 publications, including the book *Resilient Routing in Communication Networks* (Springer, 2015). From 2016 to 2020, he was leading the COST CA15127 Action *Resilient Communication Services Protecting End-user Applications from Disaster-based Failures* (RECODIS) involving more than 170 members from 31 countries. His main research interests include the resilience of communication networks and networked systems. He has also served as a TPC member of numerous conferences and journals. Recently, he has been the General Chair of ITS-T'17 and MMM-ACNS'17, the General Co-Chair of NETWORKS'16, the TPC Chair of ONDM'17, and the TPC Co-chair of IFIP Networking'19. He is a member of the Editorial Board of Optical Switching and Networking, Elsevier, and the Founder of the International Workshop on Resilient Networks Design and Modeling (RNDM).

IOANNIS TOMKOS (Fellow, IEEE) was a Full Professor and a Research Director with the Athens Information Technology Center-AIT, Greece, the Chair of Excellence Professor (Cátedras de Excelencia), University Carlos III, Spain, an Adjunct Professor with the College of Optical Sciences, The University of Arizona, Tucson, AZ, USA, an Adjunct Research Fellow with the ECE Department, University of Cyprus, an Adjunct Faculty Member with the Information Networking Institute, Carnegie Mellon University, Pittsburgh, PA, USA, a Senior Scientist with Corning Inc., Corning, NY, USA, and a Research Assistant with the University of Athens, Greece. At AIT, he founded and served as the Head for the High Speed Networks and Optical Communication (NOC) Group that was involved in more than 25 EU-funded research projects within which Prof. Tomkos served as the Principal Investigator having a consortium-wide leading role. He is currently a Professor of Optical Communications with the Department of Electrical and Computer Engineering (ECE), University of Patras. He, together with his colleagues and students, has authored more than 650 peer-reviewed archival articles, including more than 150 journal/magazine/book publications. His published work has received more than 10000 citations and his H-factor is 48 (as of December 2020 based on data from Google Scholar). For his academic achievements, he was elected as a Fellow of IEEE for contributions in Dynamic Optical Networks in 2018, a Fellow of the IET in 2010, and a Fellow of OSA in 2012.

GEORGIOS ELLINAS (Senior Member, IEEE) received the B.S., M.Sc., M.Phil., and Ph.D. degrees in electrical engineering from Columbia University. He served as an Associate Professor in electrical engineering for the City College of New York from 2002 to 2005, a Senior Network Architect with Tellium Inc., from 2000 to 2002, and a Research Scientist/Senior Research Scientist with Bell Communications Research (Bellcore) from 1993 to 2000. He is currently a Full Professor and the past Chair from 2014 to 2020 of the Department of Electrical and Computer Engineering, and a Founding Member of the KIOS Research and Innovation Center of Excellence (KIOS CoE), University of Cyprus. He has coauthored/co-edited four books on optical networks, more than 255 articles, conference papers, and book chapters, and he is the holder of 30 patents on optical networking. His research interests include in the areas of optical/telecommunication networks, transportation networks, the IoT, security of cyber-physical systems, and critical infrastructure systems. He is a Fellow of the IET in 2019, a Senior Member of OSA and ACM, and a member of the Marie Curie Fellows Association (MCFA).