Impact of High-Power Jamming Attacks on SDM Networks

Róża Goścień*, Carlos Natalino†, Lena Wosinska†, and Marija Furdek†
*Department of Systems and Computer Networks, Faculty of Electronics,
Wroclaw University of Science and Technology, Wroclaw, Poland. E-mail: roza.goscien@pwr.edu.pl
† Optical Networks Laboratory (ONLab), Royal Institute of Technology (KTH), Stockholm, Sweden.
E-mail: {carlosns, wosinska, marifur}@kth.se

***Abstract*—Space Division Multiplexing (SDM) is a promising solution to provide ultra-high capacity optical network infrastructure for rapidly increasing traffic demands. Such network infrastructure can be a target of deliberate attacks that aim at disrupting a large number of vital services. This paper assesses the effects of high-power jamming attacks in SDM optical networks utilizing Multi-Core Fibers (MCFs), where the disruptive effect of the inserted jamming signals may spread among multiple cores due to increased Inter-Core CrossTalk (ICo-XT). We first assess the jamming-induced reduction of the signal reach for different bit rates and modulation formats. The obtained reach limitations are then used to derive the maximal traffic disruption at the network level. Results indicate that connections provisioned satisfying the normal operating conditions are highly vulnerable to these attacks, potentially leading to huge data losses at the network level.**

***Index Terms*—High-power jamming attacks, optical network security, space division multiplexing.**

I. Introduction

Space Division Multiplexing (SDM) [1], [2] has been identified as a promising solution to the capacity crunch driven by the fast growth of bandwidth-intensive services. SDM enables ultra-high capacity in optical networks by utilizing a number of spatial resources, which can refer to multiple cores inside the same cladding of Multi-Core Fibers (MCFs); multiple modes inside the same core of Few-Mode Fibers (FMFs); or parallel single-mode fibers in the same bundle [3]. In weakly-coupled MCFs, which are in the focus of this work, each core within the fiber is used as a distinct communication channel, assuming sufficiently low interference between neighboring cores [4]. Key parameters determining the maximum transmission reach of optical signals in MCF are Amplified Spontaneous Emission (ASE) noise and Inter-Core CrossTalk (ICo-XT) [5].

As the critical infrastructure enabling a plethora of vital societal services, optical networks can be an enticing target of deliberate attacks aimed at service disruption [6]. High-power jamming attacks, in which an attacking signal is inserted into the network via, e.g., direct access to the fiber plant, monitoring ports, or by bending the fiber, can be harmful to optical networks deploying different technologies. In networks based on Wavelength Division Multiplexing (WDM), this attack affects co-propagating user signals by increasing the Inter-Channel CrossTalk (ICh-XT) among channels traversing the same fiber (core) [6]. In SDM-based networks, the damaging potential of jamming signals can not only affect signals inside the same core, but it can also propagate to signals in adjacent cores via increased ICo-XT. The primary requirement for increasing the network robustness to attacks is to evaluate the harmful effects caused by attacks and to quantify the damage they can cause to the network. While the damage from jamming attacks and the ways of increasing the level of physical-layer security in optical networks have been investigated in the context of Single-Mode Fibers (SMFs) [7]–[9], the harmful effects of jamming attacks in MCF-based SDM networks have not been studied so far.

To provide an assessment of the vulnerability of SDM networks to high-power jamming attacks, we evaluate the disruptive effects of jamming attacks to legitimate co-propagating signals in MCF. We first identify the maximum signal reach limited by ASE noise and ICo-XT under normal operating conditions. We then calculate the reduction of the maximum reach due to increased ICo-XT as a function of the power of the jamming signal, as well as the modulation format and bit rates of the legitimate signals. Using the developed model and ICo-XT-imposed reach limitations, we evaluate the overall traffic losses due to the physical-layer disruptions imposed by jamming attacks in the European backbone network, thus bounding the maximum extent of damage caused in the considered network. Results show that individual connections are highly vulnerable to the high-power jamming attacks, especially the ones with more complex modulation formats or longer reaches. At the network level, the attacks can disrupt a significant number of connections, causing the loss of huge amounts of data.

The remainder of this paper is organized as follows. Related works on physical-layer security aspects in optical networks are reviewed in Sec. II. Sec. III presents an assessment of the reach limitations of optical channels in an MCF imposed by ASE noise and by attacks causing excessive ICo-XT. Sec. IV expands the analysis to a network-wide scenario and evaluates the maximum possible traffic disruption. Finally, Sec. V concludes the work and presents guidelines for further investigation.

II. Related Work

As a promising solution to overcome the upcoming capacity crunch, SDM networks have been the subject of several studies

978-3-903176-07-2

focusing on a range of aspects from fiber manufacturing to the efficient spectrum management. Due to significant architectural differences, several management strategies need to be revisited, such as resource allocation algorithms, e.g., Routing and Wavelength Assignment (RWA) and Routing and Spectrum Assignment (RSA) algorithms, used in WDM and Elastic Optical Networks (EONs), respectively, need to be revisited to be suitable for SDM networks.

The work in [7] investigates the intra- and inter-channel CrossTalk (XT) effects caused by the injection of high-power jamming signals in WDM all-optical networks and shows their harmful effect to the performance of the optical channels. In [9], the authors propose approaches to decrease the overall damage caused by attacks through tailored, attack-aware routing and/or wavelength assignment. The work in [8] proposes a design strategy that enhances the conventional Dedicated Path Protection (DPP) with attack-awareness. The above-mentioned studies show that physical-layer security can be enhanced while using the same amount of optical resources as conventional, resource-saving approaches. However, these works consider a WDM optical network where the damaging effects of jamming signals stay confined in a single fiber core. In SDM networks, signal interference among adjacent cores cannot be neglected, particularly in the presence of high-power jamming signals.

The ICo-XT seems to be the main SDM drawback and limitation, which can affect the maximum transmission distance depending on the applied modulation format and bit rate. Therefore, the ICo-XT assessment is a crucial issue, and different ICo-XT models have been proposed in the literature. For instance, the authors of [10] and [11] apply very precise models, which allow estimating ICo-XT level for a particular core and transmission distance (from a source node) as a function of fiber physical characteristics, current transmission distance and number of adjacent cores.

The models can be simplified assuming the worst-case ICo-XT scenario (i.e., the core with the highest number of adjacent cores), as well as applied to find transmission reaches of different modulation formats in the presence of ICo-XT. By these means, the authors of [5] assess the modulation transmission reach as a function of the ICo-XT, the modulation format and its XT tolerance for different MCFs. Then, the work in [5] proposes a design strategy that considers SDM networks by considering the transmission reach limitations in MCFs. The work in [12] considers SDM networks and proposes an attack-aware Routing, Spectrum and Core Assignment (RSCA) strategy for design and provisioning. The strategy avoids assigning the same spectrum slot to potentially harmful signals and trusted signals if they traverse adjacent cores. This approach reduces the risks from ICo-XT impairment and related vulnerability of trusted channels. These works focus on the design and connection provision in SDM networks, but do not investigate the potential disruption caused by the ICo-XT in the presence of a malicious high-power jamming signal attack to connections provisioned considering normal operating conditions.

TABLE I
OSNR AND ICO-XT SIGNAL REQUIREMENTS [5].

	BPSK	**QPSK**	**16-QAM**	**64-QAM**
$OSNR_{min}$ [dB]	4.2	7.2	13.9	19.8
$XT_{dB,max}$ [dB]	-14	-17	-23	-29
P_S = 1 mW	L_{span} = 100 km		G = 20 dB	NF = 5.5 dB

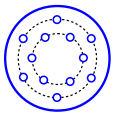


Fig. 1. 12-core double-ring MCF [14].

Different from the previous works in the literature, this work investigates traffic realized considering normal operating conditions and the most spectrally efficient modulation format is affected by the maximum reach limitations imposed by ICo-XT. We first provide an analysis of the maximum transmission reach of signals limited by ASE noise and ICo-XT under normal conditions and in the presence of a high-power jamming signal. Then, we evaluate how the reduction of signal reach disrupts traffic at a network level.

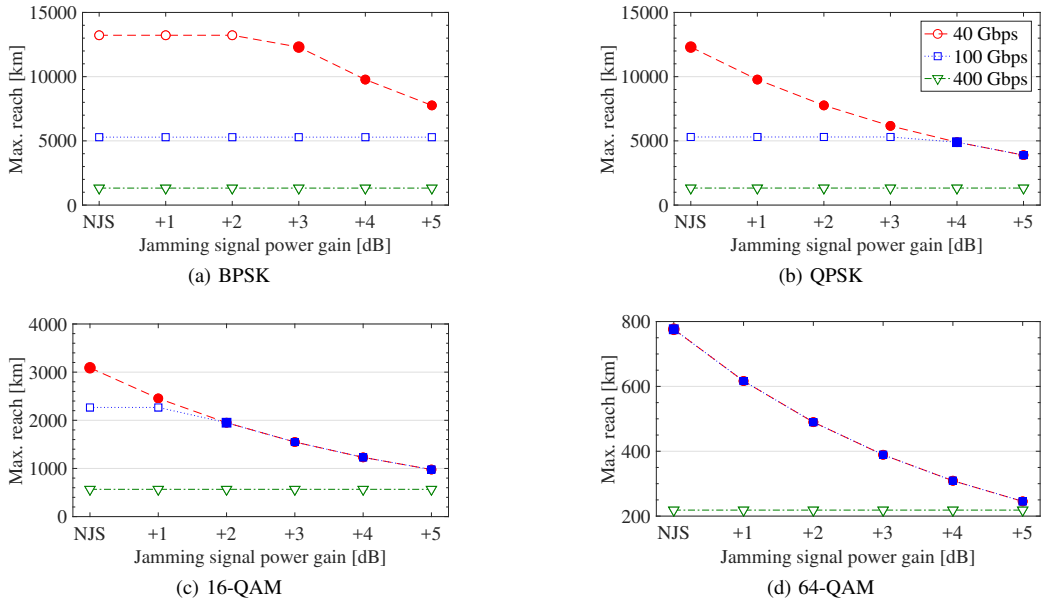
III. THE IMPACT OF JAMMING ATTACKS ON TRANSMISSION REACH IN MCF

In this section, we provide a methodology to calculate the transmission reach limitations of optical signals traversing MCF and quantify the reduction in the reach caused by jamming signal-induced ICo-XT.

The maximum transmission reach of an optically amplified signal is limited by several impairments which guide the selection of the bit rate and modulation format for each network connection. The two dominant limiting factors in MCF networks are ASE noise and ICo-XT [5], considering that the network has Digital Signal Processing (DSP)-enabled receivers, which are capable of compensating chromatic and polarization-mode dispersion, nonlinear channel backpropagation to compensate intra-channel nonlinearities, and balanced channel power.

Optical Signal-to-Noise Ratio (OSNR) requirements, which largely depend on the ASE noise, tighten with the increasing complexity of modulation formats, where more complex and spectrally efficient modulation formats require higher OSNR to achieve acceptable Bit Error Rate (BER) values. The transmission reach limitation due to noise is also inversely proportional to the signal bit rate, i.e., signals with higher bit rates have a shorter reach. The reach limitation due to ASE is calculated using (1), where P_S is the average optical power per channel, L_{span} is the distance between the equally spaced line amplifiers, $OSNR_{min}$ is the required OSNR at the receiver side (summarized in Table I), h is Planck's constant, f is the optical signal frequency, G and NF are the amplifier gain and noise factor, and R_S is the symbol rate [5], [13].

$$L_{max,OSNR} = \frac{P_S \cdot L_{span}}{OSNR_{min} \cdot h \cdot f \cdot G \cdot NF \cdot R_S} \quad (1)$$



(a) BPSK (b) QPSK

(c) 16-QAM (d) 64-QAM

Fig. 2. Maximum transmission reach limited by OSNR (white-faced markers) or XT (color-faced markers) for different bit rates. No Jamming Signal (NJS) represents the case where there is no jamming signal present in the fiber.

The reach limitation due to ICo-XT is a function of the modulation format only, where more complex modulation formats are more sensitive to ICo-XT, independent of the bit rate. This limitation is calculated using (2), where $XT_{dB,max}$ refers to the XT limit of the modulation format (described in Table I) and $XT_{dB,1km}$ refers to the fiber unitary ICo-XT (accumulated by transmission over 1 km) [5], [14].

$$L_{max,XT} = 10^{\frac{XT_{dB,max} - XT_{dB,1km}}{10}} \quad (2)$$

This analysis considers the balanced power scenario and the corresponding model from [5] as a baseline and investigates the ICo-XT effects of a harmful jamming signal with different power levels present in the fiber. Effects of the jamming signal on OSNR limits are considered negligible.

Table I describes the set of parameters, assumed as in [5], where user signals are transmitted at 1550 nm over a 12-core double-ring structure MCF with one propagation direction (see Fig. 1), yielding worst aggregate ICo-XT ($XT_{dB,1km}$) of -61.9 dB [5], [14]. A 4 dB penalty margin is also assumed for both OSNR and XT limits [5]. The considered transponder types support bit rates of 40 Gbps, 100 Gbps and 400 Gbps, as well as BPSK, QPSK, 16-QAM and 64-QAM modulation formats. The maximum transmission reach is calculated for the attack-free setup and for the worst-case attack scenario where the harmful jamming signal is inserted in one of the fiber cores in the inner ring, potentially affecting the signals in four adjacent cores via increased ICo-XT. The power gain of the jamming signal is varied from 1 to 5 dB to mimic attacks with different intensities.

Fig. 2 shows the maximum transmission reach for the different bit rates and modulation formats in the 12-core double-ring MCF showed in Fig. 1. In each scenario, the transmission reach of user signals is determined by the most limiting factor between OSNR and ICo-XT, denoted with white-faced and color-faced markers, respectively.

It is interesting to note that 400 Gbps signals are not affected by the considered attacks regardless of the used modulation format or the power of the jamming signal. This is because OSNR severely limits the reach of 400 Gbps signals already in normal operating conditions, and the attack-induced ICo-XT levels are not sufficient to exceed this limitation. However, as the modulation complexity increases, the ICo-XT limitation for 400 Gbps signals tightens and approaches the OSNR limitation. The trends for 400 Gbps signals across Figs. 2a-2d indicate that the power gain of the jamming signal should be above 5 dB to violate the OSNR threshold and impose reach limitations on these signals.

The less restrictive OSNR constraints allow for a longer reach of 40 and 100 Gbps channels, making these channels more likely to be limited by ICo-XT. The reach of 40 Gbps signals using QPSK, 16- or 64-QAM (Figs. 2b, 2c and 2d) is limited by ICo-XT even in the attack-free scenario (note the color-faced markers for the NJS case). For instance, as the power gain of the jamming signal increases, the maximum reach of 40 Gbps 64-QAM signals (Fig. 2d) decreases significantly, dropping by 20% already for 1 dB jamming signal power gain, and by 68% for 5 dB gain. Similar decrease (68%) is also experienced by 40 Gbps signals using QPSK and 16-QAM for jamming signal with 5 dB gain. For 40 Gbps QPSK signals, the drop is of 41% for jamming signal with 5 dB gain.

The reach of 100 Gbps signals in the attack-free scenario is limited by OSNR for all modulation formats but 64-QAM (Fig. 2d), where it is shaped by ICo-XT. Compared to normal operating conditions, jamming signal with 5 dB power gain reduces the reach of 100 Gbps signals by 26% (QPSK, Fig. 2b) to 68% (64-QAM, Fig. 2d). The transmission reach reduction

caused by a malicious signal shown in Fig. 2 indicates the level of disruption of individual connections which are established to satisfy the normal operating conditions, and gives an insight into the safety margins that should be considered to take this reduction into account.

IV. Network-Wide Traffic Disruption Caused by Jamming Attacks

After determining the impact of high-power jamming to the maximum transmission reach of individual connections, using the model and the assumptions from Sec. III, we now investigate the worst-case damage from a jamming attack at the network level. First, we describe the scenario and assumptions considered in this work. Then, we assess the disruption caused by the attack scenarios considered.

A. Network Scenario and Assumptions

We perform numerical experiments on the Euro28 network topology with 28 nodes and 82 links with an average length of 625 km, shown in Fig. 3. All physical links are assumed to be realized with 12-core double-ring MCFs (see Fig. 1) supporting elastic spectrum allocation with 12.5 GHz granularity and independent switching policy as in [3]. A 12.5 GHz guard-band is used between neighboring signals. Each demand can be supported by one transponder capable of serving the requested bit rate, i.e., traffic splitting/grooming is not supported. The available transponder bit rates are the same as considered in Sec. III, i.e., 40, 100 and 400 Gbps.

Each traffic matrix consists of randomly generated demands with a total traffic volume of 800 Tbps. The source and destination nodes of connection demands are uniformly distributed among all node pairs and the requested bit rate follows uniform distribution in the range between 10 and 400 Gbps.

To assign routes and spectral resources to each demand, we apply the Spectrum-Spatial Allocation (SSA) algorithm from [15], aimed at minimizing the total network spectrum usage. The algorithm begins by sorting the demands in the descending order of their bit rates. For each demand, up to 30 candidate paths are computed, and associated with a modulation format and the number of required spectrum slices. The modulation format assignment follows the Distance-Adaptive Transmission (DAT) rule from [15] aimed at maximizing the spectral efficiency and minimizing the number of required regenerators. The number of slices required per candidate path is calculated as a function of demand bit rate and the applied modulation format, using the model from [5]. During the SSA, the transmission reach is calculated using the procedure described in Sec. III for the attack-free scenario. Regenerators are deployed at network nodes only for demands which cannot be established otherwise, and do not perform spectrum/modulation conversion. The SSA heuristic then selects the candidate path, the cores and the spectrum for each demand which result in the lowest total spectrum usage.

Table II presents the distribution of the randomly generated traffic matrices in terms of bit rates. All presented results are averaged over ten different traffic matrices. For the considered

Fig. 3. Euro28 network topology with 12-core MCF.

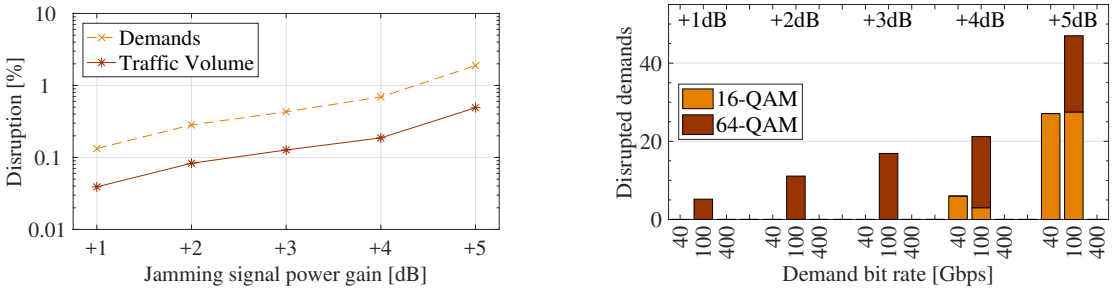
TABLE II
Traffic Matrices Bit Rates and the Modulation Formats Allocated to Satisfy the Demands.

Modulation	Bit Rate (%)			Total
	40	100	400	
BPSK	0.23	0	0	0.23
QPSK	3.55	6.15	69.39	79.1
16-QAM	4.39	8.67	6.93	19.99
64-QAM	0	0.51	0.16	0.68
Total	8.17	15.34	76.49	

traffic matrices, more than 75% of the demands are served by 400 Gbps bit rate channels, which are not affected by the analyzed attack scenarios, as shown in Sec. III. In such settings, less than 25% of the total traffic is vulnerable to an attack-induced reduction of transmission reach according to the results presented in Fig. 2. Table II also shows modulation formats selected by the SSA algorithm. For the considered SSA algorithm, 79.1% of the demands are realized using QPSK, followed by nearly 20% utilizing 16-QAM. BPSK and 64-QAM are applied to less than 1% of the demands.

B. Traffic Disruption Assessment

Considering the network scenario and assumptions presented in Sec. IV-A, we investigate the extent of disruption caused by jamming signals with different power gain values. Similar to Sec. III, the jamming signal is considered to have power gain of 1 to 5 dB relative to the legitimate signals. We consider a worst-case attack scenario where the jamming signal traverses all fiber links in the topology. While in reality the spreading of the jamming signal can be thwarted at intermediate nodes, this assumption allows us to assess an upper bound on the possible network disruption caused by this type of attacks. For each demand, we verify whether the demand is disrupted by the attack or not, considering the reach limitations presented in Sec. III. A demand is considered as disrupted if its path length exceeds the maximum reach constraint imposed by the jamming attack. The results for different attack scenarios are shown in Fig. 4. Fig. Fig. 4a shows the percentage of disrupted demands and traffic volume. Nearly 2% of all demands can be disrupted by a jamming signal with 5 dB power gain, carrying 0.5% of the total network traffic volume. Considering that the total network traffic is 800 Tbps, up to 4 Tbps can be disrupted, causing huge data losses. Moreover, if we consider only the demands



(a) Percentage of demands and traffic volume disrupted by the attack.

(b) Number of demands disrupted by the attack according to their bit rate and modulation format.

Fig. 4. Percentage, bit rate and modulation format of the demands disrupted by the attack.

vulnerable to the attack, i.e., excluding 400 Gbps signals, the percentage of disrupted demands can reach up to 8%.

Fig. 4b presents the number of disrupted demands according to their modulation format and bit rate. Only 16-QAM and 64-QAM demands are affected, which is in line with their vulnerability analysis shown in Figs. 2c and 2d. 100 Gbps signals are the most sensitive to jamming. On average, five 100 Gbps signals are affected already when considering attacks with 1 dB gain, while this number increases to 47 for 5 dB power gain. Jamming signals at 4 and 5 dB gain affect 40 Gbps demands as well, disrupting 6 and 27 demands, respectively.

V. Conclusions

This paper investigates the extent of disruption caused by high-power jamming attacks to legitimate traffic in a SDM network. We quantify the attack-induced reduction of maximum transmission reach for different bit rates and modulation formats, as well as the resulting traffic losses at the network level. The study provides an insight into the safety margins that could be considered to mitigate traffic losses and increase SDM network security. The results show that the correct modulation format is crucial not only for the spectrum efficiency, as shown in the related works, but is also of utmost importance for the resiliency of demands against high-power jamming signal attacks.

Further studies are needed to understand how different optical network technologies affect the vulnerability to physical layer attacks. In particular, the migration from WDM to SDM optical networks may require new approaches to guarantee the security of the optical layer. Moreover, the different extent of disruptions can be observed depending on the considered traffic matrices and network topology, as well as the applied SSA algorithm. Finally, in addition to jamming signal attacks, other kinds of physical layer attacks need to be studied in order to offer high security and minimize the network vulnerability.

Acknowledgment

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) and the Celtic-Plus project SENDATE-EXTEND funded by VINNOVA. Róża Goścień was supported by the National Science Centre, Poland, under Grant 2015/19/B/ST7/02490 and by statutory funds of Department of Systems and Computer Networks, Wroclaw University of Science and Technology.

References

[1] T. Mizuno, H. Takara, K. Shibahara, A. Sano, and Y. Miyamoto, “Dense space division multiplexed transmission over multicore and multimode fiber for long-haul transport systems,” *IEEE/OSA J. Lightwave Techn.*, vol. 34, no. 6, pp. 1484–1493, Feb 2016.

[2] W. Klaus, B. J. . Puttnam, R. S. Luis, J. Sakaguchi, J.-M. D. Mendinueta, Y.Awari, and N. Wada, “Advanced space division multiplexing technologies for optical networks [invited],” *IEEE/OSA J. Optical Commun. Netw.*, vol. 9, no. 4, pp. C1–C11, Apr 2017.

[3] M. Klinkowski, P. Lechowicz, and K. Walkowiak, “Survey of resource allocation schemes and algorithms in spectrally-spatially flexible optical networking,” *Opt. Switch. Netw.*, vol. 27, pp. 58–78, Sep 2017.

[4] K. Saitoh, T. Fujisawa, and T. Sato, “Design and analysis of weakly- and strongly-coupled multicore fibers,” *Proc. Photonic Netw. and Devices*, pp. NeTu2B.5.1 – 3, Jul 2017.

[5] 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. and Netw.*, vol. 8, no. 8, pp. 540–552, Aug 2016.

[6] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, “Physical-layer security in evolving optical networks,” *IEEE Com. Mag.*, vol. 54, no. 8, pp. 110–117, August 2016.

[7] Y. Peng, Z. Sun, S. Du, and K. Long, “Propagation of all-optical crosstalk attack in transparent optical networks,” *Opt. Eng.*, vol. 50, no. 8, pp. 085 002.1–3, August 2011.

[8] M. Furdek, N. Skorin-Kapov, and L. Wosinska, “Attack-aware dedicated path protection in optical networks,” *IEEE/OSA J. Lightwave Techn.*, vol. 34, no. 4, pp. 1050–1061, February 2016.

[9] N. Skorin-Kapov, M. Furdek, R. A. Pardo, and P. P. Mariño, “Wavelength assignment for reducing in-band crosstalk attack propagation in optical networks: ILP formulations and heuristic algorithms,” *European Journal of Operational Research*, vol. 222, no. 3, pp. 418 – 429, 2012.

[10] A. Muhammad, G. Zervas, and R. Forchheimer, “Resource allocation for space-division multiplexing: Optical white box versus optical black box networking,” *Journal of Lightwave Technology*, vol. 33, no. 23, pp. 4928–4941, Dec 2015.

[11] L. Zhang, N. Ansari, and A. Khreishah, “Anycast planning in space division multiplexing elastic optical networks with multi-core fibers,” *IEEE Communications Letters*, vol. 20, no. 10, pp. 1983–1986, Oct 2016.

[12] J. Zhu and Z. Zhu, “Physical-layer security in MCF-based SDM-EONs: Would crosstalk-aware service provisioning be good enough?” *IEEE/OSA J. Lightwave Techn.*, vol. 35, no. 22, pp. 4826–4837, Nov 2017.

[13] R. J. Essiambre, G. Kramer, P. J. Winzer, G. J. Foschini, and B. Goebel, “Capacity limits of optical fiber networks,” *IEEE/OSA J. Lightwave Techn.*, vol. 28, no. 4, pp. 662–701, Feb 2010.

[14] A. Sano *et al.*, “409-tb/s + 409-tb/s crosstalk suppressed bidirectional mcf transmission over 450 km using propagation-direction interleaving,” *Opt. Express*, vol. 21, no. 14, pp. 16 777–16 783, Jul 2013.

[15] R. Goścień, K. Walkowiak, and M. Klinkowski, “Distance-adaptive transmission in cloud-ready elastic optical networks,” *IEEE/OSA J. Opt. Commun. and Netw.*, vol. 6, no. 10, pp. 816–828, 2014.