Attack-Aware Dedicated Path Protection in Optical Networks

Marija Furdek, *Member, IEEE, Member, OSA*, Nina Skorin-Kapov, *Member, IEEE*,
and Lena Wosinska, *Senior Member, IEEE*

***Abstract*—Due to the high data rates in optical networks, physical-layer attacks targeting service degradation, such as power jamming, can potentially lead to large data and revenue losses. Conventional network survivability approaches which establish link-disjoint working and backup paths to protect from component faults may not provide adequate protection for such attacks. Namely, the working and the backup paths, although link-disjoint, might both be affected by a single attack scenario due to specific attack propagation characteristics. To enhance the existing survivability approaches, we utilize the concept of an attack group (AG) which incorporates these characteristics to identify connections which can simultaneously be affected by a single attack. We apply this concept to dedicated path protection (DPP) and develop attack-aware DPP (AA-DPP) approaches which aim to establish AG-disjoint primary and backup paths in a cost-effective manner. We provide a two-step ILP formulation for the routing and wavelength assignment of the working and backup paths, as well as a heuristic for larger problem instances. Numerical results indicate that the proposed approaches provide dedicated path protection schemes with enhanced attack protection without using more resources (i.e., wavelengths, average path lengths) than standard DPP methods.**

***Index Terms*—Communication system security, heuristic algorithms, mathematical programming, optical fiber networks, optimization, wavelength routing, WDM networks.**

I. Introduction

It is widely recognized that optical networks are crucial in supporting the rapidly growing global network traffic intensity in a cost-efficient manner. Therefore, issues related to optical network security become very important for ensuring proper network operation. A number of optical-layer security breaches and physical-layer attack methods have been identified in the literature [1]–[6], particularly in transparent optical networks. Attacks can induce financial losses to the clients or cause network-wide service disruption, possibly leading to huge data and revenue losses for operators. Attacks targeting service degradation, such as power jamming, typically involve inserting malicious signals into the network which can potentially propagate along configured connections causing wide-spread damage. The tightening bandwidth and reliability performance requirements of mission-critical applications, the widening areas of optical network application and increasing infrastructure accessibility all motivate the need for effective protection and restoration strategies in optical networks, not only to protect from component failures, but also from physical-layer attacks.

Optical-layer security is becoming a growing concern among operators, driving the development of intrusion detection systems (e.g., [7], [8]) and other security solutions aimed at detecting attacks or making access to critical network infrastructure more difficult. These solutions may be further combined with management paradigms related to jamming attacks such as those from [3], [9]. Although these established paradigms enable detection and source localization of attacks, they do not address the aspect of network survivability in the presence of attacks. Standard optical network protection approaches typically establish link and/or node-disjoint working and backup paths, focusing on fiber cuts and node equipment failures as the main reasons for service interruptions [10]–[12]. Although effective in the presence of failures, such approaches may not provide adequate protection in the presence of attacks which can propagate and degrade multiple link/node-disjoint paths simultaneously. To deal with this problem, we introduce the concept of so-called attack groups (AGs), extending our preliminary work from [13]. AGs identify connection paths that can affect each other in case they carry malicious signals based on the specific propagation characteristics of the considered attack(s). A connection is then assumed to be attack-protected if its primary and backup paths are AG-disjoint.

While providing enhanced security of the network routing solution, protecting all connections from propagating attacks could incur significant increase of resource usage and may not be economically viable. Consequently, instead of employing full attack protection, we propose to minimize the number of attack-unprotected connections (on top of standard failure-oriented link-disjoint protection) in such a way that little or no extra resources are required. Unlike the existing failure management paradigms related to attacks, our objective is not to detect them but to reduce their damaging effects through attack-aware network planning. We do so by modeling attack propagation characteristics with AGs and incorporating attack-awareness into the objective of the conventional link-disjoint dedicated path protection problem, referring to the approach as attack-aware dedicated path protection (AA-DPP). We consider propagating in-band jamming attacks and propose a two-step integer linear program (ILP) formulation for AA-DPP, as well as an iterative

Manuscript received September 4, 2015; revised November 20, 2015; accepted December 8, 2015. Date of publication December 16, 2015; date of current version February 10, 2016. This work was supported in part by the European Community's Seventh Framework Program FP7/2007-2013 under Grant 318137 (ICT-DISCUS), and Spanish Grant TEC2014-53071-C3-1-P (ONOFRE).

M. Furdek and L. Wosinska are with the KTH Royal Institute of Technology, Kista S-164 40, Sweden (e-mail: marifur@kth.se; wosinska@kth.se).

N. Skorin-Kapov is with the University Center of Defense, San Javier Air Force Base, Technical University of Cartagena, Murcia 30720, Spain (e-mail: nina.skorinkapov@cud.upct.es).

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

Digital Object Identifier 10.1109/JLT.2015.2509161

heuristic for larger instances. Numerical results indicate that the proposed approaches are able to protect a large number of connections from jamming attacks, while using the same amount of resources as analogous non-attack-aware DPP approaches.

The remainder of the paper is organized as follows. Section II outlines related work, while attack propagation characteristics and AGs are discussed in Section III. The AA-DPP problem definition, the two-step ILP formulation and the iterative heuristic approach are presented in Sections IV, V and VI, respectively. Section VII describes the numerical results and Section VIII concludes the paper.

II. Related Work

Numerous protection approaches have been developed to ensure reliable transmission in the presence of single, and possibly multiple, component faults [14], [15]. Protection schemes are typically divided into shared or dedicated approaches providing path or link protection. Path protection implies reserving a link- (and possibly node-) disjoint backup path for the working path of each connection, while link protection implies reserving an alternative route for each link. In shared protection, multiple backup paths can share network resources assuming that their respective primary paths are disjoint, i.e., do not fail simultaneously under single component failure. Dedicated protection schemes reserve protection paths without sharing resources, either transmitting simultaneously on both working and backup paths ($1 + 1$ protection) or only on the primary path keeping the reserved backup resources in cold standby until a failure occurs (1:1 protection). In this work, we focus on 1:1 dedicated path protection.

An ILP formulation for the dedicated path protection problem with the objective to minimize the total used capacity was proposed in [16]. An alternative formulation to minimize blocking under single-link failures is given in [17]. Since the dedicated path protection problem has been shown to be NP-complete [18], several heuristics approaches have been proposed for larger instances. Surveys of such heuristics can be found in [12] and [19].

While most protection approaches consider single component failures, several methods have also been developed to deal with multiple failures [20], [21]. The concept of shared risk groups (SRGs), where multiple network resources are assumed to fail as a group, e.g., fibers sharing the same fiber conduit, has been considered in survivability approaches by ensuring that the working and backup paths are SRG-disjoint [22]. Furthermore, protection schemes in the context of geographically correlated failures which can be a consequence of natural disasters or a physical infrastructure attack (e.g., an Electromagnetic Pulse attack or Weapons of Mass Destruction) have been studied in [23]. However, protection in the context of more covert signal degradation attacks, such as power jamming, which can affect multiple connections that do not necessarily all share the same physical components, has not yet been widely studied.

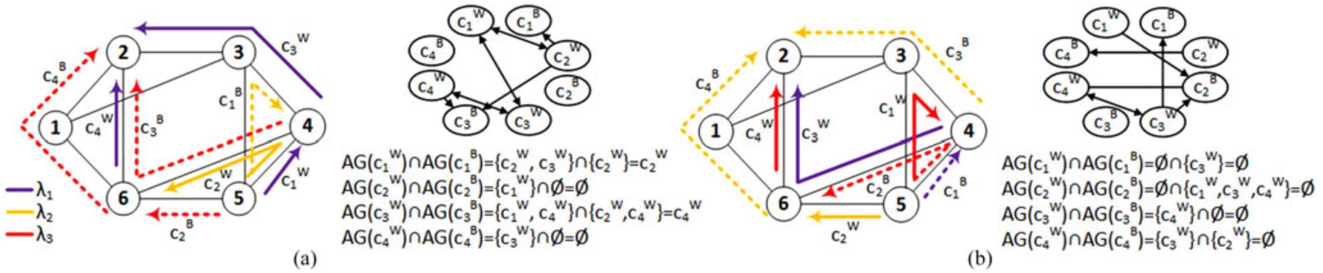
An initial approach for survivable routing and regenerator placement in the presence of power jamming attacks was proposed in [24] for translucent networks, where the propagation of attacks is reduced by adding regeneration points. In transparent optical networks, ensuring full protection from service degradation attacks would require a huge amount of resources. Thus, we propose to partially protect the network from attacks by adding attack-awareness to standard survivability approaches which consider single link failures such that little or no extra resources are incurred. Attack-awareness has been incorporated into the routing and wavelength assignment (WA) process in transparent optical networks to reduce the number of connections that can be affected by a single jamming attack in [25]–[27]. In this paper, we address the issue of survivability to provide protection in the presence of such attacks, extending our preliminary works from [13], [28] and [29]. In [28], we developed a heuristic approach for survivable WA considering only signal degradation effects of power jamming inside optical switches. In [13], we introduced the concept of AGs modeling the compound harmful effects from such attacks in both optical switches and fibers, and proposed a heuristic approach for attack-aware DPP which ensures all connections are attack-protected. In [29], we developed an ILP formulation for shared path protection again guaranteeing full attack-protection. The results of these preliminary studies suggested that obtaining full protection from attacks may induce considerable resource overhead. This indicates that schemes which maximize the degree of protection from attacks while using no extra resources compared to resource-minimizing approaches may represent more economically viable solutions. To this end, in this paper we extend upon the concept of AGs based on attack propagation characteristics and develop AA-DPP approaches to minimize the number of attack-unprotected connections in a cost-efficient manner.

III. Attack Propagation and AGs

A. Propagation Characteristics of Service Degradation Attacks

Physical-layer attacks in optical networks have been categorized according to those aimed at gaining unauthorized access to the carried data or those causing service degradation [1]–[3], [5], [6], the latter of which is considered in this paper. Service degradation attacks generally involve inserting malicious signals into the network, such as optical signals of excessive power (e.g., 5–20 dB above other, legitimate signals), to degrade other user connections. Such a signal can be inserted on a legitimate channel used in the network (in-band jamming) or on a wavelength outside the signal window (out-of-band jamming) [6] and can degrade co-propagating user channels due to increased crosstalk and nonlinear effects in fibers. Furthermore, a jamming signal can cause so-called gain competition in optical amplifiers where the high-powered signal robs weaker legitimate signals of gain. Even if electronic equalization in amplifiers counteracts gain competition in the steady-state, initial brief oscillations in gain (called transients) can occur. Additionally, in-band jamming signals can increase intra-channel crosstalk in optical switches to other user signals traversing the switch on the same wavelength.

In-band jamming attacks can be especially harmful in networks employing fixed optical add drop multiplexers (FOADMs) without variable optical attenuators since the attack could propagate along the connection it was inserted on unthwarted. Approximately 40% of current networks still employ



1
2
3
4
5
6
c_1^W
c_1^B
c_2^W
c_2^B
c_3^W
c_3^B
c_4^W
c_4^B
λ_1
λ_2
λ_3
(a)
$AG(c_1^W)\cap AG(c_1^B)=\{c_2^W, c_3^W\}\cap\{c_2^W\}=c_2^W$
$AG(c_2^W)\cap AG(c_2^B)=\{c_1^W\}\cap\emptyset=\emptyset$
$AG(c_3^W)\cap AG(c_3^B)=\{c_1^W, c_4^W\}\cap\{c_2^W,c_4^W\}=c_4^W$
$AG(c_4^W)\cap AG(c_4^B)=\{c_3^W\}\cap\emptyset=\emptyset$
(b)
$AG(c_1^W)\cap AG(c_1^B)=\emptyset\cap\{c_3^W\}=\emptyset$
$AG(c_2^W)\cap AG(c_2^B)=\emptyset\cap\{c_1^W,c_3^W,c_4^W\}=\emptyset$
$AG(c_3^W)\cap AG(c_3^B)=\{c_4^W\}\cap\emptyset=\emptyset$
$AG(c_4^W)\cap AG(c_4^B)=\{c_3^W\}\cap\{c_2^W\}=\emptyset$

Fig. 1. Two possible Dedicated Path Protection (DPP) schemes and their associated attack graphs and AGs.

FOADMs at network nodes, particularly in the metro segment. In such a scenario, all other connections sharing common fibers or switches with the attacking signal downstream of the attacking point could be affected. In some cases it may even be possible for attacked connections to gain attacking capabilities themselves and spread the attack even further beyond the reach of the original attacking signal [4].

In core networks which employ reconfigurable optical add drop multiplexers (ROADMs) at all (or most) nodes, a jamming signal would generally be attenuated at intermediate nodes. However, some propagation may be achieved depending on the strength of the jamming signal and the working range of the associated variable optical attenuators. Furthermore, amplifier transient oscillations leading to error bursts could still potentially propagate, where transients on one link could cause transients on successive links. Although amplifiers used in newer terrestrial networks work in constant gain mode with transient suppression control, there are still significant deployments with constant power based amplifiers.

In mixed line rate and future elastic optical networks, an alternative service degradation attack, which we refer to as a mixed modulation attack, could be achieved by inserting a lower line-rate OOK-modulated signal near a higher line-rate 40/100/200G channel using BPSK, QPSK or DP-QPSK modulation without allowing for enough guardband [5]. This could cause increased cross phase modulation effects significantly degrading the higher line-rate signals. If such a signal were inserted as a legitimate connection, it could propagate through the network degrading all co-propagating neighboring higher-rate channels. Such a signal would not be thwarted by power equalizing components or even be detected as malicious by power monitoring equipment.

Another possible attack scenario, called a low power QoS attack and identified in [30], could be realized by inserting a splitter at the head of a link to deliberately attenuate the power by a certain amount. In such a scenario, nodes equipped with attenuation-based power equalization downstream of the attack could actually help the attack to propagate by attenuating co-propagating channels to ensure a flat power spectrum.

B. AGs and the Considered Propagation Model

In order to model the propagation characteristics of an attack and incorporate them into the protection process, we introduce the concept of an *AG*. We define an AG of a working or backup path *i,* denoted as *AG(i),* to comprise all other working paths which, if carrying an attacking signal, could potentially degrade path *i*. Naturally, this depends on the type of attack, its propagation characteristics and physical routing and WA of all the connections in the network. Unlike most SRGs which consider multiple correlated component failures generally based on physical proximity, AGs model attacking relations between connections based on attack propagation capabilities which may affect lightpaths at widespread locations. While SRGs are a function of a set of resources (e.g., links) and denote a group of lightpaths which fail simultaneously if a certain set of resources fails, AGs are a function of an individual connection (i.e., working or backup path). Moreover, unlike SRG-failure resiliency which is typically obtained through adaptation of lightpath routing, achieving attack survivability in certain scenarios needs to additionally take into account the interplay between lightpaths that stems from the WA scheme.

The concept of AGs can be applied to individual attacks by considering their distinctive propagation characteristics or a combination of them. In this paper, we consider the propagation scenario where an attacking signal inserted on any legitimate connection could potentially compromise all other connections sharing common links with it, as well as connections assigned the same wavelength and traversing common switches with it.[1] This assumption models the primary propagation of in-band high power jamming attacks in FOADM-based networks, where all connections co-propagating with the original attacking signal can be degraded. We consider in-band jamming in FOADM-based networks since a connection protected from such an attack would also inherently be protected from an analogous attack in ROADM-based networks, as well as out-of-band jamming attacks and mixed modulation attacks in MLR or elastic networks, where propagation is more limited. Thus, the model is rather general and considers a subset of attack scenarios taking into account different network architectures. Alternative attack models could be devised to include even more attacks or tailored to specific individual ones, according to the network architecture employed.

Calculation of the AGs of individual paths based on our propagation model and the impact of different path protection schemes is illustrated in Fig. 1. Assume four directed connection requests: c_1*:(5-4),* c_2*:(5-6),* c_3*:(4-2)* and c_4*:(6-2);* and three available wavelengths: λ_1, λ_2, and λ_3. Two different dedicated path protection schemes are shown in Fig. 1(a) and (b), where the working and backup paths of each connection c_i are denoted

[1] We assume that common switches also include path source and destination nodes where, depending on the implementation, signals which are added or dropped may still traverse common components with the attacking signal.

as c_i^W and c_i^B, respectively. In order to find the AG of each path, we model attacking relations between paths with a so-called *attack graph*. In the attack graph, nodes represent the working and backup paths of individual connections and directed links indicate whether an attacking signal inserted on one of them can affect the other. Note, we consider 1:1 protection where only working paths are active and assumed to potentially carry malicious signals, i.e., are possible sources of attack.

The AG of a working or backup path is then composed of all the nodes in the attack graph with which it is connected via incoming links. For example, the AG of working path c_1^W in Fig. 1(a) would be $AG(c_1^W) = \{c_2^W, c_3^W\}$. Namely, path c_1^W could potentially be degraded by an attack inserted on path c_2^W because they share common link (5–4), as well as by an attack inserted on c_3^W because they share common switch (4) and are routed on the same wavelength (λ_1). For a connection to be attack-protected, the AGs of the primary and backup paths should be disjoint. Thus, the associated calculations of AG-disjointedness are shown in the figure. We can see that connection c_1 is not attack-protected because its working and backup paths share a common AG element, i.e., c_2^W. Similar considerations apply to connection c_3, whose working and backup paths can both potentially be degraded by an attack inserted on c_4^W.

Fig. 1(b) shows a slightly different path protection scheme which achieves better attack-protection while using the same number of wavelengths and total path length as the solution in Fig. 1(a). In Fig. 1(b), all connections are attack-protected, i.e., all connections have AG-disjoint working and backup paths, while still occupying 3 wavelengths and 12 wavelength-links equal to that of the solution in Fig. 1(a).

IV. AA-DPP: Problem Definition

The AA-DPP problem is defined as follows. Given is a physical topology graph *G = (V, E),* composed of a set of nodes *V* interconnected by a set *E* of directional links. Given are also a set of available wavelengths *W* and a set of connection requests *C*, each defined by their source and destination nodes. Solving the AA-DPP problem consists of finding a pair of link-disjoint paths for each connection request, along with their associated routing and WA schemes, while minimizing the number of attack-unprotected connections. A connection is assumed attack-unprotected if the working and backup paths of the connection are not AG-disjoint according to the attack propagation model described in Section III-B. The maximal total hop length for all established paths is constrained by a parameter *H*. No wavelength conversion is assumed meaning the wavelength continuity constraint must hold, i.e., a path (working or backup) must have the same wavelength assigned on all links along the path. The wavelength clash constraint must also hold where two paths sharing a common link cannot be assigned the same wavelength.

V. The Two-Step ILP Formulation (AA-DPP-ILP)

Due to the high complexity of the AA-DPP problem with the described propagation model, we formulate a two-step ILP which solves the routing and the WA phases subsequently. The routing phase models attacking relations between connections sharing common links, while the WA phase models attacking relations between connections traversing common switches on the same wavelength. Note that an integrated ILP could be run by combining the two formulations to find a globally optimal solution but experimental results indicate that the integrated ILP could only be run in reasonable time for extremely small instances (4 nodes, 6 connections). Thus, the two-step approach is applied here.

A. Step 1: The Routing Phase of AA-DPP-ILP

Notation and parameters:

$v \in V$ Network nodes.

$e \in E$ Directed network links.

o_e and $t_e \in V$ The source and destination node of link *e*, respectively.

$c, d \in C$ Connection requests.

o_c and $t_c \in V$ The source and destination nodes of connection *c*, respectively.

H Maximal total hop length.

Routing variables:

$p_e^c = 1$ If the working path of connection *c* uses link *e*, 0 otherwise.

$\bar{p}_e^c = 1$ If the backup path of connection *c* uses link *e*, 0 otrw.

$q_v^c = 1$ If the working path of connection *c* uses node *v*, 0 otrw.

$\bar{q}_v^c = 1$ If the backup path of connection *c* uses node *v*, 0 otrw.

Link-sharing and attack-reach variables:

$l_{c,d}^e = 1$ If the working path of connection *c* shares link *e* with the working path of connection *d*, 0 otherwise.

$\bar{l}_{c,d}^e = 1$ If the backup path of connections *c* shares link *e* with the working path of connection *d*, 0 otherwise.

$l_{c,d} = 1$ If the working path of connection *c* shares any link with the working path of connection *d*, 0 otherwise.

$\bar{l}_{c,d} = 1$ If the backup path of connection *c* shares any link with the working path of connection *d*, 0 otherwise.

$a_{c,d}^L = 1$ If the working and the backup path of connection *c* both share link(s) with the working path of connection *d* (and can, thus, be attacked by *d* on links), 0 otherwise.

$a_c^L = 1$ If the backup path of connection *c* is attack-unprotected on links, 0 otherwise.

Objective:

$$\text{Minimize} \sum_{c \in C} a_c^L \tag{1}$$

Subject to:

$$\sum_{e \in E: v = o_e, t_e} p_e^c = \begin{cases} 1, & \text{if } v = o_c \text{or} v = t_c \\ 2 \cdot q_v^c, & \text{otherwise} \end{cases} \quad \forall c \in C,\ v \in V \tag{2a}$$

$$\sum_{e \in E: v = o_e, t_e} \bar{p}_e^c = \begin{cases} 1, & \text{if } v = o_c \text{or} v = t_c \\ 2 \cdot \bar{q}_v^c, & \text{otherwise} \end{cases} \quad \forall c \in C,\ v \in V \tag{2b}$$

$$p_e^c + \bar{p}_e^c \leq 1 \quad \forall c \in C, \quad e \in E \tag{2c}$$

$$\sum_{c \in C} \sum_{e \in E} (p_e^c + \bar{p}_e^c) \leq H \tag{2d}$$

$$l_{c,d}^e = p_e^c \wedge p_e^d \quad \forall e \in E, \quad c, d \in C \tag{3a}$$

$$\bar{l}_{c,d}^e = \bar{p}_e^c \wedge p_e^d \quad \forall e \in E, \quad c, d \in C \tag{3b}$$

$$l_{c,d} = \bigvee_{e \in E} l_{c,d}^e \quad \forall c, d \in C \tag{3c}$$

$$\bar{l}_{c,d} = \bigvee_{e \in E} \bar{l}_{c,d}^e \quad \forall c, d \in C \tag{3d}$$

$$a_{c,d}^L = l_{c,d} \wedge \bar{l}_{c,d} \quad \forall c, d \in C \tag{3e}$$

$$a_c^L = \bigvee_{d \in C} a_{c,d}^L \quad \forall c \in C. \tag{3f}$$

The objective of the routing phase of AA-DPP-ILP, given in Eq. (1), is to minimize the number of attack-unprotected connections under the assumption that an attack inserted on a working path can degrade any other working or backup path if they share a common link. Eqs. (2a), (2b) define flow conservation and node usage, Eq. (2c) ensures that the working and backup paths are link-disjoint and Eq. (2d) limits the total hop length of all the paths to *H*.

Eqs. (3) of AA-DPP-ILP ensure that if the working and the backup paths of a connection *c* both share links with the working path of any other connection, then connection *c* is marked as attack-unprotected. This identifies the AG intersections which are due to sharing links with potential attacking signals. Eqs. (3a) and (3b) couple the working and the backup path of connection *c*, respectively, to any connection *d* whose working path shares a link with them, while Eqs. (3c) and (3d) mark link-sharing over all connections. Eq. (3e) identifies connections *c* whose both the working and the backup path can be attacked by a connection *d*, while Eq. (3f) denotes connection *c* as unprotected if any such connection *d* exists. For the sake of brevity, symbols $\wedge$ and $\vee$ are used to denote logical *AND* and *OR* operations, respectively. Relation $c = a \wedge b$ is implemented as $c \leq a; c \leq b; \quad c \geq a + b - 1$. Similarly, relation $c = \bigvee_i a_i$ is implemented as $c \geq a_i \quad \forall i; c \leq \sum_i a_i$.

B. Step 2: The WA Phase of AA-DPP-ILP

In the WA phase of AA-DPP-ILP, the values for the routing, link-sharing and attack-reach variables found by solving the routing phase of AA-DPP-ILP are used as input parameters, in addition to the set of nodes, links and connection requests. An additional parameter and the variables for the WA phase are as follows.

NOTATION AND PARAMETERS:

$w \in W$ Set of available wavelengths.

WA VARIABLES:

$r_w^c = 1$ If the working path of *c* uses wavelength *w*; 0 otrw.

$\bar{r}_w^c = 1$ If the backup path of *c* uses wavelength *w*; 0 otrw.

SWITCH AND WAVELENGTH-SHARING AND ATTACK-REACH VARIABLES:

$s_{v,w}^{c,d} = 1$ If the working path of connection *c* shares switch *v* and wavelength *w* with the working path of connection *d*, 0 otherwise.

$\bar{s}_{v,w}^{c,d} = 1$ If the backup path of connection *c* shares switch *v* and wavelength *w* with the working path of connection *d*, 0 otherwise.

$s^{c,d} = 1$ If the working path of connection *c* shares any common switch and a wavelength with the working path of connection *d*, 0 otherwise.

$\bar{s}^{c,d} = 1$ If the backup path of connection *c* shares any common switch and a wavelength with the working path of connection *d*, 0 otherwise.

$a_{c,d}^{LS} = 1$ If the working path of *d* can attack the working path of *c* on links, and the backup path of *c* in switches, 0 otherwise.

$a_{c,d}^{SL} = 1$ If the working path of *d* can attack the working path of *c* in switches, and the backup path of *c* on links, 0 otrw.

$a_{c,d}^{S} = 1$ If both the working and the backup path of connection *c* can be attacked by the working path of *d* in switches, 0 otherwise.

$a_{c,d} = 1$ if both the working and the backup path of connection *c* can be attacked by the working path of *d*, 0 otherwise.

$a_c = 1$ If connection *c* is attack-unprotected on links and/or switches, 0 otherwise.

Objective:

$$\text{Minimize} \sum_{c \in C} a_c \tag{4}$$

Subject to:

$$\sum_{w \in W} r_w^c = 1 \quad \forall c \in C \tag{5a}$$

$$\sum_{w \in W} \bar{r}_w^c = 1 \quad \forall c \in C \tag{5b}$$

$$\sum_{c \in C} p_e^c r_w^c + \sum_{c \in C} p_e^c r_w^c \leq 1 \quad \forall e \in E, \quad w \in W \tag{5c}$$

$$s_{v,w}^{c,d} = q_v^c \cdot r_w^c \wedge q_v^d \cdot r_w^d \quad \forall c, d \in C, \quad v \in V, \quad w \in W \tag{6a}$$

$$\bar{s}_{v,w}^{c,d} = \bar{q}_v^c \cdot \bar{r}_w^c \wedge q_v^d \cdot r_w^d \quad \forall c, d \in C, \quad v \in V, \quad w \in W \tag{6b}$$

$$s^{c,d} = \bigvee_{v \in V, w \in W} s_{v,w}^{c,d} \quad \forall c, d \in C \tag{6c}$$

$$\bar{s}^{c,d} = \bigvee_{v \in V, w \in W} \bar{s}_{v,w}^{c,d} \quad \forall c, d \in C. \tag{6d}$$

The objective of the WA phase of AA-DPP-ILP, given in Eq. (4), is to minimize the number of connections which remain unprotected from attacks (on links or inside switches) according to the assumed propagation model described in Section III-B. Eqs. (5) model the wavelength clash and continuity constraints. Eqs. (6) identify wavelength- and switch-sharing among working and backup path pairs which determine individual AGs with respect to this property. Eqs. (6a) and (6b) couple the working and the backup path of connection *c*, respectively, to any connection *d* whose working path shares a wavelength and a switch with them, while Eqs. (6c) and (6d) mark wavelength- and switch-sharing over all connections.

$$a^S_{c,d} = s^{c,d} \wedge \bar{s}^{c,d} \quad \forall c,d \in C \tag{7a}$$

$$a^{SL}_{c,d} = s^{c,d} \cdot \bar{l}_{c,d} \quad \forall c,d \in C \tag{7b}$$

$$a^{LS}_{c,d} = l_{c,d} \cdot \bar{s}^{c,d} \quad \forall c,d \in C \tag{7c}$$

$$a_{c,d} = a^S_{c,d} \vee a^L_{c,d} \vee a^{SL}_{c,d} \vee a^{LS}_{c,d} \quad \forall c,d \in C \tag{7d}$$

$$a_c = \bigvee_{d \in C} a_{c,d} \quad \forall c \in C. \tag{7e}$$

Eqs. (7) identify all possibilities in which the working and the backup path of a connection *c* can both be affected by an attacking signal carried on the working path of connection *d*, i.e., check if the working and backup paths of a connection are AG disjoint. Eq. (7a) identifies connections *c* whose working and backup paths can both be attacked by such a connection *d* in switches. Eq. (7b) identifies connections *c* whose working path can be attacked by connection *d* in switches, while its backup path can be attacked by connection *d* on links (and vice versa for Eq. (7c)). Eq. (7d) identifies connections *c* where both the working and the backup path can be attacked by a connection *d* on links and/or in switches, while Eq. (7e) denotes connection *c* as attack-unprotected if any such connection *d* exists.

C. The Complexity of AA-DPP-ILP

To get insight into the size of the proposed AA-DPP-ILP formulation, we calculate the asymptotic number of variables (*v*) and constraints (*c*) in the routing (*R*) and the WA phase (denoted as N_{v-R}, N_{c-R}, N_{v-WA} and N_{c-WA}, respectively) as a function of the number of connection demands (*C*), available wavelengths (*W*), network nodes (*V*) and edges (*E*). These relations are given as

$$N_{v-R} = 2C^2E + 3C^2 + 2CE + 2CV + C \tag{8a}$$

$$N_{c-R} = 6V^6 + 13V^4 + 2V^2 + 1 \tag{8b}$$

$$N_{v-WA} = 2C^2VW + 6C^2 + 2CW + C \tag{8c}$$

$$N_{c-WA} = 6C^2VW + 16C^2 + 3C + EW. \tag{8d}$$

If we assume an asymptotic number of connection requests of $C \approx V^2$ (i.e., a fully connected logical topology) and an asymptotic number of physical links of $E \approx V^2$ (i.e., a fully connected physical topology), then $N_{v-R} \approx V^6$, $N_{c-R} \approx V^6$, $N_{v-WA} \approx V^5W$, and $N_{c-WA} \approx V^5W$.

VI. Attack-Aware Dedicated Path Protection Heuristic (AA-DPP-H)

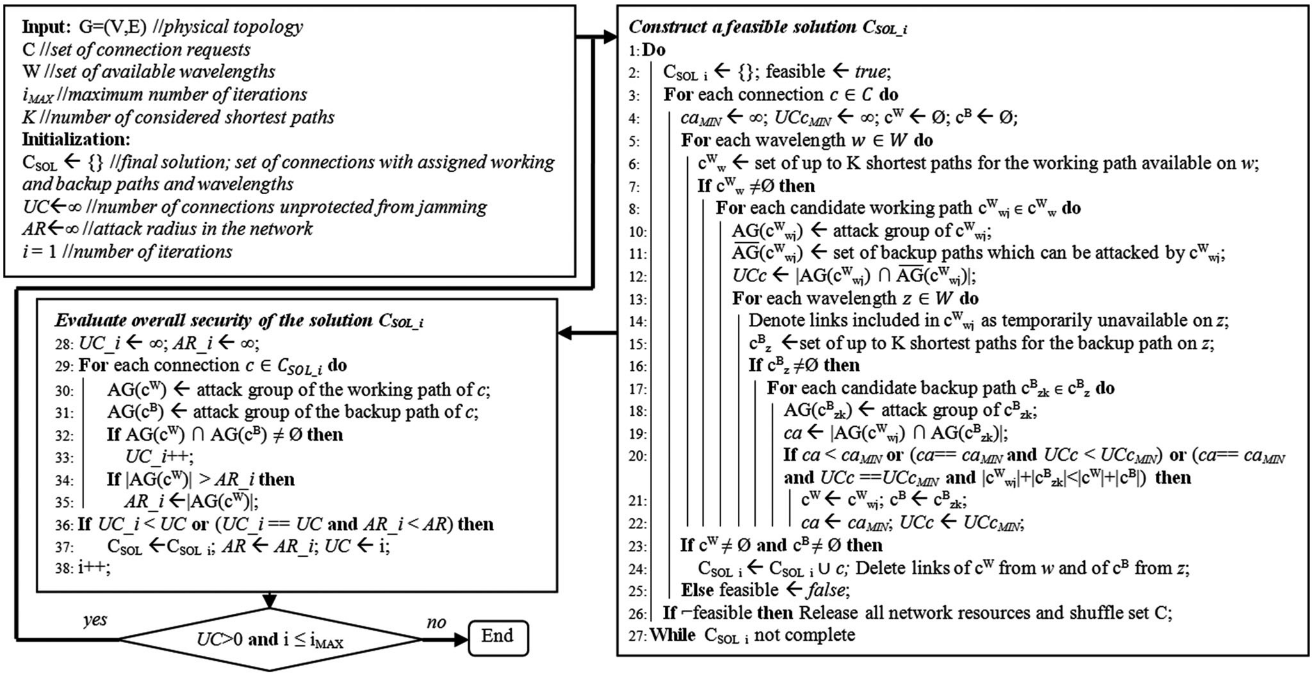
For larger problem instances, solving the two-step AA-DPP-ILP becomes computationally intractable. Therefore, we propose an iterative heuristic for attack-aware dedicated path protection, denoted as AA-DPP-H. The pseudocode of the AA-DPP-H algorithm is shown in Fig. 2. As in the ILP, the objective of AA-DPP-H is to minimize the number of attack-unprotected connections according to the propagation model described in Section III-B. In the heuristic, we also apply a secondary objective to minimize the number of working paths that can simultaneously be affected by a single attack inserted on any one of them, referred to as the attack radius (AR), as applied previously to non-survivable attack-aware RWA approaches [25]. The AR corresponds to the maximal size of the AG of any working path. For the illustrative example shown in Fig. 1(a), the AR is equal to $AR = \max\left\{|AG(c^W_1)|, |AG(c^W_2)|, |AG(c^W_3)|, |AG(c^W_4)|\right\} = \max\{2,1,2,1\} = 2$. Analogously, the AR of the DPP scheme in Fig. 1(b) is equal to 1.

The AA-DPP-H algorithm takes as input the physical topology *G* = (*V*,*E*), the set of available wavelengths *W*, the set of connection requests *C*, the maximum allowed number of iterations i_{MAX}, and the number of *K* shortest paths to be considered as candidate routes. Initially, the incumbent solution, denoted as C_{SOL}, is empty, while the number of unprotected connections (UC) and the AR are initialized to a large numerical value modeling infinity. The algorithm iteratively constructs a feasible solution C_{SOL_i} using a greedy attack-aware approach, and updates the incumbent solution if a more secure solution C_{SOL_i} is found. The algorithm ends if a solution where all connections are attack-protected is found or the maximal number of iterations is reached. Details of the construction and evaluation phases are described below.

A. Construction Phase

In order to construct a feasible solution, the algorithm processes one connection request *c* at a time while attempting to minimize *(i)* the number of potential common attackers (denoted as *ca* in the pseudocode) shared among its working path c^W and backup path c^B; and *(ii)* the number of existing connections (denoted as UC_c) whose AG-disjointedness is violated by c^W. We use a layered graph approach where a copy of the physical topology is made for each wavelength, and occupied wavelength-links in the current partial solution are deleted from their corresponding layers when searching for paths for subsequent requests. For each connection request, the approach first searches for up to *K* available shortest path candidates for c^W on each available wavelength (line 6). For each c^W candidate, denoted as c^W_{wj}, the corresponding AG is identified (line 10), as well as the set of existing backup paths which can be attacked by c^W_{wj}, denoted as $\overline{AG}$ (line 11). The latter is needed to calculate the value of UC_c as the number of elements in the intersection of sets AG and $\overline{AG}$ (line 12).

The algorithm proceeds by finding a set of up to *K* shortest path candidates for c^B on each of the available wavelengths, which are link-disjoint with c^W_{wj} (line 15). After calculating the AG of each c^B candidate, denoted as c^B_{zk} (line 18), the number of common potential attackers on c^W_{wj} and c^B_{zk} is identified (line 19) and the pair of candidate paths with the minimum value of *ca* is selected as the solution for c^W and c^B (line 20). If the value of *ca* is the same for two candidate path pairs, the pair yielding lower UC_c value is selected. The combined path length of c^W_{wj} and c^B_{zk} is used as a second tie-breaking rule to prioritize shorter paths (line 20). Finally, if c^W and c^B are found, they are added to



```
Input: G=(V,E) //physical topology
C //set of connection requests
W //set of available wavelengths
$i_{MAX}$ //maximum number of iterations
K //number of considered shortest paths
Initialization:
$C_{SOL} \leftarrow \{\}$ //final solution; set of connections with assigned working and backup paths and wavelengths
$UC \leftarrow \infty$ //number of connections unprotected from jamming
$AR \leftarrow \infty$ //attack radius in the network
$i = 1$ //number of iterations
```

```
Construct a feasible solution $C_{SOL\_i}$
1: Do
2:   $C_{SOL\ i} \leftarrow \{\}$; feasible $\leftarrow$ true;
3:   For each connection $c \in C$ do
4:     $ca_{MIN} \leftarrow \infty$; $UCc_{MIN} \leftarrow \infty$; $c^W \leftarrow \emptyset$; $c^B \leftarrow \emptyset$;
5:     For each wavelength $w \in W$ do
6:       $c^W_w \leftarrow$ set of up to K shortest paths for the working path available on $w$;
7:       If $c^W_w \neq \emptyset$ then
8:         For each candidate working path $c^W_{wj} \in c^W_w$ do
10:          $AG(c^W_{wj}) \leftarrow$ attack group of $c^W_{wj}$;
11:          $\overline{AG}(c^W_{wj}) \leftarrow$ set of backup paths which can be attacked by $c^W_{wj}$;
12:          $UCc \leftarrow |AG(c^W_{wj}) \cap \overline{AG}(c^W_{wj})|$;
13:          For each wavelength $z \in W$ do
14:            Denote links included in $c^W_{wj}$ as temporarily unavailable on $z$;
15:            $c^B_z \leftarrow$ set of up to K shortest paths for the backup path on $z$;
16:            If $c^B_z \neq \emptyset$ then
17:              For each candidate backup path $c^B_{zk} \in c^B_z$ do
18:                $AG(c^B_{zk}) \leftarrow$ attack group of $c^B_{zk}$;
19:                $ca \leftarrow |AG(c^W_{wj}) \cap AG(c^B_{zk})|$;
20:                If $ca < ca_{MIN}$ or ($ca == ca_{MIN}$ and $UCc < UCc_{MIN}$) or ($ca == ca_{MIN}$
                   and $UCc == UCc_{MIN}$ and $|c^W_{wj}|+|c^B_{zk}|<|c^W|+|c^B|$) then
21:                  $c^W \leftarrow c^W_{wj}$; $c^B \leftarrow c^B_{zk}$;
22:                  $ca \leftarrow ca_{MIN}$; $UCc \leftarrow UCc_{MIN}$;
23:    If $c^W \neq \emptyset$ and $c^B \neq \emptyset$ then
24:      $C_{SOL\ i} \leftarrow C_{SOL\ i} \cup c$; Delete links of $c^W$ from $w$ and of $c^B$ from $z$;
25:    Else feasible $\leftarrow$ false;
26:  If $\neg$feasible then Release all network resources and shuffle set C;
27: While $C_{SOL\ i}$ not complete
```

```
Evaluate overall security of the solution $C_{SOL\_i}$
28: $UC\_i \leftarrow \infty$; $AR\_i \leftarrow \infty$;
29: For each connection $c \in C_{SOL\_i}$ do
30:     $AG(c^W) \leftarrow$ attack group of the working path of $c$;
31:     $AG(c^B) \leftarrow$ attack group of the backup path of $c$;
32:     If $AG(c^W) \cap AG(c^B) \neq \emptyset$ then
33:        $UC\_i$++;
34:     If $|AG(c^W)| > AR\_i$ then
35:        $AR\_i \leftarrow |AG(c^W)|$;
36: If $UC\_i < UC$ or ($UC\_i == UC$ and $AR\_i < AR$) then
37:     $C_{SOL} \leftarrow C_{SOL\ i}$; $AR \leftarrow AR\_i$; $UC \leftarrow$ i;
38: i++;
```

Fig. 2. The pseudocode of the AA-DPP-H algorithm.

C_{SOL_i} and their links are marked as unavailable on the selected wavelengths *w* and *z* (line 24). If no feasible solution is found after checking all wavelengths, all resources are released and set *C* is shuffled randomly (line 26). The procedure is repeated until a feasible solution C_{SOL_i} is found.

B. Evaluation Phase

In the evaluation phase, the feasible solution found in the greedy construction phase is evaluated with respect to the previously described optimization criteria (i.e., number of attack-unprotected connection and the AR). The algorithm calculates the AGs for all working and backup paths (lines 30–31), identifies attack-unprotected connections (lines 32–33) and calculates the network AR (lines 34–35). If the current solution $\mathrm{C}_{\mathrm{SOL}_i}$ has fewer attack-unprotected connections UC_i, or the same UC_i but a lower AR (line 36), the incumbent solution is updated (line 37).

C. Computational Complexity

To find the *K*-shortest working and backup paths for each connection, Yen's *K* shortest path algorithm [31] (using a regular linked list implementation of Dijkstra's algorithm as a subroutine) is used, whose complexity is $O(KV^3)$. To calculate the AG of a candidate path c^W or c^B, all other working paths need to be checked for link- and switch-sharing, with complexities of $O(EC)$ (i.e., $O(V^2C)$), and $O(VC)$, respectively. To construct a feasible RWA solution, the *K* shortest working and backup paths on all *W* available wavelengths for each of the *C* connections are examined. Therefore, the overall complexity of the construction phase of AA-DPP-H is $O(C^2V^2W + CV^3WK)$. The evaluation phase calculates the AGs for all connections in the complete solution, yielding $O(V^2C^2)$ complexity.

VII. Numerical Results

A. Benchmarking Algorithms

To evaluate whether the proposed approaches can achieve significant attack-protection while using the same amount of network resources as standard non-attack-aware DPP, the algorithms are compared with two benchmarking link-disjoint DPP approaches, denoted as DPP-ILP and DPP-H, whose objectives are to minimize the lengths of the established paths and/or the number of wavelengths used. The resource consumption obtained by these algorithms is then used as input to constrain their attack-aware counterparts.

DPP-ILP is a two-step ILP formulation, analogous to AA-DPP-ILP, but instead of minimizing the number of attack-unprotected connections, the routing phase aims at minimizing the total path length used, while the WA phase minimizes the number of wavelengths used. The formulation is derived from formulation AA-DPP-ILP as follows. The link/switch-sharing and attack-reach variables are dropped in both phases, as well as input parameters *H* and *W*. The routing sub-problem of DPP-ILP is then solved with the objective of minimizing the total length of the established paths, equal to the left-hand side of Eq. (2d), and by considering only constraints Eq. (2a)–(2c) from Section V-A.

The WA sub-problem of DPP-ILP is aimed at minimizing the number of used wavelengths. Thus, the formulation employs the WA variables from Section V-B as well as an additional binary variable y_w indicating whether wavelength *w* is used in the final solution. The objective is then to minimize the total number

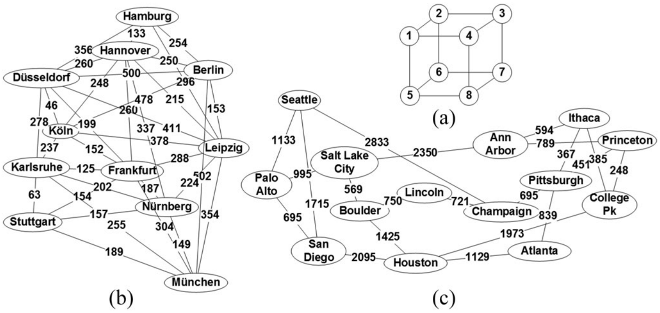


Fig. 3. The reference networks used in the simulations: the (a) 8-node, (b) GER, and (c) NSF network.

of wavelengths used, i.e., $\sum_{w \in W} y_w$. The WA phase is solved by applying the constraints described in Equations (5), as well as the following two constraints which indicate the wavelengths used:

$$r_w^c \leq y_w \quad \forall c \in C, \quad w \in W \tag{9a}$$

$$\bar{r}_w^c \leq y_w \quad \forall c \in C, \quad w \in W. \tag{9b}$$

DPP-H is a heuristic approach similar to the dynamic DPP algorithm from [32], which calculates the routes of the working and protection path sequentially by applying a shortest path algorithm assuming full wavelength-conversion. To be in line with the problem considered in this paper, the approach is modified to assume a static environment with no wavelength-conversion. Like AA-DPP-H, DPP-H is run as an iterative process with different connection request orderings, but without applying attack-awareness. In every iteration, it searches for a working and a backup path of all requests with the objective of minimizing the number of used wavelengths. The working and backup path of each connection are assigned the shortest path on the first available wavelength. The algorithm begins each iteration by using just one wavelength and adds a new one only when the working or the backup path cannot fit on any of the previously used wavelengths. At the end of the iteration, the incumbent solution is updated if the current solution uses fewer wavelengths, or if it uses the same number of wavelengths but establishes a shorter total path length.

B. Implementation Details and Experimental Setup

The two-step ILP formulations AA-DPP-ILP and DPP-ILP were solved using CPLEX v12.4, while iterative heuristics AA-DPP-H and DPP-H were implemented as a software tool in C++. All algorithms were run on an HP workstation equipped with 8 Intel Xeon 2.67 GHz processors and 16 GB RAM.

Three networks were considered, shown in Fig. 3. Due to the complexity of the two-step attack-aware ILP formulation, AA-DPP-ILP and DPP-ILP were only tested for the network shown in Fig. 3(a) with 8 nodes and 12 bi-directional links, each representing two directed links. The AA-DPP-H and DPP-H heuristics were evaluated on the 8-node network, as well as on the reference networks shown in Fig. 3(b) and (c) corresponding to the nation-wide network of Germany (GER; 11 nodes, 34 bidirectional links) and the US NSF network (14 nodes, 21 bidirectional link), respectively.

TABLE I
THE AVERAGE NUMBER OF CONNECTION REQUESTS IN THE GER AND NSF TEST CASES

Network (|*V*|,|*E*|)	*1*	*2*	*3*	*4*	*5*
GER (11,34)	100.4	125.0	150.0	174.8	200.4
NSF (14,21)	150.0	175.2	200.6	224.6	250.0

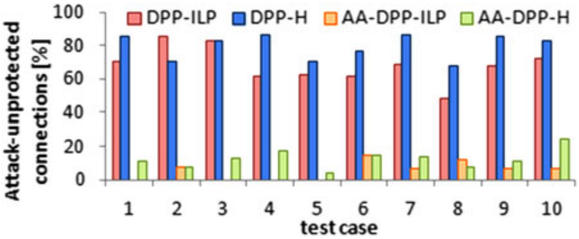


Fig. 4. The percentage of attack-unprotected connections obtained by DPP-ILP, DPP-H, AA-DPP-ILP and AA-DPP-H for the 8-node network.

Sets of connection requests were generated as follows. For the 8-node network, 1 to 6 random outgoing connection requests were assigned to each node representing long-term traffic flows. Ten such sets were created, ranging in size from 23 to 34 requests, with an average logical degree of 3.5.

For the GER and NSF networks, a multilayer approach was used to generate the connection requests. First, five traffic matrices were created for each network using the method from [33], which generates long-term traffic flow estimates between node pairs based on the populations and distances of cities corresponding to the network nodes. The generated traffic was proportional to node populations (taken from [34]) and inversely proportional to their distances, with a randomness factor set to 25% to create random fluctuations around the deterministic values. Then, assuming a connection capacity of 100 Gb/s, as many connection requests were established per node pair as needed to carry all of the offered traffic in a single logical hop, with no constraints on the number of transceivers. To do so, the generated traffic matrices were normalized to five different values in order to model different traffic loads, yielding average values of 100 to 250 connections for each test case, as shown in Table I.

To evaluate the attack-protection that can be obtained with AA-DPP-ILP while using the same amount of resources as DPP-ILP, the path length and the number of wavelengths used in the solutions obtained by DPP-ILP were fed as parameters *H* and *W*, respectively, in AA-DPP-ILP. Analogously, the number of available wavelengths in AA-DPP-H was set to the number of wavelengths obtained by DPP-H. Both iterative heuristics were run for 100 iterations and the value of parameter *K* in AA-DPP-H was set to 2, determined experimentally. Feasible solutions were found in all cases with no connection blocking. For each test case run, the length of the established working and backup paths, the number of used wavelengths, the number of attack-unprotected connections and the running times of the algorithms were recorded. The results are discussed in the next section.

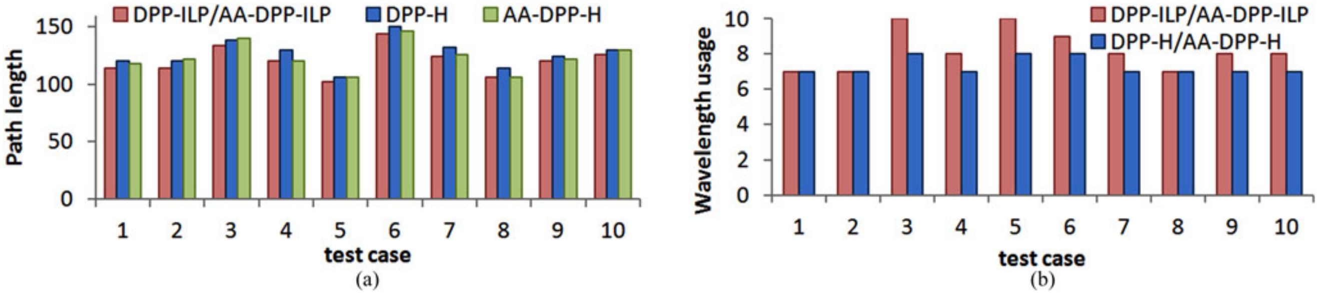


Fig. 5. (a) The total length of the established working and backup paths and (b) number of used wavelengths obtained by the AA-DPP and DPP ILPs and heuristics for the 8-node network.

C. Simulation Results

Figs. 4 and 5 show the performance of all the implemented algorithms for the 8-node test cases. Fig. 4 shows the percentage of attack-unprotected connections in the solutions obtained by each approach. The attack-aware approaches, AA-DPP-ILP and AA-DPP-H, obtain solutions in which on average only 5.5% and 12.5% of connections remain unprotected from attacks, respectively. In comparison, the attack-unaware approaches obtain solutions with an average of 68.2% (DPP-ILP) and 79.5% (DPP-H) of connections attack-unprotected. In general, AA-DPP-ILP performs best with respect to attack-protection, finding solutions with zero attack-unprotected connections in four of the ten test cases. AA-DPP-H performs somewhat worse than AA-DPP-ILP in all but one test case (recall that AA-DPP-ILP is a two-step ILP which does not necessarily find a globally optimal solution), but still significantly outperforms the non-attack-aware algorithms in all cases.

Fig. 5 shows resource consumption of the proposed approaches in terms of the total length of the established paths (see Fig. 5(a)) and the number of wavelengths used (see Fig. 5(b)). The routing phase of AA-DPP-ILP takes as input the total hop count obtained by the routing phase of DPP-ILP (whose objective is to minimize hop count), so both formulations establish solutions with equal hops and, thus, are shown together in the figure. The two-step formulations obtained slightly better results than the iterative heuristics, finding on average 2.6% shorter paths than AA-DPP-H, which in turn found solutions 2.2% shorter than DPP-H. Regarding wavelength usage, recall that the number of wavelengths used in the solutions obtained by DPP-ILP and DPP-H are fed as input parameters to their attack-aware counterparts. Therefore, AA-DPP-ILP and AA-DPP-H use the same number of wavelengths as DPP-ILP and DPP-H, respectively, and are, thus, grouped together in Fig. 5(b). Due to more restrictive routing, the two-step formulations obtain solutions using on average 12.3% more wavelengths than the iterative heuristics. In sum, we can see that the attack-aware approaches obtain enhanced solutions compared to their non-attack-aware counterparts for the 8-node network, while the choice of applying the two-step ILP or iterative heuristic depends on whether attack-protection or wavelength usage are the priority.

The degree of attack-protection in the solutions obtained by the iterative heuristics for the larger network instances is shown in Figs. 6 and 7. Fig. 6 shows the percentage of connections which remain attack-unprotected, while Fig. 7 presents the resulting network AR after running the DPP-H and AA-DPP-H algorithms. The shown values are averaged over five different traffic instances for each of the five test cases. Compared to DPP-H, AA-DPP-H obtains solutions with a significantly lower number of connections left attack-unprotected and an overall lower AR. Specifically, for the GER network (see Fig. 6(a)), AA-DPP-H leaves on average only 11% of connections unprotected (averaged over all test cases), while DPP-H leaves 83% of connections unprotected. For the NSF network (see Fig. 6(b)), the average number of UCs established by AA-DPP-H is 2% compared to 80% left unprotected by DPP-H. Furthermore, the AR obtained by AA-DPP-H is 19% and 23% lower than that of DPP-H for the GER and NSF network, respectively, as shown in Fig. 7.

Table II and Fig. 8 illustrate the resource usage of the solution obtained by iterative approaches. Note that both algorithms use the same number of wavelengths (shown in Table II), since the value obtained by DPP-H is fed as an input parameter to AA-DPP-H. The average path lengths, however, differ somewhat, particularly for the NSF network, as shown in Fig. 8. The total paths (working and backup) established by AA-DPP-H (averaged over the five test scenarios) for the GER network use the same number of hops as those set up by DPP-H (within the order of magnitude of 10^{-2}), while using the same number of wavelengths. For the NSF network, the paths set up by AA-DPP-H traverse 6% fewer hops than those established by DPP-H. This could be explained by the fact that shorter paths have a smaller number of potential attacking points (i.e., links and nodes) which generally helps reduce the number of connections affected by propagating attacks making them more favorable to AA-DPP-H. When the actual obtained path length (in km) is analyzed instead of the hop count, the average difference between DPP-H and AA-DPP-H for each test case was below 2% for both networks. Based on these results, we can conclude that the proposed attack-aware heuristic AA-DPP-H was able to significantly improve attack protection with respect to non-attack-aware approach DPP-H with no adverse effects on resource usage.

Regarding the execution times of the proposed approaches, as expected AA-DPP-ILP ran the longest, averaging 9 min per test case for the 8-node network, while DPP-ILP ran for 3 min on average. For the same test cases, AA-DPP-H ran for

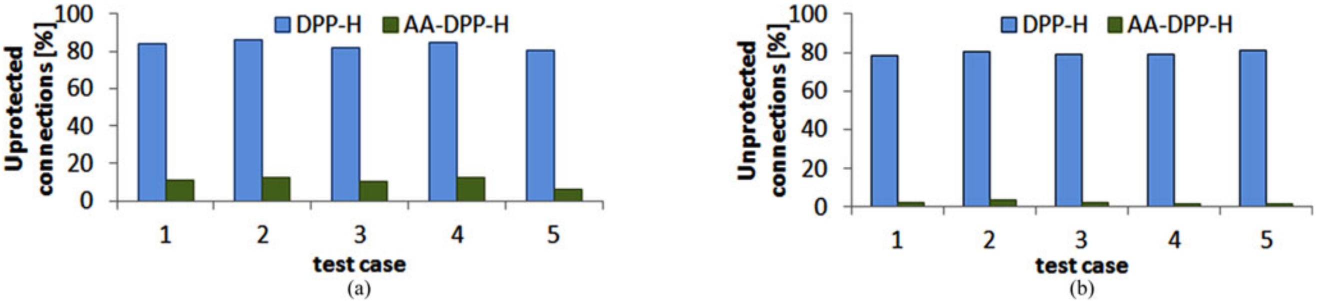


Fig. 6. The percentage of attack-unprotected connections obtained by DPP-H and AA-DPP-H for the (a) GER and (b) NSF network.

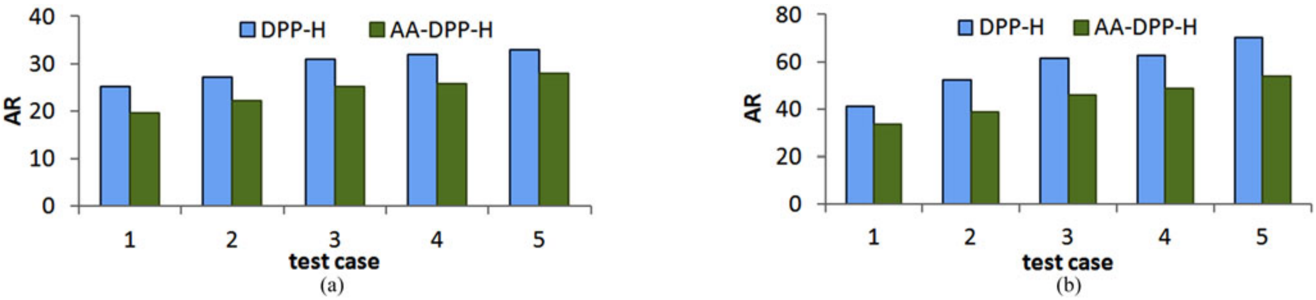


Fig. 7. The AR obtained by DPP-H and AA-DPP-H for the (a) GER and (b) NSF network.

TABLE II
THE AVERAGE NUMBER OF WAVELENGTHS USED IN THE GER AND NSF TEST SCENARIOS

Network	*1*	*2*	*3*	*4*	*5*
GER	7.0	8.2	9.8	11.0	12.6
NSF	28.2	32.8	37.4	40.8	44.8

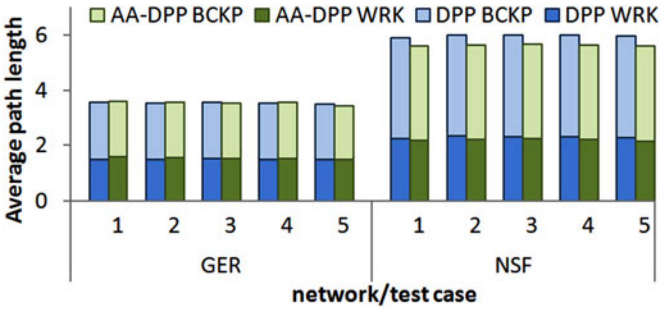


Fig. 8. The average hop count in the paths established by DPP-H and AA-DPP-H for the GER and NSF network.

TABLE III
THE AVERAGE RUNNING TIMES PER ITERATION AND THE AVERAGE NUMBER OF ITERATIONS TO THE BEST SOLUTION OVER ALL GER AND NSF TEST SCENARIOS

	Running time/iteration [s]		*Iterations to best solution*	
Network	*DPP-H*	*AA-DPP-H*	*DPP-H*	*AA-DPP-H*
GER	0.2	46.5	40.1	39.4
NSF	1.3	3106.1	52.7	49.1

approximately 1.2 s per iteration, while the simpler non-attack-aware DPP-H heuristic ran for under a fraction of a second. The average running times per iteration and the number of iterations to the best obtained solution for the iterative heuristics on the larger networks are shown in Table III. The longer duration of a single iteration of AA-DPP-H compared to DPP-H is due to the fact that many solutions are checked until a feasible one is found, and attacking relations must be calculated for each candidate path pair. This is especially true for the NSF network test cases where finding feasible solutions is more challenging due to lower connectivity and a higher number of connection requests considered. Although AA-DPP-H runs longer than DPP-H, recall that we are considering a static planning problem for which all of the shown execution times are acceptable. Furthermore, AA-DPP-H is an iterative process where fewer iterations could be run to achieve a desired tradeoff between execution time and solution quality. As an example, the percentage of UCs in the solutions obtained by running the algorithm for only ten iterations ranged between 10% and 14.3% for the GER network test cases and between 2.4% and 5% for the NSF network, which still significantly outperforms DPP-H.

VIII. CONCLUSION

This paper considers AA-DPP in optical networks. While standard protection schemes typically protect from single or multiple component failures by establishing link/node disjoint paths, such approaches may not be entirely effective in the presence of propagating physical-layer attacks. To deal with this issue, we identify potential attacking relations between connections based on specific attack propagation characteristics, forming so-called AG, and propose to establish connections whose working and the backup paths are AG-disjoint to ensure that a single attack could not affect both of them simultaneously. Since providing full attack-protection may not be economically viable due to the large amount of resources required, we propose to add attack-awareness to standard survivability approaches to reduce the number of attack-unprotected connections in a resource-efficient manner. In this paper, we focus on in-band high-power jamming attacks, and propose a two-step ILP formulation and iterative heuristic to solve the AA-DPP problem. Simulation results indicate that proposed approaches can obtain solutions with significantly enhanced attack protection while using the same amount of network resources as conventional dedicated path protection schemes. Similar approaches could be developed to include additional physical-layer attacks by applying extended attack propagation models and their corresponding AGs.

References

[1] K. 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 enhancements," *IEEE/OSA J. Lightw. Technol.*, vol. 29, no. 21, pp. 3210–3222, Nov. 2011.

[2] 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.

[3] R. Rejeb, M. S. Leeson, C. Mas Machuca, and I. Tomkos, "Control and management issues in all-optical networks," *J. Netw.*, vol. 5, no. 2, pp. 132–139, Feb. 2010.

[4] 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. 085002.1–085002.3, Aug. 2011.

[5] M. Furdek, N. Skorin-Kapov, S. Zsigmond, and L. Wosinska, "Vulnerabilities and security issues in optical networks," in *Proc. Int. Conf. Transp. Opt. Netw.*, 2014, Paper Tu.D3.5, pp. 1–4.

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

[7] Alcatel Lucent. (1830). *Photonic Service Switch* [Online]. Available: http://www.alcatel-lucent.com/products/1830-photonic-service-switch

[8] ADVA. *ConnectGuard FSP 3000 Optical Network Encryption* [Online]. Available: http://www.advaoptical.com/en/resources/data-sheets/fsp-3000-optical-network-encryption-download.aspx?PageType=WhitePaper&ItemID={5FDB7735-4222-49EA-9B08-6AA66C8FB5E5}

[9] C. Mas, I. Tomkos, and O.K. Tonguz, "Failure location algorithm for transparent optical networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 8, pp. 1508–1519, Aug. 2005.

[10] N. K. Singhal and B. Mukherjee, "Protecting multicast sessions in WDM optical mesh networks," *IEEE/OSA J. Lightw. Technol.*, vol. 21, no. 4, pp. 884–892, Apr. 2003.

[11] O. Gerstel, "Multi-layer survivability," presented at the 18th Int. Conf. Optical Network Design and Modeling, Stockholm, Sweden, May 19–22, 2014.

[12] P. Babarczi, G. Biczók, H. Øverby, J. Tapolcai, and P. Soproni, "Realization strategies of dedicated path protection: A bandwidth cost perspective," *Comput. Netw.*, vol. 59, no. 9, pp. 1974–1990, Jun. 2013.

[13] M. Furdek and N. Skorin-Kapov, "Attack-survivable routing and wavelength assignment for high-power jamming," in *Proc. 17th Int. Conf. Opt. Netw. Des. Model.*, 2013, pp. 70–75.

[14] B. Mukherjee, *Optical WDM Networks*. New York, NY, USA: Springer-Verlag, 2006.

[15] J. M. Simmons, *Optical Network Design and Planning*. New York, NY, USA: Springer-Verlag, 2014.

[16] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," *IEEE/OSA J. Lightw. Technol.*, vol. 21, no. 4, pp. 870–883, Apr. 2003.

[17] S. Chamberland, D. Oulaï Khyda, and S. Pierre, "Joint routing and wavelength assignment in wavelength division multiplexing networks for permanent and reliable paths," *Comput. Oper. Res.*, vol. 32, no. 5, pp. 1073–1087, May 2005.

[18] R. Andersen, F. Chung, A. Sen, and G. Xue, "On disjoint path pairs with wavelength continuity constraint in WDM networks," in *Proc. INFOCOM*, 2004, pp. 524–535.

[19] P.-H. Ho, "State-of-the-art progress in developing survivable routing schemes in mesh WDM networks," *IEEE Commun. Surveys Tuts.*, vol. 6, no. 4, pp. 2–16, Oct. 2004.

[20] X. Saho, Y. Bai, X. Cheng, Y.-K. Yea, and L. Heng Ngoh, "Best effort SRLG failure protection for optical WDM networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 3, no. 9, pp. 739–749, Sep. 2011.

[21] J. Ahmed, C. Cavdar, P. Monti, and L. Wosinska, "Hybrid survivability schemes achieving high connection availability with a reduced amount of backup resources," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 5, no. 10, pp. A152–A161, Oct. 2013.

[22] G. Ellinas, E. Bouillet, R. Ramamurthy, J. Labourdette, S. Chaudhuri, and K. Bala, "Routing and restoration architectures in mesh optical networks," *Opt. Netw. Mag.*, vol. 4, no. 1, pp. 91–106, Jan. 2003.

[23] M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee, "Disaster survivability in optical communication networks," *Comput. Commun.*, vol. 36, no. 6, pp. 630–644, Mar. 2013.

[24] N. Garg and R. Simha, "Computing optically disjoint paths for survivable all-optical networks," in *Proc. Opt. Fiber Commun. Conf.*, 2003, pp. 205–207.

[25] 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.

[26] M. Furdek, N. Skorin-Kapov, and M. Grbac, "Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 2, no. 11, pp. 1000–1009, Nov. 2010.

[27] N. Skorin-Kapov, M. Furdek, R. Aparicio-Pardo, and P. Pavón-Mariño, "Wavelength assignment for reducing in-band crosstalk attack propagation in optical networks: ILP formulations and heuristic algorithms," *Eur. J. Oper. Res.*, vol. 222, no. 3, pp. 418–429, Nov. 2012.

[28] M. Furdek, N. Skorin-Kapov, and A. Tzanakaki, "Survivable routing and wavelength assignment considering high-powered jamming attacks," in *Proc. Asia Commun. Photon. Conf.*, 2011, pp. 1–7.

[29] M. Furdek, N. Skorin-Kapov, and L. Wosinska, "Shared path protection under the risk of high-power jamming," in *Proc. 19th Eur. Conf. Netw. Opt. Commun.*, 2014, pp. 23–28.

[30] T. Deng and S. S. Subramaniam, "Covert low-power QoS attack in all-optical wavelength-routed networks," in *Proc. GLOBECOM*, 2004, pp. 1948–1952.

[31] E. Q. V. Martins and M. M. B. Pascoal, "A new implementation of Yen's ranking loopless paths algorithm," *4OR, Quart. J. Oper. Res.*, vol. 1, no. 2, pp. 121–133, 2003.

[32] Y. Li, W. Ni, H. Zhang, Y. Li, and X- Zheng, "Availability analytical model for permanent dedicated path protection in WDM networks," *IEEE Commun. Lett.*, vol. 16, no. 1, pp. 95–97, Jan. 2012.

[33] R. S. Cahn, *Wide Area Network Design. Concepts and Tools for Optimization*. San Mateo, CA, USA: Morgan Kaufmann, 1998.

[34] T. Brinkoff. (2015). City population [Online]. Available: www.citypopulation.de

Marija Furdek received the Dipl.-Ing. and Ph.D. degrees in telecommunications from the Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, Croatia, in 2008 and 2012, respectively.

She is working as a Researcher at the Optical Networks Lab, KTH Royal Institute of Technology, Kista, Sweden, where she completed a postdoctoral fellowship in 2013/2014. Prior to joining KTH, she was with the Department of Telecommunications, Faculty of Electrical Engineering and Computing, University of Zagreb as a Research and Teaching Assistant from 2009 to 2012 and as a Senior Research and Teaching Assistant from 2012 to 2014. She has coauthored more than 30 papers in international journals and conferences. Her research interests include planning of optical networks and optical node architecture, physical-layer security, network survivability, reliability analysis, and optimization techniques.

Dr. Furdek received the 2013 Fabio Neri Best Paper Award of the *Optical Switching and Networking Journal*. She has served as a Reviewer for many international journals and conferences, including the IEEE/OSA JOURNAL OF LIGHTWAVE TECHNOLOGY, the IEEE/OSA JOURNAL OF OPTICAL COMMUNICATIONS AND NETWORKING, OSA *Optics Letters*, IEEE ICC, IEEE HPSR, IEEE Globecom, etc. She is a Member of the OSA. She is currently serving as a General Cochair of the Photonic Networks and Devices conference, a part of the OSA Advanced Photonics Congress.

Nina Skorin-Kapov received the Dipl.-Ing. and Ph.D. degrees in telecommunications from the University of Zagreb, Zagreb, Croatia, in 2003 and 2006, respectively.

In 2006/2007, she completed a Postdoctoral Fellowship with Télécom ParisTech (formerly Ecole Nationale Superieure des Telecommunications, ENST), Paris, France. In 2008, she joined the Department of Telecommunications with the Faculty of Electrical Engineering and Computing, University of Zagreb as an Assistant Professor, and was promoted to an Associate Professor in 2012. Since 2013 she has been at the University Centre of Defense, San Javier Air Force Base, Santiago de la Ribera, Murcia, Spain, associated to the Technical University of Cartagena. She has coauthored more than 50 papers in international conferences and journals. Her main research interests include optimization and planning of communication networks, particularly in wide-area optical networks.

Dr. Skorin-Kapov received the 2013 Fabio Neri Best Paper Award of the *Optical Switching and Networking Journal*. She has served on several conference committees such as IEEE Globecom and IEEE ICC, and is currently a Technical Cochair of ONDM 2016. From 2011–2015, she served on the Editorial Board of the CIT *Journal of Computing and Information Technology*.

Lena Wosinska received the Ph.D. degree in photonics and Docent degree in optical networking from the KTH Royal Institute of Technology, Kista, Sweden, where she is currently a Full Professor in Telecommunication at the School of Information and Communication Technology (ICT).

She is the Founder and the Leader of the Optical Networks Lab (ONLab). She has been working in several EU projects and coordinating a number of national and international research projects. Her research interests include fiber access and 5G transport networks, energy efficient optical networks, photonics in switching, optical network control, reliability and survivability, and optical datacenter networks.

Prof. Wosinska has been involved in many professional activities including the Guest Editorship of IEEE, OSA, Elsevier, and Springer journals, serving as the General Chair and Cochair of several IEEE, OSA, and SPIE conferences and workshops, serving in TPC of many conferences, as well as being a Reviewer for scientific journals and project proposals. During 2007–2009, she was an Associate Editor of the OSA *Journal of Optical Networking*, and during 2009–2013, she was an Associate Editor of the IEEE/OSA JOURNAL OF OPTICAL COMMUNICATIONS AND NETWORKING. She is currently serving on the Editorial Board of the Springer *Photonic Networks Communication Journal*.