Wavelength Assignment for Reducing In-band Crosstalk Attack Propagation in Optical Networks: ILP Formulations and Heuristic Algorithms

Nina Skorin-Kapov[a], Marija Furdek[a*], Ramon Aparicio Pardo[b] and Pablo Pavón Mariño[b]

[a]University of Zagreb, Faculty of Electrical Engineering and Computing, Dept. of Telecommunications

Unska 3, HR-10000 Zagreb, Croatia

E-mail: {nina.skorin-kapov, marija.furdek}@fer.hr

[b]Technical University of Cartagena, Dept. of Information Technologies and Communications

Pza. Hospital 1, 30202 Cartagena, Spain

E-mail:{ramon.aparicio, pablo.pavon}@upct.es

Abstract

Today's Transparent Optical Networks (TONs) are highly vulnerable to various physical-layer attacks, such as high-power jamming, which can cause severe service disruption or even service denial. The transparency of TONs enables certain attacks to propagate through the network, not only increasing their damage proportions, but also making source identification and attack localization more difficult. High-power jamming attacks causing in-band crosstalk in switches are amongst the most malicious of such attacks. In this paper, we propose a wavelength assignment scheme to reduce their damage assuming limited attack propagation capabilities. This complements our previous work in [Furdek et al., 2010] where we investigated infinite jamming attack propagation to find an upper bound on the network vulnerability to such attacks. Here, we consider a more realistic scenario where crosstalk attacks can spread only via primary and/or secondary attackers and define new objective criteria for wavelength assignment, called the PAR (Primary Attack Radius) and SAR (Secondary Attack Radius), accordingly. We formulate the problem variants as integer linear programs (ILPs) with the objectives of minimizing the PAR and SAR values. Due to the intractability of the ILP formulations, for larger instances we propose GRASP (Greedy Randomized Adaptive Search Procedure) heuristic algorithms to find suboptimal solutions in reasonable time. Results show that these approaches can obtain solutions using the same number of wavelengths as classical wavelength assignment, while significantly reducing jamming attack damage proportions in optical networks.

Keywords: OR in telecommunications, integer linear programming, optical networks, physical-layer attacks, wavelength assignment, Greedy Randomized Adaptive Search Procedure (GRASP)

*Corresponding author

1. Introduction

Optical networking is evolving towards high-capacity all-optical (i.e., transparent) networks based on Wavelength Division Multiplexing (WDM). In transparent WDM networks, all-optical connections, called lightpaths, are established between pairs of nodes creating a virtual topology over the physical infrastructure. These connections can traverse multiple links in the physical topology and yet transmission via a lightpath is entirely in the optical domain.

In order to establish a given set of lightpaths, it is necessary to find for them corresponding routes in the physical topology and assign wavelengths to them subject to certain constraints. This is known as the Routing and Wavelength Assignment (RWA) problem. Sub-wavelength traffic flows are then routed over the virtual topology and combined on each lightpath using traffic grooming approaches. The two main constraints in the RWA problem are the wavelength clash constraint, which prohibits assigning the same wavelength to lightpaths which share a common physical link, and the wavelength continuity constraint, which ensures that the same wavelength must be used along the entire physical path of a lightpath.

Solving the RWA problem has been shown to be NP-complete [5]. ILP formulations for RWA can be found in [16][18], along with a wide variety of heuristics for larger network instances in [16][17][22] and references therein. Due to its complexity, RWA is often decomposed into two sub-problems: Routing (R) and Wavelength Assignment (WA), solved subsequently with various optimality criteria. Routing objectives include minimizing the average packet hop distance and congestion [1][11]. For WA, the most common objective criterion is minimizing the number of wavelengths [16]. Note that Wavelength Assignment has been shown to be equivalent to the graph coloring problem [5], which is NP-hard. An exact Branch-and-Price algorithm and heuristics for the graph coloring problem can be found in [13].

The inherent transparency of such lightpath-based networks allows for new physical-layer attack strategies exploiting component vulnerabilities and the limitations of optical monitoring techniques. Among the identified attack strategies, high-power jamming to exploit in-band crosstalk inside optical switches has the highest damage capabilities [25]. In-band crosstalk arises due to interference among signals on the same wavelength, or on wavelengths sufficiently close to fall within each other's passband. The basic source of in-band crosstalk is non-ideal port isolation of optical (de)multiplexers and switches, the key building blocks of optical nodes. Firstly, due to non-ideal demultiplexing, a small portion of each signal leaks onto unintended

demultiplexer ports. When these channels are multiplexed back onto a common output fiber, the leaked portions of each wavelength signal will be recombined with their original signals. Because of this, signals on each wavelength will have crosstalk originating from their very own components carrying the same information, but suffering from different delays and phase shifts caused by different propagation paths inside the optical node. Apart from the demultiplexing/multiplexing stages, a second important source of in-band crosstalk is located at switching fabric itself. Imperfect isolation of switch ports can also introduce significant leakage and interference of signals on the same wavelength.

An attack exploiting in-band crosstalk effects can be achieved by injecting a high-power jamming signal (e.g., 20 dB higher than the other channels) on a legitimate lightpath, called in-band jamming, which can cause significant leakage inside the switches between lightpaths on the same wavelength as the attacker [14]. Deleterious effects of an attacking signal include severe BER deterioration, decrease of the signal-to-noise ratio and eye diagram closure of the affected signals [20]. Furthermore, this crosstalk can be so high that the affected signals may receive enough energy to acquire attacking capabilities themselves. Hence, such attacks can potentially propagate through the network, affecting links and nodes not even traversed by the original attacking signal. Besides increased in-band crosstalk in the switching fabric, jamming signals can additionally affect adjacent channels inside the demultiplexers of their common switches. However, the power transfer to adjacent channels is not strong enough for them to acquire attacking capabilities [20] and is, thus, not considered in this paper.

The spreading of jamming attacks can be thwarted if Reconfigurable Optical Add-Drop-Multiplexers (ROADMs) equipped with Variable Optical Attenuators (VOA) which can dynamically adjust the power levels are deployed at the nodes. However, ROADMs comprise only around 20% of nodes in currently deployed networks while the remaining 80% of nodes employ Fixed OADMs (FOADMs) where signal power settings are determined in the system commissioning phase [26]. Furthermore, considering the incurred overhead of reconfiguration and associated costs, it is not yet clear whether future networks will be comprised of fully reconfigurable equipment with VOAs at all nodes in the network. Attenuators placed at the output of optical amplifiers, commonly employed to reduce the nonlinear effects due the amplifier's high gain, can also thwart high-power jamming attacks in case VOAs are used.

However, typical implementations consist of fixed attenuators which cannot be tuned dynamically and thus cannot react to a jamming attack [26].

Generally, physical-layer attacks can be classified into two broad categories according to their intended effect, both of which can cause severe damage to the proper functioning of the network [15]. The first refers to service degradation attacks, i.e. attacks which deteriorate the Quality of Service (QoS) and/or deny service (such as power jamming), while the second refers to tapping attacks used for traffic analysis or eavesdropping purposes. Currently, service degradation attacks are not the primary focus of coordinated attacks in optical networks, where more attention is paid to tapping (examples of recorded tapping attacks can be found in [6]). Consequently, most effort and/or investments in optical networks security are focused on securing the control plane and ensuring user data confidentiality via encryption mechanisms. Service degradation attacks, on the other hand, are mainly being addressed through improved optical monitoring techniques.

A significant number of network safety approaches, such as those from [25] and [14], focus on monitoring and localizing faults and attacks, i.e., deal with their consequences through different network restoration techniques after they have already occurred. However, these mechanisms do not prevent the attacks from happening. Since optical networks employ extremely high data rates with many "bits in flight", even short or sporadic service degradation attacks can put very large amounts of data at risk of getting lost or corrupted. Prevention approaches using improved optical components and alarming the fiber have been proposed but require additional equipment costs. Consequently, the idea of *attack-aware* optical networks planning was proposed in [23] aimed at enhancing network security in a cost-effective manner by reducing the consequences of physical-layer attacks through careful network planning without the use of costly specialized equipment. The main idea is to incorporate knowledge of the consequences of various attack scenarios in the planning phase to create a lightpath arrangement which will have the least damage in case an attack occurs. Since considering all possible attack consequences in one planning problem would be too constricting with respect to resource utilization, the approach considers individual attack scenarios, each with a different planning problem, to find resource-efficient solutions with added safety measures.

In [23], attack-aware routing was combined with classical graph coloring approaches, where the routing was aimed at minimizing the out-of-band crosstalk caused by jamming attacks in

fibers. Attack-aware wavelength assignment approaches which deal with infinitely propagating in-band crosstalk attacks to assess upper bounds were proposed in [24] and [7]. We extend upon this work here by considering the more realistic case where crosstalk attacks can maximally spread in one or two steps, as assumed in [25] and [12]. This means that secondary attacked signals are not strong enough for the attack to propagate further. Since the power of an attacking signal decreases in proportion to the distance and the number of switches it traverses, the assumption of a finite attack propagation radius more accurately illustrates real network conditions. Our wavelength assignment approach aims to minimize the maximum number of lightpaths that can be disrupted by any in-band crosstalk attack as a measure of the maximal potential damage caused, assuming 1 and 2-step attack propagation capabilities. We formulate integer linear programs (ILP) for the problem assuming both criteria and solve smaller instances to optimality using CPLEX, a software for solving integer linear programming problems. For larger problems, we develop GRASP heuristics to obtain good suboptimal solutions in reasonable time.

The rest of this paper is organized as follows. In Section 2, we define the problem models and give new objectives for wavelength assignment. Exact integer linear formulations considering the 1- and 2-hop attack propagation models are given in Sections 3 and 4, respectively, while Section 5 presents GRASP heuristics for the same problems. Computational results are given in Section 6, and Section 7 concludes the paper.

2. Problem definition

Given are a physical network and a virtual topology, i.e., a set of static lightpath demands. The physical topology is composed of a set of nodes and bidirectional links, where each node is equipped with an optical switch while each link represents 2 fibers, one in each direction. We assume fixed shortest-path routing of lightpath requests over the physical topology, reducing the Routing and Wavelength Assignment (RWA) problem to only Wavelength Assignment (WA). To solve it, it is necessary to assign wavelengths to all lightpath demands subject to the wavelength clash and continuity constraints, assuming no wavelength conversion. We propose new objectives for the problem aimed at reducing crosstalk attack propagation given a limited number of wavelengths.

The in-band crosstalk attack vulnerability of a network depends on its WA scheme according to the attack propagation model considered. We consider two models. The first assumes that an attacked lightpath does not acquire attacking capabilities itself, i.e., only primary attacks are possible. This means that a jamming signal injected on a legitimate lightpath can attack only lightpaths on the same wavelength which pass through common switches. We define the PAR (Primary Attack Radius) of a lightpath as the number of lightpaths it can attack directly (including itself) via the switches it traverses. To illustrate the calculation of the PAR, an example is given in figure 1 with five lightpaths, all on wavelength λ_1. A high-powered signal injected on lightpath 3, identified as the primary attacker, can affect lightpath 2 at their common switch B. Therefore, the PAR of LP 3 is 2 (i.e., LP 3 + LP 2). If a malicious signal is injected on lightpath 2, it can attack LP 1 at switch A, LP 3 at switch B and LP 4 at switch C, so the PAR of LP 2 is 4 (i.e., LP 1, LP 3, LP 4 and LP 2). Similarly, the PAR of LP 1 is 2, while LPs 4 and 5 have PARs of 3 and 2, respectively. To solve the WA problem for this scenario, we try to minimize the maximal PAR of any lightpath.

The second model includes the possibility of attack propagation limited to 2 steps, according to the assumptions made in [25], as well as recent experimental results from [20]. In this case, an attacked lightpath can become an attacker itself (called a secondary attacker), but lightpaths attacked by a secondary attacker cannot attack further. This model allows for lightpaths which do not even traverse the same switches to potentially attack each other. We define the SAR (Secondary Attack Radius) of a lightpath as the maximal number of lightpaths it can attack, both

as a primary and a secondary attacker. It is important to note that the secondary attacker can only attack other lightpaths in switches after its own point of attack, i.e., after the switch in which it was attacked itself. In our example, if the attacking signal is injected on LP 3, then LP 2 gets attacked directly, at their common switch B. In this case, LP 2 becomes the secondary attacker, but only after switch B, i.e., it cannot affect LP 1 in their common switch A. It can, however, propagate the attack to LP 4 at switch C. This means that the SAR of LP 3 is 3. LP 4 picks up components of the signal that attacked it, i.e. LP 2, but does not acquire the capability of spreading the attack further to LP 5 at switch D. To solve the WA problem for this model, we minimize the maximal SAR value in the network.

In-band crosstalk attack propagation depends on many factors, such as node architecture, virtual topology and other component characteristics, so it may not always occur in the described extent. However, we are focusing on the worst-case scenario where we assume that the attacking signal can be inserted anywhere in the network and that the leakage in the switching fabric is sufficient enough to not only deteriorate the quality of other signals inside their common switching fabric, but to also allow for them to, in some cases, gain attacking capabilities and spread the attack further.

Note, several impairment-aware algorithms exist in the literature aimed at assigning wavelengths mutually spaced further apart to reduce crosstalk effects. However, these approaches are mainly focused on out-of-band crosstalk between legitimate signals and not in-band crosstalk attacks and their propagation which is the topic considered in this paper. Namely, our approach considers effects caused by high-powered jamming signals outside of the working range of the traversed components. Naturally, two wavelength assignments with the same PAR/SAR values can have a significantly different distribution of wavelengths which can lead to different out-of-band crosstalk characteristics. Although we do not consider this here for simplicity of the model, it could be added to the optimization problem to achieve enhanced solutions considering both impairments and attacks (i.e. Impairment and Attack-Aware WA). Additionally, impairment-aware routing approaches which limit the lengths of the lightpaths according to physical-layer impairment estimations could be used as input to our wavelength assignment approach.

3. Integer linear programming formulation for the primary attack radius: ILP_PAR

In this section, we formulate the wavelength assignment problem aimed at minimizing the PAR as an exact integer linear program (ILP). Here, we assume maximally one lightpath per node pair for scalability, but drop this assumption in the heuristic algorithms proposed in Section 5. Note that the formulation, denoted as ILP_PAR, considers a given number of wavelengths as a constraint without attempting to minimize them. However, re-running the formulation to minimize wavelengths with the obtained PAR values fixed could additionally be applied for enhanced wavelength solutions. We use the following notation, parameters and variables.

Notation:

$(i,j);(x,y) \in \{1,\dots,N\}$	The source and destination nodes of a lightpath.
$(m,n) \in \{1,\dots,N\}$	The end nodes of a physical link.
$k \in \{1,\dots,W\}$	Wavelengths.
$r \in \{1,\dots,N\}$	Switches (located at nodes).

Parameters:

$N \in \mathbb{N}$	Number of nodes in the network.
$W \in \mathbb{N}$	Upper bound on the available number of wavelengths.
$P_{m,n} \in \{0,1\}$	The physical topology, where $P_{m,n} = 1$ if there exists a link between nodes *m* and *n*; 0 otherwise.
$V_{i,j} \in \{0,1\}$	The virtual topology, where $V_{i,j} = 1$ if there is a lightpath request between nodes *i* and *j*; 0 otherwise.
$p_{m,n}^{i,j} \in \{0,1\}$	The physical routing with respect to links, where $p_{m,n}^{i,j} = 1$ if there is a lightpath between nodes *i* and *j* and it is routed on physical link $P_{m,n}$; 0 otherwise.
$s_r^{i,j} \in \{0,1\}$	The physical routing with respect to switches, where $s_r^{i,j} = 1$ if there is a lightpath between nodes *i* and *j* and it is routed over switch *r*; 0 otherwise.

Variables:

$c_k^{i,j} \in \{0,1\}$	Wavelength assignment variables, where $c_k^{i,j} = 1$ if there is a lightpath between nodes *i* and *j* assigned wavelength $k \in W$; 0 otherwise.

$pa_{r,k}^{(i,j)(x,y)} \in \{0,1\}$ Primary attack variables, where $pa_{r,k}^{(i,j)(x,y)} = 1$ if both lightpaths $V_{i,j}$ and $V_{x,y}$ are routed via switch *r* on wavelength *k*; 0 otherwise.

$pa^{(i,j)(x,y)} \in \{0,1\}$ Primary attack variables, where $pa^{(i,j)(x,y)} = 1$ if both lightpaths $V_{i,j}$ and $V_{x,y}$ are routed via a common switch on the same wavelength; 0 otherwise.

$PAR^{(i,j)} \in \mathbb{N}$ The Primary Attack Radius (PAR) of a lightpath $V_{i,j}$.

$maxPAR \in \mathbb{N}$ The maximum PAR over all lightpaths in the network.

The problem formulation ILP_PAR is given by (1).

minimize $maxPAR$	(1a)
subject to:	
wavelength clash and continuity constraints:	
$\sum_k c_k^{i,j} = V_{i,j}, \forall i,j$	(1b)
$\sum_{i,j} p_{m,n}^{i,j} \cdot c_k^{i,j} \leq 1, \forall m,n,k$	(1c)
primary attack susceptibility constraints:	
$pa_{r,k}^{(i,j)(x,y)} \geq c_k^{i,j} \cdot s_r^{i,j} + c_k^{x,y} \cdot s_r^{x,y} - 1, \forall i,j,x,y,r,k$	(1d)
$pa_{r,k}^{(i,j)(x,y)} \leq c_k^{i,j} \cdot s_r^{i,j}, \forall i,j,x,y,r,k$	(1e)
$pa_{r,k}^{(i,j)(x,y)} \leq c_k^{x,y} \cdot s_r^{x,y}, \forall i,j,x,y,r,k$	(1f)
$pa^{(i,j)(x,y)} \geq pa_{r,k}^{(i,j)(x,y)}, \forall i,j,x,y,r,k$	(1g)
$pa^{(i,j)(x,y)} \leq \sum_{r,k} pa_{r,k}^{(i,j)(x,y)}, \forall i,j,x,y$	(1h)
non-propagating crosstalk attack radius constraints:	
$PAR^{(i,j)} = \sum_{x,y} pa^{(i,j)(x,y)}, \forall i,j$	(1i)
$PAR^{(i,j)} \geq 0$	(1j)
$maxPAR \geq PAR^{(i,j)}, \forall i,j$	(1k)

The objective (1a) minimizes the maximum number of lightpaths a jamming signal injected on any lightpath in the network could attack via direct in-band crosstalk. Constraints (1b) and (1c) are the wavelength clash and continuity constraints. This ensures that only those lightpaths that

are requested are assigned wavelengths (1b) and lightpaths traversing common physical links are assigned different wavelengths (1c). Constraints (1d)-(1h) are the primary attack susceptibility constraints. Constraints (1d)-(1f) ensure that if there are lightpaths between node pairs *(i, j)* and *(x, y)* which are both routed over switch *r* on wavelength *k*, that they are marked as mutual primary attackers. Constraints (1g)-(1h) ensure that $pa^{(i,j)(x,y)}$ is set to 1 if lightpaths *(i, j)* and *(x, y)* traverse at least one common switch on the same wavelength. Constraints (1i)-(1k) are referred to as non-propagating crosstalk attack radius constraints. Constraints (1i) and (1j) ensure that $PAR^{(i,j)}$ represents the non-propagating, i.e. primary, crosstalk attack radius of lightpath *(i, j)*. Constraint (1k) ensures that the lightpath attack radius of any lightpath is no greater than the *maxPAR*, which is being minimized in formulation *ILP_PAR*.

To get insight into the size of the proposed *ILP_PAR* formulation, we calculate the asymptotic number of variables N_{var_PAR} and constraints N_{cnstr_PAR} as a function of the number of lightpath demands *D*, network nodes *N* and available wavelengths *W*, given in equations (2a) and (2b), respectively.

$$N_{var\_PAR} = D^2 \cdot N \cdot W + D^2 + D \cdot W + D + 1 \quad (2a)$$

$$N_{cnstr\_PAR} = 4 \cdot D^2 \cdot N \cdot W + D^2 + D \cdot W + 3 \cdot D \quad (2b)$$

If we assume an asymptotic number of lightpath demands $D \approx N^2$ (i.e. fully connected logical topology), then $N_{var\_PAR} \approx N^5 \cdot W$ and $N_{cnstr\_PAR} \approx N^5 \cdot W$.

4. Integer linear programming formulation for the secondary attack radius: *ILP_SAR*

We extend the formulation from the previous section to consider secondary attacks as well, with the objective of minimizing the maximal SAR (Secondary Attack Radius) which includes both primary and secondary attacks. This formulation, denoted as ILP_SAR, is an extension of ILP_PAR with added parameters, variables and constraints as follows.

Additional notation:

$p, q \in \{1, \dots, N\}$ The source and destination nodes of a lightpath.

$s \in \{1, \dots, N\}$ Switches.

Additional parameters:

$o_{r,s}^{i,j} \in \{0,1\}$ The physical routing with respect to ordering of switches, where $o_{r,s}^{i,j} = 1$ if lightpath $V_{i,j}$ is routed over switch *r* before switch *s*; 0 otherwise.

Additional variables:

$pa_r^{(i,j)(x,y)} \in \{0,1\}$ Primary attack variables where $pa_r^{(i,j)(x,y)} = 1$ if both lightpaths $V_{i,j}$ and $V_{x,y}$ are routed via switch *r* on the *same* wavelength; 0 otherwise.

$sa_{(r,s)(x,y)}^{(i,j)(p,q)} \in \{0,1\}$ Secondary attack variables where $sa_{(r,s)(x,y)}^{(i,j)(p,q)} = 1$ if lightpath $V_{i,j}$ can indirectly, via secondary crosstalk attack, attack lightpath $V_{p,q}$ through switches *r* and *s* via lightpath $V_{x,y}$; 0 otherwise.

$sa^{(i,j)(p,q)} \in \{0,1\}$ Secondary attack variables where $sa^{(i,j)(p,q)} = 1$ if lightpath $V_{i,j}$ can indirectly, via secondary crosstalk attack, attack lightpath $V_{p,q}$; 0 otherwise.

$SAR^{(i,j)} \in \mathbb{N}$ The SAR of a lightpath $V_{i,j}$.

$maxPAR \in \mathbb{N}$ The maximum SAR of any lightpath in the network.

The formulation ILP_SAR is given by (3).

minimize *maxSAR*	(3a)
subject to: constraints (1b)-(1h)	
additional attack susceptibility constraints:	
$pa_r^{(i,j)(x,y)} = \sum_k pa_{r,k}^{(i,j)(x,y)}, \forall i,j,x,y,r$	(3b)
$pa_r^{(i,j)(x,y)} \geq pa_{r,k}^{(i,j)(x,y)}, \forall i,j,x,y,r,k$	(3c)
secondary attack susceptibility constraints:	
$sa_{(r,s)(x,y)}^{(i,j)(p,q)} \geq o_{r,s}^{x,y} \cdot \left[pa_r^{(i,j)(x,y)} + pa_s^{(x,y)(p,q)} - pa^{(i,j)(p,q)} - 1\right], \forall i,j,x,y,p,q,r,s$	(3d)
$sa_{(r,s)(x,y)}^{(i,j)(p,q)} \leq pa_r^{(i,j)(x,y)} \forall i,j,x,y,p,q,r,s$	(3e)
$sa_{(r,s)(x,y)}^{(i,j)(p,q)} \leq pa_s^{(x,y)(p,q)} \forall i,j,x,y,p,q,r,s$	(3f)
$sa^{(i,j)(p,q)} \geq sa_{(r,s)(x,y)}^{(i,j)(p,q)} \forall i,j,x,y,p,q,r,s$	(3g)
$sa^{(i,j)(p,q)} \leq \sum_{x,y,r,s} sa_{(r,s)(x,y)}^{(i,j)(p,q)} \forall i,j,p,q$	(3h)

propagating crosstalk attack radius constraints:

$$SAR^{(i,j)} = \sum_{x,y} pa^{(i,j)(x,y)} + \sum_{p,q} sa^{(i,j)(p,q)}, \forall i,j \quad (3i)$$

$$SAR^{(i,j)} \geq 0 \quad (3j)$$

$$maxSAR \geq SAR^{(i,j)}, \forall i,j \quad (3k)$$

Analogously to ILP_PAR, ILP_SAR minimizes the maximal SAR (3a). Constraints (1b)-(1h) are the same as in ILP_PAR. The remaining constraints are as follows. Constraints (3b) and (3c) are additional attack susceptibility constraints which ensure that if there are lightpaths between node pairs *(i,j)* and *(x,y)* which are both routed over switch *r* on any common wavelength, that they are marked as mutual primary attackers. Constraints (3d) – (3f) ensure that if lightpath *(i,j)* can attack lightpath *(x,y)* at switch *r*, and lightpath *(x,y)* can attack lightpath *(p,q)* at switch *s* after traversing switch *r*, *(i,j)* is marked as a secondary attacker on lightpath *(p,q)*. Constraints (3g) – (3h) ensure that $sa^{(i,j)(p,q)}$ is set to 1 if lightpath *(i,j)* can indirectly attack *(p,q)*. Constraints (3i) and (3j) ensure that $SAR^{(i,j)}$ represents the secondary, i.e. primary and secondary, crosstalk attack radius of lightpath *(i,j)*. Constraint (3k) ensures that the lightpath attack radius of any lightpath is no greater than the maxSAR, which is being minimized in formulation ILP_SAR.

The asymptotic number of variables N_{var_SAR} and constraints N_{cnstr_SAR} as a function of the number of lightpath demands *D*, network nodes *N* and available wavelengths *W* in the *ILP_SAR* formulation are given in equations (4a) and (4b).

$$N_{var\_SAR} = D^4 + D^2 \cdot N \cdot (W+1) + 2 \cdot D^2 + D \cdot W + 2 \cdot D + 2 \quad (4a)$$

$$N_{cnstr\_SAR} = 4 \cdot D^4 \cdot N \cdot W + 4 \cdot D^3 \cdot N^2 + D^2 \cdot N \cdot (W+1) + 2 \cdot D^2 + D(W+3) \quad (4b)$$

Under the same assumption of an asymptotic number of lightpath demands $D \approx N^2$ as for the *ILP_PAR* formulation, it follows that $N_{var\_SAR} \approx N^8 + N^5 \cdot W$ and $N_{cnstr\_SAR} \approx N^8 + N^5 \cdot W$.

5. GRASP heuristics for wavelength assignment

Due to the complexity of the ILP formulations, herein we present Greedy Randomized Adaptive Search Procedure (GRASP) heuristics for larger instances of the problem.

5.1. Greedy Randomized Adaptive Search Procedure (GRASP)

Greedy Randomized Adaptive Search Procedure (GRASP) is a metaheuristic for solving various combinatorial problems [21]. It has found useful applications in optical networks optimization, ranging from the design of SDH (Synchronous Digital Hierarchy) networks employing point-to-point WDM links [10], to survivable IP/MPLS-over-WSON (Internet Protocol/Multi-Protocol Label Switching over Wavelength Switched Optical Network) multi-layer optimization [19]. Each iteration of this multi-start procedure consists of two phases: a construction phase and a local search phase. In the construction phase, a feasible solution is built by incrementally adding a random element from the Restricted Candidate List (RCL). RCL contains elements which are not yet included in the partial solution and whose benefit to its quality, evaluated against a certain greedy function, is the highest. It may be limited by size or by the quality of contained elements and is iteratively re-constructed considering the remaining elements until the partial solution becomes feasible or complete. Due to the *greediness* of the algorithm used to construct the candidate list, the solution built in the construction phase is usually of good quality and offers fast local convergence, while the *randomized* selection of candidate elements added to the partial solution enables diversified exploration of the solution space. The solution obtained in the construction phase is not necessarily locally optimal, so local search is applied. In this phase, the incumbent solution is replaced with a better neighboring solution until no better solution can be found. After running these two phases for a desired number of iterations, the best solution over all is kept as the final result.

5.2. The proposed GRASP_PAR_WA and GRASP_SAR_WA heuristics

Two analogous variants of a GRASP Wavelength Assignment (GRASP_WA) heuristic are proposed, one to minimize the PAR (denoted as GRASP_PAR_WA) and the other to minimize the SAR (GRASP_SAR_WA). For the sake of brevity, in cases where no greater attack propagation details are necessary, we will refer to the objective criterion simply as the Attack Radius (AR). Besides minimizing the AR, the algorithm is designed to additionally minimize the number of wavelengths used which is the main objective for general wavelength assignment algorithms.

The input parameters include a physical topology $G = (V,E)$, where V is a set of nodes and E a set of edges, and a set of lightpath demands $\tau = \{LP_1, \ldots, LP_D\}$. Since we assume a fixed routing where each lightpath is routed on its shortest path in the physical topology, these paths are pre-calculated and each LP_i , i=1,...,D represents its corresponding shortest path in the physical topology. The set τ is sorted in descending order according to lightpath physical path lengths, which is aimed to help decrease the number of wavelengths required, as in [22]. The algorithm iteratively constructs a wavelength assignment solution and is run until the number of iterations

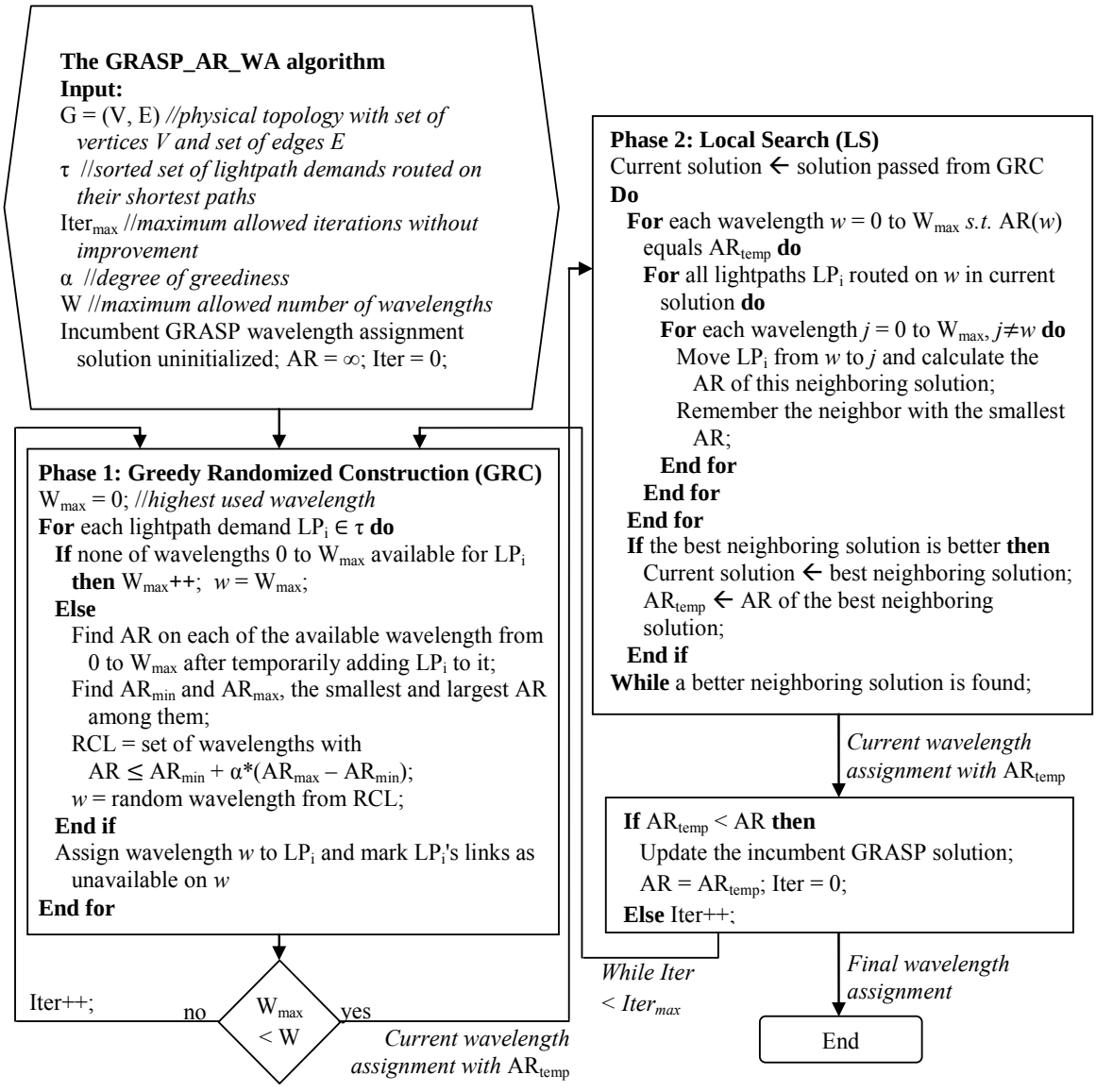

Figure 2. Flowchart of the GRASP_AR_WA algorithm.

which do not improve the incumbent solution reaches its upper limit defined in the input. The flowchart of the GRASP_AR_WA algorithm is given in figure 2, along with a textual description of the individual phases in the following subsections.

5.2.1. The construction phase

In the construction phase, a greedy randomized adaptive algorithm is used to create a feasible wavelength assignment matrix, whose element [*i,w*] is set to 1 if wavelength *w* is assigned to lightpath LP_i, and 0 otherwise. In each step, a lightpath demand is added to the partial solution, i.e., assigned a wavelength, in the following way. The attack radius AR of a wavelength, defined as the maximum AR over all lightpaths on that wavelength, is used as the fitness function to decide which wavelengths will be added to the Restricted Candidate List (RCL) for each lightpath demand. After calculating the AR which would be yielded on each of the wavelengths available for the current lightpath demand if it was added to that wavelength, we find the largest and the smallest wavelength AR among them, referred to as AR_{max} and AR_{min}, where AR_{max}=max{*AR(w)*|*w* available on LP_i}, AR_{min}=min{*AR(w)*|*w* available on LP_i}. Wavelengths *w* whose AR after adding the current lightpath demand satisfies the criterion (5) are added to the RCL.

$$AR(w) \leq AR_{min} + \alpha(AR_{max} - AR_{min}) \quad (5)$$

Parameter $\alpha \in [0,1]$ in (5), which we refer to as the degree of greediness, determines how high the relative quality of the solutions must be for them to enter into the RCL of the construction phase. For α = 0, the construction is pure greedy because only the best wavelengths, i.e. wavelengths with AR=AR_{min}, enter the RCL. A value of α = 1 gives a purely random construction (non-greedy) since all wavelengths available on the current lightpath's path are included in the RCL. Intermediate values of α tune the RCL accordingly. Once the RCL is created, a wavelength *w* from it is chosen randomly and assigned to current lightpath demand LP_i. To try to minimize the number of wavelengths used in the solution, GRASP_AR_WA first searches for RCL candidates only among the already used wavelengths. If the resulting RCL is empty, only then can a new wavelength be used. When each lightpath demand is assigned a wavelength, the construction phase is finished and the resulting WA scheme is passed to the local search phase. Due to the greedy aspect of the construction phase the found solutions are

already of good quality, while the randomness allows for diversified exploration of the solution space.

5.2.2. The local search phase

In the local search phase, the neighborhood of the solution passed from the construction phase is explored in order to find a local optimum. As evaluation function we use the AR of a WA solution, defined as the maximum AR over all lightpaths. A neighboring solution of a WA matrix A is defined as a feasible WA matrix B in which one lightpath is assigned a different wavelength than in A. The AR of each neighboring solution is calculated and the best among all neighboring solutions is found to replace the current solution in the next local search iteration and potentially update the incumbent solution. In case the ARs of two solutions are equal, the one with a lower average AR per lightpath is chosen. Generally, the local search phase starts by exploring the neighboring solutions created by moving lightpaths from the wavelength with the lowest index to other wavelengths. This may result with many neighboring solutions created by moving lightpaths which already have a satisfyingly low AR in the current WA solution. Although this technique enables wide neighborhood exploration, it can slow down the search, raising scalability issues when run for bigger network instances with a large number of lightpaths. Consequently, we start the local search from the wavelength with the highest value of AR, leading to a faster decrease of the maximum AR value, and terminate it when all wavelengths reach an equal AR.

5.2.3. Computational complexity

To calculate the PAR and SAR for d lightpaths routed on the *same* wavelength, we use the procedure described in [7] which constructs a structure called attack matrix with d rows and N columns (N is the number of nodes in the network), with elements in row i set to natural numbers corresponding to the order in which lightpath LP_i traverses certain switches, and 0 otherwise. From the attack matrix, the PAR for that wavelength can be calculated in $O(d^2)$ time by checking all lightpath pairs for switch-sharing, indicated by non-zero elements in the same columns of their corresponding rows in the attack matrix. Analogously, SAR calculation per wavelength takes $O(d^3)$ time.

The worst-case complexity of the construction phase can be calculated in the following way. This method constructs a $D \times W$ WA solution matrix, where D is the *total* number of lightpath demands, by calculating the attack radius for each lightpath demand on each of the available wavelengths. In the worst case, each of the W wavelengths is available for each of the D lightpath demands, which results in $D \cdot W$ calculations of the AR. Therefore, complexity of the GRASP_PAR_WA and GRASP_SAR_WA construction phases is $O(D^3W)$ and $O(D^4W)$, respectively.

When a $D \times W$ WA solution matrix is passed to the local search phase, its neighborhood is explored to find a solution with a lower AR. Since a neighboring solution is defined as a WA matrix where one and only one lightpath is assigned a different wavelength than in the starting solution, a $D \times W$ WA matrix has $D \cdot (W - 1)$ neighboring solutions. In the worst-case scenario, all neighboring solutions are feasible, i.e., the wavelength clash and continuity constraints hold, so the local search must calculate the AR of each, implying that a *single* iteration of the GRASP_PAR_WA and GRASP_SAR_WA local search phase also takes $O(D^3W)$ and $O(D^4W)$ time, respectively. Recall that the local search is run iteratively until no better solution is found, which makes it consume a dominant part of GRASP's execution time. However, note that this is the worst-case complexity and in a practical perspective, due to the wavelength clash and continuity constraints, only a smaller number of wavelengths is available for each lightpath demand, which significantly reduces the number of feasible WA solution and thus, required AR calculations in both phases of GRASP.

6. Numerical Results

To evaluate the performance of GRASP_AR_WA and the proposed attack-aware approach, we first generated a pool of input data aimed at capturing various characteristics of lightpath demands and their associated paths over the physical topology. Three different physical topologies were considered: the Austrian network with 5 nodes and 6 bi-directional links shown in fig. 3(a), the Pan-European network with 11 nodes and 26 bi-directional fiber links from the COST 239 project [2], shown in fig. 3(b) and the well-known NSF network consisting of 14 nodes and 24 bi-directional fiber links, shown in fig. 3(c).

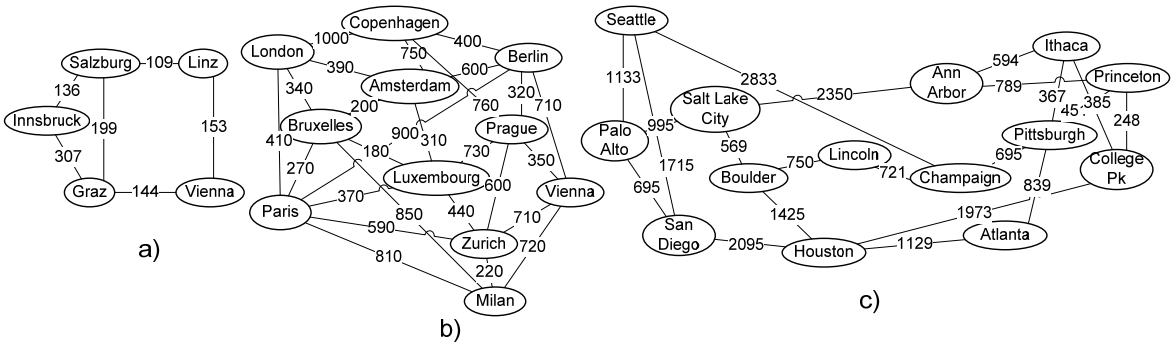

Figure 3. (a)Austrian, (b) Pan-European COST 293 and (c) NSF test network used in the simulations.

To generate lightpath demands for each network topology, we applied the same method as in [7] which uses two approaches (*Population-Based* and *Variable Characteristics*) to generate traffic matrices representing long term traffic flows between node pairs, and then generates lightpath demands from these matrices using two methods (*Traffic Threshold* and *Balanced Transceivers*). We used an additional lightpath demand generation method, denoted as *Single-Hop*, to establish direct virtual links between all nodes which exchange mutual traffic. A summary of the methods applied follows.

To generate traffic matrices, the *Population-Based* method from [4] generates traffic intensity estimates based on node populations and distances with an added random component. The node populations refer to the population of the associated cities taken from [3] and the distances refer to their air travel distances from [8]. The generated traffic is symmetric, directly proportional to node populations and inversely proportional to their distances, with a randomness factor set to

Table 1. Test data generation scenarios

Traffic matrix generation method	*Population-Based* [4]			*Variable Characteristics* [1]		
SINGLE LIGHTPATH (SL) PER NODE PAIR (Austrian network)						
Test scenario	**SL 1**	**SL 2**	**SL 3**	**SL 4**	**SL 5**	**SL 6**
Lightpath demand generation method	*TT p=0.25*	*TT p=0.5*	*BT T=3*	*TT p=0.25*	*TT p=0.5*	*BT T=3*
MULTIPLE LIGHTPATHS (ML) PER NODE PAIR (Pan-European and NSF networks)						
Test scenario	**ML 1**	**ML 2**	**ML 3**	**ML 4**	**ML 5**	**ML 6**
Lightpath demand generation method	*TT p=0.75*	*BT T=10*	*SH*	*TT p=0.75*	*BT T=10*	*SH*

25%. The second method, *Variable Characteristics* from [1] allows for tuning the level of traffic burstiness. It generates a fraction F of the traffic load uniformly distributed over $\left[0, \frac{C}{a}\right]$, while the remaining traffic is uniformly distributed over $\left[0, C \cdot \frac{\gamma}{a}\right]$. The values were set to $C = 1250$, $a = 20$, $\gamma = 10$ and $F = 0.7$, as in [1]. Ten traffic matrices were generated for each traffic generation method.

To obtain sets of lightpath demands from the generated traffic matrices three methods were used: *Traffic Threshold (TT), Balanced Transceivers (BT)*, and *Single-Hop (SH)*. The *Traffic Threshold (TT)* method creates lightpath requests between node pairs whose value is within *p* (in percentage) of the value of the maximal traffic demand in the matrix. For scalability reasons, the ILP formulation allows maximally 1 lightpath per node pair, and thus lightpath demand sets were generated accordingly for the small 5-node Austrian network. In the Single Lightpath (SL) scenarios, parameter *p* was set to 25% and 50% to create a series of denser and sparser virtual topologies with no constraints on the number of transceivers per specific node. For generality, the heuristic approach allows multiple lightpaths between node pairs. Thus, for the Multiple Lightpaths (ML) scenarios created for the larger networks (11-node Pan-European and 14-node NSF networks), the *TT* method created as many lightpaths as necessary to accommodate the offered traffic between node pairs exceeding *p* (in percentage) of the maximal traffic demand in the traffic matrix, where *p* was set to 75% to generate moderately sized virtual topologies.

The method denoted as *Balanced Transceivers (BT)* establishes lightpaths between node pairs in decreasing order of their corresponding traffic, with at most *T* transmitters and receivers per node. For the 5-node network with single lightpaths, parameter *T* was set to 3, while for the larger networks with multiple lightpaths *T* was set to 10. The third VT design method used, denoted as *Single-Hop (SH)*, was applied only to the larger networks to generate multiple lightpaths between each node pair without traffic threshold or transceiver constraints. Since this method creates direct virtual links to accommodate all offered traffic, it is not applicable to the single lightpath between node pair scenario unless all traffic between each pair can be routed over a single lightpath. Similar to TT, lightpaths are established until all offered traffic is accommodated. Since the ratio between the lightpath capacity and the maximal node-pair traffic is 1:10, there can be at most 10 lightpaths between any node pair. The described test scenarios

Table 2. Average number of lightpaths in each of the test scenarios of the 5-node Austrian, 11-node Pan-European and14-node NSF network used in the simulations.

Network	Average number of lightpaths per test scenario					
	SL 1	**SL 2**	**SL 3**	**SL 4**	**SL 5**	**SL 6**
Austrian	20	13.4	14.2	4.1	3	14.4
	ML 1	**ML 2**	**ML 3**	**ML 4**	**ML 5**	**ML 6**
Pan-European	30.8	110	478.9	76.9	1081	244.7
NSF	123.6	133.6	905.8	138.7	139.3	433.4

are summarized in table 1, and the average number of lightpaths comprising virtual topologies generated with the described methods is shown in table 2 for each test scenario.

The contributions supported in the continuation of this section are twofold. In Subsection 6.1, we first evaluate the efficiency of the proposed GRASP algorithm as a good solution approach for the Attack-Aware Wavelength Assignment problem defined in this paper. Then, in Subsection 6.2, we investigate the benefits of using this approach as a cost-effective method to improve security with respect to classical Wavelength Assignment approaches.

6.1. **Evaluation of the proposed GRASP_PAR_WA and GRASP_SAR_WA heuristics**

To evaluate the performance of the proposed GRASP_PAR_WA and GRASP_SAR_WA algorithms as efficient methods of minimizing the PAR and SAR, respectively, we first compare them with the optimal results of the ILP formulations. The heuristic algorithms were implemented in C++ and tested on an HP workstation powered by two Intel Xeon 2.53 GHz processors with 16 GB RAM. The ILPs were run in CPLEX v12.1. Since the ILPs could only be run in reasonable time for small networks and a limited number of lightpaths, we tested it for the 5-node Austrian network (fig. 3(a)) with maximally one lightpath per node pair (i.e., the SL scenarios) with parameter settings outlined in table 1. We set GRASP parameter α to 0.8 and W to 5, i.e. the number of wavelengths used by the ILPs, and allow the algorithms to run for 100 iterations without improvement. The values of the algorithm parameters were determined experimentally. Note that in this experiment for a fair comparison with the ILPs which do not minimize wavelengths, we allow the construction phase of GRASP to consider all available wavelengths when creating the RCL without attempting to minimize them.

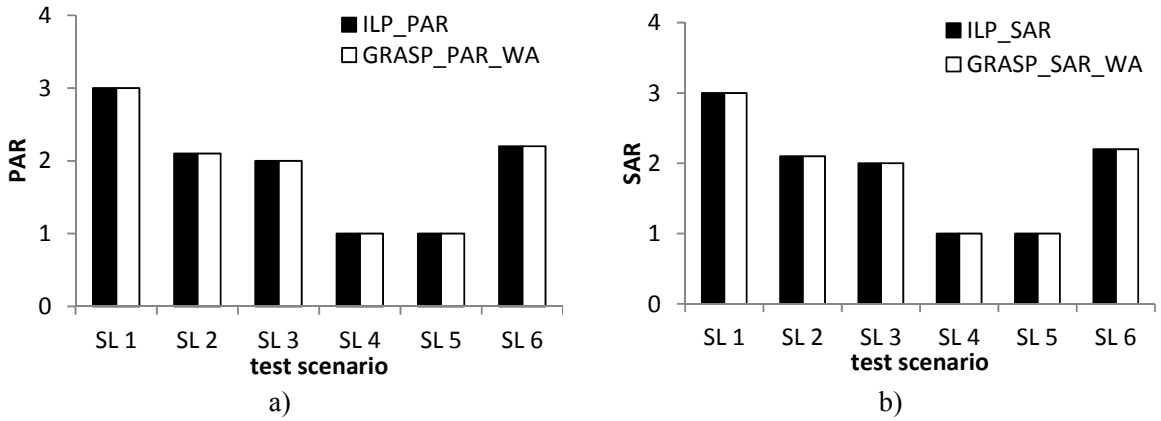

Figure 4. (a) PAR and (B) SAR values obtained by solving the ILP formulations and using the GRASP algorithms for the Austrian network.

Fig. 4 gives a comparison of the maximal PAR and SAR values obtained by the corresponding ILP formulations and GRASP algorithms. Compared to their ILP counterparts, we can see that GRASP_PAR_WA and GRASP_SAR_WA obtain optimal solutions in all test cases. The average number if iterations to the optimal solution run by the GRASP algorithms was 14.9 and 6.9 for the PAR and SAR variants, respectively.

For larger network scenarios, we performed a number of different experiments. First, to get insight into the performance of the individual parts of the proposed GRASP algorithms and their significance, we compared them with the following two variations. To validate the computational expense of running GRASP iterations in comparison with using a fast greedy algorithm, we compare it with results obtained by running a single iteration of the construction phase of GRASP_AR_WA made pure greedy by setting parameter α to 0. This algorithm, denoted as PAR/SAR_WA_greedy, stops when all lightpath demands are checked for available wavelengths and assigned the one with the lowest AR, if such a wavelength exists. If there are not enough wavelengths to accommodate all lightpath demands, wavelength blocking occurs. This pure greedy approach usually gives good quality initial solutions in very short time and allows us to investigate the improvement obtained by the GRASP iterations and in that way further tune the algorithm parameters.

The second variation of the GRASP algorithms used in the experiment, denoted as GRASPnoLS_PAR_WA and GRASPnoLS_SAR_WA, is the iterative GRASP approach with the same parameter settings as in GRASP_AR_WA but without local search, i.e. only iterative

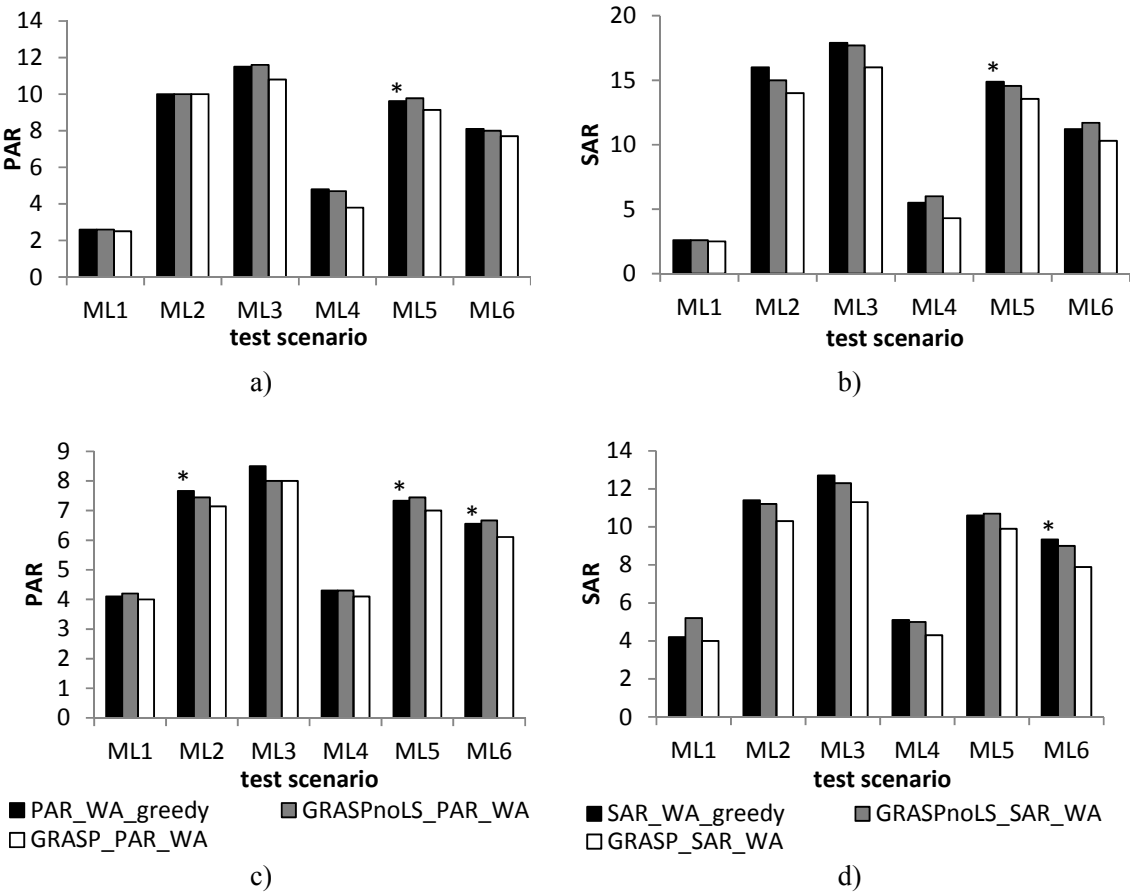

Figure 5. The PAR and SAR values obtained by the AR_WA_greedy, GRASP_AR_WA and GRASPnoLS_AR_WA for the Pan-European (a and b) and for the NSF network (c and d).
Note: Test scenarios marked with * contain test cases for which AR_WA_greedy could not find a feasible solution due to wavelength blocking.

construction is run. This allows us to investigate the benefits of the local search phase over the randomized greedy iterations.

We ran GRASP for all network scenarios for a different number of iterations without improvement, ranging up to 150. Due to algorithm's fast convergence (on average less than 3 iterations to the best solution), we finally set this value to 10 for the experiments described in this paper. Parameter α was set to 0.8 as for the previous experiment. For a fair comparison, the GRASPnoLS_AR_WA algorithms were allowed to run for the same amount of absolute time

(and not just iterations) as GRASP_AR_WA and all three algorithms were allowed to use the same number of wavelengths. The number of available wavelengths was determined by an independent WA algorithm called First Fit Decreasing (FFD), whose main objective is to minimize the number of wavelengths used, and will be explained in the following section. Additionally, we recorded the iteration in which the best solution was found by the GRASP_AR_WA variants to get insight into their convergence. The tests were run for the larger network topologies (fig. 3(b,c)) with multiple lightpaths between node pairs (i.e., the ML scenarios) with the parameter settings outlined in table 1.

Figure 5 shows the results of this comparison. The GRASP_PAR_WA and GRASP_SAR_WA algorithms obtained lower or equal PAR and SAR values in all feasible test scenarios. Note, for some test cases, the AR_WA_greedy algorithms were unable to assign wavelengths to all lightpaths due to their limited number, i.e. wavelength blocking occurred. In Figure 5, this is denoted with an asterisk next to the results in test scenarios containing such test cases. The corresponding AR* values refer to their average over the non-blocking test cases. The other two variations (GRASP with and without local search) found feasible non-blocking solutions in all test cases.

The average number of iterations (time) to the best solution for the GRASP algorithms was 1.5 (484.7 seconds) and 2 (2200.2 seconds) for the PAR and SAR variants, respectively. The GRASPnoLS algorithms naturally ran faster individual iterations due to the omission of the local search phase, but were unable to find the same solution as their full GRASP counterparts even when run for equal absolute time. The greedy algorithms ran the fastest, averaging 0.22 seconds, but failed to find feasible solutions in many cases. Furthermore, the cases for which feasible solutions were found were inferior to the solutions obtained by GRASP. Note, considering this is an offline planning problem, all the running times for the tested algorithms are acceptable for a reasonable number of iterations.

To further explore the effectiveness of the local search, we allowed GRASPnoLS_AR_WA to run until it finds a solution with the target AR equal to the one found by its GRASP_AR_WA counterpart. The results of this experiment for all six test scenarios of the NSF network are shown in fig. 6 on logarithmic scale. Due to resource limitations, if GRASPnoLS_AR_WA did not find the solution after 30 000 iterations, the simulation was stopped. Test scenarios containing such cases are marked with an asterisk in fig. 6. Even then, GRASPnoLS_AR_WA

execution time had already exceeded GRASP_AR_WA execution time by one or more orders of magnitude. According to fig. 6, GRASPnoLS_AR_WA takes significantly more time to obtain the same value of AR (if found at all) as its GRASP_AR_WA counterpart in all but one test scenario, which implies a high effectiveness of the local search phase. The only exception occurs

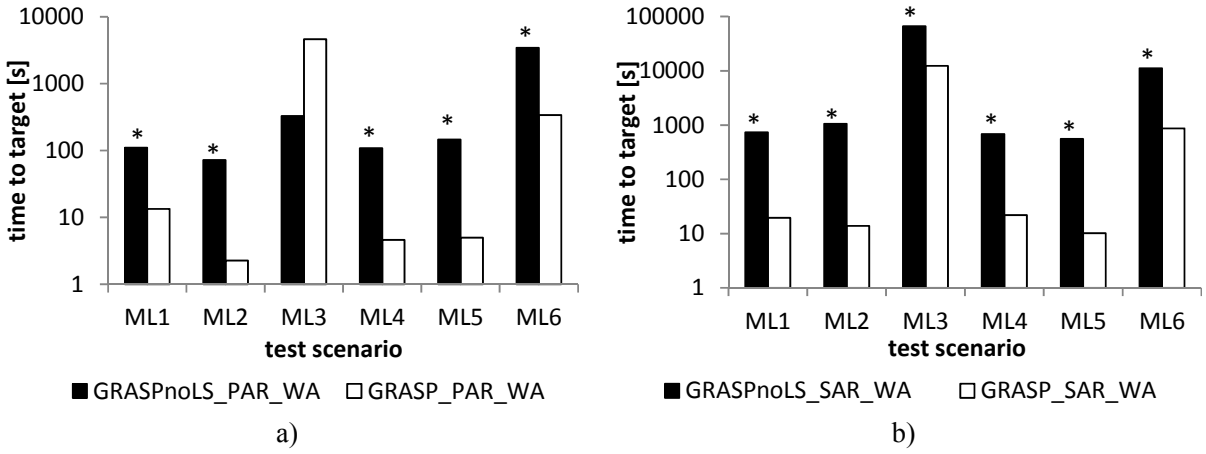

Figure 6. Time to target experiment: the time necessary for GRASPnoLS_AR_WA to achieve the same target value of (a) PAR and (b) SAR found by GRASP_AR_WA for the 6 test scenarios of the NSF network. Note: Test scenarios marked with * contain test cases for which the target was not reached within 30 000 iterations.

in the densest test scenario ML3 where GRASP_PAR_WA ran on average 1.8 iterations but required 4614.8 seconds of execution time due to a large number of AR calculations in the local search phase. For all other test scenarios, GRASP_AR_WA was significantly faster.

6.2. Evaluation of the proposed attack-aware wavelength assignment approach

Recall that our proposed attack-aware approach is a protection method aimed at reducing the potential damage that can occur in transparent optical networks in the presence of jamming attacks. However, it is critical that this approach be cost-effective. Namely, physical-layer attacks are not frequent enough for the network operator to make large investments such as buying new equipment or using significantly more resources (e.g. wavelengths) to completely prevent attacks from happening. Thus, an algorithm which achieves very low PAR/SAR values but uses a large number of wavelengths (note, this can always be achieved by setting each lightpath to its own wavelength) is not a viable option. However, if an attack occurs, although infrequent, it can cause network-wide damage. Consequently, the main idea of our approach is to

reduce this potential damage by adding attack-awareness to the network planning process, while using the *same* amount of resources the operator or bandwidth user would occupy anyway. Specifically, here our aim is to achieve maximal attack propagation reduction via wavelength assignment subject to using the same number of wavelengths as a strictly wavelength-minimizing approach (the main objective of general WA), deriving a solution the operator would be more keen to apply.

To evaluate the benefits of our attack-aware approach as a cost-effective WA method, we first ran classical WA algorithms aimed at minimizing the number of wavelengths, without caring for the PAR/SAR values. The first approach run was the classical First Fit (FF) algorithm which has been shown to perform well with respect to the number of wavelengths [9]. FF assigns to each lightpath the wavelength with the lowest wavelength index which is available on all links included in the lightpath's physical path. A new wavelength is used only in case a current lightpath cannot be assigned any of the already used wavelengths. In addition, we implemented a variant of FF denoted as First Fit Decreasing (FFD). This algorithm sorts the lightpath demands in decreasing order of the length of their physical paths before proceeding as FF, similar to a wavelength-minimizing RWA approach from [22].

We ran both FF and FFD for all the larger multi-lightpath network scenarios and recorded the lowest number of wavelengths necessary for successful non-blocking RWA. Since FFD performed better or equal to FF in all test cases, the FFD wavelength values were set as the input number of wavelengths available for each test scenario (as mentioned in Section 6.1). The PAR and SAR values obtained by the FFD algorithms were also recorded for comparison with those of the GRASP heuristics run for the same number of available wavelengths.

Additionally, we ran the so-called Random Pick (RP) algorithm since this simple approach has been shown to be crosstalk-friendly due to its random selection of wavelengths assigned to lightpaths [9]. As RP is known to be less wavelength-friendly, in many cases it is unable to find a valid solution using the given number of wavelengths. Thus, we ran RP as a multi-start algorithm and allowed it to keep searching for a non-blocking solution for the same amount of time as GRASP. Besides the random order of the wavelengths assigned, we randomly reorder the set of lightpath demands in each RP iteration.

Fig. 7 shows the maximum PAR and SAR values obtained by FFD, RP and GRASP_AR_WA for the 11-node Pan-European and 14-node NSF network. The FF algorithm performed similarly to FFD for all test scenarios with respect to the average PAR (within the order of magnitude of 10^{-2}) and significantly worse (>29% higher) for the SAR. It was, therefore, omitted for the sake of brevity. For the RP approach, test scenarios marked with an asterisk include test cases for which RP did not find a feasible non-blocking solution in the given time. The AR* values shown give the average values over all RP feasible solutions found first for each test scenario. From fig. 7 we can see that the GRASP heuristics obtain significantly smaller PAR and SAR values in all test scenarios in comparison to FFD and the crosstalk-friendlier RP. The average results over all test scenarios of the Pan European network show that GRASP_PAR_WA obtains 55.2% and

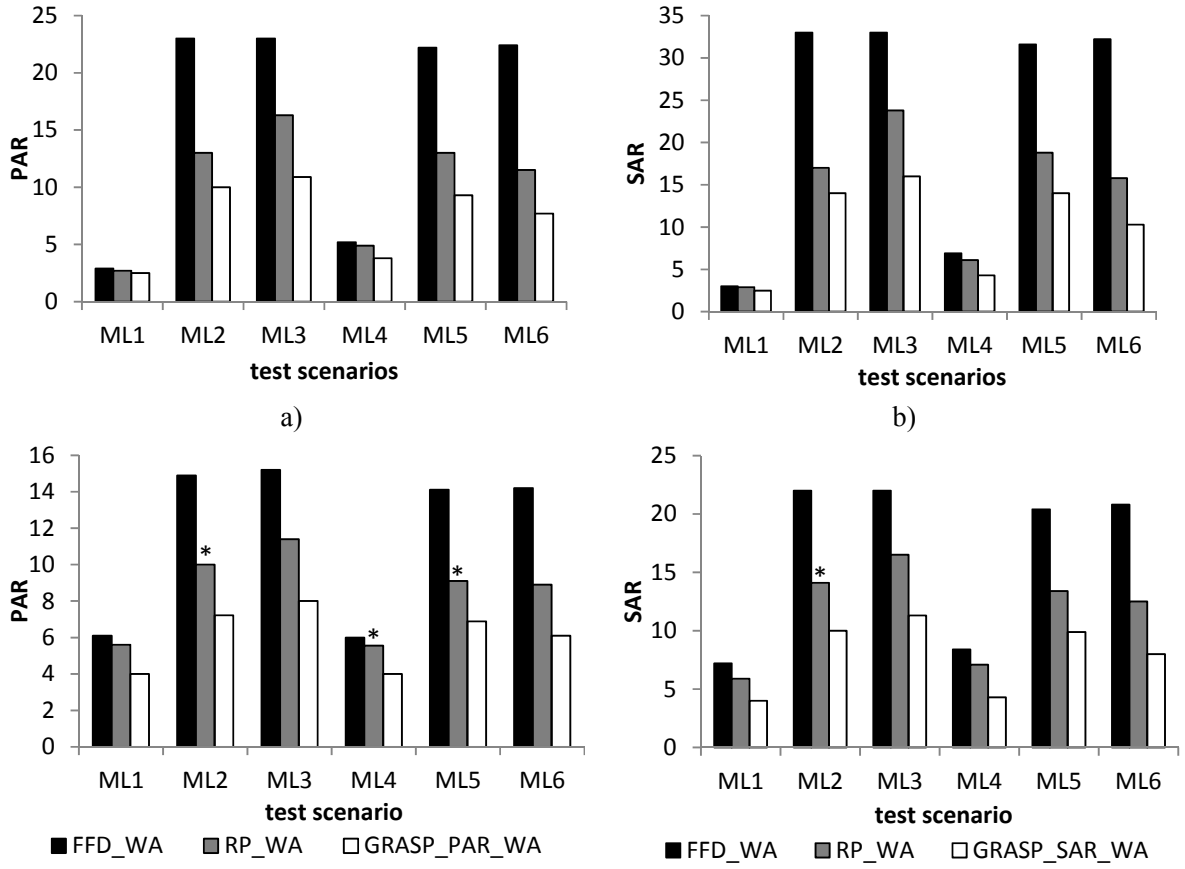

Figure 7. PAR and SAR values obtained by FFD, RP and GRASP_PAR_WA algorithms for the PanEuropean (a and b) and NSF network (c and d) in each of the six test scenarios. All algorithms have the same number of wavelengths at disposal and RP is allowed the same execution time as GRASP to search for a feasible non-blocking solution. Note: Test scenarios marked with * contain test cases for which RP could not find a feasible solution due to wavelength blocking.

27.9% lower PAR values than FFD and RP, respectively. Analogously, the SAR obtained by GRASP_SAR_WA is 56.3% and 27.6% smaller than FFD and RP. For the NSF network, GRASP_PAR_WA reduced the PAR values found by FFD and RP by 48.6% and 28.4%, while the SAR obtained by GRASP_SAR_WA was 56.9% and 37.5% smaller than in FFD and RP, respectively. Note, the true superiority of GRASP over over RP is even greater considering that RP was not able to find feasible non-blocking solutions in several cases when run for the same amount of time.

Since the number of wavelengths obtained by FF/FFD can be constricting, especially for RP, we also ran the algorithms for a larger number of available wavelengths. Again, RP was run for the same execution time as GRASP_AR_WA, and the solution with the lowest AR found was recorded. Between two solutions with the same AR, the one using fewer wavelengths was chosen. We tested this for the NSF network with W=100 for all ML test scenarios described in table 2. The relation between the number of wavelengths necessary for successful WA and the obtained PAR are shown in fig. 8 for test scenario ML3 which produces the densest virtual topologies (i.e. the highest number of lightpaths). The results for other test cases are analogous and are omitted for the sake of brevity.

We can see from figure 8 that the RP algorithm is able to obtain solutions with low PAR and SAR values due to the random selection of wavelengths, but requires all the available

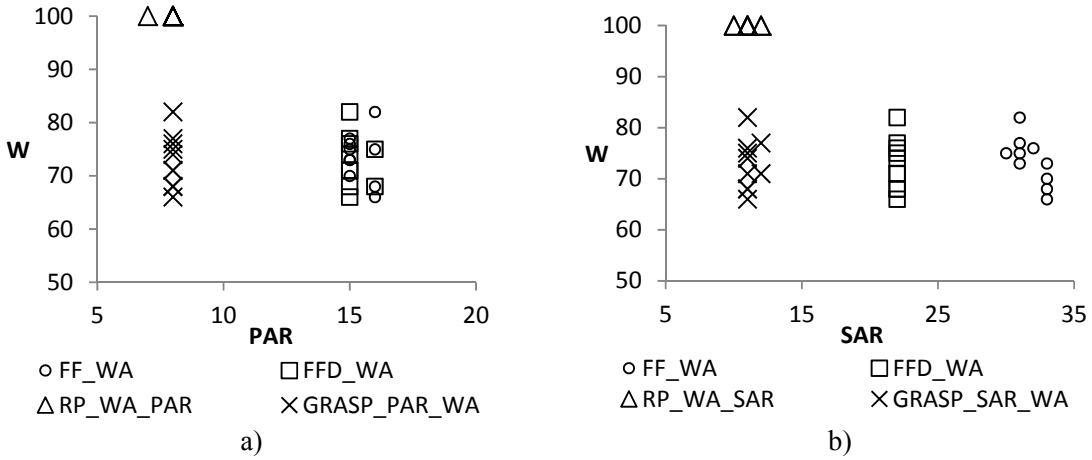

Figure 8. The trade-off between (a) the PAR and (b) SAR and the number of wavelengths used by the FF, FFD, RP and GRASP_AR_WA algorithms for the densest test scenario ML3 of the NSF network with 100 wavelengths available.

wavelengths to do so. Conversely, the FF/FFD approaches use fewer wavelengths, but at the cost of higher crosstalk propagation characteristics. The proposed GRASP_PAR_WA and GRASP_SAR_WA algorithms, however, achieve an advantageous trade-off between these two objectives, i.e. they obtain comparable PAR and SAR results with crosstalk-friendly RP, but using the same number of wavelengths as wavelength-friendly FF and FFD. Thus, they are able to achieve a good balance between crosstalk attack propagation protection and resource (i.e. wavelength) usage, validating the proposed approach as cost-effective attack-aware planning method.

Conclusion

In this paper, we propose a preventive wavelength assignment approach for minimizing the propagation of jamming attacks exploiting in-band crosstalk in optical switches. We consider two scenarios of limited attack propagation assuming a primary and/or secondary attacker. Accordingly, we define new objective criteria for wavelength assignment, called the Primary Attack Radius (PAR) and Secondary Attack Radius (SAR), and propose integer linear programming (ILP) formulations of both problem variations to find optimal solutions for small networks. For larger problem instances, we develop efficient GRASP heuristics for wavelength assignment which minimize the defined attack radius, as well as wavelength utilization. In this way, we achieve enhanced protection from high-power jamming crosstalk attacks without the use of additional resources. For future work, we plan to extend this work with survivable planning and monitoring placement, as well as out-of-band crosstalk effects, to help establish an integrated physical-layer attack-aware planning framework for transparent optical networks.

Acknowledgments

The work described in this paper was carried out with the support of the projects “A Security Planning Framework for Optical Networks (SAFE),” funded by the Unity Through Knowledge Fund (UKF) in Croatia and 036-0362027-1641, funded by the Ministry of Science, Education and Sports, Croatia. It was also developed in the framework of the MICINN/FEDER project grant TEC2010-21405-C02-02/TCM (CALM), MICINN project grant TEC2010-12250-E (FIERRO) and project "Programa de Ayudas a Grupos de Excelencia de la Región de Murcia” funded by F. Séneca (Plan Regional de Ciencia y Tecnología 2007/2010). The authors would

also like to thank the ONLab led by Prof. Lena Wosinska at the Royal Institute of Technology (KTH) in Stockholm, Sweden, for allowing us to use their facilities for algorithm simulations.

References

[1] Banerjee, D. & Mukherjee, B. (2000). Wavelength-Routed Optical Networks: Linear Formulation, Resource Budgeting Tradeoffs, and a Reconfiguration Study. *IEEE/ACM Transactions on Networking, 8, 5*, 598-607.

[2] Batchelor, P. et al. (2000). Study on the implementation of optical transparent transport networks in the European environment-Results of the research project COST 239. *Photonic Network Communications, 2, 1,* 15-32.

[3] Brinkhoff, T. City population. Available online: www.city-population.de

[4] Cahn, R. S. (1998). *Wide Area Network Design. Concepts and Tools for Optimization*. Morgan Kaufmann Publishers.

[5] Chlamtac, I., Ganz, A. & Karmi, G. (1992). Lightpath communications: an approach to high-bandwidth optical WANs. *IEEE Transactions on Communications, 40,* 1171-1182.

[6] Fouchereau, R. (2009). Fiber-Optic Networks: Is Safety Just an Optical Illusion?. IDC Technology Assessment.

[7] Furdek, M., Skorin-Kapov, N. & Grbac, M. (2010). Attack-Aware Wavelength Assignment for Localization of In-band Crosstalk Attack Propagation. *IEEE/OSA Journal of Optical Communications and Networking, 2, 11,* 1000-1009.

[8] Geobytes. City distance tool. Available online: http://www.geobytes.com/citydistancetool.htm

[9] He, J., Brandt-Pearce, M. & Subramaniam, S. (2009). QoS-Aware Wavelength Assignment With BER and Latency Constraints for All-Optical Networks. *IEEE Journal of Lightwave Technology, 27, 5,* 462-473.

[10] Höller, H., Melián, M. & Voß, S. (2008). Applying the Pilot Method to Improve VNS and GRASP Metaheuristics for the Design of SDH/WDM Networks. *European Journal of Operational Research, 191, 3,* 691-704.

[11] Krishnaswamy, R. M. & Sivarajan, K. N. (2001). Design of Logical Topologies: a Linear Formulation for Wavelength Routed Optical Networks with No Wavelength Changers. *IEEE/ACM Transactions on Networking, 9, 2,* 186-198.

[12] Liu, G. & Ji, C. (2007). Resilience of All-Optical Network Architectures under In-Band Crosstalk Attacks: A Probabilistic Graphical Model Approach. *IEEE Journal on Selected Areas in Communications, 25, 4,* 2-17.

[13] Malaguti, E., Monaci, M. & Toth, P. (2011). An Exact Approach for the Vertex Coloring Problem. *Discrete Optimization, 8, 2,174-190*.

[14] Mas, C., Tomkos, I. & Tonguz, O. K. (2005). Failure Location Algorithm for Transparent Optical Networks. *IEEE Journal on Selected Areas in Communications, 23,* 1508-1519.

[15] Médard, M., Marquis, D., Barry, R. A. & Finn, S. G. (1997). Security Issues in All-Optical Networks. *IEEE Network, 11, 3,* 42-48.

[16] Mukherjee, B. (2006). *Optical WDM Networks.* Springer Science+Business Media.

[17] Noronha, T. F., Resende, M. G. C. & Ribeiro, C. C. (2011). A biased random-key genetic algorithm for routing and wavelength assignment. *Journal of Global Optimization, 50, 3,* 503-518.

[18] Ozdaglar, A. E. & Bertsekas, D. P. (2003). Routing and Wavelength Assignment in Optical Networks. *IEEE/ACM Transactions on Networking, 11, 2,* 259-272.

[19] Pedrola, O., Ruiz, M., Velasco, L., Careglio, D., Gonzaléz de Dios, O. & Comellas, J. (2011). A GRASP with path-relinking heuristic for the survivable IP/MPLS-over-WSON multi-layer network optimization problem. *Computers & Operations Research, in press,* available online: http://dx.doi.org/10.1016/j.cor.2011.10.026

[20] Peng, Y., Sun, Z., Du, S. & Long, K. (2011). Propagation of all-optical crosstalk attack in transparent optical networks. *Optical Engineering, 50, 8,* 085002.1-3.

[21] Resende, M. G. C. & Ribeiro, C. C. (2010). Greedy Randomized Adaptive Search Procedures: Advances, Hybridizations, and Applications. In Gendreau, M. & Potvin, J. Y. (Eds.), *Handbook of Metaheuristics*, 2nd ed., Springer Science & Business Media.

[22] Skorin-Kapov, N. (2007). Routing and Wavelength Assignment in Optical Networks Using Bin Packing Based algorithms. *European Journal of Operational Research, 177, 2,* 1167-1179.

[23] Skorin-Kapov, N., Chen, J. & Wosinska, L. (2010). A New Approach to Optical Networks Security: Attack-Aware Routing and Wavelength Assignment. *IEEE/ACM Transactions on Networking, 18, 3,* 750-760.

[24] Skorin-Kapov, N. & Furdek, M. (2009). Limiting the Propagation of Intra-Channel Crosstalk Attacks in Optical Networks through Wavelength Assignment. In Optical Fiber Communication Conference and Exposition (OFC) and The National Fiber Optic Engineers Conference (NFOEC), Optical Society of America, Washington, DC, JWA65.

[25] Wu, T. & Somani, A.K. (2005). Cross-Talk Attack Monitoring and Localization in All-Optical Networks. *IEEE/ACM Transactions on Networking*, *13, 6,* 1390-1401.

[26] Zsigmond, S. (2011). External report on physical-layer attacks in optical networks. Technical report, project SAFE (http://www.fer.hr/tel/en/research/safe) supported by the Unity through Knowledge Fund (UKF), Ministry of Science, Education and Sports, Croatia.