Design of Attack-Aware WDM Networks Using a Meta-heuristic Algorithm

Konstantinos Manousakis, Georgios Ellinas

HAL Id: hal-01459660

https://hal.inria.fr/hal-01459660

Submitted on 7 Feb 2017

Design of Attack-aware WDM Networks using a Meta-Heuristic Algorithm

Konstantinos Manousakis and Georgios Ellinas

KIOS Research Center for Intelligent Systems and Networks,
Department of Electrical and Computer Engineering, University of Cyprus, Cyprus
{manousakis.konstantinos,gellinas}@ucy.ac.cy

Abstract. Transparent optical Wavelength Division Multiplexing (WDM) networks are vulnerable to physical layer attacks. This work proposes a meta-heuristic based algorithm for the planning phase of optical WDM networks while considering the impact of high-power in-band jamming attacks. The proposed heuristic algorithm serves sequentially the connections in a particular order and the meta-heuristic algorithm, called Harmony Search, is used to find better orderings in order to establish the requested connections. The objective of the proposed algorithm is to establish the requested connections in a specific way that minimizes the impact of high-power jamming signals through in-band channel crosstalk.

Keywords: physical layer attacks, routing and wavelength assignment, harmony search, optical networks.

1   Introduction

Optical networks nowadays rely on Wavelength Division Multiplexing (WDM) in order to increase their capacity. WDM enables different connections to be established concurrently through a common fiber, subject to the distinct wavelength assignment constraint; that is, the connections sharing a fiber must occupy separate wavelengths. All-optical WDM channels that may span multiple consecutive fibers are called lightpaths. In the absence of wavelength conversion, a lightpath must be assigned a common wavelength on each link it traverses; this restriction is referred to as the wavelength continuity constraint. Since lightpaths are the basic switched entities of a WDM optical network architecture, their effective establishment and usage is crucial. It is thus important to propose efficient algorithms to select the routes for the connection requests and to assign wavelengths on each of the links along these routes, among the possible choices, so as to optimize a certain performance metric. This is known as the routing and wavelength assignment (RWA) problem [1], that is usually considered under two alternative traffic models. Offline (or static) lightpath establishment addresses the case where the set of connections is known in advance, usually given in the form of a traffic matrix that describes the number of lightpaths that have to be established between each pair of nodes. Dynamic (or online) lightpath establishment

considers the case where connection requests arrive at random time instants, over a prolonged period of time, and are served upon their arrival, on a one-by-one basis. Offline RWA is usually used during the network design and planning phase, while online RWA is used during the network operation phase.

Offline RWA is known to be an NP-hard optimization problem and several heuristics and meta-heuristics have been proposed to solve the problem. A meta-heuristic is a procedure designed to find a good solution to a difficult optimization problem. Meta-heuristic algorithms can be classified as swarm intelligent techniques and evolutionary algorithms. Swarm intelligence algorithms are heuristic search methods that mimic the metaphor of natural biological evolution and/or the social behavior of species. Evolutionary algorithms use iterative progress, such as growth or development in a population and use mechanisms inspired by biological evolution, such as reproduction, mutation, recombination, and selection. Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO) are well-known and successful swarm intelligence optimization algorithms, while Genetic Algorithms (GAs) and Harmony Search (HS) are evolutionary optimization techniques. Meta-heuristic techniques that have been proposed to solve the offline RWA problem use techniques from ACO [2], GA [3], and PSO [4].

Optical telecommunication networks, providing services to users such as companies, governmental institutions, and private citizens, are considered one of the critical infrastructures of a country. In all-optical transparent networks, where a data signal remains in the optical domain for the entire path, there exist several vulnerabilities in the network that enable malicious signals to propagate through several parts of the network. Optical networks need to be able to detect and locate failures (faults or attacks) and degradations as fast and as accurately as possible, in order to restore lost traffic and repair the failure. An attack can be defined as an intentional action against the ideal and secure functioning of the network.

In this work, a meta-heuristic algorithm is used to solve the static attack-aware RWA problem. In the static case, the set of connections is known in advance and path selection and wavelength assignment are performed offline, aiming at the joint optimization of the lightpaths used by all the connection requests. The objective of the proposed offline attack-aware RWA algorithm is to design an optical network that minimizes the impact of a network attack. The algorithm uses a nature inspired meta-heuristic, mimicking the improvisation process of music players [5], known as a harmony search (HS) algorithm. The proposed attack-aware heuristic algorithm serves sequentially the connections in a particular order, and the HS algorithm is used to find better orderings.

The rest of the paper is organized as follows. Section 2 describes the physical layer attacks. In Section 3, the Harmony Search meta-heuristic and Harmony Search based attack-aware RWA algorithm are presented, followed by simulation results in Section 4. Finally, Section 5 presents some concluding remarks and avenues for future research.

2   Network Attacks

There are several physical layer attacks that can occur in transparent optical networks as presented in [6-7]. One of the most important attacks is *in-band jamming* that is the result of intra-channel crosstalk between the same wavelengths in optical switches. Another attack is the *out-of-band jamming*, where high-power signals can introduce nonlinearities, causing crosstalk effects between channels on different wavelengths in the same fiber (inter-channel crosstalk). Moreover, gain competition in optical amplifiers is another possible form of attack in optical networks, where a high-power jamming signal can increase its own power, thus resulting in reduction in the gain of the rest of the channels.
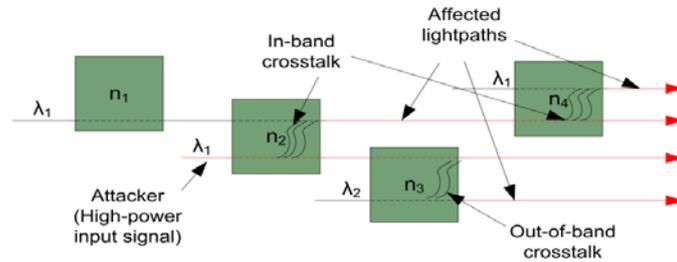

Fig. 1. High-power jamming attack propagation

In Fig. 1, the effects of in-band and out-of-band crosstalk propagation are depicted, where an attacker uses a high-power jamming signal on wavelength λ_1 to perform his attack from node n_2. Due to in-band crosstalk, this signal will affect any lightpath that crosses node n_2 and uses wavelength λ_1. Then, the affected lightpaths will perform further attacks through the nodes they cross. As can be seen from Fig. 1, the affected lightpath in node n_2 will spread the attack in node n_4 and will affect other lightpaths that use the same wavelength (λ_1). A lightpath that uses a different wavelength than the lightpath used by the attacker will not be affected, regardless of the fact that the lightpaths cross the same node. However, due to out-of-band crosstalk, a lightpath at one wavelength will affect any other lightpath using an adjacent wavelength of the same fiber. For example, in Fig. 1, the lightpath crossing node n_3 and wavelength λ_2, will be affected by the attacker, assuming that the two lightpaths use the same fiber after node n_3 (λ_1 and λ_2 are adjacent wavelengths).

When planning an optical network, the basic problem that has to be addressed is the RWA problem. Since in optical networks security of the established connections is critical, it is of paramount importance to protect the network from possible attacks. The concept of preventive, attack-aware RWA problem was proposed in [8]. In that work, the authors formulated the routing sub-problem of RWA as an integer linear program with the objective of decreasing the potential damage of jamming attacks causing out-of-band crosstalk in fibers and gain competition in optical amplifiers. A tabu search heuristic was subsequently proposed to cover larger network instances. Furthermore, in [9], authors proposed a wavelength assignment approach to limit the potential propagation of in-band crosstalk attacks through the network. Authors in

[10] extended upon their work in [9] by considering a more realistic case where cross-talk attacks can maximally spread in one or two steps. This means that secondary attacked signals are not strong enough for the attack to propagate further. In [10], authors proposed the use of wavelength-selective optical attenuators as power equalizers inside the network nodes to limit the propagation of high-power jamming attacks. They presented heuristic algorithms with the objective of minimizing the number of power equalizers needed to reduce, to a desired level, the propagation of high-power jamming attacks.

This work considers that an attack is performed by high-power jamming signals through in-band crosstalk and the objective of the proposed offline attack-aware RWA algorithm is to design an optical network that minimizes the impact of a high-power in-band jamming attacks.

3 Harmony Search Algorithm

This section describes the Harmony Search (HS) meta-heuristic algorithm as presented in [5]. HS is a search heuristic algorithm based on the improvisation process of jazz musicians. It was inspired by the observation that the aim of music is to search for a perfect state of harmony. Finding the perfect state of harmony in music is analogous to finding the optimality in an optimization process. In the HS algorithm, each musician (= decision variable) plays (= generates) a note (= a value) for finding the best harmony (= global optimum determined by objective function evaluation). The core part of the HS algorithm is the Harmony Memory (HM), where HM is a collection of random generated harmonies (=vectors). When a musician is improvising, there are three possible choices: (1) play any famous piece of music exactly from harmony memory; (2) play something similar to a known piece; or (3) compose new or random notes. Authors in [5] formalized these three options into a quantitative optimization process, and the three corresponding components become: usage of harmony memory, pitch adjusting, and randomization. Thus, harmony search tries to find a vector X which optimizes a certain objective function $f(X)$. The steps of the harmony search algorithm are as follows:

1. Initialize the harmony memory (HM) matrix:

$$\mathbf{HM} = \begin{bmatrix} x_1^1 & \cdots & x_S^1 \\ \vdots & \ddots & \vdots \\ x_1^{HMS} & \cdots & x_S^{HMS} \end{bmatrix} \Rightarrow \begin{bmatrix} f(X^1) \\ \vdots \\ f(X^{HMS}) \end{bmatrix}$$

Generate *HMS* (*Harmony Memory Size*) random vectors $X^i = (x_1^i, x_2^i, \ldots, x_S^i)$ of size S and store them in the harmony memory (HM) matrix, where S is the number of musical instruments (decision variables, x_j^i) and *HMS* is the number of random harmonies (vectors). $f(X)$ is the objective function that needs to be optimized.

2. Improvise a new harmony (Generate a new vector X^{new})

(a) For every variable x_j^{new} of the new vector X^{new} choose a value from the HM matrix $x_j^{new}, 1 \leq new \leq HMS$ with probability *HMCR* (*Harmony Memory Considering Rate*) and with probability 1- *HMCR*, choose a random value.

(b) Change the value of the variable x_j^{new} with probability *PAR* (*Pitch Adjusting Rate*), by a small amount Δ, $x_j^{new} = x_j^{new} \pm \Delta$.

3. Update the HM:
Evaluate the objective function $f(X^{new})$ of the vector X^{new}. If the value of $f(X^{new})$ is better than the worst value $f(X^{worst})$ in HM, then replace the vector X^{worst} with X^{new} in HM.

4. Check the stopping criterion:
Repeat steps 2 and 3 until the maximum iteration criterion is met.

The exact values of the parameters are discussed in Section 5.

4 Attack-aware RWA using a Meta-Heuristic Algorithm

The proposed algorithm solves the static RWA problem with the objective to minimize the impact of high-power jamming signals that spread in the network through in-band channel crosstalk. The *attack-aware heuristic* algorithm establishes the requested connections one-by-one in the form of lightpaths following a specific order. For every demand, the algorithm computes a set of candidate lightpaths. From this set, the lightpath with the minimum in-band crosstalk interaction is chosen. By minimizing the in-band channel crosstalk interactions, the spread of high-power jamming signals through in-band crosstalk is also minimized. The harmony search meta-heuristic is used to define different orderings for the requested connections. The evaluation of the objective function of the harmony search algorithm $f(X)$ is performed through simulation of the *attack-aware heuristic* algorithm. The ordering with the best value of the objective function is chosen to establish the demands. In the following subsections the main steps of the algorithm are described.

4.1 Initialization of Harmony Memory (HM)

For solving the attack-aware RWA problem using HS (Harmony Search), *HMS* (*Harmony Memory Size*) random music harmonies (random harmony vectors -X^i, $1 \leq i \leq HMS$) are initially constructed and stored in the Harmony Memory (HM) matrix. Each harmony vector $X^i = (x_1^i, x_2^i, \ldots, x_S^i)$ in the harmony memory represents the order that the demands are considered. Several values for *HMS* are discussed in the simulation section. The size S of each vector X^i is equal to the number of (*s*,*d*) pairs ($S = N^2 - N$), where N is the number of network nodes, and each element x_j^i of the vector X^i has an integer value between 1 and ($N^2 - N$). The sequence of the demands represents a music harmony in HM terminology. In order to have valid sequences for each harmony, each harmony should contain all the integers from 1 to ($N^2 - N$) and each integer should appear only once. Based on these constraints, all the requested connections are considered. A sequence is invalid if there are two or more integers with the same value.

4.2 Improvisation of a New Harmony

A new harmony is improvised (a New Harmony vector X^{new} is generated) based on the *HMCR* (*Harmony Memory Considering Rate*) and *PAR* (*Pitch Adjusting Rate*) described in Section 3. Each New Harmony vector $\mathrm{X}^{new} = \left(x_1^{new}, x_2^{new}, \ldots, x_{N^2-N}^{new}\right)$ must comply with the constraints provided in Section 4.1. For this reason, when considering a new value for each variable x_j^{new} from the set of integer values from 1 to (N^2-N), the values that have already assigned to variables $x_1^{new}, \ldots, x_{j-1}^{new}$ are removed from the available set. The *HMCR,* which ranges from 0 to 1, defines the probability to choose a variable value from HM and the *PAR* defines the probability of shifting to neighboring values within a range of possible values. If the New Harmony vector is better, in terms of the objective function cost $f(\mathrm{X}^{new})$ as presented in Section 4.3 that follows, than the worst harmony vector in HM, then the New Harmony vector is included in HM while the worst is excluded.

4.3 Objective Function – Attack-aware Heuristic Algorithm

This section describes the evaluation of the objective function $f(\mathrm{X})$ used by the harmony search algorithm. Each link l of the network is characterized by a Boolean wavelength availability vector $\overline{w_l} = [w_{li}] = (w_{l1}, w_{l2}, \ldots, w_{lW})$ whose i^{th} element w_{li} is equal to 0 if the ith wavelength of link l is utilized by a connection, and equal to 1, otherwise.

In this phase, k candidate paths P_{sd}, that have been pre-computed in the first step of the algorithm by employing a *k*-shortest path algorithm, are given as input in the *attack-aware heuristic* algorithm for serving each requested connection (*s,d*). The wavelength availability vector of a path p consisting of links $l \in p$ is defined as follows: $\overline{W_p} = [W_{pi}] = \&_{l \in p} \overline{w_l} = [\&_{l \in p} w_{li}]$, where "&" denotes the Boolean AND operation. Thus, the element W_{pi} is equal to 1 if wavelength i is available for transmission over path p. The above equation enforces the wavelength continuity constraint among the links comprising a path.

The connections are sequentially established one-by-one in the form of lightpaths. The demands are served according to the order defined by the Harmony Vector. For each demand, the candidate lightpath with the smallest number of in-band channel interactions is chosen. The objective of the attack-aware RWA heuristic algorithm is to minimize the number of lightpaths that interact with other lightpaths through in-band channel crosstalk and thus to minimize the propagation of high-power jamming signal attacks.

4.4 Flowchart of the Algorithm

The flowchart of the algorithm described in the previous subsections is given in Fig.2. The generation of a new vector X^{new} is achieved following the second step of the algo-

rithm described in section 3, taking into account the constraints of section 4.2. Moreover, the evaluation of the objective function $f(X)$ is performed following the description of section 4.3.
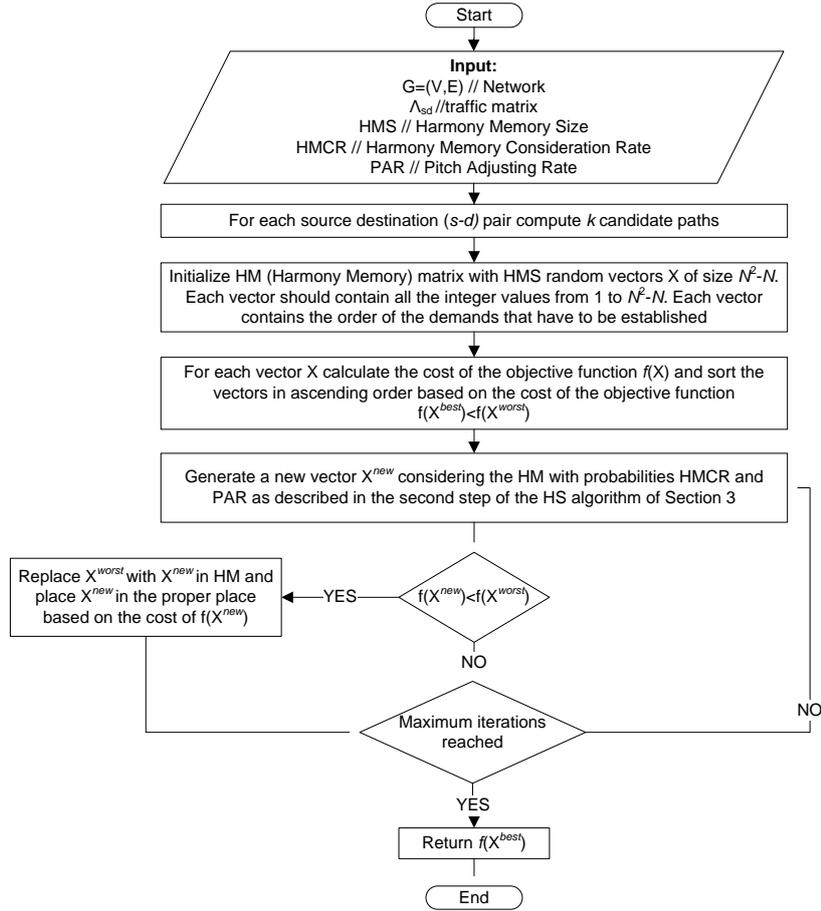
```
                          ┌──────────┐
                          │  Start   │
                          └──────────┘
                               │
                               ▼
                    ╱───────────────────────╲
                   ╱        Input:            ╲
                  ╱   G=(V,E) // Network        ╲
                 ╱   Λsd //traffic matrix         ╲
                ╱  HMS // Harmony Memory Size       ╲
               ╱ HMCR // Harmony Memory Consideration Rate
              ╱      PAR // Pitch Adjusting Rate      ╲
               ╲─────────────────────────────────────╱
                               │
                               ▼
         ┌─────────────────────────────────────────────┐
         │ For each source destination (s-d) pair       │
         │ compute k candidate paths                    │
         └─────────────────────────────────────────────┘
                               │
                               ▼
         ┌─────────────────────────────────────────────┐
         │ Initialize HM (Harmony Memory) matrix with   │
         │ HMS random vectors X of size N²-N.           │
         │ Each vector should contain all the integer   │
         │ values from 1 to N²-N. Each vector           │
         │ contains the order of the demands that have  │
         │ to be established                            │
         └─────────────────────────────────────────────┘
                               │
                               ▼
         ┌─────────────────────────────────────────────┐
         │ For each vector X calculate the cost of the  │
         │ objective function f(X) and sort the         │
         │ vectors in ascending order based on the cost │
         │ of the objective function                    │
         │          f(X^best)<f(X^worst)                │
         └─────────────────────────────────────────────┘
```

Input:
$G=(V,E)$ // Network
Λ_{sd} //traffic matrix
HMS // Harmony Memory Size
HMCR // Harmony Memory Consideration Rate
PAR // Pitch Adjusting Rate

For each source destination (*s-d*) pair compute *k* candidate paths

Initialize HM (Harmony Memory) matrix with HMS random vectors X of size N^2-N. Each vector should contain all the integer values from 1 to N^2-N. Each vector contains the order of the demands that have to be established

For each vector X calculate the cost of the objective function f(X) and sort the vectors in ascending order based on the cost of the objective function
$f(X^{best})<f(X^{worst})$

Generate a new vector X^{new} considering the HM with probabilities HMCR and PAR as described in the second step of the HS algorithm of Section 3

Replace X^{worst} with X^{new} in HM and place X^{new} in the proper place based on the cost of $f(X^{new})$ ←YES— $f(X^{new})<f(X^{worst})$

NO

Maximum iterations reached — NO

YES

Return $f(X^{best})$

End

Fig. 2. Flowchart of the algorithm

5   Simulation Results

To evaluate the performance of the proposed algorithm, a number of simulation experiments were performed using the generic Deutsche Telekom backbone network (DTnet) as shown in Fig. 3. The network consists of 14 nodes and 23 links with an average nodal degree of 2.85. The traffic load of the network is defined as the ratio of the number of requested connections to the total number of possible connections. For example, traffic load equal to 0.5 corresponds to the case were half of the entries of the traffic matrix are equal to 1 and half equal to 0.

The aim of this section is to study the impact of high-power jamming signals through in-band crosstalk and the evolution of the algorithm solution under different settings of the three important parameters: the pitch adjusting rate (PAR), the harmony memory size (HMS), and the harmony memory considering rate (HMCR). The number of maximum iterations was considered equal to 100, that corresponds to the stopping criterion of the algorithm. First, a sensitivity analysis of the harmony search model parameters was performed. Table 1 shows the analysis results for several values of the parameters (HMS = {1, 5, 10}, HMCR = {0.5, 0.8, 0.9}, and PAR = {0.1, 0.4, 0.7}).

Table 1. Results of sensitivity analysis with HS parameters.

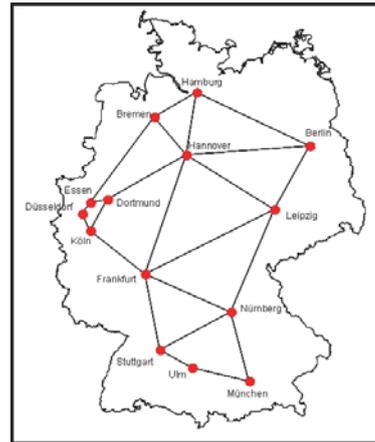| HMS	HMCR	PAR	In-band W=30	In-band W=40
1	0.5	0.1	52	14
		0.4	54	16
		0.7	50	14
	0.8	0.1	50	18
		0.4	50	14
		0.7	54	**12**
	0.9	0.1	50	14
		0.4	56	18
		0.7	50	14
5	0.5	0.1	52	14
		0.4	54	18
		0.7	56	16
	0.8	**0.1**	**48**	**14**
		0.4	52	16
		0.7	56	16
	0.9	0.1	52	16
		0.4	52	14
		0.7	52	16
10	0.5	0.1	50	18
		0.4	56	16
		0.7	54	16
	0.8	0.1	54	16
		0.4	54	18
		0.7	52	20
	0.9	0.1	56	14
		0.4	50	18
		0.7	56	16

Fig. 3. DT network topology

The term "In-band" in Table I, represents the total number of lightpaths' interactions through in-band crosstalk. The network load was equal to 0.6 and the analysis was performed for the cases of 30 and 40 available wavelengths per fiber. It is evident,

that the larger the HMCR value, the less exploration is achieved; and the algorithm further relies on stored values in HM and this potentially leads to the algorithm reaching and remaining at a local optimum. On the other hand, choosing too small a value of HMCR will decrease the algorithm efficiency and the HS will behave like a pure random search, with less assistance from the historical memory.
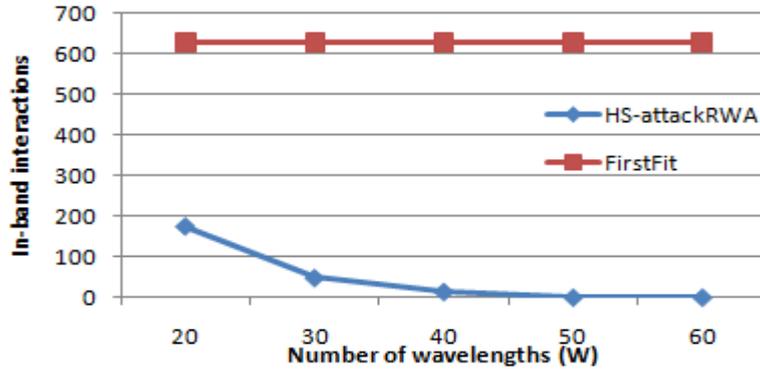

Fig. 4. In-band interactions vs number of available wavelengths

In Fig. 4, the HS attack-aware RWA algorithm was also compared to the *first-fit* algorithm, an algorithm that assigns the first available wavelength to the connections. The performance metric in this case was the number of in-band interactions versus the available number of wavelengths per fiber. For these simulations the network load was again equal to 0.6 and the three parameters used for the HS meta-heuristic, i.e., the pitch adjusting rate (PAR), the harmony memory size (HMS), and the harmony memory considering rate (HMCR) were set to the values 0.1, 5, and 0.8 respectively. These values were obtained from the sensitivity analysis as shown in Table 1 above. As can be seen from the figure, the first-fit algorithm has the same performance irrespective of the number of available wavelengths and the number of interactions is quite high (more than 600 interactions) compared to the case were the proposed HS attack-aware RWA algorithm was used. For the latter case it is shown that the proposed technique clearly outperforms the traditional RWA approach, minimizing the in-band channel interactions based on the available wavelengths. Thus, with the proposed approach the attack is contained, and it is not allowed to propagate extensively in the network, resulting in degradation of the established network connections.

6   Conclusions

This work proposed an algorithm for solving the RWA problem during the design phase of a transparent WDM optical network with the objective of minimizing the high-power in-band crosstalk propagation which is caused when a high-power jamming signal is maliciously introduced in the network at a specific network node. A meta-heuristic approach based on the harmony search technique is utilized to obtain

an ordering of the connection requests and this ordering is used during the RWA algorithm to establish all requested connections in the network. Performance results indicate that the proposed solution outperforms the traditional RWA technique that does not account for the propagation of the jamming signal due to intra-channel crosstalk, significantly minimizing this propagation in the network and thus drastically containing the effect of the attack on the network infrastructure.

Current ongoing research work on this subject focuses on the effects of inter-channel crosstalk attack propagation, as well as on the design of integer linear programming (ILP) formulations for the RWA problem, aiming at minimizing the attack propagation.

References

1. Ramaswami, R., Sivarajan, K.,: Routing and wavelength assignment in all-optical networks, IEEE/ACM Transactions on Networking, 3 (5), 489-500 (1995)
2. Haijin, Z., Naifu, Z.,: Ant colony optimization for dynamic RWA in WDM networks with partial wavelength conversion, J. Photonic Network Communications, 11 (2), 229-236 (2006)
3. Monoyios, D., Vlachos, K.,: Multiobjective genetic algorithms for solving the impairment-aware routing and wavelength assignment problem, IEEE/OSA Journal of Optical Communications and Networking, 3 (1), 40-47 (2010)
4. Martins-Filho, J., Chaves, D., Bastos-Filho, C., Aguiar, D.,: Intelligent and fast IRWA algorithm based on power series and Particle Swarm Optimization, in: Proc. of International Conference on Transparent Optical Networks, Athens, Greece, (2008)
5. Geem, Z.W., Kim, J.H., Loganathan, G.V.,: A new heuristic optimization algorithm: Harmony search, Simulation, 76 (2), 60–68 (2001)
6. Médard, M., Marquis, D., Barry, R., Finn, S.,: Security issues in all-optical networks, IEEE Network, 11 (3), 42-48 (1997)
7. Mas, C., Tomkos, I., Tonguz, O.,: Optical networks security: A failure management framework, in: Proc. of SPIE ITCom, pp. 230-241, Orlando, FL, USA, (2003)
8. Skorin-Kapov, N., Chen, J., Wosinska, L.,: A new approach to optical networks security: Attack-aware routing and wavelength assignment, IEEE/ACM Transactions on Networking, 18 (3), 750–760 (2010)
9. Furdek, M., Skorin-Kapov, N., Grbac, M.,: Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation, IEEE/OSA Journal of Optical Communications and Networking, 2 (11), 1000–1009 (2010)
10. Skorin-Kapov, N., Furdek, M., Pardo, R., Pavón Mariño, P.,: Wavelength assignment for reducing in-band crosstalk attack propagation in optical networks: ILP formulations and heuristic algorithms, European Journal of Operational Research, 222 (3), 418-429 (2012)