Providing Confidentiality in Optical Networks: Metaheuristic Techniques for the Joint Network Coding-Routing and Spectrum Allocation Problem

G. Savva, K. Manousakis, and G. Ellinas
Department of Electrical and Computer Eng. and KIOS CoE, University of Cyprus, 1678 Nicosia, Cyprus
e-mail: savva.giannis@ucy.ac.cy

ABSTRACT
In this work, novel metaheuristic algorithms are proposed to address the network coding (NC)-based routing and spectrum allocation (RSA) problem in elastic optical networks, aiming to increase the level of security against eavesdropping attacks for the network’s confidential connections. A modified simulated annealing, a genetic algorithm, as well as a combination of the two techniques are examined in terms of confidentiality and spectrum utilization. Performance results demonstrate that using metaheuristic techniques can improve the performance of NC-based RSA algorithms and thus can be utilized in real-world network scenarios.

Keywords: security, routing and spectrum allocation, network coding, simulated annealing, genetic algorithms.

1. INTRODUCTION
Connection provisioning in elastic optical networks (EONs) considers the problem of routing and spectrum allocation (RSA), which includes the routing (R - finding a path) and the spectrum allocation (SA) for a given set of demands [1]. A feasible solution to the RSA problem must satisfy the spectrum continuity constraint (a demand must be allocated on the same frequency slots across all links of its path), the non-overlapping constraint (a frequency slot on a given link is allocated to one demand at a time), and the spectrum contiguity constraint (the frequency slots used to serve a demand must be contiguous). To provide security against eavesdropping attacks in EONs, several techniques can be used, such as spread spectrum [2] and network coding (NC) [3], in combination with appropriate RSA algorithms that must be solved to ensure that attackers cannot make sense of accessed confidential information. Specifically, solving the combined NC-RSA problem now requires that two additional constraints must be satisfied: encrypted transmission (ET – confidential data streams must undergo at least one XOR operation with other established connections on all links of the confidential connection’s path), and frequency slot matching (FSM - at least a subset of the frequency slots utilized by a confidential connection must have the same id with the frequency slots of the established connections used in the XOR operations). To satisfy the ET constraint, it is enough to show that two paths that participate in the XOR process share at least two nodes that are traversed in the same order.

This work focuses on implementing metaheuristics to the NC-RSA heuristic presented in [3], in order to enhance the solutions obtained in terms of the level of confidentiality provided and the network’s resource efficiency.

2. SECURITY VIA NETWORK CODING
With network coding, different data streams transmitted in the network can be combined to implement diverse network functionalities including protection, security, and multicasting [4]. In terms of security (confidentiality in this case), this is achieved by combining data streams from different connections, preventing an attacker from making sense of accessed information. Figure 1 depicts an example of NC-based RSA in EONs, with 4 connections that must be allocated in the network, and a set of 3 candidate paths for each connection, as shown in the table below [Fig. 1(a)]. For simplicity, the assumption is that connections c2, c3, and c4 require 2 spectrum slots regardless of the path selected, while connection c1 requires 3 spectrum slots and is designated as confidential.

| id | s | d | Candidate Paths |
|----|---|---|-----------------|
| 1  | 1 | 3 | {1 – 2 – 3}, {1 – 4 – 3}, {1 – 4 – 5 – 3} |
| 2  | 4 | 6 | {4 – 5 – 6}, {4 – 5 – 3 – 6}, {4 – 3 – 6} |
| 3  | 1 | 6 | {1 – 4 – 5 – 6}, {1 – 2 – 3 – 6}, {1 – 4 – 3 – 6} |
| 4  | 1 | 3 | {1 – 4 – 3}, {1 – 2 – 3}, {1 – 4 – 5 – 3} |

Figure 1: (a) Table of connection requests and paths calculated; (b), (c) Two possible NC-RSA solutions.
One solution to the NC-RSA problem could be the one shown in Fig. 1(b), where connections $c_1$, $c_2$, $c_3$, and $c_4$ are allocated to paths $\{1-2-3\}$, $\{4-5-6\}$, $\{4-5-6\}$, and $\{1-4-3\}$ and spectrum slots 1–3, 1–2, 3–4, and 1–2, respectively. In this case, only $c_4$ can be used to secure the confidential demand $c_1$, since data on all links of $c_1$ can only undergo an XOR operation with $c_4$’s data and connection $c_4$ is allocated at partially the same spectrum slots as $c_1$. Hence, the confidential data stream $b_1 \oplus b_4$ will be transmitted on $c_1$’s path ($b_1$ and $b_4$ are the data streams transmitted by connections $c_1$ and $c_4$, respectively), i.e., the eavesdropper must access both $c_1$ and $c_4$, routed through different parts of the network, to make sense of the confidential data stream $b_1$.

The solution described above satisfies both ET and FSM constraints for the confidential connection. However, a different path selection and spectrum allocation could potentially significantly increase the level of security for $c_1$. For example, even in this simple scenario, if connections $c_1$, $c_2$, $c_3$, and $c_4$ were established on paths $\{1-4-3\}$, $\{4-5-3-6\}$, $\{1-2-3-6\}$, and $\{1-2-3\}$, and on spectrum slots 1–3, 1–2, 3–4, and 1–2, respectively [Fig. 1(c)], both ET and FSM constraints will be again satisfied for $c_1$. However, in this case, data streams $b_1 \oplus b_2 \oplus b_3 \oplus b_4$ will be transmitted through links 1–4 and 4–3, respectively, thus significantly increasing the level of security for $c_1$, as at least three diverse connections must be accessed to now compromise data stream $b_1$.

3. NC-RSA METAHEURISTIC ALGORITHMS
In this work, a series of metaheuristic algorithms are proposed that solve the NC-RSA problem in EONs in order to provide security for the confidential connections. For the non-confidential connections, the typical RSA constraints must be satisfied, while for the confidential connections, the ET and FSM constraints must also be taken into consideration. As demonstrated above, the paths (and spectrum slots) used to establish each connection can significantly affect the solution to this problem; this is also potentially true for the order in which demands are provisioned, signifying that metaheuristic techniques could improve the results obtained in [3]. In order to investigate this, three different metaheuristic algorithms are considered in this work for solving the NC-RSA problem: (i) Modified simulated annealing (SA), (ii) Genetic algorithm (GA), and (iii) Hybrid SA-GA. For each s-d pair, a set of \( k \) candidate paths is found, which is also the search space of the metaheuristics. Also, a simpler version of the heuristic algorithm presented in [3] is now utilized as the fitness function as described below.

3.1 Heuristic Algorithm – Fitness Function
The heuristic algorithm that was proposed in our previous work [3] is utilized as the fitness function to solve the NC-RSA problem and establish all connections in the network. Specifically, each non-confidential connection is provisioned in the first group of available spectrum slots (first-fit policy) using a pre-designated path selected by the metaheuristic algorithm. For each confidential connection, the minimum number of XOR operations performed over all links of the connection is calculated (denoted as XOR-SSM), and the spectrum slots that maximize this metric are selected (only the connections that share at least a subset of frequency slot ids are considered in each case to account for the FSM constraint), utilizing a path that was pre-selected by the metaheuristic. It is noted that the XOR-SSM metric must be greater than a given threshold \( T \) to accept a connection (satisfying constraint ET and thus considered secured); otherwise, the connection is rejected. Further, if XOR-SSM is the same for two sets of spectrum slots, the one that maximizes the average number of XOR operations (over all path links) is selected. By evaluating a given solution, based on the minimum number of XOR operations, the connection is evaluated based on its “weakest” link (i.e., the link having the least number of XOR operations). The heuristic function returns the average number of minimum XOR operations over all confidential demands.

3.2 Metaheuristic Algorithms
Metaheuristic techniques are a good fit to the NC-RSA problem, since the order and selection of inputs play a crucial role to the problem’s solution. The proposed techniques change the input at each iteration (order of demands and/or paths used), with the fitness function (heuristic) each time evaluating the set of inputs. This process is repeated until a specified threshold is met. In the sections that follow, different metaheuristic techniques are described and compared.

3.2.1 Modified Simulated Annealing (SA)
The proposed SA starts with a specific ordering of the connection requests and a selection of the most efficient paths for each request (calculated using the hybrid metric presented in [5]). Then, the average minimum number of XOR operations is calculated using the heuristic, and if this value is greater than the current best solution, the best solution is updated [6]. This modified SA technique consists of two sets of variables: the order of demands and the path selected for each demand. Thus, in this case, to find a new solution, the order of the demands can be interchanged, while the path selection variables can be set to any random value ranging from 1 to \( k \). The number of changes at each iteration is performed \( \text{temperature} \) times, where for each change either the order of demands is interchanged or a path is changed for a randomly selected demand. Then, after each iteration, \( \text{temperature} \) is reduced to \( (\text{temperature} \times \epsilon) \) and this process is repeated until \( \text{temperature} \) is lower than a threshold \( \epsilon \). To better
illustrate how the SA approach is structured, Fig. 2 presents two possible configurations of a solution, for 5 connections to be provisioned and 3 candidate paths per connection (i.e., \( k = 3 \)).

Figure 2. Example of an SA solution structure and a process to obtain a new solution (5 connections, \( k = 3 \)).

3.2.2 Genetic Algorithm (GA)

GAs emulate “survival of the fittest” by using evolutionary biology techniques such as natural selection, crossover, and mutation [7]. Each possible solution (i.e., chromosome) is represented by a set of genes (i.e., variables) and all chromosomes constitute a population. In this work, a random set of individual chromosomes is initialized with a random demand ordering and a random path selection (this is the initial population). Each gene is represented by a value \( x.y \), where \( x \) refers to the demand id and \( y \) represents the path selected for that demand. Thus, the order of the genes represents the order of demands that the heuristic will use as input. For the crossover operation, a constrained probabilistic approach is followed, where a random point in the genes is selected and the crossover shown in Fig. 3 is utilized so that each new gene is a possible solution to the NC-RSA problem (e.g., each demand id is used only once). Further, for the mutation operation, either the order of two genes is interchanged, or a path (i.e., \( y \)) is randomly selected for a randomly selected gene. Each chromosome’s fitness function is evaluated again using the heuristic approach, and for the selection process the roulette wheel is utilized [7], where the probability of each chromosome being added to the next generation is based on the result of its fitness function. Finally, it is noted that an elitist step takes place, where the worst chromosome is replaced by the best chromosome of the given population, in order to increase the probability for a better solution as the algorithm progresses. Figure 3 illustrates these steps for an example of 5 connections with \( k \) equal to 3.

Figure 3. Example of a chromosome structure, crossover, and mutation operations (5 connections, \( k = 3 \)).

3.2.3 Hybrid SA – GA

The hybrid algorithm proposed uses a combination of the SA and GA techniques to examine whether a combined solution will provide better results. Specifically, in this case the GA approach changes the path selected for each demand, while the SA approach modifies the demand ordering. First, a run of the GA is performed to find a set of paths that maximizes the average number of minimum XOR operations for the initial demand order. Then, the SA approach uses this set of paths and changes the order of demands, such that a demand ordering that offers better results is obtained. Then, after a specified number of SA iterations, a run of the GA algorithm takes place again, using the current best demand ordering found by the SA. It is noted that the chromosome that gave the best solution in run \( j \) of the GA, is copied random times (with values ranging from 5 to 10) in run \( j+1 \), in order to ensure continuity within the metaheuristic during its operation. Finally, this process is repeated until a threshold is met by the SA.

4. PERFORMANCE EVALUATION

The simulation setup and the parameters used in the metaheuristics are presented in Table 1. All chosen parameters for the metaheuristic approaches were selected based on several simulations. It is noted that for the hybrid case, the number of generations and population size are changed to 400 and 80, respectively, and the GA is performed every 30000 iterations. These values are used in order to reduce the running times of the hybrid approach, since the GA technique will be performed several times during the operation of SA. Also, in all cases, 500 demands are randomly generated using a uniform distribution with a bit rate ranging from 20 to 120 Gbps. Further, 10% of the demands are designated as confidential with a threshold of minimum XOR operations equal to 1. Each simulation is performed 5 times and the results of the best solution (highest fitness function), in terms of the average of the minimum number of XOR operations, are presented in Fig. 4(a), followed by the spectrum utilization and running times for each technique using different values of \( k \) [Fig. 4(b) and 4(c)].
Table 1. Simulation parameters.

| Network Characteristics/Parameters | SA Parameters | GA Parameters |
|-----------------------------------|---------------|---------------|
| Topology: NSF (14 nodes, 42 links) | Starting Temperature: 50 | Number of Generations: 4000 |
| Channel Spacing: 12.5 GHz | a: 0.999943 | Population size: 100 |
| Baud rate: 10.7 Gbaud | ε: 0.01 | Probability of mutation: 0.05 |
| Modulation Format: 16-PSK (d≤800km) | – | Probability of crossover: 0.3 |
| *(d – path length)* | 8-PSK (800<d≤1700km) | – |
| QPSK (1700<d≤4600km) | – | – |
| BPSK (4600<d≤9300km) |

As shown in the figures, all algorithms achieve an (averaged) minimum number of XOR operations that exceeds the required threshold for their confidential connections (note that for all techniques zero blocking was also observed). Nevertheless, the modified SA technique achieves the best results in terms of level of provided security, spectrum utilization, and running times, while the hybrid SA-GA technique outperforms the GA approach. Specifically, the modified SA can provide increased confidentiality utilizing far less spectrum resources compared to the other two approaches (~600 fewer spectrum slots), with a much faster running time. This is due to the simplicity of the SA metaheuristic, since the algorithm takes as input the most efficient solution in terms of spectrum resources, makes a number of changes, evaluates the new solution and repeats this process; this is contrary to the GA and hybrid SA-GA techniques, where several steps (i.e., crossover, mutation, selection) take place for each generation, prior to the evaluation of the solution for each chromosome.

5. CONCLUSIONS

In this work, three different metaheuristic approaches were investigated for the NC-RSA problem. Utilizing a modified SA approach, an efficient resource utilization solution is obtained that also maximizes the level of security for the confidential connections, with a much faster running time compared to the other proposed techniques. Currently, an ILP formulation and an enhanced SA metaheuristic are being considered, aiming to increase the level of confidentiality for the network’s connections that have specific security requirements.

ACKNOWLEDGEMENTS

This work was supported by the European Union’s Horizon 2020 research and innovation programme under grant agreement No 739551 (KIOS CoE) and from the Government of the Republic of Cyprus through the Directorate General for European Programmes, Coordination and Development. It was also supported by the Cyprus Research and Innovation Foundation under project CULTURE/AWARD-YR/0418/0014 (REALFON).

REFERENCES

[1] K. Christodouloupolous et al., “Routing and spectrum allocation in OFDM-based optical networks with elastic bandwidth allocation,” in Proc. IEEE GLOBECOM, 2010.
[2] G. Savva et al., “Eavesdropping-aware routing and spectrum/code allocation in OFDM-based EONs using spread spectrum techniques,” IEEE/OSA J. Opt. Commun. Netw., vol. 11, no. 7, pp. 409-421, 2019.
[3] G. Savva et al., “Network coding for security against eavesdropping attacks in elastic optical networks,” in Proc. ONDM, 2019.
[4] E. Manley et al., “All-optical network coding,” IEEE/OSA J. Opt. Commun. Netw., vol. 2, no. 4, pp. 175-191, 2010.
[5] G. Savva et al., “Physical layer-aware routing, spectrum, and core allocation in spectrally-spatially flexible optical networks with multicore fibers,” in Proc. IEEE ICC, 2018.
[6] S. Kirkpatrick et al., “Optimization by simulated annealing,” Science, vol. 220, no. 4598 pp. 671-680, 1983.
[7] A. E. Eiben and J. E. Smith, “Introduction to Evolutionary Computing,” Second ed., Springer, 2016.