Network Coding for Security Against Eavesdropping Attacks in Elastic Optical Networks

Giannis Savva, Konstantinos Manousakis, Georgios Ellinas

Network Coding for Security against Eavesdropping Attacks in Elastic Optical Networks

Giannis Savva, Konstantinos Manousakis, and Georgios Ellinas

KIOS CoE and Department of Electrical and Computer Engineering, University of Cyprus, 1678 Nicosia, Cyprus, gsavva07@ucy.ac.cy

Abstract. In this work, routing and spectrum allocation (RSA) algorithms together with network coding (NC) are proposed for elastic optical networks. NC has been used in optical networks for protection against link failures and also in multicasting to improve spectral efficiency. In this work, NC is used to protect confidential connections against eavesdropping attacks. The confidential signals are XOR-ed with other signals at different nodes in their path while transmitted through the network. These signals can be combined either at the source node and/or at intermediate nodes. To implement NC for confidential connections, a set of constraints for the NC problem in addition to the constraints of the RSA problem are incorporated to the algorithms. The combination of signals through network coding significantly increases the security of confidential connections, since an eavesdropper will receive a combination of signals from different connections, making it extremely difficult for the confidential signal to be decrypted. A number of RSA strategies are examined in terms of confidentiality, spectrum utilization, and blocking probability. Performance results demonstrate that network coding provides an additional layer of security for confidential connections with only a small increase in the spectrum usage.

1 Introduction

Elastic optical networks (EONs) based on orthogonal frequency division multiplexing have been proposed to address the growth of traffic in backbone networks. EONs can handle traffic demands more efficiently than wavelength division multiplexed (WDM) networks due to the orthogonality of the spectrum slices used. In EONs, the C-band can be separated in slices (frequency slots) of 25, 12.5, and 6.25GHz. Therefore, each requested connection can be allocated to a number of spectrum slots in order to be established in the network [1].

In order to solve the routing and spectrum allocation (RSA) problem in EONs and establish a connection for a given demand, the following three constraints must be satisfied: (i) the *spectrum continuity constraint* - each demand must be allocated to the same frequency slots (FS) on each link of the selected path, (ii) the *non-overlapping constraint* - a frequency slot can only be allocated to one

demand at a time, and (iii) the *spectrum contiguity constraint* - the frequency slots serving each demand must be contiguous [2].

In EONs, even short attacks can still compromise large amounts of data leading to serious security issues. For this reason, optical layer security (OLS) has received considerable attention in the last few years. Security threats for optical networks include the observation of the existence of communications (privacy), the unauthorized use of spectrum (authentication), the manipulation or destruction of data (integrity), denial of service (availability), and unauthorized access to information (confidentiality) [3–5]. In this work, the focus is on confidentiality, where an adversary tries to make sense of accessed confidential data from an optical communication channel (eavesdropping). For example, in optical networks, an attacker can eavesdrop by physically tapping into the optical fiber or by observing the crosstalk interference emitted in adjacent spectrum by confidential signals [4, 6], and can potentially go undetected for a prolonged period of time.

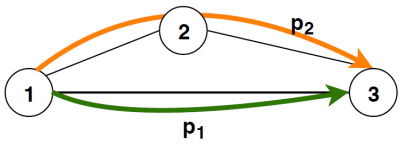
Authors in [7] utilize network coding for multicasting connections to improve network throughput. In [8] authors propose a proactive protection scheme that combines both the advantages of EONs and NC, in order to enable network resilience against optical link failures while also reducing the optical spectrum utilization. Further, authors in [9] study the effectiveness of linear network coding (LNC) in optical networks to protect connections from security threats such as eavesdropping and jamming attacks. In [10], authors propose an eavesdropping-aware RSA algorithm where demands use several paths to establish a connection based on the probability of eavesdropping. This probability however cannot be always known. In [11] authors propose an RSA algorithm with a spectrum reallocation technique to increase security in EONs, while work in [12], [13] focused on the development of algorithms for the enhancement of physical layer security by using spread spectrum techniques over EONs. These works, however, require additional spectrum resources to establish all connections.

In this work, the focus is again on security against confidential attacks in EONs, but this time novel RSA algorithms are proposed in combination with network coding. New constraints are defined to implement NC and are used as additional constraints to the RSA problem. To the best of our knowledge, this is the first time that NC has been integrated with RSA in order to provide security against eavesdropping attacks in EONs. When NC is utilized, it is extremely difficult for the attacker to compromise any confidential connection, since a number of different connections that traverse several routes will have to be compromised, in order for the attacker to make sense of the accessed confidential data.

The rest of the paper is organized as follows. NC in optical networks is discussed in Section 2, followed by the problem description in Section 3. Then, the proposed algorithm that uses NC during the solution of the RSA problem is presented in Section 4, followed by the performance results in Section 5. Finally, Section 6 concludes the paper.

2 The concept of network coding in optical networks

In NC, to enhance network security, a confidential connection can transmit an encrypted version of its data by combining it (via an XOR operation) with other co-propagated connections. Thus, in the case of an eavesdropping attack, the attacker must have knowledge of both the encrypted version of the signal and the co-propagated connections used to perform the XOR operations in order to decrypt the confidential data. It is important to note that very few works study the concept of NC for security in optical networks [9] and none considers jointly solving the NC and RSA problems.



Connection id	Requested datastream	Transmitted datastream
p_1	b_1	$b = b_1 \oplus b_2$
p_2	b_2	b_2

Fig. 1. Example of network coding involving two connections.

Fig. 1 presents a simple example where NC can be used to secure a confidential demand (connection p_1). In this example, it is assumed that connection p_1 is allocated spectrum slots 1 - 3 on path 1 - 3 and the requested datastream is represented as b_1. Also, connection p_2 transmits datastream b_2 through path 1 - 2 - 3. To provide confidentiality for connection p_1, source node 1 transmits an encrypted version of the datastream, denoted as b, where $b = b_1 \oplus b_2$, while connection p_2 transmits datastream b_2. This way, even if an adversary eavesdrops on any intermediate link along the path of confidential connection p_1, confidential data cannot be decrypted, since, in this example, the eavesdropper must also gain access to connection p_2 and datastream b_2. In this case, since both connections have the same destination, node 3 can acquire both b and b_2 signals and therefore the XOR operation can be performed between the two datastreams ($b \oplus b_2 = b_1$) to decrypt datastream b_1. Note that in this work the assumption is that an attacker can gain access to the signals by tapping individual links but cannot access the signals at network nodes as these are securely placed within the telecom providers' sites.

In opaque optical networks, the process of NC could be easily implemented, since optical signals can be received, combined, and transmitted at intermediate nodes. However, for such a technique to work in transparent optical networks, the nodes must be equipped with additional hardware in order to perform the XOR operation at the physical layer. In addition, the involved signals must use the same spectrum resources in order for NC to be enabled. Thus, the deployment of NC schemes in EONs assumes the usage of all-optical XOR gates. A review of all-optical XOR gate technology has been performed in [14]. All-optical XOR

gates are typically based on semiconductor optical amplifiers and the execution of XOR operations can be performed at line speed for transmissions up to 100Gbps, with different modulation schemes, signifying that a practical implementation of optical XOR operations for processing optical signals is indeed possible [15].

3 Problem description

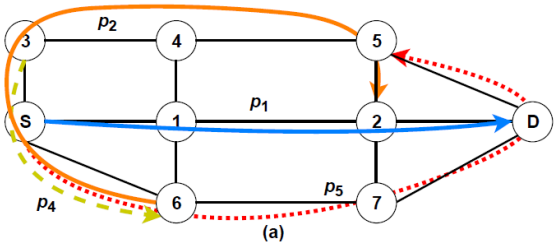
In this work, the problem of routing and spectrum allocation and network coding is jointly solved in EONs so as to also offer security for confidential demands against eavesdropping. Using NC, each confidential connection combines its data with the data from other connections and designs a network code that changes based on the data that the aforementioned connections transmit. In this work, in order for a confidential connection to be considered secure, its data must be combined with the data of other connections in the same spectrum slots in each of the links that the confidential connection traverses. Specifically, the following additional constraints must now be satisfied when solving the combined NC-RSA problem to ensure security against eavesdropping for a confidential demand:

- **Encrypted Transmission (ET)**: All links of the selected path must transmit an encrypted version of their data with at least one XOR operation with other established connections.
- **Frequency Slot Matching (FSM)**: At least a subset of the frequency slots utilized by the confidential connection must have the same id with the slots of the rest of the established connections used in the XOR operations.

To satisfy the ET constraint, an established connection must have at least two common nodes with the confidential connection (the first node will be used to encrypt the confidential connection and the second node will be used to decrypt it). Thus, an established connection with at least two common nodes with the confidential connection can either provide security for the entire path of the confidential demand (source and destination as common nodes), or it can provide security for part of the connection (source/intermediate node to intermediate/destination node). For a confidential connection to be considered secure, the selected established connections must collectively secure all links of that connection.

To satisfy the FSM constraint, at least a subset of the frequency slots utilized by the confidential connection must have the same id with the frequency slots of the rest of the established connections used in the XOR operations. This is the case, since it is assumed that no frequency conversion is performed at intermediate nodes, and therefore, the signals used for the XOR operation must be on the same frequency. However, the confidential connection is considered as secure even if only part of the signal is XOR-ed, since the eavesdropper would still have to access all connections used in the encryption process in order to decrypt the transmitted data.

Fig. 2 illustrates an example where several connections can be used in order to secure a confidential demand, extending the simple example shown in Fig. 1.



(a)

Connection id	Representation in figure	Frequency slots used
p_1		1 - 6
p_2		1 - 3
p_3		4 - 7
p_4		1 - 2
p_5		3 - 8

(b)

Link	Transmitted signal
S - 1	$c = p_1 \oplus p_2 \oplus p_5$
1 - 2	$c = p_1 \oplus p_2 \oplus p_3 \oplus p_5$
2 - D	$c = p_1 \oplus p_3 \oplus p_5$

(c)

Fig. 2. Example of NC in a 9-node network topology utilizing 5 connections.

In this example, it is assumed that connections p_2, p_3, p_4 and p_5 are currently established in the network (Fig. 2(a)) using paths 6 - S - 3 - 4 - 5 - 2, 1 - 4 - 5 - D, 3 - S - 6, and S - 6 - 7 - D - 5, respectively. Also, for simplicity, assume that each connection is assigned to the frequency slots shown in Fig. 2(b). For provisioning confidential connection request p_1, it is assumed that the S - 1 - 2 - D route is selected, along with spectrum slots 1 - 6. Since p_2 is utilized on part of the same frequency slots and has two common nodes with p_1, it can be used to encrypt the confidential signal by enabling NC on node S and decrypting the signal at node 2, providing security for links S - 1 and 1 - 2. Similarly, connections p_3 and p_5 can be further used to encrypt p_1. Note that p_4 cannot be utilized to encrypt connection p_1, since connections using routes p_1 and p_4 have only one node in common. The transmitted signals along all links of connection p_1 are presented in Figure 2(c).

As previously mentioned, in this work, a confidential connection is considered secure if it satisfies constraints ET and FSM, which is the case in this example. Also, it is noted that all spectrum slots are XOR-ed at links S - 1 and 1 - 2, whereas only a part of the signal (frequency slots 3 - 6) is XOR-ed at link 2 - D. Nevertheless, the connection is still considered as secure, since an eavesdropper would still have to access the signal of all individual connections used at each link (i.e., p_1, p_3, and p_5 for link 2 - D) in order to decrypt confidential data.

4 RSA with network coding

The proposed NC-RSA algorithm is divided into the routing and spectrum allocation sub-problems. A network planning scenario is considered, where all demands are known a priori and each demand is described by a 4-tuple (s,d,B,c), denoting the source, destination, bit-rate, and confidentiality, respectively. Confidentiality in this case is defined as a binary variable which describes the demand as confidential (1) or non-confidential (0).

4.1 Routing

For the routing sub-problem, k-shortest candidate paths that are able to satisfy a requested connection are found. These k-shortest paths can be subsequently sorted based on a number of metrics, such as the number of hops, the modulation format, or the most/least used nodes/links. Also, different routing strategies can apply for the confidential and the non-confidential connections. Specifically, in this work, each node (n) and link (l) are characterized by the number of established connections that use them (denoted as U_n and U_l respectively). Further, each path takes the value of the node/link with the highest U_n/U_l among all the nodes/links it traverses ($U_{p,n}, U_{p,l}$). The paths of the non-confidential connections can then be sorted based on the following three criteria:

- **Most used nodes/links (MUN/MUL)**: The candidate paths for each s-d pair are sorted in descending order based on the value $U_{p,n}/U_{p,l}$ of each path. By selecting the path which comprises of the most used nodes/links, the number of XOR operations for a confidential connection will potentially increase.
- **Least used nodes/links (LUN/LUL)**: In this case, the candidate paths of each connection are sorted in ascending order based on the value $U_{p,n}/U_{p,l}$. Thus, the connections will be distributed in the network in a balanced manner, and therefore confidential connections will more likely find paths that satisfy the NC constraints.
- **Maximum spectrum efficiency (MSE)**: The candidate paths are sorted in descending order based on the number of hops and the modulation format used (hybrid metric [16]). Thus, connections are established having as an aim to maximize the spectrum efficiency of the network rather than maximizing the number of XOR operations.

After sorting the paths, the non-confidential connections are established using the first path that has available spectrum resources, based on one of the three aforementioned sorting strategies. For the confidential connections, the candidate path that produces the most number of XOR operations is used, which also depends on the spectrum slots selected. To achieve this, the XOR spectrum slot metric (XOR-SSM) is introduced that counts the minimum number of XOR operations that can be performed on each link for the selected group of frequency slots. Thus, for each candidate path, XOR-SSM is calculated, and the path and frequency slots that provide the highest XOR-SSM are used to establish the confidential connection.

4.2 Spectrum Allocation

For the spectrum allocation sub-problem, available spectrum resources must be allocated for a requested connection satisfying the slot *continuity*, *contiguity*, and *non-overlapping* constraints [2]. For the non-confidential connections, the spectrum allocation is performed in a first-fit manner, where the first group of

frequency slots from the sorted candidate paths that is able to establish the connection is allocated.

For the confidential connections, the process of allocating spectrum resources is based on maximizing the number of XOR operations that can be performed for the selected path and group of frequency slots, utilizing the XOR-SSM metric. Algorithm 1 describes the NC-RSA approach for a given confidential demand. Also, the example in Fig. 3 is subsequently used to better explain the proposed algorithm.

Algorithm 1 NC-RSA for a given confidential demand

Input: $G(V, E)$, *Candidate paths* P, *Paths currently established* P_e, *Confidential demand* D $(s, d, B, 1)$

Output: Connection Establishment

1: **for** each candidate path $p \in P_{s,d}$ **do**
2: Find a set of paths $P_{used} \in P_e$ that are used by the established connections and have at least two common nodes with path p
3: Create temporary matrix $t = L \times F$, where L = number of links in path p and F = overall number of freq. slots. Initialize all matrix entries to 0.
4: **for** each path $p_u \in P_{used}$ **do**
5: Calculate the set of links in p that can be covered by p_u and increase by one the values for the links and spectrum slots that are covered by p_u within t
6: **end for**
7: Initialize XOR-SSM$_p = 0$
8: **for** each group $(a - b)$ of available spectrum slots in p that can be allocated to D **do**
9: $c_z^{a-b} = \sum_{n=a}^{b} t_{z,n}$, for $z = 1$ to L
10: $\mathcal{C}^{a-b} = min(c_1^{a-b}, ..., c_L^{a-b})$
11: XOR-SSM$_p = max$(XOR-SSM$_p, \mathcal{C}^{a-b}$)
12: **end for**
13: **end for**
14: Select p with max XOR-SSM$_p$ and establish connection

For a given confidential connection, the XOR-SSM$_p$ is calculated for each candidate path p. To do this, a temporary matrix (denoted as t in the algorithm) is used, with size $L \times F$, where L denotes the number of links of the candidate path and F denotes the overall number of frequency slots of each link in the network. Next, the set of the already established paths with at least two common nodes with the path under investigation is found (denoted as P_{used} in the algorithm). This set of paths can be used to satisfy the ET constraint. Subsequently, the values for the links and spectrum slots that are covered by p_u within t are increased by 1.

Next, for each available group of frequency slots $(a - b)$, the number of XOR operations performed on each link z of path p are calculated using the following equation: $c_z^{a-b} = \sum_{n=a}^{b} t_{z,n}$, where a and b are the starting and ending slots selected. From these computed values the minimum $\mathcal{C}^{a-b} = min(c_1^{a-b}, ..., c_L^{a-b})$

is selected (i.e., the weakest link in terms of the number of XOR operations performed to secure that link is considered). Then, for path p, the group of frequency slots with the maximum $\mathcal{C}$ is selected and is considered as the value of XOR-SSM for that path. The value of the XOR-SSM metric signifies that for any value greater than zero (i.e., x), at least x XOR operations are used to secure the confidential connection in each link. This also implies that the ET and FSM constraints are satisfied for that confidential connection. On the other hand, if XOR-SSM is zero, there is at least one link in the path where none of the spectrum slots utilized can be XOR-ed, and therefore the connection is not considered secure. Finally, when the XOR-SSM is the same for two candidate paths, the one with the least number of hops is selected, so as to increase spectrum efficiency whenever possible.

In Fig. 3, assume a network with F =5, candidate path p_4 requiring 3 frequency slots, and set P_{used} consisting of paths $\{p_1,p_2,p_3\}$, where each connection is allocated spectrum slots as shown in Fig. 3(a). The resulting t using all paths in P_{used} is shown in Fig. 3(b) (for example, p_1 contributes to cells $t_{(1,3)}$, $t_{(1,4)}$, $t_{(2,3)}$, $t_{(2,4)}$, since it can cover spectrum slots 3 and 4 in both links in p_4). To calculate the number of XOR operations on link 2, if the group of frequency slots selected is $3-5$, $c_2^{3-5}= t_{(2,3)} + t_{(2,4)} + t_{(2,5)}= 1 + 2 + 1 = 4$. The results for each link and group of spectrum slots are presented in Fig. 3(c). Also, $\mathcal{C}^{2-4}= min(c_1^{2-4}, c_2^{2-4})= min(2, 3)= 2$, and $\mathcal{C}^{1-3}$ and $\mathcal{C}^{3-5}$ are equal to 1 and 3, respectively (Fig.3(d)). Thus, XOR-SSM$_{p_4}= max(\mathcal{C}^{1-3}, \mathcal{C}^{2-4}, \mathcal{C}^{3-5})= max(1, 2, 3) = 3$, using frequency slots $3 - 5$.

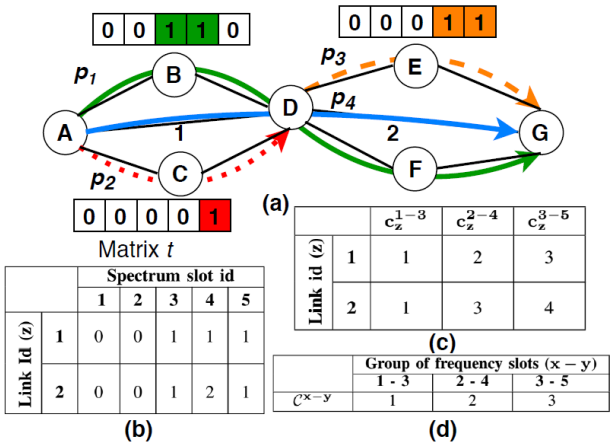


Fig. 3. Example of NC-RSA algorithm for a given confidential connection.

5 Performance evaluations

The simulation setup used to evaluate the proposed algorithms is as follows: an EON is implemented using bandwidth variable transponders that operate using multiple modulation formats: BPSK, QPSK, 8-QAM, and 16-QAM. The transmission reach for each modulation format is given by 9300, 4600, 1700, and 800 km respectively. Moreover, a flexible grid is implemented with channel spacing of 12.5GHz which results in a total of 320 spectrum slots for each link in the network with a baud rate of 10.7 Gbaud for each frequency slot. Further, the Telefonica network [17] with 30 nodes and 56 bidirectional links is used for all experiments. In all cases, demands are randomly generated using a uniform distribution for all s-d pairs, where each demand size varies from 10 to 100 Gbps. Also, 20 candidate paths are calculated offline for each s-d pair. It is noted that a large number of candidate paths is used so as to provide the confidential connections with several candidate paths that could maximize the XOR-SSM metric. Moreover, each presented result is the average of 10 experiments performed with different generated sets of demands. Finally, for all simulations, the number of demands designated as confidential is set to 40% of the overall number of requests.

First, the percentage of confidential connections that are securely established (have XOR-SSM metric greater than 1) is presented in Fig. 4 for the different sorting strategies of the candidate paths as described in Section 4. As shown in Fig. 4, using different sorting techniques has a significant effect on the number of confidential connections that can be provisioned securely in the network. Clearly, the MUN or MUL techniques provide much better results compared to the rest of the sorting techniques, since connections are forced to traverse the same node/links, and therefore, more connections with at least two common nodes can be found to perform the XOR operation with the confidential connection. Further, as shown from the results, the MUN approach outperforms MUL, with approximately 95% of the confidential connections securely established. The reader should note that for the established confidential connections that cannot be secured, extra (dummy) lightpaths can be added to accommodate the links where XOR operations are not performed just for the sole purpose of securing all confidential connections.

Next, Fig. 5 presents the blocking probability of the network when different sorting techniques are used. As shown in the figure, the MUL sorting approach provides the highest blocking probability compared to the rest of the techniques, since the paths chosen aim at using the most utilized links in order to increase security rather than maximizing the efficient use of spectrum resources. On the other hand, the MUN sorting strategy provides only 3% blocking probability for a large network load (1500 requests), while also providing security for almost all of the confidential demands.

To quantify the amount of security provided for the confidential connections, the number of XOR operations performed on each link of a confidential connection can be calculated. As discussed above, increasing the number of XOR operations performed on each link reduces the probability that an eavesdropper

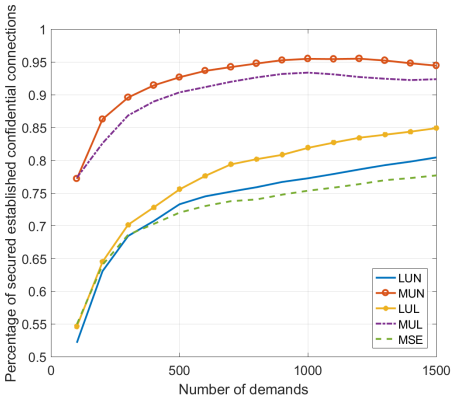


Fig. 4. Percentage of established confidential connections that are secured.

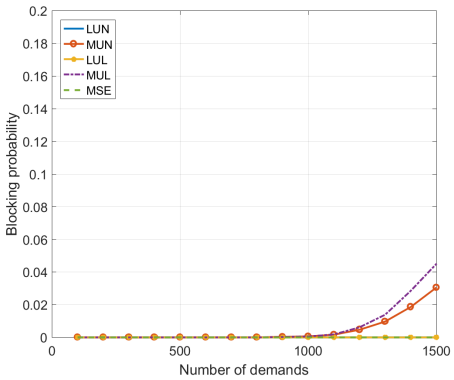


Fig. 5. Blocking probability using different sorting techniques.

can decrypt confidential data, since the eavesdropper would have to access, for each link of the confidential path, all connections that were used during the XOR process. Fig. 6 presents the average number of XOR operations per link per confidential connection in the network, when using different sorting techniques for the candidate paths.

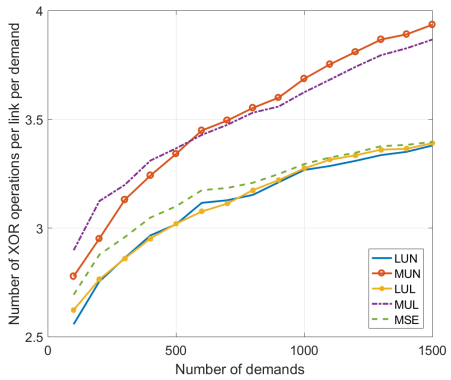


Fig. 6. Number of XOR operations per link per confidential connection.

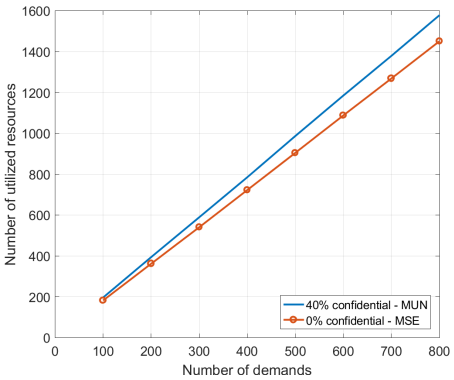


Fig. 7. Utilized spectrum resources for the MUN and MSE sorting techniques.

Using the MUN approach maximizes the number of XOR operations performed for each confidential connection compared to the rest of the sorting approaches. For MUN, up to 4 XOR operations can be performed on each link of a confidential connection, on average, compared to the least used and MSE cases, where 3.4 XOR operations are performed on each link. This means that, when MUN is utilized, an eavesdropper would have to simultaneously gain ac-

cess to information from 4 other connections that traverse different links and nodes in the network in order to decrypt the data traversing a single link of the confidential connection.

Selecting different routing and spectrum allocation strategies for each confidential connection will, on the one hand secure the confidential connections against an eavesdropping attack, but, on the other hand, could force the algorithm to deviate from an efficient spectrum utilization solution. Fig. 7 presents the number of utilized spectrum slots when using the MUN strategy, (which outperforms all other sorting approaches in terms of the number of XOR operations per confidential connection), versus the case where all connections are designated as non-confidential and the candidate paths are sorted based on the MSE technique (which maximizes spectrum efficiency). In this case, the blocking probability is set to 0% in order to obtain the exact number of spectrum resources utilized for each set of demands. As shown in the figure, the MUN sorting strategy requires more spectrum resources than MSE to establish all connections. This is to be expected and is mainly due to the usage of paths that maximize the number of XOR operations for the confidential connections, rather than using the best paths in terms of spectrum efficiency. Nevertheless, the number of additional spectrum resources required for securing the confidential connections is only slightly increased, compared to the case without any confidential requests.

6 CONCLUSIONS

In this work, a novel joint NC-RSA approach is presented in EONs to increase physical layer security against eavesdropping attacks. The proposed technique uses network coding to combine connections already established in the network with the confidential ones in order to transmit encrypted versions of their confidential data. Using this approach, an eavesdropper must now access multiple connections in the network in order to compromise any confidential information. The performance results obtained demonstrate that the MUN sorting approach for routing the candidate paths can be used to securely provision almost all (95%) of the confidential demands, while providing the best security against an eavesdropping attack with multiple connection combinations per link, and at the same time requiring only slightly increased spectrum resources, compared to the case where security is not taken into consideration. Future work will investigate routing techniques for minimizing the number of dummy lightpaths required to securely provision all confidential demands.

ACKNOWLEDGMENT

This work has been 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. This article is based

upon work from COST Action CA15127 (Resilient communication services protecting end-user applications from disaster-based failures RECODIS) supported by COST (European Cooperation in Science and Technology).

References

1. O. Gerstel, et al., "Elastic optical networking: A new dawn for the optical layer?", *IEEE Comm. Magazine*, 50(2):S12-S20, 2012.
2. K. Christodoulopoulos, et al., "Routing and spectrum allocation in OFDM-based optical networks with elastic bandwidth allocation", *Proc. IEEE Globecom*, 2010.
3. M.P. Fok, et al., "Optical layer security in fiber-optic networks", *IEEE Trans. Inf. Forensics Security*, 6(3):725-736, 2011.
4. N. Skorin-Kapov, et al., "Physical-layer security in evolving optical networks", *IEEE Comm. Magazine*, 54(8):110-117, 2016.
5. K. Manousakis, et al., "Attack-aware planning of transparent optical networks", *Optical Switching and Networking*, 19(2):97-109, 2016.
6. K. Kitayama, et al., "Security in photonic networks: Threats and security enhancement", *IEEE/OSA J. of Lightw. Techn.*, 29(21):3210-3222, 2011.
7. A. Agarwal, et al., "On the advantage of network coding for improving network throughput", *Proc. IEEE Inf. Theory Workshop*, 2004.
8. W. Ramirez, et al., "Network coding-based protection scheme for elastic optical networks," *Proc. DRCN*, 2014.
9. A. Engelmann et al., "Balancing the demands of reliability and security with linear network coding in optical networks," *Proc. IEEE ICC*, 2016.
10. W. Bei, et al., "Eavesdropping-aware routing and spectrum allocation based on multi-flow virtual concatenation for confidential information service in elastic optical networks", *Opt. Fiber Techn.*, 40:18-27, 2018.
11. S. K. Singh, et al., "Balancing data security and blocking performance with spectrum randomization in optical networks", *Proc. IEEE Globecom*, 2016.
12. G. Savva, et al.,"Eavesdropping-aware routing and spectrum allocation in EONs using spread spectrum techniques", *Proc. IEEE Globecom*, 2018.
13. G. Savva, et al., "Spread spectrum over OFDM for enhanced security in elastic optical networks", *Proc. IEEE PSC*, 2018.
14. M. Zhang, et al., "All optical XOR logic gates: Technologies and experiment demonstrations", *IEEE Comm. Mag.*, 43(5):S19-S24, 2005.
15. D. Kong, et al., "All-optical XOR gates for QPSK signal based optical networks", *Elect. Letters*, 49(7):486-488, 2013.
16. G. Savva, et al., "Physical layer-aware routing, spectrum, and core allocation in spectrally-spatially flexible optical networks with multicore fibers", *Proc. IEEE ICC*, 2018.
17. G. Savva, et al., "Connection provisioning in spectrally-spatially flexible optical networks with physical layer considerations", *Proc. ICTON*, 2018.