Network coding-based routing and spectrum allocation in elastic optical networks for enhanced physical layer security

Giannis Savva1 · Konstantinos Manousakis1 · Georgios Ellinas1

Received: 8 January 2020 / Accepted: 17 June 2020 / Published online: 6 August 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
In this work, an eavesdropping-aware routing and spectrum allocation approach is proposed utilizing network coding (NC) in elastic optical networks (EONs). To provide physical layer security in EONs and secure the confidential connections against eavesdropping attacks using NC, the signals of the confidential connections are combined (XOR-ed) with other signals at different nodes in their path, while transmitted through the network. The combination of signals through NC significantly increases the security of confidential connections, since an eavesdropper must access all individual signals, traversing different links, in order to decrypt the combined signal. A novel heuristic approach is proposed that solves the combined network coding and routing and spectrum allocation problem that also takes into account additional NC constraints that are required in order to consider a confidential connection as secure. Different routing and spectrum allocation strategies are proposed, aiming to maximize the level of security provided for the confidential demands, followed by an extensive performance evaluation of each approach in terms of the level of security provided, as well as the spectrum utilization and blocking probability, under different network conditions. Performance results demonstrate that the proposed approaches can provide efficient solutions in terms of network performance, while also providing the level of security required for each demand.

Keywords Network coding · Routing and spectrum allocation · Eavesdropping · Physical layer security · Optical networks

1 Introduction
Elastic optical networks (EONs) provide improved transmission performance and more flexible spectrum allocation compared to conventional WDM optical networks. In EONs, the C-band can be separated in slices (frequency slots) of 25, 12.5, and 6.25 GHz. Subsequently, a connection can be allocated to a number of frequency slots to satisfy its required bit rate. To establish a connection in EONs, a viable solution to the RSA problem must be found, which consists of finding a path (routing—R) from the source to the destination, along with the allocation of the required spectrum slots (spectrum allocation—SA). To find a feasible RSA solution, three basic constraints must be satisfied: (1) the spectrum continuity constraint, where each demand must be allocated the same frequency slots on each link of the selected path, (2) the non-overlapping constraint, where a frequency slot can only be allocated to one demand at a time, and (3) the spectrum contiguity constraint, where the slots serving each demand must be contiguous [1, 2].

Optical networks are considered one of the most important critical infrastructures, as many services (e.g., cloud computing) and critical applications (e.g., national security, public health) rely on these networks for data exchange. Due to the type and the amount of data transmitted, the security of optical networks is of paramount importance, since even attacks over a short time period can still compromise large amounts of critical data.

There are numerous real-world scenarios where optical networks were breached (e.g., utilizing tapping devices to access the signal transmitted via optical fibers). Hence, optical layer security has received considerable attention in recent years. Optical layer security can be divided into different categories based on the type and the purpose of the
threat. Such security threats include the observation of the existence of communication (privacy), the unauthorized use of spectrum (authentication), the manipulation or destruction of data (integrity), the denial of service (availability), and the unauthorized access to information (confidentiality) [3–11]. The focus of this work is on confidentiality, where an adversary can have undetected access to confidential data from an optical communication channel (i.e., eavesdropping) for a prolonged period of time.

Network coding (NC) is a technique where data of different connections are combined and transmitted through the network [12]. This technique can be applied to several areas of communications in order to provide additional capabilities in the system [13–15]. In this work, NC is used to provide security in EONs against eavesdropping attacks by encrypting the confidential data. Thus, with the use of NC, it is extremely difficult for an adversary to compromise any confidential connection, since a number of different connections that traverse different routes will have to be compromised in order for the attacker to make sense of the accessed confidential data. This work significantly extends our previous work presented in [16] by providing an extended analysis of NC within optical networks, followed by novel policies for allocating a path and spectrum slots for the confidential demands. Further, additional properties are considered for the paths used in the XOR operations, which are subsequently incorporated within the heuristic algorithms. Finally, extensive simulations are performed in order to compare all policies in terms of spectrum utilization, blocking probability, and the level of security provided for the confidential demands.

The rest of the paper is organized as follows. The general concept of network coding and its implementations in optical networks are discussed in Sect. 2. The combined NC-RSA problem is described in Sect. 3, followed by the proposed heuristic algorithm in Sect. 4. Next, the performance results are presented in Sect. 5, while Sect. 6 offers some concluding remarks.

2 Network coding implementations in optical networks

The application of NC to optical networks from the algorithmic and infrastructural perspectives has been investigated by the authors in [12]. Furthermore, using NC in conjunction with the RSA process, several connections can combine their transmitted data, enabling protection, multicasting, and security functionalities within the optical network. In the following, a short description of how these functionalities can be achieved, along with a discussion on the physical implementation of NC in optical networks are presented.

2.1 NC-based protection in optical networks

NC-based protection in optical networks has been widely studied [12, 17–20]. For such an approach, intermediate network nodes process a set of signals such that a destination node will receive a linear combination of signals over several disjoint paths. Then, in the case of a failure in the primary path, the destination node will still be able to recover the failed signal from the rest of the received combined signals arriving at the destination from paths that are not affected by the failure. For instance, consider the network shown in Fig. 1a. In this example, connections $1 - 4 - 6$ and $2 - 5 - 6$ transmit datastreams $a$ and $b$, respectively. To provide protection for the primary paths, using network coding, source nodes 1 and 2 also transmit their datastreams to node 3, which performs an XOR operation ($a \oplus b$). Subsequently,

![Fig. 1 Utilizing NC for a protection, b multicasting, and c security](image)
the resulting signal \((a \otimes b)\) is transmitted to the destination (i.e., node 6). In the case that connection \(1 - 4 - 6\) fails, datastream \(a\) can still be recovered by the destination node as \(a = (a \otimes b) \oplus b\). Similarly, in the case that path \(2 - 5 - 6\) fails, datastream \(b\) can still be obtained as \(b = (a \otimes b) \oplus a\).

2.2 NC-based multicasting in optical networks

NC can also be used for multicasting in optical networks. Authors in [12, 21, 22] demonstrate the utilization of network coding for multicasting connections to improve network throughput. The concept of NC in multicasting is to divide the original traffic into different lower-rate substreams and design trees in such a way that the destination nodes will be able to decode the incoming signals based on specific XOR operations. In Fig. 1b, assume that node 1 is the source node and needs to transmit datastreams \(a\) and \(b\) to both destination nodes 5 and 7. One possible solution using network coding is to transmit datastream \(a\) to node 5 and datastream \(b\) to node 7, perform the XOR operation \((a \otimes b)\) at node 4, and transmit the resulting datastream \((a \otimes b)\) to both destination nodes through paths \(4 - 6 - 7\) and \(4 - 6 - 5\). Hence, each node can obtain both datastreams \(a\) and \(b\) by using the received signals. For example, node 5 receives datastreams \(a\) and \((a \otimes b)\). Then, \(b\) can be obtained through the process \(b = a \oplus (a \otimes b)\). A similar procedure can also be performed at node 7 to obtain datastreams \(a\) and \(b\) [22, 23].

2.3 NC-based security in optical networks

Authors in [24] studied the effectiveness of linear network coding (LNC) in optical networks to protect connections from security threats such as eavesdropping and jamming attacks. To enhance the network with security capabilities, a confidential connection can transmit a coded version of its data. Hence, in the case of an eavesdropping attack, the attacker must have knowledge of both the coded version of the signal and all connections used to perform the XOR operations in order to access the confidential data. Recently, we also investigated the problem of network security in elastic optical networks using NC through a heuristic approach [16]. This is also the main topic of this work, in which a significant extension of our approach presented in [16] is provided.

Figure 1c presents a simple example where network coding can be used to provide security for a confidential connection in an optical network. As shown in this figure, the confidential datastream \(a\) is transmitted using path \(1 - 2 - 6\). Also, two non-confidential connections are established in the network using paths \(1 - 3 - 6\) and \(2 - 5 - 6\), and transmit datastreams \(b\) and \(c\), respectively. To provide security for the confidential connection using path \(1 - 2 - 6\), source node 1 transmits a coded version of datastream \(a\), namely \((a \otimes b)\), over link \(1 - 2\), and additional security is provided at link \(2 - 6\) by also using connection \(2 - 5 - 6\) and datastream \(c\). Thus, \((a \otimes b \otimes c)\) is transmitted at the second link of the confidential path. To acquire the confidential datastream \(a\) at node 6, the receiver can perform the operation \(a = b \oplus c \oplus (a \otimes b \otimes c)\). Hence, an eavesdropper must also gain access to both datastreams \(b\) and \(c\) in the network in order to be able to make sense of the confidential datastream \(a\). In other words, the eavesdropper must simultaneously tap 3 different links at different network locations to compromise datastream \(a\).

2.4 Physical layer implementation of NC in optical networks

In opaque networks, NC can be easily implemented, since signals can be received, combined, and transmitted by the intermediate nodes, providing an encrypted version of the signal at each link. 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 (optical) layer. Furthermore, all involved signals must use the same spectrum resources in order for network coding to be enabled. It was shown that NC in all-optical networks can be realized by all-optical XOR logic gates. Specifically, a review of an optical implementation of all-optical XOR gates was performed in [25]. All-optical XOR gates are typically based on semiconductor optical amplifiers (SOAs) that offer low-power consumption, easy deployment, and short latency. Experimental works have also demonstrated NC using XOR operations that can be performed at line speed for transmission above 10 Gbps and up to 100 Gbps with different modulation formats [26–28]. In addition, authors in [29] proposed and experimentally demonstrated a coherent optical layer network coding scheme on polarization-multiplexed differential quaternary phase-shift keying (PM-DQPSK) signals, in which the two PM-DQPSK signal components in the network-coded signal occupy the same channel and cannot be separated by conventional demultiplexing means. Further, authors in [30] proposed a scheme that provides optical encryption/decryption through modified XOR gates that are based on four-wave mixing (FWM) in SOAs. Regarding synchronization, authors in [31] demonstrated that the synchronization constraint in network coding of orthogonal frequency division multiplexed (OFDM) signals can be alleviated by the insertion of a cyclic prefix (with appropriate labels added to the header of the optical frames in order to identify the frames that have to be decoded). Thus, adoption of advanced synchronization methods can ensure a moderate synchronization error of the reconstructed signal, guaranteeing the performance of the system (as a slight synchronization error will not affect the system performance).

© Springer
Based on all aforementioned works, the feasibility of optical NC was clearly demonstrated and is therefore a technology that could be implemented in EONs to provide security at the physical layer against eavesdropping attacks.

3 Problem description

To provide security for confidential connections in the network against eavesdropping attacks, the combined NC-RSA problem must now be solved. More specifically, in order to find the path and the spectrum required for a confidential connection, the path is chosen so as to take advantage of the existing connections established in the network that are utilized to perform a number of XOR operations in the nodes that traverse the confidential path. Further, it should be noted that the spectrum slots selected for the confidential connection can significantly affect the choice of existing connections that can be involved in the XOR process. To consider a confidential connection as secure when using network coding, the following constraints must be satisfied.

- **Encrypted Transmission (ET)** All links of the path allocated to a confidential connection must transmit an encrypted version of their data with at least one XOR operation with other currently established connections in the network.
- **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 already established connections used in the XOR operations.

To satisfy the ET constraint, an existing 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 existing connection with at least two common nodes with the confidential connection can either be used to provide security for the entire path of the confidential demand (i.e., when the source and destination nodes are common nodes), or it can be used to provide security for a segment of the confidential connection (e.g., source to intermediate node, intermediate to intermediate node, or intermediate to destination node segments). Also, in this work, the order in which the common nodes are traversed by the connections involved in the XOR process must be the same, which will also ensure that the direction of the connections traversing the nodes are the same. Finally, the ET constraint ensures that for a secure confidential connection, the selected existing connections must collectively secure all links of the path allocated to that connection. Clearly, this is a tight constraint that could lead to longer paths, and consequently inefficient utilization of network resources, in order to provide the required level of security for the confidential connections. Nevertheless, in this work, since the focus is on security against eavesdropping attacks, a path that is completely secure (i.e., all links of the path carry encrypted information of the confidential connection) will always be preferred compared to a shorter, partially unsecured path, even at the expense of additional network resources.

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 existing connections used in the XOR operation. 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 when only part of the signal (a subset of the frequency slots) is XOR-ed, since the eavesdropper would still have to access all connections used in the encryption process in order to decrypt and make sense of the accessed confidential data.

Finally, it is important to note that to satisfy both constraints, all connections involved in the encryption process (i.e., both the confidential and the currently established connections used in the XOR operation) must be link-disjoint. This is the case, since the connections used in the XOR operation must transmit signals that are at least partially utilized on the same frequency. Thus, considering also the non-overlapping constraint of the RSA problem, all paths involved in this process must be link-disjoint.

The following example (Fig. 2) provides an illustration of the aforementioned constraints in combination with the establishment of a secure confidential connection. In this example, 4 connections \( c_2, c_3, c_4, c_5 \) utilizing paths \( p_2, p_3, p_4, p_5 \) are currently established in the network, provisioned as shown in Table 1, where each connection, \( c_s \), transmits datastream \( d_s \). Further, a confidential connection \( c_1 \) must be established in the network, requiring 2 spectrum slots and using path \( 1 - 4 - 5 \).

As also discussed previously, only the existing connections with two common nodes with the confidential connection can be used to provide security for \( c_1 \) using NC. Thus, \( c_4 \) and \( c_5 \) cannot be used to provide security for \( c_1 \), as \( c_4 \) does not have
two common nodes with \( c_1 \) and \( c_3 \) traverses its common nodes with \( c_5 \) in the opposite order compared to \( c_3 \). Further, the group of spectrum slots that will be assigned for connection \( c_1 \) is very important, since at least a subset of the frequency slots utilized by the confidential connection as well as the already existing connections that take part in the XOR process must be the same (FSM constraint). Thus, if spectrum slots \( 4 - 5 \) were used for \( c_1 \), then only \( c_3 \) can be used to provide security for the connection, while if spectrum slots \( 2 - 3 \) are used, then both \( c_2 \) and \( c_5 \) can be used to provide (a higher level of) security for \( c_1 \). Table 2 presents the transmitted datastreams for each link of the confidential connection, if allocated using spectrum slots \( 2 - 3 \). As shown in Table 2, an encrypted version of the confidential signal is transmitted at all links of the path, satisfying also the ET constraint. In this example, the destination node can successfully decrypt the data, whereas the eavesdropper must gain access to multiple additional connections that are allocated at link-disjoint paths (i.e., \( c_2 \) and \( c_3 \)) apart from the confidential one, in order to make sense of the accessed confidential datastream.

### 4 Proposed heuristic algorithm

To solve the combined NC-RSA problem, the proposed heuristic algorithm is divided into the routing (R) and spectrum allocation (SA) sub-problems. A network planning scenario is considered, where all demands are known a priori and each demand is described by a 4-tuple \((src, dest, B_c, conf)\), 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). It is noted that different classes of confidential connections could be utilized based on the minimum threshold of XOR operations (designated as \( T \) in this work) required per link. However, in this work, only the case of confidential \((T \geq 1)\) and non-confidential \((T = 0)\) demands will be considered.

#### Table 2 Datastream transmitted at each link of the confidential connection \( c_1 \)

| Link | Transmitted datastream |
|------|------------------------|
| 1 - 4 | \( d_1 \oplus d_2 \) |
| 4 - 5 | \( d_1 \oplus d_2 \oplus d_4 \) |

#### 4.1 Pre-processing phase

Prior to the utilization of the heuristic approach, a pre-processing phase is required that pre-calculates the candidate paths for each \( src\)-\( dest \) pair. Also, a node-matching procedure takes place, to ascertain whether two paths have at least two common nodes traversed in the same order, so as to satisfy the ET and FSM constraints that are required for a feasible NC-RSA solution for the confidential demands.

First, a set of \( k \) candidate paths is pre-calculated for each \( src\)-\( dest \) pair. Subsequently, to implement NC, the security level that each candidate path can provide to the rest of the candidate paths must be calculated. According to the ET constraint, all links traversed by a secure confidential connection must transmit an encrypted version of the data. This means that at least one XOR operation with the established connections must be performed for all links in the path used by the confidential connection. Let \( P \) be the set of all candidate paths, \( p \) the path under consideration \((p \in P)\), and \( P' \) the set of the rest of the candidate paths that may be used by path \( p \) to provide encryption over specific links of path \( p \) \((P = P' \cup p)\). Also, let \( \delta_{pl} \) be a coefficient which is equal to 1 if paths \( p \in P \) and \( p' \in P' \) have two common nodes and the \( l \)th link of path \( p \) can be “covered” \((i.e.,\ encryption\ is\ provided)\) by path \( p' \), and 0 otherwise.

Figure 3 provides an example of the \( \delta \) coefficients for 3 paths \([3 - 1 - 2 - 4, 2 - 5 - 6 - 4, 2 - 3 - 5]\) utilized by 3 connections in the network. Hence, the links that are covered for each pair of connections must be calculated \((\delta \) coefficient), with regards to the common nodes for each pair of paths.

Assume that in this case initially the path under consideration is path \( p_2 \). To check whether the rest of the connections can provide security for the connection using path \( p_2 \), the following procedure is followed: path \( p_2 \) has two common nodes with path \( p_1 \) \((nodes\ 2\ and\ 4)\) and since these nodes are the source and destination nodes of \( p_2 \), then connection \( p_1 \) could be used to provide security for all links that belong to \( p_2 \). Hence, the values of \( \delta_{11}^2, \delta_{12}^2, \) and \( \delta_{13}^2 \) are equal to 1 for the first, second, and third link of path \( p_2 \), respectively. It is important to note that on the other hand, connection \( p_2 \) can only provide security for the third link \((\text{link} 2 - 4)\) of connection \( p_1 \), resulting in \( \delta_{23}^2 = 1 \). Thus, clearly, \( \delta_{11}^2 \neq \delta_{23}^2 \).
Similarly, the first link of \( p_2 \) can be secured by \( p_3 \), since nodes 2 and 5 are common between these paths and therefore \( \delta_{21}^3 = 1 \). Also, in this case, \( p_2 \) can be used to provide security for all links in \( p_3 \), since nodes 2 and 5 are the source and destination nodes of \( p_3 \), respectively. Therefore, \( \delta_{22}^3 = \delta_{32}^3 = 1 \). Finally, it is noted that the order of the nodes in the path and the direction of the path itself are taken into consideration in the determination of the \( \delta \) coefficient. For example, \( p_2 \) has two common nodes with \( p_1 \) (nodes 2 and 3), but it cannot provide any security for that connection, since in path \( p_2 \), node 2 is traversed before node 3, whereas the opposite is the case with path \( p_1 \). Table 3 presents the \( \delta \) coefficients for all path combinations in this example.

To calculate the \( \delta \) coefficients, an algorithm is implemented that takes as input the set of all the pre-calculated candidate paths \( P \). Then, for each pair of candidate paths \( p \) and \( p' \) (\( p \in P \) and \( p' \in P' \)), their common nodes are found and they are stored in set \( CN \). Next, if the size of set \( CN \) is greater than 1 (i.e., there are at least two common nodes between paths \( p \) and \( p' \)), then starting from the source node, for each node \( i \) in path \( p \), if that node is included in \( CN \) (i.e., \( i \) is a common node for both \( p \) and \( p' \)), the order of the node \( i \) in \( p' \) is stored in \( S_{node} \). Subsequently, starting from the destination node of \( p \), for each node \( j \) that is traversed after node \( i \) in \( p \), if that node is included in \( CN \), the order of node \( j \) in \( p' \) is found and is stored in \( E_{node} \). If \( E_{node} \) is greater than \( S_{node} \) (i.e., node \( j \) is traversed after node \( i \) in both \( p \) and \( p' \)), then all the links between nodes \( i \) and \( j \) in \( p \) can be secured by path \( p' \). Thus, the \( \delta_{p'}^p \) coefficient is equal to 1 for all these links.

It is important to note that using this process, it is ensured that node \( i \) is traversed prior to node \( j \) in paths \( p \) and \( p' \), a necessary condition for path \( p' \) to provide security for path \( p \). Further, if more than 2 common nodes are found, the links secured may vary depending on which two common nodes are selected. However, following this procedure, the set of common nodes is selected that results in \( p' \) securing the largest number of links of path \( p \). This is a direct consequence of the way the common nodes are selected (i.e., the first common node is found while searching from the source node to the destination and the second common node is found by starting from the destination node). Finally, it is also noted that the \( \delta \) coefficient must be calculated between all paths in the set of candidate paths for a src-dest pair, since several connections with the same source and destination nodes can be established in the network via different paths. For these cases, the \( \delta \) coefficient will be equal to 1 for all links of the candidate paths, since the two common nodes found between each pair of paths are always the source and destination nodes.

### Table 3 \( \delta \) coefficients for 3 paths established in the network

| \( \delta_{p'}^p \) | \( \delta_{p1}^p \) | \( \delta_{p2}^p \) | \( \delta_{p3}^p \) |
|-----------------|--------|--------|--------|
| \( \delta_{21}^1 \) | 0      | 0      | 1      |
| \( \delta_{31}^2 \) | 0      | 0      | 0      |
| \( \delta_{12}^2 \) | 1      | 0      | 1      |
| \( \delta_{13}^1 \) | 1      | 0      | 0      |
| \( \delta_{12}^3 \) | 0      | 0      | 1      |
| \( \delta_{23}^2 \) | 1      | 1      | 1      |

### 4.2 Routing

For the routing sub-problem, the pre-calculated \( k \)-shortest candidate paths that are able to satisfy a requested connection are considered. These \( k \)-shortest paths can be sorted based on different metrics (e.g., number of hops, modulation format, most/least used nodes/links, etc.). 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 value of \( U_n/U_l \) among all the nodes/links it traverses \( (U_{pa}/U_{pl}) \). The paths of the non-confidential connections can then be sorted based on the following criteria, which provide the best results in terms of spectrum utilization and level of security, as presented in [16]:

- **Most used nodes/links (MUN/MUL)**: The candidate paths for each src-dest pair are sorted in descending order based on the value \( U_{pa}/U_{pl} \) of each path. By selecting the path which comprises the most used nodes/links, the number of XOR operations for a confidential connection will potentially increase.

- **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 defined in [32]). 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 aforementioned sorting strategies. It is noted that when the MUN or MUL techniques are utilized, the candidate paths that can be used to establish the connection under investigation are sorted based on the current state of the network at the time of connection provisioning [i.e., the number of times each node/link is used when the connection is established in the network \( (U_n/U_l) \)], and this sorting process is performed for each non-confidential connection in the network.

For the confidential connections, the candidate path that produces the most XOR operations is used, which also depends on the spectrum slots selected. To achieve this, an XOR spectrum slot metric \( (\text{XOR-SSM}_p) \) is used, that counts the number of XOR operations performed for a specific path \( p \) and group of frequency slots. In addition, the XOR-SSM metric can be further differentiated as follows:
• **Minimum XOR spectrum slot metric (MXOR)p** The MXOR_p metric counts the minimum number of XOR operations over all links of candidate path p. This is the metric that we first introduced and used in [16]. By using this metric, the aim is to maximize the level of security provided for the “weakest link” of the candidate path (the link with the least number of XOR operations performed).

• **Average XOR spectrum slot metric (AXOR)p** The AXOR_p metric calculates the average number of XOR operations per link that are provided for candidate path p. By using this metric, the aim is to maximize the average number of XOR operations performed on each link of the candidate path (provided that the minimum threshold is met, as explained below).

### 4.3 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]. To calculate the number of frequency slots f_c required for a given connection c if candidate path p is selected, we use $f_c = \left\lfloor \frac{B_c}{B_{\text{rate}} MF_p} \right\rfloor$, where $B_c$ is the bit-rate requested by connection c, $B_{\text{rate}}$ is the baud rate of each spectrum slot in the network, and $MF_p$ is the modulation format (expressed in bits/symbol) that can be used for candidate path p, which is based on the overall distance of path p.

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 one of the two aforementioned XOR-SSM metrics. Algorithm 1 below describes the NC-RSA approach for a given confidential demand. Also, an example in Fig. 4 is used to better explain the proposed algorithm when using either metric.

**Algorithm 1 NC-RSA for a given confidential demand**

**Input:** $G(V, E)$, Set of candidate paths P, Paths currently established $P_e$, Confidential demand $d$ described by $(src, dest, B_c, 1)$, XOR threshold T, Spectrum slot metric SM, overall number of frequency slots of each link in the network $F$  

**Output:** Provisioning of Confidential Connection

1. for each candidate path $p \in P_{src,dest}$ do
2. $L = \text{number of links in path } p$
3. Find a set of paths $P_{used} \in P_e$ that are used by the established connections, such that $\sum_{c \in P_{used}} p'_{c} > 0$, for each $p' \in P_{used}$
4. Create temporary matrix $t = L \times F$, and initialize all entries of $t$ to 0.
5. for each path $p_u \in P_{used}$ do
6. Using $\delta_{p_u}$ coefficient, increase by one the values for each link $l$ where $\delta_{p_u} = 1$ for the spectrum slots that are covered by $p_u$ within $t$.
7. end for
8. Initialize XOR-SSM_p = 0
9. if SM = 0 then /* MXOR is utilized */
10. for each group $(a-b)$ of available frequency slots (FS) in $p$ that can be allocated to $d$ do
11. $s_{a-b}^{n} = \sum_{z=1}^{n} l_{z,n}$, for $z = 1$ to $L$
12. $S_{a-b} = \min(s_{a-b}^{n}, ..., s_{L}^{n})$
13. XOR-SSM_p = $\max$(XOR-SSM_p, $S_{a-b}$)
14. end for
15. else /* AXOR is utilized */
16. for each group $(a-b)$ of available FS in $p$ that can be allocated to $d$ do
17. $s_{a-b}^{n} = \sum_{z=1}^{n} l_{z,n}$, for $z = 1$ to $L$
18. if $\min(s_{a-b}^{n}, ..., s_{L}^{n}) \geq T$ then
19. $S_{a-b} = \frac{\sum_{z=1}^{L} s_{a-b}^{z}}{L}$
20. XOR-SSM_p = $\max$(XOR-SSM_p, $S_{a-b}$)
21. end if
22. end for
23. end if
24. end for
25. Select candidate path $p$ with the highest value of the XOR-SSM metric.
26. if XOR-SSM_p $\geq T$ then
27. Connection is established using path $p$ and group of frequency slots $(a-b)$.
28. else
29. Connection is rejected.
30. end if
Specifically, in Algorithm 1 (NC-RSA), for a given confidential connection, the XOR-SSM\textsubscript{p} metric 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 a non-zero vector coefficient \( \delta_{pu}^p \) for path \( p \) under investigation is found (denoted as \( P_{\text{used}} \) in the algorithm, \( p \in P_{\text{used}} \)). This set of paths can be used to satisfy the ET constraint. Subsequently, for each path \( p_u \), 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: 
\[
\overline{S}^{a-b} = \sum_{n=1}^{L} t_{z,a}^{a-b},
\]
where \( a \) and \( b \) are the starting and ending slots selected. In the case that MXOR is selected, the minimum \( \overline{S}^{a-b} = \min(s_1^{a-b}, \ldots, s_L^{a-b}) \) value is selected (i.e., the weakest link in terms of the number of XOR operations performed in path \( p \) is considered). On the other hand, in the case that AXOR is selected, then if the minimum number of XOR operations on each link is greater than or equal to the given acceptable threshold \( \min(s_1^{a-b}, \ldots, s_L^{a-b}) \geq T \), the average number of XOR operations per link in the candidate path \( p \) and group of frequency slots \( (a - b) \) is calculated via 
\[
\overline{S}^{a-b} = \sum_{z=1}^{L} s_z^{a-b}/L.
\]
This procedure (for MXOR or AXOR) is repeated for all groups of frequency slots, and the group of frequency slots with the maximum value of \( \overline{S} \) is selected. In addition, this procedure is repeated for all candidate paths that can establish the confidential connection, and the candidate path \( p \) that provides the maximum XOR-SSM\textsubscript{p} is selected to establish the confidential connection (using either the MXOR or the AXOR metric). If the XOR metric found has a value greater than or equal to threshold \( T \), then the connection is established in the group of frequency slots that achieves that XOR-SSM\textsubscript{p} value. Otherwise, it is rejected.

The value of the metric (e.g., \( x \)) selected signifies that either at least \( x \) XOR operations are used to secure the confidential connection in each link (using MXOR) or an average number of \( x \) XOR operations are used to provide security for each link of that connection, given that the threshold requirement \( T \) is satisfied at each link of the path (using AXOR). Both processes also imply that the ET and FSM constraints are satisfied for that confidential connection. On the other hand, if \( x < T \), there is at least one link in the path where the threshold requirement is not satisfied, and the connection is not considered secure.

To clearly demonstrate this procedure, in Fig. 4, assume a network with \( F = 5 \) and a candidate path \( p_1 (1-2-6) \) that requires 3 frequency slots. Also, the set \( P \) of currently established paths in the network consists of \{ \( p_2, p_3, p_4, p_6, p_7, p_8, p_9 \) \}. Table 4 provides information on each path (route along with the spectrum slots that each connection utilizes). Also, the \( \delta \) coefficient is shown for each path in \( P \) and path \( p_1 \).

As discussed in the previous sections, a path must have at least two common nodes with the confidential one to provide security for that connection. Thus, \( p_4 \) is not able to provide any security for path \( p_1 \). Additionally, since the direction of the path and the common nodes plays a key role in providing security for the confidential connection, path \( p_6 \) is also not able to provide any security for the given demand. As a result, \( P_{\text{used}} \) consists of \{ \( p_2, p_3, p_4, p_6, p_7, p_8 \) \}. For example, connection \( p_2 \) contributes to cells \( t_{1,2,4} \) and \( t_{1,2,5} \), since it can cover spectrum slots 4 and 5 in the second link of \( p_1 \). On the other hand, path \( p_5 \) could provide security to the confidential connection, but since it uses the same link as \( p_1 \), the spectrum slots allocated to \( p_5 \) (i.e., slot 1) are excluded from the available group of frequency slots, so as to satisfy the non-overlapping constraint. This value is designated as ‘−’ in the \( t \) matrix. The resulting \( t \) matrix using all paths in \( P_{\text{used}} \) for this example is shown in Table 5.

### Table 4 Information for connections currently established in the network

| Path id | Path selected | Spectrum slots allocated | \( \delta_{p_1}^{p_2} \) | \( \delta_{p_2}^{p_1} \) |
|---------|---------------|--------------------------|--------------------------|--------------------------|
| \( p_2 \) | 2 − 4 − 6 − 3 | 4 − 5                    | 0                         | 1                         |
| \( p_3 \) | 1 − 4 − 5 − 6 | 3 − 4                    | 0                         | 1                         |
| \( p_4 \) | 2 − 3         | 1 − 2                    | 0                         | 0                         |
| \( p_5 \) | 1 − 2         | 1                        | 1                         | 0                         |
| \( p_6 \) | 6 − 2         | 1 − 3                    | 0                         | 0                         |
| \( p_7 \) | 2 − 3 − 6     | 4 − 5                    | 0                         | 1                         |
| \( p_8 \) | 1 − 4 − 2     | 1 − 2                    | 1                         | 0                         |

### Table 5 Number of XOR operations per slot (\( t \) matrix)

| Spectrum slot id | 1 | 2 | 3 | 4 | 5 |
|------------------|---|---|---|---|---|
| Link id          |   |   |   |   |   |
| 1 (1-2)          | 1 | 1 | 1 | 1 | 0 |
| 2 (2-6)          | 0 | 1 | 3 | 2 |   |
Next, the number of XOR operations must be calculated for each group of frequency slots that could be used to establish the confidential demand. To calculate the number of XOR operations on link 1 and frequency slots $2 - 4$, $s_{2-4}^1 = t_{1,2,1} + t_{1,3,1} + t_{1,4,1} = 1 + 1 + 1 = 3$. The same process is performed for all links that belong to the candidate path and the selected group of frequency slots $3 - 5$. It is noted that this process is not performed for spectrum slots $1 - 3$, since they are not available for the confidential demand. The result for each group of frequency slots and the links of the candidate path is shown in Table 6.

Finally, to calculate the XOR-SSM metric, $S$ must be calculated for each group of available frequency slots. In case the MXOR metric is used, $S^{x-y} = \min(s_1^{x-y}, s_2^{x-y}) = \min(3, 4) = 3$, and $S^{3-5} = \min(s_3^{3-5}, s_2^{3-5}) = \min(2, 6) = 2$ respectively, as shown in Table 7 for the group of frequency slots $2 - 4$ and $3 - 5$. Now, XOR-SSM$_{\rho_l} = \max(S^{x-y}, S^{3-5}) = \max(3, 2) = 3$, using frequency slots $2 - 4$. On the other hand, if the AXOR metric is used, $S^{x-y} = (s_1^{x-y} + s_2^{x-y})/2 = (3 + 4)/2 = 3.5$, and $S^{3-5} = (s_3^{3-5} + s_2^{3-5})/2 = (2 + 6)/2 = 4$ (Table 8). Hence, XOR-SSM$_{\rho_l} = \max(3.5, 4) = 4$ using frequency slots $3 - 5$. It is noted that, for example, in the case $T = 3$, then this would not be an acceptable solution (i.e., $\min(2, 6) = 2 < T$), and therefore, frequency slots $2 - 4$ would be selected.

Following either approach to solve the NC-RSA problem for the confidential demands will, in many cases, result in a high blocking probability, since confidential connections that do not meet the required threshold $T$ are immediately blocked. To overcome this problem, Algorithm 2 is proposed (illustrated in the flowchart of Fig. 5) that utilizes Algorithm 1 (NC-RSA) and tries to establish both confidential and non-confidential demands, while eliminating blocking due to the level of security requirements for the confidential connections.

As shown in the flowchart, the candidate paths are first pre-calculated and the $\delta$ coefficient is calculated for each pair of paths. Then, following a first come first serve policy, all connections are established in the network. For the non-confidential connections, a typical RSA is implemented with one of the routing strategies proposed, while the proposed Algorithm 1 (NC-RSA) is used for the confidential demands with either the MXOR or AXOR metrics utilized. After all demands are allocated in the network, the confidential connections, a typical RSA is implemented while eliminating blocking due to the level of security requirements for the confidential connections.
the first time the heuristic was implemented). Further, the new number of XOR operations is calculated for the already established confidential demands and for the confidential connections that were re-entered in the network. These latter confidential connections are now provisioned in the network, even if they do not meet the level of security required and are thus identified as unsecured confidential connections (see results in Fig. 10 of Sect. 5). Nevertheless, blocking still exists in the network due to the lack of network resources for both non-confidential and confidential connections. The reader should note that a modified approach was also implemented, where the confidential connections not previously provisioned were re-entered in the network multiple times in order to increase the number of these connections that would eventually meet the required level of security. However, since the algorithm did not present any improvement after the first iteration, the approach presented in the flowchart of Fig. 5, having reduced computational complexity, was finally adopted.

It is also noted that additional (dummy) lightpaths can be added with the sole purpose to ensure security for the confidential connections that do not reach the required threshold $T$. Further, if we were to sort the initial set of (static) demands (i.e., do not utilize the “first come first serve” policy), this will clearly influence the provisioning of confidential connections: if confidential connections are established first, there may not be enough established connections for the required XOR operations; on the other hand, if non-confidential connections are added first, it is not guaranteed that the confidential ones can find the appropriate path and group of spectrum slots that can provide the required level of security. These approaches constitute interesting research directions and will be considered as future work.

5 Performance evaluation

To evaluate the proposed algorithms, an EON is implemented using bandwidth variable transponders that operate using the following 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. The network topology utilized in the simulations is shown in Fig. 6, consisting of 14 nodes and 42 directed links. For this network, a flexible grid is implemented, with a channel spacing of 12.5 GHz which results in a total of 320 spectrum slots with a baud rate of 10.7 Gbauds for each link in the network. The requested demands are randomly generated using a uniform distribution for all scr-dest pairs, where each demand size varies from 20 to 100 Gbps, while the number of candidate paths used for the first set of experiments is set to 5 ($k=5$). Each presented result is the average of 10 experiments performed with different generated sets of demands, where for all simulations 30% of the overall number of demands are designated as confidential. Finally, a PC with an i7-3930K CPU and 24 GB RAM is used for all simulations.

When using network coding, the level of security provided for a confidential connection can be quantified by the minimum and average number of XOR operations performed on each link of its established path. In this work, the threshold for the number of XOR operations that a connection must have on each link of its path in order to be considered as secure is set to 1 ($T = 1$). This means that the number of XOR operations ($N$) that must be performed at each link of the path used by a given confidential connection must be $N \geq 1$, in order to consider the specific connection as secure.

By increasing the minimum number of XOR operations that occur at the links of the established path for the confidential connection, then even if an eavesdropper taps the weakest link of this confidential connection (i.e., the link with the smallest number of XOR operations performed), all connections used in these XOR operations will have to be compromised before the eavesdropper can make sense of the confidential information. The minimum number of XOR operations (averaged over all confidential demands) is presented in Fig. 7, when the three routing strategies are utilized for both the AXOR and MXOR metrics.

Using the MXOR-MUL or MXOR-MUN routing strategies provides the highest minimum number of XOR

---

**Fig. 6** Network topology used in the simulations, consisting of 14 nodes and 42 directed links.
operations performed for each demand, on average, compared to the rest of the cases examined. This is to be expected, since the MXOR metric has as an aim to select the candidate path and group of frequency slots that maximize the minimum number of XOR operations for the confidential demand. Further, it is shown that by using the AXOR metric and either the MUL or MUN routing algorithms provides results close to the ones obtained when MXOR is utilized. This is due to the fact that in this case, a relatively small number of candidate paths \( k \) is utilized. Thus, in order to satisfy the required XOR threshold for each link, while also maximizing the average number of XOR operations, a solution is selected where the minimum number of XOR operations is close to the results of the MXOR case (indeed, this is shown in Table 9, where the difference between AXOR and MXOR, in terms of the minimum number of XOR operations per demand, increases with the number of candidate paths). Finally, the MSE routing strategy provides the least number of XOR operations per confidential connection which is to be expected, since it has as an aim to add non-confidential connections in a spectrum efficient manner, rather than to provide more XOR operations for the confidential ones. Nevertheless, in all cases, the results indicate that on average, the minimum number of XOR operations that take place per link per demand is between 2–3, higher than the predefined XOR threshold \( T = 1 \).

As discussed in the previous sections, the number of XOR operations performed on each link is a key point for the level of security provided to a confidential demand. Accounting for the average number of XOR operations per link per demand is another useful metric that could describe the average number of connections that have to be compromised to make the confidential demand vulnerable. Thus, Fig. 8 presents the average number of XOR operations per link per confidential connection in the network (averaged over all confidential demands), when using different slot allocation metrics and routing techniques for the candidate paths.

As shown, the AXOR metric provides the best results in terms of the average number of XOR operations performed, which is to be expected, since it has as an aim to maximize the average number of XOR operations per link for a connection, as long as the XOR threshold is satisfied for all links. On the other hand, using the MXOR metric, which aims to maximize the minimum number of XOR operations over all links of the demand, does not always provide the best results in terms of the average number of XOR operations performed for the confidential connections. Further,

| Table 9 | Impact of \( k \) on level of security, blocking probability, and spectrum utilization |
|---------|-----------------------------|---|---|---|
| Result                                                                 | Technique | \( k \) |
|                                                                 |               | 5 | 10 | 20 |
| Average number of minimum XOR operations | MXOR-MUL | 2.45 | 2.83 | 3.09 |
|                                                                 | AXOR-MUL | 2.38 | 2.75 | 2.99 |
|                                                                 | AXOR-MSE | 2.02 | 2.19 | 2.50 |
|                                                                 | T - RSA | – | – | – |
| Average number of XOR operations per link per demand | MXOR-MUL | 2.66 | 3.17 | 3.60 |
|                                                                 | AXOR-MUL | 2.95 | 3.76 | 4.28 |
|                                                                 | AXOR-MSE | 2.36 | 2.87 | 3.57 |
|                                                                 | T - RSA | – | – | – |
| Blocking probability | MXOR-MUL | 0.04 | 0.11 | 0.17 |
|                                                                 | AXOR-MUL | 0.04 | 0.13 | 0.20 |
|                                                                 | AXOR-MSE | 0 | 0 | 0 |
|                                                                 | T - RSA | 0 | 0 | 0 |
| Number of spectrum slots utilized | MXOR-MUL | 7561 | 8429 | 9219 |
|                                                                 | AXOR-MUL | 7734 | 8723 | 9456 |
|                                                                 | AXOR-MSE | 5243 | 5754 | 6538 |
|                                                                 | T - RSA | 4232 | 4257 | 4322 |
the MUL routing strategy results in a larger number of XOR operations compared to both the MSE and MUN routing strategies when either spectrum allocation metric is used. This is due to the fact that since the direction of the paths in the XOR process is taken into consideration, a confidential path that can use other existing connections traversing a highly utilized link (i.e., traverses the nodes in the same order through a link-disjoint path) will potentially increase the number of XOR operations performed in its path. Thus, using the MUL sorting technique maximizes the utilization of specific links in the network, which subsequently results in providing a higher level of security for the confidential demands (contrary to results in [16], where the direction of the paths was not considered).

Next, the blocking probability of the network is presented (Fig. 9) when different metrics and routing techniques are utilized. In this figure, the MXOR-MSE case is excluded, since it offers the worst results in terms of the minimum and average number of XOR operations. Also, the MXOR-MUN approach is excluded to simplify the presented results, since it provides similar results to the MXOR-MUL case. In addition, the case where all connections are designated as non-confidential, allocated using the MSE routing strategy, is also presented as a benchmark (designated as “T-RSA”). It is clearly demonstrated that the AXOR-MUN routing strategy results in a much higher blocking probability compared to the AXOR-MSE case, since the paths chosen, utilizing the former strategy, aim to increase the level of security of the confidential connection, rather than to maximize the efficient use of spectrum resources, which is precisely the aim of the latter strategy. In fact, the AXOR-MSE approach satisfies the appropriate threshold of XOR operations per link in the network, while also providing a very low blocking probability, similar to the performance of the benchmark case (T-RSA).

Clearly, the number of candidate paths for each src-dest pair that a confidential connection can use will also have a great impact on the network performance in terms of the level of security, blocking probability, and spectrum utilization, as shown in Table 9. Note that only results for the MXOR-MUL, AXOR-MUL, and AXOR-MSE policies are shown, as these policies provide the best results (as previously shown in Figs. 7, 8, 9). Again, the results for the T-RSA case are provided as benchmark.

From Table 9, it is evident that the larger the number of candidate paths for each src-dest pair, the larger the number of XOR operations that can be performed for each confidential demand. Thus, both the average and minimum number of XOR operations increase as \( k \) increases, for all NC-RSA strategies. It should be noted though that as \( k \) increases, the number of additional spectrum slots utilized as well as the blocking probability will also increase, since now both confidential and non-confidential demands use paths that are not efficient in terms of spectrum utilization, but rather are chosen to maximize the number of XOR operations performed by the confidential demands. Thus, the choice of \( k \) should be one that provides a balanced solution between the efficiency of the network resources and the level of security provided for the confidential demands.

From the results presented, for any choice of \( k \), the AXOR-MUL approach provides the highest number of XOR operations on average for each confidential demand, while also satisfying the minimum threshold for each link for all confidential connections. On the other hand, the AXOR-MSE approach provides a much lower blocking probability, while achieving a slightly smaller number of XOR operations. Thus, for the rest of the simulations, the AXOR-MUL approach, which provides the best results in terms of the level of security provided for the confidential demands and the AXOR-MSE approach, which provides the most efficient usage of the spectrum while providing an acceptable level of security for the confidential connections will be utilized. In conjunction, 10 candidate paths for each src-dest pair will

**Fig. 8** Average number of XOR operations per link per confidential connection (averaged over all confidential demands)

**Fig. 9** Blocking probability for different routing strategies and XOR spectrum slot metrics
be used (i.e., \( k = 10 \)), in order to provide a balanced solution in terms of level of security and spectrum efficiency. Also, 1500 connections will now be established in the network to better illustrate how each approach performs as the number of demands increases considerably.

The percentage of the established confidential connections that are considered secure (i.e., satisfying the ET and FSM constraints) is subsequently presented in Fig. 10 for different routing techniques. Clearly, from the results presented, the MUL technique performs better compared to the MSE routing strategy, since connections are forced to traverse the same links, and therefore, more connections can be found that can be XOR-ed with the confidential connection. It is also noted that when using the MSE routing strategy, the percentage of secure connections increases with the number of demands that are established in the network, while it decreases with the number of demands when the MUL strategy is used. The former occurs because as more non-confidential connections are established in the network using their most efficient available paths, more confidential connections can find paths to use in their encryption process so as to be established in the network while achieving the required level of security. On the other hand, the latter occurs because the resources of the candidate paths that could provide security for the confidential demands are saturated, leading to the usage of less secure candidate paths. In order to secure all confidential demands, it is again noted that additional dummy lightpaths can be utilized in the XOR process in order to provide security for any unsecured confidential connections established in the network.

Next, the blocking probability is presented in Fig. 11 when more connections (1500) are established in the network and more candidate paths (\( k = 10 \)) are considered for each connection. From the results obtained, the MUL sorting strategy is shown to provide a much higher blocking probability compared to the MSE strategy. In fact, the MSE strategy provides a blocking probability close to the benchmark.
case, while also satisfying the appropriate threshold of XOR operations per link in the network (more than 90% for more than 1000 demands—Fig. 10).

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. Thus, Fig. 12 presents the number of utilized spectrum slots when using the MUL and MSE routing strategies versus the benchmark case (all connections are designated as non-confidential and the candidate paths are routed based on the MSE technique), followed by Fig. 13 that presents the average number of hops per demand for these routing strategies. In these cases, the results where there is no blocking in the network (enough network resources are available) are presented, in order to obtain the exact number of spectrum resources utilized for each set of demands. As shown in the figures, the MUL routing strategy (which provides the largest number of XOR operations, on average, for the confidential connections) requires many more spectrum resources to establish all connections, since the paths selected to establish each connection are longer (Fig. 13) compared to MSE. On the other hand, using the MSE approach to provide security for confidential connections results in an acceptable (i.e., above designated threshold) number of XOR operations on average for the confidential demands, while at the same time, it requires considerably fewer resources compared to the MUL approach. In fact, using MSE, the number of additional resources allocated to the network is slightly increased compared to the case where all connections are not confidential (“T-RSA” - benchmark case). This is the case, since all non-confidential connections are assigned using the best path available (in terms of hops and modulation format).

6 Conclusions

In this work, a novel heuristic approach is proposed that utilizes the concept of network coding in EONs to provide security for confidential connections against eavesdropping attacks. Using the proposed approach, the physical layer security is increased, since connections established at link-disjoint paths combine their datastreams to encrypt the confidential data. Thus, an eavesdropper must now compromise several connections traversing different parts of the network in order to make sense of any accessed confidential data.

Performance results indicate that using the average XOR spectrum slot metric (AXOR) to evaluate each candidate path and group of spectrum slots required for the confidential demands results in a higher number of XOR operations performed on each link of the confidential path, and thus it provides an increased level of security against an adversary that attempts to compromise confidential data. Also, the combination of the AXOR metric with the most used links (MUL) routing strategy provides the highest number of XOR operations for each confidential demand at the expense of a significant increase in the spectrum resources utilized, while the maximum spectrum efficiency (MSE) routing strategy provides a similar number of XOR operations at the expense of a small percentage of additional spectrum slots. Therefore, by using the AXOR-MSE approach, the required level of security for the confidential connections is achieved, while spectrum utilization and blocking probability results are similar to those for the benchmark case, where all connections are considered as non-confidential.

Ongoing work includes the development of integer linear programming (ILP) formulations to provide an optimal solution to the NC-RSA problem, as well as the consideration of additional physical layer constraints that are imposed by the utilization of network coding via XOR operations. In addition, a probabilistic approach is currently being investigated, where each link has a probability of being attacked. In that case, the ET constraint can be relaxed for links with a very low probability of being attacked, in an effort to better utilize network resources, while still providing security against eavesdropping attacks to all links where such an attack is likely to occur.

Acknowledgements This work has been partially 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 partially supported by the Cyprus Research and Innovation Foundation under Project CULTURE/AWARD-YR/0418/0014 (REALFON).

References

1. Gerstel, O., et al.: Elastic optical networking: a new dawn for the optical layer? IEEE Commun. Mag. 50(2), S12–S20 (2012)
2. Christodouloupolou, K., et al.: Routing and spectrum allocation in OFDM-based optical networks with elastic bandwidth allocation. In: IEEE GLOBECOM (2010)
3. Fok, M.P., et al.: Optical layer security in fiber-optic networks. IEEE Trans. Inf. Forens. Secur. 6(3), 725–736 (2011)
4. Savva, G., et al.: Spread spectrum over OFDM for enhanced security in elastic optical networks. In: IEEE PSC (2018)
5. Kitayama, K., et al.: Security in photonic networks: threats and security enhancement. IEEE/OSA J. Lightw. Technol. 29(21), 3210–3222 (2011)
6. Furdek, M., et al.: An overview of security challenges in communication networks. In: IEEE RNDM (2016)
7. Skorin-Kapov, N., et al.: Physical-layer security in evolving optical networks. IEEE Commun. Mag. 54(8), 110–117 (2016)
8. Manousakis, K., Ellinas, G.: Attack-aware planning of transparent optical networks. Opt. Switch. Netw. 19(2), 97–109 (2016)
9. Savva, G., et al.: Eavesdropping-aware routing and spectrum/code allocation in OFDM-based EONs using spread spectrum techniques. IEEE/OSA J. Opt. Commun. Netw. 11(7), 409–421 (2019)
10. Bai, W., et al.: Eavesdropping-aware routing and spectrum allocation based on multi-flow virtual concatenation for confidential information service in elastic optical networks. Opt. Fiber Technol. 40, 18–27 (2018)
11. Singh, S.K., et al.: Balancing data security and blocking performance with spectrum randomization in optical networks. In: IEEE GLOBECOM (2016)
12. Manley, E.D., et al.: All-optical network coding. IEEE/OSA J. Opt. Commun. Netw. 2(4), 175–191 (2010)
13. Beldachi, A.F., et al.: Resilient cloud-RANs adopting network coding. Optical network design and modeling (ONDM). Lect. Notes Comput. Sci. 11616, 349–361 (2020)
14. Martínez-Peñas, U., Kschischang, F.R.: Reliable and secure multi-shot network coding using linearized Reed-Solomon codes. IEEE Trans. Inf. Theory 65(8), 4785–4803 (2019)
15. Liu, X., et al.: Optimal byzantine attacker identification based on game theory in network coding enabled wireless ad hoc networks. IEEE Trans. Inf. Forens. Secur. 15, 2570–2583 (2020)
16. Savva, G., et al.: Network coding for security against eavesdropping attacks in elastic optical networks. In: IFIP ONDM (2019)
17. Ramirez, W., et al.: Network coding-based protection scheme for elastic optical networks. In: IEEE DRCN (2014)
18. Kamal, A.E., Mohandespour, M.: Network coding-based protection. Opt. Switch. Network. 11, 189–201 (2014)
19. Hai, L.T.: An optimal design framework for 1+1 routing and network coding assignment problem in WDM optical networks. IEEE Access 5, 22291–22298 (2017)
20. Hai, L.T.: On the spectrum-efficiency of QoS-aware protection in elastic optical networks. Optik 202, 163563 (2020)
21. Agarwal, A., Charikar, M.: On the advantage of network coding for improving network throughput. In: IEEE Information Theory Workshop (2004)
22. Yang, L., et al.: Incorporating network coding to formulate multicast sessions in elastic optical networks. In: IEEE ICNC (2016)
23. Kim, M., et al.: Network coding and its implications on optical networking. In: IEEE/OSA OFC (2009)
24. Engelmann, A., Jukan, A.: Balancing the demands of reliability and security with linear network coding in optical networks. In: IEEE ICC (2016)
25. Zhang, M., et al.: All optical XOR logic gates: technologies and experiment demonstration. IEEE Commun. Mag. 43(5), S19–S24 (2005)
26. Kong, D., et al.: All-optical XOR gates for QPSK signal based optical networks. Electron. Lett. 49(7), 486–488 (2013)
27. Chen, L.K., et al.: Breakthroughs in photonics 2014: optical physical-layer network coding, recent developments, and challenges. IEEE Photon. J. 7(3), 1–6 (2015)
28. Lu, G.W., et al.: Flexible and re-configurable optical three-input XOR logic gate of phase-modulated signals with multiscramm functionality for potential application in optical-physical-layer network coding. OSA Opt. Exp. 24(3), 2299–2306 (2016)
29. Li, M., et al.: Common-channel optical-physical layer network coding. IEEE Photonics Technol. Lett. 26(13), 1340–1343 (2014)
30. Zhang, M., et al.: Optical encryption/decryption of QPSK signal using FWM-based modulated XOR. Appl. Opt. 54(25), 7813–7819 (2015)
31. Guan, X., Chan, C.: Physical-layer network coding in coherent optical OFDM systems. OSA Opt. Express 23, 10057–10063 (2015)
32. Savva, G., et al.: Physical layer-aware routing, spectrum, and core allocation in spectrally-spatially flexible optical networks with multicore fibers. In: IEEE ICC (2018)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Giannis Savva received his B.Sc. degree in Electrical Engineering from the Department of Electrical and Computer Engineering at the University of Cyprus in 2017. He is currently a Ph.D. Candidate in the Department of Electrical and Computer Engineering at the University of Cyprus and a Research Assistant at the KIOS Research and Innovation Center of Excellence, University of Cyprus, Nicosia, Cyprus. Giannis is a Graduate Student Member of IEEE. His research interests are in the areas of telecommunications, resource allocation algorithms in spectrally-spatially flexible optical networks (SS-FONs), network planning, network coding, and physical layer security in optical networks.

Konstantinos Manousakis is a Senior Research Associate at the KIOS Research and Innovation Center of Excellence of the University of Cyprus. He holds a Diploma (2004) in Computer Engineering and Informatics from the University of Patras, Greece, an MSc (2007) and a Ph.D. (2011) from the same department. His research work has been published in more than 50 top tier journals and telecommunications conferences. His work has received a number of awards including a best paper award at CRITIS’2013. He is a Marie Curie Fellow, having been granted a Marie Curie Career Integration Grant for the period 2014–2018. Dr. Manousakis is the recipient of the “Cyprus Research Award—Young Researcher 2018” for the thematic area of Physical Sciences & Engineering which is awarded to a young researcher annually that has implemented high quality research work. Dr. Manousakis is a Senior Member of IEEE. His research interests include optimization algorithms for high speed networks, security in optical networks, network coding, protection, restoration techniques, and techno-economic aspects of communication networks.

Georgios Ellinas holds a B.S., M.Sc., M.Phil., and a Ph.D. in Electrical Engineering from Columbia University. He is a Professor of Electrical and Computer Engineering, the Chair of the Department of Electrical and Computer Engineering, and a founding member of the KIOS Research and Innovation Center of Excellence at the University of Cyprus. Previously, he served as Associate Professor of Electrical Engineering at the City College of New York (2002–2005), Senior Network Architect at Tellium Inc. (2000–2002), and Research Scientist/Senior Research Scientist at Bell Communications Research (Bellcore) (1993–2000). Prof. Ellinas is a Fellow of the IET (2019), a Senior Member of IEEE and OSA, and a Member of ACM, and the Marie Curie Fellows Association (MCFA). He has co-authored/co-edited four books on optical networks, more than 230 archived articles, conference papers, and book chapters, and he is the holder of 30 patents on optical networking. His publications have received more than 5000 citations. His research interests are in telecommunication networks, transportation networks, IoT, and critical infrastructure systems.