Eavesdropping-Aware Routing and Spectrum/Code Allocation in OFDM-Based EONs Using Spread Spectrum Techniques

Giannis Savva, Konstantinos Manousakis, and Georgios Ellinas

***Abstract*—In this work, eavesdropping-aware routing and spectrum/code allocation techniques are proposed for elastic optical networks (EONs) using orthogonal frequency division multiplexing (OFDM). To introduce physical (optical) layer security and protect these networks against eavesdropping attacks, spread spectrum (SS) with signal overlapping techniques are used to encode each requested confidential connection. In order to make sense of accessed information and compromise a confidential connection, an eavesdropper will now have to lock on the correct frequency, determine the correct code and symbol sequence among co-propagated overlapped signals, and decode the signal. Different novel policies are presented for the assignment of spectrum and the codes for each confidential demand along with different routing strategies, resulting in an extra layer of security for confidential demands. Depending on the spectrum/code allocation and routing policies utilized, different (extra) levels of security are added for confidential connections while also considering the spectrum utilization, the blocking rate, and the algorithmic time complexity required for connection provisioning.**

***Index Terms*—Eavesdropping; Elastic optical network (EON); Optical layer security (OLS); Routing and spectrum allocation (RSA); Spread spectrum (SS).**

I. Introduction

The ever-increasing growth of traffic in backbone networks is expected to exceed the available capacity provided by the fixed-grid wavelength division multiplexed (WDM) technology. Orthogonal frequency division multiplexing (OFDM)-based networks, often called elastic optical networks (EONs), have recently been proposed by the research community to address this bandwidth crunch. Flexible-grid networks provided by EONs can now handle traffic demands via the elastic allocation of spectrum, contrary to the fixed grid utilized in WDM networks. For instance, due to orthogonality, flexible-grid networks can now split the C-band into slices of 25, 12.5, and 6.25 GHz compared to the 50 GHz spacing of fixed-grid networks. Thus, each demand is now allocated to a number of spectrum slices, called frequency slots, leading to a more efficient utilization of spectrum resources [1–3].

In EONs, to provision a connection, the routing and spectrum allocation (RSA) problem must be solved, which includes finding a path (routing) and a required spectrum allocation (SA) for the given demand. Any feasible RSA solution must satisfy three constraints: (i) the *spectrum continuity constraint*—each demand must be allocated the same frequency slots 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 slots serving each demand must be contiguous [3,4].

In EONs, optical fibers transfer enormous amounts of data over small periods of time. Hence, important security issues arise, since even short attacks can still compromise large amounts of data. Therefore, it is important to ensure that security is considered in these evolving communication networks. Physical-layer security, also known as optical layer security (OLS), offers various benefits to the entire network. For instance, implementing a secure protocol in the optical layer could relax security measures in the upper layers and thus improve throughput. Further, if the optical layer is not properly secured, any secure protocol implemented at the upper layers would still be susceptible to attacks through the lower layers, and thus valuable information can still be extracted [5,6]. Therefore, by enabling OLS, the information of all higher layers will be hidden to an eavesdropper, making the confidential connections more secure.

OLS has received considerable attention from the research community in the last few years and can be divided into different categories based on the type and the purpose of the threat. 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) [5,7,8]. In this work, we focus on confidentiality, where an adversary tries to access confidential data from an optical communication channel

Manuscript received April 9, 2019; revised May 28, 2019; accepted May 30, 2019; published June 27, 2019 (Doc. ID 364694).

The authors are with the KIOS Research and Innovation Center of Excellence and the Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus (e-mail: savva.giannis@ucy.ac.cy).

https://doi.org/10.1364/JOCN.11.000409

(also known as 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 the adjacent spectrum by confidential signals [7,9]. Such attacks can have very serious consequences since, due to their nature, they can potentially go undetected for a prolonged period of time.

Quantum key distribution (QKD) can provide the optimal physical-layer security in optical networks using concepts of quantum physics and information theory. However, the drawbacks for using such technology include the maximum possible rate and distance, since the maximum key generation rate using QKD is around 100 kb/s over 50 km of installed fiber [10]. This signifies that substantial progress is still required prior to a practical implementation of QKD against eavesdropping attacks in backbone networks.

Another promising solution to increase confidentiality in optical communications is optical encoding [11]. In optical encoding, data are encoded using a unique key known to the source and destination nodes. Thus, even if an adversary accesses any data transmitted in the network, using that information will be practically useless without knowledge of the key. Such techniques require a key generation and a unique code allocation for each demand. Spread spectrum (SS) is a well-known technique that can be used for optical encoding in optical networks, since it uses unique keys to modulate signals [11]. SS techniques such as optical code division multiple access (OCDMA) have been proposed and demonstrated by several works in various flavors to implement optical encoding [11–13].

This work focuses on security against attacks on confidentiality in EONs and proposes a novel eavesdropping-aware solution to the RSA problem for a network planning scenario. Our previous work in [14] and [15] introduced SS techniques in EONs to increase security through optical encoding and signal overlapping. In order to make sense of confidential information accessed by an attacker through eavesdropping, the correct code and correct symbol sequence among co-propagated overlapped signals must be determined, making it extremely difficult for the eavesdropper to compromise any confidential connections. This work significantly extends our previous works ([14] and [15]) by (i) proposing additional novel policies for the spectrum/code assignment of confidential connections (including their complexity analysis) and subsequently comparing them to the ones presented in previous works; (ii) presenting different scenarios, where the eavesdropper has different levels of knowledge of the network operational parameters, and comparing each spectrum/code policy and different routing strategy to ascertain their level of security for each scenario (presenting a security analysis for the confidential connections that are established in the network for each scenario); (iii) presenting additional results on the code allocation when utilizing different spectrum allocation policies, followed by a comparison regarding the randomness of each technique; and (iv) significantly extending the performance evaluation of the proposed algorithms in terms of the blocking probability, the spectrum efficiency of each spectrum/code assignment policy and routing strategy, and the time complexity of implementing each technique.

In the rest of this paper, state-of-the-art OLS techniques are discussed in Section II, followed by a brief discussion on the SS technique and orthogonal variable spreading factor codes in Section III. Then, in Section IV, eavesdropping-aware heuristics are proposed to solve the RSA problem with novel routing and spectrum/code assignment policies, followed by their complexity analysis, while in Section V a comparison is presented in terms of the level of security each one provides. The performance evaluation of these policies is presented in Section VI, followed by Section VII, which offers some concluding remarks.

II. Related Work

There are only a few (recent) works in the literature on how to protect the network against eavesdropping attacks in EONs. Specifically, in [16], the authors propose an eavesdropping-aware RSA algorithm in which a demand uses a set of different paths in the network to establish a connection. The signal is split at specific links in the path based on the probability of eavesdropping for each link and node that is calculated based on geographical data (links close to cities, banks, etc.) and historical events (previous acts of eavesdropping). Hence, each request has a level of confidentiality. Thus, if the probability of eavesdropping is high for a confidential connection, then another path must be found. However, in practice, there are eavesdropping attacks that are not recognized even after a part of the network has been compromised. Hence, a "weak" link (in terms of confidentiality) could be falsely categorized as secure, which would lead to data transmission susceptible to eavesdropping.

Further, in [17], the authors propose a reallocation technique to increase security in optical networks. In that work, spectrum slots are reallocated after random times, while considering the blocking performance. Hence, it is difficult for an adversary to find, lock, and keep track of the appropriate bandwidth that the connection uses, since it changes frequency slots at random times. Thus, the eavesdropper cannot obtain all the confidential data for a specific connection. However, for such a technique to work, each time a reallocation takes place, the spectrum required for the reallocation must be available at that time, and therefore, demands must pre-allocate additional bandwidth to be used during the reallocation procedure. Thus, the complexity of the provisioning procedure increases considerably.

Also, in [18], the authors perform a physical-layer security analysis in the optical fiber using a wiretap channel in an OCDMA system. In this analysis, several parameters such as the security leakage factor, the number of active users, the codes used, and the transmission distance are taken into consideration in order to calculate the probability of the eavesdropper decoding a signal. Thus, the security analysis of the legitimate user's data transmitted is performed. In that work, the authors conclude that the number of active users and the code length used can improve the security of the system. Additionally, the use of linear network coding (LNC) in optical networks to protect connections from security threats such as eavesdropping and jamming attacks is studied in [19]. A security analysis of LNC in EONs and its effectiveness against an eavesdropping or jamming attack is also investigated. However, the design of RSA strategies that can exploit the benefits of using such LNC in EONs for security purposes is left as an open problem.

Finally, in [6], an overview of key-based and keyless encryption and physical-layer security techniques is provided in the context of optical multiple-input-multiple-output space-division-multiplexed (MIMO-SDM) fiber-optic communication systems. That work primarily discusses how the unique channel characteristics of MIMO-SDM can be exploited to provide various levels of physical-layer security and how these concepts and frameworks can serve as a baseline for developing new and enhanced physical-layer security solutions for future MIMO-SDM systems.

This work, as outlined below, extends the state of the art by presenting novel routing and spectrum/code allocation strategies that can be used during connection provisioning to provide an additional layer of security for the requested confidential connections, while at the same time ensuring that the utilization of the network resources, the blocking rate, and the computation complexity of the provisioning algorithms are not affected in a significant manner.

III. Spread Spectrum and Signal Overlapping

This section provides a brief tutorial on SS and signal overlapping. It is similar to what was presented in [15]. However, it is included here because an understanding of this technique is central to the remainder of the paper.

A. Spread Spectrum Technique

SS is a technique in which a signal is spread in the bandwidth domain by modulating the signal in the code dimension using a specific code sequence [11]. The bandwidth spreading for each connection depends on the code used. At the receiver, the signal is demodulated to its original bandwidth with the use of the same code. Therefore, the transmitter and the receiver must have knowledge of the code used to establish a connection. Further, multiple signals can share the same bandwidth as long as each signal uses a different code. Hence, signals can overlap, leading to an increase in resource utilization efficiency. However, each signal can experience interference from overlapping signals {multiple access interference (MAI) [5]}. To minimize MAI and its effect on the probability of error for overlapping signals, a codeset of orthogonal codes can be used. In the literature, several approaches can be found for the creation of orthogonal codesets (e.g., Walsh–Hadamard, Gold, and Kasami codes). Each of these codesets has benefits and drawbacks regarding the size of the codeset and the relationship among codes within the same codeset. Due to the dynamic nature of connections and the randomness of their requested data rates, any technique chosen must be flexible in the amount of bandwidth spreading for each connection.

B. Orthogonal Variable-Spreading-Factor Codes

Orthogonal variable-spreading-factor (OVSF) codes can provide the required flexibility for the RSA problem and significantly decrease the probability of decoding a signal in the network without knowledge of the code. Each OVSF code can be categorized based on the spreading factor (SF) it provides. As presented in Fig. 1, OVSF codes can be visualized as a tree where the spreading factor is 1 at level 0 and it doubles at each subsequent level down the tree. Thus, at a given level i, the number of available codes is 2^i. Also, at each level, the codeset is the same as the one provided by the fixed Walsh–Hadamard codes at that spreading factor [20].

In OVSF codes, a code is orthogonal to all codes at the same level. Also, a code from a given level can be orthogonal to codes at different levels as long as the following constraint is satisfied: *a code is not orthogonal to its parents or its children as presented in the tree* [20].

Figure 1 illustrates an example where three signals are assigned to codes at different levels. Each code and the ones not orthogonal to it are shown in the same color. Different colors represent the three different signals. In this example, all three signals use orthogonal codes, and therefore they can share the same bandwidth without any interference. Signals 1 (yellow) and 2 (green) use a code with spreading factor 4, whereas signal 3 (blue) uses a code with spreading factor 8. Other signals can still be allocated the same bandwidth as long as they use any of the uncolored nodes.

Using OVSF codes for modulating connections improves optical layer security, since an eavesdropper has to try all possible combinations of symbol sequences to decode a signal. Even in the case where the eavesdropper uses only orthogonal codes to decode and compromise confidential information, due to the relationship of the codes that exist at each level, the eavesdropper will still not be able to detect which code gives the correct result. Further, since connections overlap within the same bandwidth, each signal appears as random noise to the eavesdropper trying to make

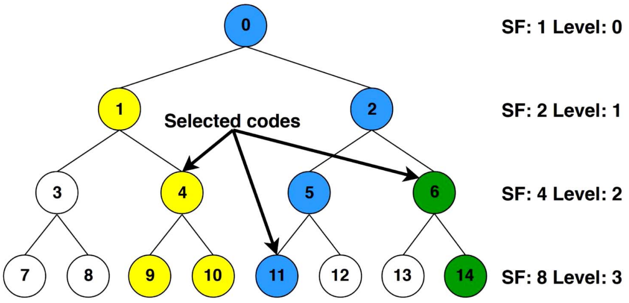

Fig. 1. Visualization of OVSF codes. Each level offers a different spreading factor [20].

sense of any accessed data. Thus, any energy detection approach aiming to acquire the code used for a given connection would not compromise security in the network.

OVSF codes offer various advantages in EONs, since each signal can experience different spreading based on network parameters such as the available spectrum, the data rate of each connection request, the allowed modulation format based on the path chosen, and the spreading codes that other overlapping signals utilize. However, as previously mentioned, spreading can downgrade the network's performance in terms of throughput and spectral efficiency, since spreading the signal to increase security also increases the number of slots required to accommodate each connection. To overcome this, new RSA strategies must be developed with an aim to find and allocate the best paths in terms of spectrum resources while also enabling overlapping between connections. This is precisely the focus of this work.

IV. Eavesdropping-Aware RSA Heuristic Algorithm

The proposed eavesdropping-aware RSA algorithm is divided into the routing (R) and spectrum allocation (SA) sub-problems. Since this is a network planning scenario, the set of demands (D) is 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 that describes the demand as confidential (1) or not confidential (0). It is noted that the proposed approach considers only either confidential or non-confidential connections so as to investigate the effect of the security policies on the spectrum utilization for a worst-case scenario (providing the maximum security for the confidential connections). The reader should note that this approach can also apply for different confidentiality levels for each connection, based on spreading and overlapping thresholds applied to each different level of confidentiality. This, however, is left as future work.

A. Routing

For the routing sub-problem, a number of k candidate paths that are able to satisfy a requested connection are found. These k-shortest paths can be subsequently sorted based on the number of hops, the minimum path length (which would result in the highest modulation format used), or a hybrid method that takes into account the ratio of these two parameters [21]. However, all aforementioned metrics aim to produce a solution that maximizes the spectrum efficiency without considering protection of the data against eavesdropping attacks.

In this work, the *confidential connections overlap (CCO)* metric that counts the number of links in each path that carry confidential connections [15] is utilized, in conjunction with three different routing strategies for calculating the routes of all requested connections:

- **Maximum Overlap**: Candidate paths are sorted in descending order based on their CCO metric. Hence, demands are forced to use paths with links that are utilized by other confidential connections.
- **Fairness Distribution**: Candidate paths are sorted in ascending order based on their CCO metric. Using this strategy, confidential demands are allocated evenly throughout the entire network, leading to an equal distribution of resources for security purposes. Thus, demands of the same source-destination pair are distributed to different paths, providing a second level of security at the optical layer.
- **Spectrum Efficiency**: Candidate paths are sorted in ascending order based on a hybrid metric that takes into account both the number of hops and the modulation format that can be used on each path [21]. Using this strategy, the paths that require the least number of spectrum slots for each connection will be selected first, which will result in increasing the spectrum efficiency of the network. It is noted that this approach does not consider the *CCO* metric when sorting the candidate paths.

It is noted that for demands that are not confidential, the RSA algorithm uses the spectrum efficiency strategy in order to better utilize network resources. These strategies have trade-offs in terms of security and spectrum efficiency as amply demonstrated in Section VI.

B. Spectrum/Code Allocation

For the SA sub-problem, available spectrum resources must be allocated for a requested connection while also satisfying the slot *continuity* and *contiguity* constraints [4]. Due to the use of the SS technique, the *non-overlapping* slot constraint is now mitigated, as overlapping is partially allowed for confidential demands where spreading is enabled. Thus, each slot can be allocated to a number of demands as long as each demand in the same slot uses an orthogonal code. In order to combine OVSF codes with the solution to the RSA problem, each spectrum slot is modeled as a tree that keeps track of the codes used for that slot. Figure 2 shows an example of spectrum slots and their modeled trees, including allocated and free spectrum slots.

In the following algorithms, each colored node in the tree takes the value 1 and the uncolored nodes take the value 0. Also, the OR operation takes two binary values as inputs, and the result equals 0 if the value of both signals is 0; otherwise, it equals 1. Thus, by performing the OR operation between the same code along two spectrum slots, the

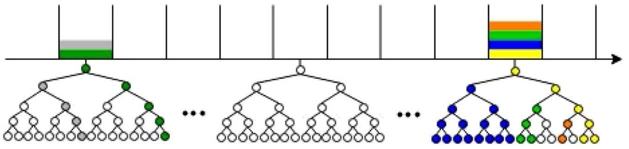

Fig. 2. Different spectrum slots and their modeled trees. Uncolored nodes represent codes that can be used for future connections.

resulting value will be equal to 0 if neither of the slots use that code or equal to 1 otherwise.

For the non-confidential connections, the candidate paths are sorted using the spectrum efficiency routing strategy and then the first path in the sorted list is selected. Since spreading is not performed for non-confidential connections, only the root node of each spectrum slot's tree is considered. If the root node has a value of 1, then at least one connection uses that slot for spreading, and thus the non-confidential connection cannot be allocated to that slot. On the other hand, if the root node has a value of 0, then the slot can be potentially used for that connection. Thus, a conventional RSA algorithm can be used for the spectrum allocation part, where first the spectrum slots of all links of the path selected are OR-ed to create one virtual link. Then, starting from the first spectrum slot, s_i in the virtual link, the algorithm performs the OR operation between spectrum slot s_i and the next $(F-1)$ spectrum slots, where F denotes the number of spectrum slots that the non-confidential connection requires [this can be obtained using Eq. (1) by setting SF = 1]. In the case that the selected path does not have any available resources to accommodate the connection, then the next candidate path is selected.

For confidential connections, the SA problem requires an additional step compared to typical spectrum allocation algorithms, that is, to find an available code that can be used in the selected spectrum slots for the requested connection. Hence, the SA problem now becomes the spectrum/code allocation problem. Also, the selected code must be orthogonal to all codes used by other demands in the same spectrum slots. Thus, the *code availability constraint* is introduced, which specifies that all slots allocated for a demand must use a code that maintains orthogonality between codes that are used by already established connections for the same set of slots. In this work, two different spectrum/code allocation policies are investigated. In the first policy, each confidential connection must allocate the same code among all spectrum slots in the chosen path (*code conservation constraint* [15]). In the second policy, a confidential connection can freely choose different codes for each slot. Irrespective of the chosen policy, the spectrum/code allocation must satisfy the *code continuity constraint* among all the links of the path for each slot.

1) Code Conservation Policy (CCP): The CCP must satisfy the *code availability* and also the *code conservation* constraints among all the selected slots. For this reason, each spectrum slot's tree has to be checked in order to find whether there exists an available code that can be used for all selected spectrum slots. The proposed policy is described in Algorithm 1.

Algorithm 1. Code Conservation Policy (CCP)

```
Input: Graph $G(V,E), D, k$
Output: Connection Assignment
Calculate $k$-shortest paths set $P$ for each $s$–$d$ pair using one of the routing strategies
for each request $r(s_r, d_r, B_r, 1) \in D$ do
    Select first shortest path $p \in P_{s_r-d_r}$
    loop 1:
    Create virtual link $v_l$ using the OR operation between the slots with the same id in all links $\in p$ and set $i = 1$
    loop 2:
    $V_{\text{tree}}$ = tree of spectrum slot $s_i$, set $j = 1$
    repeat
        $V_{\text{tree}} = V_{\text{tree}}$ OR $s_{i+j}$
        $j = j + 1$
    until $V_{\text{tree}}$ does not have an available code or the max number of slots is OR-ed [Eq. (1)]
    Find an available code in $V_{\text{tree}}$ that achieves the requested bit rate [Eq. (2)] based also on the number of slots OR-ed and the modulation format
    if an available code is found then
        Request is established, move to next request $r$
    else
        if $i ==$ maximum slot id then
            if all paths $\in P_{s_r-d_r}$ are checked then
                Request is rejected, move to next $r$
            else
                goto loop 1, using the next path $p \in P_{s_r-d_r}$
            end if
        else
            goto loop 2 and set $i = i + 1$
        end if
    end if
end for
```

In CCP, initially, the candidate path that is first in the sorted list based on the routing strategy chosen is selected. Then, to create the virtual link (v_l) that characterizes the path that is chosen, an OR operation is performed among the links within the selected path. Starting from the first spectrum slot, s_i in v_l, the virtual tree (V_{tree}) takes the value of s_i. Then, an OR operation is further performed between V_{tree} and spectrum slot s_{i+1}, and the resulting tree is stored in V_{tree}. This process is repeated until V_{tree} does not have any available codes or the number of spectrum slots checked reaches the maximum number of slots used [obtained from Eq. (1) using the maximum spreading factor]. If an available code is found in V_{tree} that can be used to accommodate the given connection, then the selected code is available on all selected spectrum slots, and the connection is established. In the case that a code is not available, the algorithm restarts the process from spectrum slot s_{i+1}. Further, if the path does not have any available resources to accommodate the given connection, then the next candidate path is selected.

For each requested connection, Eq. (1) is used to calculate the number of slots required based on the spreading factor utilized, while Eq. (2) is used to calculate the maximum bit rate [gigabits per second (Gbps)] that can be supported.

$$\text{Number of Slots} = \left\lceil \frac{\text{Requested Gbps} \cdot \text{SF}}{\text{Baud Rate} \cdot \text{Mod Format}} \right\rceil \tag{1}$$

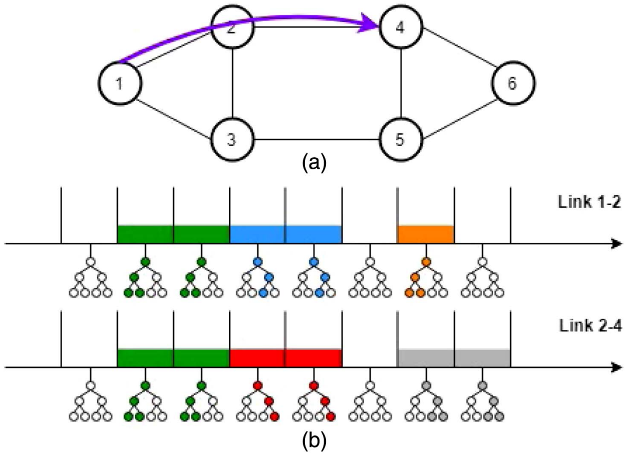

Fig. 3. (a) Six-node simple network. (b) Spectrum slots in links 1–2 and 2–4. Each color represents already established connections.

$$\text{Gbps} = \frac{\text{Num of Slots} \cdot \text{Baud Rate} \cdot \text{Mod Format}}{\text{SF}_{\text{selected}}} \qquad (2)$$

The following example illustrates the proposed SA procedure for a given connection. In Fig. 3(a), a six-node network is presented where each frequency slot supports a baud rate equal to 10.7 Gbaud. A connection requests 30 Gbps from node 1 to node 4, and the maximum spreading factor used for each spectrum slot in the network is set to 4. The path that is chosen to serve the demand is (1–2, 2–4), using quadrature phase-shift keying (QPSK) modulation format. In Fig. 3(b), all links in the path are represented, and each slot's tree is shown. In order to find a set of spectrum slots that can use the same code to allocate a given connection, each slot with the same id is OR-ed with trees from other spectrum slots at each link. For example, each spectrum slot tree with id = 1 within the links of the selected path will be OR-ed, and the spectrum slot with id = 1 in the virtual link will present this result. This process forms a virtual link v_l that represents the chosen path [shown in Fig. 4(a)].

As for this example the maximum number of spectrum slots required is 3 [Eq. (1)], the resulting (virtual) tree, shown in Fig. 4(b), can be utilized to determine whether there exists a code in the group of checked slots that can be used through all the links in the path. In this example, the rightmost code at the lowest level can be used, and the demand will allocate three spectrum slots in each link. It is noted that, following this procedure, the resulting solution satisfies the slot *continuity*, *contiguity*, *code availability*, as well as *code conservation* constraints.

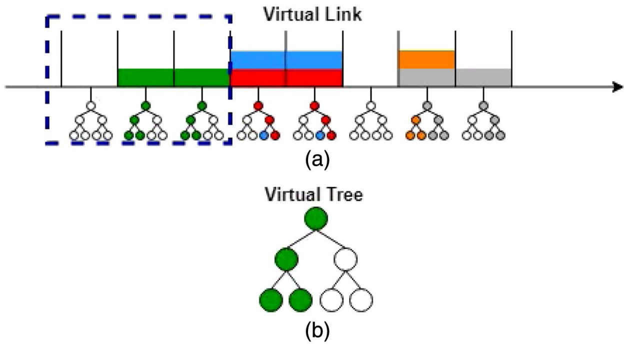

Fig. 4. (a) Virtual link created after links 1–2 and 2–4 are OR-ed. (b) The resulting virtual tree when three slots in the virtual link are OR-ed.

2) Free Code Assignment Policy (FCAP): The FCAP must satisfy the *code availability* and *continuity* constraint without the requirement of the *code conservation* constraint among all the selected slots. This policy requires only that the selected codes among all frequency slots have to be orthogonal. This policy is a more complex one, since the sum of all frequency slots and their spreading factors used must be calculated prior to the allocation of a given demand [Eq. (3)]. This policy is described in Algorithm 2.

Algorithm 2. Free Code Allocation Policy (FCAP)

```
Input: Graph $G(V, E), D, k$
Output: Connection Assignment
Calculate $k$-shortest paths set $P$ for each $s$–$d$ pair using one of the routing strategies
for each request $r(s_r, d_r, B_r, 1) \in D$ do
    Select first shortest path $p \in P_{s_r-d_r}$
  loop 1:
    Create virtual link $v_l$ using the OR operation between the slots with the same id in all links $\in p$ and set $i = 1$
  loop 2:
    Starting from $s_i$ in $v_l$, find the first group of slots [with maximum group size calculated by Eq. (1)] that have at least one available code
    Find an available code for each slot in the selected group that achieves the requested bit rate based also on the modulation format used [Eq. (3)]
    if requested bit rate is achieved [Eq. (3)] then
        Request is established, move to next request $r$
    else
        Change a code for a randomly selected slot to a lower spreading factor until the requested bit rate is achieved [Eq. (3)] or any of the codes selected reaches the SF threshold
        if requested bit rate is achieved [Eq. (3)] then
            Request is established, move to next request $r$
        else
            if $i ==$ maximum slot id then
                if all paths $\in P_{s_r-d_r}$ are checked then
                    Request is rejected, move to next $r$
                else
                    goto loop 1, using the next $p \in P_{s_r-d_r}$
                end if
            else
                goto loop 2 and set $i = i + 1$
            end if
        end if
    end if
end for
```

In FCAP, as also described in Algorithm 1 for CCP, initially the candidate path that is first in the sorted list based on the routing strategy chosen is selected, and an OR operation is performed among the links within the selected path to create the virtual link v_l, which characterizes the path that is chosen. Next, the algorithm starts from the first spectrum slot, s_i in v_l, and finds the group of frequency slots [utilizing Eq. (1) to obtain the maximum size of the group], where each spectrum slot has at least one available code. Then, for each spectrum slot, the first available code with the largest spreading factor is chosen, and if the group of frequency slots along with the codes selected are able to achieve the requested bit rate [Eq. (3)], then the connection is established. In case the requested bit rate is not achieved, a spectrum slot from the selected group is randomly chosen and its code is changed to an available code with a lower spreading factor (Step 10, Algorithm 2). This process is repeated until the requested bit rate is achieved [Eq. (3)] or any of the codes selected reach the SF threshold. If the selected group of resources is not able to establish the given connection, the algorithm repeats the process starting from spectrum slot s_{i+1}. Further, if the path does not have any available resources to accommodate the given connection, then the next candidate path is selected.

For any spectrum slot used by a confidential connection, the transmitted data must have at least an SF equal to 2 (as can be seen in Fig. 1) to enable spreading in the bandwidth domain.

$$\text{Gbps} = \sum_{i=1}^{\text{Num of Slots}} \frac{\text{Baud Rate} \cdot \text{Mod Format}}{\text{SF}_i} \qquad (3)$$

Qualitative Policy Comparison: Compared to typical RSA approaches, where the number of slots is predetermined during the routing process (based on the acceptable modulation format given by the path's length), the problem now becomes more difficult to solve since the number of spectrum slots required changes based on the available codes that can be used when either one of the two policies is utilized. Clearly, higher levels of spreading offer additional advantages in terms of network security, since larger codes are now used to modulate each signal, and thus more signals can overlap in the bandwidth domain, which subsequently increases the difficulty in making sense of accessed confidential information. Thus, both proposed policies aim at maximizing the spreading factor of each confidential connection when spectrum slots are available to satisfy a given demand by choosing codes with a higher spreading factor for each demand when multiple codes are available. This is achieved by searching through the trees starting from the lower levels and moving up to the root.

Each policy offers benefits and drawbacks regarding the spectrum efficiency of the network, the blocking rate, and the number of computations required for the spectrum/code allocation of a given demand. Also, the security provided for a confidential connection must be quantified for each spectrum/code allocation policy utilized. A qualitative comparison of the two proposed policies is presented below, followed by an extensive quantitative analysis (in conjunction with the proposed routing strategies) in the security analysis and performance sections (Sections V and VI, respectively) that follow.

First, looking at the computational complexity of the proposed policies, the CCP policy offers lower computational complexity in the spectrum/code allocation for a confidential demand compared to FCAP, since in CCP a group of frequency slots able to establish a given connection are found after a number of OR operations, whereas FCAP tries to find a feasible combination of codes for a given demand, as different codes can be assigned for each spectrum slot allocated to a confidential connection. However, using CCP reduces the flexibility of the algorithm, since in this approach the same code must be assigned for all frequency slots used for a given connection, which would increase the network's blocking rate.

On the other hand, FCAP provides higher spectrum efficiency due to the flexible allocation of different codes for the same confidential demand. Moreover, the security of a connection is further increased, since the eavesdropper has to find the spectrum that is used for the selected demand followed by decoding the code that is used for each spectrum slot independently, which is a difficult, complex, and time-consuming procedure. In addition, all codes used for each slot must now be known to both the source and the destination nodes, as opposed to CCP, where only a single code must be known by both the source and destination nodes.

In the following example (Fig. 5), both policies allocate spectrum for a 40 Gbps connection request from node 1 to node 4 in the network illustrated in Fig. 3, with the same link states and the same route chosen. Using the CCP approach, the resulting virtual tree (in green) is created when the first three frequency slots are OR-ed, as shown in Fig. 5(b). Next, the following frequency slot is also considered and the resulting virtual tree does not have an available code. As a result, these three slots (in green) will have to be checked to determine if they can accommodate the given demand. For this example, they cannot accommodate the given connection, as four frequency slots are required when using $\text{SF} = 2$ [Eq. (1)], and thus the algorithm moves to the next available group of frequency slots. On the other hand, using FCAP, the first six spectrum slots that have at least one available code are selected, as shown in Fig. 5(c). In this case, the codes are freely selected as long as the overall requested Gbps rate is met. As shown (in purple), two frequency slots use codes with $\text{SF} = 2$ and the remaining frequency slots use a code with $\text{SF} = 4$, the sum of which satisfies the requested connection rate [Eq. (3)].

Complexity Analysis: In this section, the complexity of each proposed algorithm is presented. In this analysis, the following notations are used: $|V|, k, |D|, |C|, M, F_m$, and $\text{SF}_{\max}$, which denote the number of nodes, number of candidate paths, number of requests, overall number of codes that can be used, number of spectrum slots in each optical fiber, maximum number of frequency slots requested by each connection, and maximum spreading factor used, respectively.

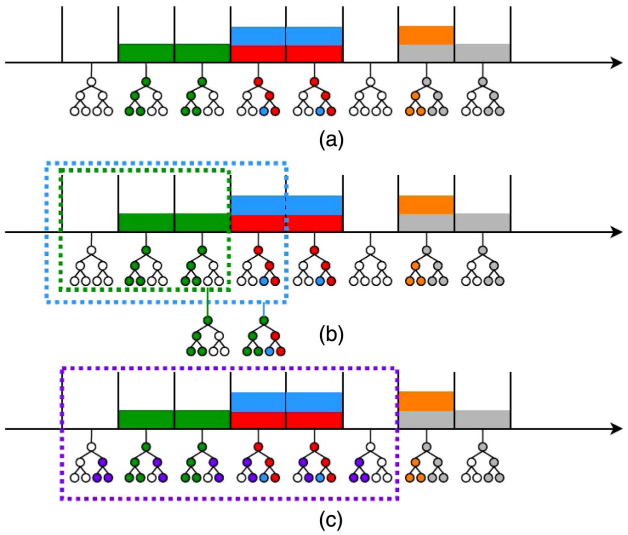

Fig. 5. (a) Virtual link created after links 1–2 and 2–4 are OR-ed. Spectrum/code allocation procedure using (b) CCP and (c) FCAP.

The calculation of k-shortest paths is performed offline, and the proposed algorithms use that pool of candidate paths. The complexity of calculating all candidate paths is $\mathcal{O}(k|V|^3)$. Also, for the following cases, the complexity of allocating one request and one candidate path is presented, meaning that the overall complexity of each algorithm in the worst case will be multiplied by $|D|k$.

For the non-confidential connections, the complexity of the algorithm is $\mathcal{O}(|V|M + MF_m)$. The term $|V|M$ corresponds to the number of computations needed to create the virtual link, considering that in the worst case, the paths selected would have a total of $|V|$ links. The term MF_m corresponds to F_m computations that are required to find if the selected group of frequency slots is available for the spectrum allocation, which will be at most repeated M times.

The overall complexity of the CCP policy is $\mathcal{O}(|V|M|C| + MF_m|C| + M|C|)$. The term $|V|M|C|$ corresponds to the calculations required to create the virtual link v_l, since the OR operation must be performed $|C|$ times for all M spectrum slots. Next, to calculate V_{tree}, the OR operation must be performed $|C|$ times between F_m spectrum slots, while in the worst case, all groups of spectrum slots would have to be checked, which is upper bounded by M. Finally, for each group of frequency slots checked, at most $|C|$ different calculations must be performed in order to find the code and spreading factor that will be used for the confidential connection.

For the FCAP policy, the overall complexity of the algorithm is $\mathcal{O}(|V|M|C| + MF_m|C| + MF_m^3\log_2(\text{SF}_{\max}))$. As presented above, the term $|V|M|C|$ corresponds to the calculations required to create v_l. Now, at most $|C|$ operations must be performed for each spectrum slot in the group of F_m slots selected to check if an available code exists, which could be performed M times at most, contributing the term $MF_m|C|$ to the complexity of the algorithm. Finally, for the selected group of frequency slots F_m, the set of chosen codes could be changed at most $F_m\log_2(\text{SF}_{\max})$ times (i.e., to select a code with a lower SF), and each time, the sum between F_m components must be calculated [Eq. (3)]. Thus, this process contributes term $MF_m^3\log_2(\text{SF}_{\max})$ to the complexity of the algorithm.

V. Security Analysis

Each policy offers benefits and drawbacks regarding the spectrum efficiency of the network and the number of computations required prior to spectrum/code allocation for a given demand. Also, the security provided for a confidential connection must be quantified for the used spectrum/code allocation policy. Therefore, in the next subsections, the proposed policies are compared based on the security that each policy provides.

The number of combinations that an eavesdropper has to try in order to decode a given connection is a metric that can be used to quantify the security provided by the two policies. Table I presents the number of combinations required by the eavesdropper when each policy is in use and for three different cases where the eavesdropper has different levels of knowledge for the network's operational parameters (described below). Also, the typical RSA approach is shown as a reference point. The following abbreviations are used for the different policies: typical RSA (T), CCP (P1), and FCAP (P2). Further, in Table I, M is defined as the number of frequency slots in each optical fiber, n is defined as the number of levels for the SF used, and x is defined as the number of frequency slots used by the connection under investigation.

Case 1: In this case, it is assumed that the eavesdropper knows several network parameters such as the overall number of frequency slots, the data rates and the modulation formats used, the policy used to allocate the spectrum, the different lengths of codewords, and the maximum spreading factor used. The eavesdropper must first find and lock on the correct frequency used by the given connection. The combinations of slots that can be allocated while satisfying the spectrum allocation constraints is $\frac{M\cdot(M+1)}{2}$. In typical RSA approaches, the eavesdropper could now acquire the signal and make sense of the accessed data. However, if the CCP approach is used, the eavesdropper must also consider the code used. Since it is assumed that the eavesdropper knows the possible length of the codewords, all possible code combinations must also be checked in order to find the correct one. The overall number of codes that can be used when only the length of the codes is known is $\sum_{i=1}^{n} 2^{2^i}$. Using FCAP, this procedure becomes much more difficult, since now the eavesdropper must check a different number of combinations based also on the number

TABLE I
Code Combinations for Each Policy for Cases 1–3

	Case 1	Case 2	Case 3
T	$\frac{M\cdot(M+1)}{2}$	–	–
P1	$\frac{M\cdot(M+1)}{2}\cdot\sum_{i=1}^{n} 2^{2^i}$	$\sum_{i=1}^{n} 2^{2^i}$	$\sum_{i=1}^{n} 2^{i}$
P2	$\sum_{i=1}^{M}(i\cdot(\sum_{j=1}^{n} 2^{2^j})^{M-i+1})$	$(\sum_{i=1}^{n} 2^{2^i})^x$	$(\sum_{i=1}^{n} 2^{i})^x$

TABLE II
FCAP—Number of Combinations

Number of Frequency Slots	Combinations (Slot id)	Number of Code Choices	Overall Combinations
1	1 2 3	$(\sum_{j=1}^{n} 2^{2^j})^1$	$3 \cdot (\sum_{j=1}^{n} 2^{2^j})^1$
2	1–2 2–3	$(\sum_{j=1}^{n} 2^{2^j})^2$	$2 \cdot (\sum_{j=1}^{n} 2^{2^j})^2$
3	1–3	$(\sum_{j=1}^{n} 2^{2^j})^3$	$(\sum_{j=1}^{n} 2^{2^j})^3$

of different frequency slots considered for the connection. Thus, the overall number of combinations can be found as $\sum_{i=1}^{M}(i \cdot (\sum_{j=1}^{n} 2^{2^j})^{M-i+1})$. As an example, in Table II, all possible slots and code combinations are presented for $M = 3$ when FCAP is utilized.

Case 2: In this case, it is assumed that the eavesdropper also knows (or has found) the correct group of frequency slots used by the connection. In this case, no further actions are required from the eavesdropper when the typical RSA approach is in use, whereas the eavesdropper will still need to check all codes in that bandwidth when CCP is used. Since the same code must be used in all selected frequency slots, the number of code combinations checked by the eavesdropper is independent of the number of frequency slots used by that connection. On the other hand, when FCAP is in use, the code combinations are a function of (i.e., powered by) the number of frequency slots used by that demand, since each frequency slot can now freely use a different code as long as one is available.

Case 3: In this case, it is assumed that the eavesdropper knows the exact group of frequency slots used and also the exact codeset used by the provider in order to encode each signal. Thus, the number of codes that the eavesdropper has to try is now reduced from $\sum_{i=1}^{n} 2^{2^i}$ to $\sum_{i=1}^{n} 2^i$ for the CCP case, whereas this sum is a function of the number of slots allocated to the connection when FCAP is in use.

In Table III, the number of combinations required to make sense of accessed data is shown for these three cases for different values of M, n, and x. As shown, FCAP clearly outperforms CCP in terms of the number of combinations required by the eavesdropper to find the correct code. Also, CCP provides a static number of combinations based only on initial parameters of the network (i.e., number of frequency slots, codeset size), whereas for FCAP the number of combinations is also a function of the number of slots used by each connection. Therefore, a large number of frequency slots will result in a significantly larger number of code combinations that the eavesdropper will have to perform in order to decode the accessed data.

TABLE III
Example of Number of Combinations

		Case 1	Case 2	Case 3
$M = 320$	Typical RSA	10^5	–	–
$n = 3$	RSA-CCP	10^8	10^3	10^1
$x = 5$	RSA-FCAP	inf	10^{16}	10^{11}
$M = 320$	Typical RSA	10^5	–	–
$n = 4$	RSA-CCP	10^{10}	10^5	10^1
$x = 10$	RSA-FCAP	inf	10^{52}	10^{19}
$M = 320$	Typical RSA	10^5	–	–
$n = 4$	RSA-CCP	10^{10}	10^5	10^1
$x = 20$	RSA-FCAP	inf	10^{101}	10^{34}

It is important to note that Cases 2 and 3 are very specific cases in which the eavesdropper knows many critical parameters (exact frequency slots and codesets) used in the network and that even for Case 1 the eavesdropper possesses important information regarding the operation of the network. Nevertheless, in all cases, even with the information possessed, it will still be extremely difficult for the eavesdropper to find and decode the correct sequence of information bits. This is due to the relationship between the codes used, since for any state of the codes that are used in a frequency slot, several codes will also result in possible solutions when using any of the two proposed policies.

Further, FCAP provides many more code combinations due to the free allocation of codes for each connection. Thus, the adversary will end up with multiple candidates that all provide acceptable signals. Moreover, any other signals allocated to different codes in the same frequency slots will act as random noise to the eavesdropper trying to decode confidential data (the graphical representations in the next section visualize the spectrum and code assignments so as to demonstrate the aforementioned benefits of these policies). Finally, it is noted that the number of combinations required by the eavesdropper to find the correct modulation format and the symbol sequence used in each demand are excluded from this analysis. These parameters, if not known, will also increase the number of combinations required by the eavesdropper to decode the confidential data.

VI. Performance Evaluation

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 12.5 GHz, which results in a total of 320 spectrum slots per link in the network with a baud rate of 10.7 Gbaud for each frequency slot. The network topology that is used in all simulations is the NSF network, which consists of 14 nodes and 21 undirected links as presented in Fig. 6.

In all cases, demands are randomly generated using a uniform distribution for all source-destination pairs, where each demand size varies from 40 to 140 Gbps. Each presented result is the average of 20 simulations performed with different generated sets of demands on a PC with an $i5 - 8400$ CPU and 8 GB RAM, while the proposed approach was implemented in the C programming language. Also, in all cases, 60% of the overall number of demands are set to confidential.

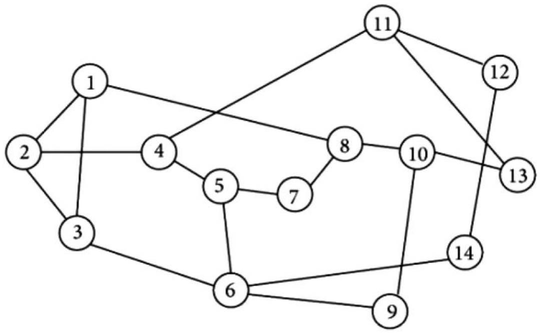

Fig. 6. NSF network that consists of 14 nodes and 21 undirected links.

First, the results of different maximum spreading factors using the CCP and FCAP policies for solving the RSA problem are presented. To evaluate each spreading factor, the number of spectrum slots utilized in each case is illustrated. Also, the spectrum efficiency (SE) strategy is used, since the number of spectrum resources is used as the evaluation criterion.

As shown in Fig. 7, with a maximum spreading factor of 2, 4, 8, and 16, the spectrum resources required, even though greater than what is required when the SE approach is used, do not increase proportionally to the spreading factor. This is mainly due to the overlapping nature of the SS techniques. Hence, for the rest of the simulations, the maximum spreading factor of 16 is used, as it provides increased security compared to the other SF cases, while at the same time it does not increase spectrum usage in a proportional manner. Also, it is noted that FCAP requires less spectrum resources to accommodate the given set of demands compared to CCP when a SF of 8 or 16 is used, since it provides a more flexible code assignment solution.

In Fig. 8, the three different routing strategies for sorting all candidate paths for a given demand (as presented in Section IV.A) are evaluated using both policies. Also, the case without spreading is shown as a benchmark. From Fig. 8, it is evident that the maximum overlap (MO) strategy forces confidential demands to be allocated in the same links when possible. As a result, the number of spectrum resources required dramatically increases using either spectrum/code allocation policy. On the other hand, using the fairness distribution (FD) strategy, where confidential demands are evenly distributed within the network, the number of additional spectrum slots required is much less for establishing the connections while adding an extra layer of security (by distributing the confidential connections evenly across the network). Nevertheless, this strategy still needs more spectrum resources compared to the SE approach. Further, again it is noted that when FCAP is implemented, the number of frequency slots required is lower compared to CCP, using any of the three routing strategies, due to the flexibility the FCAP provides in terms of code assignment. It is also noted that the blocking probability is kept to zero for all these sets of simulations in order to present the exact number of slots required to allocate all demands in the network.

In Fig. 9, the blocking rate is now presented when both policies with different routing strategies are used. Also, the

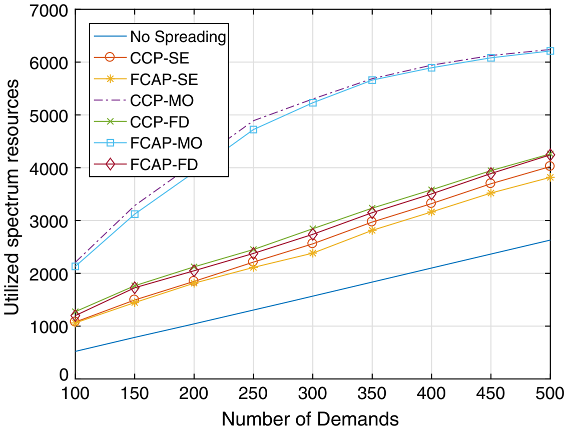

Fig. 8. Utilized spectrum for the three different routing strategies (MO, FD, and SE).

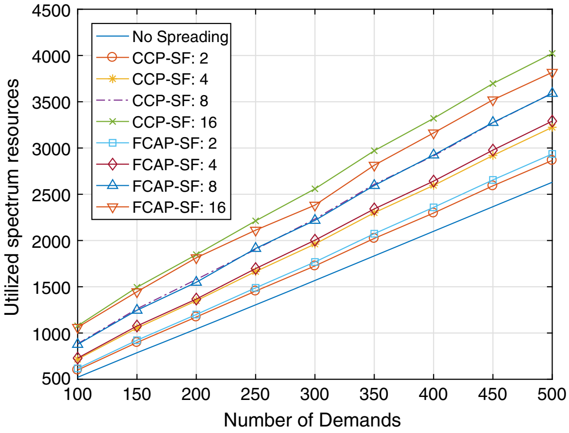

Fig. 7. Utilized spectrum resources for different SFs using the SE strategy for FCAP and CCP policies.

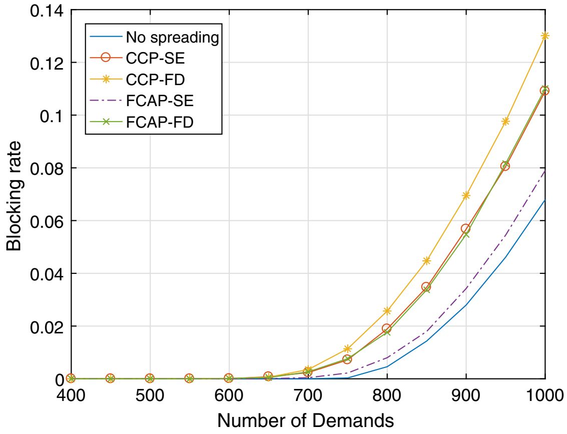

Fig. 9. Blocking rate using different policies and routing strategies.

case where all demands are not confidential (no spreading is applied) is shown as reference. As shown in the figure, the SE routing strategy offers better results compared to the FD routing strategy for both policies. Also, FCAP-FD provides similar results with CCP-SE in terms of blocking probability, whereas FCAP-SE provides the best results compared to CCP utilizing any routing strategy. This is due to the increased flexibility provided by FCAP, since the selected codes do not have to be the same for all selected frequency slots. As expected, the typical RSA approach (the case of no spreading) provides better results compared to any of the proposed polices and routing schemes. However, it should be noted that the blocking rate remains low even when spreading is used (for both FCAP and CCP), signifying that the extra layer of security provided with SS does not significantly affect the performance of the network in terms of blocking.

Apart from the blocking rate and the spectrum efficiency associated with each policy, the confidentiality that they provide must also be quantified. As discussed in Section V, each policy offers a different level of security, since the eavesdropper has to try a large number of code combinations in order to make sense of accessed confidential data. Further, as previously discussed, the number of frequency slots used by a confidential connection can play a significant role in the security level provided when FCAP is utilized. In Fig. 10, the average number of combinations per confidential demand required by the eavesdropper is presented when both policies with SE and FD routing strategies are used for all knowledge scenarios discussed in Section V. Further, since the number of combinations required by the eavesdropper to decode the signal is independent of the routing strategy used, for all simulations involving the CCP policy, only CCP-SE is considered for all knowledge scenarios investigated. As shown in the figure, the number of combinations that the eavesdropper has to try in order to decode the signal is static when CCP is used. On the other hand, a large increase in the number of combinations needed by the eavesdropper is observed when FCAP is utilized. It should be noted that the results for FCAP Case 1 are not shown, since the number of combinations required cannot be calculated by the PC used in our simulations. As shown, for FCAP, even in the case where the eavesdropper knows all the network parameters except for the exact codes used by the connection (Case 3), approximately 10^{44} different combinations are required (for a network load of 1000 demands) in order to check each combination of codes used.

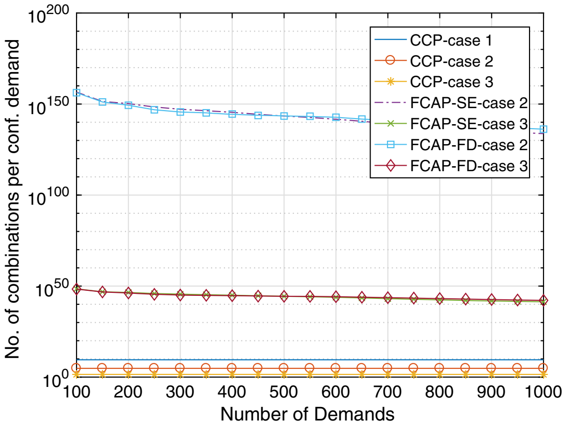

Fig. 10. Average number of combinations required for different policies, knowledge scenarios (Cases 1–3), and routing strategies.

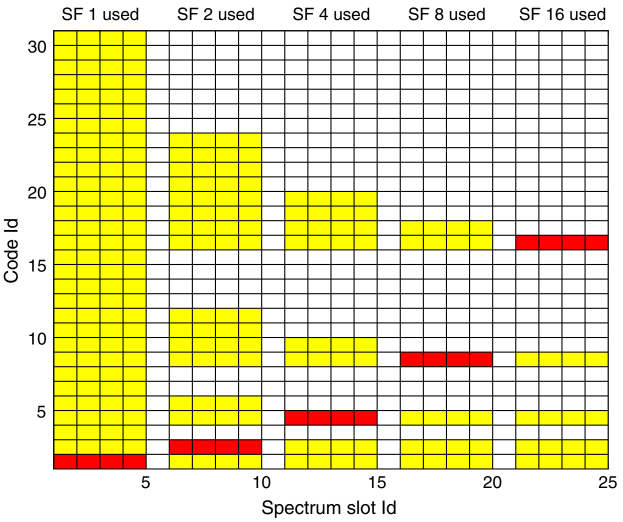

Fig. 11. Graphical representation of frequency slots versus code id used.

To visualize the state of the optical fiber and the results provided by both proposed policies, each link is graphically represented as a 2D matrix of cells as shown in Fig. 11 (the x axis denotes the slot id of the optical fiber, and the y axis denotes the code id). Red-colored cells signify that the given code is used by a demand in that frequency slot. Yellow-colored ones signify that the given code cannot be used to satisfy further connections, since it will not be orthogonal to the pre-established ones in that frequency slot. Further, white-colored cells signify that the given code can be used in this frequency slot for future connections.

To present the difference in the state of the bandwidth utilization in the optical fiber when different policies are in use, the allocation of the same connection is presented in Fig. 12. The frequency slots and the code that is used in each one are colored in red, while other codes used by established demands are colored in blue. As shown in the figure, when the CCP approach is implemented, the demand is assigned utilizing the same code in all selected frequency slots. On the other hand, by using FCAP, a different code can be used in each frequency slot in order to establish the connection. It is important to note that frequency slots preceding or following the selected ones may use the same code, which makes it difficult for the adversary to properly lock on the desired ones. Further, other currently used (blue) or non-orthogonal (yellow) codes in the same frequencies will result in possible outcomes for decoding the signal, and so the eavesdropper will have to make sense of a very large number of combinations of signals.

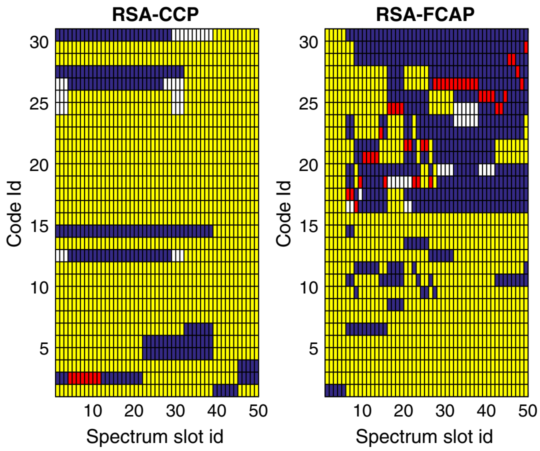

Fig. 12. Graphical spectrum/code allocation of the same connection using CCP and FCAP policy.

Finally, the CCP and FCAP policies are compared in terms of their running times. The results of both policies for the SE and FD routing strategies are presented in Fig. 13, taking into account the routing and spectrum/code allocation processes. To present the difference in the running times of both policies, all algorithmic functions are included in the running times apart from the k-shortest path calculation, since this calculation is a process that is performed offline for both algorithms in a pre-processing phase. As shown in the figure, the CCP approach offers the best results in terms of the computational time needed compared to FCAP for the allocation of a given demand. Nevertheless, as presented in the figure, the additional running time needed by FCAP to allocate connections does not increase proportionally to the additional security it provides. Also, for both policies, the computation time required using the SE routing approach is less than when the FD routing strategy is used. This is to be expected, since when using the SE routing strategy, the paths chosen are more efficient in terms of spectrum utilization (utilizing fewer hops and fewer overall frequency slots), meaning that fewer computations are required to establish the connections.

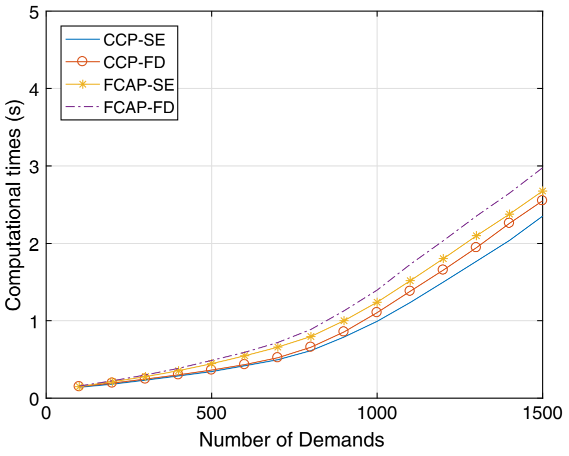

Fig. 13. Computational times using the two policies and different routing strategies.

VII. Conclusions

In this work, novel eavesdropping-aware routing heuristic algorithms and spectrum/code allocation policies are presented using the implementation of spread spectrum techniques in EONs that increase physical-layer security due to the codes used for each connection and the allowance of overlapping between connections. The proposed technique uses OVSF codes to maintain the flexibility of EONs, and the RSA problem is now modified as overlapping is partially allowed when orthogonal codes are in use.

Performance results indicate that the *free code assignment policy (FCAP)* provides increased network security, since the number of combinations required to decode the signal depends not only on network parameters but also on the number of frequency slots and codes used for that specific connection. Further, it is shown that utilizing any one of the two proposed spectrum/code allocation policies, the increase in spectrum usage is not proportional to the spreading factor, due to the overlapping between connections. In addition, the *fairness distribution (FD)* routing strategy is shown to add an extra layer of security, since in this approach the confidential connections are now distributed evenly across the network.

Thus, the FCAP spectrum/code assignment policy, in conjunction with the FD routing strategy, will substantially increase the level of network security against eavesdropping attacks, without at the same time significantly affecting key network performance parameters such as resource utilization, blocking rate, and the time complexity of the provisioning algorithms.

Ongoing work includes the combination of spread spectrum techniques with network coding approaches in order to further increase the security of confidential connections against eavesdropping attacks.

Acknowledgment

This work has been supported by the European Union's Horizon 2020 research and innovation program under grant agreement No. 739551(KIOS CoE) and by the Government of the Republic of Cyprus through the Directorate General for European Programmes, Coordination and Development.

References

[1] O. Gerstel, M. Jinno, A. Lord, and S. J. Ben Yoo, "Elastic optical networking: A new dawn for the optical layer?" *IEEE Commun. Mag.*, vol. 50, no. 2, pp. S12–S20, 2012.

[2] M. Jinno, H. Takara, B. Kozicki, Y. Tsukishima, Y. Sone, and S. Matsuoka, "Spectrum-efficient and scalable elastic optical path network: Architecture, benefits, and enabling technologies," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 66–73, 2009.

[3] K. Christodoulopoulos, I. Tomkos, and E. A. Varvarigos, "Elastic bandwidth allocation in flexible OFDM-based optical

networks," *J. Lightwave Technol.*, vol. 29, no. 9, pp. 1354–1366, 2011.

[4] K. Christodoulopoulos, I. Tomkos, and E. A. Varvarigos, "Routing and spectrum allocation in OFDM-based optical networks with elastic bandwidth allocation," in *IEEE GLOBECOM*, Miami, Florida, Dec. 2010.

[5] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucna, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 725–736, 2011.

[6] K. Guan, J. Cho, and P. J. Winzer, "Physical layer security in fiber-optic MIMO-SDM systems: An overview," *Opt. Commun.*, vol. 408, pp. 31–41, 2018.

[7] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, 2016.

[8] K. Manousakis and G. Ellinas, "Attack-aware planning of transparent optical networks," *Opt. Switching Netw.*, vol. 19, no. 2, pp. 97–109, 2016.

[9] K. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, and A. Takada, "Security in photonic networks: Threats and security enhancement," *J. Lightwave Technol.*, vol. 29, no. 21, pp. 3210–3222, 2011.

[10] M. Sasaki, M. Fujiwara, R.-B. Jin, M. Takeoka, T. S. Han, H. Endo, K.-I. Yoshino, T. Ochi, S. Asami, and A. Tajima, "Quantum photonic network: Concept, basic tools, and future issues," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, pp. 49–61, 2015.

[11] K. Fouli and M. Maier, "OCDMA and optical coding: Principles, applications, and challenges," *IEEE Commun. Mag.*, vol. 45, no. 8, pp. 27–34, 2007.

[12] X. Guo, Q. Wang, L. Zhou, L. Fang, X. Li, A. Wonfor, R. V. Penty, and I. H. White, "16-user OFDM-CDMA optical access network," in *Conf. on Lasers and Electro-Optics (CLEO)*, 2016.

[13] T. H. Shake, "Security performance of optical CDMA against eavesdropping," *J. Lightwave Technol.*, vol. 23, no. 2, pp. 655–670, 2005.

[14] G. Savva, K. Manousakis, and G. Ellinas, "Spread spectrum over OFDM for enhanced security in elastic optical networks," in *Proc. IEEE PSC*, Limassol, Cyprus, 2018.

[15] G. Savva, K. Manousakis, and G. Ellinas, "Eavesdropping-aware routing and spectrum allocation in EONs using spread spectrum techniques," in *IEEE GLOBECOM*, Abu Dhabi, UAE, Dec. 2018.

[16] W. Bei, H. Yang, A. Yu, H. Xiao, L. He, L. Feng, and J. Zhang, "Eavesdropping-aware routing and spectrum allocation based on multi-flow virtual concatenation for confidential information service in elastic optical networks," *Opt. Fiber Technol.*, vol. 40, pp. 18–27, 2018.

[17] S. K. Singh, W. Bziuk, and A. Jukan, "Balancing data security and blocking performance with spectrum randomization in optical networks," in *IEEE GLOBECOM*, Washington, DC, Dec. 2016.

[18] J. Ji, G. Zhang, W. Li, L. Sun, K. Wang, and M. Xu, "Performance analysis of physical-layer security in an OCDMA-based wiretap channel," *J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 813–818, 2017.

[19] A. Engelmann and A. Jukan, "Balancing the demands of reliability and security with linear network coding in optical networks," in *IEEE ICC*, Kuala Lumpur, Malaysia, 2016.

[20] F. Adachi, M. Sawahashi, and K. Okawa, "Tree-structured generation of orthogonal spreading codes with different lengths for forward link of DS-CDMA mobile radio," *Electron. Lett.*, vol. 33, no. 1, pp. 27–28, 1997.

[21] G. Savva, G. Ellinas, B. Shariati, and I. Tomkos, "Physical layer-aware routing, spectrum, and core allocation in spectrally-spatially flexible optical networks with multicore fibers," in *IEEE ICC*, Kansas City, Missouri, May 2018.

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. student 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 (CoE), University of Cyprus, Nicosia, Cyprus. 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 received a diploma, M.Sc., and Ph.D. degrees in computer engineering and informatics from the University of Patras, Patras, Greece, in 2004, 2007, and 2011, respectively. He is a research associate with the KIOS Center of Excellence (CoE), University of Cyprus, Nicosia, Cyprus. From 2014 to 2018 he was a Marie Curie Fellow, working on a four-year MC Career Integration Grant (CIG) in the area of optical network security. His research interests are in the area of optimization algorithms and security in optical networks.

Georgios Ellinas holds a B.Sc., M.Sc., M.Phil., and Ph.D. in electrical engineering from Columbia University. He is currently a professor and the Chair of the Department of Electrical and Computer Engineering at the University of Cyprus. Previously, he was an associate professor of electrical engineering at City College of New York. Before joining academia, he was a senior network architect at Tellium Inc. Dr. Ellinas also served as a visiting scientist/research scientist in Bellcore's Optical Networking Research Group. His research interests focus on optical networks, intelligent transportation systems, critical infrastructure systems, and IoT.