Eavesdropping-aware Routing and Spectrum Allocation in EONs using Spread Spectrum Techniques

Giannis Savva, Konstantinos Manousakis, and Georgios Ellinas
KIOS CoE and Department of Electrical and Computer Engineering
University of Cyprus, 1678 Nicosia, Cyprus
gsavva07@ucy.ac.cy

***Abstract*—In this work, eavesdropping-aware routing and spectrum allocation (RSA) 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 attain access to the signal and compromise a confidential connection, an eavesdropper will now have to lock on the correct frequency, determine the correct code and symbol sequence amongst co-propagated overlapped signals, and decode the signal. Different routing strategies and a novel spectrum allocation technique are proposed in an attempt to add an extra layer of security for confidential connections, while also considering spectrum utilization. Performance results demonstrate that while each confidential connection now requires more spectrum as a result of spreading in the bandwidth domain, the overall network spectrum usage is not increased proportionally to the spreading factor due to the utilization of spectrum overlapping techniques.**

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 flexible-grid optical networks or elastic optical networks (EONs), have been recently proposed by the research community to address this bandwidth crunch. EONs can now handle traffic demands by 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 6.25GHz compared to the 50GHz 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].

In EONs, to provision a connection, the routing and spectrum allocation (RSA) problem must be solved, that 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 frequency slots serving each demand must be contiguous [2].

Optical layer security (OLS) has received considerable attention by 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) [3]–[5]. In this work, we focus on confidentiality, where an adversary tries to access confidential data from an optical communication channel (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 adjacent spectrum by confidential signals [4], [6], and can potentially go undetected for a prolonged period of time.

A promising solution to increase confidentiality in optical communications is optical encoding [7]. In optical encoding, data are encoded using a unique key known to the source and destination nodes. Thus, even if an adversary obtains access to transmitted data, 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. 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 [7], [8].

This work focuses on security against attacks on confidentiality in EONs and proposes a novel eavesdropping-aware solution to the RSA problem for a planning scenario. This approach introduces SS techniques in EONs to increase security through optical encoding and signal overlapping. Utilizing these techniques, in order for the attacker to make sense out of the confidential information obtained through an eavesdropping attack, the correct code and correct symbol sequence amongst co-propagated overlapped signals must be determined, making it extremely difficult for the eavesdropper to compromise any confidential connections. A new constraint called *code availability* is now defined to implement the aforementioned techniques and is used as an additional constraint to the RSA problem. To the best of our knowledge, this is the first time that such an approach (spread spectrum with signal overlapping techniques) has been utilized for protection against eavesdropping attacks in EONs.

In the rest of the paper, state-of-the-art OLS techniques are discussed in Section II, followed by a brief discussion about the SS technique and orthogonal variable spreading factor codes in Section III. Then, the proposed eavesdropping-aware heuristic to solve the RSA problem is presented in Section IV, that is subsequently evaluated in Section V. Finally, Section VI 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 [9], authors propose an eavesdropping-aware RSA algorithm in which a demand uses two 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, 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 [10], the authors propose a reallocation technique to increase security in optical networks. In this 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 confidential data for a specific connection. For such technique to work, each time a reallocation takes place, the spectrum required for the reallocation must be available at that time, and therefore, connections must pre-allocate additional bandwidth to be used during the reallocation procedure. Thus, the complexity of the provisioning procedure increases.

III. Spread Spectrum and Signal Overlapping

In higher (electronic) layers, data is encrypted using encryption algorithms to ensure that if an eavesdropper gains access to the data, considerable time will be required before being able to decrypt the accessed data. Adding an extra layer of security in the optical (physical) domain will increase data confidentiality and make the data transmitted more secure. It is important to note though that any technique that is used for security purposes will require additional resources. As a result, the overall efficiency of the system in terms of actual data transmission will be reduced. To alleviate this problem, a spread spectrum with signal overlapping technique that combines resources used by different connections is utilized, in order to minimize the additional amount of bandwidth required while adding an extra layer of security in the optical domain.

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 [7]. The bandwidth spreading for each connection will depend 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) [3]). 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, Kasami codes). Each of these codesets has benefits and drawbacks regarding the size of the codeset and the relationship amongst 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 [11].

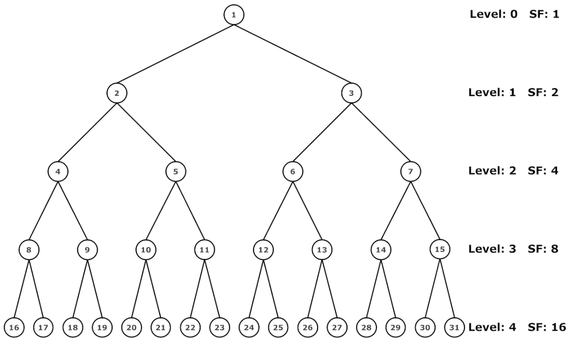

Fig. 1. Visualization of OVSF codes. Each level offers a different spreading factor [11].

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* [11]. Fig. 2 illustrates an example where 4 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 4 different signals.

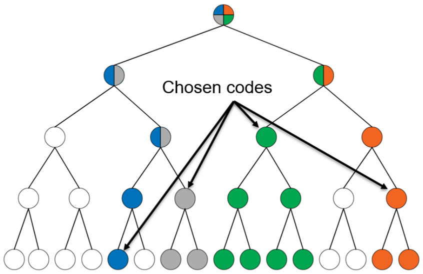

Fig. 2. Example of 4 signals using different codes within the same bandwidth.

In this example, all 4 signals use orthogonal codes and therefore they can share the same bandwidth without any interference. Signals 2 (gray) and 4 (orange) use a code with spreading factor 8, whereas signals 3 (green) and 1 (blue) use codes with spreading factors 4 and 16, respectively. 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. For instance, there are 2^{16} different combinations that could be used to establish a spreading factor of 16. Hence, all different combinations for all spreading factors are: $2^{16} + 2^8 + 2^4 + 2^2 + 2 + 1$. Even in the case that 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 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 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 having as an aim to find and allocate the best paths in terms of spectrum resources while also enabling overlapping between connections.

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, all demands are known a priori and each demand is described by a 4-tuple (*s,d,B,c*), denoting the source, destination, bit-rate, and confidentiality, respectively. Confidentiality in this case is defined as a binary variable which describes the demand as confidential (1) or not-confidential (0).

A. Routing

For the routing sub-problem, 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 which takes into account the ratio of these two parameters [12]. However, all aforementioned metrics aim to produce an RSA result that maximizes spectrum efficiency without considering protection of the data against eavesdropping attacks.

In this work, a new metric is introduced, namely the *confidential connections overlap (CCO)* metric, which counts the number of links in each path that carry confidential connections. Based on this new metric, two routing strategies are subsequently proposed. A third routing strategy is also utilized that aims at maximizing spectrum efficiency without considering the CCO metric.

- **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 based on the number of hops and the modulation format that can be used (hybrid method [12]).

Note that for non-confidential demands, the RSA algorithm uses the Spectrum Efficiency strategy so as to better utilize network resources. All aforementioned strategies have tradeoffs in terms of security and spectrum efficiency as amply demonstrated in Section V.

B. Spectrum Allocation

For the SA sub-problem, available spectrum resources must be allocated for a requested connection, while also satisfying slot *continuity* and *contiguity* constraints [2]. Due to the use of the SS technique, the *non-overlapping* slot constraint is now mitigated as overlapping is partially allowed for confidential connections where spreading is enabled. Thus, each slot can be allocated to a number of connections, as long as each connection 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 which keeps track of the codes used for that slot. Fig. 3 shows an example of spectrum slots and their modeled trees, including allocated and free spectrum slots.

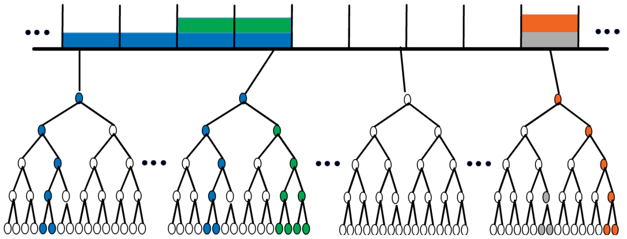

Fig. 3. Different spectrum slots and their modeled trees. Uncolored nodes represent codes that can be used for future connections.

In this work, the solution to the SA problem requires an additional step, that is, to find an available code which can be used in the selected spectrum slots for the requested connection. 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, that specifies that all slots allocated to 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, the assumption used is that a connection must allocate the same code among all spectrum slots in the chosen path. In general, however, a connection can choose different codes for each slot.

To satisfy the *code availability* constraint, each spectrum slot's tree has to be checked in order to find whether there exists an available code that can be used through all selected spectrum slots. The proposed procedure to do so is as follows:

- **Step** 1: For all spectrum slots in the path's links, each already utilized code in the tree takes the binary value 1 and each free code takes the value 0.
- **Step** 2: For all links in the path, each spectrum slot's tree is OR-ed with other slots' trees that have the same id on other links in the path. This procedure produces a *virtual link*, where each slot has a tree that characterizes all slots with the same id in the selected path.
- **Step** 3: Starting from the first slot in the virtual link, while there exists an available code in the spectrum slot's tree, it is OR-ed with the next frequency slot's tree. This procedure is repeated until the resulting tree does not have an available code or the number of slots OR-ed reaches the maximum required spectrum (spectrum slots when spreading is not applied * max spreading factor).
- **Step** 4: If the number of available spectrum slots found are enough to establish the connection (spectrum slots when spreading is not applied * spreading factor of chosen code), then the connection is established. Else, Step 3 is repeated, starting from the spectrum slot which follows the slot that was first checked in Step 3.

The following example illustrates the proposed SA procedure for a given connection.

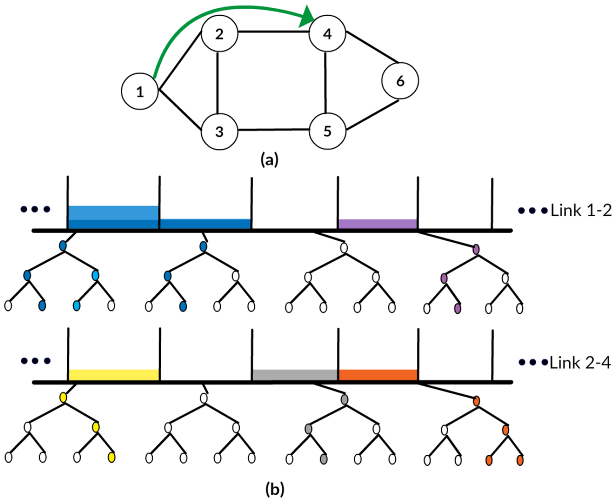

Fig. 4. (a) A 6−node network. (b) Five spectrum slots in links $1-2$ and $2-4$. Each color represents already established connections.

In Fig. 4(a), a network consisting of 6 nodes is presented. Suppose that a connection is requested from node 1 to node 4. Also, for simplicity, assume that the connection requests 1 spectrum slot (when spreading is not applied) 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: $(1-2, 2-4)$. In Fig. 4(b), all links in the path are represented and each slot's tree is shown. As discussed above, each slot with the same id is OR-ed with trees from other spectrum slots at each link to form a virtual link that represents the chosen path.

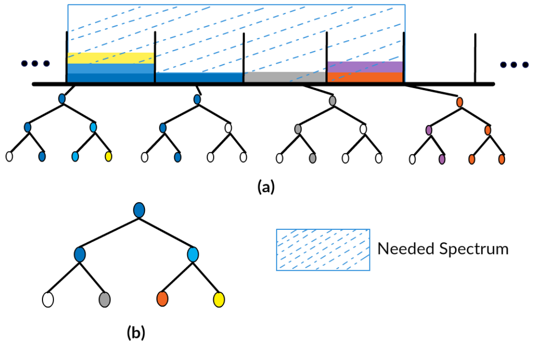

Fig. 5. (a) The virtual link created after links $1-2$ and $2-4$ are OR-ed. (b) The resulting tree when 4 slots in the virtual link are OR-ed.

In Fig. 5(a), the virtual link that describes the chosen path is presented. Following the procedure previously described in Step 3, the maximum number of spectrum slots required is 4. The resulting (virtual) tree, shown in Fig. 5(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 case, the leftmost code at the lowest level can be used and the connection will be allocated 4 spectrum slots in each link. It is noted that, following this procedure, the resulting solution satisfies the slot *continuity*, *contiguity*, and *code availability* constraints.

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 becomes more difficult to solve, since the number of spectrum slots required changes based on the available codes that can be used.

Clearly, higher levels of spreading offer advantages in terms of network security, since larger codes are used to modulate each signal. Hence, more signals can overlap in the bandwidth domain, which increases the difficulty in making sense of accessed confidential information. Thus, the proposed algorithm aims at maximizing the spreading factor of each confidential connection when spectrum slots are available to satisfy a given demand. This is achieved by searching through the trees starting from the lower levels and moving up to the root. Hence, codes with higher spreading factor are chosen for each demand when multiple codes are available.

V. 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 12.5GHz which results in a total of 320 spectrum slots for each link in the network. Further, the NSF network with 14 nodes and 50 undirected links is used for all experiments. In all cases, demands are randomly generated using a uniform distribution for all source-destination pairs, where each demand size varies from 10 to 100Gbps. Each presented result is the average of 5 experiments performed with different generated sets of demands.

First, the results of different maximum spreading factors used for the RSA algorithm utilizing the Spectrum Efficiency strategy are presented. To evaluate each spreading factor, the number of spectrum slots utilized in each case is illustrated. In this scenario, all demands are confidential, in order to examine the maximum number of additional resources required for the case where all demands experience spectrum spread. As shown in Fig. 6, with a maximum spreading factor of 2, 4, 8 and 16, the additional spectrum resources needed are $11,03\%$, $24,61\%$, $42,48\%$ and 67.40%, respectively, compared to the case where spreading is not applied. It is important to note that while each secure connection requests more spectrum as a result of spreading in the bandwidth domain, the overall network spectrum usage does not increase proportionally to the spreading factor 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 rest of the cases examined, while at the same time it does not increase spectrum usage proportionally to its spreading factor.

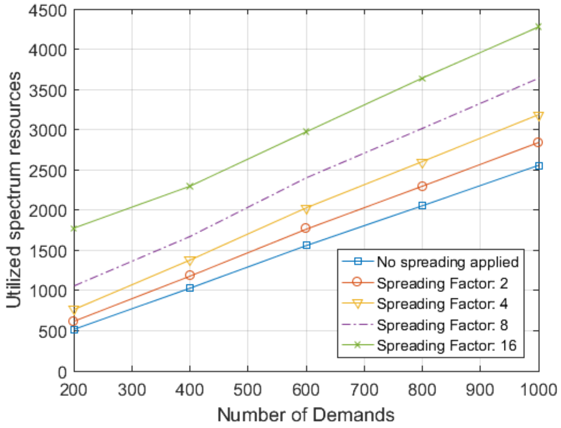

Fig. 6. Utilized spectrum resources for different spreading factors using the Spectrum Efficiency strategy.

In Fig. 7, the three different routing strategies (as presented in Section IV-A) are evaluated. Also, the case without spreading is shown as a benchmark. From Fig. 7, it is evident that the Maximum Overlap strategy forces confidential connections to be allocated to the same links when possible (increasing overlapping amongst confidential connections). However, this results in a dramatic increase in the number of spectrum resources utilized. Using the Fairness Distribution strategy, where confidential connections are evenly distributed within the network, the number of additional spectrum slots required is now much less. Nevertheless, this strategy still needs more spectrum resources compared to the Spectrum Efficiency approach.

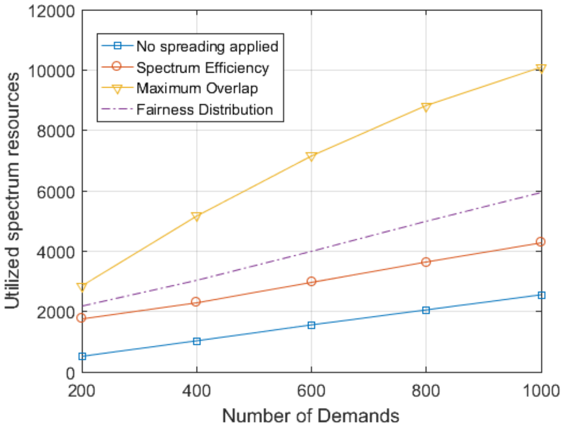

Fig. 7. Utilized spectrum for different routing strategies.

A more realistic scenario is also considered in which the number of confidential connections is only a fraction of the overall number of connections. In this case, the Spectrum Efficiency strategy, which provides the best results in terms of resource usage, and the Fairness Distribution strategy, which adds an extra layer of security without increasing resource usage considerably, are evaluated. In Fig. 8, the overall spectrum used when different percentages of connections are confidential is presented for the case where the Spectrum Efficiency strategy is utilized. As can be seen, there is a large increase in the spectrum utilized when the number of confidential connections increases from 0% to 20% of the total number of connections, due to the spreading that is implemented for the confidential connections. However, from that point on there is only a slight increase in the spectrum usage for higher percentages of confidential connections, due to the increased overlapping between different confidential connections.

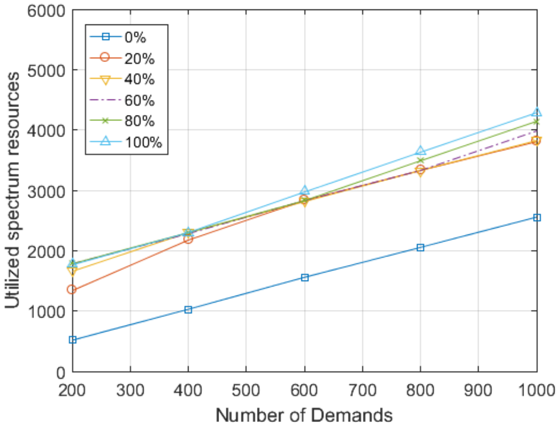

Fig. 8. Spectrum utilization for the Spectrum Efficiency strategy when the percentage of confidential connections changes.

Similarly, in Fig. 9, the overall number of spectrum resources used is presented when the Fairness Distribution strategy is considered. In this case, there is a similar increase in the spectrum resources utilized when the percentage of confidential connections changes from 0% to 20%. However, as shown in the figure, the number of resources required increases by an additional $39,11\%$ (when all connections are designated confidential) compared to the Spectrum Efficiency strategy. This is to be expected and can be seen as the *penalty* paid for providing more secure connections within the network. Nevertheless, the additional resources required are still significantly less than those required by the Maximum Overlap strategy.

VI. Conclusions

In this work, a novel eavesdropping-aware RSA approach is presented using the implementation of spread spectrum techniques in EONs to increase physical layer security. 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. The performance results obtained demonstrate the feasibility of such a technique that utilizes spectrum spreading and overlapping for increased network security.

Several routing strategies were also proposed and evaluated in terms of spectrum efficiency. From the performance results, it is clear that the Spectrum Efficiency strategy results in the lowest number of utilized resources, while the Fairness Distribution strategy provides an extra layer of security at the expense of additional resources. Future work includes different spectrum allocation policies to further increase the security of the confidential connections.

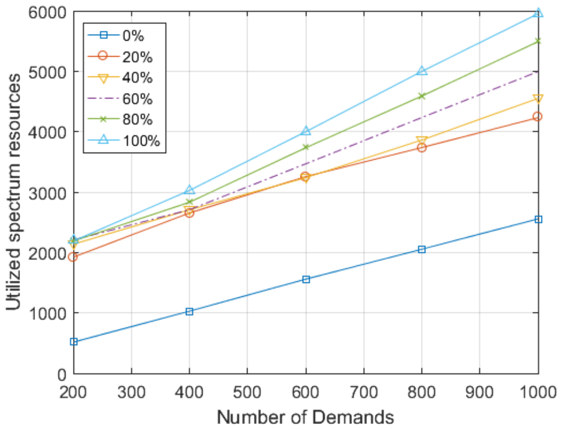

Fig. 9. Spectrum utilization for the Fairness Distribution strategy when the percentage of confidential connections changes.

Acknowledgment

This work has been supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 739551(KIOS CoE) and from the Government of the Republic of Cyprus through the Directorate General for European Programmes, Coordination and Development. This work has also received funding from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme (FP7/2007-2013) under REA Grant Agreement no 630853.

References

[1] O. Gerstel, et al., "Elastic Optical Networking: A New Dawn for the Optical Layer?", *IEEE Comm. Magazine*, 50(2):S12-S20, 2012.

[2] K. Christodoulopoulos, et al., "Routing and Spectrum Allocation in OFDM-based Optical Networks with Elastic Bandwidth Allocation", *Proc. GLOBECOM*, Miami, FL, Dec. 2010.

[3] M.P. Fok, et al., "Optical Layer Security in Fiber-Optic Networks", *IEEE Trans. Inf. Forensics Security*, 6(3):725-736, 2011.

[4] N. Skorin-Kapov, et al., "Physical-Layer Security in Evolving Optical Networks", *IEEE Comm. Magazine*, 54(8):110-117, 2016.

[5] K. Manousakis, et al., "Attack-aware Planning of Transparent Optical Networks", *Optical Switching and Networking*, 19(2):97-109, 2016.

[6] K. Kitayama, et al., "Security in Photonic Networks: Threats and Security Enhancement", IEEE/OSA J. of Lightw. Techn., 29(21):3210-3222, 2011.

[7] K. Fouli, et al., "OCDMA and Optical Coding: Principles, Applications, and Challenges", *IEEE Comm. Magazine*, 45(8):27-34, 2007.

[8] X. Guo, et al., "16-User OFDM-CDMA Optical Access Network", *Lasers and Electro-Optics*, OSA Technical Digest, paper JTh2A.132, 2016.

[9] W. Bei, et al., "Eavesdropping-aware Routing and Spectrum Allocation based on Multi-flow Virtual Concatenation for Confidential Information Service in Elastic Optical Networks", *Opt. Fiber Techn.*, 40:18-27, 2018.

[10] S. K. Singh, et al., "Balancing Data Security and Blocking Performance with Spectrum Randomization in Optical Networks", *Proc. GLOBECOM*, Washington DC, Dec. 2016.

[11] F. Adachi, et al., "Tree-structured Generation of Orthogonal Spreading Codes with Different Lengths for Forward Link of DS-CDMA Mobile Radio", *Electron. Lett.*, 33(1):27-28, 1997.

[12] G. Savva, et al., "Physical Layer-Aware Routing, Spectrum, and Core Allocation in Spectrally-Spatially Flexible Optical Networks with Multi-core Fibers", *Proc. ICC*, Kansas City, MO, May 2018.