Spread Spectrum over OFDM for Enhanced Security in Elastic Optical Networks

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

***Abstract*—In this work, spread spectrum with signal overlapping techniques are used to secure confidential connections against eavesdropping. Routing and spectrum allocation algorithms are proposed in order to establish a set of confidential and non-confidential connections in elastic optical networks, while considering spectrum utilization and enhanced security.**

***Index Terms*—routing and spectrum allocation, eavesdropping, spread spectrum**

I. Introduction

Elastic optical networks (EONs) using orthogonal frequency division multiplexing (OFDM) have recently been proposed to address the ever-increasing growth of traffic in backbone networks. Flexible-grid networks provided by EONs can more efficiently handle traffic demands by the elastic allocation of spectrum as opposed to the fixed grid utilized in WDM networks [1]. To provision a connection in EONs, the routing and spectrum allocation (RSA) problem must be solved. Any feasible RSA solution must satisfy three constraints: (i) the *spectrum continuity constraint* - each demand must be allocated to the same frequency slots on each link of the selected path, (ii) the *non-overlapping constraint* - a frequency slot on each link 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].

Security in optical networks has also gained much attention recently. A promising solution to increase security and especially confidentiality in optical communications is optical encoding [3]. 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 since it uses unique keys to modulate signals [3]. SS techniques such as optical code division multiple access (OCDMA) have been proposed and demonstrated by several works to implement optical encoding [3], [4].

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.

Other techniques, such as the one presented in [5], propose eavesdropping-aware RSA algorithms in which a demand uses more than one 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. Further, in [6], the authors propose a spectrum reallocation technique at random times to increase security in EONs. This approach makes it 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. However, 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, demands must pre-allocate additional bandwidth to be used during the reallocation procedure.

This work focuses on security against confidential attacks in EONs and proposes a novel eavesdropping-aware spread spectrum solution to the RSA problem (SS-RSA). A SS 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 security level at the optical layer. To the best of our knowledge, this is the first time that such an approach has been utilized for protection against eavesdropping attacks in EONs.

The rest of the paper is organized as follows. The SS technique in combination with RSA is discussed in Section II, followed by the proposed eavesdropping-aware RSA heuristic in Section III. This technique is evaluated in Section IV, while Section V offers some concluding remarks.

II. Spread Spectrum and RSA

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 [3]. The bandwidth spreading (spreading factor (SF) - defined as the size of the code) for each connection depends on the used code. At the receiver, the signal is demodulated to its original bandwidth with the use of the same code. Therefore, to establish a connection, both the transmitter and receiver must have knowledge of the code used. 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) [7]). To minimize MAI and its effect on the probability of error for overlapping signals, a codeset of orthogonal codes can be used. In this work, Walsh-Hadamard codes are used for the implementation of the SS techniques. However, other approaches for the creation of orthogonal codesets can also be found in the literature (e.g., Gold, Kasami codes).

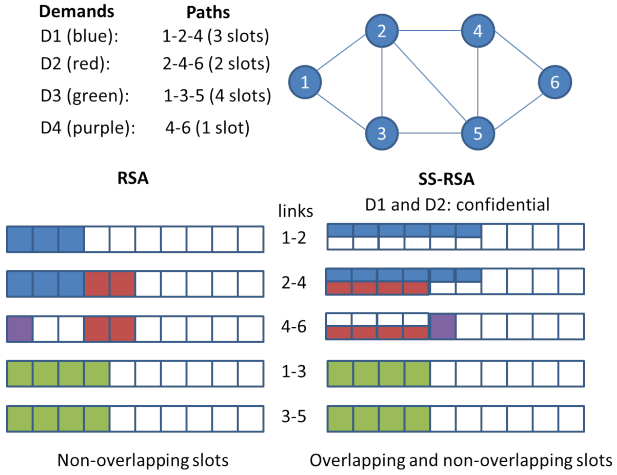

Fig. 1. Comparison of RSA and SS-RSA.

Fig. 1 shows an example of spectrum allocation for the case of the RSA problem when all the demands are non-confidential and the SS-RSA problem when demands $D1$ and $D2$ are confidential and use SS with SF equal to 2. In the latter case, demand $D1$ requires 6 slots and $D2$ 4 slots, whereas the original request of $D1$ and $D2$ is 3 and 2 slots, respectively. However, these two requests can overlap in spectrum as seen above in the figure in links $2-4$ and $4-6$ when utilizing the SS-RSA technique.

In order for the eavesdropper 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 connection. A new constraint, called *code availability*, is defined to implement the aforementioned technique and is used as an additional constraint to the RSA problem.

III. Eavesdropping-Aware RSA Heuristic

The proposed eavesdropping-aware RSA algorithm is divided into two sub-problems, namely the routing (R) sub-problem, where a path is found for a requested connection and the spectrum allocation (SA) sub-problem, where spectrum resources are allocated for each requested connection. Note that in this work, a network planning scenario is assumed, where all demands are known a priori.

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 which takes into account the ratio of these two parameters [8].

The following routing strategies are proposed:

- **Spectrum Efficiency (SE)**: Candidate paths are sorted based on the number of hops and the modulation format that can be used (hybrid method [8]). This strategy aims at maximizing spectrum efficiency, while also providing additional security against eavesdropping.
- **Maximum Overlap (MO)**: Candidate paths are sorted in descending order based on the number of links in each path that carry confidential connections. Hence, demands are forced to use paths with links that are utilized by other confidential connections. This strategy aims at maximizing security against eavesdropping.

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.

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 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.

The solution to the SA problem now also requires to find an available code which can be used in the selected spectrum slots for the requested connection. Thus, the *code availability* constraint is also introduced, which specifies that all slots allocated for a demand must use a code that maintains orthogonality between codes that are allocated by pre-established demands in the same set of slots. Therefore, each frequency slot is now represented by an array of size n, where n is the number of available codes and is based on the used SF. Also, each connection must allocate the same code among all spectrum slots in the chosen path. In this work, a first-fit approach is used for the SA heuristic that finds a slot allocation that not only satisfies the slot *continuity* and *contiguity* constraints but also the *code availability* constraint, by checking each spectrum slot in order to find whether there exists an available code that can be used through all selected spectrum slots.

IV. Performance Evaluation

The following simulation setup is used to evaluate the proposed algorithms. Bandwidth variable transponders are assumed to operate at multiple modulation formats: BPSK, QPSK, 8-QAM, and 16-QAM with transmission reach at 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. Demands are randomly generated using a uniform distribution for all source-destination pairs where each demand size varies from 20 to 100Gbps. Each presented result is the average of 5 experiments performed with different generated sets of demands.

First, the results of different SFs used for the RSA algorithm (with the Spectrum Efficiency routing strategy) are presented. To evaluate each SF, 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 in the case that all demands experience spectrum spread. As shown in Fig. 2, while the case with a SF of 16 requires additional spectrum resources as a result of spreading in the bandwidth domain, the overall network spectrum usage is not increased proportionally to the SF due to the overlapping nature of the SS techniques. Hence, for the rest of the simulations, SF of 16 is used.

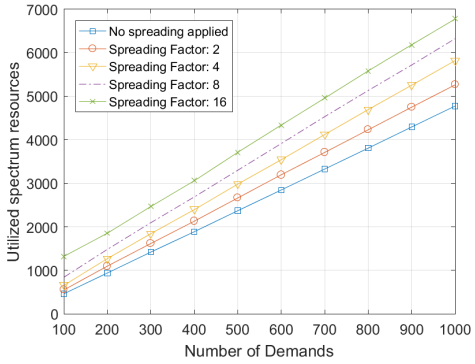

Fig. 2. Utilized spectrum resources for different spreading factors (SFs).

Next, the SE and MO routing strategies are evaluated using a SF of 16 (again, in this scenario, all demands are considered as confidential). As expected (Fig. 3), the SE approach outperforms the MO approach in terms of spectrum resources required, since the SE routing technique is designed to maximize resource efficiency. Note that the case without spreading is also presented as a reference, demonstrating that we can increase security against eavesdropping (utilizing spreading) and still keep the resource utilization low.

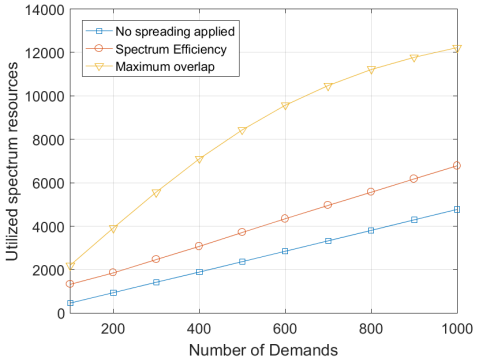

Fig. 3. Spectrum Efficiency versus Maximum Overlap approaches.

Finally, a scenario where only a portion (in this case 60%) of the overall demands are confidential is considered. As shown in Fig.4, the SE approach again provides better results than the MO strategy in terms of blocking probability, since it manages resources more efficiently, thus allowing more connections to be established in the network. The case without spreading (0% confidential demands) is again presented as a reference, demonstrating that the Spectrum Efficiency approach provides an additional level of security in the physical layers at the expense of only slightly higher blocking probability, compared to the case of no spreading.

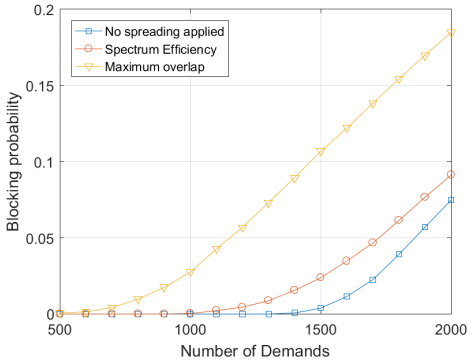

Fig. 4. Blocking probability for different routing approaches.

V. Conclusions

In this work, a novel eavesdropping-aware RSA heuristic is 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. It is shown that the proposed SE routing technique outperforms the MO routing approach in terms of both spectrum efficiency and blocking probability, as the SE strategy aims at maximizing spectrum efficiency, while also providing additional security against eavesdropping at the physical layer, compared to the MO approach that maximizes security against eavesdropping but does so irrespective of the network resources required.

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*, 2010.

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

[4] X. Guo, et al., "16-User OFDM-CDMA Optical Access Network", *Proc. CLEO*, 2016.

[5] 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.

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

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

[8] G. Savva, et al., "Physical Layer-Aware Routing, Spectrum, and Core Allocation in Spectrally-Spatially Flexible Optical Networks with Multicore Fibers", *Proc. ICC*, 2018.