

Eavesdropping Aware Routing and Spectrum/Code Allocation in CDMA based EONs using DaaS

Professor M. Padmaa

Department of ECE,
Saranathan college of Engineering,
Trichy, Tamilnadu, India.
Padmaa-ece@saranathan.ac.in

PG Student J. Vinitha

Department of ECE,
Saranathan college of Engineering,
Trichy, Tamilnadu, India.
j.vinithatkj@gmail.com

Abstract – In this paper, CDMA technique is proposed for providing physical layer security against eavesdropping in the elastic optical networks (EONs). CDMA technique is used to encode confidential information. Therefore in order to decode the original information, an eavesdropper will now have to lock on the correct frequency, determining the correct code and symbol sequence among the co-propagated overlapped signals. When the spectrum slots are randomly allocated, the gaps between the spectrum slots are created. The compact spectrum is converted into small fragments. Thus fragmentation aware routing and spectrum allocation (FA-RSA) is proposed to find the path having the contiguous spectrum. In this work, defragmentation techniques is used and also called as Defragmentation as a Service (DaaS). Defragmentation is used to satisfy spectrum contiguous constraint by aggregating the spectrum fragments and also reduces blocking probability.

Keywords– Code division multiple access(CDMA); 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 is expected to exceed the available capacity provided by the fixed grid wavelength division multiplexing(WDM) technology. Elastic optical networks(EONs) and Orthogonal frequency division multiplexing have recently been proposed by the research community to address spectrum crisis problem. For fixed-grid wavelength, the channel spacing is 50GHZ. But in this work, it is sufficient to have channel spacing as 25GHZ, 12GHZ or 6.25GHZ due to orthogonality.

The whole spectrum is divided into number of spectrum slices also called as spectrum slots or frequency slots. Each slot consists of its modulated code tree also called as orthogonal variable spreading factor codes(OVSF) tree. In OVSF, orthogonal codes are stored in tree data structure. Since each slot consists of number of orthogonal codes, many demands are allowed to share the same slot with unique code. The original information is modulated with respect to set of orthogonal codes selected in the chosen path.

Since the path is chosen in a random manner, an eavesdropper should have the knowledge of instantaneous path chosen and also set of orthogonal codes in order to decode the original information. Dijkstra's algorithm is used to find the shortest path for a given source to destination request. The codes are allocated in a random

manner. For feasible routing and spectrum allocation, three constraints must be satisfied. They are

1. Spectrum contiguity constraint
2. Spectrum continuity constraint
3. Non-overlapping constraint

In spectrum continuity constraint, the set of codes are predefined and reserved for a certain connection request. In spectrum contiguity constraint, the spectrum slots assigned for a particular request must be adjacent to each other.

Security threats such that observation of the existence of communication (privacy), unauthorized use of spectrum(authentication), manipulation or destruction of data(data integrity), denial of service(availability) and unauthorized access to information(confidentiality) are possible in optical communication networks. In this work, we focus on confidentiality and service availability to improve security and also to reduce blocking rate.

II. LITERATURE REVIEW

In [17], the authors proposed a reallocation technique to increase security in optical networks. The spectrum slots are reallocated after random time. As a result, the eavesdropper can obtain all the confidential data for a particular connection. To perform reallocation operation, the spectrum required for the reallocation process must be available at that time. Hence demands must pre-allocate additional bandwidth to be used during the reallocation

procedure. Complexity of the provisioning procedure increased considerably.

In [18], the authors proposed OCDMA (optical code division multiplexing) technique to provide physical layer security. In order to improve the security, the code length need to be increased.

In [20], the authors used orthogonal variable spreading factor(OVSF) code tree for performing encoding. In CDMA technique, multiple unique codes are used to encode the connection. All the used share the same bandwidth simultaneously but with different codes.

In [19], the authors proposed three constraints to be satisfied for feasible routing and spectrum allocation. The three constraints are spectrum continuity constraint, spectrum contiguity constraint and non overlapping constraint. These constraints are discussed in detail in this work.

III. PROPOSED SYSTEM

1. Code Division Multiple Access (cdma)

In this paper, Code division multiple access(CDMA) is used to give a access to users. CDMA is one of the spread spectrum techniques. Only when unique code is available for a particular connection, the connection could be established. Each link is divided into different slots. The slot consists of orthogonal variable spreading factor code (OVSF) tree. The codes are arranged in the tree data structure. In OVSF tree, the length of the code is $(2)^i$ at the i th level. In this technique, multiple users share the same spectrum with different codes.

$$\text{Blocking rate} = \dots (1)$$

$$\text{Spectrum efficiency} = \dots (2)$$

2. Random fit(rf) Algorithm for Routing and Spectrum Allocation(rsa)

In case of random fit algorithm, it searches for availability of free spectrum or code. Only when the orthogonal code is available, the connection request is established for the requested source and destination. If the code is unavailable, the connection request is rejected. Thus the blocking rate also gets increased. Blocking rate is defined as the ratio of number of connections blocked to the total number of connections requested. It is a undesirable parameter. The main cause for increase in blocking rate is fragmentation. Hence fragmentation aware routing and spectrum allocation (FA-RSA) algorithm is used in addition to the RF algorithm. The psedocode for RF algorithm is given below.

- Step 1 : Connection request for a source - destination pair
- Step 2 : Calculate shortest path for the given source – destination pair

Step 3 : Check code availability from the slots for the required link in the path

Step 4 : Select one code in each link for the given path

Step 5 : perform encryption between set of codes for the selected path and the original Information

Step 6 : Perform decryption at the destination to recover the original information.

3. Fragmentation Aware Routing and Spectrum Allocation Algorithm (fa-rsa)

Depending on the level of fragmentation, the path is chosen. The level of fragmentation is determined by calculating the external parameter. The path should have higher external parameter value. Such path only is said to have better contiguous spectrum.

Step 1 : first and second shortest path are found out for a given source and destination path.

Step 2: external parameter Fex1 and Fex2 are determined for first and second path respectively

Step 3 : the path having higher external parameter is said to have better spectrum contiguity property and selected for connection establishment

Step 4 : only if the code is available for the selected path, the connection is established.

$$\text{External fragmentation} () = 1 - \dots (3)$$

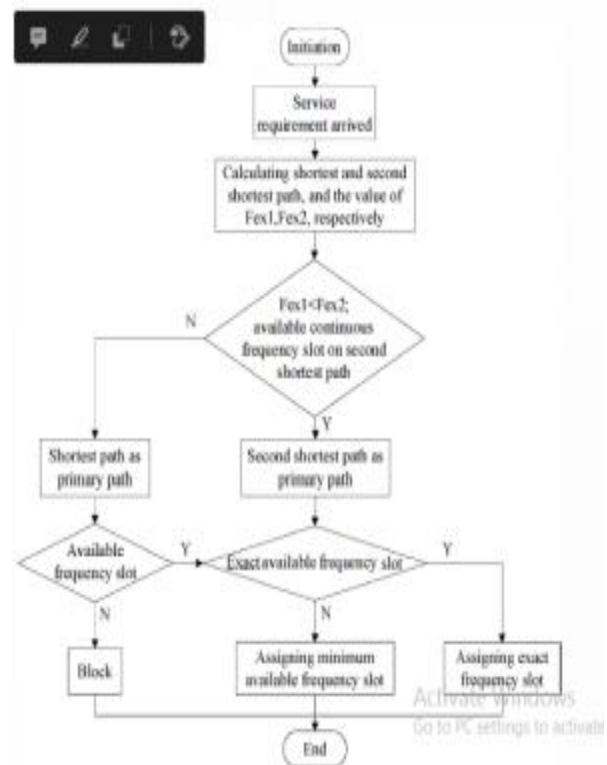


Fig.1.Flowchart for FA-RSA

4. Defragmentation As A Service (Daas)

When we use random fit (RF) algorithm for routing and spectrum allocation, two constraints such as spectrum contiguity constraint and spectrum continuity constraint are not satisfied. These two constraints play vital role for feasible RSA. To satisfy spectrum contiguous constraint, defragmentation technique is used. In case of defragmentation, all the fragments of the spectrum are aggregated. In order to reduce the blocking rate, some additional spectrum slots are reserved for the connection requests arriving during the process of defragmentation.

When the frequency slots are randomly allocated, the largest block of the spectrum is converted into small fragments also called as frequency slots. The gaps are created between frequency slots. In the case of defragmentation, the empty lowest frequency slots are occupied by the highest frequency slots. In such a way, the spectrum slots are aggregated to satisfy the spectrum contiguous constraint. There are two types of defragmentation namely defragmentation major and defragmentation minor. The process of filling smallest gaps is called as defragmentation minor. The defragmentation major is the process of filling largest gaps.

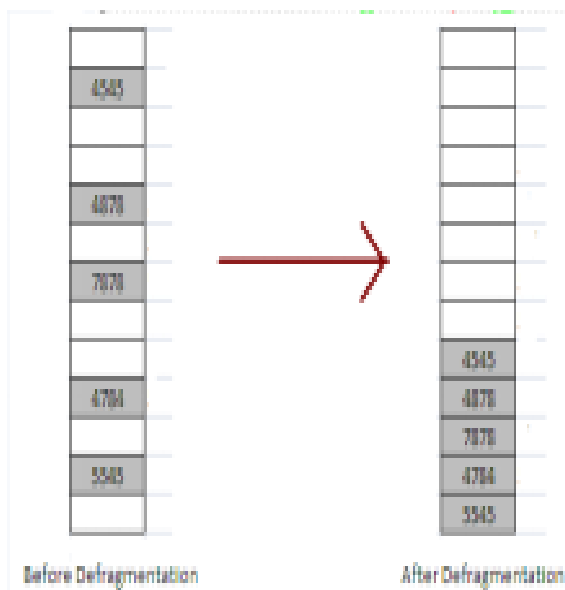


Fig.2.Defragmentation procedure.

IV. SIMULATION AND RESULTS

Blocking rate of FA-RSA is higher than FA-RSA+DF and lower than RF method. In a simple RF algorithm, since the slots are randomly assigned, the gaps are formed between the slots. As a result, spectrum contiguity constraint could not be satisfied. Thus more connections are blocked increasing blocking rate due to the lack of compact set of slots. Thus blocking rate is very high in

case of RF algorithm. FA-RSA is used for better blocking rate performance. In addition, defragmentation process is performed to reduce the blocking rate.

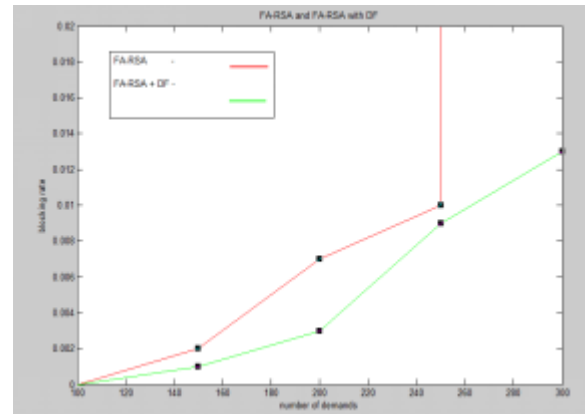


Fig .3. comparison between FA-RSA and FA-RSA+DF

V.CONCLUSION

To satisfy the spectrum contiguous constraint, defragmentation process is performed. In case of defragmentation, all the available spectrum slots are rearranged and only available spectrum slots are aggregated together for feasible routing and spectrum allocation. Defragmentation process is performed after every connection establishment. Since defragmentation process is time consuming, before performing defragmentation, fragmentation aware routing and spectrum allocation(FA-RSA) algorithm is used to select the path having better contiguous spectrum.

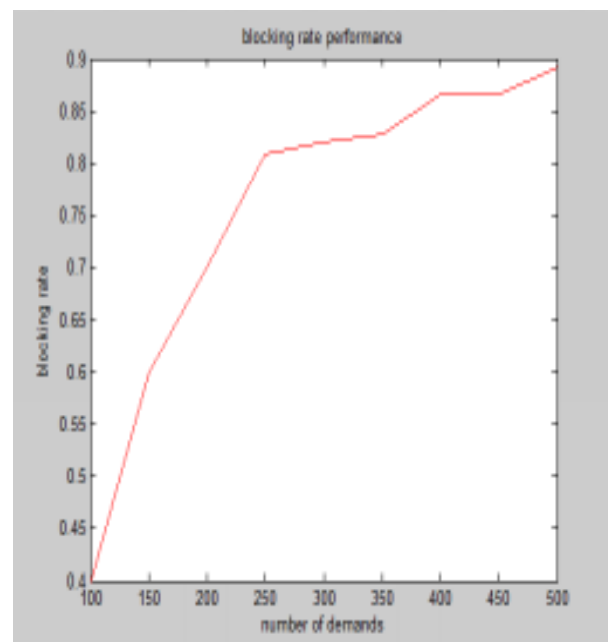


Fig..4 output for RF algorithm

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 photon 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]. Andre V.S. Xavier, Raul C. Almeida S., Joaquim F. Martins-Filho, "spectrum continuity and contiguity based dedicated protection for flexible optical networks, Federal university of pernambuco, Journal of microwaves, optoelectronics and Electromagnetic Applications, vol. 16, No. 2, June 2017.
- [20]. F. Adachi, M. Sawahashi, and K. Okawa, "Tree-structured generation of Orthogonal spreading codes with different lengths for forward link of DS-SS-CDMA mobile radio," *Electron. Lett.*, vol. 33, no. 1, pp. 27–28, 1997.