Optical Fiber Technology 40 (2018) 18–27

Contents lists available at ScienceDirect

Optical Fiber Technology

journal homepage: www.elsevier.com/locate/yofte

Regular Articles

# Eavesdropping-aware routing and spectrum allocation based on multi-flow virtual concatenation for confidential information service in elastic optical networks

Wei Bai[a], Hui Yang[a,*], Ao Yu[a], Hongyun Xiao[b], Linkuan He[a], Lei Feng[c], Jie Zhang[a]

[a] State Key Laboratory of Information Photonics and Optical Communication, Beijing University of Posts and Telecommunications, Beijing 100876, PR China
[b] ZTE Corporation, Shenzhen 518057, China
[c] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, PR China

ARTICLE INFO

*Keywords:*
Network security
Elastic optical networks
Eavesdropping attack
RSA
MFVC

ABSTRACT

The leakage of confidential information is one of important issues in the network security area. Elastic Optical Networks (EON) as a promising technology in the optical transport network is under threat from eavesdropping attacks. It is a great demand to support confidential information service (CIS) and design efficient security strategy against the eavesdropping attacks. In this paper, we propose a solution to cope with the eavesdropping attacks in routing and spectrum allocation. Firstly, we introduce probability theory to describe eavesdropping issue and achieve awareness of eavesdropping attacks. Then we propose an eavesdropping-aware routing and spectrum allocation (ES-RSA) algorithm to guarantee information security. For further improving security and network performance, we employ multi-flow virtual concatenation (MFVC) and propose an eavesdropping-aware MFVC-based secure routing and spectrum allocation (MES-RSA) algorithm. The presented simulation results show that the proposed two RSA algorithms can both achieve greater security against the eavesdropping attacks and MES-RSA can also improve the network performance efficiently.

## 1. Introduction

The number of malignant network attacks is growing rapidly over the past decade. The harms done by these attacks become more and more severe for network users. “Insecurity” has even become the most intuitive impression to people on the network. Optical networks are the main transmission networks for wide covering, large capacity and security. Due to their physical characteristics, various potential physical-layer malignant attack scenarios exist in current and future optical networks [1]. The malignant attacks in optical networks can be divided into two types according to their purposes. One type of attacks is to hinder the right information arriving at right destination, such as jamming attacks and single component attacks. The other is to eavesdrop information but not affect normal communication, such as tapping attacks. The second type attacks are always more difficult to detect than the first one since the first type attacks influence the result of communications directly and the second type attacks even hardly have any influence on the quality of communication. To defense the second type eavesdropping attacks, effective attack-detection in physical layer is the best approach [2], but that is hard to realize or takes a lot of time and cost. Therefore, the network users cannot be aware of the attacks and have to suffer this kind of sustained attacks for a long time that makes privacy and information security of users under a serious threat. So the eavesdropping attacks have been one of main security problems in the optical network. Additionally, for some special information such as military purposes or financial news, the damage caused by the leakage without awareness is far greater than that caused by the hindering transmission. Therefore, it is an urgent demand to develop confidential information service (CIS) for transmitting the special information and study effective security strategies and schemes to satisfy the security requirements of CIS.

Elastic Optical Networks (EON) is a promising technology in the optical transport network which can be used in some important scenarios such as optical interconnection between data centers [3,4]. In EON, sliceable bandwidth-variable transponder [5,6] and flexible optical cross-connect [7] are supported which can provide excellent flexibility with minimum disruption to the existing optical network infrastructures. Moreover, the optimization of optical spectrum and seamless deployment can be achieved. However, EON also faces huge potential security problems because of the lack of effective safety precautions against eavesdropping attacks just like conventional optical networks. As EON is the key development direction of optical transport

* Corresponding author at: No. 10 Xitucheng Road, Haidian District, Beijing 100876, China.
*E-mail address:* yanghui@bupt.edu.cn (H. Yang).

https://doi.org/10.1016/j.yofte.2017.10.004
Received 18 June 2017; Received in revised form 13 September 2017; Accepted 20 October 2017

network, it is significant to improve the defense capability of EON against the eavesdropping attacks.

The routing and spectrum allocation (RSA) is a key function in EON. It is equivalent to routing and wavelength allocation (RWA) in conventional WDM optical networks. It is used to find appropriate route and allocate suitable spectrum slots according to traffic demands [8]. The most common objective of RSA is to minimize the blocking probability for improving network performance. Moreover, some other factors are considered by adding new constraints or objectives in some RSA approaches such as energy efficiency, physical-layer impairments and so on [9,10]. The RSA with security considerations is used for minimizing the potential damage caused by various physical-layer attacks in [11]. Attack-aware RSA in multi-domain EONs has been invested in [12], the RSA schemes of intra and inter domain requests are differentiated with security considerations. Therefore, RSA can provide a solution for the issue of optical networks security in the network planning and provisioning process. The eavesdropping attacks have the similar characteristics with other physical-layer attacks so that the eavesdropping attacks problem also can be solved by using RSA approaches. For example, the damages caused by interchannel eavesdropping and jamming attacks can be cut down by a routing algorithm which minimizes lightpath overlapping in optical network [13]. When an eavesdropper accesses a range of spectrum, reconfiguration of connections and readjustment of occupied spectrum can prevent disclosure of information [14]. However, the existing researches on anti-eavesdrop in the optical networks focus on solving the interchannel eavesdropping and jamming attacks together, which are not valid for fiber tapping eavesdropping. Considering the purpose of eavesdropping attacks and the confidentiality requirements of CIS, traffic flow slicing and parallel transmission are the effective methods against all types of eavesdropping attacks [15]. Multi-flow virtual concatenation (MFVC) triggered by path cascading degree in EONs has been implemented for improving the spectrum efficiency and decreasing blocking probability in our previous works [16,17]. In addition, MFVC can support an implementation method for traffic flow slicing and parallel transmission. Therefore, a security RSA based on MFVC would provide an effective solution against eavesdropping attacks in optical networks in which both spectral efficiency and security of optical networks can be improved by using MFVC.

In the other hand, the probabilities of being attacked in different network positions are different because an optical network covers large area and the networks users with confidentiality requirements distribute unevenly. The happen of eavesdropping attacks can be described by the eavesdropping probability in each fiber link that can be integrated as a probability distribution on eavesdropping attacks [18]. We can improve the security against eavesdropping attacks by secure RSA which adds a secure constraint and allocates the transmission path with lower the eavesdropping probability for the CIS. Therefore, introducing the probability method provides a way to abstract and solute the eavesdropping issue.

In this paper, we first introduce the probability method to describe the security issue against eavesdropping attacks. Based on the distribution of the eavesdropping probability, the awareness of eavesdropping attacks can be realized. An eavesdropping-aware secure RSA (ES-RSA) algorithm is designed and the security of CIS is guaranteed by using the path with low eavesdropping probability. With the consideration of both spectral efficiency and information security, we propose an MFVC-based eavesdropping-aware secure routing and spectrum allocation (MES-RSA) algorithm. Based on MFVC, traffic flow slicing and parallel transmission can be achieved. The parallel transmission can enhance EON security against eavesdropping attacks. Because of traffic flow slicing, the split-spectrum [19] can be used for the transmission of traffic and the spectral efficiency is improved. By comparing with the general RSA, the improvement of security in ES-RSA and the dual improvement of network performance and security in MES-RSA are demonstrated. Additionally, the impacts on MES-RSA from maximum number of sub-flows, guard band size and maximum tolerable differential delay are also demonstrated.

The rest of the paper is organized as follows. In Section 2, we describe the network model and RSA problem statement. In Section 3, we propose ES-RSA algorithm. In Section 4, we propose MES-RSA algorithm. In Section 5, we present numerical and simulation results. At last, we conclude the paper in Section 6.

## 2. Dynamic RSA problem statement

### 2.1. Eavesdropping probability and maximum tolerable information revealing probability (MIRP)

By using probability theory, some problems in the optical networks have been solved effectively, for instance, the network survivability issue in our previous works [20,21]. Different from the other complex physical-layer attack, the occurrence of eavesdropping attack is similar to the network fault for the operator. Therefore, the network security issue against eavesdropping attacks also can be described and solved by using probability theory [22]. In this paper, we consider only the eavesdropping attacks happening in fiber link and assume that the eavesdropping attacks are mutually independent events. We use the eavesdropping probability (EP) to denote the probability that a fiber link is under an eavesdropping attacks. For a real optical network, the EP of each fiber link can be calculated based on the geographical position, history data, security deployment and so on. An example about the EP distribution is shown in Fig. 1 in which we consider a 24-node network in USA and all the nodes are labelled from 1 to 24. Because the

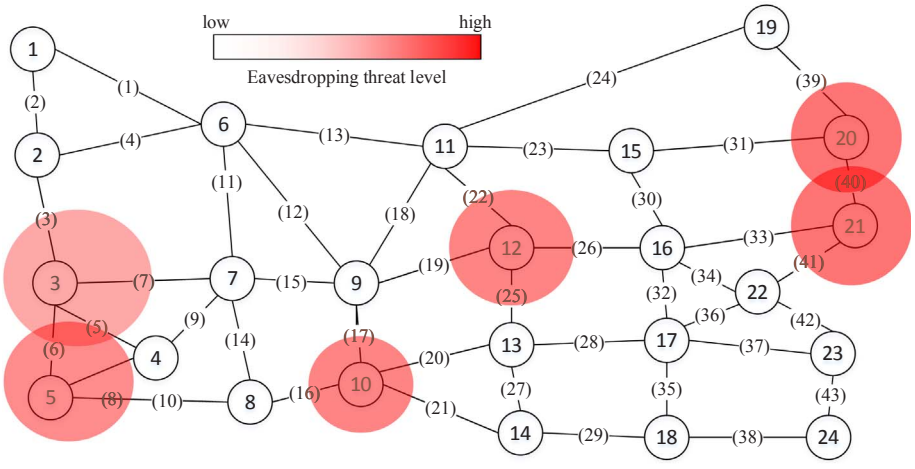


**Fig. 1.** EP distribution of the optical network.