rtgwg
Internet Draft
Intended status: Informational
Expires: January 2023

X. Li
L. Zhang
Y. Tang
Z. Shi
S. Huang
BUPT

June 30, 2022

Photonic firewall oriented routing and spectrum allocation strategy in optical networks
draft-li-rtgwg-photonic-firewall-rsa-03.txt

Status of this Memo

This Internet-Draft will expire on January 1, 2023.

Abstract

The photonic firewall oriented routing and spectrum allocation strategy in elastic optical networks is proposed. For the security detecting requirement, each light-path should pass through at least a photonic firewall. To reduce the blocking rate and improve the spectrum efficiency, the whole network is divided into several parts according to the locations of all deployed photonic firewalls. A photonic firewall is responsible for the security detecting for each part. This strategy has a low complexity and is suitable for large-scale optical networks.

Table of Contents

1. Introduction

This document describes the photonic firewall oriented routing and spectrum allocation strategy in optical networks. Optical networks which take advantages of high-speed and large-capacity has been widely applied to access, backbone transmission, data center interconnection, inter-satellite link, etc. Many new technologies are emerging with the aim of improving the capacity of optical fiber, such as optical orthogonal frequency division multiplexing (O-OFDM) and space division multiplexing (SDM). The accommodated traffic is booming, and more services are emerging, such as cloud computing, big data, augmented reality, and virtual reality. Since the accommodated traffic is very large, the secure transmission becomes more and more important. Due to the large amount of transmission information, wide coverage, and QoT sensitivity, optical networks are highly vulnerable to eavesdropping and attacks. The common attacks exist in optical networks can be simply divided into two parts. One aims for optical device and the other aims for network management. Attacks for optical fiber include eavesdropping, interception, in-band interference, signal delays [Fok2011]. To ensure secure data transmission, some security technologies such as optical encryption, quantum key distribution, chaotic encryption, node/line reinforcement, optical steganography [Wang2010], etc., have been proposed. These technologies help to ensure the confidentiality and integrity of data transmission over optical networks. However, when invasions and attacks are hidden in the transmitted data, these technologies are useless. Photonic firewall is an important network security device. It leverages the all-optical pattern matching to directly identify the signals in the optical domain, then distinguish hidden network intrusions and attacks, and finally selects corresponding defense means according to the set security policy. Thus, it can directly realize intrusion detection and security protection in the optical domain. Since the processing rate of the photonic firewall is far great than that of the electronic firewall, a photonic firewall can replace tens of thousands of electronic firewalls. In future, we believe the photonic firewall can be widely used in the optical backbone network, optical access network, optical datacenter network, etc. A photonic firewall is composed of multiple all-optical logic gate, regenerators, optical amplifiers, etc. The cost of the photonic firewall is very high. In the early stage, the photonic firewall can only be deployed just in a few places. To ensure each established light-path can be obtained the security detecting, the photonic firewall oriented routing and spectrum allocation strategy should be designed. To avoid the traffic congestion on some fiber links or a certain photonic firewall, we divide the whole topology into several parts according to the number of and the locations of all deployed

photonic firewalls. A photonic firewall is responsible for the security detecting for each connection in the each part.

2. Conventions used in this document

This document makes use of the following acronyms:

QoT: Quality of Transmission

AI: Artificial Intelligence

SDM: Space Division Multiplexing
O-OFDM: Optical Orthogonal Frequency Division Multiplexing

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying significance described in RFC 2119 [RFC2119].

3. Motivation

Photonic firewall can directly realize the intrusion detection and security protection in optical domain. A photonic firewall can replace tens of thousands of electronic firewalls. Since the cost of the photonic firewall is very high, it can only be deployed just in a few places. In order to ensure that each established light-path can be obtained the security detecting, the photonic firewall oriented routing and spectrum allocation strategy should be designed for each user request. The strategy has a low complexity and is suitable for large-scale optical networks.

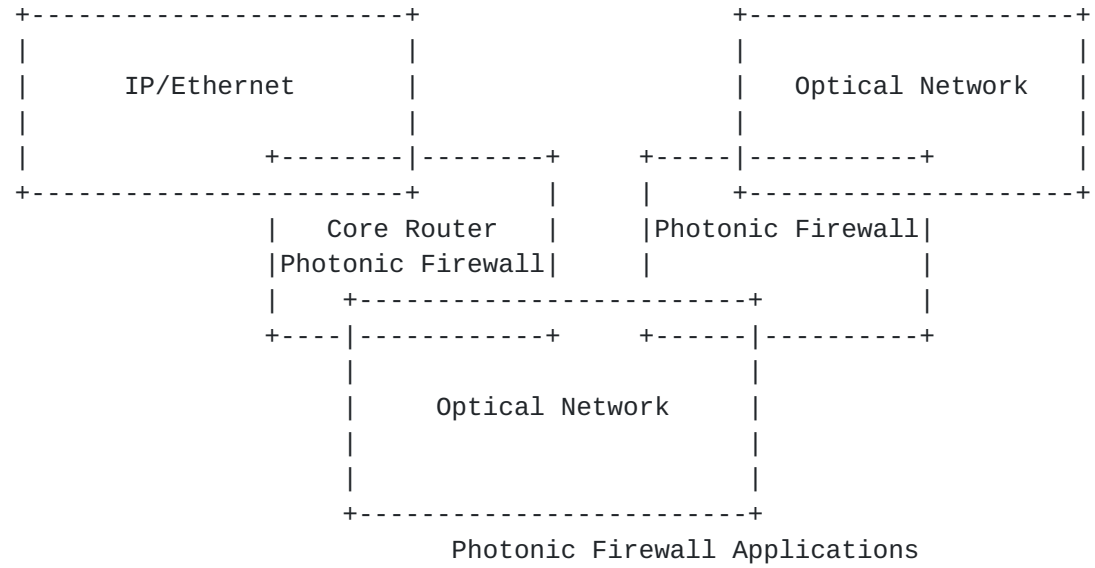
4. Photonic Firewall Oriented Routing and Spectrum Allocation Strategy

This section first gives introduce the photonic firewall and its applications in optical networks. Then, the secure connection establishment requirement is elaborated. At last, the photonic firewall oriented routing and spectrum allocation strategy is elaborated.

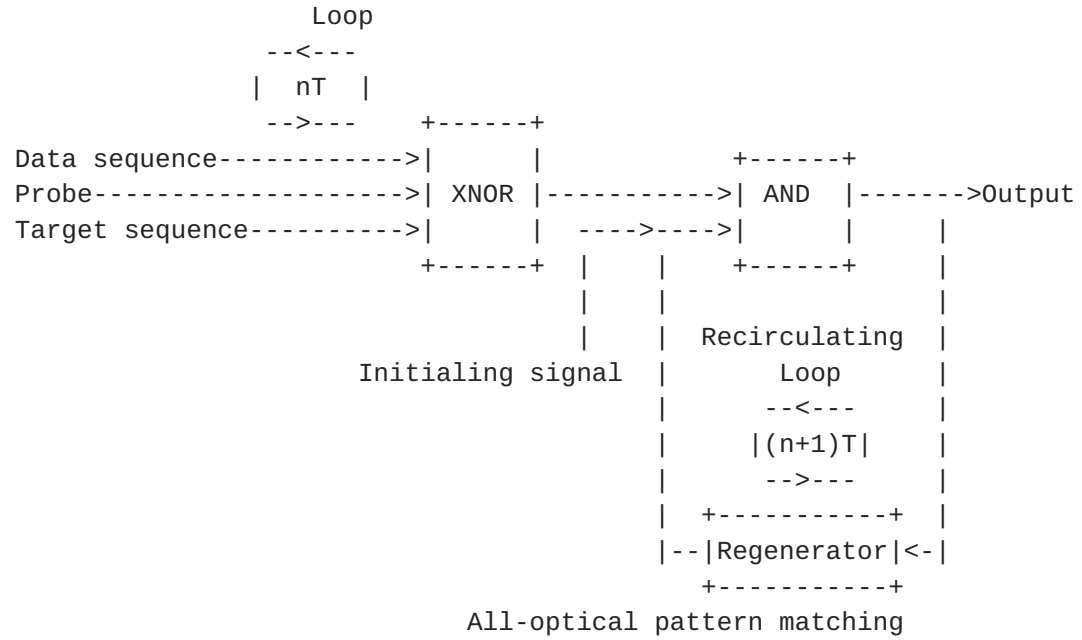
4.1. Photonic Firewall

Photonic firewall is an optical network device. It leverages the all-optical pattern matching to directly identify the signals in the optical domain, and then distinguish hidden network intrusions and

attacks. It selects corresponding defense means according to the set security policy. As presented in Figure 1, it can be deployed in the important optical switching node, gateway node, or access node. The all-optical pattern recognition is the core part of photonic firewall. It is composed of one all-optical XNOR gate, all-optical AND gate, and a regenerator, as shown in Figure 2.



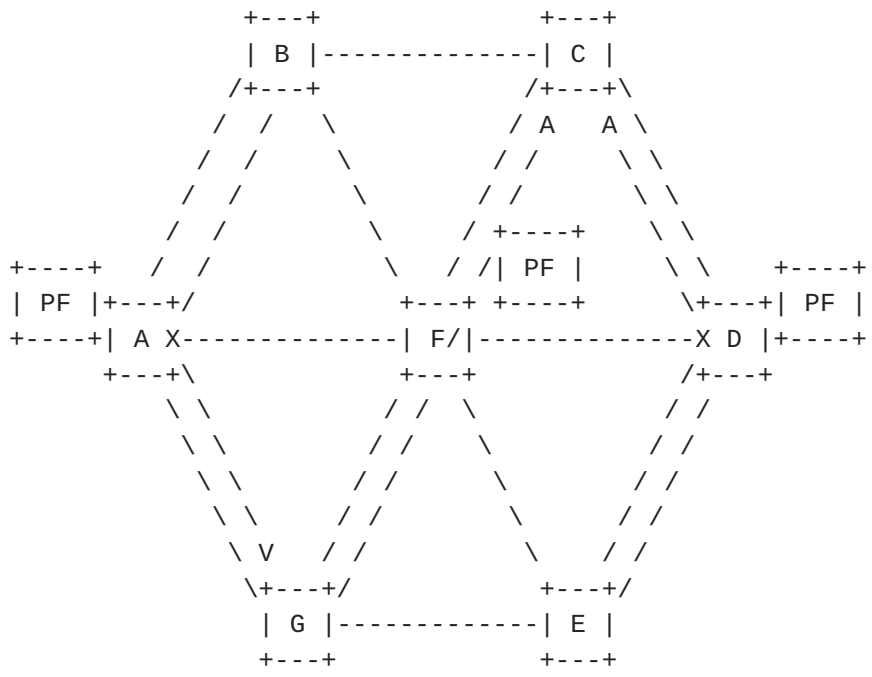
Photonic Firewall Applications



All-optical pattern matching

4.2. Secure Connection Establishment Requirement

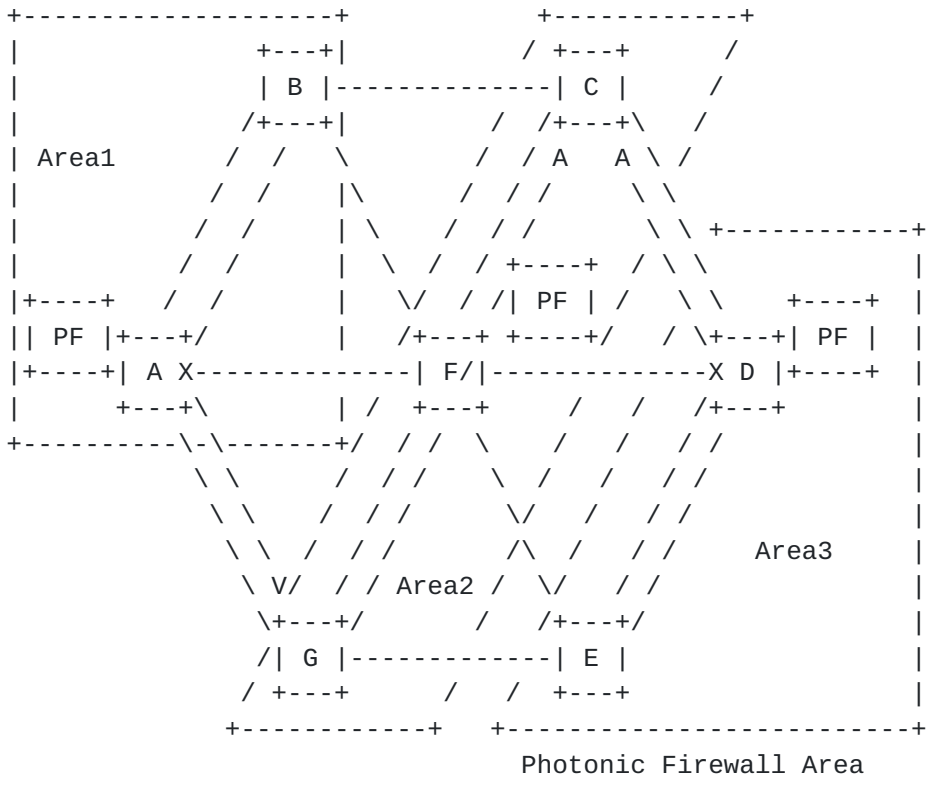
For the security detecting requirement, each light-path should pass through at least a photonic firewall. As presented in Fig. 3, three photonic firewalls are deployed in nodes A, F, and D. There are three light-paths are established in the network (B->A->G, G->F->C, and E->D->C). Each light-path passes through a photonic firewall.



Secure Connection Establishment (PF denotes photonic firewall)

4.3. Photonic Firewall oriented Routing and Spectrum Allocation Strategy

The photonic firewall oriented routing and spectrum allocation strategy adopts the greedy strategy. For each user, it calculates the closest photonic firewall. Thus, each photonic firewall has a user set in which any user is closest to it. In other words, the whole network is divided into several parts according to the locations of all deployed photonic firewalls. When a new user request arrive the network, the user first calculates the shortest path to its closest photonic firewall, and then calculates the shortest path from the photonic firewall to its destination. Finally, the First-Fit algorithm is used to conduct spectrum allocation on the two shortest paths.



As presented in Fig. 4, the whole network is divided into three parts. In each part, a photonic firewall is responsible for the security detecting for each user in this part. This strategy has a low complexity and is suitable for large-scale optical networks.

5. Security Considerations

TBD

6. IANA Considerations

This document makes no request of IANA.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

7.2. Informative References

[Fok2011] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical Layer Security in Fiber-Optic Networks", IEEE Transactions On Information Forensics and Security, vol. 6, no. 3, pp. 725-736, 2011.

[Wang2010] Z. Wang, M. P. Fok, L. Xu, J. Chang, and P. R. Prucnal, "Improving the privacy of optical steganography with temporal phase masks", Opt. Express, vol. 18, no. 6, pp. 6079-6088, 2010.

Authors' Addresses

Xin Li
Beijing University of Posts and Telecommunications
10 Xitucheng Road, Haidian District, Beijing, China

Email: xinli@bupt.edu.cn

Lu Zhang
Beijing University of Posts and Telecommunications
10 Xitucheng Road, Haidian District, Beijing, China

Email: luzhang@bupt.edu.cn

Ying Tang
Beijing University of Posts and Telecommunications
10 Xitucheng Road, Haidian District, Beijing, China

Email: ytang@bupt.edu.cn

Zicheng Shi
Beijing University of Posts and Telecommunications
10 Xitucheng Road, Haidian District, Beijing, China

Email: zchshi@bupt.edu.cn

Shanguo Huang
Beijing University of Posts and Telecommunications
10 Xitucheng Road, Haidian District, Beijing, China

Email: shghuang@bupt.edu.cn