Optical Fiber Technology 23 (2015) 108–115

Contents lists available at ScienceDirect

Optical Fiber Technology

www.elsevier.com/locate/yofte

Multipath protection for data center services in OpenFlow-based software defined elastic optical networks

Hui Yang [a,*], Lei Cheng [a], Jian Yuan [a], Jie Zhang [a], Yongli Zhao [a], Young Lee [b]

[a] State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b] Huawei USA, 5340 Legacy Road, Plano, TX 75023, USA

ARTICLE INFO

Article history:
Received 29 November 2014
Revised 26 February 2015
Available online 26 March 2015

Keywords:
Elastic optical network
Software defined network
Data center
OpenFlow
Multipath protection

ABSTRACT

With the rapid growth of data center services, the elastic optical network is a very promising networking architecture to interconnect data centers because it can elastically allocate spectrum tailored for various bandwidth requirements. In case of a link failure, to ensure a high-level quality of service (QoS) for user request after the failure becomes a research focus. In light of it, in this paper, we propose and experimentally demonstrate multipath protection for data center services in OpenFlow-based software defined elastic optical network testbed aiming at improving network reliability. We first propose an OpenFlow-based software defined elastic optical network architecture for data center service protection. Then, based on the proposed architecture, multipath protection scheme is figured based on the importance level of the service. To implement the proposed scheme in the architecture, OpenFlow protocol is extended to support multipath protection in elastic optical network. The performance of our proposed multipath protection scheme is evaluated by means of experiment on our OpenFlow-based testbed. The feasibility of our proposed scheme is also demonstrated in software defined elastic optical networks.

1. Introduction

With the rapid growth of high-bitrate applications, the data center services have attracted an amount of attention by the service providers and network operators. A large amount of service providers and enterprises are hosting their storage contents and computing resources in data centers to achieve lower delay, higher availability and efficiency at a lower cost [1]. Due to diversity and hugeness of the services, such network-based data center applications have presented the high burstiness and high-bandwidth characteristics. To accommodate such traffic demands, there is a pressing need to utilize the available optical fiber's spectrum efficiently. Due to strictly following the fixed ITU-T wavelength grids and spacing, the traditional wavelength-division-multiplexing (WDM) optical transport networks lead to low spectrum utilization. To better utilize the frequency resource and accommodate super-wavelength traffic effectively, an elastic optical network has been proposed and experimentally demonstrated [2,3]. It supports channels operating at heterogeneous line rates by allocating spectral resources tailored for a variety of connection demands in a flexible and dynamic manner [4,5]. Additionally, as a special form of multicarrier modulation, orthogonal frequency division multiplexing (OFDM) is used to split single data stream into a number of lower rate orthogonal sub-carriers, which can be partially overlapping in the spectrum domain [6]. The enabling technologies, such as OFDM-based bandwidth-variable wavelength cross-connects (BV-WXC) and bandwidth-variable transponder (BV-Transponder) have turned the elastic optical network into reality [7,8].

Additionally, a large amount of network-based data center applications require the end-to-end guaranteed quality of service (QoS). If a link failure occurs in the elastic optical network, the network protection provided in elastic optical network for the dynamic traffic will become much complex [9]. Then to ensure the high-performance QoS of user demands after a failure deserves to be the research focus. So far, optical network survivability in the optical network scenario has been well studied for the failure events [10–13]. To cope with single failure problem in WDM mesh networks, authors in [10] systematically summarize the protection schemes for survivability including dedicated-path protection, shared-path protection and shared-link protection. The bandwidth squeezed restoration scheme is proposed [11] by the manner of best-effort recovery to overcome the restored spectral insufficiency and ensure a highly survivable traffic. Authors in [12] propose and evaluate shared-path protection strategies in OFDM-based optical networks, and show that aggressive backup sharing can significantly improve capacity efficiency. The authors in [13]

* Corresponding author.
E-mail address: yanghui@bupt.edu.cn (H. Yang).

http://dx.doi.org/10.1016/j.yofte.2015.03.002
1068-5200/

propose an efficient survivable FWDM network design algorithm, which can achieve a better efficiency in terms of power consumption, spectral utilization and cost. The authors in [14] implement the path protection and restoration based on the OpenFlow-based unified control plane for multi-layer multi-granularity optical networks. However, how to realize the protection in the real environment with equipment, protocol and resource have not been mentioned in the work.

On the other hand, as a promising centralized control architecture, the software defined networking (SDN) enabled by OpenFlow protocol has gained popularity by supporting programmability of data center and network functionalities [14–16], which can provide maximum flexibility for the operators, make a unified control over various resources and abstract them as unified interface for the joint optimization of functions and services with a global view [17,18]. Compared with the generalized multiprotocol label switching (GMPLS), the SDN centralizes intelligence control functions into a controller by functional abstracting a control plane away from the data plane. The SDN enables flexible control of network traffic and provides an innovative platform for core network applications. The main idea of OpenFlow is to control the way in which individual packets are handled in the switches by providing a communication between the OpenFlow controller and OpenFlow switches (oSwitch). It brings programmable features to networking and creates a more simple and extensible architecture for the construction of optical networks. A number of work has been established in recent years, and OpenFlow extension are made to implement elastic optical networks in SDN architecture, demonstrated the extensibility of SDN framework [19,20]. But only a few of them is concentrated on network reliability (e.g., protection and restoration) since OpenFlow was original designed for supporting the switch of packets only [21,22]. Furthermore, if a proper protection mechanism can be implemented into SDN architecture, a more reliable network can be realized [23].

In light of it, in this paper, we propose and experimentally demonstrate multipath protection for data center services in OpenFlow-based software defined elastic optical network testbed aiming at improving network reliability. We first propose an OpenFlow-based software defined elastic optical network architecture for data center service protection. Then, based on the proposed architecture, multipath protection scheme is figured based on the importance level of the service. To implement the proposed scheme in the architecture, OpenFlow protocol is extended to support multipath protection in elastic optical network. The performance of our proposed multipath protection scheme is evaluated by means of experiment on our OpenFlow-based testbed. The feasibility of our proposed scheme is also demonstrated in software defined elastic optical networks.

The rest of this paper is organized as follows. Section 2 introduces the OpenFlow-based software defined elastic optical network architecture. The multipath protection scheme under this network architecture as well as the relevant OpenFlow protocol extension is proposed in Section 3. We describe the experimental environment and present the results and analysis in Section 4, and last section gives the conclusions.

2. OpenFlow-based software defined elastic optical network architecture

The OpenFlow-based software defined elastic optical network architecture for data center service protection is illustrated in Fig. 1. In the proposed architecture, the elastic optical networks can be used to deploy in the data plane. The optical network resources can be software-defined with OpenFlow and controlled by an OpenFlow controller in a unified manner. To control the

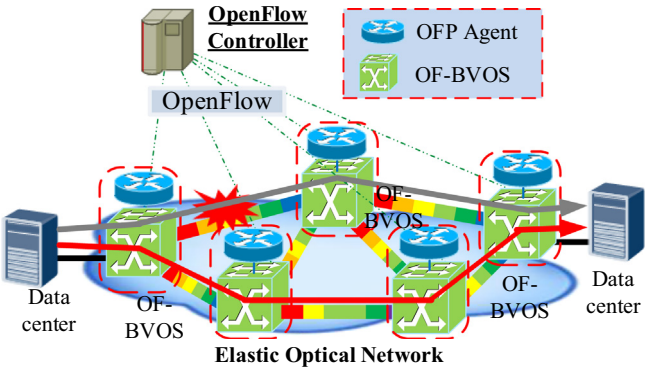

Fig. 1. The architecture of OpenFlow-based software defined elastic optical network.

networks with extended OpenFlow protocol (OFP), OpenFlow-enabled bandwidth variable optical switch with OFP agent software are required, which are referred to as OF-BVOS and demonstrated and proposed in [20]. The proposed architecture emphasizes that it effectively realizes the multipath protection through OpenFlow protocol and the optimization of optical network resources in case of the link failure. Once received a link failure information from the OC, it is responsible for the multipath protection in elastic optical network. The OC exploits optical network resources abstracted from the physical network and performs accordingly working and protection lightpaths provisioning in optical networks. The multipath protection interacting between the controller and equipment can provide backup connectivity for the user to guarantee end-to-end QoS.

To achieve the function of the proposed architecture described above, the OpenFlow controller has to be extended in order to support the multipath protection functions. The functional building blocks of controller and the basic interactions among them are described in Fig. 2. The OpenFlow controller consists of five modules, i.e., network abstraction, failure detection, path computing entity (PCE) [24] and plug-in, multipath protection and data base modules. The network abstraction module can abstract the required flexible optical resources, while the failure detection module interworks the information with OF-BVOS periodically to perceive optical networks through extended OFP. In case of a link failure, the failure detection module discovers it and delivers such failure information to the multipath protection module. When the link failure occurs in elastic optical network, the multipath protection module decides to apply multipath protection scheme associated with the optical network resources. The PCE module can

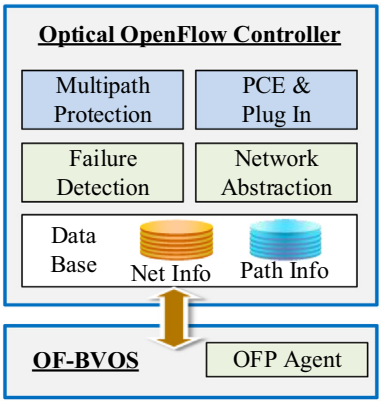

Fig. 2. The functional model of the controller in software defined elastic optical network architecture for multipath protection.