Computer Networks 133 (2018) 73–89

Contents lists available at ScienceDirect

Computer Networks

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

Survivable automatic hidden bypasses in Software-Defined Networks

Piotr Boryło*, Jerzy Domżał, Robert Wójcik

AGH University of Science and Technology, al. Mickiewicza 30, Krakow 30–059, Poland

ARTICLE INFO

Article history:
Received 20 February 2017
Revised 5 October 2017
Accepted 17 January 2018

Keywords:
Bypass
Optical
Resilience

ABSTRACT

The paper focuses on the problem of effective and resilient network resources management under condition of increasing Internet traffic. Multilayer automatic optical networks are considered as a solution usually indicated as the most appropriate for the future Internet. In this paper, we propose a Survivable Automatic Hidden Bypasses approach to enhance resource utilization and reliability in multilayer optical networks. Our solution uses the Software-Defined Networking concept to automatically create or remove hidden bypasses which are not visible at the network layer. We propose a novel survivability metric which is applied during optical bypass creation in order to handle network failures in a proactive manner. Such an approach contrasts with the most common one where bypasses are considered as a mechanism to handle network failures. We combine the metric with different restoration schemas and investigate the proposed mechanism under three failure scenarios. The mechanism of hidden bypasses increases throughput and reduces transmission delays while novel proactive survivability mechanisms neutralize negative impact of network failures.

1. Introduction

Global IP traffic is predicted to increase over threefold from 2012 to 2017, reaching 120 exabytes (10^{18} bytes) per month in 2017 [1]. This enormous growth puts pressure on network operators to develop robust, reliable and scalable backbones, as well as, to efficiently and effectively manage their network infrastructure. A multilayer optical network is the most popular and prominent architecture to meet modern requirements. However, despite many attempts to automate the process, optical networks are usually still managed manually. Optical paths are created by the administrators based on the traffic distribution developed for peak hours. Such an approach to network dimensioning and management results in over-provisioning and resource waste during off-peak hours.

The concept of Software-Defined Networking (SDN) becomes more and more popular in the context of telecommunication networks management. SDN, assumes that the control plane and the data plane are separated to simplify the management of traffic in the network. At the control plane, usually the central controller decides to which interface packets should be sent at the data plane. This concept is also used in optical networks, especially to improve the effectiveness of routing and wavelength assignment. Advantages of the SDN concept are perfectly suited to the current needs, such as on-demand network control, complete knowledge about network topology, knowledge about network flows, application-oriented approach (e.g. SDN support for fog and cloud interplay [2]) and possibility to effectively implement traffic engineering mechanisms in a centralized manner (for example, energy-aware anycast strategies [3,4]).

Several approaches to multilayer optical networks already exist. Solutions may differ with regard to the selection of egress and ingress nodes of optical path being established in the network. First extreme solution, known as opaque, denotes establishing lightpaths between adjacent nodes. Thus, all the data carried by the lightpaths is processed in the electric layer in each router on the path. This solution, is also known as non-bypass as none of the electric layer nodes is bypassed by the optical path. It is also the most efficient for lightly utilized networks. At the other extreme, full optical mesh with lightpaths between each pair of nodes can be established in the network. This solution is especially recommended for highly utilized networks which probably fully utilize established optical paths. Optical bypasses are a compromise between presented solutions. An optical bypass connects two non-adjacent network nodes skipping optical-electrical-optical conversion in intermediate nodes. A bypass can be established on demand during peak hours, in case of network congestion or to counteract a network failure. Such dynamic bypasses are designed mainly to offload electric layer, reduce energy consumption and improve network reliability.

* Corresponding author.
E-mail addresses: borylo@agh.edu.pl (P. Boryło), jdomzal@kt.agh.edu.pl (J. Domżał), robert.wojcik@kt.agh.edu.pl (R. Wójcik).

https://doi.org/10.1016/j.comnet.2018.01.022
1389-1286/

Optical paths and bypasses can be broadcasted to the electric layer or remain hidden independently from the architecture. In general, instabilities may occur if creation of optical paths is advertised to the electric layer. On the other hand, cooperation of both network layers usually results in more efficient resource utilization. Hybrid approaches are also possible and considered. Simultaneously, bypasses can also be classified with regard to the routing algorithms in the optical layer. Direct bypass is established between two nodes as long as there are traffic demands between them and usually routing is performed based on the shortest path routing. Therefore, this intuitive approach reduces the total number of required transponders and Erbium Doped Fibre Amplifiers (EDFAs). However, when optical path is established, the whole wavelength is occupied even for very small demands between nodes resulting in low network resource utilization. On the other hand, multihop bypasses allow demands between different pairs of nodes to share capacity of a single optical channel. This approach results in more efficient optical resource utilization and reduction in energy consumption (fewer energy-hungry router ports are needed). As a side effect, length of electric layer paths may increase and reduce the scale of improvement.

Our approach, presented in this paper, is an extension introducing survivability aspects to the Automatic Hidden Bypasses (AHB) mechanism proposed in [5]. We use a hidden bypass functionality as presented in [6], and add components known from SDN. Our solution takes advantage from the SDN capabilities making the process scalable, effective and completely automated. This means that bypasses are created and torn down based on existing demands in multilayer optical networks. The network decides when and how to create a new bypass as well as which flows should use it. Analysis presented in [5] shows that AHB can provide lower delays and higher throughput. The mechanism yields excellent results in both low and high loaded networks, however, up till now, survivability issues were neglected.

In this paper we focus on mechanisms for provisioning of optical bypasses in the resilient manner. We assume, that the network is controlled by the centralized controller consistent with the idea of the SDN, and the AHB concept. We propose novel survivability metric considered during optical bypass establishment in order to handle network failures in a proactive manner. We investigate proposed Survivable Automatic Hidden Bypass (SAHB) mechanism under various failure scenarios: (1) Occasional network failures, (2) disaster, and (3) failure of the critical network link. To the best of our knowledge this work is the first one that analyzes deeply the problem of resilient optical bypasses establishment in order to improve survivability of multilayer network. Such an approach contrasts with the most common one where bypasses are considered as a mechanism to handle network failures. Additionally, we join SAHB with different restoration schemas and prove that advantages are significant and valuable. The issue is important as it regards survivability in network architecture indicated as the most prominent solution for future networks with respect to the SDN network management concept.

The rest of this paper is organized as follows. The next section provides a description and references to the works related to the resilient bypasses provisioning using SDN concept. Section 3 presents the main contribution of this paper which is the Survivable Automatic Hidden Bypass concept. Simulation environment, scenarios and results are presented in Section 4. Finally, Section 5 concludes the paper.

2. Related work

General survey regarding the traffic management in multilayer networks utilizing optical bypass mechanisms was provided in our previous work [5]. Some of the described mechanisms allow for setting up optical bypasses in both, hidden (not visible at the IP layer) and announced (visible at the IP layer) versions. In some cases, it is assumed that a centralized controller is used, while others use a distributed approach. All of the mechanisms were compared to the AHB mechanism proposed in [5]. In this paper, only brief summary of general solutions will be provided as we will focus on resilience mechanisms in the context of optical bypasses.

The first category of works focuses mainly on comparison between centralized and distributed approaches. In [7], the authors provide evaluation of four dynamic bypass mechanisms in a network without a centralized controller. The simulation results presented in the paper confirm that the best results were obtained by using multihop bypass mechanisms, however, at a cost of creating and removing a high number of bypasses in the network. In [8], each network node monitors traffic through a predefined period of time. At the end of the period, if the volume of traffic towards a node exceeds a given threshold, the node may create a bypass and reroute traffic. Information about the new bypass is not announced to a routing protocol and decision to create a hidden bypass is made locally in a node and the central controller is not used. The authors of [9] confirm advantages of centralized solutions over distributed ones regarding efficiency. Another category of papers analyzes the issue from the perspective of differences between hidden and announced bypasses. The authors of [10] present hidden and announced versions of bypasses and show three methods for adapting a virtual topology to current needs. The authors show that the hidden bypass mechanisms have the lowest impact on the established topology, while the number of topology changes depends on the difference between the peak and low load values. The author of [11] proposes and analyzes a dynamic algorithm to find a set of bypasses for the Atlanta 15-node network which is periodically updated after each 15–30 min. In [12] the authors present the concept of automatically switched optical bypasses not reported to the IP layer. The central controller decides how the bypasses should be established using integer linear programming for optimization.

An example of using the SDN concept in optical networks is presented in [13], where the optical networks are controlled in an efficient way and the reliability of transmission is improved. In [14] the authors explain that the implementation of the OpenFlow controller results in an intelligent control plane for optical networks. The analysis proves that the scalable solution improves reliability of transmission, but any of those papers considers the bypass implementation. An OpenFlow-base unified control plane architecture for optical SDN is proposed in [15] and tailored to cloud services. The authors of [15] demonstrated their mechanism in a testbed built on ADVA fixed reconfigurable optical add-drop multiplexers (ROADMs). The results show that paths, in the hardware, can be established in time ranging from a few seconds to dozens of seconds. The operation of the controller takes few additional seconds and also this solution can be extended by bypass mechanisms. Provisioning cloud services over software-defined optical networks is also considered in [16] and [17]. The former work adjusts anycast strategies for optical networks to three types of cloud services while the later investigates the issue of cooperation between an SDN controller, an optical network and cloud orchestration software.

Works considering Flow-Aware Networks (FAN) in the context of bypasses are also presented. A valuable approach to multilayer FAN is found in [18]. The authors propose to extend the original FAN concept by introducing the option to route traffic flows through a newly established optical bypass. Mechanisms proposed so far, e.g. in [19], focus only on IP network layer traffic management. Three different policies are used to accept the flow for an optical bypass.