Delft University of Technology
Master's Thesis in Embedded Systems

Online Survivability in Software Defined Elastic Optical Networks

Lina He

Online Survivability in Software Defined Elastic Optical Networks

Master's Thesis in Embedded Systems

Embedded Software Section
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology
Mekelweg 4, 2628 CD Delft, The Netherlands

Lina He
4519051
linahe@student.tudelft.nl

22nd January 2018

Author

Lina He (linahe@student.tudelft.nl)

Title

Online Survivability in Software Defined Elastic Optical Networks

MSc presentation

29th January 2018

Graduation Committee

F.A. Kuipers	Delft University of Technology
J. Weber	Delft University of Technology
R. Remis	Delft University of Technology

Abstract

With the high and varying demands for network bandwidth, Elastic Optical Networks (EON), as a promising solution for future optical transport networks, have been getting increased attention due to its flexibility and efficiency. As a huge amount of data is transformed over these networks, even short failures will lead to major data loss. Network survivability is, thus especially crucial in EON. Two main criteria for evaluating the survivability performance of optical transport networks are recovery time and resource efficiency. Taking resource efficiency into consideration, we propose a multiple-backup-path protection scheme for traffic over super-channels which is the trend in EON. As the proposed multiple-backup-path protection scheme is more suitable for traffic over super-channels, we classify the traffic based on their bandwidth requirements. For different classes, we propose a survivability scheme named Hybrid Single and Multiple Backup Protection (HSMBP), which combines the single and multiple path backup protection.

Because Software Defined Networking (SDN) is an ideal architecture that allows easy control and flexibility of EON, we realize HSMBP under its architecture. Furthermore, we test this hybrid scheme in reference networks online and compared to other two protection schemes. Our simulation results show that HSMBP can effectively improve the network performance by reducing Bandwidth Blocking Probability (BBP).

Preface

I would like to express my great appreciation to my supervisor Fernando Kuipers. He gave me lots of professional advice and support during the whole thesis period. I would also like to appreciate Belma Turkovic. She instructed me about my thesis and helped me solve many problems. She is kind and creative. I am especially grateful to Jorik Oostenbrink. He is positive and thoughtful. He found a lot of mistakes in my work and helped me to correct them. Further, thanks my dear boyfriend Yuchen Huang. He encouraged me to overcome difficulties during the thesis period. His positive attitude has a large influence on me. He makes my life filled with joy. Last but not least, thanks my family for the support in my life. When I feel upset, they comfort me and encourage me. The love from my family makes me full of courage to face every challenge.

Lina He

Delft, The Netherlands
22nd January 2018

Contents

Preface **v**

1 Introduction **1**

2 Background **3**

2.1 Elastic Optical Networks 4

2.1.1 Network Model 5

2.1.2 Routing and Spectrum Assignment 6

2.2 Survivability 8

2.3 Fragmentation Issues 8

3 Related work **11**

4 Software Defined Optical Networking **15**

4.1 Network Architecture 15

4.2 Optical Extension of OpenFlow Protocol 18

4.2.1 Basic OpenFlow Protocol 18

4.2.2 OpenFlow Extension 19

4.3 OpenFlow Agent 20

5 Survivability scheme **21**

5.1 Hybrid Single and Multiple Backup Protection 21

5.1.1 Multiple Failure Protection 22

6 System and design **25**

6.1 HSMBP in SDN 25

6.1.1 Single-path Failover 26

6.1.2 Multi-path Failover 26

6.2 Path and Spectrum Provisioning in SDN 27

6.3 Path and Spectrum Computing Module 27

6.3.1 Disjoint Path Computing 28

6.3.2 Path Selection Policy 29

6.3.3 Spectrum Allocation Policy 30

6.3.4 Online RSA with HSMBP 31

7 Evaluation **35**
7.1 Evaluation Metrics 35
7.2 Experiments in NSF-14 and USB-24 36
7.2.1 Experimental Environment 37
7.2.2 Schemes Comparison 38
7.3 Experiments in Random Graph 40
7.3.1 Experimental Environment 40
7.3.2 Schemes Comparison 41
7.3.3 Influence of different parameters 43

8 Conclusions & Future Work **47**
8.1 Conclusions 47
8.2 Future Work 48

A Simulation Platform **53**
A.1 Packet Optical Convergence 54
A.2 Optical tutorial VM 55
A.3 ONOS 1.10 55

B HSMBP in NSF and USB **61**
B.1 Influence of the threshold value 61
B.2 Influence of the number of paths 63

List of Figures

2.1 The fixed and flexible grid in optical transport networks. [23] 4
2.2 The characteristics of Elastic Optical Networks. [19] 5
2.3 The model of Elastic Optical Networks. [19] 6
2.4 The node model of Elastic Optical Networks. [19] 7

4.1 The architecture comparison of SDN and SDEON. 16
4.2 The converge control of packet and circuit in SDN. [11] . . . 17
4.3 The architecture of OpenFlow 1.3. [12] 18
4.4 The Flowchart of packet flow in an OpenFlow switch. [12] . . 19
4.5 The OpenFlow Agent for optical switch. [17] 20

5.1 The single and multiple-path backup protection. 22
5.2 The protection process of HSMBP. 23

6.1 The single path backup through the fast failover group table. 26
6.2 The multipath backup protection through group table chain. 27
6.3 The Architecture of HSMBP in Software Defined Networking (SDN). 28

7.1 Topologies used in simulations marked fiber length in kilometers. 37
7.2 The performance for different schemes in NSF-14 and USB-24 39
7.3 The performance for different schemes in Random Graph . . 42
7.4 The performance for different threshold in 30-node Random Graph 44
7.5 The performance for different path number in 30-node Random Graph 45

A.1 The Multi-layer control of ONOS platform 53
A.2 The forwarding model for packet optical convergence [1] . . . 54
A.3 Two packet switches connect after adding host intent 55
A.4 The error states of optical switches. 57
A.5 The failure of installing HostToHost intent. 57
A.6 The error states of optical switches. 58

B.1 The performance for different threshold in NSF-14 and USB-24 62
B.2 The performance for different path number in USB-24 64

List of Tables

7.1 The table of simulation parameters 38
7.2 Mean values for different methods in NSF14 39
7.3 Mean values for different methods in USB24 40
7.4 The table of simulation parameters 41
7.5 Mean values for different schemes in 20-node Random Graph 41
7.6 Mean values for different schemes in 30-node Random Graph 42
7.7 Mean values for different threshold value in 30-node Random Graph 43
7.8 Mean values for different path number in 30-node Random Graph 45

B.1 Mean values for different threshold in NSF14 61
B.2 Mean values for different threshold in USB24 62
B.3 Mean values for different path number in USB24 63

Acronyms

BBP Bandwidth Blocking Probability. iii, 36, 38, 41, 43, 44, 57, 59

BFR Bandwidth Fragmentation Ratio. 36, 38, 41, 43, 44, 57, 59

CWDM Coarse Wavelength Division Multiplexing. 3

DPP Dedicated Path Protection. 11, 12, 35, 38, 41

DWDM Dense Wavelength Division Multiplexing. 3

EON Elastic Optical Networks. iii, 1, 2, 4–6, 8, 9, 11–13, 15, 16, 21, 25

GMPLS/PCE Generalized Multi-Protocol Label Switching/Path Computation Element. 15

HSMBP Hybrid Single and Multiple Backup Protection. iii, 21–23, 28, 31–33, 35, 38, 44, 57, 59

ITU-T International Telecommunication Union-Telecommunication. 3

MPP Multipath Protection. 12

OFDM Orthogonal Frequency-Division Multiplexing. 4

ONOS Open Network Operating System. 48–55

PCE Path Computation Element. 15

ROADM Reconfigurable Optical Add-drop Multiplexer. 50

RSA Routing and Spectrum Assignment. 6, 8, 9, 15, 27

RWA Routing and Wavelength Assignment. 6

SBPP Shared Backup Path Protection. 11, 12, 35, 38, 41

SDEON Software Defined Elastic Optical Networks. 15, 16

SDN Software Defined Networking. 2, 15, 16, 25, 28

SLICE Spectrum-Sliced Elastic Optical Path. 4

SPP Squeezed Path Protection. 11, 12

SUR Spectrum Utilization Ratio. 36, 38, 41, 43, 44, 57, 59

WDM Wavelength Division Multiplexing. 3, 6

Chapter 1

Introduction

Will the bandwidth growth ever stop? Likely no. The total internet demand is expected to continue to grow as a consequence of the increasing number of video streams as well as other new services such as cloud services and virtual reality/augmented reality (VR/AR). The forecast from Cisco Visual Networking Index Networks shows that global IP traffic will grow at a Compound Annual Growth Rate (CAGR) of 24 percent from 2016 to 2021 [10]. With the insatiable demand for bandwidth, optical networks have become a focus of research due to their high capacity, low attenuation, and low energy consumption. In the near future, the data flows will range from tens of gigabits up to terabits per second in optical networks. Network operators need to transport such traffic in a cost-effective and scalable manner.

An Elastic Optical Network (EON) [14] is a promising network model to achieve cost-effective and scalable optical transmission. One of the unique features of EON is its support for the super-wavelength. A super-wavelength signal is transmitted at one wavelength in a fiber-optic channel. The channels for super-wavelength signals are called “superchannels”. In EON, “superchannels” are constructed when the demand for bandwidth is too large to be handled by a single optical channel. Multiple, coherent optical carriers are combined to create a unified super-channel and these carriers traverse the optical network in one operational cycle. It can attain data rates beyond 100 *Gbps* and has efficient energy consumption. We call traffic over “superchannels” super traffic.

If the trend of “superchannels” continues in the future, the expected bit rate of an EON channel will increase to $400 - 1000$ *Gbps*. Therefore, the aggregate throughput can be tens to hundreds Tbps [30]. A small failure, such as one fiber link broken, will have a significant negative influence on the optical connections and sequentially lead to massive data loss. Thus, it is important to improve the network survivability in EON.

Currently, better survivability can be achieved by reserving additional resources for a backup path that are going to be used in cases when the primary path fails. There are multiple ways to find backup resources to protect the primary path and most solutions use dedicated reserved resources for their backup paths. These additional optical resources are reserved and cannot be used for the transmission of the actual optical transmission, thus reducing the efficiency and increasing the blocking probability. Especially, the backup path of super traffic reserving a big block of resources in each link along the backup path will highly influence the following actual optical transmission.

In this thesis, our objective is to reduce the negative influence of survivability in order to make optical transport networks more resource-efficient. To realize our objective, we will address the following research questions:

1. What makes EON a promising paradigm for optical transmission and what its main problems are?

2. Which survivability schemes exist to recover the optical traffic in EON?

3. Can the centralized control plane introduced by Software Defined Networking (SDN) be applied to control EON?

4. What survivability scheme can reduce the problems in EON and how to achieve it under the architecture of SDN?

5. What is the performance gain of our survivability scheme in comparison to existing schemes?

Our main contributions are as follows:

1. We propose an new survivability scheme for EON having super traffic.

2. We implement our scheme under the architecture of SDN.

3. We evaluate our scheme and compare it to two existing survivability schemes.

The outline of this thesis is as follows. In chapter 2, we give a general background about Elastic Optical Networks. Before proposing and achieving our methods, the related work about the current protection schemes in EON is presented in chapter 3. In the chapter 4, Software Defined Optical Networking as the control model for EON is introduced. Next, we propose our scheme in chapter 5. The detailed system and design are presented in chapter 6. We give a set of experiments to evaluate our protection scheme as described in chapter 7. The results and evaluation are also presented in this chapter. The conclusions and future work are described in chapter 8.

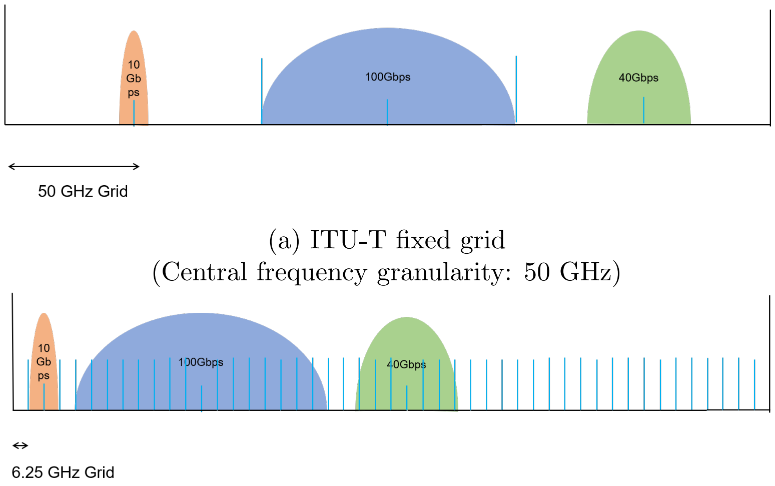
Chapter 2

Background

To improve the efficiency of optical transport networks, many different technologies have been proposed and some of them are already used in practice. One of the most important technologies is Wavelength Division Multiplexing (WDM). It multiplexes different connections into one fiber with different transmission wavelengths so that multiple traffic flows can be transmitted only over one strand of fiber. WDM systems have three patterns: normal WDM, Coarse Wavelength Division Multiplexing (CWDM) and Dense Wavelength Division Multiplexing (DWDM). Normal WDM only uses two wavelengths, 1310 nm, and 1550 nm, on one fiber. CWDM could have up to 16 channels from 1270 nm to 1610 nm and each channel has 20 nm space. DWDM has a denser grid with the wavelength band from 1530 nm to 1565 nm (the so-called C-band) [28].

For core optical networks, DWDM is more efficient than the other two. As specified by the International Telecommunication Union-Telecommunication (ITU-T), DWDM allows a fixed frequency grid with channel spaces at 12.5 GHz, 25 GHz, 50 GHz or even 100 GHz. Among them, 50GHz is most commonly used, shown in Figure 2.1a. However, the rigid bandwidth and coarse granularity make the spectrum allocation inefficient and inflexible.

In addition to the need to enhance the spectral efficiency, the dynamic and media-rich mobile environment also requires optical networks to be cost-effective and dynamically scalable. To meet the requirement of flexibility and efficiency in optical networks, the flexible spectrum grid as shown in Figure 2.1b has been proposed [16]. The main advantage of the flexible grid, when compared with the fixed grid, is that it has denser granularity and can be scaled dynamically. The channel central frequencies of signals with different bit rates can be flexibly selected with a minimum granularity of 6.25 GHz [23]. The size of the slot unit is twice the minimum granularity, 12.5 GHz. The slot width for signals with different bit rates only needs to be a multiple of 12.5 GHz. As Figure 2.1 shows, the flexible grid will need much less spectrum resources for signal transmission at 10 Gb/s, 40 Gb/s, and 100 Gb/s data rates.



(a) ITU-T fixed grid
(Central frequency granularity: 50 GHz)

(b) Flexible grid
(Slot width: 12.5 × m GHz, central frequency granularity: 6.25 GHz)

Figure 2.1: The fixed and flexible grid in optical transport networks. [23]

2.1 Elastic Optical Networks

The flexible grid is efficient for varying actual traffic demands in optical networks. In order to support the flexible grid, optical networks need to be equipped with flexible transceivers and special network elements. Adaptive transceivers, flexible grid, and intelligent network nodes make up a new "elastic" networking paradigm. In order to build an elastic network, Orthogonal Frequency-Division Multiplexing (OFDM), a multi-carrier modulation technology, is required. It splits the data stream into multiple parallel low-speed sub-carriers, so that the flexible spectrum is allowed to be switched from the input to the output ports. Based on the OFDM technology, Spectrum-Sliced Elastic Optical Path (SLICE) networks were proposed in 2009 [19], which are commonly called Elastic Optical Networks (EON). They support sub-wavelength, super-wavelength and varying data rates as shown in Figure 2.2.

- **Sub-wavelength**: Current wavelength-routed optical path networks need full bandwidth provisioning between the source and destination nodes, while EON allows the sub-wavelength transmission. The 100 Gb/s Ethernet technology is becoming standardized and popularized,

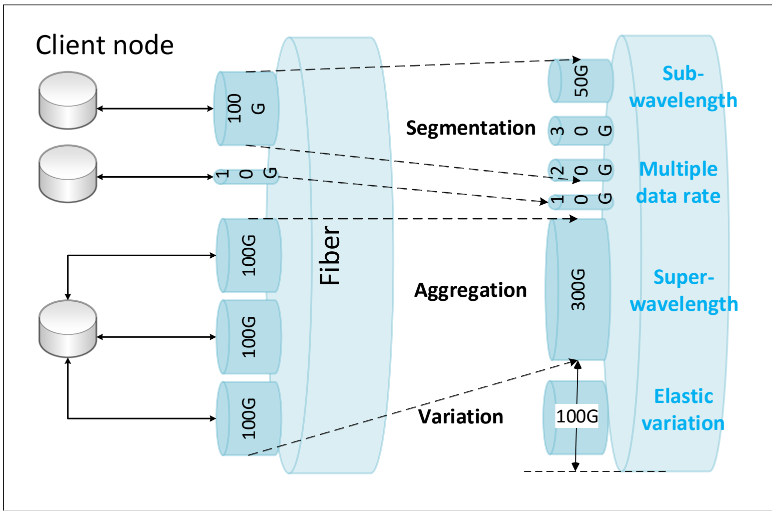


Figure 2.2: The characteristics of Elastic Optical Networks. [19]

but sometimes only a fraction of the bandwidth is required. EON allows flexible bandwidth allocation as shown in Figure 2.2. The network nodes along the optical path are also configured for the flexible bandwidth transmission. In this way, the resource usage is more efficient and the path provisioning is more cost-effective.

- **Super-wavelength**: Link aggregation, as a packet networking technology, combines multiple physical ports/links in a switch/router into a single logic port/link, which allows for traffic demands beyond the limits of a physical port/link. In EON, multiple continuous wavelengths can be combined into a super-wavelength as shown in Figure 2.2. Thus, the interval bands between the sub-wavelengths are saved.

- **Multiple data rates**: EON has a flexible grid so that appropriate spectrum can be assigned for different data rates. In other words, it allows varying data rates for different signal transmissions. Compared with fixed grid networks, it has higher resource utilization.

2.1.1 Network Model

In EON, the term "elastic" implies that the optical spectrum can be divided up flexibly for sub-wavelength and super-wavelength transmission, and the transponders can generate elastic optical paths (EOPs). EOPs are the paths with variable data rates. Thus, the network elements in EON are data-rate/bandwidth-variable Transponders (BVTs) at the network edge and data-rate/bandwidth-variable Wavelength Cross Connects (BV-WXCs) in the network core as shown in Figure 2.3. BVTs can generate elastic optical paths (EOPs). At the same time, every BV-WXC along the optical routing path will build a cross-connection with an appropriate spectrum bandwidth. In order to achieve the contiguous spectrum allocation, BV-WXC is made up of multiple bandwidth-variable Wavelength Selective Switches (BV-WSSs) as shown in Figure 2.4a. A BV-WSS performs wavelength demultiplexing/multiplexing and switches the wavelengths to different output fiber as shown in Figure 2.4b.

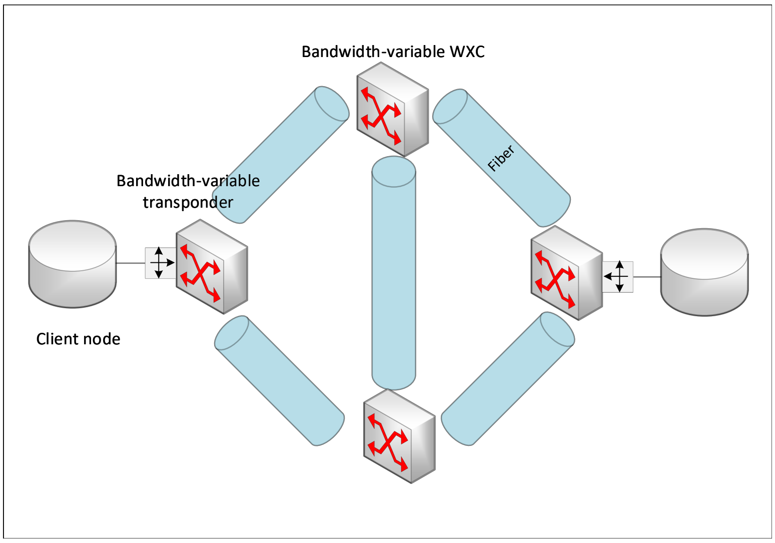


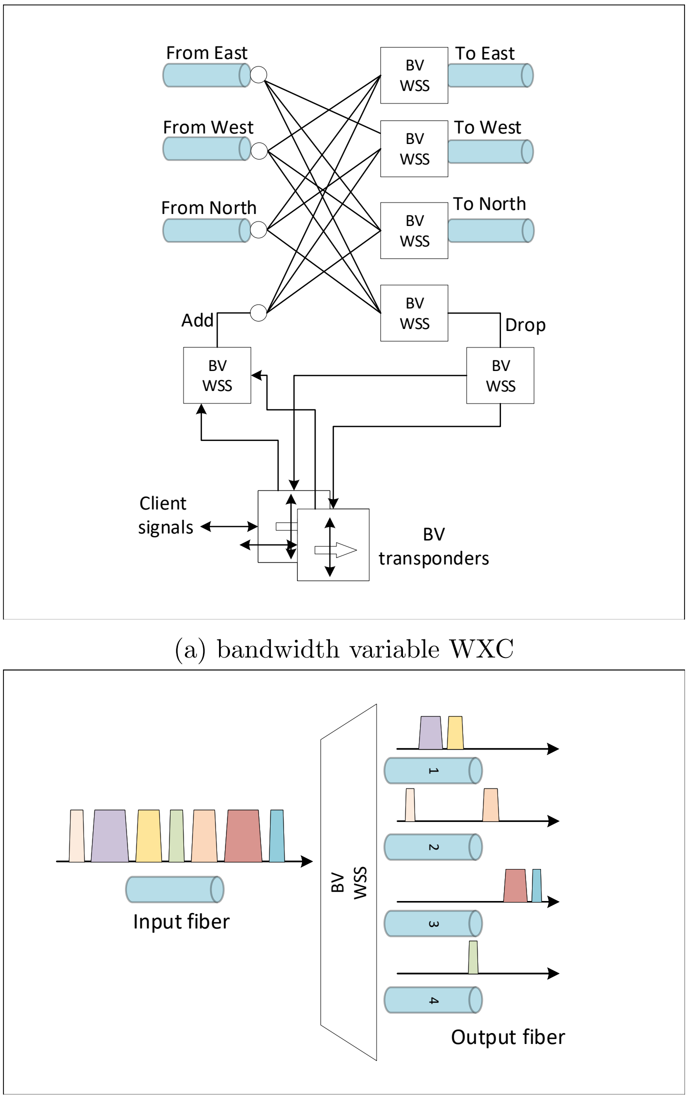
Figure 2.3: The model of Elastic Optical Networks. [19]

2.1.2 Routing and Spectrum Assignment

Conventional optical transport networks need Routing and Wavelength Assignment (RWA) algorithms to compute an end-to-end routing path and allocate appropriate wavelengths. For EON, this process is changed to Routing and Spectrum Assignment (RSA) algorithms which select a path between a source-destination pair and allocate spectrum to a traffic demand. In addition to satisfying the traffic demand, the RSA algorithms should minimize the amount of spectrum usage. Just like the constraints of RWA algorithms in WDM networks, there are also some constraints for the RSA algorithms in EON as listed below [4]:

1. **Spectrum continuity constraint**: the optical connection should allocate the same set of the spectrum along links in the end-to-end path.

2. **Spectrum contiguity constraint**: the allocated set of spectra for one connection should be adjacent.



(a) bandwidth variable WXC

(b) bandwidth variable WSS

Figure 2.4: The node model of Elastic Optical Networks. [19]

3. **Non-overlapping spectrum constraint**: the allocated spectrum of links for different connections should be non-overlapping.

4. **Transmission distance constraint**: the maximum transmission distance of the chosen modulation format should be longer than the length of the end-to-end path.

5. **Guard band constraint**: two adjacent connections should be separated by a guard band.

RSA problems can be divided into offline and online, corresponding to static and dynamic traffic respectively. In the case of static traffic, the connection requests are already known. So the purpose of the offline RSA is to set up paths to minimize the resource utilization for all the known requests. The offline RSA is proved to be NP-complete [9]. Many types of research work on solving the offline RSA problems and have proposed lots of Integer Linear Programming (ILP) formulations to optimize this kind of problems with different variants. But these processes need much computation time due to a large amount of data in a real situation. This conflicts with the real-time feature of networks. For dynamic traffic, the path is set up for each arriving connection request and the resources are released when the traffic finishes. Online RSA is more complex because of the unknown coming requests and dynamic spectrum distribution, but it is more meaningful for real networks [35]. We focus on dynamic networks and the online performance.

2.2 Survivability

Survivability is an essential requirement for optical networks. It is the ability of a network to reconfigure itself to restore the disrupted traffic caused by a failure. These failures can be divided into node failures, link failures and channel failures, which would be caused by broken switches, broken optical fiber, and broken transponders, respectively. A reliable optical network should have strong survivability.

In general, survivability schemes can be divided into two categories [15]: restoration and protection. Restoration is to recover the transmission after the failure happened, while protection is to protect the network connection in advance. Compared with protection, restoration needs some additional time to compute and configure a new routing path. In fact, the longer out of service, the more data will be lost. To guarantee the transmission quality, the time for traffic restoration including the time of fault detection is required to be below 50 ms [25]. When computing a new routing path, the various data rates in each channel and the aforementioned five constraints should be considered. It would be difficult to realize restoration within 50 ms. Thus, we focus only on protection in EON. More related work about the protection schemes is introduced in chapter 3.

2.3 Fragmentation Issues

With dynamic traffic, optical connections are continually established and released. Consequentially the optical links will accumulate more and more non-contiguous spectral bands, which is called fragmentation. In EON, the spectrum continuity constraint and the spectrum contiguity constraint are the main reasons for fragmentation. Fragmentation makes the free spectrum unusable for newly arrived connection requests, so it decreases the resource efficiency and leads to more blocking probability in optical networks. For EON with the protection scheme, a connection request needs a primary path as well as a backup path, so that more resources are occupied, which aggravates the fragmentation issues. Especially for large bandwidth transport, there will be a significant negative influence on fragmentation in EON when considering the normal protection scheme.

Towards the fragmentation issues, research is mainly about proactive and reactive fragmentation-aware RSA. Proactive fragmentation-aware RSA prevents or minimizes the spectrum fragmentation in advance, while the reactive fragmentation-aware RSA reconfigures the spectrum allocation of the connections in the dynamic network [37]. Currently, most research is about reactive fragmentation-aware RSA achieving defragmentation after fragmentation occurred. Traffic will be rerouted in the process of defragmentation, which can be time-consuming and result in extra delay to the traffic.

Chapter 3

Related work

There are a few existing literature related to survivability in EON. In this chapter, we give a brief summary of the related work. The scheme of survivability could be pre-computed (protection) or post-computed (restoration). Taken the real-time nature of the networks into consideration, there are few papers about restoration, because of the time-consuming feature. In this domain, most work is about the path computation methods.

There is more work on protection in EON. The conventional protection schemes are Dedicated Path Protection (DPP) and Shared Backup Path Protection (SBPP). DPP is the scheme to reserve one dedicated backup path. This backup path has the same amount of spectrum as the working path. These two paths are disjoint. In terms of SBPP, the backup path is shared by more than one working paths. Thus, the corresponding working paths sharing the backup path should be disjoint. There is also plenty of research on Squeezed Path Protection (SPP). This scheme reserves partial spectrum for the backup path. It means that the use of bandwidth is squeezed after a link failure. Similar to SBPP, the backup path is shared by link-disjoint working paths.

Researchers have proposed many novel ideas based on these three different protection schemes. Seydou Ba et al. [3] proposed to exchange the working and the dedicated backup paths in the dynamic networks for the sake of defragmentation. The simulation result shows that it will improve the traffic connections up to 10%. Jingjing Wu et al. [31] developed Shared Backup Path Grooming Protection (SBPGP). This method uses grooming to reduce the energy consumption in survivable optical networks. Grooming groups the lightpaths into one lightpath to be transmitted in one super channel. It can also save the resource usage for a guard band and have better performance in resource utilization compared with the SBPP. Micha Aibin et al. [2] proposed an adaptive algorithm for dynamic routing in survivable EON.

They classify the traffic into three classes through the required protection level. The traffic with the highest priority will use DPP, while traffic in the second level will be protected by SPP. The traffic with the lowest priority will use restoration rather than protection. In this way, it will reduce the usage of spectrum and then has lower block probability.

Xiaoliang Chen et al. [8] studied Availability-aware Differentiated Protection (ADP). Since different Service-Level Agreements (SLAs) require different service availability, they develop the ADP algorithm to make the protection scheme adapt to the service availability. Service availability is the probability that the lightpath is in-service. It equals the duration of the lightpath in in-service state divided by the total provision period. The experimental results show that this algorithm reduces the blocking probability with the guarantee of service availability requirements compared with DPP and SBPP.

Some work has studied the multiple lightpaths provisioning. It has the nature of partial protection. It will relieve the negative influence of the link failure. In terms of the advantage of multiple lightpaths provisioning, Shan Yin et al. [36] proposed the Shared Protection MPP (S-MPP) for multiple failures in EON. It combines the MPP and SBPP. Here MPP stands for the Multipath Provisioning. The number of paths and the shared resource is investigated for this method. The results verify that this scheme will increase the spectrum efficiency and protect the network against multiple failures. Hui Yang et al. [34] proposed the architecture of OpenFlow-based software defined elastic optical network. Based on this architecture, the multipath protection scheme is designed for the services with different importance levels. It enhances the network reliability but needs more resources because of more resource for the multiple protection paths.

The multiple lightpaths forwarding make the Multipath Protection (MPP) possible. Dharmendra Singh Yadav et al. [32] presented a strategy for survivability in EON, which is called Backup Spectrum Reservation with MultiPath Protection (BSR-MPP). In this strategy, the spectrum is separated for working and backup paths. Multiple backup paths are searched and reserved over the advance reserved backup resources when a new optical connection is required. Then, it has high resource sharing so that increases the resource efficiency and reduces the blocking probability.

Fragmentation is an important problem in EON, which reduces the resource efficiency and increases the block probabilities. Working paths defragmentation will have a negative influence on the other working paths. But, it is easy to achieve defragmentation in the backup paths without the effects on working paths. Based on this consideration, Chao Wang et al. [27][26] proposed spectrum defragmentation schemes for EON with DPP and SBPP.

There are some schemes which combine the protection and restoration for network survivability. It can be used for multiple failures. Alberto Castro et al. [7] proposed Multipath Recovery (MPR) for EON. In this scheme, the working path serves the full transmission. When the failure happens, the pre-reserved backup path serves the partial bandwidth transmission and the restoration path is established for the remaining bandwidth transmission. This scheme considers the pros and cons of protection and restoration and trades off the efficient resource utilization in restoration and fast recovery in protection.

To the best of our knowledge, there is no prior work on the survivability of super traffic. In fact, the super-wavelength transmission is the trend in optical networks.

Chapter 4

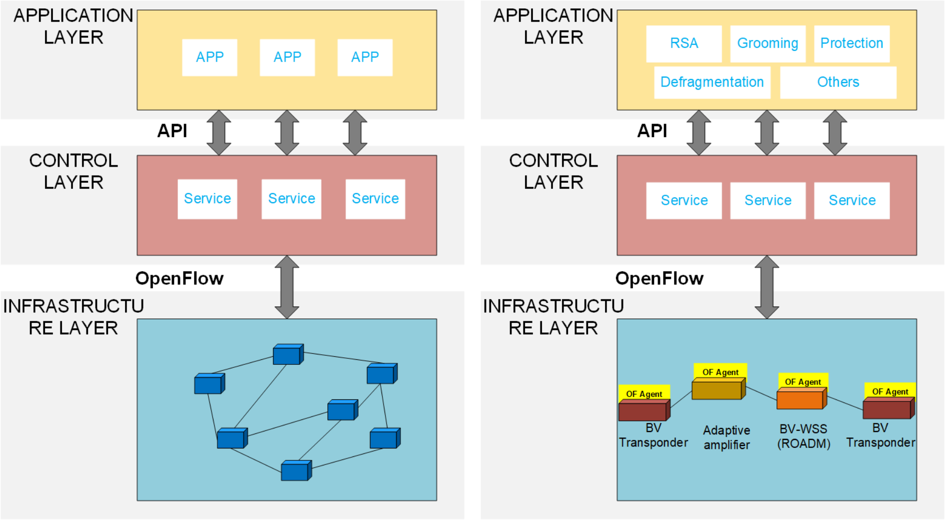
Software Defined Optical Networking

In EON, the control plane is the key technology to support dynamic, flexible and intelligent end-to-end path provisioning, failure detection and recovery. There are two control planes mainly studied for the EON. One control plane is based on Generalized Multi-Protocol Label Switching/Path Computation Element (GMPLS/PCE) in which the RSA is calculated by the Path Computation Element (PCE). This is a mature technology in optical networks. However, a GMPLS/PCE-based control plane is still not the ideal solution for EON because of its complexity and the distributed control, especially in the multilayer situations. Another choice for the control plane is OpenFlow-based SDN. It enables centralized control for networks through programming. This architecture could be used in optical networks to achieve flexibility and intelligence. Through the experiments in [21], it was shown that the GMPLS/PCE-based control plane is sensitive to the increasing number of hops in the paths. For paths with more than 3 hops, the SDN control plane will have less path provisioning latency than that of the GMPLS/PCE-based control plane due to the centralized control in SDN. The elastic optical network controlled by an SDN controller is usually called Software Defined Elastic Optical Networks (SDEON). Taken the better control into consideration, we choose SDN as the control plane for our implementation.

4.1 Network Architecture

There is already much research on SDN. The application layer, control layer, and infrastructure layer compose the general architecture of SDN as shown in Figure 4.1a. The OpenFlow protocol has become one of the widely used southbound protocols for communication between the infrastructure layer and the control layer. The northbound communication between control layer and application layer is achieved through various application programming interfaces (APIs) also called northbound interfaces (NBIs), the most common one being the REST API. The applications in the application layer direct specify functions through the controller. The typical applications include the network monitor, load balance, recovery, etc. The control layer, as the brain of the SDN, is the most important part used to control arriving flows and associate the applications. As to the infrastructure layer, it comprises a set of network elements, each of which is able to process and forward the traffic [13].

In terms of SDEON, the architecture, shown in Figure 4.1b, has the same three layers as that of SDN. But, there are also some differences in each of the layers. First of all, the network elements in the data plane of SDEON are different. The network elements in EON are data-rate/bandwidth-variable (BV) transponders and bandwidth-variable (BV) WXCs, contrary to the normal switches in an IP network. Another difference between SDEON and SDN is that the resources in SDEON control plane are spectrum slots. Moreover, when computing the routing path, modulation formats, and spectrum, the control plane needs to consider the constraints mentioned in chapter 1.

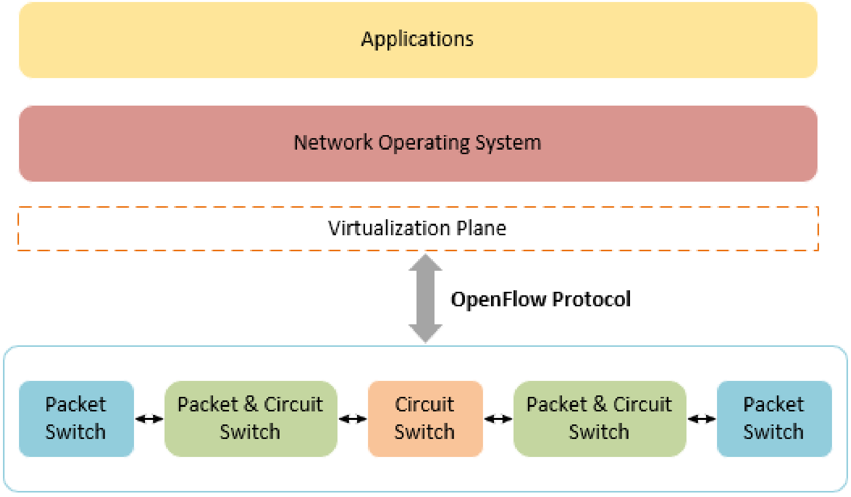


(a) The Architecture of SDN

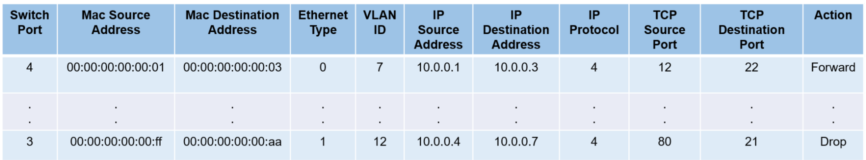
(b) The Architecture of SDEON

Figure 4.1: The architecture comparison of SDN and SDEON.

The architecture of Multi-layer SDN is presented in Figure 4.2a. In the infrastructure layer, there are three different switches: packet switch, circuit switch and packet&circuit switch. Since the packet flow in the packet layer and circuit flow in the optical layer (Figure 4.2b and Figure 4.2c) have different information, the packet&circuit switch is designed to transform the packet flows and circuit flows. Towards the control of these three types of switches, the OpenFlow protocol should be modified in the controller and in the optical network elements as well. On the controller side, the OpenFlow protocol need to be extended to control the circuit flows, while the optical network elements need the OpenFlow agents to make the communication between the controller and various switches possible.

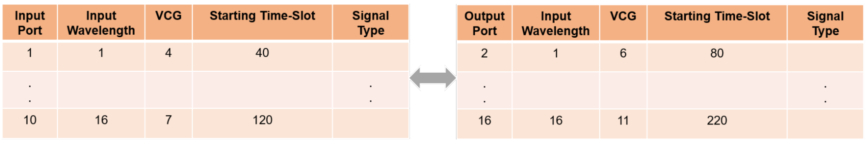


(a) The Architecture of Multi-layer SDN



Switch Port	Mac Source Address	Mac Destination Address	Ethernet Type	VLAN ID	IP Source Address	IP Destination Address	IP Protocol	TCP Source Port	TCP Destination Port	Action
4	00:00:00:00:00:01	00:00:00:00:00:03	0	7	10.0.0.1	10.0.0.3	4	12	22	Forward
. .	. .	. .	. .	. .	. .	. .	. .	. .	. .	. .
3	00:00:00:00:00:ff	00:00:00:00:00:aa	1	12	10.0.0.4	10.0.0.7	4	80	21	Drop

(b) The packet flows



Input Port	Input Wavelength	VCG	Starting Time-Slot	Signal Type
1	1	4	40	
. .				. .
10	16	7	120	

Output Port	Input Wavelength	VCG	Starting Time-Slot	Signal Type
2	1	6	80	
. .				. .
16	16	11	220	

(c) The circuit flows

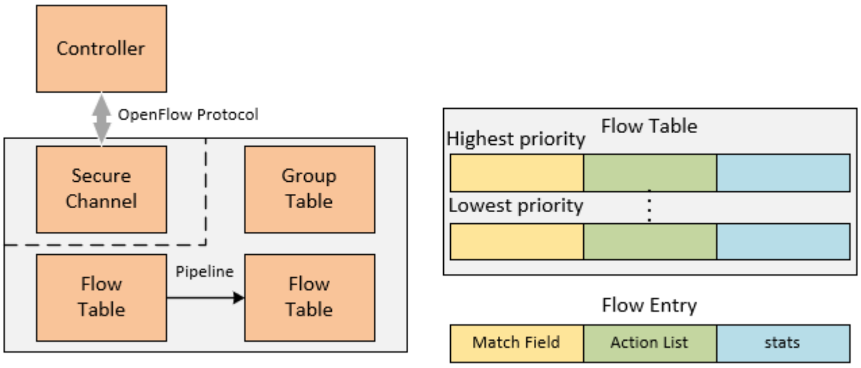
Figure 4.2: The converge control of packet and circuit in SDN. [11]

4.2 Optical Extension of OpenFlow Protocol

To control the optical characteristics, there is an optical extension of the standard OpenFlow protocol. Let us start by first explaining the standard OpenFlow protocol.

4.2.1 Basic OpenFlow Protocol

The remote controller manages the OpenFlow switches through the OpenFlow protocol. The main components of these switches are one or more flow tables, one group table, and an OpenFlow channel to communicate with the external controller as depicted in Figure 4.3a. The flow tables are sorted in a descending order by priority as shown in Figure 4.3b. They work like a pipeline to process the arriving flows. The essential idea of the OpenFlow protocol is to look up the arriving flows via match and operate the matched flows via actions such as forwarding and drop.



(a) The OpenFlow Switch

(b) The Flow Table

Figure 4.3: The architecture of OpenFlow 1.3. [12]

Each flow table contains flow entries that include the following fields

- **match fields**: the match fields consist of ingress ports, packet header fields, and metadata from a previous flow table.
- **priority**: precedence of matching flow entries.
- **instruction set**: a set of actions performed on the matching packets such as forwarding packet to port, dropping packet, etc. Or the instruction about pipeline processing.
- **counters**: statistics for matching packets.
- **timeouts**: the maximum amount of time or idle time before flow entry is expired in the switch.

- **cookie**: opaque data value assigned by the controller. It is only used by the controller to identify the flows.

If a packet arrives at a switch, the switch will match the flow entries from high priority to low priority in the first table. When matched, the instruction set in the matched flow entry is performed on this packet. If there is Goto Instruction to direct the packet to another flow table, the same process will repeat in that new flow table [12]. The whole process of the packet flow in an OpenFlow switch is presented in Figure 4.4.

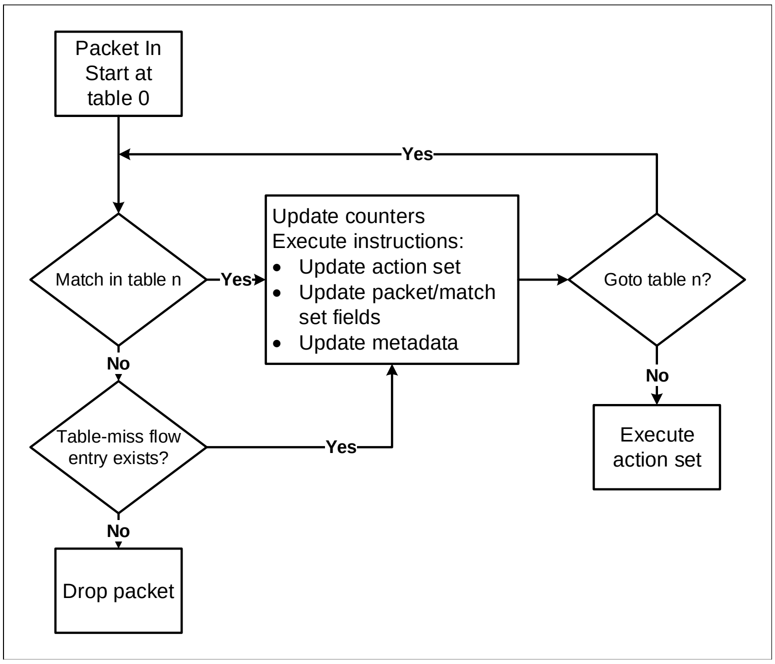


Figure 4.4: The Flowchart of packet flow in an OpenFlow switch. [12]

4.2.2 OpenFlow Extension

The current OpenFlow protocol only supports packet-based networks (L2-L4). In order to support circuit-based networks (L0-L1), the OpenFlow protocol is extended on the Match/Action mechanism. Match fields could be a port, a center frequency, a wavelength slot width, number of slots, while the Action set will be assigning the slots and cross-connect. The OpenFlow extension is different for two situations. At first, the OpenFlow extension protocol should support transmitting the optical signal between two circuit switches. Then taken the multi-layer architecture into consideration, the OpenFlow extension needs to support the transformation between the optical signal and packet [33].

4.3 OpenFlow Agent

So far, the optical elements are controlled through the Transaction Language 1 (TL1) and Command Line Interface (CLI). To make them operated by the OpenFlow extension protocol, an OpenFlow agent is attached to each optical switch. This optical agent works between the controller and the optical element to translate the instructions from the controller into TL1 commands or to translate the requests from the optical switch into OpenFlow messages. The detailed compositions of OpenFlow optical agent are shown in Figure 4.5. The OpenFlow channel module is to communicate with the controller. Besides the translator and OpenFlow channel, the port-emulation module is needed to emulate the optical ports and to send the states of these optical ports to the controller [17].

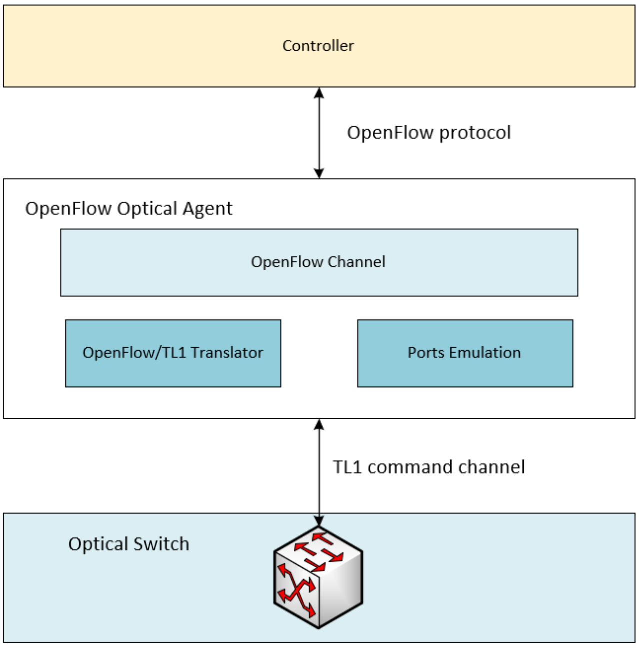


Figure 4.5: The OpenFlow Agent for optical switch. [17]

Chapter 5

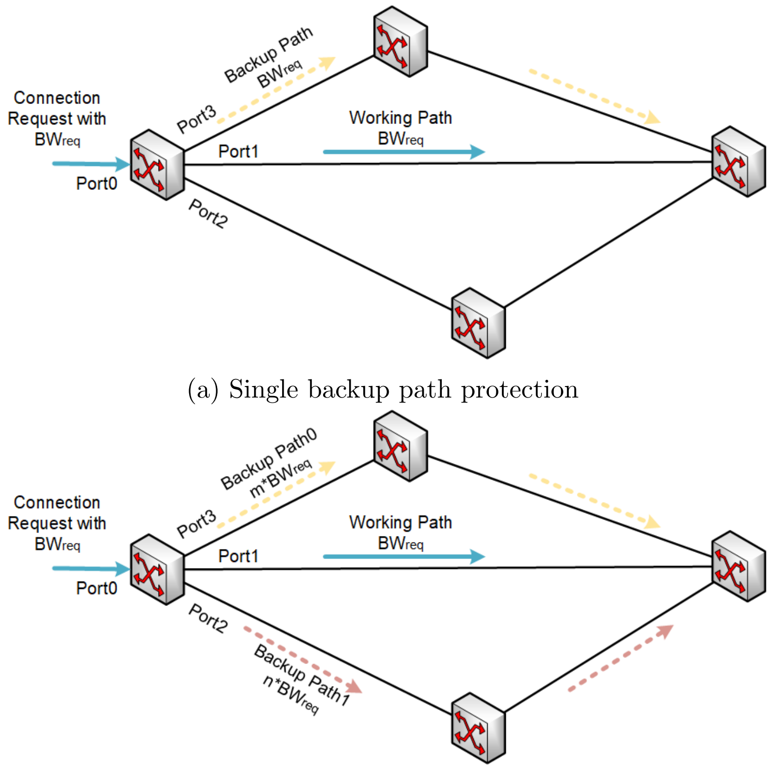
Survivability scheme

In this section, we propose a new survivability scheme for Elastic Optical Networks with super traffic. In this new survivability scheme, we use multi-path backup protection for super traffic, and the shared backup path protection scheme for all the other traffic. We call this new survivability scheme Hybrid Single and Multiple Backup Protection (HSMBP).

5.1 Hybrid Single and Multiple Backup Protection

Shared backup path protection is a popular protection method in optical networks. To achieve this protection, the same amount of bandwidth is reserved for both the backup path as well as the primary path. The reserved backup resources can be shared between different traffic with disjoint primary paths. In case of super traffic, the same large amount of bandwidth reserved in the backup path can significantly aggravate the fragmentation problem and increase the blocking probability in EON. To relieve the negative influence of super traffic, we divide this large bandwidth into multiple small bandwidths and reserve these small bandwidths for multiple backup paths.

In HSMBP, a threshold is introduced as a parameter to classify the traffic into two types (super traffic and normal traffic) based on the amount of bandwidth it requires. Different protection schemes are chosen for these different types of traffic as depicted in Figure 5.1. For example, in the single backup path case shown in Figure 5.1a, we assume that the required bandwidth BW_{req}, is reserved both in the working path as well as the backup path. In the multiple backup paths protection, BW is the threshold used to classify the traffic. If $BW_{req} < BW$, this traffic is regarded as small traffic and the reserved bandwidth is BW_{req} for both working and backup path. Otherwise, the traffic is considered to be large and BW_{req} spectrum is reserved in the working path, while $m \times BW_{req}$ and $n \times BW_{req}$ are reserved in the two backup paths, as shown in Figure 5.1b. The number of backup paths is not limited to two but the sum of the scaling sectors (e.g. m, n) needs to be 1. We call this hybrid protection scheme HSMBP.



(a) Single backup path protection

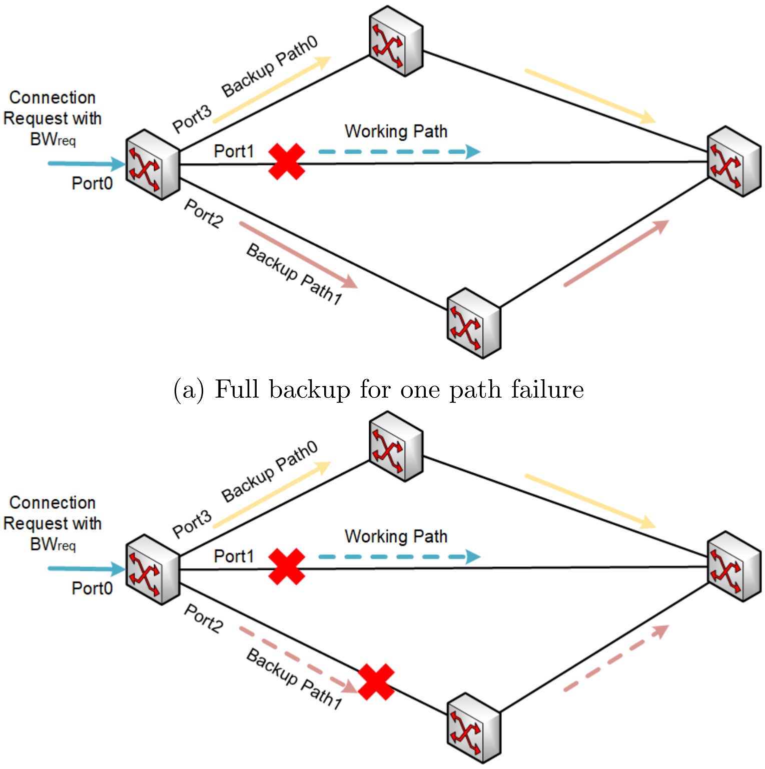
(b) Multiple backup paths protection

Figure 5.1: The single and multiple-path backup protection.

In HSMBP, there are some important parameters that need to be configured. The first one is the threshold used to classify different types of traffic. This threshold can be static and dynamic. The second parameter is the number of backup paths used, which will sequentially influence the way we divide the required bandwidth for the backup paths. These parameters can adjust HSMBP to influence the network performance. All of these parameters will be evaluated in the experimental work.

5.1.1 Multiple Failure Protection

Besides relieving the negative influence of large-bandwidth traffic, the multipath backup protection scheme is able to partially recover the optical traffic when multiple failures happen. As shown in Figure 5.2a, when a failure occurs, the optical signal is rerouted through the backup paths. It is full backup protection. However, if one of the backup paths also fails, the remaining backup paths can still be used to transmit partial optical flows. In this case, we give partial backup protection as in Figure 5.2b.



(a) Full backup for one path failure

(b) Partial backup for two path failure

Figure 5.2: The protection process of HSMBP.

Chapter 6

System and design

We implement our proposed scheme under the SDN architecture in this section. First of all, we use OpenFlow protocol to achieve single-path failover and multi-path failover in the infrastructure layer. Then, the path and spectrum provisioning is achieved for EON in the application layer. In order to support the path and spectrum provisioning, network topology and resources of the infrastructure layer are monitored by the controller through applications of resource and topology management.

6.1 HSMBP in SDN

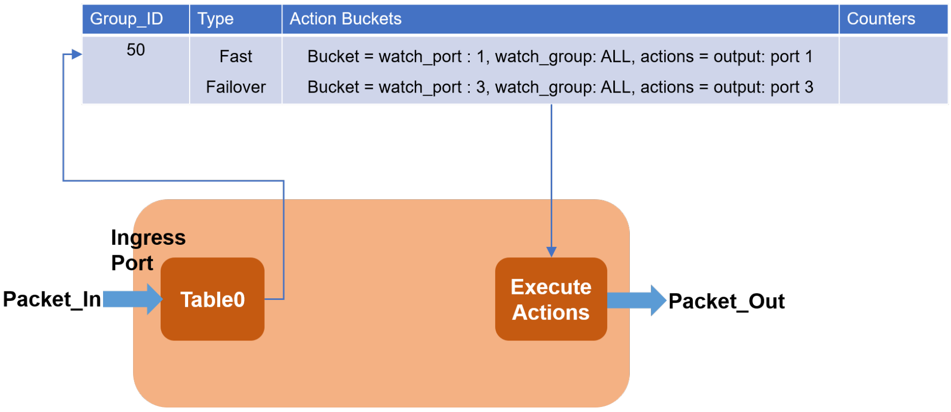
Under the architecture of SDN, the switches in the infrastructure layer will achieve the forwarding and recovery process. The controller controls the behaviour of switches through the OpenFlow protocol. These switches use flow entries to match and execute the actions for the optical traffic. Since OpenFlow version 1.3, Group tables are supported. They contain group entries and in each group entry, there is a list of buckets with a corresponding set of actions. This table, in contrast to the standard flow table, supports flooding and more complex forwarding scenarios such as multipath and fast reroute. There are four types of group tables [12].

- ALL: Execute all the action buckets in the group. It is mostly used for flooding and multicasting.
- Indirect: Execute the one defined bucket in the group. This type of group table only supports a single bucket.
- Select: Execute any one action bucket in the group. The action bucket is chosen by a switch-defined algorithm, such as round robin or load sharing.

- Fast failover: Execute the first live action bucket in the group. The liveness of action buckets will be evaluated in an order.

6.1.1 Single-path Failover

Fast failover group can be used to reroute optical signals to the preconfigured backup path in case a failure occurs in the working path. It is designed to achieve traffic recovery. We implement the single path protection through Fast failover group table. The work flow is shown in Figure 6.1. When no failure in the optical network, the first live port (port 1) is used to transmit the traffic flow. If a failure occurred in the primary path, the current first live port (port 3) is used to recover this traffic flow.



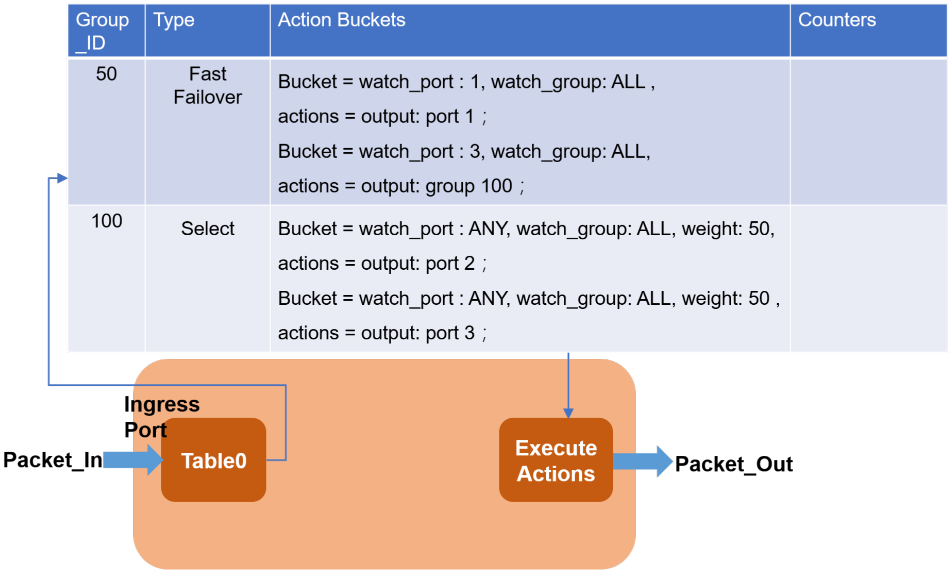
Group_ID	Type	Action Buckets	Counters

50	Fast Failover	Bucket = watch_port : 1, watch_group: ALL, actions = output: port 1
		Bucket = watch_port : 3, watch_group: ALL, actions = output: port 3	

Figure 6.1: The single path backup through the fast failover group table.

6.1.2 Multi-path Failover

The OpenFlow protocol does not support multi-path failover originally. We achieve it by combining Select and Fast failover group tables for multi-path failover as shown in Figure 6.2. After the failure, the fast failover group table will find a live action bucket, that points to the modified select group table and the optical signal will be divided and rerouted to the multiple ports through the action bucket in the select group table. The weights for the action buckets decide the amount of bandwidth used for each of the multiple paths.



Group _ID	Type	Action Buckets	Counters

50	Fast Failover	Bucket = watch_port : 1, watch_group: ALL ,
		actions = output: port 1 ;
		Bucket = watch_port : 3, watch_group: ALL,
		actions = output: group 100 ;	

100	Select	Bucket = watch_port : ANY, watch_group: ALL, weight: 50,
		actions = output: port 2 ;
		Bucket = watch_port : ANY, watch_group: ALL, weight: 50 ,
		actions = output: port 3 ;	

Figure 6.2: The multipath backup protection through group table chain.

6.2 Path and Spectrum Provisioning in SDN

The architecture of the implementation of our scheme is shown in Figure 6.3. In the control layer, there are three modules: the topology awareness module, the path and spectrum computing module, and resource management module. The topology awareness module will discover the topology of the infrastructure layer. It provides the topology information for the path and spectrum computing module to get the available paths. The resource management module will manage the spectrum resource in each optical link. It will give spectrum information to the path and spectrum computing module to find the available spectrum for the found paths.

6.3 Path and Spectrum Computing Module

The topology awareness module and the resource management module provide the topology and resource information respectively. Based on this information, the path and spectrum computing module will compute the working and backup paths and allocate the available spectrum to these paths. The core of this module is the Routing and Spectrum Assignment(RSA) algorithm. Online RSA is an NP-complete problem [9]. The traditional approaches, such as integer linear programming, are unsuitable for such problems because of their high computational complexity and high computation time. Therefore, a heuristic algorithm is considered. To simplify the problem, the RSA algorithm for dynamic networks is divided into two

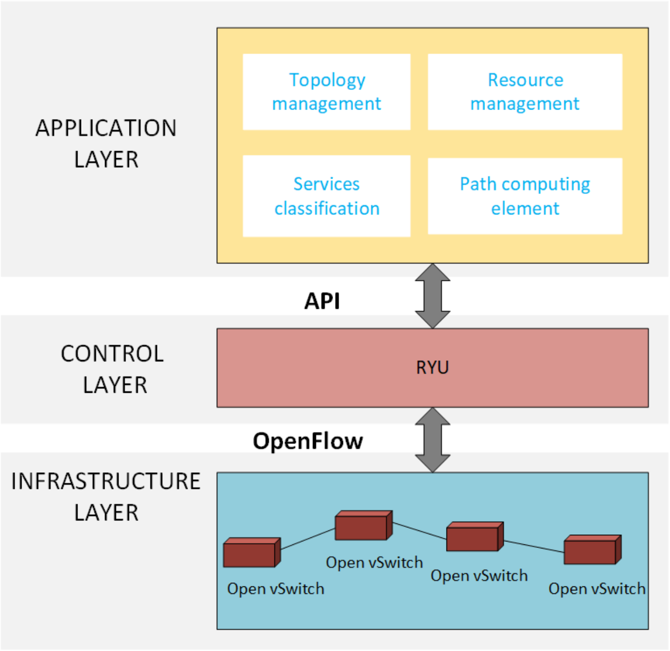


Figure 6.3: The Architecture of HSMBP in SDN.

sub-problems: the routing sub-problem and the spectrum allocation sub-problem, each of which is solved separately. The first one is routing, and the second one is spectrum allocation. The routing is to find the disjoint paths from the source to the destination and sorted these disjoint paths based on the path selection policy. In terms of spectrum allocation, the available spectrum is found and allocated along the sorted disjoint paths based on the spectrum allocation policy.

6.3.1 Disjoint Path Computing

The primary path is protected by the backup path. To achieve path protection, the backup path should have no common links or nodes (except the source and destination) with the primary path. During the routing process, the feasible disjoint paths between the source-destination pair are searched. The paths could be link-disjoint and node-disjoint. But, two link-disjoint paths can still pass through the same nodes and cannot protect the primary path from node failures. However, if the paths are node-disjoint it means that they are link-disjoint as well, and can thus protect from all failures. This is the reason why we choose the node-disjoint paths algorithm [18]. Thus, the Suurballe's algorithm will be used to get the set of candidate paths [24]. The pseudocode of the Suurballe's algorithm is presented in Algorithm 1.

Algorithm 1: Algorithm 1: Suurballe's algorithm for finding the node-disjoint paths

```
Input  : The source node and destination node $s$ and $d$;
         the graph G(V, E)
Output: $disjointPaths$
1 Each node $n$ of graph G(V, E) is split into two nodes $n_{in}$ and $n_{out}$
    and these two nodes are connected by a link with weight zero.
2 Get the shortest-path tree rooted $tree_s$ at the node $s$ through the
    Dijkstras algorithm return $disjointPaths$;
3 Transform the original graph $G$ to an auxiliary graph $G^{'}$. In graph
    $G^{'}$, the nodes and links are same as graph $G$. The weight of each
    link $u, v$ is defined by $w^{'}(u,v) = w(u,v) - d(s,v) + d(s,u)$. $d(s,v)$
    and $d(s,u)$ denote the shortest distance from node $s$ to node $v$ and
    node $u$ in graph $G$;
4 In graph $G^{'}$, remove the links along the shortest path $P$ from node $d$
    and node $s$, then reverse the directions of the links along the
    shortest path $P$ from node $s$ and node $d$;
5 Compute the shortest path $P^{'}$ from node $s$ and node $d$ in graph $G^{'}$;
6 Remove the reversed links in $P$ and $P^{'}$. The remaining links form a
    cycle with node $s$ and node $d$ inside. Two node-disjoint paths
    $disjointPaths$ between node $s$ and node $d$ are found from this cycle;
```

Two node-disjoint paths are found through the Algorithm 1. This algorithm requires two execution of Dijkstra's algorithm to find the shortest path. Every execution can be performed in time $O(|E| + |V|\,log\,|V|)$, where $|E|$ and $|V|$ are the number of edges and vertices respectively. If k disjoint paths are needed, the steps from 2 to 4 will be iterated for $(k-1)$ times. Thus, the time complexity of Suurballe's algorithm to find k node-disjoint paths is $O(k(|E| + |V|\,log\,|V|))$.

6.3.2 Path Selection Policy

The candidate paths are already calculated through the disjoint path computing algorithm. These paths are sorted and selected based on the path selection policy. Then these paths are used in the spectrum allocation part. The list of some usual path selection policies is listed below:

- Shortest Path First (SPF): sort the paths in an ascending order based on the lengths.

  $$metric_{SPF}(Path) = length(Path) \tag{6.1}$$

  where the $length(\cdot)$ returns the number of hops of the $Path$.

- Most Slots First (MSF): sort the paths in a descending order based on the sum of free spectrum along the links of a path.

$$metric_{MSF}(Path) = \sum_{e} freeSlots_{e}, e \in Path \tag{6.2}$$

- re-ordering (reMSF): sort the paths in an increasing order based on $metric_{MSF}(Path)$ divided by the highest modulation format in terms of bit per symbol M.

$$metric_{reMSF}(Path) = \frac{metric_{MSF}(Path)}{M(Path)} \tag{6.3}$$

  where $M(\cdot)$ returns the modulation level for the $Path$.

- Largest Slots-over-Hops First (LSoHF): sort the paths in a descending order based on the ratio of free spectrum along the links of a path to the hops of that path.

$$metric_{LSoHF}(Path) = \frac{\sum_{e} freeSlots_{e}}{length(Path)}, e \in Path \tag{6.4}$$

The SPF policy is the simplest one, but will lead to more blocked connection requests. Then the second policy (MSF) considers load balancing, which will result in less blocked connection requests at the price of increased resource consumption. The following policy (reMSF) re-orders the path sorted by the MSF policy. It guarantees lower spectrum utilization than the MSF policy because of allocating shorter paths. The LSoHF policy does not only consider the hops of paths, but also the available spectrum. Thus, it will balance the blocking probability and the resource consumption. We think the hops of paths and available spectrum are two most important factors for path candidates. Thus, we choose the LSoHF policy to sort the disjoint paths.

6.3.3 Spectrum Allocation Policy

After obtaining the paths, the optical resources are allocated along the links of the end-to-end path. The spectrum allocation methods select the set of spectrum also based on different policies:

- First-fit (FF): allocate the first found available spectrum along the routing path.

- Exact-fit (EF): first search for an N-sized available spectrum between the existing two connections, otherwise use the first-fit policy.

- Random-fit (RF): allocate any one available block that is large enough to the required bandwidth.

- Best-fit (BF): find the available spectrum between the existing two connections with equal or bigger size than the required N. The smallest one is allocated.

The First-fit (FF) policy is the simplest and fastest one but it does not consider defragmentation along the path. The second policy (EF) finds the exact location first, which will reduce the fragmentation to an extent. In fact, most of the time it could not find the exact-fit location and achieve defragmentation so that it will need more time to allocate the spectrum than the FF policy. Random-fit (RF) is usually considered for benchmark purposes. The final policy has the highest complexity. All the available spectrum needs to be compared to find the smallest one [22]. Different spectrum allocation policies can influence the network performance, but we only want to find the performance of HSMBP. That means we do not need a spectrum allocation policy that can alleviate fragmentation. Thus, we choose the First-fit (FF) policy to allocate spectrum.

6.3.4 Online RSA with HSMBP

We give an algorithm with HSMBP for dynamic traffic. The graph is defined as $G(V, E, B, D)$, where the V, E, B, D are the set of vertices, edges, spectrum slots and distance respectively.

The modulation level M is chosen for a path through Equation 6.5:

$$M = maxLevel(\sum_{e} d_e), e \in Path_{(s,d)} \tag{6.5}$$

where $maxLevel\,(\cdot)$ returns the highest modulation level that supports the transmission distance d_e of link e. $Path_{(s,d)}$ are the routing paths from source s to destination d.

The number N of frequency slots for the required bandwidth (BW_{req}) can be calculated through Equation 6.6:

$$N = \lceil \frac{BW_{req}}{M \times 12.5GHz} \rceil + 1 \tag{6.6}$$

where M is modulation level, 12.5 is the size of each slot and 1 is for the guard band.

The pseudocode for online RSA with HSMBP is shown in Algorithm 2. k disjoint paths are computed through the Algorithm 1 in advance. k is different for different topologies. With resource usage changing dynamically, the metrics of disjoint paths for connection requests are computed and these disjoint paths are sorted through the path selection policy in step 2. In the network graph, Algorithm 3 is used to find and assign the spectrum for the working path through the spectrum allocation policy in step 3. In Algorithm 3, the spectrum is found from the sorted paths. After the spectrum allocation for the working path, an auxiliary graph is created through Algorithm 4 to help the spectrum allocation for backup paths with shared backup resources.

In Algorithm 4, the other working paths, which overlap with the working path found in step 3, are found. The corresponding backup spectrum for these working paths is set to be unavailable. That means the backup spectrum for working paths non-overlapping with the working path found in step 3 is available. Thus, the two joint working paths would not have shared backup spectrum.

In step 5, the bandwidth required by the connection request BW_{req} is compared with the giving threshold. If BW_{req} is equal or greater than $Threshold$, the BW_{req} is divided into multiple sub-bandwidths. Then these sub-bandwidths are found and assigned along the backup paths in the auxiliary graph through Algorithm 3. In this way, multiple path backup protection is achieved for the working path. If BW_{req} is smaller than $Threshold$, the spectrum for BW_{req} is found and assigned to one backup path through Algorithm 3.

Algorithm 2: Algorithm 2: RMSA algorithm with HSMBP

```
Input  : the network graph G(V, E, B, D)
         the connection request $CR(s, d, BW_{req})$
         $Threshold$, $k$
Output: $Paths$ and $CFs$
compute $k$ node-disjoint paths $P(s, d)$ through Algorithm 1;
sort the $P(s, d)$ based on the metrics calculated through the Largest
  Slots-over-Hops First (LSoHF) path selection policy as Equation 6.4;
assign the spectrum for the working path through Algorithm 3 in
  $G(V, E, B, D)$
get the auxiliary graph $G^{'}(V, E, B, D)$ through Algorithm 4
if $BW_{req} \geq Threshold$ then
    divide the $BW_{req}$ into sub-bandwidths put the sub-bandwidths
      into $BWs$
else
    put the $BW_{req}$ into $BWs$
end
for $BW$ in $BWs$ do
    assign $BW$ spectrum for backup through Algorithm 3 in
      $G^{'}(V, E, B, D)$;
end
```

Algorithm 3: Algorithm 3: Spectrum Assigning Algorithm

```
Input  : the sorted paths $SortedPath$;
         the required bandwidth $BW_{req}$
Output: $Paths$ and $CFs$
for $Path$ in $SortedPath$ do
    determine the modulation level $M$ for the $Path$ through Equation
      6.5;
    calculate the number of slots $N$ for $BW_{req}$ through Equation 6.6;
    Find the $N$ contiguous free slots through the First-fit (FF)
      spectrum allocation policy ;
    if No $N$ contiguous free slots then
        break inner for-loops;
    else
        get $CF$ for the $path$ break inner and outer for-loops;
    end
    remove $Path$ from $SortedPath$
end
```

Algorithm 4: Algorithm 4: Getting the auxiliary graph

```
Input  : the working path $WorkingPath$;
         the original graph $G(V, E, B, D)$
Output: the auxiliary graph $G^{'}(V, E, B, D)$
create a set $Flows$
for $Link\ in\ WorkingPath$ do
    find current $flows$ in the $Link$
    add $flows$ to $Flows$
end
for $flow\ in\ Flows$ do
    find the spectrum slots $BackupSlots$ in the backup path for $flow$
    modify $BackupSlots$ to be non-available in $G(V, E, B, D)$
end
```

Chapter 7

Evaluation

In order to evaluate the performance of the schemed proposed in previous chapters, HSMBP, multiple experiments were performed. Firstly, we evaluate our scheme in different scenarios. After that, we implement two benchmark protection schemes: Dedicated Path Protection (DPP) and Shared Backup Path Protection (SBPP). DPP, the most used path-protection scheme, use one dedicated backup path with the same bandwidth as the primary path reserved to protect the primary path. A majority of research on path-protection scheme is developed based on SBPP. In SBPP, the difference from DPP is that backup resources are shared among different, disjoint primary paths. To evaluate HSMBP, we compare it with DPP and SBPP.

7.1 Evaluation Metrics

We use the metrics, including Bandwidth blocking probability (BBP), Spectrum utilization ratio (SUR), and Bandwidth fragmentation ratio (BFR), to evaluate the network performance.

- Bandwidth blocking probability (BBP): the ratio of the sum of blocked-request bandwidth $BW_{blockedReq}$ to the total amount of the requested bandwidth BW_{req}.

$$BBP = \frac{\sum BW_{blockedReq}}{\sum BW_{req}} \tag{7.1}$$

- Spectrum utilization ratio (SUR): the ratio of the sum of occupied spectrum *occupiedSpec* in each link to the total amount of spectrum resources *Spec* in the network.

$$SUR = \frac{\sum_e occupiedSpec_e}{\sum_e Spec_e}, e \in E \tag{7.2}$$

where E is the set of links in the topology.

- Bandwidth fragmentation ratio (BFR): Fragmentation refers to non-aligned, isolated and small-sized slots. It can be quantified through many ways [29]. Here, we choose the most common one. The bandwidth fragmentation ratio of link e is got through Equation 7.3.

  $$F(e) = 1 - \frac{max\left(freeBlock_e\right)}{totalFree_e}, e \in E \tag{7.3}$$

  where $max\left(\cdot\right)$ returns the number of largest contiguous free slots. $totalFree$ represents the total number of free slots. If all free slots are contiguous, F is equal to 0. If F is close to 1 then the free space is divided into lots of small blocks of 1 slot.

  Based on the definition of fragmentation, the fragmentation ratio can be calculated as Equation 7.4.

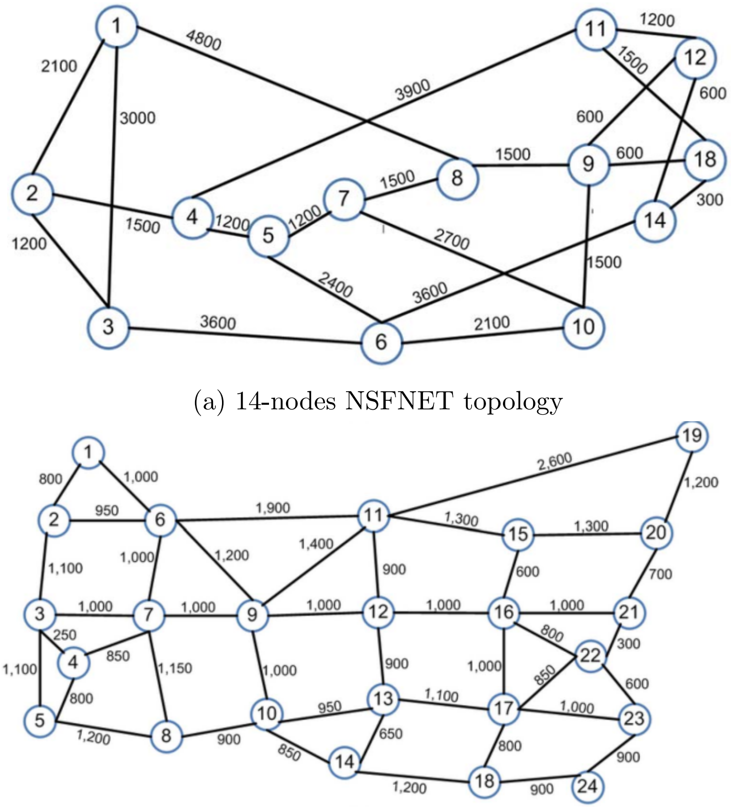
  $$BFR = \frac{\sum_e F(e)}{num(E)}, e \in E \tag{7.4}$$

  where the $num\left(\cdot\right)$ returns the number of links.

We present simulation results in different scenarios for different network topologies. The results are compared on BBP, Spectrum Utilization Ratio (SUR), and Bandwidth Fragmentation Ratio (BFR). These three metrics are related to each other. We desire lower BBP. BBP is the most important metric to evaluate the network performance. To have lower BBP, we expect lower SUR and lower BFR.

7.2 Experiments in NSF-14 and USB-24

Our initial idea about the testing topologies are the 14-node-NSFNET network, and the 24-node-US Backbone network, as shown in Figure 7.1. These two networks are widely used to test the performance of work on the long haul backbone networks [2] [3] [4] [8]. In the following experiments, we use NSF-14, USB-24 to represent these two topologies.



(a) 14-nodes NSFNET topology

(b) 24-nodes US Backbone topology

Figure 7.1: Topologies used in simulations marked fiber length in kilometers.

7.2.1 Experimental Environment

The available spectrum of links is defined for the two network topologies (NSF-14, USB-24) as follows. The spectrum of each link is divided into 300 frequency slots (FSs) with a size of 12.5 GHz. The guard band to separate the adjacent connection is assumed to be 1 GHz. Connection requests $CR\,(s, d, BW_{req}, t_{living})$ arrive one by one following the Poisson process, with average arrival rate λ. The flow duration t_{living} of connection requests follows the exponential distribution with an average of $1/\mu$ time units. Therefore, the traffic load can be quantified through λ/μ in Erlangs. The src-dst pair (s, d) is randomly chosen from the nodes in the topology. The required bandwidth of each connection request BW_{req} is randomly selected within the range of $10 - 800$ GB/s. Transmission reach for BPSK, QPSK, 8-QAM and 16-QAM signals is 9600 km, 4800 km, 2400 km and 1200 km respectively [5]. The simulation parameters are shown in Table 7.1.

Simulation Parameters		
B	number of frequency slots per link	300
BW_{slot}	bandwidth of a frequency slot	12.5 GHz
C_{slot}	capacity of a frequency slot with $M = 1$	12.5 GHz
N_{GB}	number of slots for guard-band per connection	1
M = 1	Transmission reach of BPSK	9600 km
M = 2	Transmission reach of QPSK	4800 km
M = 3	Transmission reach of 8-QAM	2400 km
M = 4	Transmission reach of 16-QAM	1200 km
K	number of path candidates for $s - d$ pair	4 for NSF; 5 for USB
C	Range of requested bandwidth	$10 - 800$ Gb/s

Table 7.1: The table of simulation parameters

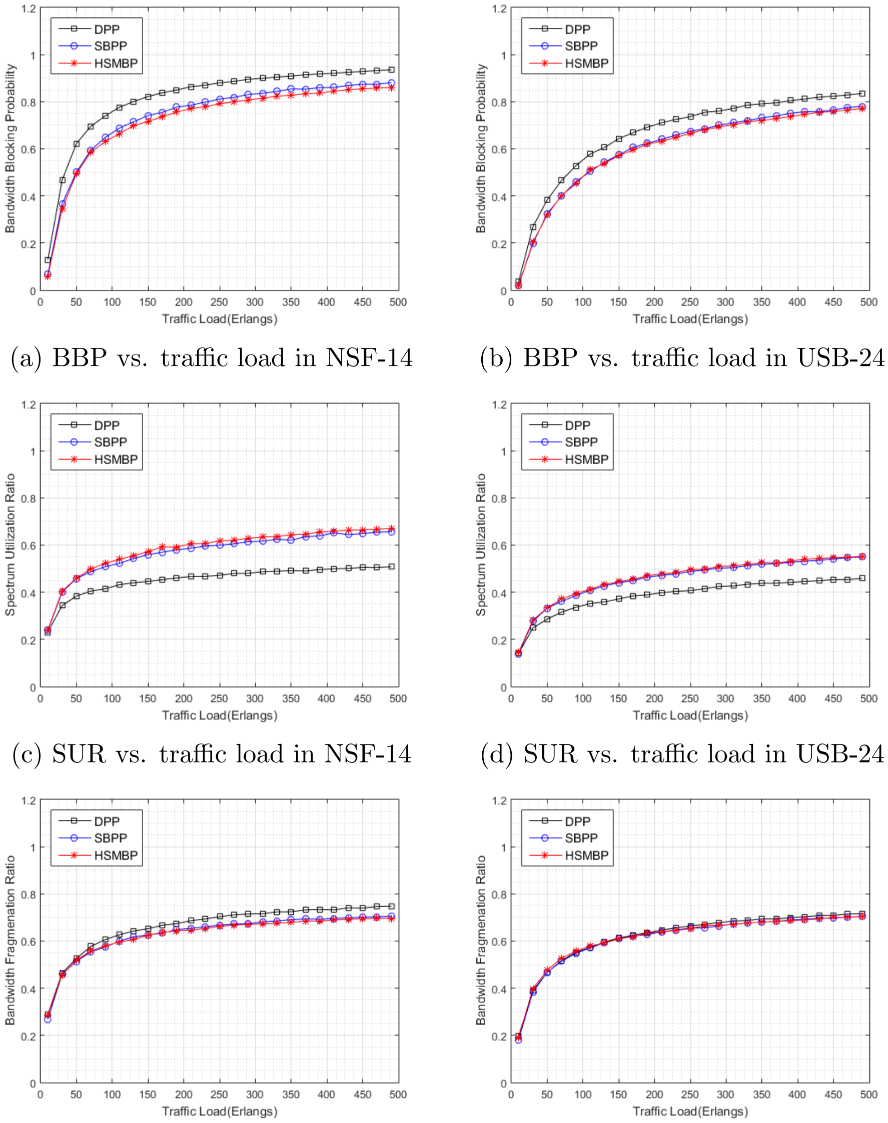
7.2.2 Schemes Comparison

From the evaluation results on HSMBP with different thresholds and number of backup paths, we find HSMBP with threshold 400, 2 backup paths has the best performance among all the scenarios. More information is in Appendix B.

The simulation results of BBP vs. traffic load, SUR vs. traffic load, BFR vs. traffic load for the NSF-14 and USB-24 topology are listed in two column as shown in Figure 7.2. The mean values of BBP, SUR, and BFR for different methods in NSF-14 and USB-24 are presented in Table 7.2 and Table 7.3 respectively.

In the first column of Figure 7.2, the performance in NSF-14 is shown. Our scheme achieves the lowest Bandwidth blocking probability (BBP) (as in Figure 7.2a, reducing the BBP by 11.2% and 2.5%) , when compared to DPP and SBPP. In terms of the results for Spectrum utilization ratio (SUR) shown in Figure 7.2c, our scheme has the highest value among the three analyzed schemes. The comparison with DPP and SBPP shows SUR is improved by 28.6% and 2.3% respectively. Similarly, our scheme, when compared to the other two, has lower Bandwidth Fragmentation Ratio (BFR) with reduction of 5.4% and 0.6% as shown in Figure 7.2e.

The second column of Figure 7.2 shows the performance in USB-24. With the increase of traffic load, the Bandwidth blocking probability (BBP) for our scheme is reduced by 1% and 10% compared with the BBP for DPP and SBPP as shown in Figure 7.2b. For the Spectrum utilization ratio (SUR) and Bandwidth fragmentation ratio (BFR) as shown in 7.2d and 7.2f, our scheme has slightly improvement (1.2% and 0.4%) compared with SBPP, while the SUR is increased by 19.4% and BFR is decreased by 1% compared with DPP.



(a) BBP vs. traffic load in NSF-14

(b) BBP vs. traffic load in USB-24

(c) SUR vs. traffic load in NSF-14

(d) SUR vs. traffic load in USB-24

(e) BFR vs. traffic load in NSF-14

(f) BFR vs. traffic load in USB-24

Figure 7.2: The performance for different schemes in NSF-14 and USB-24

Table 7.2: Mean values for different methods in NSF14

Schemes	BBP	SUR	BFR
DPP	0.8130	0.4539	0.6629
SBPP	0.7402	0.5704	0.6308
HSMBP	0.7216	0.5838	0.6269

Table 7.3: Mean values for different methods in USB24

Schemes	BBP	SUR	BFR
DPP	0.6649	0.3868	0.6196
SBPP	0.6042	0.4563	0.6109
HSMBP	0.5980	0.4618	0.6135

7.3 Experiments in Random Graph

From the results of the experiments in NSF-14 and USB-24, we can find that our scheme does not show much difference with different parameters including the threshold value, the number of paths as shown in Appendix B. As to the results of schemes comparison in NSF-14 and USB-24, our scheme also do not show a big impact on the network performance, especially in USB-24.

One reason is that the average node degrees of NSF-14 (22 links) and USB-24 (43 links) are too small (3.14 and 3.58 respectively). In our experiments, we need to reserve resources along two or three disjoint paths for working and backup. In NSF-14 and USB-24, the available resources in the disjoint paths will be occupied soon by arriving flows because the resources of the disjoint paths are limited. Then super traffics will be blocked when assigning spectrum to working path. However, our scheme focus on multiple backup paths for super traffics will have no chance to work.

Another reason is that the distance between a pair of source and destination will be long in NSF-14 and USB-24, especially in USB-24. The backup paths may have more hops and use more resources. The long distance transmission hava to use low modulation level, which means more slots even four times slots are needed for backup paths if the working path is short.

Considering a topology with high node degree and no influence of modulation, we use Erdős-Rényi random graph model to generate a random graph $G(n, p)$, where n is the number of vertices and p $(0 \leq q \leq 1)$ is a probability of connection existing between a pair of vertices [6]. We set q to be 0.8 so that every nodes can be connected and the average degree is $(n-1) \times 0.8$.

7.3.1 Experimental Environment

The same traffic model is employed to the experiments in a random graph. Most parameters also stay the same. The distance and modulation are ignored in the random graph. The simulation parameters are shown in Table 7.4.

Simulation Parameters		
B	number of frequency slots per link	100
BW_{slot}	bandwidth of a frequency slot	12.5 GHz
N_{GB}	number of slots for guard-band per connection	1
K	number of path candidates for $s-d$ pair	4
C	Range of requested bandwidth	$10-800$ Gb/s

Table 7.4: The table of simulation parameters

7.3.2 Schemes Comparison

We create two random graphs with 20 and 30 nodes respectively. Then the average degrees for these two random graphs are 15.2 and 23.2 when the connection probability is 0.8. The testing results about BBP, SUR, and BFR with increasing traffic load from 100 to 710 Erlang are shown in Figure 7.3. The first column is the results for random graph with 20 nodes and the second column presents the results for random graph with 30 nodes. Table 7.5 and Table 7.6 are mean value of BBP, SUR, and BFR for different schemes in 20-node random graph and 30-node random graph.

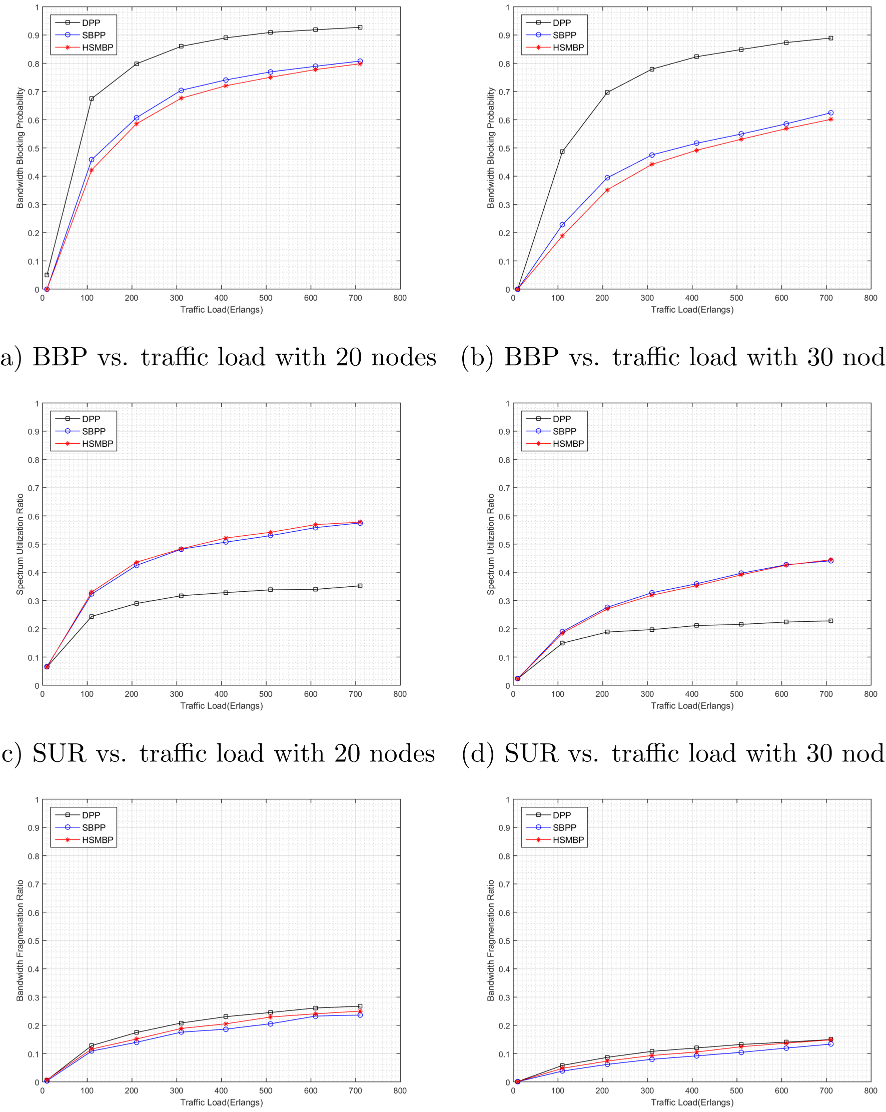
The results in 20-node random graph shows that our scheme reduces BBP by 21.5% and 3.0% compared to DPP and SBPP. It increases SUR by 55% compared to DPP, but has similar SUR with SBPP. As to BFR, our scheme reduces BFR by 8.7% compared to DPP but has higher BFR (increased by 9.2%) than SBPP.

In terms of the results in 30-node random random graph, our scheme reduces BBP by 41.2% and 5.9% compared to DPP and SBPP. There is no much difference for SUR between SBPP and our scheme. But big improvement in SUR for our scheme compared to DPP. Our scheme has lower BFR (reduced by 8.2%) than DPP but higher BFR (increased by 16.1%) than SBPP.

We can conclude that our scheme can improve the network performance by reducing BBP at a price of more BFR. But it has almost the same SUR with SBPP, which means our scheme leads more shared backup resources. Our scheme is more effective in random graph with more number of nodes.

Table 7.5: Mean values for different schemes in 20-node Random Graph

Schemes	BBP	SUR	BFR
DPP	0.7534	0.2841	0.1904
SBPP	0.6096	0.4332	0.1612
HSMBP	0.5913	0.4405	0.1738



(a) BBP vs. traffic load with 20 nodes (b) BBP vs. traffic load with 30 nodes

(c) SUR vs. traffic load with 20 nodes (d) SUR vs. traffic load with 30 nodes

(e) BFR vs. traffic load with 20 nodes (f) BFR vs. traffic load with 30 nodes

Figure 7.3: The performance for different schemes in Random Graph

Table 7.6: Mean values for different schemes in 30-node Random Graph

Schemes	BBP	SUR	BFR
DPP	0.6746	0.1796	0.0997
SBPP	0.4216	0.3051	0.0788
HSMBP	0.3968	0.3013	0.0915

7.3.3 Influence of different parameters

Our scheme has two important parameters: the threshold value to classify the type of connection requests and the number of backup paths. We investigate how these parameters affect the performance of our schemes in 30-node random graph.

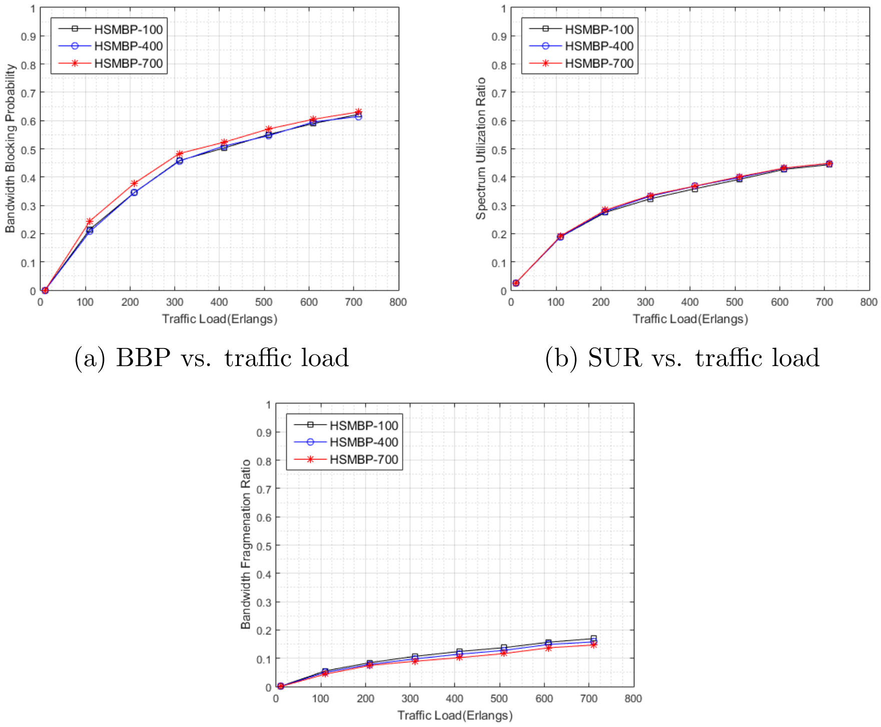
Figure 7.4 and Table 7.7 present testing results with different threshold values. In our scheme, the connection requests are classified into two types based on the amount of bandwidth they require. If a flow is above a preset threshold, and therefore falls into the group of large-bandwidth flows, multiple backup paths are used for protection. Alternatively, if the flow is below that preset threshold, a single backup path is used for protection. Since the required bandwidth is from 10 to 800 Gb/s, we test BBP, SUR, and BFR with the threshold value set to be 100, 400, and 700.

We get lower SUR and BBP when threshold is 100 as shown in Figure 7.4b, which means more backup resources are shared. This is also why our scheme with threshold 400 has lower BBP but almost the same SUR compared with the results from threshold 700. The results of BFR shown in Figure 7.4c illustrate more paths protected by multiple backup paths will lead to more fragmentation.

We get lower BBP when threshold is set to be 100 and 400 as shown in Figure 7.4a, which shows our scheme can improve the network performance by reducing BBP. The similar results in BBP for threshold 100 and 400 can imply that more paths protected by multiple backup paths does not mean less BBP. We can conclude that it is not necessary to protect small traffic through multiple backup paths which will result in no reduction of blocks but more fragmentation.

Table 7.7: Mean values for different threshold value in 30-node Random Graph

Threshold	BBP	SUR	BFR
100	0.4106	0.3043	0.1044
400	0.4094	0.3090	0.0970
700	0.4294	0.3108	0.0889



(a) BBP vs. traffic load

(b) SUR vs. traffic load

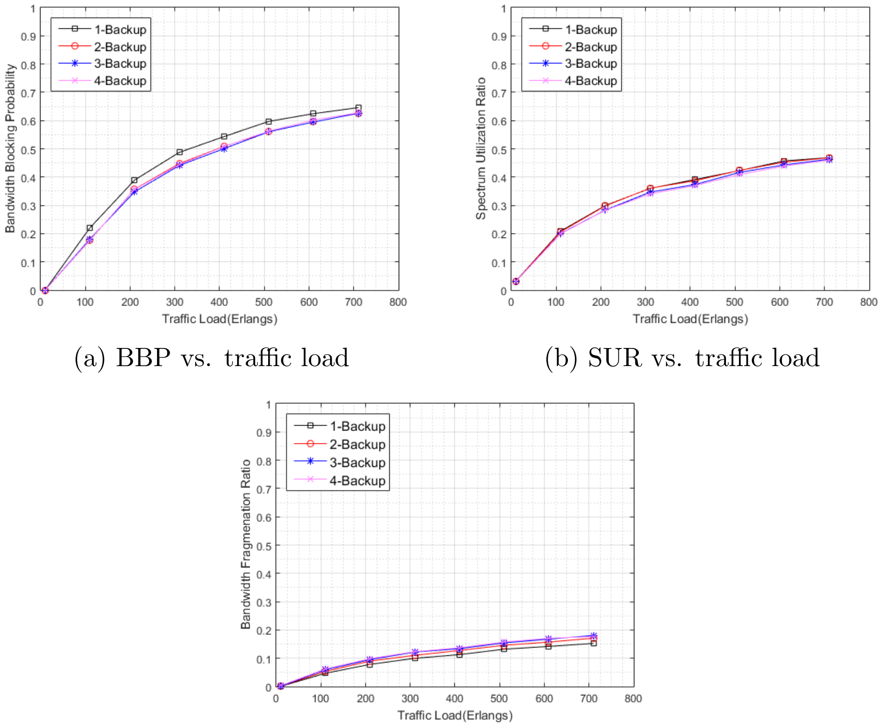
(c) BFR vs. traffic load

Figure 7.4: The performance for different threshold in 30-node Random Graph

The number of backup paths may also influence the performance of HSMBP. We change the number of backup paths to test its influence. In this test, we find 5 disjoint paths as candidates for working and backup paths. The one with single backup path is also known as SBPP.

Figure 7.5 and Table 7.8 show the results with different number of backup paths. Figure 7.5a shows multiple backup paths can has lower BBP than the result from single backup path but the change on BBP is not obvious when increasing the number of backup paths from 2 to 4. Figure 7.5b shows that more backup paths can reduce SUR. In Figure 7.5c, BFR rises with the number of backup paths increased. But the increase of BFR from 3 backup paths to 4 backup paths is not large.

We can conclude that our scheme can reduce the BBP to improve the network performance but when we increase the number of backup paths, we can not get obvious performance improvement. However, the computing complexity increases when increasing the number of backup paths.



(a) BBP vs. traffic load

(b) SUR vs. traffic load

(c) BFR vs. traffic load

Figure 7.5: The performance for different path number in 30-node Random Graph

Table 7.8: Mean values for different path number in 30-node Random Graph

Path number	BBP	SUR	BFR
1	0.4385	0.3301	0.0956
2	0.4089	0.3286	0.1070
3	0.4065	0.3197	0.1142
4	0.4098	0.3163	0.1161

Chapter 8

Conclusions & Future Work

8.1 Conclusions

In Elastic Optical Networks, the research on improving the resource utilization will never stop. Taking super traffic into consideration, we have proposed a new survivability scheme called Hybrid Single and Multiple Backup Protection (HSMBP).

We achieved this scheme under the architecture of Software defined Networking (SDN). It can help us easily monitor and manage the network resources through its centralized architecture. Then our scheme is evaluated in different scenarios. The performance of our scheme is varied depending on the settings: the threshold and the number of backup paths. Finally, our scheme was compared with two common survivability schemes: Shared Backup Path Protection (SBPP) and Dedicated Path Protection (DPP). The results show our scheme can improve network performance by reducing Bandwidth Blocking Probability (BBP) at the price of higher Bandwidth Fragmentation Ratio (BFR). Moreover, our scheme can achieve full protection for all types of traffic when one failure happens and partial protection for super traffic when multiple failures happen in the network because of the nature of multiple paths.

8.2 Future Work

We have achieved most of the work, but there is still some work to do.

First of all, we found the two-step algorithm does not fit our scheme perfectly during the experiments. A specific algorithm for our scheme can be studied in future. For example, a proper path selection policy and spectrum allocation policy can be proposed to improve the performance of our scheme.

Secondly, the survivability performance of HSMBP can be evaluated under the architecture of Software Defined Optical Networking. For example, the recovery time and complexity. Currently, the experiments are limited by current simulation platform. The problems on Open Network Operating System (ONOS) is introduced in Appendix A. The simulation platform could also be extended to support the protocol of optical networks.

Thirdly, our scheme leads to more fragmentation. We can achieve defragmentation by scheduling the backup resources.

Bibliography

[1] Linux Foundation Administrators. Open network operating system (onos), September 2017.

[2] M. Aibin and K. Walkowiak. Adaptive survivability algorithm for path protection with various traffic classes in elastic optical networks. In *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 56–62, Oct 2015.

[3] S. Ba, B. C. Chatterjee, and E. Oki. Defragmentation scheme based on exchanging primary and backup paths in 1 x002b;1 path protected elastic optical networks. *IEEE/ACM Transactions on Networking*, 25(3):1717–1731, June 2017.

[4] Edyta Biernacka, Jerzy Domzal, and Robert Wjcik. Investigation of dynamic routing and spectrum allocation methods in elastic optical networks. *ELECTRONICS AND TELECOMMUNICATIONS*, 63:85–92, 2017.

[5] A. Bocoi, M. Schuster, F. Rambach, M. Kiese, C. A. Bunge, and B. Spinnler. Reach-dependent capacity in optical networks enabled by ofdm. In *2009 Conference on Optical Fiber Communication - incudes post deadline papers*, pages 1–3, March 2009.

[6] Bla Bollobs. *Random Graphs*. Cambridge University Press, 2nd edition edition, 2001.

[7] Alberto Castro, Luis Velasco, Jaume Comellas, and Gabriel Junyent. On the benefits of multi-path recovery in flexgrid optical networks. *Photonic Network Communications*, 28(3):251–263, Dec 2014.

[8] X. Chen, M. Tornatore, S. Zhu, F. Ji, W. Zhou, C. Chen, D. Hu, L. Jiang, and Z. Zhu. Flexible availability-aware differentiated protection in software-defined elastic optical networks. *Journal of Lightwave Technology*, 33(18):3872–3882, Sept 2015.

[9] K. Christodoulopoulos, I. Tomkos, and E. A. Varvarigos. Elastic bandwidth allocation in flexible ofdm-based optical networks. *Journal of Lightwave Technology*, 29(9):1354–1366, May 2011.

[10] Cisco. Cisco visual networking index: Forecast and methodology, 20162021, September 2017.

[11] S. Das, Y. Yiakoumis, G. Parulkar, N. McKeown, P. Singh, D. Getachew, and P. D. Desai. Application-aware aggregation and traffic engineering in a converged packet-circuit network. In *2011 Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference*, pages 1–3, March 2011.

[12] Open Networking Foundation. Openflow switch specification version 1.3.0, 2012.

[13] Open Networking Foundation. Sdn architecture, 2014.

[14] O. Gerstel, M. Jinno, A. Lord, and S. J. B. Yoo. Elastic optical networking: a new dawn for the optical layer? *IEEE Communications Magazine*, 50(2):s12–s20, February 2012.

[15] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. Andr, L. Jorge, L. Martins, P. O. Ugalde, A. Pai, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore. A survey of strategies for communication networks to protect against large-scale natural disasters. In *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, pages 11–22, Sept 2016.

[16] S. Gringeri, B. Basch, V. Shukla, R. Egorov, and T. J. Xia. Flexible architectures for optical transport nodes and networks. *IEEE Communications Magazine*, 48(7):40–50, July 2010.

[17] Corporate Headquarters. Tl1 command reference for the cisco ons 15808 dwdm system, 2003.

[18] F. Iqbal and F. A. Kuipers. Disjoint paths in networks. *Wiley Encyclopedia of Electrical and Electronics Engineering*, page 111, 2015.

[19] 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 Communications Magazine*, 47(11):66–73, November 2009.

[20] L. Liu, R. Muoz, R. Casellas, T. Tsuritani, R. Martnez, and I. Morita. Openslice: An openflow-based control plane for spectrum sliced elastic optical path networks. In *2012 38th European Conference and Exhibition on Optical Communications*, pages 1–3, Sept 2012.

[21] L. Liu, T. Tsuritani, I. Morita, R. Casellas, R. Martnez, and R. Muoz. Control plane techniques for elastic optical networks: Gmpls/pce vs openflow. In *2012 IEEE Globecom Workshops*, pages 352–357, Dec 2012.

[22] A. Rosa, C. Cavdar, S. Carvalho, J. Costa, and L. Wosinska. Spectrum allocation policy modeling for elastic optical networks. In *High Capacity Optical Networks and Emerging/Enabling Technologies*, pages 242–246, Dec 2012.

[23] Zhi shu Shen, Hiroshi Hasegawa, and Ken ichi Sato. Integrity enhancement of flexible/semi-flexible grid networks that minimizes disruption in spectrum defragmentation and bitrate-dependent blocking. *J. Opt. Commun. Netw.*, 7(4):235–247, Apr 2015.

[24] J. W. Suurballe. Disjoint paths in a network. In *Networks*, page 125145, 1974.

[25] N. L. M. v. Adrichem, B. J. v. Asten, and F. A. Kuipers. Fast recovery in software-defined networks. In *2014 Third European Workshop on Software Defined Networks*, pages 61–66, Sept 2014.

[26] Chao Wang, Gangxiang Shen, Bowen Chen, and Limei Peng. Protection path-based hitless spectrum defragmentation in elastic optical networks: Shared backup path protection. In *2015 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3, March 2015.

[27] Chao Wang, Gangxiang Shen, and Limei Peng. Protection path-based hitless spectrum defragmentation for elastic optical networks: 1+1 path protection. In *Asia Communications and Photonics Conference 2014*, page AF3E.3. Optical Society of America, 2014.

[28] Wikipedia. Wavelength-division multiplexing, 2017.

[29] Paul R. Wilson, Mark S. Johnstone, Michael Neely, and David Boles. *Dynamic storage allocation: A survey and critical review*, pages 1–116. Springer Berlin Heidelberg, Berlin, Heidelberg, 1995.

[30] P. J. Winzer. Beyond 100g ethernet. *IEEE Communications Magazine*, 48(7):26–30, July 2010.

[31] J. Wu, Z. Ning, and L. Guo. Energy-efficient survivable grooming in software-defined elastic optical networks. *IEEE Access*, 5:6454–6463, 2017.

[32] Dharmendra Singh Yadav, Abhishek Chakraborty, and B.S. Manoj. A multi-backup path protection scheme for survivability in elastic optical networks. *Optical Fiber Technology*, 30(Supplement C):167 – 175, 2016.

[33] S. Yamashita, A. Yamada, K. Nakatsugawa, T. Soumiya, M. Miyabe, and T. Katagiri. Extension of openflow protocol to support optical transport network, and its implementation. In *2015 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 263–268, Oct 2015.

[34] Hui Yang, Lei Cheng, Jian Yuan, Jie Zhang, Yongli Zhao, and Young Lee. Multipath protection for data center services in openflow-based software defined elastic optical networks. *Optical Fiber Technology*, 23(Supplement C):108 – 115, 2015.

[35] S. Yang and F. Kuipers. Impairment-aware routing in translucent spectrum-sliced elastic optical path networks. In *2012 17th European Conference on Networks and Optical Communications*, pages 1–6, June 2012.

[36] S. Yin, S. Huang, B. Guo, Y. Zhou, H. Huang, M. Zhang, Y. Zhao, J. Zhang, and W. Gu. Shared-protection survivable multipath scheme in flexible-grid optical networks against multiple failures. *Journal of Lightwave Technology*, 35(2):201–211, Jan 2017.

[37] Z. Zhu, X. Chen, C. Chen, S. Ma, M. Zhang, L. Liu, and S. J. B. Yoo. Openflow-assisted online defragmentation in single-/multi-domain software-defined elastic optical networks [invited]. *IEEE/OSA Journal of Optical Communications and Networking*, 7(1):A7–A15, Jan 2015.

Appendix A

Simulation Platform

Currently, there are multiple platforms that support SDEON such as the OpenSlice [20]. ONOS is an open source platform that supports multi-layer networks as depicted in Figure A.1. We tested the optical application of ONOS. In the Optical-IP use case of ONOS, Mininet is the emulation tool to create and control the network switches, links, and hosts. The behavior of these switches is controlled by ONOS through the OpenFlow protocol. In the infrastructure layer, there are two different types of switches: the packet switches (Open vSwitch) that use the OpenFlow 1.0 and the optical switches (LINC-OE) that use the OpenFlow 1.3 protocol to communicate with the controller.

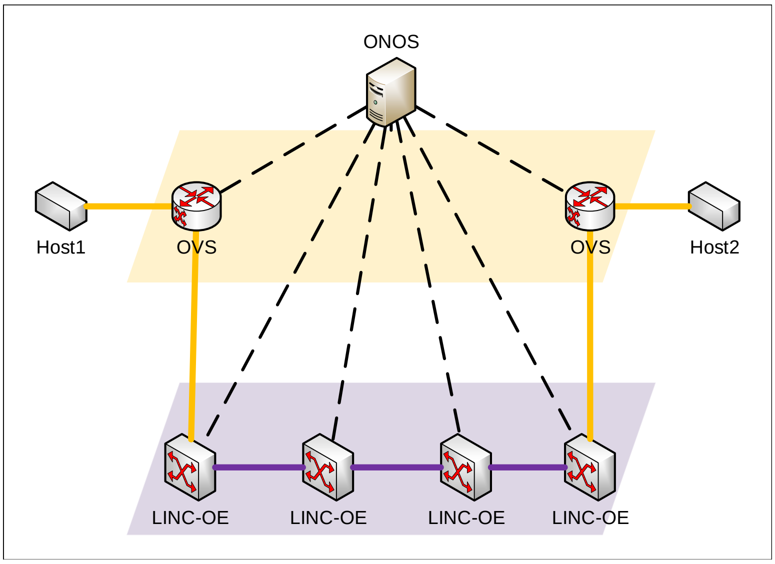
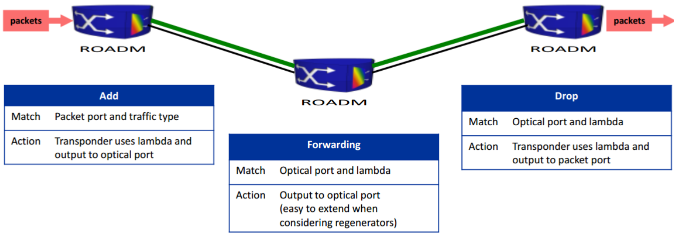


Figure A.1: The Multi-layer control of ONOS platform

A.1 Packet Optical Convergence

ONOS is able to manage and control multilayer networks. In the infrastructure layer, packet switches and optical switches are connected for packet optical convergence. The optical switch is simulated by LINC-OE (LINC-Switch for optical emulation). LINC-Switch is an OpenFlow software switch and it can be configured to emulate the Reconfigurable Optical Add-drop Multiplexer (ROADM). The configured LINC-Switch to support the optical emulation is called LINC-OE.

Based on the packet-optical model in the infrastructure plane, the optical switches connected directly with packet switches will add the optical signal when packets come from packet switch and drop that signal when packets leave from optical switches to packet switches. The optical signal is able to be forwarded between the optical switches. Thus, the optical switches have three functions: add, forwarding and drop. These optical switches are also controlled by ONOS through the OpenFlow protocol. The Match/Action in optical switches is shown in Figure A.2.



Add	
Match	Packet port and traffic type
Action	Transponder uses lambda and output to optical port

Forwarding	
Match	Optical port and lambda
Action	Output to optical port (easy to extend when considering regenerators)

Drop	
Match	Optical port and lambda
Action	Transponder uses lambda and output to packet port

Figure A.2: The forwarding model for packet optical convergence [1]

When packets come from packet switch, the optical switch receives these packets and sends them to the ONOS controller, ONOS will identify the traffic type based on the port type. Then ONOS computes the path based on the source and destination and assign the spectrum based on the required bandwidth. Sequentially, the flow tables are installed into optical switches for the path and spectrum provisioning.

The flow entry to add the packets to the corresponding optical channel is installed into the first optical switch. Then this switch will output the optical signal to the port of another optical switch. The optical switches between the first and last optical switches identify the optical signal through the port and the central frequency of optical channel and forward the matched optical signal. In the last optical switch, the optical signal is dropped and sent to the port of connected packet switch.

A.2 Optical tutorial VM

There is an official optical tutorial VM. We follow the tutorial to create a connection between two hosts. If we want to build a connection between two hosts, we need to add a host intent. But when we use app-host-intent to add host intent through CLI, the intent can be submitted successfully but it can not find a correct optical way between the two host. The two packet switches are connected directly. That means the optical switches could not be found or connected.

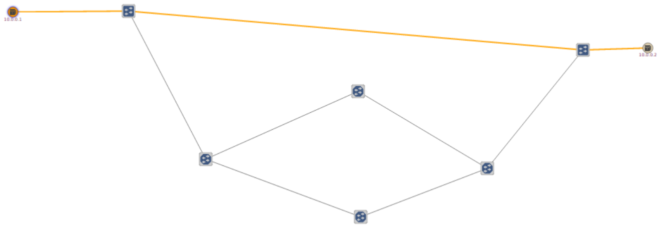


Figure A.3: Two packet switches connect after adding host intent

A.3 ONOS 1.10

We build the development environment of optical-Ip convergence in our VM. When installing and configuring ONOS 1.10, mininet and LINC-Switch, there are some little tricks.

- In the documents of ONOS, it recommends people to install and develop ONOS in Ubuntu16.04 because ONOS developers use Ubuntu 16.04 to develop the platform. The instruction of LINC-Switch shows it required Erlang version R16 or newer. In fact, LINC-Switch needs Erlang with no higher version than 17 and Ubuntu 16.04 does not have Erlang 17 and only can install Erlang 19. Finally, we must use Ubuntu 14.04 for the optical-Ip use case.
- The mininet connects the remote controller through the TCP port 6653 and 6633. ONOS connects the GUI and CLI through port 8181 and 8101 respectively. These ports should be open in advance.
- If the LINC switches do not set up correctly, the available attribute of LINC-OE will be false. In this situation, we have to restart the whole system.
- When checking the state of links in the network, it will be inactive and could not be shown through GUI. This happened when the LINC switches are set up before running the script *opticalTest.py* to set up

the network topology. So we need to check the LINC switches are correctly shut down. If not, stop LINC switches before running ONOS through the following command:

```
$sudo /linc−oe/rel/linc/bin/linc stop
```

- After launching the ONOS controller and before setting up mininet, we need to active *org.onosproject.drivers.optical* module in CLI through the command below:

  ```
  $app activate org.onosproject.optical
  ```

  The *org.onosproject.drivers.optical* module is the optical application. Then the LINC-OE switches should be started and registered to ONOS correctly when running *opticalTest.py* to set up the network topology. Some errors may occur in ONOS server as shown below.

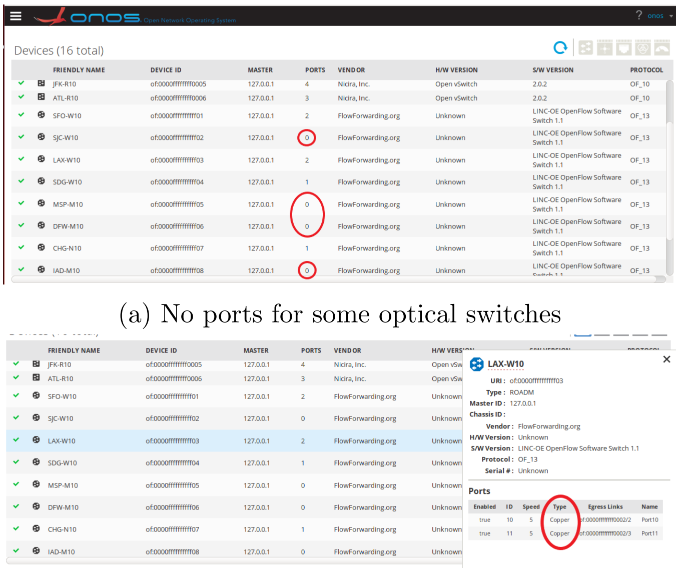
  ```
  2017−05−1021 : 50 : 10, 846|ERROR|source−registrar|ResourceDeviceListener|127−
  org.onosproject.onos − core − net − 1.10.0.SNAPSHOT|FailedtoregisterDevice : of :
  0000ffffffffff03
  2017−05−1021 : 50 : 10, 849|ERROR|source−registrar|ResourceDeviceListener|127−
  org.onosproject.onos − core − net − 1.10.0.SNAPSHOT|FailedtoregisterPort :
  [of : 0000ffffffffff03, 10]
  2017−05−1021 : 50 : 10, 851|ERROR|source−registrar|ResourceDeviceListener|127−
  org.onosproject.onos−core−net−1.10.0.SNAPSHOT|FailedtoregisterBandwidthfor
  [of : 0000ffffffffff03, 10]
  ```

  Sequentially, some problems about the ports of devices (just the optical switches) occurred as shown in the Figure A.4. Some optical switches do not have ports as in Figure A.4a. The other optical switches have ports but the type is copper as in Figure A.4b. The correct types are oms and och for optical switches.

  These are because the drivers of optical application should be activated. Thus, we activate the *org.onosproject.drivers.optical* module through the command below:

  ```
  $app activate org.onosproject.drivers.optical
  ```

- We try to install the HostToHost intent to build a connection between two hosts through both CLI and GUI. But the intents always failed and ONOS keeps installing (Figure A.5) until we stop the ONOS server. This is a little bug in ONOS platform.



Devices (16 total)

		FRIENDLY NAME	DEVICE ID	MASTER	PORTS	VENDOR	H/W VERSION	S/W VERSION	PROTOCOL
✓		JFK-R10	of:0000ffffffff0005	127.0.0.1	4	Nicira, Inc.	Open vSwitch	2.0.2	OF_10
✓		ATL-R10	of:0000ffffffff0006	127.0.0.1	3	Nicira, Inc.	Open vSwitch	2.0.2	OF_10
✓		SFO-W10	of:0000ffffffffff01	127.0.0.1	2	FlowForwarding.org	Unknown	LINC-OE OpenFlow Software Switch 1.1	OF_13
✓		SJC-W10	of:0000ffffffffff02	127.0.0.1	0	FlowForwarding.org	Unknown	LINC-OE OpenFlow Software Switch 1.1	OF_13
✓		LAX-W10	of:0000ffffffffff03	127.0.0.1	2	FlowForwarding.org	Unknown	LINC-OE OpenFlow Software Switch 1.1	OF_13
✓		SDG-W10	of:0000ffffffffff04	127.0.0.1	1	FlowForwarding.org	Unknown	LINC-OE OpenFlow Software Switch 1.1	OF_13
✓		MSP-M10	of:0000ffffffffff05	127.0.0.1	0	FlowForwarding.org	Unknown	LINC-OE OpenFlow Software Switch 1.1	OF_13
✓		DFW-M10	of:0000ffffffffff06	127.0.0.1	0	FlowForwarding.org	Unknown	LINC-OE OpenFlow Software Switch 1.1	OF_13
✓		CHG-N10	of:0000ffffffffff07	127.0.0.1	1	FlowForwarding.org	Unknown	LINC-OE OpenFlow Software Switch 1.1	OF_13
✓		IAD-M10	of:0000ffffffffff08	127.0.0.1	0	FlowForwarding.org	Unknown	LINC-OE OpenFlow Software Switch 1.1	OF_13

(a) No ports for some optical switches

		FRIENDLY NAME	DEVICE ID	MASTER	PORTS	VENDOR	H/W VERS
✓		JFK-R10	of:0000ffffffff0005	127.0.0.1	4	Nicira, Inc.	Open vSw
✓		ATL-R10	of:0000ffffffff0006	127.0.0.1	3	Nicira, Inc.	Open vSw
✓		SFO-W10	of:0000ffffffffff01	127.0.0.1	2	FlowForwarding.org	Unknown
✓		SJC-W10	of:0000ffffffffff02	127.0.0.1	0	FlowForwarding.org	Unknown
✓		LAX-W10	of:0000ffffffffff03	127.0.0.1	2	FlowForwarding.org	Unknown
✓		SDG-W10	of:0000ffffffffff04	127.0.0.1	1	FlowForwarding.org	Unknown
✓		MSP-M10	of:0000ffffffffff05	127.0.0.1	0	FlowForwarding.org	Unknown
✓		DFW-M10	of:0000ffffffffff06	127.0.0.1	0	FlowForwarding.org	Unknown
✓		CHG-N10	of:0000ffffffffff07	127.0.0.1	1	FlowForwarding.org	Unknown
✓		IAD-M10	of:0000ffffffffff08	127.0.0.1	0	FlowForwarding.org	Unknown

LAX-W10 ×

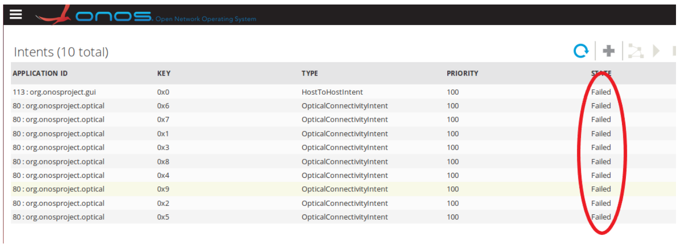
URI : of:0000ffffffffff03
Type : ROADM
Master ID : 127.0.0.1
Chassis ID :
Vendor : FlowForwarding.org
H/W Version : Unknown
S/W Version : LINC-OE OpenFlow Software Switch 1.1
Protocol : OF_13
Serial # : Unknown

Ports

Enabled	ID	Speed	Type	Egress Links	Name
true	10	5	Copper	of:0000ffffffff0002/2	Port10
true	11	5	Copper	of:0000ffffffff0002/3	Port11

(b) Copper ports for optical switches

Figure A.4: The error states of optical switches.



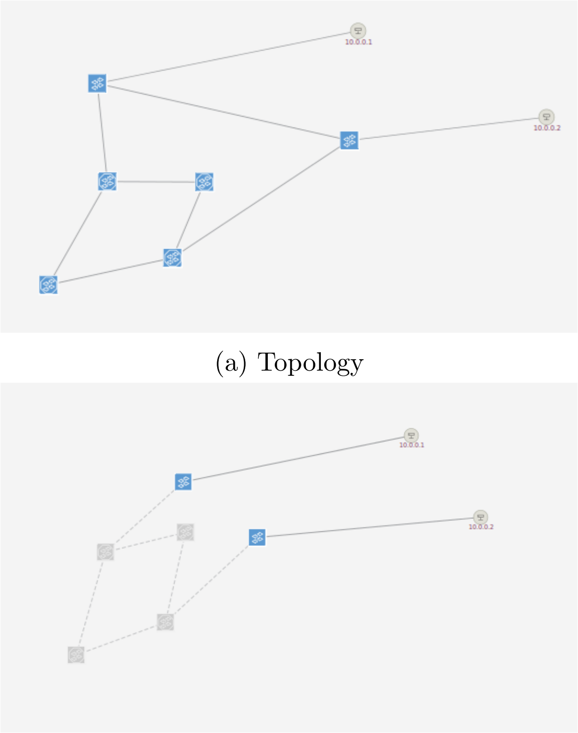
Intents (10 total)

APPLICATION ID	KEY	TYPE	PRIORITY	STATE
113 : org.onosproject.gui	0x0	HostToHostIntent	100	Failed
80 : org.onosproject.optical	0x6	OpticalConnectivityIntent	100	Failed
80 : org.onosproject.optical	0x7	OpticalConnectivityIntent	100	Failed
80 : org.onosproject.optical	0x1	OpticalConnectivityIntent	100	Failed
80 : org.onosproject.optical	0x3	OpticalConnectivityIntent	100	Failed
80 : org.onosproject.optical	0x8	OpticalConnectivityIntent	100	Failed
80 : org.onosproject.optical	0x4	OpticalConnectivityIntent	100	Failed
80 : org.onosproject.optical	0x9	OpticalConnectivityIntent	100	Failed
80 : org.onosproject.optical	0x2	OpticalConnectivityIntent	100	Failed
80 : org.onosproject.optical	0x5	OpticalConnectivityIntent	100	Failed

Figure A.5: The failure of installing HostToHost intent.

After building the development environment, I want to achieve fast failover between two hosts shown in Figure A.6a through fast-failover group tables. After flow entries and group tables are successfully installed to optical switches, two hosts are able to ping each other. That means that the optical connection for the working path is built between the two hosts. Then I attach the linc-oe terminal to break a link of the working path and test whether the fast failover group can fast reroute the flow through the backup path. When I attach the linc-oe terminal, the linc-oe will give an error and then all the optical switches become disabled as shown in Figure A.6.

The error message is shown below. It shows the message to reply the group status is badly split into multiple parts. Consequently, it could not be sent to the ONOS controller through OpenFlow protocol channel.



(a) Topology

(b) Topology after errors

Figure A.6: The error states of optical switches.

```
(linc@onos)1 > 01 : 35 : 50.792[error]
Message : ofp_message, 4, multipart_request, 335, ofp_group_stats_reply, [], ...
Channelid :< 0.804.0 >
MessagecannotbesentthroughOFPChannelbecause :
bad_multipart_split
01 : 35 : 50.891[error]
Message : ofp_message, 4, multipart_request, 337, ofp_group_stats_reply, [], ...
Channelid :< 0.802.0 >
MessagecannotbesentthroughOFPChannelbecause :
bad_multipart_split
```

We meet many problems when working on ONOS platform to develop the optical application. The information update about Optical-Ip case is too slow. A majority of information is about the old version, which is quite misleading. In the guidance documents, the specific operating environment especially the ONOS version should be clear provided at the beginning of the guidance. The optical switches are emulated through LINC switches. LINC-Switch is an open source switch developed about three years ago and its GitHub repository is not maintained for a long time. The problems about

LINC-Switch do not be discussed anymore and limited guidance documents are provided, which makes our work on LINC-OE tougher. We waste most time on some small issues when developing on ONOS and LINC switch. Finally, we give up LINC switch because it can not communicate with the controller about the status of groups.

In our implementation, we use Open vSwitch in the infrastructure layer. However, it does not support the match/action for optical carriers so that we can not evaluate the survivability performance of our scheme such as recovery granularity.

Appendix B

HSMBP in NSF and USB

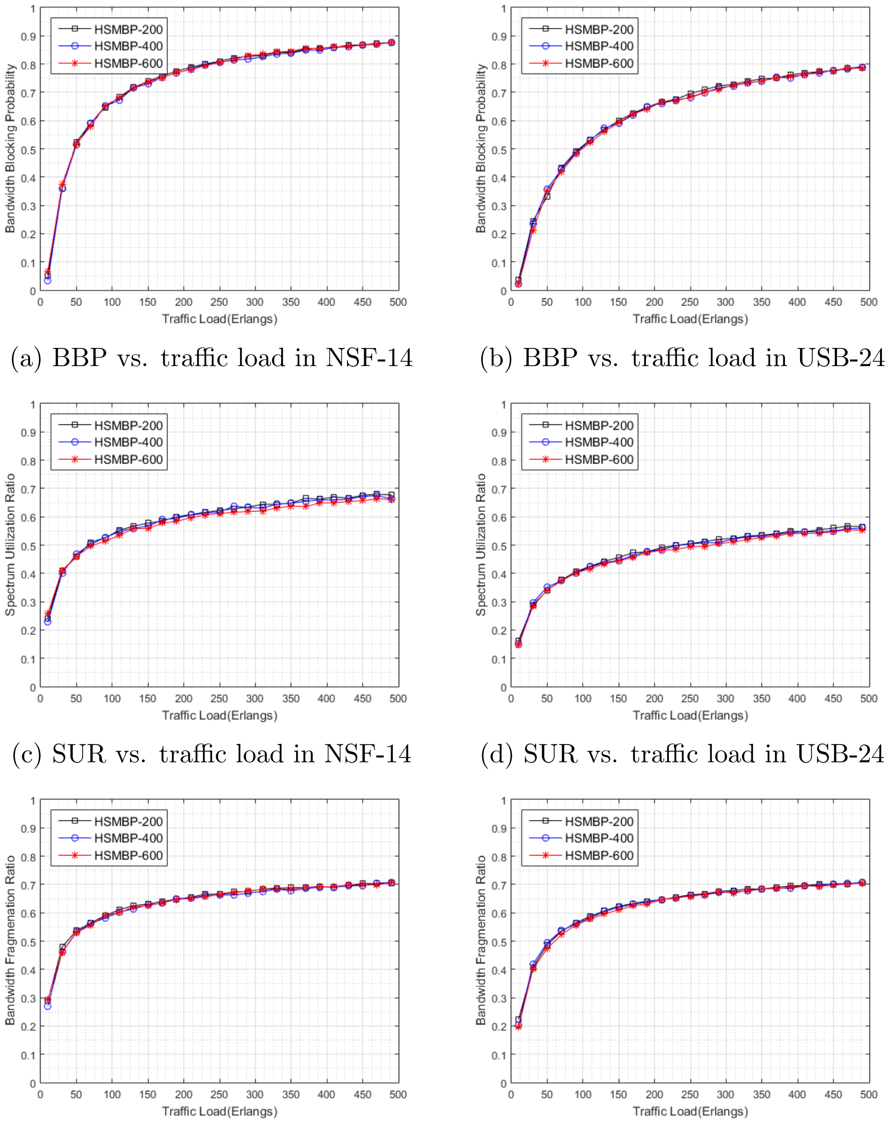
In HSMBP, three important parameters influence its performance. They are: the threshold to identify the type of connection requests; the number of backup paths. Before the comparison with other existing schemes, we investigate how these parameters affect the performance of HSMBP.

B.1 Influence of the threshold value

The first parameter in our scheme is the threshold value. It is used to classify the traffic into two types: small traffic and super traffic. The results of BBP vs. traffic load, SUR vs. traffic load, and BFR vs. traffic load are shown in Figure B.1, where the first and second column represent the performance in NSF-14 and USB-24. Table B.1 and Table B.2 present the mean values of BBP, SUR, and BFR for different threshold in NSF-14 and USB-24. The results do not have much difference among the three different thresholds. We can find that the value of the threshold doesn't have a big impact on the network performance.

Table B.1: Mean values for different threshold in NSF14

Threshold	BBP	SUR	BFR
200	0.7384	0.5907	0.6354
400	0.7337	0.5864	0.6298
600	0.7377	0.5784	0.6319



(a) BBP vs. traffic load in NSF-14

(b) BBP vs. traffic load in USB-24

(c) SUR vs. traffic load in NSF-14

(d) SUR vs. traffic load in USB-24

(e) BFR vs. traffic load in NSF-14

(f) BFR vs. traffic load in USB-24

Figure B.1: The performance for different threshold in NSF-14 and USB-24

Table B.2: Mean values for different threshold in USB24

Threshold	BBP	SUR	BFR
200	0.6240	0.4739	0.6220
400	0.6201	0.4698	0.6198
600	0.6176	0.4639	0.6156

B.2 Influence of the number of paths

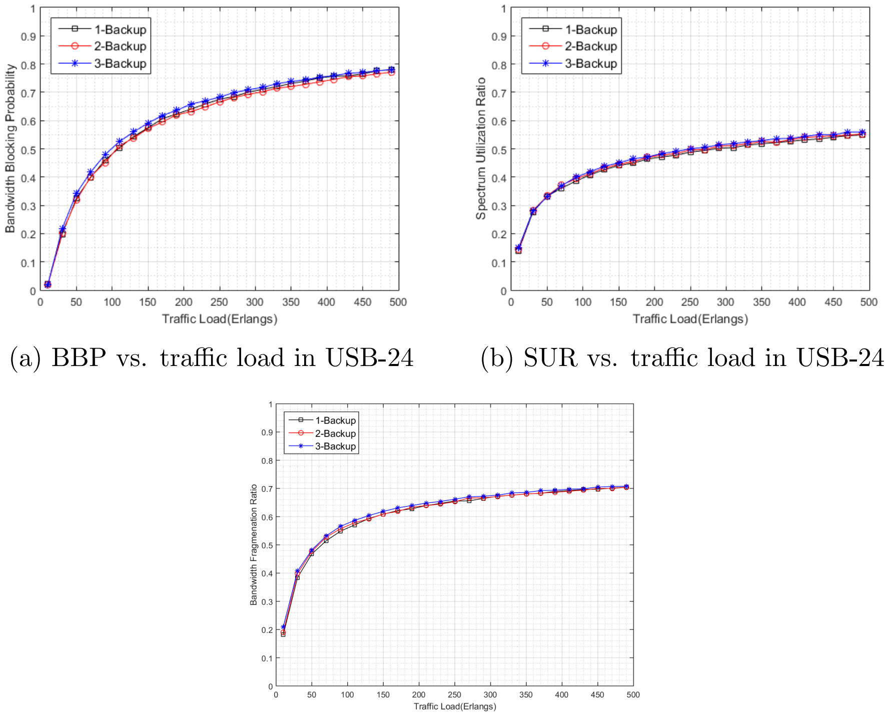
The number of backup paths could also influence the performance of HSMBP. In NSF-14, most source-destination pairs have a maximum of three disjoint paths. Thus, there are maximum two backup paths for most connection requests. In the 24 node-US Backbone, most source-destination pairs have maximum four disjoint paths so that maximum three backup paths exist for most connection requests. Therefore, we only test the performance of HSMBP (BBP, SUR, BFR) with 1, 2, and 3 backup paths with threshold 400 in 24 node-US Backbone topology.

The testing results are shown in Figure B.2. Table B.3 presents the mean values of BBP, SUR, and BFR for different number of backup paths in USB-24. HSMBP with 2 backup paths has lower BBP, SUR, and BFR than that of HSMBP with 3 backup paths. In general, a network with lower BBP will have higher SUR. But BBP and SUR are both lower in the scenario with 2 backup paths. This is because more resources used for backup or guard bands in the scenario with 3 backup paths. In our experiments, disjoint paths are sorted based on the metric LSoHF. The paths ranked behind could be longer so that more resources will be allocated along the third backup paths. Furthermore, more backup paths will need more guard bands.

We can conclude that multiple backup paths can improve the network performance. However, more backup paths do not mean better network performance.

Table B.3: Mean values for different path number in USB24

Path number	BBP	SUR	BFR
1	0.6042	0.4563	0.6109
2	0.5980	0.4618	0.6135
3	0.6146	0.4670	0.6212



(a) BBP vs. traffic load in USB-24

(b) SUR vs. traffic load in USB-24

(c) BFR vs. traffic load in USB-24

Figure B.2: The performance for different path number in USB-24