กลยุทธการออกแบบโครงข่ายหลายโดเมน สำหรับโครงข่ายนำแสงขนาดใหญ่ที่อยู่รอดได้

นายกวน กวาง ลี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2559

MULTI-DOMAIN NETWORK DESIGN STRATEGY FOR SURVIVABLE LARGE-SCALE OPTICAL NETWORKS

Mr. Quynh Quang Le

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering Program in Electrical Engineering
Department of Electrical Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2016

Thesis Title	MULTI-DOMAIN NETWORK DESIGN STRATEGY FOR SURVIVABLE LARGE-SCALE OPTICAL NETWORKS
By	Mr. Quynh Quang Le
Field of Study	Electrical Engineering
Thesis Advisor	Associate Professor Lunchakorn Wuttisittikulkij, Ph.D.
Thesis Co-Advisor	Associate Professor Poompat Saengudomlert, Ph.D.

Accepted by the Faculty of Engineering, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

.....Dean of the Faculty of Engineering
(Associate Professor Supot Teachavorasinskun, D.Eng.)

THESIS COMMITTEE

.....Chairman
(Professor Watit Benjapolakul, D.Eng.)

.....Thesis Advisor
(Associate Professor Lunchakorn Wuttisittikulkij, Ph.D.)

.....Thesis Co-Advisor
(Associate Professor Poompat Saengudomlert, Ph.D.)

.....Examiner
(Assistant Professor Chaiyachet Saivichit, Ph.D.)

.....External Examiner
(Pisit Vanichchanunt, Ph.D.)

กวน กวาง ลี : กลยุทธการออกแบบโครงข่ายหลายโดเมน สำหรับโครงข่ายนำแสงขนาดใหญ่ที่อยู่รอดได้ (MULTI-DOMAIN NETWORK DESIGN STRATEGY FOR SURVIVABLE LARGE-SCALE OPTICAL NETWORKS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ลัญฉกร วุฒิสิทธิกุลกิจ, อ.ที่ปรึกษาวิทยานิพนธ์ร่วม: ภูมิพัฒ แสงอุดมเลิศ, 92 หน้า.

วิทยานิพนธ์ฉบับนี้พิจารณาการแก้ปัญหาใหญ่ 2 ข้อในโครงข่ายใยแก้วนำแสงหลายโดเมนที่สามารถอยู่รอดได้ ได้แก่ ความเป็นส่วนตัวของโดเมน และการขยายขนาดของโครงข่าย โดยหลักการแล้ว เราสามารถปกปิดโทโพโลยีทางกายภายของโครงข่ายของแต่ละโดเมนจากโดเมนอื่น ๆ ได้โดยใช้แบบจำลองการควบรวมเพื่อสร้างเป็นโครงข่ายของโดเมนเสมือน ทำให้สามารถบรรลุตามวัตถุประสงค์ของความเป็นส่วนตัวได้ ในส่วนแรกของงานวิจัย เราพัฒนาแบบจำลองการควบรวมที่ดีขึ้นสำหรับการปกป้องแบบพี-ไซเคิลซึ่งรับประกันการปกป้องจากความเสียหายข่ายเชื่อมโยงเดียวทุกกรณีโดยให้ประสิทธิภาพที่ดีกว่าวิธีอื่น ๆ ที่มีอยู่ อีกทั้งได้สร้างสูตรโปรแกรมเชิงเส้นเลขจำนวนเต็มขึ้นเพื่อใช้จัดสรรทรัพยากรสำรองให้ได้ต้นทุนต่ำสุด ในส่วนที่สองของงานวิจัย เรานำเสนอแนววิธีการออกแบบโครงข่ายหลายโดเมนแบบใหม่ที่ใช้ในการปกป้องแบบเมชซึ่งสามารถใช้ประโยชน์จากความจุของข่ายเชื่อมโยงของโดเมนภายในและระหว่างโดเมนร่วมกันได้อย่างมีประสิทธิภาพ แนววิธีที่เสนอยังแบ่งขั้นตอนการออกแบบออกเป็น 3 ขั้นตอนอย่างเป็นระบบและเหมาะสม ซึ่งช่วยให้สามารถแก้ปัญหาโครงข่ายขนาดใหญ่ได้โดยใช้สูตรโปรแกรมเชิงเส้นเลขจำนวนเต็มที่พัฒนาขึ้นเมื่อเทียบกับการออกแบบในรูปของโครงข่ายโดเมนเดียว จากนั้นนำเสนอตัวอย่างการออกแบบโครงข่ายในทางปฏิบัติเพื่อแสดงให้เห็นถึงประสิทธิภาพของเทคนิคที่เสนอทั้งมิติของความจุสำรองและเวลาประวิง

ภาควิชา	วิศวกรรมไฟฟ้า	ลายมือชื่อนิสิต .....
สาขาวิชา	วิศวกรรมไฟฟ้า	ลายมือชื่อ อ.ที่ปรึกษาหลัก .....
ปีการศึกษา	2559	ลายมือชื่อ อ.ที่ปรึกษาร่วม .....

5870286821 : MAJOR ELECTRICAL ENGINEERING
KEYWORDS: OPTICAL NETWORKS / SURVIVABILITY / MULTI-DOMAINS / PROTECTION / OPTIMIZATION.

QUYNH QUANG LE: MULTI-DOMAIN NETWORK DESIGN STRATEGY FOR SURVIVABLE LARGE-SCALE OPTICAL NETWORKS. ADVISOR: ASSOC. PROF. LUNCHAKORN WUTTISITTIKULKIJ, Ph.D., CO-ADVISOR: ASSOC. PROF. POOMPAT SAENGUDOMLERT, Ph.D., 92 pp.

This thesis addresses two main issues of survivable multi-domain large-scale optical networks, namely domain privacy and scalability. In principle, the physical network topology of each domain can be hidden from other domains by using an aggregation model to form a network of virtual domains, thereby satisfying domain privacy requirement. First, we develop an improved aggregation model for p-cycle protection that ensures full protection against all single link failures and is more efficient than existing models. To optimize for the spare capacity requirement, Integer Linear Programming (ILP) formulations are derived. Second, we propose a new approach for multi-domain network design using shared-mesh protection where the backup capacity of intra-domain and inter-domain links can be shared more effectively. The proposed approach also provides a three-step systematic design and optimization, which allows our proposed ILP formulation to resolve larger network problems compared to single-domain network design approach. Several practical network design examples are given to illustrate the effectiveness of our proposed technique with respect to spare capacity requirement and network latency.

Department:	Electrical Engineering	Student's Signature .....
Field of Study:	Electrical Engineering	Advisor's Signature .....
Academic Year:	2016	Co-Advisor's Signature .....

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere and earnest gratitude to my supervisor Professor (Associate) Lunchakorn Wuttisittikulkij, Ph.D for his continuous support and guidance. I appreciate the time he put into the discussion on my thesis work and his numerous helpful suggestions and encouragement during the past two years.

I also would like to thank Professor (Associate) Poompat Saengudomlert for being my co-advisor. He has offered much advice and insight throughout my work.

Besides, I am grateful to all members of my thesis committee for their prompt evaluation and comments.

I also gratefully acknowledge the funding received towards my thesis from AUN/SEED-Net.

Last but not least, I am indebted to my dear parents who support me with the unconditional encouragement and love. This thesis would not have been possible without their support and encouragement.

CONTENTS

Page

Page

Page

Page

List of figures

List of tables

CHAPTER 1: INTRODUCTION

In the previous couple of decades, there has been massive enlargement in traffic demand, especially over the Internet. Such a growth is expected to continue with emerging services and applications such as IoT, sensor and machine-driven traffic, cloud computing, virtual reality, combined with live streaming video and mobile traffic. To meet with the next generation network capable of connecting human, machines and everything together over large-scale worldwide telecommunications, fiber-optic broadband is now seen as the most relevant technology because it can transmit ultrahigh speed data over extremely long distances due to broad bandwidth and low transmission attenuation provided by optical fibers.

As the network capacity increases than ever before, the need for protection against the certain types of failures become even greater. Single link failures, in particular, are most common in practical broadband networks and always lead to service interruption, causing huge loss of revenues both customers and operators. Therefore, many researchers and commercial network companies pay more attention to optical network survivability.

Most results in the field of resilient systems design are committed to the single-domain survivability, in which each network node has a complete vision of the global network information [1]. Such a supposition, in any case, is not practical on account of expansive networks, for example, multi-domain networks because different domains may not share full network information [2]. To conquer this issue, one of the solutions is forming the backup paths for each domain independently. In addition, even when the network of interest is single-domain, the benefits of partitioning a network into a number of domains are simplifying and speeding up the construction of the backup structures. Moreover, each domain can be viewed as an autonomous system, which is able to self-operate with its own network operator and administrative policies.

1.1 Motivations

Nowadays, Wavelength Division Multiplexing (WDM) network is a compelling technology to serve as the backbone for Wide Area Network (WAN), because the growth in the population of Internet users and a number of applications have been creating a growing demand for bandwidth. Additionally, the scale of transport network soon goes beyond the limit of a territory and covers the whole continent or even the entire world. When it comes to conventional network protection schemes, which are known to require sophisticated control to fully exploit the underlying network topology, the restorability of the whole network is performed as a solitary domain. This might be not computable when simulation capability does not meet the excessive size of the network, such as when the number of nodes increases up to hundred causing the complexity of optimization problem grows exponentially. Therefore, one contribution of this thesis is to evaluate the potential benefit of exploiting multi-domain networks in terms of reducing the computational time, the trade-off aspect between spare capacity cost and solution complexity of single domain protection and multi-domain protection is considered.

On the other hand, due to domain administrative policies, each node tends to keep the internal information within its domain rather than externally share this information with other nodes [3]. Subsequently, it is impossible for one node to completely observe all routing information of an entire network in the multi-domain network scenario.

In general, there are many different ways to approach a survivability issue of a multi-domain network. Each type has its own advantages and disadvantages in terms of availability, needed backup resources or recovery time. However, these proposed solutions can be categorized into two classes. In the first class, whenever a demand is assigned to a pair of source and destination nodes, two link-disjoint paths (primary path and backup path) are formed. The disadvantage of this approach is that it requires an extremely long recovery time. This is the result of routing backup traffic across the entire network. Besides, since two end nodes which are responsible for network survivability against failures by performing switching operations are supposed

to know the failure location along the primary path, it is natural to have signaling extension in order to notify failure event to each and every node on the primary path. Along these lines, this protection class requires a substantial number of resource management operations and is not considered commercially as an attractive solution, especially when the domains belong to competitive operators [2]. In the second class of solutions, each working path is regarded as a set of segments of working path, in which each segment is taken care of by the corresponding domain that holds it. Subsequently, the entire light-path is protected. This approach is rather scalable since each network operator has fully control on protecting its intra-domain links. In other words, intra-domain links are protected independently from the links of the other domains in order to maintain domain independence. However, the downside of this protection approach is that the survivability of inter-domain links connecting one domain with another is not secured by any domain. In order to overcome the obstacles mentioned above, the contribution of this thesis is proposing two different protection scenarios for multi-domain networks. The first scenario is developed based on the idea of hiding physical topology of a domain through a virtual domain, which is also known as domain aggregation. For failure recovery, p-cycle protection method is applied. On the other hand, the second scenario makes use of the shared-mesh protection technique to handle network survivability. In each scenario, the above problem is tackled differently while providing network survivability to both intra-domain links and inter-domain links.

1.2 Problem statement

This thesis focuses on providing a strategy for optical transport multi-domain network design problems. The solution can be divided into two scenarios: The first scenario is improving an aggregation model in order to achieve higher performance in terms of saving backup resources by using p-cycle protection. Our second scenario is addressing the survivability of multi-domain optical networks with link-based shared mesh protection by new proposed strategies. It is noticed that both scenarios are designed to provide protection against single-link failures when a multi-domain network is predefined.

1.3 Scope and objective

The issue of designing a protection strategy for large-scale backbone optical networks that connect data centers of different countries together is drawing the attention of researchers because it is highly complicated and an optimal solution may not be achieved with Integer Linear Programing (ILP) formulation. Moreover, optimizing networks that can handle all single-link failure events is also important in the modern broadband networks. In this thesis, we develop a design strategy based on a multi-domain techniques to achieve efficient routing and protection schemes with full spare capacity allocated. This involves two scenarios. First is when the existing aggregation model does not provide a sufficient set of the virtual domain to perform protection techniques, especially p-cycle protection technique. For example, it would be very useful if the number of working capacity for proposed aggregation model is smaller than the number of working capacity for the conventional model. Because saving backup resources is one of the most interests that concerns both vendors from service providing side and operators from the customer side. In this case, traffic that located on inter-domain links is globally protected through an entire virtual network consisting of virtual domains without considering the scalability or in other words, backup paths of inter-domain links can be routed through the entire virtual network. The protection for un-aggregated working capacity in each domain is performed separately. We develop the proposed aggregation technique using ILP approach since domain size is computable for simulation. Another setup is when aggregation stage is left for well-known existing techniques, then all working traffic on inter-domain links are protected using shared mesh protection technique. Two different strategies for re-using spare capacity to protect intra-domain links are introduced along with sets of corresponding ILP formulations.

In general, we apply proposed protection strategies to allocate spare capacity to each link based on two known fundamental techniques: p-cycle protection which provides fast recovery time but relatively inefficient of resource allocation and mesh protection which is known as most efficient in saving spare capacity but require signaling in order to acknowledge failure event. The new strategies deal with the

survivability of both intra-domain and inter-domain links and also is able to accomplish the cost-effective object.

The objective of this thesis is to design and optimize large-scale optical networks with full protection against all single-link failure using multi-domain networks.

CHAPTER 2: BACKGROUND AND LITERATURE REVIEW

2.1 Benefit and history of optical network

During the long history of the world, humanity was obsessed with its central concept of long-distance communication. The history of telecommunications is the story of evolution, which has created various kinds of transmission types as well as respective devices (see Fig. 2.1). The essential enthusiasm behind each new one was either to enhance the transmission technique in order to boost the transmission rate or to expand the transmission distance between transmitters to receivers.

Some 40,000 years ago, the earliest method of relaying messages consisted of smoke signals about the early Greeks use of fire. At that time and following decades, only one type of signal was used in transmission and the message contents were established beforehand between the sender and the receiver. Electricity has changed everything. In 1838 Samuel F.B Morse and his colleagues created the Telegraph which relayed electrical impulses Morse code – the descendant of those early smoke signals over wires [4]. Soon, those wires extended across the country and even under the ocean. In electrical systems, data is first converted into electronic signal form and then transferred from transmitter to a receiver through a channel by a carrier (in this case, the channel was electromagnetic waves). At the destination, desired information is filtered from the carrier wave and sent to next stage for further processing. Since the transmission frequency of carrier wave decides how large the system capacity is, an effective solution for improving transmission bandwidth is to increase the frequency of carrier wave. Therefore, the developing direction of the electrical communication system was to improve the bandwidth by utilizing higher frequencies so that the throughput of the system was significantly enhanced.

Figure 2.1: The evolution of telecommunication [5].

In 1960, the invention of the laser created many changes in optical frequency industry because of its very high-frequency feature. Although the transmission capability of the coherent optical system was demonstrated by many experiments in the years of 1960s, there still was a huge barrier between laboratory and commercial industry at that time because of the tremendous cost of required components [6].

Needless to say, the incredible growths of optical waveguide and semiconductor technology play an important role in the optical fiber industry. Therefore, nowadays, the optical transmission system is progressively replacing the conventional copper system especially in backbone network which requires large bandwidth and low loss. The advantages of fiber optics are described as following:

- *Bandwidth*: When it comes to bandwidth, fiber-optic cables give you more bandwidth than copper cables meaning that we can carry more information at faster speed and over longer distances than copper cables.

- *Loss*: Fiber-optic cables do not attenuate the signal the way copper cables do because the light signal does not interfere with other fiber in the same cable so that we can get clearer conversations. Moreover, fiber-optic cables are safe from lightning strikes or electrical interferences. All of this means that the quality of communication is at its highest when using fiber-optic cables.

- *Size and weight*: There are also height and weight differences between fiber and copper wires since fiber cable has a section smaller than a copper cable. In fact, a duplex fiber optic cable has a size that is fifteen percent less than a

copper cable. Imagine that if we utilize splitters through any form of wave division multiplexing than the size benefit of fiber optic cable multiplied enormously. This reduction in size is in parallel with the reduction in weight.

- *Signal security*: In terms of security fiber-optic cables are undetectable, unlike a copper cable which can be detected. Additionally, due to the fact that light signal used in fiber-optic cables do not emit electromagnetic radiation and cannot be intercepted without being detected.

- *Environmental friendliness*: Fiber-optic cables are also better for environment or greener because fibers are made from glass which comes from sand and is therefore non-intrusive manufacturers compared to copper which is mined and available in reducing quantities.

- *Cost*: Fiber-optic cables being installed for considerably longer periods of time are up to as much as three to five times longer as compared to copper there is a far lower lifetime installation cost.

2.2 Optical network standards

When we talk about optical networks, we are really talking about two generations of optical networks. In the first generation, optics was essentially used for transmission and simply to provide capacity. All the switching and other intelligent network functions were handled by electronics. Two examples of the early generation optical network are SONET (Synchronous Optical Network) and SDH (Synchronous Digital Hierarchy) networks, which form the core of the telecommunications infrastructure in North America and in Europe and Asia, respectively [4].

Second-generation optical networks have routing, switching, and intelligence in the optical layer.

2.2.1 SONET/SDH

Before describing SONET and SDH, we should acknowledge the previous existing technology which is Plesiochronous Digital Hierarchy (PDH). PDH was a widely

accepted standard in terms of multiplexing digital voice circuits. The following table expresses the benefit of SONET/SDH compared with PDH.

Table 2.1: The comparison between SONET/SDH and PDH.

	SONET/SDH	PDH
Multiplexing simplification	Simple	Difficult
Management	Complete	Mostly lacking
Interoperability	Consistent	No typical
Network availability	Faster	Slower

Due to the dramatic growth in traffic demand, it was inadequate settlement transmitting data on separate single fiber. While it is possible to use multiple fibers each as a single channel, Wavelength Division Multiplexing (WDM) technologies provide a more comprehensive solution for the problem of saving component expense. WDM refers to the ability to take multiple channels or frequencies and place them on the same fiber. This is a technology that is been very mature in large-scale carrier environments, especially in a long-haul connection where you have many different channels going across a single fiber. Each band is usually called a wavelength channel or simply a wavelength as demonstrated in Fig. 2.2. Thus, in our light-rail connection, not only do we have multiple fibers in each one of these cables, we also carry multiple channels of lights per fiber that is what gives us two different properties: one is the ability to carry much more capacity as much as 10Gbps or 40Gbps or even 100Gbps. Likewise, it also gives us the ability to selectively add and drop capacity from one of these individual fibers as you pass through switches through the topology.

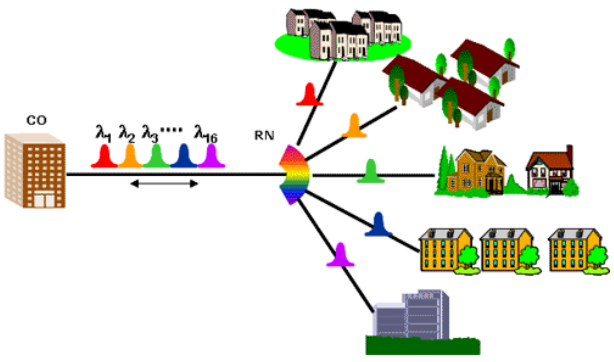


Figure 2.2: WDM network architecture [7].

It is noticed that in SONET/SDH or any system deploying in practice, dedicated transmission techniques or point-to-point transmissions are commonly used as an optical architecture. All switches in the system are simply electronic switches which contain many Optical-Electronic converters and Electronic-Optical converters. Node architecture in such WDM network is shown in Fig. 2.3 and referred to as the electronic switching node architecture.

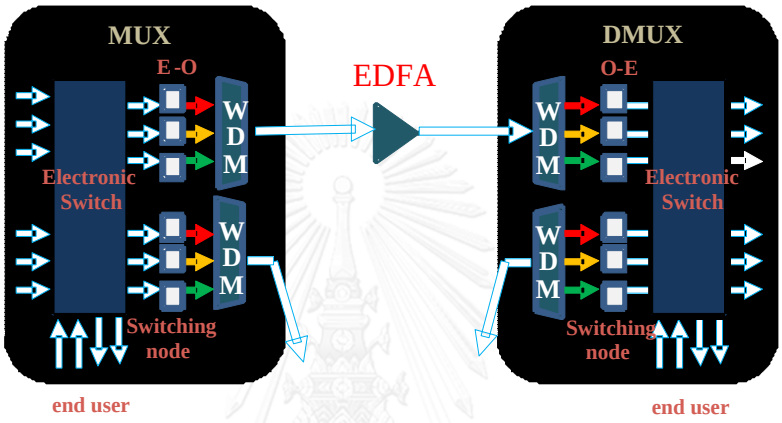


Figure 2.3: Electronic switching node architecture.

A major problem with the electronic switching architecture shown in Fig. 2.3 is that, as the traffic amount increases, the speed of electronic switching does not meet the demand of handling the incoming traffic to the switch [8]. This insufficient electronic switching speed is referred to as the electronic bottleneck.

2.2.2 All-optical networks

To help alleviate the electronic bottleneck, optical switches can be used in conjunction with electronic switches, as illustrated in Fig. 2.4. We shall refer to the node architecture as the opaque optical switching node architecture. It is important to note that this architecture allows some traffic to pass through or bypass electronic switches, yielding a lower required amount of electronic switches resources in the network.

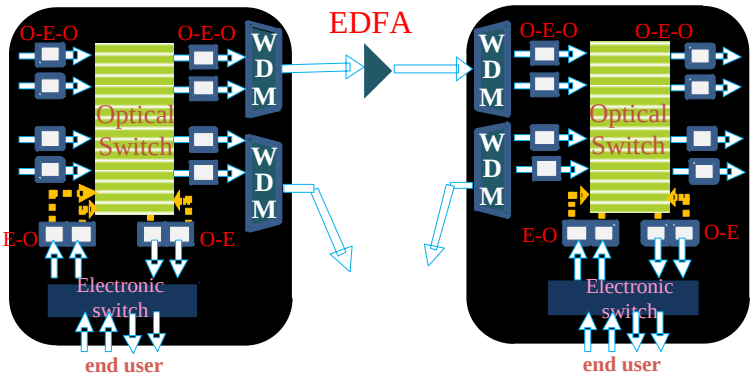


Figure 2.4: Opaque optical switching node architecture.

First, notice that, with a lot of input fibers, the opaque optical switching architecture needs a lot of Optical-Electronic-Optical (O-E-O) conversion units that can be expensive. Second, the number of ports of the optical switch in the opaque optical switching architecture can be large, leading to an expensive switch implementation.

Fig. 2.5 shows an alternative architecture that overcomes the two potential difficulties. We shall refer to the architecture in Fig. 2.5 as the transparent optical switching architecture. The transparent optical switching architecture seems to be inflexible compared to the opaque optical switching architecture. In particular, for traffic that bypasses transparent optical switching at the node, a traffic stream that enters on a certain wavelength must leave on the same wavelength. This characteristic of the switch is related to the wavelength continuity constraint which is exceptional for optical networks.

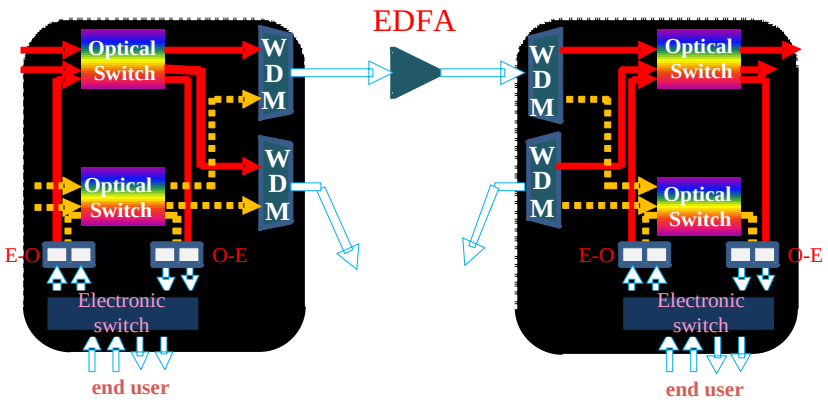


Figure 2.5: Transparent optical switching node architecture.

2.3 Network survivability

Transmission networks with high data rate require a sufficient survivable mechanism against corruptions. The effect of failure ends up noticeably serious, especially with the high-capacity systems. Revenue damage and business interruption are frequently considered as biggest concerns of the priority list. For instance, in 2004, a research company lost $100,000 USD/second and faced bankrupting risk since its operation harshly depends on the conditions of over 700 online services simultaneously [4]. On the other hand, there is always a quality agreement between service providers and its customer, such that the connection is supposed to be available 99.999% of the time, or the unconnected time have to be kept lower than 5 minutes per year [6].

Table 2.2: A comparison between protection and restoration.

Protection	**Restoration**
Traffics restored in ten to hundreds of milliseconds	Traffics restored in slower time scale
Reserving backup resources in advance so they may not be used	Discovering spare backup resources after the failure happens
Backup routes are predetermined	Backup routes can be dynamically computed
Inefficient use of resources	High resource efficiency

It stands to reason that data information from one source to destination traverse through many intermediate nodes and the connection can be corrupted for many different causes. For example, one of the most popular sources is human factors. Nature disasters are also considered as an enemy of transmission infrastructures. Moreover, although the locating and repairing jobs are not theoretically difficult, they require time and human resources since cables might locate under the ocean. Therefore, in order to satisfy 99.999% availability of signal transmission, a new feature called survivability need to be introduced into the networks so that services are still kept active while failure happens. Survivability can be roughly understood that extra capacity is provided within the network for rerouting traffic around the failure through

candidate backup structures. There are two subsets of survivability: protection and restoration. Table 2.2 presents the differences between these two subsets.

We can perform network survivability within a particular layer of the networks (see Fig. 2.6). First, one possible option is performing survivability on physical layer or layer 1 which contains the SONET/SDH, Optical Transport Network (OTN), and the optical layers. The second option is link layer or layer 2 which includes the SONET/SDH, Optical Transport Network (OTN), and the optical layers. Lastly, in the network layer, or layer 3, for example, the IP layer, protection also can be implemented.

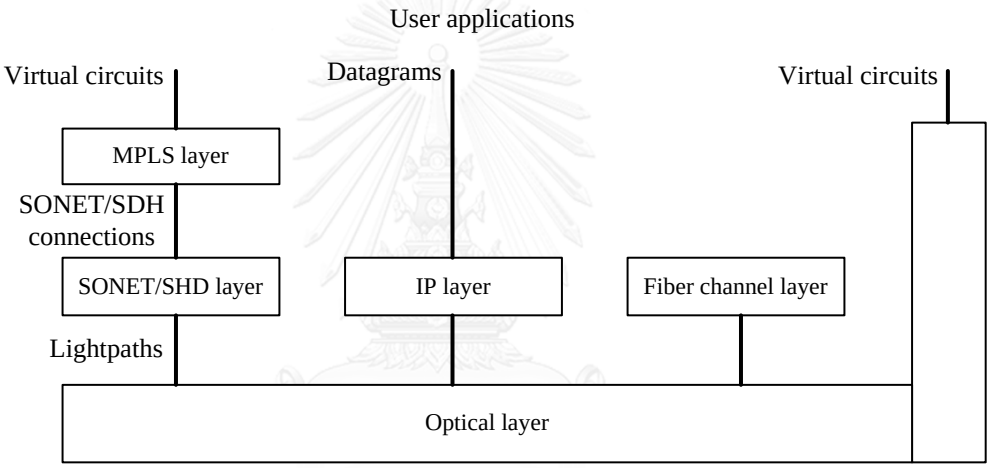


Figure 2.6: Optical network layer [6].

Different protection schemes function at different layers in the network (for example, SONET/SDH, MPLS, IP, and Ethernet) and at different sub-layers within a layer.

The optical light-paths are provided for use by its client layers, such as the SONET, IP, and Ethernet. These layers were designed to work independently for each other and not rely on protection mechanisms available in other layers. There are some reasons that raise the strong need for protection in the optical layer, despite the existence of protection mechanisms in the client layers:

- Huge cost reserving can be acknowledged by making utilization of optical layer protection rather than client layer protection. For instance, the conventional way to protect a light-path – a path from source node to destination node in optical domain in which there is no presence of optical-

electronic-optical conversion in the intermediate media between source and destination is using either SONET or IP layer. Clearly, with given condition, it is impossible for SONET and IP routers to share a wavelength. In the other hand, optical layer avoids the individual 1+1 protection scheme so that increase the chance of saving extra backup resources.

- From the view of an optical layer, it is more efficient to address network faults rather than solving them under client layer role. The reason is that, with the optical layer, when failure happens, there are much fewer components have to be involved in rerouting process compared with client layer protection.
- A drawback of using SONET protection is that in this layer, the restorable capability is limited in supporting single network corruption. However, this sometimes causes difficulty for the service provider, especially when another link fails before previously failed link gets reparation. In order to overcome this problem, optical layer offers multiple failures protection features.
- Last but not least, spare capacity efficiency is an advantage of the optical layer because of various kinds of protection techniques. One of the most popular techniques is mesh protection, which is known as the most efficient solution for optical network protection.

2.4 Optical layer protection

Actually, in the client layer, there are several protocols (SONET/SDH, IP, Ethernet, etc) that are operating simultaneously. It is natural to have a common platform in the optical layer to carry all possible protocol combinations. This also is the main reason why WDM optical layer was defined as a standard of circuit-switching oriented multi-protocol transport level. This layer is in charge of providing sufficient connectivity as well as transmission bandwidth for electronic layers in a client-server relationship as shown in Fig. 2.7.

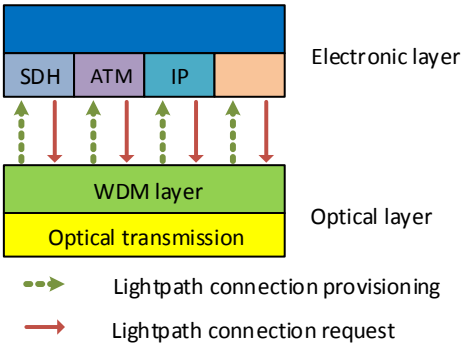


Figure 2.7: Light-path provision: a client-server relationship in a multi-protocol environment [9].

A light-path is formed by connecting a pair of source and destination node of an optical network by preserving a set of continuing WDM channels. Each light-path carries a high bit rate digital stream. It is added and dropped by electro-optical devices interfacing the WDM layer to the higher electronic layers and it is transparently switched by each WDM switching device it crosses its path. Based on the performing component types when rerouting process is required, we can categorize WDM switching into optical add-drop multiplexers (OADMs) or optical cross-connects (OXCs) according to considered protection approaches (ring protection or mesh protection).

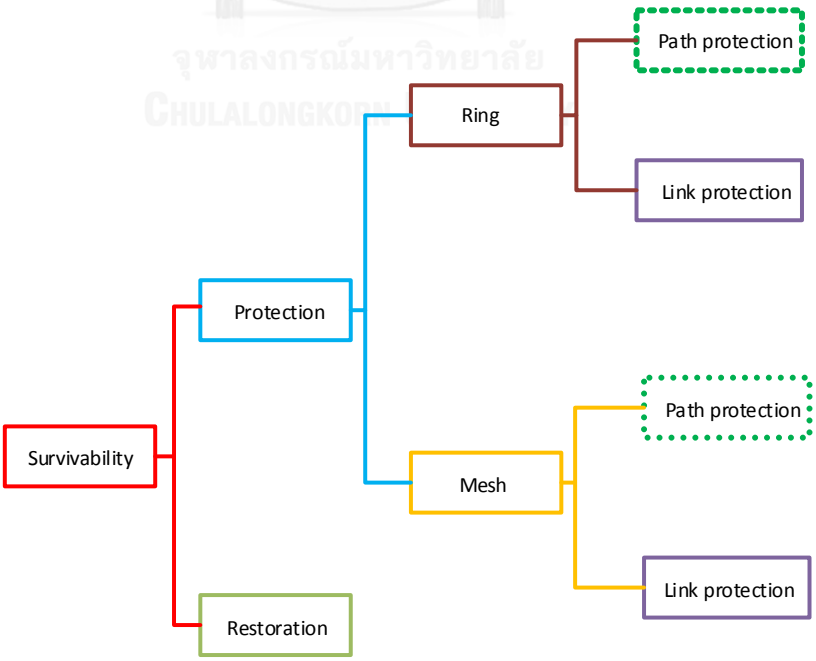


Figure 2.8: The survivability classification in WDM optical network [10].

Fig. 2.8 describes two main classes of network survivability which are protection and restoration. In the scope of this thesis, only protection class is studied since its advantage in recovery time. There are many different kinds of network topology that are commonly in different majors of engineering field, such as mesh topology, star topology, bus topology, ring topology and tree topology. However, not all of them can be used in WDM optical network, especially large WDM network or backbone network because of its capability of applying the technique to avoid interruption. Therefore, only ring network and mesh network are considered as two subsections belong to protection branch. It is noticed that in this thesis, only protection will be considered because of its advantages compared to restoration as explained in the previous section. As shown in Fig. 2.8, there are two sub-categories in each type of network: link protection and path protection. However, operation principles of these two protection techniques are different depending on which type of network (ring or mesh).

2.4.1 WDM ring network protection

A large number of WDM networks are based on ring topology since ring structure itself is simple and integrative with SONET/SDH standard [11]. One of the first contributions in protecting WDM ring network is proposed in [12] with the idea of protecting a network with only three nodes that are connected (this actually is path protection of WDM ring network that will be discussed later). Many authors have considered WDM ring architectures with link protection and path protection.

For 1+1 path protection, every connection in the network will be installed a pair of light-paths. The information signal is transmitted on both light-paths, therefore normally the receiver node can select the signal with the best quality. When a failure happens (see Fig. 2.9), there is no need of reconfiguring optical switch (or signaling) and the decisions still just depend on the receiver node. Recovery time is then very fast and total spare capacity is exactly equal total working capacity.

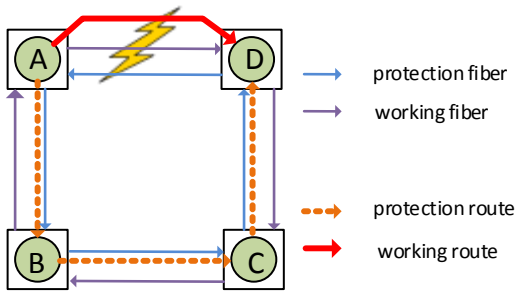


Figure 2.9: An example of dedicated protection ring when light-path AD corrupted [10].

For link based ring protection, protection switching is carried out by 2x2 optical switches in order to switch signal from one fiber to another. Fig. 2.10 shows two link protection schemes with 2-fiber (or 2 rings) and 4-fiber (or 4 rings), respectively. In a 2-fiber scheme, one fiber (a path) is working fiber and the other is backup fiber. At the transmitter, traffic is sent simultaneously on primary fiber in the clockwise direction and on the backup fiber in the counter-clockwise direction. On the other hand, in a 4-fiber scenario, the first pair of fibers (a line) is working fibers and the other pair of fibers is used for protection. In both cases, when a failure happens, these nodes on the loopback route need signaling to be identified. However, additional spare capacities are only 50% physical resources [10].

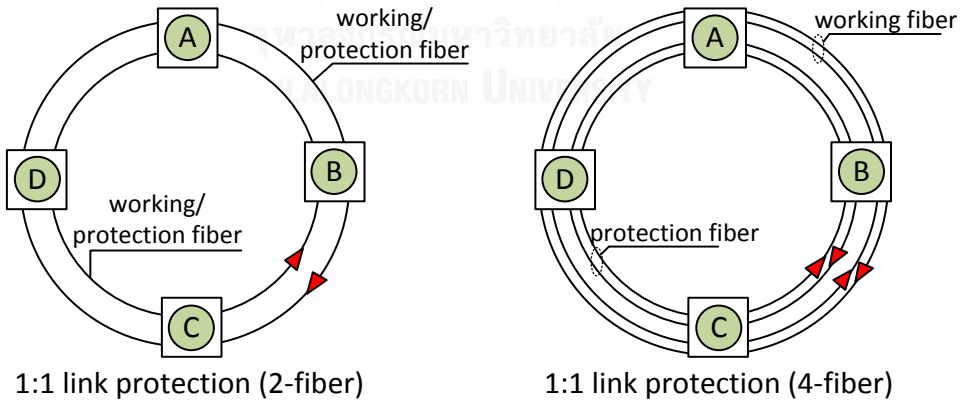


Figure 2.10: Link protection in ring network: 2-fiber link based ring protection and 4-fiber link based ring protection.

2.4.2 WDM Mesh Network Protection

Compared to Ring network structure, Mesh network structure seems to be less popular [10]. However, the technological advancements in optical transport switches

and an increasing number of DWDM – Dense Wavelength Division Multiplexing utilization enable the future infrastructure to have led telecommunications infrastructure to popularize mesh protection structure. Similar with ring network protection, there are path protection and link protection techniques for mesh network.

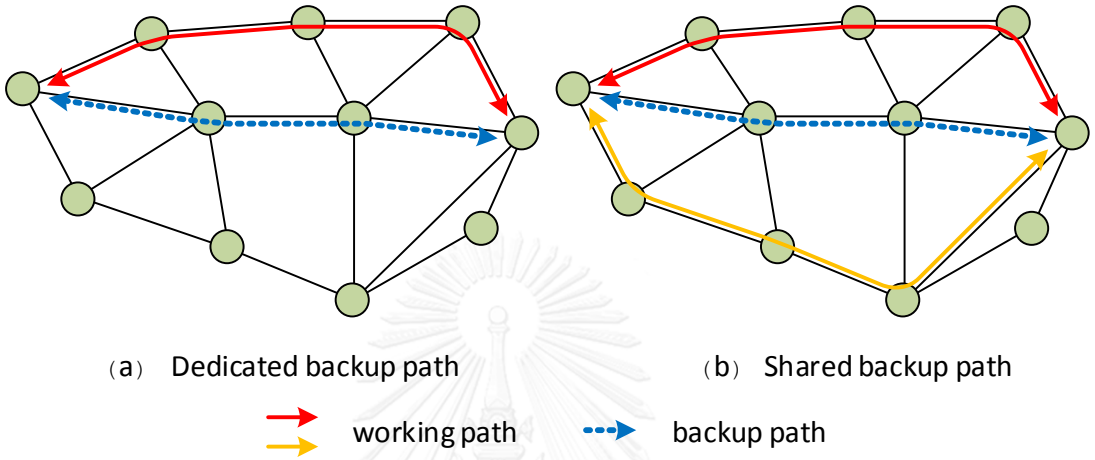


Figure 2.11: Path protection schemes in a mesh network.

Path protection requires the backup path of a request to be completely link-disjoint from the corresponding working route. In dedicated backup path scheme, data signal are sent on both primary and backup path simultaneously. On the other hand, under shared protection, a protection path can be used for other purposes when there is no failure on the primary path. Moreover, one backup path can serve several working paths since single link failure is one of the most common failure types (see Fig. 2.11).

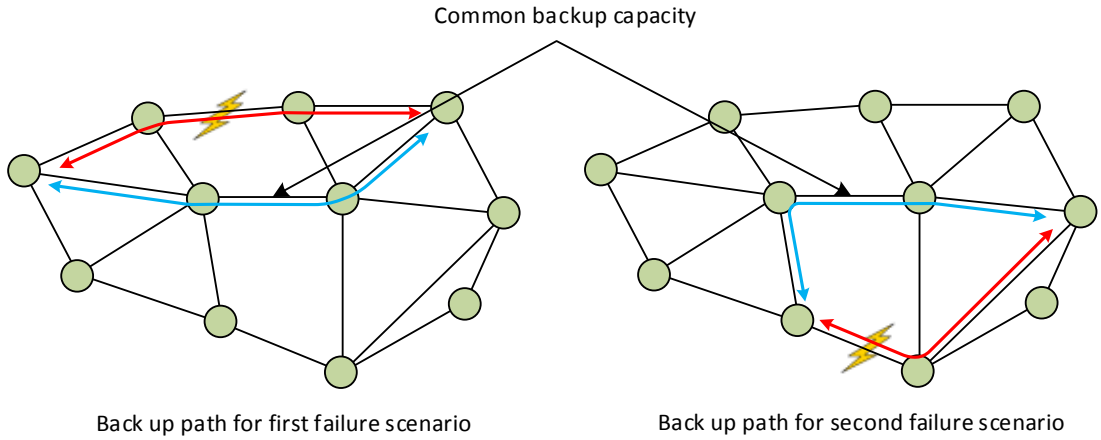


Figure 2.12: Shared backup link protection.

Last but not least, shared backup link protection offers the most efficient spare capacity since backup fibers are used for protection of multiple links. For example, Fig. 2.12 represents a network with two different link failure scenarios. The middle link of backup path in both scenarios is a common link so that backup capacity on that link can be shared to support when link failure happens.

2.5 Network protection in multiple domain networks

The problem of survivability in multi-domain networks can be solved in various ways depending on protection techniques and network topology information. Those solutions can be generally classified into two sub-problems. The first concern is how to protect each domain or the traffic that transmits within a particular area. The most popular answer for this question is to give each domain the capability to protect itself against any failure that occurs within that domain. It is clearly seen that by doing this, each domain or its owned operator can independently apply its management rules as well as quality service control for any failure event. At this point, we can choose to apply any existing protection techniques that were mentioned above to address the survivability of multi-domain optical networks. The second concern is protecting links that do not belong to any domain. The below section discusses some of the most common and effective approaches to view the multi-domain network survivability issue. The idea of each approach is described and analyzed in the simplest way in order to point out its advantages and disadvantages.

In [13], the authors consider a model in which every pair of domains are connected by exactly two inter-domain links, namely primary and secondary link. The primary serves as a backup link to provide capacities in case failure happens with either interval link (the link that belongs to a particular domain) or interval node (the node that belongs to a particular domain but is not on an inter-domain link). Meanwhile, the secondary link is reserved for protecting the primary link in case of failure happens. According to this approach, the protection process can be performed without sharing domain topology information as well as routing information. However, it spends significant resources for protection since each light-path is divided into several small segments then the protection responsibility of each is assigned to

a corresponding domain that it belongs to. Additionally, this approach requires domains to be connected to others by at least 2 inter-domain links that is not always possible in the real network.

In [14], a “sub-path protection” idea was proposed where each domain protects the segment that physically belongs to it. The authors also assume that domains communicate through border nodes without the presence of inter-domain links. This solution offers tolerable restorable time, but the assumption that inter-domain does not exist again is not practical since realistic multi-domain networks may violate that principle.

In [1] the protection strategy proceeds in two steps: firstly, the physical topology is transformed into virtual topology by aggregation technique so that primary light-paths and backup light-paths are assigned. Secondly, each domain performs intra-domain routing. Therefore, the capacity of each virtual link is mapped into a corresponding physical link. The benefit of this method is that its solution is near optimal. Nonetheless, the disadvantage of this approach is that the backup light-paths are allowed to be routed across the whole multi-domain network. Consequently, it takes longer for backup traffic to transmit to the destination. Moreover, every node on the primary light-path has to be noticed of any failure event’s location.

In [15] the authors have improved the idea in [1] by preparing a backup route for every segment of a light-path which corresponds to the shortest path within the same domain. This avoids the notification of failures to all nodes on the primary light-path. But this approach assumes that a link/segment in a domain has to be attached with one 1+1 protection link/segment. In the other words, there are more constraints on arranging primary and backup link/segment pairs or it is less flexible in solving the problem.

In [16] the authors assign the primary based on each virtual link cost instead of the shortest one in order to achieve a more efficient way of allocating light-path. The

result is more efficient than the idea in [15] but neither inter-domain links and border nodes are protected against failures.

To improve [1], [15] and [16], the authors in reference [17] form intra-domain primary sub-path by routing them over domains, while primary and backup sub-path of each domain are assigned locally. There is no domain aggregation process for this approach but routing information is still published within the domain. The disadvantage of this method is that the survivability of inter-domain links and border nodes are ignored by the authors. In addition, one node cannot have the knowledge of one the light-path whether is routed through which domain.

The proposed idea in [18] improves the drawback of not protecting inter-domain links and border node in [17] by computing another backup segment between domains for inter-domain link and border node protection purposes. This solution obtains acceptable recovery time since there is no need of informing every node on the light-path about failure. However, in term of saving resources, this approach is not efficient as the one in [1]

Most recently, in [19] the authors propose a pre-configured technique called p-cycle to protect inter-domain links. Basically, after getting the virtual network by applying aggregation, the authors allocate resources to provide 100% protection against single link (or inter-domain link). Then the virtual backup capacities are used to match with the physical topology survivability needs. This solution considers inter-domain links and border nodes as significant objects but we have to pay more to protect all working capacities on each intra-domain link. Another drawback is that the solution does not reveal the exact cost of a p-cycle on the specific physical topology since one domain with multiple links and node are now presented by only one single virtual node.

In general, the scalability concern in multi-domain networks is handled by either computing a pair of link-disjoint paths from source to destination node or protecting each segment of the primary light-path by its domain resources. However, the inter-domain link routing processes of both approaches require network aggregation in

order to avoid sharing routing information from one domain to another [20] provides an overview of three aggregation methods: Single Node (or Simple Node) aggregation, Star aggregation, and Full Mesh aggregation (see figure 2.13).

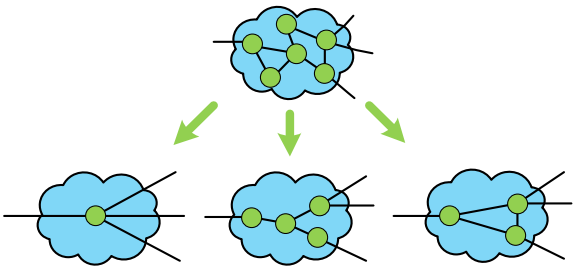


Figure 2.13: Single node (left), Star (center) and full-mesh (right) aggregation concepts.

Single node aggregation: The idea of this model is replacing the completed topology with multiple links and node by only one single node and these presented nodes are connected as in physical topology. Simple node aggregation model delivers the simplest virtual topology.

Star aggregation: The idea of this model is using a central node and all border nodes to aggregate physical topology so that its inter-domain connections remain. Virtual links are used to represent intra-domain links. All border nodes have to be connected to the central node. This model has higher complexity than single node aggregation model but lower than full-mesh aggregation model.

Full-mesh aggregation: The idea of this model is trying to preserve as much the information of physical topology as possible. Instead of having the central node, full-mesh aggregation model is formed by a set of all border nodes and the virtual links ensure those nodes are fully connected.

2.6 Integer linear programming (ILP) problems

In the previous section, we show that a set of selective elements in a real optical network can be used in mathematical optimization design problems. In order to solve the problem of multi-domain networks, these above elements are transformed into mathematical forms, such as parameters, notations, variables. Next, these materials are linked by a set of constraints which denotes the required relation between them. It is noticed that mathematical model is totally or partly different for

different network scenarios or complexity of the planning task. At this point, the optimization design problem becomes a linear optimization problem.

2.6.1 Definition of ILP problems

Before investigating on ILP, we should understand the concept of linear programming (LP) problems. The general form of a LP problem is given below.

$$\text{minimize } c^T x$$
$$\text{subject to } Ax \geq b$$

where x is set of decision variables, c is set of objective or cost coefficients, while b and A are sets of constraint coefficients.

$$x = \begin{bmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_N \end{bmatrix}, c = \begin{bmatrix} c_1 \\ \cdot \\ \cdot \\ \cdot \\ c_N \end{bmatrix}, b = \begin{bmatrix} b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_N \end{bmatrix}, A = \begin{bmatrix} a_{11} & \cdot & \cdot & \cdot & a_{1N} \\ \cdot & \cdot & & & \cdot \\ \cdot & & \cdot & & \cdot \\ \cdot & & & \cdot & \cdot \\ a_{M1} & \cdot & \cdot & \cdot & a_{MN} \end{bmatrix}$$

Note that the objective, as well as constraint functions, are linear functions of decision variables. Feasible solutions are found when all constraints are satisfied [21]. Among these feasible solutions, an optimal solution is the one that makes the objective function minimal.

The general form of an integer linear programming (ILP) problem is the extended version of LP problem, in which extra constraint is introduced as shown below.

$$\text{minimize } c^T x$$
$$\text{subject to } Ax \geq b$$
$$x \in \mathbb{Z}^N$$

2.6.2 Solving an ILP problem

An ILP problem is handled by one of these two algorithms: exact algorithms or heuristic algorithms. Exact algorithms can return the optimal solution of a feasibility ILP problem in a polynomial time when the number of variables is fixed. The most popular subset of exact algorithms is a set of cutting plan methods which solve LP

relaxation then adding linear constraints to obtain integer solution. Variants of the branch and bound methods belong to the second subset that has several advantages compared to cutting plane. For example, they can terminate earlier after an integer set of solution is found or they are able to estimate how far from the optimality point to current time.

On the other hand, heuristic algorithms are used if you are looking for a solution (may or may not be optimal solution) in an available time. Heuristic seems to be useful with the high complexity problems, however, if they could not return a solution, we have no clue to find out whether the reason is that the problem is infeasible or the algorithm is not good enough to find it.

In the scope of this thesis, I pick exact algorithms to work with because of the need for precise solutions in order to compare the performance between different protection techniques. ONO tool which is inspired by WDM Planner [22] and developed by our research group is a testing platform since it is using Pulp and GLPK supporting branch and cut method which is built by combining both branches and bound and cutting plane methods.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Modeling optical network design

In this section, we present an adequate set of concise objects relevant for network design because not every factor is mathematically considered in the optimization problems. Specifically, the modeling framework of optical network design is constructed from four subsequent sections: Hardware, capacities, connections, cost.

- Hardware: This module considers which physical hardware is necessary for describing the optimization problem. There are two most common and essential modules: fibers, switches.
- Capacities: The installed hardware offers the required functionalities to establish connections. These functionalities are quantified in terms of capacities to express the amount of traffic that a module can handle. There are several types of capacities corresponding to above hardware, such as transmission capacity and switching capacity.
- Connections: This module refers to paths in physical topology. Connections in the optical network may differ from different network types: opaque or transparent networks. In the scope of this thesis, the opaque network is used as a testing framework.
- Cost: The principal goal of an optimization problem is minimizing the total network cost. In particular architecture, selected costs are changed on purpose but an essential factor is fiber cost.

3.2 Solving optical network design

After getting a complete mathematical model, we need to select a suitable approach which makes solutions tractable but does not sacrifice too much solution quality since it is impossible to apply directly an exact approach to an optimization

problem with high complexity. The most well-known idea is divide-and-conquer which handles each stage of the problem gradually.

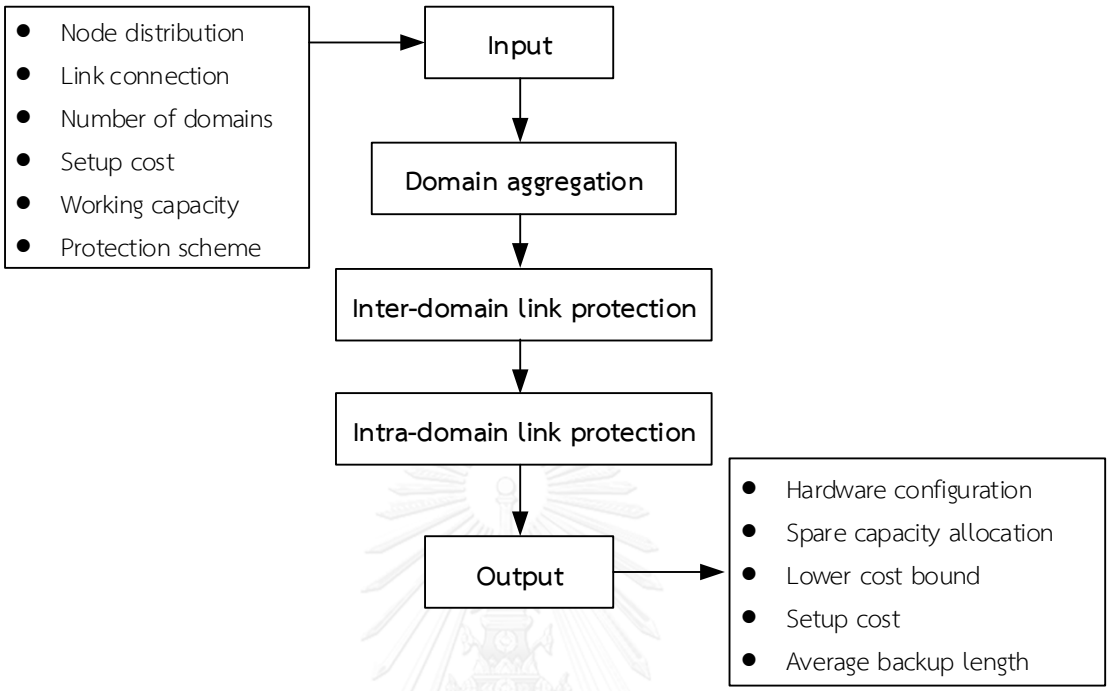


Figure 3.1: Solution method scheme.

Fig. 3.1 displays the scheme for solving the optical network design optimization in this thesis. First, input with given information of supply network (including node distribution, link connection), demand and so on is passed to a Pre-processing function of domain aggregation block. To simplify the simulation, link connection between nodes is assumed bi-directional so that working traffic demand is symmetric. The output of this block contains a new virtual topology together with capacity and cost information. Next blocks perform inter-domain and intra-domain link protection respectively. The results of inter-domain link protection block are used as the input for next stage in which backup resources can be recycled as long as the connectedness between border nodes is maintained. Because this work only considers opaque optical network, the final results are shown without wavelength assignment stage.

3.3 Mathematical models

In order to present all set of optimization models in a consistent manner, we introduce some notations for the models which are used through an entire section. A

multi-domain network included M connected domains can be denoted by graph G. The details of mathematical notations are shown as below.

M : set of connected domains of graph G D_i : set of intra-domain/physical links of domain i D' : set of virtual links of entire network I : set of inter-domain links of the multi-domain network. w_l : working capacity of link l c_l : cost of link l. Δ : large constant	
Section 3.3.1	B_i : set of border node pairs in the domain i $P(d)$: set of all paths connecting the pair of border nodes $d \in B_i$ C : set of candidate cycles
Section 3.3.2	D_i' : set of virtual links of domain i P_l : set of candidate backup routes of link l P_l^{ij} : set of candidate backup routes of link l, provided that every node of these routes either belongs to domain i or domain j. I_{ij} : set of inter-domain links between two domains i and j of the multi-domain network.

3.3.1 ILP formulation for p-cycle protection strategy

This section presents an improved aggregation model which is applied to transform physical links/intra-domain links into virtual links whose physical links are disjoint. Besides, p-cycle protection technique with link cost parameter is also introduced in order to optimize number of needed backup resources for inter-domain links and intra-domain links separately. The protection strategy can be summarized in a list of three steps as follows:

- In each domain, virtual links are formed by applying domain aggregation technique, which minimizes value of virtual capacity and remaining working capacity and satisfy following constraints:
  - Virtual link manages the connection of each pair of border nodes within domain. A virtual link relating a pair of border nodes matches to the set of working light-paths connecting these nodes in the physical topology.
  - Virtual links are physically disjointed. In other words, a light-path connecting a pair of border nodes is compulsory to be link disjointed from all other light-paths between any other node pairs.
- For inter-domain link and virtual domain link protection, backup capacities are assigned to inter-domain links and virtual domain links by applying p-cycle technique, assuming that link cost of virtual link is taken into account.
- For remaining intra-domain link protection, the working capacities that cannot be aggregated are protected using p-cycle technique within its domain.

a. Step 1: Domain aggregation

Parameters:

$$a_{l,d,p} = \begin{cases} 1, & \text{if light-path } p \text{ of border node pair } d \text{ crosses link } l \\ 0, & \text{otherwise} \end{cases}$$

Variables:

$Y_{l,d}$: an integer variable that takes the value of 1 if one of the light-paths connecting the border node pair d cross link l, otherwise, 0.

$h_{d,p}$: an integer variable that indicated the number of light-paths p connecting the pair of border node pair d

r_l : remaining working capacity on link l

The ILP problem is formulated for $\forall i \in M$ as below:

Objective function:

$$\text{minimize} \sum_{l \in D_i} r_l + \sum_{d \in B_i} \sum_{p \in P(d)} h_{d,p} \tag{3.1}$$

Subject to:

$$\forall l \in D_i : \sum_{d \in B_i} \sum_{p \in P(d)} a_{l,d,p} h_{d,p} \leq w_l \tag{3.2}$$

$$\forall l \in D_i : \sum_{d \in B_i} Y_{l,d} \leq 1 \tag{3.3}$$

$$\forall l \in D_i, \forall d \in B_i : \frac{1}{\Delta} \sum_{p \in P(d)} a_{l,d,p} h_{d,p} \leq Y_{l,d} \leq \Delta \sum_{p \in P(d)} a_{l,d,p} h_{d,p} \tag{3.4}$$

$$\forall l \in D_i : r_l = w_l - \sum_{d \in B_i} \sum_{p \in P(d)} a_{l,d,p} h_{d,p} \tag{3.5}$$

The ILP formulation determines the minimum value of virtual capacity and remaining working capacity of each domain $i \in M$ by objective function (3.1). Since both factors have a huge impact on the amount of needed backup resources, this summarizing objective function is expected to improve the efficiency of the problem. Constraint (3.2) ensures that the number of light-paths cross-link l should not exceed the number of working capacity on link l. Constraint (3.3) guarantees that the light-paths connecting virtual nodes are physically disjoint. Constraint (3.4) defines $Y_{l,d}$ that takes the value of 1 if at least one light-path of border node pair d crosses link l and 0, otherwise. Constraint (3.5) defines remaining working traffic which equals working capacity subtract by summation of virtual capacity on that link.

b. Step 2: Protecting inter-domain links and virtual domain links

Inter-domain links and virtual domain links are recovered from single link failure by applying the existing ILP formulation for p-cycle protection in [23]. The link cost parameter c_d of virtual links in each domain is presented to overcome the mentioned drawback in [3] and defined as:

$\forall i \in M, \forall d \in B_i, c_d = \sum_{l \in D_i} Y_{l,d}$ because physical link cost is assumped to be 1 unit.

Parameters:

wp_l: working capacity of virtual link and inter-domain link l

$\alpha_{l,j}$: takes the value of 1 if link l is on cycle j, otherwise, 0.

$x_{l,j}$: takes the value of 1 if link l in on cycle j, 2 if link l is a straddling link* of cycle j, otherwise, 0

(*straddling link - link has two end nodes are on the cycle but is not an on-cycle link)

Variables:

s_l : spare capacity on link l

n_j : number of cycle j that are used for protection

It is noticed that cost of link in this section refers to both sets of virtual links computed above and set of physical inter-domain links which have the unit cost.

Objective function:

$$\text{minimize}: \sum_{l \in D' \cup I} s_l c_l \tag{3.6}$$

Subject to:

$$\forall l \in D' \cup I: \; s_l = \sum_{j \in C} \alpha_{l,j} n_j \tag{3.7}$$

$$\forall l \in D' \cup I: \; wp_l \leq \sum_{j \in C} x_{l,j} n_j \tag{3.8}$$

The objective function is minimizing the total cost of spare capacity for backup. Constraint (3.7) relates the spare capacity on each link to cycles or p-cycles that protect the network. Constraint (3.8) specifies that all working traffic should be protected.

c. Step 3: Protecting remaining working capacity

The amount of working capacity in physical topology of each domain that cannot be aggregated by step 1 is again protected with the p-cycle approach in [23] which is similar to previous section except that w_l is replaced by r_l. The ILP formulation is applied for $\forall i \in M$. Each candidate protection cycle contains physical links within a single domain.

3.3.2 ILP formulation for shared mesh protection strategy

The protection strategy can be summarized in a list of three steps as follows:

- In each domain, virtual links are formed by applying conventional full mesh model for domain aggregation.
- After that, inter-domain links between domains are protected by either Global Shared Backup Mesh protection (GSBM) or Local Shared Backup Mesh protection (LSBM) approach. In this step, the number of working capacity on virtual link is assumed zero. There are two main differences between GSBM and LSBM. First, GSBM optimization problem considers all inter-domain links at once. However, in LSBM, inter-domain links of a domain pair are considered at the time. In other words, the number of ILP problems is equal to number of domain pair connected by inter-domain links. Secondly, GSBM can reroute its backup paths through entire protection topology (including inter-domain links and virtual links from domains), while LSBM limits its number of candidate backup path by accepting only paths, which traverse through domains, contained either end nodes of considered inter-domain links.
- Finally, intra-domain links are protected by either first group including GSBM and A-GSBM or second group including LSBM and A-LSBM. First group protects intra-domain links using candidate backup paths within its physical topology as well as paths traversed through other virtual domains and inter-domain links. Second group is less flexible since it uses only candidate backup paths within considered domain's physical topology and its neighbor virtual domains. It is noticed that neighbor virtual domains are domains that connects with considered domain via inter-domain links. Moreover, each group is categorized into two types: conventional one in which backup resources can only be installed on physical links of considered domain and the other one having prefix-A which emphasizes that extra spare capacity is allowed to deploy on inter-domain links and virtual domain links for protection.

a. Step 1: Domain aggregation

Aggregating physical domains into virtual domains by full mesh model [20]. The shortest physical path from one border node to another is represented by a corresponding virtual link. The cost of the virtual link l' on domain i can be calculated as follow:

$$\forall i \in M, \forall l' \in D_i', c_{l'} = \sum_{l \in S_{l'}} c_l \tag{3.9}$$

where $S_{l'}$ is a set of links on the shortest physical path of the virtual link l'.

b. Step 2: Protecting inter-domain links

The set of links in D' is taken from the previous step. However, numbers of working capacity of those links are equally zero in order to dedicate this step for inter-domain link protection.

Parameters:

$\alpha_{l,k}^{l'}$: take the value of 1 if link l' is on back up path k of link l, otherwise, 0.

$\beta_l^{l'}$: takes on the value of 1 if physical link l is on the shortest physical path represented by virtual link l', 0 otherwise.

Variables:

e_l : spare capacity on link l to protect inter-domain links

$x_{l,k}$: spare capacity on path k to back up link l

GSBM:

The ILP formulation is applied for network consisting of set of inter-domain links I and set of virtual links from every domain D'

Objective function:

minimize the cost of spare capacity for inter-domain link protection

$$\sum_{l \in D' \cup I} c_l e_l \tag{3.10}$$

Subject to:

$$\forall l \in D' \cup I: w_l = \sum_{k \in P_l} x_{l,k} \tag{3.11}$$

$$\forall l, l' \in D' \cup I,\ l \neq l': e_l \geq \sum_{k \in P_{l'}} x_{l',k} \alpha^{l}_{l',k} \tag{3.12}$$

This ILP formulation finds the minimum cost of the spare capacity on links by objective function (3.10) while satisfying two constraints. Constraint (3.11) ensures that enough backup paths were given to cover the amount of working capacity on a link of a network made of inter-domain links and virtual links. Constraint (3.12) warrants that the number of allocated spare capacity is greater or equal which actually used.

LSBM:

The ILP problem is formulated for $\forall i, j \in M$ and $I_{ij} \neq \varnothing$ as follow:

Objective function**:**

minimize the cost of spare capacity for inter-domain link protection

$$\sum_{l \in I_{ij} \cup D_i \cup D_j} c_l e_l \tag{3.13}$$

Subject to:

$$\forall l \in I_{ij} \cup D_i \cup D_j : w_l = \sum_{k \in P_l^{ij}} x_{l,k} \tag{3.14}$$

$$\forall l, l' \in I_{ij} \cup D_i \cup D_j,\ l \neq l': e_l \geq \sum_{k \in P_{l'}^{ij}} x_{l',k} \alpha^{l}_{l',k} \tag{3.15}$$

Even though the objective function and constraints of LSBM are similar to these of GSBM, the set of selective links in each approach is different because LSBM only takes the candidate routes from domains that contain either one of the two end nodes of inter-domain links. This fact can be clearly seen when comparing (3.11) with (3.14) or (3.12) with (3.115).

c. Step 3: Protecting intra-domain links

In this step, intra-domain links are protected with the advantage of having available backup resources from the previous step.

Parameters:

$\alpha_{l,k}^{l'}$: take the value of 1 if link l' is on back up path k of link l, otherwise, 0.

$\beta_{l}^{l'}$: takes on the value of 1 if physical link l is on the shortest physical path represented by virtual link l', 0 otherwise.

f_l : available spare capacity on intra-domain physical link, inter-domain link or virtual-domain link l

$$f_l = \begin{cases} e_l & \text{if } l \in I \cup D' \\ \sum_{l' \in D_i'} e_{l'} \beta_l^{l'} & \text{if } l \in D_i \end{cases}$$

Variables:

s_l : additional spare capacity on link l for intra-domain link protection

$x_{l,k}$: spare capacity on path k to back up link l

A-GSBM:

The ILP problem is formulated for $\forall i \in M$ as below:

Objective function:

minimize the additional cost of spare capacity for intra-domain link protection

$$\sum_{l \in D_i \cup I \cup (D'/D_i')} c_l s_l \tag{3.16}$$

Subject to:

$$\forall l \in D_i \cup I \cup (D' \setminus D_i') \; : \; w_l = \sum_{k \in P_l} x_{l,k} \tag{3.17}$$

$$\forall l, l' \in D_i \cup I \cup (D' \setminus D_i'),\; l \neq l' : \; s_l + f_l \geq \sum_{k \in P_{l'}} x_{l',k} \alpha_{l',k}^{l} \tag{3.18}$$

Constraint (3.17) is similar with constraints (3.11) and (3.14) except that one physical topology of a domain is now considered together with other virtual domains. Constraint (3.18) is modified from (3.12) and (3.15) in which spare capacity from step 2 can be reused.

GSBM:

In order to avoid adding extra spare capacity on inter-domain links as well as virtual links of other domains, constraint (3.19) is introduced as below:

$$\forall l \in I \cup (D' \setminus D'_i): s_l = 0 \tag{3.19}$$

A-LSBM:

The ILP problem is formulated for $\forall i \in M$. For convenience, we define set $I_i = \bigcup_{j:I_{ij} \neq \emptyset} (I_{ij} \cup D'_j)$

Objective function**:**

minimize the additional cost of spare capacity for intra-domain link protection:

$$\sum_{l \in D_i \cup I_i} c_l s_l \tag{3.20}$$

Subject to:

$$\forall l \in D_i \cup I_i : w_l = \sum_{k \in P_l} x_{l,k} \tag{3.21}$$

$$\forall l,l' \in D_i \cup I_i,\ l \neq l': s_l + f_l \geq \sum_{k \in P_{l'}} x_{l',k} \alpha^{l'}_{k,l} \tag{3.22}$$

The set of constraints for A-LSBM is modified from the set of constraints for A-GSBM (constraints 3.17-3.18) with the candidate routes are limited within the domain and its adjacent domains.

LSBM:

An additional constraint for LSBM is similar with the additional constraint for GSBM in (3.19):

$$\forall l \in I_i, s_l = 0 \tag{3.23}$$

3.4 Testing and results analysis

3.4.1 Network topologies

We use the set of two realistic network topologies with different sizes and number of domains as shown in Fig. 4.2. The first one is Tnet, a fair compromise between realistic and regular networks has seven domains and 111 nodes [19]. The second

one is LARGE-5 constructed from five different realistic topologies: EON, RedIris, Garr, Renater and SURFnet with 97 nodes and 162 links [1].

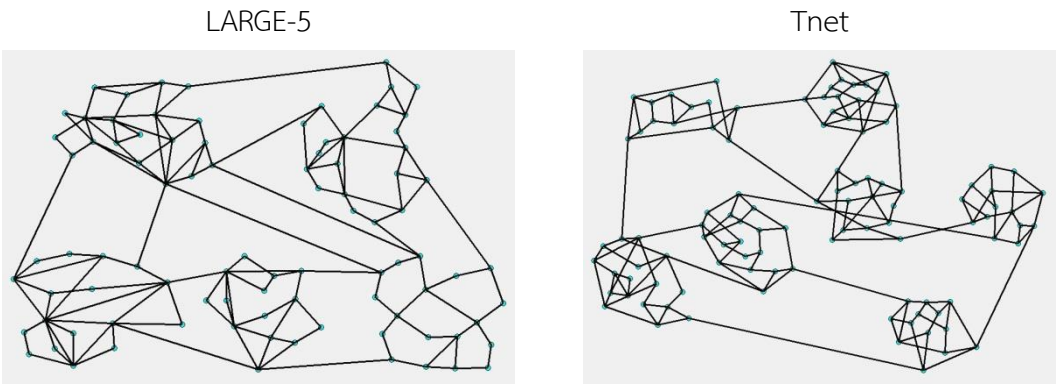


Figure 3.2: LARGE-5 and Tnet topologies.

3.4.2 Demands and survivability requirements

Each topology comes with a random integer number working capacity in the range of [1, 50] units on every link. The reason of assigning working capacity instead of doing routing assignment problem is because routing can be done using various existing techniques, such as k-shortest paths or even minimizing resources optimization problems, etc. However, this thesis focuses on the performance of protection techniques against link failure in multi-domain networks. Therefore, performing routing assignment can be neglected to reduce the working load as well as the complexity of optimization problems while keeping the accuracy of results. The ILP problems must ensure 100% restorability of the network against any single inter-domain or intra-domain link failure.

3.4.3 Hardware model

At each node, we assume that operators equip sufficient switches so that any demand for rerouting traffic can be satisfied. Additionally, the opaque network architecture is applied and the connection between two nodes is bidirectional with the same cost of 1.

3.4.4 Computing environment

For the study, all computations have been carried out on Windows-operated PC with a 3.2 GHz processor and 4 GB main memory. The described methods are

implemented in Python with some mentioned packages: Pulp [7], GLPK [22], Tkinter [24], etc.

3.4.5 Results analysis

The efficiency of a protection technique is evaluated through the amount of additional spare capacity required for survivability because resources always is one of the biggest concerns from operators and vendors as well. Besides, the average length of backup paths is also investigated in order to measure the network latency when a switch accesses the backup resources.

3.5 Limitations of study

This section presents the limitations of the study which could cause difficulties or deviation in comparison. Firstly, choosing exact algorithms to solve ILP problems increases the computational time although we try to reduce the number of variables and parameters. Secondly, working capacity of a link is static and randomly assigned from a fixed non-zero range [1, 50]. This may not realistically accurate since traffic on inter-domain links is supposed to be higher than that on intra-domain links.

CHAPTER 4: P-CYCLE PROTECTION STRATEGY IN MULTI-DOMAIN NETWORKS

4.1 Introduction

The issue of survivability in multi-domain networks can be addressed by different solutions. In general, these protection solutions in a multi-domain network can be categorized into particular groups according to different backup path computation approaches: arranging two link-disjointed paths for working and backup task, assigning protection responsibility of each segment to corresponding domain independently. This chapter focuses on the latter.

One important issue is how to assign working/backup routes for inter-domain links. Network aggregation is seen as an efficient approach to help reduce exchanging routing information between domains. For example, a complete domain with multiple links and nodes may be replaced by one single node. Alternatively, the whole domain can be represented as a central node connected to all border nodes; this is referred to as Star aggregation. The most preserved information aggregation model is full-mesh model with a set of fully connected border nodes. Fig. 2.13 shows an illustration of all three above models.

This chapter considers an improvement full-mesh aggregation model based on Drid's approach. We introduce a modified full-mesh aggregation model that not only offers more spare capacity efficiency but also ensures full protection against all single (intra-domain and inter-domain) link failures.

4.2 Drid's model for domain aggregation

4.2.1 p-cycle protection

Generally, network protection schemes are evaluated on the basis of their speed and capacity. Initially, two common schemes namely ring protection and mesh protection drawn a lot of attention of researchers. The searches of improving recovery switching

time and reducing capacity redundancy lead to the discovery of preconfigured protection cycle (p-cycle), introduced in [25]. The p-cycle performs switching as fast as ring protection (50-60 msec) and capacity efficiency approximately like mesh protection. Importantly, most studies so far on p-cycle have considered link-protecting p-cycle, which operate as shown in Fig. 4.1. The dotted line presents the considered cycle (1-2-3-4-6-1). This p-cycle does not only protect links that are part of itself (links (1-2), (2-3), (3-4), (4-6), (6-1)) as ring protection but also protects links that directly straddle the respective p-cycle (link (2-4)) as the advantage of p-cycle.

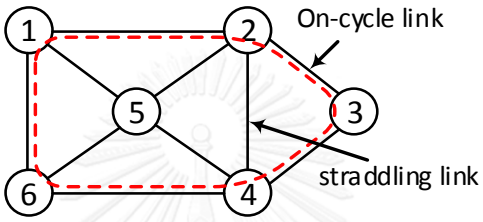


Figure 4.1: An illustration of p-cycle protection's components.

The ILP formulation that determines which cycles are selected to carry backup resources while minimizing the total cost of backup capacity can be found in [23].

4.2.2 Drid's aggregation model to protect multi-domain networks using p-cycle technique

Because of the benefit of using p-cycle in protecting networks, the idea of applying this technique in multi-domain networks is implemented in [19] with the main goal of protecting the inter-domain links. The idea of the paper is managing the inter-domain protection by applying single-node aggregation model so that one virtual node represents an entire domain. Subsequently, the restorability of inter-domain links is ensured without knowledge of all physical topology information. The drawback of this technique is that the cost of a p-cycle on the physical topology is unknown and the set of p-cycle only protects inter-domain links. To overcome these disadvantages of single-node aggregation, in [3], Drid proposed a solution which provides more topological information for each domain. In other words, instead of using a single virtual node presenting a particular physical domain, those authors develop an aggregation model, which is based on full-mesh aggregation model for p-cycle protection use in order to support multi-domain networks. From this point to

the end of the chapter, this aggregation model is referred as a conventional model or Drid's model to differentiate it with the new model that will be presented later.

This conventional aggregation technique proceeds in two steps. First, traffic demands in Fig. 4.2a are routed for each physical topology of domain based on shortest path algorithms [26]. Fig. 4.2b describes an example with a network with six nodes, of which three (A, B, E) are border nodes that connect to other domains through inter-domain links. Fig. 4.2c shows the routing result based on traffic demand matrix so that the integer number on each link is referred to as the working capacity of the corresponding link.

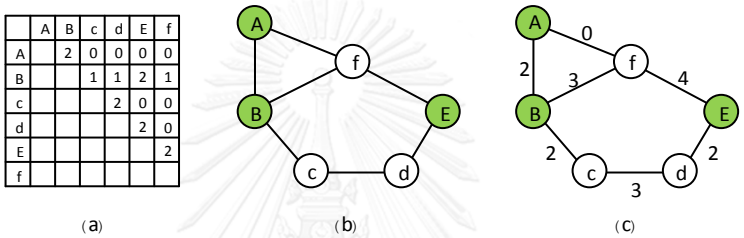


Figure 4.2: An example of (a) Traffic demands (b) the original topology with three border nodes (green) and (c) the topology with working capacity after routing.

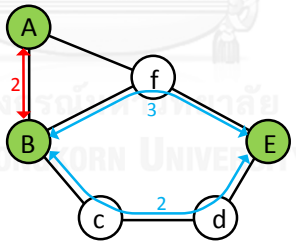


Figure 4.3: Working capacity is aggregated between border nodes in Drid's model.

In the second step, which presents the key contribution of the paper, as shown in Fig. 4.3, traffic between borders node pairs are determined by applying a set of ILP formulation. Therefore, the physical topology is transformed into a simple virtual topology as shown in Fig. 4.4a. The integer number assigning to each virtual link denotes the number of primary light-paths between one border node to another. It is noticed that the disjoined condition is compulsory for these two-virtual links or the light-paths linking one pair of border node are required to be disjointed from all the light-paths that connect any other node pairs. This model seems to offer more efficient use of backup resources because more information is published to other

domains. Moreover, the amount of working capacity left after finishing aggregation process is also protected internally for each domain. The detail of remaining working capacity is shown in Fig. 4.4b.

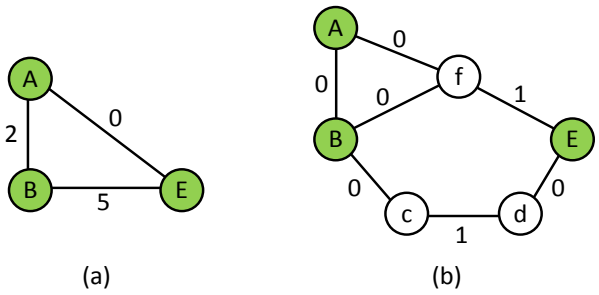


Figure 4.4: (a) Virtual topology and (b) Topology after aggregation by conventional model [3].

The aggregation model, however, remains some drawbacks in terms of traffic aggregated efficiency as well as the quality of the set of p-cycles for inter-domain link protection. Firstly, in Drid's aggregation model, the objective function is maximizing the total number of working capacity between any pair of border nodes. This raises a question about the relevance of objective function since by this approach, the remaining working capacity is not considered for optimization. This may cause inefficient traffic aggregation when the total number of unassigned working capacity is high. The second drawback is that in Drid's model, both kinds of links: intra-domain and inter-domain links own an identical value of link cost which is one unit. Although such a cost can help reduce the complexity of optimization, it causes the problem of hiding all the physical topology information of each domain. Therefore, the decision of choosing a set of backup paths for working capacity protection is affected.

4.3 Proposed aggregation model for p-cycle protection strategy in multi-domain networks

After presenting the major drawbacks of Drid's model, we develop a proposed model that allows us to tackle these limitations. As described above, the first disadvantage on objective function can be handled by taking the number of remaining working capacity after aggregation into account. In other words, the total

number virtual working capacity and remaining working capacity could be smaller if the objective function of aggregation model is minimizing the summation of total working traffic between border nodes and total remaining working capacity. The following section corresponds to step 1 of section 3.3.1. It is noticed that proposed model is obliged to obey the characteristics of virtual topology, which are:

- Virtual link manages the connection of each pair of border nodes within the domain. A virtual link relating a pair of border nodes matches to the set of working light-paths connecting these nodes in the physical topology.
- Virtual links are physically disjointed. In other words, a light-path connecting a pair of border nodes is compulsory to be link-disjointed from all other light-paths between any other node pairs.

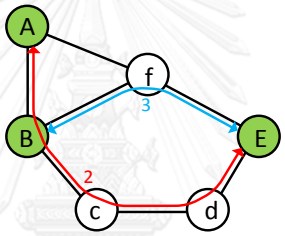


Figure 4.5: Working capacity is aggregated between border nodes in proposed model.

Since the objective function is changed in the proposed model, traffics between border node pairs are re-allocated as shown in Fig. 4.5.

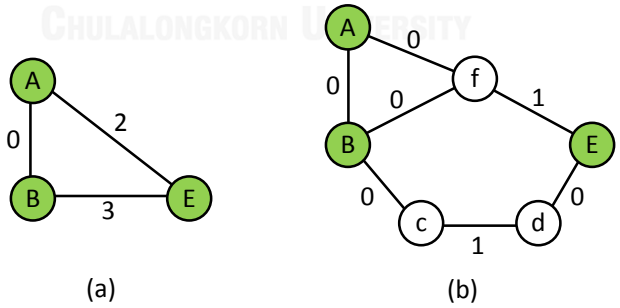


Figure 4.6: (a) Virtual topology and (b) Topology after aggregation by proposed model.

The number of virtual working capacity or the number of light-paths connecting the pair of border nodes can be calculated as follows:

$$N_{vir\_wk} = \sum_{d \in B_i} \sum_{p \in P(d)} h_{d,p} \tag{4.1}$$

Additionally, in order to control the number of remaining working capacity from each domain, a described below equation is introduced:

$$N_{remain\_wk} = \sum_{l \in L_i} r_l \tag{4.2}$$

Fig. 4.6 presents the results of proposed aggregation model, in which the total remaining working capacity is 2 as same as the conventional model, whereas the number of virtual working capacity is only 5 unit instead of 7 as shown in Table 4.1.

Table 4.1: Comparison of capacity between the Drid's model and the proposed model.

	Conventional model	Proposed model
# Virtual capacity	7	5
# Remaining capacity	2	2

Additionally, the relation between the physical set of links and the virtual link can be presented by a cost parameter in order to overcome the drawback of the deviation from the optimal solution. The details of ILP formulation for p-cycle including link cost can be found in [23].

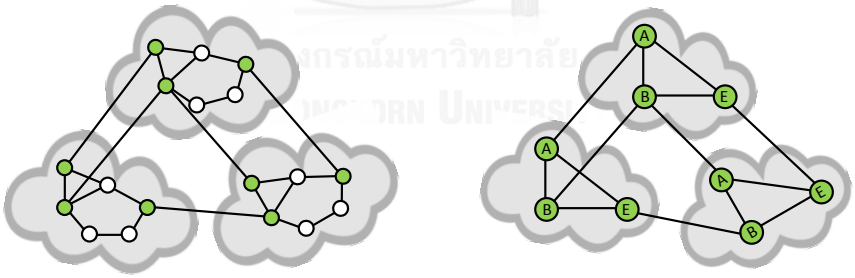
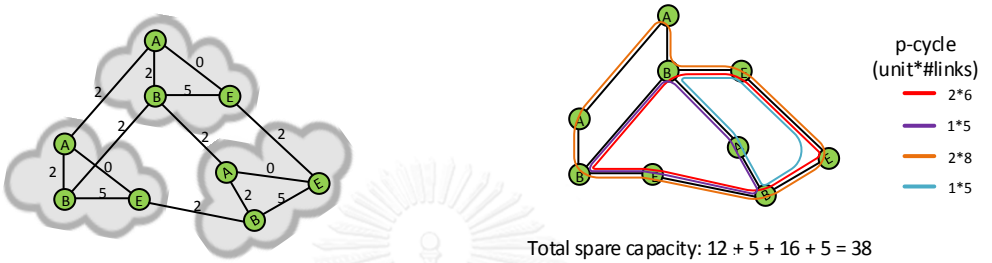


Figure 4.7: An example of a multi-domain network with working capacity on each inter-domain link equals two. (a) Physical topology. (b) Virtual topology.

To measure the improvement of proposed aggregation model, a multi-domain network which is a combination of three described physical domains is taken for analyzing purpose. The trivial case with such an assumption that working capacity on each inter-domain links is two (see Fig. 4.7a) is used in the following example. After

aggregation by conventional model and proposed model, a physical topology is achieved as shown in Fig. 4.7b.

Step 2 of Section 3.3.2 is applied to protect inter-domain links of example multi-domain networks. Next figure shows how to allocate resources for virtual multi-domain restorability using Drid's model (see Fig. 4.8a). A set of active cycles that are used for backup is presented in Fig. 4.8b.



(a) (b)

Figure 4.8: (a) Topology with virtual working capacity attached to each domain and working capacity on inter-domain links. (b) Set of active cycles for protection.

As mentioned, the working traffics that cannot be aggregated are also restored by p-cycle protection technique as shown in Fig 4.9.

Similarly, step 3 of Section 3.3.1 is used in order to find the optimal solution for virtual multi-domain protection and remaining working traffic protection using proposed model in the same manner.

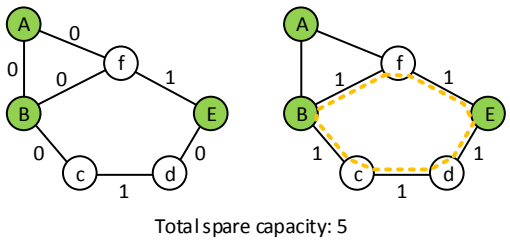


Figure 4. 9: Remaining working capacity from Drid's model is protected using conventional p-cycle approach.

Table 4.2 summarizes the differences in backup resources used for protection by Drid's model and the proposed model. With the same given input, the proposed model appears to be superior in terms of saving backup resources because of its

efficiency in protecting virtual multi-domain over Drid's model, such that 8 units of spare capacity were saved by the proposed model.

Table 4.2: Comparison between the Drid's model and the proposed model protection.

	Drid's model	Proposed model
Working capacity	58	58
Spare capacity protecting virtual multi-domain	38	26
Spare capacity protecting remaining capacity	3x5	3x5
Number of used cycles	4+1	3+1
Total spare capacity	53	41

At this point, the second drawback of Drid's paper as mentioned above is shown. Previously, those authors select the available cycle with the equal cost of every virtual link as well as inter-domain links. The virtual link on the virtual topology, however, possibly is consisted of multiple physical links so that the backup path by Drid's paper may be not even close to the optimal solution. To overcome this problem, the proposed model appoints the reasonable cost for the virtual link based on the physical light-paths which are presented by it. Therefore, by implementing link cost parameter into ILP formulation in [3], the backup cycles are more reasonable than these of Drid's paper. One way of determining the most appropriate cost for a virtual link is basing on hop count information. For example, the cost of links AB, BE, AE in Fig. 4.5 are 1, 2, and 4, respectively because of the physical paths of AB, BE and AE are correspondingly A-B, B-f-E, A-B-c-d-E.

Fig. 4.10 shows that in the case of virtual link cost is considered, the number of needed spare capacity is higher than that when every link is treated equally. The reason is that with conventional Drid's model, those authors can only claim that set of active p-cycles is able to protect "some" physical working capacities in the traversed domains, while the proposed model provides the exact solution that supports 100% physical working capacities presented by virtual links. Moreover, the total spare capacity saving efficiency obtained in the second scenario (proposed

model) is enhanced compared to that obtained by the conventional model for the example topology. This remark is justified by the fact that although the numbers of spare capacity protecting remaining working capacity in two cases are the same, the proposed model allocates physical capacity into virtual link more efficiently compared to conventional one.

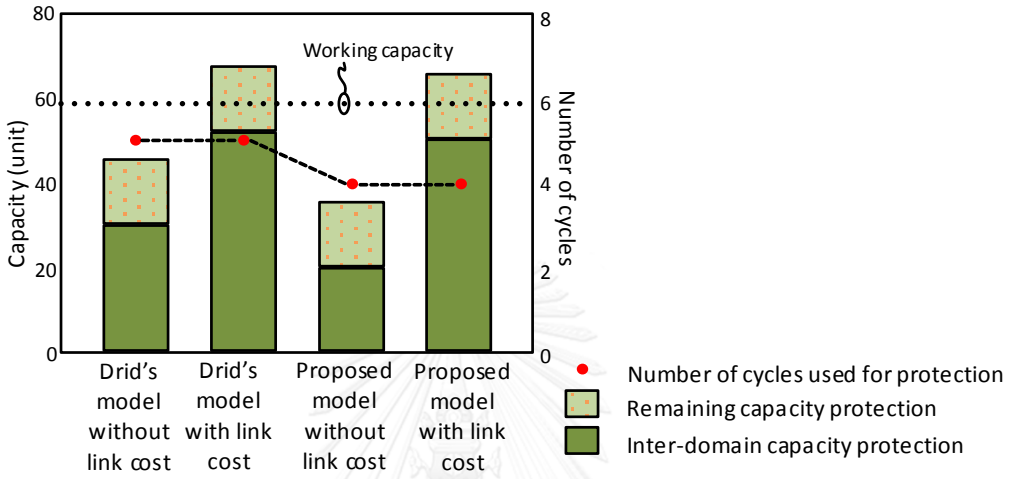


Figure 4.10: The comparison of multi-domain scenarios applying the two models.

Furthermore, a total number of cycles used to protect multi-domain network also reduces with proposed model. Thus, the network management task which is an essential factor in large networks can be simplified.

4.4 Simulation results

LARGE-5 topology in Fig. 4.2 is selected as a testing network for proposed aggregation model.

Table 4.3 implies that the total number of aggregated capacity and the remaining capacity of Drid'model is bigger than the figure of proposed model. In particularly, Drid's model tends to assign more working capacity to the virtual connections between border nodes compared with proposed model and the un-aggregated traffic in each domain of the proposed model is much fewer than traffic in Drid's model. This relieves domain from protecting the huge amount of capacity especially when domain size is enormous.

Table 4. 3: Aggregated capacity information of Drid's model and proposed model.

Domain	Physical working capacity	Aggregated capacity of Drid model	Aggregated capacity of proposed model	Remaining capacity of Drid model	Remaining capacity of proposed model
D1	368	176	104	525	264
D2	304	93	77	394	227
D3	270	194	86	284	184
D4	176	105	54	194	122
D5	286	84	47	316	238

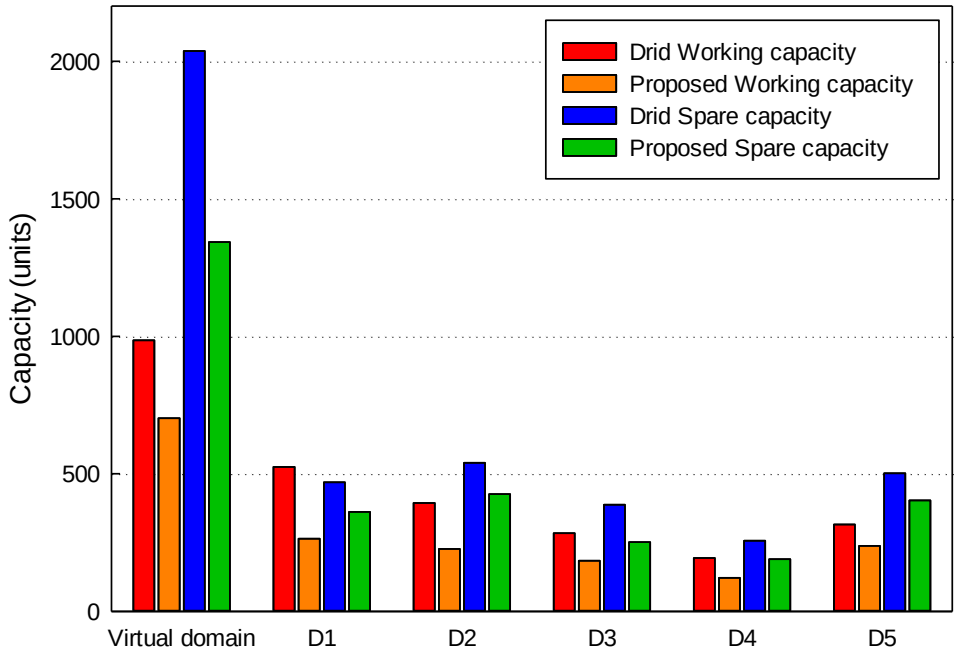


Figure 4.11: Required spare capacity for Drid's model and proposed model protection.

Fig. 4.11 shows the number of demanding capacity for multi-domain protection using Drid and the proposed model. As is presented in the bar graph, the proposed model requires less capacity to restore virtual domain and each individual physical domain. For example, the proposed model needs only two third of spare capacity for Drid's model to protect its virtual domain. Moreover, the numbers of remaining working

capacity were significantly decreased by applying proposed aggregation model. Therefore, operators do not need to spend that much resource to protect a domain like they used to do with Drid's model.

Table 4.4: Average backup length for Drid's model and proposed model protection.

	Drid's number cycles	Proposed number cycles	Drid's cycle length	Proposed cycle length
Virtual domain	11	10	23.96	26.86
D1	13	9	7.69	8.58
D2	10	7	7.61	6.17
D3	9	7	5.79	6.46
D4	10	6	6.43	8.26
D5	6	8	11.67	11.85

Beside of improving the spare capacity efficiency, the number of active cycles and the average length of backup paths also need to be considered. First, as mentioned, a number of active cycles has an impact on network management issue. In other words, the more cycles involved in protection, the more complicated the configuration problems become. Table 4.4 indicates that except in the case of domain D5, the proposed model is able to restore the multi-domain networks with a smaller number of cycles than Drid's model. Secondly, the network latency which can be affected by backup length is one of the most important concerns when it comes to optical network design. Again from Table 4.4, it is seen that Drid's model is more advantageous with the shorter average backup length compared with the proposed model in almost scenarios, except for domain D2.

4.5 Summary of p-cycle protection strategy in multi-domain networks

This chapter addressed the protection of multi-domain networks. By discussing the drawbacks of an existing solution, we proposed an improved approach for the survivability of multi-domain optical networks based on p-cycle. The proposed aggregation model which is used for scalability and domain privacy reasons enables our solution to improve the performance of saving spare capacity. Moreover, while

Drid's model only protects inter-domain traffic and some intra-domain traffic, our proposed model guarantees of covering 100% single link failure.

CHAPTER 5: SHARED-MESH PROTECTION STRATEGY IN MULTI-DOMAIN NETWORKS

5.1 Introduction

In order to allocate resources for intra-domain and inter-domain link protection while satisfying the multi-domain characteristic on domain privacy as well as scalability, various solutions have been proposed. One of the most popular solutions is quantity reduction. The idea of this approach is addressing both privacy and scalability issue at once: physical topology information is hidden so that the amount of exchanging information among domains is minimized. Aggregation models which are introduced in literature review can be applied at this point for reducing domain topology size. In [1] and [18], those authors use full mesh aggregation method in order to represent a physical topology. Every domain is aggregated into a complete graph consisting of border nodes and virtual links for connection. It is noticed that a specific aggregation criterion is required in order to decide virtual link parameters. For instance, based on traffic demand matrix and physical link information (length, cost, etc.), the shortest path between two border nodes can be computed. This mentioned criterion is also used in these two above papers so that working link capacity determines which path has the minimum-cost and is selected for aggregation.

In [1], the authors proposed Extended Shared Path Protection (ESPP) which is used for multi-domain protection purpose. This idea can be interpreted into link protection by pre-allocating working capacity into each link by applying any well-known existing techniques such as shortest path, minimize total resources, etc. This approach can be presented in three steps: In the first step, Full Mesh aggregation model is applied to every domain to construct a single virtual topology. The aggregated virtual topology consists of all virtual domains, which are linked by inter-domain links. Next step, inter-domain link protection is considered using virtual domains and inter-domain links. After this step, there is spare capacity allocated on

each virtual domain links to support inter-domain links. Lastly, intra-domain links are protected given the constraint of mapping virtual link capacity on physical links. The advantage of ESPP is its efficiency in saving backup resources. However, since the backup path of a single link may traverse the entire network, the burden in recovery time is considered as a drawback of ESPP.

In [18], the idea of new Shared Sub-Path Protection technique (SSPP) is introduced, in which the authors tackle the concern on recovery time of ESPP. In other works, the restoration paths become shorter because the area that backup path of a particular link can be re-routed is now limited to only two domains. The major disadvantage of this approach is that the amount of backup resource consumed is still higher than ESPP. Additionally, it might be impossible to find a backup path for inter-domain links when restoration paths are limited to two domains.

It is noticed that these two listed strategies above differ from other approaches because these protect both intra-domain and inter-domain links. However, the amount of consumed resources of ESPP and SSPP are relatively high. Therefore, we would like to propose a protection strategy that preserves the rule of multi-domain networks protection by keeping routing information locally, while reducing the demand for the resources. The difference between our strategy and existing ones is that backup capacity for protecting inter-domain links can be utilized for intra-domain protection procedure.

5.2 Shared mesh protection

Contrary to ring or p-cycle architectures where recovery time on a given ring is reasonably well-known, mesh networks require longer restorable time, which is affected by many factors, such as networks size, failure location, etc. Mesh protection technique is more flexible with regard to the protection structure compared to other protection techniques. For example, mesh protection approach re-routes backup paths through any arbitrary backup structure, while ring protection technique limits its backup paths in a precise topology which is a ring [4]. Consequently, mesh protection is recommended to solve the survivability problem

for networks with a high priority of spending resources. For instance, mesh protection offers 20% to 60% fewer backup resources as compared to rings. Mesh protection, however, needs more complex routing tables to arrange restoration paths. This makes communication method or signaling from source to destination node essential, especially in the scenario that one backup path can be shared among many primary paths.

5.3 Concept of novel shared backup protection strategy in multi-domain networks

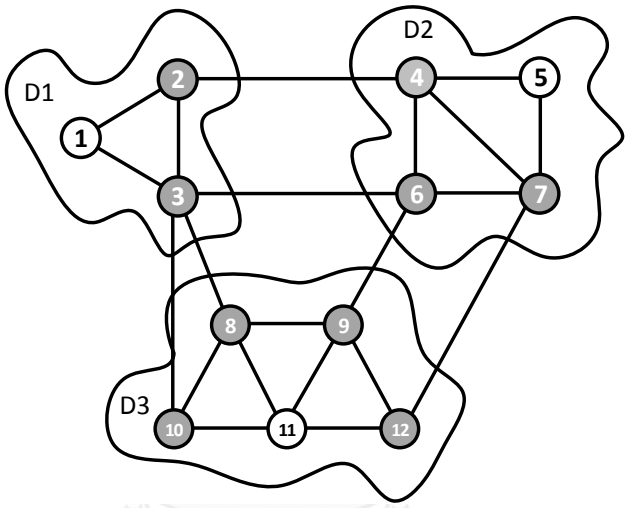


Figure 5.1: An example of multi-domain networks: a WDM network with 12 optical switches which are represented by nodes; Gray color nodes represent border nodes of the domains; white color nodes are internal nodes of a particular domain.

In this section, the concept of novel shared backup protection strategy for multi-domain networks is described so that we are able to compare the capacity redundancy (the ratio of spare over working capacity cost) of two models, namely ESPP and SSPP, before and after applying this protection strategy. In order to illustrate the concept, we look at Fig. 5.1 which shows an example of multi-domain networks. The example consists of 3 different domains: D1, D2, and D3 with the number of nodes in each domain being 3, 4 and 5, respectively.

To simplify the problem, we assume that routing task can be successfully performed before protection stage. Hence, working capacity assigned to each link is shown as in Fig. 5.2. Total working capacity of the network is 69 units.

By applying step 1 from section 3.3.2, a table for aggregation result can be achieved as follow:

Table 5.1: Virtual link cost of example multi-domain

Virtual link	Corresponding physical path	Virtual link cost
2-3	2-3	1
4-6	4-6	1
6-7	6-7	1
4-7	4-7	1
8-9	8-9	1
8-10	8-10	1
9-12	9-12	1
10-12	10-11-12	2
8-12	8-11-12	2
9-10	9-11-10	2

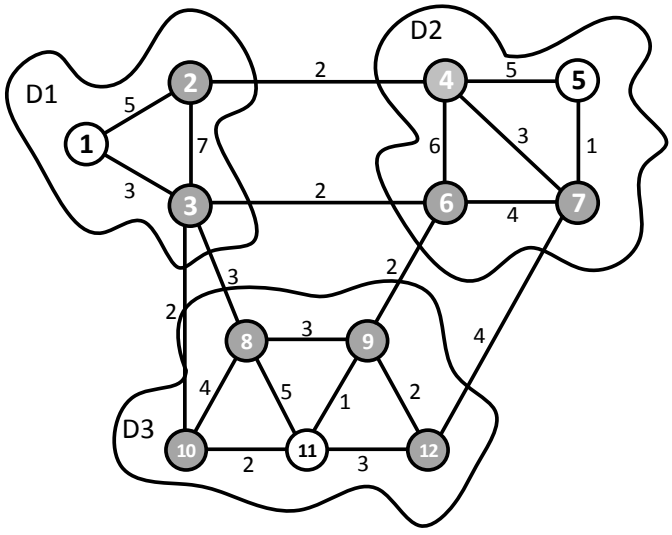


Figure 5. 2: Multi-domain network with an integer value attached to each link denotes the number of working capacity on that link.

As mentioned earlier, the novel backup protection strategy is developed on the background of ESPP and SSPP. The first scheme can be considered as Global Shared Backup Mesh (GSBM) protection and the other one is Local Shared Backup Mesh (LSBM) protection in multi-domain networks. The following sections will describe in detail both strategies.

5.3.1 Global Shared Backup Mesh protection strategy in multi-domain network

Based on the discussion above, full mesh aggregation model is used to obtain the network including three virtual domains and inter-domain links as shown in Fig. 5.3a. It is noticeable that the virtual links of each domain at this point do not carry any working capacity and there are 15 units of capacity on all inter-domain links in this example. To protect those capacities on inter-domain links, shared mesh protection technique in step 2 from Section 3.3.2 is applied in which restoration routes can traverse the whole virtual network. Fig. 5.3b shows the spare capacity allocation to achieve 100% inter-domain link failure protection. For example, from Table 5.2, link (2-4) can be restored by rerouting traffic through two different routes: (2-3-8-10-12-9-6-7-4) and (2-3-10-8-12-9-6-7-4). Since working capacities are not available for every link of protecting topology, the total backup cost needed to protect inter-domain links is relatively high. Using Table 5.2 and Fig. 5.3, the backup cost can be obtained as 16 units including 6 unit on inter-domain links (3-10, 2-4, 6-9) and 12 units on virtual links of domains (2-3, 6-7, 4-7, 8-10, 8-12, 10-12, 9-12).

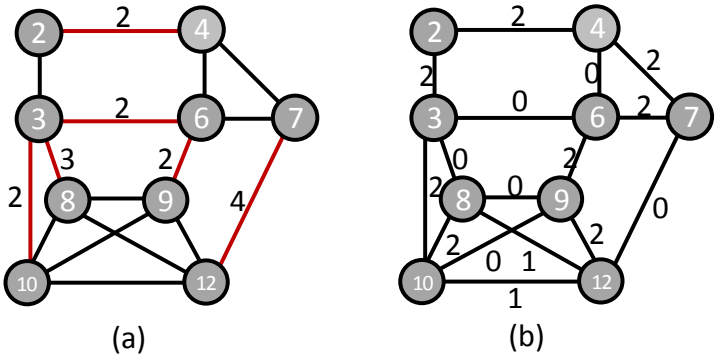


Figure 5.3: (a) Network topology after aggregation with working capacity on inter-domain links (red color); (b) Spare capacity allocation for inter-domain links protection by GSBM.

Table 5.2: Spare capacity allocation to protect failed inter-domain links

Link failure	Backup path(s)	# spare capacity
3-10	3-2-4-7-6-9-12-10	1
	3-2-4-7-6-9-12-8-10	1
3-8	3-10-8	1
	3-2-4-7-6-9-12-8	1
	3-2-4-7-6-9-12-10-8	1
3-6	3-8-12-9-6	1
	3-10-12-9-6	1
2-4	2-3-8-10-12-9-6-7-4	1
	2-3-10-8-12-9-6-7-4	1
7-12	7-6-9-12	2
	7-4-2-3-8-10-12	1
	7-4-2-3-10-8-12	1
6-9	6-7-4-2-3-8-10-12-9	1
	6-7-4-2-3-10-8-12-9	1

After inter-domain links survivability is ensured, step 3 from Section 3.3.2 is performed, so that GSBM approach will respectively protect each and every domain of D1, D2 and D3 of the network.

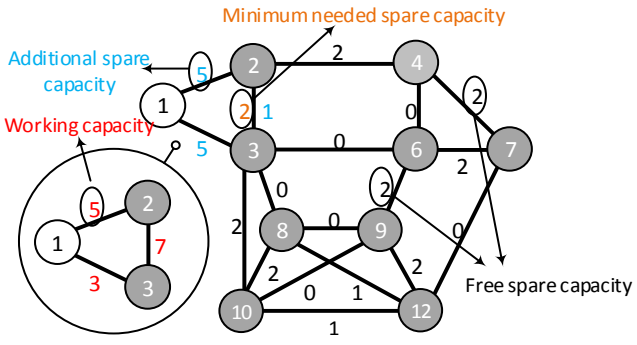


Figure 5.4: Protection scenario for domain D1 by GSBM and A-GSBM.

In this thesis, the scenario that allows additional resources on inter-domain links and virtual domain links will be attached a prefix A-, such as A-GSBM. If there is no any attachment, we understand that referred situation cannot request for extra spare

capacity from outside. In the next paragraphs, GSBM and A-GSBM are alternatively used for protecting intra-domain links of each domain in the example.

Firstly, domain D1 is considered in a scenario that includes the physical topology of D1, the virtual topology of domains D2 and D3 and the set of all inter-domain links (see Fig 5.4). The working capacity on links of D1 (red color number) is protected by rerouting backup paths which are allowed to cross inter-domain links and virtual intra-domain links as well. The black color integer number attached with inter-domain links and virtual domain links are available spare capacity from the previous step (from Fig. 5.3b) that can be reused at this stage. The orange color number also represents the available spare capacity on an intra-domain link but eventually, the total number of spare capacity on this link is forced to be not smaller than the orange color number in order to provide sufficient resources for the previous step. The detail of backup routing information for domain D1 can be found in Table 5.3 below. From Fig. 5.4 and Table 5.3, the number of required and additional backup capacity to protect domain D1 using GSBM and A-GSBM are shown in Table 5.4. For instance, using GSBM technique, link (2-3) has 2 units of free backup capacity but the number of required spare capacity on this link is 3 units (for protecting links (1-2) and (1-3)). Therefore, 1 unit of extra capacity is needed to be deployed by the operator.

Table 5.3: Spare capacity allocation to protect failed intra-domain links of D1 by GSBM and A-GSBM.

Failure link	Backup path(s)	# spare capacity
1-2	1-3-2	3
	1-3-10-12-9-6-7-4-2	1
	1-3-10-8-12-9-6-7-4-2	1
1-3	1-2-3	3
2-3	2-1-3	5
	2-4-7-6-9-12-10-3	1
	2-4-7-6-9-12-8-10-3	1

The simulation results show that in this scenario, the optimal solutions of GSBM and A-GSBM are equal and backup resources distributions of these two are also identical

with extra 11 unit of spare capacity including 5 units on each link (1-2) and link (1-3); 1 unit on link (2-3) in order to ensure the survivability of domain D1 against any single link failure in both cases (GSBM and A-GSBM).

Table 5.4: Required and additional spare capacity to protect intra-domain links of D1.

Link	Available spare capacity	GSBM		A-GSBM	
		Required capacity	Additional capacity	Required capacity	Additional capacity
1-2	0	5	5	5	5
1-3	0	5	5	5	5
2-3	2	3	1	3	1
2-4	2	1	0	1	0
3-6	0	0	0	0	0
3-8	0	0	0	0	0
3-10	2	1	0	1	0
4-6	0	0	0	0	0
4-7	2	1	0	1	0
6-7	2	1	0	1	0
6-9	2	1	0	1	0
7-12	0	0	0	0	0
8-9	0	0	0	0	0
8-10	2	1	0	1	0
8-12	1	0	0	0	0
9-10	0	0	0	0	0
9-12	2	1	0	1	0
10-12	1	1	0	1	0

It is noticed that the flexibility in selecting protection paths is a key advance of GSBM (and A-GSBM) over conventional ESPP.

The distribution of spare capacity within physical domain D1 also satisfies the physical connection between two border nodes. For example, as shown in Fig. 5.3b, the number of spare capacity between node 2 and node 3 is at least 2 units. In this

case, physical link (2-3) is in charge of proving the internal connection so that the spare capacity of link (2-3) has to be higher or equal 2 units.

In the case of the second domain which is domain D2, GSBM and A-GSBM result differently as shown in Fig. 5.5. For the first scenario referred to GSBM (see Fig. 5.5a), the number of additional resources to protect intra-domain links is 11 units with 1 unit on each link (4-5) and (4-7); 2 units on each link (4-6) and (6-7); 5 units on link (5-7). In the second scenario, besides the ability to deploy extra spare capacity on inter-domain links and virtual domain links (discussed above), A-GSBM is performed with the additional assumption that backup capacity that is already allocated to protect intra-domain links of D1 can be used to protect intra-domain links of D2. For example, available spare capacity on the virtual link (2-3) which is 2 units for protecting inter-domain links (see Fig. 5.4) is now updated to be 8 units including 5 units on (2-1-3) and 3 units on (2-3). Therefore, A-GSBM requires less backup capacity than that of GSBM which is 10 units with 1 unit on each link (2-4), (4-6), (7-12); 2 units on link (3-6); 5 units on link (5-7).

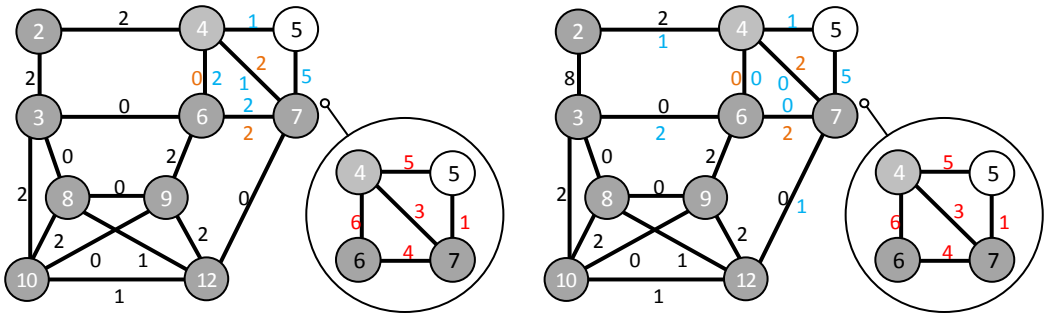


Figure 5.5: Protection scenarios for domain D2 by (a) GSBM and (b) A-GSBM.

Finally, for domain D3, there is a slight difference in assigning spare capacity from virtual connections to physical connections. Fig. 5.6 shows that virtual link (10-12) and (8-12) represents set of multi-physical links which are (10-11-12) and (8-11-12) respectively. This is the reason why we should consider virtual link cost in the optimization problems in order to achieve a result that is more efficient. In Fig 5.6a, the simulation result shows that the additional number of backup capacity to recover the domain from single link failure is 6 units with 3 unit on link 8-9; 1 unit on

each link (9-11), (9-12) and (10-11) in the case of applying GSBM. In Fig 5.6b, the available spare capacity on virtual domain links and inter-domain links are updated after allocating capacity for protecting domain D1 and D2 by the similar manner as in domain D2 protection. For instance, in Fig. 5.6b, inter-domain links (3-6), (2-4), (4-7) and (7-12) provide 2, 1, 1 and 1 more units of spare capacity respectively. A-GSBM also demands 6 units of spare capacity: 3 units on link (3-8), 1 unit on each link (7-12), (10-11), (11-12) as illustrated by blue color number in Fig. 5.6b. Although the amount of required backup resource of GSBM and A-GSBM are equal for this domain, this approach may benefit when subsequent domains can enjoy this added capacity.

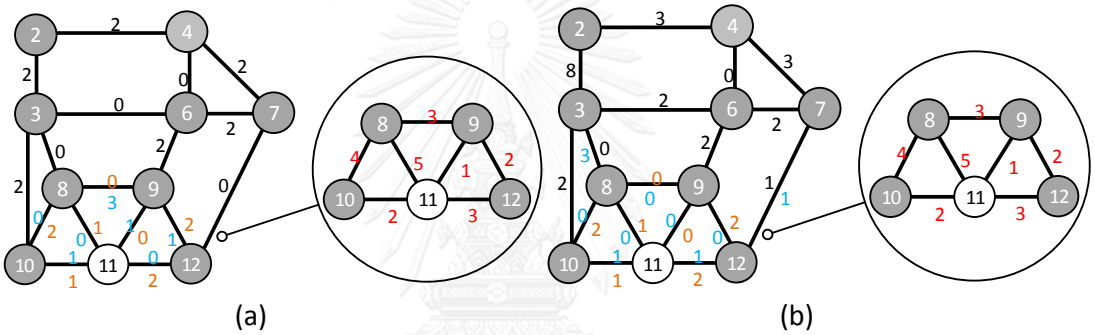


Figure 5.6: Protection scenario for domain D3 by (a) GSBM and (b) A-GSBM.

From two examples of protecting domain D2 and D3, the impact of having additional backup resources from earlier calculated domains does not exist or we can have the exact optimal solution without relying on such backup resources. For example, in Fig. 5.6b, the number spare capacity is still sufficient to protect intra-domain links of D3 even when available spare capacity on the virtual link (2-3) and (4-7) are 2 and 3 respectively. Therefore, further simulations on A-GSBM neglect updating available backup capacity of a link after each protection step to reduce the complexity of optimization problems.

Table 5.5: Spare capacity cost for multi-domain protection using GSBM and A-GSBM.

Spare capacity	GSBM [units]	A-GSBM [units]
Inter-domain links	6	14
Intra-domain links D1	13	13
Intra-domain links D2	15	10
Intra-domain links D3	14	10
Total	48	47

In a nutshell, the completed network with intra-domain and inter-domain links is considered survivable against single link failure with the distribution of spare capacity cost as shown in Table 5.5. Expectedly, the total required capacity by A-GSBM is less than that by GSBM. Moreover, the backup capacity distribution between these two approaches is also different since A-GSBM tends to assign resources on inter-domain links, while GSBM allocates them mostly on intra-domain links. As mentioned above, the length of restorable routes of GSBM might cause the serious problem in recovery time, especially with large-scale networks consisted of many separate domains. This is our motivation to tackle this issue by introducing another approach, which is Local Shared Backup Mesh protection in multi-domain networks

5.3.2 Local Shared Backup Mesh protection strategy in multi-domain networks

The important feature that makes LSBM different from GSBM is the limitation on picking backup routes of inter-domain links and intra-domain links of each domain. In the other words, the set of candidate backup routes for inter-domain links are links that are entitled to traverse domains hosting either one of the two end nodes of inter-domain links. Equivalently, backup routes of intra-domain links can be selected from these that traverse through neighbor domains. In order to illustrate the difference between LSBM and GSBM, we use the same topology with working capacity as shown in Fig. 4.2 to explain how LSBM works. Inter-domain links are first considered using ILP formulation in (3.3.2b). The following parts present how each set of inter-domain links that connects one domain to another can be restored from single link failure.

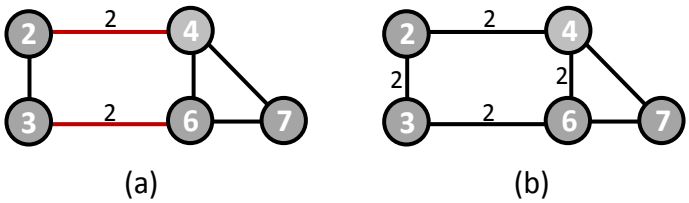


Figure 5.7: Inter-domain links between domains D1 and D2 are protected by LSBM. (a) Working capacity on inter-domain links (2-4) and (3-6). (b) Spare capacity needed to protect these inter-domain links.

Fig. 5.7a shows that two separate domains D1 and D2 need to get involved in protecting 4 working capacity on links (2-4) and (3-6). The number of backup capacity is 8 units including 2 units on each link (2,4), (4,6), (3-6) and (2-3) to cover only 4 working capacity units as shown in Fig 5.7a. In a similar manner, we can compute a set of backup routes and spare capacity to recover inter-domain links between D1-D3 and D2-D3 as well.

As shown in Fig. 5.8 and Fig. 5.9, the number of spare capacity provisioned in the inter-domain survivable network design phase is 8 and 14 for a set of inter-domain links between D1-D3 and D2-D3, respectively.

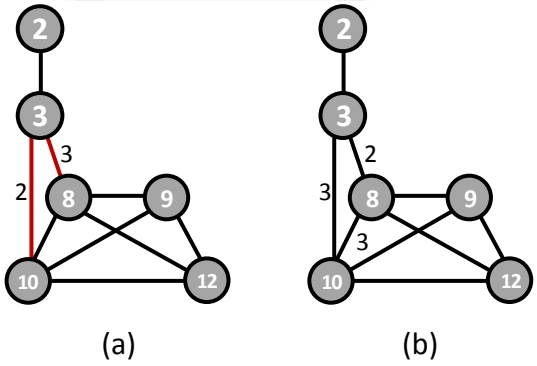


Figure 5.8: Inter-domain links between domains D1 and D3 are protected by LSBM. (a) Working capacity on inter-domain links (3-8) and (3-10). (b) Spare capacity needed to protect these inter-domain links.

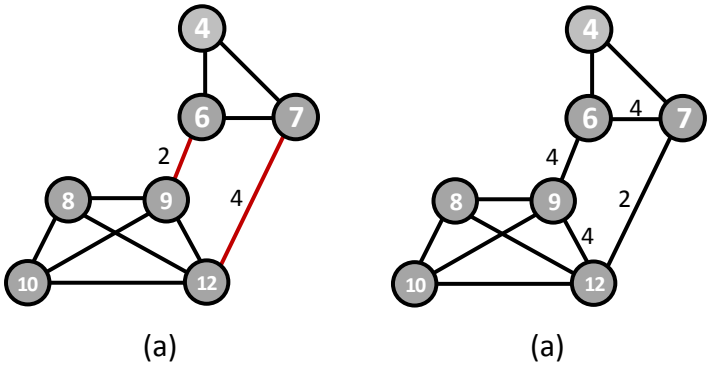


Figure 5.9: Inter-domain links between domains D2 and D3 are protected by LSBM. (a) Working capacity on inter-domain links (6-9) and (7-12). (b) Spare capacity needed to protect these inter-domain links.

The spare capacity allocation from above three sets can be assembled into one virtual topology as shown in Fig. 5.10. It is noticeable that LSBM requires more resources to protect all inter-domain links (34 units – included 13 units on inter-domain links and 21 units on virtual links) compared to GSBM which needs only 18 units of spare capacity. Such a difference can be explained by non-shared resources among backup routes of inter-domain links between a different pair of domains. However, in return, the recovery time of LSBM is significantly reduced since its backup routes never suffer from traversing the whole network like most of the routes in GSBM.

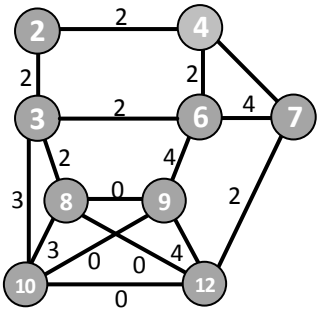


Figure 5.10: Spare capacity distribution for protecting inter-domain links by LSBM.

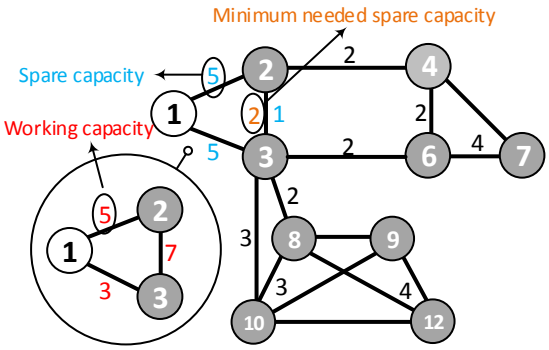


Figure 5.11: Protection scenario for domain D1 by LSBM (and A-LSBM).

Next step, LSBM, and A-LSBM are performed to protect each domain by reusing resources that are already allocated for inter-domain links restoration as described in Section 3.3.2c. Fig. 5.11 shows the situation where backup paths of intra-domain links in D1 are rerouted through inter-domain links, domains D2 and D3 as well. The optimal solution and spare capacity of LSBM and A-LSBM are identical with 11 unit of spare capacity (blue color) including 5 units on each link (1-2) and link (1-3); 1 unit on link (2-3). There is no difference in additional spare capacity of this scenario compared to GSBM from the previous section. However, the length of restoration routes, in this case, seems to be shorter than ones in GSBM. The detail of backup information for domain D1 can be found in Table 5.6.

Table 5.6: Spare capacity allocation to protect failed intra-domain links of D1 by LSBM and A-LSBM.

Failure link	Backup path(s)	# spare capacity
1-2	1-3-2	3
	1-3-6-4-2	2
	1-3-10-8-12-9-6-7-4-2	1
1-3	1-2-3	3
2-3	2-1-3	5
	2-4-6--3	2

Similarly, the optimization results of protecting domain D2 using LSBM (same as A-LSBM) is shown in Fig 5.12. The number of additional spare capacity is 9 units including 1 unit on link (4-5), 3 units on link (4-7) and 5 units on link (5-7).

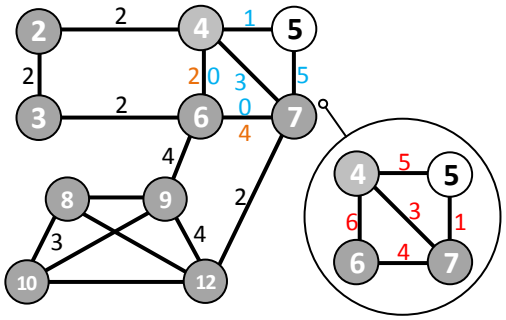


Figure 5.12: Protection scenario for domain D2 by LSBM (and A-LSBM).

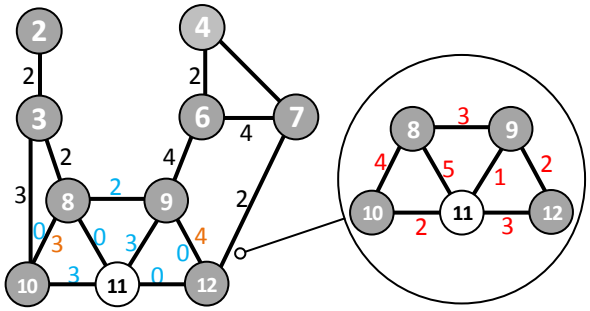


Figure 5.13: Protection scenario for domain D3 by LSBM (and A-LSBM).

Finally, LSBM and A-LSBM deploy 2 units of capacity on link (8-9), 3 units on each link (8-11) and (8-11) so that in total 8 units of additional capacity are needed to restore failed links in domain D3.

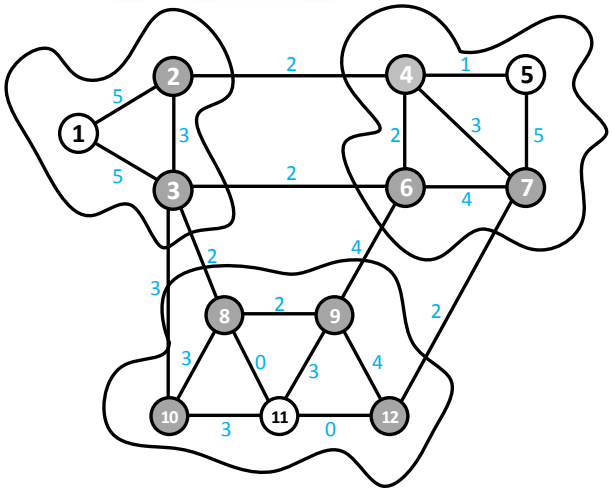


Figure 5.14: Spare capacity distribution of each link in the test network by LSBM and A-LSBM.

The number of spare capacity for protecting example network against single link failure by LSBM and A-LSBM is denoted in Fig. 5.14. For comparison purpose, Table

5.7 is made in order to provide a better understanding of GSBM, A-GSBM, LSBM and A-LSBM protection scenarios. Besides, the performances of ESPP and SSPP are also presented in order to prove the advantage as well as drawback of these new approaches. Table 5.7 reveals that with the same amount of total given working capacity needed to be recovered, regarding the amount of spare capacity for inter-domain link protection, six approaches can be categorized into two groups. In the first group, ESPP, GSBM, and A-GSBM have a common manner in handling failure on inter-domain links in which backup paths can traverse through the entire network. This approach increases efficiency in using backup resources for inter-domain traffic with only 18 unit of spare capacity required, while in the second group of SSPP, LSBM, and A-LSBM that figure is 34 units.

Table 5.7 also shows that the intra-domain protection tactic improves significantly the performances of GSMB and LSMB which is 30 and 24 units compared with ESPP and SSPP which is 44 and 43 units respectively. Additionally, in the comparison between GSMB and LSMB, it is clear that there is a trade-off between resource efficiency and recovery time. We can discuss further on this issue in the simulation section.

Table 5.7: Comparison between multi-domain protection strategies.

Protection strategy	Working capacity	Inter-domain links protection	Backup route length for inter-domain links protection	Intra-domain links protection (Extra capacity)	(*)Backup route length for intra-domain links protection	Total spare capacity
ESPP	69	18	5.2	44	2.63	62
SSPP	69	34	2.67	43	2.46	77
GSBM	69	18	5.2	30	3.44	48
A-GSBM	69	18	5.2	28	3.49	46
LSBM	69	34	2.67	24	2.42	58
A-LSBM	69	34	2.67	24	2.42	58

(*) The length of the backup route is calculated by hop count unit.

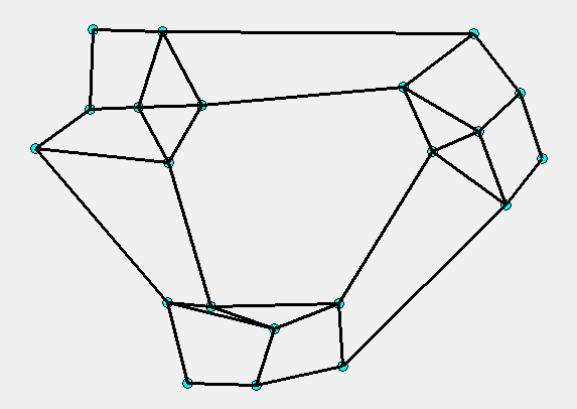


Figure 5.15: Example network topology consisted of 3 domains with 21 nodes

In order to prove the scalability of multi-domain protection schemes, an example topology is considered as shown in Fig. 5.15 to compare the efficiency as well as the complexity of multi-domain protection schemes with global optimization scheme. It is noted that, in global optimization scheme, multi-domain network is treated as a single domain network. The topology consists of 3 similar domains connected to others through pair of inter-domain links. The size of one domain or the number of nodes in one domain is selected so that a computer (Core i5 processer, 16Gbps RAM) is not able to return the optimal solution for bigger network.

Table 5.8: Comparison between global optimization and proposed strategies.

	Working capacity (units)	Spare capacity (units)	Number of ILP problems	Avg. simulation time (sec)
Global opt.	1244	730	1	1301
GSBM	1244	1063	4	35.68
A-GSBM	1244	982	4	31.43
LSBM	1244	1221	6	24.39
A-LSBM	1244	1159	6	19.75

Table 5.8 shows that 4 proposed strategies consume more backup resources for protection than the global optimal solution which is 146%, 135%, 167% and 159% for GSBM, A-GSBM, LSBM and A-LSBM, respectively. However, since the number of ILP

problems of proposed strategies increase from 1 (for global optimization) to 4 (for GSBM and A-GSBM) and 6 (for LSBM and A-LSBM), the complexity of these problems decrease dramatically. For example, it takes more than 20 minutes to solve the global optimization problem, while 4 proposed strategies help reduce the average simulation time to less than one min or even half a minute. Therefore, it is necessary to perform multi-domain protection strategy in large-scale optical networks.

5.4 Simulation results

The set of testing networks includes two topologies: Tnet and LARGE-5 (see Fig. 4.2). However, LSBM and A-LSBM only work on LARGE-5 topology with following restrictive condition: two domains are connected by at least two inter-domain links. First, Tnet topology is selected for testing two tactics: GSBM and A-GSBM for comparison with ESPP.

Fig. 5.16 reveals that although different domain requires different number of backup resources which depends on given working capacity as well as domain structure. It is clearly seen that A-GSBM is always the cheapest option for domain protection. For example, needed numbers of spare capacity for A-GSBM technique of domain D1, D3, D4, D5, and D7 are smaller than those numbers using mesh protection for single domain independently. Following after A-GSBM is GSBM considering as the second best option since it maintains the advantage of sharing existing spare capacity for inter-domain link protection to protect intra-domain links without the capability of deploying extra spare capacity. ESPP with a tight constraint of domain independence has spare capacity percentage fluctuating from 10 to over 60% compared with conventional mesh protection because it requires flow connection between border nodes.

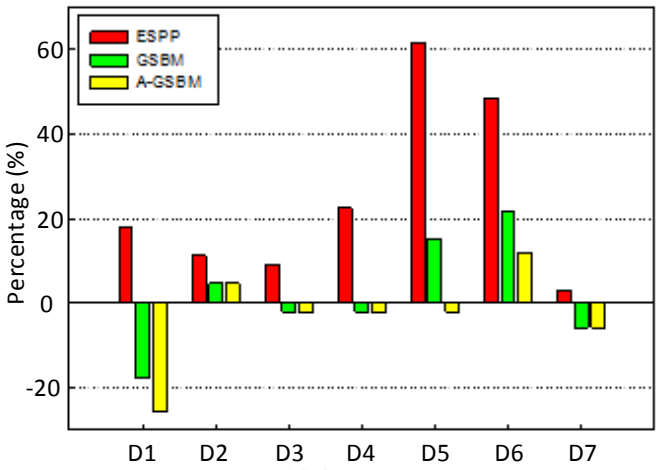


Figure 5.16: The proportion of backup capacity of ESPP, GSBM, A-GSBM for single domain compared with domain independent mesh protection in Tnet.

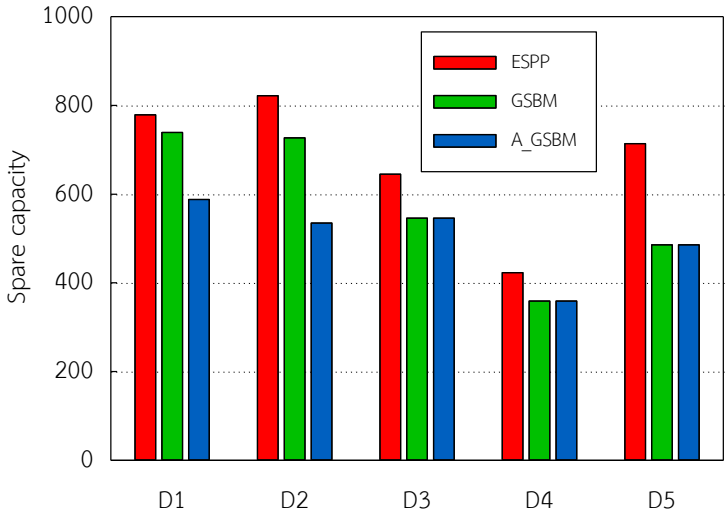


Figure 5.17: Comparison of needed backup resources between ESPP, GSBM, A-GSBM in the LARGE-5 network.

Fig. 5.17 for a second time shows the benefit in saving backup resources using GSBM and A-GSBM on LARGE-5 topology. Beside of that, the average backup path length of each technique is also considered. Because the protection paths of ESPP are not allowed to traverse outside a particular domain, its average backup length is shortest among three above approaches; such that there is no domain having a backup length greater than 6 units. For GSBM and A-GSBM, there is a trade-off between

saving resources and backup length. Except in domain D2, A-GSBM tends to lead backup paths to cross different domains for resources reusing purpose.

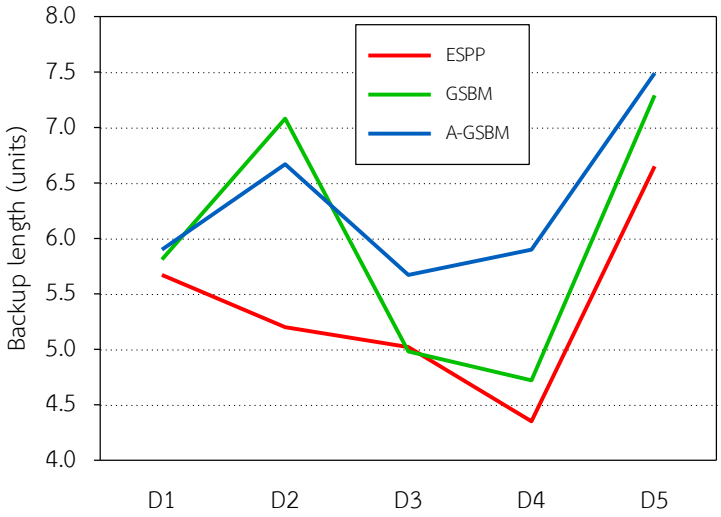


Figure 5.18: Comparison of average backup path length between ESPP, GSBM, A-GSBM in the LARGE-5 network.

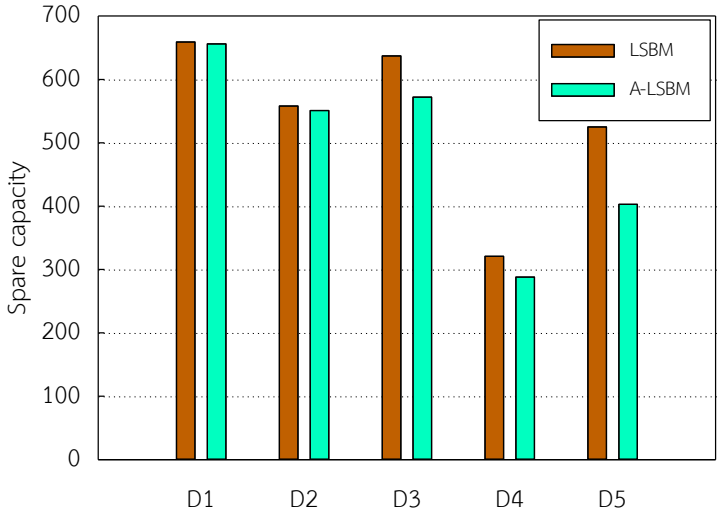


Figure 5.19: Comparison of needed backup resources between LSBM and A-LSBM in the LARGE-5 network.

The simulation results for LSBM and A-LSBM are shown in Fig. 5.17. The benefit of adding extra capacity on inter-domain/virtual domain links can be seen with domain D3, D4, and D5 protection. Unlikely to A-GSBM approach, A-LSBM also wins against

LSBM when it comes to fast recovery time ability, such that except in domain D1, A-LSBM always has around 0.5 to 2 unit length shorter than LSBM. This can be explained by the limitation in rerouting backup paths within only two adjacent domains.

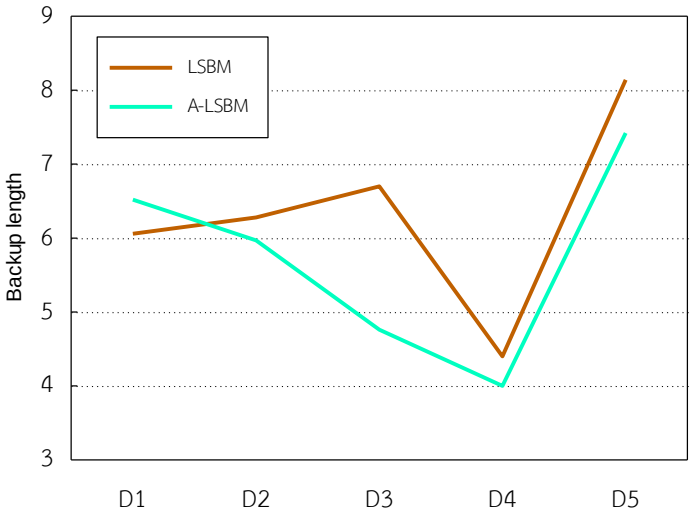


Figure 5.20: Comparison of average backup path length between LSBM and A-LSBM in the LARGE-5 network.

Table 5.9: Average backup path length for inter-domain link and intra-domain link protection.

	ESPP	GSBM	A-GSBM	LSBM	A-LSBM
Inter-domain links	9.33	9.33	9.33	3.00	3.00
D1	5.67	5.81	5.90	6.06	6.52
D2	5.20	7.08	6.67	6.28	5.97
D3	5.02	4.98	5.67	6.70	4.76
D4	4.35	4.72	5.90	4.40	4.00
D5	6.65	7.39	7.49	8.14	7.42

Table 5.8 presents precisely the information of backup path length for each described approach in detail. First of all, since LSBM and A-LSBM protection inter-domain links locally rather than asking for supports from domains like other

approaches, they have the backup length of 3 units compared to 9.33 of ESPP, GSBM, and A-GSBM. However, the backup length for intra-domain link protection depends on the domain structure (number of nodes, node degree) and working traffic demand.

Table 5.10: Summary performances of ESPP, GSBM, A-GSBM, LSBM, and A-LSBM.

	ESPP	GSBM	A-GSBM	LSBM	A-LSBM
Spare capacity	4175	3649	3306	4173	3943
Avg backup length	6.04	6.54	6.83	5.76	5.28

Table 5.9 summarizes the performances of five approaches: ESPP, GSBM, A-GSBM. LSBM and A-LSBM for the LARGE-5 topology with total working capacity are 4535 units. It is clearly seen that all four novel approaches offer more efficient performance in terms of saving backup resources compared with conventional ESPP. LSBM is most expensive solution among these four but its backup length is acceptable, while A-GSBM requires longest backup path with a promising number of needed spare capacity.

5.5 Summary of shared-mesh protection strategy in multi-domain networks

This chapter proposed four strategies for multi-domain network survivability using shared mesh protection technique in which GSBM and A-GSBM allow backup paths to traverse entire network while LSBM and A-LSBM limit these paths within 2 adjacent domains. Both approaching directions show the advantage in saving backup resources compared with their inspired approaches: ESPP and SSPP. However, these above approaches require longer restore routes which may increase network latency.

CHAPTER 6: CONCLUSION

This thesis investigates on designing two strategies for survivable multi-domain large-scale optical networks. Firstly, an improved aggregation model for domain privacy is proposed in order to offer network restorability using well-known p-cycle protection technique. The protection strategy developing from our proposed model can guarantee 100% single link failure restorability with less required backup resource compared to the conventional model.

Secondly, two different protection schemes, namely GSBM and LSBM based on shared-mesh protection technique are introduced. Both schemes improve the saving capacity efficiency compared to its inspired strategy. Each scheme can be sub-categorized into two options depending on planning demand whether saving backup resources or minimizing network latency is the default priority in the system. The numerical results show that A-GSBM is a most efficient solution in term of saving spare capacity, while A-LSBM keeps network latency low with an acceptable amount of needed backup resource.

Since this thesis concentrates on solving multi-domain survivability problem for opaque networks, our proposed strategy can be further extended for transparent optical networks. For example, routing and wavelength assignment can be applied to address the traffic demands.

APPENDIX: THE ONO TOOL

Optical Network Optimization (ONO) Tool is an open-source user-friendly software for optical network optimization. It can solve interesting optical network problems, including finding the minimum spare capacity needed to fully recover network traffic from single link failure using link protection techniques: multi-ring, p-cycle and mesh protection, and other basic problems such as finding shortest paths between network nodes and determining nodes on the network boundary. It is a Graphical User Interface (GUI) based software. Accordingly, it can be conveniently used to help in actual planning of network resource allocation with survivability or demonstrating basic concepts in optical networks for teaching and training purposes.

A.1 Introduction

In the past few decades, there has been massive growth of traffic demand, especially over the Internet. Such a growth is expected to continue with emerging services and applications such as IoT, sensor and machine-driven traffic, cloud computing, virtual reality, combined with live streaming video and mobile traffic. To meet with the next generation network capable of connecting human, machine and everything together over large-scale worldwide telecommunications, fiber-optic broadband is now seen as the most relevant technology to provide enormous capacity.

As the network capacity increases than ever before, the need for protection against certain type of failures become even greater. Single link failures in particular are most common in practical broadband networks and always lead to service interruption, causing huge loss of revenues both customers and operators. Therefore, many researchers and commercial network companies pay more attention on optical networks survivability. To date, there is no effective tool that is freely available for carrying out optical network design and optimization covering network survivability with friendly graphical user interface. In this paper, we present a development of a software tool that aims to support the whole process of optical network planning from designing topology, assigning working traffic to optimizing network protection.

The rest of this paper is organized as follows: First, we give an overview of ONO Tool and then describe its main functions in detail. We then discuss some results observing from mathematical simulations. Finally, conclusion and work plan for further consideration of ONO Tool are mentioned.

A.2 ONO Tool

ONO Tool is written in Python as an extension of WDM Planner [22] with emphasis on link protection. It works in conjunction with two other powerful open-source packages: PuLP and GNU Linear Programming Kit (GLPK) [27] to solve mixed integer linear programming problems. ONO Tool accepts the input from the user such as network topology, working traffic demand, geographical map and link protection technique and problem to be solved. It uses the programs that are developed by our team to generate the objective function, constraints and variables for relevant Integer Linear Programming (ILP) problems. PuLP, which is a modeler, is then used to call an ILP solver. In our current version, we use GLPK as an ILP solver although other effective solvers like CPLEX can be incorporated. Once an optimal solution is available, the related information is graphically displayed on the screen.

Moreover, ONO Tool also supports a new approach to randomly generate a nearly planar graph in order to achieve a more realistic set of test networks as well as finding a network boundary that can be applied to handle further sophisticated problems for WDM network optimization.

A.2.1 User interface

An example of use of interface of ONO Tool is shown in Fig. A.1. It has the following components.

1. Menu bar: The main functions of the program can be found systematically in the menu bar. It contains functions such as, Network Topology, Basic Tools, Link Protection, Maps and Help tab. Each tab carries its sub-functions that appear while you are holding the cursor over an item on the primary menu.

2. Command panel: The command panel is displayed differently based on which function the user is working on. For example, the command panel contains Create

Node menu and Create Edge buttons when the user is in Network Topology, whereas in Link Protection, the user can adjust working traffic demands and how the network is protected.

3. Network topology panel: This is the panel for displaying the network topology. It also shows the graphical map or information such as the traffic paths between network nodes and the backup capacity on each link.

4. Information panel: This panel is for displaying the information related to the computational results such as cost of a link, optimum cost of spare capacity, and so on.

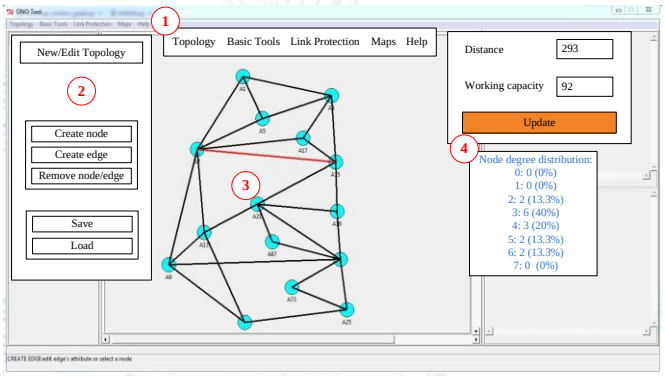


Figure A.1: ONO Tool in the New/Edit topology tab.

A.2.2 Generating random graphs

Due to the limited options on available test backbone network topologies such as Bellcore, SmallNet, NSFNet, and so on, the need of enhancing the diversity of testing resources has not been fulfilled. One efficient technique was published in [28] using a preferential attachment mechanism, but the outputs of random graphs are quite unrealistic with high crossing density. In [29], W. D. Grover introduced an algorithm to generate random planar graph with nodes being on grid using locality parameter that is maximum length of span in term of Euclidean distance. From that paper, an experimental target node degree distribution was observed based on published examples of real transport networks. Through ONO Tool, we propose an approach which is inspired by paper [29] to generate a set of nodes and links with a small number of crossing points between links.

Fig. A.2 shows an example of generating a random graph with 9 nodes firstly distributed as in Fig. A.2a. After applying step 2 of the above procedure, the set of links: (1, 9), (2, 5), (3, 5), (4, 2), (6, 3) is formed in Fig. A.2b. It is noted that, at this stage, there are still isolated nodes and nodes having degree of 1, so step 3 was introduced in Fig. A.2c in order to have (1, 6), (3, 8), (4, 9), (5, 7), (7, 8) connected. In next two figures, step 4 was implemented with more flexible connecting constraints. Finally, the node degree distribution is displayed in Fig. A.2f which is not exactly equal to the target figure, but in simulation results we can get a more similar distribution with a higher number of nodes.

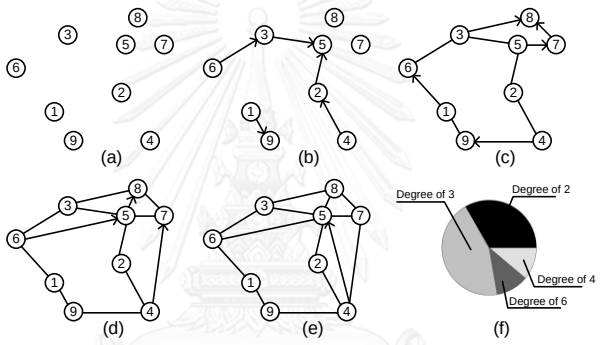


Figure A.2: An example of generating a random graph.

A.2.3 Link protection

When it comes to network survivability or protection in particular, path protection and link protection schemes are the main means of protecting wavelength-division multiplexed (WDM) networks from the losses caused by a link failure [26]. Since link failures are common, only link protection is considered in the scope of ONO Tool and this paper. Protection can be implemented using ring topologies or arbitrary mesh topologies. Ring protection tends to be simpler on the protection structure, although its additional constraints generally result in more required spare capacity as compared to mesh protection. Additionally, p-cycle protection was introduced by W. Grover with the benefit of having needed spare capacity little or no more than mesh restorable network while addressing the speed limitation of mesh-based restoration [13].

ONO Tool offers all three basic techniques: multi-ring, p-cycle and mesh protection with the identical input parameters which are working capacities of the links. The following section presents three set of ILP formulation with the purposes of:

- Protecting all the working capacities on the links.
- Spare capacity is minimized through optimization.
- Deciding on the set of ring or p-cycle or restorable paths to protect the network against a link failure which minimizes the total cost of spare capacity.

The formulation determines a set of protection cycles and a set of protection rings which minimize the total cost of spare capacity.

A.2.4 Finding a network boundary

Finding the boundary of a graph is not a difficult problem and some algorithms are known to exist, such as determining the convex hull of a finite planar set in [30]. In ONO Tool, this feature is considered useful for certain aspect of network design, especially to our current research on link protection strategy using two sub-networks [31].

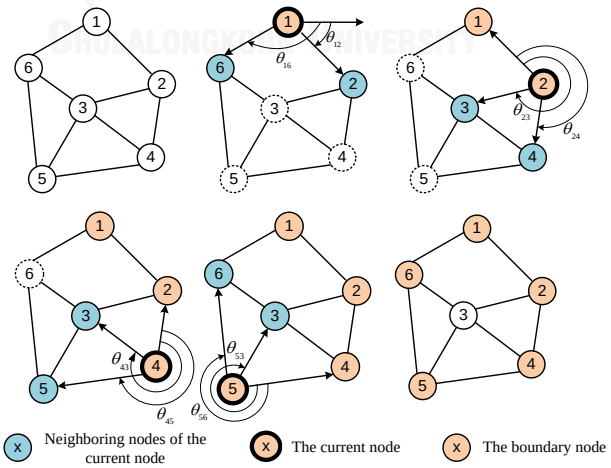


Figure A.3: An example of finding boundary nodes by the proposed algorithm.

Given a network topology of *N* nodes and *L* un-directional links that is represented by a node adjacency list, the objective is to find the boundary of the graph, which is formed as a series of connected nodes. The procedure is as follows:

1. Find the node that is located at the top of the network and assign this node as the start node.

2. From the start node, list all its neighboring nodes and form a vector for each neighboring node, which originating from the start node and ends at each corresponding neighboring node. Find an angle between these vectors with vector [1, 0] in clockwise direction. A neighboring node is chosen, if its angle is the minimal, the chosen node is then set as the current node.

3. From the current node, list all its neighboring nodes and form a vector for each neighboring node with reference to the current node. Find the angles between these vectors and the reference vector that starts at the current node and ends at its neighboring nodes. Choose the node with the minimum angle.

4. Repeat 3 until the chosen node is back to the start node.

An example of finding border nodes is shown in Fig. 3. First, node 1 was chosen as it is the highest node in the topology. In step 2, node 2 is the next border node. The next steps are the progress of having nodes 4, 5, and 6 in the border node list. Lastly, we achieve the set of boundary nodes: 1, 2, 4, 5 and 6.

A.3 Simulation results using ONO tool

An illustrative example of randomly generated networks is shown in Fig. A.4 with the number of nodes gradually increases: 20, 40, 60, 80, 100 and 120 nodes. It is clearly seen that these networks are nearly planar since the number of cross-connections are acceptable.

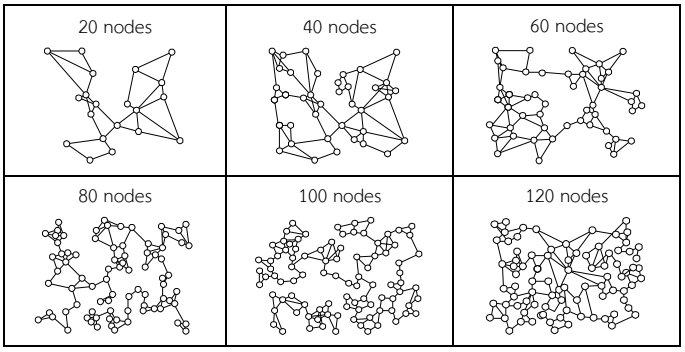


Figure A.4: An illustrative example of randomly generated networks by ONO Tool.

Fig. A.5 presents the differences in node degree distributions of 6 random networks shown in Fig. A.4. It illustrates that the node degree distributions of all networks are within ±2.5% of the target as recommended in [29]. It is particularly closer for large number of nodes.

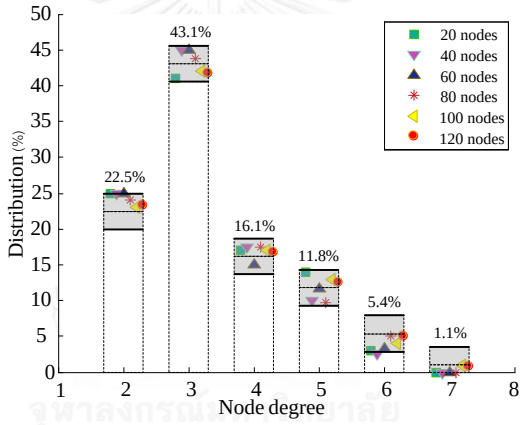


Figure A.5: Node degree distribution of randomly generated networks in the range of the target distribution.

Table A.1: The comparison of optimal results from different protection techniques.

Testing network	Working capacity	Spare capacity			Cycles used/Total cycles	
		Rings	p-cycle	Mesh	Ring	p-cycle
Bellcore	1400	1532	939	784	20/541	8/541
NSFNET	1191	1288	1001	922	15/100	10/100
SmallNet	955	1030	675	479	18/243	9/243

Table A.1 shows the numerical results of optimizing link protection using ONO Tool. Three most popular test networks: Bellcore, NSFNET and SmallNet [15] are used with

random traffic demand in the range of [0-100] (Gbps). ONO Tool does not only show the efficiency of each technique in term of saving spare capacity, but also displays every protection cycle that is used to back up working traffic and its capacities.

A.4 Conclusion

We developed a network design tool that can help solve some network design problems taking into account survivability of a network against single link failure. The tool can solve the main network optimization problems, namely, minimizing the spare capacity for 100% restoration using multi-ring, p-cycle and mesh protection technique. Our tool is easy to use and does not require a large amount of computing resources with typical sizes of backbone network. In addition, it does not require any licensed software to operate, and hence can be used to reduce the lack of educational tools in developing countries.

REFERENCES

1. Truong, D.L. and B. Thiongane, *Dynamic routing for shared path protection in multidomain optical mesh networks.* Journal of Optical Networking, 2006. **5**(1): p. 58-74.
2. Singh, H.M. and R.S. Yadav, *Partitioning-based approach to control the restored path length in p-cycle-based survivable optical networks.* Photonic Network Communications, 2016: p. 1-10.
3. Drid, H., et al., *Survivability in multi-domain optical networks using p-cycles.* Photonic Network Communications, 2010. **19**(1): p. 81-89.
4. Ramaswami, R., K. Sivarajan, and G. Sasaki, *Optical networks: a practical perspective*. 2009: Morgan Kaufmann.
5. *Google Images*. Available from: https://www.shutterstock.com/search/telecommunications.
6. Dahl, G. and M. Stoer, *A cutting plane algorithm for multicommodity survivable network design problems.* INFORMS Journal on Computing, 1998. **10**(1): p. 1-11.
7. Poulsen, H.N., et al. *Network Layer Modeling of WDM Fiber Optic Network Architectures for Aerospace Platforms*. in *2007 IEEE Avionics, Fiber-Optics and Photonics Technology Conference*. 2007.
8. Stern, T.E., G. Ellinas, and K. Bala, *Multiwavelength Optical Networks: Architectures, Design, and Control*. 2008: Cambridge University Press. 1004.
9. Pathak, B.R. and S.S. Tangade, *Survivability Issues in Optical Wavalength Division Multiplexing (WDM) Network.*
10. Maier, G., et al., *Optical network survivability: protection techniques in the WDM layer.* Photonic Network Communications, 2002. **4**(3-4): p. 251-269.
11. Wuttisittikulkij, L. and M. O'Mahony. *Multiwavelength self-healing ring transparent networks*. in *Global Telecommunications Conference, 1995. GLOBECOM'95., IEEE*. 1995. IEEE.

12. Tholey, V., et al., *Demonstration of WDM survivable unidirectional ring network using tunable channel dropping receivers.* Electronics Letters, 1994. **30**: p. 1323-1324.
13. Akyamaç, A.A., et al., *Reliability in single domain vs. multi domain optical mesh networks.* IEEE/OSA NFOEC, 2002.
14. Ou, C., et al., *Subpath protection for scalability and fast recovery in optical WDM mesh networks.* IEEE Journal on Selected Areas in Communications, 2004. **22**(9): p. 1859-1875.
15. Guo, L., *LSSP: A novel local segment-shared protection for multi-domain optical mesh networks.* Computer Communications, 2007. **30**(8): p. 1794-1801.
16. Zhang, X., et al. *On segment-shared protection for dynamic connections in multi-domain optical mesh networks*. in *Asia Pacific Optical Communications*. 2008. International Society for Optics and Photonics.
17. Guo, L., et al., *A novel domain-by-domain survivable mechanism in multi-domain wavelength-division-multiplexing optical networks.* Optical Fiber Technology, 2009. **15**(2): p. 192-196.
18. Xie, X., et al. *A shared sub-path protection strategy in multi-domain optical networks*. in *2007 Asia Optical Fiber Communication and Optoelectronics Conference*. 2007.
19. Szigeti, J., et al., *p-Cycle protection in multi-domain optical networks.* Photonic Network Communications, 2009. **17**(1): p. 35-47.
20. Lee, W.C., *Topology aggregation for hierarchical routing in ATM networks.* ACM SIGCOMM Computer Communication Review, 1995. **25**(2): p. 82-92.
21. S., P., *Optical Networks*. 2013: Asian Institute of Technology.
22. Vesarach P., Y.W., Saengdomlert P., *WDM Planner: WDM Network Optimization Tool*, in *The 31st International Conference on Circuirts/Systems, Computers and Communications*. 2016: Japan.
23. Quynh, L., et al., *Optical network optimization tool with network survivability*, in *International Conference on Electronics, Information, and Communications*. 2017: Phuket, Thailand.

24. *Tkinter*. Available from: https://wiki.python.org/moin/TkInter.

25. Grover, W.D. and D. Stamatelakis. *Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-planning network restoration*. in *Communications, 1998. ICC 98. Conference Record. 1998 IEEE International Conference on*. 1998.

26. Zyane, A., Z. Guennoun, and O. Taous. *Performance evaluation of shortest path routing algorithms in wide all-optical WDM networks*. in *2014 International Conference on Multimedia Computing and Systems (ICMCS)*. 2014.

27. Ferguson, T.S., *Linear programming: A concise introduction.* UCLA [online] http://www. math. ucla. edu/~ tom/LP. pdf, 2000.

28. Gupta, A., *Fast and effective algorithms for graph partitioning and sparse-matrix ordering.* IBM Journal of Research and Development, 1997. **41**(1.2): p. 171-183.

29. M., D. and M. B., *Maximally Balanced Connected Partition Problem in Graphs: Application in Education.* The Teaching of Mathematics, 2012. **15**: p. 121-132.

30. Mello, D.A., et al. *Inter-arrival planning for sub-graph routing protection in WDM networks*. in *International Conference on Telecommunications*. 2004. Springer Berlin Heidelberg.

31. Djidjev, H.N., *On the problem of partitioning planar graphs.* SIAM Journal on Algebraic Discrete Methods, 1982. **3**(2): p. 229-240.

REFERENCES

APPENDIX

VITA

Mr. Quynh Quang Le is currently a Master student at the department of Electrical Engineering, Chulalongkorn University (CU). He received the Bachelor of Engineering in Electronic and Telecommunications from Hanoi University of Science and Technology (HUST), Vietnam in 2014. Mr. Quynh has been awarded the AUN/SEED-Net scholarship in Master level. His research interests mainly include optical network survivability, LTE and 5G HetNets.