2017

Resilient Resource Allocation Schemes in Optical Networks

Saja Al Mamoori
University of Windsor

Resilient Resource Allocation Schemes in Optical Networks

By:
Saja Al Mamoori

A Dissertation
Submitted to the Faculty of Graduate Studies
Through the School of Computer Science
in Partial Fulfillment of the Requirements for
The Degree of Doctor of Philosophy at the
University of Windsor

Windsor, Ontario, Canada
2017

Resilient Resource Allocation Schemes in Optical Networks
by
Saja Al Mamoori

APPROVED BY:

A. Sen, External Examiner
Arizona State University

K. Li
Odette School of Business

S. Bandyopadhyay
School of Computer Science

A. Ngom
School of Computer Science

A. Jaekel, Advisor
School of Computer Science

November 22, 2017

Declaration of Co-Authorship / Previous Publication

I Co-Authorship Declaration

I hereby declare that this thesis incorporates material that is a result of joint research, as follows:

This thesis incorporates the results of my research under the supervision of Professor Arunita Jaekel. This research was part of the joint investigations carried out by Professors Arunita Jaekel and Subir Bandyopadhyay. The results of my research is covered in Chapters 3-6 of the thesis. The research reported in Chapter 4 was carried out in collaboration with a Master student, Mr. Sriharsha Varanasi. The contribution of Mr. Varanasi was to implement the integer linear program (ILP) I had developed with suggestions from Professors Arunita Jaekel and Subir Bandyopadhyay. In all cases, the key ideas, primary contributions, justifications of the methodologies, the design of the experiments, data analysis and interpretations, were performed by myself with the guidance of Professors Arunita Jaekel and Subir Bandyopadhyay.

I am aware of the University of Windsor Senate Policy on Authorship and I certify that I have properly acknowledged the contribution of other researchers to

my thesis, and have obtained written permission from each of the co-author(s) to include the above material(s) in my thesis.

I certify that, with the above qualifications, this thesis, and the research it reports, is the product of my own work.

II Declaration of Previous Publication

This thesis includes 4 original papers that have been previously published in peer reviewed journal and conferences as follows:

Thesis Chapter	Publication title/full citation	Publication status
Chapter 3	Security-aware dynamic RWA for reducing in-band and out-of-band jamming attacks in WDM Optical Networks; Al Mamoori, S.; Jaekel, A; Bandyopadhyay, S.; Sriharsha Varanasi; Journal of Networks; December 2015, DOI: 10.4304/jnw.10.11.587-596. Copyright ©2015, ACADEMY PUBLISHER.	Published
Chapter 4	Designing resilient WDM data center networks for dynamic lightpath demands; Al Mamoori S.; Jaekel A.; Bandyopadhyay S.; IEEE Symposium on Computers and Communications (ISCC), July 2017, (pp. 724-729). Copyright ©2017, IEEE.	Published
Chapter 4	Resilient RWA Algorithm Using Path Protection ffor Data Center Networks (DCNs); Al Mamoori S.; Jaekel A.; Bandyopadhyay S.; OSA Photonic Networks And Devices (OSA NETWORKS), July 2017, (pp. JTu4A-21). Copyright ©2017, Optical Society of America.	Published
Chapter 5	Robust Data Center Network Design Based on Space Division Multiplexing; Al Mamoori S.; Jaekel A.; Bandyopadhyay S.; International Conference on Computing, Networking and Communications (ICNC). March 2018, Copyright ©2018, IEEE.	Accepted for Publication IEEE

I certify that I have obtained a written permission from the copyright owner(s) to include the above published material(s) in my thesis. I certify that the above material describes work completed during my registration as graduate student at the University of Windsor.

I declare that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

Abstract

Recent studies show that deliberate malicious attacks performed by high-power signals can put large amount of data under risk. We investigate the problem of survivable optical networks resource provisioning scheme against malicious attacks, more specifically crosstalk jamming attacks. These types of attacks may cause service disruption (or possibly service denial). We consider optical networks based on wavelength-division multiplexing (WDM) technology and two types of jamming attacks: in-band and out-of-band attacks. We propose an attack-aware routing and wavelength assignments (RWA) scheme to avoid or reduce the damaging effects of potential attacking signals on individual or multiple legitimate lightpaths traversing the same optical switches and links. An integer linear programs (ILPs) as well as heuristic approaches were proposed to solve the problem. We consider dynamic traffic where each demand is defined by its start time and a duration. Our results show that the proposed approaches were able to limit the vulnerability of lightpaths to jamming attacks.

Recently, large-scale failures caused by natural disasters and/or deliberate attacks have left major parts of the networks damaged or disconnected. We also investigate the problem of disaster-aware WDM network resource provisioning in case of disasters. We propose an ILP and efficient heuristic to route the lightpaths in such a way that provides protection against disasters and minimize the network

resources such as the number of wavelength links used in the network. Our models show that significant resource savings can be achieved while accommodating users demands.

In the last few years, optical networks using Space Division Multiplexing (SDM) has been proposed as a solution to the speed bottleneck anticipated in data center (DC) networks. To our knowledge the new challenges of designing such communication systems have not been addressed yet. We propose an optimal approach to the problem of developing a path-protection scheme to handle communication requests in DC networks using elastic optical networking and space division multiplexing. We have formulated our problem as an ILP. We have also proposed a heuristic that can handle problems of practical size. Our simulations explore important features of our approach.

Dedication

To my:

parents: Fakhria Jawad and Kamil Mansour Al Mamoori

Husband: Hussein M. Al Mamoori

Daughters: Maryam and Nora

– I am so blessed to have you in my life.

Acknowledgements

It gives me immense pleasure to thank a few very important people who have helped me a lot during the whole process of my graduate studies.

At first, I would like to express my sincere gratitude to my supervisor, Dr. Arunita Jaekel, for her constant guidance and extensive support throughout my graduate studies. This work could not have been achieved without her continuous encouragement, valuable advices, suggestions and cooperation.

I would like to express my deep appreciation to Dr. Subir Bandyopadhyay for his kind support and advice during the period of my graduate study here.

I would like to thank Dr. Arunabha Sen for his kind acceptance to be the external examiner of my thesis defence.

I would like to thank members of my Ph.D. thesis committee, Dr. Subir Bandyopadhyay, Dr. Alioune Ngom and Dr. Kevin Li for their instructive advices, suggestions and comments.

I would also like to thank all the faculty and staff members at the School of Computer Science, for their cordial supports and helps, as well as everybody else who has offered any help, during my graduate study at the University of Windsor.

Finally, I would like to thank my husband, Hussein, for his endless love and care and for always being there for me.

Contents

List of Tables

List of Figures

List of Acronyms

AON - All Optical Network

BILP - Binary Integer Linear Program

DC - Data Center

DCN - Data Center Network

DPP - Dedicated Path Protection

DLA - Dynamic Lightpath Allocation

DSLA - Dynamic Survivable Lightpath Allocation

DWDM - Dense Wavelength Division Multiplexing

EON - Elastic Optical Network

ILP - Integer Linear Program

LP - Linear Program

LT - Logical Topology

LAR - Lightpath Attack Radius

IAR - In–band Attack Radius

MCNF - Multi Commodity Network Flow

MILP - Mixed Integer Linear Program

OADM - Optical Add Drop Multiplexer

OEO - Optical Electronic Optical

OFDM - Orthogonal Frequency Division Multiplexing

OTN - Optical Transport Network

OXC - Optical Cross Connect

PP - Path Protection

PT - Physical Topology

RWA - Routing and Wavelength Assignment

SDM - Space Division Multiplexing

SLA - Static Lightpath Allocation

SPP - Shared Path Protection

SRLG - Shared Risk Link Group

TON - Transparent Optical Network

WAN - Wide Area Network

WDM - Wavelength Division Multiplexing

Chapter 1

Introduction

1.1 Optical Networks Fundamentals

For the past decades, the immense growth of data traffic, primarily Internet traffic, and the significant demand for network capacity has created an ever increasing need for long-haul high-speed communication networks. Optical networks offer many advantages such as high bit rate and low attenuation and are considered as the only future-proof technology to handle such immense growth of data traffic [1–4]. The rest of this section briefly presents the main concepts and principles used in optical networks. In section 2.1 of chapter 2, we will discuss the state-of-art in optical networks in more details.

One of the main advancement in optical networks is *WDM technology*, which has made possible high throughput backbone networks [5–7]. In WDM optical networks multiple optical signals, called *lightpaths* (i.e., optical end-to-end connections) can be established between pairs of nodes [8, 9]. Each lightpath has the ability to transmit a data rate of nearly 40 Giga bits per second (Gbps). Typically, communication requests can be classified into *static* traffic and *dynamic* traffic [3, 10]. Under static

traffic scenario, requests are known in advance and established on a semi-permanent manner on the network. On the other hand, with dynamic traffic scenario, a light-path is eastablished when a request arrives and torn-down when the communication is over. In our research work, we consider dynamic traffic model.

In this dissertation, we consider transparent optical networks (TONs), also called all-optical networks (AONs). In AONs, *transparent lightpaths* are established between the source and destination to accommodate user's requests. They are called transparent because they do not undergo optical-electronic-optical (OEO) conversion at intermediate nodes. More details on AONs will be discussed in chapter 2.

A set of lightpaths is established by assigning a physical route and a wavelength to each lightpath, this is called routing and wavelength assignment (RWA) problem [11,12]. RWA is a widely discussed problem in optical network planning, which deals with the establishment of lightpaths. RWA involves finding:

- A physical route in the network topology (i.e. a path traversing one or more optical fiber(s) from the source to the destination) and
- a unique wavelength, not used by any other lightpath on all the fibers along the route

Both Integer Linear Programming (ILP) and heuristic approaches have been used to solve the RWA problem [10]. Based on the traffic scenario, RWA problem can be classified into *static RWA* and *dynamic RWA*.

In recent years, the concept of *data center network* (DCN) has received lots of attention by researchers. Mainly, a *data center* (DC) is a group of networked servers that are used for storing and distributing large amounts of data. A network of data centers is called a *Cloud*. Recently, optical networks using space division

multiplexing have been proposed as a solution to the speed bottleneck anticipated in data center networks [13]. In our research work reported in chapters 3-5, we propose efficient resource allocation approaches in WDM and SDM data center optical networks.

Optical networks are vulnerable to malicious attacks and failures. In this dissertation, we consider a type of malicious attacks called *crosstalk jamming* attacks. These types of attacks may cause large data loss and have the ability to propagate through the network. Typically, crosstalk jamming occurs at the network physical layer inside optical switches, amplifiers, and fibers. On the other hand, large-scale failures, such as disasters, can destroy major parts of the network and cause sever service unavailability and data loss. Therefore, developing survivable strategies to handle such attacks and failures are of great importance. We propose novel approaches to solve attack-aware (disaster-aware) RWA in DC optical networks with dynamic traffic in chapter 3 (4), respectively.

Recent developments in multi-core fibers (MCFs), multi-mode fibers (MMFs), or bundles of single-mode fiber(SMF) have led to the notion of *space division multiplexing* (SDM). Due to the increasing and continuous demand for bandwidth, optical fibers are expected reach their capacity limits in the next few years [14–16]. This is called optical network *capacity crunch*. SDM-based network architectures appear as a viable option for overcoming such bandwidth limitations. In SDM networks, requests can be provisioned by creating sliceable spectral-spacial superchannels (S2-SChs). We consider SDM technology in our research work reported in chapter 5.

1.2 Research Reported in this Dissertation

1.2.1 Attack-aware RWA in WDM networks

There is growing recognition of the need to develop suitable mechanisms for reducing the adverse effects of malicious attacks such as *crosstalk jamming attacks* [17]. Such types jamming attacks can be achieved by the attacker by exploiting the security vulnerabilities of optical components such as optical switches and fibers [18, 19]. The attacker can inject a high-power signal on legitimate channel to damage or deteriorate other normal signals. This may lead to service disruption or even service denial. Crosstalk jamming attacks can be classified into: i) *in-band*, also called *intra-channel* crosstalk attacks that happen inside the optical cross-connects (OXCs) [20], and ii) *out-of-band*, also called *inter-channel* crosstalk attacks that may occur in the optical fibers [21]. A detailed explanations of various types of crosstalk attacks as well as optical components' security issues will be presented in chapter 2.

In this research we propose to solve the attack-aware RWA problem under dynamic traffic scenario. The significance of our approach is that unlike previous approaches we jointly solve the routing and wavelength assignment sub-problems and consider both in-band and out-of-band attacks. Some approaches from the literature considered both types of attacks but mostly proposed with protection. The main idea is to route the primary and backup lightpaths, of a particular request, in such away to avoid being within the reach of the same attacker. To the best of our knowledge, this is the first such approach for dynamic traffic and the first to jointly consider in-band and out-of-band attacks, for either static or dynamic case.

1.2.2 Resilient DCN Design using WDM

Resilient network design to handle large-scale failures or disasters is now a popular research area [22–26]. In this dissertation, we propose an optimal approach to the problem of developing a path-protection scheme to handle requests for communication in DCNs. We consider WDM networks with dynamic traffic case. In this study, we assume that a disaster can damage all the components of the network (e.g., fibers, routers or data centres) located in a specific geographical area, (i.e., region-based disasters) [27].

We apply the principle of *shared path protection* (SPP) where backup lightpaths are allowed to share resources if the corresponding primary lightpaths are *disaster-zone disjoint* (DZ-disjoint). Lightpaths can be DZ-disjoint if they do not traverse the same disasters that may affect other lightpaths. Our problem is novel as it takes into account dynamic requests and the results obtained are interesting. The proposed approach is successful in saving significant resources while accommodating user's demands. Also, with increased number of disasters, the algorithm do not add significantly to the cost of the solution.

1.2.3 Resilient DCN Design using SDM

This thesis also proposes an optimal algorithm to design DCNs based on SDM technology that can survive single disasters. We investigate the design of a high-speed optical DCN that guarantees reliable communication, even when a disaster occurs. To achieve ultra high speed communication, we study SDM elastic optical networks. To the best of our knowledge, this is the first study of reliable DCN design using SDM.

Spectrally and spatially flexible optical networks are likely to be ideal candidates for ultra high speed communication needed for DCNs [28, 29]. In this study, we use

the networks based on the flex-grid fixed-SDM model [30]. The details and features to this model compared to other SDM models proposed will be covered in chapter 2 and 5. Since this is a very reaccent research area, we propose an optimal algorithm to solve the *routing, spectrum, and core allocation* (RSCA) problem to design a survivable DCNs to handle disasters. The network considered is SDM-based and it supports dynamic traffic. The approach uses *dedicated path protection* (DPP) technique to provision primary lightpaths in a fault-free case. The algoritms can switch to a backup lightpath in case disasters may affect the primary one. To the best of our knowledge this is the first approach that considers the RSCA problem for DCNs and dynamic traffic to survive disasters.

1.3 Thesis Objectives and Solutions Outline

This dissertation proposes an efficient strategy for resource allocation in resilient optical networks. The aim of this strategy is to minimize or avoid the damaging effects due to attacks and disasters. Also we tried to minimize network resources as a secondary objective, measured by the number of wavelength links allocated to requests for communications. All our research work consider dynamic traffic scenario. The thesis introduces new models for optimal network design against crosstalk jamming attacks and large-scale disasters. The schemes proposed and main contributions to solve each problem are given below:

- Attack-aware RWA for WDM optical networks: we propose an optimal algorithm to jointly minimize the disruptive effects of in-band and out-of-band crosstalk jamming attacks under dynamic traffic. The problem is formulated into as an integer linear program (ILP). For larger networks, we also propose a heuristic algorithm to get sup-optimal solutions in reasonable time. We have done an extensive simulations comparing the performance of these

two approaches. The proposed approaches are compared with the traditional security unaware algorithms for RWA and the results demonstrate that our proposed security-aware approaches are able to limit the vulnerability of lightpaths with very little overhead in terms of resource consumption and blocking probability.

- Disaster-aware RWA for WDM optical networks: an optimal algorithm, ILP formulation, is proposed to solve this problem under dynamic traffic. The objective is to provision resources to requests in such a way that a primary lightpath will be used in the fault free-case. In case of disasters that may affect the primary lightpath, a backup lightpath will be used. We use the concept of SPP to allow backup lightpaths to share resources. Also, we propose a heuristic to solve the problem for practical-sized networks. Our model is novel as it considers dynamic lightpath allocation for DCN with path protection. In addition, our results indicate that the proposed approach can handle more disasters with a slight increase in resource usage.

- Disaster-aware RSCA for SDM optical networks: to solve this problem, we present an ILP formulation for resource provisioning and handling disasters in DCNs using SDM technology for dynamic requests and using DPP. The importance of our work in this area is that it is the first such formulation to consider solving the RSCA problem for DCN using path protection. We adapt the flex-grid fixed SFM model to realize the SS-SChs that will be provisioned to accommodate requests. We evaluate our proposed algorithm by varying a number of parameters such as the number of DCs in the network, the number of cores per fiber, and the number of frequency slices per core.

1.4 Thesis Organization

The rest of this thesis is organized as follows. In Chapter 2 we review the related work proposed in the literature focusing on three main areas:

- Security-aware RWA for WDM networks.
- Disaster-aware RWA for WDM networks.
- Disaster-aware RSCA for SDM networks.

We present our work on optimal security-aware RWA in Chapter 3. In Chapter 4, our research work on optimal disaster-aware RWA in datacenter optical networks is presented and discussed. Chapter 5 includes our work on lightpath allocation in SDM optical networks. We give our concluding remarks of this thesis, with our suggestions for future works, in Chapter 6.

Chapter 2

State-of-Art in Optical Networks and Literature Review

2.1 State-of-Art in Optical Networks

Internet traffic and the significant demand for network capacity have created an ever increasing need for high-speed communication networks [16]. Optical networks, characterized by their huge bandwidth of up to 50 THZ per fiber, low bit error rate of 10^{-12}, low loss of 0.2 dB/km, low noise & interference, and low cost have been established as the enabling technology for backbone networks [2].

2.1.1 All-Optical Networks (AONs)

Recently, the term *transparent optical networks* (TONs), also called *all-optical networks* (AONs) [31, 32], is widely used to refer to the capability of transmitting data from its source to its destination in the optical form without optical-to-electronic

(OEO) conversions. This feature is called *transparency* [2–4]. Transparency in optical networks provides high data rates and protocol-format insensitivity, but may introduce significant vulnerabilities and challenges to the network security [18, 33]. In AONs, corresponding to each request for communication, one (or more) optical signals, called *lightpaths*, is (are) established between the source node and the destination node specified in the request.

2.1.2 Wavelength-Division Multiplexing (WDM)

WDM technology enables multiple optical signals, each having a high data rate of the order of Giga bits per second (Gbps), to be transmitted simultaneously over a single optical fiber [34]. Figure 2.1 shows an outline of WDM technology in optical networks.

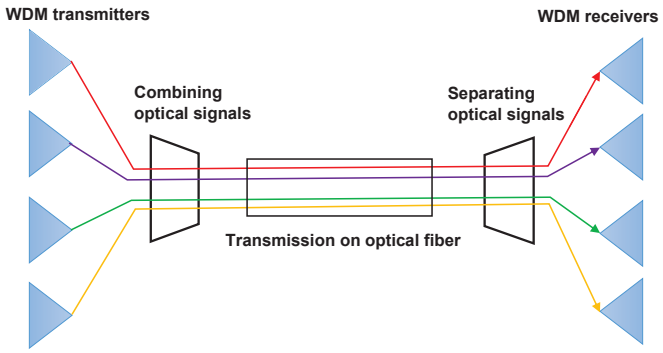


Figure 2.1: WDM technology in optical networks.

In WDM networks, the *physical topology* consists of physical links and nodes in the network whereas the *logical topology* consists of lightpaths between end nodes. Figure 2.2 a shows the physical topology of a small network topology of four end-nodes and four router nodes. Router nodes receive the data from either a source node or other router nodes and forward them to the destination node or next router node

in a route [35]. Here, the undirected lines represent fiber links and the directed lines represent lightpaths established over the physical topology. For example, lightpath L_1 can be set up to send data from end-node A to C. It starts from source node A, passes through router nodes $R1$, $R2$, $R3$, and finally reaches the destination node C. The set of lightpaths established creates the logical topology. Figure 2.2b the logical topology corresponding to the lightpaths shown in Fig. 2.2a. For example, logical edge $A \rightarrow C$ represents lightpath L_1.

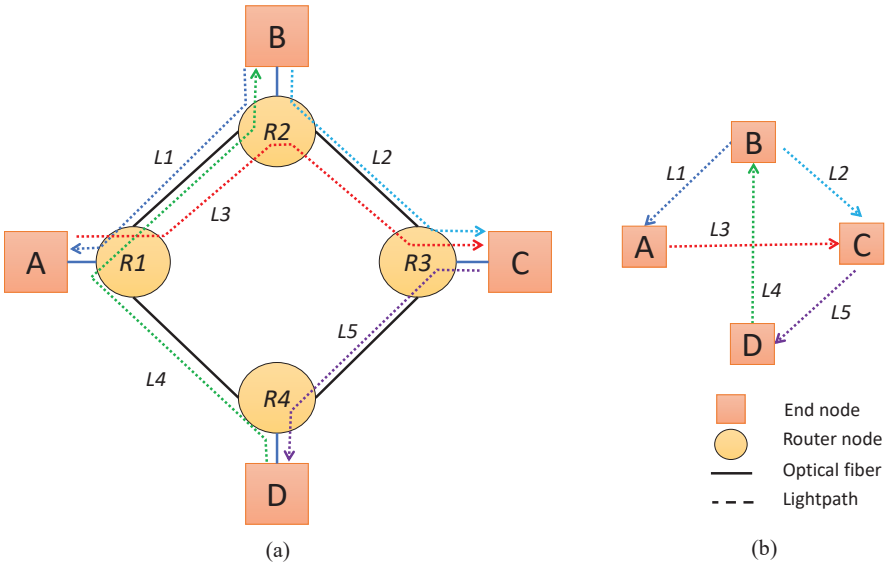


Figure 2.2: (a) Lightpaths established on the physical topology, (b) the logical topology corresponding to the physical topology.

2.1.3 Routing and Wavelength Assignment (RWA) problem

The RWA problem involves the establishment of lightpaths by finding a route and assigning a wavelength (i.e., a channel) to each lightpath [36]. RWA has been proven as NP-Complete class of decision problems in computer science [11, 37]. Therefore, several heuristic techniques has been proposed in the literature to solve this problem sub-optimally. In optical networks, lightpaths or connection requests may be

categorized into *static* and *dynamic* [11]. With static RWA, all connection requests are known in advance, and do not change significantly over relatively long periods of time. For the case of dynamic RWA, the requests are not known in advance. When a connection request arrives, a lightpath from the source node to the destination node specified in the request is set up, if possible. This lightpath is "torn down" after the communication is over, so that the resources used by the lightpath are available for future requests for communication. The objective in dynamic RWA is to set up lightpaths and assign wavelengths in a manner that minimizes the *blocking probability* - the ratio of the number of requests for communication that could be successfully handled to the total number of requests for communication [38, 39].

2.1.4 Space-Division Multiplexing (SDM)

Elastic optical networking (EON) allows each communication to dynamically adjust its resources (e.g., the optical bandwidth and modulation format), depending on bandwidth requirements and transmission characteristics for the communication [40]. SDM technology in EON networks was a result of recent developments in multi-core fibers (MCFs), multi-mode fibers (MMFs), or bundles of single-mode fiber(SMF) [41–43] to better handle the ever-increasing bandwidth demands and fiber capacity limitations. A number of modulation formats (e.g., BPSK, QPSK, 8-QAM and 16-QAM) have been proposed recently for optical networks [29]. These modulation formats have different spectral efficiencies (1, 2, 3 and 4) and different optical reaches (9600, 4800, 2400 and 1200 km) for BPSK, QPSK, 8-QAM and 16-QAM respectively [29, 44]. Available channel allocation options using the aforementioned technologies are *fixed-grid/Single* (for WDM networks), *flex-grid/single* (for EON), *flex-grid fixed-SDM* and *flex-grid flex-SDM* (For SDM networks) [30]. The last scheme offers the best utilization of spectrum resources but suffers from

fragmentation. In addition, needed technology to achieve flex-grid flex-SDM is still in the research phase [28]. In EON, a high-capacity *spectral super-channel* (SS-Ch) consists of a number of contiguous optical carriers (OCs), each using a certain modulation format and carrying a fraction of the aggregated traffic [29]. In SDM, the super-channels can be formed in both frequency and spatial domain, multiplexing several SSchs over a number of cores or modes in MCFs or MMFs, respectively, or over SMF bundles [28]. This defines a *spatial-spectral super-channel* (S2-SCh) in which the channel allocation flexibility spans over both the spectrum and space dimensions [28]. In flex-grid fixed-SDM model, a S2-SCh is a set of SSch's where the spectrum boundaries for each SSch in a S2-SCh are the same and no two S2-SCh are allowed to overlap. A diagram showing a S2-SCh is shown in Fig 2.3.

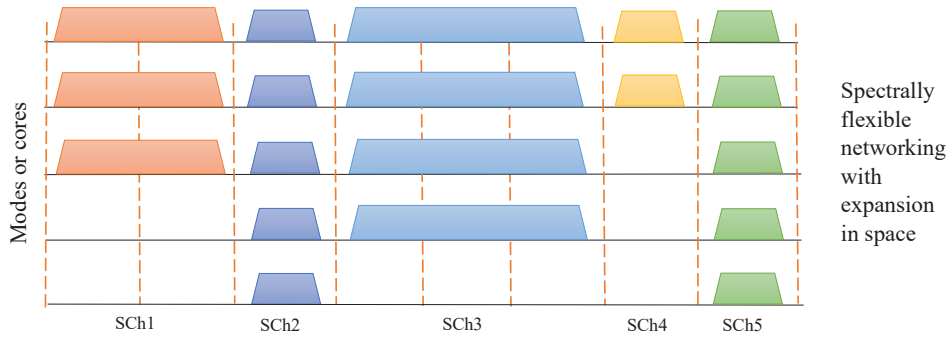


Figure 2.3: S2-SCh allocation scheme using the flex-grid fixed SDM model.

In a SDM network, for each request of communication, the routing, core and spectrum allocation (RCSA) algorithm tries to find a route and assign a set of contiguous frequency subcarriers [45]. This allows adaptive resource allocation scheme based on the bandwidth needed by the user. This allocation scheme is more efficient compared to WDM, where the entire optical channel (lightpath) bandwidth is reserved, without considering the user's requested bandwidth [15].

2.1.5 Faults and Protection Schemes in Optical Networks

There have been extensive studies on protection schemes to handle faults in optical networks [46, 47]. Mostly, the proposed schemes consider *single link failures* (SLF) only. *Path Protection* and *link protection* are most popular schemes used to handle faults, since they provide guaranteed fault recovery and fast recovery time [46]. For path protection, two techniques have been studied widely - *Dedicated Path Protection* (DPP) and *Shared Path Protection (SPP)* [10, 48–52]. Under dynamic traffic scenario and using path protection, when a new request for communication from S to D is received, the objective to make provisions for two lightpaths - a primary lightpath from S to D and a backup lightpath (also from S to D), using routes that are *fiber-disjoint*. If the system is able to handle the request for communication (i. e., the search is successful), the primary lightpath is set up and used unless there is an edge failure in the path used by the primary lightpath. Depending on the type of path protection (e.g., 1+1 dedicated path protection, 1:1 dedicated path protection or shared path protection), the backup lightpath is set up at the same time as the primary lightpath or is set up if needed. If the path used by the primary lightpath is affected by a faulty component, the communication is resumed, using the backup lightpath [51, 52].

In recent years, the SLF model was extended to the concept of *shared risk link group* (SRLG). In the SRLG model, all the fiber links located in a geographic area may be assigned the same SRLG, considering the risk of disasters such as earthquakes [53]. Path protection was originally proposed to deal with conduit cuts, but it can be extended to include general risks. For example, if the system is able to handle the request for communication (i.e., the search is successful, the primary lightpath is set up and used unless there is an edge failure in the path used by the primary lightpath [51, 52].

2.1.6 Data Center Network (DCN) and Replicated data

In recent years, telecommunication networks are rapidly evolving to support content delivery and sharing through *Cloud* services [54]. An increasing number of network users and applications rely on the services delivered by data centers (DCs). A network of data centers that provides services to customers is called a *data center network* (DCN) [55, 56]. A *data center* (DC) can be visualized as a server used for storage, computing resources, as well as distribution of large amounts of data. Typically, in such DCN systems, data is replicated among different data centers/locations. This is to ensure that the system remains operational even when some components fail [57]. Content replication also improves metrics, such as throughput, and latency [58, 59]. Figure 2.4 shows an example of a data center network.

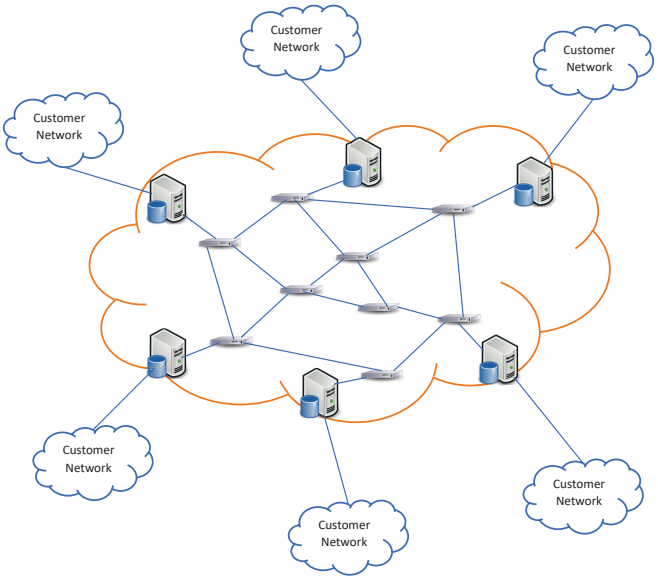


Figure 2.4: Network of datacenters.

2.1.7 Large-scale Failures in Optical networks

Recently, the concept of large-scale failure, also called *disaster*, in DCN has got a lot of attention by researchers. A *disaster* can be defined as a set of nodes and edges that may go down simultaneously [27, 60–62]. It is possible that large-scale disasters may damage both the primary and backup resources and/or affect the data center nodes. Some researchers have studied the failure of multiple components of the network but it is assumed that the source of communication S is not affected by a failure [50, 63].

2.2 Literature Review

This chapter reviews three important aspects relevant to the research reported in this thesis including:

- Attack-aware resource allocation schemes in WDM optical networks,
- Resilient resource allocation schemes in WDM optical networks, and
- Resource allocation schemes in SDM optical networks.

2.2.1 Attack-aware resource allocation schemes in WDM optical networks

2.2.1.1 Types of physical-layer attacks

Deliberate physical-layer malicious attacks can occur sporadically and can propagate in the network making attack monitoring and localization a major challenge [64]. Due to the high bandwidth carrying capacity of optical fibers, even a small malicious attack in the network can cause large amounts of data to be lost or corrupted. Therefore it becomes extremely important to make optical communication secure

against vulnerabilities in the optical network components (such as the optical fiber, optical amplifiers and optical switching fabrics) [19, 21], which can be exploited to make different types of attacks. The important vulnerabilities are as follows:

- *Intra-channel* (or *in-band*) crosstalk: is a phenomenon in which two optical signals, using the same channel (or carrier wavelength)[1], interfere with each other inside an optical switching node [20, 65], and
- *Inter-channel* (or *out-of-band*) occurs due to the interference among optical signals, using different carrier wavelengths, propagating along the same optical fibers [18, 66].

Various types of physical layer attacks may occur in transparent Optical network (TON) [18, 66]. These attacks can be broadly classified as follows:

1. **Service disruption attacks**: These attacks typically deteriorate the signal quality of legitimate communication channels, degrading the Quality of Service (QoS), or causing service denial.
2. **Tapping attacks**: These attacks compromise user privacy by achieving unauthorized access to user data, which can then be used for eavesdropping or other malicious purposes [17].

Based on the goal of the attacker, security attacks in TONs, can also be categorized as *direct attacks* and *indirect attacks* [67–69]

The cost-effective way of ensuring security is to incorporate attack awareness into the network planning phase [20]. In other words, the idea is to establish the lightpaths in such a way that, in the event of a malicious attack, the number of

[1] In the remainder of this thesis, we use the terms channel and carrier wavelength interchangeably.

lightpaths affected by the attack is as small as possible. Recent research in attack-aware RWA problem can be broadly classified into two groups:

- *Addressing out-of-band attacks*: Out-of-band attacks [21, 64] occur when a signal on a legitimate communication channel (lightpath) is adversely affected by another lightpath on a different channel, propagating along the same fiber. The *link-share attack group* of a lightpath [70] p (LAG_p) can be defined as the set of lightpaths, with which p shares at least one common link (or fiber). Based on this, the *Lightpath Attack Radius* (LAR) [21, 71], of lightpath p is calculated as: $LAR_p = |LAG_p| + 1$. In other words, LAR_p is the number of lightpaths (including p itself), with which lightpath p shares at least one link. The most common objective is to limit the damage caused by a *malicious signal*, by reducing the maximum Lightpath Attack Radius ($maxLAR$) [21], of a set of lightpaths P, and is defined as:

$$\textbf{maxLAR} = max\{LAR_p \mid p \in P\}$$

  Typical approaches attempt to find a route that minimizes $maxLAR$, and do not consider the wavelength assignment of lightpaths.

- *Addressing in-band attacks*: In-band attacks can occur due to crosstalk, when two lightpaths using the same channel (wavelength) interfere with each other inside the optical switching node. The *in-band attack group* of a lightpath p (IAG_p) can be defined as the set of lightpaths which use the same wavelength and share a common node with lightpath p. Based on this, the *In-Band Attack Radius* (IAR) of p is calculated as: $IAR_p = |IAG_p| + 1$. This is also referred to as the *Primary Attack Radius*. Existing approaches for addressing in-band attacks attempt to reduce the maximum In-band Attack Radius $maxIAR$ for

a given set of lightpaths P. These approaches typically assume the routing is specified (e.g. fixed shortest path) and focus on the wavelength assignment sub-problem.

$$\textbf{maxIAR} = max\{IAR_p \mid p \in P\}$$

The attack radius (AR) of a lightpath is the sum of its two attack radii, i.e., the maximum number of lightpaths that can be affected by a high-power jamming signal injected into that lightpath (including itself) [21, 70, 72].

$$AR_p = LAR_p + IAR_p$$

Also, the AR of a wavelength (λ) is defined as the maximum AR over all lightpaths routed on that wavelength [72].

$$AR_\lambda = max\{AR_p \mid \lambda \; assigned \; to \; p\}$$

Therefore, the maximum attack radius (maxAR) over all lightpaths is AR of the RWA scheme [21, 70, 72].

$$maxAR = max\{AR_p \mid p \in P\}$$

2.2.1.2 Component Vulnerabilities in AONs

Physical-layer security attacks in TONs can be categorized with respect to the components whose vulnerabilities can be exploited. The components are vulnerable due to characteristics, such as nonlinear effects in fibers [73], gain competition in optical amplifiers [68], and crosstalk in switches [74–76]. A discussion on different types of physical-layer attacks in TONs and some related issues can be found

in [18, 19, 33, 69, 77, 78]. An overview of possible attacks on different network components is given below.

Optical Cross-Connects (OXCs): OXCs are vulnerable to signal leaking and suffer from significant levels of crosstalk [17]. This makes it possible for lightpaths traversing a common switch and using the same carrier wavelength to leak and interfere with each other inside the optical switch, causing *in-band crosstalk*. A malicious user can create a powerful jamming attack by injecting a signal with a very high power, e.g., 20 dB above normal, whose associated leakage (i.e., crosstalk) may, in turn, lead to severe interference on other lightpaths that share a common switching node on the same carrier wavelength [20, 79].

Optical Fibers: Under normal operating conditions, transmission effects in fibers are fairly linear. High-power signals propagating long distances can introduce nonlinearities in fibers, causing *out-of-band crosstalk* or *inter-channel crosstalk* between signals on different carrier wavelengths [21]. In this case, a high-power jamming signal injected on a link can interact with other channels via nonlinear effects and cause damage to other normal/attacked signals.

Optical Amplifiers: Another situation called *gain competition* may occur in optical amplifiers and may also be used to create out-of-band crosstalk attacks [67]. EDFAs have limited gain which is proportionally divided among all incoming signals based on their power levels [18]. Thus, stronger incoming signals are assigned more gain, while weaker signals receive less amplification.

An analysis and case study of gain competition in EDFAs has been conducted in [67]. The authors have investigated the effects of gain competition with a case study in the laboratory, and have analyzed the associated risks on network operation.

2.2.1.3 Attack-Aware RWA Techniques in AONs

A wide range of techniques for handling component failures in TONs are already available in the literature. A number of recent papers have proposed static lightpath allocation approaches that take such security issues into consideration. However, most of these approaches consider the routing problem separately from the wavelength assignment problem. Recently, the idea of attack awareness or preventive physical-layer attack-aware RWA was proposed in [21]. The main idea was to consider the potential consequences of physical-layer attacks in the planning phase, while solving the RWA problem. The aim was to arrange the set of lightpaths in a way that minimizes the possible damage in case an attack occurs. The authors proposed an integer linear program (ILP) formulation for the routing part of RWA to minimize the maxLAR. For medium and large sized optical networks, a heuristic based on the tabu search, to minimize the maxLAR was proposed in [80]. Several approaches have been proposed in the literature that focus on *static* lightpath allocation schemes, with the objective of reducing the negative effects of physical-layer attacks in optical networks. Most of these approaches are capable of handling either in-band [20, 79, 81] or out-of-band crosstalk attacks [21, 80, 82, 83]. In recent years, a few approaches have considered both in-band and out-of-band crosstalk attacks simultaneously under static traffic scenrio [70, 72]. In [72] the authors have proposed a heuristic algorithm to minimize the maximum attack radius (maxAR). The attack-aware RWA problem was divided, due to its complexity, into routing (R) and wavelength assignment (WA) subproblems and was compared against Shortest-Path (SP) routing combined with the classical First Fit wavelength assignment. In [70], the authors have addressed the attack-survivability problem based on DPP approach in the presence of high-power jamming attacks. To solve the problem, a heuristic algorithm was proposed to calculate the Attack Group (AG) of each lightpath and

ensure that the primary and backup paths can not be attacked simultaneously by the same attacker.

An approach that considers minimizing inter-channel attacks in TONs under dynamic traffic was proposed in [82]. The authors here defined "lightpath overlapping" as a situation where two or more lightpaths use the same switching node or fiber link. They have proposed an algorithm to solve the routing sub-problem for two separate objectives, objective 1 is for minimizing intra-channel crosstalk attacks and objective 2 is for minimizing inter-channel crosstalk attacks. The paper did not consider the wavelength assignment sub-problem, as it assumed there are plenty of free wavelengths for a new lightpath. Solving the wavelength assignment problem and also developing a heuristic solution was presented in their extended work [83].

Attack-aware wavelength assignment approaches, which deal with "infinitely propagating" in-band crosstalk attacks to assess upper bounds were proposed in [79]. This extended the authors' work in [76], where they introduced the concept of P-CAR (Propagating Crosstalk Attack Radius). P-CAR was defined as the maximal number of lightpaths that can be affected by a jamming signal propagating on any given lightpath with respect to in-band crosstalk. The authors presented a new approach to control the propagation of such attacks, through a careful wavelength assignment strategy, which minimizes the potential damage caused by such attacks in the planning process. The infinite attack propagation scenario is not a realistic case under real network conditions. Therefore, the authors in [20], have proposed a wavelength assignment scheme to reduce crosstalk attacks that can spread only via primary and/or secondary attackers. The relative importance of this approach is that, in real networks, the crosstalk attacks can spread maximally in one or two steps. The "secondary attacker" is defined as a signal that has been attacked by the primary attacking signal, and acquired some attacking capabilities, while passing

through the same switches and using the same wavelength. The signals attacked by the second attacker cannot propagate the attack further in the network. The paper considered the wavelength assignment sub-problem and formulated it as an ILP, with the objectives of minimizing the primary attack radius (PAR) and secondary attack radius (SAR) values. To find suboptimal solutions for bigger networks in reasonable time, the paper also proposed a heuristic algorithm called GRASP (Greedy Randomized Adaptive Search Procedure).

The propagation effect of high-powered jamming attack in TONs was studied in [75]. The authors proposed an attack model called "JAP-model", considering the propagation effect of intra-channel crosstalk attacks which may cause inter-channel crosstalk attack or gain competition. They applied this model to an attack-aware routing and wavelength assignment heuristic (JAP-SP-FF), which showed decrease in blocking probabilities comparing with Shortest-Path First-Fit (SP-FF) algorithm by avoiding damaged links and wavelengths.

The concept of considering attacks in *survivable* RWA problem for AONs was introduced in [70], under the assumption that an attack can only be injected at the source node of each connection. This paper proposed an attack-aware DPP algorithm which tries to minimize the IAR values as well as the number of used wavelengths. The *attack-survivable* approaches that consider both LAR and IAR based on dedicated and shared path protection was proposed in [70, 84].

2.2.2 Disaster-aware RWA in DC Optical Networks

A data center network (DCN), also called a *cloud*, is a high speed network of data centers (DCs) that must provide reliable data base access and computing services to customers [85, 86]. Disasters or large-scale failures (e.g., an earthquake or a fire) can damage major components of a network. It is critical that the underlying DCN

is resilient and can continue to provide services in case of disasters. Large-scale disasters may damage both the primary and the backup resources and/or affect the data center nodes. In traditional path protection, data is not replicated so that each request for data communication is from a specified site. This protection scheme is not applicable to DCN as discussed below.

Cloud computing depends critically on large data centers connected by a high-speed optical network. In cloud network, users' requests for contents can be served by any DC that hosts the required content, as these contents and/or services are replicated (copied) over multiple data centers. This allows robust system design as the network will continue to provide services in case of node or fiber failure or even in case of disasters [60, 87].

When a large-scale disaster, such as an earthquake, a hurricane, or a malicious attack occurs, multiple nodes and links in the network may fail simultaneously. This leaves large parts of the network unusable and may lead to huge amounts of data being lost or compromised [61, 62]. Therefore, it is crucial to develop algorithms to design resilient networks that protect the services offered by a cloud against such disasters.

The problem of resource provisioning for resilient DCNs supporting *static* light-path demands, where traffic loads remain relatively stable are known at design time, was considered first in [60]. The authors jointly solve the problems of content placement, routing, and path/content protection in the case of disasters. The paper was the first to define a *disaster zone* (DZ) or *shared risk group* (SRG) as the set of nodes and links that may go down simultaneously because of a disaster. The problem was formulated as an ILP under anycast principle to find the number of replicas per content and primary and backup paths that are *SRG-disjoint* with the objective of minimizing the primary and shared backup resources (i.e., wavelengths). Following

the anycast principle, the DCs were not fixed in the ILP, they were variable instead. As this ILP is intractable for large problems, a two-step ILP was proposed [60] to separately solve i) content placement with content protection and ii) routing with path protection. The proposed disaster-resilient approaches were compared with the classic dedicated and shared SLF protection.

Algorithms to design resilient networks that protect the services offered by a cloud against disasters is a current research topic [25, 60, 87]. Some researchers have studied the failure of multiple components of the network but it is assumed that the source of communication S is not affected by a failure. A disaster-aware provisioning scheme was proposed in [88]. The problem of designing WDM networks for data centers to handle disasters was studied in [22, 25, 60, 87, 89].

Most of the papers proposed in the literature consider the *static* lightpath allocation case of the disaster-aware problem. Several studies focused on analysing network vulnerabilities to large-scale or regional correlated failures caused by disasters [27, 90–94]. The paper [25] studied the nature of large-scale failures (i.e., disasters) and illustrated the procedures required to determine the *risky zones* in the network. The authors presented the characteristics and classification of disasters in telecom networks. The article also defines a *risk* as the loss or penalty paid by network operators to customers.

In [95] the authors proposed a degraded-service tolerance scheme aims at reducing the protection cost. The research [22] classifies the disaster models proposed in the literature into: i) *deterministic models*, ii) *probabilistic models*, and iii) *multi-layer networks.* The paper provides a survey on the related works that consider these models and the protection schemes proposed for optical backbone networks to ensure survivability in the occurrence of disasters. In [88], which is an extension of the work in [96], the authors considered the problem of resource allocation be-

fore disasters and re-allocation after a disaster. The study presented a risk model to analyze regional failure loss, where multiple network components in a region fail simultaneously and many network connections jeopardize. The paper proposed a *proactive* (i.e., before disaster) disaster-aware provisioning scheme, with the objective of minimizing the loss/penalty in the case of a disaster. The authors also investigated a *reactive* (i.e., after disasters) scheme for reprovisioning the connections affected by correlated-cascading failures. The proposed model was formulated as an ILP. A heuristic algorithm was also proposed for larger networks.

In [89] the authors proposed a disaster-aware service provisioning scheme that multiplexes service over multiple servers/datacenters with manycasting, which was called *multipath* to multiple destinations (MMD). The proposed scheme was formulated as an ILP and a heuristic approach was used for large networks. It has been shown that selecting destinations through manycasting principle provides a high level of protection against node and link failures due to disasters. Also the proposed approach maintains some bandwidth (i.e., degraded service) in the case of a disaster, instead of no service at all.

Datacenter placement is another important problem in supporting cloud services in optical networks. Several approaches to address the datecenter network (DCN) placement problem were proposed [87, 97]. In [87] the authors proposed a static disaster-aware DCN placement to avoid placing the DC in risky (i.e., disaster) zones. Data replication is essential, since a disaster may very well affect the data centre used as the source of the primary lightpath. So, copies of each file must be stored in multiple data centers, in order to guarantee that the requested contents/files can be delivered to users, even in the event of a disaster affecting a DC. In [97] the authors studied the DCN placement problem, adapting *anycast* principle which has been demonstrated to enhance the service availability by efficient content replication in

cloud networks. Also the paper addressed the protection of cloud services against any single link failure and any particular DC failure which are assumed not to occur simultaneously. An ILP formulation was presented to obtain an optimal solution for the joint DCN placement and protection, and, for large networks, a heuristic algorithm was proposed to solve the above problems separately.

2.2.3 Resource Allocation Techniques in SDM Networks

Most of the approaches proposed in the literature for solving RSCA problem in SDM networks consider static traffic demands. In [30], the authors propose different optimization models for the different ways of realizing traffic transmission in SDM networks. Also the paper presents an analysis of the flexibility options of these models in terms of spectral-spatial resources offered. In [29], the authors proposed an optimal algorithm to solve the RSCA problem in SDM networks. The problem was formulated as an ILP with the objective of minimizing maximum number of spectrum slices required on any core of MCF of a flexgrid SDM network. Due to the ILP complexity, the authors also developed a heuristic that sorts the traffic demands based on their spectrum requirements and the path length. The paper compares the heuristic's performance with the optimal algorithm. There are several papers in the literature that considers limiting the effect of crosstalk in SDM-based optical networks. The study [98] considers solving the RSA problem to reduce crosstalk effects in elastic optical networks. To minimize or avoid crosstalk, the algorithm tries to provision super channels to requests in such a way that avoids using the same frequency band in adjacent cores. The paper [99] handles two types of requests (i) immediate-reservation (IR) requests which need to be provisioned immediately, and (ii) advance-reservation (AR) requests which can be provisioned in advance. The proposed algorithm addresses the spectrum-fragmentation caused

by ARs which tend to reserve future resource, which causes a lack of spectral-spatial resources to accommodate IRs. Recently, optical networks using SDM technology has been proposed as a solution to the speed bottleneck anticipated in data center networks [13].

Chapter 3

Attack-Aware Dynamic RWA in WDM Optical Networks

3.1 Introduction

In recent years, there is growing recognition of the need to develop suitable mechanisms for reducing the adverse effects of malicious attacks such as high power jamming and tapping attacks. A number of recent static lightpath allocation approaches have been proposed that take such security issues into consideration. Most of these approaches consider the routing problem separately from the wavelength assignment problem. In this chapter we propose a new security-aware ILP formulation, as well as an efficient heuristic for the complete security-aware dynamic routing and wavelength assignment (RWA) problem. Our motivation in this study is to address the dynamic RWA problem considering jamming attacks that exploit both in-band and out-of-band crosstalk in optical switches and fibers, respectively. To the best of our knowledge, this is the first such work to jointly consider in-band and out-of-band attacks, for either static or dynamic case.

3.2 Integer Linear Programming (ILP) Formulations

We formulate our security-aware dynamic RWA problem as an ILP formulation. We assume that all existing lightpaths that share a link with the proposed new lightpath contribute equally to its LAR value, regardless of the channel separation and/or number of shared links. Similarly, all existing lightpaths that share a common channel and node with the proposed new lightpath contribute equally to its IAR value, regardless of the number of shared nodes. We present two formulations, SA-ILP in Sec. 3.2.1 with the objective of minimizing the total LAR+IAR value for the new lightpath request. In addition, the objective function tries to minimize the path length of the newly established lightpath, as a secondary objective. In Sec. 3.2.2 we present a modified ILP formulation (SA-ILP2) with the objective of minimizing the maximum attack radius (i.e. max(LAR+IAR)) value over the entire network.

3.2.1 ILP Formulation for Security-Aware RWA (SA-ILP)

The objective function:

$$\textbf{minimize}\alpha \cdot LAR + \beta \cdot IAR + \gamma \sum x_e \tag{3.1}$$

Subject to:

1. Flow constraint:

$$\sum_{e:i\rightarrow j\in E} x_e - \sum_{e:j\rightarrow i\in E} x_e \begin{cases} 1, \text{if } i = s, \\ -1, \text{if } i = d, \quad \forall i \in N \\ 0, \text{otherwise.} \end{cases} \tag{3.2}$$

Notation

N	Set of nodes in the network.
E	Set of edges in the network.
W	Set of available channels (wavelengths) per fiber.
P	Set of existing lightpaths.

Parameters

$a_{e,p}$	where $a_{e,p} = 1$, if existing lightpath p uses edge e; 0 otherwise.
$b_{k,p}$	where $b_{k,p} = 1$, if existing lightpath p uses channel k; 0 otherwise.
$c_{j,p}$	where $c_{j,p} = 1$, if existing lightpath p uses node j; 0 otherwise.
α	the weight attached to LAR component in the objective function.
β	the weight attached to IAR component in the objective function.
γ	the weight attached to minimizing the path length in the objective function.
LAR_p	the LAR value for p^{th} existing lightpath.
IAR_p	the IAR value for p^{th} existing lightpath.
L_{max}	maximum length of any established lightpath.
s & d	source and destination of the new lightpath.

Variables

Binary Variables

x_e	where $x_e = 1$, if the new lightpath uses edge e; 0 otherwise.
y_j	where $y_j = 1$, if the new lightpath uses node j; 0 otherwise.
w_k	where $w_k = 1$, if the new lightpath uses channel k; 0 otherwise.
T_p	where $T_p = 1$, if the new lightpath shares common edge with lightpath p; 0 otherwise.
S_p	where $S_p = 1$, if the new lightpath shares common node with lightpath p; 0 otherwise.
Q_p	where $Q_p = 1$, if the new lightpath shares common node and channel with lightpath p, 0 otherwise.

Continuous Variables

$\delta_{k,e}$	where $\delta_{k,e} = 1$, if the new lightpath uses channel k on edge e; 0 otherwise.
LAR	lightpath Attack Radius of the new lightpath.
IAR	in-band Attack Radius of the new lightpath.
LAR_p^{new}	the new LAR value for p^{th} lightpath after the new lightpath is established.
IAR_p^{new}	the new IAR value for p^{th} lightpath after the new lightpath is established.
$maxAR$	the maximum attack radius over the entire network.

2. No Cycles:

$$\sum_{e:i\to j\in E} x_e \leq 1 \quad \forall i \in N \tag{3.3}$$

3. Wavelength Continuity Constraint:

$$\sum_{k} w_k = 1 \tag{3.4}$$

4. Setting the value of $\delta_{k,e}$:

$$x_e + w_k - \delta_{k,e} \leq 1 \quad \forall k \in W, e \in E \tag{3.5}$$

$$x_e \geq \delta_{k,e} \quad \forall k \in W, e \in E \tag{3.6}$$

$$w_k \geq \delta_{k,e} \quad \forall k \in W, e \in E \tag{3.7}$$

5. Wavelength Clash Constraint:

$$\delta_{k,e} + \sum_{p} a_{e,p} \cdot b_{k,p} \leq 1 \quad \forall k \in W, e \in E \tag{3.8}$$

6. Link Sharing constraints:

$$T_p \leq \sum_{e:a_{e,p}=1} x_e \quad \forall p \in P, e \ni a_{e,p} = 1 \tag{3.9}$$

$$T_p \geq x_e \cdot a_{e,p} \quad \forall p \in P, e \ni a_{e,p} = 1 \tag{3.10}$$

$$LAR = \sum_{p} T_p + 1 \tag{3.11}$$

7. Node Sharing constraints:

$$y_i \leq \sum_{e:i \to j \in E} x_e \quad \forall i \in N, i \neq d \tag{3.12}$$

$$y_d = 1 \tag{3.13}$$

$$S_p \geq y_i \cdot c_{i,p} \quad \forall p \in P, i \ni c_{i,p} = 1 \tag{3.14}$$

$$S_p \leq \sum_{j:c_{j,p}=1} y_j \quad \forall p \in P \tag{3.15}$$

8. Node-Channel Sharing Constraints:

$$S_p + \sum_{k} b_{k,p}.w_k - Q_p \leq 1 \quad \forall p \in P \tag{3.16}$$

$$S_p \geq Q_p \quad \forall p \in P \tag{3.17}$$

$$\sum_{k} b_{k,p}.w_k \geq Q_p \quad \forall p \in P \tag{3.18}$$

$$IAR = \sum_{p} Q_p \tag{3.19}$$

9. Maximum Lightpath Length:

$$\sum_{e \in E} x_e \leq L_{max} \tag{3.20}$$

The relative importance of in-band and out-of-band attacks can be adjusted by setting appropriate values for α and β in the objective function (1). In our simulations for SA-ILP (in Sec. 3.5), we have set $\alpha = \beta = 1$, $\gamma = 0.001$. For ILP-WL, the traditional ILP for dynamic RWA that minimizes the number of wavelength links, we have set $\alpha = \beta = 0$, $\gamma = 1$. Constraint (3.2) finds, for each lightpath, a route over the physical topology, (also called flow conservation equation) [11]. Constraint (3.3) ensures that there is at most one outgoing edge from any given node that is traversed by the new lightpath. This prevents loops in the physical route of the new lightpath. However, it does prevent separate loops (disconnected from the main route) from being created. The third term in the objective function minimizes the path length and additionally ensures that such extra loops are never created. Constraint (3.4) ensures that the same wavelength must be assigned along the entire route (links) traversed by the new lightpath. Constraints (3.5) - (3.7) ensures that $\delta_{k,e}$ is set to 1 if the new lightpath is routed over edge e and assigned channel k. i.e. if and only if both $w_k = 1$ and $x_e = 1$. Constraint (3.8) ensures that if the new lightpath is assigned channel k on link e (i.e. $\delta_{k,e} = 1$), then no existing lightpath can be using channel k on link e. Constraints (3.9) - (3.10) ensure that T_p will be set to 1 if the new lightpath shares at least one common edge e with an existing lightpath p; otherwise T_p is set to 0. Constraint (3.11) represents the LAR of the new lightpath. Constraint (3.12) - (3.13) determines the set of nodes that will be traversed by the new established lightpath. If the new lightpath traverses node i, then y_i will be set to 1; otherwise y_i is set to 0. Constraints (3.14) - (3.15) ensures that S_p will be 1, if the new lightpath is sharing a common node i with any of the

existing lightpath p. Constraints (3.16) - (3.18) will set Q_p to 1, if the new lightpath is sharing a common node and is assigned the same channel as the existing lightpath p. Constraint (3.19) represents the IAR of the new lightpath. The new established lightpath has not been considered in this constraint in order not to count it twice when calculating the LAR+IAR values. Constraint (3.20) ensures that the length of any newly established lightpath should not exceed the value of L_{max}.

3.2.2 Modified ILP formulation (SA-ILP2)

We extend the formulation from Sec. 3.2.1 to consider the traditional attack-aware approach with the objective of minimizing the maximum attack radius ($maxAR$). This formulation, denoted as SA-ILP2, is an extension of SA-ILP and is given below.

The objective function:

$$\textbf{minimize} maxAR \tag{3.21}$$

Subject to:

constraints 3.2 to 3.20 from SA-ILP with the following added constraints:

$$LAR_p^{new} = LAR_p + T_p \quad \forall p \in P \tag{3.22}$$

$$IAR_p^{new} = IAR_p + Q_p \quad \forall p \in P \tag{3.23}$$

$$\alpha \cdot LAR_p^{new} + \beta \cdot IAR_p^{new} \leq maxAR \quad \forall p \in P \tag{3.24}$$

$$\alpha \cdot LAR + \beta \cdot IAR \leq maxAR \tag{3.25}$$

Constraint (3.22) updates the new LAR value of the p^{th} existing lightpath if it shares any common edge with the new established lightpath. Similarly, constraint (3.23) considers the node and channel sharing possibility between the p^{th} existing lightpath and the new established lightpath and updates IAR_p^{new} value accordingly. Constraints (3.24) ((3.25)) ensures that the LAR+IAR value of the p^{th} existing (new) lightpath must not exceed the value of maxAR.

3.3 An Illustrative Example of the Attack-Aware RWA Problem

To date, the work on security-aware RWA has focused on static lightpath allocation considering out-of-band and/or in-band attacks, with the objective of minimizing the maxLAR and maxIAR values respectively. For the dynamic lightpath allocation problem considered in this chapter, these may not be the most appropriate objectives.

To illustrate the relative effects of both out-of-band and in-band attacks on different objective values, we consider a simple example of a network with 6-nodes, 9 bidirectional links, and 2 channels per fiber. A set of 6 lightpaths (L1 - L6) are already established in the network with their assigned routes and wavelengths. Fig. 3.1a shows that lightpath L6 is routed over the links 0→2→3→5→4 and is assigned wavelength $\lambda 1$. We assume that an attack is injected at the beginning of a lightpath and affects i) the LAR values of any other lightpath that shares a link with the attacking lightpath, regardless of how far the link is from the point of injection and ii) the IAR values of all lightpaths using the same channel and passing through a common node; it does not matter how far the node is from the point of injection. Note that our model assumes using the classical amplifiers (i.e. EFDAs) [21,66] not

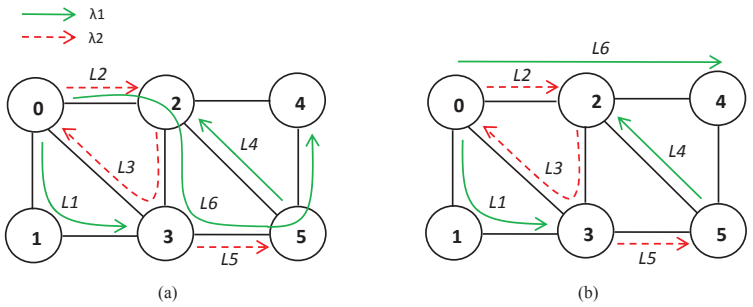


Figure 3.1: Two different RWA schemes for lightpath L6 on 6-nodes network topology.

the automatic gain control (AGC) amplifiers. The reason is with the AGC amplifier the gain of incoming signals is clamped, which prevents the attack from propagating further after the point of amplification. Let a jamming attack be injected at the beginning of lightpath L6. We count the LAR and IAR values of L6 as follows:

The LAR value for lightpath L6 is 4 as it shares common links with lightpaths L2, L3, and L5 and L6 itself. The IAR value for L6 is 3 corresponding to lightpaths L1 and L4 which share channels and common switches with lightpath L6 and L6 itself.

Fig. 3.1b shows a different routing scheme, where lightpath L6 was routed over the links 0→2→4. Here a jamming signal injected on L6 could disrupt only lightpath L2 via out-of-band crosstalk and lightpaths L1 and L4 via in-band crosstalk. Thus the $LAR_{L6} = 2$ (due to L2 and L6) and $IAR_{L6} = 3$ (due to L1, L4, and L6). If L2 was assigned $\lambda 1$ in Fig. 3.1b and L6 was assigned $\lambda 2$ we would have the value of IAR reduced to 2 (e.g., $IAR_{L6} = 2$) as L6 will share a common switch and a channel with only L3 and including L6 itself. From this we conclude that the routing and wavelength assignment scheme may significantly influence the potential damage caused by some physical-layer attacks and hence carefully routing and assigning wavelengths to lightpaths may reduce such damage to a minimum.

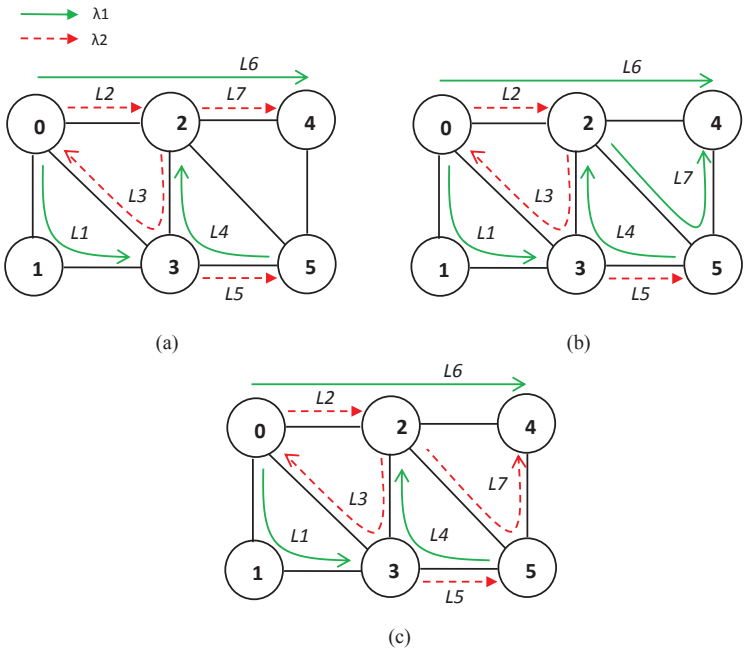


Figure 3.2: The three options of RWA for lightpath L7.

Table 3.1: *LAR* and *IAR* values for different lightpaths and maxLAR and maxIAR values of Fig. 3.1b.

	L1	L2	L3	L4	L5	L6	**max**
LAR	1	2	1	1	1	2	2
IAR	2	2	3	2	2	3	3

The attack radius values associated with each lightpath from Fig. 3.1b, as well as the overall maxLAR and maxIAR values for the network is shown in Table 3.1. We note that the maxLAR value is 2, due to L2, and L6, which share a common link with each other. Similarly, the maxIAR value is 3, corresponding to L3 (L6), routed on wavelength $\lambda 2$ ($\lambda 1$), which shares channels and common switches with lightpaths L2 and L5 (L1 and L4) respectively, including L3 and L6 themselves.

Now, we consider a different scenario where we assign the path of L4 to (5→3→2) instead of (5→2) as shown in Fig. 3.2. Let there be a request for a new lightpath

Table 3.2: Different objective values for new lightpath setup in Fig. 3.2.

Route	r1: 2→4		r2: 2→5→4	
Option	1	2	3	4
Channel	$\lambda 1$	$\lambda 2$	$\lambda 1$	$\lambda 2$
$\mathbf{LAR}_{L7}$	x	2	1	1
$\mathbf{IAR}_{L7}$	x	3	3	4
maxLAR	x	2	2	2
maxIAR	x	3	3	4

(L7) from node 2 to node 4. L4 was rerouted over the links 5→3→2 to illustrate the three RWA options of L7. We consider two potential routes r1: 2→4 and r2: 2→5→4, with the possibility of assigning channel $\lambda 1$ or $\lambda 2$ on each route.This leads to four options for RWA of the new lightpath (L7), shown in Table 3.2.

- option1: assign channel $\lambda 1$ on route $r1$ (infeasible)
- option2: assign channel $\lambda 2$ on route $r1$
- option3: assign channel $\lambda 1$ on route $r2$
- option4: assign channel $\lambda 2$ on route $r2$

Assigning channel $\lambda 1$ to L7 on route r1 (i.e. option 1) would violate the wavelength clash constraint, and is not feasible. The remaining options, ie. option2, option3 and option4 are associated with Figs. 3.2a, 3.2b, and 3.2c respectively. For these three options, the LAR and IAR values for the new lightpath as well as the overall maximum values for the network are shown in Table 3.2.

The goal of our attack-aware dynamic RWA scheme is to select a route and a wavelength for each lightpath request that minimizes the risk of attacks. If our objective is to simply minimize the maxLAR as in [21], then all three options (2,

3 and 4) are equally attractive and there is nothing to differentiate between them. Similarly, if the objective is to minimize the maxIAR as in [79], then we could choose option 2 or 4. On the other hand, trying to reduce the LAR (IAR) value of the new lightpath individually would result in selecting option 3 or 4 (option 2). The LAR and maxLAR values depend on the selected route, while the IAR and maxIAR values depend on the selected wavelength. As shown in Table 3.2 only the value of maxIAR will change with option 4, other max values will not be affected. Our goal is to jointly minimize the risk of both in-band and out-of-band attacks for a new incoming lightpath. Therefore, we need to perform routing and wavelength assignment together and use an objective function that takes into account both types of attacks. Considering only one type of attack (i.e. either in-band or out-of-band attack) can be treated as a special case of our proposed approach.

3.4 Security-Aware Dynamic RWA Heuristic Algorithm (SA-DRWA)

In this section we present our heuristic (SA-DRWA), for solving the security-aware dynamic RWA problem. SA-DRWA tries to assign a physical route and a wavelength resulting in the minimum value of (LAR+IAR), for each new lightpath. SA-DRWA first takes, as input, a physical network topology *G = (N, E)* of N nodes and E bidirectional links. The heuristic consists of two phases, an initialization phase (Phase I), which is called only once and a second phase (Phase II), which must be called for each new lightpath request. The two phases are outlined below.

- Phase I: This phase takes as input the network topology *G = (N, E)* and a parameter K. The output of this phase is R_{sd}, a set of up to K possible routes over the physical topology, for each source-destination pair *sd*.

- Phase II: This phase takes as input the RWA for a set of existing lighpaths P, the pre-computed routes R_{sd} for each node pair, the set of available channels W per fiber and the source and destination node of the new connection request. The output of this phase is a suitable RWA for the new lightpath and an updated network state.

Phase I is straightforward and uses existing K-shortest path algorithms [100,101] to pre-compute the potential routes for each node pair. The remaining discussion will focus on Phase II.

SA-DRWA processes one lightpath request at a time. When a new lightpath request, from a source s to a destination d arrives, SA-DRWA first calculates the following two parameters:

- S_e= the set of available wavelengths on link e. This is calculated based on the RWA information of existing lightpaths.

- Λ_r= the set of available wavelengths on all edges of a particular route $r \in R_{sd}$.

All the pre-computed routes from s to d are examined to calculate the available wavelengths on each of those routes. If there are no available channels on any of the routes, the new request is blocked and added to the list of blocked connection requests B. Otherwise, SA-DRWA searches for a suitable route and a wavelength. First, the current "best"value for attack radius AR_{best} is initialized to highest possible value $|P| + 1$ (i.e. the new lightpath is in the attack group of *all* existing lightpaths). Next the initial value for the path length r_{len} is set to $|N| + 1$. This means that any valid loop-free path will have a lower length. Then SA-DRWA examines each possible route r and channel assignment λ and calculates the corresponding attack radius $AR_{r,\lambda}$. If this is less than the current value AR_{best}, then (r, λ) is selected as the current best allocation and the values of AR_{best} and r_{len}

Pseudocode for SA-DRWA Heuristic Algorithm.

Phase I
Input
$G(N, E), K$ //$G(N, E)$: is physical topology N nodes and E edges. K: number of paths needed for each sd pair.
Find the set R_{sd} of K shortest paths between each (s,d) pairs over the physical topology.
Phase II
Input
RWA for set of existing lightpaths P, New lightpath request lp from s to d, W, R_{sd} //W: set of wavelengths per fiber. R_{sd}: set of pre-computed routes from s to d
Begin
for each $e \in E$ **do**
  Calculate S_e;
end for
for each route $r \in R_{sd}$ **do**
  Calculate $\Lambda_r = \bigcap_{e \in r} S_e$;
end for
if $\Lambda_r = \emptyset, \quad \forall r \in R_{sd}$ **then**
  Block new request;
  $B = B + lp$ //add lp to set of blocked lightpaths;
  Return;
end if
$AR_{best} = |P| + 1$, $r_{len} = |N| + 1$, $selected = (-1, -1)$;
for each route $r \in R_{sd}$ **do**
  Calculate LAR_r for route r;
  for each $\lambda \in \Lambda_r$ **do**
    Calculate $IAR_{r,\lambda}$ for channel λ on route r;
    Calculate $AR_{r,\lambda} = LAR_r + IAR_{r,\lambda}$
    if $(AR_{r,\lambda} < AR_{best})$ OR
$(AR_{r,\lambda} == AR_{best} AND len(r) < r_{len})$ **then**
      $AR_{best} = AR_{r,\lambda}$
      $r_{len} = len(r)$
      $selected = (r, \lambda)$
    end if
  end for
end for
$P = P + lp$ //add lp to set of existing lightpaths;
Update LAR and IAR values of all lightpaths;
Update avgLAR, avgIAR, maxLAR, maxIAR;
Return;
End

are updated accordingly. If current route/channel assignment has the same value as AR_{best}, the algorithm chooses the route with the shorter path length. If the path lengths are also equal, SA-DRWA keeps the first choice. Once all possible routes and channels have been examined, the selected route and channel are assigned to the new lightpath. After the new request has been allocated, it is added to the list of existing lightpaths P, and the algorithm updates the LAR and IAR values of all the lightpaths (including the new request) and re-computes the average and max values of LAR and IAR for the network. When a lightpath is no longer needed, the connection is torn down and all resources allocated to the lightpath are reclaimed. Furthermore, the LAR and IAR values of all continuing lightpaths are updated, as necessary.

3.5 Simulations and Numerical Results

In our simulations we considered networks of different sizes, ranging from 14 to 50-nodes including the well-known NSFNET (14-nodes) [102], ARPANET (20-nodes) [102], and USANET (24-nodes) networks [103]. We also simulated other synthetically generated network topologies, with 40 and 50-nodes. The set of lightpath requests was generated based on a Poisson-distribution [104], with randomly selected source and destination nodes. The traffic load was varied from 25 to 200 Erlang. The ILP formulation was solved using CPLEX [105], which was able to easily generate optimal solutions, even for the larger topologies and high traffic loads. We also tested our proposed SA-ILP and SA-DRWA on the above mentioned network topologies with a varied number of wavelengths per fiber of 8, 16, 24, 32, and 64. Unless explicitly mentioned otherwise, the results reported in this section are for links with 16 channels (wavelengths) ($|W| = 16$). The simulation results for other values of $|W|$ followed a similar pattern and therefore are omitted for the sake of

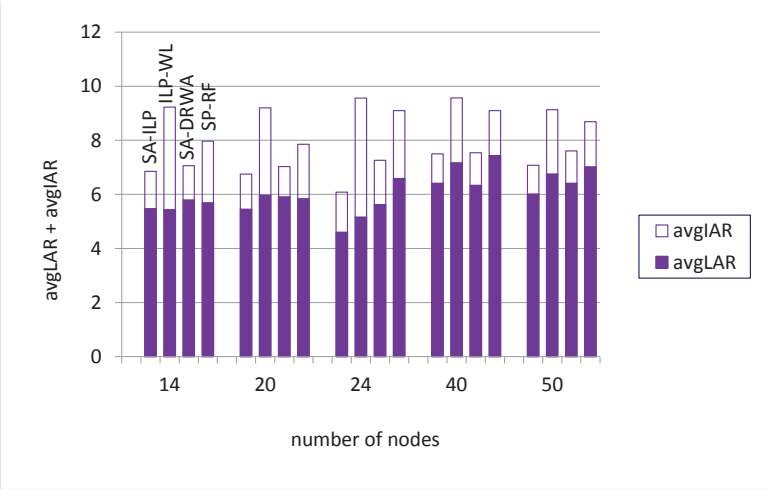
brevity. In our simulations we compared the performance of SA-ILP, SA-ILP2 and SA-DRWA to the following security unaware approaches:

1. A traditional ILP for dynamic RWA, whose objective is to minimize the number of wavelength links used (referred to as ILP-WL).

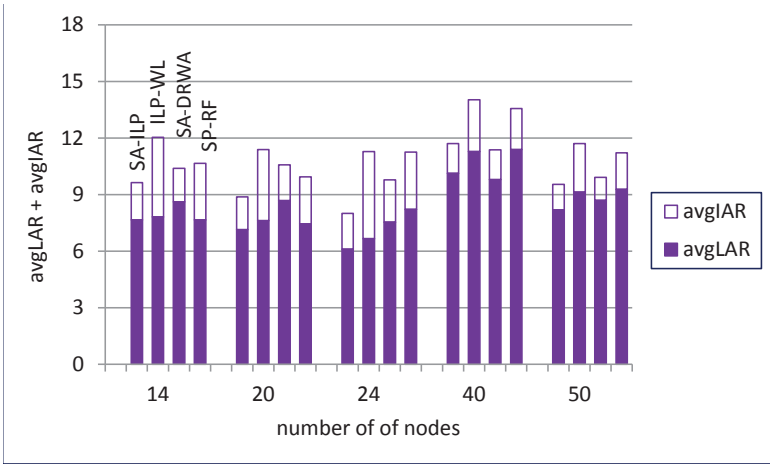
2. Two simple heuristics namely: i) SP-FF and ii) SP-RF. The heuristics are based on i) Shortest Path-First Fit (SP-FF) and ii) Shortest Path-Random Fit (SP-RF). In this section, we do not show the results of SP-FF in the diagrams, as they are close to or slightly worse than that of SP-RF.

Figs. 3.3a and 3.3b show the average LAR (avgLAR) and average IAR (avgIAR) values for the set of established lightpaths with traffic load of 50 and 75 Erlang, respectively, for different network sizes and topologies. The SA-ILP objective is to minimize the combined $avgLAR + avgIAR$ value, whereas ILP-WL minimizes the number of wavelength links for each new lightpath. For each network size, 4 bars are shown, corresponding to SA-ILP, ILP-WL, the proposed heuristic SA-DRWA, and SP-RF respectively. In terms of avgLAR values, all approaches have similar performance. The proposed security-aware approaches perform slightly better overall, with an average improvement of 10%-15%. In terms of avgIAR values, the proposed security-aware approaches (SA-ILP and SA-DRWA) have similar performance and outperform the traditional techniques, i.e. ILP-WL and SP-RF, with average improvements of 50% - 75%. The results clearly demonstrate that the security aware approaches perform significantly better than the other approaches in terms of reducing the attack radii, with the performance of SA-DRWA being close to that of SA-ILP, in most cases. Overall, the reduction in the combined attack radius (i.e. avgLAR+avgIAR) obtained using SA-ILP, range from 15% - 25%, compared to traditional approaches that are not attack-aware.

Figs. 3.4a and 3.4b compare the resource consumption (in terms of the number



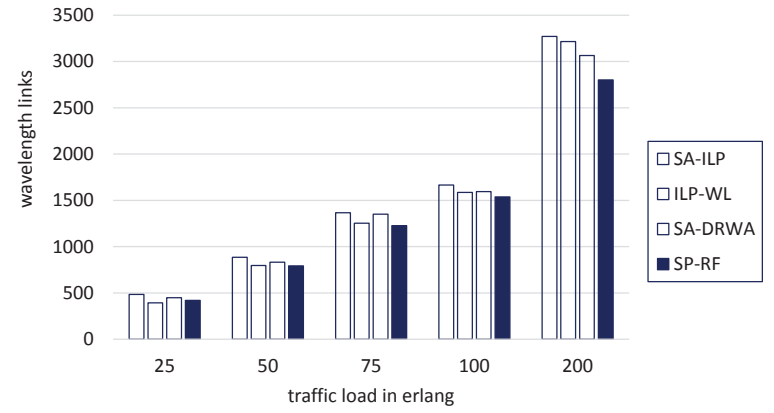
(a)



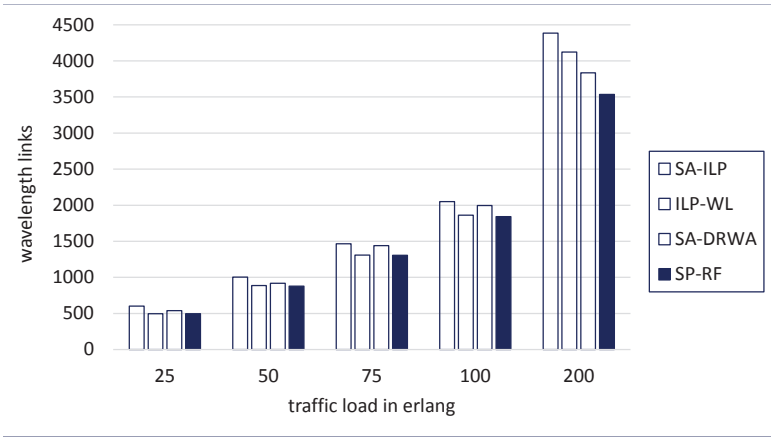
(b)

Figure 3.3: Comparison of (avgLAR+avgIAR) values for SA-ILP, ILP-WL, SA-DRWA and SP-RF, with traffic load of (a) 50 Erlang and (b) 75 Erlang.

of wavelength links used) for the different approaches for the 14-node NSFNET network and the 20-node ARPANET network, respectively. As expected, ILP-WL provides the best performance, but results for all approaches are quite close (within 10% of ILP-WL). For higher traffic loads (100 and 200 Erlang), SA-DRWA and SP-RF appear to have lower resource consumption compared to ILP-WL, but this is due to the fact that many more lightpaths are blocked using these heuristic approaches.



(a)



(b)

Figure 3.4: Comparison of resource consumption (in terms of wavelength links) using different approaches for (a) 14-node network and (b) 20-node network.

Fig. 3.5 compares the blocking probabilities for the different approaches, for different network sizes, with a traffic load of 200 Erlang, and with 16 available channels per fiber. We see that the performance of SA-ILP was very close to ILP-WL in this respect. Only in the 50-nodes topology, ILP-WL led to a slight decrease in the number of blocked lightpaths, compared to SA-ILP. The heuristic approaches typically resulted in higher blocking probabilities than the ILPs, which is expected. Overall, the results indicate that SA-ILP requires only a small overhead - less than

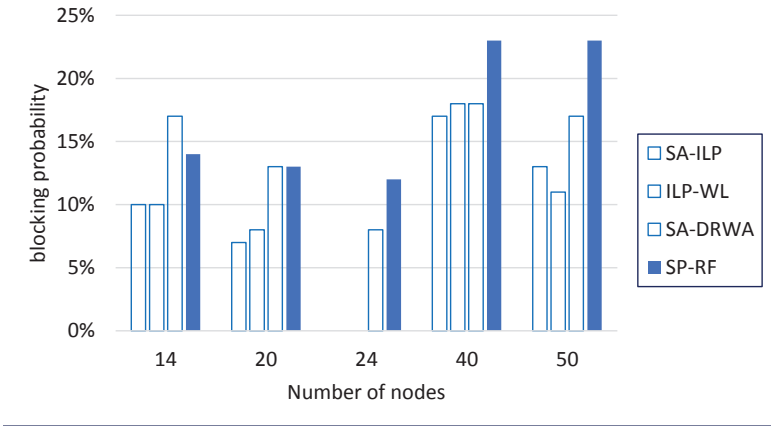
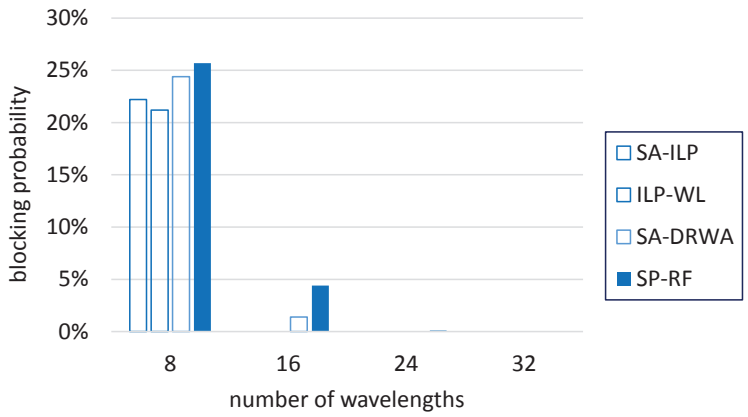


Figure 3.5: Comparison of blocking probabilities for different topologies with 200 Erlang traffic using SA-ILP, ILP-WL, SP-RF, SA-DRWA.

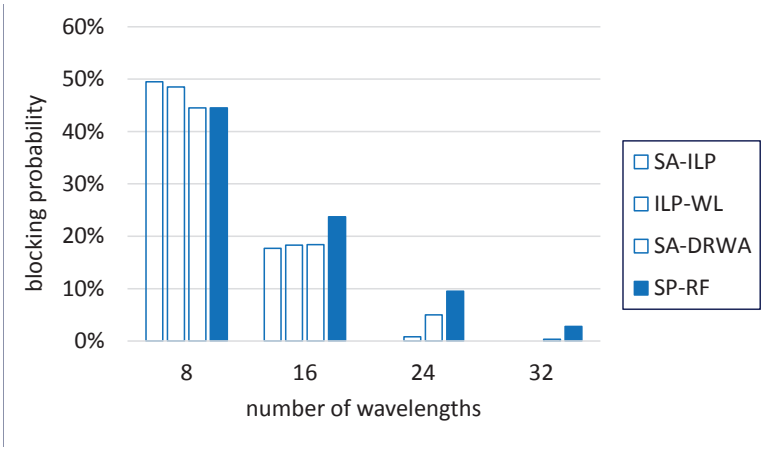
10% on average in terms of blocking probability.

Figs. 3.6a and 3.6b show how the blocking probability varies with the number of available channels per fiber ($|W|$), in a 40-node topology, with traffic loads of 100 and 200 Erlang respectively. As expected, the overall blocking probability decreases with higher values of $|W|$. There were no blocked requests for SA-ILP for 100 Erlang (16, 24 & 32 channels) and 200 Erlang (24 & 32 channels). Based on our simulations, it is clear that the proposed approach for security-aware dynamic RWA is able to reduce the vulnerability of the lightpaths to potential attacks, without incurring any significant penalties in terms of blocking probability, when compared to traditional RWA techniques.

The results reported above for SA-ILP do not place any restrictions on the maximum allowed path length. We have also tested the SA-ILP formulation under the condition of restricting the maximum path length of each new lightpath. The maximum path length (L_{max}) was selected to be 2-3 hops more than the average path lengths for the unrestricted case. For the networks with 14 to 24-nodes, this resulted in an upper limit of 6 hops; for the networks with 40-50-nodes, this resulted



(a)

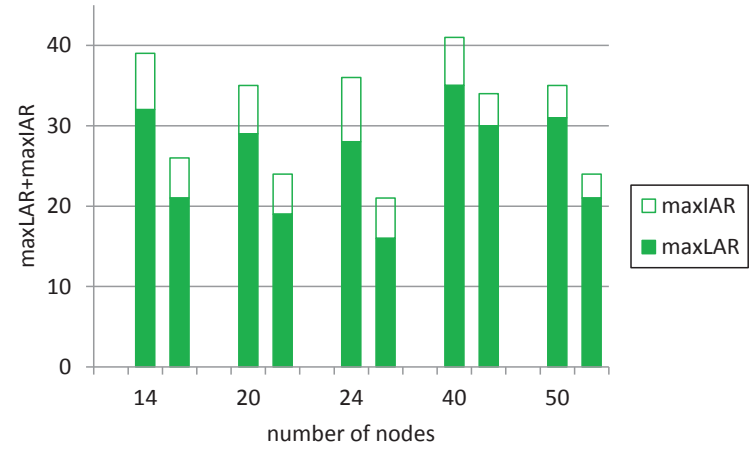


(b)

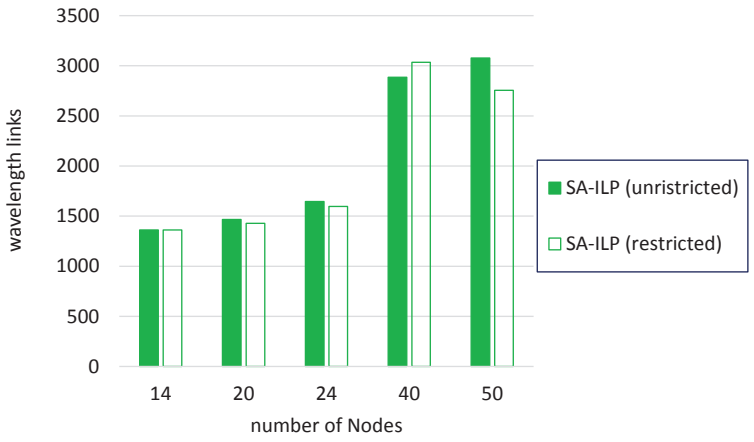
Figure 3.6: Variation of blocking probabilities with number of available channels for 40-nodes network with (a) 100 Erlang and (b) 200 Erlang traffic.

in an upper limit of 9 hops. Putting a restriction on the path length did not affect the $avgLAR + avgIAR$ values obtained using SA-ILP, however it did improve the $maxLAR + maxIAR$ values, as shown in Fig. 3.7a.

Fig. 3.7b compares the resource consumption in terms of wavelength links used obtained with and without a path length restriction for different topologies with 75 Erlang traffic load. In these figures, the 1^{st} bar shows the results with no path length restriction and the 2^{nd} bar sets $L_{max} = 6$ (for 14 to 24-nodes), or 9 (for



(a)



(b)

Figure 3.7: Performance of SA-ILP with and without path length restrictions. (a) maxLAR+maxIAR and (b) Resource utilization.

40 and 50-nodes). The results indicate that the maximum attack radius can be considerably reduced by limiting the maximum path length. Restricting the path length did not seem to significantly affect resource consumption. However, the blocking probability increased slightly for high traffic loads, when path lengths were restricted. The increase in blocking probability was only observed for the high traffic

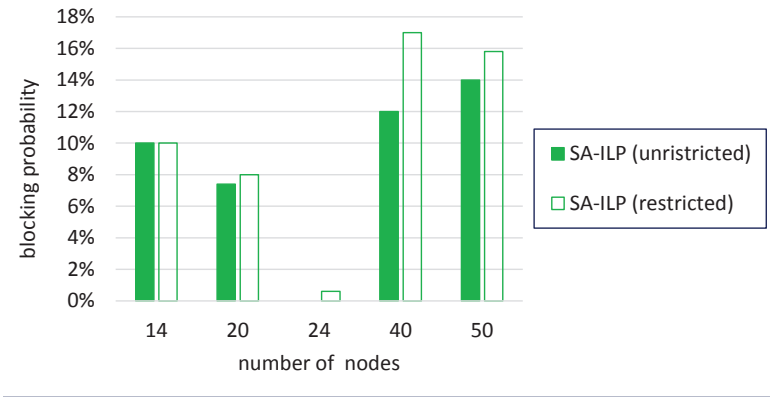
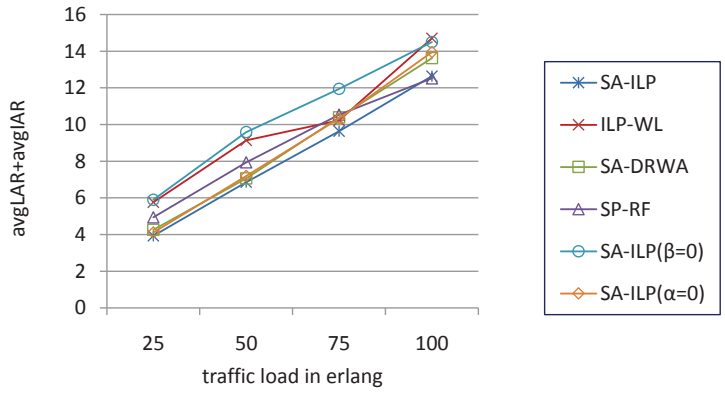


Figure 3.8: Comparison of blocking probabilities for SA-ILP with and without path length restriction for different topologies with 200 Erlang traffic.

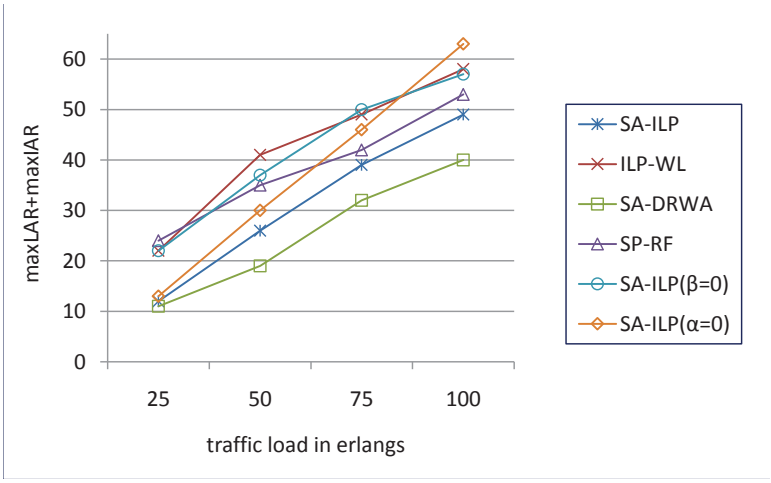
case (200 Erlang), which is shown in Fig. 3.8. So, a reduction in maximum attack radius can be achieved at the cost of slightly increased resource consumption and blocking probability, by restricting the path length.

We also tested SA-ILP with different values for α and β as follows: we set $\alpha = 0$ to minimize IAR only and $\beta = 0$ to minimize LAR only, as shown in Figs. 3.9a and 3.9b for 14-node NSFNET network and Figs. 3.10a and 3.10b for 20-node ARPANET network. The results indicate that for $avgLAR + avgIAR$ values the performance of all approaches are close, but SA-ILP and SA-DRWA consistently provide slightly better results. Setting $\alpha = 0$ (i.e. minimizing IAR only) also performs very well and yields better results than setting $\beta = 0$ (i.e. minimizing LAR only). For $maxLAR+maxIAR$ values SA-ILP and SA-DRWA clearly perform better than the other approaches overall, and as before minimizing IAR only gives better results than minimizing LAR only. The results for the 100 Erlang traffic load are somewhat anomalous, since some approaches accommodate fewer lightpaths than others.

The new modified ILP which we called SA-ILP2 performed worse than both SA-ILP and ILP-WL in almost all cases. This is because, for SA-ILP2, the new



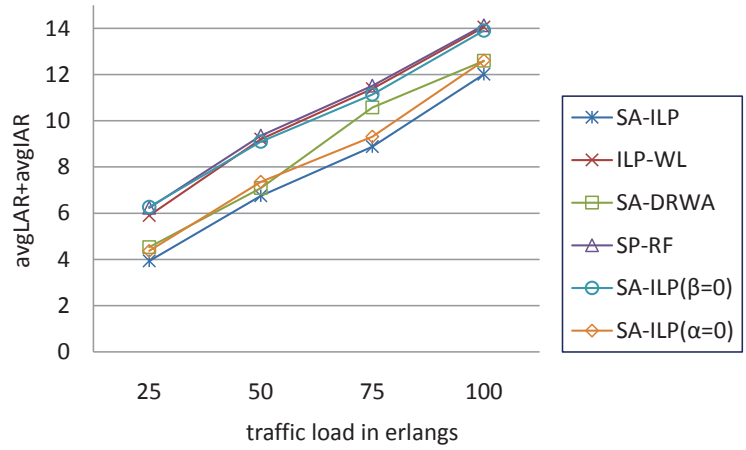
(a)



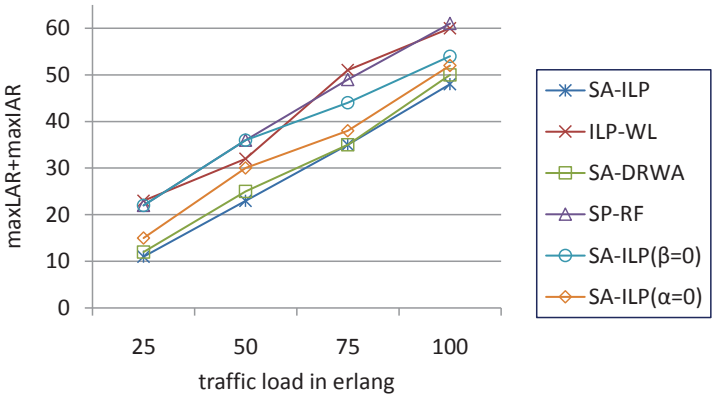
(b)

Figure 3.9: Comparison of (a) avgLAR+avgIAR and (b) maxLAR+maxIAR for all approaches for 14-node network.

lightpath may be routed over a longer path, in order to avoid inclusion in the attack group of an existing lightpath, which currently has the maximum attack radius. However, this will increase the likelihood of link and/or node sharing with other lightpaths. So, not only is the attack radius of the new lightpath typically higher (though still less than the maximum attack radius), it also has a higher chance of being in the attack group of future lightpaths. Based on our results, we conclude



(a)

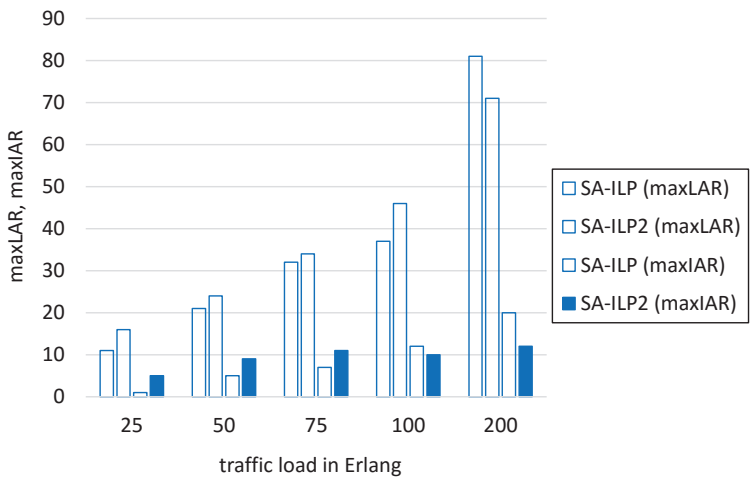


(b)

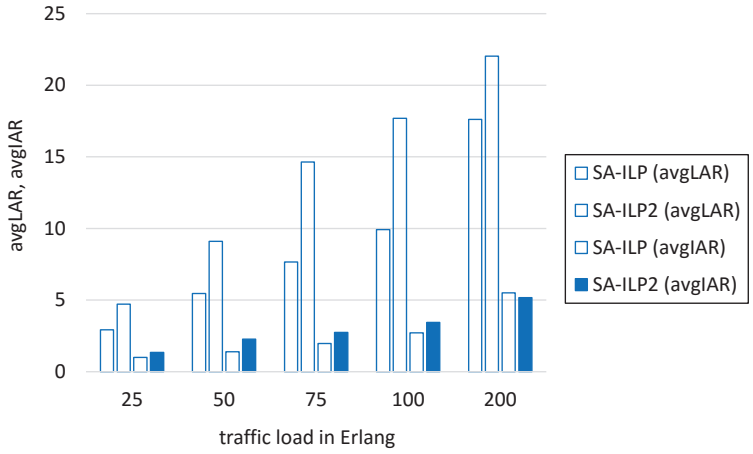
Figure 3.10: Comparison of (a) avgLAR+avgIAR and (b) maxLAR+maxIAR for all approaches for 20-node network.

that minimizing the maximum attack radius may be a suitable objective for *static* RWA; however, it is not appropriate the dynamic case, since it does not allow us to take a global view. Figs. 3.11a and 3.11b show the results of SA-ILP2 compared to SA-ILP.

Finally, we discuss the solution times for the different approaches, shown in Table 3.3. Clearly, both ILP formulations (SA-ILP and ILP-WL) require significantly



(a)



(b)

Figure 3.11: Performance of SA-ILP2 compared to SA-ILP. (a) maxLAR and maxIAR and (b) avgLAR and avgIAR.

higher solution times, compared to the heuristic approaches (SA-DRWA and SP-RF) for all network topologies and traffic loads. The actual values of the solution times are not so important, since these values will change with the specific hardware and processor used. However, the clear trend is that the ILP formulations always takes significantly longer than the heuristics. Therefore, SA-ILP can be used as

Table 3.3: Solution time per lightpath in seconds.

Topologies	Lightpaths	Traffic load	SA-ILP	ILP-WL	SA-DRWA	SP-RF
NSFNET	187	25	0.091	0.107	0.027	0.005
	360	50	0.125	0.136	0.036	0.006
	565	75	0.172	0.143	0.039	0.007
	712	100	0.184	0.152	0.039	0.007
	1380	200	0.128	0.121	0.035	0.010
ARPANET	173	25	0.087	0.121	0.040	0.006
	318	50	0.116	0.179	0.053	0.009
	487	75	0.181	0.201	0.049	0.008
	663	100	0.259	0.226	0.008	0.009
	1370	200	0.230	0.220	0.005	0.010
USANET	168	25	0.161	0.167	0.042	0.006
	336	50	0.241	0.217	0.057	0.009
	487	75	0.472	0.253	0.066	0.010
	710	100	0.323	0.263	0.066	0.011
	1373	200	0.498	0.391	0.063	0.012
40 nodes	171	25	0.292	0.292	0.064	0.023
	342	50	0.383	0.365	0.076	0.018
	501	75	0.501	0.419	0.074	0.018
	708	100	0.486	0.415	0.075	0.018
	1419	200	0.283	0.278	0.067	0.018
50 nodes	176	25	0.335	0.347	0.091	0.045
	341	50	0.416	0.434	0.103	0.029
	512	75	0.527	0.490	0.107	0.027
	694	100	0.621	0.572	0.105	0.027
	1312	200	1.269	1.054	0.092	0.024

a benchmark to evaluate SA-DRWA. However, even in cases where SA-ILP does converge, it is possible that it will not generate the optimal solutions within a reasonable time. In such cases it will be necessary to use a security aware heuristic approach, such as SA-DRWA.

Chapter 4

Resilient RWA Algorithm Using Path Protection for Data Center Networks (DCNs)

4.1 Introduction

We consider the design of resilient data center networks using WDM, where the requests for communication are *dynamic lightpath demands* (DLD) [106]. Each request in DLD has a specified duration and a start time. In WDM networks, A lightpath is established when a communication request arrives and torndown when the communication is over. The resources used for the communication are reclaimed for possible deployment in handling some future request for communication. Our proposed scheme to handle disasters uses the idea of path protection [10, 48]. In a network using path protection, for each request for communication, two lightpaths are provisioned - a *primary* lightpath, used when the network is fault-free and a *backup* lightpath to be used when a fault disrupts the primary lightpath. The

problem of resilient data center network design is significantly different from classical path protection, where the focus was on link failures. In classical path protection, each request for data communication is from a specified source node to a destination node [48] and it is assumed that the source and the destination nodes themselves are not affected by a fault. In the case of data center networks, all components (e.g., fibers, routers or data centers) of the network located within a specific geographical area, will become inoperative due to a disaster affecting the area [27]. In this scenario a disaster may very well affect the data centre used as the source of the primary lightpath. In order to guarantee services in the event of a disaster, data replication is needed, where copies of each file are stored in multiple data centers [107].

The design of resilient data centre networks, for static lightpath demands using WDM, was considered in [60]. The objective was to determine simultaneously i) the replication strategy for the files in the network, and ii) the RWA to set up, for each request for communication, the primary lightpath and the backup lightpath. The algorithm is executed before the network becomes operational. This approach is reasonable for static lightpath demands, where the requests are known at design time. Unlike the static situation considered in [60], in dynamic model requests for communication are not known at design time. Since it is not feasible to change the replication strategy in response to a request for communication, the replication strategy must be determined *before* the network is deployed and the question of provisioning of lightpaths must be considered only at run-time in response to each request for communication. Since the communication requests are not known, the replication strategy must ensure that, for *all* disaster scenarios $d \in \mathcal{D}$, path protection is possible for *all* possible communication requests. If the replication strategy determines that a file f_i needs to have m copies, the strategy must also decide which data centers $\mathcal{S}_i^1, \mathcal{S}_i^2, \ldots, \mathcal{S}_i^m$ should have a copy of file f_i. This replication strategy

must ensure that these selected data centers are such that, for any node t in the network and any file f_i,

- When the network is fault-free, it is possible to have a path from some node $\mathcal{S}_i^j$ to t, such that the length of the path is less than the optical reach [108].
- When any disaster occurs that disrupts the primary path, it is possible to have a fault-free path from some node $\mathcal{S}_i^k$ to t, such that the length of the path is less than the optical reach. We note that regardless of the disaster $d \in \mathcal{D}$ that occurs, it must be possible to use the same backup path to node t.
- The capacities of the data centers may not be exceeded.

If the above conditions are not satisfied, then, for at least one disaster, some node will be always unable to retrieve some file in the network. When processing a request for communication, the primary and the backup lightpath must satisfy the wavelength continuity constraint and the wavelength clash constraint [10]. As in any dynamic RWA, it is quite possible that resources to set up the primary and/or the backup lightpath are not available and the request has to be blocked.

We propose an ILP formulation to solve, optimally, the problem of deploying a primary lightpath and a backup lightpath to handle a request for communication. To the best of our knowledge this is the first investigation of resilient WDM networks for data centers, using dynamic RWA. Such an optimal algorithm is primarily useful as a benchmark for fast heuristics since it is relatively slow. In the following sections, we have presented the ILP and have studied the resource requirements of this algorithm. We have also developed a fast heuristic for the same problem.

4.1.1 Preamble

If a region-based disaster model [22] is used, a disaster d is characterised by a set S_d of elements, where $S_d = \{e_1, e_2, \ldots, e_p\}$, and each element $e_i \in S_d$ represents some component of the network (e.g., a fiber, a node) that will be destroyed by disaster d. In the case of a wide-area network, where the size of the area affected by a disaster is likely to be small, compared to the average distances between the nodes in the fiber network, the number of possible disasters is potentially infinite. The effect of disaster d_1 is, in every respect, more severe than disaster d_2, if $S_{d_1} \supset S_{d_2}$. In this case, we will say that disaster d_1 *dominates* disaster d_2. We define a disaster d to be a *dominant disaster* if there does not exist any other disaster $\hat{d}$, such that disaster $\hat{d}$ dominates disaster d. The number of dominant disasters is finite and can be enumerated in a straight-forward manner. Our algorithm is not dependent on the definition of a disaster and we assume, from now on, that we have enumerated the set $\mathcal{D}$ of dominant disasters that we have to take into account.

In our case the possibility of a disaster affecting all components in a region is considered. This includes the possibility of the failure of the node S used as the source of the primary lightpath. Since files are replicated in data centers, there are multiple copies of each file in the network. Such replication provides resiliency and also improved network throughput. Our scheme, like the traditional path protection scheme, also involves a primary lightpath and a backup lightpath. When there is a request for communication for a file to a destination D, both the primary and the backup lightpath start from a source of the file and ends at the destination node D. However the sources for the primary lightpath will be different from the source for the backup lightpath such that both source cannot be affected by the same region-based disaster.

4.2 An Optimal Algorithm to Solve the Disaster-Aware Dynamic RWA for DCNs

4.2.1 Replication Strategy

In this section we propose a simple replication strategy for data centers using WDM technology. In this strategy we assume that the capacity of a data center is not a limiting factor. This means that each data centre can store any number of files. The objective of this strategy is to determine a minimum number of sites where a file has to be stored to ensure the existence of a primary path from a site where the file is stored and a backup path, from another site where the file is also stored, to any node in the network. We formulated our replication problem into an ILP. This same strategy has to be used for all the files stored in the system.

Notation:

$\boldsymbol{N}$**:** the set of nodes (including the virtual node s).

$\boldsymbol{E}$**:** the set of directed edges of the network.

$\boldsymbol{S}$**:** the set of datacenters (subset of N).

$\boldsymbol{\mathcal{D}}$**:** the set of dominant disasters.

$\boldsymbol{\mathcal{E}^d}$**:** the set of edges disrupted due to disaster $d \in \mathcal{D}$.

$\boldsymbol{d_{max}}$**:** the optical reach.

$\boldsymbol{\ell_{ij}}$**:** the length of the fiber $(i, j) \in E$.

$\boldsymbol{\mathcal{E}^d}$**:** the set of edges disrupted due to disaster $d \in \mathcal{D}$.

Variables:

$\boldsymbol{x_{ij}^{kl}}$**:** a binary variable for all edge $(i,j) \in E$, all datacenters k and all destinations l where

$$x_{ij}^{kl} = \begin{cases} 1 & \text{if edge } (i,j) \text{ is used for the primary} \\ & \text{path from datacenter } k \text{ to destination } l, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{y_{ij}^{kl}}$**:** a binary variable for all edge $(i,j) \in E$, all datacenters k and all destinations l where

$$y_{ij}^{kl} = \begin{cases} 1 & \text{if edge } (i,j) \text{ is used for the backup} \\ & \text{path from datacenter } k \text{ to destination } l, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{p^{k}}$**:** a binary variable for all datacenters k where

$$p^{k} = \begin{cases} 1 & \text{if } x^{kl} = 1 \text{ for some } l \text{ or} \\ & \text{if } y^{kl} = 1 \text{ for some } l \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{x^{kl}}$**:** a binary variable for all datacenters k and all destinations l where

$$x^{kl} = \begin{cases} 1 & \text{if node } k \text{ is selected as a source for the} \\ & \text{primary path for some } l, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{y^{kl}}$**:** a binary variable for all datacenters k and all destinations l where

$$y^{kl} = \begin{cases} 1 & \text{if node } k \text{ is selected as a source for the} \\ & \text{backup path for some } l, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{P^{dl}}$**:** a binary variable for all disasters d and all destinations l where

$$P^{dl} = \begin{cases} 1 & \text{if disaster } d \text{ appears in the primary path} \\ & \text{for some } l \\ 0 & \text{otherwise.} \end{cases}$$

B^{dl}: a binary variable for all disasters d and all destinations l where

$$B^{dl} = \begin{cases} 1 & \text{if disaster } d \text{ appears in the backup path} \\ & \text{for some } l \\ 0 & \text{otherwise.} \end{cases}$$

4.2.2 Integer Linear Program Formulation

Objective: Minimize

$$\sum_{k \in S} p^k \tag{4.1}$$

Subject to:

1. flow balance constraint for primary path:

$$\sum_{j:(i,j)\in E} x_{ij}^{kl} - \sum_{j:(j,i)\in E} x_{ji}^{kl} = \begin{cases} x^{kl} & \text{if } i = k, \\ -x^{kl} & \text{if } i = l, \quad \forall i, l \in N, \forall k \in S \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

2. flow balance constraint for backup path:

$$\sum_{j:(i,j)\in E} y_{ij}^{kl} - \sum_{j:(j,i)\in E} y_{ji}^{kl} = \begin{cases} y^{kl} & \text{if } i = k, \\ -y^{kl} & \text{if } i = l, \quad \forall i, l \in N, \forall k \in S \\ 0 & \text{otherwise.} \end{cases} \tag{4.3}$$

3. Ensure that the length of the route used by the primary and backup lightpath is less than the optical reach d_{max}.

$$\sum_{j:(i,j)\in E} \ell_{ij} \cdot x_{ij}^{kl} \leq d_{max} \quad \forall l \in N, \forall k \in S \tag{4.4}$$

$$\sum_{j:(i,j)\in E} \ell_{ij} \cdot y_{ij}^{kl} \leq d_{max} \quad \forall l \in N, \forall k \in S \tag{4.5}$$

4. Only one source node for each communication l

$$\sum_{k\in S} x^{kl} = 1 \quad \forall l \in N \tag{4.6}$$

$$\sum_{k\in S} y^{kl} = 1 \quad \forall l \in N \tag{4.7}$$

5. If the primary lightpath uses any edge affected by disaster d, set P^{dl} to 1; otherwise, set P^{dl} to 0.

$$P^{dl} \geq e_{ij}^{d} \cdot x_{ij}^{kl} \quad \forall (i,j) \in \mathcal{E}^d, d \in \mathcal{D}, k \in S, l \in V \tag{4.8}$$

$$P^{dl} \leq \sum_{i,j:e_{ij}^{d}=1} x_{ij}^{kl} \quad \forall d \in \mathcal{D}, k \in S, l \in V \tag{4.9}$$

$$\sum_{d} P^{dl} = 0 \quad \forall l \in \mathcal{D} \tag{4.10}$$

6. If the backup lightpath uses any edge affected by disaster d, set B^{dl} to 1; otherwise, set B^{dl} to 0.

$$B^{dl} \geq e_{ij}^{d} \cdot y_{ij}^{kl} \quad \forall (i,j) \in \mathcal{E}^d, d \in \mathcal{D}, k \in S, l \in V - \mathcal{D} \tag{4.11}$$

$$B^{dl} \leq \sum_{i,j:e_{ij}^{d}=1} y_{ij}^{kl} \quad \forall d \in \mathcal{D}, k \in S, l \in V - \mathcal{D} \tag{4.12}$$

$$\sum_{d} B^{dl} = 0 \quad \forall l \in \mathcal{D} \tag{4.13}$$

7. Primary and backup paths are disaster-disjoint

$$P^{dl} + B^{dl} \leq 1 \quad \forall d \in \mathcal{D}, l \in V \tag{4.14}$$

8. By definition p^k is the logical OR relation of all x^{kl} (y^{kl}) which means it is 1 if a datacenter k has been chosen as a source for the primary (backup) lightpath for some l . This is equivalent to the following non-linear constraint: $p^k = x^{kl} \vee y^{kl}$

$$p^k \geq x^{kl} \quad \forall k \in S, l \in V \tag{4.15}$$

$$p^k \geq y^{kl} \quad \forall k \in S, l \in V \tag{4.16}$$

$$p^k \leq \sum_{l} x^{kl} + y^{kl} \quad \forall k \in S \tag{4.17}$$

4.2.3 Justification of the Replication ILP R_{OPT}

If the disaster d involve the destination node l of the communication it means that node l is unable to operate and hence communication to l is never possible. Replication in such a situation makes no sense and so we have excluded this case when ensuring that at most one of P^{dl} and B^{dl} may be 1 (constraint (4.14)). To

achieve that we forced both P^{dl} and B^{dl} to be 0 (constraints (4.10 and 4.13). In all remaining cases, if edge $(i,j) \in \mathcal{E}^d$ (in other words, $e_{ij}^d = 1$) and edge (i,j) appears in the selected primary path from k to l (in other words, $x_{ij}^{kl} = 1$), P^{dl} is set to 1 using constraint (4.8). If the condition for constraint (4.8) is never satisfied, constraint (4.9) forces P^{dl} to be 0. A similar argument holds for the backup path constraints (4.11) and (4.12).

By definition p^k is 1 if a DC k has been chosen as a source for the primary (backup) lightpath for some l (i.e., $x^{kl} = 1$ for some l); otherwise it is 0. If any $x^{kl} = 1$ ($y^{kl} = 1$), constraint (4.15 (constraint (4.16)) ensure that p^k to be 1. If no DC is selected as a source for the primary (backup) lightpath, constraint (4.17) forces p^k to be 0. The remaining constraints are straight-forward.

4.2.4 Disaster-aware RWA ILP

This optimal algorithm will be used when we receive a request for communicating some file f_i to node t. In general, the network is already supporting a number of on-going communication. The replication strategy and the details of each existing communication are known to us, so that, for each on-going communication, we have the routes and the channels used by the corresponding primary lightpath and the backup lightpath. If we are successful in handling the new request, we should be able to obtain details about the primary lightpath and the backup lightpath to be used that avoids any edge affected by disaster d. We must ensure that the following conditions are satisfied:

- The primary lightpath to handle the fault-free case will be from some node $\mathcal{S}_i^j, 1 \leq j \leq m$, to node t.
- The backup lightpath to be used in the case of any disaster $d \in \mathcal{D}$, that disrupts the primary lightpath, will be from some node $\mathcal{S}_i^l, 1 \leq l \leq m$. Here

$j \neq l$, since a disaster can disrupt the source $\mathcal{S}_i^j$ of the primary lightpath. Such a backup lightpath must avoid any of the edges affected by all disaster $d \in \mathcal{D}$ that disrupts the primary lightpath.

- The length of the path used by each of these lightpaths does not exceed the optical reach.
- Each lightpath satisfies the wavelength continuity constraint and the wavelength clash constraint with respect to any of the existing lightpaths.

Our objective is to minimize the cost of the resources needed to handle the new request for communication. The resources will be measured by the total number of channels used to handle this request, which were not used by any of the existing communication. For this algorithm, it convenient to categorize each channel on every fiber as follows. A *type 1* channel is not used by the primary or backup lightpath of any ongoing communication. This is the only type of channel that may be used by the new primary lightpath and also may be used by the new backup lightpath. The cost of using such a channel on a fiber will be 1. A *type 2* channel is that used by one or more backup lightpaths. Such a channel on a fiber is used to handle a set of disasters $\hat{\mathcal{D}}$, where disaster $d \in \hat{\mathcal{D}}$ disrupts exactly one primary lightpath whose corresponding backup lightpath uses this channel. A type 2 channel on a fiber may be used by the new backup lightpath, only if disaster $d \in \hat{\mathcal{D}}$ *does not disrupt* the new primary lightpath. This captures the essential idea of shared path protection. The cost of a type 2 channel on a fiber will be 0, since such a channel is already in use by existing backup lightpath(s). A *type 3* channel on a fiber is that used by the primary lightpath of some ongoing communication. Such a channel cannot be used to handle the new request.

When processing a request for transmitting file f_i to a node t, it is convenient

to visualize a new *virtual node* s and some new *virtual edges* from s as follows. For each data centre $\mathcal{S}_i^j, 1 \leq j \leq m$, we visualize a single virtual edge from virtual node s to data centre $\mathcal{S}_i^j$ of length 0.

4.2.5 ILP Formulation

We will use the following constants and variables:

$\boldsymbol{N}$**:** the set of nodes (including the virtual node s).

$\boldsymbol{E}$**:** the set of directed edges of the network. If i and j are nodes of the fiber network (including the data centers), edge $(i, j) \in E$ represents a fiber from node i to node j. Set E also includes the virtual edges from the virtual node s to each data centre $\mathcal{S}_i^l$ that contains a copy of file f_i.

$\boldsymbol{d_{max}}$**:** the optical reach.

$\boldsymbol{M}$**:** A large constant.

$\boldsymbol{\ell_{ij}}$**:** the length of the fiber $(i, j) \in E$.

$\boldsymbol{\mathcal{D}}$**:** the predefined set of disasters.

$\boldsymbol{K}$**:** set of channels per fiber.

$\boldsymbol{\mathcal{E}^d}$**:** the set of edges disrupted due to disaster $d \in \mathcal{D}$.

$\boldsymbol{c_{ij}^k}$**:** a constant where $c_{ij}^k = 1$ if channel k is used on edge (i, j), either for a primary lightpath or for a backup lightpath; 0 otherwise.

$\boldsymbol{\beta_{ij}^{kd}}$**:** a constant where $\beta_{ij}^{kd} = 1$ if channel k on edge (i, j) is used for one or more backup lightpath which do not handle disaster d; 0 otherwise.

e_{ij}^d: a constant indicating whether edge (i, j) is affected by disaster d, where $e_{ij}^d = 1$ if edge $(i, j) \in \mathcal{E}^d$; 0 otherwise.

x_{ij}: a binary variable where $x_{ij} = 1$ if edge (i, j) is used by the primary lightpath; 0 otherwise. Variable y_{ij} is defined similarly for the backup lightpath.

w_{ij}^d: a binary variable where $w_{ij}^d = 1$ if disaster d affects the primary lightpath and edge (i, j) is used by the backup lightpath; 0 otherwise.

z_P^d: a binary variable where $z_P^d = 1$ if the primary lightpath uses any edge disrupted by disaster d; 0 otherwise. Variable z_B^d is defined similarly for the backup lightpath.

μ^k: a binary variable where $\mu^k = 1$ if channel k is used by the primary lightpath; 0 otherwise. Variable ν^k is defined similarly for the backup lightpath.

s_{ij}^{kd}: a bounded variable which is constrained to have a value 1 or 0, where $s_{ij}^{kd} = 1$ if i) $z_P^d = 0$ or ii) if channel k on edge (i, j) may be shared by the new backup lightpath to handle disaster d; 0 otherwise.

s_{ij}^k: a bounded variable which is constrained to have a value 1 or 0, where $s_{ij}^k = 1$ if edge (i, j) is used by the backup lightpath of new communication and channel k on this edge may be shared with other backup lightpaths to handle all disasters that disrupt the primary lightpath; 0 otherwise.

y_{ij}^k: a bounded variable which is constrained to have a value 1 or 0, where $y_{ij}^k = 1$ if the backup lightpath uses channel k on edge (i, j); 0 otherwise.

Objective: Minimize

$$\sum_{j:(i,j)\in E} x_{ij} + \sum_{k\in K} \sum_{j:(i,j)\in E} y_{ij}^k.(1 - c_{ij}^k) \tag{4.18}$$

Subject to:

1. Enforce, for all node $i \in N$, flow conservation on the path used by the primary lightpath.

$$\sum_{j:(i,j)\in E} x_{ij} - \sum_{j:(j,i)\in E} x_{ji} = \begin{cases} 1 & \text{if } i = s, \\ -1 & \text{if } i = t, \\ 0 & \text{otherwise.} \end{cases} \tag{4.19}$$

2. For each disaster $d \in \mathcal{D}$ that disrupts the primary lightpath, enforce, for all node $i \in N$, flow conservation on the path used by the backup lightpath. This path must avoid all edges affected by disaster d. If a disaster $d \in \mathcal{D}$ does not disrupt the primary lightpath, there should not be any flow on the backup path.

$$\sum_{j:(i,j)\in E-\mathcal{E}^d} w_{ij}^d - \sum_{j:(j,i)\in E-\mathcal{E}^d} w_{ji}^d = \begin{cases} z_P^d & \text{if } i = s, \\ -z_P^d & \text{if } i = t, \\ 0 & \text{otherwise.} \end{cases} \tag{4.20}$$

3. Determine the backup path.

$$y_{ij} \leq (1 - z_P^d) \cdot M + w_{ij}^d \quad \forall (i,j) \in E, d \in \mathcal{D} \tag{4.21}$$

$$y_{ij} \geq w_{ij}^d \quad \forall (i,j) \in E, d \in \mathcal{D} \tag{4.22}$$

4. Ensure that the length of the route used by the primary (backup) lightpath is less than d_{max}.

$$\sum_{j:(i,j)\in E} \ell_{ij} \cdot x_{ij} \leq d_{max} \tag{4.23}$$

$$\sum_{j:(i,j)\in E} \ell_{ij} \cdot y_{ij} \leq d_{max} \tag{4.24}$$

5. Ensure that exactly one channel k is used for the new primary (backup) light-

path.

$$c_{ij}^{k} \cdot x_{ij} + \mu^{k} \leq 1 \quad \forall (i,j) \in E, k \in K \tag{4.25}$$

$$\sum_{k} \mu^{k} = 1 \tag{4.26}$$

$$c_{ij}^{k} \cdot y_{ij} - s_{ij}^{k} + \nu^{k} \leq 1 \quad \forall (i,j) \in E, k \in K, d \in \mathcal{D} \tag{4.27}$$

$$\sum_{k} \nu^{k} = 1 \tag{4.28}$$

6. If the primary (backup) lightpath uses any edge affected by disaster d, set z_P^d (z_B^d) to 1; otherwise, set z_P^d (z_B^d) to 0.

$$z_P^d \geq x_{ij} \quad \forall d \in \mathcal{D}, (i,j) \in E : e_{ij}^d = 1 \tag{4.29}$$

$$z_P^d \leq \sum_{i,j:e_{ij}^d=1} x_{ij} \quad \forall d \in \mathcal{D} \tag{4.30}$$

$$z_B^d \geq y_{ij} \quad \forall d \in \mathcal{D}, (i,j) \in E : e_{ij}^d = 1 \tag{4.31}$$

$$z_B^d \leq \sum_{i,j:e_{ij}^d=1} y_{ij} \quad \forall d \in \mathcal{D} \tag{4.32}$$

7. The primary lightpath and the backup lightpath must be disaster-disjoint.

$$z_P^d + z_B^d \leq 1 \quad \forall d \in \mathcal{D} \tag{4.33}$$

8. Compute the value of s_{ij}^{kd}.

$$s_{ij}^{kd} = 1 : \beta_{ij}^{kd} = 1 \quad \forall (i,j) \in E, k \in K, d \in \mathcal{D} \tag{4.34}$$

$$s_{ij}^{kd} = (1 - z_P^d) : \beta_{ij}^{kd} = 0 \quad \forall (i,j) \in E, k \in K, d \in \mathcal{D} \tag{4.35}$$

9. Compute the value of s_{ij}^k.

$$s_{ij}^k \leq s_{ij}^{kd} \quad \forall (i,j) \in E, k \in K, d \in \mathcal{D} \tag{4.36}$$

$$s_{ij}^k \leq y_{ij} \quad \forall (i,j) \in E, k \in K \tag{4.37}$$

$$s_{ij}^k \geq \sum_{d \in \mathcal{D}} s_{ij}^{kd} - |\mathcal{D}| + y_{ij} \quad \forall (i,j) \in E, k \in K \tag{4.38}$$

10. Compute the value of y_{ij}^k.

$$y_{ij}^k \leq y_{ij} \quad \forall (i,j) \in E, k \in K \tag{4.39}$$

$$y_{ij}^k \leq \nu^k \quad \forall (i,j) \in E, k \in K \tag{4.40}$$

$$y_{ij}^k \geq y_{ij} + \nu^k - 1 \quad \forall (i,j) \in E, k \in K \tag{4.41}$$

4.2.6 Justification of the ILP formulation

The objective function minimizes the number of *type 1* channels used. The first (second) term is the total number of *type 1* channels used by the primary (backup) lightpath. For the primary lightpath, a *type 1* channel is used on each edge in the path. For the backup lightpath, if for edge $(i,j) \in E$, $c_{ij}^k = 1$, channel k on edge (i,j) is a *type 2* channel, which may be shared by the new backup lightpath for free. Therefore we only count the number of edges used by the new backup lightpath for which $c_{ij}^k = 0$.

Constraint (4.20) forces the value of w_{ij}^d to be 0 if disaster d does not disrupt the primary lightpath (i.e., $z_P^d = 0$). If $z_P^d = 1$, it is the standard flow constraint equation that determines a backup path for disaster d. If $z_P^d = 0$ ($z_P^d = 1$), constraints (4.21) and (4.22) become $y_{ij} \leq M$ and $y_{ij} \geq 0$ ($y_{ij} \leq w_{ij}^d$ and $y_{ij} \geq w_{ij}^d$). Thus, if $z_P^d = 0$, disaster d imposes trivial constraints; otherwise, $y_{ij} = w_{ij}^d$.

Constraint (4.25) forces μ^k to be 0 if the primary lightpath uses edge (i, j) and channel k is already in use by some existing lightpath. If $s_{ij}^k = 0$ (i.e., channel k on edge (i, j) cannot be shared with the new backup lightpath) constraint (4.27) is the same as constraint (4.25). If $s_{ij}^k = 1$, constraint (4.27) allows ν^k to be 1. Let the path used by the primary lightpath have m edges that also appear in disaster d. If the primary lightpath is not affected (is affected) by disaster d, $m = 0$ ($m \geq 1$). If $m = 0$, constraints (4.29) and (4.30) become $z_P^d \geq 0$ and $z_P^d \leq 0$, forcing z_P^d to be 0. If $m > 0$, constraints (4.29) and (4.30) become $z_P^d \geq 1$ and $z_P^d \leq m$, forcing z_P^d to be 1, since z_P^d is a binary variable. The justification for constraints (4.31) and (4.32) are similar for the backup lightpath. Constraint (4.33) ensures that no disaster d disrupts both the primary and the backup lightpath.

By definition, $s_{ij}^{kd} = \beta_{ij}^{kd} \vee (1 - z_P^d)$ where $\vee$ symbol denotes the OR operator. It may be readily verified that s_{ij}^{kd} may be computed using constraints (4.34) and (4.35).

The value of s_{ij}^k should be 0, if any edge (i, j) is not used by the backup path (constraint (4.37)) or if, for at least one disaster d, $s_{ij}^{kd} = 0$ - so that channel k on edge (i, j) cannot handle disaster d (constraint (4.36)). We note that for all disasters $d \in \mathcal{D}$, if channel k may be shared on edge (i, j), $s_{ij}^{kd} = 1$. In such a situation $\sum_{d \in \mathcal{D}} s_{ij}^{kd} = \mathcal{D}$. If all conditions for sharing channel k on edge (i, j), constraints (4.36)) – (4.38)) become $s_{ij}^k \leq 1, s_{ij}^k \leq 1$ and $s_{ij}^k \geq 1$ respectively, giving $s_{ij}^k = 1$. The justification for constraints (4.39) – (4.41) is also similar to those for

constraints (4.36) – (4.38). Here we need to compute the value of y_{ij}^k using the non-linear constraint $y_{ij}^k = y_{ij} \cdot \nu^k$.

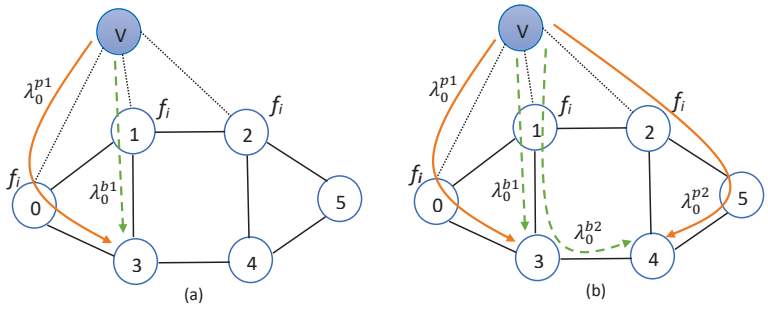


Figure 4.1: An illustrative example showing the effect of backup paths resources' sharing.

4.2.7 Illustrative Example

We illustrate a simple example of a 6-node network where the only ongoing communication is that of some file f_i being communicated to node 3 and file f_i is stored at nodes 0, 1 and 2. The network topology including the requisite virtual node connected to the three DC locations at nodes 0, 1, and 2, is shown in Fig. 4.1. We assume that there are 3 available channels (wavelengths) per fiber (i.e., $\lambda_0, \lambda_1, \lambda_2$). Fig. 4.1a shows the primary path $p1$ communicating data from DC at node 0 to node 3 using the route $v \rightarrow 0 \rightarrow 3$. Also, $p1$ is assigned channel λ_0, we denote this channel as λ_0^{p1}, as there is no other primary or backup path that uses this channel on this route. One possible backup path $b1$ created in case of a disaster that may affect $p1$ would be from DC at node 1 to the destination (node 3), $v \rightarrow 1 \rightarrow 3$. The algorithm can assign channel λ_0 to $b1$ as well (λ_0^{b1}). Suppose a new request comes to deliver file f_i to the user at node 4 (i.e., the destination). Fig. 4.1b shows the primary path $p2$ which can be assigned a route $v \rightarrow 2 \rightarrow 5 \rightarrow 4$ and a channel λ_0^{p2}. We note that we do not consider a disaster at the destination node, so when a

disaster at node 2 or 5 affects $p2$, a backup path $b2$ can be designed using the route $v \rightarrow 1 \rightarrow 3 \rightarrow 4$. Since the two backup paths, $b1$ and $b2$, need to avoid different disasters and will not be activated simultaneously, these backups can *share* the same channel λ_0. Therefore, the new backup $b2$ will still be assigned channel λ_0 as well, λ_0^{b2}. We emphasize that this sharing capabilities can lead to significant resources savings.

4.3 A Heuristic for Solving the Disaster-Aware Dynamic RWA problem for DCNs

We also propose a new heuristic algorithm for dynamic allocation of primary and backup lightpaths in a disaster-resilient DCN. The objective of the proposed algorithm is to minimize the amount of additional resources used by the new request. When processing a request for communication, we ensure that the primary and the backup lightpaths satisfy the wavelength continuity constraint and the wavelength clash constraint. We note that, as in any dynamic RWA, it is quite possible that resources to set up the primary and/or the backup lightpath will not be available and the request has to be blocked.

4.3.1 Problem Statement

Given a network using WDM, the replication strategy used and all active communication in the network, our problem is to make provisions, if possible, for a primary and a backup lightpath to handle a request for communicating file f_i to destination t. In our proposed algorithm, we have extended the notion of SPP which has been proposed for RWA for resilient communication [109, 110]. Traditional SPP involves using edge-disjoint paths from the source node to the destination node to deploy the

primary lightpath and the backup lightpath. In the case of communicating file f_i to destination t in a datacenter network, a disaster may very well affect the source of the primary lightpath. Therefore, the backup lightpath must start from a site storing the file f_i, different from that used by the primary lightpath, and terminate at the destination t. Our database stores, for each channel (λ) on each edge ($i,\ j$), whether channel (λ) on edge ($i,\ j$) is i) unused or ii) is used for a primary lightpath or iii) for backup lightpath(s). If channel λ on edge ($i,\ j$) is used for backup lightpath (s), our database stores the list of disasters that require the deployment of these backup lightpaths. We adapted the notion of shared path protection to handle our problem by ensuring that two backup lightpaths may share channel λ on edge ($i,\ j$) only if the two backup lightpaths are never deployed to handle the same disaster.

For an optimal solution our objectives are to i) set up a primary lightpath and ii) make provisions for a backup lightpath to handle, at minimum cost, a request for communicating file f_i to destination t. To achieve this, we i) determine the source s for the primary and for the backup lightpath, ii) find an optimal route for the primary and the backup lightpath, and iii) find an optimal channel for the primary and the backup lightpath. In the optimal solution we have to solve all these problems simultaneously, to minimize the total number of edge-channels used by the primary/backup lightpath that were unused before processing this request. The time needed to find an optimal solution is unacceptably high and, as a heuristic, we have set up the primary lightpath *before* setting up the backup lightpath.

In this study, we visualize a *virtual* node v and some new *virtual* edges from v to each datacenter that stores a copy of the requested file f_i. We have developed an A^* algorithm to search for an optimal primary/backup lightpath using an optimal path from v to t. Each node in the search tree represents a pair (x, L_x) where x is a node

in the network and L_x is a set of channels that may be used to reach node x from v. When evaluating a leaf node $(x,\ L_x)$ of the current search tree, we determine, using an admissible heuristic, the estimated cost of a path from v to t through x using the node (x, L_x) in the search tree.

When expanding a node $(x,\ L_x)$ in the search tree to create an edge in the search tree to node $(y,\ L_y)$, the algorithm ensures that i) there is an edge from x to y in the network topology, ii) the optical reach is not exceeded, iii) the list L_y includes all channels in L_x which are not in use on the fiber $(x \rightarrow y)$, iv) the list L_y is not empty. If these conditions are not satisfied, the node$(y,\ L_y)$ is pruned from the search tree. Our heuristic estimates the minimum number of previously unused channels on edges that will be needed to reach the destination t. We note that the heuristic used when searching for a primary path is somewhat different from that for the backup path. The cost of using a channel on an edge used by the primary lightpath always has a cost of 1. The cost of using a channel on an edge that may be shared by the backup lightpath with an existing backup lightpath has a cost of 0; otherwise the cost is 1. The psudocode of the proposed heuristic is given below.

Pseudocode for Disaster-aware Heuristic Algorithm for DCNs Using WDM.

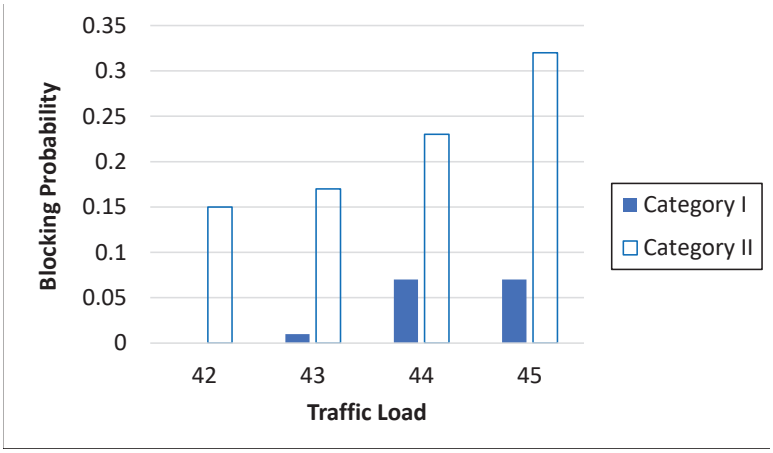
Input
$G(N, E), R, S, D, r, Q, NW\_ST$ //$G(N, E)$: is physical topology with N nodes and E edges. R: replication strategy. S: set of DCs. D: set of disasters. r: new request for communication. Q: set of new requests. NW_ST: network state.
for each new request $r \in Q$ **do**
    pPath=bPath={}; pWl=bWl=-1;
    pPath=findPrimaryPath();
    if pPath $\neq$ null **then**
        pWl = findChannel(pPath); //cost of pWl is 1
        $\mathcal{A}$ = set of disasters disrupting pPath;
        bpath=findBackupPath();
        if bPath $\neq$ null **then**
            bWl = findChannel(bPath);
            $\mathcal{L}$ = set of existing backup lightpaths;
            $\mathcal{B}$ = set of disasters disrupting $\mathcal{L}$ such that $\mathcal{A} \cap \mathcal{B} = \phi$;
            ρ = possible sharing channels between $\mathcal{L}$ and r;
            if $\rho \neq \phi$ **then** //sharing is possible
                assign pWl to bPath; //cost of bWl is 0
            end if
        else
            assign any available channel to bPath; //cost of bWl is 1
        end if
    else
        request r is blocked;
    end if
end for
request r is successful; update NW_ST with pPath, bPath, pWL, bWL
Return pPtah, bPath;
End

4.4 Experimental Results

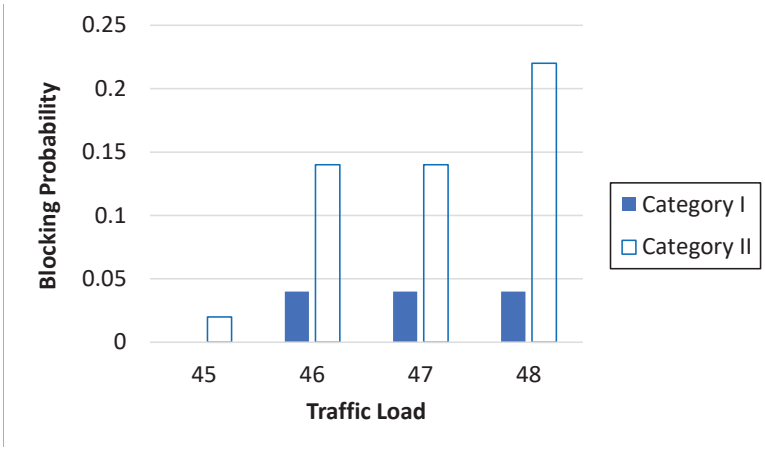
4.4.1 Optimal Algorithm Results

In this section we present the simulation results to evaluate the performance of our proposed approach, considering different networks and disaster scenarios. We used the well-known NSFNET network topology having 14 nodes and 21 links [111]. The number of wavelength per fiber was set to 8 (i.e., $|K| = 8$). We classified disaster scenarios into 2 categories: *category I*, where disaster affected only the data center nodes, and *category II*, where disasters affected any node in the network. We studied category I scenario as it is the most important case and has the most impact on the network performance. We note that in this case, only one DC will be affected at a time. So the network will still be operating but with less data sources. In our experiments, we assume that each disaster affects exactly one node and associated edges. This is reasonable since the size of the area affected by a disaster is expected to be small, compared to the length of the shortest fiber in a wide-area network. Further, the effect of the failure of any edge $i \rightarrow j$ is never more severe, compared to the failure of node i and all edges to/from i. Our algorithms reported in Section 4.2 and Section 4.3 do not depend on which nodes/edges are affected by any disaster. All results reported are the averages of 5 simulation runs. Experiments were carried out on an Intel Core i7-3537U CPU 2.50 GHz processor using IBM ILOG CPLEX version 12.6.2 [105] to solve the ILP formulation.

The simulations had 2 phases. In phase I we created a desired level of traffic on the network, the traffic load, by establishing primary and backup lightpaths for N requests for communication, where N is a predetermined constant. For each such request we established, using our ILP formulation, a primary lightpath as well as a backup lightpath, that avoided all the disasters that disrupted the primary



(a)

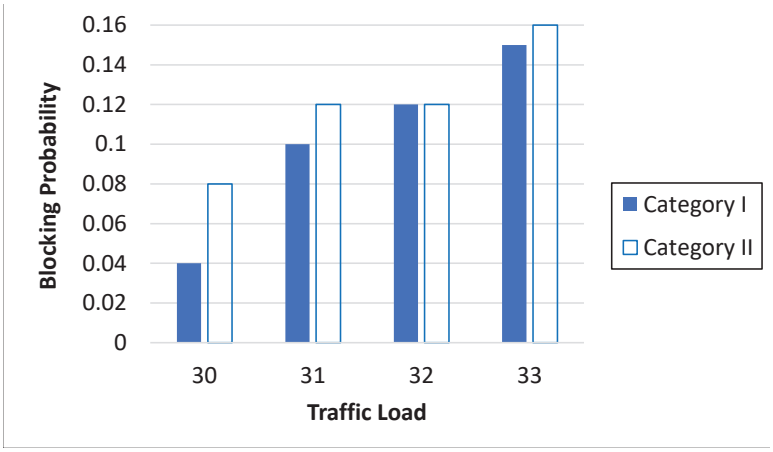


(b)

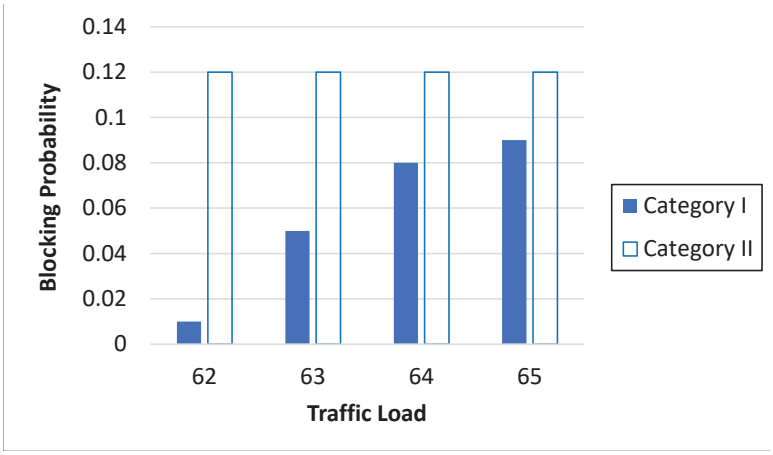
Figure 4.2: Comparison of BP of the new request with different traffic loads and 2 disaster scenarios for 14-node NSFNET network (a) 3 DCs (b) 4 DCs.

lightpath. After processing each request, we updated the network state, so that we recorded which channels on each fiber were used to handle primary lightpaths and which channels on each fiber were used for backup lightpaths. We also kept track of which disaster affects which primary lightpath(s). In Phase II, we kept the network state fixed to the state at the end of phase I. We used a set of randomly generated requests to determine the blocking probability (BP). For each new request, we used our ILP formulation to find out whether a primary lightpath and a backup lightpath

may be set up to handle that request. We have reported below the BP of under different scenarios.



(a)

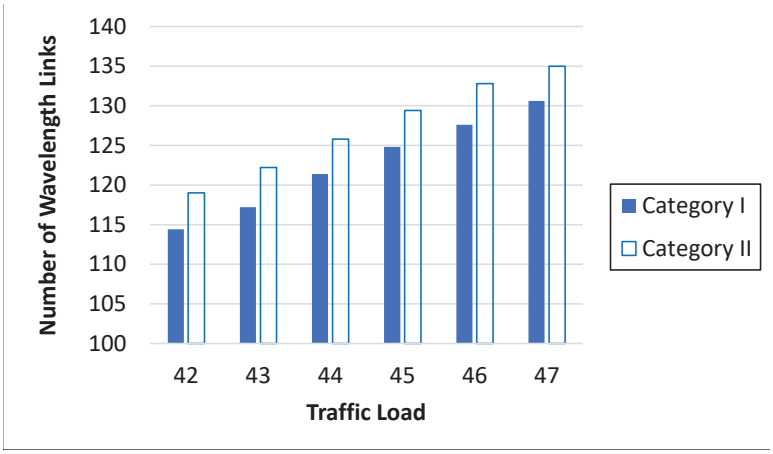


(b)

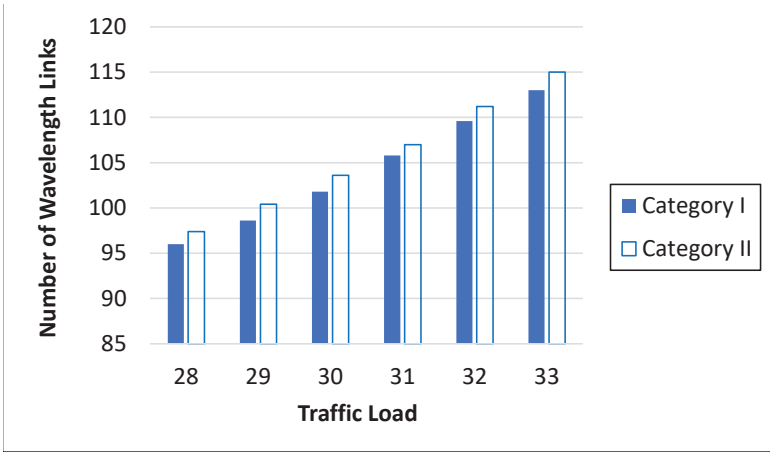
Figure 4.3: Comparison of BP of the new request with different traffic loads and 2 disaster scenarios for 20-node ARPANET network (a) 3 DCs (b) 4 DCs.

Fig. 4.2a compares the BP of new connections for the 14-node NSFNET network with different traffic loads from Phase I. We consider 3 data centers (nodes 0, 5, 9) and two disaster scenarios - category I disasters and category II disasters. Also we took into account that each data center has a copy of each file. As expected, the results show that the BP increases when the number of disasters is increased. Fig.

4.2b shows the BP for the same network and disaster scenarios of Fig. 4.2a but with 4 data centers (nodes 0, 5, 9, 12). In other words, we added an additional data center to the scenario considered in Fig.4.2a. In this figure, the BP is also higher with category II disasters than with category I similar to the situation in Fig. 4.2a. As expected, when we used an additional data center at node 12, the network can handle many more requests for connection in Phase I before reporting any blocked lightpaths or requests for connections in Phase II, which leads to much lower BP.



(a)



(b)

Figure 4.4: Resource usage with different traffic loads (a) NSFNET (b) ARPANET.

Fig. 4.3a and 4.3b report the results obtained by our proposed approach on the 20-node ARPANET network for 3 data centers (nodes 1, 7, 13) and 4 data centers (1, 7, 13, 18) respectively. The results follow a similar pattern as in NSFNET, the BP increases when trying to establish a new connection with higher traffic load. Also, higher BP is reported with disaster scenario of Category II compared to Category I. In addition, adding a new data center, as in Fig. 4.3b, enables the network to handle more requests in Phase I before we see any blocked requests in Phase II. Fig. 4.4a and 4.4b compare the resource usage as the number of lightpaths on the network grows on the NSFNET and ARPANET, respectively. Here we used 3 data centers for both networks. Fig. 4.4 illustrates the number of wavelength links needed to establish the corresponding set of connections, with their primary and backup lightpaths, for category I and category II disasters. Clearly, the resource usage values are quite similar for both disaster categories. We draw an interesting conclusion that, so far as the number of wavelength links are concerned, the cost of considering more disasters is relatively small. Finally, Fig. 4.5 shows the running time obtained by the proposed approarch for trying to setup the new request. The results are for 20-node network, 4 DCs, and category II disaster scenario. As expected for dynamic traffic case, the ILP took a fraction of a second to process the request. The running time considering category I disasters was less and not shown here in the section.

4.4.2 Heuristic Results

We present our experimental results to evaluate our proposed heuristic. We have considered two well-known network topologies, the 14-node NSFNET and 20-node ARPANET networks. Disaster scenarios are *category I*: where disasters can affect any DC node and *category II*: where disasters can affect any node in the network. Our algorithm discussed in Section 2 does not depend on which nodes/edges are af-

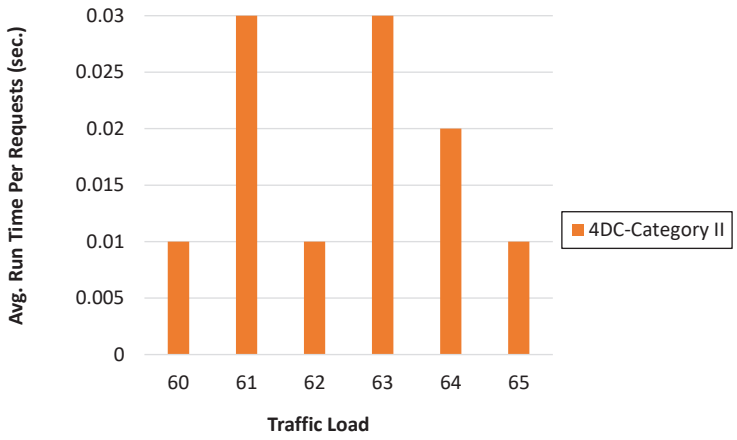


Figure 4.5: Running time per request with different traffic loads for ARPANET with 4 DCs and category II disasters.

fected by any disaster. The obtained results are the averages of at least 5 simulation runs.

The simulations had also taken 2 phases. In phase I we create a desired level of traffic on the network, the traffic load, by establishing primary and backup lightpaths for N requests for communication, where N is a predetermined constant. For each such request, the A^* heuristic algorithm establishes a primary lightpath as well as a backup lightpath, that avoided all the disasters that disrupt the primary lightpath. After processing each request, we update the network state by recording which channels on each fiber were used to handle primary lightpaths and which channels on each fiber were used for backup lightpaths. We also keep track of which disaster affects which primary lightpath(s). In Phase II, we keep the network state fixed to the state at the end of phase I. We use a set of randomly generated requests to determine the blocking probability (BP). For each request, we use our heuristic algorithm to find out whether a primary lightpath and a backup lightpath may be set up to handle that request. We have reported below the BP under different

scenarios. The A^* heuristic algorithm was developed and experiments were carried out on an Intel Core i7-3537U CPU 2.50 GHz processor using Java JDK with Eclipse KEPLER.

Fig. 4.6 and 4.7 shows the blocking probability (BP) versus different traffic loads for 14-node NSFNET network considering 3 DC locations (at nodes 0,5,9) and 4 DC locations (at nodes 0,5,9,12), respectively. We consider the two disaster categories in these experiments, category I and II. In Fig. 4.6, the results show that the blocking probability increases with higher traffic loads, as expected. Also, the BP values for disasters of category II are higher compered to category I which gives consistent results with the optimal algorithm (ILP). Fig. 4.7 shows the BP obtained by our heuristic using the same parameters of Fig. 4.7 but with 4 DCs instead of 3. Clearly, the blocking probability decreases significantly for the same values of traffic loads. Also, the BP is higher with category II disasters compared to category I.

Fig. 4.8 illustrates the BP for 20-node ARPANET network versus different traffic loads with all other parameter the same as in figures to Fig. 4.6 but the DC locations were at nodes (1,7,18) for 3 DCs. The results follow a similar patter as in Fig. 4.6, as expected. The BP gets higher with higher traffic loads. Also, the BP with category I disasters are less than their values for category II disasters. The results for 4 DCs followed a similar pattern with lower BP and higher number of accommodated requests.

Figs. 4.9, 4.10, and 4.11 shows the average resource utilization for 14-node NSFNET with 3 DCs, 14-node NSFNET with 4 DCs, and 20-node ARPANET with 3 DCs. We measure the resource utilization by the number of wavelength links for the new primary and backup lightpaths established for the new requests. We compare the resource utlization considering category I and category II disasters. Clearly, the resource consumption is slightly higher with category II disasters which

gives an interesting conclusion that, using our proposed approach, considering more disasters will not add significantly to the cost of the solution.

Finally, we show the averge path length obtained by our heuristic algorithm for 14-node NSFNET and 20-node ARPANET networks in Figs. 4.12 and 4.13, respectively. The results are reported for 3 DCs in both networks and show that, with less disasters happen in the network, the lightpats (primary and/or backup) will have a shorter path length.

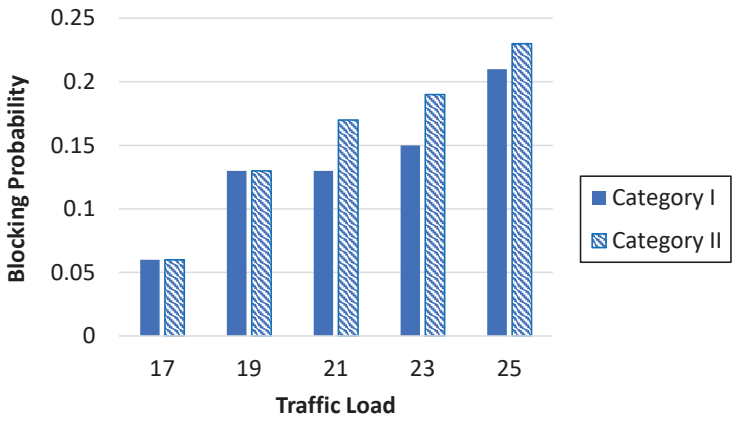


Figure 4.6: Comparison of BP with different traffic loads for 14-node NSFNET network and 3 DCs.

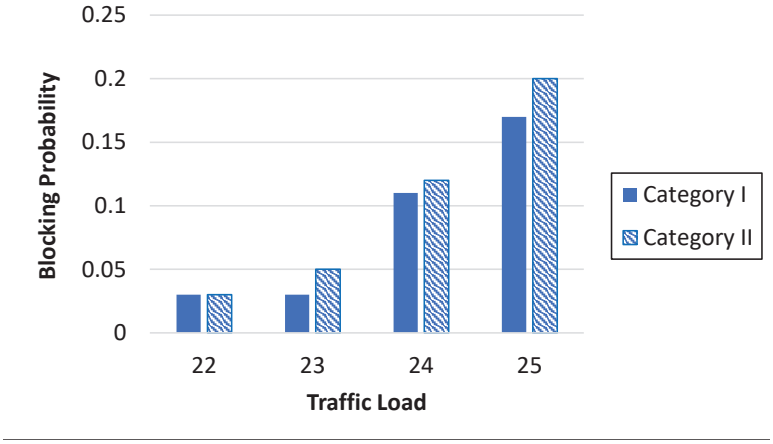


Figure 4.7: Comparison of BP with different traffic loads for 14-node NSFNET network and 4 DCs.

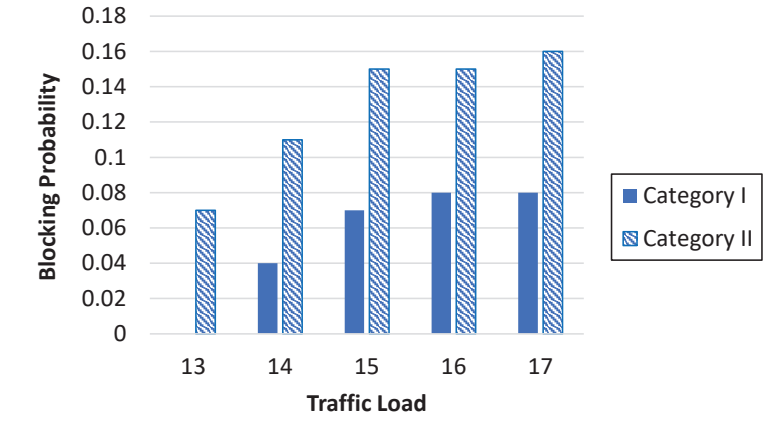


Figure 4.8: Comparison of BP with different traffic loads for 20-node ARPANET network and 3 DCs.

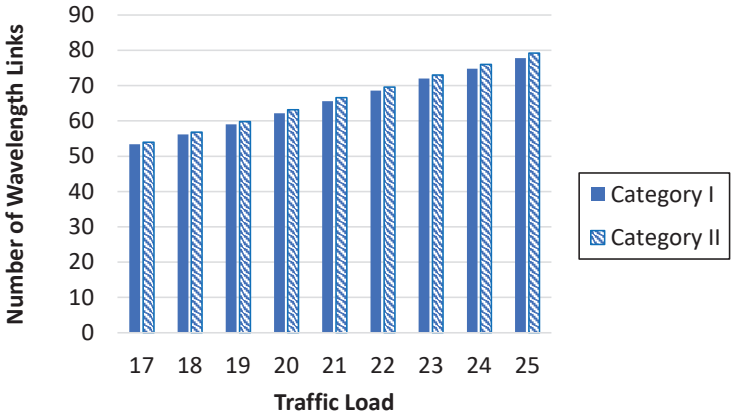


Figure 4.9: Comparison of resource utilization with different traffic loads for 14-node NSFNET network and 3 DCs.

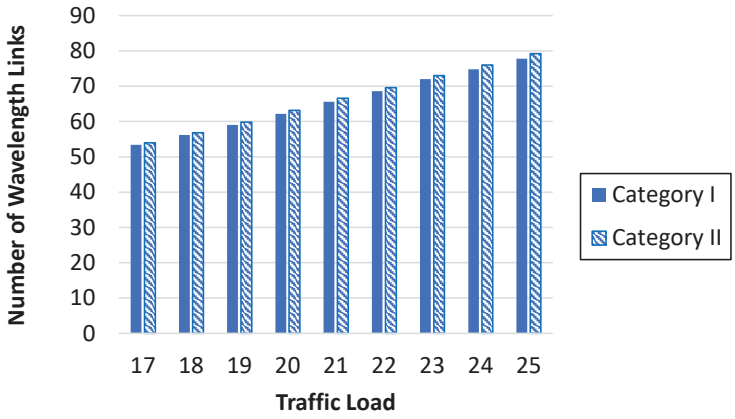


Figure 4.10: Comparison of resource utilization with different traffic loads for 14-node NSFNET network and 4 DCs.

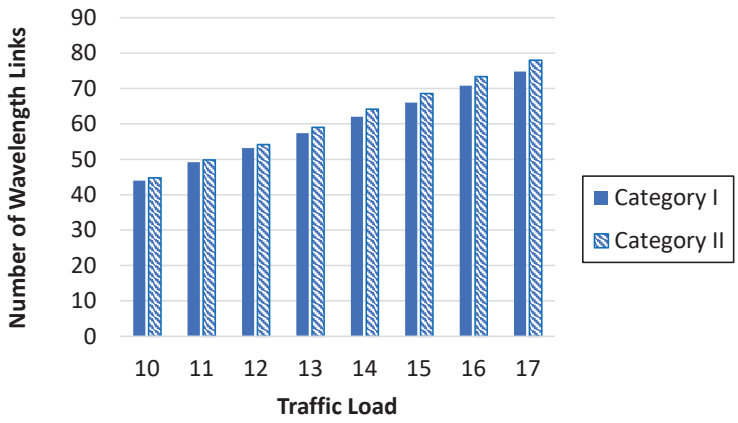


Figure 4.11: Comparison of resource utilization with different traffic loads for 20-node ARPANET network and 3 DCs.

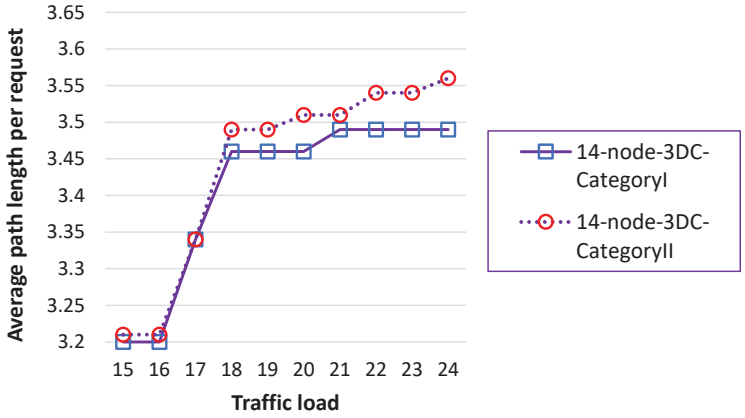


Figure 4.12: Comparison of average path length with different traffic loads for 14-node NSFNET network and 3 DCs.

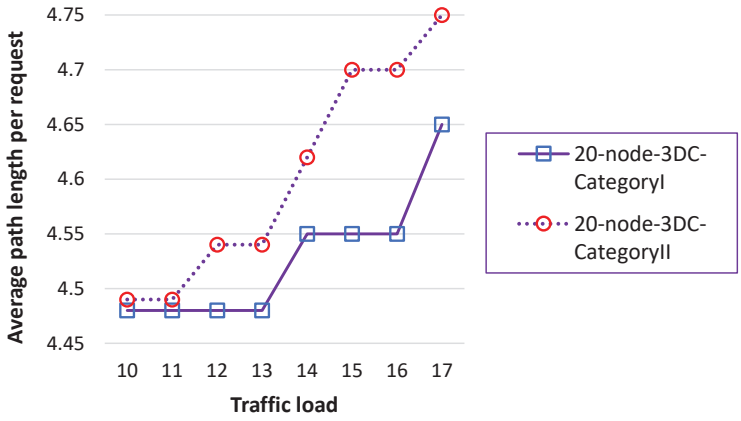


Figure 4.13: Comparison of average path length with different traffic loads for 20-node ARPANET network and 3 DCs.

Chapter 5

Robust Data Center Network Design Based on Space Division Multiplexing

5.1 Introduction

In this chapter, we present our investigations on the design of resilient elastic optical DCNs using SDM technology for dynamic traffic requests. In traditional WDM networks, it is known that dynamic RWA is expected to become more important than static RWA [112–114]. This trend is likely to be even more appropriate in DCNs, in view of the types of ultra high speed communication possible using SDM. As we mentioned earlier in Chapter 4, a robust DCN must store multiple copies of each file in the network, so that at least one copy of each file is guaranteed to be available to handle any request for that file, even after a disaster happens. In the dynamic scenario, the replication strategy must be determined *before* the network is deployed. In this probelm, we obtain the file replication information from the

replication strategy of the disaster-aware RWA in DCN using WDM presented in Chapter 4

An appropriate strategy for handling a request at run-time must take into account the replication strategy determined beforehand. The replication strategy must ensure that, for *all* disaster scenarios $d \in \mathcal{D}$, and for *all* possible communication requests, it is possible to determine a fault-free path to enable communication. If the replication strategy determines that a file f_i needs to have m copies, the strategy must also decide which data centers $\mathcal{S}_i^1, \mathcal{S}_i^2, \ldots, \mathcal{S}_i^m$ should have a copy of file f_i. When there is no disaster affecting the network, spectrum resources must be allocated, if available, on each edge of the network from a site $\mathcal{S}_i^j$, that stores a copy of file f_i, to node t, using a particular modulation format (i.e, 16-QAM, 8-QAM, QPSK, BPSK, ... etc.). The replication strategy must ensure that, for all file f_i, the selected data centers $\mathcal{S}_i^j, 1 \leq j \leq m$ are such that, for any node t in the network

- When the network is fault-free, it is possible to have a viable path from some node $\mathcal{S}_i^j$ to t. A viable path for communication is such that the length of the path is less than the optical reach for BPSK format (which has the longest optical reach). We will call this the *primary path*. The actual modulation format used should be the most efficient (i.e., having the highest packing density [44]) possible for the length of the path for primary communication.

- When any disaster d occurs that disrupts the primary path, it is still possible to have a fault-free viable path for backup communication, from some node $\mathcal{S}_i^k$ to t. We will call this the *backup path*. We note that for all disaster d that disrupts the primary path, it must be possible to use the same backup path for communication to node t.

- The capacities of the data centers may not be exceeded.

If the above conditions are not satisfied, then, for at least one disaster, some node will always be unable to retrieve some file in the network. Our proposed scheme to handle disasters uses the idea of dedicated path protection [10, 110], originally proposed for WDM networks. We have used the term *primary communication* to refer to the scheme for communication in a fault-free network. For all disasters $d \in \mathcal{D}$ that disrupt the primary communication scheme, we must use a *backup communication* scheme. When the network processes a request for communicating a file f_i to node t, the network already has a number of requests in progress. For these requests, currently in progress, the details of the primary as well as the backup communication schemes are known. Our objective is to obtain, if possible, details about the primary and the backup communication to handle the new request to communication file f_i to some node t satisfying the following conditions:

- The primary communication will be from some node $\mathcal{S}_i^j, 1 \leq j \leq m$, to node t.
- The backup communication will be from some node $\mathcal{S}_i^l, 1 \leq l \leq m$. Here $j \neq l$, since a disaster can disrupt the source $\mathcal{S}_i^j$ used in the primary communication. This scheme for backup communication cannot use any of the edges affected by all disaster $d \in \mathcal{D}$ that disrupts the primary communication.
- The length of the path used by the primary (backup) communication will determine the optimum modulation format to be used [44] by the primary (backup) communication.

Our optimal algorithm given below uses an ILP and processes a new request for communicating some file f_i to some t. The scheme determines, if possible, the primary as well as the backup communication scheme. These communication schemes include the path used, the spectrum allotted, the cores used and the recommended

modulation format.

5.2 Optimal RWA for SDM Optical Network under Dynamic Traffic

We will measure the cost of the resources needed to handle the new request by the sum of the spectrum bandwidths needed for the primary and the backup communication. It is convenient to visualize a new *virtual node* s and some new *virtual edges* from s as follows. For each data centre $\mathcal{S}_i^j, 1 \leq j \leq m$, we visualize a single virtual edge from virtual node s to data centre $\mathcal{S}_i^j$ of length 0. In this way we can use the well-known network flow algorithms to determine the schemes for primary and backup communication.

In the description below we have referred to a set G_{ij} of *gaps* on edge $(i, j) \in E$, where E is the set of bidirectional edges in the physical network topology. The following example informally explains how we define gaps. Fig. 5.1 shows a bundle of fibers, representing a link from node i to node j. Selected portions of available spectrum on each fiber in this bundle are already allotted to existing communication. Fig. 5.1 shows a possible allocation of spectrum using the flex-grid fixed-SDM model. For instance, cores 0 and 1 (respectively 2 and 3) are carrying parts of the payload for 3 (respectively 2 and 1) different request for communication. If a new request for communication uses this link $i \rightarrow j$, the spectrum allotted to the new communication must be within the bandwidths shown in Fig. 5.1. We call these permissible bandwidths the "gaps" on edge (i, j). In the situation described in Fig. 5.1, there are 3 gaps, where gap 0 (respectively gap 1 and gap 2) has a starting subcarrier a_{ij}^0 (respectively a_{ij}^1 , a_{ij}^2) and ending subcarrier b_{ij}^0 (respectively b_{ij}^1 and

b^2_{ij}). A new request using this link $i \to j$ must be allotted a bandwidth which lies within one of these 3 gaps.

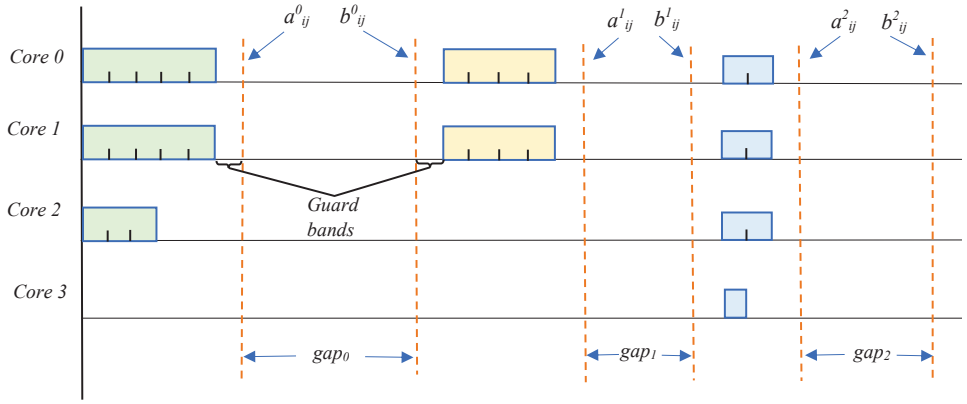


Figure 5.1: Figure illustrating "gaps".

5.2.1 Notation used

$\boldsymbol{N(E)}$**:** set of end nodes (bidirectional edges) in the physical network topology.

$\boldsymbol{E^d}$**:** set of bidirectional edges (i.e., links) in the network that are not disrupted by disaster d.

$\boldsymbol{G_{ij}}$**:** set of all gaps on edge $(i, j) \in E$.

$\boldsymbol{\mathcal{C}}$**:** set of cores per fiber.

$\boldsymbol{s(t)}$**:** source (destination) of the new request for communication. In this problem s is the virtual node discussed above.

$\boldsymbol{\mathcal{B}}$**:** a constant denoting the bandwidth requested, measured by the total number of subcarriers needed for the communication, using BPSK.

$\boldsymbol{k_0}$**:** a constant denoting the packing density for the 16-QAM format[1].

[1]Other modulation formats will be handled similarly.

$\boldsymbol{\eta^P}$**:** number of subcarriers needed for the primary communication.

$\boldsymbol{d_0}$**:** constant denoting optical reach, using 16-QAM format[2].

$\boldsymbol{\mathcal{M}}$**:** a large number.

$\boldsymbol{a_{ij}^g(b_{ij}^g)}$**:** a constant for all gap $g \in G_{ij}$ and edge $(i,j) \in E$ that represents the starting (ending) subcarrier wavelength of the g^{th} spectrum gap of core c on edge (i,j).

$\boldsymbol{\ell_{ij}}$**:** an integer variable denoting the length of the edge $(i,j) \in E$.

$\boldsymbol{\mathcal{F}_0^P}$**:** a binary variable with a value 1 if the primary communication uses 16-QAM format; 0 otherwise.

$\boldsymbol{\mathcal{G}_1^P}$**:** a binary variable with a value 1 if the primary communication *may use* 8-QAM format; 0 otherwise.

$\boldsymbol{\mathcal{G}_2^P}$**:** a binary variable with a value 1 if the primary communication *may use* QPSK format; 0 otherwise.

$\boldsymbol{\mathcal{F}_1^P}$**:** a binary variable with a value 1 if the primary communication uses 8-QAM format; 0 otherwise.

$\boldsymbol{\mathcal{F}_2^P}$**:** a binary variable with a value 1 if the primary communication uses QPSK format; 0 otherwise.

$\boldsymbol{\ell^P}$**:** an integer variable denoting the length of the path used by the primary communication scheme.

$\boldsymbol{w_{ij}^d}$**:** a binary variable for all edge $(i,j) \in E$ where $w_{ij}^d = 1$ if edge (i,j) appears in the path used to handle disaster d; 0 otherwise.

$\boldsymbol{W}$**:** a set of all w_{ij}^d, for all edge $(i,j) \in E$ and disaster $d \in \mathcal{D}$.

$\boldsymbol{x_{ij}(y_{ij})}$**:** a binary variable for all edge $(i,j) \in E$ where $x_{ij} = 1 (y_{ij} = 1)$ if the path used by the primary (backup) communication scheme for the new request uses edge (i,j); 0 otherwise.

$\boldsymbol{x_{ij}^{g}}$**:** a binary variable for all gap $g \in G$ and edge $(i,j) \in E$ where $x_{ij}^{g} = 1$ if gap g of core c on edge (i,j) is used by the primary communication scheme; 0 otherwise.

$\boldsymbol{\theta(\omega)}$**:** an integer variable representing the starting subcarrier number of the new request for the primary (backup) communication scheme.

$\boldsymbol{\phi(\psi)}$**:** an integer variable representing the ending subcarrier number of the new request for the primary (backup) communication scheme.

$\boldsymbol{k}$**:** the number of paths to be generated from s to t.

$\boldsymbol{\mathcal{P}^{st}}$**,** $\boldsymbol{(\mathcal{Q}^{st})}$**:** the set of candidate paths from s to t for the primary (backup) communication.

$\boldsymbol{p(b)}$**:** path for primary (backup) communication.

$\boldsymbol{\mathcal{F}^{P}(\mathcal{F}^{B})}$**:** modulation format for primary (backup) communication.

$\boldsymbol{G}$**:** Spectrum gap information for all edge $(i,j) \in E$.

$\boldsymbol{\mathcal{D}^{p}}$**:** set of disasters that may affect the primary path.

$\boldsymbol{E^{new}}$**:** set of edges that are not affected ny disasters that may affect the primary path.

5.2.2 ILP for an optimal solution

Objective function:

$$minimize \quad (\phi - \theta) + (\psi - \omega) \tag{5.1}$$

Subject to:

1. Flow balance equations must be satisfied by the primary path used for the primary communication (backup path used when disaster d happens, $\forall d \in \mathcal{D}$):

$$\sum_{i:i\to j\in E} x_{ij} - \sum_{i:j\to i\in E} x_{ji} = \begin{cases} 1, \text{if } i = s, \\ -1, \text{if } i = t, \quad \forall i \in N \\ 0, \text{otherwise.} \end{cases} \tag{5.2}$$

$$\sum_{j:(i,j)\in E^d} w_{ij}^d - \sum_{j:(j,i)\in E^d} w_{ji}^d = \begin{cases} q^d & \text{if } i = s, \\ -q^d & \text{if } i = t, \quad \forall i \in N \\ 0 & \text{otherwise.} \end{cases} \tag{5.3}$$

2. Set $q^d = 1$, if disaster d disrupts the primary communication. Otherwise, set $q^d = 0$.

$$q^d \geq x_{ij} \quad \forall (i,j) \in E^d, d \in \mathcal{D} \tag{5.4}$$

$$q^d \leq \sum_{i,j:(i,j)\in E^d} x_{ij} \quad \forall d \in \mathcal{D} \tag{5.5}$$

3. Determine the backup path to be used when *any* disaster happens.

$$y_{ij} \leq (1 - q^d) \cdot \mathcal{M} + w_{ij}^d \quad \forall (i,j) \in E, d \in \mathcal{D} \tag{5.6}$$

$$y_{ij} \geq w_{ij}^d \quad \forall (i,j) \in E, d \in \mathcal{D} \tag{5.7}$$

4. Find the length of the primary path.

$$\ell^P = \sum_{i,j:(i,j)\in E} x_{ij} \cdot \ell_{ij} \tag{5.8}$$

5. Determine whether 16-QAM is the best modulation format to be used for the primary communication[2].

$$\mathcal{M} \cdot \mathcal{F}_0^P \geq (d_0 - \ell^P) \tag{5.9}$$

$$\mathcal{M} \cdot (1 - \mathcal{F}_0^P) \geq (\ell^P - d_0) \tag{5.10}$$

5a. Determine whether 8-QAM *may be* used for the primary communication.

$$\mathcal{M} \cdot \mathcal{G}_1^P \geq (d_1 - \ell^P) \tag{5.11}$$

$$\mathcal{M} \cdot (1 - \mathcal{G}_1^P) \geq (\ell^P - d_1) \tag{5.12}$$

5b. Determine whether 8-QAM *is the best* modulation format to be used for the primary communication.

$$\mathcal{F}_1^P \leq \mathcal{G}_1^P \tag{5.13}$$

$$\mathcal{F}_1^P \leq 1 - \mathcal{F}_0^P \tag{5.14}$$

$$\mathcal{F}_1^P \geq \mathcal{G}_1^P - \mathcal{F}_0^P \tag{5.15}$$

5c. Determine whether QPSK *may be* used for the primary communication.

$$\mathcal{M} \cdot \mathcal{G}_2^P \geq (d_2 - \ell^P) \tag{5.16}$$

$$\mathcal{M} \cdot (1 - \mathcal{G}_2^P) \geq (\ell^P - d_2) \tag{5.17}$$

5d. Determine whether QPSK *is the best* modulation format to be used for the primary communication.

$$\mathcal{F}_2^P \leq \mathcal{G}_2^P \tag{5.18}$$

$$\mathcal{F}_2^P \leq 1 - \mathcal{F}_0^P \tag{5.19}$$

$$\mathcal{F}_2^P \leq 1 - \mathcal{F}_1^P \tag{5.20}$$

$$\mathcal{F}_2^P \geq \mathcal{G}_2^P - \mathcal{F}_0^P - \mathcal{F}_1^P \tag{5.21}$$

6. Find the number of subcarriers needed for the primary communication.

$$\eta^P \geq \mathcal{F}_0^P \cdot \mathcal{B}/k_0 \tag{5.22}$$

$$\eta^P \leq \mathcal{M}.(1 - \mathcal{F}_0^P) + \mathcal{B}/k_0 \tag{5.23}$$

7. Exactly one spectrum gap of one core must be used on each fiber on the path used for the primary communication of the new request:

$$\sum_{g \in G_{ij}} x_{ij}^g = x_{ij} \quad \forall (i,j) \in E \tag{5.24}$$

8. The starting subcarrier of the primary communication for the new request must be greater than or equal to the starting subcarrier of the g^{th} gap of core c on edge (i,j)

$$\theta \geq a_{ij}^g \cdot x_{ij}^g \quad \forall (i,j) \in E, g \in G_{ij} \tag{5.25}$$

9. The ending subcarrier of the primary communication for the new request must be less than or equal to the ending subcarrier of the g^{th} gap of core c on edge (i,j)

$$\phi \leq b_{ij}^g + M \cdot (1 - x_{ij}^g) \quad \forall (i,j) \in E, g \in G_{ij} \tag{5.26}$$

10. The total number of subcarriers on all gaps and cores used by the primary communication must be greater than or equal to the required bandwidth.

$$(\phi - \theta + 1) \geq \eta^P / |\mathcal{C}| \tag{5.27}$$

Due to lack of space, we have omitted constraints which are similar to those outlined above. Constraints very similar to (5.9) - (5.23) may be used to determine whether the modulation format 8-QAM, QPSK or BPSK is the best modulation format for the primary communication.

Constraints similar to (5.8) - (5.27) may be used to determine the modulation format, the spectrum and the cores to be used to determine the scheme for the backup communication.

5.2.3 Explanations for the constraints used in the ILP

We note that $\phi-\theta+1$ ($\psi-\omega+1$) denotes the spectrum used for the primary (backup) communication. The objective function minimizes the sum of the spectrums used for the primary and backup communication.

If $q^d = 0$, constraint (5.3) ensures that $w_{ij}^d = 0$, so that constraints (5.6) and (5.7) become $y_{ij} \leq \mathcal{M}$ and $y_{ij} \geq 0$, both trivial constraints. If $q^d = 1$, constraint (5.6) and (5.7) become $y_{ij} \leq w_{ij}^d$ and $y_{ij} \geq w_{ij}^d$, so that $y_{ij} = w_{ij}^d$. In other words, the path for the backup communication is defined by y_{ij}, which avoids all disasters that affect the path for the primary communication. Constraints (5.9) and (5.10) ensure that $\mathcal{F}_0^P = 1$, if the length of the path for the primary communication does not exceed the optical reach d_0 for 16-QAM; otherwise $\mathcal{F}_0^P = 0$. If $\mathcal{F}_0^P = 1$, constraints (5.22) and (5.23) ensure that $\eta^P = \mathcal{B}/k_0$; otherwise, constraints (5.22) and (5.23) become trivial. Thus, if 16-QAM can be used, the number of subcarriers η^P is determined by the packing density for 16-QAM. Similar constraints (not included above) check if some other modulation format(e.g., 8-QAM, QPSK, BPSK) is appropriate for the length of the primary path. Explanations for the remaining constraints are straight-forward. This optimal algorithm is not usable for networks of practical size and available bandwidth. To address this, we have given below a relaxed version of the above ILP. Explanations for constraints (5.11) and (5.12) are like constraints (5.9) and (5.10) and ensure that $\mathcal{G}_1^P = 1$, if the length of the path for the primary communication does not exceed the optical reach d_1 for 8-QAM; otherwise $\mathcal{G}_1^P = 0$. In other words, if $\mathcal{G}_1^P = 1$, 8-QAM *may be used* for the primary communication. If the length of the path for the primary communication does not exceed the optical reach d_0 for 16-QAM, it clearly does not exceed the optical reach d_1 for 8-QAM. Therefore, if $\mathcal{F}_0^P = 1$, $\mathcal{G}_1^P$ will always be 1. Our objective is to make sure that we should use 16-QAM, if possible; otherwise, we should use 8-QAM, if possible. In

other words, $\mathcal{F}_1^P = 1$ only when $\mathcal{F}_0^P = 0$ and $\mathcal{G}_1^P = 1$; otherwise it is 0. It may be readily verified that constraints (5.13), (5.20) and (5.15) ensures that this condition. Explanations for constraints (5.16) and (5.17) are like constraints (5.11) and (5.12) and ensure that $\mathcal{G}_2^P = 1$, if the length of the path for the primary communication does not exceed the optical reach d_2 for QPSK; otherwise $\mathcal{G}_2^P = 0$. To determine $\mathcal{F}_2^P$ we use a technique similar to that for $\mathcal{F}_1^P$. Here we need to ensure that $\mathcal{F}_2^P = 1$ *only when* $\mathcal{G}_2^P = 1$ (i.e., QPSK may be used) *and* $\mathcal{F}_1^P = 0$ (i.e., 8-QAM cannot be used) *and* $\mathcal{F}_0^P = 1$ (i.e., 16-QAM cannot be used). It may be verified that constraints (5.18) – (5.21) ensures that this condition is satisfied. The equations for BPSK is very similar.

5.3 A heuristic for RWA using SDM under Dynamic Traffic

In this heuristic we have used the following relaxations to the approach used in the ILP described above:

- Instead of considering all possible paths from the virtual node s to the requesting node t, we have restricted our search to a selected number of pre-computed paths[2].
- We have determined the schemes for the primary and the backup communication sequentially, in two separate steps, rather than finding them simultaneously.

The relaxations used in our heuristic mean that the solutions may not be optimal but the heuristic is useful, since it generates near-optimal solutions for practical-sized

[2]We have used 3 precomputed paths from each data centers to each destination node.

networks in reasonable time. In describing the heuristic, we have used the notation described in Section 5.2.1. In addition we have used the following symbols:

- k denotes the number of pre-computed paths from s to t.
- $\mathcal{P}^{st}$ ($\mathcal{Q}^{st}$) denotes the set of k paths from s to t when there is no disaster (when a disaster $d \in \mathcal{D}$ disrupts the path selected for primary communication).
- p (b) denotes the path selected from $\mathcal{P}^{st}$ ($\mathcal{Q}^{st}$) to handle the scheme for primary (backup) communication.
- $\mathcal{F}^P$ denotes the set $\{\mathcal{F}_0^P, \mathcal{F}_1^P, \mathcal{F}_2^P, \mathcal{F}_3^P\}$. The heuristic ensures that exactly one element of $\mathcal{F}^P = 1$ and all the other values are 0. This allows us to determine the appropriate modulation format for the primary communication scheme.
- $\mathcal{F}^B$ denotes the set $\{\mathcal{F}_0^B, \mathcal{F}_1^B, \mathcal{F}_2^B, \mathcal{F}_3^B\}$. This is used just like $\mathcal{F}^P$, for the backup communication scheme.
- $\mathcal{D}^p$ denotes the set of all disasters in $\mathcal{D}$ that affect the path p used by the primary communication.
- G denotes the set of all gaps G_{ij} for all $(i, j) \in E$.
- E^{new} denotes the set of edges of the network that are not affected by any disaster in $\mathcal{D}^p$.

In the heuristic, we have used the following functions:

1. *findpaths*(N, E, s, t, k) returns k shortest paths from s to t, if they exist, where the length of each fiber is taken as 1. We used $k = 3$ in our experiments. In other words, this function determines the best 3 paths, having the fewest number of links.

2. $RSA(\mathcal{P}^{st}, G, \mathcal{B})$ (RSA$(\mathcal{Q}^{st}, G, \mathcal{B})$ carries out RSA for the primary (backup) communication scheme by selecting a path $p \in \mathcal{P}^{st}$, so that a total bandwidth of $\mathcal{B}$ may be handled using the most efficient modulation format $\mathcal{F}^P$ ($\mathcal{F}^B$). The function also updates the gap information G with the spectrum used by primary communication, using ILP1 - an ILP informally described below.

3. $disastersAffectingPrimaryPath(p, \mathcal{D})$ returns $\mathcal{D}^p$. Disasters affecting the destination node t will not be included in $\mathcal{D}^p$, since communication to t is possible only if t itself is not affected by a disaster.

4. $removeDisruptedEdges(d, E^{new})$ returns the set of edges in E^{new} that survive disaster $d \in \mathcal{D}^p$.

A relaxed version of our heuristic is given below (Algorithm 5.1), where we have assumed that the RSA for the primary and the backup communication are always successful.

Pseudocode for Disaster-aware Heuristic Algorithm for DCNs Using SDM

1: $\mathcal{P}^{st} \leftarrow findpaths(N, E, s, t, k)$
2: $(p, \mathcal{F}^P, G) \leftarrow RSA(\mathcal{P}^{st}, G, \mathcal{B})$
3: $\mathcal{D}^p \leftarrow disastersAffectingPrimaryPath(p, \mathcal{D})$
4: $E^{new} \leftarrow E$
5: **for all** $(d \in \mathcal{D}^p)$ **do**
6: $\quad E^{new} \leftarrow removeDisruptedEdges(d, E^{new})$
7: **end for**
8: $\mathcal{Q}^{st} \leftarrow findpaths(N, E^{new}, s, t, k)$
9: $(b, \mathcal{F}^B, G) \leftarrow RSA(\mathcal{Q}^{st}, G, \mathcal{B})$

To determine the scheme for primary communication we use the function $RSA(\mathcal{P}^{st}, G, \mathcal{B})$ which includes invoking the Integer Linear Formulation ILP1, a simplified version of the ILP described in Section 5.2.1. In ILP1, we find the scheme for primary communication by i) selecting the "best" path $s \rightarrow \ldots \rightarrow t$ from the set of pre-computed paths $\mathcal{P}^{st}$ and ii) carrying out RSA on the selected path. To do so, we

- Eliminated, from the ILP described above, constraints 5.3, 5.6, 5.7, which deal with the scheme for backup communication.
- Replaced flow balance equation 5.2 by a constraint that states that exactly one route from the pre-computed routes $\mathcal{P}^{st}$ ($\mathcal{Q}^{st}$) will be selected. The values of x_{ij} (y_{ij}), for all $(i,j) \in E$, may be computed from this selected route.

The ILP used in the heuristic is included as Appendix A of this thesis. To determine the scheme for backup communication, we use a similar process with the function $RSA(\mathcal{Q}^{st}, G, \mathcal{B})$. The remaining functions are trivial.

5.4 Simulation results

In this section we present our experimental results using the heuristic outlined in Section 5.3. In our approach we have to specify the disasters that have to be considered. The disaster scenario we considered in our experiments is the case when a disaster can affect any one node in the network along with edges associated with that node. When a node, say node i, is affected by a disaster, all edges $i \rightarrow j$ ($j \rightarrow i$) from (to) node i also fails. In our simulations we consider only this type of disasters because they are more "severe" compared to the failure of single edges (for instance due to a fiber cut). If the network can handle the failure of node i, the same strategy can also handle the failure of any one or more edges from/to node i. This also means that, for our simulations, in the wide area networks we are considering, the nodes are sufficiently far away so that 2 nodes cannot be affected by the same disaster. It is important to note that these are only simplifying assumptions in our simulations. The formulation given above can handle any generalization of the disaster scenarios such as two nodes failing or a complex SRLG type of situation.

We consider the well-known 14-node NSFNET network for our simulations. In

series I (II) of our experiments, the number of cores per fiber is 4 (7). We consider two situations for the number of frequency slots (slices) per core - 50 and 60.

In series I, we consider three scenarios where the number of DCs are 2, 3, and 4. When the number of DCs is 2 (respectively 3 and 4) the locations of the DCs are (4, 12), (respectively (0, 4, 12), and (0, 4, 10, 13)). Our results represent the average of 5 simulation runs. The set of lightpath requests is generated, based on a Poisson-distribution [104], with randomly selected files and destination nodes. The traffic load is varied from 25 to 200 Erlang.

Fig. 5.2 shows the results obtained by our proposed approach for 3 DCs and 4 cores per fiber, we compare the blocking probability (BP) in the cases of 50 and 60 frequency slots per core. As expected, the BP decreases when the number of slots are increased. Fig. 5.3 is for 4 DC's and the results show that the blocking probability decreases significantly when we increase the number of DCs.

Fig. 5.4 shows the BP if there is only 2 DCs in the network. Other parameters such as the number of cores per fiber and number of frequency slots per core are the same as in Figs. 5.2 and 5.3. The trends in this case are very similar to the cases of 3 and 4 data centers given above.

In series II, we use the same DC and disasters scenarios but assume 7 cores per fiber links, instead of 4 cores we use in series I. Fig. 5.5 illustrates the performance of our approach when the number of cores is increased to 7 cores per fiber and 3 DCs. As expected, the BP decreased significantly with 7 cores compared to 4 cores and the approach is able to accommodate requests up to 200 Erlang with low BP.

We also report the resource usage, measured by the number of frequency slots allocated per request obtained by our proposed approach. Fig. 5.6 shows how the resource utilization, measured by the number of frequency slots allocated per request, for 14-node NSFNET network increases as the number of frequency slots

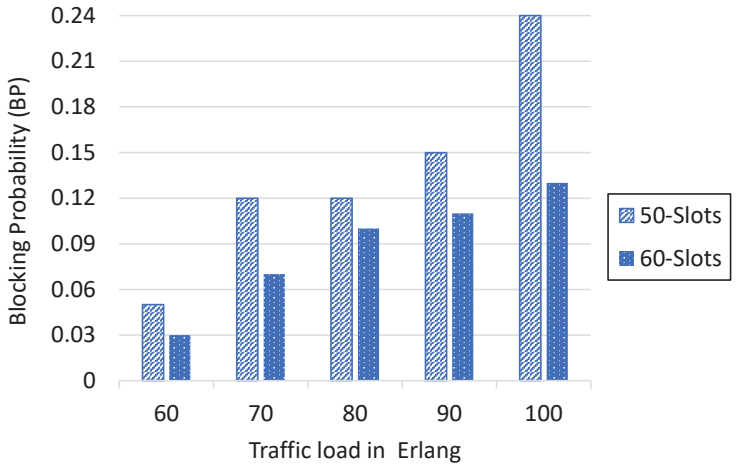


Figure 5.2: Blocking probability obtained by proposed approach for 14-node NSF network with 3 DCs and 4 cores per fiber link.

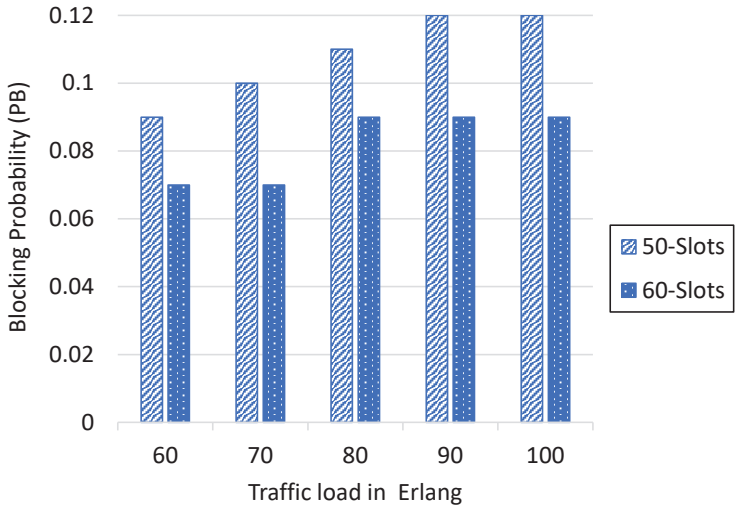


Figure 5.3: Blocking probability obtained by proposed approach for 14-node NSF network with 4 DCs and 4 cores per fiber link.

per core is increased. This is expected since the blocking probability is reduced when more resources are available (Fig. 5.2). This means more requests are allotted spectrum instead of being blocked and more frequency slots are allotted. We carried

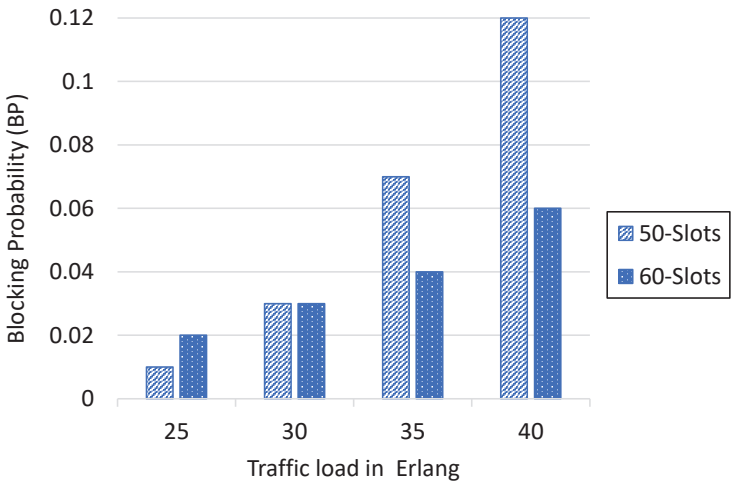


Figure 5.4: Blocking probability obtained by proposed approach for 14-node NSF network with 2 DCs and 4 cores per fiber link.

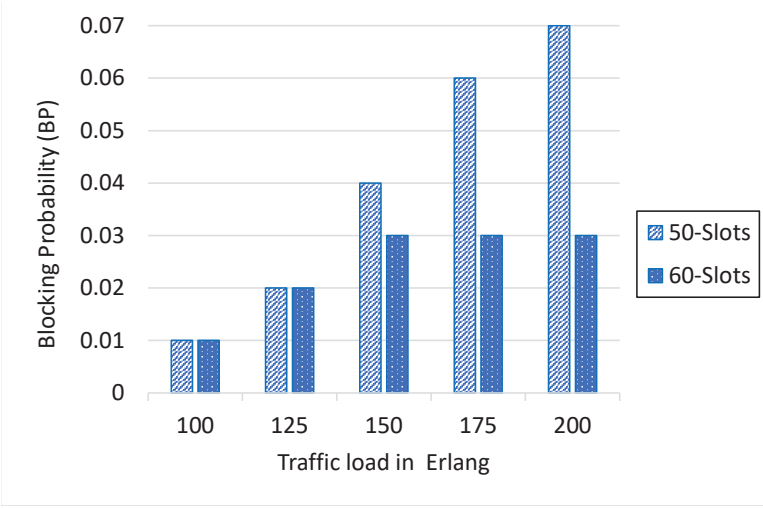


Figure 5.5: Blocking probability obtained by proposed approach for 14-node NSFNET network with 3 DCs and 7 cores per fiber link.

out more experiments using 2 and 4 DCs as shown below in Figs. 5.7 and 5.8. The trends are very similar to those of 5.6.

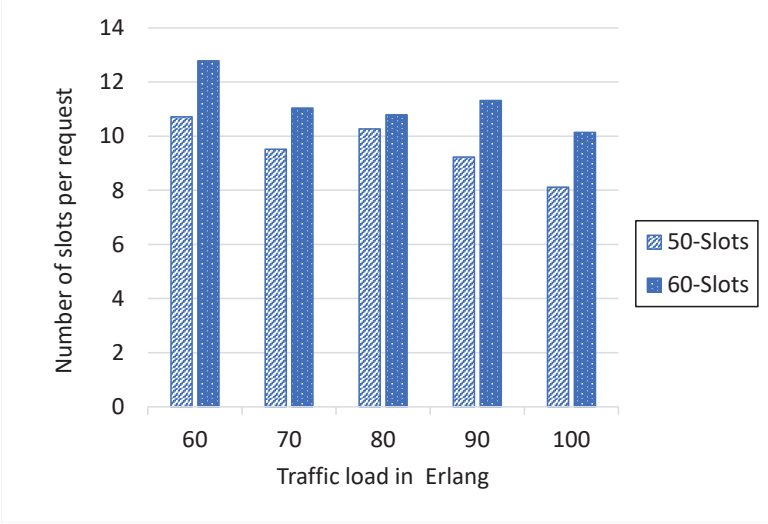


Figure 5.6: Resource utilization obtained by proposed approach for 14-node NSFNET network with 3 DCs and 4 cores per fiber link.

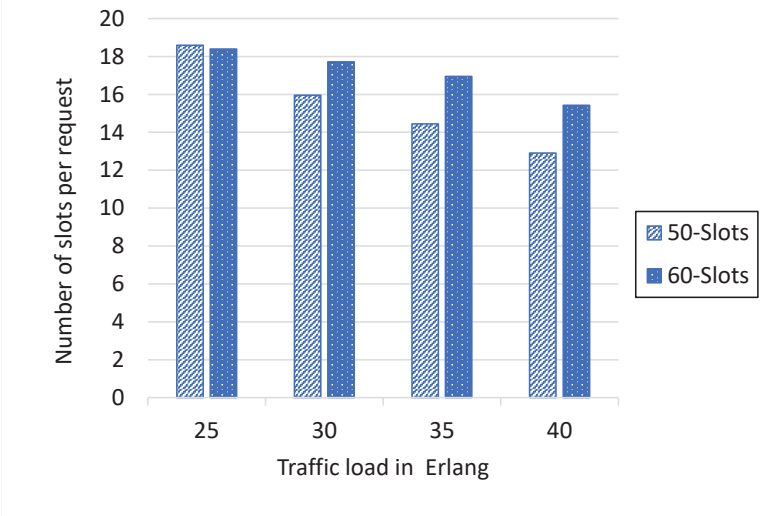


Figure 5.7: Resource utilization obtained by proposed approach for 14-node NSFNET network with 2 DCs and 4 cores per fiber link.

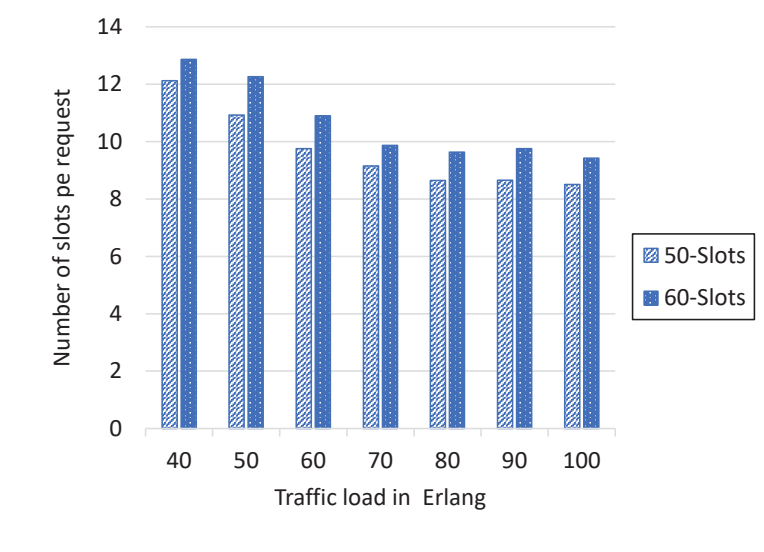


Figure 5.8: Resource utilization obtained by proposed approach for 14-node NSFNET network with 4 DCs and 4 cores per fiber link.

Chapter 6

Conclusions and Future Works

6.1 Conclusions

In this Ph.D. dissertation, we have presented novel algorithms to obtain optimal solutions for different design problems in wide area optical networks.

We have reported our works on three major aspects of optimal design of WDM/SDM optical network. These are:

- Optimal attack-aware resource allocation in WDM optical networks,
- Optimal disaster-aware lightpath allocation with path protection in WDM networks, and
- Optimal resilient spectral-spatial resource allocation with protection in SDM networks.

For optimal security-aware problem, we consider transparent optical networks with dynamic traffic scenario. We present a new ILP formulation as well as an efficient heuristic (SA-DRWA) for minimizing both the in-band and out-of-band crosstalk jamming attacks. The proposed approaches are compared with the tra-

ditional security unaware algorithms for RWA, and have been tested with various network topologies and traffic loads. Simulation results demonstrate that our proposed security-aware approaches were able to limit the vulnerability of lightpaths, by reducing the combined attack radius (AR), with very little overhead in terms of resource consumption and blocking probability.

For optimal disaster-aware network design, we consider WDM DC networks and dynamic traffic. We are given a list of potential disasters, where each disaster affects a specified set of nodes/links in the network. Since a disaster can occur anywhere in the network, including at DC nodes, we assume an appropriate replication strategy has been implemented, so that the required content is available at multiple nodes. We have presented an optimal ILP formulation that finds a suitable primary path and a backup path such that the required content can be delivered to the destination node under all possible disaster scenarios. The RWA implemented by our ILP satisfies the wavelength continuity constraint and also ensures that the length of the selected routes (both primary and backup) are always less than the optical reach. It is interesting to note that our simulations show that, when we consider all possible disaster scenarios, the resources needed are only slightly more, compared to the case when we consider disasters at DC nodes only. So, considering additional disasters does not add significantly to the cost of the solution. The proposed ILP formulation provides optimal solutions that can be used as a benchmark, for evaluating fast, heuristic algorithms that we also presented in chapter 4 section 4.3.

Finally, for optimal resilient SDM network design, we consider elastic optical networks based on SDM technology to handle dynamic requests for communication that can guarantee communication when a disaster affects a part of the network. In our approach, each file stored in a DCN must have multiple copies. In such a system the traditional notion of path protection had to be modified to take account

of the possibility of the failure of the DC storing the file to be communicated. The work is interesting because this is the first approach to develop robust data communication schemes for DC using SDM networks. The protection scheme used is different from standard protection schemes. We have considered the flexgrid-fixed SDM model to create the SSChs for allocating resources to requests. This model is already technologically viable. We evaluate our proposed approached by varying relevant parameters and report the blocking probability for the 14-node NSFNET network. Our results indicate that the BP can be reduced by increasing i) number of frequency slots per core, ii) number of cores per fiber, and iii) number of DC nodes in the network.

6.2 Future Works

One possible enhancement to the attack-aware problem for dynamic traffic is to incorporate protection. This approach can be developed using either DPP or SPP. The strategy must ensure that the primary and backup lightpaths to be established for the new request are not simultaneously within the reach of any potential attacking signal that is already existing in the network. By deploying SPP, the approach can achieve resource savings in the network by allowing the backup lightpath of the new communication to share resources with other existing backup lightpaths.

The design of disaster-survivable DCN has become a major challenge. We proposed an optimal algorithm and heuristic to solve this problem under dynamic traffic scenario. One possible future work direction is to use scheduled traffic which is suitable for periodic applications. The challenge is that if the problem is formulated as an ILP model, it may very well become intractable for large networks. To handle this issue, an efficient heuristic can be developed that will generate near-optimal results in reasonable time.

For survivable DCN design using SDM, an interesting direction to our future work is probably using the flex-grid flex model which provides the best flexility among other models in terms of allocating spectral-spacial resources. Another improvement could be using SPP technique instead of DPP as this will lead to significant resource savings.

Appendix A

1. ILP used in used in Section 5.3

The symbols used in the ILP in addition to those described in Section 5.2.1.

R: a set of pre-computed paths between each source-destination pair, we assume $R = 3$.

$\alpha_{ij}^{sd,r}$: a constant for all source-destination $s, d \in N$, pre-computed route $r \in R$ and edge $(i, j) \in E$ where $\alpha_{ij}^{sd,r} = 1$ if and only if the r^{th} route between source s and destination d uses edge (i, j).

p_r: a binary variable for all pre-computed paths $r \in R$ where $p_r = 1$ if the r^{th} route is used by the new request.

m_r: a constant for all pre-computed paths $r \in R$ denoting the packing density possible for the modulation format corresponding to the length of the r^{th} pre-computed route.

Objective function:

$$minimize \quad \phi - \theta + 1 \tag{1}$$

Subject to:

1. Ensure that only one path is chosen among the $|R|$ pre-computed paths for the new request.

$$\sum_{r \in R} p_r = 1 \tag{2}$$

2. x_{ij} will be 1 if the new request uses the r^{th} route and edge (i, j) is part of that r^{th} route.

$$x_{ij} = \sum_{r \in R} p_r \cdot \alpha_{ij}^{sd,r} \quad \forall s, d \in N, i, j \in E \tag{3}$$

3. Exactly 1 gap on link $(i, j) \in E$ must be used if and only if x_{ij} is 1.

$$\sum_{g \in G_{ij}} x_{ij}^{g} = x_{ij} \quad \forall i, j \in E \tag{4}$$

4. The starting subcarrier of the new request must be greater than or equal to the starting subcarrier of the g^{th} gap on edge (i, j).

$$\theta \geq a_{ij}^{g} \cdot x_{ij}^{g} \quad \forall i, j \in E, g \in G_{ij} \tag{5}$$

5. The ending subcarrier of the new request must be less than or equal to the ending subcarrier of the g^{th} gap on edge (i, j).

$$\phi \leq b_{ij}^{g} + \mathcal{M} \cdot (1 - x_{ij}^{g}) \quad \forall i, j \in E, g \in G_{ij} \tag{6}$$

6. The total number of subcarriers must be greater than or equal to the required bandwidth per core for the packing density appropriate for the r^{th} selected for this communication.

$$(\phi - \theta + 1) \geq \mathcal{B}/[|\mathcal{C}| \cdot \sum_{r \in R} (p_r \cdot m_r)] \tag{7}$$

Bibliography

[1] Bijoy Chand Chatterjee, Nityananda Sarma, Partha Pratim Sahu, and Eiji Oki. Introduction to optical network. In *Routing and Wavelength Assignment for WDM-based Optical Networks*, pages 1–16. Springer, 2017.

[2] Rajiv Ramaswami, Kumar Sivarajan, and Galen Sasaki. *Optical networks: a practical perspective*. Morgan Kaufmann, 2009.

[3] Jane M Simmons. *Optical network design and planning*. Springer, 2014.

[4] Giancarlo De Marchis and Roberto Sabella. *Optical Networks: Design and Modelling/IFIP TC6 Second International Working Conference on Optical Network Design and Modelling (ONDM98) February 9-11, 1998 Rome, Italy*, volume 19. Springer, 2013.

[5] Ivan Kaminow, Tingye Li, and Alan E Willner. *Optical fiber telecommunications VB: systems and networks*. Elsevier, 2010.

[6] C Siva Ram Murthy and Mohan Gurusamy. *WDM optical networks: concepts, design, and algorithms*. Prentice Hall, 2002.

[7] Amitabha Banerjee, Youngil Park, Frederick Clarke, Huan Song, Sunhee Yang, Glen Kramer, Kwangjoon Kim, and Biswanath Mukherjee. Wavelength-division-multiplexed passive optical network (wdm-pon) technologies for

broadband access: a review. *Journal of optical networking*, 4(11):737–758, 2005.

[8] David Schenk and Peter M Krummrich. A novel approach to reduce the impact of physical layer restrictions in dynamically switched transparent optical networks. *Journal of Lightwave Technology*, 34(9):2304–2310, 2016.

[9] Biswanath Mukherjee. *Optical WDM networks*. Springer Science & Business Media, 2006.

[10] Subir Bandyopadhyay. *Dissemination of Information in Optical Networks:: From Technology to Algorithms*. Springer Science & Business Media, 2007.

[11] Hui Zang, Jason P Jue, Biswanath Mukherjee, et al. A review of routing and wavelength assignment approaches for wavelength-routed optical wdm networks. *Optical networks magazine*, 1(1):47–60, 2000.

[12] Bijoy Chand Chatterjee, Nityananda Sarma, Partha Pratim Sahu, and Eiji Oki. Performance analysis of major conventional routing and wavelength assignment approaches. In *Routing and Wavelength Assignment for WDM-based Optical Networks*, pages 35–43. Springer, 2017.

[13] Liang Zhang and Zuqing Zhu. Spectrum-efficient anycast in elastic optical inter-datacenter networks. *Optical Switching and Networking*, 14:250–259, 2014.

[14] Andrew Chralyvy. Plenary paper: The coming capacity crunch. In *Optical Communication, 2009. ECOC'09. 35th European Conference on*, pages 1–1. IEEE, 2009.

[15] Peter J Winzer. Optical networking beyond wdm. *IEEE Photonics Journal*, 4(2):647–651, 2012.

[16] Peter J Winzer. Scaling optical fiber networks: Challenges and solutions. *Optics and Photonics News*, 26(3):28–35, 2015.

[17] Nina Skorin-Kapov, Marija Furdek, Szilard Zsigmond, and Lena Wosinska. Physical-layer security in evolving optical networks. *IEEE Communications Magazine*, 54(8):110–117, 2016.

[18] Marija Furdek. Physical-layer attacks in optical wdm networks and attack-aware network planning. *European Journal of Operational Research*, 178(2):1160–1167, 2011.

[19] Marija Furdek, Nina Skorin-Kapov, Szilard Zsigmond, and Lena Wosinska. Vulnerabilities and security issues in optical networks. In *Transparent Optical Networks (ICTON), 2014 16th International Conference on*, pages 1–4. IEEE, 2014.

[20] Nina Skorin-Kapov, Marija Furdek, Ramon Aparicio Pardo, and Pablo Pavón Mariño. Wavelength assignment for reducing in-band crosstalk attack propagation in optical networks: Ilp formulations and heuristic algorithms. *European journal of operational research*, 222(3):418–429, 2012.

[21] Nina Skorin-Kapov, Jiajia Chen, and Lena Wosinska. A new approach to optical networks security: Attack-aware routing and wavelength assignment. *IEEE/ACM Transactions on Networking (TON)*, 18(3):750–760, 2010.

[22] M Farhan Habib, Massimo Tornatore, Ferhat Dikbiyik, and Biswanath Mukherjee. Disaster survivability in optical communication networks. *Computer Communications*, 36(6):630–644, 2013.

[23] M Farhan Habib, Massimo Tornatore, Marc De Leenheer, Ferhat Dikbiyik, and Biswanath Mukherjee. A disaster-resilient multi-content optical datacenter

network architecture. In *Transparent Optical Networks (ICTON), 2011 13th International Conference on*, pages 1–4. IEEE, 2011.

[24] Sifat Ferdousi, Massimo Tornatore, M Farhan Habib, and Biswanath Mukherjee. Rapid data evacuation for large-scale disasters in optical cloud networks. *Journal of Optical Communications and Networking*, 7(12):B163–B172, 2015.

[25] Biswanath Mukherjee, M Habib, and Ferhat Dikbiyik. Network adaptability from disaster disruptions and cascading failures. *IEEE Communications Magazine*, 52(5):230–238, 2014.

[26] Carlos Colman Meixner, Ferhat Dikbiyik, Massimo Tornatore, Chen-Nee Chuah, and Biswanath Mukherjee. Disaster-resilient virtual-network mapping and adaptation in optical networks. In *Optical Network Design and Modeling (ONDM), 2013 17th International Conference on*, pages 107–112. IEEE, 2013.

[27] Pankaj K Agarwal, Alon Efrat, Shashidhara K Ganjugunte, David Hay, Swaminathan Sankararaman, and Gil Zussman. The resilience of wdm networks to probabilistic geographical failures. *IEEE/ACM Transactions on Networking (TON)*, 21(5):1525–1538, 2013.

[28] Dimitrios Klonidis, Filippo Cugini, Ori Gerstel, Masahiko Jinno, Victor Lopez, Eleni Palkopoulou, Motoyoshi Sekiya, Domenico Siracusa, Gilles Thouénon, and Christophe Betoule. Spectrally and spatially flexible optical network planning and operations. *IEEE Communications Magazine*, 53(2):69–78, 2015.

[29] Ajmal Muhammad, Georgios Zervas, Dimitra Simeonidou, and Robert Forchheimer. Routing, spectrum and core allocation in flexgrid sdm networks with multi-core fibers. In *Optical Network Design and Modeling, 2014 International Conference on*, pages 192–197. IEEE, 2014.

[30] Krzysztof Walkowiak, Piotr Lechowicz, Mirosław Klinkowski, and Arunabha Sen. Ilp modeling of flexgrid sdm optical networks. In *Telecommunications Network Strategy and Planning Symposium (Networks), 2016 17th International*, pages 121–126. IEEE, 2016.

[31] Byrav Ramamurthy, Helena Feng, Debasish Datta, Jonathan P Heritage, and Biswanath Mukherjee. Transparent vs. opaque vs. translucent wavelength-routed optical networks. In *Optical Fiber Communication Conference*, page TuF2. Optical Society of America, 1999.

[32] Samir Chatterjee and Suzanne Pawlowski. All-optical networks. *Communications of the ACM*, 42(6):74–83, 1999.

[33] R Rejeb, I Pavlosoglou, MS Leeson, and RJ Green. Securing all-optical networks. In *Transparent Optical Networks, 2003. Proceedings of 2003 5th International Conference on*, volume 1, pages 87–90. IEEE, 2003.

[34] Krishna M Sivalingam and Suresh Subramaniam. *Optical WDM networks: Principles and practice*, volume 554. Springer Science & Business Media, 2000.

[35] Ying Chen. Resource allocation for periodic traffic demands in wdm networks. 2013.

[36] Thomas G Robertazzi. Optical networks for telecommunications. In *Introduction to Computer Networking*, pages 67–79. Springer, 2017.

[37] Imrich Chlamtac, Aura Ganz, and Gadi Karmi. Lightpath communications: An approach to high bandwidth optical wan's. *IEEE transactions on communications*, 40(7):1171–1182, 1992.

[38] Siamak Azodolmolky, Mirosław Klinkowski, Eva Marin, Davide Careglio, Josep Solé Pareta, and Ioannis Tomkos. A survey on physical layer impairments aware routing and wavelength assignment algorithms in optical networks. *Computer Networks*, 53(7):926–944, 2009.

[39] Siamak Azodolmolky, Marianna Angelou, Ioannis Tomkos, Tania Panayiotou, Georgios Ellinas, et al. Impairment-aware optical networking: A survey. In *WDM Systems and Networks*, pages 443–479. Springer, 2012.

[40] Ori Gerstel, Masahiko Jinno, Andrew Lord, and SJ Ben Yoo. Elastic optical networking: A new dawn for the optical layer? *IEEE Communications Magazine*, 50(2), 2012.

[41] Domenico Siracusa, Federico Pederzolli, Dimitrios Klonidisz, Vıctor Lopezy, and Elio Salvadori. Resource allocation policies in sdm optical networks. In *Optical Network Design and Modeling (ONDM), 2015 International Conference on*, pages 168–173. IEEE, 2015.

[42] D Siracusa, F Pederzolli, PS Khodashenas, JM Rivas-Moscoso, D Klonidis, E Salvadori, and I Tomkos. Spectral vs. spatial super-channel allocation in sdm networks under independent and joint switching paradigms. In *Optical Communication (ECOC), 2015 European Conference on*, pages 1–3. IEEE, 2015.

[43] RGH Van Uden, R Amezcua Correa, E Antonio Lopez, FM Huijskens, Cen Xia, G Li, A Schülzgen, H De Waardt, AMJ Koonen, and CM Okonkwo. Ultra-high-density spatial division multiplexing with a few-mode multicore fibre. *Nature Photonics*, 8(11):865–870, 2014.

[44] Jose-Luis Izquierdo-Zaragoza, Pablo Pavon-Marino, and Maria-Victoria Bueno-Delgado. Distance-adaptive online rsa algorithms for heterogeneous flex-grid networks. In *Optical Network Design and Modeling, 2014 International Conference on*, pages 204–209. IEEE, 2014.

[45] Hideki Tode and Yusuke Hirota. Routing, spectrum and core assignment for space division multiplexing elastic optical networks. In *Telecommunications Network Strategy and Planning Symposium (Networks), 2014 16th International*, pages 1–7. IEEE, 2014.

[46] Dongyun Zhou and Suresh Subramaniam. Survivability in optical networks. *IEEE network*, 14(6):16–23, 2000.

[47] Ornan Gerstel and Rajiv Ramaswami. Optical layer survivability-an implementation perspective. *IEEE Journal on Selected areas in Communications*, 18(10):1885–1899, 2000.

[48] S Ramamurthy, Laxman Sahasrabuddhe, and Biswanath Mukherjee. Survivable wdm mesh networks. *Journal of Lightwave Technology*, 21(4):870, 2003.

[49] Narendra K Singhal, Laxman H Sahasrabuddhe, and Biswanath Mukherjee. Provisioning of survivable multicast sessions against single link failures in optical wdm mesh networks. *Journal of lightwave technology*, 21(11):2587, 2003.

[50] Biswanath Mukherjee. Wdm optical communication networks: progress and challenges. *IEEE Journal on Selected Areas in communications*, 18(10):1810–1824, 2000.

[51] Hui Zang, Canhui Ou, and Biswanath Mukherjee. Path-protection routing and wavelength assignment (rwa) in wdm mesh networks under duct-layer constraints. *IEEE/ACM Transactions on networking*, 11(2):248–258, 2003.

[52] Canhui Sam Ou, Jing Zhang, Hui Zang, Laxman H Sahasrabuddhe, and Biswanath Mukherjee. New and improved approaches for shared-path protection in wdm mesh networks. *Journal of Lightwave Technology*, 22(5):1223, 2004.

[53] Lu Shen, Xi Yang, and Byrav Ramamurthy. Shared risk link group (srlg)-diverse path provisioning under hybrid service level agreements in wavelength-routed optical mesh networks. *IEEE/ACM Transactions on Networking (ToN)*, 13(4):918–931, 2005.

[54] Yashpalsinh Jadeja and Kirit Modi. Cloud computing-concepts, architecture and challenges. In *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*, pages 877–880. IEEE, 2012.

[55] Peter Mell, Tim Grance, et al. The nist definition of cloud computing. 2011.

[56] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. *Communications of the ACM*, 53(4):50–58, 2010.

[57] Fei Xie, Jun Yan, and Jun Shen. Towards cost reduction in cloud-based workflow management through data replication. In *Advanced Cloud and Big Data (CBD), 2017 Fifth International Conference on*, pages 94–99. IEEE, 2017.

[58] Yaser Mansouri, Adel Nadjaran Toosi, and Rajkumar Buyya. Cost optimization for dynamic replication and migration of data in cloud data centers. *IEEE Transactions on Cloud Computing*, 2017.

[59] Rajkumar Buyya, Mukaddim Pathan, and Athena Vakali. *Content delivery networks*, volume 9. Springer Science & Business Media, 2008.

[60] M Farhan Habib, Massimo Tornatore, Marc De Leenheer, Ferhat Dikbiyik, and Biswanath Mukherjee. Design of disaster-resilient optical datacenter networks. *Journal of Lightwave Technology*, 30(16):2563–2573, 2012.

[61] Kenneth Hewitt. *Regions of risk: a geographical introduction to disasters*. Routledge, 2014.

[62] Roselinda R Schulman. Disaster recovery issues and solutions. *A White Paper, Hitachi Data Systems*, 2004.

[63] Ruth Bergman and Muriel Medard. Fault isolation for communication networks for isolating the source of faults comprising attacks, failures, and other network propagating errors, August 27 2002. US Patent 6,442,694.

[64] Ridha Rejeb, Mark S Leeson, and Roger J Green. Fault and attack management in all-optical networks. *IEEE Communications Magazine*, 44(11), 2006.

[65] Carmen Mas, Ioannis Tomkos, and Ozan K Tonguz. Failure location algorithm for transparent optical networks. *IEEE Journal on Selected Areas in Communications*, 23(8):1508–1519, 2005.

[66] Marija Furdek and Nina Skorin-Kapov. Physical-layer attacks in transparent optical networks. In *Optical Communications Systems*. InTech, 2012.

[67] Marija Furdek, Marko Bosiljevac, Nina Skorin-Kapov, and Zvonimir Šipuš. Gain competition in optical amplifiers: A case study. In *MIPRO, 2010 Proceedings of the 33rd International Convention*, pages 467–472. IEEE, 2010.

[68] Tao Deng and Suresh Subramaniam. Analysis of optical amplifier gain competition attack in a point-to-point wdm link. In *ITCom 2002: The Convergence of Information Technologies and Communications*, pages 249–261. International Society for Optics and Photonics, 2002.

[69] Marija Furdek. Physical-layer attacks in optical wdm networks and attack-aware network planning. *European Journal of Operational Research*, 178(2):1160–1167, 2011.

[70] Marija Furdek and Nina Skorin-Kapov. Attack-survivable routing and wavelength assignment for high-power jamming. In *Optical Network Design and Modeling (ONDM), 2013 17th International Conference on*, pages 70–75. IEEE, 2013.

[71] Amornrat Jirattigalachote, Nina Skorin-Kapov, Marija Furdek, Jiajia Chen, Paolo Monti, and Lena Wosinska. Sparse power equalization placement for limiting jamming attack propagation in transparent optical networks. *Optical Switching and Networking*, 8(4):249–258, 2011.

[72] Marija Furdek, Jiajia Chen, Nina Skorin-Kapov, and Lena Wosinska. Compound attack-aware routing and wavelength assignment against power jamming. In *Communications and Photonics Conference and Exhibition, 2011. ACP. Asia*, pages 1–3. IEEE, 2011.

[73] Govind P Agrawal. *Nonlinear fiber optics*. Academic press, 2007.

[74] Guanglei Liu and Chuanyi Ji. Resilience of all-optical network architectures under in-band crosstalk attacks: a probabilistic graphical model approach. *IEEE Journal on Selected Areas in Communications*, 25(3), 2007.

[75] Yunfeng Peng, Zeyu Sun, Shu Du, and Keping Long. Propagation of all-optical crosstalk attack in transparent optical networks. *Optical Engineering*, 50(8):085002–085002, 2011.

[76] Nina Skorin-Kapov and Marija Furdek. Limiting the propagation of intra-channel crosstalk attacks in optical networks through wavelength assignment. In *Optical Fiber Communication-incudes post deadline papers, 2009. OFC 2009. Conference on*, pages 1–3. IEEE, 2009.

[77] Muriel Medard, Douglas Marquis, Richard A Barry, and Steven G Finn. Security issues in all-optical networks. *IEEE network*, 11(3):42–48, 1997.

[78] Shoba Krishnan and Anita Borude. Security issues in all-optical networks. In *SRII Global Conference (SRII), 2011 Annual*, pages 790–794. IEEE, 2011.

[79] Marija Furdek, Nina Skorin-Kapov, and Maša Grbac. Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation. *Journal of Optical Communications and Networking*, 2(11):1000–1009, 2010.

[80] Nina Skorin-Kapov, Jiajia Chen, and Lena Wosinska. A tabu search algorithm for attack-aware lightpath routing. In *Transparent Optical Networks, 2008. ICTON 2008. 10th Anniversary International Conference on*, volume 3, pages 42–45. IEEE, 2008.

[81] Konstantinos Manousakis and Georgios Ellinas. Minimizing the impact of in-band jamming attacks in wdm optical networks. In *International Workshop on Critical Information Infrastructures Security*, pages 38–49. Springer, 2013.

[82] Shengli Yuan, Lei Chen, and Ming Yang. Minimizing inter channel attacks in wdm optical network. *International Journal of Future Computer and Communication*, 2(1):7, 2013.

[83] Shengli Yuan and Daniel Stewart. Protection of optical networks against interchannel eavesdropping and jamming attacks. In *Computational Science and Computational Intelligence (CSCI), 2014 International Conference on*, volume 1, pages 34–38. IEEE, 2014.

[84] Marija Furdek, Nina Skorin-Kapov, and Lena Wosinska. Shared path protection under the risk of high-power jamming. In *Networks and Optical Communications-(NOC), 2014 19th European Conference on*, pages 23–28. IEEE, 2014.

[85] Krishna Kant. Data center evolution: A tutorial on state of the art, issues, and challenges. *Computer Networks*, 53(17):2939–2965, 2009.

[86] Divyakant Agrawal, Sudipto Das, and Amr El Abbadi. Big data and cloud computing: current state and future opportunities. In *Proceedings of the 14th International Conference on Extending Database Technology*, pages 530–533. ACM, 2011.

[87] Sifat Ferdousi, Ferhat Dikbiyik, M Farhan Habib, Massimo Tornatore, and Biswanath Mukherjee. Disaster-aware datacenter placement and dynamic content management in cloud networks. *Journal of Optical Communications and Networking*, 7(7):681–694, 2015.

[88] Ferhat Dikbiyik, Massimo Tornatore, and Biswanath Mukherjee. Minimizing the risk from disaster failures in optical backbone networks. *Journal of Lightwave Technology*, 32(18):3175–3183, 2014.

[89] S Sedef Savas, Ferhat Dikbiyik, M Farhan Habib, Massimo Tornatore, and Biswanath Mukherjee. Disaster-aware service provisioning with manycasting in cloud networks. *Photonic Network Communications*, 28(2):123–134, 2014.

[90] Michael T Frederick, Pallab Datta, and Arun K Somani. Sub-graph routing: A generalized fault-tolerant strategy for link failures in wdm optical networks. *Computer Networks*, 50(2):181–199, 2006.

[91] Sebastian Neumayer, Gil Zussman, Reuven Cohen, and Eytan Modiano. Assessing the vulnerability of the fiber infrastructure to disasters. *IEEE/ACM Transactions on Networking (TON)*, 19(6):1610–1623, 2011.

[92] Sujogya Banerjee, Shahrzad Shirazipourazad, and Arunabha Sen. Design and analysis of networks with large components in presence of region-based faults. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–6. IEEE, 2011.

[93] Arunabha Sen, Sudheendra Murthy, and Sujogya Banerjee. Region-based connectivity-a new paradigm for design of fault-tolerant networks. In *High Performance Switching and Routing, 2009. HPSR 2009. International Conference on*, pages 1–7. IEEE, 2009.

[94] Mahshid Rahnamay-Naeini, J Pezoa, Ghady Azar, Nasir Ghani, and M Hayat. Modeling stochastic correlated network failures and assessing their effects on reliability. *IEEE ICC, Kyoto, Japan*, 2010.

[95] S Sedef Savas, M Farhan Habib, Massimo Tornatore, Ferhat Dikbiyik, and Biswanath Mukherjee. Network adaptability to disaster disruptions by exploiting degraded-service tolerance. *IEEE Communications Magazine*, 52(12):58–65, 2014.

[96] Ferhat Dikbiyik, Abu S Reaz, Marc De Leenheer, and Biswanath Mukherjee. Minimizing the disaster risk in optical telecom networks. In *Optical Fiber Communication Conference*, pages OTh4B–2. Optical Society of America, 2012.

[97] Jie Xiao, Hong Wen, Bin Wu, Xiaohong Jiang, Pin-Han Ho, and Lei Zhang. Joint design on dcn placement and survivable cloud service provision over all-optical mesh networks. *IEEE Transactions on Communications*, 62(1):235–245, 2014.

[98] Kai Morita and Kouji Hirata. Dynamic spectrum allocation method for reducing crosstalk in multi-core fiber networks. In *Information Networking (ICOIN), 2017 International Conference on*, pages 686–688. IEEE, 2017.

[99] Seitaro Sugihara, Yusuke Hirota, Shohei Fujii, Hideki Tode, and Takashi Watanabe. Dynamic resource allocation for immediate and advance reservation in space-division-multiplexing-based elastic optical networks. *Journal of Optical Communications and Networking*, 9(3):183–197, 2017.

[100] S Skiena. Dijkstras algorithm. *Implementing Discrete Mathematics: Combinatorics and Graph Theory with Mathematica, Reading, MA: Addison-Wesley*, pages 225–227, 1990.

[101] Ernesto QV Martins and Marta MB Pascoal. A new implementation of yens ranking loopless paths algorithm. *4OR: A Quarterly Journal of Operations Research*, 1(2):121–133, 2003.

[102] Sun-il Kim, Xiaolan J Zhang, and Steven S Lumetta. Rapid and efficient protection for all-optical wdm mesh networks. *IEEE Journal on Selected Areas in Communications*, 25(9), 2007.

[103] Andre Costa Drummond and Paulo Jose de Souza. An algorithm for resource allocation and partial protection of transparent optical wdm networks with service differentiation. In *Computer Networks and Distributed Systems (SBRC), 2014 Brazilian Symposium on*, pages 361–368. IEEE, 2014.

[104] http://www.fiber-optic-solutions.com/use-wdm-fiber-capacity-expansion.html.

[105] ILOG Cplex. 7.0 reference manual. *Accessed as HTML document, distributed with ILOG CPLEX*, 7, 2000.

[106] Hui Zang, Jason P Jue, Laxman Sahasrabuddhe, Ramu Ramamurthy, and Biswanath Mukherjee. Dynamic lightpath establishment in wavelength routed wdm networks. *IEEE Communications Magazine*, 39(9):100–108, 2001.

[107] F Lo Presti, Chiara Petrioli, and Claudio Vicari. Distributed dynamic replica placement and request redirection in content delivery networks. In *Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, 2007. MASCOTS'07. 15th International Symposium on*, pages 366–373. IEEE, 2007.

[108] Jane M Simmons. On determining the optimal optical reach for a long-haul network. *Journal of Lightwave Technology*, 23(3):1039, 2005.

[109] Xi Yang, Lu Shen, and Byrav Ramamurthy. Survivable lightpath provisioning in wdm mesh networks under shared path protection and signal quality constraints. *Journal of Lightwave Technology*, 23(4):1556, 2005.

[110] Senthil Ramamurthy and Biswanath Mukherjee. Survivable wdm mesh networks. part i-protection. In *INFOCOM'99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 744–751. IEEE, 1999.

[111] Murari Sridharan, Murti V Salapaka, and Arun K Somani. A practical approach to operating survivable wdm networks. *IEEE journal on selected areas in communications*, 20(1):34–46, 2002.

[112] Vinh Trong Le, Xiaohong Jiang, Son Hong Ngo, and Susumu Horiguchi. Dynamic rwa based on the combination of mobile agents technique and genetic algorithms in wdm networks with sparse wavelength conversion. *IEICE transactions on information and systems*, 88(9):2067–2078, 2005.

[113] Xiaowen Chu and Bo Li. Dynamic routing and wavelength assignment in the presence of wavelength conversion for all-optical networks. *IEEE/ACM Transactions on Networking (TON)*, 13(3):704–715, 2005.

[114] Michael Duser and Polina Bayvel. Analysis of a dynamically wavelength-routed optical burst switched network architecture. *Journal of Lightwave Technology*, 20(4):574, 2002.

Vita Auctoris

Saja Al Mamoori He obtained her B.Sc. and M.Sc. degrees in Computer Science and Information Systems from The University of Technology, Baghdad - Iraq in 2000 and 2003, respectively. She is currently a candidate for the Doctoral degree in Computer Science at the University of Windsor, Ontario and hopes to graduate in Fall 2017.