1-8-2016

Attack-Aware Routing and Wavelength Assignment of Scheduled Lightpath Demands

Hongbo Zhao
University of Windsor

Attack-Aware Routing and Wavelength Assignment of Scheduled Lightpath Demands

By

Hongbo Zhao

A Thesis
Submitted to the Faculty of Graduate Studies
through the School of Computer Science
in Partial Fulfillment of the Requirements for
the Degree of Master of Science
at the University of Windsor

Windsor, Ontario, Canada

2016

Attack-Aware Routing and Wavelength Assignment of Scheduled Lightpath Demands

by

Hongbo Zhao

APPROVED BY:

Dr. Esam Abdel-Raheem
Department of Electrical and ComputerEngineering

Dr. Dan Wu
School of Computer Science

Dr. Arunita Jaekel
School of Computer Science

Jan 6, 2016

DECLARATION OF ORIGINALITY

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyones 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 and have included copies of such copyright clearances to my appendix.

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

In Transparent Optical Networks, traffic is carried over lightpaths, creating a virtual topology over the physical connections of optical fibers. Due to the increasingly high data rates and the vulnerabilities related to the transparency of optical network, security issues in transparent wavelength division multiplexing (WDM) optical networks have become of great significance to network managers. In this thesis, we introduce some basic concepts of transparent optical network, the types and circumstances of physical-layer attacks and analysis of related work at first. In addition, based on the previous researches, we present a novel approach and several new objective criterions for the problem of attack-aware routing and wavelength assignment. Integer Linear Programming (ILP) formulation is used to solve the routing sub-problem with the objective to minimize the disruption of physical-layer attack as well as to optimize Routing and Wavelength Assignment (RWA) of scheduled transparent optical network.

DEDICATION

To my Loving Family:

Father: Jinrong Zhao

Mother: Baiyan Tang

ACKNOWLEDGEMENTS

I would love to express my deepest gratitude to my master supervisor, Dr. Arunita Jaekel, for her teaching and support throughout my graduate studies. She provides me with great ideas about thesis topic, simulation cases and at the same time spends much time instructing me on proposal, program, testing, thesis writing and defense.

Also, I want to appreciate the members of my M.Sc. thesis committee, internal reader Dr. Dan Wu and external reader Dr. Esam Abdel-Raheem for their professional assistance and guidance on my research and thesis.

Hongbo Zhao

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

Introduction

1.1 Overview

Optical networks constitute a telecommunication network architecture on the basis of optical fibers, which uses signals encoded onto light to transmit information among various nodes[13]. Optical communication provides large capacity over long distances, high reliability transmission, interconnection and management for multi-node networks. Optical networks rely on a series of optical components, e.g. optical amplifiers, lasers or LEDs, multiplexer, demultiplexer, optical switch, etc. and wavelength division multiplexing (WDM) technology, In recent years, optical network has emerged to replace traditional metal communication network and is becoming more and more widely used all over the world.

However, security issues of optical network has attracted great attention. Due to the high data rates and the vulnerabilities associated with transparency, physical-layer attacks caused by high-powered jamming signal can seriously degrade network performance, lead to loss of user data and must be dealt with efficiently[2]. How to well detect and localize the attack at the lowest possible cost has become a hot issue. In this thesis, we proposed a new objective criterion for security-aware routing and wavelength assignment (RWA) problem of scheduled network and formulate the routing sub-problem as an integer linear program (ILP). The intention is to minimize the threat of attack by reasonable network design and identify potential lightpaths and switches which may be influenced by various types of attack.

1.1.1 Advantages of Optical Network

Optical network uses glass (or plastic) threads (fibers) to transmit data. As shown in Fig. 1.1, a fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves[12].

In comparison with traditional metal communication lines, fiber optics have several advantages:

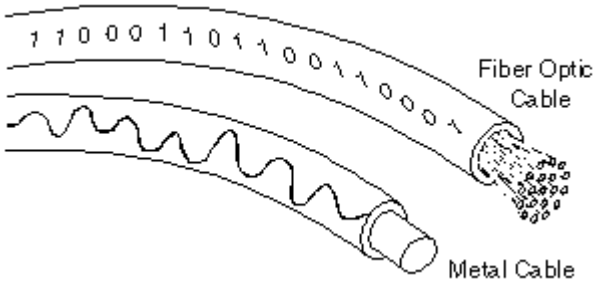


Fig. 1.1: Optical Fiber Cable & Metal Cable [12]

- Fiber optic cables are less susceptible than metal cables to interference.
- Fiber optic cables are much thinner and lighter than metal wires.
- Data can be transmitted digitally.

1.1.2 Wavelength-Division Multiplexing (WDM)

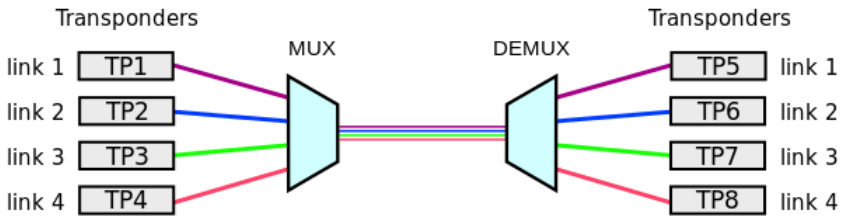


Fig. 1.2: WDM Components [13]

In fiber-optic communications,wavelength-division multiplexing(WDM) is a technology which multiplexes a number of optical carrier signals onto a single optical fiberby

using different wavelengths of laser light[22]. As demonstrated in Fig. 1.2, a WDM system uses a multiplexer at the transmitter to join the several signals together and a demultiplexer at the receiver to split them apart. The use of WDM makes it possible that two or more optical signals with different wavelengths can transmit information on the same optical cable, which reduces physical and manufacturing complexity and boosts the reliability of the system. In addition, it can be fast recovered when faults or attacks occur.

1.1.3 Opaque & Transparent Optical Network

According to whether or not the transmitted signal undergoes an optical to electronic to optical (OEO) conversion at different places in the network, the optical network can be mainly divided into (i) Opaque Network and (ii) Transparent Network.

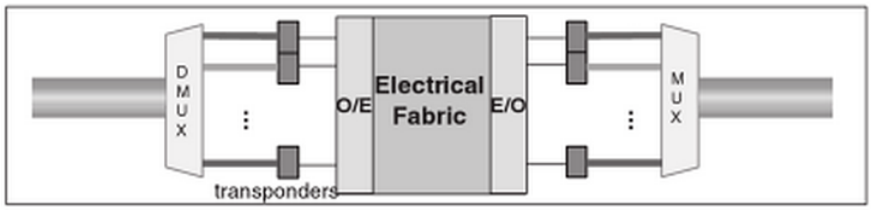


Fig. 1.3: Opaque Optical Network Topology [14]

As described from Fig 1.3, it is a network topology of opaque optical network and the OEO conversion occurs in the opaque switch.

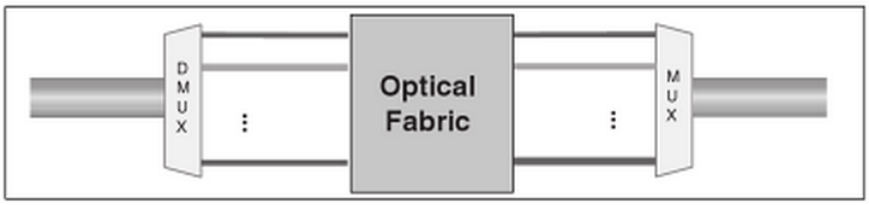


Fig. 1.4: Transparent Optical Network Topology [14]

Fig 1.4 demonstrates a transparent optical network topology, from this graph we can see that there are no WDM transponders in transparent optical network. The lightpath signals remain in an optical format from the source to the destination without undergoing OEO conversion.

1.1.4 Routing and Wavelength Assignment (RWA)

Given a set of connections, the problem of setting up lightpaths by routing and assigning a wavelength to each connection is called the Routing and Wavelength Assignment (RWA) problem. That is to say, in setting up a lightpath, a route must be selected and a wavelength must be assigned to the lightpath. If no wavelength is available for this lightpath on the selected route, the connection request is blocked. Also, the RWA problem must be subject to the following two constrains:

- Wavelength Continuity Constraint: If no wavelength converters are available, the same wavelength must be assigned along the entire route of a lightpath.
- Wavelength Clash Constraint: Any two lightpaths sharing a common fiber link cannot be assigned the same wavelength.

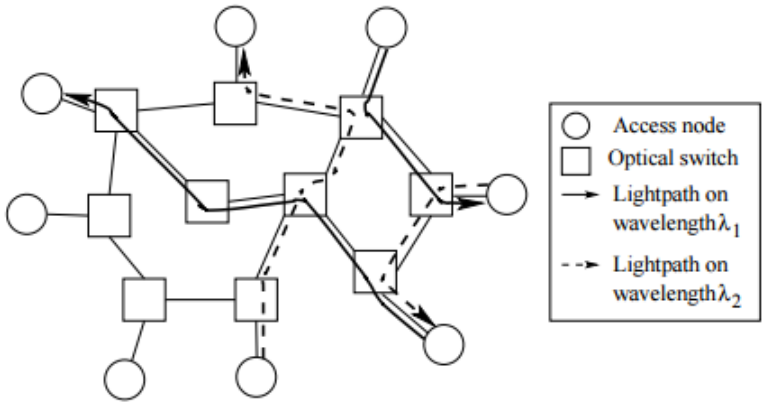


Fig. 1.5: a wavelength-routed optical network with lightpath connections [17]

Fig 1.5 illustrates a wavelength-routed network, where lightpaths have been set up between pairs of nodes on different wavelengths. We can see from the diagram, although two or more lightpath share the same optical link, they have to be provided different wavelength. Typically, connection requests (demands) may be of three types: static, scheduled and dynamic[23].

- Static Traffic: The demands are allocated for the entire duration of the network, time dimension not being considered in general.

- Dynamic Traffic: The start times and durations of demands are generated randomly based on certain traffic distributions or probability

- Scheduled Traffic: In scheduled traffic, time dimension of demands should be explicitly considered, which means we need to specify the specific time intervals. As seen from Table 1.1, there are three demands, r_1, r_2 and r_3. Each demand is represented by a tuple (s,d,t_s,t_e) where s and d are the source and destination node, t_s and t_e are the starting time and ending time.

TABLE 1.1: an Example of Scheduled Demand Set

Demands	s	d	t_s	t_e
r_1	2	9	05:00	09:20
r_2	5	2	07:00	12:40
r_3	3	7	08:00	14:00

1.2 Motivation

Along with the development and wide application of transparent wavelength division multiplexing (WDM) optical networks, security issues and physical-layer attack management have become increasingly important to the network manager. The major advantages of transparent optical networks depend on their character of transparency, which allows high-speed connections without undergoing optical to electronical to optical (OEO) conversion at intermediate nodes. However, it is also the transparency that leads to vulnerabilities in security and enhances the difficulties in detecting and localizing attacks because monitoring must be performed in the optical domain[3]. In addition, detecting techniques aiming at detecting and localizing attacks relied on information from specialized optical monitoring equipment can be quite expensive. In general the more reliable performance of the network required, the more resources are needed and thus the cost of the security equipment is higher[9].

In this thesis, we are aiming at minimize the potential damage of various attacks on the optical network without the need for specialized equipment. Accordingly, the approach we propose takes into account the potential factors of physical-layer attacks

when solving the RWA problem. Integer Linear Programming (ILP) is a mathematical optimization program which can be used to solve the routing sub-problem with the objective to minimize the crosstalk attack radius and in-band attack radius in scheduled optical network. In summary, our approach relies on optimally arranging the set of lightpaths to minimize the possible disruptions caused by various attack scenarios to reduce the number of lightpaths attacked, which can not only reduce the potential network service disruption but also make failure detection and localization algorithms be faster since they only need to search fewer potential lightpaths[4].

1.3 Problem Statement

In this thesis, we propose a novel algorithm which uses integer linear program (ILP) to address the security-aware routing and wavelength assignment problem in scheduled transparent WDM optical network. Given is a physical network which includes nodes and links and a virtual topology, i.e. a set of scheduled lightpath demands. The physical edges are assumed to be bidirectional, each representing a pair of optical fibers. The RWA problem which searches for physical paths corresponding to lightpath requests should be subject to the wavelength continuity constraints and wavelength clash constrains. We set enough wavelengths (channels) to accommodate the set of lightpaths. We also select random time intervals between 1 and 24, during which each lightpath request is acquired. In order to better measure physical-layer attack, we introduce two concepts, i.e. Lightpath Attack Radius (LAR) and In-band Attack Radius (IAR), which will be presented in detail in the next chapter. The approach to optical networks security is aimed at minimizing the potential damage caused by several major physical-layer attacks including gain competition, inter-channel crosstalk attack and in-band crosstalk attack[2]. Several simulation scenarios (including different number of nodes, lightpath demands, intervals, etc.) will be created to acquire the objective values. Then we compare them with the cases which are also with the objective of minimizing lightpath congestion (i.e. shortest path of each lightpath request) but only not considering the security, so that we can prove the advantages of our security-aware routing and wavelength assignment approach in scheduled optical

network.

1.4 Solution Outline

In this thesis, we present optimal Integer Linear Program (ILP) formulations for solving security-aware scheduled RWA problems. IBM ILOG CPLEX Optimization software is used to solve the formulations. The major contribution of this thesis are:

- A novel algorithm and ILP formulations to address the security-aware RWA Problem for scheduled traffic which has not been done.
- Several objectives that comprehensively take both lightpath attack radius (LAR) and in-band attack radius (IAR) into consideration.
- Comparison of the security performance (anti-attack capacities) between our approach and traditional RWA approach without considering security for various lightpath demands and different scales of network

1.5 Organization of Thesis

The remainder of the thesis is organized as follows: Chapter 2 presents the necessary introductions of some important concepts such as physical layer attacks, differences between network faults and attacks and the literature review of previous research associated with network attack detection and localization, security-aware RWA problem, etc. In Chapter 3, we propose our algorithm and describe the details about ILP formulations. Chapter 4 presents the simulation results that we carry out, analysis about them and comparison with existing methods. Chapter 5 makes a conclusion of our work and discusses some probable directions for further research and work.

CHAPTER II

Review of Related Work

2.1 Fault and Attack Management

The physical layer (layer 1) sits at the bottom of the Open System Interconnect (OSI) model (As shown in Fig. 2.1), which is designed to transmit bit streams through electric signals, lights or radio transmissions.

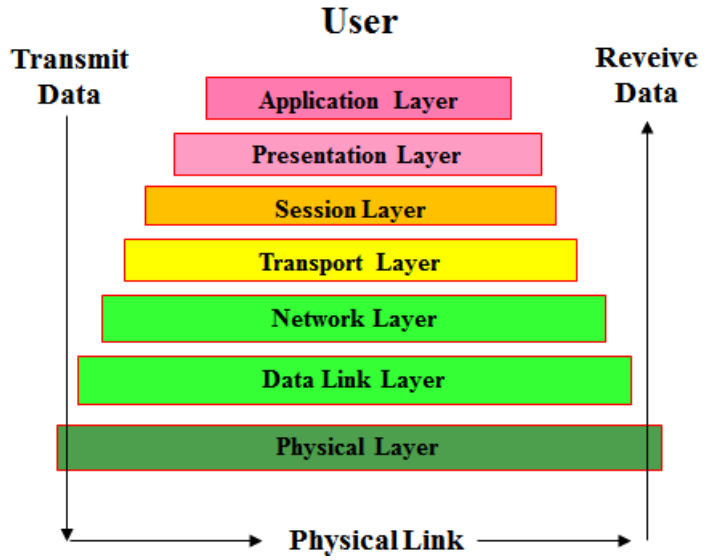


Fig. 2.1: the Seven Layers of OSI

Security issues due to transparency in optical network components is a major challenges for network management[3]. The thesis titled Fault and Attack Management in All-Optical Networks[4] covers management issues with particular emphasis on complications due to the unique characteristics and behaviors of transparent network components. In addition, an algorithm is also presented for multiple attack localization and identification of optical networks.

There are several kinds of attacks, including fiber cuts, power jamming (amplifier attack), crosstalk attack (switch node attack) and correlated jamming (tapping attack), etc[20].Among them, some can be seen as a kind of optical component fault, such as fiber attack. Others, like crosstalk attack, can affect lightpaths that traverse the same link or node with the attack connections. Crosstalk attack has higher damage capabilities, which our approach mainly focuses on.

2.1.1 Differences between Attack and Fault

In general, there are three main differences between an attack and a fault.

- An attack appears and disappears sporadically in the network due to attack signal injection, while a fault occurs usually because of physical natural fatigue and aging of optical devices and components, so it happens slower than an attack.

- Attacks may trigger multiple erroneous and undesirable alarms due to their characteristic of propagation. For example, when a lightpath is being attacked, it can in turn attack other lightpaths with which it shares the same physical links or switches. But faults can only lead to single alarm, it will not affect other lightpaths.

- For fault recovery, rerouting of traffic channels can solve all resulting problems. However, the same approach cannot solve all resulting problems of an attack. As describes in Fig 2.2, when the link (2,3) fails, rerouting Primary connection can solve this problem (use Backup lightpath). If an attack signal is injected at Node 1 and we still treat such attack as a component fault and reroute Primary connection to Backup, we can see this method cannot solve the problem, because Backup lightpath is still affected by attack signal.

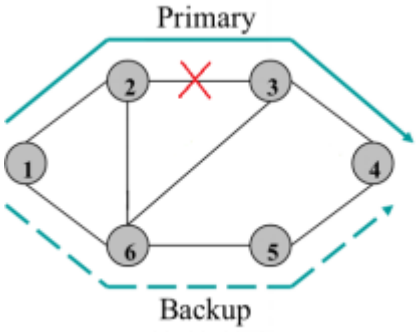


Fig. 2.2: Rerouting Connections can solve link failure

2.1.2 Attack Types in All-Optical Networks

All-Optical Networks provide transparency capabilities, allowing routing and switching of traffic without any modification or examination of signals in the network [4]. Admittedly, transparency character has many advantages in supporting high data rate communications, it also brings new challenges that not exist in traditional networks. Attacks can be considered from different viewpoints. From an attackers perspective, attacks can be widely divided into six areas: traffic analysis, eavesdropping, data delay, service denial, QoS degradation and spoofing [18]. Because some of these areas have similar characters, the attacks can also be grouped into two main categories, i.e. service disruption and eavesdropping.

TABLE 2.1: an Example of Scheduled Demand Set[9]

Attack Type	Attack Method	Component
Service Disruption	In-band jamming power	Fiber
	Out-of-band jamming power	Fiber
	Intentional Crosstalk	Splitter
		Filter
		Switch
	Gain Competition	Amplifier
Eavesdropping	Unauthorized Observation	Fiber
		Tap

As it describes in the Table 2.1, there are various physical-layer attacks that can happen in different components of TONs. Details about attack methods will be presented below.

Gain Competition

In order to implement an attack, the attacker needs to gain access to the network. For example, to commit an in-band or out-of-band jamming attack, the attacker can take advantage of the specific characteristics of optical component such as optical amplifiers and cause gain competition attack[4].

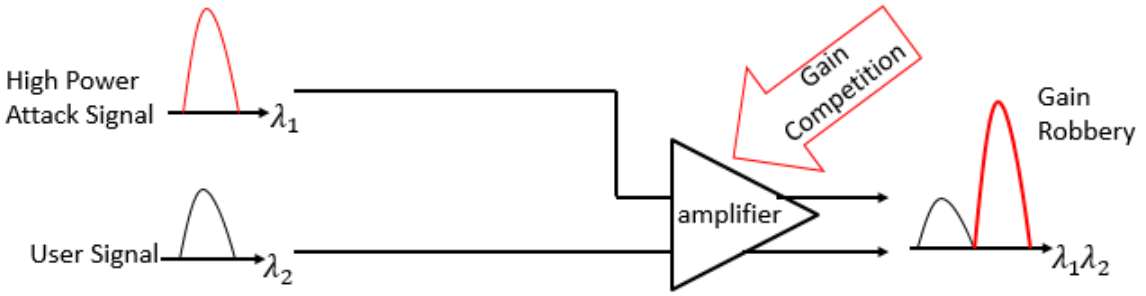


Fig. 2.3: Gain Competition in amplifiers

Fig 2.3 depicts the Gain Competition in an optical amplifier. The attacker injects a high powered signal at wavelength λ_1 (usually 20-30dB larger than user signal) into a transparent optical network. When they traverse an amplifier, because the amplifier cannot distinguish between attack signals and legitimate network signals, the attack signal can acquire more energy and additionally increase its power, which leads to the user signal power loss(the supply of gain is finite in amplifier). The scenario of power robbery in amplifier is known as a gain competition attack. As a result, channel λ_1 robs channel λ_2 of power and propagates downstream through successive optical components, affecting other legal channels along its route and causing degrading or denying network service.

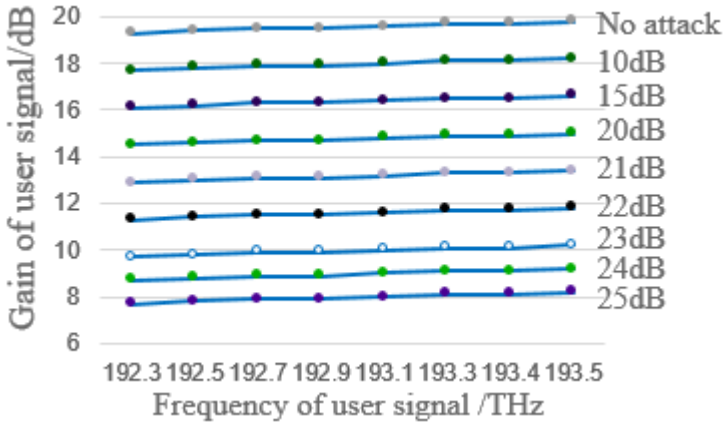


Fig. 2.4: Simulation diagram of gain competition attack

In the year 2010, Furdek et al. [19] verify the gain competition attack arise by high power signal injected in Erbium Doped Fiber Amplifier (EDFA). EDFA is optical amplifier that use a doped optical fiber as a gain medium to amplify an optical signal. As described in Fig 2.4, the frequency of attack signal is 192.1 THz and the user signal are 192.3, 192.5, 192.7, 192.9, 193.3, 193.5 THz. When the power of attack signal is 10dB larger than user signal, the gain of user signal starts to decrease. The more increase in the power of attack signal, the more decrease in the gain of user signal.

Inter-channel Crosstalk Attack

Moreover, long distance transformation and high-power signals injection may result in another attack called Inter-channel Crosstalk[3].

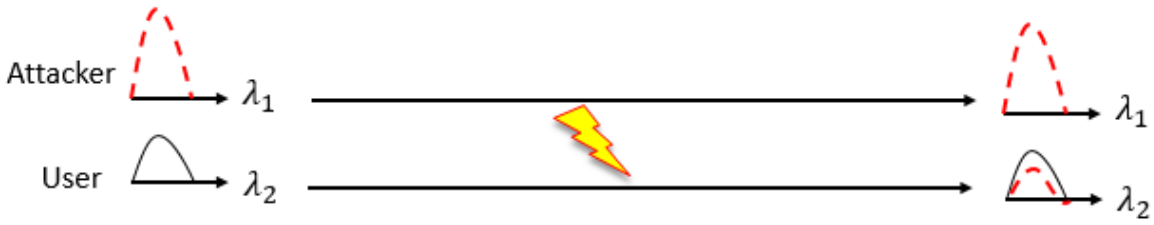


Fig. 2.5: Inter-channel Crosstalk

Fig 2.5 shows a high-power jamming signal, which uses a different wavelength from user signal, injected on a link. The jamming signal is able to disrupt the lightpath it is injected on and the other lightpaths with which it shares the common links.

In-band (Intra-channel) Crosstalk Attack Propagation

Marija Furdek et al. also propose a type of attack, which is similar to in-band crosstalk attack introduced above, called in-band crosstalk attack propagation[2]. The attack signal may not only affect connections traversing common switches, but also if enough power is transferred to the affected connection, these connections may also acquire attack abilities themselves [2]. That is to say, the attack can propagate to other lightpaths through the network and disrupt other legitimate lightpaths far beyond the original attacker [20].

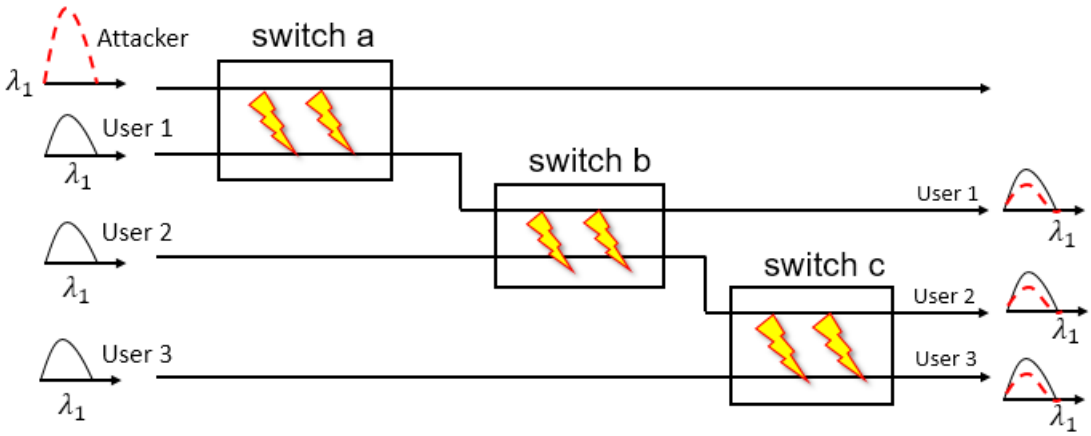


Fig. 2.6: In-band crosstalk attack propagation[2]

Fig 2.6 displays a diagram about in-band crosstalk attack propagation. The attack signal is injected into the network at switch a. First, it will attack User 1 's signal at their common switch a. Then, the signal of legitimate User 1 acquires the attack power and it attacks User 2 at switch b. Finally, the User 2 who also acquires the attack power from user 1 disrupts User 3 at their common switch c. From this example we can see that the attacker has the ability to affect User 2 's and User 3 's signal even though they do not share any common physical components.

Eavesdropping

Eavesdropping attack is a realization of unauthorized observation [21], which may happen at several points in the network. Among them, two eavesdropping examples require more attention. One example comes from component crosstalk: the demultiplexer is an important component in wavelength division multiplexing (WDM) optical network which is used to split wavelength received from a single fiber onto separated physical paths. The crosstalk level of demultiplexer is between 0.03% to 1.0%. However, it is just because of the low ratio of crosstalk level, a little of each wavelength leaks onto the wrong path. If attackers detect the leaked signal and it is very likely that some of data from the stream can be recovered. The other example of eavesdropping is relevant to the optical amplifier. When signals passing through the amplifier, they will undergo a slight amplitude modulation on the basis of the presence or absence of signal on adjacent channels [21]. Due to the leak of signal, the attacker may recover some intended signal on an adjacent channel.

2.2 Objectives for Attack-aware RWA Problem

The attack-aware routing and wavelength assignment (RWA) is aimed at minimizing the potential damage caused by physical-layer attacks. We are trying to achieve the prevention measures through careful network planning. In other words, by solving the RWA problem, we try to reduce vulnerabilities to attacks without the requirement of specific network monitoring components. So, proper objectives which are able to estimate the impact of attack can definitely be an important part in RWA problem solving.

2.2.1 Lightpath Attack Radius (maxLAR)

In order to better estimate the influence of inter-channel crosstalk attack, an objective criterion for the RWA problem is maximum Lightpath Attack Radius (maxLAR)[3]. Lightpath Attack Radius (LAR) is defined for every specific lightpath to describe if it is injected jamming signal, the number of legitimate data lightpaths it can attack

(on links). However, maxLAR is aimed at the whole network, which is defined as the number of legitimate data lightpaths any one jamming signal can attack (on links). In other words, maxLAR describes the maximum number of lightpaths (including itself) any one lightpath shares a common directed physical link with. What is more, there is a relevant concept called Lightpath Attack Group (LAG). It depicts the set of legitimate lightpaths which are probably attacked by the lightpath that is injected jamming signal.

Moreover, in wavelength-convertible networks, the concept of network congestion is the same as the number of wavelength used. As defined, maxLAR is also the upper bound of network congestion as well as the number of wavelengths actually required. By minimizing this value, we can not only reduce the threat of physical-layer attack, but also decrease the worst case of congestion.

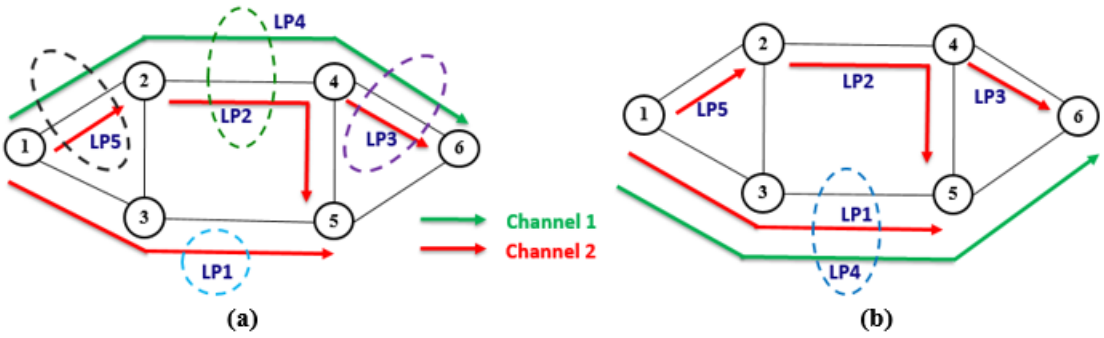


Fig. 2.7: maxLAR of two RWA schemes with the same lightpath demands

Fig 2.7 displays two RWA schemes with the same network topology, wavelength assignment and lightpath requests. According to Fig 2.7 (a), the the set of lightpath attack group (LAG) and the value of lightpath attack radius (LAR) for each lightpath is shown in Table 2.2.

TABLE 2.2: Lightpath Attack Radius of each lightpath in Fig 2.7 (a)

	LP1	LP2	LP3	LP4	LP5
LAG	{LP1}	{LP2,LP4}	{LP3,LP4}	{LP2,LP3,LP4,LP5}	{LP4,LP5}
LAR	1	2	2	4	2

Specifically, for example, the lightpath attack radius of Lightpath 1 is 1, because it does not share any physical link with other lightpath, which means if the attack signal being injected in LP1, it can only interfere LP1 itself. Similarly, for Lightpath 4 (LP4) in the topology, due to the fact that it shares the link 1-2 with LP5, link 2-4 with LP2 and link 4-6 with LP3, the value of LAR for LP4 is 4, which represents if LP4 is attacked, except itself, LP2, LP3 and LP5 will also be disrupted because they share at least one common link with LP4. According to the data of Table 2.2, the maxLAR of the network topology Fig 2.7 (a) is

$$maxLAR = LAR_{LP4} = 4$$

In comparison with Fig 2.7 (a), the only difference of Fig 2.7 (b) is the lightpath route of LP4. In Fig 2.7 (a), LP4 traverses links 1-2, 2-4 and 4-6 while in Fig 2.7 (b) the route is changed to 1-3, 3-5 and 5-6. So, the corresponding value of LAR for each lightpath may be different.

TABLE 2.3: Lightpath Attack Radius of each lightpath in Fig 2.7 (b)

	LP1	LP2	LP3	LP4	LP5
LAG	{LP1,LP4}	{LP2}	{LP3}	{LP1,LP4}	{LP5}
LAR	2	1	1	2	1

We can see from Table 2.3, LP1 only shares the same link (3-5) with LP4 and vise versa, so the values of LAR for LP1 and LP4 are both 1+1=2 for this network topology. In addition, the values of LAR of LP2, LP3 and LP5 are all equal to 1 because these three lightpath share no links with other lightpaths. Hence the maxLAR

of Fig 2.7 (b) is:

$$maxLAR = LAR_{LP1} = LAR_{LP4} = 2$$

Please note that the value of maxLAR can represent the degree of disruption by physical attack. In this example, maxLAR of Fig 2.7 (a) is 4 but the value is 2 in Fig 2.7 (b), which means a jamming signal injected on any legitimate lightpath could disrupt at most 4 lightpaths if the lightpath routes arranged the same as Fig 2.7 (a), however it can only disrupt at most 2 lightpaths in Fig 2.7 (b). From the example above, we can come to the conclusion that the value of maxLAR is related to the route of lightpaths. That is to say, it is reasonable to minimize the potential attack threat of inter-channel crosstalk by rerouting the lightpaths.

2.2.2 In-band Crosstalk Attack Radius (maxIAR)

In-band crosstalk attack radius is also defined as a measure to estimate the impact of in-band crosstalk attack. In length-selective switches, attack signals can attack other lightpaths transmitted on the same wavelength with which they share at least one common switch. That is to say, in-band crosstalk attack has two characteristics: (1) Lightpaths which are on the same wavelength can be attacked; (2) it generally happened in switches including the source and destination nodes of a lightpath. Similar to maxLAR, there are also In-band Attack Radius (IAR) and In-band Attack Group (IAG) defined aiming at each lightpath. IAG describes the set of lightpaths with which one specific lightpath shares the common switch and transmitted on the same wavelength, while IAR describes the number of lightpaths in the set of IAG for each lightpath.

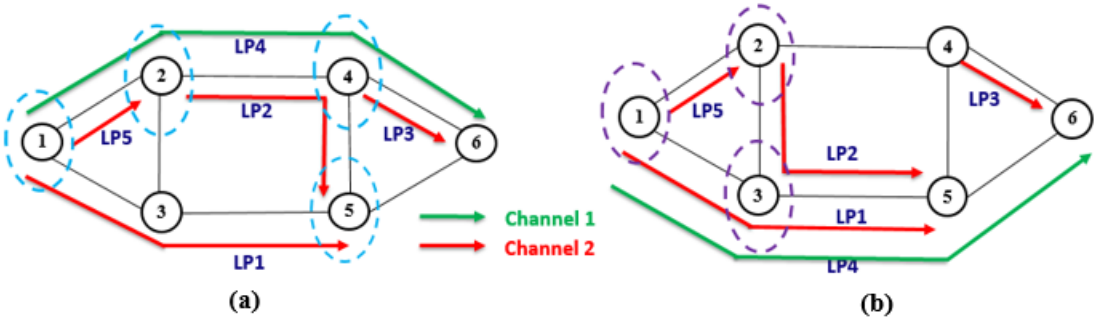


Fig. 2.8: maxIAR of two RWA schemes with the same lightpath demands

As demonstrated in Fig 2.8, two RWA schemes are of the same network topology, channel assignment and lightpath demands. However, the lightpath route of LP2 and LP4 are different. In Fig 2.8 (a), LP2 is routed via nodes 2-4-5, LP4 is routed via nodes 1-2-4-6. In Fig 2.8 (b), LP2 is routed via nodes 2-3-5, whereas LP4 is routed via nodes 1-3-5-6.

TABLE 2.4: In-band Attack Radius of each lightpath in Fig 2.8 (a)

	LP1	LP2	LP3	LP4	LP5
IAG	{LP1,LP2,LP5}	{LP1,LP2,LP3,LP5}	{LP2,LP3}	{LP4}	{LP1,LP2,LP5}
IAR	3	4	2	1	3

Table 2.4 presents the value of IAR for each lightpath. If a high-powered signal is injected on lightpath 1 (LP1) at its source node 1, the attacker can potentially disrupt LP5 in their common node (switch) 1 and LP2 in their common node 5. Therefore, the IAR of lightpath 1 is IAR_{LP1}=2+1=3, 1 represents LP1 itself. LP2 shares the common node 2, node 4 and node 5 with the lightpath LP5, LP3 and LP1, respectively. So, the IAR value of LP2 is IAR_{LP2}=3+1=4. Similarly, LP3 can affect LP2 at node 4 (IAR_{LP3}=1+1=2), LP5 may have impact on LP1 and LP2 at node 1 and 2, respectively (IAR_{LP5}=2+1=3). Note that LP4 cannot being attacked when LP2, LP3 or LP5 being injected attack signal, because they are on the different wavelengths in spite of sharing at least one common switch. Therefore, LP4 cannot

attack other lightpaths in this RWA scheme. From the table, we can get the maximum in-band attack radius:

$$maxIAR = IAR_{LP2} = 4$$

TABLE 2.5: In-band Attack Radius of each lightpath in Fig 2.8 (b)

	LP1	LP2	LP3	LP4	LP5
IAG	{LP1,LP2,LP5}	{LP1,LP2,LP5}	{LP3}	{LP4}	{LP1,LP2,LP5}
IAR	3	3	1	1	3

As can be seen in Table 2.5, the values of IAR for each lightpath in Fig 2.8 (b) are 3, 3, 1, 1 and 3 for lightpath 1, 2, 3, 4 and 5, respectively. Therefore, the value of maximum in-band attack radius for this RWA scheme is:

$$maxIAR = IAR_{LP1} = IAR_{LP2} = IAR_{LP5} = 3$$

So, for Fig 2.8 (b), because we change the routes of lightpath 2 (LP2), causing LP2 and LP3 from sharing one common switch 4 in Fig 2.8 (a) to no common switch in Fig 2.8 (b), reducing the value of maxIAR from 4 to 3, thus decreasing the potential attack threat from in-band crosstalk attack.

2.3 Review of Related Work

A summary of Attack-aware planning and optimization in Transparent Optical Network (TONs) can be found in [1]. It presents a novel security framework on the basis of protection and provides an example of gain competition and propagating intra-channel crosstalk attack-scenarios.

In referenced paper [3], Nina Skorin-Kapov et al. present a novel objective criterion called maxLAR, which is used to measure the largest number of lightpaths sharing a common link with any other lightpath. Most important, authors give an ILP formulation for the routing sub-problem of RWA with the objective of minimiz-

ing maxLAR and prove that by minimizing the value of maxLAR, we can limit the maximal disruption caused by various physical-layer attacks including inter-channel crosstalk attack. In order to solve the routing sub-problem for large network, they propose a tabu search heuristic aimed at minimize maxLAR.

The concept of propagating crosstalk attack radius (P-CAR) is proposed in [2]. Marija Furdek et al. propose attack-aware wavelength assignment that minimizes the worst-case potential propagation of in-band crosstalk jamming attacks. In this thesis, P-CAR is defined as an objective criterion for routing sub-problem of RWA. Fig 2.9 displays an example of RWA scheme for P-CAR calculation.

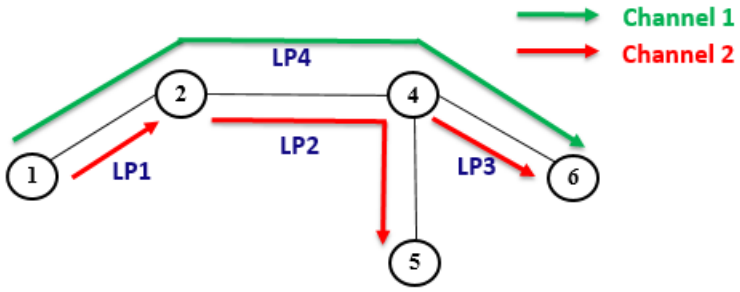


Fig. 2.9: an example of RWA scheme for P-CAR

In Fig 2.9, there are four lightpath demands. If an attack signal is injected on lightpath 1 (LP1) at its source node 1, the lightpath maybe attacks LP2 at their common switch 2, which then propagate to lightpath 3 (LP3) in switch 4. So, P-CAR of LP1 is P-CAR (LP1) = 2 + 1 = 3. Note that, LP4 cannot be affected because it is on different channel from the other three lightpaths.

Through comparison with other algorithms, tests indicate that the proposed algorithms in the paper can acquire much lower P-CAR values with little or no increase in the number of wavelengths used. Moreover, the results reflect that only taking the upper bound of P-CAR value (maxPCAR) into account is precise enough to acquire result which is very close to the actual P-CAR value, but reduces complexity.

The paper [4] is related to fault and attack management in All-Optical Networks. In TONs, the character of transparency makes the network vulnerable to multiple forms of attack, such as service disruption, QoS degradation and eavesdropping at-

tacks, causing large quantities of data to be lost or compromised. In order to deal with the problem, authors compare existing supervisory and monitoring techniques such as BER measurements, Optical Power Meters, Pilot tones, Optical Time Domain Reflectometers, etc. and their scales of application involving monitoring the attack of in-band jamming, out-of-band jamming as well as time distortion, noise and accuracy of these devices. In addition, an outline of Multiple Attack Localization and Identification (MALI) algorithm has been proposed, which can make a contribution to faults and attacks management of All-Optical Networks.

In referenced paper [5], the authors present and introduce various attack detection methods by supervisory techniques for All-Optical Networks. The techniques can be widely categorized into two types: Methods of statistical analysis of communication data and methods of diagnosing a signal. Moreover, a new method for detecting attacks is described in this paper. This method is based on the mathematical relationship between input and output signals which is known by network manager. Hence, we can detect an attack by comparing input signals with output signals.

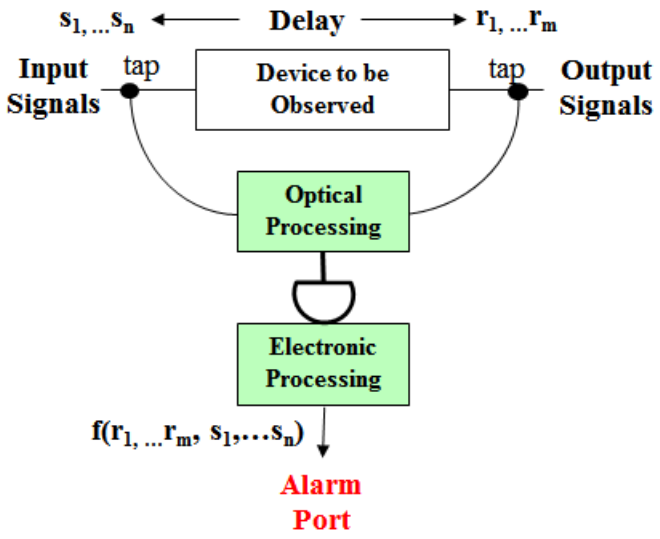


Fig. 2.10: A New Detection Method[21]

As displayed in Fig 2.10, several input signals (S_1, S_2,...S_n) pass the monitoring device from the left and exit at the right (Output signals: r_1, r_2,...r_n). Function f (r_1,...r_m,s_1,...s_n) measures device operation relevant to some parameters. Whether or not an alarm is generated depends on the value of function f. The alarm port is

connected to network management system which is applied to manage the alarms. This is a basic idea of using monitor device to detect the attack. Therefore, combining different approaches in Transparent Optical Network protection, it is a perfect way to use attack-aware RWA to regulate the route of lightpaths and wavelength assignment properly, then install some detection components in some possible places, where threat of being attacked exists.

2.4 Summary of Referenced Paper

We have analyzed five papers in Chapter 2.3, which are the most related to our research, Table 2.7 describes whether or not some important points relevant to our research being included in these papers.

TABLE 2.6: Summary of Referenced Papers

	Paper [1]	**Paper [2]**	**Paper [3]**	**Paper [4]**	**Paper [5]**
Proposed Approach	ILP (maxLAR, P-CAR)	ILP (P-CAR) and Tabu Search	ILP (maxLAR)	Multiple Attack Localization and Identification Algorithm (MALI)	Input and Output Signals analysis
Solved Attack Type	In-band Crosstalk, Inter-channel Crosstalk, Gain Competition	in-band crosstalk	Gain Competition, inter-channel crosstalk	help improve faults and attacks management	sporadic jamming, multipoint attacks, Control System and Protocol Attacks
Traffic Model	Static	Static	Static	Static	Static&Dynamic

From Table 2.6, we can see that [1],[2] and [3] propose ILP formulation to solve the RWA problem. Among them, paper [1] can be seen as a summarization of using ILP to solve in-band and out-of-band jamming attacks. Paper [2] is aimed at in-band

crosstalk attack with the objective of P-CAR and propose Tabu search to deal with large network and paper [3] targets at solving inter-channel crosstalk attack by ILP formulation with the objective of maxLAR. In paper [4], authors propose Multiple Attack Localization and Identification (MALI) Algorithm to help boost faults and attacks management. In Paper [5], a novel input and output signals comparison algorithm is proposed to solve various attacks.

CHAPTER III

Security-aware Scheduled RWA

3.1 Introduction

In this chapter, we are going to introduce our proposed approach for solving the security-aware Routing and Wavelength Assignment of Scheduled Networks. The problem definition, detailed ILP formulation (including objectives, constraints) and description about each constraint will be presented in the following sections. The objectives of the proposed ILP formulation will combine *In-band Attack Radius (IAR)* and *Lightpath Attack Radius (LAR)* to effectively minimize the potential damage caused by both in-band and out-of-band attacks. Unlike previous work on attack-aware RWA, our proposed approach considers the *scheduled traffic model (STM)*, which has not been addressed before.

In this chapter, we present different simulation cases and the results of RWA problem from our proposed approach. We also compare the objective values obtained using our approach ILP_AR1, ILP_AR2, ILP_SUM_AR2 and ILP_SUM_AR1 with the corresponding values obtained using a traditional attack-unaware RWA scheme (ILP_SPATH).

Unlike existing attack-aware RWA techniques we consider the scheduled traffic model, which means we consider the time dimension in our proposed ILP formulation. Furthermore, traditional static RWA can be treated as a special case of our approach (by setting a single time interval for all the lightpath demands). Finally, the objectives in our ILP formulation take into account both in-band attack radius (IAR) and lightpath attack radius (LAR), so it can handle multiple types of attacks.

3.2 Problem Definition

We are given a network topology (as shown in Fig 3.1), with the set of available wavelengths on each fiber. Each link in the physical network links is bi-directional, which is implemented by a pair of uni-directional optical fibers. For example, Fig 3.1 shows a transparent optical network topology with 6 nodes and 8 bi-directional physical links. We are also given a set of scheduled lightpath demands, with the source, destination, start and end time specified for each demand (as shown in Fig. 3.2). We assume that the number of wavelengths is sufficient for accommodating all the demands.

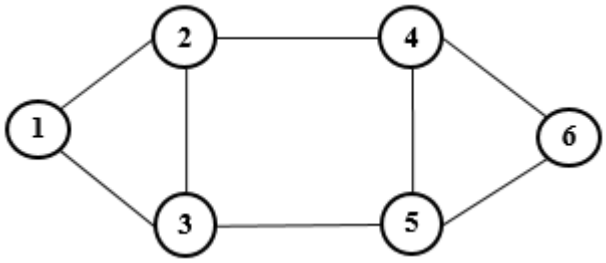
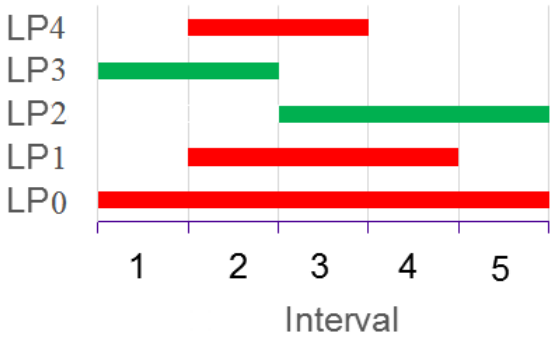


Fig. 3.1: an example of physical network topology

S	D
1	3
2	1
2	4
5	6
3	5

(a)



(b)

Fig. 3.2: lightpath demands and intervals for each demand

3.2.1 LAR and IAR in Scheduled Networks

In this section, we discuss how to calculate the LAR and IAR values for scheduled lightpaths, which is slightly different from the calculations for static lightpaths discussed in Sec. 2.2.

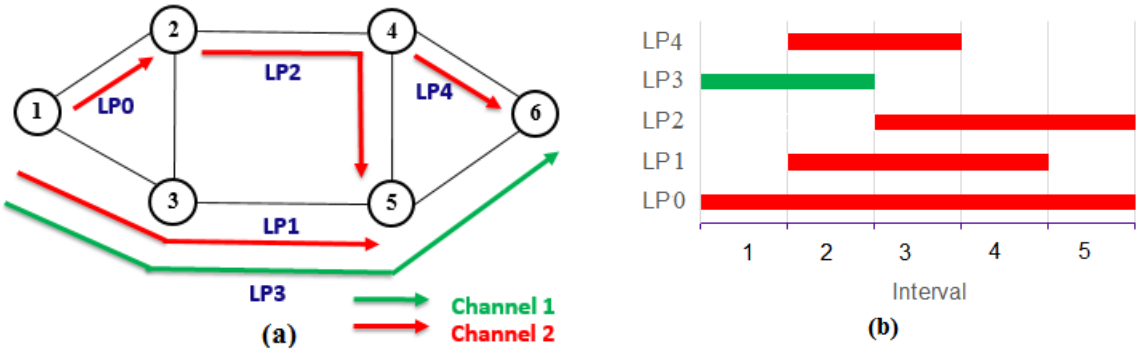


Fig. 3.3: an example of RWA and interval assignment

Fig. 3.3(a) shows five lightpath demands with their assigned routes and channels. Fig. 3.3(b) displays the starting time and ending time of each lightpath request. We have introduced the calculation methods of $maxLAR$ and $maxIAR$ in static networks. In the scheduled traffic model, a lightpath p that shares a common link with lightpath q is not automatically in the attack group of q. We have $p \in AG_q$ only if an additional condition is satisfied that p and q overlap in time. A similar condition must also be satisfied for the in-band attack group, if two lightpaths p and q share a common node and wavelength. Also, unlike static lightpaths, the attack group for each lightpath is not constant and may change with time as new lightpaths become active. Based on this, the LAR (IAR) for each lightpath in Fig 3.3, during differnet intervals, is given in Table 3.1 (Table 3.2).

TABLE 3.1: the value of LAR of each lightpath during each interval

	LP0	LP1	LP2	LP3	LP4
Interval 1	1	0	0	1	0
Interval 2	1	2	0	2	1
Interval 3	1	1	1	0	1
Interval 4	1	1	1	0	1
Interval 5	1	0	1	0	0

For example, in Interval 1, only LP0 and LP3 are active, but they do not traverse any common link, so the values of LAR for LP0 and LP3 in Interval 1 are both 1. For the other lightpaths (LP1, LP2 and LP4) which are not active during interval 1, their values of LAR are set to be 0. In interval 2, because LP1 and LP3 are both active and sharing the common links (1-3) and (3-5), hence LAR_{LP1} and LAR_{LP3} in interval 2 is 1+1=2.

TABLE 3.2: the value of IAR of each lightpath during each interval

	LP0	LP1	LP2	LP3	LP4
Interval 1	1	0	0	1	0
Interval 2	2	2	0	1	1
Interval 3	3	3	3	0	2
Interval 4	3	3	3	0	2
Interval 5	2	0	2	0	0

As described in Table 3.2, according to the definition of in-band Attack Radius, for interval 1, although LP0 and LP3 are both active and sharing the same node 1, they are not assigned the same wavelength, therefore the IAR values of LP0 and LP3

in interval 1 are both 1, while other lightpaths which are not active during interval 1 are set to be 0. In interval 2, LP0, LP1, LP3 and LP4 are all active, but only LP0 and LP1 share the same node and are on the same wavelength, so $\text{IAR}_{LP0} = \text{IAR}_{LP1}$ =2. The IAR values for each lightpath can be calculated in a similar fashion, for each interval.

3.3 Proposed ILP Formulation

3.3.1 ILP Formulation : ILP_AR1

In this section, we formulate the routing sub-problem as an ILP with different objectives combining LAR and IAR to solve the security-aware scheduled RWA problem.

Input Parameters

$G(N, E)$: Physical network topology

N: Set of nodes.

E: Set of edges.

W: Set of channels (wavelengths) on a fiber.

M: Number of intervals in the network.

$hmax$: An upper bound on the number of hops of a lightpath.

P: set of lightpaths.

s_p, d_p: source, destination of lightpath p.

Input Parameters to be pre-calculated

$$t_{p,q} \geq a_{p,m} \cdot a_{q,m} \quad \forall p, q \in P, \forall m = 1, 2, ..., M \tag{1}$$

$$t_{p,q} \leq \sum_{m} a_{p,m} \cdot a_{q,m} \quad \forall p, q \in P \tag{2}$$

Constraints (1)-(2) are used to calculate whether or not two different lightpaths are time-disjoint or not. If $t_{p,q} = 1$, it means that lightpath p and q are not time-disjoint, i.e. there is at least one time interval (possibly more) during which both lightpaths are active. The $t_{p,q}$ values are pre-calculated and given as input to the ILP.

Variables

$$a_{p,m} = \begin{cases} 1 & \text{if lightpath } p \text{ is active during interval } m, \\ 0 & \text{otherwise.} \end{cases}$$

$$t_{p,q} = \begin{cases} 1 & \text{if lightpaths } p \text{ and } q \text{ are both active during one or more} \\ & \text{common intervals,} \\ 0 & \text{otherwise.} \end{cases}$$

$$x_{p,e} = \begin{cases} 1 & \text{if lightpath } p \text{ uses edge } e \text{ ,} \\ 0 & \text{otherwise.} \end{cases}$$

$$y_{p,i} = \begin{cases} 1 & \text{if lightpath } p \text{ passes through node } i, \\ 0 & \text{otherwise.} \end{cases}$$

$$\omega_{p,k} = \begin{cases} 1 & \text{if lightpath } p \text{ is assigned channel } k, \\ 0 & \text{otherwise.} \end{cases}$$

$$\alpha_{p,q} = \begin{cases} 1 & \text{if lightpaths } p \text{ and } q \text{ share at least one common edge,} \\ 0 & \text{otherwise.} \end{cases}$$

$$\alpha^{e}_{p,q} = \begin{cases} 1 & \text{if lightpaths } p \text{ and } q \text{ share a common edge } e, \\ 0 & \text{otherwise.} \end{cases}$$

$$\beta_{p,q} = \begin{cases} 1 & \text{if lightpaths } p \text{ and } q \text{ share at least one common node} \\ 0 & \text{otherwise.} \end{cases}$$

$$\beta^{i}_{p,q} = \begin{cases} 1 & \text{if lightpaths } p \text{ and } q \text{ share a common node } i, \\ 0 & \text{otherwise.} \end{cases}$$

$$\gamma_{p,q} = \begin{cases} 1 & \text{if lightpaths } p \text{ and } q \text{ use the same channel,} \\ 0 & \text{otherwise.} \end{cases}$$

$$\gamma_{p,q}^{k} = \begin{cases} 1 & \text{if lightpaths } p \text{ and } q \text{ both use channel } k, \\ 0 & \text{otherwise.} \end{cases}$$

$$\delta_{p,q} = \begin{cases} 1 & \text{if lightpaths } p \text{ and } q \text{ use the same channel and have at least} \\ & \text{one common node,} \\ 0 & \text{otherwise.} \end{cases}$$

Notation Used

p,q: Used to identify an indivdual lightpath, $p,q \in P$.

e: Used to identify an a physical link (edge) of the network, $e \in E$.

i,j: Used to identify a specific node in the network, $i,j \in N$.

k: Used to identify a specific channel on a fiber, $k \in W$.

m: Used to identify a specific time interval number, m = 1,2,3, ... M.

(1) Objective functions

Objective 1: Minimize

$$maxAR1 \tag{3}$$

maxAR1 is the upper bound of $AR1_{p,m} = IAR_{p,m} + LAR_{p,m}$, for any lightpath p in any interval m of the network.

Subject to the following constraints:

1. Flow Conservation Constraints

$$\sum_{e:i\to j\in E} x_{p,e} - \sum_{e:j\to i\in E} x_{p,e} = \begin{cases} 1 & \text{if } i = s_p \\ -1 & \text{if } i = d_p \quad \forall i \in N, \forall p \in P \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

$$\sum_{e:i\to j\in E} x_{p,e} \leq 1 \quad \forall i \in N, \forall p \in P \tag{5}$$

Constraints (4) and (5) ensure flow conservation of lightpaths. Constraint (4) finds a valid path over the physical topology, for each lightpath. Constraint (5) ensures that the path does not contain any loops.

2. Wavelength continuity constraint

$$\sum_{k} \omega_{p,k} = 1 \quad \forall p \in P \tag{6}$$

Constraints (6) ensures that a lightpath must be assigned the same wavelength on each link it passes without wavelength conversion.

3. Defining $\alpha_{p,q}$ (link sharing)

$$x_{p,e} + x_{q,e} - \alpha^e_{p,q} \leq 1 \quad \forall p, q \in P, p \neq q, \forall e \in E \tag{7}$$

$$x_{p,e} \geq \alpha^e_{p,q} \quad \forall p, q \in P, p \neq q, \forall e \in E \tag{8}$$

$$x_{q,e} \geq \alpha^e_{p,q} \quad \forall p, q \in P, p \neq q, \forall e \in E \tag{9}$$

$$\alpha_{p,q} \geq \alpha^e_{p,q} \quad \forall p, q \in P, p \neq q, \forall e \in E \tag{10}$$

$$\alpha_{p,q} \leq \sum_{e \in E} \alpha_{p,q}^{e} \quad \forall p, q \in P, p \neq q \tag{11}$$

Constraints (7)-(9) sets the value of $\alpha_{p,q}^{e} = 1$ if lightpath p and lightpath q are both routed over link e. Constraints (10) and (11) determine if two lightpaths p and q share at least one (possibly more) common link(s), and if so, set $\alpha_{p,q} = 1$.

4. Node usage constraint

$$y_{p,i} = \sum_{e:i \to j \in E} x_{p,e} \quad \forall p \in P, \forall i \in N, i \neq d_p \tag{12}$$

$$y_{p,d_p} = 1 \quad \forall p \in P \tag{13}$$

Constraint (12) determines if a lightpath p traverses a specific node i in its selected route. If so the value of $y_{p,i}$ is set to 1. Constraint (13) states that the destination node of a lightpath must be on the selected route.

5. Defining $\beta_{p,q}$ (node sharing)

$$y_{p,i} + y_{q,i} - \beta_{p,q}^{i} \leq 1 \quad \forall p, q \in P, p \neq q, \forall i \in N \tag{14}$$

$$y_{p,i} \geq \beta_{p,q}^{i} \quad \forall p, q \in P, p \neq q, \forall i \in N \tag{15}$$

$$y_{q,i} \geq \beta_{p,q}^{i} \quad \forall p, q \in P, p \neq q, \forall i \in N \tag{16}$$

$$\beta_{p,q} \geq \beta_{p,q}^{i} \quad \forall p, q \in P, p \neq q, \forall i \in N \tag{17}$$

$$\beta_{p,q} \leq \sum_{i \in N} \beta_{p,q}^{i} \quad \forall p, q \in P, p \neq q \tag{18}$$

Constraint (14)-(18) are very similar to constraint (7)-(11) and are used to determine if two lightpaths p and lightpath q pass through at least one (possibly more) common node(s). If so these constraints are used to set $\beta_{p,q}$=1.

6. Defining $\gamma_{p,q}$ (channel sharing)

$$\omega_{p,k} + \omega_{q,k} - \gamma_{p,q}^{k} \leq 1 \quad \forall p, q \in P, p \neq q, \forall k \in W \tag{19}$$

$$\omega_{p,k} \geq \gamma_{p,q}^{k} \quad \forall p, q \in P, p \neq q, \forall k \in W \tag{20}$$

$$\omega_{q,k} \geq \gamma_{p,q}^{k} \quad \forall p, q \in P, p \neq q, \forall k \in W \tag{21}$$

$$\gamma_{p,q} = \sum_{k} \gamma_{p,q}^{k} \quad \forall p, q \in P, p \neq q \tag{22}$$

Similarly, constraint (19)-(22) are applied to define channel-sharing and set the value of $\gamma_{p,q} = 1$, if lightpath p and lightpath q are assigned the same channel (or wavelength) k.

7. Defining $\delta_{p,q}$ (node-channel sharing)

$$\beta_{p,q} + \gamma_{p,q} - \delta_{p,q} \leq 1 \quad \forall p, q \in P, p \neq q \tag{23}$$

$$\beta_{p,q} \geq \delta_{p,q} \quad \forall p, q \in P, p \neq q \tag{24}$$

$$\gamma_{p,q} \geq \delta_{p,q} \quad \forall p, q \in P, p \neq q \tag{25}$$

Constraint (23)-(25) define node-channel sharing. If lightpath p and q pass through at least one common node (i.e. $\beta_{p,q} = 1$) and share the same channel (i.e. $\gamma_{p,q} = 1$), then we set $\delta_{p,q}$=1. The value of this variable determines if lightpath p might be in the attack group of lightpath q.

8. wavelength clash constraint

$$\alpha_{p,q} + \gamma_{p,q} + t_{p,q} \leq 2 \quad \forall p, q \in P, p \neq q \tag{26}$$

Constraint (26) ensures that if two or more lightpaths share a common fiber link, they cannot be assigned the same wavelength.

9. *LAR/IAR* of lightpath p (attack radius in interval m)

$$LAR_{p,m} = a_{p,m} \cdot (\sum_{q \in P, p \neq q} \alpha_{p,q} \cdot a_{q,m} + 1) \quad \forall p \in P, \forall m = 1, 2, ..., M \tag{27}$$

$$IAR_{p,m} = a_{p,m} \cdot (\sum_{q \in P, p \neq q} \delta_{p,q} \cdot a_{q,m} + 1) \quad \forall p \in P, \forall m = 1, 2, ..., M \tag{28}$$

Constraint (27) (constraint (28)) is used to calculate Lightpath Attack Radius (LAR) (In-band Attack Radius (IAR)) value for lightpath p during interval m. The goal is to keep this value as low as possible.

10. Total LAR and IAR of lightpath p (over all intervals)

$$LAR_p = \sum_{q \in P, p \neq q} \alpha_{p,q} \cdot t_{p,q} + 1 \quad \forall p \in P \tag{29}$$

$$IAR_p = \sum_{q \in P, p \neq q} \delta_{p,q} \cdot t_{p,q} + 1 \quad \forall p \in P \tag{30}$$

Constraint (29) (constraint (30)) defines the total Lightpath Attack Radius (LAR) (In-band Attack Radius (IAR)) value for lightpath p over all intervals.

11. *MaxAR1* in interval m

$$IAR_{p,m} + LAR_{p,m} \leq maxAR1 \quad \forall p \in P, \forall m = 1, 2, ..., M \tag{31}$$

Constraint (31) ensures that the total attack radius of any lightpath p during any given time interval m (i.e. $AR1_{p,m} = IAR_{p,m} + LAR_{p,m}$) is no greater than the *maxAR1*, which is the value being minimized.

12. Total *maxAR2* over all intervals

$$IAR_p + LAR_p \leq maxAR2 \quad \forall p \in P \tag{32}$$

Constraint (32) ensures that the total attack radius of any lightpath (over all intervals), *maxAR2*. This variable can be minimized (instead of *maxAR1*) as an alternative objective function

13. Hop Bound Constraints

$$\sum_{e: i \to j \in E} x_{p,e} \leq hmax \quad \forall p \in P \tag{33}$$

Constraint (33) ensures that the maximum number of hops (i.e. path length) of a lightpath does not exceed a pre-specified upper limit *hmax*.

By solving the ILP formulation above, we can get the optimal routing scheme with regard to proposed objective function.

3.4 Alternative objective functions

In this section, we consider some alternative objective functions that can be used, with the same set of constraints as discussed in the previous section.

3.4.1 ILP Formulation : ILP_AR2

This formulation is similar to ILP_AR1 presented in the previous section, with the following modification.

Objective function is modified as follows:

Objective 2: Minimize

$$maxAR2 \tag{34}$$

maxAR2 is the upper bound of $AR2_p = IAR_p + LAR_p$, for all lightpath $p \in P$. So this objective minimizes the maximum Attack Radius (*AR2* value) for any lightpath.

All other variables and constraints are identical to ILP_AR1.

3.4.2 ILP Formulation : ILP_SUM_AR2

The ILP formulation regarding ILP_SUM_AR2 is also similar to ILP_AR1 presented in the previous section, with the following modification.

Objective function is modified as follows:

Objective 3: Minimize

$$\sum_{p \in P} LAR_p + IAR_p \tag{35}$$

Objective 3 tries to minimize the total attack radius (combining LAR and IAR)

of all the lightpath over all intervals. It is the summation of *AR2* of each lightpath.

All other variables and constraints are identical to ILP_AR1.

3.4.3 ILP Formulation : ILP_SUM_AR1

The ILP formulation with regard to ILP_SUM_AR1 is also similar to ILP_AR1 presented in the previous section, with the following modification.

Objective function is modified as follows:

Objective 4: Minimize

$$\sum_{m} \sum_{p \in P} LAR_{p,m} + IAR_{p,m} \tag{36}$$

Objective 4 minimizes the total attack radius ($AR1_{p,m} = IAR_{p,m} + LAR_{p,m}$) over all lightpaths and all intervals.

All other variables and constraints are identical to ILP_AR1.

3.4.4 ILP Formulation : ILP_SPATH

This formulation does not consider attacks but simply minimizes the total path length of all lightpaths. So, this is a traditional attack-unaware ILP for RWA.

Objective function is modified as follows:

Objective 5: Minimize

$$\sum_{p \in P} \sum_{e \in E} x_{p,e} \tag{37}$$

All other variables and constraints are identical to ILP_AR1.

3.4.5 Summary of ILP Objectives

In summary, there are five objective functions proposed in this chapter, as presented below:

TABLE 3.3: Proposed ILP formulations and objectives

ID	ILP Formulation Name	Objectives
Objective 1	ILP_AR1	Minimize $maxAR_1$
Objective 2	ILP_AR2	Minimize $maxAR_2$
Objective 3	ILP_SUM_AR2	Minimize $\sum_p LAR_p + IAR_p$
Objective 4	ILP_SUM_AR1	Minimize $\sum_m \sum_p LAR_{p,m}+IAR_{p,m}$
Objective 5	ILP_SPATH	Minimize $\sum_p \sum_e x_{p,e}$

Objective 1 to Objective 4 are our proposed attack-aware objectives in order to minimize the attack radius of a network, while Objective 5 is a traditional attack-unaware approach aimed at minimizing the total physical links used. Then we will create C programs to implement all the five ILP formulations and run different simulation cases in CPLEX Optimization Studio 12.6. The running results will be presented in the next chapter.

CHAPTER IV

Experimental Results

In this chapter, we present different simulation cases and the results of RWA problem from our proposed approach.We also compare the objective values obtained using our approach ILP_AR1, ILP_AR2, ILP_SUM_AR2 and ILP_SUM_AR1 with the corresponding values obtained using a traditional attack-unaware RWA scheme.

Unlike existing attack-aware RWA techniques, we consider the scheduled traffic model, which means we consider the time dimension in our proposed ILP formulation, Furthermore, traditional static RWA can be treated as a special case of our approach (by setting a single time interval for all the lightpath demands). Finally, the objectives in our ILP formulation takes into account both in-band attack radius (IAR) and lightpath attack radius (LAR), so it can handle multiple types of attacks.

4.1 Experimental Setup

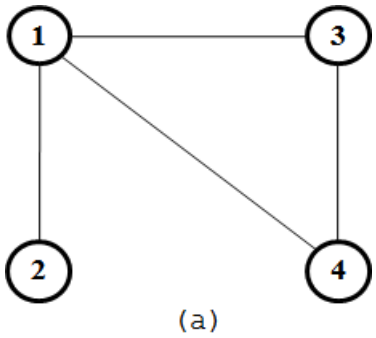
We test the proposed ILP formulation with different network topologies and lightpath demand sets. For each topology and demand set size, we considered 3 levels of traffic load - low, medium and high, and for each case, we used 5 randomly generated demand sets. So, the results reported in this chapter are the average of 5 simulation runs.

- Simulations of different network topologies
  - 20 demands for 10-node network
  - 20 demands for 14-node network
  - 20 demands for 20-node network

- Simulations of different demand size
  - 14-node network with 10 demands
  - 14-node network with 20 demands
  - 14-node network with 40 demands

4.1.1 Physical Topologies

We have considered 3 well-known physical topologies: a 10-node network with 22 bi-directional links[32], a 14-node network with 21 bi-directional links[31] and a 20-node network with 31 bi-directional links[30]. We also assume that each fiber (uni-directional) can accommodate 16 channels (wavelengths). Each physical topology is saved in a text file, following the format in Fig. 4.1.



(a)

1	2
1	3
1	4
2	1
3	1
3	4
4	1
4	3

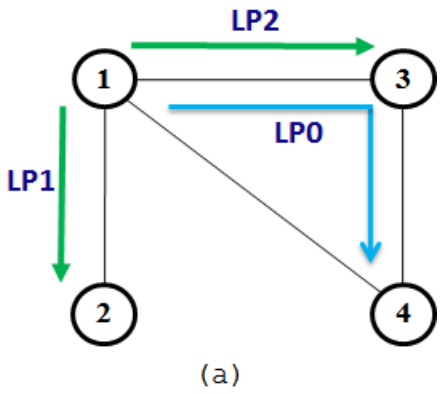
(b)

Fig. 4.1: an example of network topology and its physical-link storage format

Fig 4.1(a) shows a simple network topology with 4 nodes and 4 bi-directional links (8 uni-directional fibers). Each row in Fig.4.1(b) represents a uni-directional fiber link specified by the starting and ending node of the link.

4.1.2 Lightpath Demand Sets

A set of scheduled lightpath demands is specified as a m*4 matrix, where m is the demand set size, i.e. the number of lightpaths in the demand set. Each row represents a single lightpath (p) and specifies its source (s_p), destination (d_p), start time(st_p) and end of window(et_p) respectively. Each demand set is stored in a separate file.



(a)

1	4	3	10
1	2	5	23
1	3	17	19

(b)

Fig. 4.2: an example of (a)RWA scheme and (b)its lightpath demand storage format

Fig 4.2(b) shows a set of 3 lightpath demands (Row 1: LP0, Row 2: LP1, Row 3: LP2). For example, (LP0: 1 4 3 10) means LP0 is a lightpath demand from node 1 to node 4 and it is active during interval 3 to interval 10. A possible routing for the demand set of Fig. 4.2(b) is shown in Fig. 4.2(a).

In addition, we classify the lightpath demand sets into three categories according to the time span of each demand. The longer the duration of a demand, the more resources it uses. Also, if a demand set consists of longer demands, it is likely that that there will be more overlap (in time) among different demands leading to a larger attack group. Based on this observation, we define the following three classes of demand sets:

- Low demand overlap (LDO): For a LDO demand set, the duration of each demand is between 1 and 10 intervals.

$$1 \leq (last\ interval - first\ interval) \leq 10$$

- Medium demand overlap (MDO): For a MDO demand set, the duration of each demand is between 1 and 24 intervals.

$$1 \leq (last\ interval - first\ interval) \leq 24$$

- High demand overlap (HDO): For a HDO demand set, the duration of each

demand is between 10 and 24 intervals.

$$10 \leq (last\ interval - first\ interval) \leq 24$$

Next, we will run the ILP formulation with the objectives of our approach ILP_AR1, ILP_AR2, ILP_SUM_AR2, ILP_SUM_AR1 and the shortest path ILP_SPATH for all the parts of simulations presented above.

4.2 Results of Experiment

In this section, we will run our ILP formulation with the 5 different objective functions presented in Chapter 3, denoted as ILP_AR1 for Objective 1, ILP_AR2 for Objective 2, ILP_SUM_AR2 for Objective 3, ILP_SUM_AR1 for Objective 4 and ILP_SPATH for Objective 5. CPLEX ver. 12.6 is used for solving linear programming problems. For each network topology, the lightpath demands are randomly generated based on the demand size traffic load (LDO, MDO, HDO).

We compare our proposed algorithm with a traditional security-unaware algorithm (denoted as ILP_SPATH), which aims at minimizing the total path length for the set of lightpaths and does not consider their vulnerability to attacks.

4.2.1 Comparison of objective values for different networks

Table 4.1 compares the value of Objective 1 (*maxAR1*) for the proposed approach and the attack-unaware approach for different network sizes and traffic loads. Each value in the table below is the average of 5 test cases.

TABLE 4.1: Comparison of Objective 1 for 20 Demands

Objective function: *maxAR1*						
	LDO		MDO		HDO	
No. of Nodes	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach
10	2	4	2	5	3	6
14	3	4	3	5	5	6
20	3	5	4	7	7	9

We can see from Table 4.1 that the values of maxAR1 obtained using our proposed algorithm (ILP_AR1) are consistently lower than those obtained using the traditional attack-unaware algorithm (ILP_SPATH). The achieved reductions range from 16.7% - 60%. Comparisons for Objectives 2, 3, and 4 are presented in Table 4.2, 4.3 and 4.4 respectively.

TABLE 4.2: Comparison of Objective 2 for 20 Demands

Objective function: *maxAR2*						
	LDO		MDO		HDO	
No. of Nodes	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach
10	2	4	2	6	3	6
14	3	4	5	6	5	7
20	3	6	5	7	8	10

TABLE 4.3: Comparison of Objective 3 for 20 Demands

Objective function: $\sum_p \boldsymbol{LAR}_p + \boldsymbol{IAR}_p$						
	LDO		MDO		HDO	
No. of Nodes	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach
10	40	50	40	60	47	80
14	41	54	48	79	56	93
20	43	62	53	82	64	97

TABLE 4.4: Comparison of Objective 4 for 20 Demands

Objective function: $\sum_m \sum_p \boldsymbol{LAR}_{p,m}+\boldsymbol{IAR}_{p,m}$						
	LDO		MDO		HDO	
No. of Nodes	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach
10	210	253	304	394	689	965
14	190	230	448	571	823	995
20	208	254	450	618	850	1169

Table 4.2 - Table 4.4 clearly demonstrate that our proposed approach results in smaller values of attack radius for all cases. The average reductions range from 16.7% (for Objective 2) to 66.7% (for Objective 2).

Fig. 4.3 - Fig. 4.5 show the comparison results for Objective 4 for different levels of demand overlap. The network size is shown along the x-axis and the value of attack radius on y-axis. The improvements range from 17.0% (for LDO case) to 28.6% (for HDO case). For each network, the objective value increases with the level of demand overlap (from LDO to HDO), indicating that vulnerability to attacks increase with

more interactions among lightpaths. The results for the other objectives follow a similar pattern.

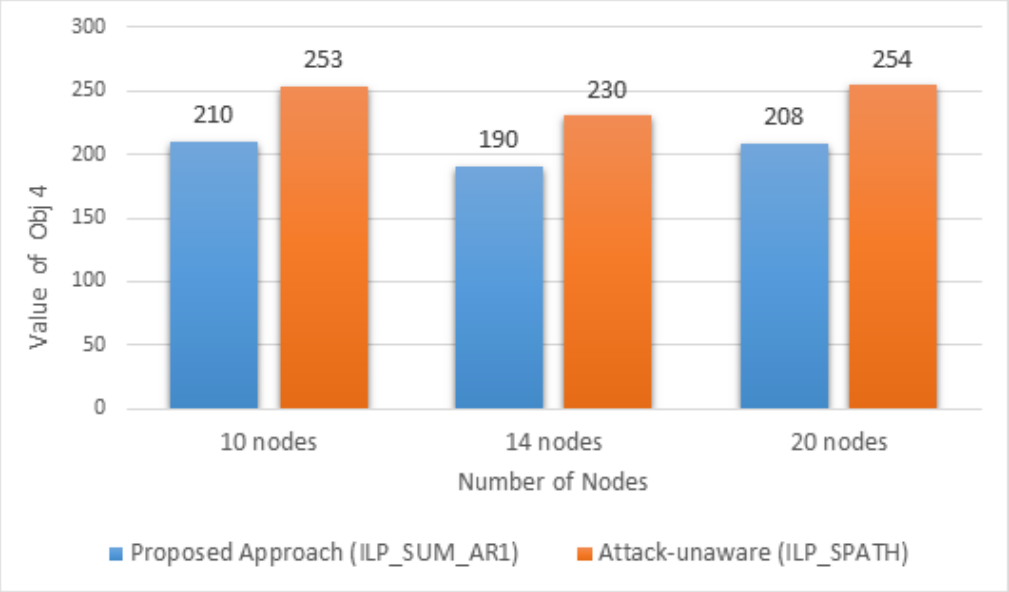


Fig. 4.3: Results of Objective 4 for LDO with 20 demands

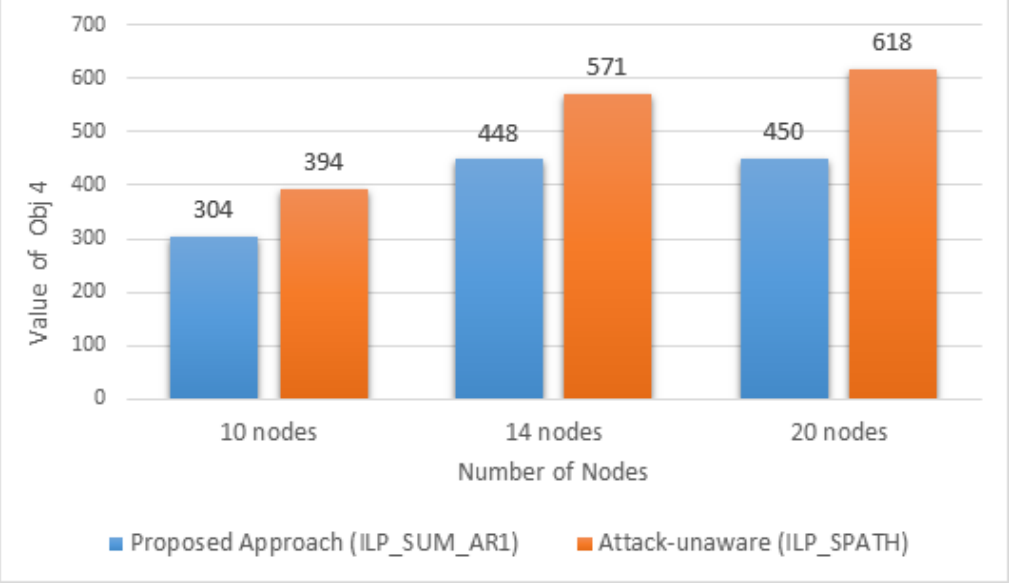


Fig. 4.4: Results of Objective 4 for MDO with 20 demands

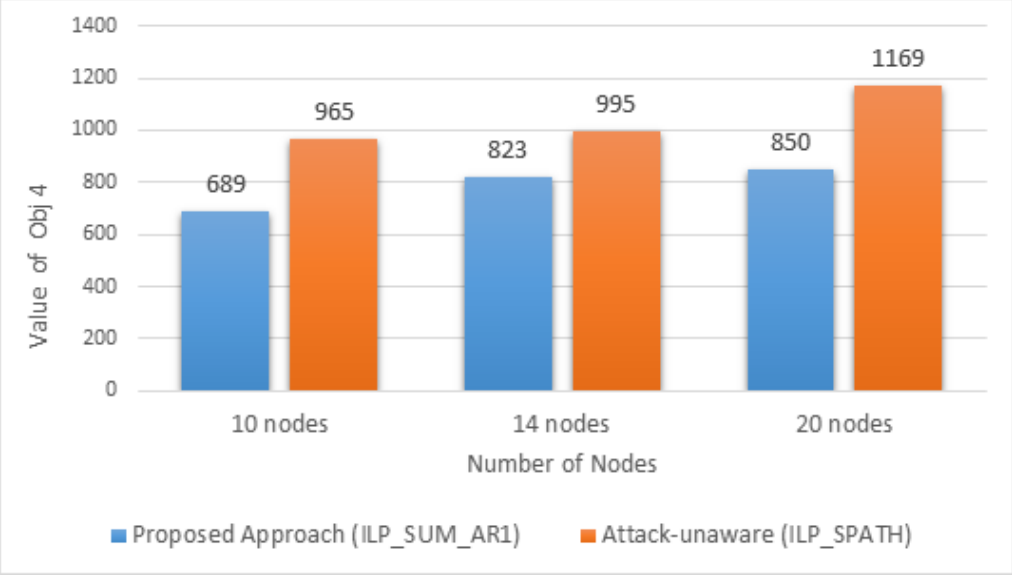


Fig. 4.5: Results of Objective 4 for HDO with 20 demands

4.2.2 Comparison of objective values of various demand sizes

Table 4.5 - Table 4.8 show how each objective value varies with the demand size for the 14-node network topology.

TABLE 4.5: Comparison of Objective 1 values with different demand sizes for 14-node Network

Objective function: *maxAR1*						
	LDO		MDO		HDO	
No. of Demands	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach
10	2	4	2	5	2	6
20	3	4	3	5	5	6
40	5	6	6	10	7	12

TABLE 4.6: Comparison of Objective 2 values with different demand sizes for 14-node Network

Objective function: *maxAR2*						
	LDO		MDO		HDO	
No. of Demands	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach
10	2	4	2	4	2	6
20	3	4	5	6	5	7
40	5	7	7	13	7	12

TABLE 4.7: Comparison of Objective 3 values with different demand sizes for 14-node Network

Objective function: $\sum_p \boldsymbol{LAR}_p + \boldsymbol{IAR}_p$						
	LDO		MDO		HDO	
No. of Demands	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach
10	20	38	25	46	31	54
20	41	54	48	79	56	93
40	117	146	157	247	194	265

TABLE 4.8: Comparison of Objective 4 values with different demand sizes for 14-node Network

Objective function: $\sum_m \sum_p \boldsymbol{LAR}_{p,m}+\boldsymbol{IAR}_{p,m}$						
	LDO		MDO		HDO	
No. of Demands	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach	Proposed Approach	Attack-unaware Approach
10	96	162	132	166	278	460
20	190	230	448	571	823	995
40	507	601	1062	1317	2323	2867

As expected the objective values increase steadily with demand size for all networks for both the proposed approach and the attack-unaware approach. The average improvements obtained using the proposed approach range from 16.7% to 66.7%.

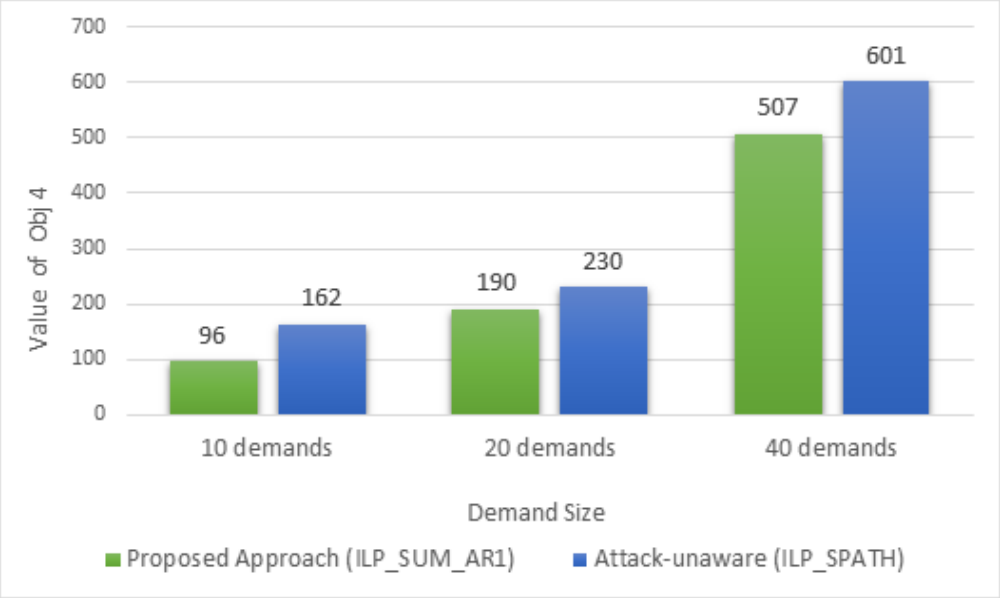


Fig. 4.6: Variation of Objective 4 with demand size in 14-node network for LDO

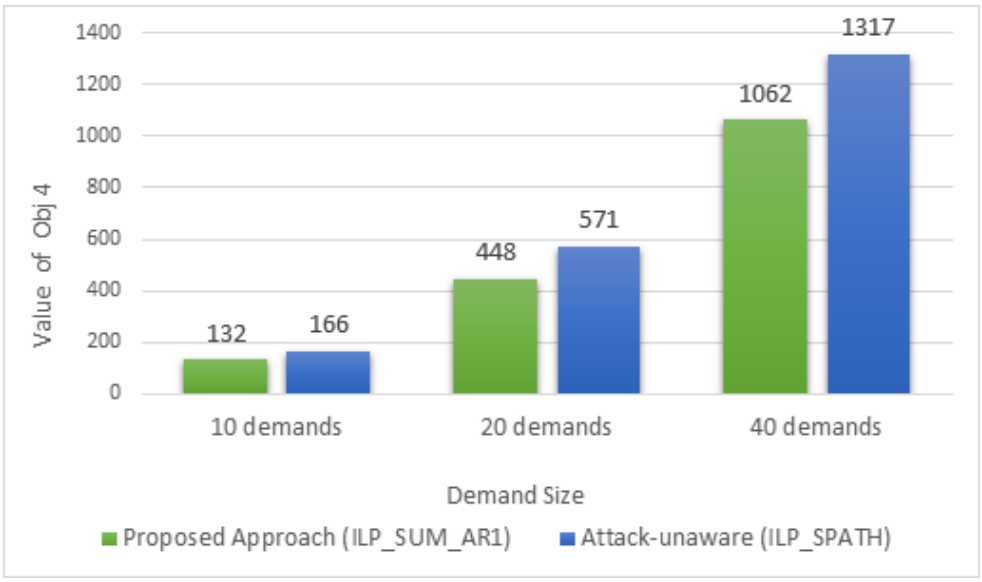


Fig. 4.7: Variation of Objective 4 with demand size in 14-node network for MDO

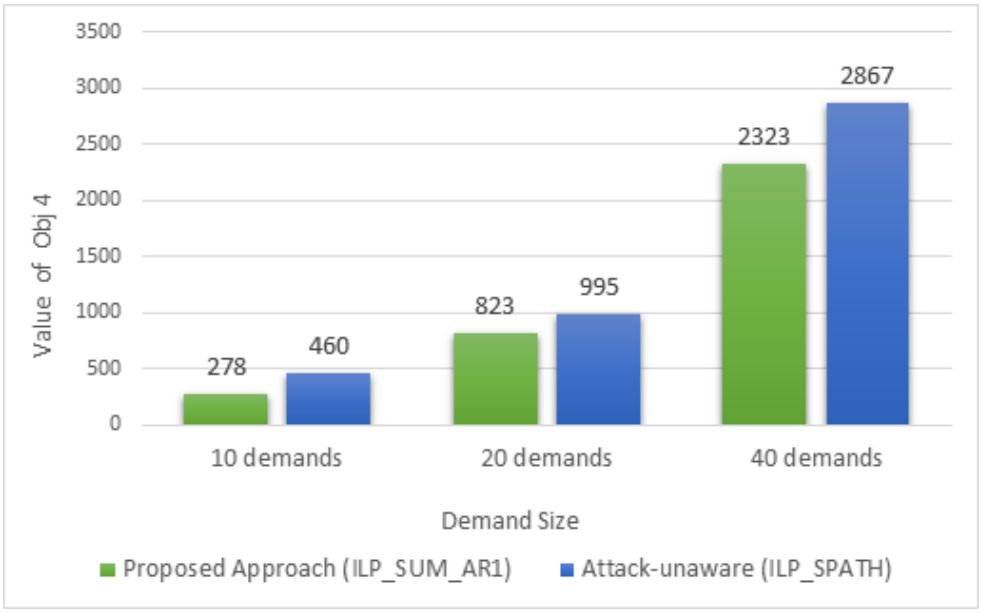


Fig. 4.8: Variation of Objective 4 with demand size in 14-node network for HDO

Fig. 4.6 - Fig. 4.8 show how the values for Objective 4 vary with demand size, in a 14-node network, for LDO, MDO and HDO traffic respectively. The demand set size is shown along the x-axis and the value of attack radius on y-axis. The improvements

range from 15.6% (for LDO case) to 40.7% (for LDO case). For each network, the objective value increases with the size of the demand set. The results for the other objectives follow a similar pattern.

4.2.3 Comparison of path lengths

Table 4.9 - Table 4.11 compare the average path length of a lightpath using the different approaches for LDO, MDO and HDO traffic respectively.

TABLE 4.9: Comparison of average path lengths for LDO traffic

	Average path length obtained using				
	Proposed approach				**Attack-unaware**
No. of Nodes	Objective 1	Objective 2	Objective 3	Objective 4	ILP_SPATH
10	2.15	2.0	2.2	2.3	1.6
14	2.55	2.8	3.35	3.35	1.95
20	4.05	3.65	4.35	3.9	2.9

TABLE 4.10: Comparison of average path lengths for MDO traffic

	Average path length obtained using				
	Proposed approach				**Attack-unaware**
No. of Nodes	Objective 1	Objective 2	Objective 3	Objective 4	ILP_SPATH
10	2.2	2.1	2.25	2.35	1.55
14	3	2.8	3	3.45	1.95
20	4.3	3.8	4.2	4.25	2.95

TABLE 4.11: Comparison of average path lengths for HDO traffic

	Average path length obtained using				
	Proposed approach				**Attack-unaware**
No. of Nodes	Objective 1	Objective 2	Objective 3	Objective 4	ILP_SPATH
10	2.35	2.35	2.15	2.05	1.6
14	2.45	2.4	2.7	2.85	1.95
20	3.4	3.5	3.85	3.7	2.75

Based on Tables 4.9 - 4.11, we can see that the attack-unaware algorithm (ILP_SPATH) results in shorter paths on average. This is because it always selects the shortest path, even if the route is heavily congested. The attack-aware approaches on the other hand try to distribute the load so that potential interactions among lightpaths is minimized. This may result in selecting longer, but less congested, paths for some lightpaths. However, considering the security issue, the increase of path lengths is still acceptable.

CHAPTER V

Conclusion and Future Work

5.1 Conclusion

Due to the increasing high data rates and the vulnerabilities in transparent optical networks, security issues related to transparency has become of great importance. There are many types of physical-layer attacks such as gain competition, inter-channel crosstalk and in-band crosstalk. All of these can lead to serious damage of network such as user data loss, performance degradation, etc. In order to minimize the disruption due to these attacks, various approaches have been proposed for attack detection and localization. Our proposed approach does not need some specialized detection devices, instead, it relies on the application of ILP formulation to solve the routing and wavelength assignment (RWA) problem and minimize the overall attack radius, thus reducing the potential threat of attacks. Unlike previous work in this area, we address the attack-aware RWA problem for the scheduled traffic model, which has not been considered before. We also take into account both in-band and out-of-band attacks. In order to evaluate the performance of our approach, we use various network topologies, lightpath demands and compare our results with their corresponding values obtained from using a traditional shortest path algorithm. The results indicate that the proposed approach reduces the attack radius at the cost of increasing the path length of the demands, compared to security-unaware approaches.

5.2 Future Work

In this thesis, we have considered the security-aware RWA problems for the *fixed window* scheduled traffic model, which means the starting time and ending time of a lightpath demand is given in advance. In the future, this can be extended to also consider the *sliding* scheduled traffic model. In sliding scheduled traffic model, the starting time and ending time of a demand is not fixed, instead, the demand holding time τ is specified along with a larger time window when the demand can be allocated. This gives additional flexibility to the ILP, which must determine the start time of each demand in addition to performing RWA.

It is also possible to consider faults and incorporate fault management techniques such as path protection and restoration into the ILP. For larger networks, with hundreds of demands, it may be necessary to develop fast heuristic algorithms, which can generate good solutions in a reasonable time.

REFERENCES

[1] Skorin-Kapov, Nina. "Attack-aware planning and optimization in transparent optical networks." Asia Communications and Photonics Conference and Exhibition. International Society for Optics and Photonics, 2010.

[2] Furdek, Marija, Nina Skorin-Kapov, and Maa Grbac. "Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation." Journal of Optical Communications and Networking 2.11 (2010): 1000-1009.

[3] Skorin-Kapov, Nina, Jiajia Chen, and Lena Wosinska. "A new approach to optical networks security: attack-aware routing and wavelength assignment."Networking, IEEE/ACM Transactions on 18.3 (2010): 750-760.

[4] Rejeb, Ridha, Mark S. Leeson, and Roger J. Green. "Fault and attack management in all-optical networks." Communications Magazine, IEEE 44.11 (2006): 79-86.

[5] Mdard, Muriel, Stephen R. Chinn, and Poompat Saengudomlert. "Attack detection in all-optical networks." Optical Fiber Communication Conference and Exhibit, 1998. OFC'98., Technical Digest. IEEE, 1998.

[6] Ramamurthy, Byrav, et al. "Transparent vs. opaque vs. translucent wavelength-routed optical networks." (1999).

[7] http://mstar.unex.es/index.php?option=com_content&view=article&id=53&Itemid=55

[8] Jaekel, Arunita, and Ying Chen. "Resource provisioning for survivable WDM

networks under a sliding scheduled traffic model." Optical Switching and Networking 6.1 (2009): 44-54.

[9] Furdek, Marija, Nina Skorin-Kapov, and Maa Grbac. "Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation." Journal of Optical Communications and Networking 2.11 (2010): 1000-1009.

[10] Zhu, Keyao, and Biswanath Mukherjee. "A review of traffic grooming in WDM optical networks: Architectures and challenges." Optical Networks Magazine 4.2 (2003): 55-64.

[11] Rejeb, Ridha, Mark S. Leeson, and Roger J. Green. "Fault and attack management in all-optical networks." Communications Magazine, IEEE 44.11 (2006): 79-86.

[12] Ramamurthy, Byrav, et al. "Transparent vs. opaque vs. translucent wavelength-routed optical networks." (1999).

[13] https://en.wikipedia.org/wiki/Optical_networking

[14] Jean-Francouis Labourdette, Tellium, Opaque and Transparent Networking. Optical Networks Magazine, May//June 2003.

[15] Zhang Yinfa, Ren Shuai, Wang Peng, Li Ming, Wang Jingyu. Research Progress of Effect of High Power Signal on Optical Networks and Protection Technology [J]. Laser & Optoelectronics Progress, 2014, 51(10): 100003

[16] Zang, Hui, Jason P. Jue, and Biswanath Mukherjee. "A review of routing and wavelength assignment approaches for wavelength- routed optical WDM networks." Optical Networks Magazine 1.1 (2000): 47-60.

[17] Jue, Jason P. "Lightpath establishment in wavelength-routed WDM optical networks." Optical networks. Springer US, 2001. 99-122.

[18] M. Medard, S. R. Chinn, and P. Saengudomlert, Node Wrappers for QoS Monitoring in Transparent Optical Nodes, J. High Speed Networks, vol. 10, no. 4, 2001, pp. 247-68.

[19] Furdek, Marija, et al. "Gain competition in optical amplifiers: A case study."MIPRO, 2010 Proceedings of the 33rd International Convention. IEEE, 2010.

[20] Wu, Tao, and Arun K. Somani. "Cross-talk attack monitoring and localization in all-optical networks." IEEE/ACM Transactions on Networking (TON) 13.6 (2005): 1390-1401.

[21] Wang, Bin, et al. "Traffic grooming under a sliding scheduled traffic model in WDM optical networks." IEEE Workshop on Traffic Grooming in WDM Networks. 2004.

[22] https://en.wikipedia.org/wiki/Wavelength-division_multiplexing

[23] Figueira, Silvia, et al. "DWDM-RAM: Enabling grid services with dynamic optical networks." Cluster Computing and the Grid, 2004. CCGrid 2004. IEEE International Symposium on. IEEE, 2004.

[24] Mas, Carmen, Ioannis Tomkos, and Ozan K. Tonguz. "Failure location algorithm for transparent optical networks." Selected Areas in Communications, IEEE Journal on 23.8 (2005): 1508-1519.

[25] Zang, Hui, et al. "Dynamic lightpath establishment in wavelength routed WDM networks." Communications Magazine, IEEE 39.9 (2001): 100-108.

[26] Chu, Xiaowen, Bo Li, and Zhensheng Zhang. "A dynamic RWA algorithm in a wavelength-routed all-optical network with wavelength converters." INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. Vol. 3. IEEE, 2003.

[27] Chu, Xiaowen, Bo Li, and Zhensheng Zhang. "A dynamic RWA algorithm in a wavelength-routed all-optical network with wavelength converters." INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. Vol. 3. IEEE, 2003.

[28] Hill, G. R. "A wavelength routing approach to optical communications networks." INFOCOM'88. Networks: Evolution or Revolution, Proceedings. Seventh Annual Joint Conference of the IEEE Computer and Communcations Societies, IEEE. IEEE, 1988.

[29] Lee, Kuo-Chun, and Victor OK Li. "Routing and switching in a wavelength convertible optical network." INFOCOM'93. Proceedings. Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies. Networking: Foundation for the Future, IEEE. IEEE, 1993.

[30] Banerjee, Dhritiman, and Biswanath Mukherjee. "Wavelength-routed optical networks: Linear formulation, resource budgeting tradeoffs, and a reconfiguration study." IEEE/ACM Transactions on Networking (TON) 8.5 (2000): 598-607.

[31] Ramaswami, Rajiv, and Kumar N. Sivarajan. "Design of logical topologies for wavelength-routed optical networks." Selected Areas in Communications, IEEE Journal on 14.5 (1996): 840-851.

[32] Savvides, Andreas, Heemin Park, and Mani B. Srivastava. "The bits and flops of the n-hop multilateration primitive for node localization problems." Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications. ACM, 2002.

VITA AUCTORIS

NAME:	Hongbo Zhao
PLACE OF BIRTH:	Shenyang, Liaoning province, China
YEAR OF BIRTH:	1990
EDUCATION:	Northeastern University, B.Eng., Information Security, Shenyang, China, 2013
	University of Windsor, M.Sc in Computer Science, Windsor, Ontario, 2016