2016

Attack Aware RWA for Sliding Window Scheduled Traffic Model

Meenakshi Nizampatnam
University of Windsor

Attack Aware RWA for Sliding Window Scheduled Traffic Model

By

Meenakshi Nizampatnam

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 RWA for Sliding Window Scheduled Traffic Model

By

Meenakshi Nizampatnam

APPROVED BY:

Dr. Mitra Mirhassani, External Reader

Electrical & Computer Engineering

_____

Dr. Stephanos Mavromoustakos, Internal Reader

School of Computer Science

_____

Dr. Arunita Jaekel, Advisor

School of Computer Science

_____

May 2, 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 anyone's copyright nor violate any proprietary 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 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 (TONs), the data signals remain in the optical domain for the entire transmission path. The capability of handling high data rates and features like transparency makes TONs susceptible to several physical layer attacks. Hence, designing TONs with a capability of handling such high power jamming attacks is an important network security problem. In this work, we propose an integer linear program (ILP) formulation to control the propagation of these physical layer attacks in TONs, for the demands which need periodic bandwidth usage at certain predefined timings. There are two different approaches for handling these scheduled traffic demands, fixed window and sliding window. Our research deals with the sliding window scheduled traffic model, which is more flexible when compared with fixed window, as the start and end timings of the demand are unknown and they slide within a larger window setting. Hence, we present an ILP to handle the routing and wavelength assignment (RWA) problem for sliding window scheduled traffic model, with an objective to minimize the attack radius for all the commodities.

DEDICATION

To my loving Family

Husband: Ajay Reddy Bokka

Father: Sai Prasad Nizampatnam

Mother: Devi Bharathi Nizampatnam

Father-in-law: Padma Reddy Bokka

Mother-in-law: Karuna Bokka

ACKNOWLEDGEMENTS

I take this as an opportunity to express my sincere gratitude to my advisor, Dr. Arunita Jaekel, for her valuable guidance during my research. This work could not have been accomplished without her continuous support, advice and encouragement. I would like to thank my thesis committee members Dr. Stephanos Mavromoustakos and Dr. Mitra Mirhassani for their professional assistance and valuable time.

I would also like to thank Saja Al Mamoori, Karen Bourdeau and the entire computer science faculty members for all the support they provided throughout my years of study. I would like to express my deepest gratitude to my family for being a source of motivation and strength.

Meenakshi Nizampatnam

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AG - Attack Groups

DEMUX - Optical Demultiplexer

DHT - Demand Holding Time

EDFAs - Erbium-doped Fiber Amplifiers

IAG - In-band Attack Group

IAR - In-band sharing Attack Radius

IBM - International Business Management

ILOG CPLEX - Optimization Software Package

ILP - Integer Linear Programming

LAG - Link-share Attack Group

LANs - Local Area Networks

LAR - Link share Attack Radius

maxLAR - Maximum link-share attack radius

MUX - Optical Multiplexer

OA - Optical Amplifiers

OADM - Optical Add or Drop Multiplexer

OEO - Optical-Electronic-Optical

OSI - Open System Interconnect

OXC - Optical Cross Connect

PAR - Primary Attack Radius

RWA - Routing and Wavelength Assignment

SAR - Secondary Attack Radius

STM - Scheduled Traffic Model

Tb/s - Tera bits per second

TONs - Transparent Optical Networks

WDM - Wavelength Division Multiplexing

WWW - World Wide Web

1. INTRODUCTION

1.1 Overview

The Internet or the *World Wide Web* (WWW) has been growing at a tremendous rate and creating a revolution in the communication and business world, since its evolution. Because of the extensive applications and services of the internet, a rapid growth has been observed in the usage since 1995. By the end of 2015, almost 46.4% of the world population has become users of the internet [29]. In the recent years, an addition of versatile services and modern technologies increased the scope of the internet enormously. The introduction of the optical fiber technology in the telecommunication industry is one of the reasons for this massive growth. The very high bandwidth capacity of the optical fiber media over the metallic based communication system improved the capability to accommodate the future information traffic needs [11]. A record growth of 832.5% is observed between the years 2000 to 2015 regarding the worldwide usage of the internet [29].

The advantages associated with the optical fiber communication system gave them a long-term success in the telecommunication industry. The optical fiber systems allow signal transmissions over the longer distances with low transmission loss. The bandwidth capacities in the optical fiber networks are flexible to accommodate the growing bandwidth requirements. The technology advancements like the *Wavelength Division Multiplexing* (WDM) technology and the *Erbium-doped Fiber Amplifiers* (EDFAs) have improved the data transmission rates over a *terabit per second* (Tb/s). The fiber optic communication systems can be used effectively in all ranges of network

complexity, from simple *Local Area Networks* (LANs) to more complex and costly long-distance telephone trunking [11]. Hence, contemplating these numerous utilities of optical fiber networks, it is necessary to provide a secure and well-organized service to handle the future traffic necessities.

1.2 Motivation

One of the main advantages of the optical fiber networks over the copper cable networks is security. The dielectric nature of the optical fiber cable helps in establishing such secure connections. But, there are several vulnerabilities associated with various components in the optical fiber networks that create many crosstalks and nonlinearities. A trained attacker can take advantage of such vulnerabilities to create different types of attacks. Also, acquiring illegitimate access to the fiber optic cable can always turn into a security hazard [11] [24].

The following events are some of the recent attempts on attacking various optical fiber networks to obtain illegal access to the data signals.

1. In 2003, an illegal eavesdropping device was discovered hooked into Verizon's optical network [32].

2. In 2005, Kimberllie Witcher noted in his research paper published by the SANS Institute, that industry experts feel that it is as easy to hack a fiber optic cable as a copper cable [32].

3. On 22nd June 2015, Pierluigi Paganini has written an article about Kevin Mitnick hacking an optical fiber data cable just by using an optical fiber clip-on coupler [33].

All these events demonstrate the potential security threats associated with the optical fiber networks. The devices that are used for breaching these networks are getting more affordable day by day. In addition, various open source packet analyzer softwares like Wireshark (used by Kevin Mitnick [33]) are available for free in the market now a days [34]. Hence, it is important to model technologies that handle these attacks on optical fiber networks to provide a secure and robust service for the rapidly growing future traffic requirements.

1.3 Problem statement

Transparent Optical Networks (TONs) are capable of accommodating the rapidly growing future internet traffic requirements. Despite the difficulties associated with building and operating the TONs, they are advantageous in various aspects. TONs associated with WDM technology are capable of transferring huge amounts of data with very fast transmission rates. In addition, these networks guarantee a more flexible and scalable optical networks as they permit future-proofing in case of potential service upgrades and changes [13] [31]. That is, the TON's network transparency feature makes them insensitive towards the data rates and the protocol formats used by the lightpath service [24]. Also, these networks allow the service provider to offer a variety of different services to be used on the top of the same infrastructure [13].

Hence, in TONs, the routing and switching of traffic are performed without subjecting the signal to any modifications or examinations within the network [31]. Data signals in these networks are only re-amplified, but not re-shaped and re-timed (as in 3R regeneration) at the intermediate nodes. Thus, it is hard to find the changes in the modulation or intensity of the data signals that exceed the specified characteristics of the given network modulation format. Hence, a malicious signal that enters the TON can traverse through multiple nodes and links without undergoing any *Optical-Electronic-Optical* (OEO) conversions [24].

Thus, the uncontrolled and undetected propagation of malicious signals in the TONs can degrade the service and provide illegal access to the data signals. When combined with the WDM technology, even a slightest disruption in the TONs can cause a huge data loss. These disruptions can either be unintended component faults or intended attacks [24]. Figure 1.1 shows the differences between the faults and the attacks.

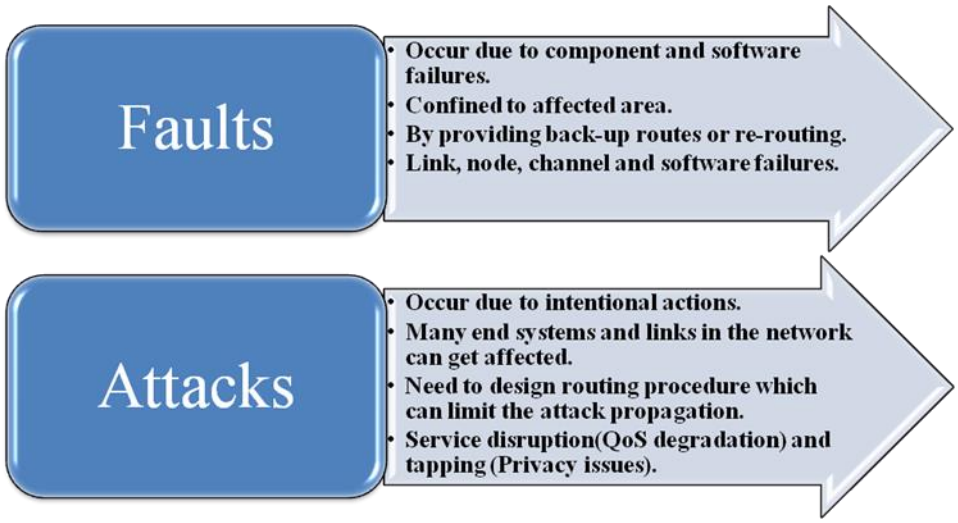


Figure 1.1 Differences between the faults and the attacks.

The unintended faults are comparatively less harmful than attacks as they are confined to the affected area and simple rerouting or providing backup paths can mitigate the effects. Whereas, the attacker signals make sporadic entry into the network and propagate through various links and nodes in the network spreading the attack. In addition, it is hard to monitor the physical layer attacks in TONs, as the signal remains in the optical domain throughout its path. Hence, it is hard to monitor, localize and control the spread of the attacks that happen in the bottom (physical) layer of the *Open System Interconnect* (OSI) [35] model.

The physical layer attacks are broadly divided into two categories, namely service disruptions and tapping [31]. The service disruption attacks degrade the performance of the TONs by disturbing the desired signal transmission. Whereas, tapping attacks help in traffic analysis and eavesdropping by providing unauthorized access to the data signals [24]. Table 1.1 summarizes the various methods of attacks and targeted components.

Table 1.1 Summary of various attacks, attack methods and targeted components [31]

Attack type	Attack method	Component
Service Disruption	In-band jamming power	Fiber
	Out-band jamming power	Fiber
	Intentional crosstalk	Splitter
		Filter
		Switch
		Combiner
	Gain competition	Amplifier
Eavesdropping	Unauthorized observation	Fiber
		Tap

The targeted components can be summarized into three main categories, optical fibers, switching nodes and optical amplifiers. Hence, reducing the interactions among the signals that share same nodes, links and wavelengths can eventually reduce the overall attack radius for all the signals in the network. Thus, it is possible to control the spread of the malicious signal by performing a secure and robust *Routing and Wavelength Assignment* (RWA) for all the signals over the physical topology.

1.4 Solution outline

The main focus of this thesis is on creating an *Integer Linear Program* (ILP) formulation called the attack aware RWA for sliding window scheduled traffic model, to handle physical layer attacks in TONs. The major features of this ILP are as follows:

1. An attack aware ILP formulation is designed for the sliding window scheduled traffic model with a main objective of reducing the attack radius for all the requested connections in the optical communication network.

2. Three main segments of constraints are covered in the ILP formulation namely, the basic RWA constraints, the sliding window scheduling constraints and the main attack aware constraints.

3. The basic RWA constraints cover the flow conservation, wavelength clash constraint, loop control and wavelength continuity constraints. These are discussed in more detail in Chapter 2.

4. The sliding window scheduling constraints provide an appropriate start time to the lightpath requests and make them active during consecutive intervals starting from the calculated start time.

5. The attack aware constraints calculate the *link share attack radius* (LAR) and the *in-band sharing attack radius* (IAR) values, in order to obtain a total attack radius for all the lightpath requests in all the intervals.

6. An adjustment is proposed for the scheduling constraints to make the attack aware ILP formulation capable of handling the fixed window scheduled traffic demands.

7. A different objective function is offered for the ILP formulation to obtain an attack unaware ILP formulation for sliding window scheduled traffic model.

8. As covered in [17], four different objective functions for different values of the total attack radius are provided for the same set of constraints.

9. To solve all the proposed ILP formulations, IBM ILOG CPLEX optimization software is used [30].

10. Various experimentations are carried out on all the proposed ILP formulations in order to test the attack survivability of the proposed attack aware RWA for sliding window scheduled traffic model.

1.5 Thesis organization

The rest of the thesis is organized as follows: In chapter 2 an elaborated overview of different optical networking components and concepts are covered. In addition, the literature review is also included in this chapter. Chapter 3 presents the proposed attack

aware ILP for sliding window scheduled traffic model. Different objective functions, the set of constraints and the proposed adjustments for the fixed window traffic model and the attack unaware model are defined in this section. In chapter 4, the simulation results for all the proposed ILPs are compared, analyzed and recorded. Finally, the conclusion and the scope for future work are discussed in the chapter 5.

2. REVIEW

2.1 Overview of Fiber-optic Networks

The use of the fiber optic networks has been increased in an enormous way since its invention in early 1970's [11]. These networks has become an important part of world's communication technology because of their capability to handle massive amounts of data (tera bits per second) by connecting different continents. In recent years, various advantages like low signal attenuation and distortion, low cost and high bandwidth capabilities, made them a crucial part in the telecommunication industry.

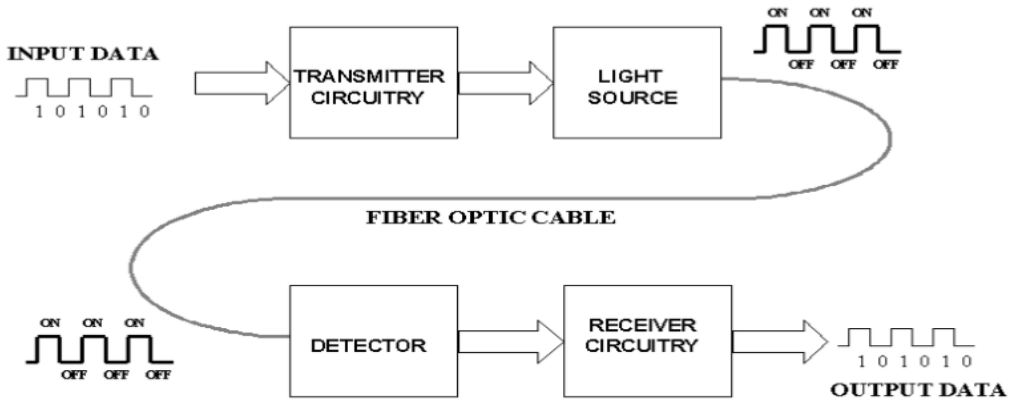


Figure 2.1: Basic architecture of an optical fiber network [11]

Figure 2.1, shows the basic structure of an optical fiber network. The primary communication medium for these networks are optical fibers. Transmitters and receivers are used to convert electrical signals to optical signals and vice versa, respectively at the end nodes. In between the end nodes, sometimes it is necessary to regenerate the optical signal to strengthen it. Based on the number of all optical paths that a transmission in an optical network experience, three approaches are provided. They are transparent or All

optical, opaque and translucent [12]. In all optical networks, there will be no *Optical-Electrical-Optical* (OEO) conversion at intermediate nodes, whereas in opaque networks, it will be done at all the nodes present. The translucent networks are an intermediate approach where the conversion takes place only at few selected nodes. In this thesis, our concentration is on the *Transparent Optical Networks* (TONs).

2.1.1 Optical Fiber

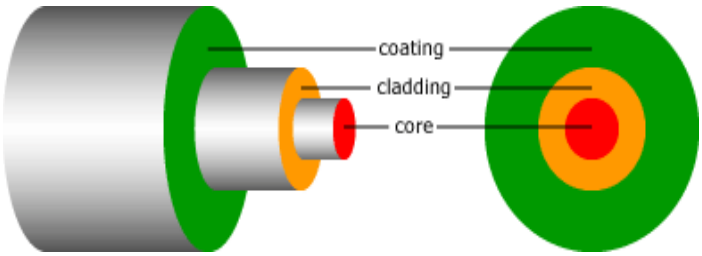
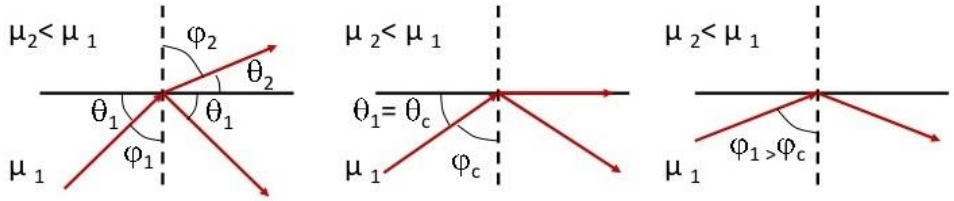


Figure 2.2: Basic Structure of an Optical Fiber [8]

An optical fiber is a glass or plastic thread like structure carrying signals in the form of light pulses. The light signal inserted at one end of the optical fiber reaches to the other end with high speed and low transmission loss [7]. The main components of the optical fiber are core, cladding and protective buffer, which are shown in the Figure 2.2. Inside the fiber optic cable, the light signal remains within the core throughout its path from the source to the destination. This is made possible by creating a series of total internal reflections.



(a) (b) (c)

Figure 2.3: (a) Refraction, (b) Critical angle and (c) Total internal reflection [10]

As shown in the Figure 2.3 (a), when a light ray passes from a material with high refractive index (μ_1), with an angle of incidence (Φ_1), to a material of low refractive index (μ_2), then the light signal will be refracted into the lesser dense medium with an angle (Φ_2), with the normal along with a partial reflection into the denser medium [9]. According to the snell's law of refraction, the following equations satisfy this condition,

$$\mu_1 . sin\, \Phi_1 = \mu_2 . sin\, \Phi_2 \qquad (1)$$

When the angle of refraction (Φ_2) becomes 90°, it is said to be a limiting case as the refracted ray meets with the interface between the two mediums. Also, no further refraction is possible for this light signal. This transmission is shown in the Figure 2.3 (b) and Eq 2 depicts the adaptation of this condition in Eq 1. The angle of incidence in this case is called the critical angle (Φ_c).

$$sin\, \Phi_c = \frac{\mu_2}{\mu_1} \qquad (2)$$

If the angle of incidence is increased more than the critical angle, then the light signal will experience the total internal reflection as shown in the Figure 2.3 (c). Thus, the lightpath remains within the denser medium throughout the transaction. To meet the

transmission qualities of the optical fibers with the transmission properties of the available light sources, near-infrared range of wavelengths is chosen for the fiber optic transmission [11].

2.1.2 Optical Fiber Network Components

In this section, a brief overview of some of the optical fiber networking components [13] [26] that are mentioned in this thesis are discussed. The vulnerabilities associated with different optical networking components lead to several non-linearities and crosstalks during optical transmission [24]. This can ultimately turn into an attack, if it gets into the hands of an attacker. Hence, it is necessary to gain knowledge of the key optical networking components.

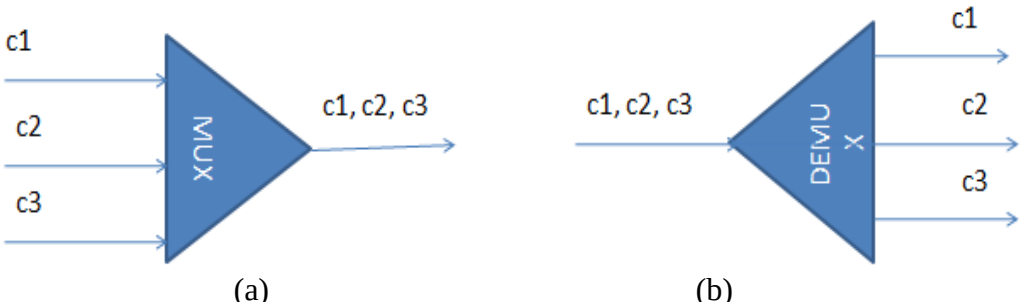


Figure 2.4: (a) Optical Multiplexer (MUX), (b) Optical Demultiplexer (DEMUX)

First, the *Optical Multiplexer* (MUX) and the *Optical Demultiplexer* (DEMUX) are two important components in an optical WDM network, used to combine or split different wavelengths carrying signals onto a single optical fiber or vice versa, respectively. The Figure 2.4 (a) shows an Optical Multiplexer, which receives optical signals from various channels to merge and couple them into one optical fiber. Whereas,

Figure 2.4 (b) shows an *Optical Demultiplexer*, which does the exact opposite of an Optical Multiplexer. It receives a single light beam and splits it onto different channels carrying signals. The MUXs are totally passive devices, where as DEMUXs can be either active or passive.

The Figure 2.5 depicts an *Optical Add or Drop Multiplexer* (OADM), which selectively drops one or more channels carrying optical signals leaving the channel empty. The OADM allocates that free channel to another signal carrying data which transmits in the same direction of flow [13]. These devices can be classified into two types, fixed or dynamic. The fixed OADMs are more reliable and are built using passive devices. The wavelength selection is static in these devices, between the optical DEMUX/MUX. In the dynamic OADMs, the wavelength selection is reconfigurable. These devices can only handle simple networks like ring and linear topologies, where traffic load is less.

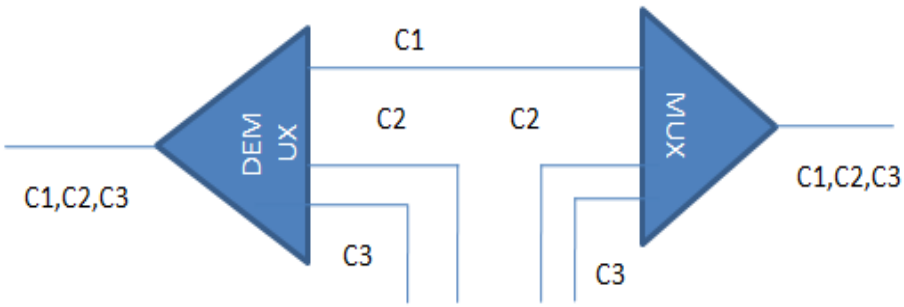
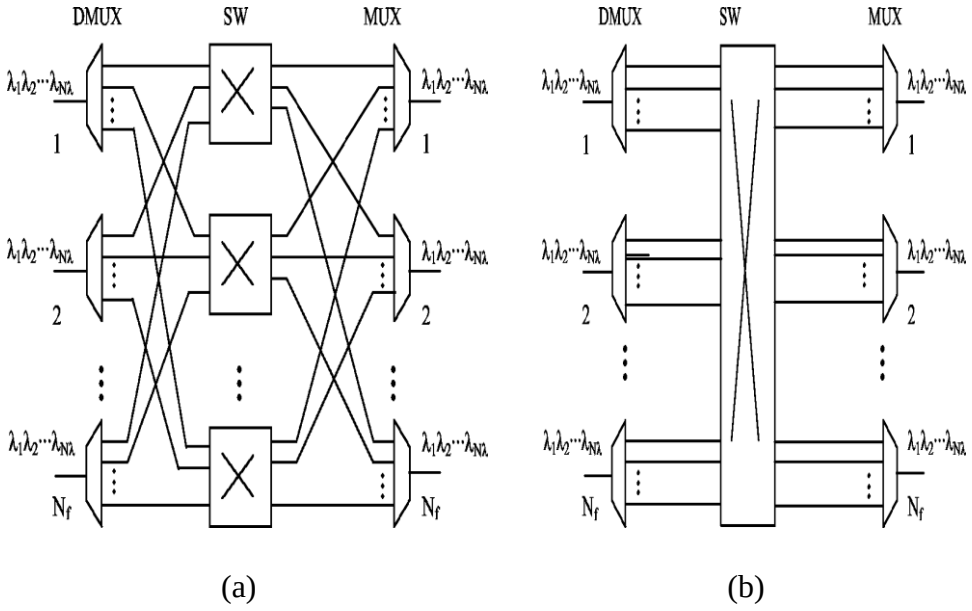


Figure 2.5: Optical Add or Drop Multiplexer (OADM)

The *Optical Cross Connect switch* (OXC) is another important device, which routes the optical signals between the outputs of DEMUX and the inputs of the MUX.

Even though, the functioning of an OXC resembles an OADM, these devices are essential for handling larger networks, whereas OADMs are useful for simple networks [13]. An OXC normally consists of MUXs, DEMUXs and optical switching fabric [24]. The main functionalities of an OXC include, routing and re-routing lightpath demands, wavelength switching and conversion. How the signals on the input fiber routes towards the output fibers inside an OXC can be determined in two ways., *static* and *dynamic*. The diagrammatic representation of both the static and dynamic OXCs is presented in Figures 2.6 (a) & (b) respectively.



(a) (b)

Figure 2.6: (a) Static and (b) Dynamic Optical Cross Connect Switch [27]

In the static cross connect switch, the connections between the respective DEMUXs and MUXs is fixed. Hence, the routing of signals between different switches in the node is static. Different passive devices are used in the architecture of static OXCs. In dynamic OXC, it is possible to modify the routing of signals according to the

requirement. As the switch ports are closely connected, it is possible for the device to turn out to be a source of in-band crosstalk, where the signals of same wavelength interact with each other and leak within. This can lead to the most hazardous and strong in-band crosstalk attack [24].

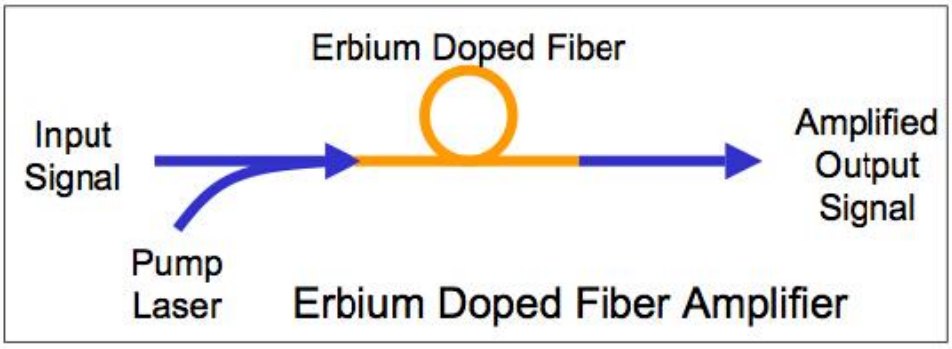


Figure 2.7: Optical Amplifier (OA) [28]

The *Optical Amplifiers* (OA), are basically used to amplify the signal that is attenuated during the transmission process [24]. In TON's, where the signal remains in the optical domain throughout its path, it is necessary to provide a proper gain to the signals, in order to maintain the QoS. *Erbium-doped Fiber Amplifiers* (EDFAs), are the most popular OAs in use. The EDFAs operate at the 1550 nm wavelength region, with approximately 35 nm gain. In the Figure 2.7, shows the basic architecture of an EDFA.

2.2 Wavelength Division Multiplexing

The *Wavelength Division Multiplexing* (WDM) [13] is a revolutionary technology, which divides bandwidth on a single optical fiber into various independent and separate channels based on wavelengths. Every data channel is represented with a

unique wavelength. This technology improves the capacity of an optical fiber tremendously. This method is not only efficient but also cost effective. By simply adjusting the end nodes with more channel bearing capacities, the overall transmission capability of the existing system can be enhanced to a great extent. Hence, there is no need to transform the whole system, to handle potential bandwidth requirements. Along with all the advantages, flexibility is provided for complex optical networks, with the transparency offered by the WDM networks. In Figure 2.8, data signals on individual channels (colors: purple, blue, green and pink) are sent from respective transponders (TP1 - TP4) to be multiplexed and traverse on a single optical fiber cable. And, at the receiver's end they are demultiplexed and sent to respective receivers (TP5 - TP8) to reach their appropriate destinations.

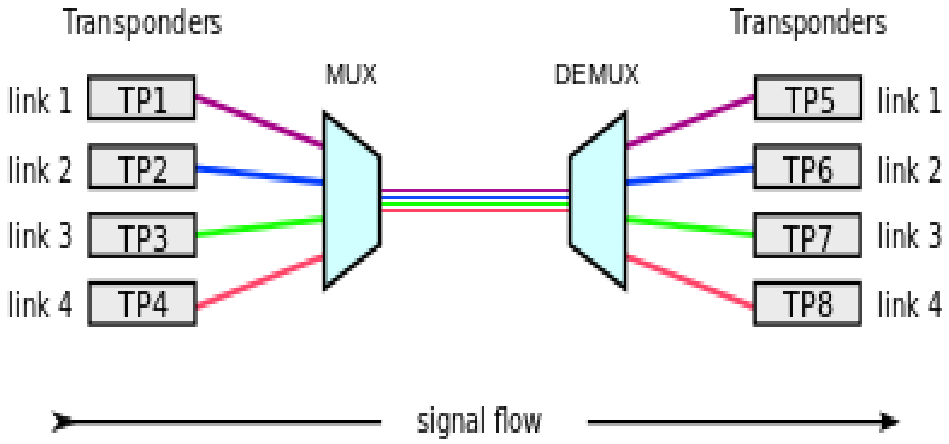


Figure 2.8: *Wavelength Division Multiplexing* (WDM)

2.3 Physical and Virtual Topologies

A *physical topology* of an optical network with four nodes is shown in the Figure 2.9 [16]. The circles represent nodes (E0 - E3), rectangles are routers (R0 - R3) and the

solid lines represent the bidirectional optical fiber links between the nodes. This topology shows how the different end systems are connected within the network.

The dashed lines are the requested lightpaths from one node to another node in the optical network. A *lightpath* can be defined as an all-optical data communication link between a source and a destination node in the network. The originating node at the start of the dashed line is the source node for a lightpath demand and the end node is the destination. Different colors (red - λ1& blue - λ2) of the dashed lines represent different wavelengths that are allocated to different lightpaths, on the physical topology. The virtual topology can be obtained from the Figure 2.9, just by connecting the source and destination nodes, with respective lightpath demands as directed arrows between them.

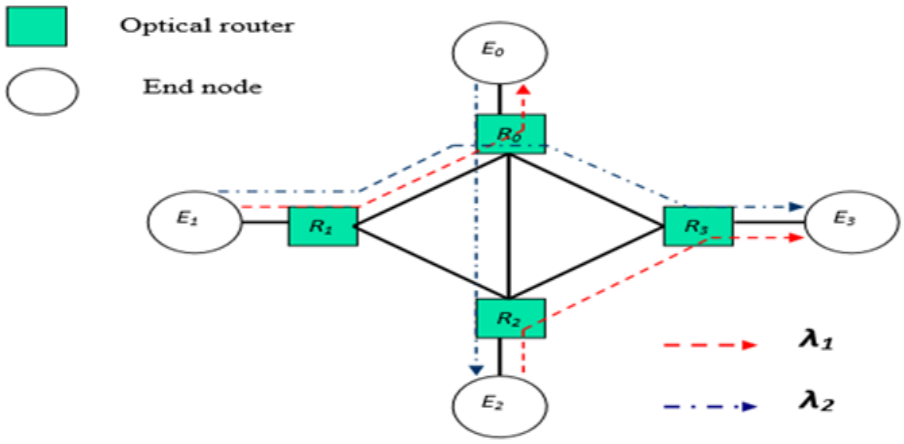


Figure 2.9: Physical Topology Example

2.4 Routing and Wavelength Assignment (RWA) Problem

It is important to effectively serve the connection requests made between the source and the destination pairs in order to maintain robust communication in the WDM

optical networks. Hence, allocating an effective path and an available wavelength for the lightpaths in an optical network is a significant optimization problem called *Routing and Wavelength Assignment* (RWA) [14]. Solving this problem is vital to improve the efficiency of all optical WDM networks. Apart from balancing the flow of requests in the network, an RWA should follow three main constraints [15].

1. **Loop Control Constraint**: A check should be conducted on every requested lightpath, to control the formation of cycles in its route from the source node to the destination.

2. **Wavelength Continuity Constraint**: Same wavelength must be used by a lightpath on all paths throughout its route from the source node to the destination node.

3. **Wavelength Clash Constraint**: Distinct wavelengths must be allotted to the lightpaths sharing same optical fiber at the same time.

2.4.1 Traffic Models

The allocation of an RWA for the requested lightpath demands, can be carried out in three different ways [16], namely *static*, *dynamic* and *scheduled traffic models*. The scheduled traffic model is further divided into two different traffic models called *fixed window scheduled traffic model* and *sliding window scheduled traffic model* [18]. Different traffic models can be chosen according to one's necessities.

First, the static traffic model is an offline traffic model, where a set of communication links is known in advance and mostly don't change over-time. This method is used in a number of papers in the literature [2] -[6]. The static lightpath demands are comparatively steady for long periods of times when verified with other

models. The main objective for this offline RWA is to successfully establish as many connections as possible. The input for this model can be given in the form of a simple traffic matrix, which shows the number of connection requests made in between a source and destination pair. This traffic model is mostly used in the network planning and design phase [19].

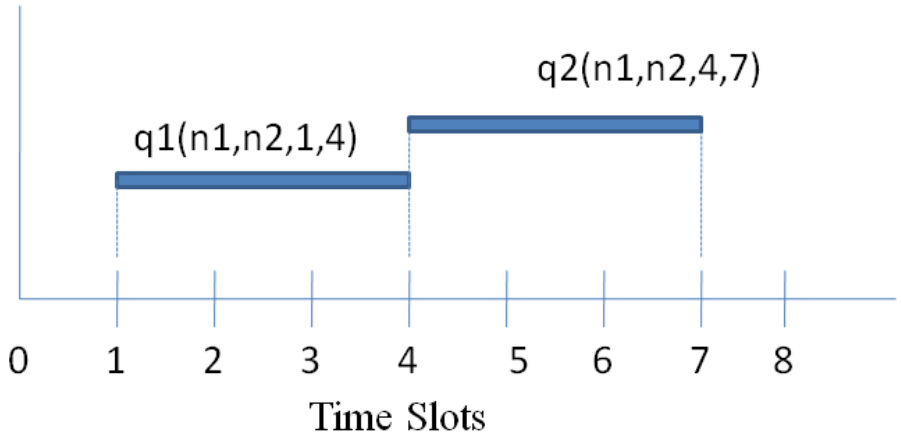


Figure 2.10: Fixed window scheduled traffic model example

The dynamic traffic model [1] is a more general case, where the connection requests enter and leave the network at random time intervals. Also, the duration of the lightpath demands is not known in advance. The resource utilization can be enhanced using this traffic model as the resources used by the departed lightpath demand can be reused by the new demands entering the network. The main objective of this online RWA will be minimizing the blocking probabilities. This model is used mainly in the network operation phase [19].

The Scheduled lightpath allocation method is useful for the demands in need of periodic bandwidth usage at preset timings [21]. This *scheduled traffic model* (STM) has

static characteristics as the lightpath requests are known in advance and also contains dynamic characteristics as the demands enter and leave the network at predefined timings. The time-flexibility feature made this traffic model stand out among other traffic models. This method can be used to allocate routes for lightpath requests between the main office and the regional units during office hours and between a bank and its remote backup storage facility for data backup during non-functional hours [18]. These demands cannot be fulfilled efficiently by using dynamic traffic model which is less reliable in situations like this. That is, for a dynamic traffic scenario, at times when the network load is high, it might get impossible to allocate space for an important video conference or cancel a backup schedule, which can lead to functional disorders in the respective organizations. The solution for such scenarios can be scheduled traffic model.

In the fixed window scheduled traffic model [17] [21], the set up and tear down timings of the requested demands are fixed. That is, the *demand holding time* (DHT) for a lightpath demand is equal to the difference between the start and end times of the lightpath demand. The addition of time dimension made this model more operational than the static traffic model. In this method, a tuple (s_p, d_p, st_p, et_p) represents a lighpath demand p. Where s_p and d_p are the source node and the destination node of the lightpath demand p and st_p and et_p are the start time and the end time of the request in the network. A better resource utilization can be achieved with this method as the resources can be shared by different time disjoint lightpaths. In Figure 2.10, two lightpaths *q1* and *q2* originating from nodes *n1* to *n2* are considered as an example. On an 8-point time scale and with only one wavelength, the tuples *q1 (n1, n2, 1, 4)* and *q2 (n1, n2, 4, 7)* are established as shown in the Figure 2.10. Even though there is only one wavelength, as the

demands are time-disjoint, they can use the same wavelength at different time slots. Hence, the communication links for both the demands can be allocated, despite resource sharing.

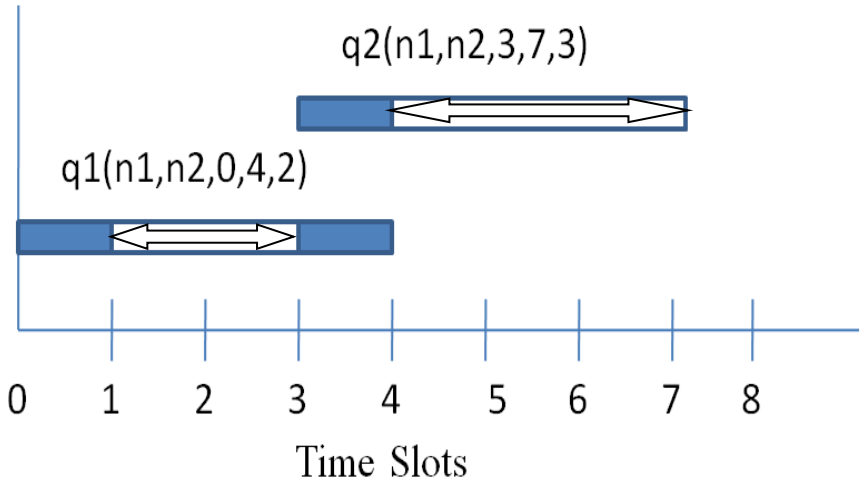


Figure 2.11: Sliding window scheduled traffic model example

To meet the future internet needs better than the fixed window model, a more flexible traffic model is introduced, namely the sliding window scheduled traffic model [18] [20] [22] [23]. As from fixed window traffic model, it is clear that, reserving the bandwidth for future usage is better than making a sporadic entry into the network without any planning. In the sliding window STM, the start time of the lightpath is not specified in advance, but can slide within a larger window. So, the start time can be selected to optimize the desired design objectives. This method provides a better quality of service when compared with other traffic models described above.

The flexibility in pricing can be achieved by establishing the lightpaths at the low cost timings of the network usage, and this feature not only allows the time flexibility but

also reduces the resource utilization cost for the service providers. Hence, it is a best solution to adopt for periodic lightpath requests at pre-planned timings, but implementing this traffic scenario is difficult when compared with the remaining traffic models because of the complexity in generating the start times for all the demands inside the given window.

A lightpath demand *p* under this traffic scenario can be represented by a tuple $(s_p, d_p, \alpha_p, \omega_p, \tau_p)$, where s_p and d_p are the same as in the fixed window traffic model, α_p and ω_p are the given start and end times of the larger time window during which the demand must be allocated, and finally τ_p $(0 < \tau_p <= (\omega_p - \alpha_p))$ is the *demand holding time* (DHT). The set up time st_p of the demand *p* will be generated within the specified window. The example provided in the Figure 2. 11 used the similar dimensions as that of the fixed window traffic model example. The lightpaths *q1 (n1, n2, 0, 4, 2)* and *q2 (n1, n2, 3, 7, 3)*, are originating from node *n1* and ending at node *n2*, with DHTs *2, 3* respectively. Also the specified windows for the lightpaths *q1* and *q2* are ranging *0-4* and *3-7* respectively. As shown in the Figure 2.11, it is possible for the requests to slide within the specified window, which is represented as the bidirectional arrows (lightpaths) on the top of the shaded region (larger windows). The arrangement of lightpaths can be made either on the basis of low pricing or less busy times to obtain enhanced network efficiency.

2.5 Physical Layer Attacks

The TONs are susceptible to several physical layer attacks because of the transparency associated with them. In this thesis, our main focus is on the most disastrous high power jamming attacks [24], whose localization and detection is rather hard. An

overview of these attacks which are created by using different weaknesses related to optical networking components is discussed in this section. The main high power jamming attacks are namely *in-band jamming attack, out-of-band jamming attack and gain competition*.

The *intra-channel crosstalk* between the signals on the same wavelength inside an optical switch causes *in-band jamming attack* or *intra channel crosstalk attack* [1]. This attack is more dominant and harmful than the other high power jamming attacks, as the signals are on the same wavelength as that of the attacker signal [24] [25]. When a high powered attacking signal is injected on a wavelength, all the signals using that wavelength and sharing a common switch gets attacked. It is possible that, if the attacker signal is strong, it can make the neighboring signals gain the attacking properties. So that, the recently attacked signals can spread the attack further in the network. Hence, even the signals which are not in component sharing with the main attacker can get affected. As, the secondary attacker has no physical component sharing with the main attacker signal, the localization and identification of these attacks are more complicated. So, it is clear that the attacks, that take advantage of the intra channel crosstalk in the optical switches are more damaging.

In the Figure 2.12, an example in-band jamming attack scenario is explained diagrammatically. In the Figure 2.12, the blue rectangular boxes represent nodes, black dotted boxes symbolize optical fibers and arrowed lines are the optical signals. Three types of signals are shown in the picture, the plain red arrows represent the signals using wavelength $\lambda 1$, the plain green arrow shows the signal using wavelength $\lambda 2$ and the dotted arrow is the attacker signal. The high power jamming signal on the wavelength $\lambda 1$

is used as an attacker from node *n2* [19]. In the common optical switch inside the node *n2*, the signal that starts at node *n1* and propagates on the same wavelength *λ1*gets affected. The recently affected signal from *n1* acquires the attacking properties and when it passes through the common switch in node *n3*, affects the new signal on the same wavelength *λ1*, by spreading the attack further in the network. But, the other signal that passes through node *n4* remains intact as it is on a different wavelength from the main attacker signal which passes through the node *n4*. This happens because they are on different wavelengths and are transmitting on different optical fibers after crossing the node *n4*.

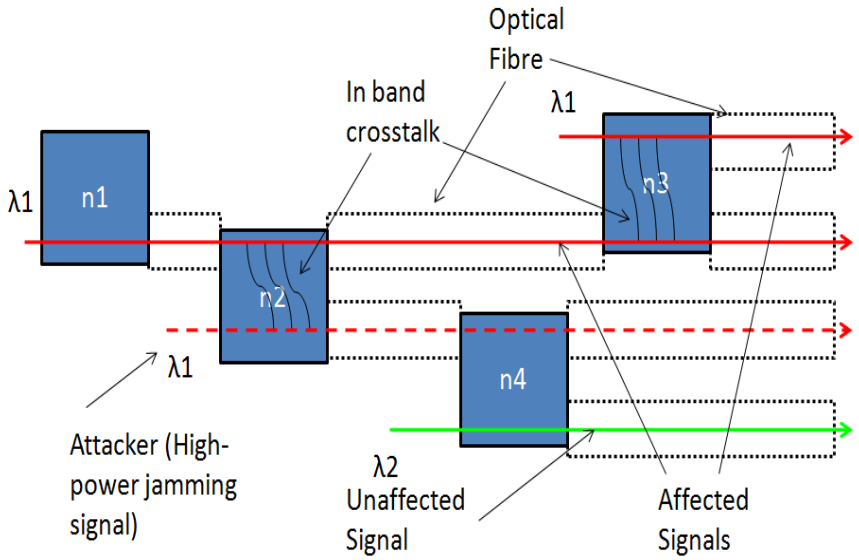


Figure 2.12: In band Jamming Attack Propagation

The main objective of the attack aware ILPs created to handle in-band jamming attacks, is to minimize the spread of the attack by reducing the interaction between signals that share common wavelengths and propagate through same nodes [1] [3-5] [17]. A popular method to identify such nodes is to reduce the *In-band Attack Radius* (IAR) of

all the active commodities in the network [1] [3] [17]. The value of IAR for a lightpath demand *p* is obtained by generating an *In-band Attack Group* (IAGp) containing lightpaths which are on the same wavelength and are sharing common nodes with the lightpath *p*. The number of lighpaths that are in such sharing gives the *IARp* value of the demand *p*. Different papers in the literature have used this concept to create different attack aware ILPs.

The *inter channel crosstalk* between signals on different wavelengths which transmit over the same optical fiber results in *out-of-band jamming attack* [2] [24]. This crosstalk normally occurs within the optical fiber, either because of longer distances or the non linearities in the optical fiber. When the attacker introduces a high powered signal into the optical fiber, it can interfere with the signals on other wavelengths because of the optical fiber non linearities. The Raman gain effect and cross-phase modulation are some of the causes that create non linearities in optical fibers [24].

The Figure 2.13 depicts a sample out-of-band jamming attack propagation. The high power jamming signal is passing through the node *n1* on the wavelength *λ1*. The signal originating from node *n2* and on wavelength *λ2* gets affected after crossing the node n2, as it is sharing the same optical fiber with the attacker signal, assuming that they are propagating on adjacent wavelengths.

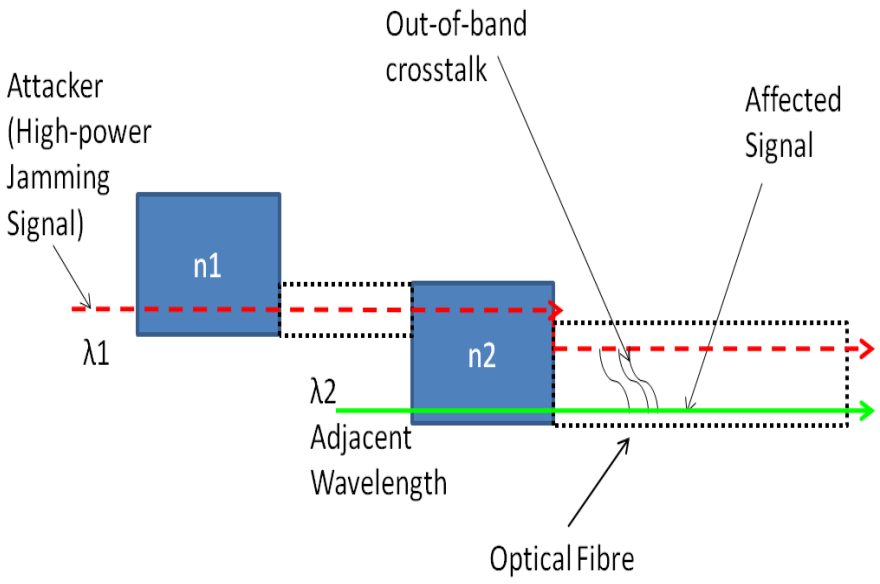


Figure 2.13: Out-of-band Jamming Attack Propagation

While working on the RWA problem with attack aware properties, the ILP looks for the lightpaths sharing the same links in the optical network, to handle out-of-band jamming attacks [1-2] [5-6] [17]. A similar method is used in literature to handle out-of-band jamming attacks, as that of in-band jamming attacks. The *Link-share Attack Group* (LAGp) is generated for a lightpath *p*, in which all lightpaths that are in link-sharing with *p* are registered. Again, the *Link-share Attack Radius* (LAR) is calculated using the LAGp values. The main objective of the attack aware ILP that handles out of band jamming attacks, is to minimize the LAR values of all the lightpaths. Finally, the AR value can be acquired just by combining both the LAR and IAR values of all the lightpaths.

In TONs, as the lightpaths remain in the optical domain throughout its path, it is necessary to amplify the signal at some planned intervals [24]. *Erbium-doped fiber amplifiers* (EDFAs) are normally used for the purpose of transparent amplification of

such signals. Usually in EDFAs, the gain will be provided to optical signals with respect to the power levels, which can lead to gain competition. An effective and strong out-of-band jamming attack can be generated using this gain competition effect. When a high power jamming attack is introduced on a wavelength different from the other optical signals, but within the pass band of the EDFA, an unsystematic gain will be provided to it. The high powered signal acquires more gain by stealing the gain of legitimate signals on other wavelengths. Thus, the attack will be propagated further in the network, exploiting several other vulnerabilities of TONs. The Figure 2.14, shows a scenario of gain competition pictorially.

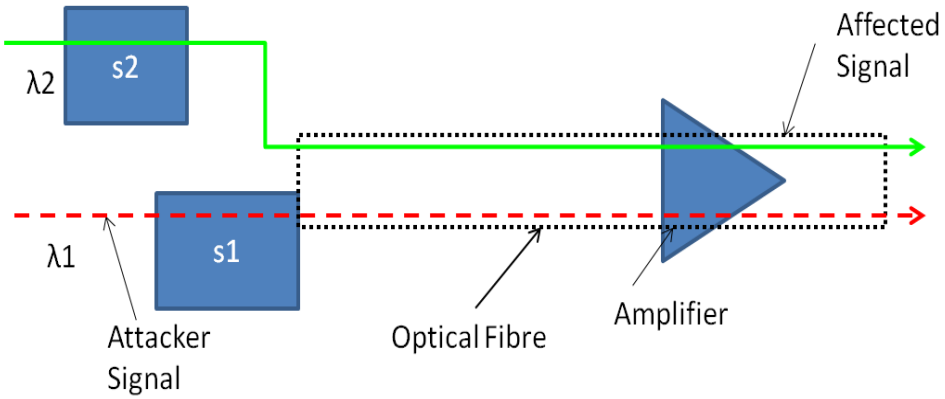


Figure 2.14: Gain Competition

2.6 Related Works

Different works related to various attacks in the transparent optical networks (TONs) are presented in this section. The works mentioned in here, mainly concentrated on the In-band and out-of-band jamming attacks in optical fiber networks. In these

papers, broad range of solution approaches are proposed and are experimented under different traffic models.

Skorin-Kapov, N., et al. 2010 [2]: For static traffic scenario, where all the lightpaths enter the network at the same time, an ILP is proposed to handle the out-of-band and gain competition attacks. The authors planned the routing of commodities in order to avoid routes which are participating in maximal link sharing. The main objective of this ILP is to minimize the *Maximum link-share attack radius* (maxLAR), which can be calculated as the maximum number of lightpaths that are link sharing with a single lightpath demand in the network. The secondary objective of this formulation is to reduce the average load on the network.

Skorin-Kapov, N., et al. 2012 [3]: The authors proposed an ILP to handle in-band attack propagation in all optical WDM networks for offline planning problem. Both the direct and indirect in-band crosstalk propagations are examined and are minimized in order to control the propagation. The main objectives of these two ILPs are minimizing the maximum *primary attack radius* (PAR) and the maximum *secondary attack radius* (SAR) values respectively. The ILP-PAR simply checks for the lightpaths which are sharing the same switch and are traversing on the same wavelength and calculates the PAR value. Whereas, ILP-SAR takes the constraints of ILP-PAR and calculates the SAR value by checking the spread of in-band crosstalk over the network indirectly by already attacked signals. Upon considering the complexity and scalability issues, the further propagation and transformation of in-band jamming attacks into other physical layer attacks is not covered. Also, they assumed that maximum only one lightpath demand can

serve a pair of nodes. Most of these conditions are ignored while generating a heuristic approach for this problem.

Manousakis, K., et al. 2013 [4]: The spread of in-band crosstalk attack is controlled in this paper, by proposing an ILP for RWA problem for static traffic instance. LP-relaxation techniques are given for handling the larger networks. The k-shortest path algorithm is used to obtain k candidate paths for each connection request in the first phase, which is given as an input to the ILP proposed. The main objective of this ILP is to control the interactions among the lightpaths which trigger the in-band jamming attacks along with minimizing the wavelength utilization on every link or simply network load.

Furdek, M., et al., 2015 [6]: An ILP is proposed in this paper which covers both the attack aware and the dedicated path problems, to obtain a fully protected optical network. The 1:1 method of dedicated path protection [6] is used in this paper, where the backup paths are strictly reserved for the failed lightpaths. That is, only working lightpaths are active and are considered as possible attack sources. The ILP is decomposed into two parts to reduce complexity - the routing subpart and the wavelength assignment subpart. Attack groups (AGs) are calculated for all the lightpaths to acquire the group of lightpaths which are in link, node or channel sharing. The first phase of the ILP checks for the working or backup lightpaths which are in link sharing with other lightpaths. Whereas, in the second phase in-band sharing is checked for both the working and back up lightpaths. The main objective of both the ILPs is to minimize the unprotected connections from physical layer attacks.

Jaekel, A., et al. 2015 [1]: Routing of Lightpath demands on the optical fiber network is carried out in a manner that minimizes the adverse effects of the high power jamming attacks. An ILP is proposed to handle the in-band and out-of-band jamming attacks for both static and dynamic traffic scenarios. The main objective is to minimize the attack radius for all the lightpath demands. LAR and IAR are calculated for lightpath demands in order to obtain the combined value of attack radius. A security aware heuristic approach is also presented in this paper for large networks to handle dynamic lightpath requests. A network instance along with existing lightpath demands and number of channels are given to the algorithm, which calculates the LAR, IAR and available channel for the new request, if a route over the network can be provided, otherwise it is blocked.

Hongbo, Z., et al. 2016 [17]: The main objective of the ILP presented in this paper is to reduce the propagation of both the in-band and the out-of-band jamming attacks. This ILP is designed to build an attack aware RWA for the fixed window scheduled traffic model. The input to this ILP contains the source and the destination nodes for the lightpath demand along with the set up and tear down timings. As the time disjoint feature describes the allocation of resources among the lightpaths, the lightpaths interacting in time are calculated before starting the ILP and is given as an input to it. The lightpaths which are in link-sharing, channel-sharing and node-sharing with other lightpath demands at all the intervals are calculated and the values of LAR and IAR are measured. Finally, the combined value of total attack radius for all the lightpaths in all intervals is minimized to obtain the final objective value for this ILP. Four different objectives are proposed for the same ILP to check different scenarios within the system.

Also, the ILP is tested with a basic RWA with no attack aware constraints. The results showed that this ILP has minimized the spread of physical layer attacks by reducing the link sharing and node sharing among the lightpaths which are interacting over time.

Manousakis, K., et al. 2016 [5]: This paper is published as an extension to the paper [4]. An ILP is proposed to handle the propagation of both in-band and out-of-band jamming attacks for the static lightpath allocation problem. In addition to the formulation in [4], interactions among the lightpaths, which are sharing a common link are calculated and are added to the objective to cover the inter channel crosstalk susceptibility. In the first phase of programming, a set of *k* candidate paths is obtained using Dijkstra's algorithm [4]. The acquired routes for all the source and destination pairs are given as an input to the ILP, of which the objective is to control the spread of both inter and intra channel cross talk attacks. A different approach to this problem is proposed as an ILP formulation called A-RWA-convex, where cost functions of both the attacks are minimized as the main objective along with the overall cost of the network.

Summary: Table 2.1, summarizes the papers discussed under the related works section and gives a brief overview of the relevant literature survey papers

Table 2.1: Literature Survey Summary

R. No.	Reference	Types of Attacks	Traffic Model	RWA	Heuristic	ILP
[2]	Skorin-Kapov, N., et al. 2010	Out-of-band and Gain competition attacks	Static Traffic	Yes	TS_LAR	ILP_LAR
[3]	Skorin-Kapov, N., et al. 2012	In-band Jamming Attack	Static Traffic	Yes	GRASP_PAR_WA, GRASP_SAR_WA	ILP_PAR, ILP_SAR
[4]	Manousakis, K., et al. 2013	In-band Jamming Attack	Static Traffic	Yes	No	A-RWA, A-RWA-pw, A-RWA-p and LP relaxation techniques
[6]	Furdek, M., et al., 2015	In-band and Out-of-band Jamming Attacks	Static Traffic	Yes	AA-DPP-H	2-step AA-DPP-ILP
[1]	Jaekel, Arunita, et al. 2015	In-band and Out-of-band Jamming Attacks	Static and Dynamic Traffic	Yes	SA-DWA	ILP-SA
[17]	Hongbo Zhao et al., 2016	In-band and Out-of-band Jamming Attacks	Fixed Window Scheduled Traffic	Yes	No	SD-AA-RWA
[5]	Manousakis, K., et al. 2016	In-band and Out-of-band Jamming Attacks	Static Traffic	Yes	3-Phase Heuristic	A-RWA-p, A-RWA, A-RWA-convex, A-RWA-convex (relaxed)

3. ATTACK AWARE RWA FOR SLIDING WINDOW SCHEDULED TRAFFIC MODEL

3.1 Introduction

This chapter introduces the proposed ILP formulation called the *attack aware RWA for sliding window scheduled traffic model*. The main objective of this ILP formulation is to minimize the attack radius for all the lightpaths in the network. By reducing the attack radius, the interactions among the lightpaths that can cause in-band and out-of-band jamming attacks in the network are minimized. Thus, by solving the proposed ILP formulation the impact of the high power jamming attacks is lessened. Different variations of objective functions are proposed to solve the problem.

A complete presentation of ILP formulation with various objective functions and a set of constraints is provided in the following sections along with a detailed explanation. A simple variation is proposed for the ILP formulation to make it feasible for the fixed window scheduled traffic model. Also, an attack unaware approach for the proposed ILP formulation is defined. These various approaches help in testing the proposed system in different situations, which are discussed in the later chapters.

3.2 Solution approach

There are different ways to handle the spread of the high power jamming attacks in TONs. Most of the attack handling approaches are reactive in nature as they concentrate more on the network recovery [24] after facing an attack. However, the possibility of potential damage associated with this approach can be dangerous. Recently,

another prevention based approach has been introduced. In this method, the attack handling procedures are incorporated within the network planning phase [24]. The existing works on attack aware RWA have addressed the static, dynamic and fixed window scheduled traffic models [1] [2-6] [17]. Unlike these studies, we consider the sliding window scheduled traffic model for our attack aware RWA problem.

In our approach, the routing of lightpath requests is carried out in order to reduce the interactions among the lightpaths that cause various physical layer attacks. The main idea of our ILP is to reduce the attack radius for all the lightpaths in the network in all the intervals in order to handle different types of attacks. The LAR and IAR values are calculated for all the lightpaths in all the intervals to obtain the total attack radius value. The obtained attack radius value is minimized as the main objective in the ILP in order to achieve an optimal attack aware routing for all the requested lightpath demands. Also, in the sliding window scheduled traffic model the start time of the lightpath demand is unknown. Hence, we assign an appropriate start time for the lightpath demands using our ILP. Finally, with an addition of the basic RWA constraints our proposed ILP becomes complete.

3.3 Proposed ILP formulation

In this section, the ILP formulation for the attack aware RWA for sliding window scheduled traffic model is presented. Different objectives are proposed for different combinations of LAR and IAR values to solve the attack aware RWA problem. At the end of this section, a simple modification is added to the ILP to make it viable for the fixed window traffic. The input parameters for the ILP are as follows.

Input Parameters:

- A physical topology *G [N, E]*.
- *N*: A set of nodes.
- *E*: A set of edges (physical fiber links) between the nodes of the network.
- An edge (s_e, d_e), where s_e (d_e) is the source (destination) node of the edge $e \in E$.
- *W*: A set of available wavelengths on each fiber.
- *P*: A set of lightpath requests made between different nodes of the network.
- A lightpath demand $p \in P$ is given as a tuple $(s_p, d_p, \alpha_p, \omega_p, \tau_p)$, where s_p (d_p) is the source (destination) node of the lightpath *p*, α_p (ω_p) is the start (end) time of the larger window and τ_p $(0 < \tau_p <= (\omega_p - \alpha_p))$ is the DHT of the lightpath *p*.
- *M*: The number of available time intervals.
- *H*: An upper bound on the number of hops of a lightpath demand on the network.

Important Notations:

- *p, q*: Represents two different lightpath requests, $p, q \in P$ & $p \neq q$.
- *e:* Represents an available link in the network, $e \in E$.
- *i, j*: Represents two different nodes in the network. $i, j \in N$.
- *m*: Represents a specific time interval, $m \in M$.
- *k*: Represents an individual channel on a single optical fiber, $k \in W$.

Binary Variables:

- $x_{p,e}$: 1 if a lightpath *p* uses edge *e*, 0 otherwise.
- $y_{p,i}$: 1 if a lightpath *p* passes through a node *i*, 0 otherwise.
- $w_{p,k}$: 1 if a lightpath *p* is assigned to channel *k*, 0 otherwise.
- $a_{p,m}$: 1 if a lightpath *p* is active during an interval *m*, 0 otherwise.
- $st_{p,m}$: 1 if a lightpath *p* starts at an interval *m*, 0 otherwise.
- $\alpha_{p,q}$: 1 if the lightpaths *p* and *q* share at least one common edge, 0 otherwise.
- $\beta_{p,q}$: 1 if the lightpaths *p* and *q* share at least one common node, 0 otherwise.
- $\gamma_{p,q}$: 1 if the lightpaths *p* and *q* use the same channel, 0 otherwise.
- $\delta_{p,q}$: 1 if the lightpaths *p* and *q* use the same channel and have at least one common node, 0 otherwise.
- $T_{p,q}$: 1 if the lightpaths *p* and *q* are active during at least one common time interval, 0 otherwise.

Continuous Variables:

- $T_{p,q}^{m}$: 1 if the lightpaths *p* and *q* are both active during a common interval *m*, 0 otherwise.
- $\alpha_{p,q}^{e}$: 1 if the lightpaths *p* and *q* share a common edge *e*, 0 otherwise.
- $\beta_{p,q}^{i}$: 1 if the lightpaths *p* and *q* share a common node *i*, 0 otherwise.
- $\gamma_{p,q}^{k}$: 1 if the lightpaths *p* and *q* both use channel *k*, 0 otherwise.

- $LAR_{p,q}^{m}$: 1 if the lightpath *p* has link-sharing with lightpath *q* during interval *m*, 0 otherwise.
- $IAR_{p,q}^{m}$: 1 if the lightpath *p* has in-band sharing with lightpath *q* during interval *m*, 0 otherwise.
- $LARP_{p}^{q}$: 1 if the lightpath *p* is in the LAG of lightpath *q*, 0 otherwise.
- $IARP_{p}^{q}$: 1 if the lightpath *p* is in the IAG of lightpath *q*, 0 otherwise.

Integer Variables:

- $LAR_{p,m}$: The number of lightpaths that are in the LAG of a lightpath *p* (including itself) during an interval *m*.
- $IAR_{p,m}$: The number of lightpaths that are in the IAG of a lightpath *p* (including itself) during an interval *m*.
- LAR_{p} : The number of lightpaths that are in the LAG of a lightpath *p* (including itself) over all the intervals.
- IAR_{p} : The number of lightpaths that are in the IAG of a lightpath *p* (including itself) over all the intervals.
- $maxAR_{p,m}$: An upper bound on all the attack radius values ($AR_{p,m} = LAR_{p,m} + IAR_{p,m}$) calculated for any lightpath *p* during any interval *m*.
- $maxAR_{p}$: An upper bound on all the attack radius values ($AR_{p} = LAR_{p} + IAR_{p}$) calculated for any lightpath *p* over all the intervals.

ILP Formulation: *ILP_SUM_AR*$_{p,m}$

Objective function 1:

$$Minimize \ \sum_m \sum_{p \in P} \ (LAR_{p,m} + \ IAR_{p,m}) \qquad (1)$$

The objective function in *(1)* minimizes the total attack radius *($AR_{p,m}$ = $LAR_{p,m}$ + $IAR_{p,m}$)*, over all the lightpaths in all the intervals. The values of $LAR_{p,m}$& $IAR_{p,m}$ are combined to form the total attack radius $AR_{p,m}$ for any given lightpath *p* in any specified interval *m*.

Subject to:

Routing and wavelength assignment constraints:

$$\sum_{e:i \to j \in E} x_{p,e} - \sum_{e:j \to i \in E} x_{p,e} = \begin{cases} 1 & \text{if } i = sp \\ -1 & \text{if } i = dp \quad \forall i \in N, \forall p \in P \\ 0 & \text{otherwise.} \end{cases} \qquad (2)$$

$$\sum_{e:i \to j \in E} x_{p,e} \leq 1, \ \forall i \in N, \forall p \in P \qquad (3)$$

$$\sum_{k \in W} w_{p,k} = 1, \ \forall p \in P \qquad (4)$$

The constraints *(2)* - *(4)* are the basic routing and wavelength assignment constraints. The constraint *(2)* is the traditional flow conservation constraint. This allocates an efficient path to the lightpath *p* over all possible edges *e* in the physical topology. The constraint *(3)* is the loop control constraint. This eliminates the formation of loops in the path selected for the transmission of the lightpath *p*. The constraint *(4)* is the wavelength continuity constraint. This ensures that the same wavelength *k* is allotted to the lightpath *p* throughout its route. This is an essential constraint as wavelength converters are not used in our simulation.

Sliding window scheduling constraints:

$$\sum_{m \in M} st_{p,m} = 1, \ \forall p \in P, \forall m \in M, \alpha_p \leq m \leq \omega_p - \tau_p \qquad (5)$$

$$\sum_{m \in M} a_{p,m} = \tau_p, \forall p \in P, \forall m \in M, \alpha_p \leq m \leq \omega_p \quad (6)$$

$$a_{p,m+i} \geq st_{p,m}, \forall p \in P, 0 \leq i < \tau_p, \forall m \in M, \alpha_p \leq m \leq \omega_p \quad (7)$$

The constraints *(5)* - *(7)* are scheduling constraints. In sliding window scheduled traffic model the lightpath demand *p*'s start time ($st_{p,m}$) slides within the larger window from α_p to ω_p - τ_p. The constraint *(5)* calculates the actual start time for the lightpath *p* and makes sure that it has only one possible start time. The constraint *(6)* activates the lightpath for a τ_p number of intervals. Whereas, the constraint *(7)* makes the lightpath active for a sequential number of time intervals starting from $st_{p,m}$.

Link sharing constraints:

$$x_{p,e} + x_{q,e} - \alpha^e_{p,q} \leq 1, \forall p,q \in P, p \neq q, \forall e \in E \quad (8)$$

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

$$x_{q,e} \geq \alpha^e_{p,q}, \forall p,q \in P, p \neq q, \forall e \in E \quad (10)$$

$$\alpha_{p,q} \geq \alpha^e_{p,q}, \forall p,q \in P, p \neq q, \forall e \in E \quad (11)$$

$$\alpha_{p,q} \leq \sum_{e \in E} \alpha^e_{p,q}, \forall p,q \in P, p \neq q \quad (12)$$

The constraints *(8)* - *(12)* are the link sharing constraints that help in calculating the LAR values. If two individual lightpaths *p* and *q* traverse through the same edge *e*, the value of $\alpha^e_{p,q}$ is set to 1. The constraints *(8)* - *(10)* shows the calculation of the $\alpha^e_{p,q}$ value. When *p* and *q* share at least one (or more) common edge (s) the $\alpha_{p,q}$ value will become 1. The constraints *(11)* - *(12)* depict the equations for calculating the $\alpha_{p,q}$ value. This

variable determines whether the lightpath q may be in the link share attack group of the lightpath p (if they are both active during a common time interval).

Node usage Constraints:

$$y_{p,i} = \sum_{e:i\to j\in E} x_{p,e},\ \forall p \in P,\ \forall i \in N,\ i \neq d_p \qquad (13)$$

$$y_{p,dp} = 1,\ \forall p \in P \qquad (14)$$

The constraints *(13)* - *(14)* determine the node usage of all the requested lightpaths. The constraint *(13)* sets the value of $y_{p,i}$ to 1, if the lightpath p passes through the node i on its path when $i \neq d_p$. Whereas the constraint *(14)* states that the destination node d_p must be covered in the route selected for transmitting the lightpath p and sets the value of $y_{p,dp}$ to 1.

Node sharing constraints:

$$y_{p,i} + y_{q,i} - \beta^i_{p,q} \leq 1,\ \forall p,q \in P,\ p \neq q,\ \forall i \in N \qquad (15)$$

$$y_{p,i} \geq \beta^i_{p,q},\ \forall p,q \in P,\ p \neq q,\ \forall i \in N \qquad (16)$$

$$y_{q,i} \geq \beta^i_{p,q},\ \forall p,q \in P,\ p \neq q,\ \forall i \in N \qquad (17)$$

$$\beta_{p,q} \geq \beta^i_{p,q},\ \forall p,q \in P,\ p \neq q,\ \forall i \in N \qquad (18)$$

$$\beta_{p,q} \leq \sum_{i \in N} \beta^i_{p,q},\ \forall p,q \in P,\ p \neq q \qquad (19)$$

The constraints *(15)* - *(19)* are the node sharing constraints that help in calculating the *IAR* values. The constraints *(15)* - *(17)* shows the calculation of $\beta^i_{p,q}$. If two individual lightpaths p and q share a node i on their path from the source node to the destination

node, the value of $\beta_{p,q}^{i}$ is set to 1. The constraints *(18)* - *(19)* set $\beta_{p,q}$ value to 1, if the lightpaths *p* and *q* share at least one (or more) common node (s) on their specified routes.

Channel sharing constraints:

$$w_{p,k} + w_{q,k} - \gamma_{p,q}^{k} \leq 1, \ \forall p,q \in P, \ p \neq q, \ \forall k \in W \qquad (20)$$

$$w_{p,k} \geq \gamma_{p,q}^{k}, \ \forall p,q \in P, \ p \neq q, \ \forall k \in W \qquad (21)$$

$$w_{q,k} \geq \gamma_{p,q}^{k}, \ \forall p,q \in P, \ p \neq q, \ \forall k \in W \qquad (22)$$

$$\gamma_{p,q} = \sum_{k \in W} \gamma_{p,q}^{k}, \ \forall p,q \in P, \ p \neq q \qquad (23)$$

Here, the constraints *(20)* - *(23)* determine the channel sharing. If two individual lightpaths *p* and *q* share a channel *k* on their route, the value of $\gamma_{p,q}^{k}$ is set to 1 using the constraints *(20)* - *(22)*. The constraint *(23)* makes the $\gamma_{p,q}$ value 1, if the same wavelength is provided to both the lightpaths *p* and *q*.

In-band sharing constraints:

$$\beta_{p,q} + \gamma_{p,q} - \delta_{p,q} \leq 1, \ \forall p,q \in P, \ p \neq q \qquad (24)$$

$$\beta_{p,q} \geq \delta_{p,q}, \ \forall p,q \in P, \ p \neq q \qquad (25)$$

$$\gamma_{p,q} \geq \delta_{p,q}, \ \forall p,q \in P, \ p \neq q \qquad (26)$$

Finally, the constraints *(24)* - *(26)* define the variable $\delta_{p,q}$. This variable is set to 1 if the lightpath *q* is in the in-band sharing (i.e., $\beta_{p,q}$ = 1 and $\gamma_{p,q}$ = 1) with the lightpath *p*.

Time sharing constraints:

$$a_{p,m} + a_{q,m} - T^{m}_{p,q} \leq 1, \forall p,q \in P, p \neq q, \forall m \in M \quad (27)$$

$$a_{p,m} \geq T^{m}_{p,q}, \forall p,q \in P, p \neq q, \forall m \in M \quad (28)$$

$$a_{q,m} \geq T^{m}_{p,q}, \forall p,q \in P, p \neq q, \forall m \in M \quad (29)$$

$$T_{p,q} \geq T^{m}_{p,q}, \forall p,q \in P, p \neq q, \forall m \in M \quad (30)$$

$$T_{p,q} \leq \sum_{m \in M} T^{m}_{p,q}, \forall p,q \in P, p \neq q \quad (31)$$

The constraints *(27)* - *(31)* are the time sharing constraints. If two individual lightpaths *p* and *q* are active during the interval *m* the value of the variable $T^{m}_{p,q}$ is set to 1. This calculation is depicted in the constraints *(27)* - *(29)*. The constraints *(30)* - *(31)* set the value of the variable $T_{p,q}$ to 1 if the lightpaths *p* and *q* share at least one (or more) common interval (s).

Wavelength clash constraint:

$$\alpha_{p,q} + \gamma_{p,q} + T^{m}_{p,q} \leq 2, \forall p,q \in P, p \neq q, \forall m \in M \quad (32)$$

The constraint *(32)* is the wavelength clash constraint. This RWA constraint makes sure that a distinct wavelength is provided for all the lightpaths that share a common link.

$LAR_{p,m}$ constraints:

$$\alpha_{p,q} + T^{m}_{p,q} - LAR^{m}_{p,q} \leq 1, \forall p,q \in P, p \neq q, \forall m \in M \quad (33)$$

$$\alpha_{p,q} \geq LAR^{m}_{p,q}, \forall p,q \in P, p \neq q, \forall m \in M \quad (34)$$

$$T_{p,q}^{m} \geq LAR_{p,q}^{m},\ \forall p,q \in P,\ p \neq q,\ \forall m \in M \quad (35)$$

$$LAR_{p,m} = \sum_{q \in P, p \neq q} LAR_{p,q}^{m} + a_{p,m},\ \forall p \in P,\ \forall m \in M \quad (36)$$

LAR_p constraints:

$$\alpha_{p,q} + T_{p,q} - LARP_{p}^{q} \leq 1,\ \forall p,q \in P,\ p \neq q \quad (37)$$

$$\alpha_{p,q} \geq LARP_{p}^{q},\ \forall p,q \in P,\ p \neq q \quad (38)$$

$$T_{p,q} \geq LARP_{p}^{q},\ \forall p,q \in P,\ p \neq q \quad (39)$$

$$LAR_{p} = \sum_{q \in P, p \neq q} LARP_{p}^{q} + 1,\ \forall p \in P \quad (40)$$

The constraints *(33)* - *(35)* set the value of $LAR_{p,q}^{m}$ to 1, if the lightpath *q* is in the link-sharing with the lightpath *p* in the interval *m*. All the values of $LAR_{p,q}^{m}$ are summed over *q* in the constraint *(36)* to acquire the number of lightpaths that are in the LAG of the lightpath *p* (including itself) in the interval m ($LAR_{p,m}$). Similarly, the constraints *(37)* - *(40)* calculate the number of lightpaths that are in the LAG of the lightpath *p* (including itself) over all the intervals (LAR_{p}).

$IAR_{p,m}$ constraints:

$$\delta_{p,q} + T_{p,q}^{m} - IAR_{p,q}^{m} \leq 1,\ \forall p,q \in P,\ p \neq q,\ \forall m \in M \quad (41)$$

$$\delta_{p,q} \geq IAR_{p,q}^{m},\ \forall p,q \in P,\ p \neq q,\ \forall m \in M \quad (42)$$

$$T_{p,q}^{m} \geq IAR_{p,q}^{m},\ \forall p,q \in P,\ p \neq q,\ \forall m \in M \quad (43)$$

$$IAR_{p,m} = \sum_{q \in P, p \neq q} IAR_{p,q}^{m} + a_{p,m},\ \forall p \in P,\ \forall m \in M \quad (44)$$

IAR_p constraints:

$$\delta_{p,q} + T_{p,q} - IARP_p^q \leq 1, \forall p,q \in P, p \neq q \quad (45)$$

$$\delta_{p,q} \geq IARP_p^q, \forall p,q \in P, p \neq q \quad (46)$$

$$T_{p,q} \geq IARP_p^q, \forall p,q \in P, p \neq q \quad (47)$$

$$IAR_p = \sum_{q \in P, p \neq q} IARP_p^q + 1, \forall p \in P \quad (48)$$

The constraints *(41)* - *(43)* set the value of $IAR_{p,q}^m$ to 1 if the lightpath *q* is in the node and channel sharing with the lightpath *p* in the interval *m*. These values are summed over *q* in the constraint *(44)* to obtain the number of lightpaths that are in the IAG of the lightpath *p* (including itself) in the interval *m* ($IAR_{p,m}$). The constraints *(45)* - *(48)* calculate the IAR_p value to obtain the number of lightpaths that are in the IAG of the lightpath *p* (including itself) over all the intervals.

Attack radius constraints:

$$LAR_{p,m} + IAR_{p,m} \leq maxAR_{p,m}, \forall p \in P, \forall m \in M \quad (49)$$

$$LAR_p + IAR_p \leq maxAR_p, \forall p \in P \quad (50)$$

The constraints *(49)* and *(50)* show the calculation of variables $maxAR_{p,m}$ and $maxAR_p$ respectively. The $maxAR_{p,m}$ variable can be defined as a maximum limit on all the attack radius values obtained for all the lightpaths *p* during the interval *m*. Whereas, the $maxAR_p$ variable can be defined as a maximum limit for the attack radius values obtained for any lightpath *p* over *all* the intervals.

Hop count constraints:

$$\sum_{e:i\to j\in E} x_{p,e} \leq H, \forall p \in P \qquad (51)$$

Finally the constraint *(51)* limits the path length of a lightpath *p* with a maximum bound on the number of hops. This constraint reduces the risk of unnecessary interactions between the lightpaths [2] by limiting the number of hops in the transmission of lightpath *p*.

3.3.1 Modification for Fixed window scheduled traffic model:

In the fixed window scheduled traffic model the $st_{p,m}$ of the demand *p* is fixed and is given as an input to the ILP [17]. For both the STMs, the remaining ILP formulations for scheduling the demands is similar. Thus, just by adjusting the start time of the lightpath request *p*, the ILP formulation becomes feasible for the fixed window scheduled traffic model. Here, a new constraint is proposed for this purpose.,

$$st_{p,\alpha_p} = 1, \forall p \in P \qquad (52)$$

The constraint *(52)* states that the larger window start time (α_p) is directly taken as the starting interval for the lightpath demand *p*. This allows the start time of the lightpath demand to be fixed to a specified time interval, and states that each lightpath demand is scheduled to start in the earliest possible time interval.

3.4 Some alternative objective functions:

In this section, four more objective functions are defined to support the proposed ILP formulation *(ILP_SUM_$AR_{p,m}$)*. All these objective functions are proposed for the same set of constraints stated in the section 3.3.

3.4.1 ILP Formulation: $ILP\_MaxAR_{p,m}$

The following objective function is a special case of the objective function proposed in the section 3.3. The value to be minimized under this objective function is calculated by the constraint *(49)*.

Objective function 2:

$$Minimize\ MaxAR_{p,m} \qquad (53)$$

The objective function *(53)* minimizes the maximum bound of all the $AR_{p,m}$ values for all the lightpaths $p \in P$ in all the intervals m $\in M$.

3.4.2 ILP Formulation: $ILP\_SUM\_AR_p$

An alternative objective function is proposed to handle a different scenario of attack propagation. The following objective function minimizes the total attack radius *($AR_p = LAR_p + IAR_p$)* for all the lightpaths. The AR_p value can be defined as the total attack radius of any lightpath *p* over all the intervals.

Objective function 3:

$$Minimize\ \sum_{p \in P} (LAR_p + IAR_p) \qquad (54)$$

The objective function *(54)* uses the variables *(LAR_p, IAR_p)* calculated under the constraints *(37)* - *(40)* and *(45)* - *(48)*.

3.4.3 ILP Formulation: ILP_MaxAR_p

The following objective function is a special case of the objective function proposed in the section 3.4.2. The constraint *(50)* calculates the value $MaxAR_p$ value.

Objective function 4:

$$Minimize\ MaxAR_p \qquad (55)$$

The objective function *(55)* minimizes the maximum bound on all the AR_p values for all the lightpaths $p \in P$.

3.4.4 ILP Formulation: *ILP_SPATH*

An alternative objective function is built for the proposed ILP formulation to make it unaware of the attack propagation in the network. Hence, the overall path length is minimized as an objective to make it a *traditional RWA for sliding window scheduled traffic model*.

Objective function 5:

$$Minimize\ \sum_{p \in P} \sum_{e:i \to j \in E} x_{p,e} \qquad (56)$$

The objective function *(56)* minimizes the total path length for any lightpath *p* on any edge *e* in the physical topology. This objective does not take into consideration any of the attack aware constraints in the ILP formulation. Thus, the interactions among the

lightpaths that trigger various attacks in the network won't be controlled in the *ILP_SPATH* formulation

3.5 A summary of ILP formulations:

In this section all the variations of ILP formulations and different approaches that are discussed in the above sections are summarized and tabulated. A total of three RWA approaches are discussed, namely

1. Attack aware RWA for sliding window scheduled traffic model,

2. Attack aware RWA for fixed window scheduled traffic model and

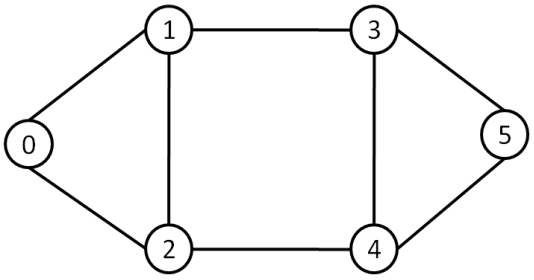
3. Attack unaware RWA for sliding window scheduled traffic model (ILP_SPATH).

Table 3.1 Different variations of ILP formulations

Name	ILP Formulation	Objective function
Objective function 1	$ILP\_SUM\_AR_{p,m}$	$Minimize \sum_m \sum_{p \in P} (LAR_{p,m} + IAR_{p,m})$
Objective function 2	$ILP\_MaxAR_{p,m}$	$Minimize\ MaxAR_{p,m}$
Objective function 3	$ILP\_SUM\_AR_p$	$Minimize \sum_{p \in P} (LAR_p + IAR_p)$
Objective function 4	ILP_MaxAR_p	$Minimize\ MaxAR_p$

Under every model four different objectives are proposed, namely $ILP\_SUM\_AR_{p,m}$, $ILP\_MaxAR_{p,m}$, $ILP\_SUM\_AR_p$ and ILP_MaxAR_p. The table 3.1 summarizes different objective functions and their respective ILP formulations.

3.6 An illustrative example:



(a)

	s_p	d_p	α_p	ω_p	T_p
LP0	4	0	1	4	2
LP1	4	3	0	5	4
LP2	4	2	0	5	4
LP3	5	4	1	5	3
LP4	3	2	0	3	2

(b)

Figure 3.1: (a) A sample physical topology and (b) A sample set of lightpath requests

An illustrative example is discussed in this section in order to explain the working of the proposed ILP. The physical topology used in this example is depicted in the figure 3.1 (a). It is a 6-node topology with 8 bi-directional links. A set of five lightpath requests is given in the figure 3.1 (b). According to the lightpath requests table, the lightpath LP0 originates from node-4 and ends at node-0. The larger window timings for this lightpath start at interval-1 and end at interval-4 and have a DHT of 2 intervals. Besides, it is assumed that a pair of wavelengths is available on each fiber and a maximum of five intervals is offered for use.

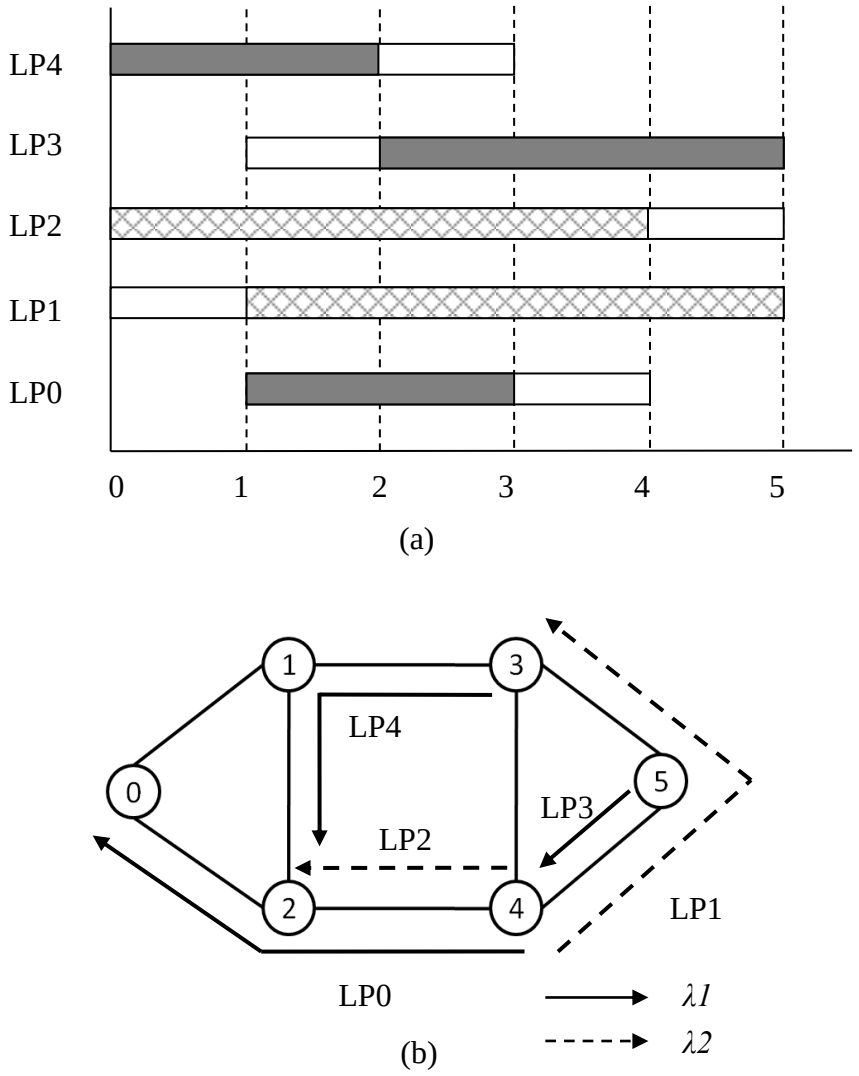


Figure 3.2: (a) Start time allocation and (b) Routing of lightpath demands.

The lightpath allocation involving sliding window scheduled traffic model provides an appropriate start time for all the lightpath requests. Hence, in addition to the routing of lightpath demands, our ILP assigns an appropriate start time to all the lightpaths. One possible solution is shown in the Figure 3.2 (a) & (b). The lightpath LP0 starts at the interval 1 and is active for two consecutive intervals 1 and 2 as the DHT for this commodity is 2. Likewise, all other lightpaths are initiated at a proper time interval.

The solid lines and the dashed lines in Figure 3.2 (a) and (b) represent the wavelengths $\lambda 1$ and $\lambda 2$ respectively. Figure 3.2 (b) shows the routing of lightpath demands on the given physical topology. For instance, the lightpath LP0 passes through the edges 4-2 and 2-0 using wavelength $\lambda 1$. In our attack aware ILP, this routing, start time and wavelength assignment for the lightpath requests is carried out in order to minimize the total attack radius of all the lightpath demands.

Table 3.2 The LAR values for all the lightpath demands in all the intervals

	LP0		**LP1**		**LP2**		**LP3**		**LP4**		**TOTAL**
	$LAG_{p,m}$	$LAR_{p,m}$	$LAG_{p,m}$	$LAR_{p,m}$	$LAG_{p,m}$	$LAR_{p,m}$	$LAG_{p,m}$	$LAR_{p,m}$	$LAG_{p,m}$	$LAR_{p,m}$	max $LAR_{p,m}$
INTERVAL 0	-	0	-	0	LP2	1	-	0	LP4	1	1
INTERVAL 1	LP0,LP2	2	LP1	1	LP0,LP2	2	-	0	LP4	1	2
INTERVAL 2	LP0,LP2	2	LP1	1	LP0,LP2	2	LP3	1	-	0	2
INTERVAL 3	-	0	LP1	1	LP2	1	LP3	1	-	0	1
INTERVAL 4	-	0	LP1	1	-	0	LP3	1	-	0	1
TOTAL	LP0,LP2	4	LP1	4	LP0, LP2	6	LP3	3	LP4	2	max LAR_p =2

Hence, it is essential to observe the calculation of LAR and IAR values. Table 3.2 shows the LAR values obtained from the given example solution. From the Figure 3.2 (b), we can observe that the lightpaths LP0 and LP2 are using the same edge 4-2 on different wavelengths. So, the LAR values in the intervals 1 and 2 become 2 for both the

demands. But, as the lightpath LP0 is inactive during the intervals 0 and 3, the LAR values for the lightpath LP2 are recorded as 1.

Table 3.3 The IAR values for all the lightpath demands in all the intervals

	LP0		**LP1**		**LP2**		**LP3**		**LP4**		**TOTAL**
	$IAG_{p,m}$	$IAR_{p,m}$	$IAG_{p,m}$	$IAR_{p,m}$	$IAG_{p,m}$	$IAR_{p,m}$	$IAG_{p,m}$	$IAR_{p,m}$	$IAG_{p,m}$	$IAR_{p,m}$	max $IAR_{p,m}$
INTERVAL 0	-	0	-	0	LP2	1	-	0	LP4	1	1
INTERVAL 1	LP0,LP4	2	LP1,LP2	2	LP1,LP2	2	-	0	LP0,LP4	2	2
INTERVAL 2	LP0,LP3	2	LP1,LP2	2	LP1,LP2	2	LP0,LP3	2	-	0	2
INTERVAL 3	-	0	LP1,LP2	2	LP1,LP2	2	LP3	1	-	0	2
INTERVAL 4	-	0	LP1	1	-	0	LP3	1	-	0	1
TOTAL	LP0,LP4,LP3	4	LP1,LP2	7	LP1, LP2	7	LP0,LP3	4	LP0,LP4	3	max IAR_p =2

Table 3.3 shows the IAR values for our sample solution. From the figure 3.2 (b) we can observe that the lightpaths LP1 and LP2 are traversing on the wavelength *λ2* and sharing the node 4. So, the values of IAR in the intervals 1, 2 and 3 become 2, as they are interacting in time. However, as the lightpaths are time disjoint in the intervals 0 and 4, the value of the IAR remains 1 in their respective active intervals.

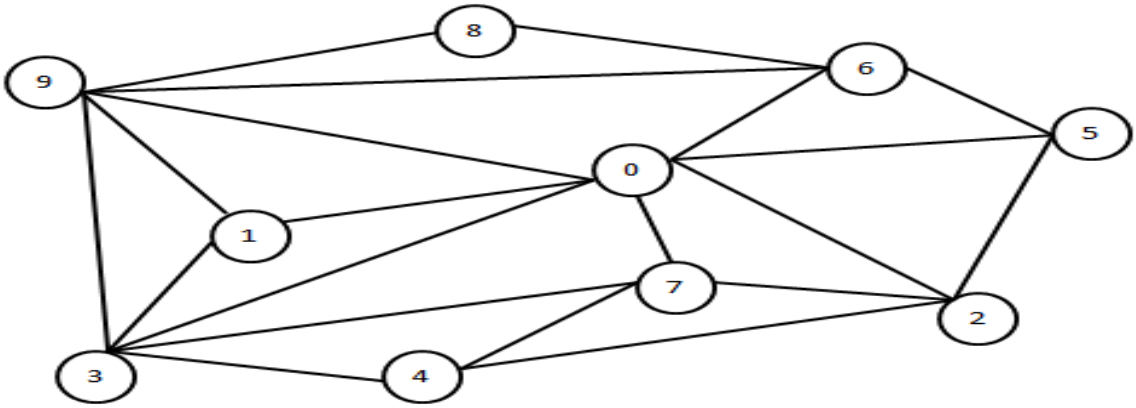
4. EXPERIMENTATION AND RESULTS

This chapter presents the analysis of the simulation results for the proposed ILP formulations. All transitions proposed for the ILP formulation in Chapter 3 are implemented to assist in testing the performance of the proposed system. Optimal solutions for all simulations are obtained by solving the ILP formulations using IBM ILOG CPLEX 12.6.2 optimization studio.

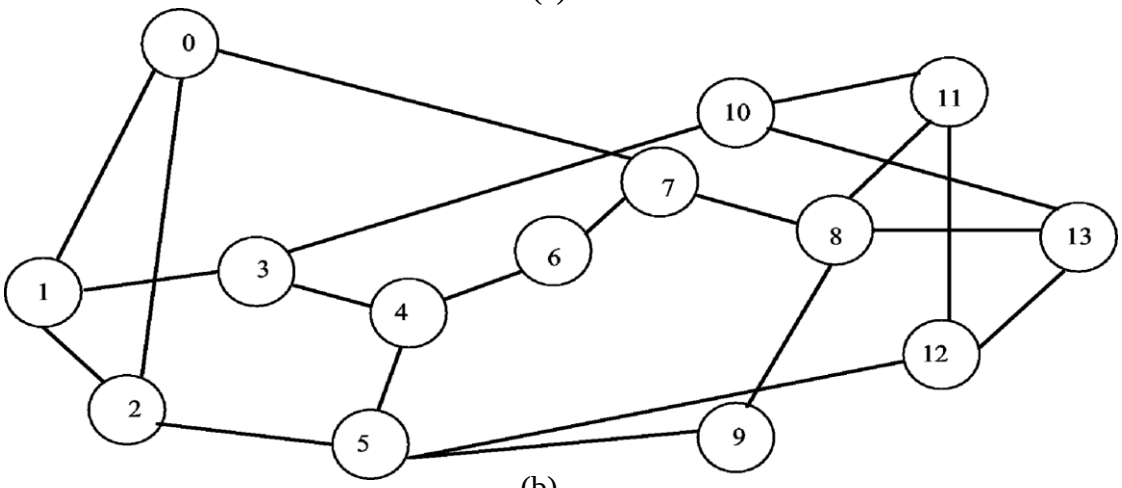
4.1 Simulation parameters

Three well known network topologies of varying sizes are used for this experimentation. Figure 4.1 shows the 10-node network with 20 bidirectional links (DT10 [37]), 14-node network with 21 bidirectional links (NSFNET [36]) and 20-node network with 31 bidirectional links [38], respectively. These physical topology files are given as a text file and consist of all edges of the network, where each row represents an individual source and destination pair.

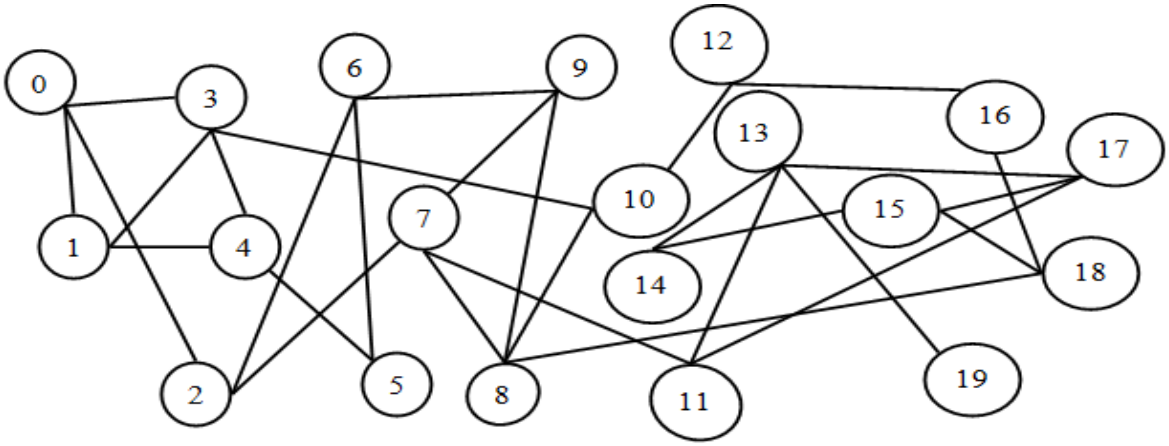
The lightpath demands for this model are different from the fixed window traffic model in [17]. Unlike the fixed window demand set, the start and end times of the larger time window and DHT values are given in place of exact start and end times of lightpath demands. Hence, the sliding window demand set has five parameters, namely source, destination, larger window start time, larger window end time and DHT. All these values are stored in a text file where an individual row represents a single lightpath demand.



(a)



(b)



(c)

Figure 4.1 (a) 10-node network topology (DT10)[37], (b) 14-node network topology (NSFNET)[36] & (c) 20-node network topology [38].

According to the lightpath classification in [17], the demand sets are divided into three different categories on the basis of overlapping. It is clear that, the longer the DHT, the more lightpaths tend to overlap in time, leading to increased congestion. Hence, to test the proposed system with different levels of complexity, the following three variations of demand sets are used.

1. *Low Demand Overlap* (LDO),

2. *Medium Demand Overlap* (MDO) and

3. *High Demand Overlap* (HDO).

If the DHT ranges from 1 to 10, 1 to 24 and 10 to 24 intervals, demand sets are said to be in LDO, MDO and HDO range respectively.

4.2 Comparison of experimental results

The attack aware RWA for the fixed window scheduled traffic model has been already shown as a better solution to minimize the attack propagation in optical networks, when compared with the traditional attack unaware approach [17]. In the fixed window scheduled traffic model, the demand start time and end time are specified in advance. However, in our proposed approach, the most flexible and effective sliding window scheduled traffic model has been considered. Hence, we examine how these additional advancements in demand scheduling and routing techniques influence the attack aware RWA problem.

In this section, various simulation results for the proposed ILP formulations with different sizes of demand sets and network topologies are presented. All three levels of

traffic load (LDO, MDO & HDO) are considered for each size of demand set and network topology. For every such case, the average of five simulation results is recorded and tabulated in this section. The following three different simulation scenarios have been considered for each set of input parameters.

1. **Attack aware RWA for the sliding window scheduled traffic model**: This ILP formulation minimizes the attack radius and selects an appropriate start time for all the demands on the network. This is our proposed approach.

2. **Attack aware RWA for the fixed window scheduled traffic model**: This approach also minimizes the attack radius for all the requested demands in order to achieve the attack aware RWA. However, each demand in this model starts at a predefined time interval.

3. **Attack unaware RWA for the sliding window scheduled traffic model**: This ILP formulation disregards the attack aware properties and focuses on providing a shortest path for each demand on the network.

4.2.1 Comparison of different network topologies

In this section, simulations are carried out for different sizes of network topologies ranging from 10 nodes to 20 nodes on the same number of demands (20 demands). Table 4.1 shows the results of the objective *ILP_SUM_AR*$_{p,m}$ for all three approaches and traffic loads. From this table we can observe that the values obtained for our proposed model *ILP_SUM_AR*$_{p,m}$ (Sliding) outperform the *ILP_SUM_AR*$_{p,m}$ (Fixed) and *ILP_SPATH* models.

Table 4.1 Objective values of $ILP\_SUM\_AR_{p,m}$ for 20 lightpath demands.

Objective Function: *Minimize* $\sum_m \sum_{p \in P}(LAR_{p,m} + IAR_{p,m})$									
	LDO			MDO			HDO		
No. of Nodes	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	214	222	270	356	374	496	660	698	904
14	190	214	226	420	476	584	814	858	1066
20	226	248	302	600	674	784	952	1046	1156

Table 4.2 Objective values of $ILP\_SUM\_AR_p$ for 20 lightpath demands.

Objective Function: *Minimize* $\sum_{p \in P}(LAR_p + IAR_p)$									
	LDO			MDO			HDO		
No. of Nodes	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	40	48	68	48	56	80	56	56	72
14	40	56	60	48	64	72	76	80	100
20	44	48	84	72	84	120	112	116	120

Tables 4.2 - 4.4 follow the same pattern as Table 4.1 and show a consistent reduction in the potential interactions among lightpaths. For example, Table 4.4 shows a rise in the improvement range for our proposed approach, ILP_MaxAR_p(Sliding), ranging from 40% to 66.7% with the attack unaware approach, *ILP_SPATH*, and 0% to 50% with the next best approach, ILP_MaxAR_p (Fixed).

Table 4.3 Objective values of $ILP\_MaxAR_{p,m}$ for 20 lightpath demands.

Objective Function: *Minimize* $maxARpm$									
	LDO			MDO			HDO		
No. of Nodes	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	2	3	5	3	3	5	3	3	7
14	2	3	5	3	4	5	3	5	8
20	3	4	4	5	7	9	8	8	9

Table 4.4 Objective values of ILP_MaxAR_{p} for 20 lightpath demands.

Objective Function: *Minimize* $maxARp$									
	LDO			MDO			HDO		
No. of Nodes	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	2	3	6	3	4	7	4	4	7
14	2	4	6	3	5	9	6	8	10
20	3	6	9	6	9	12	8	9	14

Figures 4.2 - 4.4 show the graphical representation of all three traffic scenario's for the results of objective function $ILP\_SUM\_AR_{p,m}$, where the x-axis represents the number of nodes (10, 14 and 20) and the y-axis shows attack radius values of varying ranges. From the graphs, we can observe a standard growth in attack radius values with an increase in the network complexity and demand overlapping. However, Figure 4.2

depicts a different behavior in the case of 14-node topology, which experienced lesser values of attack radius than the less complex 10-node topology. Various reasons, like the complexity levels of demand sets, number of nodes and links in the network and their distribution, influence such situations.

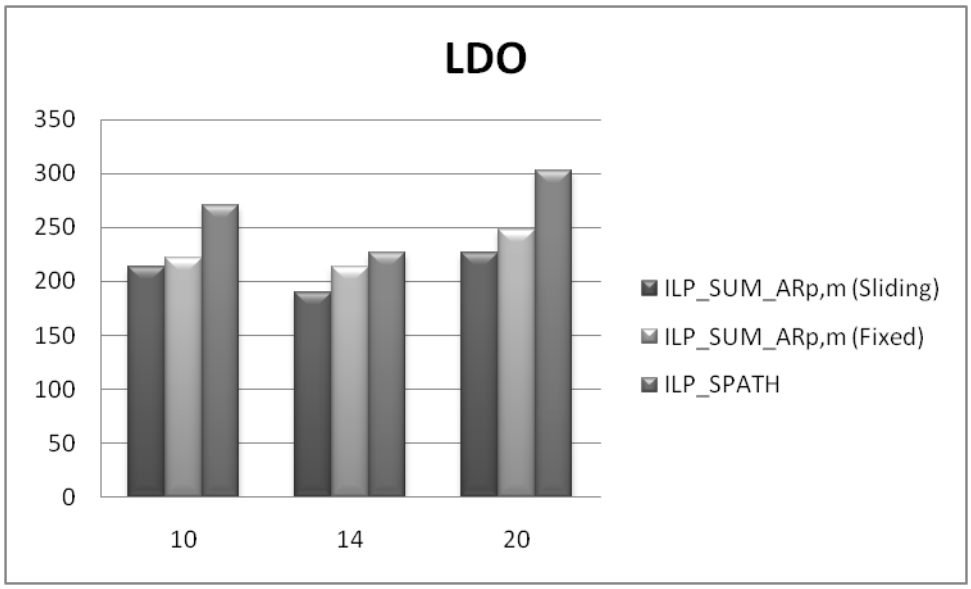


Figure 4.2 Objective values of *ILP_SUM_AR*$_{p,m}$ for LDO, with 20 lightpath demands.

It is observed that the gap between the sliding and fixed models is less when compared with the gap between the sliding and attack unaware models. The improvement range of 3.6% to 11.7% has been observed when the proposed model *ILP_SUM_AR*$_{p,m}$ (Sliding) is compared with *ILP_SUM_AR*$_{p,m}$ (Fixed). It increases from 15.9% to 28.2%, when the comparison is made between *ILP_SUM_AR*$_{p,m}$(Sliding) and *ILP_SPATH*. This indicates that the flexibility in choosing the appropriate demand start time can increase the capacity of attack handling in optical communication networks.

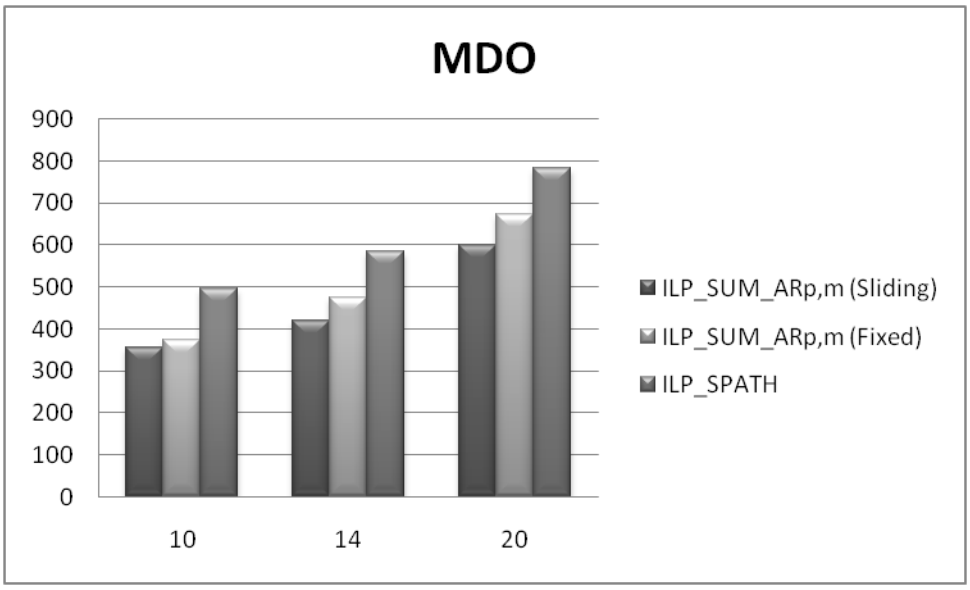


Figure 4.3 Objective values of $ILP\_SUM\_AR_{p,m}$ for MDO, with 20 lightpath demands.

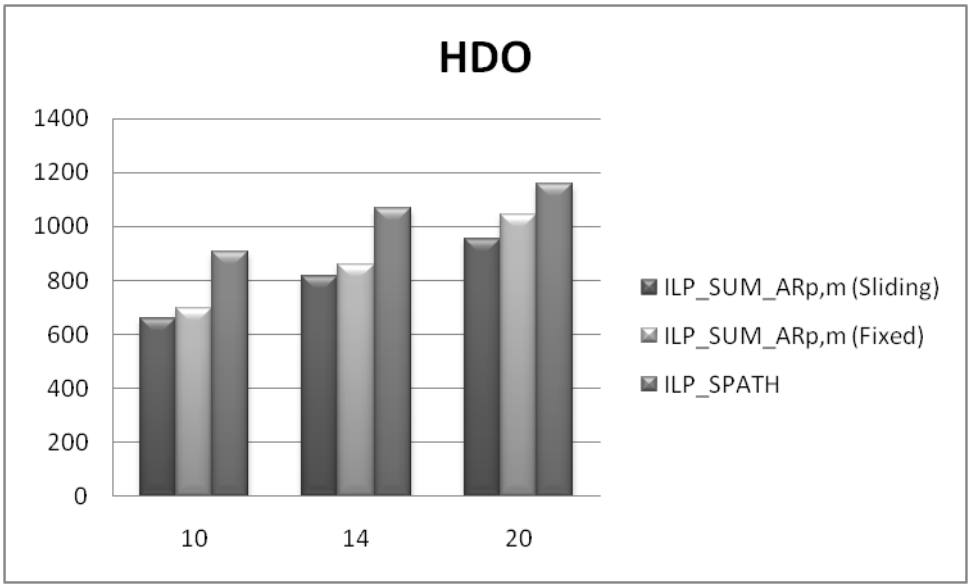


Figure 4.4 Objective values of $ILP\_SUM\_AR_{p,m}$ for HDO, with 20 lightpath demands.

4.2.2 Comparison of different demand sizes:

In this section, simulations are carried out for different demand sizes ranging from 10 to 40 numbers of demands under 10-node topology. All three instances of demand sets, namely LDO, MDO and HDO for all three approaches are considered in this comparison.

Table 4.5 Objective values of $ILP\_SUM\_AR_{p,m}$ for 10-node topology.

Objective Function: *Minimize* $\sum_m \sum_{p \in P}(LAR_{p,m} + IAR_{p,m})$									
	LDO			MDO			HDO		
No. of Demands	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	94	97	113	210	230	307	472	523	639
20	214	222	270	356	374	496	660	698	904
40	436	546	603	1189	1283	1338	2597	2706	3250

Table 4.6 Objective values of $ILP\_SUM\_AR_p$ for 10-node topology.

Objective Function: *Minimize* $\sum_{p \in P}(LAR_p + IAR_p)$									
	LDO			MDO			HDO		
No. of Demands	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	20	20	24	20	21	28	21	22	31
15	30	31	39	32	34	48	35	36	58
20	40	48	68	48	56	80	56	56	72

Table 4.7 Objective values of $ILP\_MaxAR_{p,m}$ for 10-node topology.

Objective Function: *Minimize maxARpm*									
	LDO			MDO			HDO		
No. of Demands	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	2	2	4	2	2	5	3	3	6
15	2	3	4	2	3	5	3	3	6
20	2	3	5	3	3	5	3	3	7

Table 4.8 Objective values of ILP_MaxAR_{p} for 10-node topology.

Objective Function: *Minimize maxARp*									
	LDO			MDO			HDO		
No. of Demands	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	2	2	4	2	3	4	3	3	6
15	2	3	5	3	3	6	4	4	6
20	2	3	6	3	4	7	4	4	7

Table 4.5, show objective values of the $ILP\_SUM\_AR_{p,m}$ with 10, 20 and 40 demands. Simulations are also carried out with 10, 15 and 20 demands for the $ILP\_SUM\_AR_{p}$, $ILP\_MaxAR_{p,m}$ and ILP_MaxAR_{p}. Tables 4.6 - 4.8 show the results of these objective values under all three traffic scenarios.

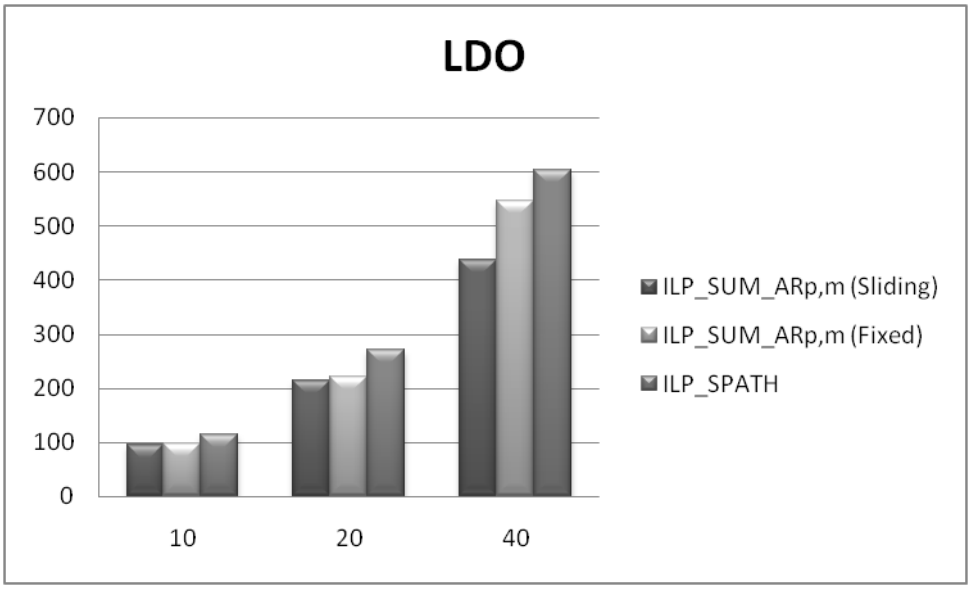


Figure 4.5 Objective values of $ILP\_SUM\_AR_{p,m}$ for LDO, with 10-node topology.

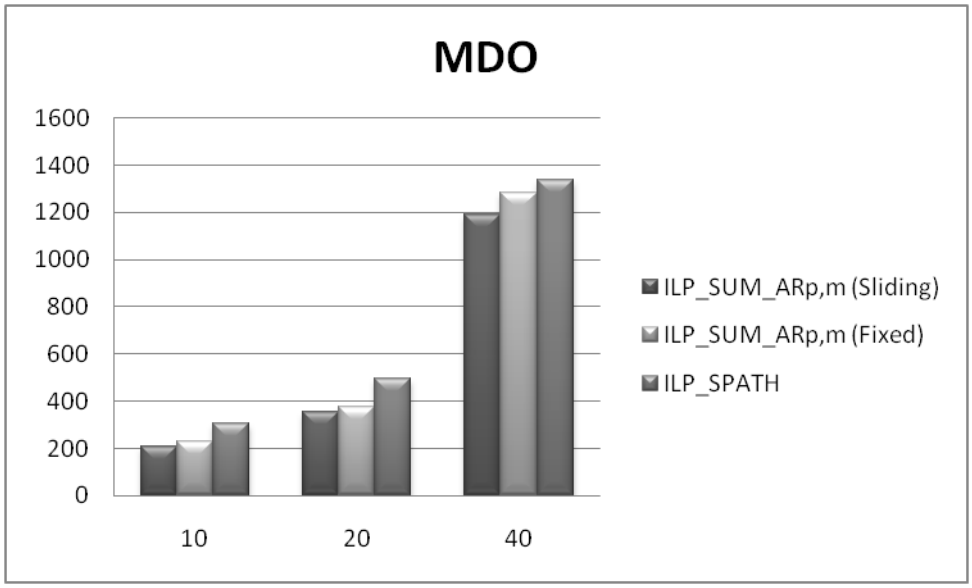


Figure 4.6 Objective values of $ILP\_SUM\_AR_{p,m}$ for MDO, with 10-node topology.

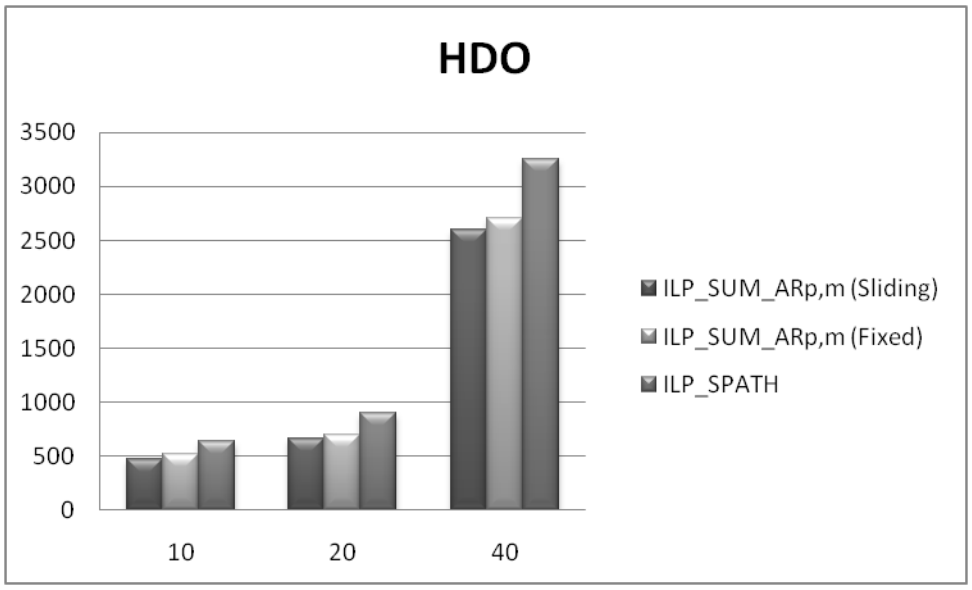


Figure 4.7 Objective values of *ILP_SUM_*$AR_{p,m}$ for HDO, with 10-node topology.

A standard growth is observed in the objective values with an increase in the demand size, under all three approaches. The proposed approach performs better than the existing best approach and attack unaware approach in all cases. For example, if we examine the *ILP_SUM_* $AR_{p,m}$ (Sliding) approach, an average of 3% to 20.1% improvement is observed when compared with the *ILP_SUM_*$AR_{p,m}$ (Fixed) approach and 11.1% to 28.2% with the *ILP_SPATH* approach.

A graphical representation of objective values of *ILP_SUM_*$AR_{p,m}$ for LDO, MDO and HDO traffic demands, with 10-node topology are shown in Figures 4.5 - 4.7. The objective values are depicted on x-axis and demand sizes on y-axis. A similar pattern is followed by all other proposed objectives.

4.2.3 Comparison of average path lengths:

In this section, average path lengths of a lightpath in all the given network topologies are compared for all three approaches (the sliding window approach, the fixed window approach and the attack unaware approach) under all proposed objectives. Tables 4.9 - 4.11 shows the tabulated results for all three categories of demand sets (LDO, MDO and HDO).

Table 4.9 Average path lengths of all proposed objectives for LDO demands.

	$ILP\_SUM\_AR_{p,m}$		$ILP\_SUM\_AR_{p}$		$ILP\_MaxAR_{p,m}$		ILP_MaxAR_{p}		*ILP_SPATH*
No. of Nodes	Sliding window approach	Fixed window approach	Sliding window approach	Fixed window approach	Sliding window approach	Fixed window approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	2.45	3.1	3.55	2.95	3	2.35	3.5	3	1.9
14	3.85	3.65	3.9	3.55	3.65	3.55	3.8	3.6	2.2
20	4.75	4.8	4.3	4.55	4.95	3.5	4.75	3.4	3.15

As expected, for all traffic loads, average path lengths increase with the number of nodes and links in the network. Tables 4.9 - 4.11, show that, *ILP_SPATH* continuously experience smaller average path lengths in all levels of the traffic complexity. Whereas, both sliding window and fixed window approaches, observe longer path lengths on average for all objectives. This happens as they try to minimize interactions among all lightpaths in the network, in order to control the attack propagation. Hence, the attack aware models try to select less crowded paths, resulting in choosing longer paths for

some lightpaths. This penalty associated with path lengths in attack aware approaches is acceptable as they provide secure demand allocation.

Table 4.10 Average path lengths of all proposed objectives for MDO demands.

	$ILP\_SUM\_AR_{p,m}$		$ILP\_SUM\_AR_{p}$		$ILP\_MaxAR_{p,m}$		ILP_MaxAR_{p}		ILP_SPATH
No. of Nodes	Sliding window approach	Fixed window approach	Sliding window approach	Fixed window approach	Sliding window approach	Fixed window approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	2.5	2.15	3.15	2.45	2.35	2.8	2.3	2.4	1.7
14	3.2	3.1	3.15	2.8	2.9	3.35	3	3.2	2.2
20	3.1	3.55	4.05	3.55	3.25	3.6	3.3	3	2.8

Table 4.11 Average path lengths of all proposed objectives for HDO demands.

	$ILP\_SUM\_AR_{p,m}$		$ILP\_SUM\_AR_{p}$		$ILP\_MaxAR_{p,m}$		ILP_MaxAR_{p}		ILP_SPATH
No. of Nodes	Sliding window approach	Fixed window approach	Sliding window approach	Fixed window approach	Sliding window approach	Fixed window approach	Sliding window approach	Fixed window approach	Attack unaware approach
10	2.05	1.9	1.95	1.9	2.55	2.6	2.6	2.65	1.5
14	2.55	2.5	2.6	2.45	3.25	2.6	2.85	3.25	2.05
20	4.7	4.8	4.35	4.3	3.7	4.15	4.05	3.6	3.4

5. CONCLUSION AND FUTURE WORK

5.1 Conclusion

In this thesis, we have proposed an ILP for the attack aware RWA for the sliding window scheduled traffic model. The main objective of this model is to reduce the total attack radius for all requested lightpath demands on the network. This model not only provides an appropriate route and an effective wavelength for the lightpaths, but also assigns a suitable start time for them, within a predefined time range. Our approach tries to route the lightpaths in order to minimize the number of lightpaths that share same nodes, links and wavelengths. This helps in reducing the effects of various physical layer attacks, namely in-band jamming attacks, out-of-band jamming attacks and gain competition attacks.

To test the performance of the proposed ILP, four different objective functions are offered for the same set of constraints. We have used different standard network topologies like NSFNET and DT10, to conduct our simulations. We have compared our model with the attack aware RWA for the fixed window scheduled traffic model [17] and attack unaware RWA for the sliding window scheduled traffic model. Our experimental results indicate that, the time flexibility associated with sliding window scheduling gives best objective values, when compared with the previous best technique and attack unaware model.

5.2Future work

In case of sliding and fixed window scheduled traffic models, the data transmission is continuous, once the lightpath is established between the source and destination nodes. The transmission process doesn't terminate until the entire data is transmitted to the other end. Perhaps, it may be possible to divide the scheduled lightpath demand into two or more individual segments and send them separately within the predefined time range. This traffic model is called segmented or non-continuous sliding window scheduled traffic model [16]. It takes the flexibility of demand allocation to another level by providing more scope for handling attacks. Hence, an attack aware RWA for the segmented sliding window traffic model can be implemented as a future work.

In order to obtain a fully secure and robust RWA, it may be possible to incorporate the fault tolerance techniques like shared and dedicated path protection [6], along with our attack aware ILP approach. Also, to handle larger network instances, a fast heuristic approach may be proposed to accommodate a large number of demands with faster execution times.

REFERENCES

[1] Jaekel, A., Bandyopadhyay, S., Al-Mamoori, S., & Varanasi, S. (2015, January). Security-Aware Dynamic Lightpath Allocation Scheme for WDM Networks. In *Proceedings of the 2015 International Conference on Distributed Computing and Networking* (p. 12). ACM.

[2] Skorin-Kapov, N., Chen, J., & Wosinska, L. (2010). A new approach to optical networks security: attack-aware routing and wavelength assignment.*Networking, IEEE/ACM Transactions on*, *18*(3), 750-760.

[3] Skorin-Kapov, N., Furdek, M., Pardo, R. A., & Mariño, P. P. (2012). 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.

[4] Manousakis, K., & Ellinas, G. (2013). Minimizing the Impact of In-band Jamming Attacks in WDM Optical Networks. In *Critical Information Infrastructures Security* (pp. 38-49). Springer International Publishing.

[5] Manousakis, K., & Ellinas, G. (2016). Attack-aware planning of transparent optical networks. *Optical Switching and Networking*, *19*, 97-109.

[6] Furdek, M., Skorin-Kapov, N., & Wosinska, L. (2015). Attack-Aware Dedicated Path Protection in Optical Networks.

[7] Dutton, H. J. (1998). *Understanding optical communications* (pp. 61-62). New Jersey: Prentice Hall PTR.

[8] http://stage.ofsoptics.com/knowledge_base/fiber101.php -- Retrieved on 15th Feb 2016.

[9] Senior, J. M., & Jamro, M. Y. (2009). *Optical fiber communications: principles and practice*. Pearson Education.

[10] http://www.slideshare.net/ankushsaini123/6796optical-fibres -- Retrieved on 15th Feb 2016.

[11] Massa, N. (2000). Fiber optic telecommunication. *Fundamentals of Photonics. University of Conneticut*.

[12] Ramamurthy, B., Feng, H., Datta, D., Heritage, J. P., & Mukherjee, B. (1999). Transparent vs. opaque vs. translucent wavelength-routed optical networks.

[13] Ramaswami, R. (1998). KN sivarajan," Optical Networks-A Practical Perspective". *Morgan Kaufmann Publishers, 1*, 998.

[14] Ramaswami, R., & Sivarajan, K. N. (1995). Routing and wavelength assignment in all-optical networks. *IEEE/ACM Transactions on Networking (TON)*, *3*(5), 489-500.

[15] Rouskas, G. N., & Perros, H. G. (2002). A tutorial on optical networks. In*Advanced lectures on networking* (pp. 155-193). Springer Berlin Heidelberg.

[16] Chen, Y. (2013). Resource Allocation for Periodic Traffic Demands in WDM Networks.

[17] Hangbo Zhao (2016). Attack Aware Routing and Wavelength Assignment of Scheduled Lightpath Demands.

[18] Jaekel, A., & Chen, Y. (2009). Resource provisioning for survivable WDM networks under a sliding scheduled traffic model. *Optical Switching and Networking*, *6*(1), 44-54.

[19] Manousakis, K., & Ellinas, G. (2013). Design of Attack-Aware WDM Networks Using a Meta-heuristic Algorithm. In *Artificial Intelligence Applications and Innovations* (pp. 677-686). Springer Berlin Heidelberg.

[20] Su, W., Sasaki, G., Su, C. F., & Balasubramanian, A. (2006). Scheduling of periodic connections with flexibility. *Optical Switching and Networking*, *3*(3), 158-172.

[21] Kuri, J., Puech, N., Gagnaire, M., Dotaro, E., & Douville, R. (2003). Routing and wavelength assignment of scheduled lightpath demands. *Selected Areas in Communications, IEEE Journal on*, *21*(8), 1231-1240.

[22] Andrei, D., Yen, H. H., Tornatore, M., Martel, C. U., & Mukherjee, B. (2009). Integrated provisioning of sliding scheduled services over WDM optical networks [Invited]. *Journal of Optical Communications and Networking*, *1*(2), A94-A105.

[23] Wang, B., Li, T., Luo, X., Fan, Y., & Xin, C. (2005, October). On service provisioning under a scheduled traffic model in reconfigurable WDM optical networks. In *Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on* (pp. 13-22). IEEE.

[24] Furdek, M. (2011). Physical-layer attacks in optical WDM networks and attack-aware network planning. *European Journal of Operational Research*,*178*(2), 1160-1167.

[25] Wu, T., & Somani, A. K. (2005). Cross-talk attack monitoring and localization in all-optical networks. *IEEE/ACM Transactions on Networking (TON)*, *13*(6), 1390-1401.

[26] Koçyiğit, A., GÖKIŞIK, D., & Bilgen, S. (2001). All-optical networking.*TURKISH JOURNAL OF ELECTRICAL ENGINEERING & COMPUTER SCIENCES*, *9*(2), 69-122.

[27] http://opticalengineering.spiedigitallibrary.org/article.aspx?articleid=1077128 -- Retrived on 25th February 2016.

[28] http://www.fiber-optic-tutorial.com/category/network-solutions/edfa-amplifier -- Retrived on 25th February 2016.

[29] http://www.internetworldstats.com/stats.htm -- Retrived on 9th March 2016.

[30] AMPL, I. CPLEX software. *ILOG website: www. ilog. com/ products/ cplex*.

[31] Rejeb, R., Leeson, M. S., & Green, R. J. (2006). Fault and attack management in all-optical networks. *Communications Magazine, IEEE*,*44*(11), 79-86.

[32] http://www.computerweekly.com/news/2240103787/Fiber-optic-networks-vulnerable-to-attack -- Retrieved on 22nd March 2016.

[33] http://securityaffairs.co/wordpress/37987/hacking/kevin-mitnick-hack-fiber-optic.html -- Retrieved on 22nd March 2016.

[34] Combs, G. (2007). Wireshark. *Web page: http://www. wireshark. org/last modified*, 12-02.

[35] https://en.wikipedia.org/wiki/OSI_model#Layer_1:_Physical_Layer -- Retrieved on 22nd March 2016.

[36] Cui, X., Li, Y., Cao, Y., Zhang, H., Guo, Y., & Zheng, X. (2007). Dynamic priority-based alternate routing for multiple classes of traffic in intelligent optical networks. *Optical Engineering*, *46*(2), 025002-025002.

[37] Wang, Z., Dueñas-Osorio, L., & Padgett, J. E. (2015). A new mutually reinforcing network node and link ranking algorithm. *Scientific reports*, *5*.

[38] Banerjee, D., & Mukherjee, B. (2000). Wavelength-routed optical networks: Linear formulation, resource budgeting tradeoffs, and a reconfiguration study.*IEEE/ACM Transactions on Networking (TON)*, *8*(5), 598-607.

VITA AUCTORIS

NAME:	Meenakshi Nizampatnam
PLACE OF BIRTH:	Tenali, India
YEAR OF BIRTH:	1989
EDUCATION:	Board of Intermediate, Andhra Pradesh, India, 2006 Vignan's Lara Institute of Technology and Science, India, 2011 University of Windsor, M.Sc., Windsor, ON, 2016