2016

Attack-aware routing and wavelength assignment for dynamic traffic in WDM networks

Marcel El Soury
University of Windsor

Attack-aware routing and wavelength assignment for dynamic traffic in WDM networks

by
Marcel El Soury

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
2015

Attack-aware routing and wavelength assignment for dynamic traffic in WDM networks

by
Marcel El Soury

APPROVED BY:

Dr. Myron Hlynka
Department of Mathematics and Statistics

Dr. Boubakeur Boufama
School of Computer Science

Dr. Arunita Jaekel, Advisor
School of Computer Science

Dr. Subir Bandyopadhyay, Advisor
School of Computer Science

December 04, 2015

DECLARATION OF ORIGINALITY

I certify that the above material describes work completed during my registration as graduate student at the University of Windsor.

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

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

ABSTRACT

Transparent Optical Networks (TONs) can communicate large amount of data at a high speed among nodes of the network. So, any type of failure whether caused by component failure or caused by an attack can cause a significant loss of data. In case of faults, the network can restore its functionality, by identifying the malfunctioning component of the network and solving the problem. This is not the case with a deliberate, malicious attack. That is why security and attack management is becoming a very important issue in WDM networks.

In the previous years, a number of researchers worked on solving the attack problem. One common approach is to plan the network in a way that minimizes the influence of an attack, by using appropriate routing and wavelength assignment (RWA) strategies. Most of the research in this area focuses on the static traffic model, where the set of traffic demands is known in advance. In this thesis, we propose a new security-aware RWA technique for dynamic traffic, using dedicated path protection. The goal is to improve the performance of WDM networks by accommodating more traffic demands, while reducing the probability of disruption due to malicious attacks.

DEDICATION

To my loving family:

Wife: Rania Nejem

Kids: Elias. Antoine and Christina

ACKNOWLEDGEMENTS

I would like to take this opportunity to convey my sincere thanks to my supervisors, Dr. Arunita Jaekel and Dr. Subir Bandyopadhyay, for their constant guidance and support all throughout my graduate studies. This work could not have been achieved without their continuous encouragement, advice and suggestions.

I would like to thank members of my M.Sc. thesis committee, Dr. Boubakeur Boufama, and Dr. Myron Hlynka for their valuable time, suggestions and constructive comments.

Finally, I would like to thank Dr. Ziad Kobti, for his extensive support and guidance.

Marcel El Soury

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1.Introduction

Optical network is a group of two or more computing devices linked via optical fibers in order to share resources, exchange files, or allow electronic communications. The main reason to use optical networks is that they can transfer a huge amount of data at a very high speed over wide areas.

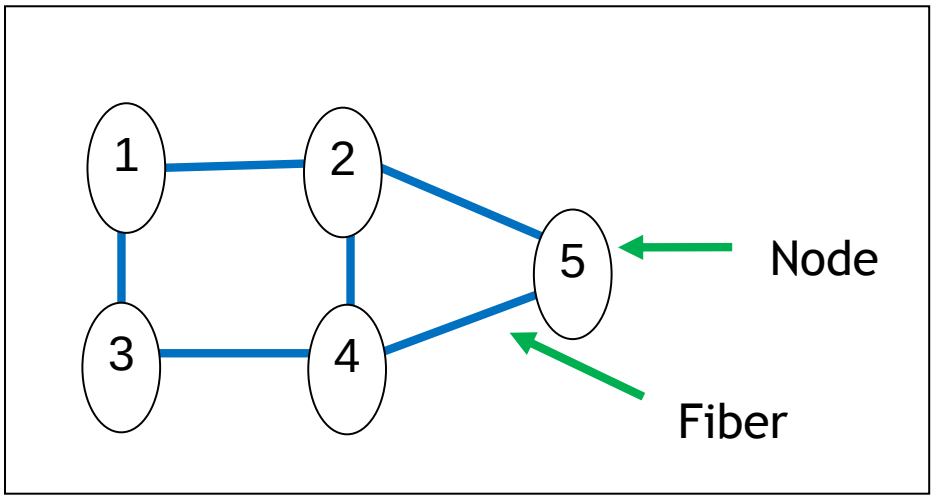

Figure 1-1 illustrates a 5 node networks

1.1 Wavelength Division Multiplexing (WDM)

An optical fiber can handle a very large amount of data, around 50 terabits per second. In the first generation of the optical networks, the huge capacity of the optical fiber (bandwidth) was used by only one user. None of the existing electronic devices, that can be connected to an optical network, can transmit or receive data at such a high speed. A certain method called Wavelength Division Multiplexing (WDM) is used in order to benefit as much as possible of the capacity of the optical fiber.

In WDM networks, the bandwidth is divided into non-overlapping ranges of frequencies, called channels, where each channel corresponds to a different carrier wavelength and is capable of transmitting data independently of the other channels.

The Wavelength Division Multiplexing method combine the data from different devices using different wavelengths and transmit them over one optical fiber and at the

receiving end the Wavelength Division Multiplexing method split the signals and distribute them to their appropriate destinations. WDM networks use switches in order to manage how different signals are directed to their corresponding destinations.

As an optical signal propagates along optical fibers, the quality of the signal, in terms of amplitude, bit error rate, shape and phase degrades. Amplifiers are used in optical networks in order to overcome this limitation.

1.2 Routing And Wavelength Assignment (RWA)

A lightpath allows two nodes to communicate in the optical domain. A lightpath traverses multiple fibre links in order to allow the communication between the source and destination nodes. Each lightpath is specified by a route and a carrier wavelength. The Routing And Wavelength Assignment (RWA) problem is act of choosing a route and assigning a wavelength to lightpaths while respecting that each lightpath should use its assigned wavelength over all its route (continuity constraint), and if two lightpaths are sharing a link they should use two different wavelengths (clash constraint).

The following figure shows two lightpaths using two links each, one from node 1 to node 4 (using carrier wavelength $\lambda 1$) and another lightpath from node 1 to node 3 (using carrier wavelength $\lambda 2$). Figure 1.2 illustrates how lightpaths respect the continuity and clash constraints.

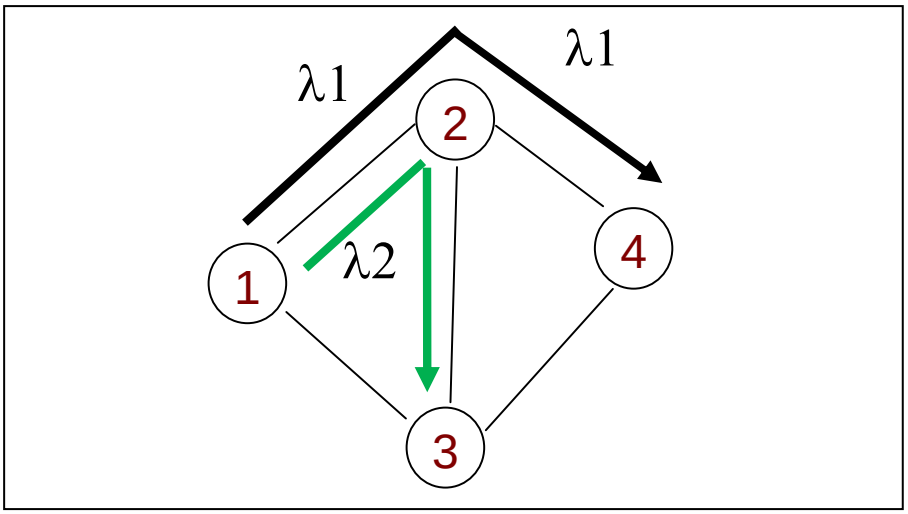

Figure 1-2 Continuity and Clash Constraints.

1.3 Attacks

While the data travels through the optical network as light signals, it is vulnerable to some physical impairments other then the degradation of the signal while propagating long distance. Physical layer impairments can be classified into linear and nonlinear effects. Regardless of the signal power, linear impairments affect the wavelengths (channels) individually, while nonlinear impairments cause disturbance and interference between the optical channels. Those external impairments can occur either when two or more lightpaths use same wavelength and share a common node (in-band) or if they use different wavelength but share a common link (out-of-band).

One of the characteristics of an optical amplifier is the gain competition. The amplifier has a limited number of upper-state photons used for signal amplification. These photons are distributed among the incoming signals proportionally to their powers. If the power of one of the signals exceeds a certain level (20 db above normal), it may influence the power to amplify the other signals and it may leak into other signals with lower power, which can influence the performance of the network. Malicious users can benefit from this case by injecting a high power signal on a legitimate signal and attack other signals in the network.

1.4 Attack-Aware RWA

In order to prevent the previously mentioned type of attacks, attack-aware RWA should be used. In attack-aware RWA two approaches can be used. The first approach is to design the network and route the lightpaths in a way to minimize the number of lightpaths that can be attacked simultaneously. The second approach is the path protection that has two types:

Shared path protection, where shared backup resources are used whenever an attack occurs.

Dedicated path protection, where a backup lightpath is assigned for each working lightpath. If the working lightpath is being attacked at a certain node or at a certain link then the data transmitted over that path will not reach its destination in a proper way.

Therefore, there is a need for a parallel path (backup lightpath) that does not share any node or any link with the working lightpath to be used in order to prevent the attacked part of the working lightpath. The backup lightpath is used when the working lightpath is under attack. This is the approach that we are going to use in our research because the dedicated path protection model is easier to implement and test and I left the shared path protection for future work.

Figure 1.3 illustrates a sample connection in the dedicated path protection approaches

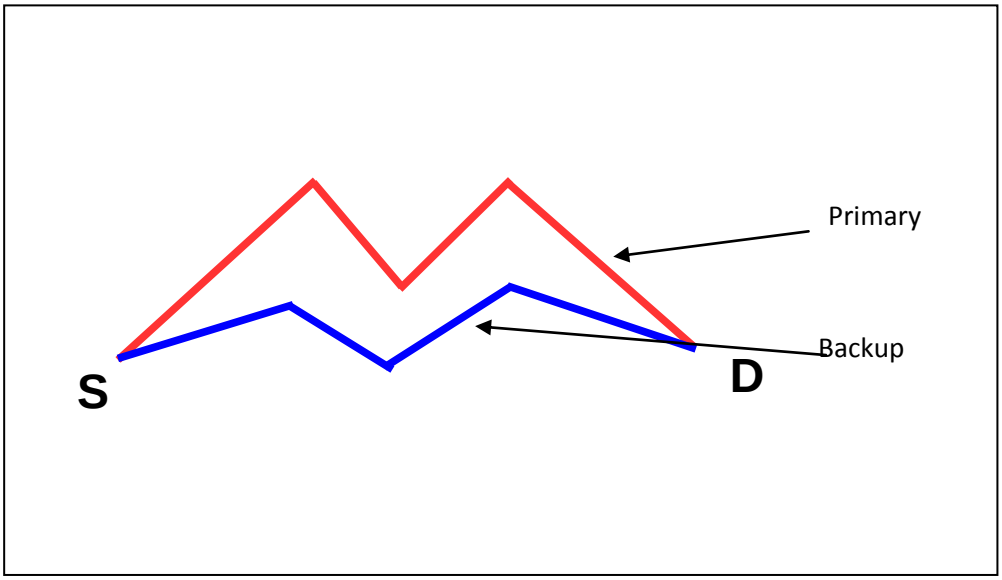

Figure 1-3 dedicated path protection

The primary and backup lightpaths of one connection must not share a common link or a common intermediate node to prevent simultaneous attack which leads to the lost of transmitted data over that connection.

Most work on security-aware RWA in WDM network considers the static traffic case, where all the lightpaths that are to be set up in the network are known beforehand. In the case of dynamic traffic, where lightpath requests arrive one by one in response to user requests, link failures were handled using path protection.

1.5 Solution Approach

In my thesis, I am going to study the attack-aware routing and wavelength assignment for dynamic traffic in WDM networks using the dedicated path protection approach. I believe that considering that an attacking signal on a certain channel can only influence certain adjacent channels will have a significant impact on the performance and cost of a network. I am going to study the blocking probability of a WDM network using my approach and compare it with the approach used in [5] and the approach that does not use any attack-aware model.

1.6 Organization of Thesis

Chapter 2 contains a detailed review of the fundamental concepts of WDM optical networks and other related topics on RWA. A review of the previous works on attack-aware in optical networks, is also presented in Chapter 2. Chapter 3 describes different security models and also the implementation of our algorithm. The results of the tests that we ran is found in chapter 4. And finally the conclusion is in chapter 5.

2 Background Review

2.1 Optical Networks:

Communication networks consists of two or more computing devices linked via a form of communication medium, in order to share resources, exchange files, or allow electronic communications [12]. The medium may be wired e.g. coaxial cable, optical fiber, twisted pair cables, or wireless e.g. radio, micro, infrared waves.

An optical network is a communication network that uses fiber optic cables as the main communication medium to convert and transmit data as light pulses between sender (source) and receiver (destination) nodes [13]. Optical networks allow fast and reliable communication, with very low loss of signal over long distances, and the capacity to transmit at very high data rates (bandwidth) [14],[15] .

2.2 Optical Fiber:

An optical fiber is a thin strand of glass that acts like a pipe for light over long distances. It is used as a medium to transmit light from one end to the other end of the fiber. Fig. 2.1 shows the cross-section of an optical fiber consisting of a core, which carries the actual light, surrounded by cladding, a layer of glass with lower refractive index than the core, a buffer coating and a jacket which act as two protective layers [16].

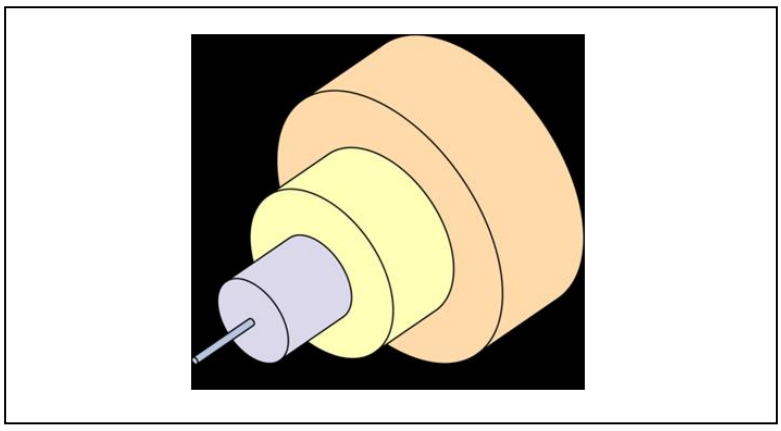

Figure 2-1 Single mode fiber [17]

The cladding has a lower refractive index than the core; this allows the signal to

propagate inside the core based on the phenomenon of *total internal reflection* [18]. If the angle of incidence at the boundary of the two materials is greater than a certain angle called *critical angle* [18], the wave cannot pass through and is entirely reflected (totally internally reflected).

The critical angle is measured with respect to the perpendicular line to the refractive boundary; it is the incident angle when the refracted light is parallel to the boundary at the incidence point (no signal is defused to the cladding). The light will be totally internally reflected if the incident angle is greater than the critical angle. Figure 2.2 illustrates the principle of refraction and total internal reflection.

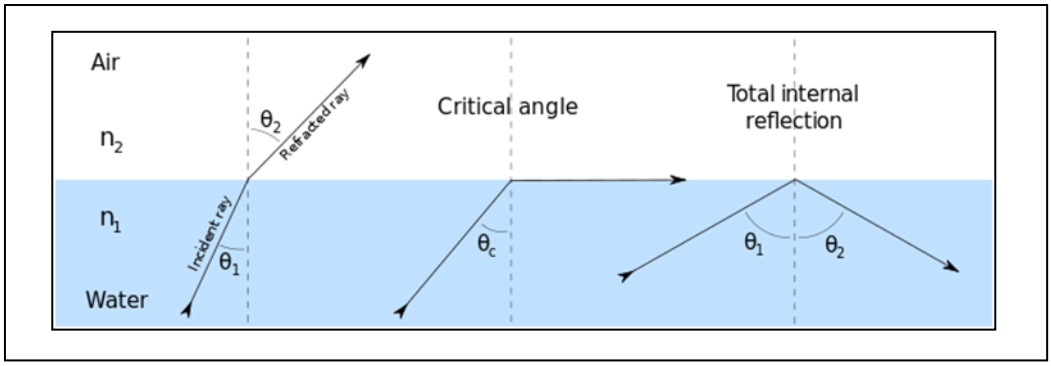

Figure 2-2 Example of total internal reflection [18]

There are two major types of fiber optic cables: single mode cable and multimode cable.

Single mode fiber:

Single mode cable is a single strand of glass fiber with a diameter of 8.3 to 10 microns. It carries higher bandwidth than multimode fiber [19]. Single mode fiber is used in many applications, where data is sent using multiple frequencies with same mode so only one cable is needed [19]. In single-mode fiber we can have waves of light with different frequencies but of the same mode. Single mode fiber has a higher transmission rate and up to 50 times more distance than multimode, but it also costs more. Single-mode fiber has a much smaller core than multimode. The small core and single (propagation mode) ray of light eliminates any distortion (signal degradation caused by light propagation of different frequencies at different speeds) that could result from

overlapping light pulses, and provides the least signal attenuation (loss of signal intensity). Most WDM networks use single-mode optical fibers.

Multimode fiber:

Multimode cable has a little bit bigger diameter, with a common diameters in the 50-to-100 micron range, it gives high bandwidth at high speeds over medium distances, such as within a building or on a campus. Typical multimode links have data rates of 10 Mbit/s to 10 Gbit/s over link lengths of up to 600 meters (2000 feet) [20]. Designers now use single mode fiber in new applications using Gigabit and beyond because multiple paths of light can cause signal distortion at the receiving end, resulting in an unclear and incomplete data transmission in long cables. Figure 2.3 represents a model of simple fiber optic data link [21], including a Source-User pair, Transmitter and Receiver with their connectors.

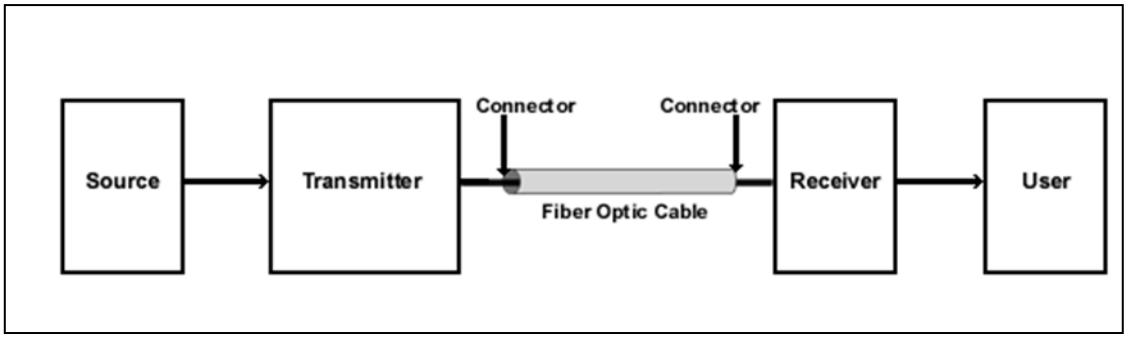

Figure 2-3 Example of simple fiber optic data link

2.3 Optical Network Components

2.3.1 Transmitter:

The transmitter in a fiber optic data link gets the data from the source as digital electrical signal, then emits and modulates a light coupled into the optical fiber cable in order to represent the received digital data [21]. The main component of a transmitter is a laser diode (LD) that can be modulated at a very high speed and produces a coherent high power light that can be coupled efficiently to the fiber optic cable.

2.3.2 Receiver:

Fiber optic cable provides the data to the receiver as an optical signal. The receiver then translates it to its best estimates of the binary data. It then provides this data to the user in the form of an electrical signal. The main component of a receiver is a photodiode. The photodiode senses the light output of the fiber optic cable which is detected and then converted to an electrical signal. The demodulation decision process is carried out on the resulting electrical signal to identify the digital data it represents [21].

2.3.3 Connectors:

The connector is a mechanical device mounted on the end of a fiber optic cable, transmitter or receiver to direct and collect light. It allows it to be matched to a similar device. The Transmitter provides the information light to the fiber optic cable through a connector. The Receiver gets the information light from the fiber optic cable through a connector. [10].

2.4 Wavelength Division Multiplexing (WDM)

The bandwidth that optical fiber cable provides is much more than the bandwidth required by a single source-user pair, which leads to a great waste of the optical fibre capacity. The solution of this problem is to make multiple source-user pairs share the huge bandwidth of the same fiber. The technique that allows this sharing of optical fibre bandwidth is known as *multiplexing* [11]. At the source side, there is a *multiplexer* that combines the different signals and sends them over the optical fiber cable. At the user side, there is a *demultiplexer* that separates the combined stream and directs each of these signals to the corresponding User.

Figure 2.4 gives simple illustration of multiplexing and demultiplexing [22]:

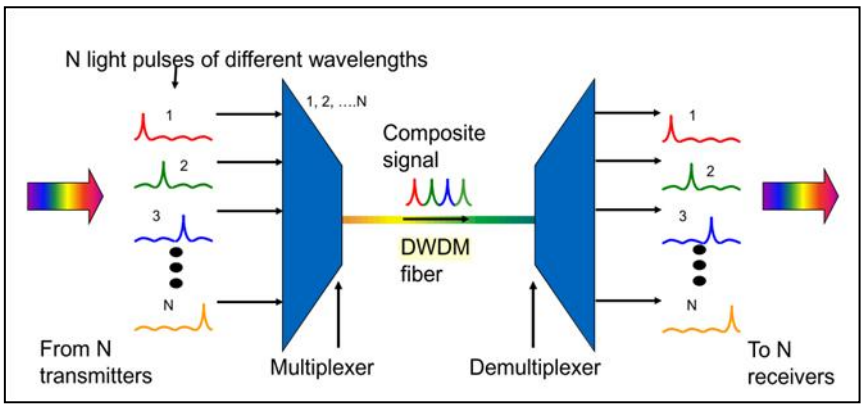

Figure 2-4 Example of multiplexing

Wavelength division multiplexing (WDM) is a technique that increases the utilization of the capacity of optical fiber link by combining, transmitting, and separating data into several channels [22]. The data stream from each source is assigned an optical wavelength. The multiplexer then couples all of optical signals generated for all sources into the fiber optic cable. These different wavelength optical signals propagate simultaneously. Since our focus in this thesis is on WDM, we will explain it in more details in the coming section.

A single mode optical fiber cable has a very low loss transmission with an enormous bandwidth (tens of terahertz) that no existing opto-elctronic sender or receiver device can handle. Wavelength Division Multiplexing (WDM) addresses these problems by dividing the bandwidth into several low speed channels (10 Gbits/s to 100 Gbits/s) and reaching a high total data rate by combing several channels.

There are two types of WDM:

i) coarse wavelength division multiplexing (CWDM) [23], which uses a relatively small number of channels, four or eight, and a large channel spacing of 20 nm, and

ii) dense wavelength division multiplexing (DWDM), which uses a large number of channels (40, 80, or 160), and a correspondingly small channel spacing of 12.5, 25, 50 or 100 GHz.

2.5 Routing And Wavelength Assignment (RWA)

In optical networks, users communicate via end-to-end optical channels known as *lightpaths* [24]. A lightpath may traverse multiple fibre links in order to allow the communication between two nodes. Each lightpath is characterized by a route and a wavelength. When establishing a lightpath, two constraints should be respected: the *wavelength continuity constraint* and the *wavelength clash constraint*. The wavelength continuity constraint states that each lightpath must use the same wavelength on all the fiber links that it traverses. The wavelength clash constraint states that when two lightpaths share a common fiber link each should be assigned a different wavelength. The *routing and wavelength assignment* (RWA) [25] problem is to find a route over the physical topology and an available wavelength on the selected route, for each lightpath request. If no such route and wavelength can be found, then the connection request is blocked.

The RWA problem can be divided into two main categories based on the traffic model: static traffic and dynamic traffic. In the *static* RWA problem, all lightpath requests are known in advance, and the routing and wavelength assignment operations are performed off-line [9]. Different objectives can be used, e.g. to minimize the number of wavelengths used, or to maximize the number of connections that can be established. In the *dynamic* RWA problem, lightpath requests arrive randomly and resources are allocates on-demand [9]. Typically, the objective is to minimize the blocking probability [9].

2.6 Fault Management in Optical Networks

In a WDM network, failure of a network element may cause failure of several optical channels leading to large data loss which can interrupt communication services. To deal with network element failure two main strategies can be used: protection and restoration [3]. In *protection* based approaches, backup resources of the network in advance are reserved in advance. In *restoration* based approaches, online spare backup resources are found and used after fault is detected.

Protection techniques may be further classified as *link* protection or *path* protection [28].

In the case of link protection, backup paths and wavelengths are reserved around each link on the primary path. These backups are used by all the connections traversing the failed link. In the case of path protection, for each connection a primary path and a backup path are reserved. In case of any failure on the primary path the connection will automatically switch to the backup path.

There are two types of path-protections: dedicated path-protection and shared path-protection.

Protection	**Description**
dedicated path-protection	Allocate a dedicated backup path for each primary path
shared path-protection	sharing backup path resources among multiple primary paths

2.6.1 Dedicated Path Protection (DPP)

Dedicated path protection is an end-to-end protection scheme used in network architectures to protect against inevitable failures of network that might affect the services offered to end customers

Using dedicated path protection scheme, if a connection is to be established between node S and node D, two lightpaths should be allocated for this connection, a primary path and a backup path. In case of no failure, the primary path is used to transmit data. If a fault occurs along the primary path then the backup path is used. The two allocated paths (primary and backup) should have no common links (i.e. should be link disjoint) in order to prevent simultaneous failure of both paths. In case where the common resource fail then both paths will be discarded and the connection will not be established as consequence.

There are two techniques that could be considered while using dedicated path protection, 1+1 and 1:1.

1+1 Technique:

In 1+1 technique, data is transmitted simultaneously over both the primary and backup paths [26]. First, the data transmitted over the primary path is received by the last node. It gets checked and if any error is detected, then automatically the backup path is considered and checked. This technique is fast but it is bandwidth consuming.

1:1 Technique:

The 1:1 technique is similar to the 1+1, but data is not transmitted on the backup path until a failure occurs. If a failure occurs on the primary path, the backup lightpath is established and is used to re-route the traffic. This technique is a little bit slower.

2.6.2 Shared path protection (SPP)

The approach of shared path protection scheme is to share a backup channel among different primary paths. In other words, one backup channel can be used to protect various primary paths [26]. Using the shared path protection technique can help use the network resources in more efficient way. Although it is using the backup path concept, but it allows sharing of resources among multiple backup paths. A backup path is used whenever failure occurs along the corresponding primary path.

2.7 Attacks in Optical Networks

Because of the high rate of data transmitted over transparent optical networks, any failure or intentional attack can have a serious influence on the amount of data that can be corrupted. Therefore security and attack management is becoming a very important issue. Transparency is an optical network feature that allows routing and switching of data without conversion or regeneration. This is one important reason that makes an attack have a serious impact on data in a transparent optical network. Transparency introduces significant changes to the security paradigm of optical networks by allowing signals to propagate through the network undetected. This creates a security vulnerability which can be used by attackers to degrade the network performance [27].

The damage caused by an attack is more dangerous and more difficult to prevent than link or node failure. A component failure can affect lightpaths using that component, while an attack can affect many users and many parts of the network. The transparent optical network components that are most vulnerable to attacks are: the fiber, the amplifier and the switch. The fiber attack caused by cutting or bending the fiber can also be considered as component failure because it can be either cut or bent [27]. However another type of attack called *jamming attack* [27], is caused by using a legitimate channel to insert a high powered signal. A jamming attack causes *crosstalk* (the high powered signal leaks into another signal) [27] in amplifiers and switches, which leads to degradation and service disruption.

Crosstalk is one of the most dangerous types of attacks because it does not affect only the attacked connection but it has the ability to change an attacked signal into a potential attacker. Two kinds of crosstalk have been considered in the literature: in-band crosstalk [27] and out-of-band crosstalk [27].

Attack Method	**Means**
In-Band Jamming	Use high powered signal using same channel and share a common switch.
Out-of-Band Jamming	Use high powered signal using different channels and share a common link.

2.7.1 In-band crosstalk:

An attack using in-band crosstalk can be achieved by injecting a high-power jamming signal (e.g., 20 dB higher than the other channels) on a legitimate lightpath, which can cause significant leakage inside the switches between lightpaths using the same wavelength as the attacker. The attacked signal may receive enough energy from the attacking signal through the crosstalk, which makes it a potential attacker for other signals.

Figure 2.5 represents the in-band crosstalk in a switch (intra channel crosstalk) and gain competition [5]: User1 and the attacker are using the same channel (λ1) and sharing a common switch. Since the power of the attacker signal is higher than the power of user1 signal, the attacker signal will leak into user1 signal (in-band crosstalk) and the gain competition is discussed in section 2.7.2.

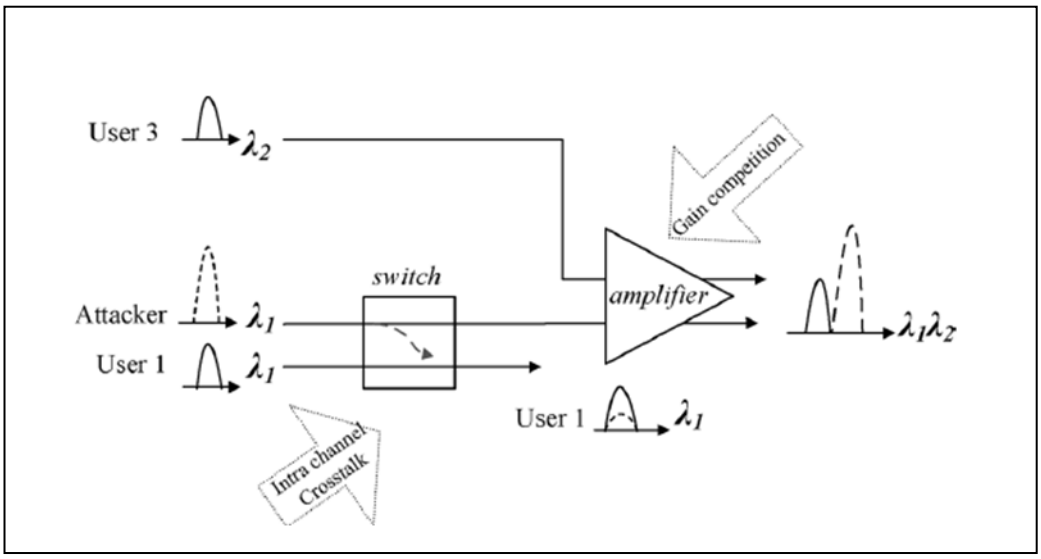

Figure 2-5 in-band crosstalk

2.7.2 Out-of-band crosstalk

Amplifiers are one of the most important parts of optical WDM networks, they are used to restore the strength of optical signals that might be lost while the signals propagate through the network (attenuation). There are several different types of amplifiers available, such as Erbium-doped fiber amplifiers (EDFAs), Praseodymiumdoped fiber amplifiers (PDFAs), and semiconductor optical amplifiers (SOAs) [27].

EDFAs are the most commonly used; they are made of short optical fibers doped with the rare earth element erbium. Light from external semiconductor lasers is coupled into the fiber exciting the erbium atoms. Therefore, when optical signals enter the fiber, they stimulate the excited erbium atoms to emit photons at the same wavelength as the incoming signal [27]

The amplifier has a limited number of photons which will be divided among users in proportion to their signal strength, this is known as gain competition. The attacker can use a high power signal, a high power jamming attack, to use the majority of the available photons which will reduce the gain of the weaker users.

Furthermore, long distances and high-power signals can introduce nonlinearities in the fiber causing interchannel crosstalk effects between signals on different wavelengths (out-of-band crosstalk). Therefore, if a jamming signal is injected on a legitimate lightpath, it can disrupt the lightpath it is injected on and the other lightpaths with which it is sharing a common link, because of gain competition in amplifiers and interchannel crosstalk on fibers.

Figure 2.6 represents two signals sharing same fiber but using different channels. The signal using channel λ1 (attacker) has enough high power that affects the signal on channel λ2 (out-of-band crosstalk).

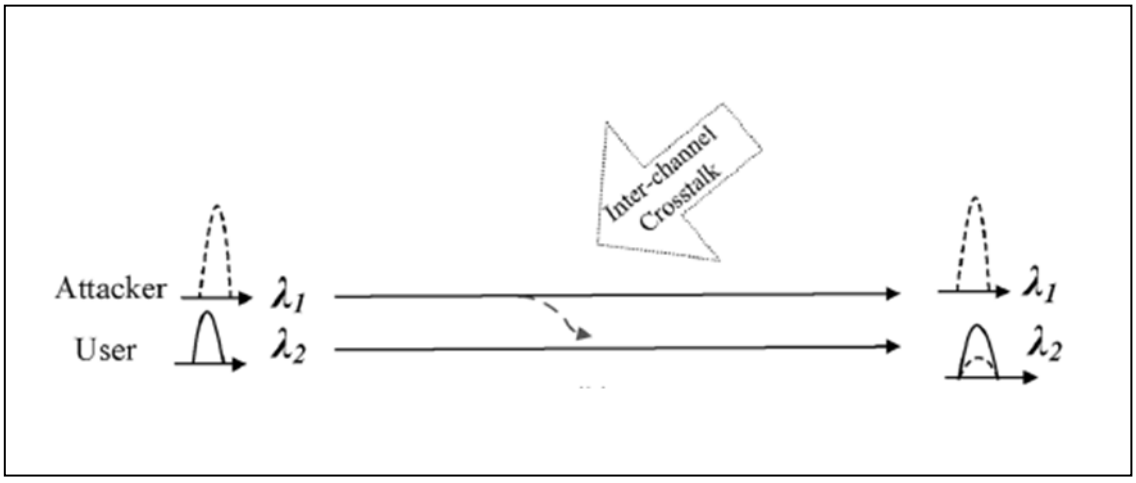

Figure 2-6 shows interchannel crosstalk [5]

2.8 Attack Group

Attack group (AG) is the set of lightpaths that can attack each other using high power jamming [5]. Attack group is the union of the link-share attack group and the in-band attack group.

The *link-share attack group* of a lightpath p (LAG_p) can be defined as the set of lightpaths, with which p shares at least one common link (or fiber). Based on this, the *Lightpath Attack Radius (LAR)* [5] of p is calculated as: $LAR_p = |LAG_p| + 1$. In other words, LAR_p is the number of lightpaths (including itself), with which p shares at least one link.

The *in- band attack group* of a lightpath p (IAG_p) can be defined as the set of lightpaths which p can attack directly, using the same wavelength. All the lightpaths in the group, IAG_p, use the same wavelength and share a common node with lightpath p. Based on this, the *In-Band Attack Radius* (***IAR***) of p is calculated as: $IAR_p = |IAG_p| + 1$.

Based on the above definitions, the attack group of a lightpath p is defined as:

$$AG_p = LAG_p \cup IAG_p \qquad (2.1)$$

2.9 Literature Review

In this section we review the existing literature for attack-aware RWA in optical networks. The first group of papers [7], [2], [8], [9], [4], [10] and [1] are all concerned with the prevention aspect of an attack to minimize its effect on the network. The second group of papers [3], [5] and [6] are concerned with the issue of path protection by choosing working paths and their backup paths in a way to protect the network.

2.9.1. **Preventive approach:**

The problem that [7] addressed is to minimize the possible reachability of a jamming attack with respect to gain competition and inter-channel crosstalk.

The authors proposed a tabu search algorithm (TS-JAR) for the routing subproblem to "minimize the Jamming Attack Radius, while accommodating all the lightpath demands and to minimize the upper bound on the number of wavelengths required for successful Wavelength Assignment (WA) and potentially reduce lightpath congestion".

First they limit potential physical routes to the K-shortest paths between node pairs. Then, for the neighbouring solutions they construct the conflict graph CG(X) of the current solution X, where each node represents a lightpath and a link between two nodes

means that the lightpaths share a common physical link. The maximum degree of a conflict graph is the JAR of the routing scheme. They define the reduced neighborhood be the set of nodes in the conflict graph whose degree is: Degree (Lpi) $\leq \alpha \cdot$ JAR(X), $0 \leq \alpha \leq 1$. If the value of α is reduced, then the neighborhood size is enlarged to consider more potential solutions but this will influence the execution time of the algorithm. The authors claim that their tabu search heuristic algorithm helps to minimize the JAR, to find suboptimal solutions, and to minimize the upper bound on the number of wavelengths required for successful wavelength assignment and reduces congestion with respect to shortest path routing.

In [2], the authors consider physical layer attacks, especially intra-channel crosstalk attacks, which can seriously affect the service. This kind of attacks can reach connections not even sharing components with the attacking signal. The new idea proposed by the authors, in this paper, is a new objective for the WA problem: minimizing the maximal radius of intra-channel crosstalk attack propagation. They call this measure the Propagating Crosstalk Attack Radius (P-CAR), which is the maximum number of lightpaths one jamming signal can affect by propagating intra-channel crosstalk in switches. Reducing the P-CAR enables the authors to limit intra-channel crosstalk attacks, with minimum or no extra cost, by planning the network carefully.

In their model, the authors use fixed shortest path routing to assign physical routes to lightpath demands. Also they consider that a jamming signal can attack all lightpaths using the same wavelength and sharing the same switch only at intermediate nodes.

They model the attacking relations as Attack Graphs. Lightpaths routed on the same wavelength are represented by the nodes of a single attack graph. Each node has outgoing directed links to other nodes it can attack. The P-CAR of a given wavelength is the maximum out-degree of the attack graph of that wavelength, incremented by 1. The authors claim that their algorithms achieve significantly smaller attack damage and this is done with no extra resources. They also claim that considering only the upper bound on the P-CAR, when assigning wavelengths is precise enough, while it significantly reduces complexity.

In [8], the authors addressed the problem of intra-channel crosstalk attacks in switches and the potential damage caused by such attacks. The authors propose a new objective function for the WA problem which is to minimize the Propagating Crosstalk Attack Radius (P-CAR). The Propagating Crosstalk Attack Radius is the maximum number of lightpaths a jamming signal injected on any legitimate data lightpath can attack via propagating intra-channel crosstalk in switches.

In order to concentrate on wavelength assignment, the authors used fixed shortest path routing. They used a layered graph approach, where each layer of the physical topology represents a different wavelength. They used the Best Fit P-CAR Wavelength Assignment algorithm that takes lightpaths in random order and routes them on the layer which yields the lowest P-CAR after accommodating the lightpath. The P-CAR on each layer is calculated by finding the attack graph corresponding to that wavelength using a recursive algorithm and then finding its maximum degree incremented by one. They used the Best Fit Decreasing P-CAR Wavelength Assignment algorithm that sorts the lightpaths in decreasing order of their shortest paths and then proceeds as BF_PCAR_WA. They also used two additional approaches, First Fit Wavelength Assignment and First Fit Decreasing Wavelength Assignment) algorithms which place lightpaths on the first layers in random order or in decreasing order of their shortest paths. The authors claim that their proposed GRASP heuristics obtain significantly smaller PAR and SAR values in all test scenarios in comparison to FFD and the crosstalk-friendlier RP.

In [9], the authors tackle the problem of attacks that can influence data propagating the optical fibers of transparent networks. They mention the growing size of data exchanged among users of networks which reflected the possible size of damage that could cause an attack. The new idea that the authors propose is routing lightpaths in a way to limit the damage of an attack with no additional cost. The authors propose an ILP formulation and add a new objective criterion for the RWA problem; they call it the maximum Lightpath Attack Radius (maxLAR). Their objective is to minimize the maxLAR and accommodate all the demands in order to minimize the number of damaged lightpaths. This also can help in the detection, localization and recovery phases. They

also used a tabu search algorithm (TS-LAR) for large networks. The authors claim that the TS-LAR heuristic significantly outperformed all the other approaches with respect to the maxLAR.

In [4], the authors address the problem of vulnerability of transparent optical network to physical-layer attacks and the damage caused to the huge amount of data propagating the network. In this paper, the authors define a new objective criterion to evaluate the impact of jamming attacks in RWA, they call it the Maximum Attack Radius (maxAR). They calculate the Out-of-band Attack Radius (OAR) and the In-band Attack Radius (IAR) of Lpi in order to find the maxAR which is their sum + 1. They define the AR of a wavelength as the maximum AR over all lightpaths routed on that wavelength, and the AR of an RWA scheme as the maximum AR over all lightpaths. Then they propose a heuristic algorithm to minimize this new objective via wavelength assignment over the attack-aware routing approach. The authors claim that their proposed algorithm is able to not only limit the consequences of potential jamming attacks, but also minimizes the wavelength usage at the same time.

In [1], the authors addressed the problem of securing optical networks from high power jamming and tapping attacks which are considered as malicious attacks. In this paper, the authors present a new approach that jointly minimizes the effects of both in-band and out-of-band attacks and solves the routing and wavelength assignment (RWA) problem dynamically. They developed an ILP formulation with objective to minimize the LAR and IAR values and the path length of the newly established lightpath in order to prevent loops in some areas of the network. They also propose a heuristic for dynamic RWA (SA-DWA) in which they find a set of possible routes over the physical topology for each source-destination pair. Using the previous information with the set of existing lightpaths already established over the network with their physical routes and assigned wavelengths, the heuristic calculates the set of available channels on a link and the set of available wavelengths on all edges of a particular route. The authors claim that the proposed approach for security-aware dynamic RWA can reduce the vulnerability of the lightpaths to potential attacks, at the cost of obtaining some high blocking probability, when compared to traditional RWA techniques.

2.9.2. Protection approach:

In [3], the authors addressed the survivability of optical networks facing jamming attacks using in-band crosstalk in switches. The authors propose a dedicated attack-aware backup path protection algorithm. It consists of separating the primary path and the backup path into different attack groups to ensure survivability of the network against jamming attacks in switches. In addition, by limiting the maximum number of lightpaths each lightpath can attack, the damage from in-band jamming attack will be limited.

They assume that an attack can be inserted anywhere along any primary path, or in case of a previous link failure, along an active backup path. To ensure survivability of connections under an attack they need to assign different wavelengths to the primary and backup path of every lightpath.

They proposed an algorithm which they call "Attack-Aware Dedicated Path Protection (AA-DPP) algorithm". They compare the AA-DPP with a generic algorithm for dedicated path protection they call Dedicated Path Protection (DPP) aimed only at minimizing the number of wavelengths necessary for protection from single-link failures, without considering attacks. The authors claim that the AA-DPP algorithm obtains lower IAR and average IAR values than DPP in all scenarios, at the cost of some increase in the number of wavelengths, and AA-DPP achieves lower WLU and AHD values for backup paths than DPP in almost all test scenarios.

In [5], the authors addressed the problem of routing and wavelength assignment survivability. In this paper, the authors introduce the Attack Group (AG) of each lightpath and specify an exclusive backup path for each lightpath which cannot be attacked by the same attacker. AG of a lightpath LP is the set of lightpaths which can attack LP. A high-powered jamming signal can affect lightpaths using a common wavelength, i.e. in-band effect which they call AG_i set, or using different wavelength than the attacker, i.e. out-of-band effect, which they call AG_o set. So the AG of LP is the union set of AG_i and AG_o of that LP.

To ensure the protection, the working and the backup path must be AG-disjoint, which means that the intersection of AG_s of the working and the backup path of each

connection is an empty set. To calculate the AG of a lightpath LP, they represent the relations among lightpaths by an attack graph, where nodes are lightpaths. If two lightpaths can affect each other their corresponding nodes are connected. The AG_i of a lightpath are its neighbouring nodes using the same wavelength, and the AG_o are the neighbouring nodes using different wavelengths. The attack radius AR, an objective criterion used to minimize the damage caused by an attack, of LP equals the size of its AG, incremented by one.

The authors also introduce an algorithm that they call Attack-Survivable Routing and Wavelength Assignment (AS-RWA). To evaluate the AS-RWA algorithm, they compared it against a generic algorithm for Dedicated Path Protection (DPP) and the Attack-Survivable Wavelength Assignment (AS-WA) algorithm. The authors claim that their proposed approach can achieve enhanced connection security under high-power jamming attacks with efficient wavelength-link usage.

In [6], the authors state that conventional network survivability approaches protect transmission in case of component faults but do not provide good protection from jamming since the working and backup paths of a connection may both be affected by the same jamming signal. In this paper, the author extends their previous work [5] by adding a new approach for Jamming Aware Shared Path Protection (JA-SPP) to achieve survivability in the presence of jamming signals in a more resource-efficient way.

In JA-SPP, backup paths of two connections must not share resources if their working paths are both within reach of any common potential jamming signal which could affect them at the same time. They also considered that the working and the backup paths of each connection in JA-SPP must not share any physical link to protect from link failures. In addition, resource-sharing among backup paths whose respective working paths share common physical links is prohibited and the wavelength clash and continuity constraints must hold. The authors claim that JA-SPP protects from both single link failures and high-power jamming, while maintaining the same level of resource usage efficiency as standard single link failure SPP with no jamming-awareness.

Most of the previous work deals with the preventive approach in case of an attack, and in case of the protection approach either the in-band or the out-of-band attack for the static traffic model. One of the papers [5] considers both cases of an attack, but the approach proposes a very strict interpretation of when two lightpaths are not in each other's link-share attack group, i.e. any two lightpaths sharing a common link are assumed to be capable of attacking each other, without taking into consideration that the power of a jamming signal decreases when the distance between the attacking lightpath and the attacked lightpath increases.

3 Proposed Solution

3.1 Introduction

In this chapter, we discuss our proposed model for estimating the attack group of a lightpath. As mentioned in sec 2.8 the attack group of a lightpath p (AG_p) represents the set of lightpaths that may be 'attacked' i.e. may experience significant loss of signal quality, by malicious actions on lightpath p. We note that inclusion in the attack group is a symmetric relationship. In other words, for two lightpaths p and q, if $q \in AG_p$ then $p \in AG_q$. Based on the definition of attack group given in eqn 2.1, [5] defined a model for attack-aware survivable RWA in optical networks, which has been discussed in Sec. 2.8. In this chapter, we first discuss our proposed model and highlight the differences between the two models, through a simple illustrative example. Then, we discuss our software application to evaluate the performance of our proposed model.

Because of the huge amount of data transmitted over the optical networks, there might be a significant number of lightpaths that share common switches. If two of the lightpaths, sharing a switch, are using the same channel then there might be a crosstalk (leakage of one signal into the other) between the two lightpaths. An attacker can exploit this type of crosstalk to influence signals of other users. In addition, there might be crosstalk among lightpaths that are not using the same channel, but which are sharing one or more fiber links. Signals using different channels may interfere with neighbouring channels. Typically the amount of interference decreases as channel separation increases.

3.2 Proposed model

Our proposed model uses the same definition for in-band attack group of a lightpath p as given in Sec. 2.8 which is given below.

$$IAG_p = |IAG_p| + 1 \qquad (3.1)$$

However the definition of the lightpath attack group is modified as follows.

$$LAG_{pi} = \{q : (q \text{ shares at least one common link with } p) \wedge (|k_p - k_q| \leq i)\} \quad (3.2)$$

Here k_p and k_q represent the channel assigned to lightpath *p* and *q* respectively, and *i* represents the channel separation of the two lightpaths, in terms of the channel numbers. So, in the proposed models, a lightpath p that shares a common link with lightpath *q*, may not necessarily belong to the attack group of *q*. Whether or not $p \in AG_q$ depends of the channel spacing between the two lightpaths. It is well known that the interference and crosstalk between two lightpaths sharing a common link decreases as the channel spacing between their assigned channels increases [11]. The actual value of channel spacing for which the crosstalk may be ignored depends on a number of factors, such as the signal strength of the attacking and attacked signals, the type of modulation used and the properties of the fiber. Therefore, our model provides a flexible definition of the attack group, where the value of *i* can be varied depending on the signal characteristics and fiber properties. In our simulations, we have used *i*=1 or *i*=2, i.e., an attacking signal can affect only the adjacent channels or second adjacent channels. The model used in [5] can be considered a special case of our model, where *i*= |*K*| and *K* is the set of available channels on a fiber link. When considering path protection, we use the same conditions identified in the previous section.

Fig. 3.1 shows a fiber with 8 available channels, numbered 0 – 7. If an attacking signal is introduced on channel 3, it will attack lightpaths on adjacent channels only (i.e. channel 2 and channel 4), if *i*=1 in eqn (3.2). If *i*=2, then in addition to the adjacent channels, the attacking signal can also disrupt lightpaths on the second-adjacent channels (i.e. channel 1 and channel 5). However, signals on channels 0, 6 and 7 will not be affected by this attack.

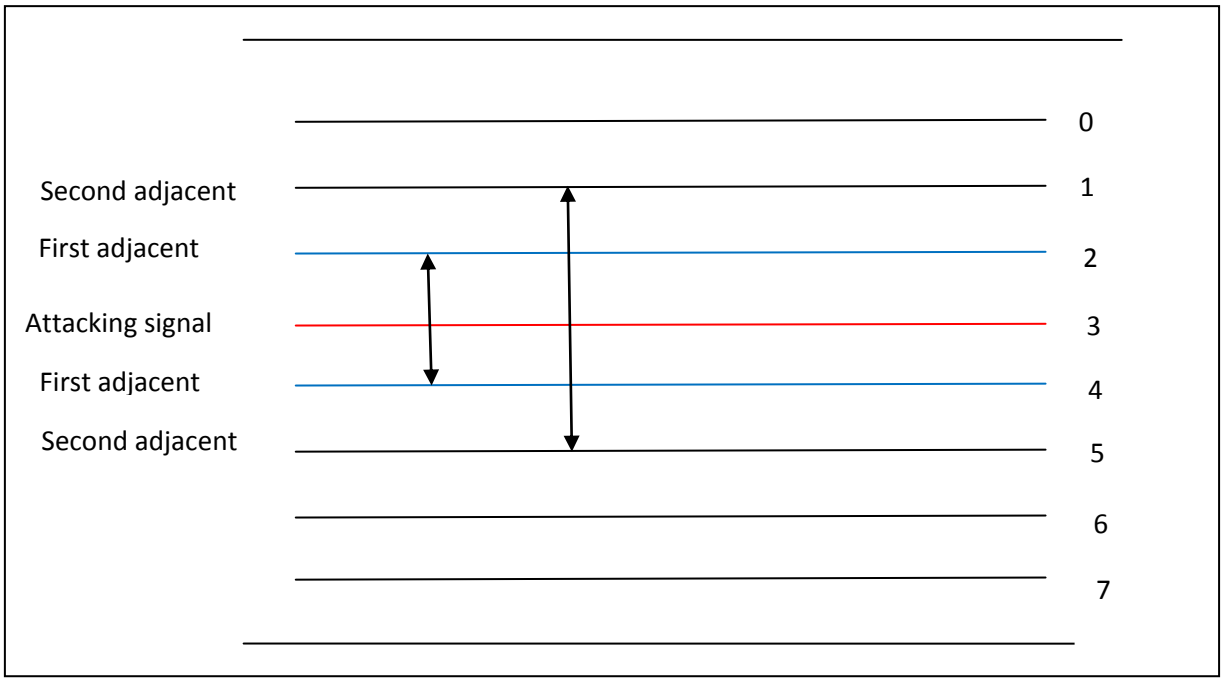

Figure 3-1 first and second adjacent channels

3.3 Attack Aware RWA with DPP

When using DPP, two lightpaths must be set up for each connection request *p* between a pair of source and destination nodes; one is called working or *primary* lightpath and the other is called *backup* lightpath. We will identify the working and backup lightpaths, for a connection *p*, as p_w and p_b respectively. The backup lightpath is not used unless the primary lightpath is disrupted, either due to a fault in the network or an attack. The primary and backup lightpaths of a connection must be both link and node disjoint. If this condition is not satisfied any attack on a common node or link may potentially be able to disrupt both the primary and the backup lightpaths simultaneously. If this happens, the connection will not be able to survive the attack.

When considering the RWA problem with DPP, for each new connection request *p*, we check if

1) Both the primary and backup lightpaths can be attacked simultaneously by any primary lightpath or any backup lightpath of an existing connection *q*. In other words ($p_w \in AG_{q_w}$ and $p_b \in AG_{q_w}$) or ($p_w \in AG_{q_b}$ and $p_b \in AG_{q_b}$)

2) Moreover, we check if any of the primary or backup lightpaths of the new connection can simultaneously attack both the primary and backup lighpaths of any existing connection q. In other words ($q_w \in AG_{p_w}$ and $q_w \in AG_{p_b}$) or ($q_b \in AG_{p_w}$ and $q_b \in AG_{p_b}$)

If either of the above conditions is true, then the corresponding route and wavelength assignment should not be allowed for the new request.

This is illustrated in Fig. 3.2. Here $p1_w$ and $p1_b$ are the primary and backup lightpaths for a connection request from node 1 to node 6. Similarly, $p2_w$ and $p2_b$ are the primary and backup lightpaths for a second connection request from node 2 to node 3. In this example $p1_w$ and $p1_b$ are node and link disjoint. However, both of them are vulnerable to an attack through the backup lightpath $p2_b$ for connection 2. Lightpath $p2_b$ uses channel λ1 and can attack lightpath $p1_w$, which uses channel λ2, since they share a common link 3→4. Also, $p2_b$ can attack lightpath $p1_b$ using channel λ1, due to in-band crosstalk at node 2 and node 3. On the other hand, if we assign wavelength λ4 for lightpath $p1_w$, then based on eqn (3.1), with i=2, $p2_b$ can no longer attack $p1_w$ and this would be a valid RWA.

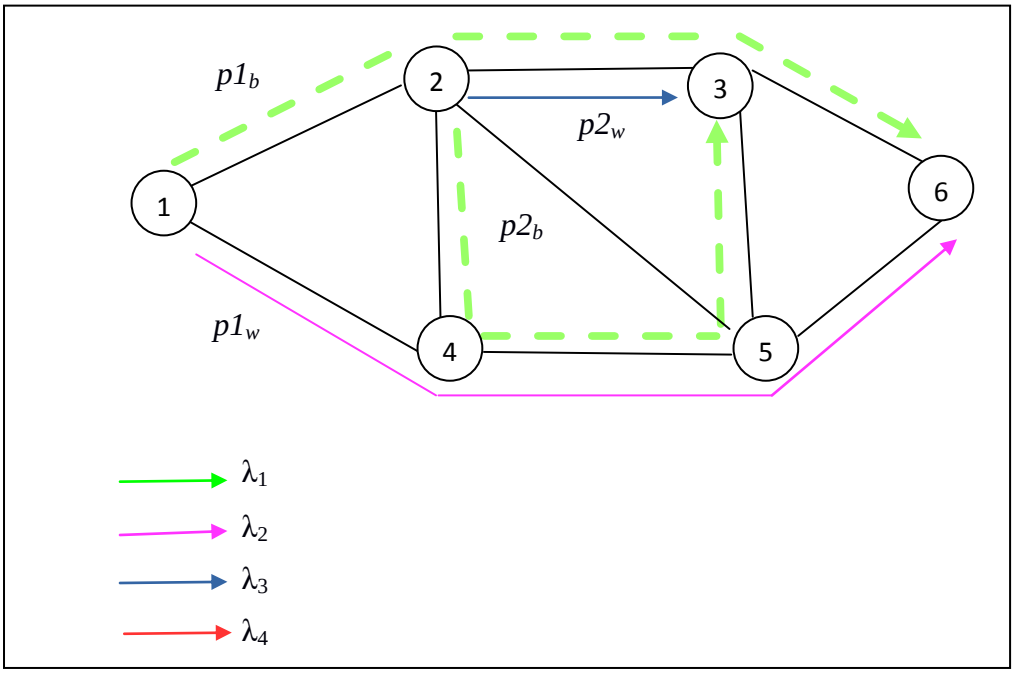

Figure 3-2 Illustration for working and backup lightpaths vulnerable to attacks by a common lightpath

3.4 Illustrative Example

In this section we use a simple illustrative example to show how to determine the attack groups for different lightpaths and calculate maximum attack radius for a given RWA, using our model as well as the attack-aware dedicated path protection (AA-DPP) model in [5]. We consider the network of Fig. 3.3, consisting of 6 nodes network, 9 bidirectional links, where each optical fiber has 4 wavelengths: λ1, λ2, λ3 and λ4. Three connections have been established over the network, each with a primary and a backup lightpath. The RWA for the set of lightpaths is given in Table 3.1. To differentiate between the primary lightpath and backup lightpath of a connection, we use solid lines and dashed, respectively.

Table 3-1 Used channels and Connections of Fig. 3.3

	Connection 1	Connection 2	Connection 3
Primary route	1→4→5→6	2→3	1→2
Backup route	1→2→3→6	2→4→5→3	1→4→2
Primary channel	λ4	λ3	λ4
Backup channel	λ1	λ1	λ2

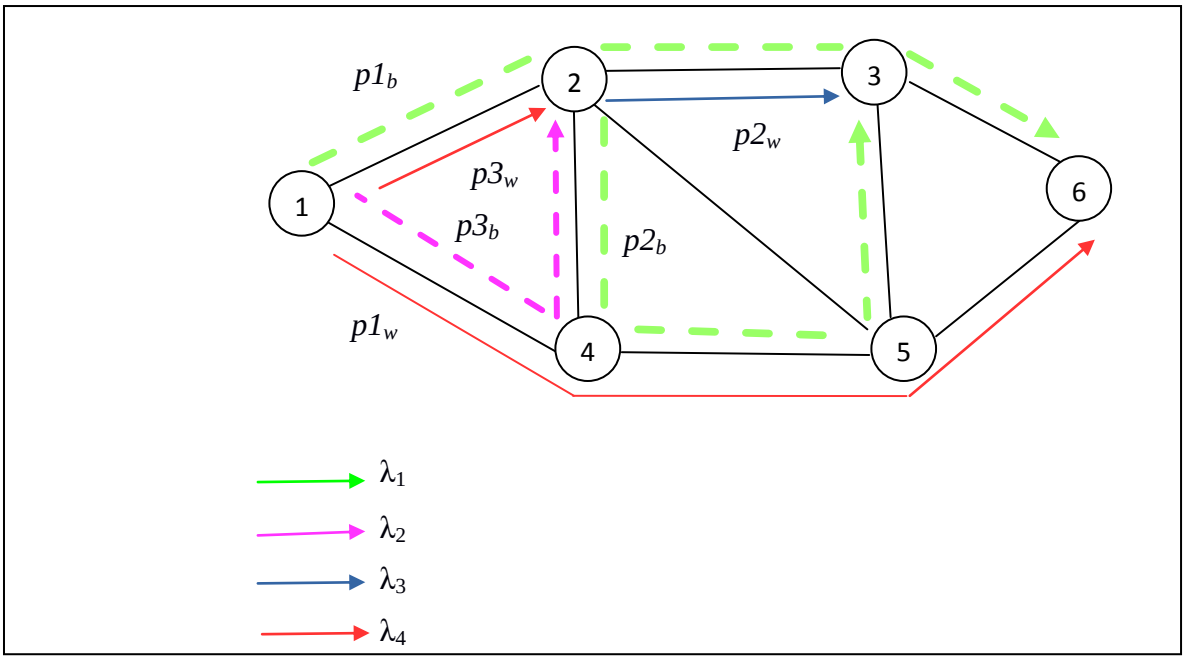

Figure 3-3 lightpaths of three connections

As an example, we will calculate the in-band attack group (AG_i) and out-of-band attack group (AG_o) for lightpath $p1_w$, the primary lightpath for connection 1. For all three approaches, the in-band attack group of $p1_w$ includes only lightpath $p3_w$, since $p1_w$ is the only other lightpath using channel λ4 and it shares a common node (node 1) with $p1_w$. For out-of-band attack group, the results will be different for each approach. Using AA-DPP, both $p2_b$ and $p3_b$ are included in the attack group, since $p2_b$ ($p3_b$) shares link 4→5 (1→4) with $p1_w$. Using our proposed approach, with i=1, no other lightpath will be included in the out-of-band attack group of $p1_w$. This is because, although both $p2_b$ and $p3_b$ share a common link with $p1_w$, neither one uses an adjacent channel. Finally, using our proposed approach with i=2, only $p3_b$ will be included in the attack group, since it uses the second-adjacent channel λ2.

In a similar fashion, the in-band and out-of-band attack groups for all the lightpaths are calculated and shown in Table 3.2

Table 3-2 Attack Groups of Fig 3.3 Using AA-DPP and the Proposed Approach

Lightpaths	AG_i (same for all cases)	AG_o			Total Attack Radius ($\|AG_i\|+\|AG_o\|$)		
		AA-DPP[*]	Proposed		AA-DPP[*]	Proposed	
			$i = 1$	$i = 2$		$i = 1$	$i = 2$
$p1_w$	$p3_w$	$p2_b$, $p3_b$		$p3_b$	3	1	2
$p1_b$	$p2_b$	$p2_w$, $p3_w$		$p2_w$	3	1	2
$p2_w$		$p1_b$		$p1_b$	1	0	1
$p2_b$	$p1_b$	$p1_w$			2	1	1
$p3_w$	$p1_w$	$p1_b$			2	1	1
$p3_b$		$p1_w$		$p1_w$	1	0	1

3.5 Experiments Steps

A primary objective of this research is to investigate the cost of security-aware RWA algorithms. The authors in [5] did not study the overhead associated with the approach they proposed. In a network where each fiber may support up to 32 channels, if one channel is used by a lightpath *L*, all the remaining 31 channels will be considered to be under attack, so that up to 32 primary/backup paths will need to be taken into account. For all these 32 lightpaths the routing algorithm must ensure that lightpath L does not attack the corresponding backup/primary lightpaths. In other words, after lightpath *L* is established, the presence of this path imposes significant restrictions on the paths/ channel numbers that may be used by subsequent connections. The net effect is that some of the connections which could be established if this threat due to lightpath *L* did not exist, will no longer be allowed. The lightpath L therefore not only uses one channel on each fiber in its path it blocks additional resources of the network and, in effect, increases the cost of the network.

One of our objectives is to study the effect of AA-DPP approach on the cost of the network. In addition, we are going to study our approach which simplifies the attack model by making some constraints less strict which will affect the attack radius.

Our approach is that the influence of an attacking signal will create less impairment to channels which are not adjacent to the channel used by the attacking signal. The theoretical foundations of this approach are being studied by another graduate student in our group. In our simplified model we are considering that the effect of an attacking signal will be most harmful to the signals using adjacent channels and the second adjacent channels and not very significant to other channels. The other graduate student has established that this does not affect the quality of the solution.

In our experiments, we are going to study the effect of

- AA-DPP approach on the network performance,
- Our simplified model on the performance of the network.

This comparative study will be based on the blocking probability of connections in the network. The blocking probability is calculated using the number of blocked requests divided by the total number of requests. Our approach is that, for a given set of resources in a network, if the adoption of strategy *S1*, the blocking probability is less than the blocking probability if strategy *S2*, it means that strategy *S1* allows us to handle more requests than strategy *S2* and the operational expenses (OPEX) using strategy *S1* is lower.

We are going to compare the results of 4 models:

- AA-DPP model,
- our model using the first adjacent channel as the source of security threat,
- our model with the first and the second adjacent channel as the sources of security threat, and
- the dedicated path protection model, where security threats are not taken into account.

In order to be consistent while running the tests, we are going to use same network topology and the same set of requests with the four models.

3.6 Our Model

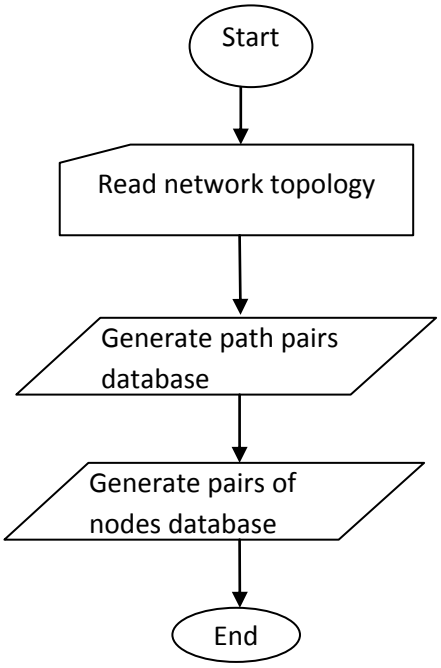

Figure 3-5 Pre-processing phase

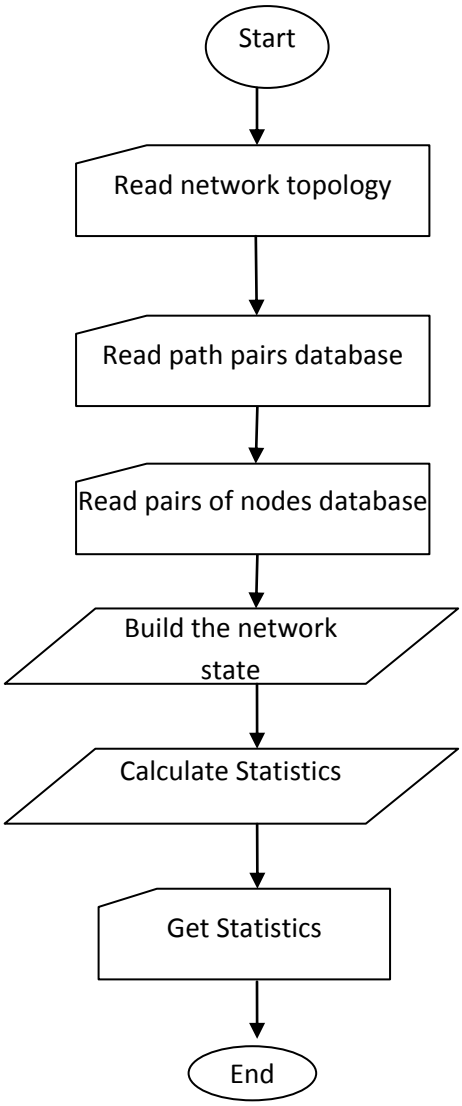

Figure 3-4 Online phase

Since there are less than 10 existing wide-area optical networks, we have generated synthetic networks with different sizes to test our algorithm. Our work may be divided into two main phases: a pre-processing phase and an online phase.

3.6.1 Pre-Processing Phase

Because searching for a route to assign to a lightpath is time consuming, we pre-computed, in advance, a certain number of alternative routes for each pair of nodes in the network. So whenever we have to process a request for communication, we need not waste time on searching for a route, we just looked up some promising paths from the pre-computed set of paths and use it.

The pre-processing phase consists of the following:

1. Read the topology of the network from an input file into a two dimensional table.

2. Generate some pairs of primary and backup edge disjoint lightpaths for each pair of nodes. These pairs of lightpaths will be used in the online phase to establish a new request between the two corresponding nodes. We are using the First-Fit approach in order to specify which combination of primary-backup lightpaths to be used. If none of the generated combinations works then the request will be considered as blocked request.

3. Generating a sequence of random pairs of numbers between 0 and N (where N is the number of nodes in the network) and saved into a file to be used during the online phase. These pairs of numbers represent the source and destination nodes of requests.

3.6.2 Reading Network Topology

Our algorithm starts by reading the data that defines the network topology, specifying the nodes and the links, from a text file. The data is supplied in the form of a two dimensional table of size NxN, where N is the number of nodes in the network. The following example illustrates the representation of a network topology.

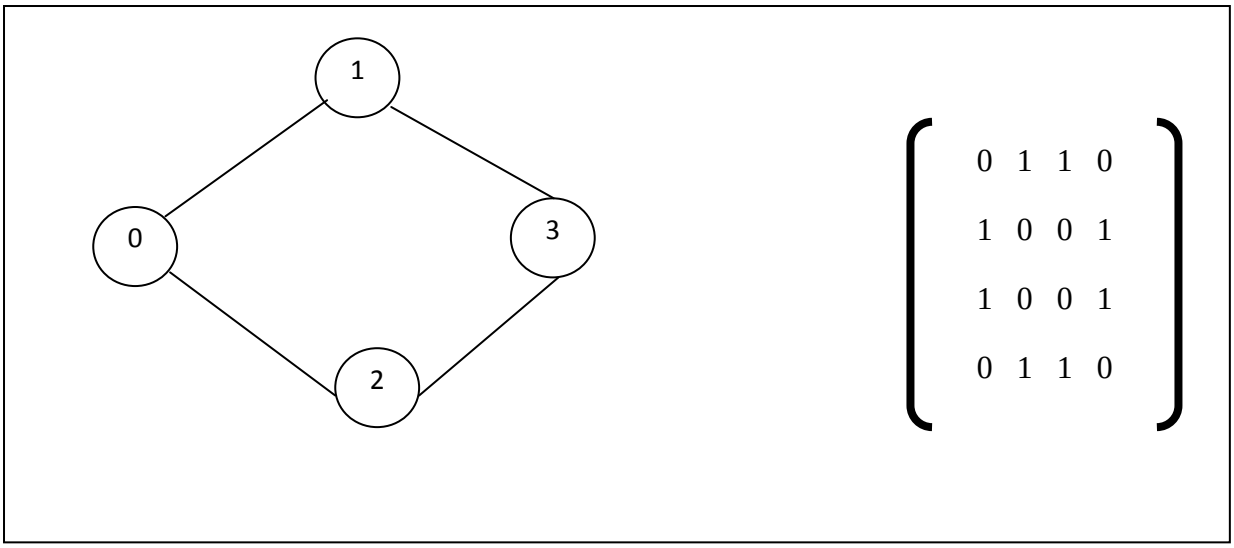

Figure 3-6 Example of reading network topology

Each edge connecting two nodes represents a bidirectional fiber link, which means that data can be transmitted in both directions. For instance, node 0 is linked to node 1 with an edge, meaning that data can be sent from node 0 to node 1 and from node 1 to node 0. In the table, if the value in row *i* and column *j* is 1(0), it means there is a link (there is no link) between node *i* and node *j*.

Number the edges of the bidirectional links. The following figure gives a simple example about numbering the edges.

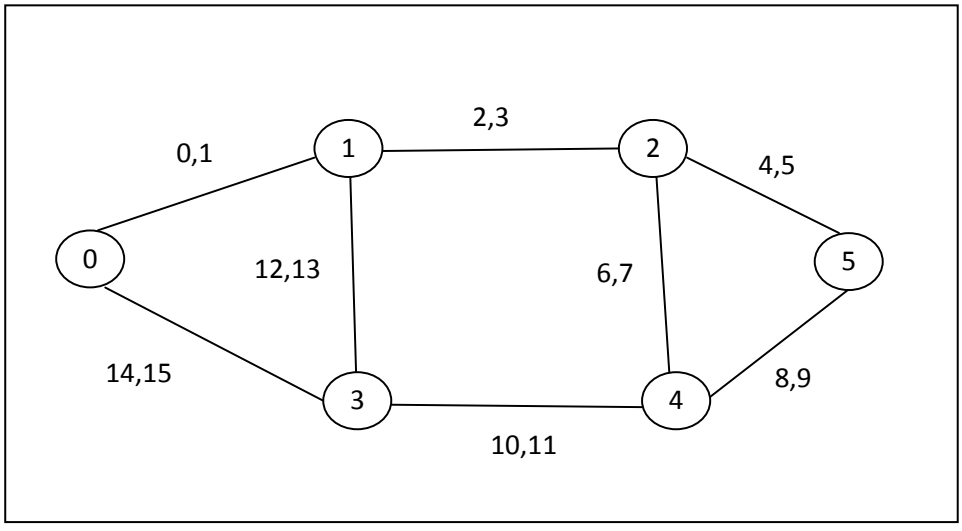

Figure 3-7 Example of numbering the edges

3.6.3 Generate Database of edge-disjoint paths

After reading the network topology, we generated a database of potential paths that may be used to handle connection. For each pair of nodes (*i*, *j*) in the network, we have generated *m* pairs of edge disjoint paths between *i* and *j*, for some predetermined value of *m* (we used *m* = 9). In dedicated path protection approach, each connection involves identifying two paths which do not have any common edge. One of these paths is called the *primary path*, which is used to transmit the data in the absence of "problems". Here the problem could be an edge failure or a security threat on any edge or node in the path. When such a problem occurs, communication will switch from the primary path to the *back-up path.* Since the backup path does not share any link with the primary path, we have to ensure that both paths cannot be attacked simultaneously. Our database contains *m* pairs of edge-disjoint paths. At the time of establishing a connection from, say, node *s* to node *d*, one of these *m* pairs of paths will be used. We will designate one of the paths in the selected pair as the primary path and the other as the backup path.

To find the edge disjoint paths, we have implemented Yen's Algorithm to first find *k* shortest paths between each pair of nodes in the network, where *k* is a predetermined number (we used *k* = 3). Those *k* paths are used as the primary paths. For each of the primary paths, we deleted, from the network, the edges that appear in the path and found *k* shortest paths again. These resulting paths are used as the backup paths. We therefore get a total of $m = k^2$ pairs of paths. Each set of pairs of paths between the two nodes is saved in our database. We have used this database when establishing a connection for a new request.

The following figure represents a simplified example of generated combinations of primary-backup lightpaths for the pair of nodes (0,4).

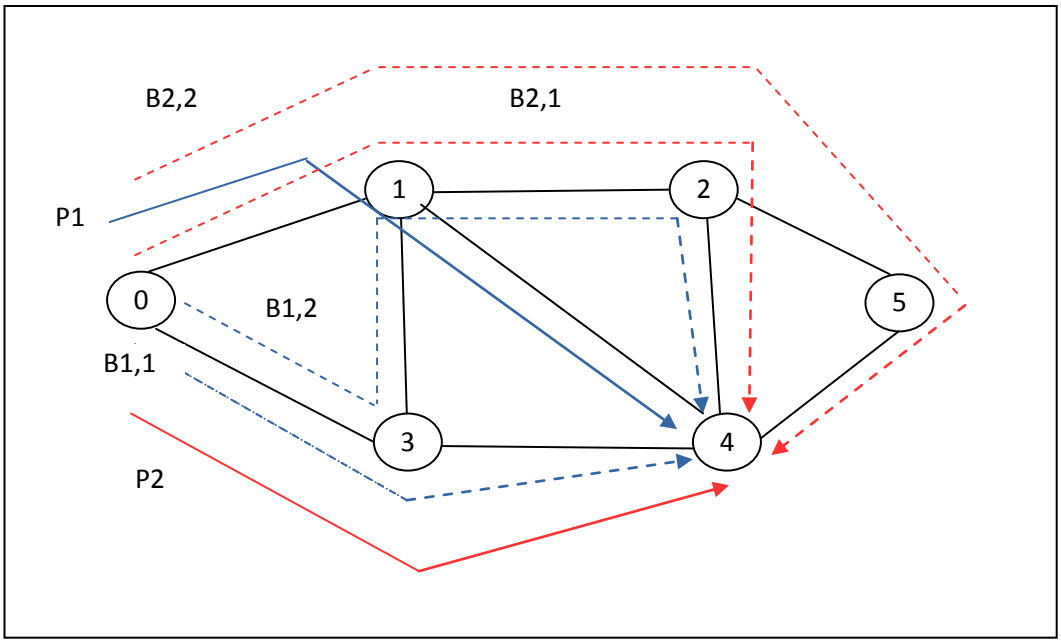

Figure 3-8 Example of generated primary-backup lightpaths

In this example, P1 represents a primary path from node 0 to node 4, B1,1 and B1,2 represent its corresponding backup paths. P2 represents another primary path, B2,1 and B2,2 its corresponding backups. Since we are using the dedicated path protection approach, the primary path and its backups should be edge disjoint.

The combinations can be as follows:

(P1;B1,1) , (P1;B1,2) , (P2;B2,1) , (P2;B2,2).

If the first combination cannot be established then the next will be checked and so on, until we find the first acceptable combination of paths, based on the corresponding attack model, that is going to be used. If none of the combinations is acceptable then the request from node 0 to node 4 is going to be blocked and another request is considered.

3.6.4 Online Phase

3.6.4.1 Setting up the network state

In order to study the blocking probability of a network in a realistic manner, this network should be carrying a certain amount of traffic when a new request for communication is considered. The amount of traffic is critically important in such studies. If the network has relatively few existing connections, it is most likely that the new connection can be handled and the resulting blocking probability will be low. If the network is already handling too many connections, it is very likely that the new connection cannot be handled and the corresponding blocking probability will be high.

All working connections should respect the dedicated path protection approach and the attack model to be tested. To build the network state, we have created a file, used as an input file to help build the network state, with randomly chosen pairs of nodes (s, d) from the network, each pair representing the source node s and destination node d of a request for connection. Our program read, from the input file, node pairs (s, d), and attempted to establish a connection from the source node s to the destination node d. If the connection can be established, then it is saved as working connection and we moved to the next pair of nodes in the input file. If the connection cannot be established, then we just move to the next pair of nodes and we keep repeating this until we reach the desired number of working connections in the network.

To check if a connection can be established, we have followed the algorithm 3.1.

Algorithm 1 Check_Connection

Input: New Request: R = (*s*,*d*), Network Topology, Pairs Of Paths Database , Network state, edges_channels table (shows the used and unused channels of each edge in the network)

Output: returns 1 if the connection can be established or 0 if the connection cannot be established.

```
1.  edge_disjoint_paths ← find_edge_disjoint_paths(s, d, Pairs_Of_Paths_Database)
2.  If EMPTY (edge_disjoint_paths) then
3.     Return 0      // there is no pair of edge disjoint paths to establish the connection
4.  Else
5.    For each  path_pair ∈ edge_disjoint_paths
6.         P ← primary_ path
7.        b ← backup_ path
8.        P_free_channels ← find_free_channels(p)
9.        b_free_channels ← find_free_channels(b)
10.       if NOT_EMPTY(P_free_channels) AND NOT_EMPTY(b_free_channels) then
11.          for each p_channel ∈ p_free_channels
12.               for each b_channel ∈b_free_channels
13.                    for each connection ∈ Network_State
14.                         if attack( p, connection_p) and attack( p, connection_b) then
15.                            OR ( b, connection_p) and attack( b, connection_b)
16.                             OR ( connection_p, p) and attack(  connection_p, b)
17.                              OR ( connection_b, p) and attack(  connection_b, b)
18.                            Break
19.                         End if
20.                   End for
21.                   If connection == NULL then
22.                      Return 1  // the new  connection is neither attacking nor attacked
23.                   End if
24.                End for
25.             End for
26.          End if
27.     End for
28.     Return 0 // all pairs of paths are scanned and the connection cannot be
        established
29.  End if
```

Algorithm 3.1Check_Connection Algorithm

We have to find a viable path pair to handle the request for connection, say from *s* to *d*. For a pair of edge disjoint primary-backup connection to be acceptable, i) it should not attack any existing connection and ii) no existing connection should attack the new connection. This means that

- both the primary and the backup lightpaths to handle the new request should not be attacked simultaneously by the primary or backup lightpath of any existing connection
- the primary or the backup lightpath of the new request should not attack simultaneously the primary and backup lightpaths of an existing connection,

For the in-band attack which occurs in a switch for instance, two lightpaths should not use the same channel if they share a common switch. For the out-of -band attack that occurs in a common link, the two lightpaths should use different channels where the permitted difference between the channel numbers is determined by the attack model we are using. For instance, if we consider that adjacent and second adjacent channels may attack each other, then, if the first lightpath is using channel (c) the second lightpath should use channel c_1 (where $|c - c_1| \geq 3$), in order not to attack each other.

So while establishing a new connection, channels should be assigned to the primary and backup lightpaths in a way to avoid both in-band and out-of-band attacks.

The database of primary-backup paths created in the pre-processing phase, gives pairs of edge disjoint primary and backup paths from *s* to *d*. We checked each path pair, until we either found an acceptable path pair or we determined that no path pairs in the database satisfied our conditions. If we succeed in finding a path pair from *s* to *d* and channel allocations, we saved the information and a working connection in the network state. If, after checking all the corresponding primary-backup pairs, we could not find an acceptable pair, then this connection cannot be established and we have to move on to another request.

After reaching the desired load on the network, we start studying the cases where new request for connection arrives, say from node *s* to node *d*. We check whether the new request can be accommodated by making provisions for a primary path and a backup path

both from *s* to *d*, satisfying the requirements of the attack model we are studying. If the new request cannot be accommodated, the request is blocked. We considered all possible node pairs (*s*, *d*) and calculated the blocking probability of the network by the ratio of the number of all the blocked calls to the total number of node pairs. A network with a low blocking probability means that it can handle more requests, which indicates that the performance of the network is better than a network with a higher blocking probability. This approach allows us compare the model proposed by [5] and our model.

The same approach that we used to build the network state will be used to process each new request for communication in the online phase. The only difference is that we just update the statistics that will be used to calculate the blocking probability.

4 Results

In optical networks using dynamic traffic RWA, the network performance is measured in terms of a metric called lightpath blocking probability [4], defined as the ratio of the number of lightpath requests that could not be accommodated (i.e., are *blocked*) to the total number of lightpath requests. An increase in number of set up requests means a decrease in the lightpath blocking probability, therefore a better network performance.

In this chapter we report the results of our simulations used to evaluate the performance of our proposed approach and compare the results with those obtained using AA-DPP [5] approach.. The simulations have been run using both real (NSFNET 14-node topology) and synthetic (20-node and 40-node) network topologies. For the synthetic networks, 5 different topologies were generated for each size considered. A link between two nodes in the physical network is assumed to be composed of 2 separate uni-directional optical fibers, where each fiber supports either 8,16 or 32 channels. Traffic load values between 20 existing connections (low traffic) to 105 existing connections (high traffic) were used in the simulations. For each of these traffic load values, 5 different sequences of connection requests were generated. As a result, for synthetic networks each blocking probability reported in this section is the average of 25 simulation runs. For each traffic load, we first initialized the network by setting up the required number of ongoing connections. Then we tried to establish new connections, with different source-destination nodes, on top of the existing traffic load.

4.1 Blocking probability vs. Demand size

Tables 4.1, 4.2 and 4.3 show how the blocking probability changes when the traffic load is varied, for 16 channels per fiber. The Attack-Unaware DPP (AU-DPPP) represents the traditional DPP algorithm, which does not consider potential attacks. In AU-DPP, a connection is never blocked due to vulnerability to attacking lightpaths; it can only be blocked due unavailability of suitable channels to route the corresponding

working and backup lightpaths, due to network congestion. Therefore, in all these simulations, we expect that the AU-DPP approach will have the best performance, and is included as a reference point to evaluate the remaining approaches. As expected, the blocking probability in general increases with the traffic load.

Table 4-1 Shows The Blocking Probability vs. Demand Size-14 nodes, 16 channels

	Blocking Probability (%)			
Traffic Load	**20**	**25**	**30**	**35**
Approach				
AA-DPP[5]	17.49	17.49	19.93	23.27
Proposed (*i*=1)	7.25	7.25	8.66	15.38
Proposed (*i*=2)	7.25	7.25	8.00	16.40
Attack-Unaware DPP (AU-DPP)	7.25	7.25	7.25	11.78

Table 4.1 depicts that the blocking probability of AA-DPP [5] approach is higher than our approach and the simple dedicated path protection approach in all considered traffic demands load. Table 4.1 shows that the average blocking probability of AA-DPP network is 17.49% with 20, and 25 existing connections, while for our approach, the blocking probability is similar to AU-DPP at 7.25% for the. As the traffic load increases, the difference in blocking probability between AU-DPP and the proposed approach becomes more noticeable. However, the proposed approach still consistently performs better that AA-DPP.

Table 4-2 Shows The Blocking Probability vs. Demand Size-20 nodes, 16 channels

	Blocking Probability (%)			
Traffic Load	**20**	**25**	**30**	**35**
Approach				
AA-DPP	16.94	16.94	19.15	27.44

Proposed (*i*=1)	10.74	10.74	13.80	18.99
Proposed (*i*=2)	10.74	10.74	13.77	18.69
attack-unaware DPP	10.74	10.74	11.17	15.24

Tables 4.2 and 4.3 display the average blocking probabilities for networks of 20 nodes and 40 nodes respectively, with fibers of 16 channels. The traffic load varied between 20 to 35 connections (90 to 105 connections). The results follow a similar pattern as for the 14-node case in general.

Table 4-3 Shows The Blocking Probability vs. Demand Size-40 nodes, 16 channels

	Blocking Probability (%)			
Traffic Load	**90**	**95**	**100**	**105**
Approach				
AA-DPP	6.50	9.89	16.04	21.20
Proposed (*i*=1)	6.39	9.53	15.70	23.58
Proposed (*i*=2)	6.22	8.82	14.67	21.94
AU-DPP	4.84	7.50	13.81	19.27

Fig. 4.1 shows that in all cases where different traffic loads have been used, the blocking probability of our proposed approach is less than the blocking probability of AA-DPP.

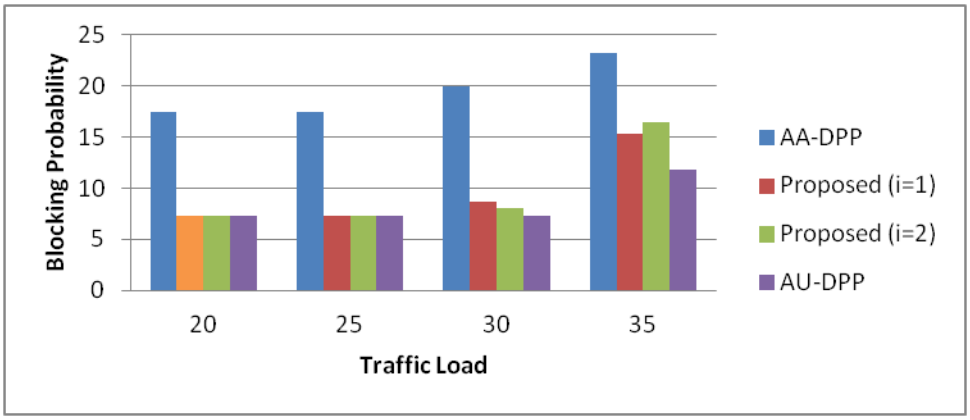

Figure 4-1 Comparison of blocking probabilities using different approaches

4.2 Blocking probability vs. Channels

In this section, we study how the blocking probability varies with the number of available channels per fiber. Tables 4.4, 4.5 and 4.6 represent the blocking probability of 14-nodes, 20-nodes and 40 nodes network respectively using fibers with 8, 16 and 32 channels. The three tables show that the blocking probability of AA-DPP consistently exceeds all the other approaches. The performance of our proposed approach is very close to that of AU-DPP, particularly when the network is less congested (i.e. more available channels per fiber). As the network congestion increases, the performance of the proposed approach degrades somewhat compared to AU-DPP, but is still better than AA-DPP.

Table 4-4 14-nodes network with 20 demands

	Blocking Probability		
Channels per fiber	**8**	**16**	**32**
Approach			
AA-DPP	62.55	17.49	17.49
Proposed (*i*=1)	57.78	7.25	7.25
Proposed (*i*=2)	58.37	7.25	7.25
AU-DPP	42.24	7.25	7.25

Table 4.4 shows that the blocking probability decreases when the number of channels per fiber increases from 8 channels per fiber to 16 channels per fiber and then remains constant when the number of channels increases from 16 to 32 per fiber.

Table 4-5 20-nodes network with 20 demands

	Blocking Probability		
Channels per fiber	**8**	**16**	**32**
Approach			
AA-DPP	59.75	16.94	16.94
Proposed (*i*=1)	55.58	10.74	10.74
Proposed (*i*=2)	55.29	10.74	10.74

AU-DPP	45.00	10.74	10.74

Table 4-6 40-nodes network with 90 demands

	Blocking Probability		
Channels per fiber	**8**	**16**	**32**
Approach			
AA-DPP	99.33	6.50	0.35
Proposed (*i*=1)	99.31	6.39	0.33
Proposed (*i*=2)	99.31	6.22	0.33
AU-DPP	99.09	4.84	0.33

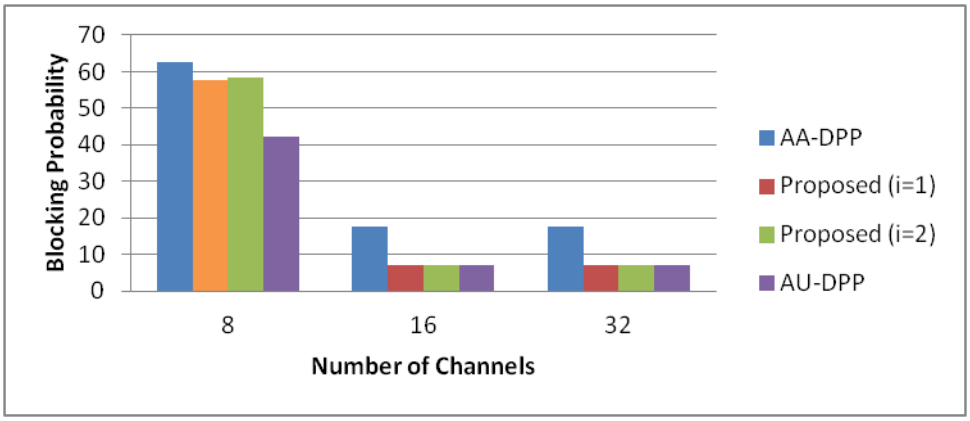

Figure 4-2 Comparison of blocking probabilities with different number of channels

Fig. 4.2 shows that the blocking probability of the AA-DPP approach exceeds the blocking probability of the proposed approached tested with different number of channels per fiber.

5 Conclusion and Future Work

5.1 Conclusion

In this thesis, we have developed a novel heuristic attack-aware RWA with dynamic traffic load in WDM networks. In the heuristic, we have used the dedication path protection scheme to secure the transmission of data in case an attack occurs in any part of the network.

To test the heuristic, we have used existing network topologies and generated synthetic network topologies as well. We have used different sizes of networks (14, 20, and 40 nodes) and different number of channels per fiber for each network size.

The heuristic studies the blocking probability for each network considering under different traffic loads and with different number of channels per fiber, We considered two attack models: i) where the attacking signal can affect the first adjacent channel only and ii) where it can affect the both the first and second adjacent channels as described in Section 3.2.

We have compared our results to the results in [5], where the attacking signal can affect all the channels of the fiber. We found that the blocking probability of our proposed heuristic is lower than the blocking probability of the approach used in [5].

5.2 Future Work

For future work, we may consider studying the performance of the WDM networks using the shared path protection approach, which typically leads to better utilization of available resources. Another future work may be to develop an optimal ILP formulation, which can be used as a benchmark to evaluate the performance of different heuristics.

References

[1] Jaekel, Arunita, Bandyopadhyay, Subir, Al-Mamoori, Saja And Varanasi, Sriharsha,(2015) Security-Aware Dynamic Lightpath Allocation Scheme for WDM Networks, *ICDCN*, Jan. 4-7, 2015.

[2] Furdek, M., And Skorin-Kapov, N. (2009). A scalable wavelength assignment approach for preventive crosstalk attack localization in optical networks. *In 10th International Conference on Telecommunications, 2009. ConTEL 2009.* IEEE, 311-318.

[3] Furdek, M., Skorin-Kapov, N., And Tzanakaki, A.(2011a) Survivable routing and wavelength assignment considering high-powered jamming attacks. *In SPIE/OSA/IEEE Asia Communications and Photonics, International Society for Optics and Photonics*, 83101H- 83101H.

[4] Furdek, M., Chen, J., Skorin-Kapov, N., And Wosinska, L. (2011b) Compound attack-aware routing and wavelength assignment against power jamming. *In Communications and Photonics Conference and Exhibition, 2011. ACP. Asia, IEEE*, 1-3.

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

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

[7] Skorin-Kapov, N., Chen, J., And Wosinska, L (2008). A tabu search algorithm for attack-aware lightpath routing. *In International Conference on Transparent Optical Networks, 2008. ICTON 2008. 10th Anniversary* 2008(3), IEEE, 42-45.

[8] Skorin-Kapov, N., And Furdek, M. (2009). Limiting the propagation of intra-channel crosstalk attacks in optical networks through wavelength assignment. *In Optical Fiber Communication Conference, Optical Society of America,* JWA65.

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

[10] Skorin-Kapov, N., Furdek, M., Pardo, R. A., And Marino, 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.

[11] R. Tripathi, R. Gangwar, and N. Singh, "Reduction of crosstalk in wavelength division multiplexed fiber optic communication systems," *Progress In Electromagnetics Research*, Vol. 77, 367-378, 2007.

[12] Marija Furdek and Nina Skorin-Kapov (2012). Physical-Layer Attacks in Transparent Optical Networks, Optical Communications Systems, Dr. Narottam Das (Ed.), ISBN: 978-953-51-0170-3, InTech, DOI: 10.5772/29836. Available from: http://www.intechopen.com/books/optical-communications-systems/physical-layer-attacks-in-transparent-optical-networks

[13] Wang, Hungjen, Modiano, Eytan, and Médard, Muriel (2002). Partial path protection for WDM networks: End-to-end recovery using local failure information. *Computers and Communications. Proceedings. ISCC 2002. Seventh International Symposium on*. IEEE, 2002.

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

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

[16] Ramaswami, Rajiv, and Sivarajan, Kumar N.. "Routing and wavelength assignment in all-optical networks." *IEEE/ACM Transactions on Networking (TON)* 3.5 (1995): 489-500.

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

[18] Le, Vinh Trong, et al. "Dynamic RWA based on the combination of mobile agents technique and genetic algorithms in WDM networks with sparse wavelength conversion." *IEICE transactions on information and systems* 88.9 (2005): 2067-2078.

[19] Chu, Xiaowen, and Li, Bo. "Dynamic routing and wavelength assignment in the presence of wavelength conversion for all-optical networks." *IEEE/ACM Transactions on Networking (TON)* 13.3 (2005): 704-715.

[20] Anand, Vishal, and Qiao, Chunming. "Static versus dynamic establishment of protection paths in WDM networks." *Journal of High Speed Networks* 10.4 (2001): 317-327.

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

[22] Dutta, Rudra, and Rouskas, George N.. "Traffic grooming in WDM networks: Past and future." *Network, IEEE* 16.6 (2002): 46-56.

[23] Kodian, Adil, and Grover, Wayne D.. "Failure-independent path-protecting p-cycles: efficient and simple fully preconnected optical-path protection." *Lightwave Technology, Journal of* 23.10 (2005): 3241-3259.

[24] Truong, D. L., and Thiongane, B.. "Dynamic routing for shared path protection in multidomain optical mesh networks." *Journal of Optical Networking* 5.1 (2006): 58-74.

[25] Jirattigalachote, Amornrat, Cavdar, Cicek, Monti, Paolo, Wosinska, Lena, and Tzanakaki, Anna. "Dynamic provisioning strategies for energy efficient WDM networks with dedicated path protection." *Optical Switching and Networking* 8, no. 3 (2011): 201-213.

[26] Muhammad, Ajmal, Monti, Paolo, Cerutti, Isabella, Wosinska, Lena, Castoldi, Piero, and Tzanakaki, Anna. "Energy-efficient WDM network planning with dedicated protection resources in sleep mode." In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1-5. IEEE, 2010.

[27] Azodolmolky, Siamak, Pointurier, Yvan, Angelou, Marianna, Solé-Pareta, Josep, and Tomkos, Ioannis. "An offline impairment aware RWA algorithm with dedicated path protection consideration." *Proc. IEEE/OSA OFC/NFOEC, OWI1* (2009): 1-3.

[28] Ngo, Son Hong, Jiang, Xiaohong, and Horiguchi, Susumu. "An ant-based approach for dynamic RWA in optical WDM networks." *Photonic Network Communications* 11, no. 1 (2006): 39-48.

[29] Huang, Yurong, Heritage Jonathan P., and Mukherjee, Biswanath. "Connection provisioning with transmission impairment consideration in optical WDM networks with high-speed channels." *Lightwave Technology, Journal of* 23.3 (2005): 982-993.

[30] Zhang, Qiong, Xie, Weisheng, She Qingya, Wang, Xi, Palacharla, Paparao, and Sekiya, Motoyoshi. "RWA for network virtualization in optical WDM networks." In *Optical Fiber Communication Conference*, pp. JTh2A-65. Optical Society of America, 2013.

[31] Liu, Guanglei, and Ji, Chuanyi. "Resilience of all-optical network architectures under in-band crosstalk attacks: a probabilistic graphical model approach." *Selected Areas in Communications, IEEE Journal on* 25.3 (2007): 2-17.

[32] Peng, Yunfeng, Sun, Zeyu, Du, Shu, and Long, Keping. "Propagation of all-optical crosstalk attack in transparent optical networks." *Optical Engineering* 50, no. 8 (2011): 085002-085002.

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

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

[35] http://www.techopedia.com/definition/25597/computer-network. (As per June 25,2015).

[36] http://www.techopedia.com/definition/23643/optical-network. (As per June 25,2015).

[37] https://en.wikipedia.org/wiki/Optical_networking. (As per June 25,2015).

[38] https://en.wikipedia.org/wiki/Fiber-optic_communication. (As per June 25,2015).
[39] https://en.wikipedia.org/wiki/Optical_fiber. (As per June 27,2015).
[40] https://en.wikipedia.org/wiki/Optical_fiber#/media/File:Singlemode_fibre_structure.svg . (As per June 27,2015).
[41] https://en.wikipedia.org/wiki/Total_internal_reflection . (As per June 27,2015).
[42] https://en.wikipedia.org/wiki/Single-mode_optical_fiber. (As per June 27,2015).
[43] https://en.wikipedia.org/wiki/Multi-mode_optical_fiber. (As per June 30,2015).
[44] http://www.telebyteusa.com/foprimer/foch2.htm. (As per June 30,2015).
[45] http://www.telebyteusa.com/foprimer/foch3.htm. (As per June 30,2015).
[46] https://en.wikipedia.org/wiki/Wavelength-division_multiplexing. (As per June 30,2015).
[47] http://www.igi-global.com/dictionary/lightpath/17153. (As per June 30,2015).
[48] https://en.wikipedia.org/wiki/Routing_and_wavelength_assignment. (As per June 30,2015).
[49] https://en.wikipedia.org/wiki/Path_protection. (As per June 30,2015).

VITA AUCTORIS

NAME:	Marcel El Soury
PLACE OF BIRTH:	Tripoli, Lebanon
YEAR OF BIRTH:	1971
EDUCATION:	University of Balaman, Al Koora, Lebanon Bachelor of Sciences, Computer Science 1992-1995
	University of Windsor, Windsor ON, Canada Master of Science, Computer Science 2013-2016