

# Comprehensive Security Strategy for All-Optical Networks

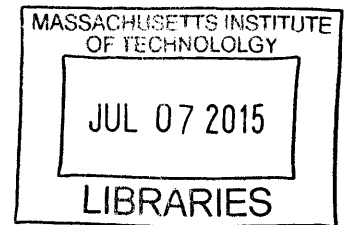
Antonia Lynn Feffer  
B.S. Electrical Engineering  
United States Military Academy (2013)

Submitted to the Department of Electrical Engineering and Computer Science  
in partial fulfillment of the requirements for the degree of  
Master of Science  
in  
Electrical Engineering and Computer Science  
at the  
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2015

© 2015 Massachusetts Institute of Technology. All rights reserved.

**ARCHIVES**



*[Handwritten signature]*  
**Signature redacted**

Author .....

.....  
Department of Electrical Engineering and Computer Science  
May 20, 2015

*[Handwritten signature]*  
**Signature redacted**

Certified By ...

.....  
Vincent W.S. Chan  
Joan and Irwin Jacobs Professor of Electrical Engineering and Computer Science  
Thesis Supervisor

*[Handwritten signature]*  
**Signature redacted**

Accepted By .....

.....  
*[Handwritten initials]*  
Leslie A. Kolodziejski  
Chair, Department Committee on Graduate Students



The views expressed in this work are those of the author and do not reflect the official policy or position of the United States Army, Department of Defense, or the United States Government.



# Comprehensive Security Strategy for All-Optical Networks

by

Antonia Lynn Feffer

Submitted to the Department of Electrical Engineering and Computer Science on May 20, 2015  
in partial fulfillment of the requirements for the degree of Master of Science in Electrical  
Engineering and Computer Science

## Abstract

Optical networking is a powerful means of communication in modern times of high bandwidth demands and high data speeds. While developments in optical networking continue to progress, however, the security implications they create have not yet caught up.

In this thesis, we characterize a selection of damaging attacks against optical networks. By providing a detailed description of the attacks, we are also able to better understand their effects across the different layers of the network model. We also propose the current best practices for sensing and detection of these attacks when they occur, as well as mitigation techniques to limit the damage they incur. The attacks are not fully eliminated, however, and so we also identify remaining vulnerabilities these attacks can exploit.

After characterizing the attacks, we propose a method for diagnosing attacks as they occur within a network given the analysis we have conducted. We also propose an algorithm for diagnosing attacks, as well as a monitoring system framework that relies on the establishment of autonomous zones of the network in order to efficiently limit damage and quarantine problem areas from the rest of the healthy network. This framework can be applied to a wide variety of network set-ups and topologies, with the ability to customize it to fit the needs of the system.

Thesis Supervisor: Vincent W.S. Chan

Title: Joan and Irwin Jacobs Professor of Electrical Engineering and Computer Science



## **Acknowledgments**

First and foremost, I would like to thank Professor Chan for taking me into his research group, and for all the learning opportunities and mentoring he has provided me during my time at MIT. I would also like to thank the National GEM Consortium, as well as the United States Army, the MIT EECS Department and MIT's Office for Diversity Graduate Education for providing me with financial support and the opportunity to pursue an advanced degree.

I am very grateful to all the instructors and mentors I had at West Point for providing me with the skills and academic preparation needed to be successful at MIT. I am incredibly thankful to the NSBE Excel Scholars program and the West Point Scholarship Program for pushing me to apply to graduate school and helping me achieve that goal.

I could not have asked for a better research group to have been a part of, so I would like to thank my fellow members of the "Chan Clan" for being supportive and making my time here very enjoyable. I am incredibly fortunate to have met so many great people during my time in Cambridge, and I am thankful to all my friends here for making this an unforgettable experience.

Finally, and most importantly, I would like to thank my family for being a constant source of support and encouragement, especially when I most needed it. I definitely would not be here today without all the love and reassurance you all have given me. I would also like to thank "the kids," especially my sister, Jianna, for pushing me to excel so that I could set a good example for all of you. In particular, I would like to thank Sam, Nana, and my mother, Eraina for believing in me and pushing me to reach my full potential.





# Contents

<b>1</b>	<b>Introduction.....</b>	<b>19</b>
1.1	Security Strategy Development .....	20
1.1.1	Practical Security Applications .....	20
1.1.2	Components of Security Planning.....	21
1.2	Thesis Organization .....	24
<b>2</b>	<b>Description of Attacks .....</b>	<b>27</b>
2.1	Cutting/Bending/Tapping Fibers .....	28
2.2	Out-of-Band Crosstalk.....	31
2.3	In-Band Crosstalk .....	32
2.4	Repeat-Back Jamming .....	34
2.5	Gain Competition/Out-of-Band Jamming.....	37
2.6	Power Transients.....	39
2.7	Control Plane/Looping Attack .....	42
2.8	SNMP Modification.....	43
2.9	Link State Protocol (LSP) False Advertising.....	44
2.10	Summary for Chapter 2.....	46
<b>3</b>	<b>Sensing, Detection, Localization, &amp; Mitigation.....</b>	<b>49</b>

3.1	Cutting/Bending/Tapping Fibers .....	49
3.2	Repeat-Back Jamming .....	58
3.3	Out-of-Band Crosstalk .....	64
3.4	In-Band Crosstalk .....	65
3.5	Gain Competition/Out-of-Band Jamming.....	67
3.6	Power Transients.....	70
3.7	Control Plane Attack (Looping Attack).....	75
3.8	Simple Network Management Protocol (SNMP) Modification .....	78
3.9	Link State Protocol (LSP) False Advertising.....	80
3.10	Summary of Chapter 3 .....	81
<b>4</b>	<b>Security Strategy Formulation .....</b>	<b>83</b>
4.1	Attack Diagnosis Framework .....	83
4.1.1	Diagnoses Model.....	84
4.1.2	Algorithm for Effective Attack Response.....	85
4.2	Monitoring System Implementation .....	86
4.3	Network Quarantine and Recovery Process .....	89
4.3.1	Determining Quarantine Area .....	90
4.3.2	Segmentation via Autonomous Zones.....	91
4.3.3	Introduction of the Network Management Hub .....	91
4.3.4	Impact of Quarantine.....	94

4.4	Summary of Chapter 4.....	96
<b>5</b>	<b>Conclusion .....</b>	<b>97</b>
5.1	Summary of Contributions.....	97
5.2	Future Work and Challenges .....	98
<b>A</b>	<b>Chapter 3 Equation Derivations.....</b>	<b>101</b>
	Derivation of Equation 3.1.....	101
	Derivation of Equation 3.3.....	102
	Derivation of Equation 3.7.....	103
<b>B</b>	<b>List of References for Figure 1.1 .....</b>	<b>105</b>
	<b>Bibliography .....</b>	<b>107</b>

# List of Figures

## 1.1 Attack Research by Country

Graph depicting the number of groups working on research concerning each of the optical attacks with respect to all-optical networks, categorized by country.

## 1.2 Steps in Security Development

Flowchart depicting the essential steps to follow in developing an effective security plan

## 2.1 Signal Power After Power Reduction Attack

Diagrams illustrating the effects of an attack that induces a loss of power. (a) Signal strengths of a collection of wavelengths in a lightpath. (b) Signal strengths of the same wavelengths after  $\lambda_{green}$  has experienced an unanticipated loss of power. (c) Signal strengths of the wavelengths shown in (b) after passing through an optical amplifier.

## 2.2 Out-of-Band Crosstalk

Figure depicting how out-of-band crosstalk can occur. Signals (commonly of a high power level) “bleed” into adjacent signals of different wavelengths, causing components of the signals to mix.

## 2.3 In-Band Crosstalk Attack

Figure depicting how in-band crosstalk can occur. A lightpath is separated into its component wavelengths imperfectly, resulting in fragments of the wavelengths to appear on other ports for different wavelengths. When the constituent wavelengths are recombined, the fragments destructively interfere with their original wavelength signals.

## **2.4 In-Band Crosstalk Eavesdropping Attack**

Figure depicting how an eavesdropping attack via in-band crosstalk can occur. An attacker exploits the crosstalk over an empty switch channel to tap the traversing signal. The attacker may also inject a signal to have crosstalk imprinted on via this method.

## **2.5 Repeat-Back Jamming Attack**

Figure depicting how a repeat-back jamming attack can occur. A signal is tapped from the channel and reinserted (reintroduced signal shown as a dotted line) back into the channel with the original signal, leading to destructive interference.

## **2.6 Repeat-Back Jamming Analysis**

Graph showing the effects of a repeat-back jamming attack at different phase shifts (translating into delay times). The x-axis gives the amount of the original signal that is tapped away (-1dB is equivalent to a loss of ~80% of the signal), with the resulting power of the recombined signal shown on the y-axis.

## **2.7 Gain Competition Attack**

Figure depicting how a gain competition attack can occur. A high-powered signal is injected into the channel prior to it passing through an optical amplifier. Due to the proportional nature of EDFA power allocation, the high-powered signal deprives the other signals of upper-level photons [5], resulting in weaker gain for the other signals.

## **2.8 Attack via Power Transients**

Figure depicting how an attack using power transients can occur. A malicious user abruptly activates a lightpath, resulting in a power transient that corrupts all other currently transmitting frames.

## **2.9 Power Transients Analysis**

Graphs depicting effects of power transients [28]. Graph (a) depicts signal power as lightpath is activated/deactivated. Graph (b) shows the effect of a power transient as a function of varying adiabatic switching times. Graph (c) shows overshoot and undershoot of various lightpath configurations.

## **2.10 Control Plane/Looping Attack**

Figure depicting how a control plane attack can occur. The attacker tampers with the control plane software, allowing them to alter traffic flows and network configurations. The yellow route shown is caused by malicious rerouting via the control plane.

## **2.11 Attack via SNMP Modification**

Figure depicting how an attack via SNMP modification can occur. The attacker infiltrates the SNMP protocol and generates false status information for network components, which is then passed along to other nodes.

## **2.12 Attack via LSP Modification**

Figure depicting how an attack via LSP false advertising can occur. The attacker tampers with the LSP protocol and generates false status advertisements, which are then propagated throughout the network via LSP.

## **3.1 Power Level Monitoring Localization without Redundancy**

Diagram showing the spatial layout of power level monitors spaced at their maximum operational range (max range is 2 link in this scenario). When an attack occurs (denoted by red X), the precision is limited to the localization range of the device, and thus the attack is localized to an area of 2 links.

### **3.2 Power Level Monitoring Localization with Redundancy**

Diagram showing the spatial layout of power level monitors where the monitoring span overlaps with one another, creating an effective localization range of 1 link. When an attack occurs (denoted by red X), it can thus be localized to an area of one link.

### **3.3 Arrival Rate Analysis for $\lambda = 50$ tps**

Graph showing the relationship between a value  $p$  and the probability of observing an arrival rate outside of  $\lambda \pm \lambda p$ , where  $\lambda$  is the anticipated arrival rate. It is established that the likelihood of seeing a value outside of the specified interval decreases as  $p$  increases.

### **4.1 Retrofitting of Autonomous Zones onto Existing Network**

Figure illustrating how autonomous zones could be retrofitted over a preexisting network architecture. The red circles represent established autonomous zones, which are manually designated to ensure they meet all the qualifications for a true autonomous zone.

### **4.2 Depiction of Autonomous Zone (AD) Network with Network Management Hubs (NMHs)**

Figure depicting an example network comprised of communicating autonomous zones (denoted by red circle), with network management hubs (denoted by yellow boxes) that constitute a separate diagnostic network (denoted by green links).

### **4.3 Example of Quarantine Recovery Process Event Flow**

Figure depicts the series of events generated by the quarantine recovery process in an example situation. After the first quarantine, the cost increases exponentially during the probationary period. As another quarantine is triggered during the probationary period,

the cost again increases exponentially. After the resulting probationary period, the cost reverts to the previous value until it eventually returns to its original cost.



# List of Tables

## 2.1 Description of Select Fiber Tapping Attacks

Table compares a selection of fiber tapping attacks based upon the amount of power loss the attacked signal incurs, the ease of applying the method in a real-world setting, and the attack's ability to be detected by network monitoring.

## 2.2 Classification of Common Attack Effects

Table lists common symptoms of various attacks, separated by layer. The classification of these symptoms is a combination of the layer designator (the number/letter found in parentheses next to the layer name) and the letter assignment in the left-hand column.

## 2.3 Comparison of Multilayer Attack Effects

Table lists the originating layer of each attack, as well as the effects the attack has across the other network layers. Uses Table 2.2 to give more detailed description of attack effects.

## 4.1 Diagnosis Framework for Potential Attacks

Table lists the most prominent symptoms for each attack, which is then used to develop the diagnosis scheme for identifying and treating the various attacks listed.

## 4.2 Diagnosis Algorithm

Table lists the steps that the algorithm uses in order to accurately diagnose an attack based on observed system operation and identified faults. Algorithm follows the attack-symptom matching found in Table 4.1.

### **4.3 Monitoring System Applications**

Table lists the different attacks analyzed and gives the recommended sensing methods for detecting the known symptoms the attacks generate (as described in Table 4.1).

### **4.4 Localization Range for Optical Attacks**

Table lists the smallest localization range for each attack based upon analysis done in Chapter 3 and the recommended sensing methods described by Table 4.3.

# Chapter 1

## Introduction

With the introduction of fiber optic technology as a replacement for copper cables in the 1970s, optical networking has been a strong source of innovation and engineering in the telecommunications industry. As demands for network capacities reach higher and higher levels as it has with the ubiquity of streaming video and other capacity-consuming applications, the use of all-optical networks becomes more and more justified.

All-optical networks (AONs) provide a tremendous amount of bandwidth, with a single cable capable of achieving a data rate of 30THz [24]. The ability to support very high data transmission rates also allows it to be relatively cost efficient, in comparison to electronic packet switching networks of the same size. AONs also eliminate the need for the regeneration of signals during transmission, as networks rely on the propagation of lightpaths from end to end.

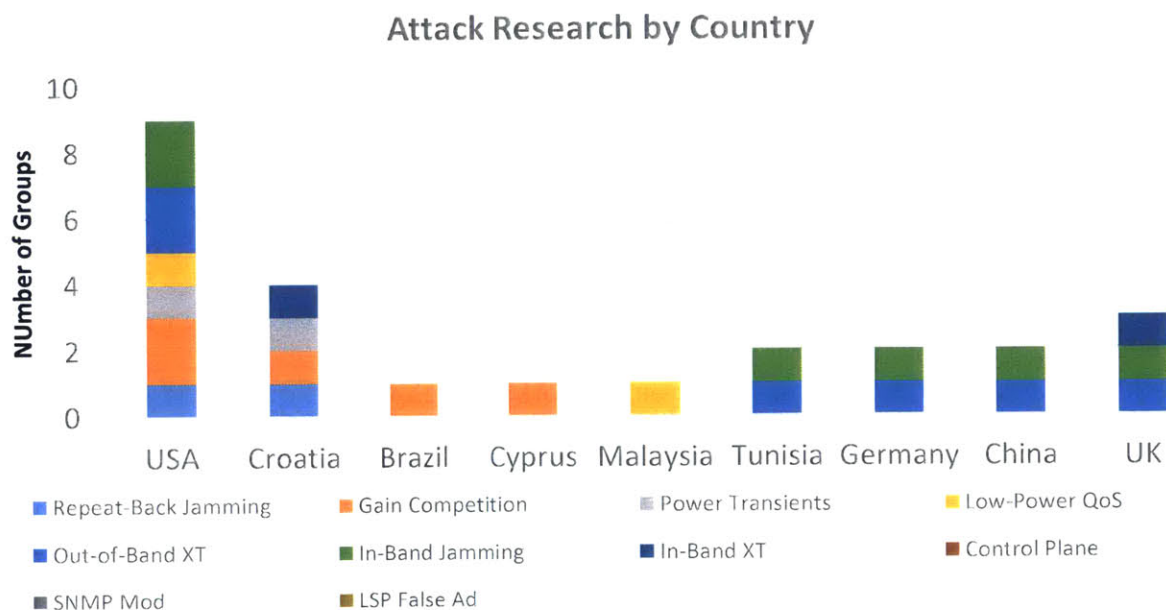
For all the benefits of optical networking, however, there are still significant flaws in their implementation. Optical devices that are required to establish and maintain a broad, diverse network, such as optical amplifiers, switches, and cross-connects, are susceptible to a wide array of attacks that can have a crippling effect on network throughput and quality of service. The rapid growth of optical networking research and transition into the real world has outpaced the creation of defensive and protective measures to ensure that the communications are robust against attack. In this work, we seek to help close that knowledge gap and create a more secure optical networking environment.

## 1.1 Security Strategy Development

An essential aspect in increasing network robustness is the development of defensive and preventative measures that are effective in thwarting attack. To do this, we must first develop a security strategy, which outlines the process in which attacks are handled on either a proactive or reactive basis.

### 1.1.1 Practical Security Applications

The subject of optical network attacks and defense is relatively under-researched in comparison to their counterparts in electronics-based communications, the pool of knowledge is steadily increasing. The following chart, Figure 1.1, shows which attacks are being researched and where, giving a sense of who is interested in the subject and which attacks have been more



**Figure 1.1 – Attack Research by Country.** Graph displays the number of groups publishing optical network attack/security research, categorized by country.

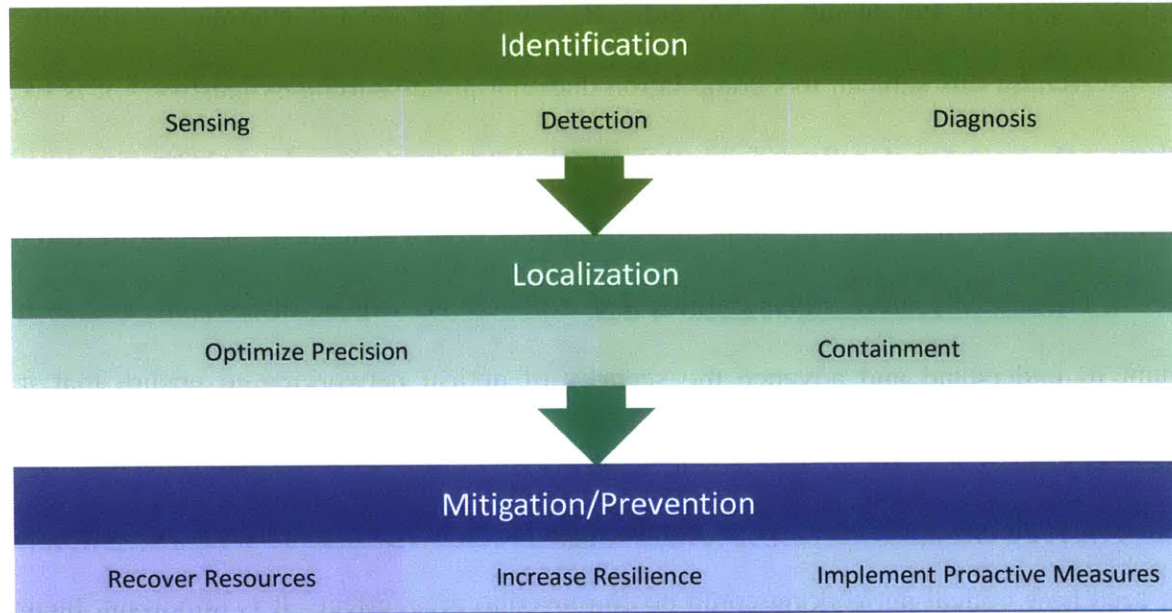
extensively explored (full listing in Appendix B). Although the list attempts to identify all groups researching this subject, this compilation does not promise to be exhaustive – it is likely that there are groups not reflected on this graph, and there are almost certainly groups researching the topic that have not yet published findings to be catalogued. As more research is conducted, undoubtedly more vulnerabilities and exploitations will be discovered, and so it is important to understand and advance the security of optical networking to ensure that it is keeping pace.

From high-speed in home fiber connections to high-capacity military networks, it is readily seen how optical networking could be employed to great effect. It is important, then, to ensure that these networks are adequately defended against any acts of malice that would diminish the performance benefits and cause the network to fail to meet the service expectations of its users.

### **1.1.2 Components of Security Planning**

The first step in a defensive security plan is the identification of an attack when it arises. This is achieved through monitoring of the network and checking for known signs of attacks or any other abnormalities in standard network operation. *Sensing* is the observation of the quality of service, processes, and actions of the network in order to characterize its behavior. *Detection* is the discovery of an abnormal process or action, and is usually achieved through sensing, making sensing and detection a joint concept in this context.

Another critical component of an effective security strategy is the ability to localize an attack once identified. *Localization* is the ability to pinpoint the origin of the event with a reasonable degree of certainty. Finding a precise point of origin for an attack can be a very challenging task



**Figure 1.2 – Steps in Security Development**

without exhaustive, constant monitoring of the network, but the ability to localize the origin to a limited area through the use of multiple sensors can be just as effective as a single sensor of the same small resolution. For all-optical networks, lightpaths have a long span (as much as across the continent) and attacks can be thousands of miles away and thus increases the difficulty of localization. *Resolution* in this case refers to the minimum size at which an event can be accurately measured or observed. Thus, as the resolution size becomes smaller, the precision in which an event can be localized increases.

At several points in this work, we use proposed methods for sensing and detection to also localize an attack. Intuitively, it can be seen that if a sensing device registers an abnormality indicative of an attack, then it can be reasonably concluded that the attack originated at some point along the span over which the device measures. This span, thus, is referred to as the *localization range* of the device. Using the minimum number of devices possible to fully monitor the network, the smallest area to which an attack could be pinpointed would be equivalent to the localization range of the devices used.

In a heterogeneous network, different sensing devices may be used in conjunction with one another, leading to varying localization ranges. Introducing redundancy so that multiple devices cover the same areas can also decrease the uncertainty for where precisely an attack originated, effectively decreasing the localization range. The *network resolution* is defined as the greatest operational localization range at which an event can be localized in the network. As a result, the network resolution is limited by the least precise localization method in place in the network.

Once the attack has been localized to the most precise level possible, then the attack must be contained to prevent it from spreading to other areas of the network. In this work, we refer to containment of the attack to a region as a *quarantine* of the attack area. By quarantining the area, the attack can no longer propagate its effects outside of the containment area, thus limiting the damage it can inflict upon the network. While quarantining attack areas may impact network performance by potentially shutting down healthy areas as well, we believe the benefits are much greater in that the attack threat is eliminated from the network while under quarantine, and its damage restricted.

The final aspect of an effective security plan is having effective mitigation tactics in place to further limit the amount of damage an attack may inflict, as well as to create a more robust network that can continue to function properly despite attack. Resilience is a critical component for any mitigation strategy, both in terms of recovering from an attack and continuing on despite attack. As previously discussed, containing the problem to a limited area may be an effective solution for a time, but it should not last indefinitely; eventually, the affected area should be returned to a functional state and reintroduced into the network, restoring network resources and

bringing it back to its full operational capacity. The faster a network can recover from an attack, the better its performance and service quality.

Resiliency can also be attained through increasing the robustness of the system, making it more difficult to be completely disabled by an attack. The use of forward error correcting code is a classic example of one such method, allowing messages to still be transmitted and received correctly despite events that would otherwise hinder performance and reduce throughput.

Finally, anticipating attacks and preparing proactive automated defenses against them is an important element of attack mitigation, as it prevents issues from arising before they even begin, making it more difficult for adversaries to damage the network and even serving as a deterrent for future attacks.

## **1.2 Thesis Organization**

The rest of the thesis is organized as follows:

In Chapter 2, we introduce the attacks this work focuses on through detailed descriptions of their mechanics. We also examine where the attacks originate and the effects that they generate across multiple layers of the network.

In Chapter 3, we delve into the aspects of the attacks required for effective security planning. First, we examine the various methods of sensing and detection that could be used for each attack. We then discuss the limitations on localizing the origin point of the attack, which is critical to efficiently eliminating the threat. Next, we cover a variation of ways in which the attacks can be mitigated and protective measures that can be put in place to proactively guard against them. Finally, we outline the remaining vulnerabilities that could be exploited by an attacker, despite the defensive measures taken to protect the network.



In Chapter 4, we propose a methodology for attack diagnosis which relies on the analysis done in the previous sections. We then define a methodology for implementing a monitoring system to best fit the requirements of an arbitrary network, allowing for flexibility and customization in application. Finally, we develop a preventative quarantine system for networks under attack that incorporates the use of autonomous zones to minimize performance loss and eliminate the threat of attack.

Finally, in Chapter 5, we conclude the thesis with a summary of our contributions and discussions of promising future areas of research.



# Chapter 2

## Description of Attacks

The first step in creating a successful security strategy is understanding the applicable set of challenges. The following chapter describes the known and other feasible attacks against all-optical networks (AONs) and serves as a starting point for developing an effective defense against adversarial attacks. The attacks can affect any layers of the networks, from the physical to the application layer, and even the network management and control planes. In most of the attacks known, entry at a given network layer almost always affects the performance of other layers, although those consequential effects are not often registered and/or discussed. Ultimately, the network performance the application layer sees is the correct performance metric, as the end-user experience is what is critical to acceptable network performance. The following is a list of attacks we have considered.

- 1) Cutting/Bending/Tapping Fibers
- 2) Out-of-Band Crosstalk
- 3) In-Band Crosstalk
- 4) Repeat-Back Jamming
- 5) Gain Competition/Out-of-Band Jamming
- 6) Power Transients
- 7) Control Plane/Looping Attack
- 8) Simple Network Management Protocol (SNMP) Modification

## 9) Link State Protocol (LSP) False Advertising

While the list is rather comprehensive, there is no evidence that it is anything close to exhaustive.

We will discuss the techniques to identify, localize, and mitigate these attacks in Chapter 3.

### 2.1 Cutting/Bending/Tapping Fibers

Both cutting and bending of the fiber are attacks that originate purely in the physical layer. With cutting, an attacker cuts or nicks the fiber to create a surface imperfection, resulting in light loss with resulting performance degradations. The result of such an attack could range from degradation of service via signal power reduction to total denial of service if a fiber is irrecoverably damaged or severed.

In a bending attack, a malicious user bends the optical fiber to a point at which the angle of the light travelling through the fiber surpasses the critical angle for total internal reflection, resulting in the light radiating out of the fiber and dissipating into its surroundings. The result would be a degradation of Quality of Service (QoS), as the signal power is reduced. A malicious user could also exploit the light radiating from a fiber to use as part of a tapping scheme, intercepting user data. Table 2.1 outlines a variety of attacks mentioned in [27], classifying them

Method of Tapping	Power Loss Incurred	Ease of Application	Detectability
Fiber Bending	Depends on bend radius	Relatively easy	Varies with subtlety of bend
Optical Splitting	As low as ~1dB	Moderate	High
Evanescent Coupling	1-2dB	Difficult	Moderate
V-Groove Cut	As low as ~1dB	Very difficult	Difficult
Scattering	As low as ~1dB	Extremely difficult	Very difficult

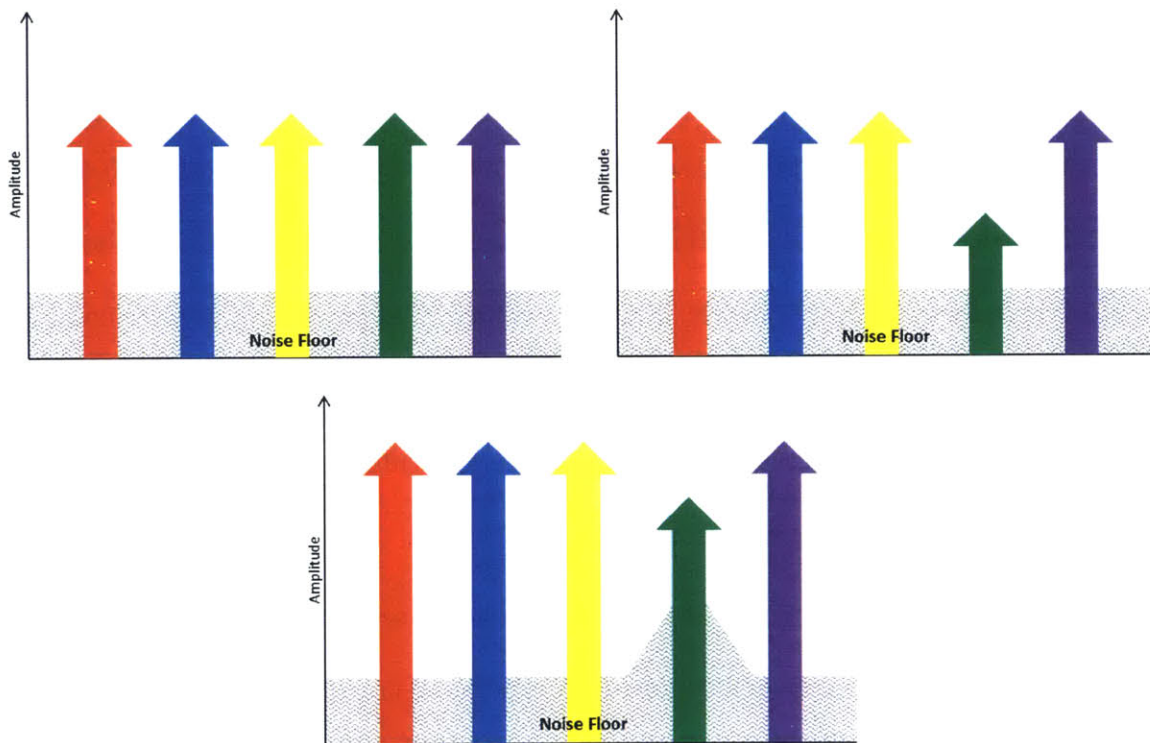
**Table 2.1 - Description of Select Fiber Tapping Attacks. Attack methods are classified based upon power loss incurred by the attacked signal, the ability to perform the method in a practical setting, and the ease in which it can be detected by sensing methods.**

based upon the optical power loss incurred through the application of the method, as well as the ease of actually conducting the attack in a real-world setting, and the degree of ease to which it can be detected by sensing devices

Fiber bending is the physical bending of the optical fiber in order to radiate light out of it, as previously described. Optical splitting literally splits a signal into two identical signals via splicing of the fiber onto either end of the splitter, which is an intrusive task [27]. Evanescent coupling is similar in nature to the optical splitting method, although it achieves the tap by polishing the cladding of both the target and a capture fiber close to the core to a point at which some light could be coupled out through the adjacently-placed capture fiber, which is very difficult to achieve without the use of sophisticated equipment, although it has the advantage over optical splitting in that it does not induce service disruption [27]. V-groove cutting involves making a precision-shaped cut into the fiber cladding, which would allow light to be coupled out through the side of the fiber, resulting in very little loss, but a painstakingly complicated implementation process [27]. Finally, scattering involved the employment of an Excimer UV laser to etch a Bragg Grating onto the fiber, allowing the light to be tapped out – although being the most advanced and hardest to detect, it is also the hardest to practically execute and requires a significant amount of instrumentation [27]. For this range of tapping attacks, it is apparent that the ease of performing the attack shares a close correlation with the difficulty of detection, with the more subtle attacks being the hardest to implement.

Naturally, with a clear cutting attack, the user would see a total denial of service as the physical medium has been irrecoverably halted. A bending or tapping attack, however, would be less obvious. If a portion of the signal were radiated or tapped out, the user would see an overall decrease in power that could result in a lower signal to noise ratio, with the amount of power lost

directly affecting the packet loss rate and/or the decoded bit error rate after the error correcting code. As the lightpath continues to propagate through the network, this power reduction could become more problematic as devices like optical amplifiers will intensify the problem, as shown in Figure 2.1. Depending on how much the quality is degraded, the signal is open to being incorrectly routed and/or triggering the transport layer protocol to slow down transmission. In the Transmission Control Protocol (TCP) for example, poor message quality could lead to erroneous packets being discarded, requiring retransmission. This, in turn, could trigger TCP to begin to decrease the window size due to perceived congestion, which substantially throttles back transmission rate, reducing throughput by as much as two orders of magnitude. Thus, the initial problem of diminished signal power is exacerbated across subsequent layers with a multiplier effect.



**Figure 2.1 – Signal Power During Power Reduction Attack; (a) Signal power levels across multiple wavelengths during normal network operation; (b) Signal power levels after  $\lambda_{green}$  experiences a decrease in power; (c) Signal power levels after lightpath passes through optical amplifier, amplifying noise as well as signal**

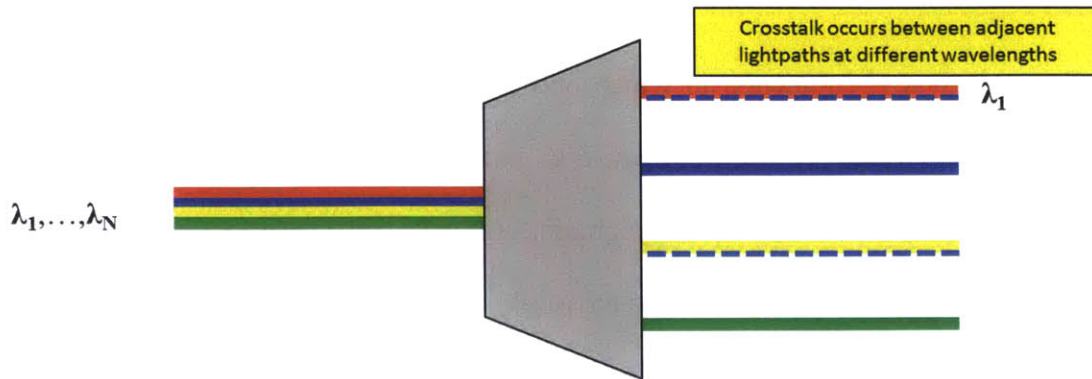
## 2.2 Out-of-Band Crosstalk

Crosstalk is a phenomenon in which one transmitted signal undesirably affects another signal, a process which is well-known and extensively researched in electronics-based communication systems. In the optical domain, crosstalk can occur in a number of different ways, one of which is through out-of-band crosstalk. Out-of-band crosstalk occurs when a signal from one wavelength being transmitted in a channel has a detrimental effect on a neighboring signal of a different wavelength. Out-of-band crosstalk is more prevalent when high signal powers are involved [18], which is fairly unlikely in all-optical networks where signals are propagated long distances.

One of the main sources of this type of optical crosstalk is through the nonideal response of system multiplexers and/or demultiplexers [6]. Figure 2.2 illustrates how crosstalk occurs during demultiplexing – as the signal is separated into its component wavelengths, it is possible that the process is not perfectly executed, and thus the data of one wavelength can “bleed” into that of adjacent wavelengths, creating crosstalk.

Another main cause of optical crosstalk is via coupling within an optical switch. In this scenario, the switch output ports are imperfectly isolated from one another, and thus it is possible for the wavelength signals to mix and create crosstalk [18].

Although demultiplexers can be the source of crosstalk, they can also serve to decrease or eliminate it by serving as a filter and removing the elements of the attacking signal as they divide the lightpath. Optical filters can also be used to achieve the same effect, only allowing specific wavelengths to pass and consequently reducing or eliminating the attacking signal components.



**Figure 2.2 – Out-of-Band Crosstalk Attack. In this example, the blue and green wavelengths create crosstalk on adjacent lightpaths, denoted by the dashed lines.**

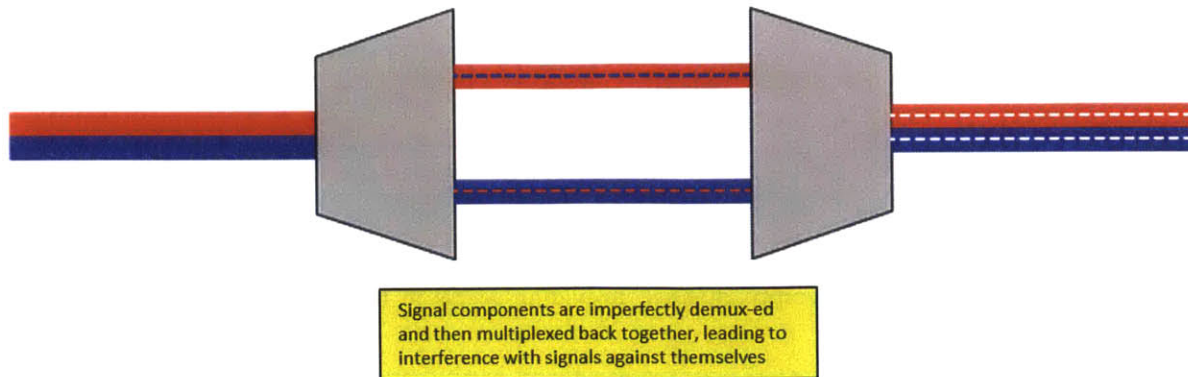
While crosstalk can occur during normal system operation, the malicious induction of crosstalk could be very damaging to the network. Out-of-band crosstalk can be generated through the insertion of a high-powered signal, which is more likely to produce the phenomenon. The resulting crosstalk can lead to corrupted packets being received due to the merging of the signals, which in turn could complicate routing as the destination information becomes undecipherable, as well as lead to retransmission requests that prompt the transport layer to start decreasing its window size as a protective measure. This results in reduced throughput and an underutilization of network resources, with the resulting reduction in capacity possibly felt by the end-users.

### 2.3 In-Band Crosstalk

Another form of crosstalk is known as in-band crosstalk, in which a signal of the same wavelength detrimentally affects another signal. Due to the fact that the crosstalk occurs on the same wavelength throughout the attack, it can be much more damaging than out-of-band crosstalk, as the attacking signal is indistinguishable spectrally from the benign signal.

A main source of this type of crosstalk also stems from multiplexing/demultiplexing. An example of this is shown in Figure 2.3. Due to the poor isolation of the ports of the device, a



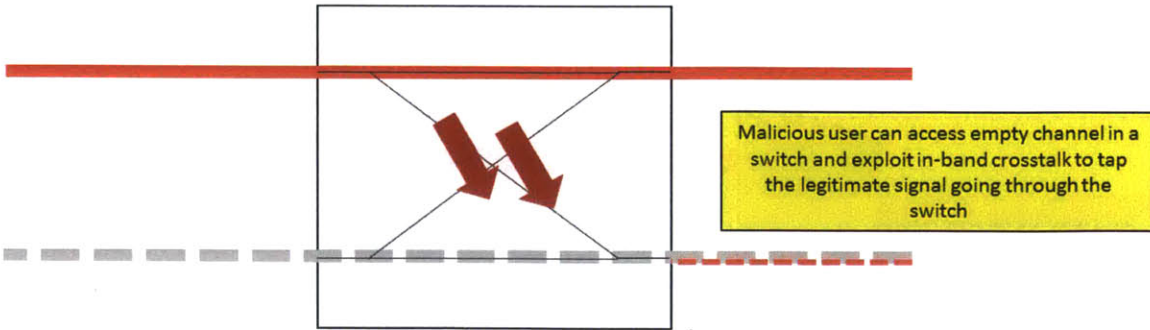


**Figure 2.3 – In-Band Crosstalk Attack.** In this example, components of other lightpaths are not fully separated, creating destructive interference when recombined (denoted by dashed white lines).

small fragment of each wavelength signal can leak onto the ports reserved for other wavelengths during demultiplexing; when eventually multiplexed back together, those small signal fragments will be combined with everything else in the unified channel, resulting in crosstalk effects on a wavelength from delayed (phase shifted) components of itself [4]. The poor isolation of switch ports can also cause in-band crosstalk in the same manner as out-of-band crosstalk.

The resulting crosstalk can lead to destructive interference of the signal against itself, as the juxtaposed components are recombined. This could, in turn, diminish the signal quality to a point where the messages are no longer readable by the receiver, causing network and transport layer issues like those in an out-of-band jamming attack, and causing network throughput to suffer. Crosstalk in general is an attack that can propagate with relative ease, as most times it can be initiated by a comparatively high signal power, and thus it is important to cut off the attack before its effects are disseminated through the network.

An attacker may also exploit naturally-occurring crosstalk to “eavesdrop” on signal transmissions passing through a switch, as illustrated in Figure 2.4. By accessing an empty channel, a malicious user can effectively tap a signal, picking up a portion of the signal



**Figure 2.4 – In-Band Crosstalk Eavesdropping Attack.** In this example, natural crosstalk from the red signal is picked up on the empty channel, providing access to the signal information via an artificial tap.

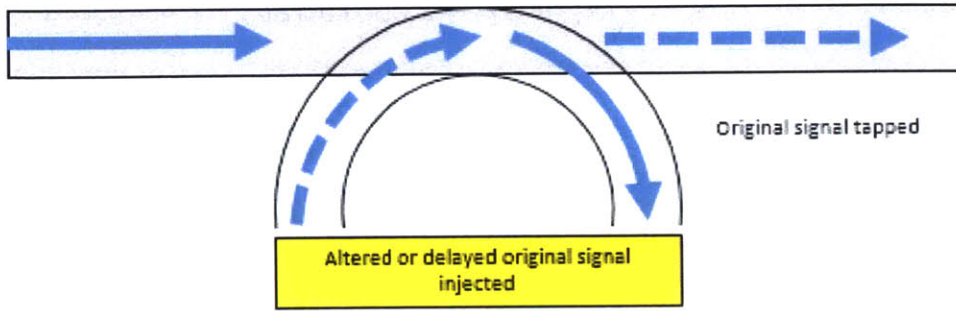
traversing the switch through innate crosstalk (the causes of which have been previously described) [4].

With access to the signal, and perhaps the data, being transmitted, the malicious user can learn more about the network, or even use the signal for other nefarious purposes, such as repeat-back jamming, described in the next section.

## 2.4 Repeat-Back Jamming

In a repeat-back jamming attack, a malicious user taps a portion of a signal from a fiber and re-inserts it into the fiber after some delay. The resulting signal is thus a coherent combination of the original signal and the reintroduced signal, as shown in Figure 2.5. Although mentioned in [4] and [5], this attack has not been described in detail or characterized before.

In such an attack, the signal deteriorates due to the mismatched phases of the original signal and the reintroduced, delayed signal, leading to destructive interference and quality degradations. This type of attack is especially difficult to detect due to the use of interference that looks like the signal against itself. When done at a level slightly higher than the level of acceptable signal quality, it seems as if the signal has naturally deteriorated. Attack propagation for long haul optical lightpaths is another concern from this attack, as a small signal deterioration can be exacerbated as the signal travels through optical amplifiers and other various components,



**Figure 2.5 – Repeat-Back Jamming Attack.** In this example, a portion of the blue signal is tapped out and reintroduced after some delay, incurring a phase shift (denoted by dashed line). The signals then recombine, causing destructive interference.

making the point of origin of the attack extremely difficult to locate. In particular, the signal to noise ratio of the attacked wavelength is diminished, particularly after picking up more ASE noise of subsequent amplifiers, and even after equalization, the signal to noise ratio will not recover.

Repeat-back jamming makes the signal vulnerable to destructive interference of the delayed signal against the original signal. The amount of phase shift incurred is a function of the delay introduced into the system, most easily accomplished through the rerouting of a signal through an arbitrary path before reintroducing it. This phase shift can be calculated using the following equation, where  $d$  is the length of the path and  $\lambda$  is the wavelength of the light.

$$\Delta\theta = \frac{2\pi d}{\lambda} \quad (2.1)$$

Depending on their relative strengths and the amount of phase difference between them, the signal could be dramatically diminished. The following equations give the resulting signal strength,  $S_n$ , and magnitude of phase change,  $\theta_n$ , after a repeat-back jamming attack with  $\Delta\theta$  representing the overall phase shift (modulo  $2\pi$ ) between the original and delayed signals, and  $S_o$  and  $S_d$  representing the signal strength of the original and delayed signals, respectively.

$$S_n = \sqrt{S_o^2 + S_d^2 + 2S_oS_d \cos(\Delta\theta)} \quad (2.2)$$

$$\theta_n = \sin^{-1} \left( \frac{S_d \sin(\Delta\theta)}{S_o + S_d \cos(\Delta\theta)} \right) \quad (2.2)$$

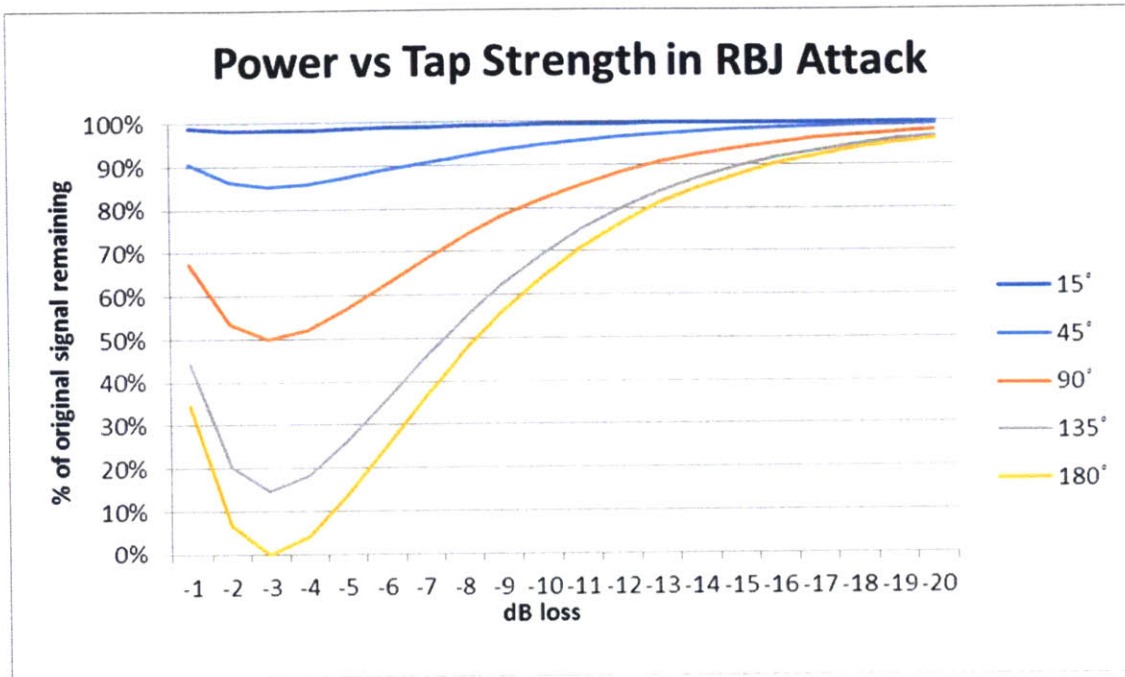
The effectiveness of a repeat-back jamming attack is a function of both the tap strength and the added delay (in the form of a phase shift) induced by the attacker. Figure 2.6 shows this effectiveness by comparing phase shifts of the reintroduced signal across different tap strengths (with the tap strength being the strength of the reintroduced signal), and the resulting effect on the continuing signal.

The most detrimental effects amongst any amount of delay are when -3dB of the original signal is tapped, which is approximately 50% - the amount of the remaining original signal is approximately equal to the amount that is tapped and then reintroduced. For a smaller tap percentage, an optical amplifier can be used to boost the small amount of tap signal to the same strength of the pass-through signal. Overall, the most devastating phase shift is when the two signals are 180° out of phase, which intuitively makes sense. It is hard for the attacker to determine exactly what fiber delay constitutes a 180 degree phase shift, but all that has to be done is to either modulate the delay fiber length (as in using a stretcher) or an electronic phase shifter that can be varied over 2π phase shifts, creating deep fades often enough to completely disrupt network operations.

Although repeat-back jamming seems benign in appearance, the effects of the attack are readily seen across many network layers. Even without seeing the intrusion of the malicious user into the network, the introduction of a moderate to extreme phase shift has very visible effects –

---

<sup>1</sup> Although correct in magnitude, the quadrant in which the phase is located depends upon the originating quadrants of the original and delayed signal phases.



**Figure 2.6 - Power vs Tap Strength in Repeat-Back Jamming Attack.** Graph shows amount of original signal power lost according to the amount of power tapped out and reintroduced, for a range of different phase shift amounts

the phase shift results in a decrease in signal power that is characterized above. Similar to the effects of a tapping attack, this decrease in signal power can lead to incorrectly received messages that cannot be recovered in the data-link layer. This can lead to routing issues in the network layer and trigger a response in the transport layer after an excessive amount of retransmission requests, once again amplifying the link layer problem and substantially reducing the overall transmission rate (by as much as 20dB).

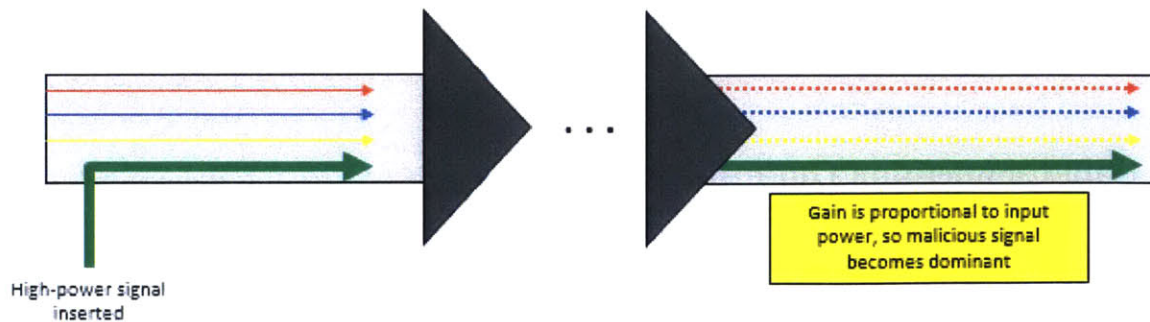
## 2.5 Gain Competition/Out-of-Band Jamming

In a gain competition attack, also known as out-of-band jamming, a malicious user exploits the physical properties of an EDFA amplifier to degrade the performance of the overall

channel. To do this, an attacker gains access to a single wavelength channel and injects a high-powered signal into the stream, as illustrated in Figure 2.7.

An EDFA amplifier works by allotting its amplification power proportionally to the incoming signals within its wavelength range, and thus when a sudden, significantly higher-power signal is introduced while the other legitimate signals stay at the same magnitude, it is allotted a much higher proportion of the power, and thus the power of all other legitimate signals is reduced. This can lead to attenuation of the legitimate signals, and thus a higher bit error rate and service degradation. With a single gain competition attack, a malicious user can affect many wavelengths at once. The disproportionate power across different wavelengths will also propagate if allowed to go unchecked, causing greater signal deterioration as it passes through more amplifiers, each of which causes a more dramatic gain competition attack.

Similar to previous attacks covered, the damage from gain competition essentially comes from diminished signal power. The difference, however, is that in the case of gain competition, the signal itself is not tampered with; instead, the signal is weakened as it is robbed of the full amplification it requires to continue to efficiently propagate. As the signal becomes weaker, it runs into the same issues that an attenuated signal would face – messages possibly being

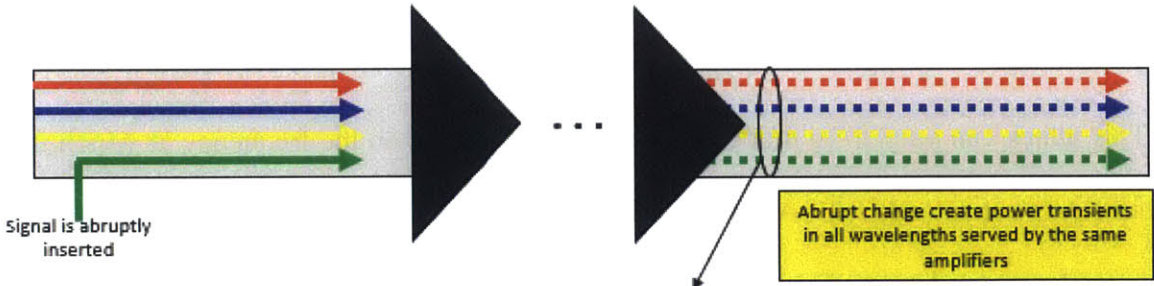


**Figure 2.7 - Gain Competition Attack.** In this example, the high-powered green signal enters the EDFA amplifier, leading to disproportional power allotment and weakening the output power of the legitimate signals.

received incorrectly and undecodable by the data link layer, resulting in routing issues and triggering of window-closing of the transport layer protocol. Gain competition affects many wavelengths at once, as every lightpath but the offending one suffers, and thus network throttling and diminished performance can occur very quickly, as many lightpaths are generating retransmission requests and causing the TCP windows to rapidly decrease and reduce throughput to essentially one packet per roundtrip time. From the end-user perspective, it will appear as if something is wrong with the channel itself, as transmission rates are suddenly throttled back drastically and virtually all lightpaths are affected.

### 2.6 Power Transients

During benign system operation, small power spikes can occur as lightpaths in a channel abruptly become active. This momentary pulse, if unchecked, will unfortunately corrupt any data frame that is also being transmitted at that time, which could cause the need for retransmission of that frame [29]. Figure 2.8 illustrates this phenomenon, which outwardly appears very similar to gain competition. A key difference is that power transients are very abrupt and are only momentarily present, whereas in gain competition, the offending signal is free to persist as long as desired.



**Figure 2.8 - Attack via Power Transients.** In this example, the green signal injects an abrupt power transient, caused by turn-on of the lightpath, resulting in the data frames of all other lightpaths to be corrupted.

Figure 2.9(a) is a graphical representation of the physical event of a wavelength lightpath being activated, or “added,” and subsequently “removed” in the form of a step function. The momentary spike in power when the lightpath is added is referred to as the overshoot, and the sudden, dramatic lapse in signal power as the lightpath is removed is referred to as the undershoot. The amount of overshoot (and conversely, the undershoot) is a function of the actual process of activating the lightpath, as well. Figure 2.9(b) shows this relationship between the overshoot amount and the switching time, which is the time it takes to switch the lightpath on – the faster the switching time, the greater the overshoot. For a legitimate user, the proper technique to use during turn-on to avoid affecting the other users is called adiabatic switching, which uses a gradual switching process to induce turn-on slowly, over a period of ~5 milliseconds, instead of abruptly. However, an attacker would not be as cooperative and can inflict the maximum damage by turning on as a step function or even as close to an impulse as possible.

The presence of gentle power transients due to adiabatic switching are expected during normal system operation and are not indicative of any sort of attack, but the injection of malicious, large power transients can have a devastating effect on network performance. An attacker may force power transients to occur through access to a physical lightpath, turning on and off as desired. Thus, the attacker can exploit power transients to corrupt frames at will on other lightpaths and at multiple times, leading to issues in higher layers of the network.

This attack can vary from moderate to severe depending on the frequency at which these power transients are introduced. Although originating in the physical layer, this attack hits the data-link and upper layers hard as it damages all simultaneously transmitted frames, necessitating retransmission if they are beyond recovery. The affected frames also create



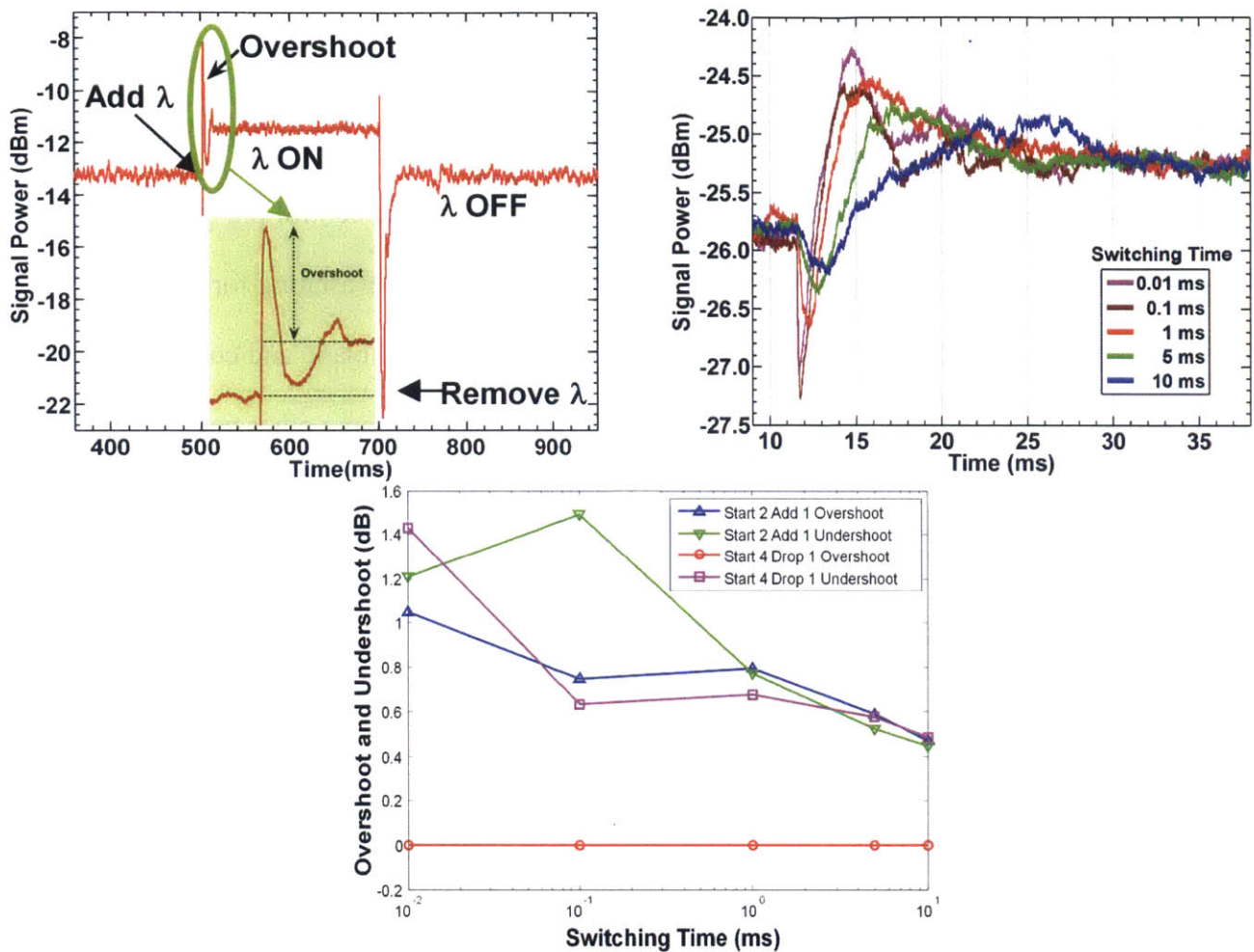


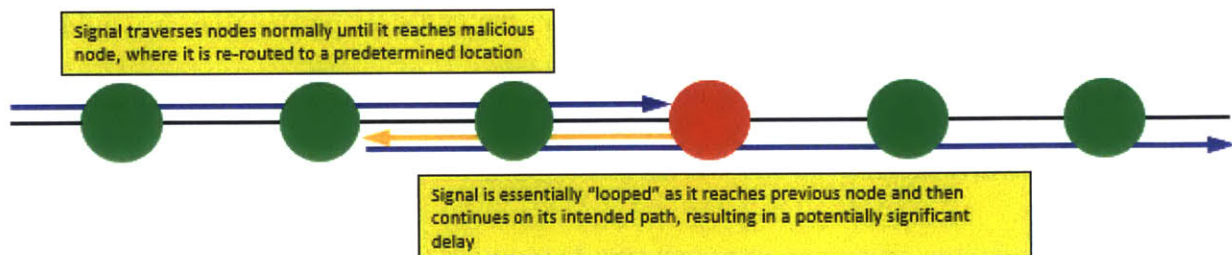
Figure 2.9 - Graphs Depicting Effects of Power Transients [28]: (a) depicts signal power as lightpath is activated/deactivated, (b) shows the effect of a power transient as a function of varying adiabatic switching times, (c) overshoot and undershoot of various lightpath configurations

network layer routing issues if they are not discernable, and the rapid influx of retransmission requests could prompt the transport layer protocol to decrease the window size, potentially severely curbing network transmission capabilities, and even causing the network to oscillate. Due to the momentary nature of these transients, from the end user perspective, it would just appear as if packets were arbitrarily being corrupted and dropped, and network performance was consequently diminished.

## 2.7 Control Plane/Looping Attack

In an all-optical network, the control plane functions as the entity which manages and directs all the network devices in the area. Thus, network settings and configurations and the establishment of connections for traffic are ultimately regulated by the control plane. It is clear, then, to see how a malicious user having access to this plane can be devastating for the network. In the “looping” attack, this malicious user gains access to the control plane and configures it to unnecessarily reroute an incoming signal to a previous point or even some other point not in the original lightpath before continuing forward to its intended destination, as shown in Figure 2.10.

If the signal is not able to continue on the same path, due to being placed in an infinite loop or simply discarded, it results in a complete denial of service as the signal becomes trapped or lost. Even if the signal is able to get out of the loop and continue on the designated lightpath, a new set of issues may arise due to the potentially significant delay and extra amplified spontaneous emission (ASE) noise incurred – reception issues could be caused by the excessive travel time, resulting in dropped or delayed packets. This attack is especially difficult to handle, as it looks like legitimate network operation with the control plane handling scheduling and traffic flows, or even appearing to be diagnostics running during normal network operation. Another critical aspect of this attack is that the control plane can, and often does, oversee the entire network, meaning that a nefarious user only needs to gain access at a single point to inflict



**Figure 2.10 - Control Plane Attack.** In this example, the routing of the red node is modified to redirect to a previous point, deviating from its intended path.

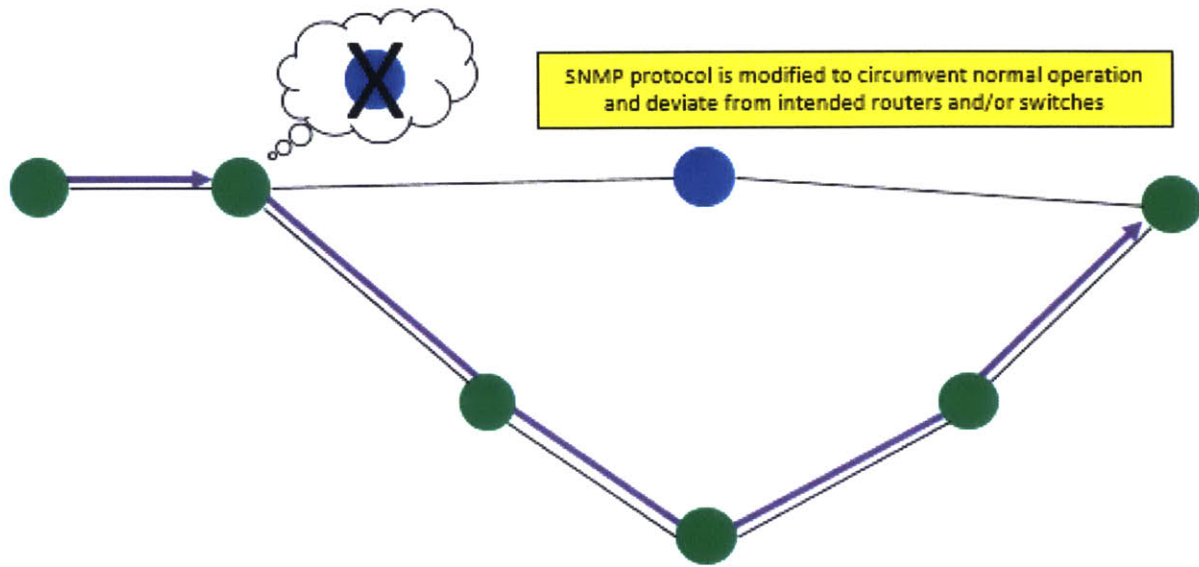
damage anywhere within the network itself. Localization, thus, is a daunting task, with no real clues as to the true origin point of the attack. It is possible that the detection scheme must be done at the cyber level where the control plane is being attacked electronically.

A control plane attack originates at the network management and control layer, but its effects are able to trickle down significantly into lower layers. Looping, for instance, interferes with established routing in the network, generating paths that are not efficient or possibly not even valid. Looping and other significant delays caused by this attack will also trigger a response by the transport layer protocol, causing it to perceive congestion in the network and decrease the TCP window size to preserve communication. This, of course, exacerbates the problem, causing transmission to be throttled in an otherwise healthy network.

## **2.8 Simple Network Management Protocol (SNMP) Modification**

The Simple Network Management Protocol (SNMP) serves as a common management protocol for network devices (i.e.: status updates, configuration data, etc) [17]. By hacking into and tampering with the SNMP protocol, a malicious user can circumvent normal network operation and cause data transmission to deviate from intended routes via switches and other devices under SNMP control. Figure 2.11 illustrates one such attack via SNMP modification.

The attacker thus has the ability to generate false status updates and consequently modify routes, even making some legitimate routes invalid. The result could be anything from significant time delays to outright denial of service. There is no glaring outside indication that SNMP has been modified or abused, so this type of attack is very challenging to detect. Newer version of SNMP, such as SNMPv3, attempt to fill in some of the security gaps of its predecessors through additional protection measures such as authentication [17], but most



**Figure 2.11 - Attack via SNMP Modification.** In this example, the status of the blue node is falsely updated to unavailable via SNMP, resulting in suboptimal network performance.

existing networks continue to use older versions of SNMP, as there is not much perceived push to make the potentially costly and cumbersome switch.

SNMP modification attack is a particular subset of a control plane attack, with network management being manipulated through this application layer-based protocol. Through this application layer access, an attacker can trigger the same routing and transport layer issues as in the aforementioned control plane layer attack through the propagation of false SNMP information. It may not be as fast as a control plane attack due to this required processing and subsequent propagation time, but the potential for inflicted damage on the network is still great.

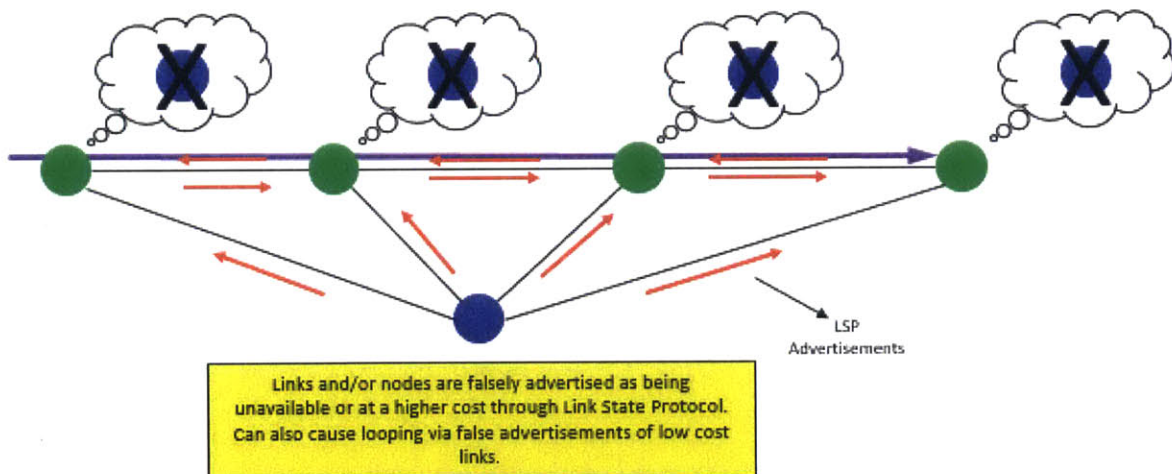
## 2.9 Link State Protocol (LSP) False Advertising

The Link State Protocol (LSP) is an active network routing protocol that relies on nodes propagating their and others' statuses in order to give every node an idea of what the network looks like and which routes are available and efficient. By accessing and tampering with the

LSP, a malicious user can generate and subsequently propagate false status updates, which are trusted by the other benign nodes. For example, an attacker may falsely claim that a node is down or a route invalid, leading to delays and possible congestion. It can also advertise a superior-performing node, causing routing to that compromised node for any of the attacks noted above. In the example in Figure 2.12, LSP false advertising has lead the nodes adjacent to the blue node to believe that it is no longer viable for routing purposes, even though it is operating normally.

Conversely, the attack could be designed to claim that an invalid route is actually valid, leading to packet loss and denial of service. Not only does this type of attack create congestion and impede communication, but it also diverts valuable resources as the network tries to alleviate the situation.

Although originating in the network layer, this attack is very similar in operation to an attack via SNMP modification. The false information in this case is propagated through the link state protocol, and results in the same triggering of network and transport layer responses.



**Figure 2.12 - Attack via LSP False Advertising.** In this example, the LSP is modified to generate and propagate false unavailability advertisements for the blue node, leading to suboptimal network performance.

## 2.10 Summary for Chapter 2

From the attack descriptions, it is apparent that these attacks have far-reaching effects that transcend the attack's origin layer. Table 2.2, below, outlines some of the common issues that arise within the different layers of the network due to attacks like those described above. Table 2.3 lists the originating layer for each of these attacks and uses the classification system from Table 2.2 to illustrate how far-reaching the effects of these attacks actually are. The attack effects in Table 2.2 are classified by their origin layer (the layer number is found in parentheses in the top-most row of the table) and by the corresponding letter in the left-most column of the table. An effect of signal attenuation, thus, is classified as 1B. Table 2.3 utilizes this classification system to make it easier to compare the multilayer effects of each attack.

The fact that attacks like these span several layers is often overlooked in in attack defense analysis, resulting in security solutions that only partially solve the issues arising from these attacks. An effective security solution needs to take a multi-layer approach to the problem in order to best protect the network. The following chapter expands upon these attacks, using their properties to determine the best way to detect and sense them, as well as localize the attacks within the network and mitigate the damage caused.

	<b>Physical (1)</b>	<b>Data-Link (2)</b>	<b>Network (3)</b>	<b>Transport (4)</b>	<b>Application (7)</b>	<b>Network Management &amp; Control (N)</b>
<b>A</b>	Total loss of fiber medium	Incorrectly received messages requiring retransmission	Indecipherable messages creating routing issues	Triggering of TCP window closure	Protocol operation deviation, less efficient	Deviation from normal, efficient operation
<b>B</b>	Signal attenuation		Messages routed incorrectly, potentially lost			
<b>C</b>	Crosstalk occurs					
<b>D</b>	Destructive interference					

**Table 2.2 - Common Issues Across Network Layers. Common results of network attacks, categorized by layer (noted in parentheses) are presented, with identifying letter designators in the left-hand column.**

<b>Attacks</b>		<b>Physical</b>	<b>Data-Link</b>	<b>Network</b>	<b>Transport</b>	<b>Application</b>	<b>Network Management &amp; Control</b>
Cutting/Bending/Tapping	<i>Origin</i>	Cutting or bending of the fiber					
	<i>Effects</i>	1A/1B (multiple)	2A	3A	4A		
Gain Competition	<i>Origin</i>	Insertion of high-powered signal					
	<i>Effects</i>	1B (multiple)	2A	3A	4A		
Power Transients	<i>Origin</i>	Maliciously generated power transients					
	<i>Effects</i>	1B (multiple)	2A	3A	4A		
Out-of-Band Crosstalk	<i>Origin</i>	High-powered signal insertion					
	<i>Effects</i>	1C	2A	3A	4A		
In-Band Crosstalk	<i>Origin</i>	High-powered signal insertion					
	<i>Effects</i>	1C	2A	3A	4A		
In-Band Crosstalk - Eavesdropping	<i>Origin</i>	Exploitation of empty channel					
	<i>Effects</i>	1B, 1C	2A	3A	4A		
Repeat-Back Jamming	<i>Origin</i>	Tapping and reinsertion of delayed signal portion					
	<i>Effects</i>	1D	2A	3A	4A		
Control Plane Attack	<i>Origin</i>						Control plane exploited
	<i>Effects</i>			3B	4A		NA
SNMP Modification	<i>Origin</i>					SNMP exploited	
	<i>Effects</i>			3B	4A	7A	NA
LSP False Advertising	<i>Origin</i>			LSP exploited			
	<i>Effects</i>			3B	4A		NA

**Table 2.3 - Attack Effects by Layer.** The table lists the originating layer for each attack, as well as the effects experienced across the various network layers as a result. Table relies on common network issues experienced as listed in Table 2.2.



# Chapter 3

## Sensing, Detection, Localization, & Mitigation

With a working knowledge of what the outlined attacks are, this chapter focuses on what can be done to prevent them from bringing down a network. The key to an effective security solution against any attack is being able to sense its effects and detect its presence, localizing it to pinpoint where the attack is originating from, and mitigating the damage that it can inflict while subsequently eliminating, or at least isolating, the threat.

While none of these attacks are fully addressed, and methods for mitigation fully developed, we present the current best practices for combating these attacks, as well as an idea of what remaining vulnerabilities exist that could still be exploited.

### 3.1 Cutting/Bending/Tapping Fibers

#### *Sensing and Detection Capabilities*

##### **i. *Power Level Monitoring***

Although an attack that outright severs the fiber would be easy to identify, lesser symptoms of an attack are more difficult to identify. With power level monitoring implemented in the network as a diagnostic tool, it is possible to determine if a significant portion (above a user-specified threshold) of light in a fiber or from the channel is being radiated or dissipated through either bending or tapping schemes. Power level monitoring can be performed by a variety of devices, including power meters, optical loss test sets

(OLTSs), and optical time domain reflectometry (OTDR) [10], although we will discuss OTDR as a separate entity.

Depending upon the resolution of the device being used, which can be as high as 0.1 dB [10], even small amounts of power loss could be detected and configured to trigger an alarm that would quickly alert a network manager to the fact that an anomaly is present and thus facilitate quick action against it. The range of a power level monitoring tool is dependent upon its dynamic range, or the range from its maximum input power to its minimum readable power [12]. As the light propagates, natural fiber and component attenuation will occur, so the total distance that can be accurately covered by a power level monitoring device is determined by

$$d = \frac{h * c * v}{\lambda * (1 - P_{loss}) * 10^{(P_o - P_{min} - 30)/10}}, \quad (3.1)$$

where  $h$  is Planck's constant, equivalent to  $6.626 \times 10^{-34}$  J·s,  $c$  is the speed of light at approximately  $3.0 \times 10^8$  m/s,  $v$  is the speed of the light propagating through the fiber at approximately  $2.0 \times 10^8$  m/s,  $\lambda$  is the wavelength of the light in meters, and  $P_o$ ,  $P_{loss}$ , and  $P_{min}$  are the initial input power, attenuation and component loss across the length of the fiber, and the minimum sensitivity of the device in dBm, respectfully. The derivation for (3.1) can be found in Appendix A. It is important to note that power level monitoring is only useful as a detection tool when it has a benign reference point – an initial power measurement taken during an attack that has already diminished power will not register that it is abnormal unless the power level during normal network operation is measured or known. This is a well-known technique that is widely available as a product.

## ii. *Intrusion Detection via Optical Time Domain Reflectometry (OTDR)*

Optical Time Domain Reflectometry (OTDR) is a sensing tool that relies on the transmission and reflection of pulse signals through a channel to determine the status of the fiber. OTDR devices are extremely useful in determining and giving the location of fiber breaks, significant bends, and overall signal attenuation due to tapping. The main vulnerability of OTDR is that it is limited in its capacity to recognize more subtle changes, as it examines average channel phenomena over time [30]. The effectiveness of OTDR detection, then, is a function of the device sensitivity, with more sensitive equipment being more costly.

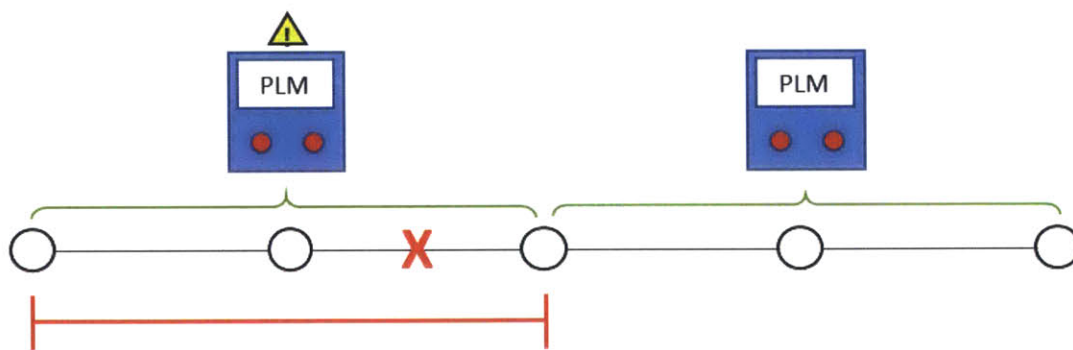
An OTDR device would be extremely useful in determining where and when a bending, tapping, or cutting attack is taking place, given that these attacks are very abrupt in nature, and thus difficult to conceal from being detected via this method. The observable distance using OTDR is also dependent upon the dynamic range of the device [12], and using Equation 3.1, the maximum detection distance (range of the commercial device) for the device can also be calculated. The resolution of the device, however, can range anywhere from approximately 4 centimeters to 40 meters, depending upon the device and configuration by the user [12].

### ***Localization***

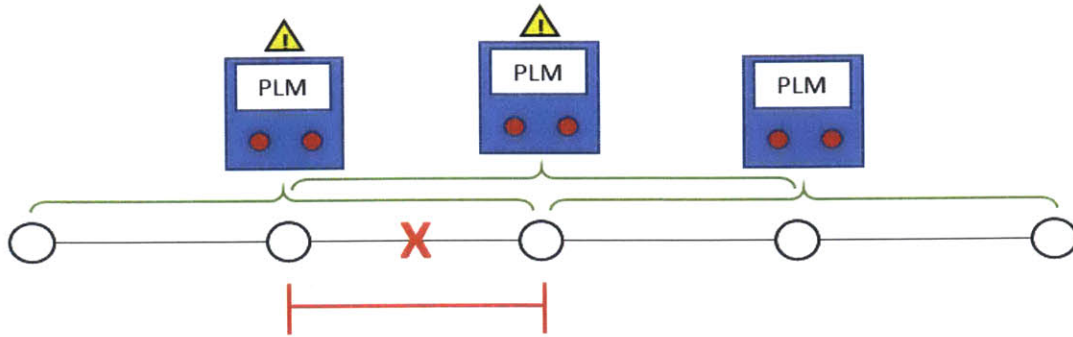
While detection may be relatively easy in a full cutting attack, localization is not necessarily trivial, rivaling that of a bending or tapping attack. While the effects of any one of these attacks can propagate, the origin of the attack is located on a single link or switch in the network. The key to stopping this type of attack, thus, is finding and shutting off that point of access. Assuming that the attacker has not yet gained physical access to the lightpaths in the network, it

would be relatively simple to identify their initial entry location via OTDR, as the possibility of scraping away the cladding or bending the fiber at a rate too gradual for detection is highly improbable in a practical setting. The issue then becomes the cost of inserting enough OTDR devices to cover the entire span of the network, leaving no gaps in coverage; as the size of the network increases, this endeavor becomes more and more costly.

Assuming that an attacker already has physical access to the lightpaths within the network, localization becomes slightly more difficult. The next line of defense is power level monitoring, in which detection is possible for a drop in signal power within the detectable range of the device. This localization method, thus, is limited to the range in which the power level monitoring device covers, with the maximum coverage area previously defined in Equation 3.1. Unlike OTDR, power level monitoring devices could benefit from introducing redundancy in the monitoring scheme, as they do not have the same precision with localization as OTDR does. Figures 3.1 and 3.2 show how detection redundancy in power level monitoring would be effective in decreasing the localization range from the maximum measurement distance of the device.



**Figure 3.1 - Power Level Monitoring Localization without Redundancy. With a device measurement range of 2 links, the attack (denoted by a red X) can be localized to an area of 2 links.**



**Figure 3.2 - Power Level Monitoring Localization with Redundancy.** The device measurement range is 2 links, but with overlapping coverage areas, the effective resolution is 1 link. Thus, the attack (denoted by a red X) can be localized to a single link.

In Figure 3.1, the maximum effective sensing range of the devices is assumed to be two links, and the devices are placed in intervals of their maximum sensing range, minimizing the number of devices used. When the second link in the chain is disabled, however, the device can only conclude that an issue has occurred within its maximum sensing range (i.e.: it has a localization resolution of 2 links), so it is not clear which of the two links it is monitoring has gone down. In Figure 3.2, redundancy is introduced to shorten the localization resolution of monitoring network to one link through overlapping measurement areas. Thus, when the second link goes down in this scenario, it can be concluded that the issue is within the second link specifically. This method assumes that only one fault will occur within the maximum sensing range of a device at a time. To calculate the total number of devices needed to achieve a specified localization resolution, the following equation can be used.

$$M_{total} = \left\lceil \frac{n \left( 2 - \frac{r}{d} \right)}{d} \right\rceil \quad (3.2)$$

In the above equation,  $n$  represents the total number of links under observation,  $r$  is the desired localization resolution, and  $d$  is the maximum sensing distance of the devices.

Using more than the minimum amount of devices required could be beneficial in confirming and pinpointing where issues occur, but it would also increase the overall network cost and the management overhead as a result of synthesizing the additional information, so the practical and economical needs of the network must be taken into consideration. The implementation of a monitoring system including these components, as well as methods for finding and diagnosing faults, is discussed at length in Chapter 4.

### ***Possible Attack Mitigation***

#### ***i. Physical Security – Limiting Access***

Outright prevention of attacks such as these is most easily ascertained through the limitation of physical access to optical devices and fibers by those who are not authorized by the managing network entity. While implementation of stringent physical security would serve as a deterrent against intruders with ill intent, the realistic application of such measures may not be very practical. One of the great advantages of using all-optical networks is their ability to span very long distances, but with this benefit comes the drawback of having to physically secure the network across those distances. Thus, an absolute, effective level of physical security may be very difficult, if not impossible, to maintain across the span of all fibers and devices in the network.

#### ***ii. Physical Hardening – Fiber Construction***

In the same vein as physical security, physical hardening of the fibers themselves would also serve as a deterrent against intrusion of the network, as it would make it more difficult for attackers to cut, splice, or bend the fiber enough to significantly tap or

diminish the signals. A typical fiber consists of a core where the light is propagated, cladding of a lower refractive index to facilitate total internal reflection and help confine the light to the core, and a buffer layer and external jacket to isolate and protect the internal components [11]. Although the core and cladding are more constrained in their abilities to be physically hardened due to transmission constraints, the buffer and jacket layers can be changed to materials that are more difficult to penetrate or bend, making the aforementioned attacks much more difficult to accomplish. This hardening, thus, of the construction of the fiber itself can significantly impact the ease in which a nefarious user can affect the light inside.

One solution would be the use of bend-insensitive fibers, which increase the resiliency of a fiber against bending attacks through the incorporation of a layer of glass with a lower refraction index around the core, allowing light that would otherwise be radiated out of the core to be reflected back in [19]. The bend-insensitive design can allow a single mode fiber to be bent to a radius as small as 7.5mm with insignificant loss, making them up to 400% more robust than a standard single mode fiber [20]. Research has shown that these bend-insensitive fibers are also highly compatible with single mode and some multimode fibers, allowing them to be incorporated into existing systems with relative ease [19]. The use of bend-insensitive fibers, thus, would serve as an effective mitigation option that can be put into place with relative ease and relatively low cost, while reaping many practical benefits.

In real-world applications, fibers are oftentimes bundled together within a cable, so physical hardening of this cable can be equally as important as the hardening of the fibers, themselves. Cables exist in the market today that incorporate measures of

protection against penetration and tampering, including cables with an armored layer (usually some type of metal or occasionally hard plastic) [21], although the construction of the cable itself is often a factor of its intended operating environment and subsequent performance requirements.

Physical hardening as a mitigation solution is an excellent idea to implement in new optical networks that have not yet been constructed, but its usefulness can severely decrease when applied to existing optical networks with fibers and devices already established and in place that cannot simply integrate heterogeneous components. In such a scenario, implementing physical hardening across the network would require the replacement of all current fibers, which translates to high costs and labor time.

**iii. *M-fold Spatial Diversity***

Introducing redundancy is an effective method of mitigation, given that the redundant paths are not collocated, but rather in entirely separate physical locations. From a purely logical outlook, it is much more difficult for an attacker to corrupt the same link in multiple locations than it would be with no redundancy, meaning that a viable path would still exist even if one or several links were under attack on the same path. By introducing not just redundancy, but spatial diversity, the level of difficulty it takes for an attacker to fully shut down a path would increase by a factor of  $M$  with every additional fold introduced, as compared to normal network operation.

The key thought behind this form of mitigation is that the paths are not just diverse, but physically separated, housed in completely separate cables and wired through different geographical locations (as in different risk groups). Often in existing networks



with redundancy, the disjoint paths traverse the same cable bundles and/or conduits, severely decreasing the work an attacker has to do to render the redundancy ineffective. For this reason, the spatial diversity aspect is critical, as it radically reduces the probability that an attacker can disable the disjoint paths during the same infiltration.

Naturally, the drawback of introducing several layers of spatial diversity is significant cost increases, but as with all the mitigation methods mentioned, the costs must be compared to the additional security provided, and a balance must be struck which optimizes both for the demands of the network [23]. Additional paths created to maintain redundancy will also lead to an increased usage of network resources, and so there is also a network bandwidth utilization cost that must be considered. The introduction of spatial diversity also requires a significant increase in the control and management efforts, as the network manager must be aware of the complete physical layout of the network and all viable routes in order to maintain physical diversity within redundancy.

### ***Remaining Vulnerabilities***

#### ***i. Establishment of Reference Measurements***

If using solely power level monitoring to detect an attack, then there must be a benign point of reference to compare power gains and losses to in order to correctly interpret system behavior. If the initial power measurement is made while an attack that reduces signal power is already underway, then the point of reference is incorrect, and the attack may continue on undetected. A return to benign system operation may even trigger an alarm in that it is perceived as abnormal compared to the inaccurate basis measurements.

If a known and verified typical operational power level measurement range does not exist, then a method should be developed to extrapolate the information based on prior operational data to confirm that the current measurements taken as a point of reference are correct and not already affected by any adverse action or occurrence. This, however, may not always be possible. Nonetheless, the final detection scheme is the quality of the lightpath as compared to what is expected. One can assume the network is under attack if the quality of service is below expected levels, and move on to the localization phase to pinpoint the attack or failure point. Thus, attack localization and fault localization are basically the same functions.

## **3.2 Repeat-Back Jamming**

### ***Sensing and Detection Capabilities***

#### **i. *Power Level Monitoring***

From the analysis in Chapter 2, it is apparent that repeat-back jamming can inflict moderate to severe signal attenuation during an attack. Based on this result, power level monitoring is a potential tool for the detection of an attack, but its effectiveness could be diminished if employing a power-measuring device over the entire fiber instead of taking wavelength measurements. As Figure 2.6 shows, at low phase shifts and/or tapping magnitudes, the effect is very slight, meaning it could go undetected by a power monitoring device, particularly if the attack is only against a single wavelength or a small set of wavelengths within a large group. Thus, power level monitoring would be most effective if it was performed on a per-wavelength basis, although it is still possible to use aggregate power level monitoring to sense the attack.

**ii. *Intrusion Detection***

A key component of repeat-back jamming is the ability of the attacker to tap into a legitimate channel and signal. Thus, an early-stage detection tool would be to implement an effective form of intrusion detection in the system such as OTDR, as described in Section 3.1, as repeat-back jamming requires tapping. With OTDR in place over a fiber, the initial entrance of a malicious tap could almost immediately be flagged, and an appropriate response triggered.

**iii. *Phase Detection***

Arguably the most powerful detection tool available against repeat-back jamming is phase detection, as it is an extremely difficult task to try to match the phase of an original signal with that of a delayed and reintroduced signal.

The ability to detect minute phase changes relies on the sensitivity of the receiver device. The minimum phase change that can be detected is found via the following formula, the derivation of which can be found in Appendix A.

$$\Delta\theta_{min} \geq \frac{2\pi}{\tau_D} \left[ \frac{L * n}{c} - \left( 1 - \frac{1}{L_i} \right) \right] \quad (3.3)$$

In the above equation,  $L$  represents the length of the optical cavity in meters,  $n$  is the refractive index of the cladding material,  $L_i$  is the loss coefficient, and  $\tau_D$  represents the time the receiver can detect change in, measured in seconds. Thus, holding all other variables as a constant part of the system, the slower the receiver detection time, the smaller amount of change in phase shift can be detected. Phase detection can be performed via a variety of methods, such as through an electronic phase detector or

optical heterodyne dual detection, as described in [31]. Typical phase shifts of  $\sim 1$  degree can be detected. If the repeat-back jammer is sweeping its phase shift over  $2\pi$ , then surely the jamming signal can be detected.

#### iv. *Tapping for Diagnostics*

Another method that may be employed for detection is a set-aside tapping channel controlled by a network management entity, used solely for diagnostic purposes. This tap would take as low as -20dB of the signal (tapped right after a boost amplifier) and amplify it in order to get a reasonably accurate representation of the full signal. This diagnostic signal could be compared to the original signal at a later point to check for phase or power inconsistencies, thus alerting the monitor to suspicious activity within the channel. The signal itself can also be demodulated to see if the quality of the link is still acceptable.

#### *Localization*

For repeat-back jamming, the localization methods relying on power-level monitoring and OTDR have the same limitations as previously discussed in Section 3.1. There are, however, additional means of detecting and localizing an attack for repeat-back jamming, such as phase detection. The distance over which phase detection is effective is a function of the coherence time of the wave. The distance over which this coherence time is valid is referred to as the coherence length, and is calculated by the following equation, as described by [32].

$$L = \frac{2\lambda^2 \ln 2}{\pi n \Delta\lambda} \quad (3.4)$$

In the above equation,  $\Delta\lambda$  represents the spectral width of the source, while  $n$  is the refractive index of the medium. Thus, the coherence length  $L$  is the maximum detectable length of the phase detection method, meaning that if an attack is identified via phase detection, the area where the attack originated could be confined to a section of the network as small as  $L$ . Localization via phase detection is then limited to the effective resolution of the devices put into the network. As with the previous methods, the amount of devices put in place is dependent upon the allowable budget and acceptable protection level required of the network.

### ***Possible Attack Mitigation***

#### ***i. Access Denial/Service Shutdown***

One method to ensure that an attacker can no longer do damage on a network link is to completely shut down the link once the malicious activity has been detected and localized. This would prevent the attacker from gaining access through that link and force them to seek access elsewhere via a new access point, and with the previously discussed challenges in creating a new tapping point without being detected, this could make a successful attack much harder for a malicious attacker. If other access points for an attack exist already, then the new access points need to be shut down, but the memory of the old access points must be retained to prevent the attacker returning to a previous attack point.

The effectiveness of this mitigation tactic is shutting down the least amount of healthy network while ensuring that the threat is neutralized. Thus, localization becomes critical in determining which areas are impacted and should be quarantined, as well as how big this area should be. More analysis of the network quarantining scheme can be found in Chapter 4.

## ***Remaining Vulnerabilities***

As seen in the analysis of the attack's effects in Chapter 2, repeat-back jamming is most dangerous when the phase shift induced is closest to 180 degrees. Such a major phase shift, however, is relatively noticeable and thus easier to identify. For an effective, deceptive attack, a malicious user would want to inflict the most damage while still remaining under the radar in terms of detectability. With the above detection mechanisms, the only significant method for an attacker to go undetected would be finding a way to sync up the delayed signal's phase with that of the original signal in order to hide their presence, or at least get as close to the phase of the original signal as possible. Given the complex nature of an optical signal, it would be immensely challenging to try to sync the phases of the two signals, although not impossible. This will require the attacker to tap and perform measurements at the reintroduction point of the delayed signal.

### ***i. "Phase Sweeping"***

A special case of a repeat-back jamming attack that an attacker could employ to work around the proposed detection techniques and use to hinder successful transmission is the incorporation of a "phase sweep" into the repeat-back jamming attack. With this method, the malicious user would not use a static delay for the reintroduced signal, but instead would sequentially change the delay or phase so that the phase varied at a predetermined rate, meaning that for at least a portion of the total attack time, the phase of the attacking signal and that of the original signal would approximately match, making the attacker virtually invisible during that span of time.

This phase sweep could be performed through physical stretching of the tapping medium, thus increasing or otherwise altering the length of the path and varying the delay. The phase sweep could also be created through the use of an electronic phase variation device, which would have the ability to alter the phase through a 360 degree range. Continually varying the phase can create an oscillating wave of signal attenuation, which would be harder to diagnose than a static attenuation level, but still possible if continuous monitoring is performed. This, however, will make time sharing of diagnostic equipment to monitor multiple lightpaths logistically complicated, and may lead to having to invest in many more monitors than if the phase is static.

**ii. *Amplifying Tapped Signal***

A method of disguising the attack is through the amplification of a tapped signal. In this scheme, a signal is tapped as per a typical repeat-back jamming attack, but only a very small portion that would be very difficult to detect. This miniscule tapped signal is then amplified to a much stronger signal, and then reintroduced into the channel at a point far from where it was tapped. With this, an attacker can disguise the true origin point of the attack, while also inflicting damage in a different area of the network by reinserting the amplified, delayed signal. The resulting damage would still be detectable if it resulted in a significant signal attenuation, but the point of attack origin could be better hidden and more difficult to trace, given that the attacker is able to thwart whatever mitigation techniques are put into place against outright tapping attacks. This method would also make it harder to diagnose the attack as repeat-back jamming instead of some other type of attack inducing signal attenuation, which could lead to an incorrect mitigation response.

### **3.3 Out-of-Band Crosstalk**

#### ***Sensing and Detection Capabilities***

##### **i. *Power Level Monitoring***

High signal power can serve as a catalyst for crosstalk to occur, so monitoring the network power levels can be a useful sensing tool, although it would be far more beneficial to use fine-grain power monitoring in this instance. Power level monitoring does have significant limitations, however, as crosstalk can occur without significantly higher signal powers present, and thus power level monitoring would be ineffective.

##### **ii. *Bit Error Rate Monitoring***

The inherent nature of crosstalk leads to affected packets being corrupted, and these errors can be observed and compared to an established or verified point of reference for the uncorrected bit error rate (BER) for normal system operation. Then, a significant rise in the BER can be indicative of some form of attack, especially if the BER is seen to change in a small amount of time (such as over one second), although which specific attack is occurring will not be discernable from this method alone.

##### **iii. *Waveform Analysis***

The raw signal waveform can be digitized, as in a coherent receiver. The sampled waveform over multiple bits can be averaged (decision directed by the error-corrected output) to examine the fidelity of the signal. The averaged waveform can reveal the presence of a repeat-back jammer adding its signal at a shifted phase, as well. This is a very sensitive test used only if the BER test does not reveal any issues.



## ***Localization***

Crosstalk can also easily be propagated and its effects multiplied as it traverses the network, meaning that it could originate in one location at an undetectable level and trigger an alarm somewhere else. Many proposed methods of localization for crosstalk are incorporated into routing and wavelength assignment (RWA) designs, which we will discuss in the next section. [2] proposes a method of implementing a monitoring system which relies on power measurements to seek out and localize a crosstalk attack to its originating link, given only one attack occurs on a fiber at a time.

## ***Possible Mitigation Techniques***

### ***i. Routing and Wavelength Assignment (RWA) Schemes***

A routing and wavelength assignment (RWA) problem consists of developing a physical topology and wavelength assignment scheme within certain constraints [4]. Many RWA solutions have been proposed for lessening the effects of a crosstalk attack, such as in [2, 3, 4]. These schemes rely on cleverly configuring the network layout and subsequent traffic routes in order to localize crosstalk and limit how far it can propagate.

RWA solutions have been proven to be very effective against crosstalk, but for an existing network infrastructure, the financial and labor costs of reconfiguring the network to meet specific RWA topologies and routing networks could be very high and impractical to implement.

## **3.4 In-Band Crosstalk**

### ***Sensing and Detection Capabilities***

**i. *Phase Detection***

In an in-band crosstalk attack, a signal is combined with delayed, phase shifted components of itself, similar to in a repeat-back jamming attack. If above the threshold given in (3.3), then we can detect the resultant phase shift of the recombined signal and register that it is atypical and possibly indicative of an attack.

**ii. *Bit Error Rate Monitoring***

Bit error rate monitoring for in-band crosstalk attacks is identical to that of out-of-band crosstalk. While an attack may be registered and flagged as suspicious activity, it is not clear which attack is occurring.

***Localization***

The localization for in-band crosstalk attacks does not significantly differ from that of out-of-band crosstalk attacks, except that there is also the added tool of phase detection, and with it, a localization range that can be found via (3.4) when the minimum number of devices are used to completely monitor the network.

***Possible Mitigation Techniques***

**i. *Routing and Wavelength Assignment (RWA) Schemes***

RWA solutions for in-band crosstalk are identical to those described in Section 3.3, with some solutions even being effective against both in-band and out-of-band crosstalk [4].

## 3.5 Gain Competition/Out-of-Band Jamming

### *Sensing and Detection Capabilities*

#### i. *Power Level Monitoring*

As seen in Figure 2.7, gain competition requires a high-powered malicious signal, and results in attenuation of the legitimate users' signals. Sensing possibilities, thus, can include pinpointing when a signal suddenly greatly increases in strength beyond normal specifications, or when a significant portion of signals suddenly experience a marked decrease in power. Power level monitoring, consequently, is a useful tool in identifying these power fluctuations. For this attack, the power level measurements can be coarse, such as monitoring the total power in a band of wavelengths (not the whole fiber) and picking up on the diminished power of several wavelengths at once, or fine grain, as in per-wavelength, which could also sense and potentially identify the offending signal.

The only caution for using this method of detection is ensuring that there is an adequate buffer between standard operational input power and maximum input power for the device, as a huge signal power increase could fall outside the acceptable range, and could even damage the monitoring tool.

### *Localization*

For a gain competition attack, the best sensing method, and thus the best localization method, is through the use of power level monitoring. Logically, a coarse power level monitoring tool is going to be less costly than a fine-grain device, so if cost is a vital factor in network planning, the type of power-level monitoring method used could also impact the amount of devices in the network, and thus, the localization range. Although using a fine-grain device would be less

economical, it could be more beneficial to network efficiency as it could help to identify which wavelength is causing the gain competition attack, allowing the network administrator to turn off access to that specific wavelength instead of the entire band, mitigating the impact on network performance.

### ***Possible Attack Mitigation***

#### ***i. Automatic Gain Control***

Gain competition attacks can create damage that propagates, which could exacerbate the problem, so damage mitigation is crucial. One key mitigation method is the use of amplifiers with automatic gain control, which monitors power levels for each incoming wavelengths and limits the amount of gain any one wavelength can receive [3]. Thus, gain competition attacks would not be able to incur nearly as much damage, as the highly disproportionate gain allocation would be prevented. The shortcoming of some automatic gain control devices, however, is that they are only able to apply constraints for power deviations within a predetermined interval, meaning that a deviation larger than what it is capable of regulating will still be able to cause gain competition and inflict damage. In addition, they can only adapt to quasi-static power changes, meaning they will be too slow to deal with cross-coupled transient attacks.

Optical Limiting Amplifiers (OLAs) allow for a dynamic range of input power, which deals with the major flaw of static input limits that automatic gain control possesses [3]. OLAs work by first filtering each wavelength, analyzing and comparing the incoming lightpaths and attenuating signals, via a variable optical attenuator (VOA), that lie outside

of the acceptable power range [8]. The device is then able to effectively dynamically equalize the power levels without worrying about preconfigured ranges.

## **ii. *Dynamic Gain Equalizers***

To cope with the limitations of static gain equalization, a more active system is required. As a result, dynamic gain equalization was created to handle changing amplifier loads and balance minor fluctuations in the transmission fiber and the optical amplifier itself [16]. Dynamic gain equalizers (DGEs) work through the use of a feedback loop to monitor and adjust amplifier output per wavelength, equalizing the power output across the lightpaths [16].

Optimal DGE placement in a network would be one device following every 4-6 amplifiers [15]. The span of the amplifier chain in the network, thus, dictates how many DGEs will be required. In this case, using more than the optimal amount of DGEs will not be beneficial, but could actually be detrimental to network performance as it causes the optical signal to noise ratio across the various wavelengths to experience greater variance [15], as well as diminishing the overall signal to noise ratio, reducing the span of the lightpaths.

## ***Remaining Vulnerabilities***

### **i. *Crosstalk Due To Poor Isolation***

As discussed in Section 3.2, a strong signal travelling through an optical device such as a switch can “bleed” over into adjacent signals. A gain competition attack generates the same type of high-powered signal used in a jamming attack. Poor isolation between

channels thus leads to crosstalk occurring, and if the signal is able to leak into neighboring signals before reaching a mitigation device such as a DGE, then there is a strong chance of crosstalk occurring, as channel isolation is usually not perfect, or even marginal, in standard operation.

## 3.6 Power Transients

### *Sensing and Detection Capabilities*

#### i. *Arrival Rate Analysis*

As discussed in Chapter 2, power transients are possible within standard network operation, although relatively infrequently. Based on this knowledge, we are able to model the amount of power transients occurring in the network and analytically determine whether or not what we are experiencing is atypical, revealing the likely presence of an attacker. The arrival rate for benign power transients that can occur during normal system operation is modeled as a Poisson process of a rate  $\lambda$ . Given this rate, either known or determined, it is possible to characterize the system and determine the probability of attack by observing how frequently power transients occur and comparing it to analytical expectations. The probability of a given difference between an observed arrival rate for power transients  $X$  and the expected arrival rate being greater than some value  $\epsilon$  is upper-bounded by the Chebyshev inequality as follows:

$$\Pr\{|X - \lambda| \geq \epsilon\} \leq \frac{\lambda}{\epsilon^2}. \quad (3.5)$$

In the above (3.5), the variance is simplified to  $\lambda$ , as the variance for a Poisson process is equal to its mean. For a generalized, comparative expression, a threshold can be incorporated into Equation 3.4 to yield the following result:

$$Pr\{X \notin [\lambda - \lambda p, \lambda + \lambda p]\} \leq \frac{1}{\lambda p^2}. \quad (3.6)$$

where  $\lambda$  is the known arrival rate, and  $p$  is some fraction of the arrival rate serving as the threshold value. Figure 3.3 illustrates this relationship for a Poisson power transient arrival rate of 50 transients per second<sup>2</sup>.

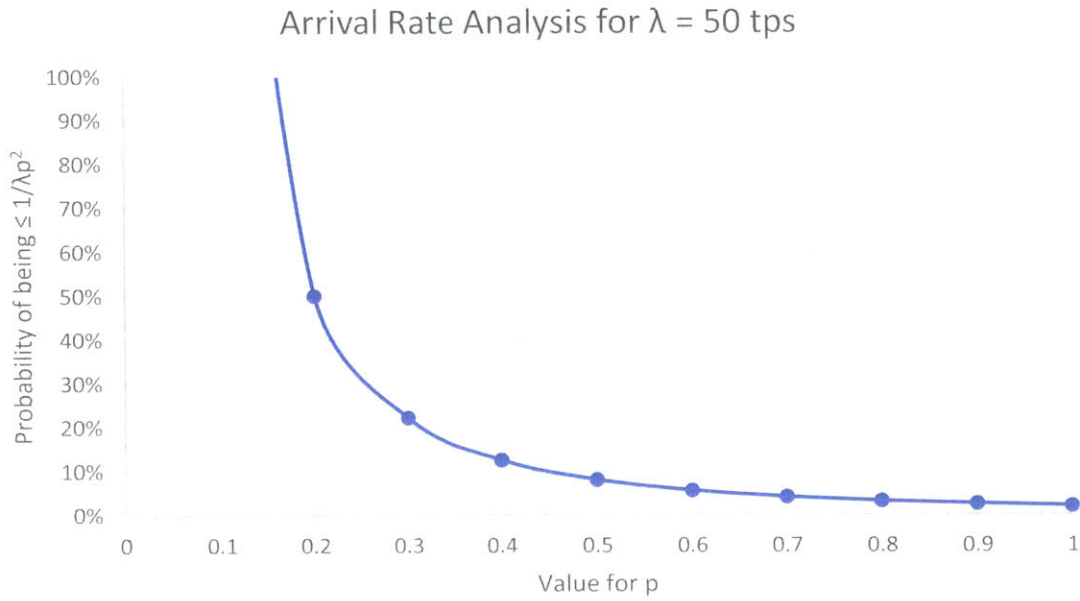
To determine whether an arrival rate of  $\lambda$  is correct in comparison to an arrival rate of mean  $\bar{x}$  given an observed arrival rate of  $Z$ , then we can apply a Neyman-Pearson test with hypothesis  $H_0 = \lambda$  and  $H_A = \bar{x}$ , where  $\bar{x} > \lambda$ . The following test with a significance  $\alpha = 0.05$  is given in (3.7); through this test, we can analytically determine whether or not the observed arrival rate is abnormal in comparison to the null hypothesis  $\lambda$ . A derivation of (3.7) can be found in Appendix A.

$$\frac{L(\lambda|Z)}{L(\bar{x}|Z)} \leq \frac{-\ln(1 - 0.05\lambda)}{\lambda} \quad (3.7)$$

If the probability of an observed arrival rate occurring is improbable and/or outside of an established threshold, it is possible to configure some type of system response alerting network managers to the phenomenon, allowing for a quick resolution of the issue.

---

<sup>2</sup> Based on a data rate of 100 frames per second (10Gb/s capacity with frames of size 100Mb)



**Figure 3.3 - Arrival Rate Analysis for  $\lambda = 50$  tps. The graph depicts the probability that the arrival rate is within the threshold of (3.6) for given values of  $p$  (which translate to percentages).**

## ii. *Switch Time Analysis*

As discussed in Chapter 2, adiabatic switching can and should be used in benign network operation so as to avoid problems with power transients. Monitoring of the amount of time it takes for wavelength turn-on and turn-off, thus, can be an effective tool for detecting a power transients attack, as a nefarious user will likely induce switch times that are more step-like in nature, given the intention is to inflict as much damage as possible. Applying Cantelli's Inequality to this analysis yields the following equation:

$$Pr\{\bar{T} - T_{obs} \geq \epsilon\} \leq \frac{\sigma_{\bar{T}}^2}{\sigma_{\bar{T}}^2 + \epsilon^2}. \quad (3.8)$$

In Equation 3.8,  $T_{obs}$  represents the observed switching time for a turn-on, while  $\bar{T}$  represents the known or anticipated value for the switching time, and  $\sigma_{\bar{T}}^2$  represents the variance of the expected switching time, with  $\epsilon$  being an arbitrary value. A malicious



power transient attack would be as impulse-like as possible, desiring as fast a switching time as possible, so to simplify this equation, we could approximate  $T_{obs}$  to be approximately 0. Substituting this information into Equation 3.8, it can be rewritten as

$$Pr\{T_{obs} \approx 0\} \leq \frac{\sigma_T^2}{\sigma_T^2 + T^2}. \quad (3.9)$$

This equation highlights the fact that it is very improbable for the switching time to approach a step function, particularly if the adiabatic switching time is very high.

### iii. *Power Level Monitoring*

This attack relies on the injection of periodic power transients to disrupt proper message transmission, so looking for these sudden spikes in power via power level monitoring could be effective in finding when and possibly where the transients are occurring (given sensitive-enough equipment). This method requires the time series of the history of the optical channel power instead of just an average power measurement, as used in gain competition measurements. Since power transients affect all transmitting wavelengths, the power level monitoring used for this attack only has to be performed on a single wavelength in the channel, as the attack's effects can be seen at that level. The number of devices required is dependent upon the dynamic range of the device itself, as previously outlined.

### iv. *TCP Window Monitoring*

Through the injection of these transients, which results in corrupted message transmissions, an attacker could trigger the closing of the TCP window for the session,

leading to loss of throughput and potentially severe service degradation. By monitoring the TCP windows at the end-user process (or a test-user pair), one can observe window closing and deduce when packets are being dropped.

This detection mechanism requires multi-layer monitoring, as well as network-user coordination. If the network has an in-band network management and control system, then the network management TCP sessions can also be used as part of the monitoring system. Although this method would be helpful in detecting an ongoing attack, it does not help in differentiating the type of attack being used, and thus serves as a general attack warning than a diagnosis tool.

**v. *Bit Error Rate Monitoring***

The biggest harm power transients cause are the corruption of message frames being transmitted in optical flow switching [25], thus increasing the bit error rate for the session, potentially significantly. By monitoring the time history of the bit error rate and comparing it to a previously known and verified bit error rate from benign system operation, it is possible to deduce if the network suddenly comes under some type of attack.

Recent work done in [13] describes a method of monitoring bit error rate over time to proactively switch to an alternate route before significant packet loss occurs. This method would serve not only as a detection mechanism, but also as a mitigation tool through the subsequent employment of M-fold spatial diversity described in Section 3.1, allowing the path to be preemptively switched and subsequently bypassing the point of origin of the current attack.

## ***Localization***

Although an attack via power transients has a wide variety of detection options, few of them are helpful in terms of localization. Power level monitoring can be used to localize to the extent of its effective range, as previously described, but methods such as TCP monitoring occur at the end-user level, and thus do not give much hints in terms of where the attack originated. As a result, the only effective means of localization for this type of attack is through the use of power level monitoring.

## ***Possible Attack Mitigation***

### ***i. Strong Error Correcting Code***

Error correcting code can be a very resilient ally in recovering corrupted messages after an attack. With a robust, effective code, it is possible to still receive correct messages and not have transmission impeded despite power transients occurring. Error correcting code, however, is far from the end-all solution, as it can only correct up to a certain number of power transients. Thus, an adversary can still one-up the system's defenses by injecting transients past the point it is able to compensate for.

## **3.7 Control Plane Attack (Looping Attack)**

### ***Sensing and Detection Capabilities***

#### ***i. TCP Window Monitoring***

With a looping attack, there is a significant probability of packets being lost or severely delayed, which in turn can trigger the transport layer protocol to retransmit packets if ARQ is implemented. As TCP sees these packets being "lost," it will begin to close its window

size, as it believes that congestion or some other phenomenon is leading to these dropped packets. This severely throttles channel throughput as the window size can collapse to virtually zero, exacerbating the problem. By examining the TCP window size from the end-user (via test sessions) perspective, it is possible to see the window size over time and determine if something is occurring that is triggering TCP window closing and throttling transmission. As described in Section 3.6, this will not indicate that a control plane attack is what is causing the disturbance, and so is also a general detection scheme for any sort of TCP abnormality, malicious or not.

### ***Localization***

One of the reasons why a control plane attack is so dangerous is because of the extreme difficulty that exists with localizing its origin point. As described in Chapter 2, the control plane attack is basically the brain behind the network, serving as the decision-making hub for traffic flows and connections. Once that brain has been infiltrated, an attack could occur wherever the control plane has power over, which in most cases is the entire network. Thus, the only way to really stop the attack is to find and shut off access to the entry point. Control plane cyber-attacks are beyond the scope of this work, and its security in relation to cyber-attacks should be addressed separately. With an integrated, segmented TCP monitoring system as described in Section 3.6, it is possible to localize the areas impacted by the attack, but as previously mentioned, this is not necessarily the attack's origin point, and thus would not do anything to eliminate the threat.

## ***Possible Attack Mitigation***

### ***i. Partitioning of Control Plane***

While the control plane manages the operational logistics of the entire network, it does not necessarily have to be a single entity that has dominion over all; alternatively, it may consist of several disjoint planes over autonomous zones that communicate with each other, or are unified in a hierarchical fashion [26], with each subplane independently controlling its own partition of the network. It is assumed, however, that any one control plane cannot access the configuration of any other plane, meaning that they are fully independent in terms of configuration and subsequently free from manipulation by other planes. By segmenting the control plane, the access that an attacker after infiltration is limited to the local plane, and does not permit access to the configuration of any others. This segmentation, however, causes the network to operate less efficiently than if it were operating as a single unified entity.

Although this mitigation method does not necessarily eliminate the threat, it confines it to a subsection of the network, preventing it from doing a considerably greater amount of damage. This method also assists in localization, as the attack, once identified, can be localized to a specific subset of the network, which can then be quarantined to prevent issues from spreading throughout the other healthy sections.

### ***ii. “Last Known Good Configuration”***

Similar to the option offered by the operating system of a computer after a crash, this mitigation method utilizes the storage of previous control plane configurations that allowed the network to operate at a satisfactory level. With each modification of the control plane, the previous configuration and its degree of efficiency (determined as a function of

throughput), is recorded. If at any point a modification of the control plane occurs to where the efficiency of the network is unsatisfactory, the network manager will have the option to “roll back” to a previous configuration of higher efficiency.

While this mitigation tool could be very valuable, there are also drawbacks associated with it. Rolling back to previous configurations may undo damage caused by an attacker, but it also may revert to a configuration that no longer suits the needs or demands of the network, creating additional issues. Thus, an experienced network manager or decision-making entity must be able to employ this option with the requirements of the network and an idea of effects of the roll-back in mind.

### **3.8 Simple Network Management Protocol (SNMP) Modification**

#### *Sensing and Detection Capabilities*

##### **i. TCP Window Monitoring**

Similar to the sensing of a control plane attack mentioned in Section 3.7, an SNMP attack may be detected through the behavior of the transport layer protocol. By examining the TCP window size from the end-user perspective, it is possible to see the window size over time and determine if something is occurring that is triggering TCP window closing and throttling transmission. By creating inaccurate device status updates, extended packet travel times could result in retransmission requests and/or timeouts, which would also prompt TCP window closing. Again, this would only serve as a general abnormality indicator, as previously explained.

## ii. *Byzantine Fault Tolerance Schemes*

Nearly every type of network in existence has at one point or another had to deal with conflicting information being passed around, requiring a decision on what to believe. This age-old problem is known as the Byzantine Generals', or Two-Army Problem [14], and is applicable in the case of this attack. In an SNMP modification attack, the protocol will be manipulated to generate false information, which will eventually conflict with information coming from elsewhere that reflects the true state of the network object. When this occurs, the system should ideally be able to continue normal operations despite the faulty information until the maximum fault tolerance level is reached, possessing a degree of Byzantine fault tolerance. While Byzantine fault tolerance schemes are essentially useful as a mitigation strategy, it is also possible to employ them to root out which nodes are spreading conflicting information and thus identify the potential targets of an attack. Once more than one-third of the nodes are compromised, however, is it no longer effective as either a detection or mitigation technique, as the faulty nodes can no longer be differentiated from the benign nodes [14]. This fault tolerance scheme must employ a means of authentication and integrity of information, which can possibly be ascertained via SNMPv3 [17]. An implementation design for this method is outside of the scope of this paper, however, and we will simply emphasize the usefulness of such a scheme.

### *Localization*

SNMP modification attacks share the same localization issues as control plane attacks. Consequently, the key to localization also lies with segmentation of the network to prevent the effects of SNMP tampering from permitting access and control to the rest of the network.

### **3.9 Link State Protocol (LSP) False Advertising**

#### ***Sensing and Detection Capabilities***

##### **i. *TCP Window Monitoring***

Similar to the previous attacks affecting network management, an LSP attack may be seen through the behavior of the transport layer protocol. By examining the TCP window size from the end-user perspective, it is possible to see the time history of the window and determine whether or not the system is suffering from some issue through the protocol's response. Just as with the previous two attacks, an LSP attack cannot be identified purely from this method, but this type of monitoring can indicate that the network needs attention.

##### **ii. *Byzantine Fault Tolerance Schemes***

The Byzantine fault tolerance mitigation tactic for an LSP attack is identical to that of the SNMP modification attack covered in Section 3.8, with the difference that LSP relies on messages propagating through the network to spread false information. As a result, Byzantine fault tolerance is even more applicable, given that other nodes inadvertently begin to pass on false information. Thus, once a false advertisement is passed along by more than one-third of the nodes present, then it becomes indistinguishable from the truth and then the mitigation tactic becomes unhelpful.

#### ***Localization***

LSP attacks are similar to the previous two attacks in that they influence management decision-making, causing inefficient choices to be made and thus reducing the efficiency of the network. Limiting the influence area of these messages is thus key to defeating the attack, and



so segmentation of the network in terms of access and information management and control is essential. Consequently, this provides a means of localization for the network, as sections where the attack is detected can be quarantined to limit the damage incurred.

### **3.10 Summary of Chapter 3**

In this chapter, the most effective methods for sensing and localizing each attack are discussed, but the question that remains is how to best apply this information in a practical network setting. Limited resources and limited budgets are very real constraints, and a network planner and/or manager must carefully consider what the network requires in terms of security with a realistic sense of what is feasible.

Chapter 4 outlines what a comprehensive solution looks like, incorporating these sensing, localization, and mitigation techniques into a framework that allows the network architect to find an effective security solution that best fits the system's needs and limitations.



# Chapter 4

## Security Strategy Formulation

Taking into account all of the information, resources, and advice outlined in the previous chapters, it is time to combine them all into the development of a viable plan for security. The goal of this work is to provide a framework on which a security strategy can be built for any network, planned or preexisting, and thus must be able to be applied to a variety of networks and still be effective. In the following chapter, we propose a methodology for diagnosing network attacks, a framework for monitoring implementation, and a threat containment scheme that can be applied to a wide range of network types and can be customized to best fit the demands specific networks.

### **4.1 Attack Diagnosis Framework**

In a network, an attack is much like a disease, as it hinders healthy operation. Following this analogy, the most effective way to eliminate a disease is through accurate diagnosis and subsequent treatment based upon what is effective against that particular disease. Similarly, the best way to approach a network attack is to accurately identify it and respond according to what works against that specific attack. Through the analysis conducted in Chapter 3, it is clear that taking the steps to mitigate the wrong attack could adversely affect system operation. For example, if a repeat-back jamming attack is occurring, the problem could be worsened by rolling back to a previous network configuration that does not optimize performance if mistakenly

thought to be a control plane attack. In order to avoid such an instance of mistaken identities, we propose a framework for identifying and correctly diagnosing which attacks are occurring based upon the “symptoms” they illicit.

### 4.1.1 Diagnoses Model

Looking at the effects caused by all the attacks discussed in Chapter 2, we will create a method of diagnosing which attack is most probable given the phenomena observed. Table 4.1 provides a useful aid for making such diagnoses.

ATTACKS	SYMPTOMS					
	Significant phase shift/delay	Abnormally high signal power	Marked signal attenuation	Manipulated system response	Instance of intrusion	Increased BER/packet corruption
Tapping/Bending			X		X	
Out-of-Band Crosstalk		X				X
In-Band Crosstalk	X		X			
Repeat-Back Jamming	X		X		X	
Gain Competition		X	X			
Power Transients		X				X
Control Plane Attack				X		
SNMP Modification				X		
LSP False Advertising				X		

**Table 4.1 – Diagnosis Framework for Potential Attacks.** Table lists known, prominent symptoms for each attack listed.

The wide range of attacks also have a wide range of symptoms, with no two attacks (except for upper-layer originating attacks – control plane, SNMP and LSP attacks) sharing the exact same list of symptoms. Thus, it is possible to differentiate between the attacks based upon the observed assortment of effects.

### 4.1.2 Algorithm for Effective Attack Response

Within the network management entity, a diagnostic algorithm should exist to correctly identify the attack and subsequently initiate the mitigation techniques discussed in Chapter 3 to mitigate it. This algorithm should operate as follows:

<b>1</b>	Record symptoms as they are experienced via sensing methods
<b>2</b>	Once an initial symptom is registered, initiate mitigation actions
<b>3</b>	Once at least 2 symptoms have been registered, give initial diagnosis (Priority given to manipulated system response – immediate action taken)
<b>4</b>	Continue to check for symptoms; if less than 2 symptoms are registered, clear diagnosis; if no symptoms are registered, end mitigation actions

**Table 4.2 - Diagnostic Algorithm**

The algorithm uses two symptoms to make a diagnosis as that is the minimum number of symptoms required for any non-management attack. Using this algorithm, the network management entity will iterate over the list of symptoms, checking for their presence via the monitoring system consisting of all the network sensing devices implemented. The algorithm suggests a fairly aggressive precautionary response, as mitigation actions are required before an initial diagnosis is even made.

Mitigation actions in this algorithm refer to the precautionary shutdown of the afflicted area of the network, in order to deny the attacker continued access to the network, as well as to reduce







the probability of the attack spreading. The process by which areas under attack are quarantined will be discussed in Section 4.3 in depth.





















## **4.2 Monitoring System Implementation**

From all of the sensing and detection methods listed in Chapter 3, the list can be condensed to a list of six methods. The following is a list of those methods ordered according to usefulness within a network that values attack diagnosability:

- 1) Power Level Monitoring – to include both coarse and fine-grain measurements
- 2) TCP Window Monitoring
- 3) Optical Time Domain Reflectometry (OTDR)
- 4) BER/Signal Quality Measurement – to include BER monitoring and arrival rate analysis
- 5) Phase Detection
- 6) Byzantine Fault Tolerance

The implementation of all of these methods is discussed in detail in Chapter 3. The logic behind this ordering can be extrapolated from Table 4.3, which pictorially describes the relationship between the various sensing methods and the symptoms of an attack. It is clear from the table that power level monitoring can detect symptoms across the widest range of attacks, and thus is the most essential tool to identify an issue as it arises. Power level monitoring can also be used to differentiate between the attacks based upon whether it senses a noticeable increase or decrease in power levels. If fine-grain power level monitoring is used, it can also assist in locating the offending wavelength in an attack such as gain competition or power

- Sensing and Localization Methods**
-  Phase Detection
  -  Power Level Monitoring
  -  OTDR
  -  BER/Signal Quality Measurement
  -  TCP Window Monitoring
  -  Byzantine Fault Tolerance

ATTACKS	SYMPTOMS	Significant phase shift/delay	Abnormally high signal power	Marked signal attenuation	Instance of intrusion	Manipulated system response	Increased bit error rate/corruption
		Tapping/Bending					
Repeat-Back Jamming							
Gain Competition							
Power Transients						 	
Out-of-Band Crosstalk							
In-Band Crosstalk							
Control Plane Attack						 	
SNMP Modification						 	
LSP False Advertising						 	

**Table 4.3 - Monitoring System Applications.** Table depicts the sensing methods that can be applied to detect the attack symptoms, as depicted in Table 4.1.

transients, meaning that the malicious signal could be turned off without having to shut down the entire signal band, allowing for better network efficiency than could otherwise be attained.

The second most valuable sensing method is TCP window monitoring, because, although it cannot uniquely identify an attack on its own, it is extremely useful in indicating whether or not any attack is occurring. It also helps fill the detection gap left by power level monitoring, which is unable to detect the upper-layer attacks. Although not quite as powerful a localization

aid as other sensing methods, TCP window monitoring is ranked second on the list because of the relative ease information can be extracted given a test user station, as well as its effectiveness as a diagnostic tool in conjunction with power level monitoring. Since the network managers are not usually privy to the end-user TCP information, either the network must seek cooperation with the users or initiate probe TCP sessions itself.

Use of OTDR devices is the next-most beneficial sensing tool, as it not only provides the most powerful localization tool, but is also useful in detecting any intrusion into the network, which may also be required for other attacks that do not list it as a prominent symptom in Table 4.1. Although potentially costly, the benefits of this added localization ability will help to reduce the quarantine area of the network should it become necessary, sparing otherwise diminished network efficiency.

BER and/or signal quality measurements should be the next tools implemented, as they can help identify the previously undiagnosed in-band crosstalk and can confirm the presence of out-of-band crosstalk. This type of sensing can also be done at the end points of a lightpath, meaning it is less involved and subsequently less costly to implement.

Phase detection is the next sensing method in the arsenal to be deployed, as it serves to confirm the identities of several more attacks. Phase detection is a powerful tool that, in conjunction with the previously mentioned sensing techniques, serves to strongly support a diagnosis, and also has the ability to better-identify attacks that are notoriously subtle in nature that can possibly go undetected despite other sensing methods in place. It is lower in the list, however, because of the implementation costs, which could become very high as many devices would be required.



The final step in a full-fledged monitoring system is the application of a Byzantine fault tolerance scheme, as discussed in Chapter 3. This scheme would serve to confirm an attack as an upper-layer attack, although it would not be very beneficial for other attacks. Its low ranking comes as a result of its limited applications and the likely high level of effort it would take to implement.

Using this information and this prioritization, a network planner and/or manager could apply it to according to the needs of the network – a low budget could mean cutting out more costly methods such as OTDR, or a known susceptibility to crosstalk could mean favoring phase detection over TCP window monitoring. The point of this analysis is to suggest a framework for devising an effective security strategy that takes into consideration the strengths and weaknesses of various sensing options, allowing it to be molded to best-fit a specific network’s needs and constraints.

### **4.3 Network Quarantine and Recovery Process**

The most effective mitigation tactic against any attack is the denial of access to the network. This oftentimes can only be accomplished by shutting network operation at the point of attack, and as discussed in Chapter 3, identifying the precise origin point for an attack can be very difficult. The concept of quarantining a section of the network is stopping all network operation within the affected area and isolating it from communication with the rest of the network, preventing the effects of an attack from spreading to the rest of the network. The quarantine area is a function of the localization capabilities, with tighter localization equating to less loss of healthy network operation due to precautionary shutdown.

### 4.3.1 Determining Quarantine Area

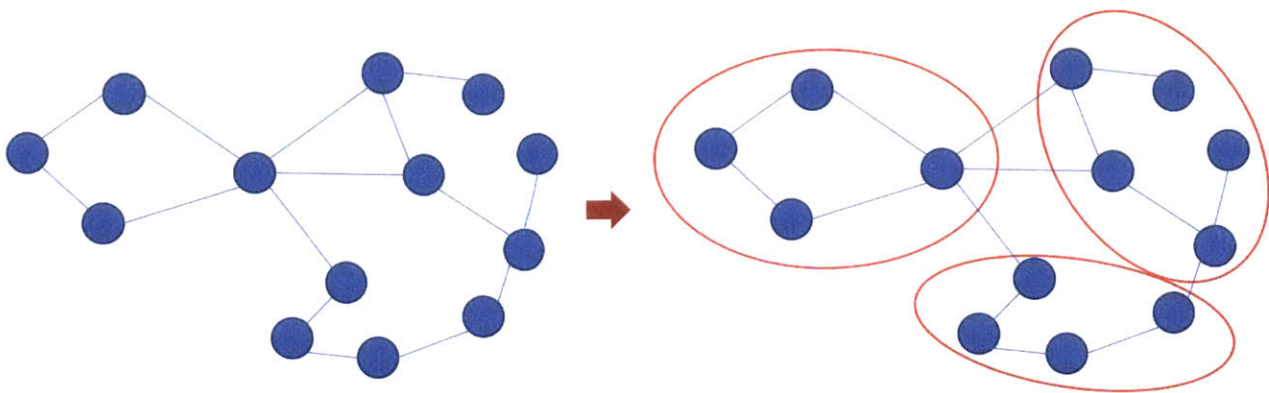
The extent of the localization capabilities for each of the aforementioned sensing methods is discussed in Chapter 3. Assuming all the methods are enacted in the network at their full maximum detection range, the localization range, equivalent to the quarantine area, for each of the attacks are as listed in Table 4.4. From Table 4.4, it is clear that the only attacks which do not yet have a quantifiable localization range are the upper-layer attacks – the control plane, SNMP and LSP attacks. As discussed in Chapter 3, an essential tool for localization, as well as for general attack mitigation purposes, is the segmentation of the network into independent, self-managed zones that are capable of communicating with one another while preventing the spread of intruder access and control.

Attack	Localization Range		
	$PLM = \frac{h \cdot c \cdot v}{\lambda \cdot (1 - P_{loss}) \cdot 10^{(P_o - P_{min} - 30)/10}}$	OTDR = max(device resolution, link length)	$PD = \frac{2\lambda^2 \ln 2}{\pi n \Delta \lambda}$
Tapping/Bending	min(PLM, OTDR)		
Out-of-Band Crosstalk	PLM		
In-Band Crosstalk	min(PD, PLM)		
Repeat-Back Jamming	min(PLM, OTDR, PD)		
Gain Competition	PLM		
Power Transients	PLM		
Upper-Layer Attacks	Dependent on size of management segmentation		

**Table 4.4 - Localization Range for Optical Attacks.** Table gives the minimum localization range for each attack based upon the sensing methods available given by Table 4.3.

### 4.3.2 Segmentation via Autonomous Zones

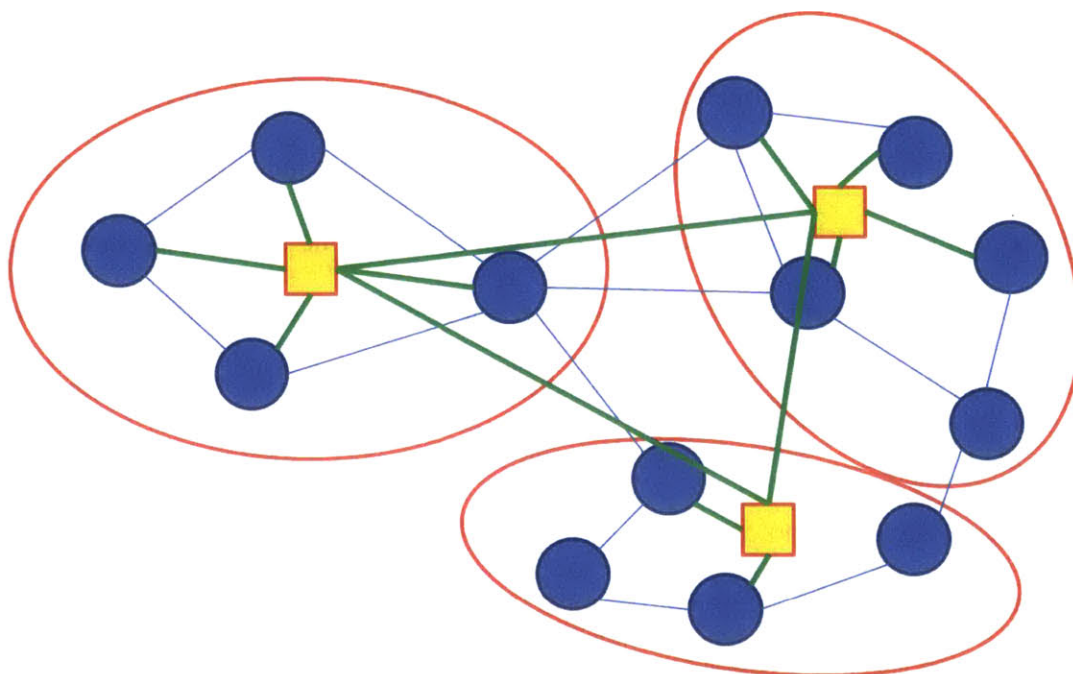
One way for the segmentation of the network to be effective from a security standpoint is to make each zone autonomous, responsible for its own management and control functions. These autonomous zones must also be able to still communicate with one another, as messages could have to travel between several different zones to reach their destinations. These zones may be retrofitted onto established networks, meaning the autonomous zone logical topology is placed over preexisting physical infrastructure, so the solutions presented should be generally applicable and not specific to any one topology. An example of fitting autonomous zones over an existing network is given in Figure 4.1.



**Figure 4.1 – Retrofitting of Autonomous Zones onto Existing Network. The autonomous zones (depicted by red circles) are placed over existing network architecture by network managing entity.**

### 4.3.3 Introduction of the Network Management Hub

The proposed network management hub is the attack management entity located within each network segment, allowing it to run diagnostics and ensure the zone is functioning correctly. The network management hub runs the diagnosis algorithm outlined in Section 4.1, and is able to quarantine the zone should it become necessary, through the disabling and shutting down of all zone components in relation to the rest of the network. The network management hub, or NMH,



**Figure 4.2 – Depiction of Autonomous Zone network with Network Management Hubs. Green lines represent the off-band signaling network implemented for monitoring and diagnostic purposes, with yellow boxes representing network management hubs.**

does not necessarily have to be co-located with the segment’s control plane, however, and should realistically be a logically separate unit, as otherwise it could be susceptible to tampering during a control plane attack. The localization range of an NMH is not limited to the size of the NMH, but instead incorporates information from other sensing devices present within its authority, and with access and operational control over the zone, it can quarantine subsets of the zone as prompted by the other sensing methods. Figure 4.2 gives an illustration of what a segmented network using NMHs would look like.

In order for the NMH to effectively run diagnostics, it must be able to communicate with the nodes under its supervision to determine whether any faults have occurred. To do this, a probing process must be established, through which the NMH can assess the operational state of the zone. In [22], a probing algorithm is suggested that relies on sending out probing signals based upon feedback, in the form of the probe syndrome. The probe syndrome,  $S_p$ , is found as follows:

$$S_p = \begin{cases} 0 & \text{probing signal received back} \\ 1 & \text{otherwise} \end{cases} \quad (4.1)$$

The steps for implementing this probing mechanism from [22] are as follows:

1. Probing signals are sent sequentially over valid lightpaths
2. If the probe syndrome is equal to 0, then stop probing; otherwise, continue to probe following localization algorithm until the fault is found a localized

There are a variety of different algorithms for fault localization via probing as described in step 2, such as the run-length coding-based algorithm described in [9]. This overall probing technique assumes link failures occur independently. Applied to the concept of network management hubs and autonomous zones, the probing scheme would be conducted within each zone, with the probing signals generated and analyzed by the NMHs.

While it may not be directly connected to each node, like in Figure 4.2, there must be enough nodes capable of communication with the NMH so that it can accurately assess the state of the zone. The work done in [22] gives the number of nodes that must be equipped with TX/RX pairs for NMH communication as lower-bounded by the following equation:

$$\eta^*(\alpha_F) \leq \frac{ndp^2}{4\alpha_F} \quad (4.2)$$

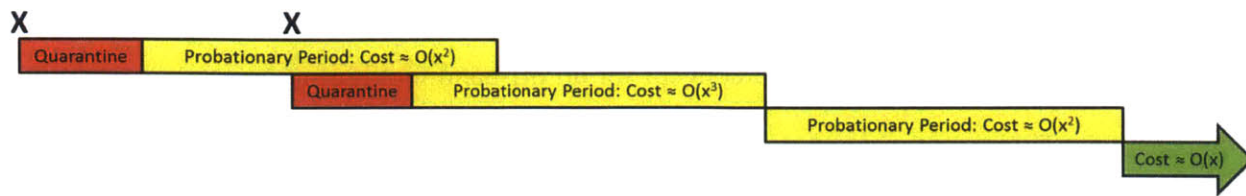
In this calculation,  $\eta^*(\alpha_F)$  represents the fraction of nodes within the dominion of the NMH that are required to have the TX/RX pairs,  $n$  is the total number of nodes in the zone,  $d$  is the node degree,  $p$  is the probability of node failure, and  $\alpha_F$  is the tolerable cumulative undiagnosability probability, which is the total probability that is deemed acceptable in which a failure event in the zone could not be uniquely identified. This probability stems from the fact that there are less TX/RX pairs than there are nodes, and thus the state of each link may not be able to conclusively

be determined. The bound is based upon an Eulerian-trail topology, which can be generalized to most topologies [22], and which can be taken into consideration during the network segmentation phase. This bound should be applied for each autonomous zone as if it were its own individual topology, and not applied over the entire network as a whole. The lower-bound for the amount of nodes that must communicate with NMH must also be taken into account when partitioning the autonomous zones, so that the NMH is not over constrained.

The NMHs themselves will be able to communicate with adjacent NMHs and nodes in their respective zones via an off-band signaling network, as depicted by the green lines in Figure 4.2. This will allow the NMHs to share their availability status with others when inter-zonal communication might otherwise be hindered, such as during a quarantine, as well as allow the zone to perform internal testing to determine if it is still under attack. The key component to this monitoring system is the integrity of the underlying NMH system; if an NMH becomes compromised, then the entire system is at risk and can be rendered ineffective. Thus, a method of ensuring the integrity of the NMHs is vital, such as through an authentication system.

#### **4.3.4 Impact of Quarantine**

The establishment of NMHs within each network zone will be extremely beneficial in terms of localization and diagnostics, but what if it becomes necessary to quarantine a zone? How will that effect overall network operation? In the event of network quarantine, the NMH will direct the entire zone to cease operation and immediately cut off all access to the rest of the network, but the NMH will remain active, sending messages to all adjacent zones informing them that its zone has been quarantined, and running diagnostics within the zone.



**Figure 4.3 – Example of Quarantine Recovery Process Event Flow. After a quarantine period, the zone enters a probationary period during which the cost of outgoing links rises exponentially. This continues for every subsequent quarantine during a probation until the period is completed without issue, at which point the cost begins to decrease exponentially**

While performing those diagnostics, if any of the symptoms of an attack are present, then the zone will remain under quarantine. If the attack symptoms are no longer present after a predetermined amount of time, however, the NMH will reactivate the zone, but at a price. Once flagged for quarantine, the NMH will be placed under a probationary period for a set duration of time after the quarantine has lifted. During this period of increased surveillance, the NMH will effectively increase the cost of all links that communicate with nodes outside of the zone, making them less likely to be used for inter-zonal communication. With each flagging for quarantine within the probationary period, the cost for outgoing links rises exponentially, possibly reaching a point where all communication not directly involving a node in that zone will completely bypass it, and the time the region is on probation is restarted. Figure 4.3 illustrates this concept, with the Xs marking the diagnoses of attacks. After each quarantine period, the cost of the outgoing links rises exponentially during the probationary period, and does not begin to return to its original value until the probationary period passes without incident. This will not directly impede traffic flows between nodes within and outside of the zone, but it will significantly lessen the likelihood of through-traffic from entering the zone, particularly if many quarantine flags are raised.

#### **4.4 Summary of Chapter 4**

The high-level introduction of a concept for an off-band monitoring network is presented in this chapter. This monitoring network will interface with the various sensing devices in place in the network, as well as with some of the nodes within the network to perform diagnostic testing, all to ensure that an accurate diagnosis of an attack can be found. This monitoring system relies on the concept of autonomous zones in order to segment control and provide the ability to quarantine problem zones.



# Chapter 5

## Conclusion

### 5.1 Summary of Contributions

In the introductory chapter of this thesis, we briefly describe the structure and application of all-optical networks. The necessary components for effective security planning and the requirements of a successful defensive strategy were also discussed.

Chapter 2 gave a detailed description of each of the nine presented attacks. The characterization of each attack included illustrations of the attack process, the mechanics of the attack, and an explanation of the resulting effects at both the originating layer and subsequent layers. A few of the presented attacks, such as repeat-back jamming and control plane attack, had not previously been characterized to such an extent.

Chapter 3 took a methodical approach to characterizing the security concerns for each attack. We first discussed the best tools for sensing and detecting the presence of an attack in the network. We then discussed the issues concerning localization and identified the resolution of the attack origin point based upon the sensing methods employed. Next, we proposed several tactics for limiting the amount of damage that the attacks could induce within the network, as well as highlighting some preventative measures that could be taken to ward off future attacks. Finally, we recognized vulnerabilities that still remained after all other sensing and mitigation techniques were put into action.

Lastly, Chapter 4 presented an algorithm for diagnoses of attacks in a network based upon the observable effects within the network. We also proposed a prioritization for the implementation of monitoring tools in an arbitrary network based upon analysis of effectiveness in diagnosability and implementation costs. A novel scheme for segmentation of the network that would allow for the precautionary shutdown of attack areas was then defined, with a methodology presented for the application of a quarantine system within the network to mitigate damage and eliminate attacker threats.

## **5.2 Future Work and Challenges**

In this work, we covered several of the most devastating optical attacks known at great length, but there are still more optical network attacks to be researched and characterized, and surely even more to be discovered. In the world of cyber security, it seems as if for every threat that is eliminated, more threats or vulnerabilities arise, and thus there is always further work to be carried out.

A significant starting point for this ongoing work would be the full development of a Byzantine fault tolerance scheme that could challenge management-level attacks, such as the control plane attack. The control plane attack is by far one of the more problematic issues facing the future of AON security, and any additional means of detection, localization, or mitigation are extremely welcome.

Finally, quantifying the effectiveness of the security framework proposed in this thesis would be a rewarding future task. Through simulation, or perhaps even physical experimentation, the analytical validity of the ideas presented in this work could be tested and compared to a real-

world application, thus providing insight as to the accuracy of the network models and validation of the underlying assumptions and analysis.



# Appendix A

## Chapter 3 Equation Derivations

### Derivation of Equation 3.1

$h = \text{Planck's constant } (\sim 6.262 \times 10^{-34} \text{ J/s})$      $c = \text{speed of light } (\sim 3.0 \times 10^8 \text{ m/s})$

$\lambda = \text{wavelength (m)}$      $v = \text{speed of light in medium } (\sim 2.0 \times 10^8 \text{ m/s})$

$P_{\text{loss}} = \text{power line loss (dBm)}$      $P_0 = \text{initial signal power (dBm)}$

$P_{\text{min}} = \text{minimum readable device power (dBm)}$

The Planck-Einstein relation for the energy of a photon is given as:

$$\text{Energy} = \frac{h * c}{\lambda}$$

The length of time the photon travels could then be found via the following equation:

$$\text{time} = \frac{\text{Energy}}{\text{Power}}$$

Using this relationship, we can solve for the distance the light travels by using the speed of the light in the medium,  $\sim 2.0 * 10^8$ .

$$\text{distance} = \frac{\text{Energy} * v}{\text{Power}}$$

Energy of the light was calculated in (1). The power is dependent upon the dynamic range of the device with respect to where the power level initially started from. Thus, it is the initial power  $P_0$  minus the minimum power required for measurement,  $P_{\text{min}}$ . Because the measurements are

customarily in dBm, the following equation must be used to convert the power to the required Watts:

$$Power (W) = 10^{(P_o - P_{min} - 30)/10}$$

Because the system also incurs line losses as the signal traverses the fiber, the distance must also incorporate a term to account for this loss. Thus, the true distance  $d$  becomes:

$$d = distance - distance(P_{loss}) = distance(1 - P_{loss})$$

Combining all the previous equations, we get Equation (3.1):

$$d = \frac{h * c * v}{\lambda * (1 - P_{loss}) * 10^{(P_o - P_{min} - 30)/10}}$$

### Derivation of Equation 3.3

$L$  = length of optical cavity (m)

$c$  = speed of light (~3.0 x 10<sup>8</sup> m/s)

$n$  = cladding index of refraction

$L_i$  = coefficient of loss

$\tau_D$  = receiver minimum detection time (s)

$\theta$  = phase shift (rad)

The lifetime of a photon is given by the following equation:

$$\tau_p = \frac{L}{c/n} - loss = \frac{L * n}{c} - \left(1 - \frac{1}{L_i}\right)$$

Photon lifetime can also be related to phase shift via the following inequality:

$$\tau_p \leq \frac{\Delta\theta * \tau_D}{2\pi},$$

where  $\tau_D$  is the time in which the receiver can detect change, given as a specification of the receiver.

Combining the first two equations, we can solve for the minimum detectable phase shift, shown by Equation (3.3).

$$\Delta\theta_{min} \geq \frac{2\pi}{\tau_D} \left[ \frac{L * n}{c} - \left( 1 - \frac{1}{L_i} \right) \right]$$

### Derivation of Equation 3.7

In order to determine which mean should be accepted as the accurate mean for an observed average arrival time, we run a Neyman-Pearson test with the following specifications for hypotheses for the mean:

$$H_0 = \lambda \quad H_A = \bar{x},$$

where  $\bar{x} > \lambda$ .

From this point, we can solve for the critical value C for an observed arrival rate z as follows:

$$\begin{aligned} C &= \{z: f_x(z; \lambda) \geq k * f_x(z; \bar{x})\} \\ &= \{z: \lambda \exp(-\lambda z) \geq k * \bar{x} \exp(-\bar{x}z)\} \\ &= \{z: \exp(-\lambda z) \geq k' * \exp(-\bar{x}z)\} \\ &= \{z: \exp(-\lambda z) \geq \exp(k'') \exp(-\bar{x}z)\} \\ &= \{z: -\lambda z \geq k'' - \bar{x}z\} \\ &= \{z: z \leq k'''\} \end{aligned}$$

For a significance level of  $\alpha = 0.05$ , then we must solve for  $k'''$  in the following equation:

$$\begin{aligned} \alpha &= \int_0^{k'''} \exp(-\lambda z) dz \\ &= \frac{1}{\lambda} (1 - \exp(-\lambda k''')) \end{aligned}$$

Solving for  $k'''$ , we obtain the following result:

$$k''' = \frac{-\ln(1 - 0.05\lambda)}{\lambda}$$

The Neyman-Pearson test is given as follows:

$$\frac{L(\lambda|Z)}{L(\bar{x}|Z)} \leq \frac{-\ln(1 - 0.05\lambda)}{\lambda}$$

If (A) is false, then the null hypothesis is rejected in favor of the alternate hypothesis.

$$Pr \left\{ \frac{L(\lambda|Z)}{L(\bar{x}|Z)} \leq \frac{-\ln(1 - 0.05\lambda)}{\lambda} \right\} = 0.05$$



# Appendix B

## List of References for Figure 1.1\*

Furdek, M., & Skorin-Kapov, N. (2011, May). Physical-layer attacks in all-optical WDM networks. In *MIPRO, 2011 Proceedings of the 34th International Convention* (pp. 446-451). IEEE.

Jedidi, A., Rejeb, R., & Abid, M. (2011). Detection and localization of crosstalk in an all-optical network. *Journal of Optics*, 13(1), 015506.

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.

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.

Peng, Y., Sun, Z., Du, S., & Long, K. (2011). Propagation of all-optical crosstalk attack in transparent optical networks. *Optical Engineering*, 50(8), 085002-085002.

Ramaswami, R., & Humblet, P. A. (1990). Amplifier induced crosstalk in multichannel optical networks. *Lightwave Technology, Journal of*, 8(12), 1882-1896.

Rejeb, R., Leeson, M. S., & Green, R. J. (2006). Multiple attack localization and identification in all-optical networks. *Optical Switching and Networking*, 3(1), 41-49.

Santos, C. C., & Assis, K. D. R. (2011, June). Optical networks security: Design to avoid the jamming attacks. In *Transparent Optical Networks (ICTON), 2011 13th International Conference on* (pp. 1-4). IEEE.

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.

Skorin-Kapov, N., Furdek, M., Aparicio Pardo, R., & 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.

Wu, T., & Somani, A. K. (2002, July). Attack monitoring and localization in all-optical networks. In *ITCom 2002: The Convergence of Information Technologies and Communications* (pp. 235-248). International Society for Optics and Photonics.

Wu, T., & Somani, A. K. (2003, December). Necessary and sufficient condition for k crosstalk attacks localization in all-optical networks. In *Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE* (Vol. 5, pp. 2541-2546). IEEE.

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.

Patel, J. K., Kim, S. U., Su, D. H., Subramaniam, S., & Choi, H. A. (2001). *A framework for managing faults and attacks in WDM optical networks*. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD.

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

Rejeb, R., Leeson, M. S., Machuca, C. M., & Tomkos, I. (2010). Control and management issues in all-optical networks. *Journal of Networks*, 5(2), 132-139.

\*Important Note: These reference are in no way fully exhaustive of all research presently being done, and is current up to the end of 2014.

# Bibliography

- [1] Thefoa.org. The FOA Reference For Fiber Optics - OTDR FAQs. 2015. [Online]. Available: <http://www.thefoa.org/tech/ref/testing/OTDR/OTDR-FAQS.html>.
- [2] T. Wu and A. Somani. Cross-talk attack monitoring and localization in all-optical networks. *IEEE/ACM Trans. Networking*, vol. 13, no. 6, pp. 1390-1401, 2005.
- [3] N. Skorin-Kapov, M. Furdek, R. Aparicio Pardo and P. Mariño. Wavelength assignment for reducing in-band crosstalk attack propagation in optical networks: ILP formulations and heuristic algorithms. *European Journal of Operational Research*, vol. 222, no. 3, pp. 418-429, 2012.
- [4] M. Furdek, N. Skorin-Kapov and M. Grbac. Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation. *J. Opt. Commun. Netw.*, vol. 2, no. 11, p. 1000, 2010.
- [5] M. Medard, D. Marquis, R. Barry and S. Finn. Security issues in all-optical networks. *IEEE Network*, vol. 11, no. 3, pp. 42-48, 1997.
- [6] R. Rejeb, M. Leeson and R. Green. Multiple attack localization and identification in all-optical networks. *Optical Switching and Networking*, vol. 3, no. 1, pp. 41-49, 2006.
- [7] Y. Shen, K. Lu and W. Gu. Coherent and incoherent crosstalk in WDM optical networks. *J. Lightwave Technology*, vol. 17, no. 5, pp. 759-764, 1999.
- [8] Y. Jin, Q. Jiang and M. Kavehrad. Performance degradation due to crosstalk in multiwavelength optical networks using dynamic wavelength routing. *IEEE Photonics Technology Letters*, vol. 7, no. 10, pp. 1210-1212, 1995.
- [9] Y. Wen, V. Chan and L. Zheng. Efficient fault-diagnosis algorithms for all-optical WDM networks with probabilistic link failures. *J. Lightwave Technol.*, vol. 23, no. 10, pp. 3358-3371, 2005.
- [10] Thefoa.org. The FOA Reference For Fiber Optics - Measuring Power. 2014. [Online]. Available: <http://www.thefoa.org/tech/ref/testing/test/power.html>.
- [11] R. Steenbergen. Everything you always wanted to know about optical networking - but were afraid to ask. NANOG 48, 2010.
- [12] J. Laferriere, G. Lietaert, R. Taws and S. Wolszczak. *Reference Guide to Fiber Optic Testing*, 2nd ed. Saint-Etienne: JDS Uniphase Corporation. 2011.

- [13] O. Gerstel, I. Leung, G. Nicholl, H. Sohel, W. Wakim, and K. Wollenweber. "Near-Hitless Protection in IPoDWDM Networks," in *Optical Fiber Communication Conference/National Fiber Optic Engineers Conference*, OSA Technical Digest (CD) (Optical Society of America, 2008), paper NWD4.
- [14] R. Perlman. Network layer protocols with byzantine robustness, Ph.D dissertation. Massachusetts Institute of Technology, 1989.
- [15] Y. Chen, C. Visone, R. Pavlik, D. Al-Salameh and J. Tomlimson. System test of dynamic gain equalizer in long haul transmission. *IEEE/LEOS Summer Topi All-Optical Networking: Existing and Emerging Architecture and Applications/Dynamic Enablers of Next-Generation Optical Communications Systems/Fast Optical Processing in Optical Transmission/VCSEL and Microcavity Lasers.*, 2002.
- [16] J. Hecht. Many roads lead to dynamic gain equalization on optical networks. *LaserFocusWorld*, vol. 38, no. 10, 2015.
- [17] W. Stallings. Security comes to SNMP: the new SNMPv3 proposed internet standards. *The Internet Protocol Journal*, vol. 1, no. 3, 1998.
- [18] M. Furdek and N. Skorin-Kapov. Physical-layer attacks in all-optical WDM networks. *MIPRO, 2011 Proceedings of the 34th International Convention*, pp. 46-451, 2011.
- [19] Thefoa.org. 'The FOA Reference For Fiber Optics - Bend Insensitive Fiber. 2011. [Online]. Available: <http://www.thefoa.org/tech/ref/fiber/BIfiber.html>.
- [20] Berk-Tek. Bend Insensitive Multimode Fiber: A new twist for high bandwidth fibers.
- [21] Thefoa.org. The FOA Reference For Fiber Optics - Outside Plant Fiber Optic Cables. 2015. [Online]. Available: <http://www.thefoa.org/tech/ref/OSP/cable.html>.
- [22] Y. Wen. Scalable fault management architecture for dynamic optical networks : an information-theoretic approach. Ph.D dissertation. Massachusetts Institute of Technology, 2008.
- [23] Y. Wen and V.W.S. Chan. Ultra-reliable communication over vulnerable all-optical networks via lightpath diversity. *IEEE J. Select. Areas Commun.*, vol. 23, no. 8, pp. 1572-1587, 2005.
- [24] L. Zhang. Fast scheduling for optical flow switching, M.S. thesis. Massachusetts Institute of Technology, 2010.
- [25] V.W.S. Chan. Optical flow switching networks. *Proceedings of the IEEE*, vol. 100, no. 5, pp. 1079-1091, 2012.

- [26] J. Chapin and V. Chan. Architecture concepts for a future heterogeneous, survivable tactical internet. *Military Communications Conference, MILCOM 2013 - 2013 IEEE*, pp. 1874-1879, 2013.
- [27] K. Shaneman and S. Gray. Optical network security: technical analysis of fiber tapping mechanisms and methods for detection and prevention. *IEEE MILCOM 2004. Military Communications Conference, 2004.*, vol. 2, pp. 711-716, 2004.
- [28] J. Junio, L. Zhang and V. Chan. Physical layer characteristics and design of long haul fast turn-on/off's and flow switched all-optical networks. *Optical Fiber Communication Conference*, pp. 1-3, 2014.
- [29] A. Song. Optical Flow-Switched Transport Layer Protocol Simulation Analysis. Massachusetts Institute of Technology, 2015.
- [30] M. Medard, D. Marquis, S. R. Chinn, "Attack Detection Methods for All-Optical Networks", in Proc. of Network and Distributed Systems Security Symposium, Session 3, paper 2, San Diego, California, 1998.
- [31] G. Abbas, V.W.S. Chan, T. Yee. A dual-detector optical heterodyne receiver for local oscillator noise suppression. *J. Lightwave Technol.*, vol. 3, no. 5, pp. 1110-1122, 1985.
- [32] W. Drexler and J. Fujimoto. *Optical coherence tomography*. Berlin: Springer, 2008.