

# A Framework for Managing Faults and Attacks in All-Optical Transport Networks

Jigesh K. Patel<sup>1</sup>, Sung U. Kim<sup>1</sup>, David H. Su<sup>1</sup>, Suresh Subramaniam<sup>2</sup>, and Hyeong-Ah Choi<sup>2</sup>

<sup>1</sup>National Institute of Standards and Technology

Gaithersburg, MD 20899

{patel,kimsu,dsu}@antd.nist.gov

<sup>2</sup>The George Washington University

Washington, DC 20052

{suresh,choi}@seas.gwu.edu

## Abstract

*Fault and attack survivability in all-optical transport networks (AOTNs) require new approaches because of unique transmission characteristics. Specifically, fiber nonlinearities and network transparency to transmitted signal types may make the network vulnerable to unorthodox attacks. Furthermore, unlike in electronic networks that regenerate signals at every node, attack detection and isolation schemes may not have access to the overhead bits used to transport supervisory information between regenerators or switching sites to perform their functions. This paper presents a discussion on attack scenarios and proposes a conceptual framework for modeling faults and attacks in AOTNs.*

## 1 Introduction

Core transport networks are currently in a transition period evolving from SONET/SDH-based Time Division Multiplexed (TDM) networks utilizing a single wavelength to Wavelength Division Multiplexed (WDM) networks with multiple wavelengths strictly for fiber capacity expansion, and most recently, toward WDM-based all-optical networks. In AOTNs, short and sporadic failures of network elements (e.g., fiber link, amplifier, optical cross-connect (OXC), optical add-drop multiplexer (OADM), etc.) may cause a large amount of data loss. As the widespread deployment of high-capacity WDM systems in the core transport network continues, the survivability of WDM AOTNs in the presence of faults and attacks is becoming a critical issue and currently receives great attention from the research community.

Technical advances and development progress in optical

network elements such as OXCs and OADMs, and of terminal and line devices such as lasers and amplifiers have enabled optical network designers to provision *lightpaths* and switch them via *wavelength routing*. A lightpath is an all-optical path over which data is carried on a single wavelength in AOTNs.<sup>1</sup> The lightpaths are capable of being dynamically switched inside the optical network by OXCs that are sensitive only to the lightpath origin and the wavelength over which it is carried. Such routing is called wavelength routing and renders the lightpaths *transparent* to variables such as modulation format, bit-rate and protocol type.

In AOTNs, data does not undergo opto-electronic conversion and remains in optical. An architectural model for an AOTN is depicted in Figure 1 in which IP traffics are injected into AOTN ingress nodes from various conventional electronic domain networks such as LANs, MANs, and ATMs. The IP protocol framework will become a dominant form of data transfer in the future, and there has been an increasing interest in implementing IP over WDM by using optical networking. In this framework, ingress nodes perform traffic aggregation and route optical data packets to egress nodes. Once the optical data packet is assembled, the AOTN transports optical packets from source to destination nodes through a lightpath that is established between ingress and egress nodes (via wavelength routing using control protocol). A fiber segment carries high-speed data flows, consisting of many multiplexed channels. At the destination egress node, the traffic is de-segregated and delivered to the destination network. Core AOTN OXC switches are interconnected via a WDM optical transport network and perform forwarding of the optical data packets in the all-optical signal domain.

The security for AOTNs combines elements present in

---

<sup>1</sup>A lightpath may be carried over multiple wavelengths if wavelength conversion facilities are available within the AOTN.

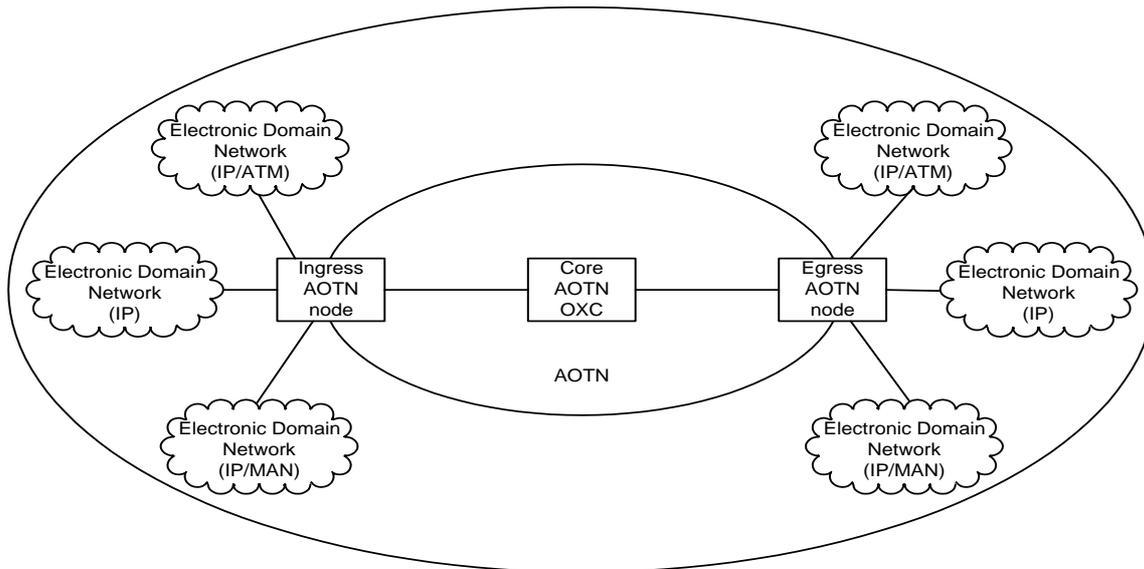


Figure 1: An architectural model for AOTN.

traditional electronic or electro-optic networks with additional aspects that are particular to AOTNs. For point-to-point TDM links and ring-based networks, SONET protection schemes are very mature and provide relatively secure transmission for commercial telecommunication carriers. However AOTN mesh networks based on WDM introduce extra complexity in providing security and survivability. Security concerns for AOTNs are not altogether different from those for conventional networks. However, there are several additional concerns mainly resulting from the physical device characteristics. Without overemphasizing the most obvious type of intrusion, viz., fiber cut, we limit the scope of this paper to outline the security issues in a framework that can be used subsequently for further analysis and modeling of attacks in AOTNs.

The rest of the paper is organized as follows. In Section 2, we present the architecture of an AOTN. A framework for fault and attack management is outlined in Section 3. We also discuss possible attacks on the optical layers, detection and localization, and protection/restoration issues. Finally, our conclusions are presented in Section 4.

## 2 AOTN Architecture

An AOTN introduces new physical components such as OADM and optical cross connect OXC that may change potential modes of attack from those that are known for electronic or electro-optic networks. For example, relatively high crosstalk between WDM channels within existing components can be exploited either to tap communications, or to perform service disruption by injecting mali-

cious signals into a network. Nonlinearities in fibers and devices can lead to undesirable cross-modulations, which may cause service disruption or subtle tapping attacks. Figure 2 represents a model of AOTN. A configuration of the AOTN is shown in Figure 2 (a) and a corresponding layered architecture for AOTN described in ITU-T G.872 [9] is shown in Figure 2 (b). A lightpath consists of a number of intermediate OXCs between the source and the destination nodes, interconnected by fiber segments, amplifiers and optional taps. The optical components that constitute an OXC include a switch (with or without wavelength conversion functionality), a demultiplexer comprising signal splitters and optical filters, and a multiplexer made up of signal combiners. A WDM node contains a transmitter array (Tx) and a receiver array (Rx).

The functionality of an AOTN can be decomposed into the following hierarchical layers (from top to bottom) [9]: Optical Channel (OCh) layer, Optical Multiplex Section (OMS) layer and Optical Transmission Section (OTS) layer. The OTS layer provides optical signal propagation functionality and represents the transmission medium, taps, and amplification modules. The OMS layer enables wavelength routing functions, and the OCh layer handles channels for information content. In the next section, we discuss faults and attacks in AOTNs and present our framework for their management.

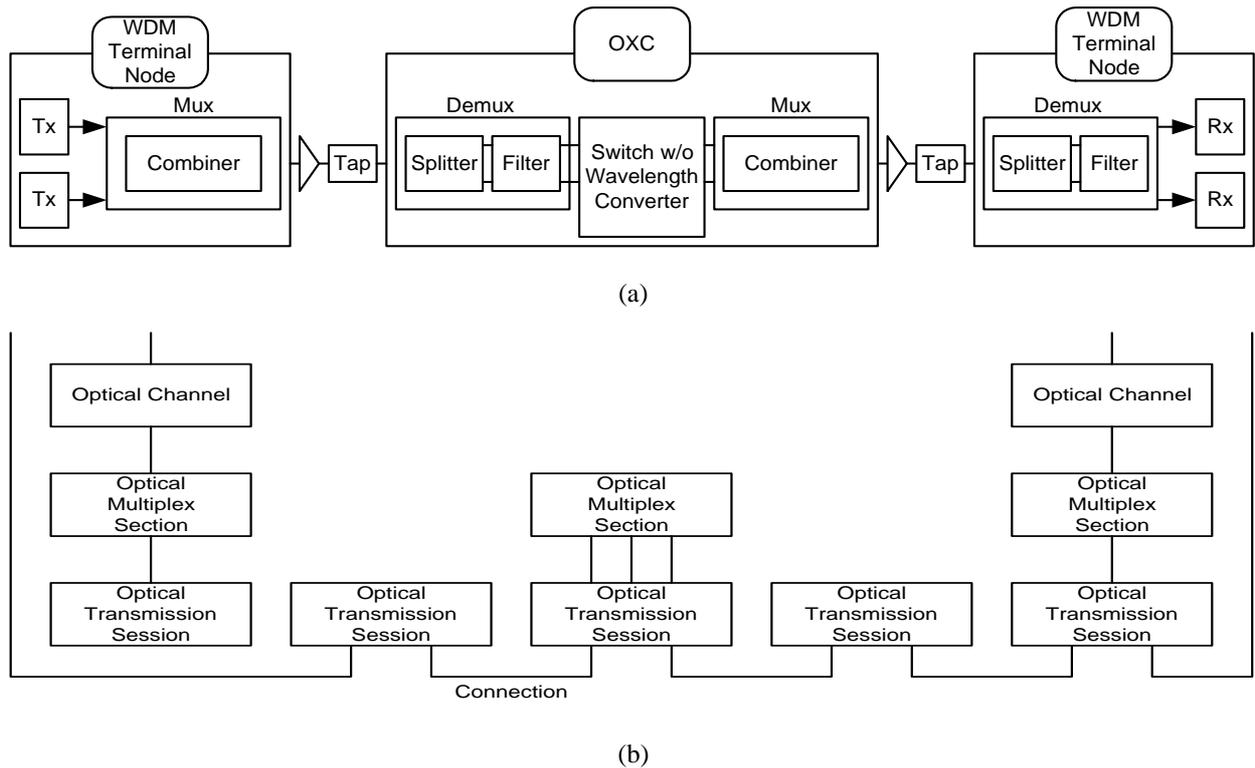


Figure 2: A model of AOTN.

### 3 A Framework for Fault and Attack Management

#### 3.1 Faults and Attacks

An optical signal undergoes many transmission impairments throughout its route. These impairments range from simple attenuation to complex nonlinear effects and polarization dependent losses. The peculiar behavior of the fiber transmission medium and active/passive elements in the network makes an AOTN vulnerable to unscrupulous attacks, thereby jeopardizing the security of information. These attacks may range from a simple physical access to the medium and its subsequent manipulation, to more complex exploitations of characteristics of optical devices on the link. The attacks related to the physical access of medium or devices are easier to detect and rectify. On the other hand, attacks exploiting device characteristics necessitate more involved diagnostic expertise, complex remedial measures, even more systematic detection schemes and control protocols.

There are several factors why optical networks require additional attention in terms of attack modeling. First, optical components and architectures have additional accessibility and vulnerability constraints. This is because any alteration in the optical signal due to easy access will pass

through subsequent elements. Second, the physical properties of transmission create unique opportunities for the determined attacker. The particular physical property of interest is the transparency of lightpaths. This refers to the fact that optical components along a connection do not process the optical signals. This transparency poses a threat that a signal can be forced into the network at a remote location and, by judicious choice of wavelength, affect many different parts of the network. Third, optical technology allows for different attack opportunities; for example, the crosstalk level in switches may be sufficiently low for normal operation but may not be low enough to prevent an attacker from transmitting a high-power jamming signal that would disrupt service.<sup>2</sup>

The management of attacks involves the protection of secure data. The security can be at the logical (or semantic level) (i.e., protect the information content of the data if an attacker is able to access them) or at the physical level (i.e., protect the data from being accessed/disrupted by the attacker) [12]. This paper is restricted to the physical security aspect. In general, fault and attack survivability in AOTNs can be summarized as illustrated in Figure 3.

<sup>2</sup>Conventional networks also exhibit cross-talk. On the other hand, all-optical switching in AOTN generates multiple orders of cross-talk that can potentially worsen the Quality of Service (QoS) as it propagates along different nonlinear elements.

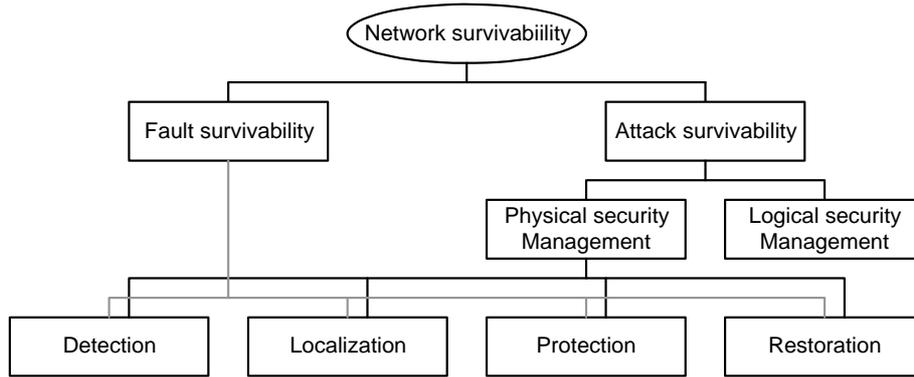


Figure 3: Network Survivability.

The main goals of fault survivability (fault management) are to set up routes in anticipation of faults (protection), locate the faults (detection and localization), and to re-route the affected connections (restoration). Protection is the primary mechanism used to deal with faults. In protection, preplanned protection resources (fibers, nodes, etc.) are set aside for restoring traffic when the working path is established. On the other hand, restoration dynamically discovers an alternate route from spare resources in the network for disrupted traffic, once a fault is detected. Fault detection is one of the crucial functions and may be a prerequisite for restorations. The inability of AOTNs to reconstruct data streams at nodes within transparent networks complicates segment-by-segment monitoring of communication links. Nevertheless, many common faults (such as fiber cuts and node malfunctions) may be detected by optical monitoring methods. On the other hand, a resourceful attacker may thwart detection with the relatively simple monitoring methods available now. Although research on attack survivability for AOTN is relatively scant, many interesting issues exist [12]. The following is a brief review of the literature in this area that we are aware of. Ramaswamy and Humblet [15] have analyzed amplifier induced crosstalk and saturation components that may be potentially used by an intruder for service disruption. Medard, Chinn et al. [13] have considered the case when an erbium doped fiber amplifier (EDFA) is under attack. The detection technique in [13] involves both optical and electronic signal processing, and is commercially non-feasible at this time. Zhou et. al. [19] and Gillner et. al. [5] provide extensive analysis of cross-talks on AOTNs. While unintentional crosstalk may result in an unauthorized access to critical information, it can also intentionally lead to disruption of service at the behest of a malicious attacker. Note that many of the traditional security problems related to logical security present in traditional electronic networks are still present in AOTNs. However, the approach for logical security (such as encryption, privacy and authentication) taking into con-

sideration AOTN physical characteristics opens up avenues for further research.

### 3.2 Conceptual Modeling of Attacks

Figure 4 shows a segment of an AOTN link with ports vulnerable to possible attacks numbered. We present here a brief description of transmission impairments and possible types of attacks each of these ports may experience.

#### 3.2.1 Fiber (attack point 1 in Figure 4)

An optical signal carrying high-speed data will experience attenuation, dispersion, non-linear effects and polarization dependent losses. While the use of amplifiers can solve attenuation, amplifiers also contribute additional impairments. The use of specific types of fibers (such as dispersion-shifted, polarization-maintaining fibers) may be suggested for reducing dispersion and polarization related degradations, but they, in turn, may introduce other problems such as crosstalk. Simple physical attacks like cutting of the cable can easily be detected by existing metrology techniques and can also be prevented by increasing physical security-related measures [8, 6]. On the other hand, providing easy physical access to the fiber cable can also cause unauthorized access and subsequent manipulation of the information by way of tapping or by sensing the optical mode leakage. In order to detect this kind of information, more sophisticated measurement techniques are needed.

#### 3.2.2 Tap (attack point 2 in Figure 4)

The purpose of providing taps is to facilitate easy monitoring, and providing efficient splicing ports for increased demand thereby adding flexibility to the network. Insertion loss and information leakage are associated transmission impairments which can again be eliminated by using amplifiers at the expense of additional vulnerability to attacks as we shall see next. Access to taps also provides an

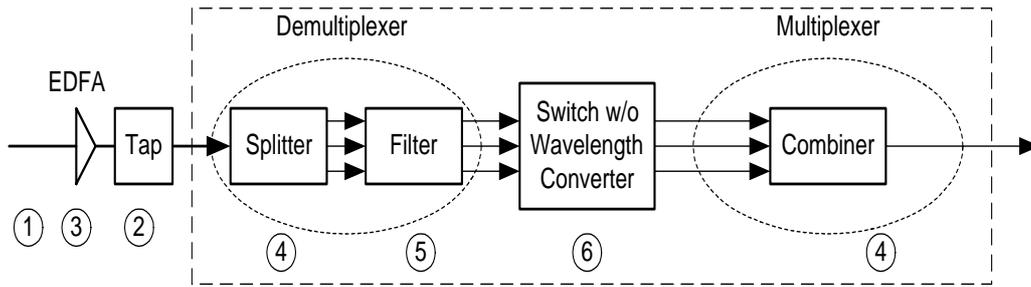


Figure 4: An Optical Cross-Connect (OXC) node.

opportunity to the attacker to have access to the signal and to tamper with it by way of either changing the signal power or signal polarization or similar signal properties. This can create problems for subsequent amplifiers and other polarization sensitive network elements and may result in service disruption. Such tampering can be thwarted by minimizing the number of taps and by increasing the physical security in order to prevent access, but detection of a tampered signal may not be easy.

### 3.2.3 Erbium Doped Fiber Amplifiers (attack point 3 in Figure 4)

Semiconductor optical amplifiers (SOA) have bandwidths of the order of 100 nm, which is much higher than those of EDFAs (35nm). On the other hand, it is possible to have high gains and output powers with EDFAs. Also, SOAs introduce severe crosstalk when used in WDM systems [16] and so EDFAs are widely preferred and used for AOTNs. In addition to amplified spontaneous emissions (ASE) and necessity for flattening the gain spectrum, EDFAs introduce a system penalty in the presence of other interfering channels. This system penalty can be decomposed into two components. The first component arises from the steady-state reduction in the amplifier gain due to the increase in the average input power. This is also referred to as the saturation component. The second component is the component arising from the variation in the gain due to the randomness of the total input power around the mean value. This is known as the crosstalk component [3]. It is known that when the number of channels is small, the cross-talk component dominates, but when the number of channels is large, the saturation component dominates. For high data-rate transmission (i.e., data rates much higher than the response time of the amplifier to a change in input power level), the cross-talk component is no longer present and only the steady-state gain reduction is retained [15]. An intruder may block transmission of other channels or can disrupt the entire service by exploiting this weakness of the EDFAs. Even a legitimate user can cause an attack by transmitting at high power levels so as to deteriorate EDFA performance. The

use of multi-stage EDFAs in a link requires extra precautions and system margins. One can detect this kind of attack by in situ verification of the following equality around the EDFA along the link or around the cross-connect or node (if it employs EDFAs as an integral part):  $\lambda_i = \lambda_o \pm \lambda_{d/a}$  where  $\lambda_i$  is total number of wavelength at the input of the “block” (can be an EDFA or an OXC node),  $\lambda_o$  is the total number of wavelengths at its output and  $\lambda_{d/a}$  is the total number of wavelengths dropped or added at the node by OADMs. One possible solution we propose to mitigate this type of attack is to equalize gain by way of pre-emphasis and de-emphasis as the case may be, before sending the signals to the EDFA. This can be done by optical processing or by electronic processing with their obvious inherent merits/demerits.

### 3.2.4 Splitter/Combiner (attack point 4 in Figure 4)

Typically, a demultiplexer comprises of an optical splitter followed by an optical filter. The power loss introduced by a splitter is its insertion loss. If the splitter itself also performs the function of a filter, it can cause signal degradation and can pose vulnerability to intentional attacks as described below for the case of a filter.

### 3.2.5 Filter (attack point 5 in Figure 4)

A good optical filter should have a low insertion loss. The loss should also be independent of the state of polarization of the input signals. The filter should be insensitive to variations in ambient temperature. As more and more filters are cascaded in a WDM system, the passband becomes progressively narrower. To ensure reasonably broad passbands at the end of the cascade, the individual filters should have very flat passbands. At the same time, the passband skirts should be sharp to reduce the amount of energy passed through from the adjacent channels. This energy is seen as crosstalk and degrades the system performance. Such crosstalk can also result in an unauthorized access to information. An intentional high power level may subsequently result in high crosstalk levels thereby blocking other legit-

imate users and can constitute an intrusion. This type of attack is not easy to detect and not easy to rectify on-line. Precautionary measures include power equalization before and after filtering and the use of high quality optical filters.

### 3.2.6 Switch (attack point 6 in Figure 4)

An optical switch also is subject to crosstalk due to non-ideal switching. When an interfering signal has been suppressed once with reference to the main signal, it results in a first-order crosstalk. If it is suppressed twice, it results in a second order crosstalk, and so on. Due to multiple switches and multiple nodes in a network, propagation of crosstalk becomes more and more complex. An intruder can also exploit polarization dependent properties of switches and filters to cause service disruption by way of manipulating the signal polarization. A legitimate user can also cause serious threats by changing transmitter power levels and thereby introducing intentional crosstalk to disrupt service or can utilize sensitive reception techniques to gain unauthorized access to the information from crosstalk. While equalizing power levels will eliminate the former type of attack, the latter type of unauthorized information access is not easy to detect. Non-blocking type of switches may also employ wavelength converters and thereby can also contribute to crosstalk in addition to the associated noise, insertion loss and polarization dependent losses.

## 3.3 Analysis of Attack Management

In this section, we describe attack management using the management section model illustrated in Figure 5. Figure 5 (a) shows the various management sections we propose, and Figure 5 (b) shows the sections at the OXC. With reference to the model shown in Figure 5, we categorize attack management issues at three functional levels, and they are discussed below.

### 3.3.1 Management of Direct Attacks

As discussed earlier, there are certain physical link elements with their own peculiar characteristics that are more likely to be exploited by an intruder as direct attack ports. This creates a need for comprehensive management tools at physical and upper layers. Table 1 summarizes sub-sections that fall under this category along with corresponding attack detection and isolation features.

Subsection	Characteristic Attack	Detection and Isolation Mechanism
TIS	1. Tapping only	Continuous monitoring of average power levels before and after the tap
	2. Tapping and jamming following signal processing	Difficult to decide whether anomaly or attack
	3. Jamming only	Difficult
OAS	1. Gain competition due to local attack	In-situ channel equality test, but difficult.
	2. Gain competition due to remote attack	
	3. Crosstalk	Difficult to detect as attack without electronic conversion (and subsequent BER measurements)
OTS	Fiber cut	Standard fault localizing metrology

### 3.3.2 Management of Indirect Attacks

There are certain sections that are unlikely to be attacked directly either because a direct attack is too complicated to generate the desired effect or because the ports are not easily accessible to the potential intruders. Although these are less likely attacks, their detection, isolation and restoration become too complex, costly and debatable. Table 2 summarizes management-related issues for such attacks.

Subsection	Characteristic Attack	Detection and Isolation Mechanism
DS	Intentional crosstalk	Complex
SS	1. Intentional crosstalk	
	2. Unauthorized access through add/drop ports	
MS	Intentional crosstalk propagation from preceding blocks	

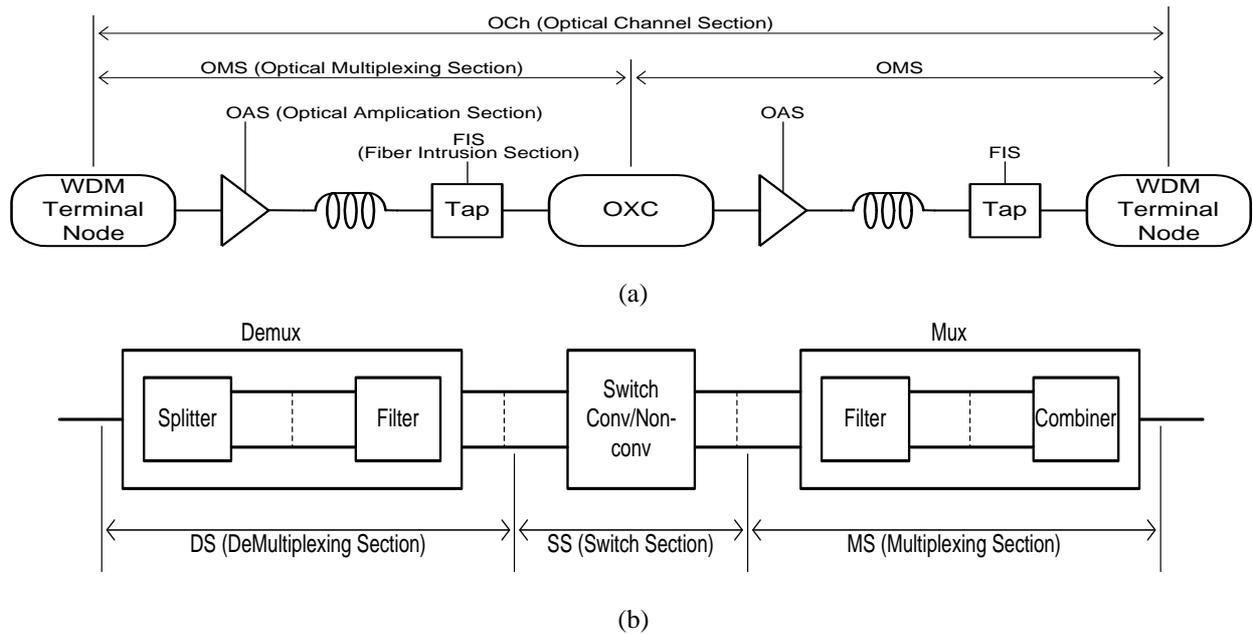


Figure 5: Management Sections.

### 3.3.3 Management of Pseudo-Attacks

In dynamically reconfigurable networks, the quality of the signals may change significantly depending on the design of the physical network. For example, the add/drop of an extra wavelength at an OADM may influence the quality of the signals on other wavelengths. These anomalies are not intrusions, but may be detected as attacks by intrusion surveillance algorithms. We call them as pseudo-attacks and these can be overcome in part or full by proper design implementation.

### 3.4 Detection and Localization

The detection of faults and attacks could potentially be faster at the optical layer than at higher layers. However, monitoring signals at the optical layers is usually limited to power and signal spectra measurements. No robust standard or technique exists to date for monitoring the network performance or for detecting faults and attacks at the optical layers. Recently, several schemes have been proposed for monitoring transparent optical channels (i.e., lightpaths): (1) monitoring optical channel continuity [14] through laser bias currents or the optically received or transmitted power levels, and (2) monitoring optical channel quality [10] through error-detecting codes, sampling methods, spectral methods, and indirect methods. Among these schemes, error-detecting codes are the best for estimating the bit error rates (BERs), but they require access to the electrical signals. Sampling methods are the most accurate for monitoring signals at the optical level. However, they

are too difficult and complicated to be used in every network element. The spectral time averaging methods are simpler but ignore all distortion aspects, and are thus very inaccurate. Although standards based on these schemes are likely to emerge in the future, there has been some research on adapting schemes for electronic networks. For instance, attack detection and management schemes for amplifiers and fibers have been proposed in [2] and [13]. Fault/attack localization refers to the identification of the faulty component or source of attack. Very little is understood about this topic in AOTNs at this time. It is expected that sophisticated distributed algorithms would be required to accurately and precisely identify the location of faults. Attack localization is even more challenging because attacks may propagate and affect several lightpaths over a wide geographical area.

### 3.5 Protection and Restoration

#### 3.5.1 Optical Layer Level

Protection at the optical layers may be provided either at the OCh level or the OMS level in WDM ring networks. In the OCh protection approach, a failed lightpath may be fixed by converting an optical signal from a given wavelength into a different one, avoiding the rerouting of the signal.<sup>3</sup> This is equivalent to span routing in SONET, with the difference that even two fiber WDM rings can provide such

<sup>3</sup>For example, this may be done when a transmitter or a switch in an OXC at a particular wavelength fails.

capability for OCh protection. Note that recent contributions to the ANSI T1X1.5 committee emphasize the need for automation of the OCh layer to establish optical channels in real time and provide a variety of protection levels depending upon user demand, ranging from 1+1, 1:1, to 1:N [14]. In the OMS layer, however, span protection will require four fiber rings, as in SONET. These extra features will undoubtedly introduce extra complexity in the optical layer automatic protection switching (APS) protocols. Because of the multiplicity of alternate routes, efficient protection in mesh networks is more complex. To date, large-scale efforts are underway to develop standards that will run the fault (related to some kind of attacks) recovery function at WDM optical layers [10]. Within the optical layers, survivability mechanisms will continue to offer the fastest possible recovery from fiber cuts and flexible management of protection capacity. However, optical protection/restoration schemes are still in their infancy and it will take some time for standards to emerge. Overall, it is expected that WDM network survivability schemes will mirror SONET survivability schemes, implying both protection and restoration [11].

### 3.5.2 Electrical Level

One of the problems with pure optical transparency is that electronic frame-monitoring schemes cannot be applied in the AOTN's core to detect/localize faults and some kinds of attacks. Optical monitoring schemes for transparent optical channels are currently under investigation and standards are expected to emerge in the near future. Meanwhile, the frame-monitoring layer (i.e., optical adaptation layer) between the WDM optical layer and the higher layer (e.g., IP layer) can be used for fault and attack detection and localization. However, per-channel monitoring inside the AOTN core will likely require some processing overhead such as O-E conversion and frame monitoring taking signaling into consideration (i.e., in-band or out-of-band signaling mechanism). In OIF and ANSI T1X1.5, the proposals for implementing frame-monitoring layer overhead information include the use of a TDM frame-like "SONET-lite" [18] or "digital wrapper" [1] to support OCh layer management functions such as performance monitoring, connectivity, and fault/attack indicator monitoring.

### 3.5.3 Control Protocol Level

Each of the IP/MPLS layer, adaptation layer, and the optical layer incorporates its own protection and restoration functions. Basically, the IP/MPLS over WDM framework provides three schemes according to protection/restoration granularity: fiber protection/restoration at the OMS level, channel protection/restoration at the OCh layer, and flow protection at the IP/MPLS layer. IP layer protection scheme

uses traffic rerouting when failure or attack occurs inside the working entity. Within the MPLS framework, IETF draft [7] considered LSP restoration schemes. In this approach, in order to improve susceptibility to node and link faults (related to attack problems), hop disjointed backup routes can be used [6]. Although MPLS promises IP-layer protection with fast restoration and path switching, the Internet draft [19] comments that fast recovery is still hampered by Label Switched Path (LSP) failure detection. For example, even a single fiber cut or node failure will affect multiple LSPs, which means that hundreds of ingress routers of LSPs should be notified. Multiple LSP failures also lead to even more Label Switch Routers (LSRs) to update the topological and forwarding information. Within the MPLS framework, fiber-level protection schemes can be employed to improve this kind of scalability problem by using link-based LSP restoration concept in conjunction with the MPLS label stacking function. Nevertheless, this solution requires additional fiber diversity provision and fiber cut/switchover event. On the other hand, network service survivability within IP/MPLS over WDM requires that the survivability at optical layers very carefully could coordinate with the functions already provided by existing network layer protocols (ATM, SONET/SDH, etc.). In summary, in order to achieve maximum network survivability in optical MPLS networks, the implementation of protection/restoration, fault and attack detection and localization must be coordinated at both IP/MPLS layer and WDM optical layer.

## 4 Conclusions

Fault and attack management in AOTNs is critical because of high data rates. Attacks exploiting device characteristics may require involved diagnostic expertise and complex detection and restoration procedures. In this paper, we provided a basic framework for attack management in an AOTN. We discussed possible attack scenarios at the physical layer and presented a conceptual modeling of attacks and possible protection schemes in AOTNs. Our future research will deal with the issue of practically feasible attack management and its modeling based on this preliminary work. Our work should give insight into the broad concerns of additional management functions involved in all-optical transport networks.

### Acknowledgement

This work was supported in part by the DARPA under SPAWAR grant N66001-00-18949 (co-funded by NSA).

## References

- [1] P. Bonenfant, J. Ballintine, and G. Newsome, "Optical Transport Networking with 'Digital Wrappers,'" Optical Internetworking Forum OIF 99.011, Jan. 1999.
- [2] L. Chung-Sheng and R. Ramaswami, "Automatic Fault Detection, Isolation, and Recovery in Transparent All-Optical Networks," *IEEE Journal of Lightwave Technology*, vol. 15, no. 10, Oct. 1997, pp. 1784-1793.
- [3] E. Desurvire, *Erbium-Doped Fiber Amplifiers: Principles and Applications*, John Wiley & Sons, Inc., NY, 1994.
- [4] N. Ghani and S. Dixit, "Channel Provisioning for Higher-Layer Protocols in WDM Networks," *Proceedings of the SPIE All Optical Networking Conference: Architecture, Control, and Management Issues*, Boston, MA, September 1999.
- [5] L. Gillner, C. P. Larsen, and M. Gustavsson, "Scalability of Optical Multiwavelength Networks: Crosstalk Analysis," *IEEE Journal of Lightwave Technology*, vol. 17, no. 1, Jan. 1999, pp. 58- 67.
- [6] B. Griffiths, "Developments in and Applications of Fibre Optic Intrusion Detection Sensors," *Proceedings of 29th Annual 1995 International Carnahan Conference on Security Technology, Institute of Electrical and Electronics Security Technology*, 1995, pp. 325 -330.
- [7] D. Haskin and R. Krishnan, "A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute," IEFT Draft draft-haskin-mpls-fast-reroute-01.txt, June 1999.
- [8] J. P. Hazan, M. Steers, G. Delmas, and J. L. Nagel, "Buried Optical Fibre Pressure Sensor for Intrusion Detection," *Proceedings of 1989 International Carnahan Conference on Security Technology*, 1989, pp. 149 - 154.
- [9] ITU-T Rec. G.872, "Optical Transport Networks," Feb. 1999.
- [10] C. P. Larsen and P. O. Anderson, "Signal Quality Monitoring in Optical Networks," *Optical Networks Magazine*, vol. 1, No. 4, Oct. 2000, pp. 17-23.
- [11] J. Manchester, P. Bonenfant, and C. Nowton, "The Evolution of Transport Network Survivability," *IEEE Communications Magazine*, vol. 37, no. 8, Aug 1999, pp. 44-51.
- [12] M. Medard et. al., "Security issues in all-optical networks," *IEEE Networks*, pp. 42-48, May/June 1997.
- [13] M. Medard, R. Chinn, and Saengudomlert, "Attack Detection in All-Optical Networks," *Technical Digest of Optical Fiber Conference (OFC)*, 1998, pp. 272-273.
- [14] L. E. Nelson, S. T. Cundiff, and C. R. Giles, "Optical Monitoring using Data Correlation for WDM Systems," *IEEE Photonics Technology Letters*, vol. 10, No. 7, Jul. 1998, pp.1030-1032.
- [15] R. Ramaswami and P. A. Humblet, "Amplifier Induced Crosstalk in Multichannel Optical Networks," *IEEE Journal of Lightwave Technology*, vol. 8, no. 12, Dec. 1990, pp. 1882-1896.
- [16] R. Ramaswami and K. N. Sivarajan, *Optical Networks: A Practical Perspective*, Morgan Kaufmann Publishers, Inc., CA, 1998.
- [17] S. Shew, "Fast Restoration of MPLS Label Switched Paths," Internet draft, work in progress, June 1999.
- [18] J. Sosnosky and Z. Lin, "Planning for Broadband Multilayer Survivability," T1X1.5, May 1999.
- [19] J. Zhou, R. Cadeddu, E. Casaccia, C. Cavazzoni, and M. J. O'Mahony, "Crosstalk in Multiwavelength Optical Cross-Connect Networks," *IEEE Journal of LightwaveTechnology*, vol. 14, no. 6, June 1996, pp. 1423-1435.