REAL TIME SECURING OF ALL-OPTICAL NETWORKS AGAINST SECURITY ATTACKS AT THE PHYSICAL LEVEL

Fahmida Rahman[1] and Mohammed Arozullah[2]
Department of Electrical Engineering and Computer Science, The Catholic University of America, Washington, D.C. 20064, USA
[1]fahmida_irin@yahoo.com
[2]arozullah@cua.edu

ABSTRACT

This paper deals with protecting all-optical networks (AON) from security attacks at the physical level. It firstly presents an overall high level protocol for establishment, management and on-the-fly restoration of optimal secure lightpaths established by applying constraint-based open shortest path first (OSPF) source routing using proposed security databases of components. Secondly it presents a protocol for using fiber diversity between adjacent nodes to protect against attacks on fiber links. Thirdly it presents analytical models of propagation of security attacks on optical amplifiers and switches. These models are then used to develop security envelopes around these components, to calculate security indices and on-the-fly real-time restoration of components in case of an attack. Fourthly it presents simulation results for evaluation of the performance of these on-the-fly restoration schemes. These on-the-fly restoration schemes eliminate need for tearing down of attacked lightpaths and prevent consequent loss of large amount of data.

KEYWORDS

All-Optical Network Security, erbium-doped fiber amplifier (EDFA) gain adjustment, Optical Switch crosstalk

1. INTRODUCTION AND BACKGROUND

All-optical networks differ from other optical networks in the sense that AONs consistof mainly optical components, provide data transparency and do not use any optical-to-electronic conversion throughout the network. Such special features provide higher bandwidths and greater data rates in AON than in electro-optical networks. However these characteristics also provide greater security risks in these networks. Although AONs may suffer from the attacks typically performed in traditional electronic and electro-optic networks, security issues in AONs are significantly different from those of the traditional networks. Due to data transparency, high data rates of light-paths, lack of regeneration,unique characteristics of high crosstalk and cross modulation in optical devices, attacks in AONs spread quickly through links attached to an attacked node without detection.This results in loss or compromise of large amount of data and may lead to disabling of portions of a network. This is not the case in electronic or opto-electronic networks where regeneration prevents propagation of attacks [1].Therefore, attack detection and network restoration in AON is different from those in electro-optic or electronic networks and deserves special consideration and solution.

DOI : 10.5121/ijnsa.2013.5401

The three primary AON components that are vulnerable to security attacksare optical amplifiers, fibers and optical switches. These optical components are specifically prone to gain competition and crosstalk respectively. Crosstalk causes signalin one channel to leak into unintended channels producing interference toother optical signals passing through the AON. Optical switches and other similar components exhibit high crosstalk due to non-ideal demultiplexing and space switching. Coherent crosstalk in wavelength routers, for instance within wavelength selective switches for WDM systems, can allow an illegitimate user on a particular channel on one fiber (i.e., attacker) to jam another user on the same wavelength on a different fiber, which is known as *in-band jamming attack*. Thus an in-band jammer who injects a signal on a single wavelength into a link using high power transmitter can destroy many signals on that wavelength since channels of the same wavelength from different fibers share the same switching plane. An attacker, a person internal to the network oran external remote person, can disrupt the operation of an optical node by exploiting these cross-talk characteristics of switches by injecting a very high power attack signal through the wavelength selective switch [2]. A second type of attack, known as *gain competitionattack*, exploits gain competition property of optical amplifiers.If an attacker injects a strong signal at a wavelength outside the communication band, but within the passband of the amplifier then the gains of the legitimate signals may be reduced considerably. The attack can work because the amplifier cannot distinguish between attack signals and legitimate signals and provides gain to each signal indiscriminately in proportion to its strength from a finite supply of gain. As a result the legitimate signals become weaker and weaker.The gain competition attack, also known as *out-of-band jamming attack*, can result in denial of service tolegitimate users. In some instances, it may be possible to deny service to manyusers from a legitimate network access point via the gain competition attack [2].

To foil the in-band and out-of-band jamming attacks in AON, some preventive countermeasures have been proposed in [1], [2], [3], [4], [5], [6], [7], [8], [9] and [10] which are primarily focused on detection and attack localization, i.e., reactive approach. Three types of preventive countermeasure categories are primarily focused in [1]: 1) incorporating band limiting filters to thwart signals outside certain band to prevent out-of-band gain competition and reducing vulnerabilities intrinsic to hardware, 2) providing anti-jamming transmission schemes such as CDMA or TDMA that are hardened for anti-jamming and anti-tapping measures and 3) protocols and architecture designs adapted to AONs, such as avoiding compromised link for sensitive communications. Although [1] mentions some suggestions for preventive measure, these suggested preventive countermeasures are not implemented as a secured system and therefore, there is no in-depth discussion about how to implement these ideas, what challenges may arise through adoption of such security measures and how much security they may provide to AONs.The concept of attack aware network planning has also been proposed in [11], [12], [13] and [14]. In [11], the propagation of high-power jamming attack is stopped by using power equalizers in different nodes, which suggests placing the optical attenuators within optical components.

This paper deals with incorporating security in AONs using both proactive prevention techniques and reactive on-the-fly restoration techniques.Establishment and restoration of secured lightpaths are performed using three major steps as shown in Figure 1: generation and management of component security database at source nodes, establishment of secured lightpath, and partial restoration of lightpathin case of an attack. First, security indices representing security risk factorsof componentsare calculated and security databasesare created for the AON infrastructure.

Thesesecurity databases provide a basis for establishing the secured lightpath. Second, initially aconstraint based routing algorithm,using the security databases,computes the most secured lightpath from a source to a destination passing through the most secure components of the AON. Fiber diversity between adjacent nodes on a secure lightpathis used to provide redundant lightpath to protect against attacks on fibers.Third, on-the-fly approach of partial restoration is adopted to restore the lightpath when attack happens in the components. The partial restoration is effected by providing security envelopes around vulnerable components. The on-the-fly restoration of lightpathsensures minimum loss of data and avoids the need for tearing down the attacked lightpath and establishing a new one.The later process may be time consuming and undesirable in many circumstances.

The proposed restoration methods involve using additional devices to provide the security envelopes. This may entail additional expenses. Thus the use of such devices in all the nodes may not be economically feasible. However, it is important to note that unchecked attacks may spread through a considerable part of a network and cause loss of large amount of data. The cost of losing large amount of data and tearing down and reestablishing a lightpath may be considerable too. In any case the use of additional devices for restorationshould be minimized and these should be placed in selective nodes only. Reference [11] presents a method for selecting such placements. The results in [11] can be used forproper placement ofsecurity envelopes proposed in this paper.

The rest of the paper is organized as follows.Section 2 presents overall high level protocols for security hardening of AON, generation, management and updating of component security databases at source nodes, constraint based secure lightpath calculation, and attack monitoring and restoration of attacked components. Section 3 discusses details of analytical modeling, security index calculation and setting up and operation of security envelopes for on-the –fly restoration of attacked components optical amplifiers and optical switches. It also presents protocol for protection against attacks on fibers by using fiber diversity between adjacent nodes on a lightpath. Section 4 discusses conclusion of the paper.

2.OVERALL PROTOCOL FOR SECURITY HARDENING OF AON AGAINST ATTACKS AT THE PHYSICAL LEVEL

The secured AON in our project integrates AON architecture, management, control and lightpath establishment. The secured AON is based on redundancy, rerouting, security status of components and constraint based source routing. As explained earlier, attacks in AON produce high crosstalk and gain robbing in the components such as optical switch and optical amplifier. These attack-related characteristics are studied in depth to detect whether optical components are under attack. We maintain a history of attacks of the components of AON networks in a database. During the lightpath computation, the database comprising history of attacks is considered to generate a possible attack free route for the lightpath. Next, the optical data is sent on the redundant path of computed lightpath. During lightpath travel, if any component of the route is under attack, then an on-the-fly partial restoration is performed to continue the transfer of optical data instead of tearing the lightpath. In our study, we assumed the following assumptions for our proposed AON system: at least two parallel fibers between each and every adjacent nodes are available to provide redundant route, source nodes are capable of performing constraint based routing decisions, and each intermediate node is capable of implementing the routing decision

provided by the source node. In summary, the overall protocol consists of the following steps shown in Figure 1. The detailed workings of the various operations shown in Figure 1 are presented in the following section.

2.1. Generation and management of component security databases at source nodes

The source nodes in the AON store component security databases similar to the one shown in Figure 2. The database consists of current security status of the components in the AON. Any time the security status of a component changes the database is updated through the exchange of messages between the relevant components and source nodes. The database and protocols to exchange the

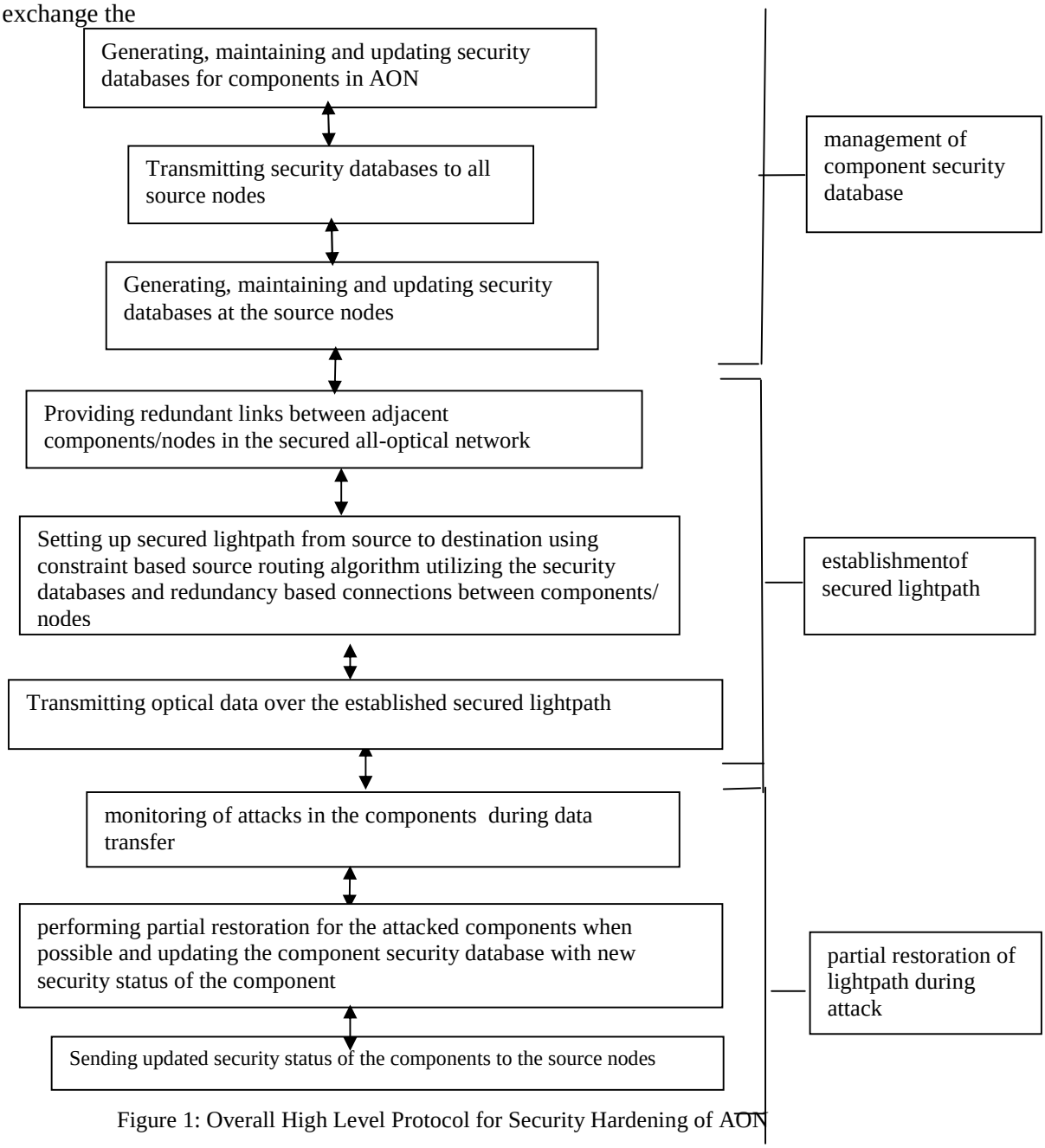

Figure 1: Overall High Level Protocol for Security Hardening of AON

security status information can be performed in electronic domain. At any instant of time the components of AON have one of multiple security states, such as, secured, attacked and restored. These security states are monitored locally at the components and are sent to the source nodes for recording in the database. The status information may be updated periodically or during any change of any state. Figure 2 shows the typical security database with three possible security states for a component: secured, restored or attacked. The attacked components have the highest security indices and the secured components have the lowest indices.

Components	Security condition	Security index
OA #1	Secured	1
Switch	restored	3
OADM #1	Attacked	7
OA #2	Secured	1

Figure 2: Typical security database at a source node

2.2.Protocol for calculation of route of secured lightpath based on component security indices in security database at source nodes

For any lightpath requestfrom a user, the relevant source node computes the optimal secured route by using constraint based Open Shortest Path First (OSPF) routing algorithm. Open Shortest Path First (OSPF) algorithm calculates the optimal shortest path from a source to a destination by considering link weights of the links between adjacent nodes on the lightpath.Usually link weight represents the length of the link. However, in this paper the security states of the components have been incorporated in the link weight as shown in equation 1 below.
Link weight = f(security status, distance)

= A * [(security index of component at the beginning of the link + security index of thecomponent at the end of the link)/2] * distance between the two components, where A is a security weight for the link (1)

Figure 4 shows optimal route calculation for an example network with the link weights shown on the corresponding links of a number of paths from a source node to a destination node. Given the security database and the distances, the link weights are calculated using equation 1. The OSPF algorithm calculates the total link weights of the various paths. Path 2 is selected as the optimal path as it has the least total link weight from the source to the destination. The flow chart of calculation is shown in Figure 3.The highlighted path in Figure 4 is selected as the optimal lightpathsince the sum of link weights of the links on this path is smallest of the sum of link weights over all other paths.

2.3.High level protocol for securing lightpath from attacks on fibers using fiber diversity between adjacent nodes

After the optimal secured lightpath has been computed, two different optical links on two different parallel fibers are used to send data from one node to the next node on the lightpath. This redundancy does not cost much since many unused optical wavelengths and fibers are

available in the optical network. This fiber diversity process provides security against attack on fibers since it is highly probable that attack may occur on one fiber but not on both. At every step of transmission strengths of the two received optical signals at a receiving node are measured and the better of the two received signals is accepted. Then the accepted signal is transmitted to the next node on the lightpath over two parallel fibers. This process is repeated until the signal reaches the destination node. In addition, the nodes can maintain a history of attacks on these wavelengths and fibers. Figure 5 summarizes the fiber diversity based data transmission in a secure lightpath.

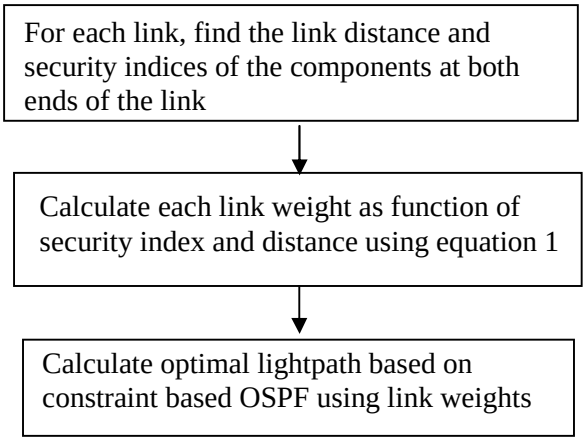

Figure 3: Flow chart of constraint based source routing to select optimal lightpath

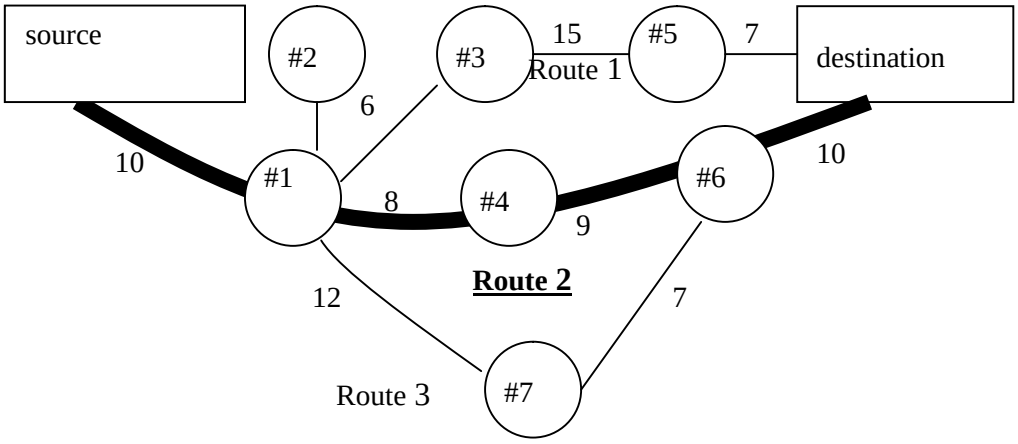

Figure 4: Calculation of secured lightpath from a source to a destination in an example network

2.4.Attack monitoring and lightpath restoration in the optical nodes/components

The AON components, such as amplifiers and switches, can be attacked during light path traverse. There is an attack monitoring scheme in each component and a temporary restoration will be performed during attack so that light path has not been teared down due to possible attack and adverse scenario, which will be described shortly. The flowchart in Figure 6 provides the basic operation of our secured AON architecture.

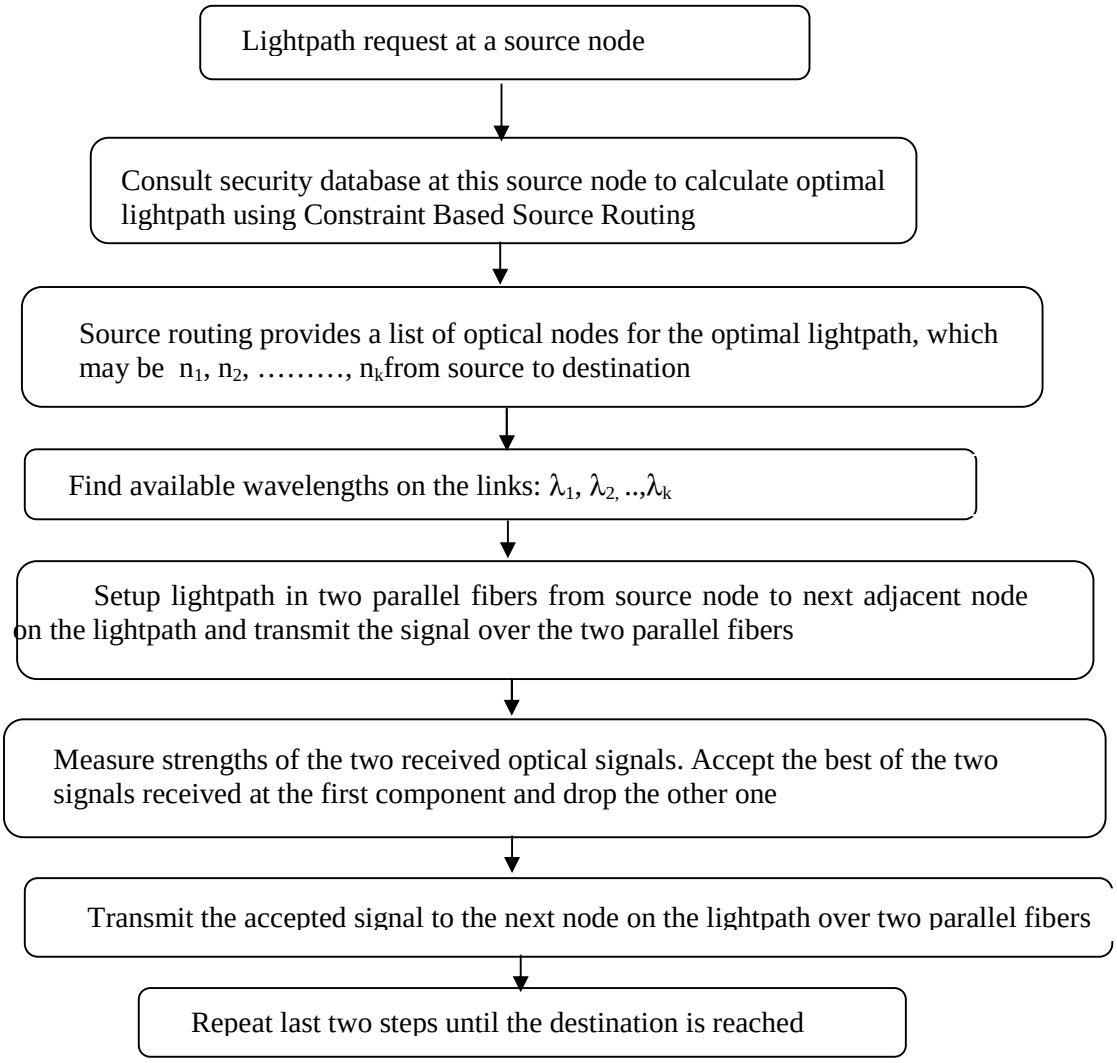

Figure 5: Fiber diversity based data transmission in secure lightpath

3.ATTACK MONITORING, SECURITY INDEX CALCULATION AND ON-THE-FLY RESTORATION OF ATTACKED COMPONENTS USING SECURITY ENVELOPES AROUND THEM

Constraint based source routing algorithm uses the security indices of components to compute the route of light paths. Security index of a component indicates whether the component is attacked, restored or never attacked. Detecting attack in components depends on the properties of the respective component. This paper presents use of analytical models of operation of two components, namely EDFA optical amplifier and optical cross-connect (OXC) to develop

security envelopes around them. These security envelopes, in turn, are used to compute security indices and for on-the-fly restoration of these components during attack condition. In this section is presented details of protection and restoration against physical level attacks on EDFA optical amplifiers, OXC and fiber links.

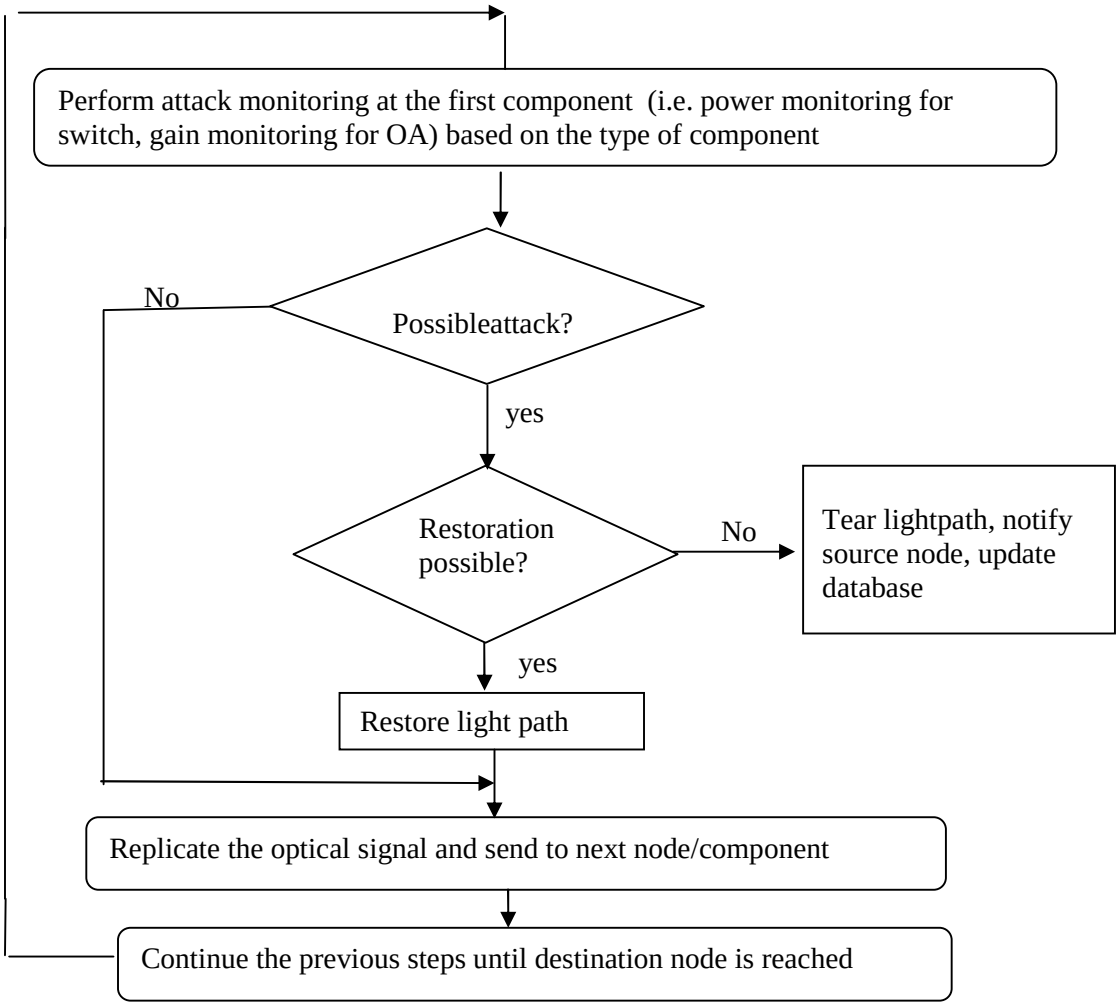

Figure 6.Attack monitoring and restoration in the components in light path

3.1.Attack monitoring, security index computation and on-the-fly partial restoration in Erbium Doped Fiber Amplifier (EDFA)

The out-of-band jamming attack in optical amplifiers, also known as gain robbing or gain competition attack, reduces the strength of legitimate signals. This may lead to denial of service to these legitimate users. This is illustrated in Figure 7. One possible solution is to locate and remove the source of attack signal. However, in real life, detection,location and removal of an attack signal is time consuming and difficult. In a high data rate network like AON a lot of data may be lost or damaged during this time.Since gain robbing attack of EDFA does not totally

destroy the legitimate signals, it will be better if the strength of these signals can be increased by on-the-fly compensation of the gain of the EDFA. This way loss of data can be minimized and the need for tearing down and reestablishment of lightpathis avoided. In this section such a system is presented.In this system the EDFA system is monitored for attack signals and extra pump power is provided on-the-fly when attack signal robs the gain of the legitimate signals.

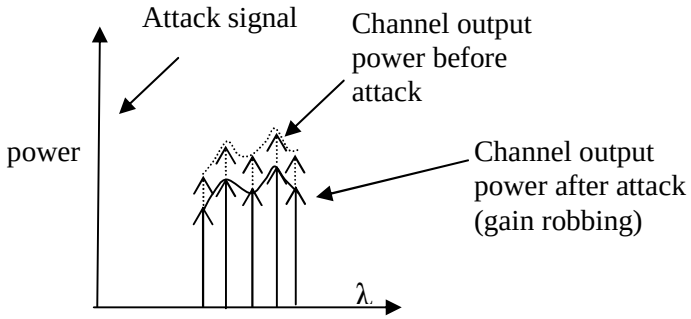

Figure 7: EDFA attack and gain robbing

3.1.1. Analytical model for EDFA and operation of security envelope used for attack monitoring and on-the-fly restoration of gain

Figure 8 shows the model of security envelope used for monitoring attack and adjusting gain during attack. The control signal P_k^{in} is added to the multiplexed input signal ΣP_{sin}via an add element. The combined signal is amplified by the EDFA. A drop element is employed to separate out the control signalP_k^{out}. Examples of available add and drop elements, such as channel selectors/circulators, can be found in [15]. Next, the controller calculates the required input to the pump power generator to produce appropriate amount of pump power. This proper pump power is used to adjust the gain of EDFA.

For attack monitoring, a monitor signal P_k^{in} is introduced in the optical light path of EDFA. The monitor signal is provided as a control channel in the lightpath and the corresponding output signal P_k^{out} is continuously monitored by the system for detection of possible attack. When there is a possible attack, the value of P_k^{out} is decreased because of the gain decrease. Then the EDFA and the corresponding lightpathwould be restored on-the-fly by increasing gain of the legitimate signals by increasing pump power.Controller decides about the attack based on gain reduction of the control channel.The attack monitoring and partial restoration in multi-channel amplification in EDFA can be explained with the following two equations (3) and (4). Controller controls the pump power based on equation (4) provided below. If an attack on an EDFA is confirmed then the source databases containing security indices of component is updated with new status of the EDFA.

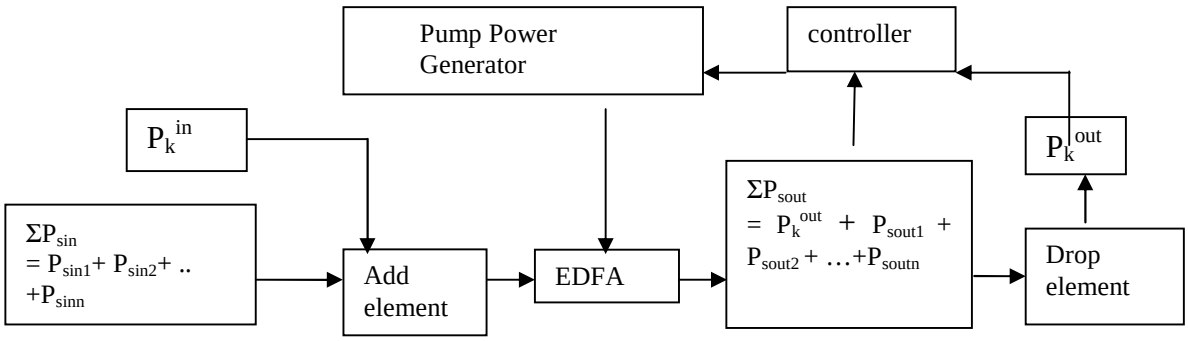

Figure 8: Security envelope for attack monitoring and on-the-fly gain restoration during attack

In EDFA the pump power excites electrons in Erbium atoms from lower to higher energy levels. For any EDFA with cross-section area A, Chinn in [16] develops the differential equation for the upper state population density N_2. The value of steady state upper level population $N_2$is given by equation (2), where τ is the lifetime, P_p is pump power, P_i is i^{th} signal power, Γ_p ,Γ_s are confinement factors for pump channel and signal,σp_a is the absorption cross-section for pump, σi_a is the absorption cross-section for i^{th} signal, σi_e is the emission cross-section for i^{th} signal, ν_i, ν_p are optical signal and pump frequencies and h is Plank's constant.

$$N_2 = [\tau P_p \Gamma_p \sigma_{p_a} / h\nu_p A + \sum_i P_i \Gamma_s \sigma_{i_a} \tau / h\nu_i A] / [1 + \tau P_p \Gamma_p \sigma_{p_a} / h\nu_p A + \sum_i \{\tau P_i \Gamma_s (\sigma_{i_a} + \sigma_{i_e}) / h\nu_i A\}] \quad (2)$$

Equation (2) provides relationship among steady state N_2, pump power P_p and signal power P_i. Accordingly, if one channel in the input signal becomes stronger, the total input power $P_i$becomes higher and N_2becomes lower. This phenomenon is known as gain saturation. An attacker can exploit the gain saturation property of EDFA by inserting a strong so that the legitimate signals can be deprived of the photons. However, according to equation (2), if input power changes, the corresponding change of pump power can compensate for loss of N_2. Therefore, it is possible to maintain the gain of the legitimate channels by providing extra pump power when attack is detected. Such a temporary restoration of gain of the legitimate signals maintain light path for data transfer, which is necessary to minimize data loss. For multi-channel EDFA, different wavelengths have different gains. When total input power of the optical signal with multiple beams increases, the gains of the individual beams decrease due to gain saturation property of EDFA. Thus, when an attack signal has high power, total input power increases and individual gains of the different channels, including the control channel, decrease. The gain of control signal can be monitored for attack detection by the controller of Figure 8 to determine whether gain of the control signal is dropped to a predetermined minimum. In this case, the EDFA node can be considered as attacked. The security index database at sources can then be updated with this new security index. Then a new lightpath can be created for next data transfer while maintaining current data transfer in the current lightpath.

An EDFA amplifier of length L with a density of Erbium ion ρ within an active volume of cross sectional area A is considered. An arbitrary beam with wavelength λ_k and input power P_k^{in} traveling through the amplifier has the following output power [17]:

$$P_k^{out} = P_k^{in} \exp[-\alpha_k L] \exp[(P_{in} - P_{out})/P_k^{IS}] \quad (3)$$

where $P_k^{IS} = A/\Gamma_k(\sigma^k_e + \sigma^k_a)\,\tau$, known as intrinsic saturation power, σ^k_e , σ^k_a are the stimulated emission and absorption cross section at wavelength λ_k, Γ_k is the confinementfactor of the amplifier at wavelength λ_k for the amplifier,$\alpha_k = \rho\Gamma_k\sigma^k_a$, is the absorption constant and τ = the spontaneous lifetime of the upper level.

Total input power: $P_{in} = \Sigma_{j=1,\,N} P_j^{in}$ and total output power: $P_{out} = \Sigma_{j=1,\,N} P_j^{out}$
For control channel k, the equation (3) can be written as:
$g_k = \exp[-\alpha_k L]\,[\exp(P_{pin} - P_{pout})/P_k^{IS}.\ \exp(\Sigma P_{sin} - \Sigma P_{sout})/\ P_k^{IS}]$
where $g_k = P_k^{out}/P_k^{in}$, ΣP_{sin} = total signal input power, ΣP_{sout} = total signal output power, P_{pin} = pump input power and P_{pout} = pump output power
Define,$P_{pin} - P_{pout} = \Delta P_p$ and $\Sigma P_{sin} - \Sigma P_{sout} = \Delta P_s$
If one signal among the existing signals gets stronger, gain changes from g_k to g_k' andΔP_s changes to $\Delta P_s'$. Then, $g_{k'} = \exp[-\alpha_k L]\,[\exp(\Delta P_p)/\ P_k^{IS}.\ \exp(\Delta P_s')/\ P_k^{IS}]$
Thus, $g_k / g_{k'} = (\exp[\Delta P_s/\ P_k^{IS}])\ /(\exp[\Delta P_s'/\ P_k^{IS}]) = \exp([\Delta P_s/\ P_k^{IS}] - [\Delta P_s'/\ P_k^{IS}])$
Assuming that, new pump power P_{pin}' changes the gain back to its original value and the corresponding power difference changes to $\Delta P_s''$.
$g_k'' = \exp[-\alpha_k L]\,[\exp(\Delta P_p')/\ P_k^{IS}.\ \exp(\Delta P_s'')/\ P_k^{IS}]$, where $\Delta P_p' = P_{pin}' - P_{pout}'$
Then, $g_k = g_k''$, which gives the following relationships:
$\Delta P_s - \Delta P_s'' = \Delta P_p' - \Delta P_p$
Again,$\Delta P_s'' - \Delta P_s' = \Sigma P_{sout}' - \Sigma P_{sout}''$
If k is the control channel and g_k, $g_k'$are known then,
$g_k / g_{k'} = \exp([\Delta P_s/\ P_k^{IS}] - [\Delta P_s'/\ P_k^{IS}])$
$= \exp[(1/\ P_k^{IS})\,(\Delta P_s - \Delta P_s')]$
$\ln g_k / g_{k'} = (1/P_k^{IS})\,(\Delta P_s - \Delta P_s')$
Thus, $\Delta P_p' - \Delta P_p = \Sigma P_{sout}'' - \Sigma P_{sout}' + P_k^{IS} \ln g_k / g_{k'}$
By selecting suitable parameters, pump output power can be made negligible. For simplification, it is assumed that pump output power is zero. Such an assumption is valid for the amplifier with suitable design parameters. This leads us to the desired equation for the controller. The controller will control the pump based on the following expressions:

$P_{pin}' - P_{pin} = P_k^{IS} \ln g_k / g_{k'} + \Sigma P_{sout}'' - \Sigma P_{sout}'$

$P_{pin}' - P_{pin} = P_k^{IS} \ln (P_k^{out}/P_k^{out'}) + \Sigma P_{sout}'' - \Sigma P_{sout}'$ (4)

Since $P_k^{out'}$,P_k^{out},$\Sigma P_{sout}''$, $\Sigma P_{sout}'$ can be measured by optical power meter, the change of pump power can be calculated by the controller according to the equation (4) to set the gain of the control channel back to its original value. In our project, the controller performs the calculation adaptively by changing the pump power incrementally until the two sides of the equation (4) are balanced.The "$P_k^{IS} \ln (P_k^{out}/P_k^{out'})$" is the starting value for the pump power change and then pump power is incrementally increased until desired gain has been reached.Thus, the data transfer via lightpath is not blocked in the presence of the attack signal.

3.1.2.Performance Evaluation using MATLAB Simulation

In order to study the effectiveness of therestoration model, a MATLAB simulation has been performed, where 5 different channels.with the corresponding α_k and P_k^{IS}were taken from [18]. The pump power is set with 8mW at 908 nm for a 30 m long EDFA. The input power of each channel was set to 0.1mW. To simulate the performance of the amplifier under attack, the input

power of channel 2 was increased by 1 mW. It was found that gains of the channels have dropped to around 40% of the original gains because of the high attack signal. Finally, increase of pump power by 11.25mW caused the gains of the channels to come closer to their original values. The simulation results are shown in Table 1 and Table 2.

As explained previously, the amplifier is considered to be under attack when gain of the control channel drops below a certain threshold value. In the above example, the threshold value is taken to be 50% of the original gain. However, other threshold values can also be chosen to determine whether the amplifier is under attack. As shown in Table 1 and Table 2, the individual gains of the channels are close to the original gains after adjusting pump power. Thus, overall EDFA gain is also close to the original value after adjusting pump power.

The proposed gain restoration scheme shown in Figure 8 restores the gains of all WDM signals including the attack signal to their pre-attack values. Thus the output powers of the useful signals are restored to their expected amplified values. However, amplified value of the attack signal becomes high because its initial value is much higher than the useful signals. This may cause crosstalk effect in the cross-connects when the EDFA is followed by switching devices in the WDM system. However, in our proposed scheme for protecting switching devices (explained later in relation to Figure 13) power equalizers/limiters are incorporated in the switching devices. These equalizers/limiters would limit the power of the attack signal so that the crosstalk effect due to this signal is reduced to an acceptable level.

Table 1: Simulation Results showing effect of attack signal restoration by applying appropriate pump power

	Channel 1 (1.5617 nm)	Channel 2 (1.5609 nm)	Channel 3 (1.5584 nm)	Channel 4 (1.5568 nm)	Channel 5 (1.556 nm)
α_k[1/m]	0.105	0.105	0.1130	0.1160	0.1170
P_k^{IS}[mW]	0.365	0.365	0.350	0.339	0.339
Input power before attack [mW]	0.1	0.1	0.1	0.1	0.1
Output Power before attack [mW]	1.23	1.23	1.24	1.37	1.33
gain before attack (pump power = 8mW)	12.38	12.38	12.41	13.75	13.34
Input power after attack [mW]	0.1	1.1	0.1	0.1	0.1
Output Power after attack [mW]	0.516	5.677	0.498	0.535	0.52
gain after attack	5.16	5.16	4.98	5.35	5.2
gain after adjustment of pump power (pump power = 19.25mW)	12.30	12.30	12.32	13.64	13.24
Output Power after adjustment of pump power	1.23	13.52	1.23	1.36	1.32

Table 2: input power, output power and EDFA gain before and after attack

	Total signal input power [mW]	Total signal output power [mW]	Overall EDFA gain
Before Attack	0.5	6.43	12.86
After attack but before pump power adjustment	1.5	7.75	5.17
After attack and after pump power adjustment	1.5	18.67	12.45

Thus our proposed gain restoration scheme is useful in the sense that it restores the gains of the legitimate signals and the intended service is not denied. As EDFA primarily suffers from cross-gain modulation, restoring power of legitimate signals is the most important job to continue the service.

3.2.Attack monitoring, security index calculation and partial restoration in optical cross-connects

High cross-talk in wavelength selective switches can be exploited by an attacker to perform in-band jamming by injecting a very high power attack signal. In-band jamming attack is difficult to localize, and causes service disruption without breaking or disrupting the fiber by jamming the data signal in legitimate light path. Therefore, it is necessary to minimize the crosstalk of a switch as far as possible. Switch crosstalk depends on coherence time, polarization, phase mismatch and input power of the switch, where first three factors are design dependent. The crosstalk can be severe if the power of the attack signal is very high and it can lead to denial of service by jamming the switch.

One way to prevent the jamming by crosstalk is to use limiting amplifiers to limit the input powers if the input powers of the channels are out of limit. Figure 9 shows a switch with the pre-emphasis/de-emphasis amplifiers to limit the power in each channel. The filter/amplifier prevents overpowering of any channel and hence prevents attacks. However, this technique requires inserting limiting amplifier within the switch, which is inflexible and infeasible when comes to use the already existing switches. Therefore, it is desirable that limiting amplifiers would be placed outside of the switch so as to use them with the existing switches.

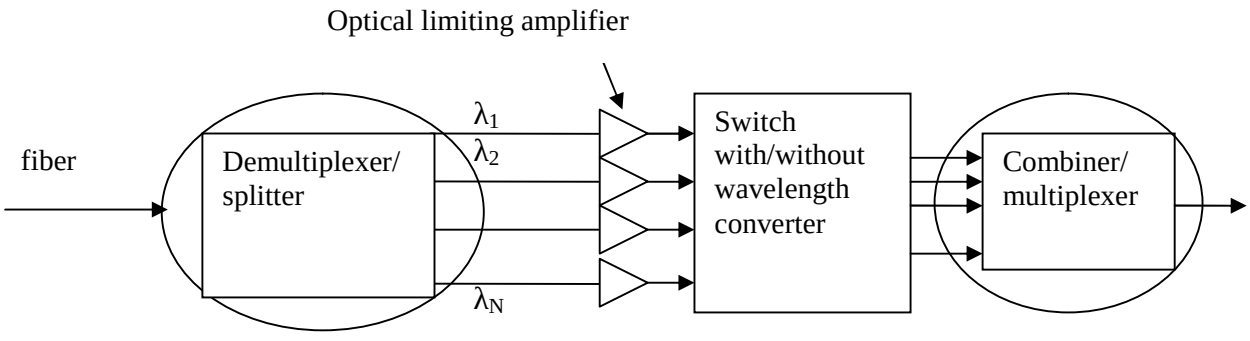

Figure 9: incorporating pre-emphasis/de-emphasis filter within an OXC of AON

3.2.1.Analytical model for crosstalk in optical cross-connects incorporating optical switches

In this paper an analytical model of the crosstalk effect in a typical optical cross-connect (OXC) consisting of N multiplexer/demultiplexer pairs and M optical switches as shown in Figure 10 is developed. Then the power/crosstalk relationship developed in this model is used to provide security envelopes around the switches. A crosstalk analysis of the OXC shown in Figure 10 has been performed following reference [19], [20]. Equation (5) represents the total crosstalk power impinged on signal λ_{11} of the OXC shown in Figure 10.

Total Crosstalk power in λ_{11} =

$$1/2\,E^2\sum_{i=1}^{X_1}\varepsilon_i b_s^{\,2}(t-\tau_i) \quad + \quad E^2\sum_{i=1}^{X_1}\sum_{k=i+1}^{X_1}\sqrt{\varepsilon_i\varepsilon_k}\,bs(t-\tau_i)bs(t-\tau_k)\cos(w_s\tau_i-w_s\tau_k)\cos\theta_{ik}+$$

$$1/2\sum_{j=2}^{N}\sum_{K=1}^{Xj}\varepsilon_{jk}E^2 b_j^{\,2}(t-\tau_{jk})+E^2\sum_{i=1}^{X_1}\sqrt{\varepsilon_i}\,bs(t)bs(t-\tau_i)\cos w_s\tau_i\cos\theta_i$$

$$+E^2\sum_{j=2}^{N}\sum_{k=1}^{X_j}\sqrt{\varepsilon_{jk}}\,bs(t)bs(t-\tau_{jk})\cos w_s\tau_{jk}\cos(\varphi_s(t)-\varphi_j(t))\cos\theta_{jk} \qquad (5)$$

where, E = the signal field amplitude which is assumed to be unchanged

X_1, X_j = number of crosstalk contributions leaked from λ_{11} and λ_{j1} respectively

$b_s(t)$, $b_j(t)$ (j = [2,N]) = binary data sequences with either 0 or 1 in a bit period T of λ_{11} and λ_{j1} respectively.

w_s, w_j = center frequencies of the lasers

φ_s, φ_j = phase noises of the lasers

τ_i, $\tau_{jk=}$ respective propagation delay differences between contributions

$\varepsilon_i, \varepsilon_{jk}$= the optical power relative to the actual signal for the crosstalk components (i refers to crosstalk contribution from the signal itself, j refers to the crosstalk contributions from other fibers)

θ_i, θ_{jk}= polarization angle differences between crosstalk contributions and the signal

Equation (5) shows that crosstalk depends on polarization matching (θ_i, θ_{jk}), delay differences (τ_i, τ_{jk}), crosstalk power ratios ($\varepsilon_i, \varepsilon_{jk}$), center frequencies ($w_s$, w_j) and phase noises (φ_s, φ_j). Many of these parameters are design issues and OXC should be designed such that the impact of crosstalk is reduced. In this paper, crosstalk to signal power ratio is used to control attack scenario because this relates to the power of the input signal.

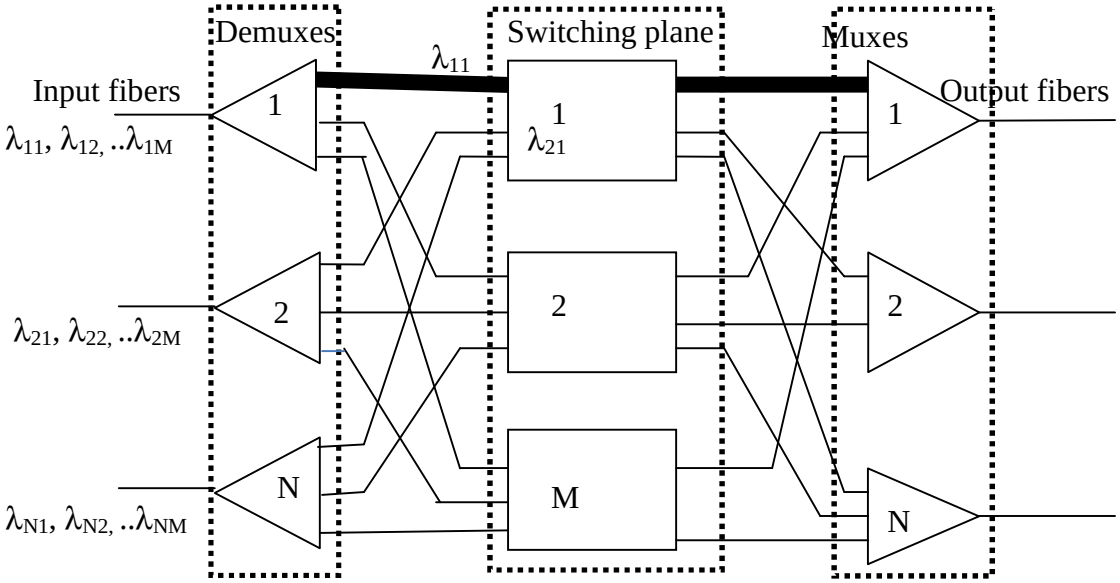

Figure10: A typical N*M OXC over which the crosstalk characteristics have been studied

3.2.1.1. Specific case of crosstalk calculation: Effect of power of λ_{21} on crosstalk in λ_{11}

This section describes specific case of how input power of one channel can affect the crosstalk in another channel. Specifically, the following analysis describes the crosstalk effect in λ_{11} whenthe power of λ_{21} is increased.There are 5 terms in the equation (5). The two terms in equation (6), dependent on j = 2..N, represent beat part between signal and incoherent crosstalk that are coming from the fibers other than the fiber containing the signal.

Total Crosstalk power on λ_{11} $= 1/2 \sum_{j=2}^{N} \sum_{K=1}^{Xj} \varepsilon_{jk} E^2 b_j^2 (t - \tau_{jk})$

$$+ E^2 \sum_{j=2}^{N} \sum_{k=1}^{X_j} \sqrt{\varepsilon_{jk}}\, bs(t) bs(t - \tau_{jk}) \cos w_s \tau_{jk} \cos(\varphi_s(t) - \varphi_j(t)) \cos \theta_{jk} \qquad (6)$$

To simplify analysis, the worst case condition is assumed, where signals are perfectly polarized, with zero delay differences and zero phase differences among signals and b_j,s are all 1. In such worst case condition, all the cosine terms in equation (6) will be unity. Then

$$\text{Total Crosstalk power in } \lambda_{11} = 1/2\, E^2 \sum_{j=2}^{N} \sum_{K=1}^{Xj} \varepsilon_{jk} + E^2 \sum_{j=2}^{N} \sum_{k=1}^{X_j} \sqrt{\varepsilon_{jk}} \qquad (7)$$

Now if the crosstalk from only λ_{21} is considered, then the worst case crosstalk power coming from λ_{21} in the signal at λ_{11} is given by expression (8).

$$\tfrac{1}{2}\, E^2 \sum_{k=1}^{X_2} \varepsilon_{2k} + E^2 \sum_{k=1}^{X_2} \sqrt{\varepsilon_{2k}} \qquad (8)$$

For simplicity, it is further assumed that all crosstalk power to signal power ratios for λ_{21} are same i.e. $\varepsilon_{2k} = \varepsilon_2$ for all k.

Thus λ_{21} dependent crosstalk power in λ_{11} = $\frac{1}{2} E^2 X_2 \varepsilon_2 + \frac{1}{2} E^2 \sqrt{\varepsilon_2} X_2$ (9)

The worst case crosstalk occurs when X_2 has its maximum value of M. In this case, the worst case value of λ_{21} dependent crosstalk power in λ_{11}

$= \frac{1}{2} E^2 X_2 \varepsilon_2 + \frac{1}{2} E^2 \sqrt{\varepsilon_2} X_2 = M/2(E^2 \varepsilon_2 + E^2 \sqrt{\varepsilon_2})$

$= M(\varepsilon_2 + \sqrt{\varepsilon_2})$ *signal power in λ_{11} , where signal power in $\lambda_{11} = \frac{1}{2} E^2$

Thus, ε_2 determines how much the λ_{21} induced crosstalk affects the signal in λ_{11}. Then the ratio of worst case λ_{21} dependent crosstalk power to the signal power in λ_{11}

$= M (\varepsilon_2 + \sqrt{\varepsilon_2})$ (10)

The rest of the part of equation (5) represents the λ_{21} independent crosstalk power.

Thusλ_{21} independent crosstalk power in λ_{11}= $1/2\, E^2 \sum_{i=1}^{X_1} \varepsilon_i + E^2 \sum_{i=1}^{X_1} \sum_{k=i+1}^{X_1} \sqrt{\varepsilon_i \varepsilon_k} +$

$1/2\, E^2 \sum_{j=3}^{N} \sum_{K=1}^{Xj} \varepsilon_{jk} + E^2 \sum_{i=1}^{X_1} \sqrt{\varepsilon_i} + E^2 \sum_{j=3}^{N} \sum_{k=1}^{X_j} \sqrt{\varepsilon_{jk}}$ (11)

Thereforeworst case λ_{21} dependent crosstalk power depends on M, the number of switches in the OXC and ε_2, thecomponent crosstalk power to signal power ratio. In real OXC design, typical value for ε_2 is below -40 db. Equation (10) has been plotted below in Figure 11 for different values of M where epsilon stands for ε_2. It is seen that for given M,crosstalk increases rapidly when ε_2 is above -40 db.Equation (5) shows that optical crosstalk in a channel increases if the signal powers in other adjacent channels are increased. The component crosstalk to signal ratio, ε is one of the parameters that can be exploited by an attacker to jam the OXC with crosstalk power. For example, the crosstalk contribution ε_2 from λ_{21} in λ_{11} increases if power of λ_{21} increases. Therefore, an attacker can increase the power of an attacking signal in one channel to increase the crosstalk interference in adjacent channels. To foil the attack, it is necessary to keep the values of ε_2 lower than threshold values of the acceptable crosstalk. If ε_2 and power relationship are known for an OXC, it is possible to check whether the optical power measured is within the desired range to provide acceptable ε_2 for the OXC.

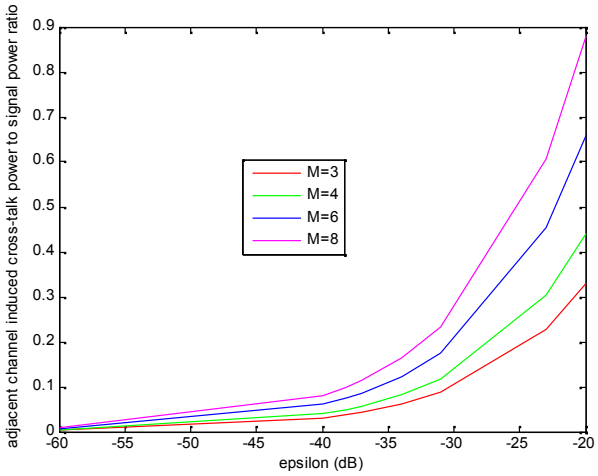

Figure 11: The ratio of worst case λ_{21} induced crosstalk power to the signal power in λ_{11}versus component crosstalk

Figure 12 shows a security envelope that detects attack and restores the system on-the-fly. The system measures the total incoming signals on input lines, estimates the crosstalk and takes corrective action if the crosstalk goes above an acceptable level. If the crosstalk is deemed to be higher than the acceptable level then the signal is passed through a bank of amplitude limiting amplifiers before it goes to the switch. Otherwise the signal is sent directly to the switch.
ε_2 is defined as:

$$\varepsilon_2 = \text{Crosstalk power leaked from } \lambda_{21} / \text{ Power of actual signal} \qquad (12)$$

The crosstalk power from λ_{21} in λ_{11} depends on the actual power of λ_{21} [21]. However, the actual relationship between crosstalk power from λ_{21} and the input power of λ_{21} depends on the switch architecture and can be found by experiment. In this paper, it is assumed that a linear relationship exists between crosstalk power from λ_{21} and the actual power of λ_{21} and equation (12) can be written as:

$$\varepsilon_2 = B*\text{Power}(\lambda_{21})/\text{Power}(P_s) \qquad (13)$$

where B is the crosstalk parameter of the demultiplexor indicating the fraction for input power that leaked to other channels as crosstalk, power(λ_{21}) is the power of channel λ_{21} and power(Ps) is the power of the signal λ_{11}.

Figure 13 shows our proposed switch architecture to foil the jamming attack by increasing power to the channel. The power of the optical channels in the fiber is measured. When power of the optical signal in the fiber is beyond acceptable range, the signal will pass through demultiplexors and power limiters to limit the fiber as indicated by dotted path #1 in Figure 12. Otherwise, the optical signal continues in the fiber as indicated by dotted path #2. The input power can be related with crosstalk [22] and the switch can be operated with acceptable power so that possible maximum crosstalk is within a limit. Depending on the power of the fiber, the switch has been marked as “attacked” and the database has been updated for the fiber. Therefore, the optical path continues and data loss can be prevented. In Figures 12 and 13, the limiting amplifiers are used, however, optical power attenuators can also be used. The optical buffer is inserted to compensate for the delay related to power measurement of the optical signal.

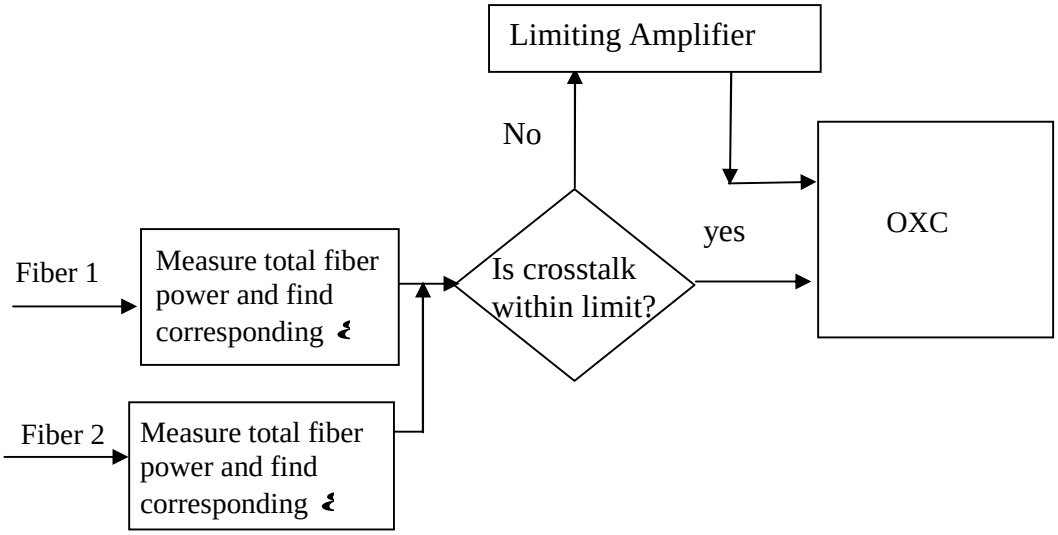

Figure 12. Outline of monitoring and restoration of out of range crosstalk in switches

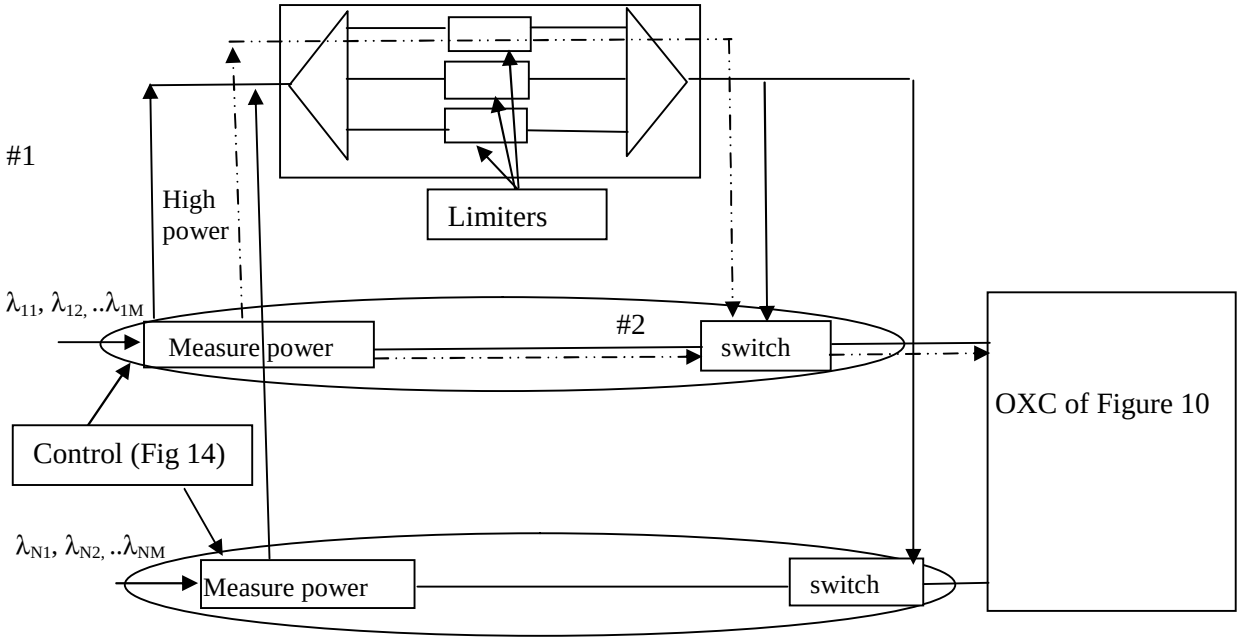

Fig 13: Proposed security envelope to control the high power jamming attack

Figure 14 shows the control operation of Figure 13. When measured signal power is beyond acceptable range, a control signal e is activated to close the two switches #1 and #2 in the upward directions so that the optical signal is demultiplexed to individual channels and each channel is power limited.

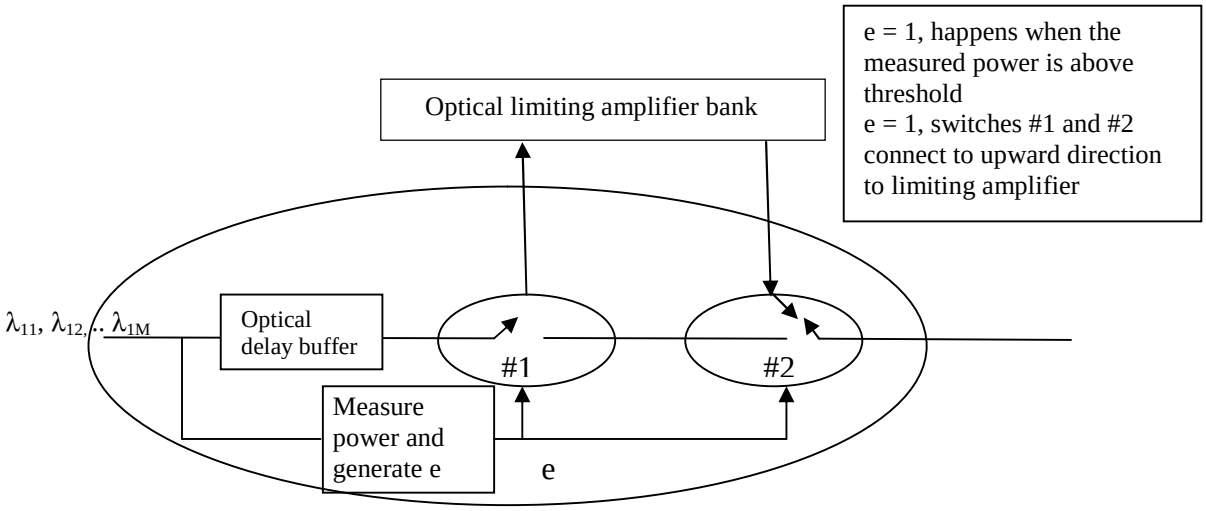

Figure 14: Detouring of light path via power limiters when measured fiber power is high

For an OXC with architecture shown in Figure 10, we assumed B = -50 dB and the normal power of any channel is -20 dBm (i.e. 0.01mW). In such a case, when a channel power is 0.1 mW (10 times the normal power) in a four channel system, the value of ϵ is -40 dB [equation (13)]. Therefore, when the combined fiber power of a fiber in Figure 13 is 0.13 mW or more, a channel may be underattacked as the corresponding ϵ approaches the threshold value, which is -40 dB in our case (Figure 11). When combined power of any fiber is out of range (i.e., more than threshold value, which is 0.13mW in our example), the control passes the light signal via the limiters to limit the power of each channel of the fiber. Hence the switch operates in the safe range of crosstalk.

4. CONCLUSION

To prevent service degradation and even service denial due to security attacks in transparent AON, it is necessary to establish secure lightpaths that provide protection against data loss. This paper presents protocols for security aware light path establishment by incorporating security indices of optical components in lightpath route computation. It then presents analytical models of operation of EDFA and optical crossconnects. These models are then used to establish schemes for security attack monitoring and real time restoration from security attacks in EDFA and optical crossconnects by providing security envelopes around them. Performance of these schemes is evaluated by using simulation. The proposed restoration schemes provide defense against various jamming attacks, which are predominant in optical components due to intrinsic vulnerabilities associated with them. The simulation results show that the optical components, e.g., EDFA and OXC, can work properly under attack scenarios by using the proposed scheme.

The security envelope, being external to the components, is capable of protecting components like optical amplifiers and optical cross-connects (OXC) without requiring any internal modification or redesign of the original design of them. Thus the security envelopes can be applied to protect components of any vintage. The results of this paper make it possible to save time, effort and cost involved in tearing down and reestablishing lightpaths in case of an attack

and to avoid consequent loss of significant amount of data in transmission. It is important to note that if the components at the physical level are security compromised then the operation of the whole network may be in jeopardy as the signals coming from upper layers will not be transmitted properly.

5.REFERENCES

[1] M. Medard, D. Marquis, R. Barry and S. Finn, "Security issues in all-Optical Network,"IEEE network, May/Jun 1997, Vol. 11, Issue 3, pp 42 – 48.

[2] Muriel Medard, Douglas Marquis, and Stephen R. Chinn, "Attack Detection methods for All-Optical Networks,"Proc Symposium on Network and Distributed System Security (NDSS), 1998.

[3] J. Patel, S. Kim, D. Su, S. Subramaniam, H. Choi, "A Framework for Managing Faults and Attacks in WDM Optical Networks,"Proc DARPA Information Survivability Conference & Exposition II, 2001, Vol. 2, pp 137 – 145.

[4] R. Rejeb, I. Pavlosoglou, M. Leeson, R. Green, "Management Issues in Transparent Optical Network,"Proc 6th International Conference on Transparent Optical Networks, July 2004, Vol 1, pp 248-254.

[5] P. Saengudomlert, "Analysis and detection of Jamming attacks in an all-optical network,"MS Theses, MIT, May 8 1998, http://web.mit.edu/medard/www/tengotheisis.pdf.

[6] R. Rejeb, M. Lessen, R. Green, "Fault and Attack Management in All-Optical Networks,"IEEECommunications, November 2006, Vol. 44, Issue 11, pp 79-86.

[7] S. Kartalopoulos, "Optical network security: countermeasures in view of channel attacks,"Proc MillCom 2006, October, pp 1-5.

[8] R. Rejeb, I. Pavlosoglou, M.S. Leeson and M.S. Green, "Securing All-Optical Networks,"Proc 5th International Conference on Transparent Optical Network, 29 June-3 July 2003, Vol. 1, pp 87- 90.

[9] Tao Wu, and Arun Somani, "Cross-Talk Attack Monitoring and Localization in All-Optical Networks,"IEEE/ACM Transactions on networking, December 2005, Vol. 13, No. 6.

[10] Y. Peng, Z. Sun, S. Du, K. Long, "Propagation of all-optical crosstalk attackin transparent optical networks,"Optical Engineering, 50, 8, 2011.

[11] A. Jirratigalachote, N. Skorin-Kapov, M. Furdek, J. Chen, P. Monti, L. Wosinska, "Sparse Power Equalization Placement for Limiting Jamming Attack Propagation in Transparent Optical Networks,"Optical Switching and Networking, 2011, Vol. 8, Issue 4.

[12] VakaMurali Mohan, MalliKarjuna Reddy, K.R.N. Kiron Kumar, "A New Approach to Optical Networks Security: Attack-Aware Routing and Wavelength Assignment,"IJCA Special Issues on "2nd National Conference- Computing, Communication and Sensor Network" CCSN, 2011.

[13] N. Skorin-Kapov, J. Chen, L. Wosinska, "A New Approach to Optical Networks Security: Attack Aware Routing and Wavelength Assignment,"IEEE/ACM Transactions on Networking, 18, 3, 2010.

[14] M. Furdek, N. Skorin-Kapov, M. Grbac, "Attack-Aware Wavelength Assignment for Localization of In-band Crosstalk Attack Propagation,"IEEE/OSA Journal of Optical Communications and Networking, 2, 11, 2010.

[15] Gary Duerksen, "Bidirectional WDM Optical Communication System With Bidirectional Add-Drop Multiplexing," US Patent 6,608,709, August 19, 2003.

[16] Stephen Chinn, "Simplified Modeling of Transients in Gain-Clamped Erbium-Doped Fiber Amplifiers,"Journal of Lightwave Technology, June 1998, Vol. 16, No. 9.

[17] A. A. M. Saleh, R.M. Jopson, J.D. Evankow and J. Aspel, "Modeling of Gain in Erbium-Doped Fiber Amplifiers,"IEEE Photonics Technology Letters, October 1990, Vol. 2, No. 10.

[18] Stephan Packnicke, Peter Krummrich, Edgar Voges, and Erich Gottwald, "Transient gain dynamics in long-haul transmission systems with electronic EDFA gain control,"Journal of Optical Networking, September 2007, Vol 6, No. 9.

[19] TeckYoong Chai, Tee Hiang Cheng, Sanjay K. Bose, Chao Lu, and GangxiangShen, "Crosstalk Analysis for Limited-Wavelength-Interchanging Cross Connects,"IEEE Photonics TechnologyLetters, May 2002, Vol. 14, No. 5.
[20] YunfengShen, Keije Lu, and WanyiGu, "Coherent and Incoherent Crosstalk in WDM Optical Networks,"Juornal of Lightwave Technology, May 1999, Vol 17, No. 5.
[21] Yoshitomo Okawachi, OnurKuzucu, Mark A. Foster, Reza Salem, Amy C. Turner-Foster, AleksandrBiberman, Noam Ophir, Keren Bergman, Michal Lipson, and Alexander L. Gaeta, "Characterization of Nonlinear Optical Crosstalk in Silicon Nanowaveguides,"IEEE Photonics Technology letters, February 1, 2012, Vol. 24, No. 3.
[22] Tim Gyselings, Greet Morthier and RoelBaets, "Crosstalk Analysis of Multiwavelength Optical Cross Connects,"Journal of Lightwave Technology, August 1999, Vol 17, No. 8.

Authors:

FahmidaRahman is currently a Ph.D. candidate at the Catholic University of America. Her main research interest is the security in optical Networks. She received her B.S. from Bangladesh University of Engineering and Technology, Bangladesh in 1995 and M.S. from Gannon University, Pennsylvania, USA in 1999, majoring in Electrical Engineering.

Mohammed Arozullah earned his Ph. D. in Electrical Engineering in 1967. Since then he has been involved in higher education in Canada and the United States. Currently he is Professor of Electrical Engineering and Computer Science at the Catholic University of America in Washington, D.C. Previously he has been in the faculty of Queen's University in Canada and Clarkson University in USA. He was a former Chairman of the Communication Systems Committee of the Communications Society of IEEE. He is a life member of IEEE He has published nearly 100 technical papers and have chaired technical sessions at IEEE and other conferences.