

Attack monitoring and localization in All-Optical Networks

Tao Wu · Arun K. Somani

© Springer Science + Business Media, LLC 2006

Abstract An attacker's connection can propagate quickly to different parts of a transparent All-Optical Network. Such attacks affect the normal traffic and cause a quality of service degradation or outright service denial. Attack monitors can collect the information of each link and each node to help diagnose the attacker's exact location.

Quick detection and localization of an attack source helps avoid losing large amounts of data in an all-optical network. However, to detect attack sources, it is not necessary to put monitors on all nodes. Since not every wavelength on every link is being used all the time, we propose to use the idle wavelengths to setup diagnostic connections and obtain the necessary information needed for diagnosis purposes. We show that placing a relatively small number of monitors at some key nodes in a network is sufficient to achieve level of performance. However, the monitor placement policy, routing policy, and diagnosis method are challenging problems.

We, in this paper, first develop a monitor placement policy, a test connection policy, and a routing policy based on our definition of crosstalk attack and monitor node models. With these policies, we show that we can always detect and localize the malicious connections as long as there is no more than one malicious connection on each wavelength in the whole network. After this, we develop a scalable diagnosis method, which can localize the sources of the such malicious attacks in a fast manner.

Keywords Crosstalk · Attack · Monitor · AON

1 Introduction

An All-Optical Network (AON) is a network where the user-network interface is optical and the data does not undergo optical to electrical conversion within the network. AONs are attractive because they deliver very high data rates, and support a broad class of applications. The ability to route large amounts of data and access different channels makes an AON a very attractive option for providing very high-rate access in WANs, MANs, and even LANs.

Although AONs are a viable technology for future telecommunication and data networks, their intrinsic security differences with existing electro-optic and electronic networks have received attention only recently. Security in AONs is an important research area, and it is different from communication and computer security in general. AONs introduce new physical layer mechanisms that may change potential models of attack from those that are known for electronic networks. AONs are typically used to carry extremely high data rates. Moreover, AONs' transparency characteristic means that data does not undergo optical-to-electrical or electrical-to-optical conversion. Thus, connections in such networks are amplified, but may not be regenerated at intermediate components. This transparency characteristic has many advantages in certain aspects, however, it also creates many security vulnerabilities that do not exist in traditional networks. In a network with regeneration ability, an anomalous connection will lose its attack capability after passing through an intermediary node, while in a network without regeneration ability, a malicious connection can propagate from its primary source to other nodes without losing its

T. Wu (✉) · A. K. Somani
Dependable Computing & Networking Laboratory,
Department of Electrical and Computer Engineering,
Iowa State University, Ames, IA 50011
e-mail: wutao@microsoft.com

A. K. Somani
e-mail: arun@iastate.edu

attack capability. Transparency and non-regeneration features make attack detection and localization difficult.

1.1 Attack types

Generally, there are three main differences between an attack and a failure.

1. Attacks may spread to many users and many parts of the network, while a component failure only affects those connections passing through it;
2. Attacks attempt to avoid detection, while the failure cannot do that;
3. Rerouting traffic connections using a scheme to tolerate hardware failure cannot solve the problem caused by an attack connection.

There are several kinds of attacks, including fiber cuts (fiber attack), power jamming (amplifier attack), crosstalk attack (switching node attack), and correlated jamming (tapping attack), etc. Some of these attacks, such as fiber cuts, can be treated as a component failure. Other attacks, like correlated jamming, can only affect those connections that are sharing the same link or the same node with the attack connections.

Among all these attack methods, crosstalk attack has higher damage capabilities. The attacker injects a malicious connection which has very high power energy, beyond expected value. When this connection passes through a wavelength selective switch, the leakage energy (crosstalk) of this malicious connection can be significant and affect the normal connections passing through the same switch. In this paper, we only focus on the crosstalk attack. Unlike other attacks, a crosstalk attack can not only affect those connections sharing the same link or node with it, but also may induce attack capabilities to those connections that are attacked [1]. As shown in Fig. 1, the crosstalk attack happens at a wavelength

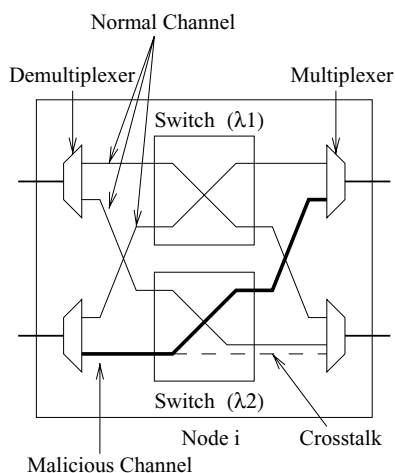


Fig. 1 Example of crosstalk attack using wavelength selective switches

switch and only affects those normal connections in the same wavelength. Figure 2 shows the crosstalk attack propagation mechanism. This characteristic makes attack connection localization more difficult.

1.2 Previous work

Although attack monitoring and localization is important for security of AON, unfortunately, neither a clear attack model nor a monitor model has been established yet in previous papers.

There has been some work [1–4] in the area of attack localization in AONs, and some detection methods are proposed. However, these papers do not discuss whether these methods guarantee to localize every attack connection. If a method cannot guarantee to localize every attack connection, normal connections will take a risk of being attacked by those undiscovered attack connections. Moreover, these papers assume that all nodes are equipped with monitors. Other researches [5, 6] describe the capability of an optical monitoring module. Generally, an optical monitor can measure single connection optical power as well as its optical SNR (signal noise ratio). However, it is doubtful that a monitor device will be less expensive in the near future. Therefore, to install a monitor at each node in the network is likely extremely expensive.

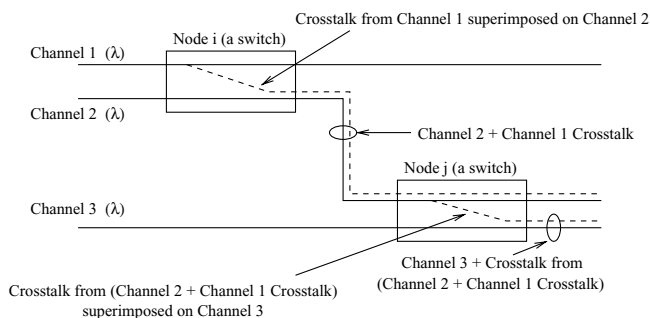
Other methods [7–9] provide probabilistic approaches to fault diagnosis in network. Instead of localizing the exact faulty components, these approaches give the most likely fault set. There are some drawbacks of these approaches if we apply them to our attack localization problem. These approaches only give the most likely set instead of determining the exact location of the source. We still need further steps to analyze where the exact location of the source is, and the time consumed by the further analysis may result in a huge data loss.

A network management system using supervisory connections [10, 11] can detect and monitor the performance of the devices in the network. The advantage of this scheme is that a monitor device can be put in a remote place while the drawback is that some extra supervisory connections are needed to send control signal and detection data. This method provides the necessary technique required by sparse monitoring concept.

1.3 Feasibility of sparse monitor network

Because a network management system using supervisory connections can detect and monitor the performance of network devices remotely, detecting attack sources is not necessarily equivalent to putting monitors at all nodes. In fact, those connections affected by attack can provide valuable information about distribution of attack locations. Thus, if

Fig. 2 Example of crosstalk attack propagation



we can monitor all connections in whole network, we may obtain the necessary information needed for our diagnostic purpose. If normal connections cannot provide sufficient information, we can derive the monitoring information from some test connections. From previous research [12] we notice that generally the number of idle wavelengths in a network is very large. For example, in a 4×4 mesh-torus network if the connection load of each source-destination pair is 0.3 and the number of wavelengths on each link is 8, then the number of idle wavelengths on each link could be 5 with a probability of more than 70%. This information is helpful in establishing a test connection. Moreover, existing connections can also be monitored for malicious attacks. These two together allow us to create a capable diagnostic system. We believe and show that this diagnostic information is sufficient for localizing an attack connection.

The rest of the paper is organized as follows. First, we propose a crosstalk attack and monitor model based on some previous work [1, 2, 4, 5, 10, 11] as well as one sparse monitor placement method. Based on this monitor placing, routing, and test connection setting policies, we prove that we can always localize malicious homo-wavelength crosstalk attacks in a network. In the following section, we give an example to explain our algorithm and demonstrate its capabilities. Finally, we present our conclusions.

2 Crosstalk attack and monitor model

Before we explain our crosstalk attack detection and localization method based on sparse monitors, we describe our models for the node, crosstalk attack, and monitor.

2.1 Node model

We assume that every node in our network has the following characteristics.

1. The node can perform routing and switching. Without the switching capability, the node cannot propagate a crosstalk attack to other normal connections. In such a

case, the node need not be considered as a potential attack propagation node.

2. Some nodes can support monitoring capability as described in the following (monitor model part). We call a node supporting monitoring capability as a *monitor node* and a node without this capability as a *non-monitor node*.

2.2 Crosstalk attack model

As shown in Fig. 1, the crosstalk attack connection only affects the same wavelength connections at the wavelength selective switches. The following items describe our crosstalk attack model.

1. *Up-stream* and *down-stream neighbor nodes*: For a certain node on a certain connection path, its *up-stream neighbor node (UNN)* is the previous node on that path. Similarly, its *down-stream neighbor node (DNN)* is the next node on that path. In the rest of this paper, $UNN(\text{node } A, \text{connection } C)$ denotes the UNN of node A on connection C . Similarly, $DNN(\text{node } A, \text{connection } C)$ denotes the DNN of node A on connection C .
2. The *original attack flow (OAF)* has a much higher energy level than permitted on a normal connection. The leakage of energy at a switch from the attack connection influences all other normal connections using the same wavelength on other fibers. The ability of an OAF to influence normal connections is same on its path.
3. A normal connection sharing a same nodes with the OAF will be affected, and this connection will be called as a *secondary attacked flow (SAF)*. The SAF has limited attack capability. That is, if a normal connection C gets affected by an OAF at node u , then the connection C has attack capability only at node $DNN(u, C)$.
4. A normal connection influenced by an SAF is called a *final attacked flow (FAF)*. The FAF does not have the attack propagation capability.
5. A connection not affected by either OAF or SAF is called an *attack-free flow (AFF)*. Similarly, a node that is neither a PAN nor a SAN is called an *attack-free node (AFN)*. The union of AFF, SAF, and FAF is called an *innocent flow (IF)* set.

As shown in Fig. 2, connection 1 is the OAF, connection 2 is the SAF, and connection 3 is the FAF, while node i is the PAN, and node j is SAN. Connection 1 can propagate its malicious attack to connection 3 by affecting connection 2. According to this, it is expected that the OAF pollutes any connections passing through the PAN, and the SAF pollutes any normal connection passing through a SAN.

2.3 Monitor node model

We call a node installed with a monitor device as a monitor node, or a monitor. A node without a monitor device is called a non-monitor node.

1. A monitor node can monitor all traffic passing through it, including the traffic that originated/terminated at the node.
2. The monitor node can detect the input/output connection power in all parts including its demultiplexer, multiplexer, switch plane, etc. to see if any power level is beyond the expected value. Figure 3 shows a crosstalk attack monitoring mechanism for selective wavelength switches. If a connection passes through a monitor with very high power, then we say that this connection is in *attack-status* at that monitor. A connection can be in an attack/non-attack status at a monitor. We use A/\bar{A} to indicate the attack/non-attack status of the connection.
3. If there are at least two connections which have attack capabilities passing through a same monitor, then there are two possibilities.

- (a) One connection is an OAF while all the others are SAFs. Because $P(OAF) > P(SAF)$, the monitor node can detect that one connection has higher power than others do, and the monitor considers only this connection (OAF) to have attack capability. Thus, only OAF will be set A , while other SAFs will be set \bar{A} .

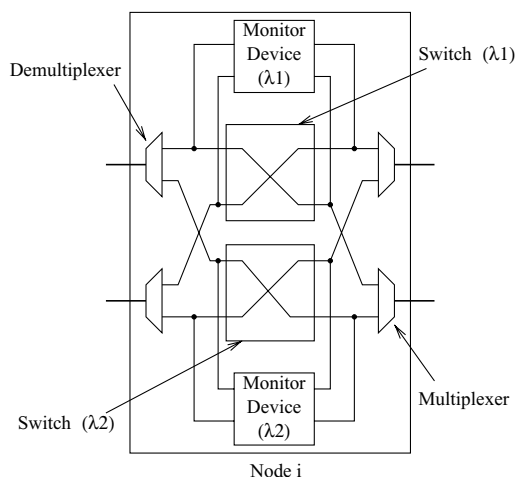


Fig. 3 Attack monitoring mechanism for selective wavelength switches

- (b) All these connections are SAFs. In this situation, the monitor can detect several connections which have the similar unexpected high power, then the monitor set all these connections to A .

2.4 Monitor placement policy

To guarantee the exact location of the OAF in a network, we need to determine a monitor placement and a routing policy after we choose a monitor model. Before describing the monitor placement algorithm, we need the following definitions.

1. *One-hop-distance monitor (OHM)*: If a monitor is connected directly to a non-monitor node, then this monitor is an OHM to this non-monitor node.
2. *Degree of a node*: The degree of a node is the number of links that intersect with this node.
3. *Pendant node*: A node with degree one is called a pendant node.

The following monitor placement is required to guarantee location of an OAF :

1. For each non-monitor node with degree d , it must have d OHMs.
2. A node with a degree more than one and having a pendant node as a neighbor must be a monitor node.

2.5 Test connection setting policy

We assume that each link in the network is bi-directional so that there are two fibers for different directions in each link. According to our monitoring mechanism, there are two kinds of connections: one is the *normal connection* which is set up by users, and the other is the *test connection* which is requested by the network management system. A test connection is an important method in determining if a node is a PAN or not. There are two kinds of test connections based on whether the connection is originating from or terminating at a node. If a test connection is originating from a node, we call it *output test connection (OTC)* of that node, otherwise, we call it the *input test connection (ITC)* of that node. We use the following rules to set up test connections.

1. For a non-monitor node, if there is a normal connection on wavelength λ terminating at this node, one OTC to one of its OHMs is required when there does not exist normal connection from this node to any of its OHMs on the same wavelength.
2. For a monitor node, if there is a normal connection on wavelength λ originating, passing or terminating at the node, it needs to set up one OTC and one ITC to each of its neighbor nodes (irrespective of whether that is a

monitor node or not) on the same wavelength when there is no corresponding normal connection on the same link.

2.6 Routing policy

To guarantee the exact location of the OAF in a network, we use the following rules to set up a connection.

1. For any two of the normal connections (excluding test connection) originating from a non-monitor node, at least one must pass through two different monitors.
2. Normally we use the shortest path algorithm except the above case.

3 OAF detection

According to our crosstalk attack model, the crosstalk attack only affects the same wavelength connections at the wavelength selective switch. To simplify our analysis, in the following parts of our paper, we always assume there is no wavelength converter in the whole network. According to our model, a monitor node can be in one of following states:

Attack-free state: All connections passing through this monitor node must be in \bar{A} status. Moreover, for a \bar{A} connection, its UNN must be an INode, while this connection must be IFlow. All connections passing through an INode must be IFlows.

Attacked state: At least one connection passing through this node is in status A . A monitor node cannot know if this node is a SAN or PAN. Its input connections can be in \bar{A} or A status.

- A. For a \bar{A} connection: It must be an IFlow.
- C. For an A connection:

- I. If there are more than one such connections, all of those connections are IFlows, and these connections' UNNs must be PANs.
- II. If this connection starts at this monitor node, then this connection must be the OAF, otherwise its UNN must be a PAN.

Claim: With above new sparse monitoring policies, a network is one-OAF diagnosable.

Proof: An arbitrary network is denoted by a graph $G(V, E)$ where V is the set of all nodes, and E is the set of all connections between the nodes. Let M denote the set of monitor nodes and $M \subset V$. For any connection C_i established in the network, using $CV_i = \{cv_{ij} : cv_{ij} \text{ is a Node on } C_i\}$, denote the path of that connection and the nodes are listed in order on

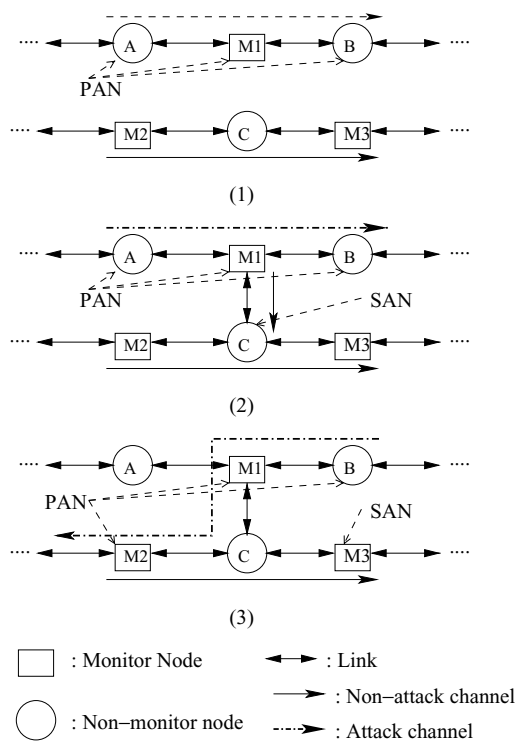


Fig. 4 Scenario I of normal connection

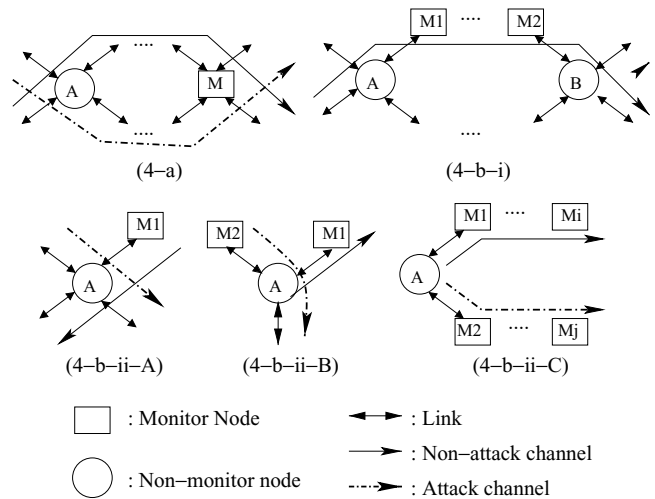
the path. According to our monitor placement policy, every connection (including the OAF) must have at least one monitor node on its path. If we are always able to detect whether a connection is an IFlow or not, then the only connection which cannot be an IFlow is the OAF.

First, we consider that there is only one wavelength λ in the whole network. For every IFlow C_i , there can only be one of following situations:

1. No PAN or SAN on its path, as the connection $\{\dots, M_2, \dots, C, M_2, \dots\}$ shown in Fig. 4 (1). Then at least one monitor can record its state as \bar{A} , so the connection must be an IFlow.
2. No PAN but at least one SAN on its path, as the connection $\{\dots, M_2, \dots, C, M_2, \dots\}$ shown in Fig. 4 (2). The state of this connection can only be \bar{A} , so it must be an IFlow.
3. Sharing at least one link with the OAF, as the connection $\{\dots, M_2, \dots, C, M_2, \dots\}$ shown in Fig. 4 (3). According to our monitor placement policy, at least one node on such link must be a monitor node. At this monitor node, the state of this connection can only be \bar{A} , so this connection must be an IFlow.
4. At least one PAN on its path, but no sharing link with OAF. In this case, there are two possibilities.

- (a) At least one of these nodes is a monitor, as the normal connection shown in Fig. 5(4-a). Then at this monitor,

Fig. 5 Scenario II of normal connection



- the state of connection C_i can only be \bar{A} , so this connection must be an IFlow.
- (b) None of these nodes is a monitor. In this case there are also two possibilities.
- (i) There are at least two PANs, as the normal connection shown in Fig. 5(4-b-i). Suppose the two shared nodes are nodes A and B . Then, connection C_i is of the form $\{\dots, A, M_1, \dots, M_2, B, \dots\}$, where M_1 and M_2 are monitors. M_1 and M_2 can be the same node. Suppose the UNN of M_2 is node X , then the connection C_i is of the form $\{\dots, A, M_1, \dots, X, M_2, B, \dots\}$. According to our test connection setting policy, there must be a connection from node B to node M_2 . Because B is a PAN, the state of segment $(B \rightarrow M_2)$ must be A . If the state of segment $(X \rightarrow M_2)$ is A , there are two A state connections at a monitor at the same time. According to the above monitor state's analysis, both of these connections must be IFlows. If the state of segment $(X \rightarrow M_2)$ is not A , then C_i must be an IFlow.
- (ii) There is only one shared node between connection C_i and OAF. Assume the shared node is node A , then there can be three scenarios.
- (A) Suppose connection C_i is of the form $\{\dots, M_1, A, \dots\}$, as the normal connection shown in Fig. 5(4-b-ii-A). Then, at monitor M_1 , the state of connection cannot be A . Thus connection C_i must be an IFlow.
- (B) Suppose node A is the originating node of connection C_i , as the normal connection shown in Fig. 5(4-b-ii-B), then the connection is of the form of $\{A, M_1, \dots\}$. If OAF does not originate from node A , OAF is of the form $\{\dots, M_2, A, \dots\}$.

If the OAF is originating from monitor node M_2 , then the state of the OAF at monitor node

M_2 will be A and the OAF would be located at M_2 .

If $\text{UNN}(M_2, \text{OAF})$ is node X , in this case, the OAF is of the form $\{\dots, X, M_2, A, \dots\}$. Because the state of segment $(X \rightarrow M_2)$ is A , X must be a PAN. An OAF must pass through all known PANs. Now, connection C_i does not pass through PAN X . Thus it must be an IFlow.

- (C) Suppose both connection C_i and OAF originate from node A , as the normal connection shown in Fig. 5(4-b-ii-C). Connection C_i is of the form $\{A, M_1, \dots\}$ while the OAF is of the form $\{A, M_2, \dots\}$. According to our routing policy, either connection C_i or OAF must pass through at least two different monitors. Therefore the following two situations arise.
- If connection C_i passes through at least two monitors on its path, then it is of the form $\{A, M_1, \dots, M_i, \dots\}$. Assume $\text{UNN}(M_i, C_i)$ is node I and $I \neq A$, then, node I cannot be a PAN and the state of segment $(I \rightarrow M_i)$ cannot be A , connection C_i must be an IFlow.
 - If the OAF has at least two monitors on its path, and it is of the form $\{A, M_2, \dots, M_j, \dots\}$. Assume $\text{UNN}(M_j, \text{OAF})$ is node J and $J \neq A$, then, the state of segment $(J \rightarrow M_j)$ must be A and we have at least two known PAN: A and J . Since J is not included in the path of connection C_i , C_i must be an IFlow.

Second, we consider that there are multiple wavelengths in the whole network. We restrict that no more than one crosstalk attack appears on each wavelength and there is no

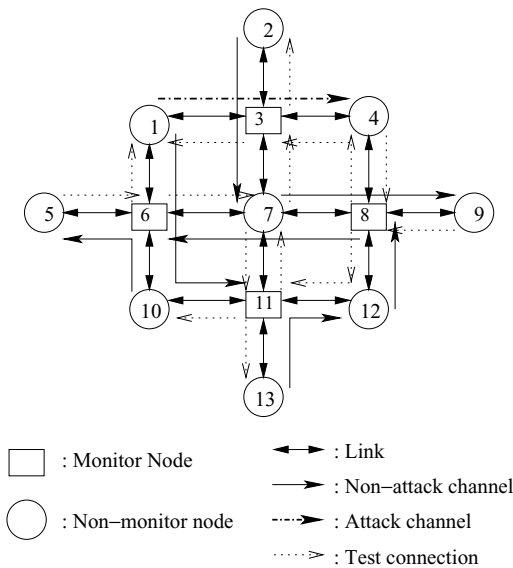


Fig. 6 A 13-node mesh network with one attack connection

wavelength converter in the whole network. According to our crosstalk attack model, the crosstalk attack connection can only affect the same wavelength connections at the wavelength selective switches. Therefore, a crosstalk attack on one wavelength does not have the chance to affect the normal connections on other wavelengths. We have already proved that we can detect all the connections in IFlow set on one wavelength. Therefore, we can always detect the connections in IFlow set on all wavelengths in the whole network.

Conclusion: As long as there is no more than one OAF on each wavelength and there is no wavelength converter in whole network, we can always localize the OAFs based on our models and policies. □

4 Example

4.1 Example 1

As shown in Fig. 6, this is a 13-node mesh network. There are a total of 4 monitor nodes which meet the two requirements of our monitor placement policies. Because the malicious connection can only affect the normal connections in the same wavelength based on our model, only those connections which use the same wavelength λ with the malicious connection need to be analyzed. In this network, every link is bi-directional and there is only one wavelength λ in each direction. We assume that all the connections shown in this example use wavelength λ .

Suppose we have some normal connections and only one of them is a malicious connection. We need to set up some test connections to assist our diagnosing.

The current normal connection set is:

Normal connection set = $\{1 \rightarrow 3 \rightarrow 4, 1 \rightarrow 6 \rightarrow 10 \rightarrow 11, 10 \rightarrow 6 \rightarrow 5, 13 \rightarrow 11 \rightarrow 12, 12 \rightarrow 8, 8 \rightarrow 7 \rightarrow 6, 7 \rightarrow 8 \rightarrow 9, 2 \rightarrow 3 \rightarrow 7\}$.

Among these connections, connection $1 \rightarrow 3 \rightarrow 4$ is the OAF.

Based on these normal connections, according to our test connection setting up policy, we get the test connection set as following:

Test connection set = $\{3 \rightarrow 2, 3 \rightarrow 1, 4 \rightarrow 3, 4 \rightarrow 8, 6 \rightarrow 1, 7 \rightarrow 3, 8 \rightarrow 4, 5 \rightarrow 6, 6 \rightarrow 7, 9 \rightarrow 8, 11 \rightarrow 10, 11 \rightarrow 7, 7 \rightarrow 11, 8 \rightarrow 12, 12 \rightarrow 11, 11 \rightarrow 13\}$

According to above assumption, the connection state in monitor nodes 3, 6, 8, and 11 are shown in Table ??.

Thus, the initial attack connection set is:

AF set = $\{1 \rightarrow 3 \rightarrow 4, 2 \rightarrow 3 \rightarrow 7, 3 \rightarrow 4, 7 \rightarrow 3, 1 \rightarrow 6 \rightarrow 10 \rightarrow 11, 8 \rightarrow 7 \rightarrow 6, 7 \rightarrow 8 \rightarrow 9, 4 \rightarrow 8, 7 \rightarrow 11\}$.

Because monitor nodes 3, 6, and 8 receive some A state connections, they are in attack state. Only monitor node 11 is in attack-free state.

For monitor node 11,

$\{1 \rightarrow 6 \rightarrow 10 \rightarrow 11\}$ is $\bar{A} \Rightarrow \{1 \rightarrow 6 \rightarrow 10 \rightarrow 11\} \in IFlow\ set$;

$\{13 \rightarrow 11 \rightarrow 12\}$ is $\bar{A} \Rightarrow \{13 \rightarrow 11 \rightarrow 12\} \in IFlow\ set$ and node 13 $\in INode\ set$;

$\{7 \rightarrow 11\}$ is $\bar{A} \Rightarrow \{7 \rightarrow 11\} \in IFlow\ set$;

$\{12 \rightarrow 11\}$ is $\bar{A} \Rightarrow \{12 \rightarrow 11\} \in IFlow\ set$ and node 12 $\in INode\ set$;

$\{11 \rightarrow 7\}$ is $\bar{A} \Rightarrow \{11 \rightarrow 7\} \in IFlow\ set$;

$\{11 \rightarrow 10\}$ is $\bar{A} \Rightarrow \{11 \rightarrow 10\} \in IFlow\ set$;

$\{11 \rightarrow 13\}$ is $\bar{A} \Rightarrow \{11 \rightarrow 13\} \in IFlow\ set$.

For monitor node 3,

$\{1 \rightarrow 3 \rightarrow 4\}$ is $A \Rightarrow$ node 1 $\in PAN\ set$;

$\{2 \rightarrow 3 \rightarrow 7\}$ is $\bar{A} \Rightarrow \{2 \rightarrow 3 \rightarrow 7\} \in IFlow\ set$;

$\{4 \rightarrow 3\}$ is $\bar{A} \Rightarrow \{4 \rightarrow 3\} \in IFlow\ set$;

$\{7 \rightarrow 3\}$ is $\bar{A} \Rightarrow \{7 \rightarrow 3\} \in IFlow\ set$;

$\{3 \rightarrow 2\}$ is $\bar{A} \Rightarrow \{3 \rightarrow 2\} \in IFlow\ set$;

$\{3 \rightarrow 1\}$ is $\bar{A} \Rightarrow \{3 \rightarrow 1\} \in IFlow\ set$.

For monitor node 6,

$\{1 \rightarrow 6 \rightarrow 10 \rightarrow 11\}$ is $A \Rightarrow$ node 1 $\in PAN\ set$;

$\{10 \rightarrow 6 \rightarrow 5\}$ is $\bar{A} \Rightarrow \{10 \rightarrow 6 \rightarrow 5\} \in IFlow\ set$ and node 10 $\in INode\ set$;

$\{6 \rightarrow 1\}$ is $\bar{A} \Rightarrow \{6 \rightarrow 1\} \in IFlow\ set$;

$\{5 \rightarrow 6\}$ is $\bar{A} \Rightarrow \{5 \rightarrow 6\} \in IFlow\ set$ and node 5 $\in INode\ set$;

$\{8 \rightarrow 7 \rightarrow 6\}$ is $\bar{A} \Rightarrow \{8 \rightarrow 7 \rightarrow 6\} \in IFlow\ set$;

$\{6 \rightarrow 7\}$ is $\bar{A} \Rightarrow \{6 \rightarrow 7\} \in IFlow\ set$.

Same to deal with those connections passing through monitor node 8:

Table 1 Connection state in monitor nodes

Monitor 3		Monitor 6		Monitor 8		Monitor 11	
Connection	State	Connection	State	Connection	State	Connection	State
1 → 3 → 4	A	1 → 6 → 10 → 11	A	7 → 8 → 9	\bar{A}	1 → 6 → 10 → 11	\bar{A}
2 → 3 → 7	\bar{A}	6 → 7	\bar{A}	8 → 7 → 6	\bar{A}	13 → 11 → 12	\bar{A}
3 → 2	\bar{A}	10 → 6 → 5	\bar{A}	12 → 8	\bar{A}	7 → 11	\bar{A}
4 → 3	\bar{A}	6 → 1	\bar{A}	8 → 4	A	11 → 7	\bar{A}
7 → 3	\bar{A}	5 → 6	\bar{A}	9 → 8	\bar{A}	12 → 11	\bar{A}
3 → 1	\bar{A}	8 → 7 → 6	\bar{A}	4 → 8	A	11 → 10	\bar{A}
				8 → 12	\bar{A}	11 → 13	\bar{A}

$\{7 \rightarrow 8 \rightarrow 9\}$ is $\bar{A} \Rightarrow \{7 \rightarrow 8 \rightarrow 9\} \in IFlow$ set;
 $\{8 \rightarrow 7 \rightarrow 6\}$ is $\bar{A} \Rightarrow \{8 \rightarrow 7 \rightarrow 6\} \in IFlow$ set;
 $\{12 \rightarrow 8\}$ is $\bar{A} \Rightarrow \{12 \rightarrow 8\} \in IFlow$ set and node 12 $\in INode$ set,
 $\{8 \rightarrow 4\}$ is $\bar{A} \Rightarrow \{8 \rightarrow 4\} \in IFlow$ set;
 $\{4 \rightarrow 8\}$ is $A \Rightarrow$ node 4 $\in PAN$ set;
 $\{9 \rightarrow 8\}$ is $\bar{A} \Rightarrow \{9 \rightarrow 8\} \in IFlow$ set;
 $\{8 \rightarrow 12\}$ is $\bar{A} \Rightarrow \{8 \rightarrow 12\} \in IFlow$ set.

Now, only $\{1 \rightarrow 3 \rightarrow 4, 4 \rightarrow 8\}$ should be left in AF set, while PAN set should include $\{1, 4\}$. Only $\{1 \rightarrow 3 \rightarrow 4\}$ passes through both nodes 1 and 4. So, connection $\{1 \rightarrow 3 \rightarrow 4\}$ must be the malicious connection.

4.2 Example 2

Now, let us consider there is only one crosstalk attack connection on each wavelength, as shown in Fig. 7. In this example, there are two wavelengths λ_1 and λ_2 in the network, and we use two panels to represent them. There is one attack connection on each wavelength, connection $\{1 \rightarrow 2\}$ on λ_1 and connection $\{1 \rightarrow 4\}$ on λ_2 . Monitor node 1 can easily determine that these two connections are crosstalk attack connections because both of them originate from monitor node 1. Because there is only one crosstalk attack on each wavelength, and a

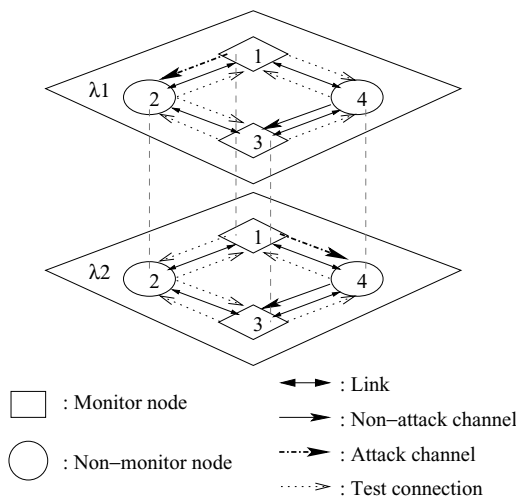


Fig. 7 Two attack connections on different wavelength

crosstalk attack on λ_1 cannot affect connections on λ_2 , our method has already located the malicious connections in the network.

This method is also easily applied into a larger network. Suppose we have M monitors in the network, and each monitor has average d_m degree. Suppose that on each input/output port of a monitor, there are at most c connections, then each monitor only needs to deal with $d_m \times c$ connections' states. In fact, the time complexity and computation complexity are linear to the product of connections and the number of monitors $O(M \times d_m \times c)$.

5 Conclusion

It is very important to detect and localize an attack connection quickly in a transparent AON. Quick detection and localization of an attack source can help avoid losing large amounts of data in an All-Optical Network, however, detecting attack sources is not necessarily the same as putting monitors on all nodes. Since not every wavelength on every link is being used at all times, we propose to use the idle wavelengths to setup diagnostic connections and get the necessary information needed for diagnosis purposes. Placing a relatively small number of monitors on some key nodes in a network can be sufficient for a certain level of performance. In this paper, we focus on the crosstalk attack. First, we give the attack model and monitor model. Based on these models, we determine the monitor placement policy, test connection setting policy, and routing policy. We prove that we can always localize the crosstalk attacks as long as there is no more than one attack on each wavelength in the whole network using our models and policies. Finally, we use several examples to show the efficiency of the method. Moreover, we find this method has fast speed and scalability as well.

References

- Advanced Networks Group, *All-Optical Network Security* (MIT Lincoln Laboratory, December 1998).
- R. Bergman, M. Medard, and S. Chan, Distributed algorithms for attack localization in all-optical networks, *Network and Distributed System Security Symposium* (1998).

3. M. Medard, D. Marquis, R.A. Barry, and S.G. Finn, Security issues in all-optical networks, *IEEE Network* 11(3) (1997) 42–48.
4. M. Medard, D. Marquis, and S.R. Chinn, Attack detection methods for all-optical networks, *Network and Distributed System Security Symposium* (1998).
5. W.T. Anderson, J. Jackel, G.-K. Chang, H.Dai, The monet project-a final report, *IEEE Journal of Lightwave Technology* 18(2) (2000) 1988–2009.
6. N. Golmie, T.D. Ndousse, and D.H. Su, A differentiated optical services model for wdm networks, *IEEE Communication Magazine* (February 2000) pp. 68–73.
7. R.H. Deng, A.A. Lazar, and W. Wang, A probabilistic approach to fault diagnosis in linear lightwave networks, *IEEE Journal on Selected Areas in Communications* 11(9) (1993) 1438–1448.
8. I. Katzela, G. Ellinas, and T.E. Stern, Fault diagnosis in the linear lightwave network, *Dig. LEOS Summer Topical Meeting* (1995) pp. 41–42.
9. I. Katzela and M. Schwartz, Schemes for fault identification in communication networks, *IEEE/ACM Transactions on Networking* 3(6) (1995) 753–764.
10. C.-S. Li and R. Ramaswami, Fault detection, isolation, and open fiber control in transparent all-optical networks, *GLOBECOM '96* 1 (1996) 157–162.
11. C.-S. Li and R. Ramaswami, Automatic fault detection, isolation, and recovery in transparent all-optical networks, *IEEE Journal of Lightwave Technology* 15 (1997) 1784–1793.
12. L. Li, Dynamic wavelength routing in multifiber wdm network, Ph.D. Thesis, Iowa State University (2000).



Arun K. Somani is currently Jerry R. Junkins Chair Professor of Electrical and Computer Engineering at Iowa State University. He earned his

MSEE and Ph.D. degrees in electrical engineering from the McGill University, Montreal, Canada, in 1983 and 1985, respectively. He worked as Scientific Officer for Govt. of India, New Delhi from 1974 to 1982. From 1985 to 1997, he was a faculty member at the University of Washington, Seattle, WA, where he was a Professor of EE and CSE from 1995 onwards. From 1997 to 2002, he served as David C. Nicholas Professor of Electrical and Computer Engineering at Iowa State University. Professor Somani's research interests are in the area of fault tolerant computing, computer communication and networks, wireless and optical networking, computer architecture, and parallel computer systems.



Tao Wu received the B.S. and M.S.E.E. degrees in telecommunication engineering from the University of Electronic Science and Technology of China, Sichuan, China, in 1993 and 1996, respectively, and the Ph.D. degree in computer and electrical engineering from Iowa State University, Ames, in 2003.

He is currently a Software Engineer with Microsoft Corporation. His research interests are in the area of WDM-based optical networking, network security, and image processing.