

Cross-Talk Attack Monitoring and Localization in All-Optical Networks

Tao Wu, *Member, IEEE*, and Arun K. Somani, *Fellow, IEEE*

Abstract—The effects of an attack connection can propagate quickly to different parts of an all-optical transparent network. Such attacks affect the normal traffic and can either cause service degradation or outright service denial. Quick detection and localization of an attack source can avoid losing large amounts of data in an all-optical network. Attack monitors can collect the information from connections and nodes for diagnostic purpose. However, to detect attack sources, it is not necessary to put monitors at all nodes. Since those connections affected by the attack connection would provide valuable information for diagnosis, we show that by placing a relatively small number of monitors on a selected set of nodes in a network is sufficient to achieve the required level of performance. However, the actual monitor placement, routing, and attack diagnosis are challenging problems that need research attention.

In this paper, we first develop our models of crosstalk attack and monitor node. With these models, we prove the necessary and sufficient condition for one-crosstalk-attack diagnosable networks. Next, we develop a scalable diagnosis method which can localize the attack connection efficiently with sparse monitor nodes in the network.

Index Terms—All-optical network, attack, crosstalk, diagnosability of attacks, sparse monitoring.

I. INTRODUCTION

AN all-optical network (AON) is a network where the user-network interface is optical and the data do 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. First and foremost is loss of an opportunity to detect security problems. 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 attack capability. Transparency and nonregeneration features make attack detection and localization difficult.

A. 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. Fig. 1 shows the difference between a component failure and an attack connection. Fig. 1(a) shows that link (2,4) fails. Then, re-routing connection c_2 can solve this problem. In Fig. 1(b), an attack connection c_2 is introduced and it affects a normal connection c_1 . If we still treat such scenario as a component failure, and re-routing both c_1 and c_2 to new paths, then, we can see that this method does not solve any problem: attack connection c_2 can still affect connection c_1 .

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 a link or 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 (20 dB higher than normal power), much beyond the expected normal value. When this connection passes through a wavelength selective switch, the leakage energy (crosstalk) from this malicious connection can be significant and affect the normal connections passing through

Manuscript received April 14, 2003; revised October 1, 2004; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor A. Fumagalli. This work was supported in part by a contract from G. W. U, funded by the Defense Advanced Research Projects Agency under grant N66001-00-1-8949 and co-funded by NSA and NSF grant numbers 0306007 and 0323374.

The authors are with the Dependable Computing and Networking Laboratory, Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (e-mail: wutao@microsoft.com; arun@iastate.edu).
Digital Object Identifier 10.1109/TNET.2005.860103

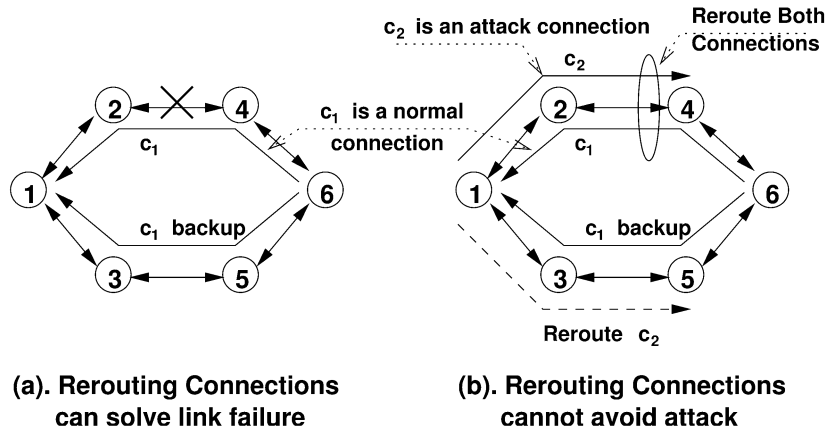


Fig. 1. Difference between failure and attack.

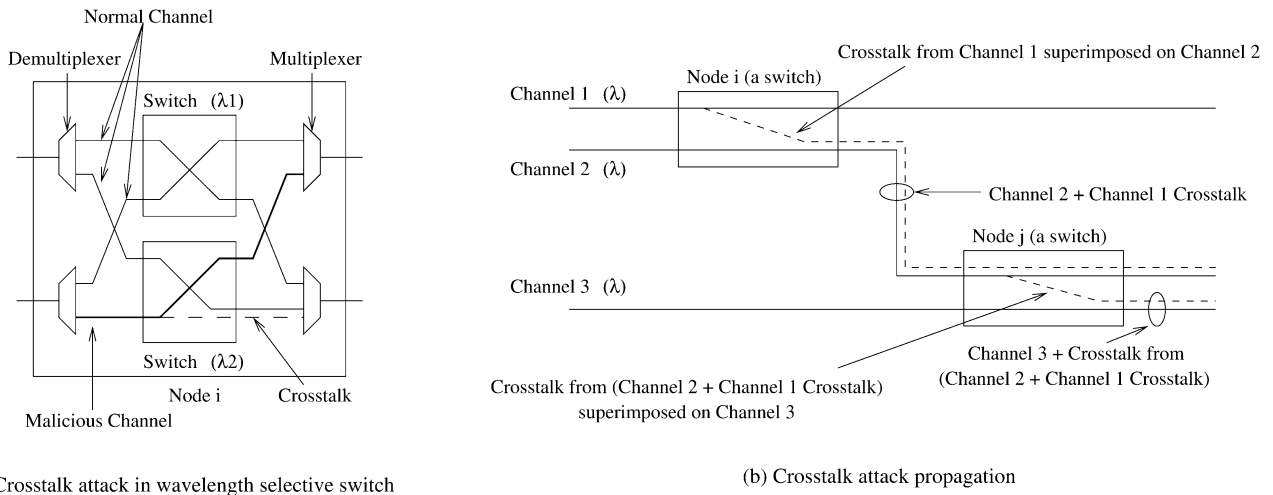


Fig. 2. Example of crosstalk attack.

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 a link or node with it, but also may induce attack capabilities to those connections that are affected [1], [2]. Fig. 2(a) depicts a switch supportive wavelength routing [1], [2]. The crosstalk attack happens at a wavelength switch and only affects those normal connections using the same wavelength as they pass through the same switch. Fig. 2(b) shows the crosstalk attack propagation mechanism [1], [2]. Channel 2 and channel 1 pass through the same switch. Some of the high energy is coupled to channel 2 from channel 1. This allows channel 2 to also acquire attack capability. This propagation characteristic makes attack connection localization more difficult.

B. Related Work

There are many reasons why, in AONs, attacks must be detected and identified at all nodes in the network. One reason is that the high data rate of AONs requires the attack detection as soon as possible. Another reason is that a service disruption attack can spread throughout the network. There is some prior work [1]–[4] done in the area of attack localization in AONs. These papers only considered networks in which all nodes had

monitors. Other methods [5]–[7] can provide probabilistic approaches to fault diagnosis in network. They are not suitable for the attack localization problem, because these approaches only identify a most likely set of locations instead of determining the exact location of the source. We, therefore, still need further steps to analyze where the exact location of the source is.

The capability of an optical monitoring module have been researched by several researchers [8], [9]. Generally, an optical monitor device is expensive and can measure single channel optical power. It is doubtful that a monitor device will become less expensive in the near future. Therefore, to install monitors for all wavelengths at all nodes in a network is likely to be very expensive.

C. Motivation

A network management system using supervisory channels [10], [11] can detect and monitor the performance of network devices remotely. Thus, detecting attack sources does not necessarily require equipping all nodes with monitors. Since the connections affected by an attack connection can also provide valuable information about distribution of attack locations, if we can monitor all connections in whole networks, we may obtain a large amount of information needed for diagnostic purpose. If

normal connections cannot provide sufficient information, we derive more monitoring information by establishing some additional test connections. We show that the diagnostic information obtained from regular established and test connection together is sufficient to diagnose an attack connection and its location.

The rest of this paper is organized as follows. First, we provide a crosstalk attack and a monitor model based on some previous work [1], [2], [4], [8], [10], [11]. Next, we develop the necessary and sufficient conditions to localize a single crosstalk attack in the whole network. Following that, a sparse monitor placement policy, a test connection setup policy, as well as a routing policy are developed to aid the diagnostic process. Based on these policies, we prove that we can always localize all malicious crosstalk attacks as long as there is no more than one crosstalk attack on any wavelength in the network with sparse monitors. In the following section, we show some examples to explain our algorithm and demonstrate its capabilities. Finally, we present our conclusions.

II. CROSSTALK ATTACK AND MONITOR MODEL

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

A. Node Model

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

- 1) A node can perform routing and switching. Without the switching capability a node cannot propagate a crosstalk attack to other normal connections. Thus, nodes without switching capabilities should 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 *nonmonitor node*.

B. Crosstalk Attack Model

As shown in Fig. 2(a), the crosstalk attack connection only affects the same wavelength connections at the wavelength selective switch nodes. The following items describe our crosstalk attack and its propagation model.

- 1) *Up-stream and down-stream neighbor nodes*: For a node on the path of a connection, 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 (20 dB higher or more than normal signal) than that expected on a normal connection. In this paper, we assume that an OAF enters the network as a normal signal:

upload to a network switch from local fiber. Thus, we can eliminate the following probability: this OAF is injected to a fiber far away from a switch, and other connections (could be in same wavelength or different wavelengths) in that fiber are affected. 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 node is called a *primary attacked node* (PAN) if there is an OAF originating, terminating or passing through this node.
- 4) A normal connection sharing the same nodes with an OAF will be affected. This affected connection is called 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 A , then the connection C has attack capability only at node $DNN(A, C)$, and we call $DNN(A, C)$ as a *secondary attacked node* (SAN).
- 5) A normal connection influenced by an SAF is called a *final attacked flow* (FAF). The FAF does not have the attack propagation capability.
- 6) 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, while the union of AFN and SAN is called an *innocent node* (INode) set.
- 7) *Power Level*: Because the OAF, the SAF, and the FAF have different attack capabilities, the power level of these connections follow the relation

$$P(OAF) > P(SAF) > P(FAF) > P(AFF).$$

As shown in Fig. 2(b), connection (channel) 1 is the OAF, connection (channel) 2 is the SAF, and connection (channel) 3 is the FAF. Node i is the PAN and node j is SAN. Connection 1 can propagate its malicious attack to connection 3 by affecting connection 2. It is expected that a OAF pollutes any connections passing through a PAN, and a SAF pollutes any normal connection passing through a SAN.

C. Monitor Node Model

We call a node equipped with a monitor device as a *monitor node*, or a monitor. A node without a monitor device is called a *nonmonitor node*. The most significant feature that can differentiate crosstalk attack from other attacks is its extremely high power. Based on this, we select an optical power detector as our monitor device. Other equipment (such as a BER detector) is also helpful. However, there is one major drawback of such equipment: more time is required to analyze signals. For example, the optical signal has to be converted into electrical signals before the BER detector can check that signal's bit error rate. Moreover, such equipment is more expensive than a power detector. Thus, in this paper, only an optical power detector is selected as the monitor device.

- 1) A monitor node can monitor all traffic passing through it, including the traffic that originated/terminated at the node.

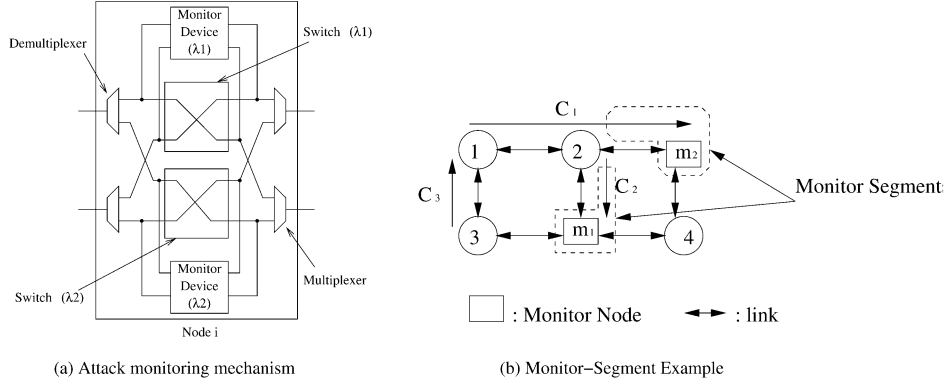


Fig. 3. Attack monitoring mechanism and monitor segment.

- 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 above the expected value. A special case is that sometimes more than one connections' power levels may be above the threshold. Our monitor model can treat this in two different ways as described in the next bullet. Several researchers have developed methods [1], [4], [10] to measure the power levels to monitor the input and output connection power level. We use similar methods to monitor separate wavelengths in the input and output fibers. The crosstalk attack monitoring mechanism for selective wavelength switches is shown in Fig. 3(a). In this figure, one monitor device is installed in a switch to monitor both input and output signals power on the same wavelength. Signal on different wavelength is monitored by different monitor device. If wavelength detection can be synchronized in the entire network, then, with "round-robin" scheme, one monitor device in a switch is enough to monitor all wavelengths.
- 3) If a connection with very high power (20 dB higher than normal) 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/nonattack status at a monitor. We use A/\bar{A} to indicate the attack/nonattack status of the connection.
- 4) 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 the status of OAF is set to A , while the status of the other SAFs are set to \bar{A} .
 - (b) All these connections are SAFs. In this situation, the monitor can detect several connections which have the similar unexpected equal high powers, then the status of all these connections in this monitor are set to A .

III. NECESSARY AND SUFFICIENT CONDITIONS

We assume that there is at most one OAF in the whole network. A network is called one-OAF diagnosable if a single OAF

can always be detected and localized from monitor information available from all the present connections. Next, we discuss the necessary and sufficient condition for one-OAF diagnosable network.

Let the network be denoted by a graph $G(V, E)$. V is the set of nodes, $\{v_0, v_1, \dots\}$, and E is the set of fiber links, $\{e_1, e_2, \dots\}$. Let M denote the set of monitor nodes, and let N denote the set of nonmonitor nodes, $M \subseteq V$, $N \subset V$, and $M \cup N = V$.

On this graph $G(V, E)$, some connections are established. Let $C = R \cup T$ denote the set of connections in the network, where R is the set of regular connections, and T is the set of test connections.

Let c_i be a connection consisting of node $\{u_0, u_1, u_2, \dots, u_k, \dots, u_m\}$. Let $U(c_i)$ denote the set of nodes on connection c_i 's path. Then, c_{ij} denotes a one-hop segment $(u_j \rightarrow u_{j+1})$ on connection c_i .

There can be three kind of relations between a monitor and a connection:

- 1) *direct monitor*: a monitor m is a direct monitor of a connection c if $m \in U(c)$;
- 2) *one-hop monitor*: a monitor m is a one-hop monitor of a connection c if $m \notin U(c)$ and $\exists (u \rightarrow m)$ where $u \in U(c)$;
- 3) *nonmonitor*: a monitor m is a nonmonitor of a connection c if $m \notin U(c)$ and $\nexists (u \rightarrow m)$ where $u \in U(c)$.

A. Monitor Segment

Monitor Segment: A monitor segment mc is a one-hop segment $(u \rightarrow m) \in$ connection c that ends at monitor node m . Let MSC denote the set of the monitor segments. Let $m_i c_j$ denote all elements in one particular monitor segment: one-hop segment $(u \rightarrow m_i) \in c_j$ ends at monitor node m_i . Mostly, we use m_{sc} to denote a common monitor segment, and m_{sc_k} as one common monitor segment in monitor segment set MSC . Two monitor segments are shown in Fig. 3(b), one is made by connection C_2 and monitor node m_1 , denoted by $m_1 C_2$, while the other is made by one-hop segment on connection C_1 , from node 2 to node m_2 , and monitor node m_2 , denoted by $m_2 C_1$.

A monitor segment $m_{sc} = (u \rightarrow m)$ is monitoring a connection c if and only if the following two conditions are satisfied:

- 1) if the monitor m is a *direct monitor* of this connection, while the segment $(u \rightarrow m) \in c$; or

TABLE I
TRUTH TABLE FOR MONITOR SEGMENT AND ITS
MONITORING/NONMONITORING CONNECTIONS

Relation	$S(msc)$	$S(c)$
msc monitoring c	A	<i>uncertain</i>
(msc, c)	\bar{A}	<i>IF</i>
msc non-monitoring c	A	<i>IF</i>
	\bar{A}	<i>uncertain</i>

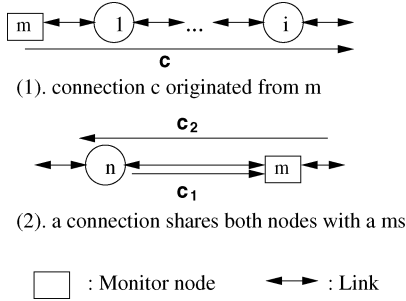


Fig. 4. Special monitor segment.

- 2) if the monitor m is a *one-hop monitor* of a connection c , where $u \in U(c)$, and $m \notin U(c)$.

For example, in Fig. 3(b), monitor m_2 is a direct monitor for connection C_1 , and monitor m_1 is a one-hop monitor for connection C_1 . According to our definition, both monitor segments m_1C_2 and m_2C_1 are monitoring connection C_1 , and none of them is monitoring connection C_3 . Let (msc, c) denote this relation between monitor segment msc and connection c . Consequently, the status of the segment $(u \rightarrow m)$ indicated by monitor m is the *status of the monitor segment*, denoted by $S(msc)$. For example, in Fig. 3(b), if the status of C_2 in monitor m_1 is indicated as A , then the status of the monitor segment m_1C_2 is A . $S(msc)$ can be either A or \bar{A} .

The *status of a connection* can be either *IF* or *uncertain*. *IF* means that the connection is determined as *IF*, and *uncertain* means that the connection cannot be determined either as *IF* or as *OAF*. Let $S(c)$ denote the status of connection c . Table I shows the relations between a monitor segment status and its monitoring connection's status.

For a connection c , which is not being monitoring by msc , we say that msc has a *nonmonitoring* relation with c . Table I also shows the relations between a monitor segment and its nonmonitoring connection.

Fig. 4 depicts two special cases of monitor segment.

Fig. 4(1) shows the monitor m as the originating node of the connection c . For this case, monitor m and connection c makes up a special monitor segment msc , and only connection c is monitored by this monitor segment, while all other connections are not monitored. If $S(msc) = A$, all other connections can be identified as *IF*.

Fig. 4(2) shows the relation between a monitor segment mc_1 and a connection c_2 , where $c_1 \notin c_2$, and $n, m \in U(c_2)$. In this case, both c_1 and c_2 share the same nodes n and m . While

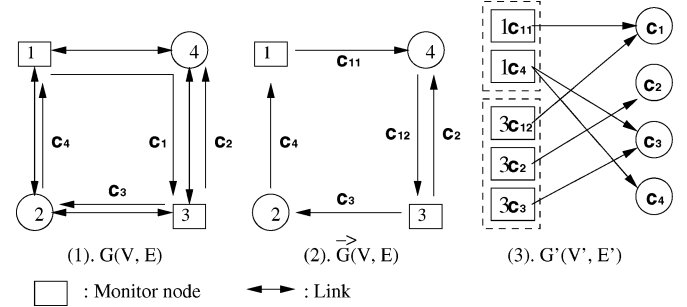


Fig. 5. Monitor segment example.

it seems that c_2 is monitored by msc_1 , in fact the relation between connection c_2 and the monitor segment msc_1 is *nonmonitoring*. We can explain it in two ways. First, according to our definition of *monitoring*, the only two cases of monitoring are either the segment is a part of the monitored connection, or the monitored connection does not pass through the monitor. The example provided by Fig. 4(2) does not fit either of these definitions. Second, according to truth table, suppose the status of msc_1 is \bar{A} . We cannot make sure if c_2 is *IF* or not. According to Table I, this is a *nonmonitor* relation.

We can represent the monitor nodes and monitor segments in graph $G(V, E)$, using a bipartite graph $G'(V', E')$. One side of the bipartite graph shows the monitor segments and the other side of the graph shows the connections. The graph is shown in Fig. 5(1) and the corresponding bipartite graph in Fig. 5(3) depicts the connections set up in the network. Fig. 5(2) shows a graph with all connections separated into one-hop segments. For example, c_{1-1} is the first segment of connection c_1 shown in Fig. 5(1). In graph $G'(V', E')$, the vertices set $V' = \{mc_{ij}\} \cap \{C_k\}$ consists of the monitor segments and the connection, i.e., $mc_{ij} \in MC$, and $c_k \in C$. For example, $3c_{12}$ is a monitor segment made up by monitor node 3 and one-hop segment c_{12} shown in Fig. 5(2). An edge in G' depicts a relation between a monitor segment and a connection. In this figure, a directed edge from a monitor segment msc to a connection c describes the monitoring relation between this pair of monitor segment and connection. A pair (msc, c) denotes the edge.

Let $\Gamma(msc_i) = \{c_j | (msc_i, c_j) \in E'\}$ denote the set of connections monitored by a monitor segment msc_i . Let $\Gamma^{-1}(c_i) = \{msc_j | (msc_j, c_i) \in E'\}$ denote the set of monitor segments monitoring a connection c_i .

A connection is called *UnIdentified* if we cannot obtain the status of the connection directly from the set of all monitor segments' status in the network. Fig. 6 shows an example to help understand this concept. A network and its connections are shown in Fig. 6. If connection c_1 is the *OAF*, according to the truth table we can identify the status for both the monitor segments and connections, as shown in Table II. The monitor segments can only identify the status of c_2 and c_3 as *IFs*, and status of connection c_1 as *uncertain* according to both monitor segments' results.

B. Theorem and Proof

Lemma 1: In any network, if this system is one-*OAF* diagnosable, then the $|UnIdentified\ connection| \leq 1$.

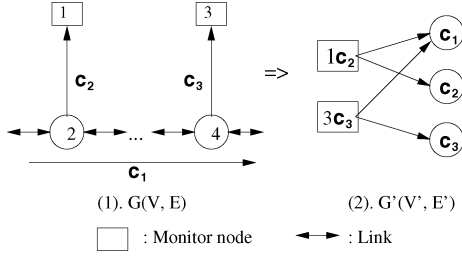


Fig. 6. UnIdentified connection.

TABLE II

STATUS OF THE CONNECTIONS AND THE MONITOR SEGMENTS SHOWN IN FIG. 6

monitor-segments	$S(msc)$	$S(c_1)$	$S(c_2)$	$S(c_3)$
$S(1c_2)$	A	<i>uncertain</i>	<i>uncertain</i>	IF
$S(3c_3)$	A	<i>uncertain</i>	IF	<i>uncertain</i>

Proof: Obvious. \blacksquare

Lemma 2: For an arbitrary connection c_i , if c_i is UnIdentified, then $S(msc_i) = A$ for $\forall msc_i \in \Gamma^{-1}(c_i)$.

Proof: Suppose one $msc_k \in \Gamma^{-1}(c_i)$ has a status $S(msc_k) = \bar{A}$. Then, according to Table I, $S(c_i) = IF$. This contradicts the condition. \blacksquare

Theorem 3: For any arbitrary pair of connections c_i and c_j in a given monitor segment graph G' , if $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$, then for this network with the connection set C , $|UnIdentified\ connection| \leq 1$ holds.

Proof: (Necessity). Suppose $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$, then there are two possibilities.

- 1) $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j) = \emptyset$. Then for all $msc_x \in MSC$, there always exists a *nonmonitoring* relation to both c_i and c_j . If for all $msc_x \in MSC$, $S(msc_x) = \bar{A}$, then according to Table I, the status for both c_i and c_j must be uncertain. All other connections will have a status of IF . Thus, these two connections will be UnIdentified, and $|UnIdentified\ connection| > 1$.
- 2) $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j) \neq \emptyset$. Fig. 7(1) shows a network which has n nodes and at least two connections, $c_i = \{2 \rightarrow 1\}$ and $c_j = \{2 \rightarrow 3\}$. Assume that both node 1 and 3 are monitor nodes and node 2 is nonmonitor node, as shown in Fig. 7(2). Fig. 7(3) shows the monitor segment graph G' , where monitor segment msc_m to msc_n denote those monitor segments passing through node 2 except monitor segments $1c_i$ and $3c_j$. According to Fig. 7(3), $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j) \neq \emptyset$. Suppose c_i is the OAF, then all monitor segments would have state A , which make both c_i and c_j in uncertain status. Again, $|UnIdentified\ connection| > 1$.

(Sufficiency). Suppose $|UnIdentified\ connection| > 1$. Then, there are only three possibilities.

- 1) At least two UnIdentified connections have $\Gamma^{-1}(c) = \emptyset$. Arbitrarily pick a pair of connections c_i and c_j from this UnIdentified connection set, and we get $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j) = \emptyset$. Obviously, this contradicts our condition.

- 2) One UnIdentified connection c_i has $\Gamma^{-1}(c_i) = \emptyset$, and at least another UnIdentified connection c_j has $\Gamma^{-1}(c_j) \neq \emptyset$. Then, according to Lemma 2, in graph G' , there exists at least one edge (msc_j, c_j) while $S(msc_j) = A$. Because of $\Gamma^{-1}(c_i) = \emptyset$, the monitor segment msc_j has nonmonitoring relation with c_i . According to Table I, if $S(msc_j) = A$, then $S(c_i) = IF$. Thus, c_i is not UnIdentified. This contradicts the assumption.
- 3) At least 2 UnIdentified connections have $\Gamma^{-1}(c) \neq \emptyset$. Arbitrarily select two connections c_i and c_j from this set. There are two possible cases:

Case I: $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$. Suppose one monitor segment $msc_i \in \Gamma^{-1}(c_i)$ but $msc_i \notin \Gamma^{-1}(c_j)$. Then, edge (msc_i, c_j) does not exist in graph G' . Thus, monitor segment msc_i must have nonmonitoring on c_j . Because c_i is UnIdentified, according to lemma 2, $S(msc_i) = A$, which implies that $S(c_j) = IF$, referring to Table I. Thus, c_j is not UnIdentified, this contradicts our assumption.

Case II: $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$. This contradicts the condition. Thus, if $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$, then $|UnIdentified\ connection| \leq 1$ always holds. \blacksquare

C. Global Status of a Connection According to Monitor Segment

For a given monitor segment msc_i , there are only two relations between msc_i and an arbitrary connection c_j : monitoring or nonmonitoring. Let monitoring and nonmonitoring relations be denoted by two values: 1 and 0, respectively. Then, a vector $\overrightarrow{r_i}$ can be used to denote such relation between msc_i and all connections in the network:

$$\overrightarrow{r_i} = \{r_i(c_j) | c_j \in C\}$$

and a *Relation Matrix* R can be created as

$$R = \begin{pmatrix} \overrightarrow{r_1} \\ \overrightarrow{r_2} \\ \dots \\ \overrightarrow{r_m} \end{pmatrix} = \begin{pmatrix} r_1(c_1) & r_1(c_2) & \dots & r_1(c_n) \\ r_2(c_1) & r_2(c_2) & \dots & r_2(c_n) \\ \dots & \dots & \dots & \dots \\ r_m(c_1) & r_m(c_2) & \dots & r_m(c_n) \end{pmatrix}$$

where $r_i(c_j)$ denotes the relation between msc_i and c_j

$$r_i(c_j) = \begin{cases} 1, & \text{if } msc_i \text{ monitor } c_j \\ 0, & \text{if } msc_i \text{ not monitor } c_j. \end{cases}$$

With a given status of the monitor segment, we can get the corresponding status of all connections. For example, in Table II, according to the status of monitor segment $S(1c_2)$, all status of three connections, $S(c_1)$, $S(c_2)$, and $S(c_3)$, can be derived. Let us assume that there are total n connections and m monitor segments in the network. Let vector $\overrightarrow{S_i(c)} = \{S_i(c_1), S_i(c_2), \dots, S_i(c_n)\}$ denote all connections' status given by msc_i , where $S_i(c_j)$ denotes status of c_j derived from status of msc_i .

Now, set two possible connection status, IF and *uncertain*, as 1 and 0, respectively. Similarly, set two possible monitor segment status, A and \bar{A} , as 1 and 0, respectively. Then, according

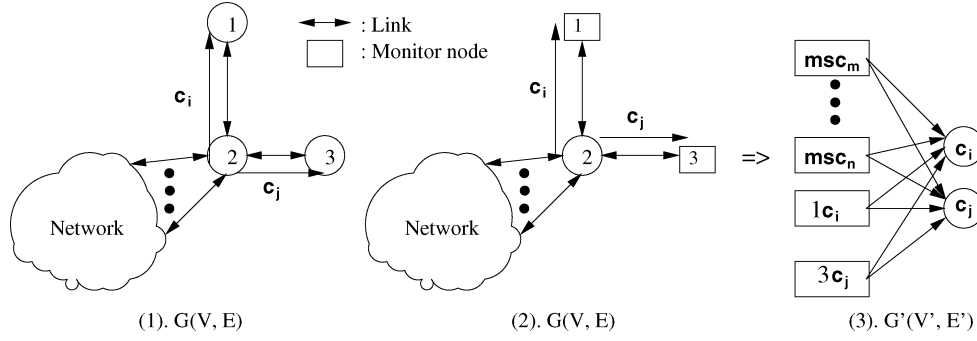


Fig. 7. Two connections with same $\Gamma^{-1}(c)$ sets.

to the truth table, Table I, we can derive $S_i(c_j)$ from $S(msc_i)$ and $r_i(c_j)$:

$$S_i(c_j) = S(msc_i) \oplus r_i(c_j)$$

while $\overrightarrow{S_i(c)}$ from $S(msc_i)$ and $\overrightarrow{r_i}$:

$$\overrightarrow{S_i(c)} = [S(msc_i) \cdot \vec{1}] \oplus \overrightarrow{r_i}$$

where $\vec{1}$ is a $1 \times n$ vector, and \oplus is XOR.

Then, a *Status Matrix* can be obtained

$$\begin{pmatrix} \overrightarrow{S_1(c)} \\ \overrightarrow{S_2(c)} \\ \dots \\ \overrightarrow{S_m(c)} \end{pmatrix} = \begin{pmatrix} S_1(c_1) & S_1(c_2) & \dots & S_1(c_n) \\ S_2(c_1) & S_2(c_2) & \dots & S_2(c_n) \\ \dots & \dots & \dots & \dots \\ S_m(c_1) & S_m(c_2) & \dots & S_m(c_n) \end{pmatrix} \\ = \left\{ \begin{pmatrix} S(msc_1) \\ S(msc_2) \\ \dots \\ S(msc_m) \end{pmatrix} \times \overrightarrow{1} \right\} \oplus \begin{pmatrix} \overrightarrow{r_1} \\ \overrightarrow{r_2} \\ \dots \\ \overrightarrow{r_m} \end{pmatrix}.$$

Let $S(c_j)$ denote the sum of the j th column in the above matrix

$$S(c_j) = \sum_{i=1}^m S_i(c_j) = \sum_{i=1}^m [S(msc_i) \oplus r_i(c_j)].$$

Now, if we define a new operation $*$ as

$$\overrightarrow{X} * \overrightarrow{Y}^T = \sum_{i=1}^n [x_i \oplus y_i]$$

where \overrightarrow{X} and \overrightarrow{Y} are $1 \times n$ vectors, and x_i and y_i are their elements, then, vector $\overrightarrow{S(c)}$ can be denoted by $S(msc_i)$ and the relation matrix is as follows:

$$\begin{aligned} \overrightarrow{S(c)} &= (S(c_1) \quad \dots \quad S(c_n)) \\ &= (S(msc_1) \quad \dots \quad S(msc_m)) \\ &\quad * \begin{pmatrix} r_1(c_1) & \dots & r_1(c_n) \\ \dots & \dots & \dots \\ r_m(c_1) & \dots & r_m(c_n) \end{pmatrix}. \end{aligned}$$

The global status of connection c_j can be obtained as

$$\text{Status of } c_j = \begin{cases} IF, & \text{if } S(c_j) > 0 \\ UnIdentified, & \text{if } S(c_j) = 0. \end{cases}$$

This provides the algorithm to locate the attack connection on each wavelength.

In this paper, we assume that a connection will not pass a device that will affect the connection's power dramatically, for example, clamped amplifier. However, if a connection passes through a clamped amplifier, that does not mean our algorithm is useless. We can simply separate this connection into two parts, before the amplifier and after the amplifier, and treat the two parts as two different connections. Then, our algorithm can still be implemented. For example, suppose there is a network as shown in Fig. 5(1), and there is a clamped amplifier at node 4. Connection c_1 is passing through that amplifier. Then, we can separate c_1 into two parts, c_{11} and c_{12} , as shown in Fig. 5(2), and treat them as different connections. By keeping all monitor segments in Fig. 5(3), and replacing node c_1 with c_{11} and c_{12} , we can get a new bipartite graph. The necessary and sufficient condition still works for this new graph.

IV. EFFICIENT SPARSE MONITORING POLICY AND ROUTING ALGORITHM

The previous section provides the necessary and sufficient condition to one-OAF diagnosable network, but how to place the monitors and setup test connections is still an open question. In this section, first we propose a sparse monitoring method, that is to place the monitor and set regular and test connections, and then we prove that any network defined using such method is one-OAF diagnosable. Before describing the detail, we need to introduce some definitions.

- 1) *One-hop-distance monitor (OHM)*: If a monitor is connected directly to a nonmonitor node, then this monitor is an OHM to this nonmonitor node.
- 2) *Degree of a node*: The degree of a node u is the number of links that are incident on node u . It is denoted by $D(u)$.
- 3) *Pendant node*: A node with degree one is called a pendant node.

A. Sparse Monitoring Policy for Sparsely Connected Network

Based on the necessary and sufficient conditions, how to optimize monitor node placement is a challenge. However, this paper does not try to solve this problem. Here we only try to give one possible solution that will satisfy the necessary and sufficient conditions, and we will prove it in the latter part of this section.

1) 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.

The following is our sparse monitor placement policy:

- a) for a nonmonitor node u , it must have $D(u)$ OHMs;
- b) for a node u with a pendant node as its neighbor, it must be a monitor node.

Because of this strict monitor placement policy, a sparsely connected network needs fewer monitor nodes than a densely connected network does. For example, for a star network, setting the central node to monitor node is enough to satisfy our placement policy. For a fully connected network, because $D(u)$ is large, the number of required monitor nodes will be much greater than the star topology network needs, if the total number of nodes are same in both networks.

2) Test Connection Setup Policy

We assume that each link in the network is bidirectional so that there are two fibers for two directions in each link. According to our monitoring mechanism, there are two kinds of connections: the *normal connections*, which are set up by users, and the *test connections*, which are requested by the network management system. Establishing test connections is an important step in determining if a node is a PAN or not. We use the following rules to set up test connections.

Test Connection Set Up

For a nonmonitor node u , if there is a normal connection on wavelength λ passing through or terminating at a node u , one test connection from node u to each OHM is needed if no normal connection provides a monitor segment on the corresponding link.

Fig. 8 shows a network that has two monitor nodes and two nonmonitor nodes. There are two normal connections, connection $c_1(1 \rightarrow 2 \rightarrow 4)$ and connection $c_2(4 \rightarrow 3)$. According to our test connection policy, for each nonmonitor node, if there is a normal connection passing through or terminating at a node u , one test connection from this node to each OHM is needed, if no normal connection provides a monitor segment on the corresponding link. In this example, both node 1 and node 4 satisfy this condition. Thus, for node 4, two test connections from 4 to monitor node 2 and 3 are required. Because connection c_2 already exists on link (4, 3), only one test connection $t_1(4 \rightarrow 2)$ is necessary. From this example, we can find that the test connection will not affect normal

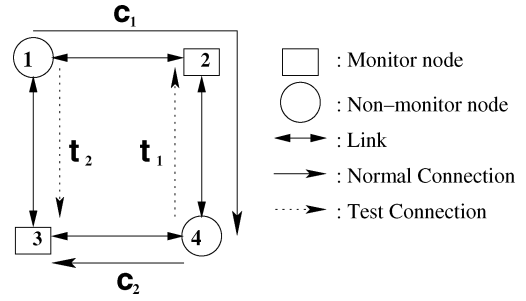


Fig. 8. Example of test connection.

connections: test connections only use those links that are not occupied by normal connections, and normal connections also provide detection function. If a normal connect requires a link used by a test connection, we can just disconnect the test connection, free that link to the normal request, and still keep our diagnosing capability.

3) Routing policy

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

No more than one normal connection (excluding test connection) originated from a nonmonitor node may pass through less than three different nodes (including source and destination). Otherwise, any path selection algorithm, such as shortest path algorithm, can be used.

According to our crosstalk attack model, the crosstalk attack only affects the same wavelength connection at the wavelength selective switch. To simplify our analysis, in the following parts, we assume that there is no wavelength converter in the whole network, and for each link, only one fiber exists in each direction.

In the following, we prove that a network is always one-OAF diagnosable if it is designed using the models and policies described above.

Claim 4: With the above monitor placement, test connection setup, as well as routing policies, a network with one fiber on each link and without wavelength converter is one-OAF diagnosable on each wavelength.

Proof: With a given network denoted by graph $G(V, E)$, let M denote the set of monitor nodes, and let N denote the set of nonmonitor nodes, $M \subseteq V, N \subset V$, and $M \cup N = V$. Let $C = R \cup T$ denote the set of connections in the network, where R is the regular set of connections, and T is the set of test connections. Let c_i be a connection consisting of node $\{u_0, u_1, u_2, \dots, u_k, \dots\}$. Let $U(c_i)$ denote the set of nodes on connection c_i 's path. Then, c_{ij} denotes a one-hop segment ($u_j \rightarrow u_{j+1}$) on connection c_i .

First, in each link, we assume there is only one wavelength on each direction.

- 1) According to the sparse monitor placement policy, for a nonmonitor node, its neighbor node must be a monitor node, which means, on each link, at least one node is a monitor node. Thus, for one connection c , at least one monitor node $m \in U(c)$. According to the definition of

monitor segment, at least one monitor segment monitors this connection, i.e., $\Gamma^{-1}(c) \neq \emptyset$ holds $\forall c \in C$.

- 2) According to Theorem 3, for any arbitrary pair of connections, the necessary and sufficient condition for a one-OAF diagnosable network is that their monitoring monitor segments set should not be the same. Now, suppose there exist two connection c_i and c_j such that $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$, then there are two possibilities.

a) At least one of them originates from a monitor node. Without loss of generality, we assume that c_i originates from monitor m . According to previous discussion about special cases of monitor segment, any connection originating from a monitor can make up a special monitor segment that would only monitor this connection. Thus, a monitor segment mc_i made up by c_i and m does not monitor other connections including c_j , i.e., $mc_i \in \Gamma^{-1}(c_i)$ and $mc_i \notin \Gamma^{-1}(c_j)$, and therefore, $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$. This is a contradiction of our assumption.

b) None of these connections originates from a monitor node. Then, there are two possible cases.

i) The sources of these two connections are different, i.e., c_i 's source is node n_i , and c_j 's source is node n_j . Because at least one monitor exists on each link, $DNN(n_i, c_i)$ and $DNN(n_j, c_j)$ must be monitor nodes. Let $m_i = DNN(n_i, c_i)$ and $m_j = DNN(n_j, c_j)$. No matter whether $m_i = m_j$ or not, because $n_i \notin U(c_j)$ and $n_j \notin U(c_i)$, monitor segment $m_i c_i$ can only monitor connection c_i , while monitor segment $m_j c_j$ can only monitor connection c_j . Thus, $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$. This contradicts the assumption.

ii) The two connections have a common nonmonitor source node n . According to routing policy, at least one connection should pass three nodes. Without loss of generality, let us assume that c_i has at least three different nodes on its path, and the first three nodes on its path are: n, m_i , and u_i . For each link, because only one wavelength exists on each direction and at least one monitor node exists on it, the first two nodes on c_j 's path should be n and m_j , where $m_j \neq m_i$ and $m_i \notin U(c_j)$. Now let us consider node $u_i \in U(c_i)$.

A) If u_i is a monitor node, then segment $(m_i \rightarrow u_i) \in U(c_i)$ plus monitor u_i makes a monitor segment that does not monitor connection c_j . Thus, $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$, and it is contradiction of the assumption.

B) If u_i is a nonmonitor node, then according to monitor placement policy, there should be at least another OHM for node u_i besides monitor m_i . We use m' , $m' \neq m_i$ to denote one of such OHMs. According to test connection setup policy, either normal connection segments or test connections should exist as $(u_i \rightarrow m_i)$ and $(u_i \rightarrow m')$. If $u_i \in U(c_j)$, then connection c_j should be monitored by a monitor segment composed of seg-

ment $(u_i \rightarrow m_i)$ and monitor m_i , while connection c_i should not be monitored by the same monitor segment. Alternatively if $u_i \notin U(c_j)$, then connection c_i should be monitored by a monitor segment composed by segment $(u_i \rightarrow m')$ and monitor m' , while connection c_j should not be monitored by the same monitor segment. We can draw same conclusion, $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$, from both cases, and this contradicts our assumption.

From the above analysis, we know that we cannot find two connections in the network such that $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$ based on previous policies, with the assumption of one wavelength on one direction. Thus, under this condition, the network is one-OAF diagnosable.

Next, we agree that a multi-wavelength network is one-OAF diagnosable for each wavelength if there is no wavelength converter.

Although there are multiple wavelengths 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 any relationship to affect the normal connections on other wavelengths. We have already shown that we can diagnose all connections on one wavelength. Therefore, we can always detect OAFs on each wavelength in the whole network, as long as there is only one OAF on the wavelength. ■

B. Connection Routing Algorithm in One-OAF Networks

We also develop one practicable routing algorithm. Without loss of generality, we develop a variant of the shortest-path algorithm that satisfy the above routing constrains. Fig. 10 shows the flow chart for the algorithm.

Suppose maximum output degree of network node is $\text{Max}\{D(u)\} = d_N$, then, with this routing algorithm, at most d_N connections should be checked before we can make decision for the connection request.

V. EXAMPLE OF SPARSELY CONNECTED NETWORK

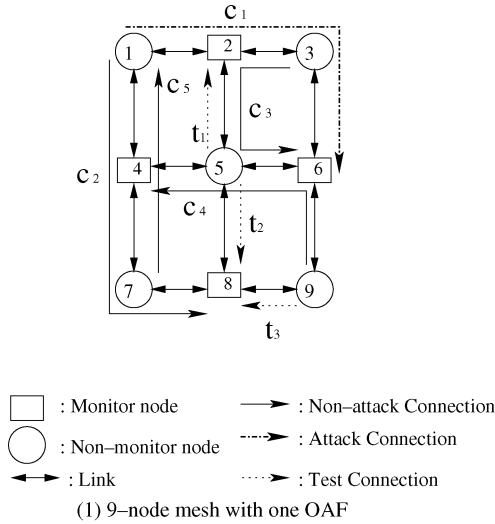
Fig. 9(1) depicts a nine-node bidirectional mesh network. According to sparse monitor placement policy, four monitor nodes are necessary in this network. Here, we choose nodes 2, 4, 6, and 8 as the monitor nodes, and the rest nodes as nonmonitor nodes. By considering that attack connection can only affect connections in same wavelength, to simplify our example, we assume that only one wavelength is supported in this network.

Suppose we have some normal connections and only one of them is a OAF.

The current normal connection set is

Normal connection set

$$= \{c_1(1 \rightarrow 2 \rightarrow 3 \rightarrow 6), \\ c_2(1 \rightarrow 4 \rightarrow 7 \rightarrow 8), c_3(3 \rightarrow 2 \rightarrow 5 \rightarrow 6), \\ c_4(9 \rightarrow 6 \rightarrow 5 \rightarrow 4), c_5(7 \rightarrow 4 \rightarrow 1)\}.$$



Monitor-Segments	C ₁	C ₂	C ₃	C ₄	C ₅	t ₁	t ₂	t ₃	Connections
2C ₁	1	1	0	0	1	0	0	0	0
2C ₃	0	0	1	0	0	0	0	0	0
2t ₁	0	0	0	1	0	1	1	0	0
4C ₂	1	1	0	0	0	0	0	0	0
4C ₄	0	0	0	1	0	1	1	0	0
4C ₅	0	0	0	0	1	0	0	0	0
6C ₁	1	0	0	0	0	0	0	0	0
6C ₃	0	0	1	0	0	1	1	0	0
6C ₄	0	0	0	1	0	0	0	1	0
8C ₂	0	1	0	0	1	0	0	0	0
8t ₂	0	0	0	1	0	0	1	0	0
8t ₃	0	0	0	1	0	0	0	1	0

(2) Relation Matrix of monitor-segments and connections

Fig. 9. Diagnose the OAF in the network without test connection.

According to our test connection setup policy, for each non-monitor node, at least one normal connection or one test connection must exist from this node to every one of its OHMs, thus, the test connection set is

$$Test\ connection\ set = \{t_1(5 \rightarrow 2), t_2(5 \rightarrow 8), t_3(9 \rightarrow 8)\}$$

Thus, the current monitor segment set is

$$msc = \{2c_1, 2c_3, 2t_1, 4c_2, 4c_4, 4c_5, 6c_1, 6c_3, 6c_4, 8c_2, 8t_2, 8t_3\}$$

and the relation matrix between these monitor segments and the connections is shown in Fig. 9(2).

Let us assume that connection $\{c_1(1 \rightarrow 2 \rightarrow 3 \rightarrow 6)\}$ is the OAF. Then, we can get the status of all monitor segments immediately:

$$\begin{aligned} S(2c_1) &= A = 1 \\ S(2c_3) &= \bar{A} = 0 \\ S(2t_1) &= \bar{A} = 0 \\ S(4c_2) &= A = 1 \\ S(4c_4) &= \bar{A} = 0 \\ S(4c_5) &= \bar{A} = 0 \\ S(6c_1) &= A = 1 \\ S(6c_3) &= \bar{A} = 0 \\ S(6c_4) &= \bar{A} = 0 \\ S(8c_2) &= \bar{A} = 0 \\ S(8t_2) &= \bar{A} = 0 \\ S(8t_3) &= \bar{A} = 0. \end{aligned}$$

Thus, $\overrightarrow{S(msc)}$ is obtained as

$$\begin{aligned} \overrightarrow{S(msc)} &= (S(2c_1) S(2c_3) S(2t_1) S(4c_2) \\ &\quad S(4c_4) S(4c_5) S(6c_1) S(6c_3) \\ &\quad S(6c_4) S(8c_2) S(8t_2) S(8t_3)) \\ &= (1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0). \end{aligned}$$

Then, vector $\overrightarrow{S(c)}$ is obtained as

$$\begin{aligned} \overrightarrow{S(c)} &= (S(c_1) S(c_2) S(c_3) S(c_4) \\ &\quad S(c_5) S(t_1) S(t_2) S(t_3)) \\ &= (1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0) \\ &\quad * \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \\ &= (0\ 2\ 5\ 8\ 4\ 6\ 7\ 5). \end{aligned}$$

$S(c_2)$, $S(c_3)$, $S(c_4)$, $S(c_5)$, $S(t_1)$, $S(t_2)$, and $S(t_3)$ are greater than 0, which means connections c_2 , c_3 , c_4 , c_5 , t_1 , t_2 , and t_3 are all IFs. Since $S(c_1) = 0$, it implies that c_1 is in UnIdentified status. Thus, the only UnIdentified connection c_1 must be OAF.

According to this example, we can draw the following conclusions.

- 1) Test connections will not utilize additional resources that are not free in the network. According to our test connection setup policy, a test connection is needed only if there is no monitor segment on one link. If a test connection cannot be set because no spare resource on a certain link, then the resource must be used by other connection, which can be used as monitor segment. Thus, test connections will not affect the network throughput.
- 2) This method is easily applied into a larger network. Suppose we have $|M|$ monitors in the network, and $\text{Max}\{D(m)\} = d_M, m \in M$, then the total number of monitor segment will be no more than $|M| \times d_M$.

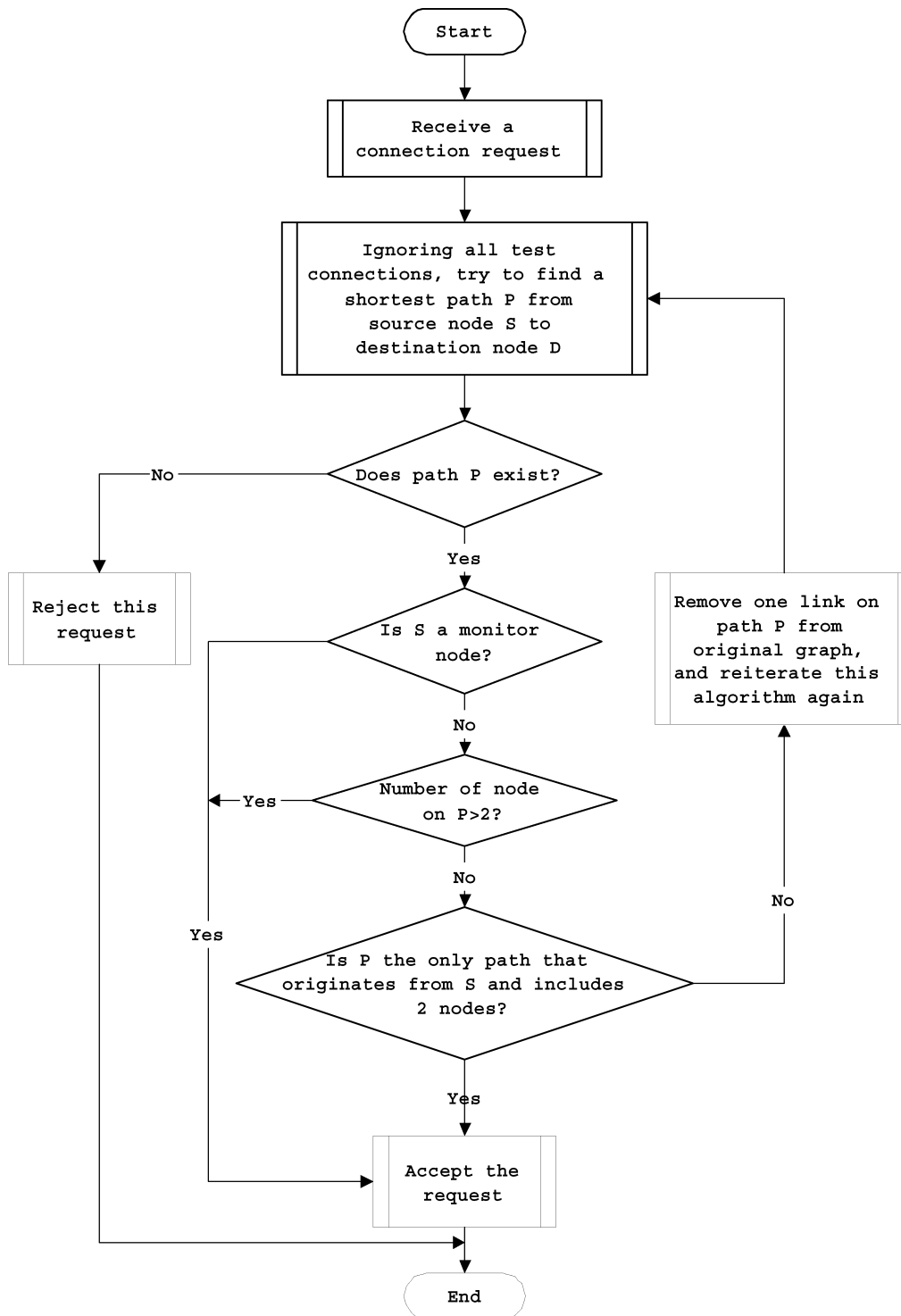


Fig. 10. Flow chart of routing algorithm.

Also, assume there are total $|C|$ connections in whole network, then the relation matrix size will be no more than $(|M| \times d_M) \times |C|$. Thus, for determining OAF, the computation complexity is $O((|M| \times d_M)^2 \times |C|)$, and the only operations needed in computation are $+$ and \oplus .

- 3) For a mesh network, only about half of the nodes as monitor nodes will satisfy our diagnostic conditions. By considering the expensive price of the monitor device, this provides a great advantage.

- 4) If no wavelength converter is available in a w -wavelength network, two connections on different wavelength cannot affect with each other. Thus, according to Theorem 3, this network is w -OAF diagnosable as long as there is at most one-OAF per wavelength.

VI. CONCLUSION

It is important to detect and localize an attack connection quickly in a transparent AON. Quick detection and localization

of an attack source can avoid losing large amounts of data in an AON. However, detecting attack sources is not necessarily the same as putting monitors on all nodes. In this paper, we prove necessary and sufficient conditions for one-OAF diagnosable network, and proposed a sparse monitoring method for such network. The key ideas used in our solution are: 1) employing status of connections as diagnostic data and 2) placing a relatively small number of monitors on a selected set of nodes in a network is sufficient to achieve the required level of performance.

Specifically, we focus on the crosstalk attack and make the following contributions. 1) We develop the crosstalk attack model and monitor model. 2) Based on these models, we prove necessary and sufficient conditions for one-OAF diagnosable network. 3) We propose a efficient monitor placement policy, a test connection setup policy, and a routing policy as well as develop a practicable routing algorithm for such network. 4) We prove that our policies are sufficient to localize all crosstalk attacks, as long as there is no more than one attack on each wavelength in the whole network. The computation complexity of OAF localization algorithm is not high and is scalable.

In this paper, only crosstalk attacks are considered. If other types of attacks also exist in the same network simultaneously, then this solution has to be modified. How to detect and localize other types of attacks and how to localize more than one type of attack in one network will be the focus of future work. Besides the detection of crosstalk attacks, the methodology of monitoring equipment placement can also be used to monitor other optical network service quality or link performance parameters. For example, the same application can be extended to monitor polarization mode dispersion (PMD) that is also truly transparent end-to-end in an optical network. To be practical, we should look at other factors for monitoring and solutions for an optimal strategy.

REFERENCES

- [1] A. N. Group, *All-Optical Network Security*. Cambridge, MA: MIT Lincoln Laboratory, 1998.
- [2] R. Bergman, M. Medard, and S. Chan, "Distributed algorithms for attack localization in all-optical networks," in *Proc. Network and Distributed System Security Symp.*, San Diego, CA, 1998.
- [3] M. Medard, D. Marquis, R. A. Barry, and S. G. Finn, "Security issues in all-optical networks," *IEEE Network*, vol. 11, no. 3, pp. 42–48, May/Jun. 1997.
- [4] M. Medard, D. Marquis, and S. R. Chinn, "Attack detection methods for all-optical networks," in *Proc. Network and Distributed System Security Symp.*, San Diego, CA, 1998.
- [5] 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*, vol. 11, no. 9, pp. 1438–1448, Dec. 1993.
- [6] I. Katzela, G. Ellinas, and T. E. Stern, "Fault diagnosis in the linear lightwave network," in *Dig. LEOS Summer Topical Meeting*, 1995, pp. 41–42.

- [7] I. Katzela and M. Schwartz, "Schemes for fault identification in communication networks," *IEEE/ACM Trans. Netw.*, vol. 3, no. 6, pp. 753–764, Dec. 1995.
- [8] W. T. Anderson *et al.*, "The MONET project—a final report," *J. Lightw. Technol.*, vol. 18, no. 12, pp. 1988–2009, Dec. 2000.
- [9] N. Golmie, T. D. Ndousse, and D. H. Su, "A differentiated optical services model for WDM networks," *IEEE Commun. Mag.*, vol. 38, no. 2, pp. 68–73, Feb. 2000.
- [10] C.-S. Li and R. Ramaswami, "Fault detection, isolation, and open fiber control in transparent all-optical networks," in *Proc. IEEE GLOBECOM*, vol. 1, 1996, pp. 157–162.
- [11] —, "Automatic fault detection, isolation, and recovery in transparent all-optical networks," *J. Lightw. Technol.*, vol. 15, no. 10, pp. 1784–1793, Oct. 1997.



Tao Wu (S'95–M'04) 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.



Arun K. Somani (M'83–SM'88–F'99) received the M.S.E.E. and Ph.D. degrees in electrical engineering from McGill University, Montreal, Canada, in 1983 and 1985, respectively.

He is currently Jerry R. Junkins Endowed Chair Professor of Electrical and Computer Engineering at Iowa State University, Ames. He worked as Scientific Officer for the Government of India, New Delhi, from 1974 to 1982 and as a faculty member at the University of Washington, Seattle, from 1985 to 1997 in the electrical engineering and

engineering departments, where he was promoted to Full Professor in September 1995. His research interests are in the area of fault tolerant computing, computer interconnection networks, WDM-based optical networking, and parallel computer system architecture. He is the chief architect of an anti-submarine warfare system (developed for Indian navy) and Meshkin fault-tolerant computer system architecture (developed for the Boeing Company). He has also developed several robust interconnection topologies, architected, designed, and implemented a 46-node multi-computer cluster-based system, Proteus, using a large grain message-passing model and separate data and control planes, and uses fiber optic communication links. His current research is in developing scalable architectures and algorithms to manage, control, and deliver dependable service efficiently for network employing optical fiber technology, wavelength division multiplexing, wavelength conversion, wavelength sharing, traffic grooming, access network design, Fault and Attack Management (FAM) in optical networking.

Prof. Somani has served on several program committees of various conferences in his research areas. He was the General Chair of IEEE Fault Tolerant Computing Symposium 1997, Technical Program Committee Chair of the International Conference on Computer Communications and Networks 1999 and OPTICOMM 2003, and General Chair of BroadNets 2005. He has served as an IEEE distinguished visitor and IEEE distinguished tutorial speaker. He has been elected a Fellow of IEEE for his contributions to theory and applications of computer networks.