

Necessary and Sufficient Condition for k Crosstalk Attacks Localization in All-Optical Networks

Tao Wu and Arun K. Somani
Dependable Computing & Networking Laboratory
Department of Electrical and Computer Engineering
Iowa State University, Ames, IA 50011
E-Mail: {wutao, arun}@iastate.edu

Abstract—An All-Optical Network (AON) is a network in which data does not undergo optical-to-electrical and electrical-to-optical conversion within the network. Transparency and non-regeneration features make attack detection and localization in AONs difficult. Among all attack methods, crosstalk attack has higher damage capabilities. In this paper, we make the following contributions. (1) We provide the crosstalk attack model and monitor model. (2) Based on these models, we prove necessary and sufficient conditions for k -crosstalk attacks diagnosable network. The key ideas used in our solution are to employ status of connections as diagnostic data. (3) We propose an efficient monitor placement policy, a test connection setup policy, and a routing policy for such network. These conditions will lead to efficient k -attack detection and diagnosis algorithms.

Index Terms—rosstalk, Attack, Monitor, AONrosstalk, Attack, Monitor, AONC

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. Although AON is a viable technology for future telecommunication and data networks, its intrinsic security differences with existing electro-optic and electronic networks has received attention only recently. AONs introduce new physical layer mechanisms that may change potential models of attack from those that are known for electronic networks. 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. A malicious connection can propagate from its primary source to other nodes without losing its attack capability. Transparency and non-regeneration features make attack detection and localization difficult.

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;

The research reported in this paper is funded in part by a contract from G. W. U, funded by the the Defense Advanced Research Projects Agency under grant N66001-00-1-8949 and co-funded by NSA.

- 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 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, 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 the same switch. A crosstalk attack cannot only affect those connections sharing a link or node with it, but also may induce attack capabilities to those connections that are affected[1]. Figure 1 shows the crosstalk attack propagation mechanism. 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 2 to also acquire attack capability. This propagation characteristic makes attack connection localization more difficult.

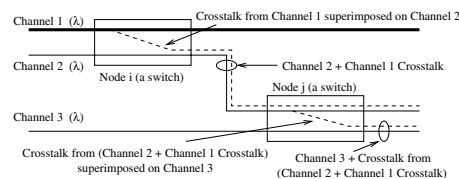


Fig. 1. Example of crosstalk attack

The prior work [1], [2], [3], [4] only considered networks in which all nodes are equipped with monitors. Some methods [5], [6], [7] provide probabilistic approaches to fault diagnosis in network, not suitable for the attack localization problem, as they can only identify a most likely set. We still need further steps to analyze where the exact location of the source is.

Necessary and sufficient condition are identified in papers[8], [9] for a single cross-talk attack.

The capability of an optical monitoring module have been researched by several researchers [10], [11]. To install monitors for all wavelengths at all nodes in a network is likely to be very expensive. A network management system using supervisory channels [12], [13] can detect and monitor the performance of network devices remotely. If normal connections cannot provide sufficient information, we can derive the monitoring information by establishing some additional test connections. We show that this diagnostic information is sufficient for localizing an attack connection.

The rest of the paper is organized as follows. First, we provide a crosstalk attack and a monitor model based on some previous work [1], [2], [4], [8], [9], [10], [12], [13]. Next, we develop a necessary and sufficient condition to localize k co-existing crosstalk attacks in an AON. 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. In the following section, we show one example to explain our algorithm and demonstrate its capabilities. Finally, we present our conclusions.

II. CROSSTALK ATTACK AND MONITOR MODEL

Node model: A node can perform routing and switching; some nodes can support monitoring capability. A node supporting monitoring capability is called a *monitor node*.

Crosstalk attack model:

- 1) *down-stream neighbor nodes:* For a node on the path of a connection, its *down-stream neighbor node (DNN)* is the next node on that path. $DNN(\text{node } A, \text{connection } C)$ denotes the DNN of node A on connection C .
- 2) The *original attack flow (OAF)* has a much higher energy level and its ability to influence other connections is same on all links on its path. A node is called a *primary attacked node (PAN)* if there is an OAF originating, terminating or traversing this node.
- 3) A normal connection affected by an OAF is called a *secondary attacked flow (SAF)*. The SAF has limited attack capability, i.e., if it is affected at node A , then its attack capability is only at $DNN(A, C)$. $DNN(A, C)$ is called *secondary attacked node (SAN)*. Because an OAF has very strong power (i.e., 0.1W or higher), comparing with normal signal's power (i.e., 0.1mW), even -20dB (1mW) crosstalk from the OAF is still enough to induce the attack capability to the affected signals, while this loss is almost nothing for the OAF itself. However, those affected signals will lose its energy quickly in case of fiber attenuation. Therefore, it is most likely that a SAF can only affect those connections traversing the SAN.
- 4) A connection influenced by an SAF is called a *final attacked flow (FAF)*. Except OAFs and SAFs, the remaining connections in the network do not have attack capabilities. Except the OAFs, the union of remaining

connections, including FAFs and SAFs, is called an *innocent flow (IF)* set.

- 5) *Power Level:* The power levels of the OAF, the SAF, and the FAF follow the relation: $P(OAF) > P(SAF) > P(FAF)$.

In Figure 1, connection 1 is the OAF, connection 2 is the SAF, and connection 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.

Monitor Node Model:

- 1) A monitor node can monitor all traffic passing through it, including the traffic that originated/terminated at the node. Monitor node can detect the input/output connection power in all parts including its demultiplexer, multiplexer, switch plane, etc. Signal on different wavelength is monitored by different monitor device.
- 2) A connection is determined to be in an attack/non-attack status, indicated by A/\bar{A} , at a monitor.
- 3) If there are OAFs traversing this monitor node, then only OAFs will be set to A . Without OAFs, then only SAFs will be set to A . All other connections will be set to \bar{A} .

III. NECESSARY AND SUFFICIENT CONDITIONS

A network is called k -OAF diagnosable if up to k co-existing OAFs can always be detected and localized from monitor information. 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 non-monitor nodes, $M \subseteq V$, $N \subseteq V$, and $M \cup N = V$. 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 $\{u_0, u_1, \dots, u_m\}$. 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) *non-monitor:* a monitor m is a non-monitor of a connection c if $m \notin U(c)$ and $\nexists (u \rightarrow m)$ where $u \in U(c)$.

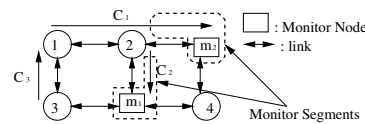


Fig. 2. Monitor-Segment Example

A. Monitor-Segment

Monitor-Segment: A monitor segment mc is a one-hop segment 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 c_j ends at monitor node m_i . Mostly, we use $m_s c_i$ to denote one common monitor segment in monitor-segment set MSC . Two monitor segments are shown in Figure 2, 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 and monitor node m_2 , denoted by $m_2 c_1$.

A monitor segment $m_s c = (u \rightarrow m)$ 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 (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 Figure 2, 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 $m_1 c_2$ and $m_2 c_1$ are monitoring connection c_1 , and none of them is monitoring connection c_3 . Let $(m_s c, c)$ denote this relation between monitor-segment $m_s c$ 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 $S(m_s c)$. For example, in Figure 2, if the status of c_2 in monitor m_1 is indicated as A , then the status of the monitor-segment $m_1 c_2$ is A . $S(m_s c)$ can be either A or \bar{A} . For a connection c , which is not being monitoring by $m_s c$, we say that $m_s c$ has a *non-monitoring* relation with c .

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 neither as IF nor as OAF. Let $S(c)$ denote the status of connection c . If $m_s c$ is monitoring a connection c , then $S(m_s c) = A$ means $S(c) = uncertain$, $S(m_s c) = \bar{A}$ means $S(c) = IF$, otherwise, either $S(m_s c) = A$ or $S(m_s c) = \bar{A}$ means $S(c) = uncertain$.

We can represent the monitor and monitor segments using a bipartite graph $G'(V', E')$, where the nodes (V') of the bipartite graph are the monitor segments and the connections, and E' denotes their monitoring relations. Figure 3 shows the corresponding one-hop segments, and relationship between a monitor-segment $m_s c$ and a connection c .

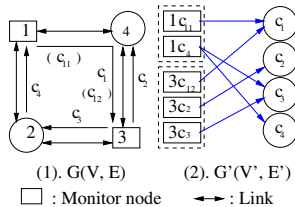


Fig. 3. Monitor-Segment Example

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

B. Theorem and Proof

Lemma 1: If $m_s c \notin \Gamma^{-1}(c)$, c cannot affect the $m_s c$ status even if c is an OAF.

Lemma 2: For a connection $c_i \notin \{c_{j_1}, \dots, c_{j_k}\}$, $c_i \in C$ and $\{c_{j_1}, \dots, c_{j_k}\} \subseteq C$, if $\Gamma^{-1}(c_i) \not\subseteq \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$, then $\Gamma^{-1}(c_i) \not\subseteq \cup_{j=j_m}^{j_n} \Gamma^{-1}(c_j)$, where $\{c_{j_m}, \dots, c_{j_n}\} \subseteq \{c_{j_1}, \dots, c_{j_k}\}$.

Lemma 3: If a connection c is an OAF, then c must be in *UnIdentified* status.

Corollary 1: If there is a total of m *UnIdentified* connections in the network, then there are no more than m OAFs in the network simultaneously.

Above proof are omitted for lack of space.

Theorem 1: For any connection $c_i \notin \{c_{j_1}, \dots, c_{j_k}\}$, where $c_i \in C$, and $\{c_{j_1}, \dots, c_{j_k}\} \subseteq C$ is an arbitrary subset of existing connections in the network, if $\Gamma^{-1}(c_i) \not\subseteq \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$, and there are $k+1$ *UnIdentified* connections in the network, then there must be at least $k+1$ OAFs in the network.

Proof:

We prove this theorem by induction.

Initial step: suppose $k=1$. Then, $\Gamma^{-1}(c_i) \not\subseteq \Gamma^{-1}(c_j)$, for $\forall c_i, c_j \in C$. Assume an arbitrary pair of connections c_a and c_b are *UnIdentified* connections, but there is no more than one OAF in the network. There can be 3 possibilities.

- 1) There is no OAF in the network. Then, every $m_s c$ in the network should be in \bar{A} status, thus, all connections should be in *IF* status. This contradicts our assumption.
- 2) One of c_a or c_b is an OAF. Without loss of generality, assume c_b is an OAF. Since $\Gamma^{-1}(c_a) \not\subseteq \Gamma^{-1}(c_b)$, there exists at least one $m_s c$ m such that $m \in \Gamma^{-1}(c_a)$ and $m \notin \Gamma^{-1}(c_b)$. According to Lemma 1, c_b cannot affect the status of m . Then, m must be in \bar{A} status, which implies c_a is not an *UnIdentified* connection. This contradicts our assumption.
- 3) Another OAF c_m exists. According to the given condition, $\Gamma^{-1}(c_a) \not\subseteq \Gamma^{-1}(c_m)$. Thus there exists at least one $m_s c$ m such that $m \in \Gamma^{-1}(c_a)$ and $m \notin \Gamma^{-1}(c_m)$ must exist. According to Lemma 1, c_m cannot affect the status of m . Then, m must be in \bar{A} status, which implies c_a is not *UnIdentified* connection. This again contradicts our assumption.

Thus, the number of OAFs, $|OAF|$, is at least 2, which implies that this theorem is true when $k=1$.

Induction step: suppose this theorem is true for $k-1$, i.e., $\Gamma^{-1}(c_i) \not\subseteq \cup_{j=j_1}^{j_{k-1}} \Gamma^{-1}(c_j)$, where $c_i \notin \{c_{j_1}, \dots, c_{j_{k-1}}\}$, $c_i \in C$, and $\{c_{j_1}, \dots, c_{j_{k-1}}\} \subseteq C$ is an arbitrary subset of existing connections in the network, then there must be at least k OAFs in the network simultaneously if there exist k *UnIdentified* connections in the network.

Suppose $\Gamma^{-1}(c_i) \not\subseteq \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$ is true for all $c_i \notin \{c_{j_1}, \dots, c_{j_k}\}$, and suppose $k+1$ *UnIdentified* connections in the network are $c_{n_1}, \dots, c_{n_{k+1}}$. Since $\Gamma^{-1}(c_i) \not\subseteq \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$,

from Lemma 2, $\Gamma^{-1}(c_i) \not\subseteq \cup_{j=j_1}^{j_k-1} \Gamma^{-1}(c_j)$ is also satisfied. Since there are at least k *UnIdentified* connections in the network, therefore there are at least k OAFs, c_{m_1}, \dots, c_{m_k} , exist. According to our assumption, $\Gamma^{-1}(c_{n_i}) \not\subseteq \cup_{m=m_1}^{m_k} \Gamma^{-1}(c_m)$, there exists an *msc* msc_{n_i} such that $msc_{n_i} \in \Gamma^{-1}(c_{n_i})$ and $msc_{n_i} \notin \cup_{m=m_1}^{m_k} \Gamma^{-1}(c_m)$.

According to Lemma 1, all $c_m \in \{c_{m_1}, \dots, c_{m_k}\}$ cannot affect msc_{n_i} . Thus there must exist at least one extra OAF that affects the status of msc_{n_i} . Therefore, at least $k+1$ OAFs must exist in the network. Thus the theorem holds for all values of k . ■

Theorem 2 (Necessary and sufficient condition): In a network with up to k OAFs simultaneously, $|UnIdentified\ Connection| \leq k$, if and only if for any connection c_i and any arbitrary subset of k connections $\{c_{j_1}, \dots, c_{j_k}\}$, $c_i \notin \{c_{j_1}, \dots, c_{j_k}\}$, $\Gamma^{-1}(c_i) \not\subseteq \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$, is always satisfied.

Proof: Necessity:

Without loss of generality, suppose a subset of k connections, i.e., $\{c_{j_1}, \dots, c_{j_k}\}$ are all OAFs. According to lemma 3, all OAFs are unidentified. Then, for some connection $c_i \notin \{c_{j_1}, \dots, c_{j_k}\}$, there are two possibilities.

- 1) $\Gamma^{-1}(c_i) = \emptyset$. Obviously, $\Gamma^{-1}(c_i) \subseteq \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$. Since there is no *msc* $\in \Gamma^{-1}(c_i)$, c_i is unidentified. According to lemma 3, all OAFs are unidentified along with $\{c_{j_1}, \dots, c_{j_k}\}$, and thus $|UnIdentified\ Connection| > k$.
- 2) $\Gamma^{-1}(c_i) \neq \emptyset$ and suppose $\Gamma^{-1}(c_i) \subseteq \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$, then for all *msc* $\in \Gamma^{-1}(c_i)$, $msc \in \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$ holds. Obviously, all *msc* $\in \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$ must be in *A* status. Therefore, *msc* $\in \Gamma^{-1}(c_i)$ are also in *A* state, thus c_i is also UnIdentified and $|UnIdentified\ Connection| > k$.

Sufficiency:

Suppose $|UnIdentified\ Connection| \geq k + 1$, and for every unidentified connection c , $\Gamma^{-1}(c) \neq \emptyset$. Assume that for any connection c_i and any arbitrary subset of k connections $\{c_{j_1}, \dots, c_{j_k}\}$, $c_i \notin \{c_{j_1}, \dots, c_{j_k}\}$, $\Gamma^{-1}(c_i) \not\subseteq \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$, is always satisfied. According to Theorem 1, at this time, the number of OAFs is at least $k + 1$, which contradicts our assumption that there are no more than k OAFs in the network simultaneously.

Thus, the theorem holds. ■

Corollary 2: For any connection $c_i \notin \{c_{j_1}, \dots, c_{j_k}\}$, where $c_i \in C$, and any arbitrary subset $\{c_{j_1}, \dots, c_{j_k}\} \subseteq C$ in the network, if $\Gamma^{-1}(c_i) \not\subseteq \cup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$ is always true, then for $m \leq k$,

- 1) there are no more than m *UnIdentified* connections in the network if there are only m OAFs exist in the network;
- 2) there are exactly m OAFs if there exist m *UnIdentified* connections;
- 3) if there exist m *UnIdentified* connections, these m connections must be m OAFs.

Proof: Omitted for lack of space.

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 non-monitoring, denoted by 1 and 0, respectively. A vector $\vec{r}_i = \{r_i(c_j) | c_j \in C\}$, is used to denote such this relationship and a *Relation Matrix* \mathcal{R} can be created as:

$$\mathcal{R} = \begin{pmatrix} \vec{r}_1 \\ \vdots \\ \vec{r}_m \end{pmatrix} = \begin{pmatrix} r_1(c_1) & \dots & r_1(c_n) \\ \dots & \dots & \dots \\ r_m(c_1) & \dots & r_m(c_n) \end{pmatrix}.$$

Let n denote the total number of connections and m denote the total number of monitor-segments. $r_i(c_j) = 1$ if *msc_i* monitor c_j , otherwise, $r_i(c_j) = 0$.

Using the status of monitor-segments, we can get the corresponding status of all connections. Let vector $\vec{S}_i(\vec{c}) = \{S_i(c_1), S_i(c_2), \dots, S_i(c_n)\}$ denote all connections' status given by *msc_i*, where $S_i(c_j)$ denotes status of c_j derived from status of *msc_i*. Let the status of a connection, i.e., *IF* and *uncertain* be denoted as 1 and 0, respectively. Similarly, let the status of monitor-segment $S(msc_i)$, i.e., *A* and \bar{A} be denoted as 1 and 0, respectively. Then, $S_i(c_j) = \{S(msc_i) \times r_i(c_j)\} \oplus r_i(c_j)$; and $\vec{S}_i(\vec{c}) = \{[S(msc_i) \cdot \vec{1}] \times \vec{r}_i\} \oplus \vec{r}_i$; where $\vec{1}$ is a $1 \times n$ vector, \times is *AND*, and \oplus is *XOR*.

Then, a *Status Matrix* can be obtained.

$$\begin{pmatrix} \vec{S}_1(\vec{c}) \\ \vdots \\ \vec{S}_m(\vec{c}) \end{pmatrix} = \left\{ \left(\begin{matrix} S(msc_1) \\ \dots \\ S(msc_m) \end{matrix} \right) \cdot \vec{1} \right\} \times \begin{pmatrix} \vec{r}_1 \\ \vdots \\ \vec{r}_m \end{pmatrix} \oplus \begin{pmatrix} \vec{r}_1 \\ \vdots \\ \vec{r}_m \end{pmatrix}.$$

Let $S(c_j)$ denote the sum of j th column in above matrix, $S(c_j) = \sum_{i=1}^m S_i(c_j) = \sum_{i=1}^m \{[S(msc_i) \times r_i(c_j)] \oplus r_i(c_j)\}$. Now, if we define a new operation $*$ as: $\vec{X} * \vec{Y}^T = \sum_{i=1}^n \{[x_i \times y_i] \oplus y_i\}$, \vec{X} and \vec{Y} are $1 \times n$ vectors, x_i and y_i are their elements; then, vector $\vec{S}(\vec{c})$ can be denoted by $S(msc_i)$ and relation matrix as follows.

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

The global status of connection c_j can be obtained as: if $S(c_j) > 0$, then *Status of* $c_j = \text{IF}$, and if $S(c_j) = 0$, then *Status of* $c_j = \text{UnIdentified}$. According to corollary 2, if status of connection c_j is UnIdentified, then c_j must be an OAF. This provides the algorithm for locating the attack connections of each wavelength.

IV. A SPARSE MONITORING POLICY AND ROUTING ALGORITHM

Previous section provides the necessary and sufficient condition to k -OAF diagnosable network, but how to place the monitors and setup test connections is still an open question. Since the more OAF in a network, the more complicated algorithm will be, thus, only a 2-OAF diagnosable network is discussed in this section. We first propose a sparse monitoring scheme, which includes of monitor placement as well as regular and test connections setting policies, then we prove that any network using such method is 2-OAF diagnosable.

- 1) **Monitor placement policy:** A neighbor of a degree one node and all neighbors of a non-monitor node must have monitor.
- 2) **Test Connection Setup Policy:** For a non-monitor node u , if there is a normal connection c on wavelength λ passing through or terminating at u , one test connection from u to each of its neighbors (which must be monitors), except u 's up-stream neighbor node, is needed if no normal connection provides a monitor-segment on the corresponding link.
- 3) **Routing policy:** If a connection c_i 's source is a non-monitor node that is also on another connection c_j 's path, then, c_i must pass through three continuous nodes $(n_1, n_2, n_3) \not\subseteq U(c_j) \cup U(c_k)$, where $c_k \neq c_i, c_j$ is an arbitrary connection in the network. Otherwise, any path selection algorithm, such as shortest path algorithm, can be used.

Claim 1: 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 2-OAF diagnosable on each wavelength. **Proof:** See Appendix.

V. EXAMPLE OF SPARSELY CONNECTED NETWORK

Figure 4 (1) depicts a 9-node bi-directional mesh network. For this to be a 2-OAF diagnosable network, four monitors are necessary. We choose nodes 2, 4, 6, and 8 as the monitor nodes. To simplify our discussion, we assume that only one wavelength is supported in this network.

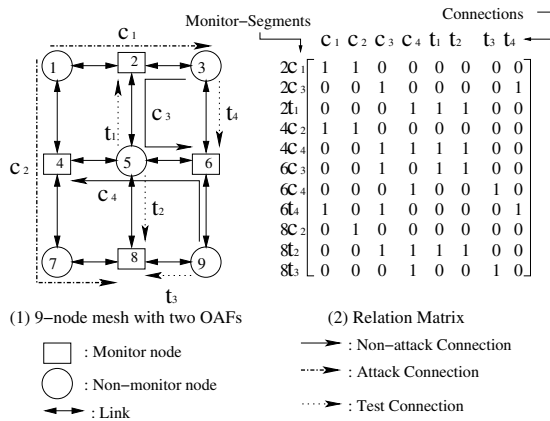


Fig. 4. Diagnose the OAF in the network without test connection

Let current normal connection set to be $\{c_1(1 \rightarrow 2 \rightarrow 3), c_2(1 \rightarrow 4 \rightarrow 7 \rightarrow 8), c_3(3 \rightarrow 2 \rightarrow 5 \rightarrow 6), c_4(9 \rightarrow 6 \rightarrow 5 \rightarrow 4)\}$. According to our test connection setup policy, we need the test connections set $\{t_1(5 \rightarrow 2), t_2(5 \rightarrow 8), t_3(9 \rightarrow 8), t_4(3 \rightarrow 6)\}$. Thus, $msc = \{2c_1, 2c_3, 2t_1, 4c_2, 4c_4, 6c_3, 6c_4, 6t_4, 8c_2, 8t_2, 8t_3\}$, and the relation matrix between these monitor-segments and the connections is shown in Figure 4 (2).

Let us assume that connection $\{c_1(1 \rightarrow 2 \rightarrow 3)\}$ and $\{c_2(1 \rightarrow 4 \rightarrow 7 \rightarrow 8)\}$ are OAFs. Then, we can get the status of all monitor-segments immediately: $S(2c_1) = A = 1, S(2c_3) =$

$\bar{A} = 0, S(2t_1) = \bar{A} = 0, S(4c_2) = A = 1, S(4c_4) = \bar{A} = 0, S(6c_3) = \bar{A} = 0, S(6c_4) = \bar{A} = 0, S(6t_4) = A = 1, S(8c_2) = A = 1, S(8t_2) = \bar{A} = 0, \text{ and } S(8t_3) = \bar{A} = 0$. Thus, $\overline{S(msc)}$ is obtained as: $\overline{S(msc)} = (1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0)$. Then, vector $\overline{S(c)}$ is obtained as:

$$\overline{S(c)} = (0\ 0\ 4\ 4\ 4\ 4\ 2\ 1).$$

$S(c_3), S(c_4), S(t_1), S(t_2), S(t_3)$, and $S(t_4)$ are greater than 0, which means connections c_3, c_4, t_1, t_2, t_3 , and t_4 are all IFs. Since $S(c_1) = 0$ and $S(c_2) = 0$, it implies that both c_1 and c_2 are in UnIdentified status. Thus, according to corollary 2, the UnIdentified connection c_1 and c_2 must be OAFs.

We make the following additional observations: (1) Test connections will not utilize additional resources that are not free in the network. Thus, test connections will not affect the network throughput. (2) This method is easily applied to a larger network. Let d_M be the largest degree of any monitor node. The computation complexity is $O((|M| \times d_M)^2 \times |C|)$, and the only operations needed in computation are $+$ as well as logical operation \times and \oplus . (3) For a mesh network, only about half of the nodes as monitor nodes will satisfy our diagnostic conditions. (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 2, this network is kw -OAF diagnosable as long as there is at most k -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 k -OAF diagnosable network, and proposed a sparse monitoring method for 2-OAF diagnosable network. The key ideas used in our solution are: (1) employing status of connections as diagnostic data, (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 condition for k -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.

REFERENCES

- [1] A. N. Group, "All-optical network security," MIT Lincoln Laboratory, December 1998.

- [2] 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**, pp. 42–48, May/June 1997.
- [4] M. Medard, D. Marquis, and S. R. Chinn, "Attack detection methods for all-optical networks," *Network and Distributed System Security Symposium*, 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* **11**, pp. 1438–1448, December 1993.
- [6] I. Katzela, G. Ellinas, and T. E. Stern, "Fault diagnosis in the linear lightwave network," *Dig. LEOS Summer Topical Meeting*, pp. 41–42, 1995.
- [7] I. Katzela and M. Schwartz, "Schemes for fault identification in communication networks," *IEEE/ACM Transactions on Networking* **3**, pp. 753–764, December 1995.
- [8] T. Wu and A. Somani, "Attack monitoring and localization in all-optical networks," *OptiComm'02 Proceedings*, July 2002.
- [9] T. Wu and A. Somani, "Attack monitoring and localization in all-optical networks," *APOC'02 Proceedings*, October 2002.
- [10] W. T. Anderson, J. Jackel, G.-K. Chang, and H. D. et al., "The monet project-a final report," *IEEE Journal of Lightwave Technology* **18**, pp. 1988–2009, December 2000.
- [11] N. Golmie, T. D. Ndousse, and D. H. Su, "A differentiated optical services model for wdm networks," *IEEE Communication Magazine*, pp. 68–73, February 2000.
- [12] C.-S. Li and R. Ramaswami, "Fault detection, isolation, and open fiber control in transparent all-optical networks," *GLOBECOM '96* **1**, pp. 157–162, 1996.
- [13] C.-S. Li and R. Ramaswami, "Automatic fault detection, isolation, and recovery in transparent all-optical networks," *IEEE Journal of Lightwave Technology* **15**, pp. 1784–1793, October 1997.

APPENDIX

Claim 1: 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 2-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 non-monitor 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 $U(c_i)$ denote the set of nodes on connection c_i 's path.

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

- 1) According to the sparse monitor placement policy, for a non-monitor 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 2, for any three arbitrary connections c_i , c_j , and c_k , the necessary and sufficient condition for an 2-OAF diagnosable network is $\Gamma^{-1}(c_i) \not\subseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$. Now, suppose $\Gamma^{-1}(c_i) \subseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$, then there are two possibilities.
 - a) c_i 's source node is a non-monitor node. Then, there are two possible cases.

- i) Connection c_i 's source node $n_i \notin U(c_j) \cup U(c_k)$. Because at least one monitor exists on each link, $DNN(n_i, c_i)$ must be a monitor node. Let $m_i = DNN(n_i, c_i)$. Since $n_i \notin U(c_j) \cup U(c_k)$, monitor-segment $m_i c_i$ can only monitor connection c_i , thus, $\Gamma^{-1}(c_i) \not\subseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$. This contradicts the assumption.
- ii) $n_i \in U(c_j) \cup U(c_k)$. Without loss of generality, suppose $n_i \in U(c_j)$. According to routing policy, connection c_i should pass three continuous nodes that are not in $U(c_j) \cup U(c_k)$. According to lemma 4, there is always a monitor-segment $m_{sc_i} \notin \Gamma^{-1}(c_j)$ as well as $m_{sc_i} \notin \Gamma^{-1}(c_k)$, thus $\Gamma^{-1}(c_i) \not\subseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$. This contradicts the assumption.
- b) c_i 's source node is a monitor node. According to previous discussing 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 m_{sc_i} made up by c_i and m does not monitor other connections including c_j and c_k , i.e., $m_{sc_i} \in \Gamma^{-1}(c_i)$, and $m_{sc_i} \notin \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$. $\Gamma^{-1}(c_i) \not\subseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$, this contradicts our assumption.

From the above analysis, we know that we cannot find three connections in the network such that $\Gamma^{-1}(c_i) \subseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$ based on previous policies, with the assumption of one wavelength on one direction. Thus, under this condition, the network is 2-OAF diagnosable.

Next, we agree that a multi-wavelength network is 2-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 chance 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 are no more than 2 OAFs on each wavelength.

■