Resilient Architecture of All-Optical Networks: Probabilistic Graphical Models for Crosstalk Attack Propagation

Guanglei Liu and Chuanyi Ji

School of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, GA 30332, USA
Email: {guanglei, jic}@ece.gatech.edu

Abstract— **We study the resilience of all-optical network (AON) architectures under in-band crosstalk attacks. We first develop a cross-layer model that captures attack propagation based on probabilistic graphical models. At the physical layer, we use a directed probabilistic graph (Bayesian Belief Network) to model the attack propagation under static network traffic and a given source of attack. At the network layer, we use an undirected probabilistic graph (Random Field) to represent the probability distribution of active connections in the network. The cross-layer model is obtained by combining the physical- and the network-layer models into a factor graph representation. We then derive bounds on the network resilience for regular topologies. We show that for ring, star, and mesh-torus networks with link-shortest path routing and all-to-all traffic, the average network resilience loss grows linearly with respect to the network load when the network load is light; grows polynomially with respect to the probability of attack propagation from node to node along the attacker's route. We then show that the sum-product algorithm can be used for computationally efficient evaluation of network resilience for irregular topologies.**

I. Introduction

All-optical network (AON) is a promising technology for next-generation optical networks. However, AONs are susceptible to malicious attacks because the signals remain in optical domain within the network and are difficult to be monitored closely [1]. Due to the high data rate supported by AONs, even attacks of a short duration can result in a large amount of data loss. Hence, security of AONs upon attacks has become an important issue, where an open question is how to incorporate security against malicious attacks in the design and engineering of AON architectures. Investigations of this question are important as AONs are still at an early stage of deployment. The goal of this work is to study how network architecture impacts resilience in the context of in-band crosstalk attacks in AONs.

Crosstalk attacks were first studied in [1]. Crosstalk in AONs is caused by signal leakage among different inputs at non-ideal network devices, e.g. optical switches. The most detrimental type of crosstalk is in-band crosstalk, where the crosstalk element is within the same wavelength as the signal. In-band crosstalk attacks can happen at fiber links or network nodes. In this work, we consider the case where an attacker gains legitimate access to a network node and inserts a flow with strong signal power into the network [1][2]. Due to the crosstalk effects of wavelength switches, a small fraction of the signal from the attacker's flow may leak into other normal flows in the shared switching plane. The leakage superimposed onto normal flows may exceed a predetermined threshold for quality of service requirement, and those flows are defined as being affected by the attack at network nodes.

To investigate the impacts of network architectures against in-band crosstalk attacks, we focus on three aspects of network architectures: (a) physical layer vulnerabilities, which are related to attack propagation and determined by the characteristics of optical devices, (b) physical topology of the AON, and (c) wavelength usage at the network layer, which is characterized by the load of the network. Our goal is to quantify the effects of these factors in mitigating the impacts of crosstalk attacks. Here, a major challenge is to characterize the interactions of different aspects of network architecture during crosstalk attack propagation, which is cross-layer in nature.

We apply probabilistic graphical models [3] to characterize the cross-layer interactions during attack propagation. Specifically, at the physical layer, a directed probabilistic graph (Bayesian Belief Network) is developed to model attack propagation under static network traffic and a given attack source. At the network layer, an undirected probabilistic graph (Random Field) is used to represent the probability distribution of active connections using wavelengths of the same nominal value. The physical- and the network-layer models are then combined into a cross-layer model using a factor graph representation [4].

The cross-layer model is developed using a bottom-up approach and provides an explicit representation of the dependencies between the physical- and the network-layer. Furthermore, it facilitates the study of network architecture on network resilience. Specifically, for regular topologies, we derive bounds on the network resilience. For irregular topologies, the cross-layer model provides computationally efficient methods for studying the resilience.

II. Problem Formulation

Define the topology of an AON as an undirected graph $G(\mathbf{V},\mathbf{E})$, with $\mathbf{V}$ being the set of nodes and $\mathbf{E}$ being the set of bi-directional links. Denote $V_i \sim V_j$ if there is one bi-directional link between node V_i and V_j. Assume that all connections supported by the network are bi-directional and use routes in a fixed set $\mathbf{R}$. Each bi-directional connection consists of two unidirectional flows in each direction using the same wavelength on the same network route.[1] Furthermore, on the same network link, different bi-directional connections must use distinct wavelengths. Assume that there are no wavelength converters in the AON. This work considers single-source in-band crosstalk attacks [2]. That is, crosstalk attack is started at the source node of a unidirectional flow on wavelength of nominal value λ, and propagates to downstream

[1] Each bi-directional link is made up of two optical fibers, one for each direction. Throughout the paper, the term "connection" is used specifically for bi-directional traffic; the term "flow" is used for uni-directional traffic.

flows that use wavelengths of the same nominal value. As this work focuses on in-band crosstalk attacks, "flows" and "connections'' are to be used in the rest of the paper without referring to associations with wavelength λ.

The problem we shall consider includes: (a) developing the cross-layer model, and (b) using the model to quantify the network resilience. Let S_i be a random variable that denotes the number of active flows affected by the in-band crosstalk attack at the switching plane of node V_i. $\mathbf{S} = (S_i : i \in \mathbf{V})$ corresponds to the number of affected flows at all nodes in the network. Let N_{ij} denote the status of route r_{ij} between node i and node j, where $r_{ij} \in \mathbf{R} : N_{ij} = 1$ if there is an active connection on route r_{ij}; $N_{ij} = 0$, otherwise. Then Vector $\mathbf{N} = (N_{ij} : r_{ij} \in \mathbf{R})$ represent the status of all routes in $\mathbf{R}$. Denote f_{sd} as the flow that starts from node s and terminates at node d. Then we need to obtain the following quantities to characterize attack propagation in the network.

(a) $P(\mathbf{S} \mid \mathbf{N} = \mathbf{n},\ R_f = f_{sd})$: The probability distribution of the number of flows affected at the switching plane of each network node given the status of network routes $\mathbf{n}$ and the source of attack R_f, where R_f denotes the unidirectional flow where the attack originates. This probability captures attack propagation under static network traffic $\mathbf{n}$ and a given source of attack f_{sd}, and is to be characterized by directed probabilistic graph in Section III A.

(b) $P(\mathbf{N} \mid R_f = f_{sd})$: The probability distribution of the status of network routes given the source of attack, which is to be captured by an undirected probabilistic graph in Section III B.

(c) $P(\mathbf{S} \mid R_f = f_{sd})$: The probability distribution of the number of flows affected at each node given the source of attack. This models attack propagation under dynamic traffic when the attack starts on flow f_{sd}. This combines the physical- and the network-layer models from (a) and (b), and shall be described using a factor graph representation in Section III C.

The cross-layer model is then used to study network resilience based on the network resilience loss and average network resilience loss defined as follows.

Definition 1: Given that there is a crosstalk attack started on flow f_{sd}, the network resilience loss is defined as

$$M_{f_{sd}} = \sum_{V_i \in \mathbf{V}} E_{f_{sd}}[S_i], \qquad (1)$$

where $E_{f_{sd}}[S_i] = \sum_{S_i} s_i P(S_i = s_i \mid R_f = f_{sd})$ is the expected number of affected flows at node V_i given the source of the attack. $M_{f_{sd}}$ shows how resilient a network is when the attack starts from a particular flow.

Definition 2: The average network resilience loss is defined as $M = E_{R_f}[M_{f_{sd}}]$, where $E_{R_f}[\,]$ stands for the expectation over the source of the attack R_f, i.e.,

$$M = \sum_{f_{sd}} M_{f_{sd}}\ P(R_f = f_{sd}), \qquad (2)$$

where $P(R_f = f_{sd}) = P(N_{sd} = 1)/2 \mid \mathbf{R} \mid$, under the assumption that each network route in $\mathbf{R}$ is equally likely to be the attacker's route, and the attack is started on one of the two flows on the attacker's route with equal probability.

III. Cross-Layer Model of Attack Propagation

We first model attack propagation under static network traffic and a given source of attack.

A. Physical-Layer Model

The prior work, e.g. [2], assumes that crosstalk attacks propagate in a deterministic fashion. This assumption holds for attack propagation in a given network infrastructure with deterministic jamming power at the source node of attack. However, the propagation is random if the strength of the jamming power at the source node is random. The stronger the jamming power inserted by the attacker, the farther an attack may propagate in the network. As he jamming power of the attacker at the source node of attack can have a wide range of values, in this work, we assume random jamming power at the source node of attack.

Consider that the crosstalk attack started on flow f_{sd}. Define the set of nodes traversed by flow f_{sd} as $\mathbf{V}_{f_{sd}} = \{V_1, V_2, ..., V_k\}$, with V_1 and V_k being the source and destination of flow f_{sd}. Then the crosstalk attack may propagate along route r_{sd}. Denote the signal power of flow f_{sd} in the switching plane of node V_i as a random variable U_i, $i = 1, 2, ...k$. The attenuation of the attacker's jamming power within the network can be captured using deterministic functions that depend on the characteristics of optical devices at the physical layer [5].

Let the status of node V_i be a random variable X_i, where $X_i = 1$ if the level of crosstalk incurred by normal flows from the attacker's flow at the switching plane of node V_i exceeds the threshold for a Quality of Service (QoS) constraint, and $X_i = 0$ otherwise. Then each node in $\mathbf{V}_{f_{sd}}$ may be affected due to the high signal power of the attacker's flow. Normal flows that are affected at the switching plane of a node $V_i, i = 1, ..., k$, may have increased power due to the crosstalk superimposed by the attacker's flow. However, these flows are assumed to have no attacking capability, as their crosstalk leakage to other flows in the same switching plane is negligible. Currently optical switches with a crosstalk ratio much less than -35dB are commercially available. Thus, we assume that only nodes along the attacker's route may be affected by the crosstalk attack.

Then it suffices to focus on $\mathbf{X}_{f_{sd}} = (X_i : V_i \in \mathbf{V}_{f_{sd}})$, which denotes the status of all the nodes along the attacker's route. Assume that, under normal operations, the amplifiers work at gain-clamped region and make up for the signal losses between two network nodes. It can be shown that the jamming power of flow f_{sd} at node V_{i+1} is no more than its jamming power at node $V_i, i = 1, ..., k-1$. Assume that the optical switches in the network have the same crosstalk ratio and threshold of crosstalk leakage for the definition of node affection, it can be proved that $\{X_i : V_i \in \mathbf{V}_{f_{sd}}\}$ form a Markov Chain [5]. Furthermore,

$$P(X_{i+1} = 1 \mid X_i = x_i, R_f = f_{sd}) = \alpha_i x_i, \quad i = 1, 2, ..., k-1, \qquad (3)$$

and $P(X_1 = 1) = 1$. Here $\alpha_i = P(X_{i+1} = 1 \mid X_i = 1, R_f = f_{sd})$ is the conditional probability that characterizes the attack

propagation at the physical layer, where the values of α_i's are determined by physical layer parameters such as: nodal loss ratios, amplifier gain characteristics, and fiber attenuation ratios (see [5] for details). In the rest of the paper, we assume that α_i's are known.

Next we consider the number of active flows at node V_i. Let $\mathbf{R}_{ij}$ be the set of network routes that use link ij. Under static traffic, $\sum_{r_{uv}\in\mathbf{R}_{ij}} n_{uv}$ corresponds to the number of flows that enter the switching plane of node V_i through link ij; $\sum_{r_{ih}\in\mathbf{R}_{ij}} n_{ih}$ corresponds to the number of flows that are locally originated at node V_i and enter the network through link ij. Hence, under static network traffic, the number of affected flows at the switching plane of node $V_i, V_i \in \mathbf{V}_{f_{sd}}$ is given by

$$P(S_i = s_i \mid X_i = x_i, \mathbf{N} = \mathbf{n}, R_f = f_{sd}) = \begin{cases} 1, & if\ s_i = \sum_{V_i \sim V_j} \{\sum_{r_{uv}\in\mathbf{R}_{ij}} n_{uv} + \sum_{r_{ih}\in\mathbf{R}_{ij}} n_{ih}\}\ \&\ X_i = 1; \\ & or\ s_i = 1\ \&\ X_i = 0, \\ 0, & otherwise. \end{cases} \quad (4)$$

This means that, when node V_i is affected by attack, all the active flows at the switching plane of node V_i are affected by the attack; otherwise, if node V_i is not affected by the crosstalk attack, only flow f_{sd} is affected by the attack at node V_i.

Combining (3) and (4), we have the physical layer attack propagation model,

$$P(\mathbf{S}_{f_{sd}} \mid \mathbf{N} = \mathbf{n},\ R_f = f_{sd}) = \sum_{\mathbf{X}_{f_{sd}}} \prod_{i=1}^{k-1} P(X_{i+1} \mid X_i, R_f = f_{sd}) \prod_{i=1}^{k} P(S_i \mid X_i, \mathbf{N} = \mathbf{n}, R_f = f_{sd}), \quad (5)$$

where $\mathbf{S}_{f_{sd}} = (S_i : V_i \in \mathbf{V}_{f_{sd}})$, and $\mathbf{X}_{f_{sd}} = (\mathbf{X}_i : V_i \in \mathbf{V}_{f_{sd}})$.

Therefore, under static network traffic (given $\mathbf{N} = \mathbf{n}$), $(X_i, S_i : V_i \in V_{f_{sd}})$ forms a directed probabilistic graph (Bayesian Belief Network). Each node in the Belief Network represents either X_i or S_i, $V_i \in \mathbf{V}_{f_{sd}}$ There is one directed edge from X_i to X_{i+1} and one directed edge from X_i to S_i respectively. Note that, given $\mathbf{N} = \mathbf{n}$ and $X_i = x_i$, S_i is deterministic, but S_i is included for an explicit graphical representation of attack propagation.

Fig. 1 shows an example of a simple mesh network where all the route in $\mathbf{R}$ marked in dashed lines. Suppose that the crosstalk attack is started on flow *BD*. Then the Bayesian Belief Network representation of attack propagation is shown in Fig. 2.

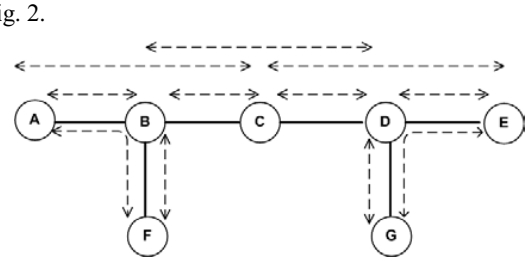

Fig. 1. A mesh network with 11 routes.

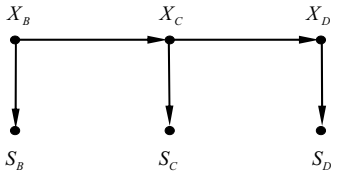

Fig. 2. Bayesian Belief Network representation when the attack started on flow *BD*; mesh network in Fig. 1.

B. Network-Layer Model

To characterize attack propagation under dynamic network traffic, we need to develop a network-layer model, $P(\mathbf{N} \mid R_f = f_{sd})$. It suffices to find $P(\mathbf{N})$, which can be characterized by an undirected probabilistic graph.

The network-layer model is formed as follows. Each vertex in the undirected probabilistic graph represents the status of a route $N_{ij}, r_{ij} \in R$. Furthermore, the status of all network routes that share the same link forms a clique. For instance, Fig. 3 shows the undirected probabilistic graph representation of the example network in Fig. 1. In [6], it has been shown that the steady state distribution of the number of calls in progress in loss networks without control form a Markov Random Field (MRF), which is one type of undirected probabilistic graph. Here we generalize the MRF representation in [6] to an undirected probabilistic graph representation to include the dependence among different routes due to the capacity constraint and the network load.

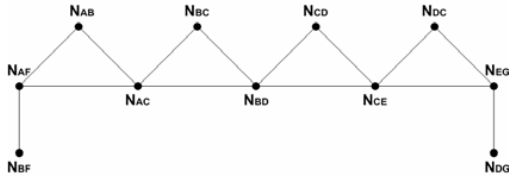

Fig. 3. Undirected Probabilistic Graph representation of network layer; mesh network in Fig. 1.

The joint probability distribution of $\mathbf{N}$ can be obtained by specifying proper clique potentials. Specifically, let the clique be $C_{ij}, C_{ij} = \{N_{sd} : r_{sd} \in \mathbf{R}_{ij}\}$. Let the potential function of C_{ij} be ψ_{ij}. Then, (1) $\psi_{ij} \neq 0$ if and only if the capacity constraint is satisfied, i.e., at most one connection is active on routes in $\mathbf{R}_{ij}$ (at each link, wavelength λ can only be used for one connection); (2) $\psi_{ij} = \gamma_{ij}$ if there is an active connection on link ij; otherwise, $\psi_{ij} = 1 - \gamma_{ij}$, where $0 \le \gamma_{ij} < 1$. Then, the joint probability of the status of all routes in $\mathbf{R}$ satisfies

$$P(\mathbf{N}) = \frac{1}{Z_{\mathbf{N}}} \prod_{(V_i \sim V_j)} \gamma_{ij}^{\sum_{r_{uv}\in\mathbf{R}_{ij}} N_{uv}} (1-\gamma_{ij})^{(1-\sum_{r_{uv}\in\mathbf{R}_{ij}} N_{uv})} I_1(\sum_{r_{uv}\in\mathbf{R}_{ij}} N_{uv}), \quad (6)$$

where $I_1(\sum_{r_{uv}\in\mathbf{R}_{ij}} N_{uv}) = 1$ if $\sum_{r_{uv}\in\mathbf{R}_{ij}} N_{uv} = 0$ or 1; and $I_1(\sum_{r_{uv}\in\mathbf{R}_{ij}} N_{uv}) = 0$ otherwise. Thus the dependencies of routes that result from the capacity constraints are captured. Meanwhile, the wavelength load of the network, i.e., the probability that wavelength λ is used at link ij's, is characterized by parameters γ_{ij}'s. When $\gamma_{ij} \equiv \gamma, \forall\, i \sim j$, we

can relate γ to the wavelength load through the following proposition.

Proposition 1: Let ρ denote the average wavelength load in the network, $\rho = E_{P(\mathbf{N})}[\sum_{V_i \sim V_j} \sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv} / |\mathbf{E}|]$. If in (6), $\gamma_{ij} \equiv \gamma, \forall\, i \sim j$, then ρ monotonically increases in γ.

For simplicity, in the rest of the work, we assume that $\gamma_{ij} \equiv \gamma$, $\forall\, i \sim j$.

C. Cross-Layer Model

The cross-layer model can be obtained by combining the physical- and the network-layer model using a factor graph [4], which corresponds to the following joint probability,

$$\begin{aligned} &P(\mathbf{X}_{f_{sd}}, \mathbf{S}_{f_{sd}}, \mathbf{N} \mid R_f = f_{sd}) \\ &= P(\mathbf{S}_{f_{sd}}, \mathbf{X}_{f_{sd}} \mid \mathbf{N}, R_f = f_{sd}) P(\mathbf{N} \mid R_f = f_{sd}), \end{aligned} \tag{7}$$

where $\mathbf{X}_{f_{sd}} = (X_i : V_i \in \mathbf{V}_{f_{sd}})$ and $\mathbf{S}_{f_{sd}} = (S_i : V_i \in \mathbf{V}_{f_{sd}})$.

The application of factor graph provides two advantages: (1) It shows the intricate dependencies among different network components during a crosstalk attack; (2) it provides computationally efficient algorithms to evaluate the network resilience loss, which shall be discussed in Section IV.

Fig. 4 shows the factor graph representation for the mesh network in Fig. 1 when the attack is started from flow *BD*. The lower portion of the factor graph represents attack propagation at the physical layer. As the attack may propagate from node V_i to V_{i+1}, $V_i, V_{i+1} \in \mathbf{V}_{f_{sd}}$, X_i and X_{i+1} are connected to the same factor node $P(X_{i+1} \mid X_i, R_f = f_{BD})$. Furthermore, the number of affected flows at node V_i is determined by X_i and routes that traverses node V_i. Therefore, S_i, X_i, and those routes passing through node V_i are connected to the factor node that corresponds to the conditional probability in (4).

The upper portion of the factor graph characterizes the dependence at the network layer. All the network routes that share a common network link ij are connected to the clique function ψ_{ij} in (6). Here, the factor graph provides an explicit representation of the dependencies among different network components during attack propagation.

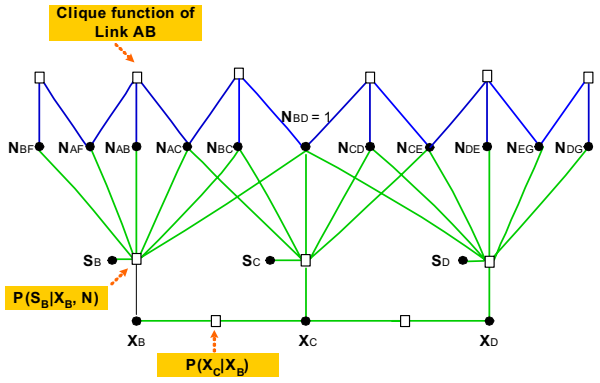

Fig. 4. Factor graph representation of mesh network in Fig. 1; attack started from flow *BD*.

IV. Network Resilience

We now use the cross-layer model to study network resilience. For simplicity, we assume that $\alpha_i \equiv \alpha, \forall V_i \in \mathbf{V}_{f_{sd}}$.

A. Regular Topologies

We first derive analytical results on network resilience for regular network topologies under a given wavelength load ρ and physical layer vulnerability α. The proofs and derivations can be found in [5].

Theorem 1: For a *ring* network, assume the route set $\mathbf{R}$ consists of the two-link disjoint routes between each pair of nodes in the network. Let k be the number of nodes traversed by the attacker's flow f_{sd}. Then, the network resilience loss $M_{f_{sd}}$ satisfies

$$v_1 + 2(1+\alpha^{k-1})\gamma \le M_{f_{sd}} \le v_1 + 2(1+\alpha^{k-1})\rho, \tag{8}$$

where $v_1 = k + 2\sum_{i=1}^{k} \alpha^{i-1}$. Furthermore, for $0 < \rho << 1$, $\rho = \gamma + o(\rho)$, and the upper and the lower bounds in (8) meet

$$M_{f_{sd}} = v_1 + 2(1+\alpha^{k-1})\rho + o(\rho). \tag{9}$$

Theorem 2: For a *star* network, assume that the route set $\mathbf{R}$ consists of the routes between each pair of nodes in the network. Let $m, m > 1$, be the number of nodes in the network. Denote the hub node of the star network as A_m. $M_{f_{sd}}$ satisfies,

$$M_{f_{sd}} \ge \begin{cases} 3+\alpha+(m-2)\alpha\gamma, & \text{if } f_{sd} = f_{A_i A_m}, i = 1,\ldots,m-1, \\ 3+\alpha+(m-2)\gamma, & \text{if } f_{sd} = f_{A_m A_i}, i = 1,\ldots,m-1, \\ 4+\alpha+\alpha^2+(m-3)\alpha\gamma, & \text{otherwise.} \end{cases} \tag{10}$$

$$M_{f_{sd}} \le \begin{cases} 3+\alpha+2(m-2)\alpha\rho, & \text{if } f_{sd} = f_{A_i A_m}, i = 1,\ldots,m-1, \\ 3+\alpha+2(m-2)\rho, & \text{if } f_{sd} = f_{A_m A_i}, i = 1,\ldots,m-1, \\ 4+\alpha+\alpha^2+2(m-3)\alpha\rho, & \text{otherwise.} \end{cases} \tag{11}$$

Furthermore, for $0 < \rho << 1$, the bounds in (10) and (11) are tight, and

$$M_{f_{sd}} = \begin{cases} 3+\alpha+2(m-2)\alpha\rho+o(\rho), & \text{if } f_{sd} = f_{A_i A_m}, i = 1,\ldots,m-1, \\ 3+\alpha+2(m-2)\rho+o(\rho), & \text{if } f_{sd} = f_{A_m A_i}, i = 1,\ldots,m-1, \\ 4+\alpha+\alpha^2+2(m-3)\alpha\rho+o(\rho), & \text{otherwise.} \end{cases} \tag{12}$$

We compare $M_{f_{sd}}$ for ring and star networks. In both cases, $M_{f_{sd}}$ is linearly increasing in ρ for $0 < \rho << 1$. However, for ring network, $M_{f_{sd}}$ is polynomially increasing in α; whereas for star network, $M_{f_{sd}}$ is linearly increasing in α. For ring networks, $M_{f_{sd}}$ is linearly increasing in k (the number of nodes in $\mathbf{V}_{f_{sd}}$). In contrast, for star networks, $M_{f_{sd}}$ is linearly increasing in m (the number of nodes in the network).

We also derive upper and lower bound of $M_{f_{sd}}$ for arbitrary physical topologies and summarize the results in Table I, where $|\mathbf{E}_{f_{sd}}|$ is the number of links that are incidental on nodes in the set $\mathbf{V}_{f_{sd}}$, and d_i is the nodal degree of node V_i.

Table I
Bounds of Network Resilience Loss $M_{f_{sd}}$

bounds α	Upper bound of $M_{f_{sd}}$	Lower bound of $M_{f_{sd}}$
$\alpha \to 1$	$2\sum_{i=1}^{k} d_i + (4-2k) - O(1-\alpha)$	$2k - O(1-\alpha)$
$\alpha \to 0$	$k + 2d_1 - 1 + O(\alpha)$	$k + 1 + O(\alpha)$

In addition, we compare the average resilience loss M for ring, star, and mesh-torus networks, and summarize the result in Table II. It can be observed that: (1) When the network load is low ($0 < \rho << 1$), M is $O(\rho/m)$. This is because when the load is close to 0, the network is most likely in either of two states: (a) there is no active connection in the network; or (b) there is an active connection of link length 1; (2) When the network load is high ($\rho \to 1$), the star network is the least resilient, with M being $O(\alpha)$. This is because, for the star network, nodes in the set $\mathbf{V}_{f_{sd}}, \forall r_{sd} \in \mathbf{R}$, has the most number of neighboring links. Ring and mesh-torus networks show good network resilience in $O(\rho/m)$.

Table II
Average Network Resilience Loss (*M*)

M	$\rho \to 0$	$\rho \to 1$
Ring network	$\rho(3+\alpha)/(m-1)$	$O(1/m)$
Star network	$\rho(3+\alpha)/m$	$O(\alpha)$
Mesh-torus	$2\rho(3+\alpha)/(m-1)$	$\begin{cases} O(1/(1-\alpha)m), & \text{if } \alpha \neq 1, \\ O(1/\sqrt{m}), & \text{otherwise.} \end{cases}$

B. Irregular Topologies

For networks with irregular topologies, we resort to the sum-product algorithm on the factor graph. The sum-product algorithm is then compared with the exact resilience calculation through enumerations of all network traffic patterns. Enumeration has computational complexity exponential in the number of routes, and is not applicable to networks with a large number of routes. The sum-product algorithm provides exact or approximate results depending on whether the factor graph is loopy or not [4]. We consider three networks shown in Fig. 5. In each network, the route set has 21 routes, which corresponds to one link-shortest route between each pair of nodes. Using the sum-product algorithm, we first compute $M_{f_{sd}}$, the network resilience loss given the source of attack. We then compute the average network resilience loss M.

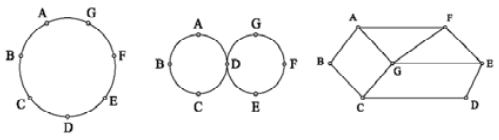

Fig. 5. 7-node ring, double-ring, and mesh networks.

Fig. 6 depicts the relationship between ρ and average network resilience loss M for networks in Fig. 5 with $\alpha = 0.6$. It shows that: (1) M monotonically increases with ρ, in networks with all-to-all traffic and link-shortest path routing. Moreover, for low load, M increases linearly with ρ; (2) The sum-product algorithm results in an almost exact M even though the factor graphs representations for the mesh and ring networks contain loops. The performance of sum-product algorithm is not as accurate yet acceptable for the double-ring network. This suggests that the sum-product algorithm can be used for large networks where exact calculation of resilience is infeasible.

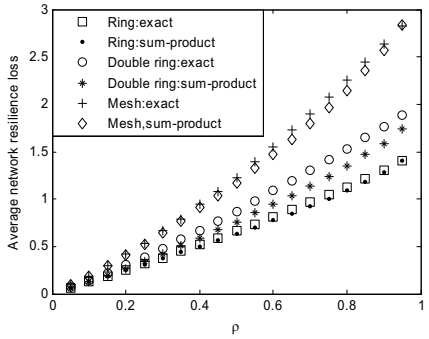

Fig. 6. Average network resilience loss vs. wavelength load; $\alpha = 0.6$, networks in Fig. 5.

V. SUMMARY

In this work, we have studied resilience of all optical network architectures against crosstalk attacks. We have shown that probabilistic graphical models can integrate attack propagation at the physical layer and dependent connections at the network layer into a cross-layer model. The cross-layer model provides an explicit representation of the dependencies between the physical and the network layer. Furthermore, the model facilitates analytical study of network resilience on regular topologies and provides the computationally efficient sum-product algorithm for evaluation of network resilience of irregular topologies. We have found that the ring and mesh-torus network show good resilience, which are inversely proportional to the number of the nodes in the network.

There are several open issues for future research. One direction is to develop physical-layer models of attack propagation under less stringent conditions.

REFERENCES

[1] 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/June 1997.

[2] T. Wu and A. K. Somani, "Cross-talk attack monitoring and localization in all-optical network," *IEEE/ACM Transactions on Networking,* Vol. 13, No. 6, pp. 1390-1401, December 2005.

[3] P. Smyth, D. Heckerman, and M. I. Jordan, "Probabilistic independence networks for hidden markov probability models," *Neural Computation*, 9, pp. 227-270, 1997.

[4] F. R. Kschischang, B. J. Frey, and H-A Loeliger, "Factor graph and the sum-product algorithm," *IEEE Transactions on Information Theory*, Vol. 47, No. 2, pp. 498-519, 2001.

[5] G. Liu and C. Ji, "Graphical Models for Resilience of All-Optical Networks under In-Band Crosstalk Attacks," *Technical Report*, School of ECE, Georgia Insitute of Technology, 2005.

[6] S. Zachary and Ilze Ziedins, "Loss networks and Markov Random Field," *Journal of Applied Probability*, no. 2, pp. 403-414, 1999.