Probabilistic Graphical Models for Resilience of All-Optical Networks under Crosstalk Attacks[*]

Abstract: We develop a framework based on probabilistic graphical models to study the resilience of all-optical networks under crosstalk attacks. Using this framework, we identify key factors that affect the network resilience.

1. Introduction

Resilience of all-optical networks (*AON*) is an important topic because of the high data rates supported by the network. Previous research mainly focuses on resilience of *AON* under network faults, e.g., network fault protection and restoration [1][2]; while resilience of all-optical network under malicious attacks needs more understanding. Examples of intentional attacks in *AON*'s include inband-jamming, crosstalk attack, and taping attack [3], among which, crosstalk attack is the most disruptive due to its potential to cause cascading failures in the network. Prior research in crosstalk attacks is mostly on attack management, e.g., attack detection and localization [4-5]. This paper focuses on (1) identifying and quantifying the key factors that affect the resilience of *AON* under crosstalk attack; (2) developing an approach based on graphical models to investigate complex dependencies that result from interactions of network nodes, links, and active connections under the attacks.

We define network resilience as the average percentage of nodes in the *AON* that are affected by the crosstalk attack. We study the network resilience using a two-layer model. At the physical layer, a directed graph (Bayesian Belief network) is used to model fault propagation, provided that the source of the crosstalk attack is known. At the upper layer, an undirected graph (Markov Random Field) is used to represent the probability distribution of active traffic flows in the network. The model can then be combined into a two-layer representation as a chain graph that is further converted into a factor graph [6]. The graphical models provide an explicit view of the spatial dependencies and interactions between the physical and the network layer, as well as a computationally efficient approach (sum-product algorithm) for evaluating the network resilience. Using graphical models, we show several factors that affect network resilience under crosstalk attacks: (1) wavelength load, (2) the interaction of network topology and the set of routes, (3) and wavelength assignment schemes.

2. Problem Formulation

We represent the *AON* as an undirected graph $G(V,E)$, with V being the set of *OXC* nodes, and $E=\{e_{ij}, i, j\in V\}$ being the set of links in the network. Assuming fixed routing, we let R be the set of network routes, and E_r be the set of links used by route $r, r\in R.$ We assume that there are no wavelength converters in the *AON*, all the traffic flows supported by the network are bi-directional, and the same wavelength is used in both directions for each flow. This is assumed for simplicity of illustration; while the work presented in this paper can be extend to networks supporting unidirectional traffic easily. The crosstalk attack is assumed to originate at the source of a traffic flow using a particular wavelength λ, and crosstalk only propagates through flows using the same nominal wavelength, i.e., λ. Therefore we ignore the effects of crosstalk attacks on wavelength channels of different nominal values, e.g., gain competition effect [3]. Based on the concept of network performance index [7], network resilience is defined as the average percentage of *OXC* nodes in the network that are affected by the crosstalks. We intend to answer the following questions for *AON* under crosstalk attacks: (1) How the statuses of different network components (e.g., network nodes, links and connections) interact with one another? (2) What are the key factors that affect the network resilience?

2.1 Two-Layer Model

(1) Physical layer: Bayesian Network

Following the definition in [5], we consider the original attack flow (*OAF*) as the flow where the attack is initiated, a secondary attacked flow (*SAF*) as a normal connection affected by an *OAF*, and a final attack flow (*FAF*) as a

[*] This work is supported in part by *NSF* 0300605.

connection influenced by an *SAF*. Reference [5] assumed that the fault propagates in a deterministic fashion upon crosstalk attacks. In most cases, the consequences of fault propagation upon attacks may vary because of many factors, e.g., the injected power at the source, the level of power attenuation along the fibers. Therefore, we propose a probabilistic approach based on Bayesian Belief network to model fault propagation.

Define the set of nodes traversed by the *OAF* as V_{OAF}. Define $V_{SAF} = \{V_i \in V \setminus V_{OAF} : e_{ij} \in E, V_j \in V_{OAF}\}$, which is the set of nodes not in V_{OAF} but are neighbors of nodes in V_{OAF}. Assume that only nodes in $V_{OAF} \cup V_{SAF}$ can be affected by the crosstalk attack. The Bayesian Belief network essentially assumes that: (1) the attack is initiated from one source node of one bi-directional flow (referred to as *OAF*), and then propagates from the source node to the other source node of the *OAF*; (2) The source node of the attack is affected by the attack with probability 1. For other nodes in V_{OAF}, their status only depends on their immediate upstream node along the *OAF*. If the immediate upstream node is not affected, then the node of interest is not affected; otherwise, the node is affected with probability α; (3) The attack also propagates from nodes in V_{OAF} to nodes in V_{SAF} through *SAF*s. It is assumed that the status of a node i in V_{SAF} only depends on its neighbors in V_{OAF}. Furthermore, each affected neighbor in V_{OAF} affects node i with probability β independently of all other nodes, if and only if the wavelength λ, on which the crosstalk is initiated, is used on the link between the two nodes. The value of α and β indicate how easily the fault may propagate in the network, which may depend on many factors, e.g., the power of the malicious signal injected to the network, and the power attenuations along the fibers. When $\alpha = 1, \beta = 1,$ the fault model presented in this paper reduces to the deterministic model proposed in [5]. The Bayesian Belief network shows how the statuses of different network nodes interact with each other through those of *OAF* and *SAF*s.

(2) Network Layer: Markov Random Field

A probabilistic distribution of active traffic flows at the time of crosstalk attacks is essential for the representation of attack propagation through active connections (*OAF* and *SAF*s), which leads to an upper-layer representation of traffic flows based on Markov random field (*MRF*). Let $n_i = 1$ if there is an active flow on route r_i using wavelength λ; $n_i = 0$, otherwise. Let $\mathbf{n} = (n_1, n_2, ..., n_{|R|})$ represent all flows in a network. Define a traffic pattern as a valid configuration of $\mathbf{n}$. A traffic pattern represents one possible way of using wavelength λ on the fixed set of network routes R. Let $w_k = 1$ if wavelength λ is used on link $k, \forall\, k \in E$, and let $\mathbf{W} = (w_1, w_2, ..., w_{|E|})$. A traffic pattern satisfies the following two conditions: (a) $w_k = \sum_{r \in R_k} n_r$, and (b) $w_k = 0, 1.$ Assume that wavelength λ is used independently in the network with probability γ_k. γ_k can be considered as the pseudo-load of link $k, \forall\, k \in E$ with $0 < \gamma_k < 1$. Note that normally the true marginal probability of $P(w_k = 1) \neq \gamma_k$, because the usages of wavelength λ on different links in the network are usually dependent if those links share one or more routes in the network, or equivalently, different network routes share network links. Assume that traffic patterns with the same wavelength usage $\mathbf{W}$ have the same probability, then the joint probability distribution of $\mathbf{n}$ and $\mathbf{W}$ is

$$P(\mathbf{n}, \mathbf{W}) = \frac{1}{Z_{\mathbf{n},\mathbf{W}}} \prod_{k \in E} (\gamma_k^{(w_k)} (1-\gamma_k)^{(1-w_k)} I(w_k, \sum_{i \in R_k} n_i)), \quad n_i, w_k \in \{0,1\}, \forall i \in R, k \in E. \qquad (1)$$

where $I(w_k, \sum_{i \in R_k} n_i) = 1$ if $w_k = \sum_{i \in R_k} n_i$, and 0 otherwise. The indicator function $I(.)$ guarantees that wavelength λ can only be used at most once in each link of the optical network. Here undirected graph (*MRF*) provides an intuitive representation of the dependencies of flows on different routes due to the capacity constraint. It describes how different routes interact and affect the wavelength usage at each link. Combining the Bayesian Belief network of the fault propagation and the *MRF* representation of traffic flows, we have a chain graph representation of the network resilience. The chain graph can be converted into a factor graph, and then the sum-product algorithm [6] can be used for fast and efficient evaluation of network resilience.

2.2 Example: 6-Node Mesh Network

Due to the space limit, we briefly introduce an example network as shown in Fig. 1. We assume that there is one shortest route between each possible source-destination pair in the network, and there are 15 routes in total (table I). Suppose there is one crosstalk initiated at node *B* along route *BE*, then the chain graph representation and the factor graph representation of network resilience are shown in Fig. 2 and Fig. 3 respectively. The statuses of network nodes, i.e., $X_A, X_{B,} X_C, X_D$, and X_E form the lower layer of the chain graph in Fig. 2, while the statuses of network links and flows form the upper layer of the chain graph. One example of the conditional probability defined in Fig. 3 is $P(X_A = 1 | X_B, w_{AB}) = \alpha$ if $X_B = 1$ and $w_{AB} = 1$; and $P(X_A = 1 | X_B, w_{AB}) = 0$ otherwise.

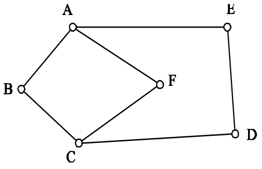
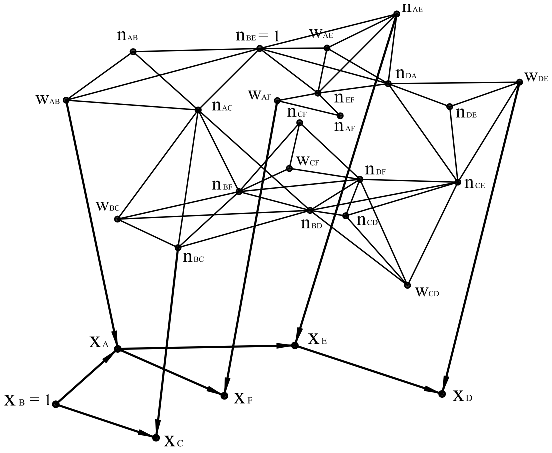


Fig. 1. 6-node mesh network

TABLE 1: Routing Table of the 6-node mesh network

Route	Used Links	Route	Used Links	Route	Used Links
r_{AB}	{AB}	r_{BC}	{BC}	r_{CE}	{CD, DE}
r_{AC}	{AB, BC}	r_{BD}	{BC, CD}	r_{CF}	{CF}
r_{AD}	{AE, DE}	r_{BE}	{AB, AE}	r_{DE}	{DE}
r_{AE}	{AE}	r_{BF}	{BC, CF}	r_{DF}	{CD, CF}
r_{AF}	{AF}	r_{CD}	{CD}	r_{EF}	{AE, AF}



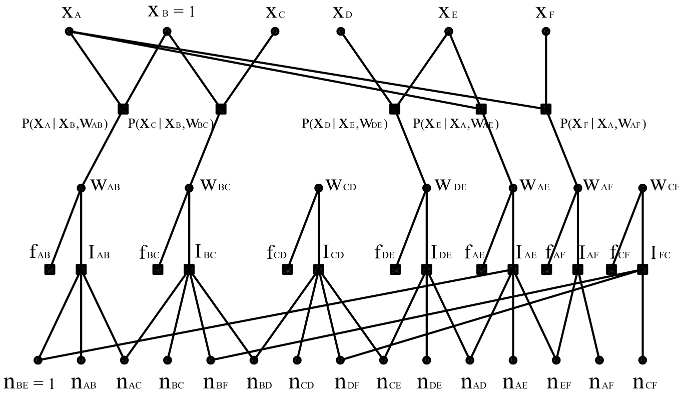


Fig.2. Chain graph representation of example in Section 2.2.

Fig. 3. Factor graph representation of example in Section 2.2.

3. Results

Based on the study of different network topologies, we find the following factors that affect the network resilience upon crosstalk attacks. (1) Wavelength load, i.e., the probability that wavelength λ, on which the attack is initiated, is used in the network. The higher the wavelength load, the less resilient the *AON*; (2) The interaction between the network physical topology and the set of fixed routes supported by the network. The physical topology of the network alone cannot determine the network resilience upon crosstalk attacks. For example, starting the attack at a network node with a higher nodal degree will not necessarily make the network less resilient; (3) Wavelength assignment schemes. We use simulations to study the resilience of the *NSF* network where traffic arrivals follow a Poisson process. It is found that when the network load is low, least-loaded wavelength assignment gives the best performance in terms of network resilience, while most-loaded wavelength assignment gives the worst performance; Random wavelength assignment provides better performance than first-fit assignment. When the network load is high, the four wavelength assignment schemes have similar performance in terms of network resilience.

References:

[1].B. Mukherjee, S. Ramamurthy, D. Banerjee, and A. Mukherjee, “Some principles for designing a wide-area optical network,” *Proc. IEEE INFOCOM’94*, pp. 110-119, 1994.

[2]. D. Xu, Y. Xiong, and C. Qiao, “Novel algorithms for shared segment protection,” *IEEE JSAC*, Series in Optical Communications Networks, Vol. 21, No. 8, pp. 1320-1331, Oct. 2003.

[3]. M. Medard, D. Marquis, R. A. Barry, and S. G. Finn, “Secuity issues in all-ptical networks,” *IEEE Network*, Vol. 11, No. 3, pp. 42-48, May/June 1997.

[4]. J. K. Patel, S. U. Kim, D. H. Su, S. Subramaniam, and H-A Choi, “A framework for managing faults and attacks in WDM optical networks,” *Proc. of the DAPRA Information Survivability Conference and Exposition*, 2001.

[5]. T. Wu, and A. K. Somani, “Necessary and sufficient condition for *k* crosstalk attacks localization in all-optical networks,” *Proc. of IEEE Globecom* 2003.

[6]. 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.

[7] A. M. Rushdi, “Performance indexes of a telecommunication network,” *IEEE Transactions on Reliability*, Vol. R-37, pp. 57-64, 1988.