Survivability for All-Optical Network against Optical Attacks

Nikhil Garg, Luv Kohli, Rahul Simha

***Abstract*— Security in an all-optical network can be compromised by an attacker that injects a powerful signal on a wavelength, resulting in crosstalk or gain competition, thus disrupting service. Conventional methods for survivability do not protect against such optical attacks. This paper considers the problem of finding two paths for given wavelength channels in the network such that they one of them remains available in the event of an optical attack. We term these paths as optically disjoint to each other.**

***Index Terms*—all-optical networks, attacks, disjoint paths, survivability.**

I. Introduction

The use of optical technology, in particular Wavelength Division Multiplexing (WDM), has revolutionized the transmission of voice and data. An enormous and easily accessible bandwidth is available today with the utilization of the considerable optical capacity of the fiber. On the other hand, the optical domain introduces its own set of challenges. Apart from the failure and attack scenarios present in conventional networks, there are certain hardware vulnerabilities present in the optical networks. Optical devices, such as switches and amplifiers are prone to crosstalk and gain competition. To this end, a technique is desired to avoid and minimize data loss due to these optical-domain specific phenomena. At the same time, we note that a fiber cut can result in a large loss of data whose recovery can overwhelm memory resources at the end nodes.

Much research has been done to provide a robust and reliable network. Survivable networks can be designed to recover from various failure and attack scenarios. Recovery can be dynamic as well as pre-planned, depending upon the network demands. Pre-planned recovery schemes are fast on one hand but require redundant network resources, whereas dynamic schemes can optimally utilize the available resources. Traditional networks are slow and the protocols they use can withstand the latency of the dynamic mechanisms. But recovery time in the faster pptical networks has to be much less, and as such pre-planned schemes are more suitable. Accordingly, much research has addressed the problem of finding primary and protection paths for optical connections. However, this body of work has not considered some unusual characteristics of an all-optical network. In this paper, we consider the problem of finding primary and protection paths while taking optical separation into account. The objective is to provide security in case of an optical attack. In this manner, an attack on one wavelength will affect as few other wavelengths as possible. Our goal is to find disjoint paths in a given network so that primary and protection paths are optically disjoint. We term our problem the Optically Disjoint Paths problem (ODP).

Although we will also consider networks containing some opto-electrical equipment, we nevertheless refer to these networks as All-Optical Networks (AONs) for reasons that will be clear in the paper.

Past work on the topic of primary and protection paths have extensively been considering only non-optical attacks and failures scenarios. None of them really consider the harware specific weaknesses of the network. Medard et al [3] have considered redundant trees for computing preplanned protection paths that are edge(node) disjoint, but these paths do not protect against optical attacks, that are caused by the physical characteristics of the underlying hardware. The optical specific issues have been discussed in [7], [8]. [10] have discussed the harware attacks, but their work primarily involves localization of these attacks in order to rectify them, or block such attacks. However the scheme is still dynamic and requires time for software processing and messages to be exchanged between network nodes during the localization protocol. Even if such attacks are localized, there has to be recovery scheme fast enough to avoid data loses and reliable enough to establish a valid data connection. Optical attacks result from failure propogation as discussed in [10], and differs from failure propogation as studied by [5], which relates to the hierarchy of the network, where failure restoration becomes impossible to achieve since the higher layers responsible for restoration, are themselves experiencing failure. This is usually the case in a WDM network, where the logical topology as provided by the IP network is built upon the physical topology provided by the optical fibers. A single failure in the optical layer, can result in multiple failures in the logical domain, diving the IP network into several isolated components. In this paper, we study failure propogation only at the physical level, where a malicious channel can affect other channels through optical devices.

The paper is organized as follows: Optical Networks and Optical Attacks have been discussed in detail in Section II and Section III. A formal definition of the problem and its NP-Completeness proof is provided in Section IV. The proposed algorithm has been described in Section V. Section VI presents the results from the heuristic algorithm, with the conclusions in Section VII.

II. All Optical Networks

An all optical network is a network, where the underlying interface between the user and the network is optical. As a result of the optical devices there are no optical-to-electrical conversions. Absence of any electrical conversion, makes the network fast and flexible. Terabit-per-second networks are already

Department of Computer Science, The George Washington University, Washington DC 20052. Email:nikhil@seas.gwu.edu

Department of Computer Science, The George Washington University, Washington Dc 20052. Email: lkohli@seas.gwu.edu

Department of Computer Science, The George Washington University, Washington DC, 20052. Email: simha@seas.gwu.edu

available in laboratories. Since fiber optic technology is progressing faster than the electronic technology, these networks also hold promise in terms of cost of employment. In future, the cost of optical devices is expected to fall sharply, making them highly attractive. These networks, as they exist today, employ two schemes, Time Division Multiplexing(TDM) and Wavelength Division Multiplexing (WDM). We would be consider only WDM networks in this paper. In a WDM network, each link(fiber) is divided into several channels, that carry independent data. These channels are actually different wavelengths supported by an optical fiber. A connection between any two nodes is a wavelength route between those two nodes. These wavelengths paths are illustrated by Figure 1. Each node is an optical switch that routes optical signals coming from one fiber to another fiber. As is evident from Figure 1, wavelengths blue, green and red are used by the top-left user in the figure, and the optical switch routes different colour wavelengths to different routers in the network, so that they are later available to their correct users at the other end of the network, resulting in a wavelength connection between the various user-pairs. A signal suffers enegry losses that are proportional to the fiber length they traverse. Often the distance between neighbouring switches(nodes) is enormous, especially in backbone networks, and amplifiers are placed at various intervals along the fiber length to re-strengthen the signal. All the nodes apply some amplification before passing the signal through the switch.

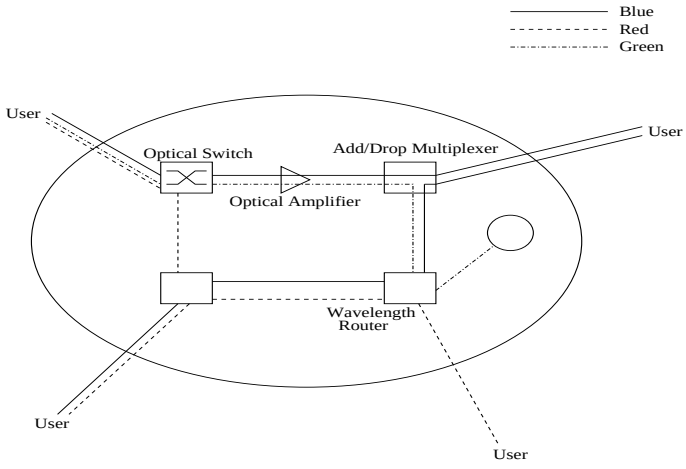

Fig. 1. An All-Optical Network

Some of the features of AON can be used to voilate the security and privacy of the network. These networks are susceptible to eavesdropping through fiber cuts, degrading quality of service or total denial of service. These vulnerabilities can be classified into physical and hardware specific. Issues of eavesdropping and tapping fall into the physical category, where the fibers have to be physically insecure to provide access to the attacker. There are no corrective measures for such attacks and physical inaccessibility of the entire network seems to be the only solution. However, the hardware vulnerabilites are more critical and cause more damage. The routing provided by the network is transparent. Signals that are trasmitted through the network are amplified at various network components, but are never re-generated. As a result a malicious signal may be designed to pass through a transparent part of the network, and disrupt service on part of the network. This is in contrast to a traditional network, where any malicious or abnormal signal would be discarded by the intermediate node, and would not be regenerated or an error message would be sent over the network.

III. Optical Attacks

The three primary components of the optical network that can be attacked are the fibers, the amplifiers and the optical switches. Of these, the optical fiber can be used to tap network traffic, or disrupt servie by cutting the fiber. These can only be avoided by making the fibers physically inaccessible, which is an almost unachievable task for a Wide-Area Network (WAN) or a Metropolitan Area Network(MAN). The two other components can be subjected to service denial or service degradation attacks that can be avoided. We would discuss these attacks in some detail next.

Optical Amplifiers

Typically optical amplifiers are rare-earth doped amplifiers. They work on the principal that there is a pool of available upper-state photons for signal attenuation. All the wavelengths share the same common pool of photons. This leads towards a gain competition phenonmenon. A strong signal(possibly a nefarious user) can deprive the weaker signals of photons, reducing its gain, thereby further weakening the signal. The severity of the attack depends on the distance of the attacker from the amplifier(the relative strength of the two signals), and can even result in a denial of service for some legitimate users.

Wavelength Switches

These switches route signals from different wavelengths to different outputs. They always suffer from some amount of cross-talk. Crosstalk is the phenonmenon which permits inputs to cause interference on other optical signals passing through these devices. Figure 2 explains the example of crosstalk. Wavelength red is being demultiplexed and later outputted at correct fiber through a multiplexer. However some signal leaks onto the blue plane and is combined with the blue signal output at its output fiber. Most switches use amplifiers as well to provide some attenuation to the outgoing(incoming) signals. These amplifiers as explained earlier can further effect the already contaminated signal. A more sophisticated attack by using a combination of the crosstalk and amplifier gain competition can potentially disrupt the entire node itself.

Upstream and Downstream Nodes

A node m is defined as an upstream (downstream) node from another node n if it receives data earlier (later) than the node n, while data is being transmitted between two nodes (they could be m and/or n) through a virtual path consisting of nodes m and n.

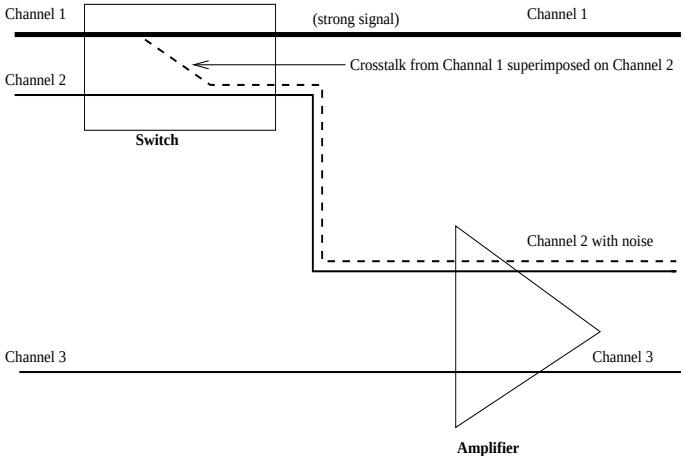

Fig. 2. Crosstalk from a strong channel introduces noise in a weaker channel

Optical Attack Propogation

Optical attacks can further damage the network because of their ability to propogate. An optical attack can propagate downstream of a node if it is not detected and stopped. A sufficiently strong signal can induce enough noice on a valid channel, such that the disrupted channel can then start to act as a malicious channel, and induce further service disruption on other channels. But , in the rest of the paper, we will assume that a wavelength attack cannot propagate downstream from an electrical switch. We also assume that any optical attack would not propagate beyond the channels that are directly affected by the attacking channel, that is, an attack cannot propagate by induction.

We can now define the term Optically Disjoint, based on our assumptions and definitions for optical attacks and its propogation. Two paths are termed as optically disjoint when they are node-disjoint paths (may not always be the case if some electrical switches are used) and there does not exist a channel that shares optical devices upstream of an opto-electrical-opto(OEO) switch with both paths, implying an optical attack on one of them cannot affect the other path. Network topology cannot always be rich enough to provide for optically disjoint paths in a fully-optical network, since it requires a huge amount of redundancy. Hence we introduce the concept of providing electrical switches at critical nodes in the network to allow existence of such optically disjoint paths, at the cost of minimum number of such switches in the network. We would refer to the Optically disjoint paths as OD paths in the rest of the paper.

IV. Problem Statement of ODP

Given a connected all optical network $N = (V, E)$ and a set of connection requests R , the objective is to provide connections with two paths primary and protection, such that the protection path and the primary path are optically disjoint. Any solution for the above problem would require the network topology to be rich enough to provide such paths. This may not always be possible. We propose a solution by placing OEO switches at certain nodes in the network. The assumption here is that once a signal passes through an OEO switch (upstream), any irregularity associated with it is discovered, and is blocked. As a result it is unable to affect channels downstream from that switch and the two paths are still considered to be optically disjoint. A topology assumption made in the algorithm is that there are enough wavelengths available on each link for any path chosen by the algorithm to be successfully routed over the network.

Proposition 1: ODP is NP-hard.

Proof. The well-known NP-complete problem of Maximum Length-Bounded Disjoint Paths can be reduced to an instance of the ODP problem. Therefore ODP is NP-hard.

V. Algorithm

We propose a greedy heuristics for the placement of OEO switches and construction of OD paths. Although the algorithm does not guarantee to find the optimal OEO requirement for the OD paths problem, it provides a greedy approach for the solution. The algorithm is based on the principle that the number of nodes that would eventually need such OEO switches should be minimized. For that the total number of hops (path length in case of unit length edges) the paths of the various connection requests got through should be minimized. The problem of minimizing the sum of the paths between two node pairs is a known NP-hard problem. Hence we focus on minimizing the number of hops for the primary paths.

The primary path length has been fixed, as a result we establish a backup path that would be in the least optical conflict with the primary path. A backup path, if found, is established. Otherwise a single node is converted to an electrical node until all backup paths have been established. As has been discussed previously, an upstream electrical node can stop any optical attack from propogating further. Hence it suffices to place an OEO switch at the most upstream node on a path. This heuristic works on the criteria of the most useful upstream node. At each iteration it identifies the best upstream node, that upon being converted to an electrical node would provide the maximum number of OD paths. The algorithm is defined next.

Step 1 Establish the shortest paths as the primary paths for all the connection requests.

Step 2 For each pair (s,d), compute intersects(s,d) = number of other pairs whose primary path intersects with its primary path.

Step 3 In increasing order of intersects(s,d), do

- 3.1 Compute the node-disjoint backup path for (s,d), such that it is also node-disjoint with all the primary paths that intersect with (s,d)'s primary path.

Step 4 While all the optically-disjoint have not been found do

- 4.1 Compute the list of all upstream nodes.
- 4.2 Identify the best upstream node, using the criteria that the best upstream node provides the maximum optically-disjoint paths.
- 4.3 Label the best upstream node.
- 4.4 Re-compute the backup paths as in Step 3, but by excluding those primary paths from the node-disjoint path list in Step 3.1, that have a labeled node as its first intersection node with the primary path of the current request-pair.

Step 5 All the labeled nodes are the nodes that are assigned OEO switches.

VI. Computation Results

The test networks were randomly created for different network size parameters , mainly the number of nodes, and edge connectivity. The minimum criteria being a connected network. Figure 3 provides an estimate for the redundancy required in a network, to provide a solution for the optically disjoint problem , using the algorithm proposed in the paper. As expected, a highly redundant network, with less connection requirement can easily provide such paths with a sufficiently small ratio for the number of OEO nodes in the network to the total number of nodes. We further observe that this ratio improves with the size of the network. With only 8% of the nodes needing an OEO for a 75 node network, a fairly good solution can be provided using our algoritm.

We define *saturation point* as the value of parameter set consisting of the edge connectivity of the network, and the number of connection requests, at which the ratio is 1. Computation results prove that saturation point for networks of various sizes is reached when the connection requests percentage is over 75% irrespective of the edge connectivity. However, below this limit smaller networks can still provide a below saturation solution even for a fairly large connection request percentage.

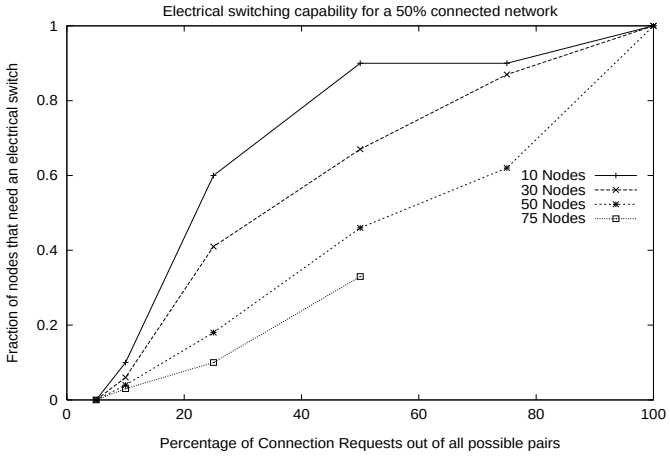

Fig. 3. OEO ratio with respect to the connection request demand

VII. Conclusions

We discussed in this paper, the importance of providing a backup path that considers optical separation, and termed such primary and backup paths as Optically Disjoint Paths. Since such paths cannot be established for all topologies, we proposed the use of electrical switches in the network to help in establishing optically-disjoint paths. We then presented a heuristic that can establish optically disjoint paths for any arbitrary connected network topology by efficient placement of electrical switches, that requires a small OEO capability from a sufficiently large network. Areas of interesting future work include handling multiple attacks and considering topologies that some electrical switching capability.

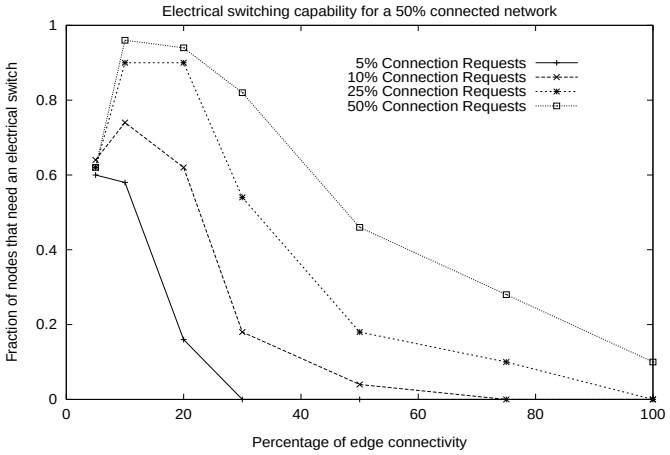

Fig. 4. OEO ratio with respect to the redundancy requirement of the network

References

[1] R. Garey and D.S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, Freeman, San Francisco (1979).

[2] Nikhil Garg, Rahul Simha, and Wenxun Xing, Algorithms for Budget-Constrained Survivable Topology Design, IEEE International Conference on Communications, (2002).

[3] Muriel Mdard, Steven G. Finn, Richard A. Barry, and Robert G. Gallager, Redundant Trees for Preplanned Recovery in Arbitrary Vertex-Redundant pr Edge-Redundant Graphs, IEEE/ACM Transaction on Networking, Vol. 7, No. 5 (1999), pp. 641-651.

[4] Murat Alanyali, and Ender Ayanoglu, Provisioning Algorithms for WDM Optical Networks, IEEE/AACM Transactions on Networks, Vol 7, No 5, October 1999.

[5] Olivier Crochat, Jean-Yves Le Boudec and Ornam Gerstel, Protection Interoperability for WDM Optical Networks, IEEE/ACM Transactions on Networking, Vol 8, No 3, June 2000.

[6] Rajiv Ramaswami, Pierre A Humblet, Amplifi er Induced Crosstalk in Multichannel Optical Networks, Journal of Lightwave Technology, Vol 8, No 12, December 1990.

[7] Muriel Medard, Douglas Marquis, Richard A Barry, and Steven G Finn, Security Issues in All-Optical Networks, IEEE Networks, May/June 1997.

[8] Arthur S Morris III, In Search of Transparent Networks, IEEE Spectrum October 2001.

[9] Sashisekaran Thiagarajan and Arun K Somani, An Effi cient Algorithm for Optimal Converter Placement on Wavelength-Routed Networks with Arbitrary Topologies, 1999.

[10] Ruth Bergman, and Muriel Medard, Distributed Algorithms for Attack Localization in Optical Networks.