Minimizing Inter Channel Attacks in WDM Optical Networks

Shengli Yuan, Lei Chen, and Ming Yang

Abstract—**Wavelength-division-multiplexing (WDM) optical networks provide higher data rate and stronger security than many other transport technologies. Yet optical networks are not completely immune to security treats, among which are interchannel attacks by exploiting the crosstalk effects, including eavesdropping and jamming. In this paper, we develop a novel routing algorithm to minimize lightpath overlapping thus minimize the damage caused by an interchannel attack. The algorithm has a running time that is exponential only to the number of existing lightpaths but polynomial to the network size.**

Index Terms—**Optical network security, interchannel attacks, eavesdropping, jamming, lightpath routing.**

I. Introduction

With the rapid advances in wavelength-division-multiplexing (WDM) technology, a lightpath is now capable of transporting traffic at data rate up to 100 Gbits/s or even 160Gbits/s, which makes WDM the dominate technology for transport networks [1]-[3]. At the same time, modern societies are becoming increasingly relied on communication networks. More and more sensitive, confidential or even classified information are being carried over the optical transport networks. A security attack can cause significant data loss or compromises, even if it is short and infrequent. Therefore it is of great interests to both the end users and the network operators to ensure network integrity and protect against various security attacks.

Security can be addressed either at the application layer, or at the network infrastructure layer. Application layer security includes various cryptography algorithms and protocols that are associated with individual applications. They are mostly based on the assumed computational difficulty of breaking security ciphers [4]. However, the rapid advances of computer technology and cryptanalysis have led to repeated breaking of the security ciphers that were once consider unbreakable. Efforts are now underway to develop more sophisticated and much stronger ciphers, including the ones based on quantum mechanics [5]. Therefore, it is insufficient to address security concerns merely at the application layer. Additional security can be obtained from security measurements at the network infrastructure layer, which protect all traffic carried by the transport networks.

Even though optical transport networks are generally considered more secure than copper-wire-based or wireless networks, they are still susceptible to security attacks ranging from fiber cuts to jamming [6][7]. Some of the attacks require an attacker to have physical access to network equipment, as in the case of fiber cutting and tapping, while others may be much stealthier, as in the case of interchannel eavesdropping and jamming. The latter is especially difficult to counter because an attacker may launch such an attack from a legitimately acquired data channel. This is explained as follows.

Users communicate through end-to-end lightpaths in WDM networks. All signals stay optical throughout a lightpath and there is no optic-electro conversion, thus a lightpath is a transparent circuit. The optical switching nodes provide signal amplification but no bit regeneration. With today's technology, each fiber link may supports up to several hundred lightpaths, each on a different wavelength channel. A low level interchannel crosstalk exists at the switching node, as well as on the fiber links when under high power input or long distance. This crosstalk effect is negligible when a lightpath is carrying normal traffic. But an attacker can exploit the crosstalk effects and launch both jamming and eavesdropping attacks. For both attacks, an attacker first legitimately acquires a lightpath. Then for a jamming attack, the attacker injects a high-power jamming signal into the acquired lightpath which may in turn lead to severe interference on other lightpaths that share a common switching node or fiber links. For an eavesdropping attack, the attacker stays silent and quietly collects the leakage signals from neighboring lightpaths. Useful information may be extracted when the collected signals are amplified.

Both types of attacks can be carried out without physical access to a switching node or fiber links, but they can cause substantial damages. We must develop effective countermeasures at the optical network layer. There are generally three strategies to enhance network security: prevention, detection and reaction. With preventative measurement, we try to remove the conditions which an attacker must rely on to initiate a successful attack. With detective and reactive measurements, we try to stop an ongoing attack and to minimize the damage. For prevention schemes to work effectively, potential treats and failures must be carefully analyzed and identified. Once the potential treats and failures are assessed, the next logical step is to route the communication paths in a way such that the possibility of an attack is reduced to minimum.

In this paper we develop a solution that can reduce the possibility of, or can even prevent the interchannel eavesdropping and jamming attacks. In the following section, we define the problem mathematically, and propose a novel algorithm with a running time that is polynomial to the network size. We then conclude the study in Section 3.

Manuscript received April 9, 2012; revised May 23, 2012.

S. L. Yuan is with Department of Computer and Mathematical Sciences, University of Houston-Downtown, TX 77002, USA (e-mail: yuans@uhd.edu)

L. Lei is Department of Computer Science, Sam Houston State University, Huntsville, TX 77341, USA

M. Yang is with School of Computing and Software Engineering, Southern Polytechnic State University, Marietta, GA30060-2896,USA

DOI: 10.7763/IJFCC.2012.V2.109

II. Problem Definition and Solution

A. Problem Definition

The fundamental idea of our solution is to minimize lightpath overlapping in optical networks. Here lightpath overlapping is defined as two or more lightpaths going through the same switching node or fiber link. When lightpath overlapping is minimized, the number of victim lightpaths from an interchannel jamming attack or an eavesdropping attack is minimized even if an attacker is able to access a legitimate lightpath. If we can completely eliminate lightpath overlapping, then an attacker will be unable to perform the interchannel attacks on any other lightpaths. Another benefit of minimum lightpath overlapping is increased network reliability. Because the number of common switching nodes or fiber links is reduced, the number of lightpaths that may be disrupted by the failure of a node or fiber link is also reduced to minimum.

Based on the number of given connection requests, network optimization problems can be categorized as either static traffic problems or dynamic traffic problems. For static traffic problems, all connection requests are given ahead of time. The objective is to achieve optimization over all the connections. On the other hand, for dynamic traffic problem, a connection request arrives one at a time. The objective is to achieve optimization for one connection request only. In real life, static traffic problems are handled by batch processing while dynamic traffic problems are handled by online processing.

In [8], Shkorin-Kapov, Chen and Wosinska studied the interchannel-attacks minimization problem under static traffic. The problem is NP-hard. They proposed an integral linear formulation (ILP) solution for small networks that give near-optimal results. For larger networks they proposed a tabu search heuristic algorithm combined with a graph coloring algorithm. In this paper, we study the interchannel-attacks minimization problem under dynamic traffic. Our search of recent literatures yielded no results. Therefore our work is likely to be the first on this topic.

The problem is defined as follows. Given network $G = (N, L)$ where N is the set of nodes, L is the set of links (assume they are bidirectional), also given existing set of lightpaths $P = \{ p_1, p_2, p_3, ..., p_l, ...p_L \}$, and node-lightpath parameters $\{ n_i^l \mid n_i^l = 1$ if lightpath p_l goes through switching node i where $i \in N$ and $p_l \in P$; and $n_i^l = 0$ if lightpath p_l does not go through switching node $i \}$, find one path p_{sd} from source node s to destination node t such that p_{sd} goes through common switching nodes shared with the minimum number of existing lightpaths in P, i.e.,

Minimize

$$\sum_i [(\sum_i n_i^{sd} n_i^l) / (\sum_i n_i^{sd} n_i^l)] \text{ for } \sum_i n_i^{sd} n_i^l \neq 0 \tag{Obj-1}$$

If p_{sd} shares common switching nodes with the minimum number of existing lightpaths in P, then it also shares common fiber links with the minimum number of existing lightpaths. Subsequently we minimize the number of victim lightpaths of an interchannel attack launched by an attacker using p_{sd} via crosstalks at common switching nodes or on common fiber links.

A weaker objective is to find a path that only shares common fiber links with the minimum number of existing lightpaths without concerning node sharing. Subsequently we minimize the number of victim lightpath of an interchannel attack by an attacker using p_{sd} via crosstalks only on common fiber links. In this case we replace the node-lightpath parameters $\{ n_i^l \}$ with fiber-lightpath parameters, i.e., $\{ f_{i,j}^l \mid f_{i,j}^l = 1$ if lightpath p_l goes through fiber link between node i and j where $i, j \in N$ and $p_l \in P$; and $f_{i,j}^l = 0$ if lightpath p_l does not go through fiber link between node i and $j \}$, the objective is now changed to finding a path p_{sd} from source node s to destination node t such that p_{sd} shares common fiber links with the minimum number of existing lightpaths in P, i.e.,

Minimize

$$\sum_l \left[(\sum_i \sum_j f_{i,j}^{sd} f_{i,j}^l) / (\sum_i \sum_j f_{i,j}^{sd} f_{i,j}^l) \right] \text{for } \sum_i \sum_j f_{i,j}^{sd} f_{i,j}^l \neq 0 \tag{Obj-2}$$

We now develop a novel algorithm to solve for Obj-1. We then apply the algorithm for Obj-2 with minor modifications. The algorithm has a running time that is only exponential to the number of existing lightpaths but polynomial to the network size.

For the following discussion, we focus on the routing issue. Even though wavelength assignment is another important issue for WDM networks, here we assume there are always plenty of free wavelengths for a new lightpath.

B. Solution for Obj-1

First we try to find the path p_{sd} without sharing any switching nodes with existing lightpaths. In order to do so, we create an auxiliary graph G^0 by removing from G all the switching nodes $\{n_i\}$ with a corresponding node-lightpath parameter $n_i^l = 1$ for all lightpaths $\{ p_l \mid p_l \in P \}$. Afterwards we run a shortest path algorithm with (s, t, G^0) as input. If it returns successfully, p_{sd} is set to the yielded path.

Otherwise we try to find the path p_{sd} that shares switching nodes with one existing lightpath. In order to do so, we create auxiliary graphs $G^1, G^2, G^3, ..., G^L$ by removing from G all the switching nodes $\{n_i\}$ with a corresponding node-lightpath parameter $n_i^1 = 1$, $n_i^2 = 1$, $n_i^3 = 1$, ... , $n_i^L = 1$ respectively for each lightpath $p_l \in P$. Afterwards we run a shortest path algorithm with (s, t, G^1) as input, then repeat it with (s, t, G^2) as input, and so on until finally repeating it with (s, t, G^L) as input. If any of the executions returns successfully, we compare the lengths of the retuned paths and set the shortest one to p_{sd}.

If the previous step fails, we try to find the path p_{sd} that shares switching nodes with two existing lightpaths. In order to do so, we create auxiliary graphs $G^{1,2}, G^{1,3}, ... , G^{1,L}, G^{2,3}, G^{2,4}, ... , G^{2,L}, ... , G^{L-1,L}$ by removing from G all the switching nodes $\{n_i\}$ with a corresponding node-lightpath parameter ($n_i^1 = 1$ and $n_i^2 = 1$), ($n_i^1 = 1$ and $n_i^3 = 1$), ... , ($n_i^1 =$

1 and $n_i^L = 1$), ($n_i^2 = 1$ and $n_i^3 = 1$), ($n_i^2 = 1$ and $n_i^4 = 1$), ... , ($n_i^2 = 1$ and $n_i^L = 1$), ... , ($n_i^{L-1} = 1$ and $n_i^L = 1$) respectively for each lightpath $p_l \in P$. Afterwards we run a shortest path algorithm with (s, t, $G^{1,2}$) as input, then repeat it with (s, t, $G^{1,3}$) as input, and so on until finally repeating it with (s, t, $G^{L-1,L}$) as input. If any of the executions returns successfully, we compare the lengths of the retuned paths and set the shortest one to p_{sd} .

If the previous step fails, we try to find the path p_{sd} that shares switching nodes with three existing lightpaths. When they fail, we try to find the path p_{sd} that shares switching nodes with four existing lightpaths. This process continues until we try to find the path p_{sd} that shares switching nodes with all existing lightpaths. The running time for each shortest-path procedure is O(|N|log|N|) [9]. There are at most 2L auxiliary graphs which we need to run the procedure for. Therefore the total running time of this solution is O(2^L|N|log|N|) for the worst case, which is exponential to only the number of existing lightpaths but polynomial to the network size.

C. Solution for Obj-2

The only modification we make to the solution for Obj-2 is how we create the auxiliary graphs. Instead of removing the switching nodes that are on the existing lightpaths, we now remove the fiber links that are on the existing lightpaths. For instance, in order to find the path p_{sd} that shares no fiber links with any existing lightpaths, we create an auxiliary graph G^0 by removing from G all the fiber links $\{f_{i,j}\}$ between nodes i and j with a corresponding fiber-lightpath parameter $f_{i,j}^l = 1$ for all lightpaths $\{ p_l \mid p_l \in P \}$. Afterwards we run a shortest path algorithm with (s, t, G^0) as input. If it returns successfully, p_{sd} is set to the yielded path. Otherwise we check other auxiliary graphs following similar steps as in for Obj-1 except that we remove fiber links rather than switching nodes.

Similarly, the running time for each shortest-path procedure is O(|N|log|N|). There are at most 2^L auxiliary graphs which we need to run the procedure for. Therefore the total running time of this solution is O(2^L|N|log|N|) for the worst case, which is exponential to only the number of existing lightpaths but polynomial to the network size.

III. Conclusion

In this paper we studied the problem of minimizing interchannel attacks in WDM optical networks for dynamic traffic. We developed a novel algorithm that always yields the optimal result if it exists with a running time that is polynomial to network size. A side benefit of this solution is increased network reliability in the event of a switching node failure or a fiber link failure.

For future study on the subject, we may investigate more efficient solutions with better running time. The wavelength assignment should be studied. We may also explore better heuristic solutions as well.

References

[1] T. Wuth, M. W. Chbat, and V. F. Kamalov, “Multi-rate (100G/40G/10G) Transport over Deployed Optical Networks,” in *Proceedings, Optical Fiber communication/National Fiber Optic Engineers Conference*, pp. 1-9. February, 2008.

[2] D. C. Lee, “100G and DWDM: Application Climate, Network and Service Architecture,” in *Proceedings, Optical Fiber communication/National Fiber Optic Engineers Conference*, pp. 1-3, February, 2008.

[3] R. Akimoto, S. Gozu, T. Mozume, K. Akita, G. W. Cong, T. Hasama, and H. Ishikawa, “All-optical wavelength conversion at 160Gb/s by inter subband transition switches utilizing efficient XPM in InGaAs/AlAsSb coupled double quantum well,” in *Proceedings, 35th European Conference on Optical Communication* (ECOC '09), pp. 1-2. September, 2009.

[4] C. Kaufman, R. Perlman, and M. Speciner, Network Security: Private Communication in *a* Public World (2nd Edition), Prentice Hall

[5] M. S. Sharbaf, "Quantum cryptography: An emerging technology in network security," *IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 13-19, Nov. 2011

[6] 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, 1997

[7] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, “Optical Layer Security in Fiber-optic Networks,” *IEEE Transactions on* Information Forensics and Security, vol. 6, no. 3, September 2011, pp. 725 - 736

[8] N. S. Kapov, J. Chen, and L. Wosinska, “A New Approach to Optical Network Security: Attack-Aware Routing and Wavelength Assignment,” *IEEE/ACM Transactions on Networking*, vol. 18, no. 3, June 2010, pp.750-760

[9] T. Cormen, C. Leiserson, R. Rivest, and C. Stein, *Introduction to Algorithms, 2nd ed*, 2001.