# Limiting the Propagation of Intra-channel Crosstalk Attacks in Optical Networks through Wavelength Assignment

**Nina Skorin-Kapov and Marija Furdek**
*Department. of Telecommunications, University of Zagreb, Unska 3, 10000 Zagreb, Croatia, tel: (+385) 1 6129 731, fax: (+385) 1 6129 832*
*nina.skorin-kapov@fer.hr, marija.furdek@fer.hr*

**Abstract:** Physical layer attacks in transparent optical networks are a serious security threat to network operation. We propose a novel protection approach based on wavelength assignment which limits the maximal propagation of intra-channel crosstalk attacks.

**OCIS codes**: (060.4251) Networks, assignment and routing algorithms, (060.4261) Networks, protection and restoration

## 1. Introduction

In Transparent Optical Networks (TONs), all-optical data connections, called lightpaths, are established between pairs of nodes forming a virtual topology over the physical interconnections of optical fibers. In order to establish a given set of lightpaths, it is necessary to efficiently solve the Routing and Wavelength Assignment (RWA) problem. Namely, each lightpath must be routed over the physical topology and assigned a certain wavelength subject to the following constraints. The wavelength clash constraint states that lightpaths traversing a common physical fiber cannot be assigned the same wavelengths, while the wavelength continuity constraint states that the entire lightpath must be assigned the same wavelength. The RWA problem has been shown to be NP-complete and, thus, several heuristic algorithms have been proposed to solve it sub-optimally. Common objectives for the RWA problem are to minimize the number of wavelengths [1] used or minimize lightpath congestion [2].

The high data rates and transparency in transparent optical networks make them highly vulnerable to physical layer attacks, such as power jamming and tapping [3]. Among the most malicious attacks with high damage capabilities are crosstalk attacks [4]. Most approaches proposed to deal with such issues are based on detection and restoration mechanisms which handle attacks after they occur. Additionally, some physical prevention mechanisms have been proposed, such as alarming fiber to prevent tampering. In [5], we investigated the possibilities of performing attack-aware routing to minimize the potential disruption caused by gain competition attacks in amplifiers and inter-channel crosstalk on fibers. Here we propose a novel approach aimed to limit the *propagation* of intra-channel crosstalk attacks in switches through careful wavelength assignment, minimizing the potential damage caused by such attacks in the planning process.

## 2. Intra-channel Crosstalk Attacks in All-Optical Networks

In fibers, long distances and high-power signals can introduce nonlinearities causing crosstalk effects between channels on different wavelengths, called inter-channel crosstalk. In optical switches, channels on the same wavelength can interfere with each other causing intra-channel crosstalk. Intra-channel crosstalk is much more influential of the two, since optical filters cannot remove the acquired undesirable leakage [6]. A deliberate intra-channel crosstalk attack is achieved by injecting a high-powered signal (e.g. 20 dB higher than the other channels) on a legitimate lightpath causing such significant leakage that attacked signals can acquire attacking capabilities themselves. Consequently, such an attack can propagate though the network, affecting links and nodes not even traversed by the original attacking signal. An example is shown in Fig. 1.a. where the attacker is able to attack User 2 (via User 1) even though they do not traverse any common components. Not only can this cause wide-spread service disruption, but it makes identifying and localizing the source much more difficult.

## 3. A new objective for the RWA problem: The Propagating Crosstalk Attack Radius (P-CAR)

Herein, we propose a new objective function for the WA problem. Namely, we wish to minimize what we refer to as the *Propagating Crosstalk Attack Radius* (P-CAR). We define the *Propagating Crosstalk Attack Radius* as the maximum number of lightpaths a jamming signal injected on any legitimate data lightpath can attack via propagating intra-channel crosstalk in switches. We assume that a jamming signal can potentially attack all lightpaths transmitted on the same wavelength with which it shares at least one common switch. Attacked lightpaths

The work described in this paper was carried out with the support of the BONE-project ("Building the Future Optical Network in Europe"), a Network of Excellence funded by the European Commission through the 7th ICT-Framework Programme.

can then acquire attacking capabilities themselves, further attacking lightpaths at switches *after* the attacking point, which can in turn also become attackers, and so on. Here we assume that an attack can propagate indefinitely in order to consider the worst case scenario of the disruption caused by a potential intra-channel crosstalk attack.

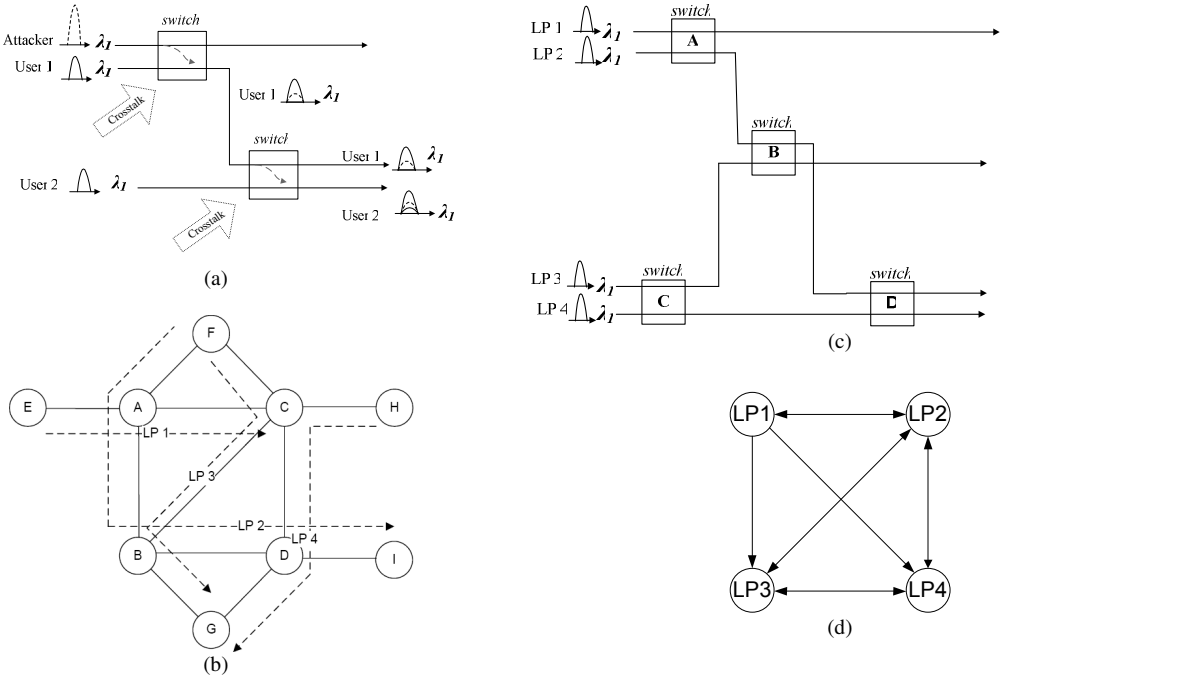



Fig.1. (a) An example of a propagating intra-channel crosstalk attack. (b) A sample routing scheme for four lightpaths, (c) the potential attacking points (intermediate switches traversed by at least two lightpaths) and (d) the corresponding attack graph.

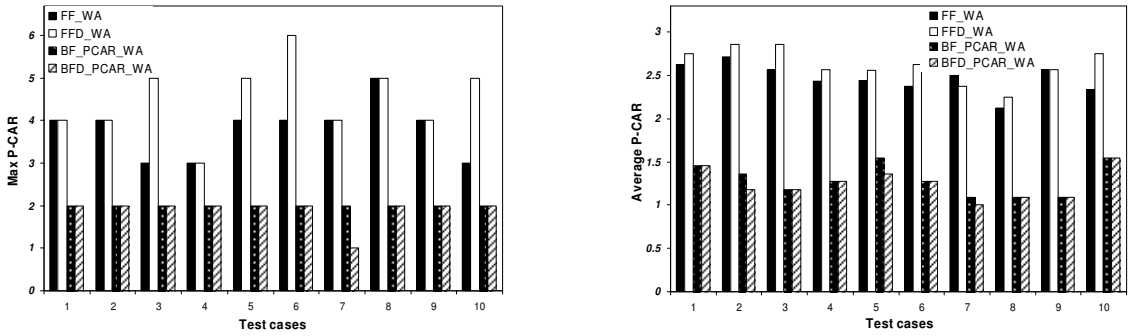
Consider the following example, shown in Fig. 1.b., depicting a routing scheme for a set of four lightpaths. Since all the lightpaths are link disjoint, they can all be assigned the same wavelength, denoted as $\lambda_1$. If a jamming signal is injected on one of them, it can attack all lightpaths it meets at switches after the injection point, which can in turn become potential attackers after *their* attacking point. Note that lightpaths originate at a transceiver at their source node and terminate at a receiver at their destination node without passing through a cross-connect and, thus, do not pick up any crosstalk at their end nodes. Consequently, potential intra-channel crosstalk attack points are only found at intermediate switches traversed by more than one lightpath, shown in Fig. 1.c.

In this example, we can see that if a high-powered signal is injected at the beginning of lightpath 1 (LP 1), it can attack LP 2 via switch A, which in turn can attack LP 3 via switch B and LP 4 via switch D. Thus LP 1's attack radius is 4 (including itself). LP 3 can attack LP 4 via switch C and LP 2 via switch B. Since LP 2 acquired attacking capabilities at switch B, it can only attack after this point, i.e. it cannot attack LP 1 at switch A. Thus, the attack radius of LP 3 is 3. The P-CAR for wavelength $\lambda_1$ is the maximum attack radius of any one lightpath transmitted over $\lambda_1$. If there are multiple wavelengths, the maximum P-CAR for a RWA scheme is the maximum P-CAR over all wavelengths. We can model the attack radii of the lightpaths routed on a common wavelength with a graph, which we call the *Attack Graph*, where each node represents a lightpath with outgoing links to nodes corresponding to lightpaths it can *directly or indirectly* attack. The Attack Graph for our example is shown in Fig. 1.d. The maximum out-degree of any node incremented by one (i.e. the lightpath on which the attacking signal was injected) is the value for the P-CAR on that wavelength, which in our example is 4.

**4. Heuristics for the WA problem: BF_PCAR_WA and BFD_PCAR_WA**

To solve RWA, we modify the heuristics based on bin packing with the objective to minimize wavelengths from [1] to incorporate our new objective, minimizing the P-CAR. We assume fixed shortest path routing and, thus, only concentrate on wavelength assignment. The algorithms run as follows. Given is a set of lightpaths, a physical topology and a fixed number of available wavelengths. We use a layered graph approach, where each layer of the physical topology represents a different wavelength. To solve wavelength assignment, we must route each lightpath on one of the available layers, such that lightpaths routed on the same layer are link disjoint. We assume there are enough wavelengths to cover the entire set of given lightpath demands and our objective is to minimize the maximum P-CAR over all layers. The BF_PCAR_WA (Best Fit P-CAR Wavelength Assignment) algorithm takes lightpaths in random order and routes them on the layer which yields the lowest P-CAR after accommodating the

lightpath, i.e. on the layer which yields the 'best fit'. The P-CAR on each layer is calculated by finding the attack graph corresponding to that wavelength using a recursive algorithm and then finding its maximum degree incremented by one. The BFD_PCAR_WA (Best Fit Decreasing P-CAR Wavelength Assignment) algorithm first sorts the lightpaths in decreasing order of their shortest paths and then proceeds as BF_PCAR_WA. For comparison purposes, we also consider two straightforward approaches we call the FF_WA (First Fit Wavelength Assignment) and FFD_WA (First Fit Decreasing Wavelength Assignment) algorithms which place lightpaths on the first layers onto which they fit in random order or in decreasing order of their shortest paths, respectively.




(a) (b)

Fig.2. The (a) maximum and (b) average P-CAR values obtained by the implemented algorithms for 11 available wavelengths.

## 5. Numerical results

We implemented the FF_WA, FFD_WA, BF_PCAR_WA and BFD_PCAR_WA algorithms in C++ and tested on the well-known 14-node NSF network. We created 10 different virtual topologies, i.e., sets of lightpaths, corresponding to 10 different traffic matrices. The traffic matrices were generated using the method in [7], where a fraction F of the traffic is uniformly distributed over [0, C/a] while the remaining traffic is uniformly distributed over [0, C ·ε /a]. The values were set to C=1250, a=20, ε=10, and F=0.7 as in [7]. Lightpaths are established between pairs of nodes in decreasing order of their corresponding traffic, with at most 5 lightpaths originating and terminating at each node. The number of available wavelengths was set to 11 because this was the minimum number of wavelengths which enabled the algorithms to accommodate all lightpath requests. We compared the maximum and average P-CAR values of the solutions obtained by the algorithms shown in Fig 2.a. and 2.b. respectively. We can see that the BF_PCAR_WA and BFD_PCAR_WA yield significantly better values for the P-CAR in all cases.

## 6. Conclusion

In this paper, we propose a novel approach to dealing with the problem of propagating intra-channel crosstalk attacks in transparent optical networks. Instead of developing monitoring and reaction techniques which require extra equipment and resources to deal with attacks after they occur, we propose to limit the maximal damage caused by such attacks in the planning process through careful wavelength assignment. We introduce a new objective, called the Propagating Crosstalk Attack Radius (P-CAR), and propose heuristic algorithms to obtain suboptimal solutions. Future work will include combining our wavelength assignment algorithms with attack-aware routing to minimize the potential damage caused by a set of attacks, including inter-channel crosstalk, power jamming exploiting gain competition in optical amplifiers, and tapping attacks.

## 7. References

[1] N. Skorin-Kapov, "Routing and Wavelength Assignment in Optical Networks Using Bin Packing Based algorithms," European Journal of Operational Research **177**, 1167-1179 (2007).

[2] D. Banerjee and B. Mukherjee, "A Practical Approach for Routing and Wavelength Assignmnet in Large Wavelength-Routed Optical Newtorks", IEEE Journal on Selected Areas in Communications **14**, 903—908 (1996).

[3] C. Mas, I. Tomkos and O. K. Tonguz, Failure Location Algorithm for Transparent Optical Networks. IEEE Journal on Selected Areas in Communications **23**, 1508-1519 (2005).

[4] T. Wu and A. K. Somani, Cross-Talk Attack Monitoring and Localization in All-Optical Networks. IEEE/ACM Transactions on Networking **13**, 1390-1401 (2005).

[5] N. Skorin-Kapov, J. Chen, L.Wosinska, "A tabu search algorithm for attack-aware lightpath routing" in the Proc. of ICTON'08, (Athens Institute of Technology, Athens 2008) pp.42-45.

[6] T. Deng, S. Subramaniam, J. Xu, "Crosstalk-aware wavelength assignment in dynamic wavelength-routed optical networks" in Proc. of Broadnets'04 (MIT, Boston, 2004), pp. 140-149.

[7] D. Banerjee and B. Mukherjee. "Wavelength-Routed Optical Networks: Linear Formulation, Resource Budgeting Tradeoffs, and a Reconfiguration Study", IEEE/ACM Transactions on Networking **8**, 598-607 (2000).