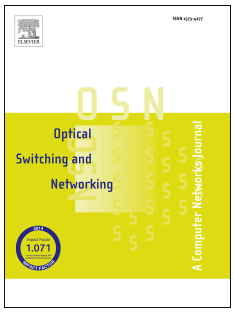
Accepted Manuscript



Attack-aware resource planning and sparse monitor placement in optical networks

D. Monoyios, K. Manousakis, C. Christodoulou, K. Vlachos, G. Ellinas

PII: S1573-4277(17)30220-5

DOI: 10.1016/j.osn.2018.03.003

Reference: OSN 477

To appear in: *Optical Switching and Networking*

Received Date: 1 November 2017

Revised Date: 11 March 2018

Accepted Date: 23 March 2018

Please cite this article as: D. Monoyios, K. Manousakis, C. Christodoulou, K. Vlachos, G. Ellinas, Attack-aware resource planning and sparse monitor placement in optical networks, *Optical Switching and Networking* (2018), doi: 10.1016/j.osn.2018.03.003.

Attack-aware Resource Planning and Sparse Monitor Placement in Optical Networks

D. Monoyios[1], K. Manousakis[2], C. Christodoulou[2], K. Vlachos[1], G. Ellinas[2]
[1]Computer Engineering and Informatics Dept. and Computer Technology Inst., Univ. of Patras, Rio, Greece
[2]KIOS Research and Innovation Center of Excellence and Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus
e-mail: {dmonogio@ceid.upatras.gr, manouso@ucy.ac.cy, christodoulou.chrysovalanto@ucy.ac.cy, kvlachos@ceid.upatras.gr, gellinas@ucy.ac.cy}

Abstract

This work presents joint optimization algorithms for lightpath establishment as well as sparse placement of optical performance monitoring (OPM) equipment in optical networks. OPMs are necessary to efficiently monitor the impact of physical layer attacks and are usually placed at locations that are more probable to be impacted by jamming attacks. A jamming attack is defined as a harmful signal interference with other signals, leading to service degradation, that is possible through intra-channel or inter-channel crosstalk effects. An Integer Linear Program (ILP) formulation is proposed to solve the problem of attack-aware routing and wavelength assignment (Aa-RWA), jointly with the placement of OPM equipment, in order to minimize the impact of physical layer jamming attacks in optical networks. Moreover, a Genetic Algorithm (GA) is proposed to solve the same optimization problem. The proposed GA algorithm is compared to the ILP formulation as well as to an attack-unaware RWA algorithm that has as an objective the minimization of the number of wavelengths required to accommodate all traffic demands, not accounting for the crosstalk interactions. Simulation results indicate that the proposed GA algorithm provides a solution that is close to the optimal in terms of crosstalk interactions, while also providing a very good solution in resource usage, measured in terms of the required number of wavelengths.

Keywords- *routing and wavelength assignment; monitor placement; physical layer attacks; optical networks.*

1 Introduction

With the exponential network traffic growth, optical network operators are required to provide upgraded architectures for their large-scale data transport networks in order to accommodate the increasing traffic, while also avoiding service disruption due to either malicious attacks or faults. Optical performance monitors in wavelength division multiplexed (WDM) optical networks are currently being utilized by the network operators for effective fault/attack detection as well as signal monitoring, thus ensuring better quality-of-transmission (QoT) for these networks. In all-optical WDM networks, data are transmitted through lightpaths, realized by determining a path between the source and the destination of a connection and allocating an available wavelength on all the links of that path. The selection of the path and the wavelength to be used by a lightpath is an important optimization problem, known as the routing and wavelength assignment (RWA) problem [1], [2]. The RWA problem belongs to the category of NP-complete problems, that is, the computational time for these problems would increase exponentially with the problem size. Thus, a wide range of optimization methods and heuristics have been proposed to solve various optical network optimization problems related to RWA [3], [4]. Genetic algorithms (GAs) are stochastic search optimization methods that are widely used in combinatorial optimization and parameter tuning applications and have also been used for solving the RWA problem [5], [6].

All-optical networks are vulnerable to physical layer attacks, such as high-power jamming attacks, as long as the data signals remain in the optical domain throughout the path, and are not regenerated at intermediate nodes. An *attack* is defined as an intentional action against the ideal and secure functioning of the network [7]. Significant research work has been carried over the last few years on the topic of physical layer threats and attacks in optical networks [7]-[17].