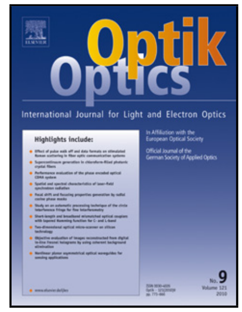

Title: Summation And Division of Status Algorithm For Multiple Crosstalk Attacks Source Identification

Author: H.W. Siew S.C. Tan C.K. Lee

PII: S0030-4026(16)31606-0
DOI: http://dx.doi.org/doi:10.1016/j.ijleo.2016.12.056
Reference: IJLEO 58686

To appear in:

Received date: 3-2-2016
Revised date: 3-6-2016
Accepted date: 20-12-2016

Please cite this article as: H.W.Siew, S.C.Tan, C.K.Lee, Summation And Division of Status Algorithm For Multiple Crosstalk Attacks Source Identification, Optik - International Journal for Light and Electron Optics http://dx.doi.org/10.1016/j.ijleo.2016.12.056

Summation And Division of Status Algorithm For Multiple Crosstalk Attacks Source Identification

H.W.Siew[1a], S.C.Tan[1], C.K.Lee[2]

hw.siew.hongwei@gmail.com[1a], sctan1@mmu.edu.my[1], cklee@mmu.edu.my[2]

Faculty of Computing and Informatics[1], Faculty of Engineering[2]. Multimedia University. Cyberjaya. Malaysia

ABSTRACT All Optical Networks operate in optical domain eliminating the process of Optical-to-Electrical-to-Optical contributes to the transparency characteristics of all optical networks. Transparency of all optical networks makes it vulnerable in term of physical security where the attacks cannot be detected at its transparent components. Hence, it is important to identify the source of crosstalk attack so that network management system can take accurate actions to ensure network survivability. In this paper, a multiple crosstalk attack source identification algorithm called Summation And Division Status is proposed and evaluated via the crosstalk attack propagation model where the crosstalk attacks contaminated all nodes in the network. The result obtained shows that the proposed algorithm successfully identifies multiple sources of crosstalk attack in Grid, NSF and Mesh networks.

keywords: *Crosstalk Attack, all optical network, detection and identification.*

1. Introduction

All-Optical Networks (AONs) are emerging as promising technology for data network infrastructure due to its high data rate. Signals within AON operate in optical domain and thus eliminating the process of "Optical-to-Electrical-to-Optical (OEO)" conversion. This elimination of OEO conversion contributes to the transparency characteristic of AON. As the result, AON allows high transfer rate up to Terabits per second has been reported [1]. However, transparency of AON makes it vulnerable in term of physical security where the attacks cannot be detected at its transparent components. Among them, the aggregate effect of crosstalk over an AON is more significant compared to others vulnerabilities [2]. Thus, crosstalk attack in AON is investigated here.

Many studies have been conducted on the nature of crosstalk attack propagation and the localization of crosstalk attack of crosstalk attack in AON [2-14]. The propagation and impact of crosstalk in AON has been presented in [3-7]. Two main factors determine the impact of crosstalk in a network is architecture of optical switch and the topology of network [6]. The vulnerabilities of different optical switch architecture to different optical switch architecture to crosstalk are presented in [3, 4]. In [5], the resilience of various network topologies is studied with respect to crosstalk attack. Deng [9] proposed a fault diagnosis algorithm using probabilistic reasoning in linear lightpath networks. Similarly, a system of alarm correlation and fault localization is proposed in [10]. However, both methods [9, 10] manage to localize set of most likely locations of source of attack. Other research works [8, 11-15] reported the detection and localization of crosstalk attack in AON for a small interconnected network with few optical fiber links under the crosstalk attack propagation up to two levels. Jedidi proposes the use of Crosstalk Identification and Monitoring System device for crosstalk localization [14]. In [11], a distributed algorithm for crosstalk attack localization is proposed and single source crosstalk attack is demonstrated. Similarly, multiple crosstalk attack localization using distributed approach is reported in [8]. On the other hand, Tao proposes an algorithm which manages to localize the source of crosstalk attack under sparse monitoring for single source crosstalk attack in a simple interconnected Grid network [15].

In this paper, a new algorithm called Summation And Division of Status (SADS) is proposed for multiple crosstalk attack source identification. The proposed algorithm employs simple step of summation and division of attacks status to localize the source of attacks. The proposed algorithm is tested successfully under worst case scenario where the crosstalk attack contaminated all nodes in 6-node Grid, 14-node NSF and 15-node Mesh networks.

The rest of this paper is organized as the following. In Section 2, we discuss the crosstalk attack propagation model and