Computer Networks 60 (2014) 129–146

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Self-healing in transparent optical packet switching mesh networks: A reinforcement learning perspective

Iván S. Razo-Zapata *, Gerardo Castañón, Carlos Mex-Perera

Department of Electrical and Computer Engineering, Tecnológico de Monterrey, Campus Monterrey, Av. Eugenio Garza Sada 2501 Sur, Col. Tecnológico, Monterrey, NL CP 64849, Mexico

ARTICLE INFO

Article history:
Received 22 June 2013
Received in revised form 24 September 2013
Accepted 4 November 2013
Available online 11 November 2013

Keywords:
Optical packet switching networks
Dimensioning
Reinforcement learning
Self-healing
Attacks
Monte Carlo simulation

ABSTRACT

While transparent optical networks become more and more popular as the basis of the Next Generation Internet (NGI) infrastructure, such networks raise many security issues because they lack the massive use of optoelectronic monitoring. To increase these networks' security, they will need to be equipped with proactive and reactive mechanisms to protect themselves not only from failures and attacks but also from ordinary reliability problems. This work presents a novel self-healing framework to deal with attacks on Transparent Optical Packet Switching (TOPS) mesh networks. Contrary to traditional approaches which deal with attacks at the fiber level, our framework allows to overcome attacks at the wavelength level as well as to understand how they impact the network's performance. The framework has two phases: the dimensioning phase (DP) dynamically determines the optical resources for a given mesh network topology whereas the learning phase (LP) generates an intelligent policy to gracefully overcome attacks in the network. DP uses heuristic reasoning to engineer the network while LP relies on a reinforcement learning algorithm that yields a self-healing policy within the network. We use a Monte Carlo simulation to analyze the performance of the aforementioned framework not only under different types of attacks but also using three realistically sized mesh topologies with up to 40 nodes. We compare our framework against shortest path (SP) and multiple path routing (MPR) showing that the self-organized routing outperforms both, leading to a reduction in packet loss of up to 88% with average packet loss rates of 1×10^{-3}. Finally, some conclusions are presented as well as future research lines.

1. Introduction

Transparent Optical Packet Switching (TOPS) networks are a relatively new technology for very high data communication rates, flexible switching and broadband application support. More specifically, they provide transparency features allowing data routing and switching without interpretation or regression of signals within the network, *i.e.* without opto-electronic-opto conversions [1]. Since TOPS networks only contain transparent optical components, they not only differ from the traditional optical networks but also bring about a new set of problems for network security such as power drop (PD), wavelength misalignment (WM), In-Band Jamming (IBJ) and Out-Band Jamming (OBJ) [2].

Because of these problems, the wavelengths channels are seriously affected, *i.e.* they may remain inoperable for a given period of time. Moreover, these problems occur mainly due to failures and attacks. According to Rejeb et al., failures occur due to the physical natural fatigue and aging of optical devices [3]. They occur once and remain within the devices until they are repaired. Contrary, the attacks appear and disappear often sporadically anywhere in the network, causing additional failures and

* Corresponding author. Tel./fax: +52 8181582293.
E-mail addresses: A00804384@itesm.mx (I.S. Razo-Zapata), gerardo.castanon@itesm.mx (G. Castañón), carlosmex@itesm.mx (C. Mex-Perera).

1389-1286/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.bjp.2013.11.002

problems to it [3]. In this sense, we aim at providing a framework to overcome attacks that cause wavelengths to be inoperable such as PD, WM, IBJ and OBJ.

Since network security countermeasures are categorized into three types of practices: *prevention*, *detection* and *reaction*, an attack-resilient mechanism for TOPS networks must cover them all [3]. In this research, we focus on *prevention* and *reaction* issues assuming that attack *detection* has been solved. Nonetheless, as the detection phase is of utmost importance to allow a proper reaction, we assume a detection mechanism with capabilities not only to detect wavelength attacks such as PD, WM, IBJ and OBJ but also with decentralized properties to use local information during the detection [4]. Helping in this way to achieve a self-healing behavior based on local changes [5].

We have previously explored several strategies to design an attack-resilient framework including prevention and reaction capabilities [6–10]. Motivated by our findings, we have decided to implement a framework with two phases. The first phase (prevention) relies on a heuristic algorithm to dimension/engineer the resources within a TOPS network while the second phase (reaction) applies a Reinforcement Learning (RL) algorithm to achieve an SH behavior and gracefully overcome attacks.

The contribution of this research is threefold. First, it presents an SH framework to gracefully overcome *wavelength attacks* in TOPS networks. Second, it shows how *wavelength attacks* can be included to engineer as well as to train TOPS networks. Third, it is the first time that reinforcement learning techniques are applied to achieve SH within TOPS networks. In the end, the SH framework leads to reductions in packet loss of up to 88%.

The rest of the paper is organized as follows. The related work is presented in Section 2 while Section 3 presents the tools used to simulate real-world TOPS mesh networks. Later on, Section 4 presents our SH framework and Section 5 presents the numerical results. Afterwards, Section 6 provides a general discussion. Finally, next to the general conclusions we also provide some future research lines in Section 7.

2. Related work

Rejeb et al. have performed an analysis on the nature of failures and attacks in transparent optical networks suggesting that attacks are more harmful than failures as they exhibit more complex behavior [3]. Attacks are not only harder to detect but also harder to solve as their effects spread rapidly through the network and might cause additional failures. Moreover, Rejeb et al. also argue that whereas rerouting traffic can solve all the problems caused by failures, rerouting traffic can not solve all resulting problems when the network suffers attacks. Based on the previous argument, we assume that failures can be subsumed by attacks. Consequently in what follows, we refer to failures and attacks as attacks.

Common attacks in transparent optical networks are: power drop (PD) which is caused by any change in the optical power like cutting or bending fibers, In-Band Jamming (IBJ) which is the result of intrachannel crosstalk due to different signals exchanging undesirable information in a switch as they have the same wavelength, Out-Band Jamming (OBJ) that includes interchannel crosstalk and nonlinearities initiated by an attacker that inserts power at a wavelength outside the signal window causing Raman effect and cross-gain modulation that will affect the signal, and wavelength misalignment (WM) caused by a transmitter emitting a signal with a wavelength slightly different than the expected one [2].

Since PD, IBJ, OBJ and WM can all affect one or more wavelengths within a fiber, resilience mechanisms to overcome attacks at a wavelength level are required. As previously mentioned, an attack-resilient mechanism for TOPS networks must cover *prevention*, *detection* and *reaction* issues [3]. In TOPS networks, *prevention* schemes that aim to reduce vulnerabilities include network design, component design, provisioning, operational regulations among others [3]. A common mechanism to protect TOPS networks is to equip the optical nodes with several alternative paths to forward packets, *e.g.* multiple path routing (MPR) [11,12] which provides a quick way to solve contention of packets, faults, and attacks using alternate routing. A similar routing scheme is the self-protecting multi-path (SPM) [13] which allows to protect a network based on many disjoint paths.

The *detection* of multiple attacks has been previously shown to be NP-complete for graph-based systems [14]. Nonetheless the detection of attacks in TOPS networks has been addressed from different perspectives. For example, Tapolcai et al. [15] present an algorithm that can achieve so-called unambiguous failure localization (UFL) of single link failures. Although, a failing link can be precisely identified, phenomenon at wavelength level is overseen, *i.e.* if within a link only some wavelengths are being attacked, the algorithm will determine that the full link is under attack which will prevent free wavelengths of being used. Mas et al. [2] propose an algorithm based on a binary tree that computes information gathered from different types of monitoring devices such as optical power meters, optical spectrum analyzers and strategies such as bit-error rate monitoring. The algorithm allows to detect wavelength attacks such as PD, WM, IBJ and OBJ. Rejeb et al. [4] present the so-called MALI algorithm that relies on monitoring Optical Cross-Connect (OXC) nodes in a distributed manner which allows to detect wavelength attacks using local information gathered from each OXC node. Recently, Furdek et al. have proposed an algorithm to achieve a certain degree of attack localization, such algorithm is based on the computation of the so-called propagating crosstalk attack radius (P-CAR) [16]. By limiting the maximal radius of IBJ attack propagation the algorithm gives an idea about where attacks are more likely to occur. Nonetheless, as mentioned in [2], there is still not an accurate method to locate attacks in TOPS networks.

The design of *reaction* mechanisms has been recently addressed from a learning perspective [17]. The idea is that if a network experiences problems under certain network conditions (failures or attacks), it learns them, and then tries to keep away from any such conditions or unforeseen but similar conditions which are expected to