Chapter 12

Self-Healing on Transparent Optical Packet Switching Mesh Networks: Overcoming Failures and Attacks

Iván S. Razo-Zapata
ITESM, Mexico

Gerardo Castañón
ITESM, Mexico

Carlos Mex-Perera
ITESM, Mexico

ABSTRACT

This work presents a novel approach for dealing with failures and attacks on Transparent Optical Packet Switching (TOPS) mesh networks. The approach is composed of two phases, whereas the first one dynamically dimensions the resources in the network, the second one applies an incremental learning algorithm that generates an intelligent policy. At each node, such a policy allows a self-healing behavior when there are failures or attacks in the network. Finally, the performance of this approach is presented as well as future research lines.

INTRODUCTION

Transparent optical packet switching (TOPS) networks are becoming more and more attractive due to their ability to reduce power consumption and total cost; this cost reduction is obtained through the use of a lower number of transponders. TOPS networks can also avoid the bottleneck of optoelectronic conversion and switching at each node (Yoo, 2006). However, transparency raises many security vulnerabilities as well as reliability issues that do not exist in traditional optoelectronic networks (Mas et al., 2005).

Security and reliability issues are of utmost importance in transparent optical networks given...
the extremely large fiber throughput, the lack of optoelectronic conversions and the rapid propagation of attacks among other features. Fast and successful reaction and restoration mechanisms performed by failure management can prevent loss of large amounts of critical data, which can cause severe service disruption (Tomkos et al., 2004).

In order to deal with failures and attacks (Skorin-Kapov et al. 2007) have already considered intelligent and self-organized mechanisms. The main argument is that autonomous elements of the network, such as optical switches, can dynamically adapt to changes due to failures and attacks by, for instance, reconfiguring data lightpaths.

In this work we propose a self-organized approach to deal with failures in transparent networks. Our approach relies on two phases. The first one is a dynamic dimensioning where TOPS resources are determined; one of our claims is that by a good dimensioning, the network provides higher flexibility to deal with failures and attacks. The second phase is an incremental learning process in which the TOPS network continuously learns a self-healing strategy to overcome failures and attacks. Multiple Path Routing (MPR) is used on both phases to route packets, i.e. nodes have knowledge of different paths for different targets (Castañón et al., 2000).

**PROBLEM DESCRIPTION**

TOPS mesh networks are a relatively new technology for very high data rate communications, flexible switching and broadband application support. More specifically, they provide transparency features allowing routing and switching of data without interpretation or regression of signals within the network, i.e. without opto-electronic-opto conversions. Such networks contain only transparent optical components and therefore differ from the optical networks currently used. In particular, the nature of TOPS components and architectures brings about a new set of problems for network security, such as the design of resilient mechanism for dealing with failures and attacks.

Before explaining some issues regarding design of resilient mechanisms, it is worthwhile making some comments about failures and attacks. As already established by Rejeb et al. (2006), failures occurs due to physical natural fatigue and ageing of optical devices. They occur once and remain within devices until they are repaired. Contrary, attacks appear and disappear often sporadically anywhere in the network, causing additional failures and problems in the network. Based on the previous argument, we assume that failures are subsumed by attacks. Consequently in the rest of the text, we refer to failures and attacks just as attacks.

When designing failure-resilient mechanisms for TOPS mesh networks, it is not only fast-response that becomes an issue but also problems as attack detection & location, and adaptability. In the next paragraphs we provide broader explanation regarding these issues.

**Attack Detection and Location**

Since in TOPS networks multiple optical signals co-propagate in fiber and optical components, possibly affecting each other directly or indirectly, the quality of a signal is sometimes dependent on or degraded by other signals making difficult the task of determining whether such degradation is caused by an attack or not. In addition, once the attack is detected, the localization task is still not trivial. Mas et al. (2005) have already described in which ways optical components can mask attacks in the network. For instance, a regenerator can mask an attack regarding power drop that occurred before the regenerator, therefore monitoring devices located after it are not able to locate the attack on that channel.

Even more, as discussed by Medard et al. (1998) signals can be maliciously designed to pass through transparent components, causing undesirable effects at remote components and
Related Content

[www.igi-global.com/chapter/cross-layer-radio-resource-management/49755?camid=4v1a](www.igi-global.com/chapter/cross-layer-radio-resource-management/49755?camid=4v1a)

An Exploration of the Critical Need for Formal Training in Leadership for Cybersecurity and Technology Management Professionals

Internet of Things: Privacy and Security Implications
[www.igi-global.com/article/internet-of-things/179894?camid=4v1a](www.igi-global.com/article/internet-of-things/179894?camid=4v1a)

Internet of Things in E-Health: An Application of Wearables in Prevention and Well-Being
[www.igi-global.com/chapter/internet-of-things-in-e-health/179791?camid=4v1a](www.igi-global.com/chapter/internet-of-things-in-e-health/179791?camid=4v1a)