Optimal Monitoring Equipment Placement for Fault and Attack Location in Transparent Optical Networks

Carmen Mas Machuca*and Ioannis Tomkos

Athens Information Technology (AIT) Center, Markopoulo Av, PO. BOX 68, 19002 Peania, Athens, Greece
{cmas,itom}@ait.edu.gr

Abstract. Last decade, network security has become a very sensitive and important topic for equipment manufacturers and network operators. Physical layer security in opaque optical networks relies on the information obtained at the opaque nodes where the signal is electronically regenerated. However, in transparent optical networks, security is even more complex since the optical signals are not regenerated and, therefore, faults and attacks are more difficult to be detected and isolated. Our work deals with the study of the optical placement of monitoring equipment which may help operators to optimize the investment on their equipment while increasing the accuracy to locate the faults and attacks (so-called failures). For this purpose, we have extended our Transparent Failure Location Algorithm (TFLA), which is able to locate failure(s) in transparent optical networks in presence of false and/or lost alarms to propose an optimal location for new monitoring equipment. and tested it for the Pan-European network.

1. Introduction

Network management involves configuration, performance, fault, accounting and security management functionalities. Fault management relies on the information retrieved from the monitoring equipment in order to detect faults and react to them. Opaque networks allow supervising the signal at each opaque node where the optical signal is converted to the electrical domain. However, in transparent networks the data remains in the optical domain all along its path (i.e. without going through any optical-to-electrical conversion but through optical amplification and optical switching in the near future, and optical regeneration and conversion further in the future) and the optical signal is more exposed to degradation without being noticed by the network management system. On the other hand, the information received by the network management system is more limited in transparent networks as it relies on analog signal measurements at some points of the network, whereas in opaque networks per bit or BER performance based monitoring is available. However, we should point out that when the transmission speed increases, BER monitoring becomes very expensive as it requires high speed signal processing.

Fault management deals with the prevention, detection, and reaction to faults. Prevention deals with the component and network design so that it can prevent faults.

When the fault has occurred, detection takes care of learning about the existence of the fault and to identify it. Finally, reaction manages to restore the connections that have been disturbed by the fault. All these functionalities become even more important in optical networks because of (i) the high bit rates that cause a huge amount of information to be lost (ii) the high latency of the network that allows a lot of data to get into the network when the fault occurs, (iii) the fault identification that should be efficient and exact in order to restore the connections and isolate the fault efficiently[1]. Fault identification is based on the alarms received by the network management system and it should cope with the existence of false and/or lost alarms. When there are two or more simultaneous faults, the number of alarms increases considerably, the alarms arrive intermingled to the management system, and the problem of locating the faults becomes even more difficult.

Fault management can be extended to also cover attacks. Attack can be defined as an intentional action against the ideal and secure functioning of the network. Attacks can be classified as eavesdropping or service disruption[2]. Hence, we can define as failure the set of faults and attacks that can interrupt the ideal functioning of the network. In this paper, we will present an algorithm to locate failures (both faults and attacks) in transparent optical network in presence of false and/or lost alarms and some results when the algorithm is applied to the Pan-European network.

The paper is organized as follows. Sect. 2 introduces transparent optical networks including an overview of their components and an example of a possible attack. Sect. 3 presents the Transparent Failure Location Algorithm (TFLA) which includes the methodology of the algorithm. Sect. presents some results on the study of the optimal location of new monitoring equipment. Finally, Sect. 5 concludes the paper.

2. Performance monitoring in transparent optical networks

In transparent optical networks the signal remains in the optical domain along its path without going through any optic-to-electric conversion. These networks are very promising as they reduce unnecessary, expensive optoelectronic conversions, offer high data-rate, provide flexible switching, and support multiple types of clients (different bit rates, modulation formats, protocols, etc.).

Transparent optical networks contain two classes of network components: (i) Optical components which take care of the optical signal transmission and are not able to generate alarms, and (ii) Monitoring equipment (ME) which is able to generate alarms and notifications when the optical signal is not the expected one. The alarms generated by monitoring equipment depend on the kind of equipment and its characteristics. The failure of the monitoring equipment does not interrupt/modify the data transmission and therefore their failure is not as relevant as the failure of an optical component. Moreover, when monitoring equipment fails, it may result in the loss of alarms which will be considered in the proposed algorithm as lost alarms.

As discussed previously, transparent optical networks are more vulnerable to failures than opaque networks because (i) the quality of the optical signal is not evaluated at each node and (ii) a single failure can affect more channels than in opaque networks, as there are no transparency boundaries supported by optoelectronic regenerators. An example of this is shown in Fig. 1. In this scenario, an attacker inserts optical power at a wavelength that is already used (λ2). This attack will cause an increase of the optical power at that wavelength that will disturb neighbouring channels (e.g. when traversing an optical amplifier such as EDFA, the gain that λ2 channel will experience will be greater than the gain of λ1 channel (case *a* of Fig. 1)). Even after filtering channel λ1 at the wavelength demultiplexer, there is some residual optical power at λ2 higher than the one specified in the system, so it can degrade the performance of its neighbouring channels (case *b* of Fig. 1). When there are optical switches, crosstalk is very critical. In our example, λ2 channel of Fibre Nf could be disturbed by λ2 channel of Fibre 1 due to crosstalk (case *c* of Fig. 1). The degree of crosstalk is closely related to the optical power pumped by the attacker.

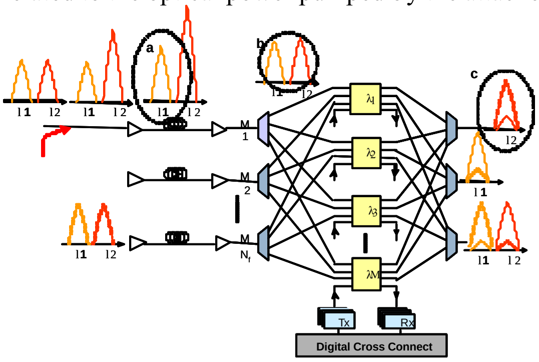

Fig. 1. Example of an attack on an Optical Cross-connect (OXC) with wavelength selective architecture and its propagation through different network components

The attacks that may occur in a transparent optical network can be classified into four categories[3] based on the effects they inflict on the signal: power drop (e.g. power decrease and cut), in-band jamming (including also intrachannel crosstalk), out-band jamming (including also interchannel crosstalk and non-linearities), and wavelength misalignment.

3. Transparent Failure Location Algorithm

The failure location algorithm has to be able to locate the optical component or set of optical components that cause the received alarms in case of failure. The problem of locating multiple failures has been shown to be NP-complete even in the ideal scenario of receiving each of the expected alarms[4]. The complexity increases further when lost and false alarms are considered. In order to minimize as much as possible the time to locate failure(s), the complexity of the proposed algorithm has been concentrated in a Pre-Computational Phase (PCP) so that the computation to be carried out when new alarms reach the manager is kept as small as possible. The second phase, which is called Core Phase (CP), consists just in traversing a simple binary tree when alarms reach the manager. The proposed PCP has been implemented on the basis of an algorithm used to locate multiple faults in non-ideal opaque networks[5]. This algorithm uses an important concept *Domain(component*) which is defined as the set of network components that will generate an alarm when this component fails. The result of the PCP is a binary tree with a depth equal to the number of monitoring components and whose leaves correspond to different failure scenarios with an accepted number of false and lost alarms (*mismatching threshold*). We have extended this algorithm to the case of transparent networks (so-called Transparent Failure Location Algorithm or TFLA)[3]. In this case the algorithm computes as many domains for each component as types of failures (four in our case: power drop, in-band and out-band jamming, and wavelength misalignment). The extended algorithm includes the proposal of an optical location for new monitoring equipment as presented in next section.

4. Optimal monitoring equipment location

The optimal location problem for new monitoring equipment (ME) has been studied. We define *optimal location* as the position of the ME that minimizes the number of network elements that are candidates to have a failure ie. that minimizes the result given by the TFLA. For this purpose, the algorithm while computing the domains of all the optical components, it stores the series *(Xa,Yb)* with the highest number of components located between *Xa* (a transmitter or the first optical component right after a monitoring equipment), and *Yb* (the following monitoring equipment). This length is so-called MSL standing for Maximum Segment Length. By definition, the optimal position for a new ME will be the one that divides the series *(Xa,Yb)* in two series *(Xa,Xc)* and *(Xc+1,Yb)* with *Lac* and *Lc+1 b* as close as possible. In this way, after including this ME in this position, the network components that are candidates to be faulty will be certainly reduced.

4.1 Established channels based

For long term channels, the extended TFLA was run on the Pan-European Topology network[6] within a ring between Madrid, Barcelona, Lyon, Paris and Bordeaux (Fig. 2) that is assumed to be transparent. Optical Add/Drop Multiplexers (OADMs) are located at the cities of Madrid, Barcelona and Bordeaux, whereas Optical Cross-Connects (OXCs) are located at Paris and Lyon. The assumed architecture for the OXCs and OADMs is Wavelength Selective (as shown in Fig. 1).The number of amplifiers needed for each link depends on the distance between the cities. Due to the overall ring length, optical regeneration is needed in some nodes (Barcelona, Paris and Bordeaux). Three different channels have been considered: Ch. 1 from Barcelona to Madrid, Ch.2 from Barcelona to Bordeaux via Madrid, and Ch. 3 from Madrid to Paris via Bordeaux Three cases have been compared:
Case 1: A single ME is installed at the end of each channel.
Case 2: One ME is installed at the location proposed by TFLA (at Madrid's node).
Case 3: One new ME (one more than Case 2) is installed at the location proposed by TFLA, which is at the output of Bordeaux's node.
The TFLA was run for the three cases considering that there are no false or lost alarms. The number of optical components that could be faulty was studied for two scenarios and plotted in Fig. 3:

Scenario I: when receiving an alarm from the receiver of Ch. 2 at Bordeaux and **Scenario II:** when receiving two alarms issued by the monitoring equipment located when dropping Ch. 1 at Madrid and Ch. 2 at Bordeaux.
For both scenarios an important reduction on the number of candidates to be faulty is shown (e.g. 90% less in Scenario II when one ME was included).

4.2 Topology based

The previous work shows the improvement on the failure location when new ME is located where the TFLA proposed based on the established channels. However, network operators may be more interested in the location of new ME based on the network topology rather than the channel based approach. The reason is that the established channels are not fixed and may change with the time, and hence, if we had optimized the ME location for a particular set of established channels, it won't be optimal if the set change.

The extension of the TFLA could be used for any topology if we are able to find the longest channel that can be established in the given topology. We focused on the case of interconnected Pan-European rings shown in Fig. 4 and tested three scenarios: Scenario 1 with a single ring (Ring 1) of 57 network elements, Scenario 2 with a double ring (Ring 1 and Ring 2) of 119 optical components, and Scenario 3 with a triple ring (Ring 1 and Ring 3 interconnected through Ring 2), of 193 components. In all cases, only one ME was been considered initially. New ME was installed in the proposed location and the number of candidates was decreasing (shown in Fig. 5).

The problem of minimizing the MSL is a partition problem with rate 2. For all these scenarios, in order to decrease the maximum segment length to 2^{-n} of its original value, 2^{n}-1 monitoring equipment should be installed (the location is given by the extended TFLA and it is in the middle of the longest segment).

5. Conclusions

This paper described the fault location problem in transparent optical networks and its extension to failure location and optimal placement of new monitoring equipment. Transparent networks are more vulnerable than opaque networks to failures due to the absence of electrical conversion of the optical signal and the cost of the optical monitoring equipment. Some work has been presented on attack location but it was limited to specific network components. We have proposed an algorithm called TFLA able to locate fault and attacks in transparent networks coping with the existence of some false and/or lost alarms. Simulation results on the optimal placement of monitoring equipment in a transparent Pan-European Network have been presented. It is anticipated that these results can be exploited by network operators since this algorithm may help them to decide whether to invest on some expensive monitoring equipment depending on whether the result returned by the TFLA reduces or not.

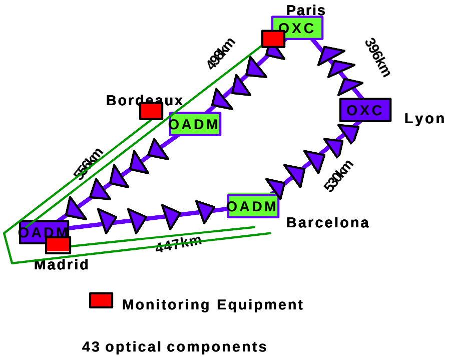

Fig. 2. Considered European transparent ring including the amplifiers and the regeneration nodes needed and the considered ME

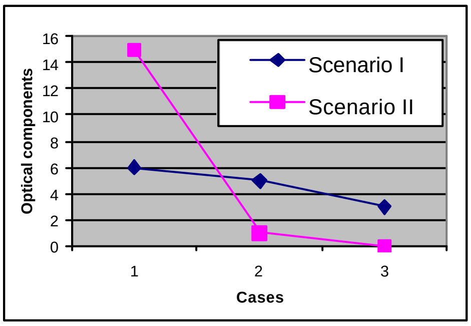

Fig. 3. Graph showing the decrease of the number of optical components that are candidate to have a failure when including new ME

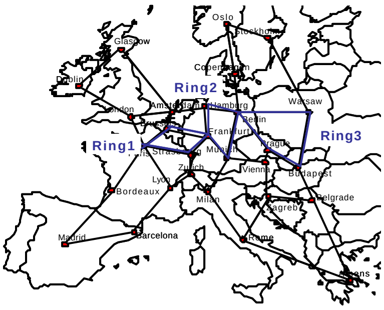

Fig. 4. Pan-European network with three interconnected rings

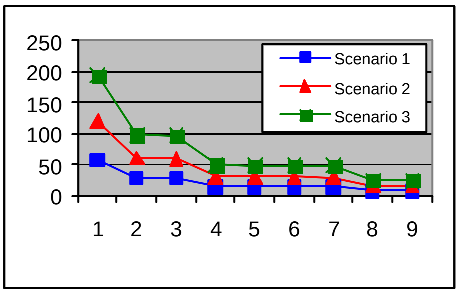

Fig. 5. Decrease of the maximum segment length as a function of the installed ME

References

1. M. Medard et al., "Node wrappers for QoS monitoring in transparent optical nodes", Journal of High Speed Networks, Vol. 10, 2001, pp. 247-268
2. M. Medard, D. Marquis, R. A. Barry, and S. G. Finn “Security Issues in all-optical Networks” IEEE Network, May/June 1997, pp. 42-48.
3. C. Mas, I. Tomkos and O. K. Tonguz., “Optical Network Security: A Failure Management Framework” ITCom 2003, 5247 Session, pp. 230-241, Sept. 2003.
4. N. S. V. Rao. “Computational Complexity Issues in operative Diagnosis of graph-based systems”, IEEE Transactions on Computers, 42(4), April 1993
5. C. Mas and P. Thiran “An efficient algorithm for locating soft and hard failures in WDM networks” JSAC Special Issue on protocols and architectures for next generation WDM optical networks, Vol. 18, Oct. 2000.
6. S. De Maesschalck et al., “Reference Scenario for a Pan-European Network” COST 266 Report, August 2002