Hardware-Based Monitoring Method for All-Optical Components

A. Jedidi[1], R. Rejeb[2], B. Rejeb[1], M. Abid[1], M.S. Leeson[2], and R.J. Green[2]
[1]National School of Engineering, University of Sfax, Tunisia
[2]School of Engineering, University of Warwick, UK

ABSTRACT
In emerging All-Optical Networks (AONs), efficient monitoring and estimation of signal quality along a lightpath[1] are of highest interest because of their importance in diagnosing and assessing the overall health of the network. This is because transmission in these networks is limited by a number of effects such as optical crosstalk and amplified spontaneous emission. In particular, crosstalk is additive and can be exploited to perform service disruption attacks upon the whole network. Since these attacks can spread rapidly through the network, causing additional awkward failures and triggering multiple undesirable alarms, they must be detected and identified at any point in the network where they may occur. Due to network transparency[2], this requires particularly the availability of expert diagnostic techniques to measure and control the smallest granular component, the wavelength channel. However, to monitor all wavelengths at several detection points in a node is likely to be a very expensive solution. In this paper we briefly overview optical crosstalk mechanisms that arise in AON components. We then propose a hardware-based method for monitoring performance degradation in AON Components that can participate in some tasks for performance management of AONs.
Keywords: all-optical networks, securing optical networks, attack management, monitoring device.

1. INTRODUCTION

The presence of a network management system is essential to ensure efficient, secure, and continuous operation of any network. Specifically, a network management implementation should be capable of handling the configuration, fault, performance, security, accounting, and safety in the network. Network management for AONs faces additional challenges and still unsolved problems. An important implication of using AON components in optical communication systems is that available methods generally used to manage and monitor the health of the network may no longer be appropriate. While some of available management mechanisms are applicable to different types of network architectures, many of them are not adequate for AONs and must therefore be carefully addressed [1]-[4]. By their nature, AON components are particularly vulnerable to various forms of denial of service and eavesdropping attacks. Since these attacks can spread rapidly through the network, causing additional failures and triggering multiple alarms, they must be detected and identified at any point in the network where they may occur [3]. However, to monitor all wavelength channels at several detection points in any node in the network is likely to be a very expensive solution.

A key component in any management system is the performance management as it provides signal quality measurements at very low Bit Error Rates (BERs) and fault diagnostic support for fault management. Performance management is still a major complication for AONs. In particular, signal quality monitoring is too difficult in AONs as the analogue nature of optical signals means that miscellaneous transmission impairments aggregate and can impact the signal quality enough to reduce the Quality of Service (QoS) without precluding all network services. This results in the continuous monitoring and identification of the impairments becoming challenging in the event of transmission failures. However, a simple and reliable signal quality monitoring method does not exist at present. Despite new methods for performance monitoring having been proposed, no robust standards or techniques exist to date for guaranteeing the QoS in AONs. Therefore, the need for more sophisticated mechanisms that assist managing the proper function of AONs is highly desirable [3]-[9].

In this paper, we propose a hardware-based method for monitoring performance degradation in AONs. First, we present a brief overview of typical forms of optical crosstalk that may arise in AONs from the components they employ. Then, we present the key concepts of the hardware-based Monitoring Device Block (MDB). Next, we consider the internal architecture of this device focusing particularly on its functional concept. After that we present open directions for future work and conclude the paper.

2. CROSSTALK IN AON COMPONENTS

Optical crosstalk is present in AON components and degrades the quality of signals, increasing their BER performance as they travel through the network. In AONs, optical crosstalk arises in two forms namely *interchannel crosstalk* and *intrachannel crosstalk* [9]. The former arises between adjacent signals at different wavelengths, whilst the latter occurs between signals at the same nominal wavelength.

Interchannel crosstalk arises when the crosstalk signal is at a wavelength sufficiently different from the affected signal's wavelength that the difference is larger than the receiver's electrical bandwidth. Interchannel

[1] A lightpath is defined as an *end-to-end* optical connection between a source and a destination node.
[2] A component is called X-transparent if it forwards incoming signals from input to output without examining the X aspect of the signal. For example, AON components are electrically transparent.

crosstalk can arise from a variety of sources. One potential source is in a wavelength demultiplexer, shown in Figure 1 (a), that imperfectly separates the incoming wavelengths to different output ports. Another arises in an optical switch, shown in Figure 1 (b), that is switching different wavelengths because of imperfect isolation between the switch ports. Although the main interchannel crosstalk components usually come from the two adjacent channels, and the components from the other channels are usually negligible, interchannel crosstalk effects can also occur through more indirect interactions. A simple example occurs in an optical amplifier if one channel affects the gain seen by another channel, which can lead to service disruption attacks [3]. Another example is with regard to nonlinearities in optical fibers and devices that can lead to undesirable cross-modulations and consequently cause service disruption or subtle tapping attacks. In particular, under high power inputs or over long distances, optical fibers exhibit nonlinear effects that cause interactions among signals on different wavelengths. For instance, a signal on one wavelength may cause amplification or attenuation of a signal on another wavelength through cross-phase modulation and Raman gain effect[3]. Thus, there are crosstalk effects among wavelengths in transmission fibers, which can be exploited by sophisticated attackers. Interchannel crosstalk, therefore, should be earnestly taken into consideration by any channel that contributes such components, even if the main crosstalk components usually come from the two adjacent channels and in many cases can be eliminated by optical filters or wavelength demultiplexers.

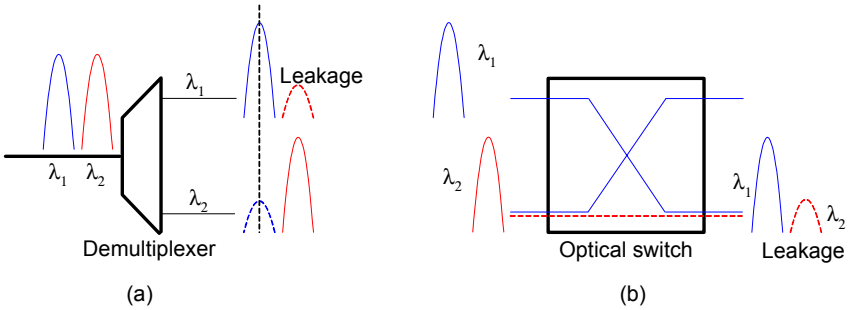

Figure 1. Sources of interchannel crosstalk. (a) Crosstalk arises in a demultiplexer due to imperfect separation of wavelengths. (b) Crosstalk arises in an optical switch due to non-ideal isolation of one port from the other.

Intrachannel crosstalk arises when the crosstalk signal is at the same wavelength as that of the affected signal or sufficiently close to it that the difference in wavelengths is within the receiver's electrical bandwidth. Intrachannel crosstalk arises in transmission links due to reflections. This is usually not a major problem in such links since these reflections can be controlled and eliminated. However, intrachannel crosstalk can be a major problem in AONs when it arises from other sources. One potential source arises from cascading a wavelength demultiplexer with a wavelength multiplexer (demux/mux) as shown in Figure 2 (a). Another source is in an optical switch, shown in Figure 2 (b), switching the same-wavelength signals, due to the non-ideal isolation of one switch port from the other. Compared to interchannel crosstalk, intrachannel crosstalk effects are of prime importance for AONs because they can lead to severe power penalties and cannot be eliminated by filters or wavelength demultiplexers.

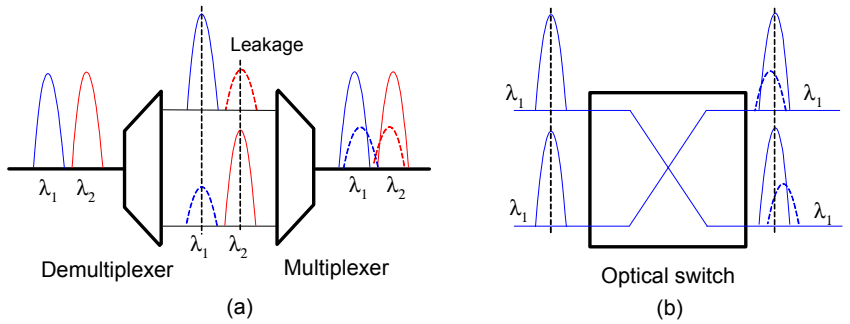

Figure 2. Sources of intrachannel crosstalk. (a) Crosstalk arises from cascading a wavelength demultiplexer with a wavelength multiplexer. (b) Crosstalk arises in an optical switch switching signals of the same wavelength.

Optical-Cross-connects (OXCs) are essential key components enabling traffic to be switched entirely in the optical domain, where lightpaths can be set up and taken down as needed without having to be statically provisioned. Although these components offer many advantages for communication systems, they are particularly vulnerable to various forms of crosstalk attacks. One of the serious problems related to network

[3] Raman effect or stimulated scattering is one of the non-linear effects that can be used to degrade the quality of optical signals.

transparency is the fact that optical crosstalk is additive, and thus the aggregate effect of crosstalk over a whole network may be more nefarious than a single point of crosstalk. As the resulting degradations accumulate and grow rapidly become severe with network size, they constitute a serious issue for AONs. As a matter of fact, both forms of optical crosstalk can arise in OXC nodes. In particular, intrachannel crosstalk, whose effects can be much more severe than interchannel crosstalk, arises from cascaded wavelength demux/mux pairs and in optical switches.

3. PERFORMANCE MONITORING METHOD

In this section we propose a hardware-based method for supervising performance degradation that may occur in OXC nodes. In the following description, a typical OXC node is assumed to consist of n wavelength demultiplexers on the input side, m optical space switches[4], and n wavelength multiplexers on the output side. On each incoming fiber, m wavelength channels are separated using a demultiplexer. The outputs of the demultiplexers are directed to the optical space switches, so that the outputs having the same wavelength are directed to the same switch. Then, they are directed to multiplexers associated with output ports. Finally, the multiplexed outputs are sent to outgoing fibers [9].

The basic idea of this method is to compare *some selected* input signals with output signals passing through an OXC node in a real-time fashion. As shown in Figure 3, this method is based on a MDB entity, which inserts taps into selected input and output signal paths, and splits off portions of signals for testing purpose. The taped optical signals are then photo-detected in the Optical Processing Block (OPB) and the resulting electrical signal is processed into several Child MDBs (CMDBs). Each CMDB is composed of several comparator $comp_i$ blocks. Hence, the numbers of CMDB and $comp_i$ blocks to be utilized can vary from 1 to m and from 1 to n, respectively. In this consideration, we assume that the numbers of CMDBs and $comp_i$ are equal to m and $n-1$, respectively.

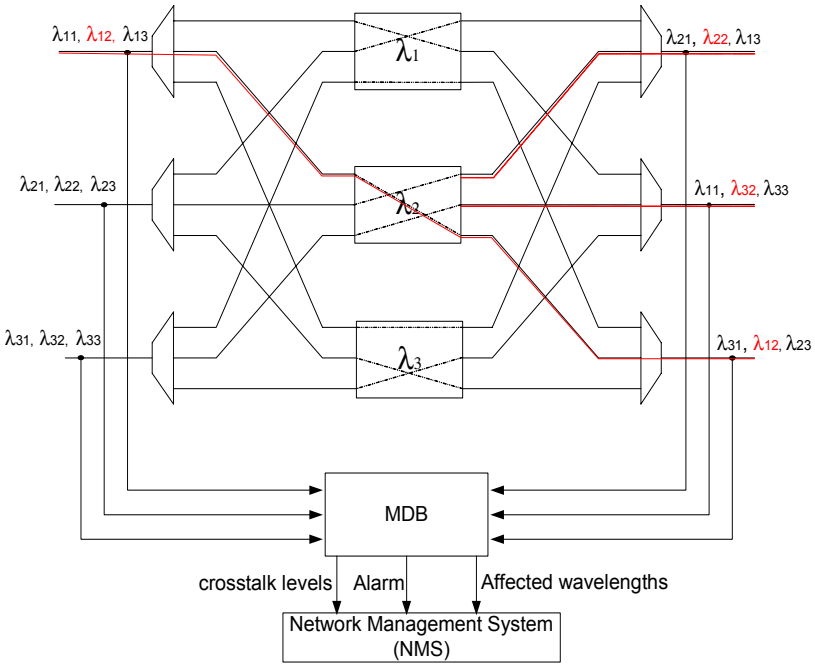

Figure 3. Hardware-based monitoring device block in OXC.

The internal architecture of the MDB (where $m = n = 3$) is depicted in Figure 4. Each *CMDB* λ_i is dedicated for controlling several input and output signals of the same wavelength λ_i. This has the advantage of monitoring the quality of several signals simultaneously in a short time. The $comp_i$ block is the smallest component of the MDB, and is responsible for detecting signal variation between an input and output signals of the same wavelength λ_i. In this example *CMDB* λ_1 activates $comp_1$ to compare λ_{11}^i and $\left(\lambda_{11}^o, \lambda_{21}^o, \lambda_{31}^o\right)$ and $comp_2$ to enable comparison of λ_{21}^i and $\left(\lambda_{11}^o, \lambda_{21}^o, \lambda_{31}^o\right)$. The signal quality of λ_{31}^i will be estimated analytically. Once the presence of performance degradation been detected, the alarm block generates an alarm and notifies the

[4] In this OXC node model, one switch is used for switching channels of the same wavelength.

management system so that it can take correct decisions (for example, which offender lightpaths should be disconnected or rerouted) and perform the appropriate protection and restoration procedures.

Compared with other methods presented in [9] and [10], it is apparent that this method is more advantageous offering the benefit of rapid and accurate detection of performance degradation in AON components in a real-time fashion. Thus, it may ensure relaxing the high cost and complexity of signal quality monitoring in AONs. One of the main benefits of this method lies in the fact that it does not require a prior knowledge of performance-related parameters used in the network such as power levels, amplifier gain statistics, crosstalk, and amplified spontaneous emission components. Another important benefit is that this method can be used independently from the signal nature and current configuration of the AON components employed. Furthermore, the MDB can provide additional performance-related information that can be used in some tasks for fault and performance management of AONs. In particular, this information can be very useful for provisioning requested lightpaths.

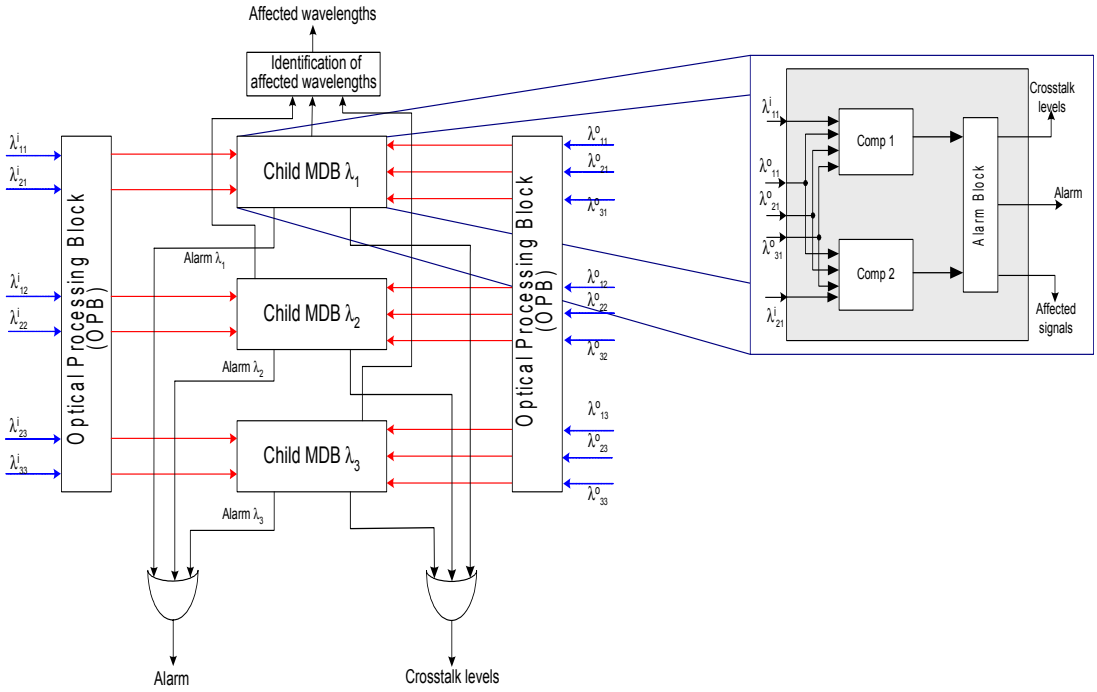

Figure 4. Internal architecture of monitoring device block.

Although this method may offer several benefits, there are several related issues that require further consideration. First, the design concepts for the functional relationship between this method and available management systems should be explored. In particular, the development of efficient schemes for performance degradation resistant network control and management algorithms should be taken into consideration. Second, available and proposed control and management protocols that provision lightpaths within the network may be investigated and where necessary adapted for the peculiarities of this monitoring method. In particular, some extensions are required to adapt routing and signalling protocols, which may be employed for disseminating additional control information among nodes within the network. Finally, there are issues regarding how to provide appropriate reactions after the detection of performance degradation in the network.

4. CONCLUSION

As more intelligence and control mechanisms are added to optical networks, the deployment of an efficient and secure management system, using suitable control and monitoring methods, is highly desirable. Whilst some of the available management mechanisms are applicable to different types of network architectures, many of these are not adequate for AONs. An important implication of using AON components in communication systems is that available methods that are used to manage and monitor the health of the network may no longer be appropriate. Therefore, without additional control mechanisms a break in the core of an optical network might not be detectable.

In this paper we analyzed optical crosstalk forms that may arise in AON components. Then, we proposed a hardware-based monitoring method that can manage with fewer measurements for estimating the health of multiple signals passing through an OXC node in a real-time fashion. As a direct consequence, this method can be used for supervising performance degradation in AON components offering the benefit of relaxing the high cost and complexity of signal quality monitoring for future AON management solutions.

REFERENCES

[1] R. Rejeb, M. S. Leeson, R. J. Green, “Fault and attack management in all-optical networks”, *IEEE Communications Magazine,* vol. 44, no. 11, pp. 79-86, November 2006.

[2] C. Mas Machuca, I. Tomkos, O. K. Tonguz, “Optical networks security: a failure management framework”, *ITCom, Optical Communications & Multimedia Networks*, Orlando, Florida, 7-11 Sep. 2003.

[3] M. Medard, S. R. Chinn, P. Saengudomlert. "Node wrappers for QoS monitoring in transparent optical nodes", *Journal of High Speed Networks*, vol. 10, no. 4, pp. 247-268, 2001.

[4] C. Larsen, P. Andersson, “Signal quality monitoring in optical networks”, *Optical Networks Magazine*, vol. 1, no. 4, pp. 17-23, 2000.

[5] R. Bergman, M. Médard, S. Chan, “Distributed algorithms for attack localization in all-optical networks”, *Network and Distributed System Security Symposium*, San Diego, 1998.

[6] J. K. Patel, S. U. Kim, D. Su, "A framework for managing faults and attacks in WDM optical networks," Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX 2001), vol. II, pp. 137-145, June 2001.

[7] T. Wu, A. K. Somani, "Attack monitoring and localization in all-optical networks", *in Proceedings of OptiCom*, pp. 235-248, July 2002.

[8] C. Mas Machuca, I. Tomkos, O. Tonguz, “Failure location algorithm for transparent optical networks”, *IEEE Journal on Selected Areas in Communications, Vol. 23, No. 8,* pp. 1508-1519, 2005.

[9] R. Rejeb, M. S. Leeson, R. J. Green, “Multiple attack localization and identification in all-optical networks”, *Optical Switching and Networking*, vol. 3, no. 1, pp. 41-49, July 2006.

[10] R. Rejeb, M. S. Leeson, R. J. Green, “Cost optimization method for multiple attack localization and identification in all-optical networks”, *7th IEEE International Conference on Transparent Optical Networks (ICTON2005)*, vol. 1, pp. 101-106, Barcelona, July 2005.