Performance Monitoring Method for All-Optical Networks

A. JEDIDI[1], R. REJEB[2] and, M. ABID[1]
[1]CES Laboratory, National School of Engineering, University of Sfax, Tunisia
[2]Institute for Advanced Engineering and Research, Germany
E-mail: a.jedidi@mobile-manager.eu

***Abstract*—All-Optical Networks provide ultra-fast data rates, but present a new set of challenges for network security. However optical performance monitoring (OPM) and optical network management (ONM) are essential in building a reliable, high-capacity, and service-differentiation enabled all-optical network. One of the serious problems with transparency[1] is the fact that optical crosstalk is additive, and thus the aggregate effect of crosstalk over a whole AON may be more nefarious than a single point of crosstalk. 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. 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. In this paper we present a novel method for attack identification and localization in networks with a minimum of complexity and cost. This method can participate in some tasks for fault management in optical network.**

***Keywords*— All-Optical Networks, Attack Management, Performance Monitoring, Optical Crosstalk, Hardware Conception.**

I. INTRODUCTION

All-Optical Networks (AONs) is a network, where the user-network interface is optical and the data does undergo optical to electrical conversion within the network. AONs are attractive because they promise very high rates, flexible switching and broad application support. However, 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.

An important implication of using AON components in optical communication systems is that available methods that are used to manage and monitor the health of the network may no longer be appropriate. One of the serious problems with transparency is the fact that optical crosstalk is additive, and thus the aggregate effect of crosstalk over a whole AON may be more nefarious than a single point of crosstalk [1]-[4]. Therefore, efficient monitoring and estimation of signal quality along a lightpath[2] are of highest interest because of their importance in diagnosing and assessing the overall health of the network.

Recent proposals to overcome the difficulty of monitoring the continuity and estimating the signal quality of lightpaths in AONs include error detecting codes, sampling, and spectral methods. However, most of these methods are too difficult to implement in every AON component or require access to the electrical domain [3]-[5]. Although there are many reasons why crosstalk attacks must be detected and identified at any point in the network where they may occur, it has been shown that it is not necessary to put monitors at all AON nodes [6], [7]. Furthermore, it has been shown that monitoring information for any established lightpath on the input and output sides of each optical cross-connect (OXC) node is sufficient to localize the source of multiple crosstalk attacks and to identify their natures in AONs [8]. But for all that, performance management is still a major complication for AONs, particularly, because 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. Although new methods for detection and localization of crosstalk have been proposed, no robust standards or techniques exist to date for guaranteeing the QoS in AONs. Therefore, the need for expert diagnostic techniques and more sophisticated management mechanisms that assist managing and assessing the proper function of AON components is highly desirable.

In this paper, we propose a new method to supervisory and monitoring performance degradation in AONs. In section II, we briefly analyze optical crosstalk specifically intra-crosstalk forms that may arise in OXC nodes. In section III, we present the key concepts of Crosstalk Monitoring System (CMS). In section IV, we propose the internal architecture and design of this system. Last, in section V, we discuss the simulation result and present the open directions for future work.

[1]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.

[2]A lightpath is defined as an end-to-end optical connection between a source and a destination node.

II. CROSSTALK IN OXCS NODES

Optical-Cross-connects (OXCs) are essential key network elements enabling reconfigurable optical networks, where lightpaths can be set up and taken down as needed without having to be statically provisioned. A typical structure of an OXC node is shown in Figure1. The OXC node consists of n wavelength demultiplexers on the input side, m optical space switches3, 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. However, while cross-connecting wavelengths from input to output fibers, these AON components introduce crosstalk effects that can impact the transmission performance seriously [9].

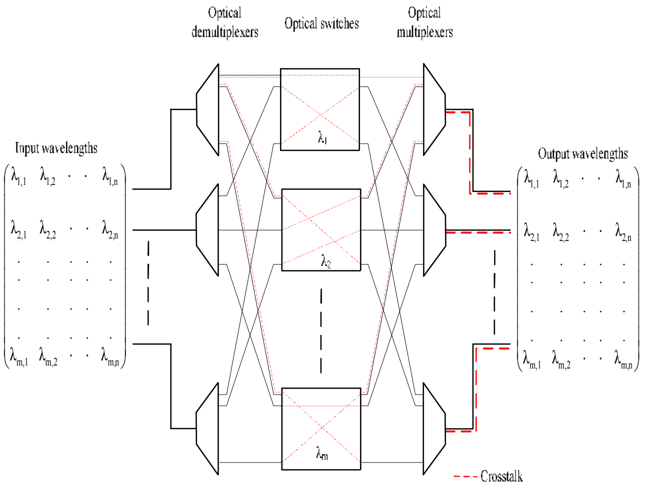

Figure1: A typical structure of an OXC node. The node consists of n wavelength demultiplexers, m optical switches, and n wavelength multiplexers.

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 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. In particular, crosstalk suppression becomes particularly important in networks, where a signal propagates through many nodes and accumulates crosstalk from different element at each node such as multiplexers, demultiplexers, and switches. As the resulting degradations accumulate and grow rapidly become severe with network size, they constitute a serious issue for AONs.

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

Optical crosstalk is present in AON components and degrades the quality of signals, increasing their BER (Bit Error Rate) performance as they travel through the network. As a matter of fact, both forms of optical crosstalk can arise in OXC nodes: interchannel crosstalk and intrachannel crosstalk [9].

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 crosstalk can also occur through more indirect interactions, for example, if one channel affects the gain seen by another channel, as with nonlinearities. 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 second place, 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.

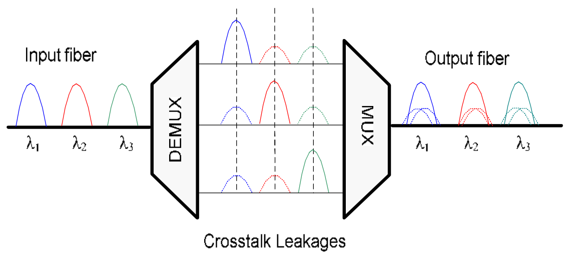

Figure 2: Intrachannel crosstalk arises from cascading a wavelengths demultiplexer / multiplexer.

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. For that, we consider the intrachannel crosstalk in the rest of the paper.

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. As shown in Figure2, the demultiplexer ideally separates the incoming wavelength channels to different output ports. It is because of the non-ideal crosstalk specification of optical filters and demultiplexers that a small portion of the signal at one wavelength, for example, λ_1, leaks into other wavelengths (λ_2, λ_3). When these wavelengths are combined again into a single outgoing fiber by the multiplexer, the small portions of λ_1 that leak into other channels will also leak back into the common outgoing fiber at the output side of the node. This causes intrachannel crosstalk since the signal of wavelength λ_1 and the crosstalk leakages of the same wavelength, even if they contain the same data, are not in phase with each other due to different delays encountered by them.

Another source of intrachannel crosstalk arises in an optical switch that is switching signals of the same wavelength. Figure3 shows schematically the traces of crosstalk components that arise by switching four channels of wavelength λ_1. The solid arrows and dashed traces indicate the affected signal and crosstalk components caused, respectively. Intrachannel crosstalk arises in an optical switch when a portion of a signal leaks into another signal as they pass through the same switch at the same time. This occurs due to the non-ideal isolation of one switch port from the other. Each output port of the switch includes three additional crosstalk components. Thus, each channel that passes through an optical switch is mixed with other crosstalk leakages of the same wavelength.

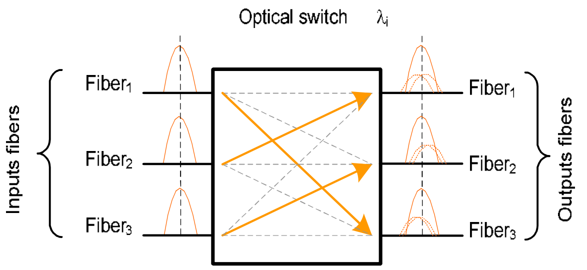

Figure 3: Intrachannel crosstalk arising in an optical switch

III. Crosstalk Identification and Localization System

As introduced in section 2, optical cross-connect nodes are essential key network elements in AONs. Although these elements offer many advantages for communication systems enabling traffic to be switched entirely in the optical domain, they are particularly vulnerable to various forms of optical crosstalk. In this section, we propose a novel approach to localize and identify crosstalk at any point in the network where they may occur. Then, this method guarantees an efficient localization of crosstalk in the entire network with real-times function. As a direct consequence, this method offers the benefit of relaxing the high cost and complexity of signal quality monitoring for future AON management solutions.

To identify the source and assess the value of crosstalk, the CMS use the routing and wavelength information, from Routing and Wavelength Assignment module (RWA), of channels on the input and output side of OXC node of any established lightpath. With each passage of the optical signal of an OXC, a crosstalk is added to it [2]-[11].

To understand quantitatively the principal functionality of CMS, we consider a sample network which is composed of OXC nodes as shown in figure4.

If we consider the routing path (red line in figure4, for example), we note in the worst case that at each passage from a stage to another a value of crosstalk is added in signal. The signal power at the output of the first stage is given by:

$$P_1 = P_0 \cdot (1 + X_{intra1}) \quad (1)$$

Where, P_0 is the input signal power and X_{intra1} is the intracrosstalk of OXC 1. Similarly at the output of 2nd and 3rd stages, the signal power are given as, respectively:

$$P_2 = P_1 \cdot (1 + X_{intra2}) \quad (2)$$

$$P_3 = P_2 \cdot (1 + X_{intra3}) \quad (3)$$

Then, the signal power P_k at the output of k stage is defined as:

$$\begin{aligned} P_k &= P_{k-1} \cdot (1 + X_{intrak}) \\ &= P_0 \cdot (1 + X_{intra1}) \cdot (1 + X_{intra2}) \cdot (1 + X_{intra3}) \cdots (1 + X_{intrak}) \end{aligned} \quad (4)$$

For simplification, we assume that crosstalk is the same in each OXC nodes. Consequently, the signal power P_k is given by: $P_k = P_0 \cdot (1 + X_{intra})^k$ (5)

We define the normalized crosstalk at any stage as:

$$X_n = \frac{P_k - P_0}{P_0} \quad (6)$$

Consequently the value of the crosstalk depends on the number of stage and it is given by:

$$X_n = (1 + X_{intra})^k - 1 \quad (7)$$

Where, k=1, 2, …,n represents the number of series stages and X_{intra} is the OXC crosstalk.

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 Figure4, this method is based on a device, the Crosstalk Monitoring System (CMS), 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 crosstalk identification after that pass in crosstalk localization.

The internal architecture of the CMS is depicted in Figure5. It is composed of two main parts: the Crosstalk Identification Block and Crosstalk Localization Block.

The Crosstalk Identification Block is responsible for the detection and determination the value of crosstalk. For that, we use the input output signal path passing through a destination node in a real-time fashion. We split 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 Crosstalk Value Block (CVB).

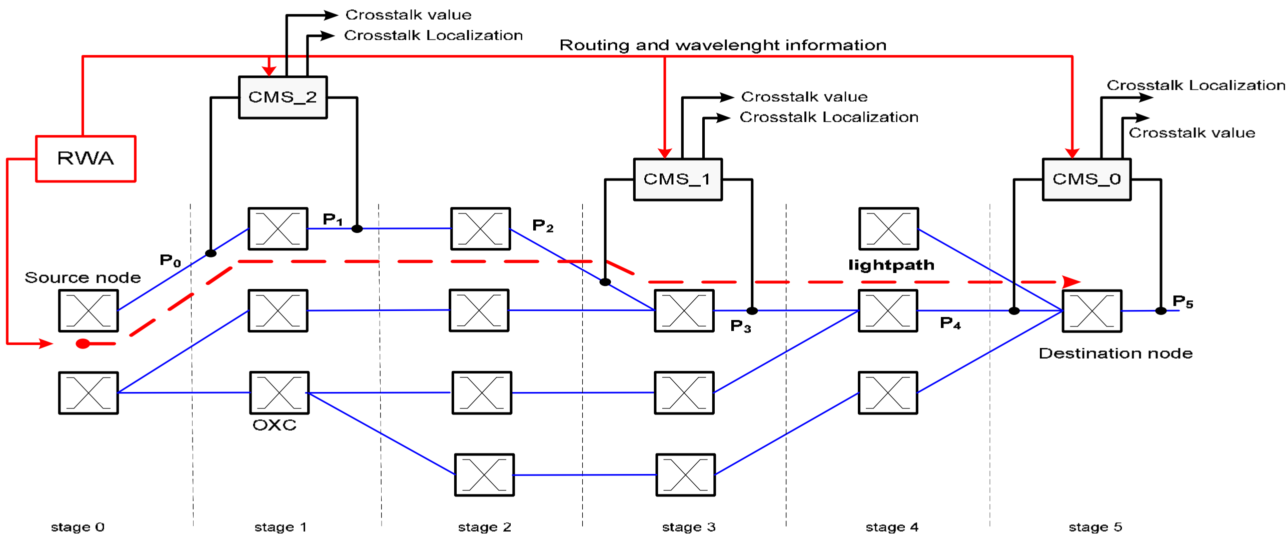

Figure 4: CMS in the network architecture

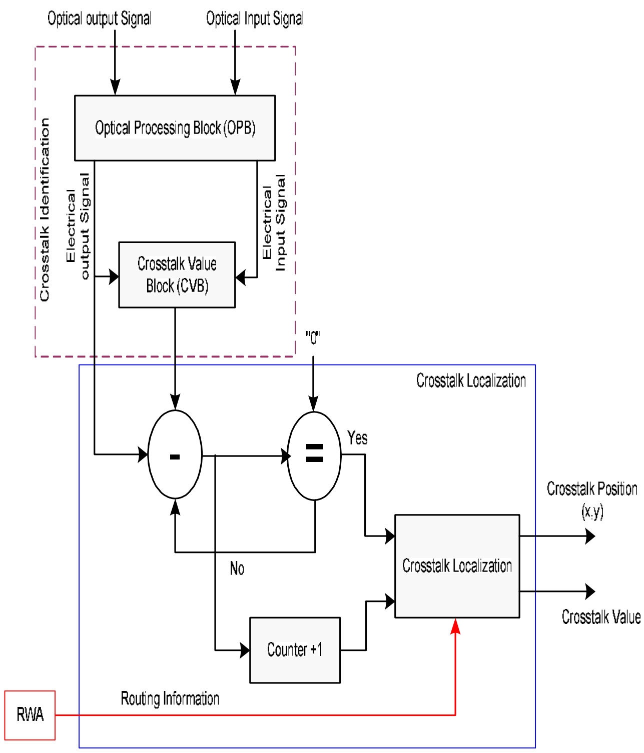

Figure 5: Internal architecture of CMS

CVB calculates the value of crosstalk. Then, this means that the value of crosstalk is used by the Crosstalk Localization part.

The Crosstalk Localization Block is composed by two processes. First, we make successive differences between the value of the crosstalk and the input signal up to zero. This block counts the number of different operation N. Second, we use this quantity and routing information to localize crosstalk in the network. In fact, we follow the ligthpath described by the routing information and account the number of the nodes corresponding to N. Finally we localize the node that caused crosstalk precisely these coordinates (x,y). When x is the number of stage and y is the number of node in the correspondent stage.

IV. Discussion and Results

One of the serious problems with crosstalk is in fact that is additive and his value depends on the number of stages, as shown in equation 7. In this section we discuss the feasibility of CMS in network. Especially, we discuss the number of CMS blocks used in network to have an efficient system to detect and localize crosstalk.

A. Only one CMS:

We propose to use only one CMS module to connect at destination node. However, to identify the source and estimate the value of crosstalk, the CMS use routing information of channels on the input and output side of destination node of any established lightpath. The performance evaluation of CMS is shown in Figure6. The internal design and simulation of this device was performed by a hardware simulation tools (Project Navigator of Xilinx and ModelSim) with a frequency of 300 MHz. The curve shows the execution times as a function of the number of stage of network in the worst case (that is crosstalk arises in each node stage). In this case, the execution times increase with the number of node stage. As result, the real-time operation of our system is attractive and efficient when we have a few stages in network.

The blue curve shows the Lookup Table (LUT) as a function of the number of stage. LUT increase with the number of router stage because we have more and more operation blocks. Then, LUT reflects the occupation area of CILS in chip.

B. Many CMS

To Solve the problem arising in the preceding paragraph we propose to implement several CMS blocks when we have a network which has many stages. This number of CMS varies according to the desired execution time and the size of the stages of the network. For example if we takes a network made up of 6 stages, we can thus implement a CMS module for each two stages of network, then, the execution time will be 9.2 NS and we use Three CMS.

Consequently, the number of CMS is a compromise between the execution time which reflects the real-time operation of our system and the cost of implementation of CMS.

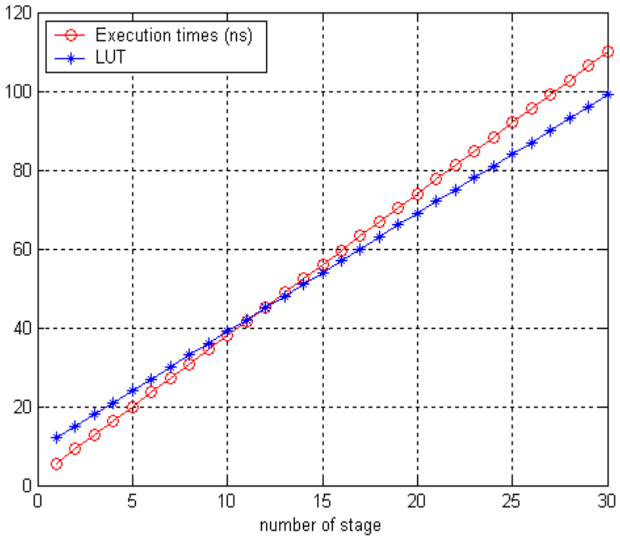

Figure 6: Execution times and LUT vs. number of stages in all optical network

Compared with other proposed methods [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. 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 is flexible at implementation and can be used in real-time fashion.

V. 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 new method that can be used for identifying and localizing crosstalk in 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] L. E. Nelson, S. T. Cundiff, and C. R. Giles, “Optical Monitoring using Data Correlation for WDM Systems”, *IEEE Photonics Technology Letters*, vol. 10, no. 7, pp.1030-1032, July 1998.

[2] A. Jedidi, R. Rejeb, B. Rejeb, M. Abid, M.S. Leeson, and R.J. Green, “Hardware-based monitoring method for all-optical components”, *IEEE International Conference on Transparent Optical Networks - 'Mediterranean Winter' (ICTON-MW07)*, Sousse, December 2007.

[3] M. Medard, S. R. Chinn, and 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, and P. Andersson, “Signal Quality Monitoring in Optical Networks”, Optical Networks Magazine, vol. 1, no. 4, pp. 17-23, 2000.

[5] R. Bergman, M. Médard, and 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, and 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 and 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, and 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, and 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 R. Rejeb, M. S. Leeson, and R. J. Green, “Fault and Attack Management in All-Optical Networks”, IEEE *Communications Magazine*, vol. 44, no. 11, pp. 79-86, November 2006.

[11] A. Jedidi, R. Rejeb, B. Rejeb, M. Abid, M.S. Leeson, and R.J. Green, “Design of Monitoring Device Block for All-Optical Components”, *IEEE International Conference on Transparent Optical Networks - 'Mediterranean Winter'* Sousse, December 2007.