Distinguishing between an Eavesdropper and Component Degradations in Secure Optical Systems and Networks

STAMATIOS V. KARTALOPOULOS, PhD
Williams Professor in Telecommunications Networking
ECE Department, TCOM graduate program
The University of Oklahoma
4502 E. 41st Street, Tulsa, OK 74135
USA

Abstract: - Advances in photonic technology drive the next generation communications network to be "mostly-optical" and able to transport an enormous aggregate client traffic, a good part of which is of high importance and sensitivity and thus classified. As such, the optical signal is of interest to eavesdroppers. However, interception of the optical medium affects the characteristics and the quality of the optical signal. The latter is also the result of simple photonic component degradation and impairment. Similarly, an increase of wavelength density in fiber increases the photon-matter interactions which also contribute to signal distortions. Therefore, in a multi-wavelength communications network, malicious interceptions may emulate parametric degradations of optical and photonic devices. Thus, the best defense is a good understanding of the degradation mechanisms in a secure optical link. In this paper we review degradation and failure mechanisms of optical components, we identify observable parameters and predictors, and we conclusively infer degradations/failures that affect the signal quality, service and network, so that a malicious interception can be distinguished from a degrading mechanism. We also present a cost effective and efficient remedial strategy for channel reassignment and/or switch to protection.

Keywords: - Optical Secure Links, WDM Fault management, Fast protection strategies, WDM Link engineering

1 Introduction

Modern communications networks gradually become "photonic". The next generation network will be "all-optical" and electronics will be assist monitoring, control and management. In addition, the number of wavelengths per fiber is increasing and so is bandwidth scalability [1]. Similarly, with the maturing of wavelength converters, optical channels are switched in the photonic regime eliminating optical to electrical to optical conversions [2]. Thus, the robustness, reliability, availability and security of the next generation optical network will greatly depend on the proper and expected functionality of optical and photonic devices such as filters, amplifiers, cross-connects, wavelength converters, optical add-drop multiplexers, and so on, and also of the ability to monitor and detect degradations of the optical signal.

The paramount objective in optical communications is to transmit an optical signal that reaches the receiver at the expected strength and acceptable noise and distortion content. However, as the network becomes more "optical", the signal is subject to degradations due to material non-linearity and optical component degradations and failures. Similarly, as more wavelengths are crowded in a fiber, more distortion is contributed that equally affects the optical signal integrity. However, an interception of the fiber medium by a malicious eavesdropper is also manifested by degradation of the optical signal properties and quality. Thus, in a multi-wavelength communications network, malicious interceptions may emulate parametric degradations of optical and photonic devices and the eavesdropper may go un-noticed. The best defense in this case is a thorough understanding of the parametric degradation mechanisms in a multi-wavelength secure optical communications link. The latter will lead to an intelligent strategy that effectively monitors, detects, localizes, and isolates faults, to distinguish between a malicious intercept and natural degradations and to provide uninterrupted service via fast and cost-efficient protection mechanisms [3, 4].

In this paper we overview the degradation/failure mechanisms of optical components; we identify observable parameters and predictors; we conclusively infer a degradation/failure that affects the quality of signal, service and network, and we develop cost effective and efficient remedial strategies.

2 Optical signal integrity

2.1 Sources of Degradations and Faults

When light interacts with matter, the electric and magnetic fields of light interact with fields within the molecular and atomic structure of matter. As a result, it is refracted, reflected, diffracted, polarized, absorbed, stimulated, scattered, delayed, intermodulated, and so on. Moreover, light interacts with light directly or indirectly via the non-linearity properties of matter. Some interactions play a primary role to the transmission characteristics of light and some others a secondary and thus they may be ignored. However, the spectral separation of optical channel, the spectral content of signal, the strength of signal, the polarization state, the data rate, the modulation strategy and the transmission medium characteristics are key variables that determine the degree of interaction with matter. Thus, as the number of wavelengths in the fiber medium increases, and as the bit-rate of the optical signal increases or its bit-period reaches the realm of fempto-second, even secondary and tertiary interactions play a crucial role regarding the integrity of the optical signal.

The properties of optical materials that comprise a device change with mechanical stress, pressure and temperature variations and occasionally with the presence of strong electromagnetic fields. In addition, they change with aging, molecular and ionic migration, and contamination. And these changes affect the interaction of light with matter and the propagation of the optical signal through it, which often escalate to failures causing disruption of service.

In general, degradations are differentiated from failures as:

- Degradation is a discrepancy between the actual and the desired characteristic of an item. For example, when the noise content of the optical signal increases, the bit error rate increases thus deviating from its desired characteristic (degrading signal integrity).
- Failure is a persistent interruption in the ability of a component to perform a required function as expected. For example, a laser source, a photodetector, a broken fiber, or any optical component that ceases to function as expected (impacting the intelligence of the signal in the long term). In this case, intermittent failure may also be defined as a failure that may persist over long and random periods.

2.2 Optical systems

Currently, optical communications systems and networks are classified as opto-electronic or “opaque”. That is, the transmission medium is optical but signal processing and switching within a node is electronic. In contrast, the next generation optical communications nodes will have more “optical” functionality including switching. An early experimental all-optical WDM network in the US was the Metropolitan Optical Network (MONET) [5].

Opaque systems have many advantages. They perform signal monitoring and switching using a well known technology in complexity, development and economics. However, the conversion of the optical signal to electrical and back to optical is complex and costly. Moreover, opaque systems suffer from bandwidth scalability, and traffic versatility. That is, the switching fabric is implemented for a specific category of traffic type and data rate (e.g. OC-N, or IP) and its bandwidth limits are fixed and difficult to scale.

All-optical systems have also many advantages. They avoid OEO conversions, switching is on the wavelength level, and thus the fabric is insensitive to traffic type and data rate making bandwidth scalability and elasticity an easier task.

2.3 The WDM optical signal

In traditional optical networks that operated at a single channel (1310 and/or 1550 nm), link failures were manifested by loss of signal (LOS). Such failures were relatively easily localized. However, in WDM networks, one needs to distinguish LOS between optical channel LOS (OC-LOS) and optical link LOS (OL-LOS). For example, a fiber cut will cause OL-LOS as it affects all optical channels in the fiber. A failing mirror of a MEMS device or a degrading/failing component will affect a single OCh (e.g., laser or detector) causing OC-LOS of one (and perhaps more) OChs. That is, OC-LOS may be caused by any of several possible faults of passive or active optical devices and thus fault localization in this case is not an easy task. Similar arguments hold if the fiber is tapped. One or more of the optical channels in the fiber are affected. In addition, systems that support wavelength dynamic assignment and re-assignment, wavelength converters may be degraded/failed; clearly, such failure further complicates the lightpath integrity across the network. Thus, if fault detection mechanisms are strategically included in key devices, then faults are detected early and localized, so that remedial actions are triggered to uninterruptedly provide service. Figure 1 illustrates a general WDM link of a point to point with add-drop node. This link contains lasers and modulators, filters, multiplexer, preamplifier, the transmission medium, dispersion compensator, OADM (which consists of several components including a switch), post-amplifier, optical equalizers, demultiplexer and receivers.

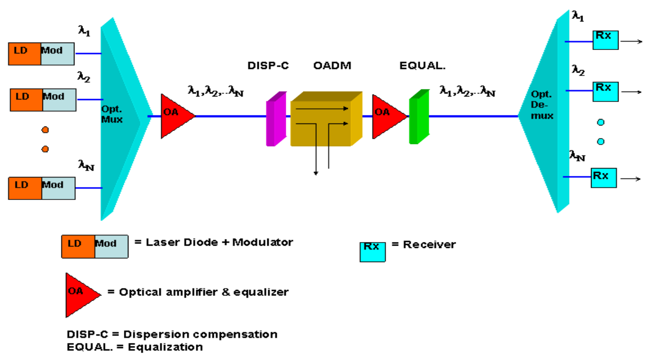

Figure 1: A general WDM link of a point to point with add-drop node.

2.4 Contributors to optical signal degradation

To support the arguments made in section 2.3, we examine the parameters that affect the integrity of the optical signal. Based on this, a root cause analysis leads to intelligently distinguish between interceptions and degradations/faults and to the development of cost effective and efficient fault/degradation remedial strategies. For example, the bit-error rate (BER) is an observable quantity at the receiver, which is widely used as a performance metric. However, BER increase may have been caused by the contribution of one or more degrading parameters on the optical path. Thus, how can one deduct which degrading parameter causes signal degradation? For instance, some of the most important and possible degrading parameters that can increase BER are:

- Optical signal power level
- Optical Channel (OCh) center frequency
- Pulse shape skew and kurtosis
- Optical Channel width (related to spectral broadening)
- Optical Channel separation
- Dispersion (chromatic, polarization), residual dispersion and slope
- State of Polarization (SoP) stability
- Modulation depth (peak to valley)
- Modulation stability (peak and valley)
- Material non-linearity and birefrigence, as a function of temperature, pressure and fields (for both, components and transmission medium).

The degree that each of the above parameters influences the quality and/or integrity of the optical signal is summarized in Table 1.

Thus, although BER is a performance metric for signal integrity, BER itself does not identify or localize the degradation. As an example, BER increase is a manifestation of optical power degradation, noise and jitter. Hence, is the BER increase because of a degrading optical amplifier? Or, is it because of increased insertion loss? Or, is it induced by a non-linear phenomenon? Clearly, the question is complex, and it can be answered if more photonic parameters are detected and cross-correlated.

3 A general node example

3.1 A cross-connecting node

Figure 2 captures a general multifiber and multiwavelength WDM cross-connecting node with add-drop capability, which for simplicity is shown on protected physical rings. The node also includes a supervisory channel. This may be out-of-signal and in the same fiber, in-signal, or out-of-signal and in separate fiber. Optical channels from each fiber are demultiplexed, and each lightbeam (optical channel) is monitored for power, wavelength, pulse-shape, BER, OSNR, and Q-factor. Monitoring these performance parameters and signal quality has already been elaborated in [6, 7]. Correlation of performance data leads to an early warning of either a malicious attack or a natural degradation/fault of the link. Depending on the outcome, then an alarm is issued and a remedial action is triggered to either restore the link or reroute traffic to the protection link.

Within the system, an optical cross-connect (such as MEMS) redirects lightbeams that have a signature tag attached to them, each lightbeam is monitored for power, for wavelength (wavelength converters may be used to convert the wavelength of the lightbeam) and for its tag to detect misrouting.

Detectors (small rectangles in Figure 2) report performance data to the “degradation/fault management” (FM) function of the node where they are analyzed, correlated and stored. The objective is to readily detect a degradation/fault within the node, correlate it, localize it and based on an intelligent algorithm, to initiate remedial actions. However, until the remedial action is completed, as part of a notification procedure, the downstream power may be turned off for the next node to detect, and an alarm indication signal may be sent upstream to alert the upstream node of the fault received. Similarly, when an OL-LOS is detected, then the downstream power of all channels is turned off and alarm messages are sent upstream.

3.3 Potential impact on Fault Management

3.2.1 Power loss indication

The power level of an OCh is monitored at the entry point of the OXC system as well as at the exit point, Figure 2. If the optical cross-connect operates as expected, then the power level of an OCh at both entry and exit points is the same, minus the insertion loss. If this is not true, then excessive differential power indicates a mis-switch, which if persistent, it should be viewed as an OCh failure; differential threshold levels are set to distinguish between acceptable, degraded, and faulty operation.

Similarly, power loss of a lightbeam indicates that the data flow of a specific OCh has been interrupted. If the power monitor at the input of the node detects power loss, then, power for that channel is lost; any device (passive or active) on the link and up to the detector (included) may be potentially at fault. In this case, a performance status notifies the Fault Management function of the node, and “move to protection” process is initiated.

If the power monitor at the output of the cross-connect detects power loss (but not at the input), then most likely there is a failure any device on the path between input-output. In this case, the remedial action is to move the failed path to a protection path within the cross-connect. This implies that protecting paths have been reserved within the node. If protection however is not supported, then:

- Loss of OCh is declared and the output power is shut off for this channel (downstream).
- An alarm indication signal for this OCh is generated upstream.
- The upstream node “moves” the OCh, for which the corresponding cross-connecting path failed, to another OCh. It also sends supervisory data to the downstream node, which copies onto the next node, and so on.

3.2.2 Multiple power loss indication

When multiple power monitors at the inputs of the cross-connect detect failures, it is possible that the data flow of multiple OChs have been interrupted. This type of failure cannot be attributed to an ingress fiber cut because in such case all OCh monitors would detect a failure. Thus, the node monitors report failures to the “fault management” which turns off the power of corresponding channels downstream and generates alarm indications upstream.

3.2.3 OCh bit error rate

Typically, the BER of an optical channel is monitored at the receiving end of an optical path. However, research has demonstrated that there are methods to monitor BER, the Q-factor and signal to noise ratio (SNR) of an optical channel at any entry point of a node, in-line and without service interruption. As already discussed, increased BER on an OCh may be caused by one of several degradation mechanisms. Thus, assuming that BER is monitored at the input of a node, then:

- If the BER at the node input (see Figure 2) is persistently below an acceptable threshold level, an OCh re-routing action should be initiated to restore the degraded OCh.
- If the monitored BER at the node output is persistently above an acceptable threshold level (but not at the input), then a device on the input-output path within the node is at fault and a switch to intra-node protection path should be initiated.

4 Conclusions

Performance monitoring and fault management are critical functions on the node and the network level. In addition, intelligent detection strategies and advanced optical technology are necessary for the all-optical intelligent network to distinguish between a malicious attacker and degrading/failing mechanisms. In this paper we have focused on a network with WDM cross-connecting nodes that are:

- Compact.
- More "optical" and less "electronic".
- Optical components are monitored for performance and for functionality.
- A comprehensive strategy for degradation/fault monitoring, detection, localization and remedial action has been developed.
- Optical tag monitoring and replacement enhances the downstream and upstream internode communication assuring the lightpath integrity.
- Dynamic wavelength re-assignment is accomplished with fast acquisition time devices.
- Traffic is protected and flow control is maintained by autonomous fast remedial actions.

We have also illustrated the importance of degradation/fault monitoring, detection, and localization and also the importance of distinguishing between eavesdropper and natural causes. We have illustrated that fault detection that is solely based on power and BER is incomplete. We have also illustrated that, when BER, SNR, Q-factor, pulse shape, and power monitoring is employed at each input of a node, then correlation will reveal the type of degradation or if a fiber has been attacked. In the absence of fiber attack, when BER remains persistently below an acceptable threshold level, then a dynamic wavelength re-assignment process may be initiated via an upstream/downstream supervisory channel.

References

[1] S.V. Kartalopoulos, "Elastic Bandwidth", *IEEE Circuits and Devices Mag*., vol. 18. no. 1, pp. 8-13, Jan. 2002.

[2] S.V. Kartalopoulos, "*DWDM: Networks, Devices, and Technology*", Wiley & Sons/IEEE Press, 2003.

[3] N. Shibata, K. Nosu, K. Iwashita, and Y. Azuma, "Transmission Limitations Due to Fiber Nonlinearities in Optical FDM Systems", *IEEE JSAC,* vol. SAC-8, no. 6. August 1990, pp. 1068-1077.

[4] S.V. Kartalopoulos, "*Fault Detectability in DWDM: Towards Higher Signal Quality & System Reliability*", IEEE Press, January 2001

[5] Y. Chen, M.T. Fatehi, H.J. LaRoche, J.Z. Larsen, and B.L. Nelson, "Metro Optical Networking", *Bell Labs Techn. J.*, vol. 4, no. 1, 1999, pp. 163-186.

[6] S.V. Kartalopoulos, *Optical Bit Error Rate*, Wiley & Sons/IEEE Press, 2004.

[7] S.V. Kartalopoulos, "Channel Error Estimation in Next Generation Optical Networks", WSEAS Transactions on Circuits and Systems, vol. 3, issue 10, December 2004, pp. 2281-2284.

Table 1: Parametric influences on the optical signal quality

Degraded parameter	**Effect on signal**
1. Optical signal power level:	Reduces eye opening; increases BER
2. OCh center frequency deviation:	Reduces eye opening; increases BER, increases cross-talk
3. OCh width (broadening):	Reduces eye opening; increases BER, increases cross-talk
4. OChs (spacing) separation (combined effects of items 2 and 3)	Reduces eye opening; increases BER
5. Dispersion (chromatic, polarization):	Eye-closure due to chromatic dispersion, eye closure due to PMD induced DGD, increases ISI and BER
6. SoP instability:	Increases BER, increases jitter/wander
7. Modulation depth (peak to valley):	Reduces eye opening, increases BER
8. Modulation stability (peak and valley):	Reduces eye opening, increases BER
9. Signal echo and singing	Adds to laser chirp, to signal jitter and noise
10. Material (fiber) non-linearities:	Eye-closure due to DGD caused by SPM, induces XPM, SPM and FWM on multiplexed opt signals.

where DGD is Dispersion Group Delay, FWM is Four-wave mixing, SPM is self phase modulation, XPM is Cross-polarization modulation, and ISI is Inter-symbol interference

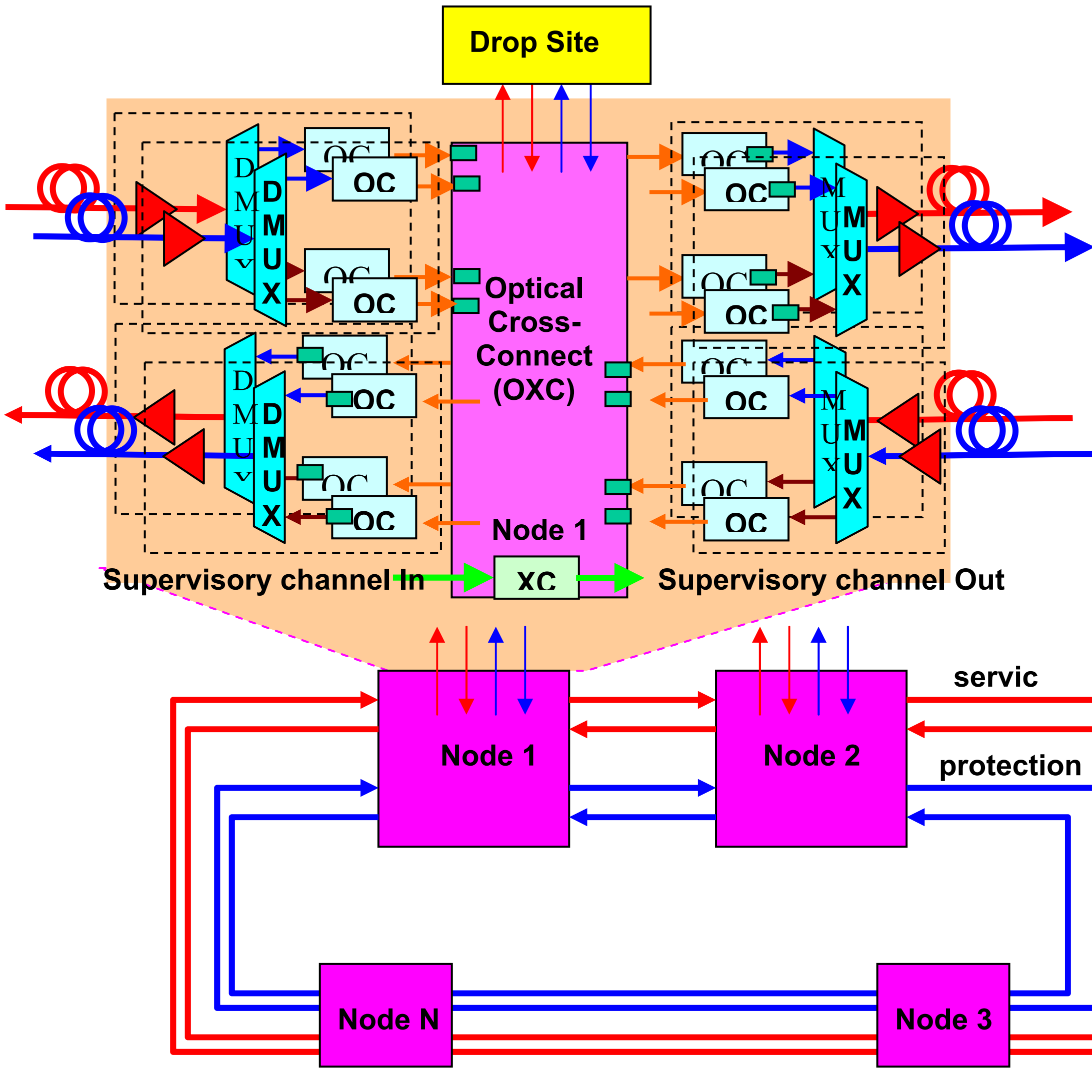

Figure 2: A general WDM node on protected rings (a similar node is used in mesh network topologies)