OPTIMIZATION OF PERFORMANCE MONITORING AND ATTACK DETECTION IN ALL OPTICAL NETWORKS

Răzvan RUGHINIŞ[1], George MILESCU[2], Mircea BARDAC[3], Nicolae ŢĂPUŞ[4]

Articolul propune optimizări în abordarea provocărilor curente în monitorizarea performanţelor şi detectarea atacurilor în reţelele integral optice (AON), centrându-se pe riscurile de securitate care derivă din infrastructura optică. Pornind de la discutarea metodelor de testare, a metricilor şi a tehnologiilor disponibile pentru prevenirea atacurilor în AON, articolul evidenţiază principalele vulnerabilităţi şi soluţii posibile in metodele de monitorizare si detectare a atacurilor, propunând o abordare bazată pe eşantionarea semnalelor de probă. Eşantionarea aleatoare introduce economii semnificative, estimate statistic, în efortul de monitorizare.

The article proposes optimizations to address the challenges of performance monitoring and attack detection in All Optical Networks, with a focus on specific security risks related to the optical infrastructure. An analysis of testing methods, metrics and available equipments in relation to attack strategies for AONs highlights the main vulnerabilities and discusses hybrid solutions, proposing a sampling approach to pilot tone monitoring. Random sampling introduces significant savings of energy in monitoring efforts, as it results from statistical estimates.

Keywords: All Optical Networks, Performance monitoring, Attack detection

1. Introduction

The use of optical fiber has become widespread in computer networks, allowing for significantly larger bandwidths, increased network flexibility and security. At the same time, optical networks have specific administration requirements in relation to electronic networks. This specificity is even larger in All Optical Networks (AON). The concept of AON is discussed in the Introduction, and its specific security and testing requirements are discussed in the next sections.

[1] Assoc. Prof., Department of Automatics and Computer Science, University POLITEHNICA of Bucharest, Romania, e-mail: razvan.rughinis@cs.pub.ro

[2] Assistant., Department of Automatics and Computer Science, University POLITEHNICA of Bucharest, Romania, george.milescu@cs.pub.ro

[3] Assistant., Department of Automatics and Computer Science, University POLITEHNICA of Bucharest, Romania, mircea.bardac@cs.pub.ro

[4] Prof., Department of Automatics and Computer Science, University POLITEHNICA of Bucharest, Romania, nicolae.tapus@cs.pub.ro

Optical networks have rapidly evolved from the use of optical fiber as pipes for efficient transportation of information, by increasingly adding new functionalities to the optical layer. The most important benefits of optical fiber in comparison to copper wires are its ability to carry increased bandwidth and its immunity to electrical interferences. Its main disadvantages are the higher costs and difficulty in installation. Optical fiber is mainly used in WANs, spanning large distances (hundreds of meters or more), and in situations where the bit rate must exceed several Mb/s. It may also be used in industrial contexts where copper is not suitable because of environmental conditions.

The gradual increase in traffic and bandwidth needs has led to new technologies to improve the capacity of fiber communication systems. Bit rates have steadily increased from 155 Mb/s to 622 Mb/s, then to 2,488 Mb/s, and finally to 10 Gb/s. The second improvement in capacity is due to multiplexing – combining multiple data streams over a shared medium. Time division multiplexing (TDM) refers to interleaving streams in time, each one transmitting alternatively in its allocated time slot. Statistical time division multiplexing (STDM) uses variable time slots, according to traffic demands. Still, many backbone networks required rates higher than 10Gb/s, thus confronting the physical limits of lasers, which could not be turned on and off more rapidly [1]. Wavelength division multiplexing (WDM) has overcome this limit by using different wavelengths for the interweaving streams, all of them being transmitted simultaneously. The WDM system is efficient for large distance transmission, using a multiplexor (Mux) for the transmitter and a demultiplexor (Demux) at the receiver. Each fiber uses a filter at its destination, filtering all wavelengths but one. Resulting signals may be routed towards the destination or recombined for subsequent transmissions. The WDM technology has made fast improvements since its launch in the 70's: while the first WDM system could combine 2 channels, current systems can combine up to 160 signals, thus extending a 10Gbp system up to a theoretical value of 1Tbps by using just one fiber optic pair. Such systems are commercially available, and systems with more than 200 channels are currently tested in laboratories. This technology using multiple channels relies on very close wavelengths (0.1nm) - thus its designation as dense wavelength-division multiplexing, or DWDM.

DWDM provides raw capacity which needs to be managed. For example, a specific routing problem related to wavelength division multiplexing refers to the Routing and Wavelength Assignment (RWA) Problem: given the physical topology and the required connections, the RWA problem is to select a suitable lightpath and wavelength among the many possible choices for each connection so that no two paths sharing a link are assigned the same wavelength.

Intelligent optical networks (ION) make use of optical switching of signals, besides optical transmissions, in order to cut costs. The reconfigurable optical add-drop multiplexer (ROADM) allows for remote switching of traffic from a WDM system at wavelength level, thus adding and dropping data channels on a transport fiber without converting all channels to electronic signals and again to optical signals. The ROADM makes possible flexibility in planning bandwidth assignment, allows for remote reconfiguration and for automatic power balancing. Since 2005 it has been increasingly used in metro optical systems, while before it was restricted to long-haul DWDM systems.

IONs also use optical switches (or optical cross-connects - OXC), which may be of two types: the optical-electrical-optical (O-E-O) switches, and the optical-optical-optical (O-O-O) ones. They offer distinct advantages and they can be combined to optimize network management. The All Optical Network (AON) relies exclusively on optical transmission and O-O-O devices. Their main benefits derive from the larger bandwidth available in the optical domain: avoiding optical-electronic-optical conversions allows, in theory, for one thousand times greater data rates than possible with electro-optic networks. Currently such networks are mainly confined to the research area [2]. The leading technology in O-O-O switches is the Micro-Electro-Mechanical Systems (MEMS), using control mechanisms to tilt mirrors in multiple directions. A summary evaluation of MEMS in relation with competing technologies is presented in Table 1 [3].

Table 1.

Performance of optical switch technologies relying on all-optical fabrics [IEC]

	Free-space		Guided-wave	
	MEMS	Liquid crystal	Thermo-optic bubble	Thermo-optic / Electro-optic waveguide
Scalability	Good	Poor	Poor	Poor
Loss	Good	Unsure	Poor	Unsure
Switching time	Good	Unsure	Unsure	Good
Cross-talk	Good	Unsure	Unsure	Unsure
Polarization effects	Good	Unsure / Good	Unsure / Good	Poor
Wavelength independence	Good	Good	Good	Poor
Bit-rate independence	Good	Good	Good	Good
Power consumption	Good	Good	Poor	Poor

The evolution of optical networks from transportation conduits to complex reconfigurable systems has led to the emergence of technologies for distributed monitoring reporting to an integrated optical control plane, monitoring and controlling network elements, producing and aggregating information, and managing optical signals. The optical control plane is of critical importance for current optical network platforms [4]. In subsequent sections the needs and challenges of the control plane are discussed, in relation with testing devices and techniques.

2. Specific risks in optical networks

There are multiple failures that can affect optical networks: fiber cuts, transmitter or receiver breakdowns, optical amplifier breakdowns, or failures of switch nodes [5]. In addition to this, optical networks may be subject to malicious intrusions, and attack-detection schemes are necessary to prevent massive data loss. Given the large volume of data transiting optical networks and their frequent use in critical mission traffic, even brief and infrequent failures of network elements may lead to unacceptable losses in an AON.

Another specific risk derives from the optical medium transparency: all optical devices in an AON ignore the user payload [6]. Therefore, an intruding signal can be inserted in a network and, by using an appropriate wavelength; it can then reach diverse and remote parts of the network. This diffusion of malicious signals can be blocked by electronic conversion which subjects traffic to a more rigorous inspection.

Moreover, physical access to optical fiber and devices allows for relatively straightforward attack means. For example, bare fiber may be tapped by bending it slightly and allowing some light to leak out. This process is easily achieved with commercially available clip-on devices, allowing the easy interception of unencrypted data. The crosstalk level in switches may allow a malicious outsider to disrupt service by a high-power jamming signal.

Therefore, failures and security risks in AONs must be addressed with technologies adapted to these novel challenges.

3. Optimization of performance monitoring in DWDM networks

Interventions to prevent and correct failures and security problems may take place at the physical level, by optimizing optical infrastructure and devices, or at network level - by introducing routing protocols that take into consideration performance metrics. For example, in [7] a routing and wavelength assignment algorithm is proposed that incorporates information on fiber impairments in routing decisions. Metrics such as optical signal-to-noise ratio (OSNR) and polarization mode dispersion (PMD) effect are estimated in the physical layer and then used for lightpath computation.

Still, for physical and network level interventions as well, a central issue is information processing: testing the quality of network functioning, distributing the resulting information and processing it under time constraints. The main structural advantage of optical networks, namely their significantly higher bandwidths, involves the necessity of increased surveillance, since a rare malfunction would disrupt traffic on a large scale, and a security breach would affect a potentially larger volume of mission-critical data.

One of the most important sources of failure in optical networks is signal attenuation (optical power loss) as it travels through the media. Portable optical loss test sets are available to measure this parameter in the field. Optical amplifiers using erbium-doped fiber (EDFAs) are used to extend the lengths of the links between electronic regenerators, or even to eliminate the need for electronic regeneration in the case of AONs.

The increasing reliance on DWDM systems has multiplied the metrics that have to be measured on the field in order to monitor network functioning and to detect anomalies. The most important change introduced by the DWDM is the requirement to make distinct characterizations of components and links as a function of wavelength.

Moreover, intelligent optical networks evolve towards all optical networks, requiring physical layer monitoring which is bit-rate-, format- and protocol-independent. Dynamic reconfigurable networks require monitoring systems that do not depend on prior knowledge of signal source and trajectory [8].

4. Proposed strategies for attack detection in optical networks

There are two main types of security issues in optical networks: tapping, which provides unauthorized access to data, and service disruption, which degrades the Quality of Service QoS or prevents transmission.

The specific elements in Figure 1 are subject to particular attack vulnerabilities [6]. Optical fiber (2) may be interrupted or tapped; while interruption of service is easily detectable, tapping requires more sophisticated testing. TAPs themselves allow attackers to tamper with signal properties (such as power or polarization). Amplifiers may be used for “gain competition” attacks, by which alien high-power signals jammed into the network deprive legitimate weaker signals of power, thus leading to service degradation or denial. Switches and fiber are vulnerable to crosstalk-based attacks. For example, a malicious user may request a legitimate data channel and leave it empty. Consequently, its wavelength will only carry echoes from crosstalk with neighboring channels, which can be amplified and delivered to the attacker [11]. There are multiple combinations of jamming, tapping and crosstalk attacks, including malicious simulations of attacks, that can impair the network functioning.

An efficient security policy incorporates prevention, detection and reaction measures. Testing is key for detecting attacks.

Overt attacks, aiming at denial of service by inducing element failure, are easier to detect by physical layer tests, since they involve clear signal degradation or interruption. Covert attacks, aiming for signal tapping, are difficult to recognize because bit error rates (BER) on fiber are very low (10-11 or lower) and even small interferences may cause significant increases in BER. A solution consists in redundant transmission of one stream across different paths and comparing the output signals, but this leads to high network resource utilization [12].

Overall, there are two main types of attack detection: statistical analysis of data and measuring the results of a diagnosis probe. Several types of methods relying on optical means have been deployed [13], [14], [2]:

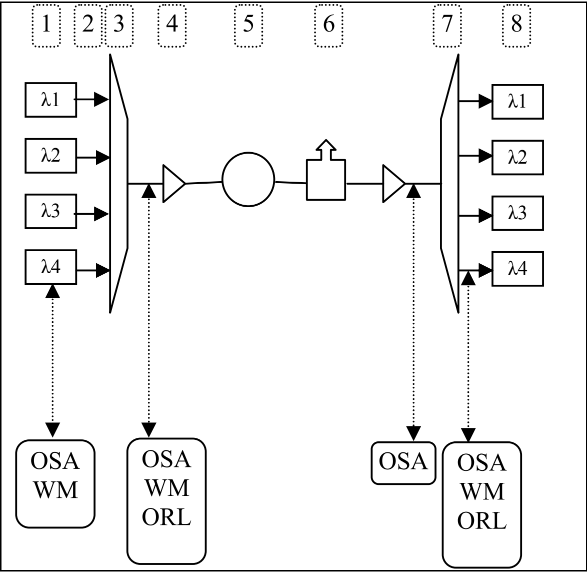
- Statistical detection of power anomalies;
- Statistical spectral analysis: OSAs may be used to detect a change in spectrum shape, even if that change in shape does not entail a change in power over the whole channel;
- Pilot tone methods – sending a probe signal for diagnosis purposes; probing signals are sent to investigate the functioning of the network, and their results are interpreted to detect possible failures. There are two strategies for probing: adaptive probing or non-adaptive probing. Adaptive probing relies on a first set of signals to make a diagnosis and a second set to further the investigation, depending on previous results. This method uses relatively few probes but risks having large delays in diagnosis, given its sequential nature. Non-adaptive fault diagnosis schemes use independent probes to identify failures [5];
- Optical Time Domain Reflectometry Methods, which analyze the pilot tone echos.

For example, tapping attacks may be detected by continuous monitoring of average power levels, identifying differences in levels before and after the tap. Still, if tapping is complementing by jamming, detection becomes difficult by means of power anomalies. Gain competitions attack detection require complicated local channel equality tests, but they may be prevented by balancing gains (either optically or electronically) before sending signals to the EDFA. Crosstalk attacks are difficult to measure without electronic conversion and BER measurements [6], but, insofar as they aim for eavesdropping, they may be prevented by traffic encryption.

5. Proposed AON metrics and testing algorithms

The main parameters that need to be measured in order to monitor the state of an optical network are [8] - [10]:

- The optical signal-to-noise ratio (OSNR) for each channel, taking into account the noise floor between channels in order to measure adequately the noise level; this is the main performance indicator in DWDM systems;
- Crosstalk – the level of noise and contributions from other channels in the passband of the tested channel;
- Channel power, in order to check whether the distribution of power over the bandwidth of the optical amplifiers (EDFAs) is balanced;
- Channel center wavelength and spacing, in order to detect drifts in Distributed Feed-Back (DFB) laser sources;
- The total optical power, which is useful in order to estimate non-linear adverse effects;



1: Transmitter
2: Optical fiber: physical tapping, crosstalk attacks
3: Multiplexor (Mux)
4: Amplifier (EDFA): gain competition attacks
5: Optical cross-connect (OXC): crosstalk attacks
5: TAP: signal tampering attacks
6: Demultiplexor (Demux)
8: Receiver

OSA: Optical Spectrum Analyzer
WM: Wavelength meter
ORL: Optical return loss monitoring

Fig. 1. Main attack risks and elements of test equipment for DWDM systems

- Chromatic dispersion, the result of different spectral components traveling at different speed in the optical fiber, leading to detection errors in the receiver;

- Polarization-mode dispersion (PMD), the result of an asymmetry of the fiber core, by which light polarized in one axis travels slightly faster than light polarized in the orthogonal axis, resulting in a limitation of the transmission distance;

- The quality factor (Q-factor);

- Time jitter, which is a significant performance factor for high-bit-rate optical systems if the jitter occurs over a non-negligible fraction of the bit period;

- The bit error rate BER, which indicates the transmission performance of the network; it requires electronic conversion of the optical signal.

In order to measure these parameters, the following pieces of equipment are increasingly necessary in field operations:

- The optical spectrum analyzer (OSA), which has been widely used in laboratories to this purpose, but it is not transferrable to the field because of its size, weight, fragility and sophistication;

- The wavelength meter, which must also transit from laboratory versions to portable versions;

- Optical Loss Test Sets (OLTS) calibrated at specific wavelengths in order to measure the power of each channel at the Demux output and for other channels, such as the optical supervisory channels (OSC);

- Optical Time Domain Reflectometer (OTDR) capable of testing performance at the long wavelength of 1625 nm, allowing for preventive estimates of critical points (since optical losses due to fiber bending are higher at 1625 nm that in the normal DWDM wavelengths);
- Back reflection meters in order to measure the optical return loss (ORL) for each channel wavelength.

Data collection in optical networks is also facilitated by the use of Test Access Points (TAPs), which are passive instruments that capture and then divide a data stream on an optical link, usually between a switch and device, generating two identical streams. One of them continues its way through the network, while the second is directed through an analyzer, thus allowing to connect the analyzer at any time without breaking the signal.

6. A sampling based approach of performance testing in AONs

Several reviews of security and quality of service assurance in AONs conclude that their technological features, in particular their transparency, induce higher risks and demand specific monitoring strategies which are highly measurement and computationally intensive [15], [16], [17]. A solution to such challenges consists in deploying a sampling approach, by introducing a random selection in testing performance levels. This strategy is particularly suitable for pilot tone methods, allowing for better coverage of network overall functioning by means of probe signals for diagnosis purposes.

The volume of a simple random sample for a given population of signals of a very large size (considered infinite, for approximation purposes) can be easily determined as a function of the desired margin of error and degree of confidence. The margin of error represents the desired accuracy of measurement. The degree of confidence indicates the risks one is willing to take when relying on the measured values; typical values are probabilities of 95% and 99%. For example, a degree of confidence of 99% implies that in 1% of all possible similar samples, the observed result is due only to chance and does not reflect underlying population values.

The minimum sample size required for estimating an unknown proportion p with a given margin of error, abbreviated ME, and a given confidence level, abbreviated CL, is easy to determine by several steps [18]:

- Calculation of the alpha level: $\alpha = 1 - CL$;
- Finding the critical standard score z from a normal distribution table or calculator [19], as a function of α; assuming that the sample estimate may be larger or smaller than the real value, than a two tailed hypothesis test is required and z represents the value for which the cumulative probability equals $1- \alpha/2$. For example, for a confidence level of 95% $\alpha=0.05$ and $z=1.96$;

- Calculating the minimum sample size n according to the following formula:

$$n = [(z^2 * p * (1\text{-}p)) + ME^2] / (ME^2) \qquad [1]$$

where p represents the expected value of the proportion. The most conservative value of n is derived for p=0.5, which correspond to the maximum expected variance in the population.

For example, for an infinite population, a margin of error of 1% and a degree of confidence of 0.95 the minimum sample size when expecting maximum variability is n=9604 observations.

It follows that relying on randomly sampled observations leads to considerable saving in comparison to continuous or proportional monitoring, while allowing for the liberty of deciding the degree of precision in measurement and the degree of confidence in the results of the measurement.

7. Conclusions

The article analyzes the current security risks in AONs and proposes methods for optimizing protection, taking into account specific metrics for monitoring traffic, required pieces of equipment, and the need to optimize energy consumption.

Efficient performance testing for all optical networks is required both for failure identification and attack detection. While AONs greatly improve bandwidth, their transparency makes them particularly vulnerable to covert attacks which are difficult to detect by optical means. Optic-electronic-optic conversions are often more valuable as opportunities for traffic inspection than as signal regeneration means. Considerable advances in the portability of optical equipment are required to allow for more relevant network testing in the field. Hybrid systems may be designed which rely on O-E-O conversions for classes of guaranteed traffic while benefitting from the cost reductions of the O-O-O traffic for best-effort categories.

Significant cost reductions in monitoring efforts may also be introduced by relying on random sampling techniques in testing performance levels. We propose a pilot tone approach in performance monitoring supported by random sampling, and we discuss energy savings as a function of desired accuracy and confidence levels. Further research is required to recommend specific sampling algorithms adapted to particular network requirements.

REFERENCES

[1] *K. N. Sivarajan*, “Optical Networking Systems – Trends and Opportunities”, A Tejas Networking White Paper, http://www.tejasnetworks.com/news/optical-networking-systems-trends-opportunities.pdf

[2] *M. Medard, D. Marquis, S. Chinn*, “Attack Detection Methods for All-Optical Networks”, 1998 Network and Distributed System Security Symposium, sponsored by the Internet

Society, session 3, paper 1, http://www.isoc.org/isoc/conferences/ndss/98/medard.pdf (1998)

[3] *The International Engineering Consortium*, "Optical switches: making optical networks a brilliant reality", http://www.iec.org/online/tutorials/acrobat/opt_switch.pdf (2007)

[4] *M. Cahill, G. Bartolini, M. Lourie, L. Domash*, "Tunable Thin Film Filters for Intelligent WDM Networks", Proc. SPIE Vol. 6286, "Advances in Thin Film Coatings for Optical Applications III," Ed. M. J. Ellison (2006)

[5] *N. Harvey, M. Patrascu, Y. Wen, S. Yekhanin, V. S. Chan*, "Non-Adaptive Fault Diagnosis for All-Optical Networks via Combinatorial Group Testing on Graphs", INFOCOM 2007. 26th IEEE International Conference on Computer Communications, 1, 697 (2007)

[6] *J.K. Patel, S.U. Kim, D.H. Su, S. Subramaniam, H. Choi*, "A Framework for Managing Faults and Attacks in WDM Optical Networks", DARPA Information Survivability Conference and Exposition (DISCEX II'01), 2, 1137 (2001)

[7] *Y. Huang, J.P. Heritage, B.Mukherjee*, "Connection Provisioning With Transmission Impairment Consideration in Optical WDM Networks With High-Speed Channels", Journal of Lightwave Technology, 23, 982 (2005)

[8] *W. Chen*, "Signal Processing for Optical Performance Monitoring and Impairment Mitigation", unpublished PhD Thesis, available at http://www.ee.unimelb.edu.au/multimedia/research/cubin_Wei_Chen_thesis.pdf (2006)

[9] *L. Meflah, B. Thomsen, J. Mitchell, P. Bayvel, G. Lehmann, S. Santoni, B. Bollenz*, "Advanced Optical Performance Monitoring for Dynamically Reconfigurable Networks", Networks and Optical Communications (NOC), http://www.ee.ucl.ac.uk/~ong/publications/papers/Meflah_NOC2005.pdf (2005)

[10] *I.O. Nasieva, S. Boscolo, S.K. Turitsyn*, "Bit error rate improvement by nonlinear optical decision element", Optics Letters 31,1205 (2006)

[11] *N. Skorin-Kapov, O. Tonguz, N. Puech*, "Self-Organization in Transparent Optical Networks: A New Approach to Security", 9th International Conference on Telecommunications ConTel 2007, 7 (2007)

[12] *M. Medard, D. Marquis, A. Barry, S. Finn*, "Security Issues in All Optical Networks", IEEE Network Magazine, 1, 42 (1997)

[13] *T. Wu, A.K. Somani*, "Attack monitoring and localization in All-Optical Networks", Cluster Computing, 9, 465 (2006)

[14] *H. Rohde, D. Shupke*, "Securing Passive Optical Networks Against Signal Injection Attacks", Lecture Notes in Computer Science, 4534, 96 (2007)

[15] *R. Rejeb, I. Pavlosoglou, M.S. Leeson and R. J. Green*, "Management Issues in Transparent Optical Networks", Proceedings of 2004 6th International Conference on Transparent Optical Networks, 248-254. Retrieved October 4, 2010 at http://www.eng.warwick.ac.uk/yiannis/papers/paper07.pdf

[16] *R. Rejeb, I. Pavlosoglou, M.S. Leeson and R. J. Green*, "Securing All-Optical Networks". Retrieved February 4, 2011 at http://www.eng.warwick.ac.uk/yiannis/papers/paper04.pdf

[17] *J.K. Patel, S.U. Kim, D.H. Su, S. Subramaniam, H.-A. Choi*, A Framework for Managing Faults and Attacks in WDM Optical Networks. Retrieved February 1, 2011 at http://www.antd.nist.gov/pubs/discex.pdf

[18] *StatTrek,* Statistics Tutorial: Sample size. Retrieved February 4, 2011 at http://stattrek.com/Lesson6/SampleSize.aspx

[19] *StatTrek*, Cumulative Normal Distribution Calculator: Online Statistical Table. Retrieved February 4, 2011 at http://stattrek.com/Tables/Normal.aspx