2010 International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)

Failure Localization in Transparent Optical Networks

Dimitri Staessens*, Konstantinos Manousakis†, Didier Colle*, Uri Mahlab‡, Mario Pickavet*,
Emmanouel Varvarigos† and Piet Demeester*
* Ghent University - IBBT, Deptartment of Information Technology (INTEC),
Gaston Crommenlaan 8 bus 201, 9050 Ghent, Belgium.
Email: {dimitri.staessens, didier.colle, mario.pickavet, piet.demeester}@intec.ugent.be
† Research Academic Computer Technology Institute,
Nikou Kazantzaki street, University Campus of Patras, 26500 Patras, Greece.
Email: {manousak, manos}@ceid.upatras.gr
‡ ECI Telecom, 30 Hasivim St., 49517 Petach Tikva, Israel, and
Holon Institute of Technology (HIT), Electrical Engineering Department,
52 Golomb street, 58102 Holon, Israel.
Email: uri.mahlab@ecitele.com

***Abstract*—In this paper, we address failure localization from both a practical and a theoretical perspective. After summarizing the state-of-the-art of failure localization algorithms and monitoring techniques, an overview of the most prevalent failures in optical core networks is presented. We review the role of the Optical Supervisory Channel and how it reports problems to the management plane. We analyze different equipment, investigating where most failures occur and how these failures can be monitored. We conclude that in-band OSNR monitoring is the most important monitoring technique for failure localization purposes. We give a general probabilistic model for failure localization and assess its limitations using the mutual information metric. We give a simple example for computing this mutual information and show that is it a valid metric for evaluation of the failure localization problem. For practical applications, with imperfect monitoring equipment and countless possible failures, the mutual information may be prohibitingly low. Initial analysis of the problem shows that we need intense and accurate monitoring in order to increase the mutual information for the problem and to be able to localize failures accurately.**

I. Introduction

Modern telecommunications networks need to be able to detect and locate failures and degrations as fast and as accurately as possible, in order to restore lost traffic and repair the failure. While protection and restoration mechanisms can cope with traffic loss without exact knowledge of the failure type and location, most of the time spent reparing failures is spent in finding the precise cause.

Failures can be detected using various monitoring devices. These vary from simple photodetectors (detecting loss of light or attenuation), over OSNR (Optical Signal to Noise Ratio) monitors to Bit Error Rate (BER) monitoring, which is automatically performed at the termination point of each lightpath. More advanced monitoring techniques can specifically detect residual Chromatic Dispersion and other impairments. The failure localization problem is stated as, given a number of alarms in the network, where is the failures causing these alarms.

General probabilistic models for localizing network failures have been examined in [1], [2] and [3]. In [1] the network element failures are modeled in a dependency graph, where each node (element) has an a-priori probability to fail by itself (primary failure). When a node fails it will emit an alarm. A directed edge $e_i \rightarrow e_j$ indicated that element e_i depends on e_j and has a probability $P(e_i|e_j)$ to malfunction (and emit an alarm) due to the failure of e_j. The probabilities are assumed known and based on empirical and historical knowledge. [1] assumes that alarms only carry information about the emitting node, while [2] makes use of Alarm Reporting Functions in order to create classes of objects and [3] defines a hierarchical dependency graph consisting of services, protocols and functions and defining multiple failure modes per element. Both [2] and [3] transform their extended and hierarchical dependency graph into a simpler flat causality graph, mapping the extra information from the alarm messages into this graph. Note that we can consider the causality graph as a dependency graph. Also, each node has a single failure mode i.e. elements can only fail in one way (due to the primary fault) and emit only a specific alarm message (due to secondary malfunction). [1] examines the Maximum Mutual Dependency algorithm. The complexity is estimated to $O(N^3)$. [2] proposes an alarm domain extraction algorithm and [3] examines two algorithms, a combinatorial that uses a metric of goodness and an iterative heuristic (entitled Incremental Hypothesis Update) that uses a belief metric. The first one has $O(2^N)$ complexity which practically may be polynomial, while the complexity of the second one is $O(N^4)$.

A probabilistic approach is examined under a real environment [4]. They extract a hierarchical causality graph of tree topology and perform the reasoning by unfolding the hierarchy and just keeping the most probable problem.

In [5] authors propose an algorithm for locating multiple failures at the physical layer of a WDM network. Given the set of triggered alarms for each failure in the network, and

978-1-4244-7286-4/10/$26.00 ©2010 IEEE

a set of triggered alarms (may include false/missing alarms), find all possible failures which are capable of producing these alarms. The proposed algorithm does not rely on timestamps nor on failure probabilities as in [1].

Different techniques for distributed monitoring are described in literature. [6] showed the feasibility of a fault detection scheme for all-optical networks based on their decomposition into monitoring-cycles (m-cycles). In [7] authors formulate an m-cycle construction for fault detection as a cycle cover problem with certain constraints. They propose a heuristic spanning-tree based cycle construction algorithm that they apply to four typical networks. To detect and locate network faults, it is not necessary to put monitors on all links, lightpaths, or nodes. For example, some authors proposed a diagnosis method with sparse monitoring nodes (multiple monitors may be required) particularly for crosstalk attacks, which could be considered as special cases of network faults in a wide sense [8].

In [9] authors investigate the m-trail design problem. They conduct a bound analysis on the minimum length of alarm code required for unambiguous failure localization. Then, a novel algorithm based on random code assignment (RCA) and random code swapping (RCS) is developed for solving the m-trail design problem. The algorithm was verified by comparing with an Integer Linear Program (ILP), and the results demonstrated its superiority in minimizing the fault management cost and bandwidth consumption while achieving significant reduction in computation time.

Authors in [10] provide quantitative performance analysis for flat and hierarchically distributed monitoring and fault-localization in all-optical networks. They present an efficient heuristic and compare achievable improvements in monitor activation and fault-localization complexity for both schemes. A centralized, flat monitoring model consists of a central fault-manager which receives alarms from all monitors in the network and processes them simultaneously. Using such a model for monitoring large Transparent Optical Networks (TONs) can result in flooding the central manager with a large number of redundant alarms, delaying fault localization and service restoration.

In [11] authors propose the fault localization method using integrated network alarm correlation technique based on Consolidated Inventory Database (CID) which stores the network equipments details and the connection data among them. The proposed method collects the network alarms from various NMSes(Network Management System) which manages its own network domain. Authors claim that the analysis of alarm correlation based on the detailed end-to-end network view point is necessary to improve the effect of fault localization technique on complicated telecommunication networks. They propose fault localization method which covers complex networks, e.g., SDH networks, IP backbone networks, IP access domain networks, xDSL networks and etc.

This paper is further organized as follows. In Section II we give a general overview of the network resources for failure management and an generic classication of failure types. In Section III we summarize the most typical failures occuring in optical networks. In Section IV we give the probabilistic description of the failure localization problem. Section V provides an example to evaluate the model and Section VI provides some directions for future work and concludes the paper.

II. Issues in network failure localization

Most networks use an Optical Supervisory Channel (OSC) for for remote node management, monitoring and control [13]. This OSC is typically a low bandwidth (STM-1) out-of-band (usually at 1510 nm), full duplex point-to-point communication and control channel. It is common practice to use the Digital Communication Channel (DCC) section of the STM-1 header or the General Communication Channel (GCC) of OTN for this purpose. In every managed node (e.g. amplifier, regenerator, cross connect) the channel is dropped, the relevant data is inspected, instructions are performed and possible replies are added. This reframing typically takes $100-200\mu s$.

There are many types of service disruptions in optical networks, which we can classify in two major types. On the one hand, we have *hard failures*, such as fiber cuts and failure of a network line card. Fiber cuts happen all too frequently, due to human error such as construction workers breaking a cable or due to natural causes, such as earthquakes. Line card failures can for instance happen due to short circuiting. These failures occur suddenly and have a severe impact on services, causing major loss of traffic. On the other hand, we have *soft failures* such as end-of-life of an amplifier. These are more subtle changes in performance, causing a wide spectrum of service degradations which are far more difficult to detect and locate.

We can differentiate between failures that are self-reported throught the management systems, and those are not. If some malfunctioning can be detected in a cost-efficient way, the equipment itself will implement a self-diagnostics subsystem and report these types of failures immediately. For other failures, such as noise increases, the detection requires OSNR monitoring, which is very expensive. These kind of degradations will usually not be self-reported.

Most hard failures (causing sudden loss of transmission) are self-reported, while only some soft failures are. Soft failures that are not self-reported may be very hard to detect and nearly impossible to accurately locate. We will now give an overview of the most prevalent network element failures and their consequences.

III. Failures modes in Optical networks

This section was compiled from IEC equipment specifications [12] and discussions with (sub)system design engineers.

1) Optical fibers and connectors: The most common failure in an optical network is a fiber cut. Fiber cuts are self-reported, because they generate loss of light, which is easily detected at neighboring managed sites and then reported to the management plane using the OSC. A lot more difficult to locate are fiber bending (macrobending) and lossy connectors due

TABLE I
FAILURE MODES IN OPTICAL NETWORKS

Equipment type	Failure mode	degradation	Monitor types triggered	self-reported
VOA/DGE/DTE	unknown	wrong attenuation		yes
V-mux	total	attenuation max		yes
	total	attenuation fixed		yes
tunable filter+ tunable DCF	drift of passband	noise due to XT (channel)	OSNR	no
	narrowing	distortion	possible OSNR, definitely BER	no
		wrong DCF length (ISI)	OSNR	no
switch, WSS	subsytem failure	noise due to XT	OSNR	no
	narrowing	FC (@ provisioning)		no
tx	end of life	drift	OSNR	no
	wrong power			yes
rx	complete	channel lost		yes
	electrical unit failure	noise		yes
fiber	bending	attenuation		no
	bad connector	attenuation/LOL		no
amplifier	low/high output			yes
	gain			yes
	gain tilt			no
	pump	noise (all channels)	OSNR / OSA	no

to dust or burning. Connector burning is commonly observed in high-power systems, for instance at a Raman pump laser, but could also occur due to amplifier transient effects. Usually transient effects are managed within the amplifiers, but after significant channel drop in a transparent network (for instance due to a fiber cut on a neighboring link) or malfunction of the transient management subsystem, it is possible for a transient to increase the power on a channel to disruptive levels.

Fiber bending and bad connectors cause loss over a wide spectrum, ranging from 0 to 20 dB. High loss will be self-reported like a fiber cut, but low loss due to minor bending or a little dust can be within design limits. This loss will lead to decreased OSNR. At an amplifier site, a lower power input signal is compensated by higher gain toward the output port, so that the net effect is a decreased OSNR of the output signal, which deteriorates with every subsequent amplification. The number of affected channels is dependent on the location of the bad connector or fiber bend. If the loss occurs before multiplexing, it will affect only a single channel. If it occurs after multiplexing, it will deteriorate all channels on the fiber. Depending on this location, localization techniques using out-of-band monitoring are not able to detect this failure.

2) Amplifiers: Amplifiers can cause different types of signal degradation. If an amplifier cannot reach its target output power due to malfunction of the gain control or power loss of the pump laser, this is usually detected by a photodiode and reported to the management system. Similarly, if the output power is too high this will be reported. However, variations of pump laser wavelength due to the aging or due to malfunctions of the temperature control system can increase optical noise. Most amplifier failures usually affect all channels, but if there is tilt in the amplifier gain, channels with higher amplification will show increased noise. This may make these failures difficult to detect using out-of-band monitoring techniques.

3) Variable Optical Attenuators: Another type of equipment that is widely used are Variable Optical Attenuators (VOAs). These are commonly used in arrays for Dynamic Gain Equalisation (DGE) in OXCs and multiplexers and tilt compensation in amplifiers. The effect of malfunction of these components is usually a change in power (when the VOA gets stuck in maximum gain or no gain) or a loss of control if the VOA gets stuck on its current gain level. The last failure of the VOA will not lead to an immediate signal degradation. All these failures are easily detected using photodiodes and therefore can be considered self-reported.

4) Tunable Filters: The use of tunable filters in the network can also lead to OSNR degradations and increased BER. An application for filters is Dispersion Compensation in systems with multiple datarates, where higher datarates require more compensation. The filter will select the higher rate wavelength for transmission through additional DCF to compensate for residual chromatic dispersion. Narrowing of the passband can create signal distortion which will lead to BER increase, but may not be detected by OSNR measurement. Another problem is Filter Concatenation (FC), however this is only encountered at channel provisioning and is not a network failure in the strict sense. Drift of the filter passband may create noise due to crosstalk (XT), and if the DCF is of the wrong length, we may get Inter-Symbol Interference, which will again lead to increased OSNR.

5) Optical Cross Connects: Optical Cross Connects exhibit similar problems as tunable filters since they use similar technology (e.g. MEMS). Attenuation problems, for instance due to misalignment of MEMS, are typically self-reported, but limited loss and XT leading to decreased OSNR are much more difficult to detect. Depending on the switch design, these failures affect single channels or all channels passing through it.

6) Transmitters and Receivers: Most failures of transmitters and receivers are also easily detected. Wrong output power is self-reported since the transmitter usually uses a feedback loop to control its output power. If it cannot reach the correct ouput power, the unit sends an alarm through the OSC. A transmitter which reaches end-of-life and starts drifting will lead to misalignment with various filters, with distortion and possible OSNR decrease as a result. This failure is hard to locate. Receiver failures (destroyed receivers or electrical failures) are also self-reported.

A summary of these failure modes is given in Table I. From this section, we can conclude that the most important quantity to monitor in optical networks is noise, more specifically (in-band) OSNR. These monitors have a certain margin of error and are quite expensive. These factors make practical failure localization a difficult problem.

IV. General Problem Statement

A. Definition

A network consists of a set of elements $E = \{e_1, \dots, e_n\}$, which can fail with a certain probability $P_E(e_i) \in [0,1]$. We define a network failure f_j as a set of element failures, so the set of network failures $F = \{f_1, \dots, f_{2^n}\}$ is the power set of E. F includes the non-failure case. The probability of a network failure $P_F(f_i)$ can, in theory, be computed from the element failure probabilities and the dependency between these failures. Each network element failure can trigger alarms through different monitors. Call the set of alarms $A = \{a_1, \dots, a_m\}$. An observation o_i is a set of alarms that are raised due to some network failure f_i with probability $P_{O|F}(o_j|f_i)$. The set of observations O is the power set of the set of alarms and has 2^m elements. The problem is to find the most likely network failure $f_x \in F$ which explains the observation $o_y \in O$, $f_x = \max_z \big(P_{O|F}(o_y|f_z)P_F(f_z)\big)$.

This general model describes the general problem of network failure localization. Every derived approach (i.e. a failure localization algorithm) will approximate the solution of this problem. The accuracy of the model will depend on the quality of the initial probabilities and the amount of information that is contained in the alarms. We will now assess the efficiency of the approach using the mutual information [14] metric. This metric gives a quantitative measure how sure we can be, given observation o_i, that network failure f_j is indeed the cause.

The above problem description is NP-complete and therefore computationally infeasible for large networks. In a network with n elements and m alarms, the number of probabilities is $2^n * 2^m = 2^{n+m}$.

B. Mutual Information, Self-Information and Entropy

Let $x_1, \dots, x_k$ be the X sample space and $y_1, \dots, y_l$ be the Y sample space in an XY joint ensemble. We want a quantitative measure of how much the occurence of y_j in the Y ensemble tells us about the occurence of the possibility x_i in the X ensemble. The occurence of $y = y_j$ changes the probability of $x = x_i$ from the *a priori* probability $P_X(x_i)$ to the *a posteriori* probability $P_{X|Y}(x_i|y_j)$. This measure is called the mutual information between y_j and x_i and is defined as

$$I_{X;Y}(x_i;y_j) = I_{Y;X}(y_j;x_i) = \log \frac{P_{X|Y}(x_i|y_j)}{P_X(x_i)} \tag{1}$$

The term *mutual* information comes from the symmetry of equation (1). The (weighted) average mutual information between X and Y is defined as:

$$I(X;Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} P_{XY}(x_i,y_j) \log \frac{P_{X|Y}(x_i|y_j)}{P_X(x_i)} \tag{2}$$

where $P_{XY}(x_i,y_j) = P_X(x_i)P_{Y|X}(y_i|x_i) = P_Y(y_i)P_{X|Y}(x_i|y_i)$ is the probability of observing $X = x_i$ and $Y = y_i$ simultaneously. If an event x_i is fully specified by the occurence of y_j, i.e. $P_{X|Y}(x_i|y_j) = 1$ the mutual information between x_i and y_j becomes:

$$\begin{aligned} I_{X;Y}(x_i;y_j) &= \log \frac{P_{X|Y}(x_i|y_j)}{P_X(x_i)} \\ &= \log \frac{1}{P_X(x_i)} = I_X(x_i) \end{aligned} \tag{3}$$

and we call this the self-information of the event $x = x_i$. The entropy of an ensemble X is the (weighted) average self-information of the ensemble and is given by:

$$\begin{aligned} H_X(X) &= \sum_{i=1}^{n} P_X(x_i) \log \frac{1}{P_X(x_i)} \\ &= -\sum_{i=1}^{n} P_X(x_i) \log P_X(x_i) \end{aligned} \tag{4}$$

V. Efficiency of the probabilistic model

The efficiency of any failure localization in an optical network will strictly depend on the mutual information between monitors and failures. In the ideal case, self-reported failures have mutual information equal to the self-information, meaning that the probability of the reported failure, when we receive the alarm indicating this failure, is 100%. Of course, implementing perfect monitoring for every conceivable set of failures in the network is impossible.

From a theoretical viewpoint, all probabilities are considered as input for the model. Of course, from a practical perspective, this is where the real difficulties are encountered. The a priori failure probabilities for the equipment can be more or less estimated from experience [1], but the conditional probabilities for the alarms are far less straightforward to compute. Most models [1] [5] take these to be 1, i.e. if the equipment fails, the alarm(s) will be raised and vice versa. However, for real networks this is not the case, as we illustrated above.

Even small changes in these probabilities have a huge impact on the mutual information. This is intuitively understood by considering the following example. If you monitor some equipment with a failure probability of 10^{-4}, with 100% accuracy, when your alarm is raised you are 100% sure that this failure occured. However, if you monitor the same element with 99.99% accuracy, when you have an alarm, you have roughly 50% chance that the element failed and 50% chance it's a false alarm, since both events are equally likely. It are these a posteriori probabilities that are summed to compute the mutual information in Eq. (2).

A. Example

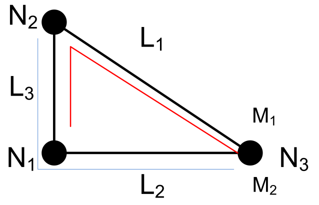

Fig. 1. Definition

In Figure 1, we give a small example for a simple 3 node ring network with 2 monitors at the end of 2-hop paths. We make the following simplifying assumptions. First, the failures are statistically independent, second the monitors work perfectly. We only consider 3 possible failures associated with the three links. Call the three nodes N_1, N_2, N_3 with two monitors M_1 and M_2 located in node N_3. The links L_1, L_2, L_3 have length $5, 4, 3$ respectively and there are two lightpaths, one from N_1 to N_3 along $L_3 - L_1$, monitored by M_1 and from N_2 to N_3 along $L_3 - L_2$, monitored b M_2. Failure of L_1 triggers M_1, failure of L_2 triggers M_2 and failure of L_3 triggers both monitors. All multiple link failures will trigger M_1 and M_2, meaning we cannot fully distinguish between multiple link failures and the single failure L_3. We assume the probability of a failure per unit length to be 10^{-4}.

We can thus construct the following sets: $E = \{L_1, L_2, L_3\}$, $F = \{\emptyset, L_1, L_2, L_3, L_1L_2, L_1L_3, L_2L_3, L_1L_2L_3\}$, $A = \{M_1, M_2\}$, $O = \{\emptyset, M_1, M_2, M_1M_2\}$.

TABLE II
ENTROPY OF THE FAILURES

failure f	$P(f)$	$\log \frac{1}{P(f)}$	$P(f) \log \frac{1}{P(f)}$
$\emptyset$	0.9988005	0.0017316	0.001729
L_1	0.0004996	10.966794	0.005480
L_2	0.0003997	11.288867	0.004512
L_3	0.0002997	11.704049	0.003508
L_1L_2	$1.199\ 10^{-07}$	22.991183	$2.758\ 10^{-06}$
L_1L_3	$1.499\ 10^{-07}$	22.669111	$3.400\ 10^{-06}$
L_2L_3	$1.999\ 10^{-07}$	22.253930	$4.449\ 10^{-06}$
$L_1L_2L_3$	$6\ 10^{-11}$	33.956247	$2.037\ 10^{-09}$
	1		0.015239663

The a priori probabilities are given in Table II, together with the quantities to compute the entropy. The table immediately confirms what was to be expected: the highest information content lies in the single failures and the abscence of failures. In order compute the mutual information, we need the a priori probability of a monitor triggering, i.e. the a priori probabilities of the observations. These are easily computed to be $P_O(\emptyset) = 0.99880047$, $P_O(M_1) = 0.00049965$, $P_O(M_2) = 0.00039968$ and $P_O(M_1M_2) = 0.0003002$.

Calculation of the average mutual information is given in Table III. The first column shows the mutual information between each failure and the observation. Since the conditional probability equals 1, this is equal to the self-information in the monitors (see Eq. (1). Note that the probabilities $P_{FO}(fo)$, needed for computation of the mutual information between the two sets, are completely dependent on the failures, so $P_{FO}(fo) = P_F(f)$ if we assume perfect monitoring.

TABLE III
MUTUAL INFORMATION

f	o	$I(f;o)$	$P_{FO}(fo).I(f;o)$
$\emptyset$	$\emptyset$	0.001731595	0.001729518
L_1	M_1	10.96679435	0.005479559
L_2	M_2	11.28886678	0.004511935
L_3	M_1M_2	11.70178869	0.003507378
L_1L_2	M_1M_2	11.70178869	$2.33966\ 10^{-06}$
L_1L_2	M_1M_2	11.70178869	$1.75457\ 10^{-06}$
L_2L_3	M_1M_2	11.70178869	$1.40351\ 10^{-06}$
$L_1L_2L_3$	M_1M_2	11.70178869	$7.02107\ 10^{-10}$
			0.015233882

We see, that in this simple example, the mutual information is lower than the entropy of the failures, meaning we cannot distinguish all failures. Should we have placed three monitors (with perfect accuracy), there would of course be no ambiguity. An algorithm which focusses on single failures would in this case perform almost as well as the complete solution.

In real networks we need to take caution with this example. First, failures occur with a large distribution of failure probabilities. Some dual failures may be more common than other single failures. Second, monitoring is not perfect, and we cannot choose to omit certain failure types. If we assume imperfect monitoring, say with inaccuray of 10^{-8}, we can compute the entropy for this scenario to be 0.015239663. For the mutual information, we find the value 0.015233699, or a ratio of 0.9996. This is an example where we can distinguish all single failures, and double failures are much less likely and contribute little to the total mutual information. An algorithm focussing on single failures has mutual information 0.015228207 (this is easily computed by omitting the contributions of multiple failures to the mutual information) or ratio 0.99925, and can be considered a good algrrithm.

If we take the same example (with inaccuracy 10^{-8}, but the second lightpath is from N_1 to N_3 along L_2, then M_2 triggers only when L_2 fails and failure of L_3 cannot be distinguished. In this case, we can compute the mutual information to be 0.014474206 or a ratio of 0.94977. This may seem like a good value, but we know that this example cannot locate all single failures, so this value is already an indication of inadequate monitoring.

In Figure 2 we plot the mutual information versus the monitor accuracy. The monitor accuracy is shown as the logarithm of the accuracy (-4 meaning 0.9999 accuracy). This figure clearly shows a sudden drop in mutual information around 10^{-4}, exactly the range of the failure probabilities of the elements. This shows that mutual information is also a good indicator for the monitoring accuracy, and inversely shows that accurate monitoring is paramount in failure localization.

We find already in these simple examples that the mutual information is lower than the entropy of the failures, meaning we cannot distinguish all failures. Should we have placed three monitors (with perfect accuracy), there would of course be

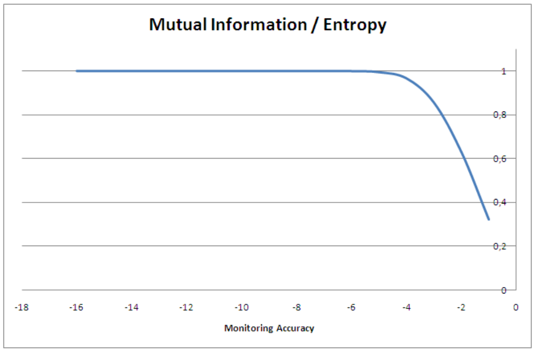

Fig. 2. Mutual Information vs Monitor Accuracy

no ambiguity. In real networks failures occur with a large distribution of failure probabilities. Some dual failures may be more common than other single failures.

VI. Conclusions and Future Work

We have summarized different possible failures in optical networks and how they can be monitored. From this summary, OSNR monitoring proves to be the most important form of monitoring to install in the network. We show that the mutual information between the monitors (i.e observations) and failures is a good metric for failure localization efficiency, both in the case of insufficient monitoring and inaccurate monitoring. In the ideal case, the mutual information between the monitors and the failures should equal the entropy of the failures.

In ongoing work, we will investigate the sensitivity of the mutual information to the number of monitors, their location and the accuracy of the monitoring. We will try to find exact boundaries for the mutual information where monitoring is accurate enough to locate all major failures. We will use this model for locating the optimum placement of monitors.

Acknowledgment

This work was supported by the European Commission within the BONE-project ('Building the Future Optical Network in Europe'), a Network of Excellence, and Strep DICONET ('Dynamic Impairment Constraint Networking for Transparent Mesh Optical Networks'), both funded through the 7th ICT-Framework Programme.

References

[1] I. Katzela and M. Schwartz, *Schemes for Fault Identification in Communication Networks*, IEEE/ACM Transactions on Networking, Vol. 3 (6), 1995, pp. 753-764.

[2] J. Choi, M. Choi and S.H. Lee, *An Alarm Correlation and Fault Identification Scheme Based on OSI Managed Object Classes*, Proc. IEEE Int'l Conference on Communications ICC 1999, pp.1547-1551.

[3] M. Steinder and A.S. Sethi, *Non-Deterministic Diqgnosis of End-to-End Service Failures in a Multi-Layer Communication System*, Proc. IEEE Int'l Conference on Computer Communications and Networks 2001, pp. 374-379

[4] C.S. Chao, D.L. Yang and A.C. Liu, *An automated Fault Diagnosis System Using Hierarchical Reasoning and Alarm Correlation*, Journal of Network and Systems Management,Vol.9 (2), 2001, pp.183-202.

[5] C. Mas and P. Thiran, *An efficient algorithm for locating soft and hard failures in WDM networks*, IEEE Journal On Selected Areas In Communications, Vol. 18, No. 10, October 2000.

[6] T. Wu and A.K. Somani, *Necessary and Sufficient Condition for k Crosstalk attacks localization in All-optical Networks*, Proc. IEEE Globecom 2003, pp. 2541-2546.

[7] H. Zeng, C. Huang and A. Vukovic *A novel fault detection and localization scheme for mesh all-optical networks based on monitoring-cycles*, Photonic Network Communication, Vol. 11, 2006, pp.277-286.

[8] T. Wu and A.K. Somani, *Attack monitoring and localization in all optical networks*, Proc. of SPIE Opticommun 2002: Optical Networking and Communications, vol. 4874, pp. 235-248.

[9] J. Tapolcai, B. Wu and P.H. Ho, *On monitoring and failure localization in mesh all-optical networks*, Proc. IEEE INFOCOM 2009

[10] S. Stanic and S. Subramaniam *A Comparison of Flat and Hierarchical Fault-Localization in Transparent Optical Networks*, OFC/NFOEC, 2008

[11] J. Kim, Y. Yang, S. Park, S. Lee and B. Chung *Fault Localization for Heterogeneous Networks Using Alarm Correlation on Consolidated Inventory Database*, Springer LNCS , pp. 82-91, 2008.

[12] IEC86C, Document 62343-6-6 *DYNAMIC MODULES Failure Mode Effect Analysis for Optical Units of Dynamic Modules*

[13] R. Ramaswami and K. N. Sivarajan, *Optical Networks, A Practical Perspective*, 2nd ed., Morgan Kaufmann, New York, 2001.

[14] R.G. Gallager, *Information Theory and Reliable Communication*, John Wiley & Sons, New York, 1968