Failure Location Algorithm for Transparent Optical Networks

Carmen Mas, *Member, IEEE*, Ioannis Tomkos, and Ozan K. Tonguz, *Member, IEEE*

***Abstract*—Fault and attack management has become a very important issue for network operators that are interested to offer a secure and resilient network capable to prevent and localize, as accurately as possible, any failure (fault or attack) that may occur. Hence, an efficient failure location method is needed. To locate failures in opaque optical networks, existing methods which allow monitoring of the optical signal at every regeneration site can be used. However, to the best of our knowledge, no method exists today that performs failure location for transparent optical networks. Such networks are more vulnerable to failures than opaque networks since failures propagate without being isolated due to optoelectronic conversions. In this paper, we present a failure location algorithm that aims to locate single and multiple failures in transparent optical networks. The failure location algorithm developed in this paper can cope with ideal scenarios (i.e., no false and/or lost alarms), as well as with nonideal scenarios having false and/or lost alarms.**

***Index Terms*—All-optical networks, failure location, fault management, optical network security.**

I. Introduction

THE EXPLOSION of Internet traffic and the emergence of new applications have enforced the evolution of backbone networks toward wavelength-division-multiplexed (WDM) optical networks. Today's WDM networks are opaque networks able to transmit up to 160 wavelengths per fiber and packing more than 800 fibers into one cable. Therefore, one of the main advantages of these networks is the extremely high capacity that they offer. However, when a fault occurs thousands of connections may be interrupted and huge amounts of data (thousands of gigabits) are lost. Several groups and individual researchers are currently working not only on how to restore the affected connection as fast as possible but also on how to locate the fault accurately. For example, when link protection is used instead of path protection, the fault location should be fast and correct so that the restored link is the right one and is activated rapidly so that the amount of lost data is minimized.

It is clear, however, that not only faults but attacks also should be considered and located rapidly. An "attack" may be defined as an intentional action against the ideal and secure functioning of the network. Attacks can broadly be classified as eavesdropping or service disruption. Attacks could differ in nature ranging from malicious users (i.e., users inserting higher signal power) to eavesdroppers. One can define "failures" as the faults and attacks that can interrupt the ideal functioning of the network.

Failure management of optical networks deals with the prevention, detection, and reaction to failures. Prevention deals with the subsystem, system, and network design so that the number of possible faults is minimized. When the failure occurs, detection finds out the existence of the failure and deals with its identification. Finally, reaction manages to restore the connections that have been disrupted by the failure. All these functionalities become even more important in optical networks because of: 1) the high bit rates that cause a huge amount of information loss; 2) the high latency of the network that allows a large amount of data to get into the network when the fault occurs; and 3) the fault identification that should be efficient and exact in order to restore the connections and isolate the fault efficiently [1].

The failure management relies on the information collected from the network. In transparent networks, this information is delivered by the monitoring equipment, which supervises the signal after tapping and, therefore, without influencing the optical signal transmission. Opaque networks allow signal monitoring at least at each node where the signal is converted to electrical form. However, in transparent networks the monitoring of the signal is more complicated since it should be done in the optical domain and the optical signal is converted to the electrical domain only at the end of the lightpath.

Failure location or identification is based on the received alarms by the network management system. When there are two or more simultaneous failures the number of alarms increases considerably and the problem of locating the failure becomes more complicated. The problem of locating multiple faults has been shown to be NP-complete even in the ideal scenario that no lost or false alarms exist [2]. In this paper, we study the multiple failure location in transparent networks where the failures are more deleterious and affect longer distances. The failure location also covers the nonideal scenario, where lost and/or false alarms may exist. The problem of finding the location of extra monitoring equipment covered also in this paper is of interest to network operators that want to install it in a place that will improve the locating of failures. Our results show that the number of elements that are potential candidates to have a failure decreases drastically when monitoring equipment is placed in the proposed location.

The remainder of this paper is organized as follows. Section II describes failure management related issues in transparent optical networks such as different types of failures. Section III provides the problem formulation while Section IV describes

Manuscript received March 31, 2004; revised March 18, 2005. This work was supported in part by Cylab, Carnegie Mellon University, Pittsburgh, PA.

C. Mas and I. Tomkos are with the Athens Information Technology (AIT) Center, Peania 19002, Athens, Greece (e-mail: cmas@ait.edu.gr; itom@ait.edu.gr).

O. K. Tonguz is with the Electrical and Computer Engineering Department, Carnegie Mellon University, Pittsburgh, PA 15213-3890 USA (e-mail: tonguz@ece.cmu.edu).

Digital Object Identifier 10.1109/JSAC.2005.852182

TABLE I
FAILURE DETECTION CAPABILITIES OF MONITORING EQUIPMENT THAT CAN BE USED IN TRANSPARENT NETWORKS

Monitoring Equipment	Power	In-band Jamming	Out-band Jamming	Wavelength Misalignment	Time Distortion
Optical Power Meter	Yes	No	No	No	No
Optical Spectrum Analyzer	Yes	No	Yes	No[a]	No
Eye Monitoring	Yes	Yes	Yes	No	Yes
BER Monitoring	Yes	Yes	Yes	No	Yes
Wavemeter	Yes	No	No	Yes	No

[a]OSAs have low resolution to detect small wavelength misalignments

the transparent failure location algorithm (TFLA). Section V presents simulation results showing the influence of the type of monitoring equipment used and its location. Finally, conclusions are drawn in Section VI, while the auxiliary material is relegated to the Appendix.

II. FAILURE LOCATION IN TRANSPARENT OPTICAL NETWORKS

Transparent optical networks are very promising as they reduce unnecessary, expensive optoelectronic conversions, offer high data-rate, provide flexible switching, and support multiple types of clients (different bit rates, modulation formats, protocols, etc.).

This section first describes the monitoring equipment that may be used to detect failures, then it gives some examples of faults and attacks that may occur in these types of networks and it concludes with a classification of the considered failures.

A. Monitoring Equipment and Their Failure Detection Capabilities

Transparent optical networks contain two classes of network components: 1) *optical components* which take care of the optical signal transmission and are not able to send alarms and 2)*monitoring equipment* which is able to send alarms and notifications when the optical signal is not the expected one. The alarms sent by monitoring equipment depend on the kind of equipment used and its characteristics. The failure of the monitoring equipment does not interrupt/modify the data transmission and, therefore, their failure is not as relevant as the failure of an optical component. Moreover, when monitoring equipment fails, it may result in the loss of an alarm which will be considered as "lost" in the proposed algorithm.

Different types of monitoring equipment exist in the market place today and are used in transparent optical networks [3]. The majority of monitoring equipment work by tapping part of the optical signal using, for example, couplers. We assume that for monitoring purposes, the optical signal can be converted to the electrical domain, as, for example, in the case of bit-error rate (BER) monitoring, where the signal is electrically received so that the BER can be calculated.

We distinguish six different types of monitoring equipment whose failure detection capabilities are summarized in Table I.

- Optical power meter (PM): This monitoring equipment is able to detect any change in the power of the optical signal. It may be able to send alarm when the measured power is different from the expected one.
- Optical spectrum analyzer (OSA) [4]: This equipment is able to perform analog optical signal monitoring by measuring the spectrum of the optical signal. The parameters that can be measured are channel power, channel center wavelength, and optical signal-to-noise ratio (OSNR) which provides important information on the quality of the optical signal. For example, it is able to detect OSNR changes (even if they do not cause optical power variations) and the presence of unexpected out-of-band signals.
- Eye monitoring: It is able to monitor the eye diagram. This diagram gives information on the signal distortion. After processing the histograms obtained from the eye diagram, statistical characteristics of the optical signal can be obtained. However, to obtain the histogram, the amplitude of the eye should be measured which requires either synchronous or asynchronous sampling of the optical signal [5], [6].
- BER monitoring: After converting the signal to the electrical domain, this equipment is able to calculate the BER which is sensitive to the noise and to time distortion. This equipment is sensitive to impairments such as crosstalk, chromatic and polarization mode dispersion, and optical nonlinearities.
- Wavemeter is an accurate monitoring equipment able to detect any variation in the used wavelength and power. This equipment is used by the maintenance personnel to check and verify that the used wavelengths are the expected ones.
- Pilot tones and optical time domain reflectometry (OTDR) techniques are other techniques that are commonly used to monitor the performance of the network. They are beyond the scope of this paper.

B. Considered Failures

The failures that may occur in a transparent optical network can be classified into four categories based on the effects they inflict on the signal.

- Power drop: This failure includes any fault or attack that causes a change in the optical power. One example is when the optical fiber is cut or bent.
- In-band jamming (IBJ): This failure is the result of intrachannel crosstalk. For example, two different signals with the same wavelength in a switch may "exchange" information undesirably. For example, an attacker may increase gradually the power of one channel with respect to the other channels at the input so that the output of some channels may be too low or too high (low-power channels get less gain than high-power channels: power equalization).
- Out-band jamming: This failure includes interchannel crosstalk and nonlinearities. For example, an attacker may insert power at a wavelength outside the signal window and cause Raman effect and cross-gain modulation [in semiconductor optical amplifiers (SOAs)] that will affect the signal. The problem with this attack is that although a filter may remove the out-band disturbing

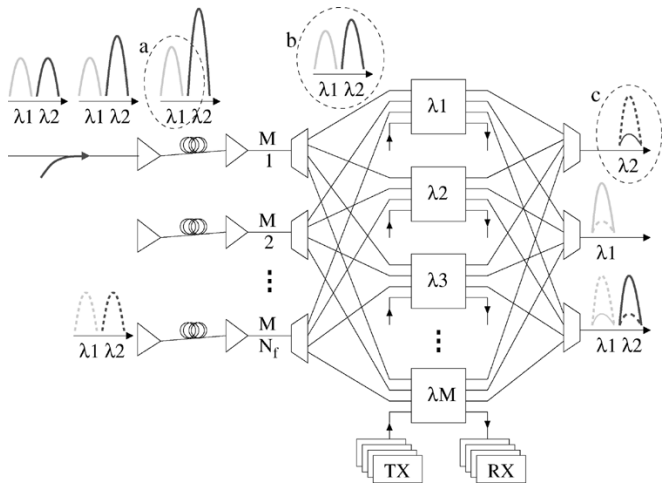

Fig. 1. Example of an attack on an optical cross-connect (OXC) with wavelength selective architecture and its propagation through different network components.

signal, the damage is already within the data and it will not be detected until being received and monitored by a BER or eye monitor.

- Wavelength misalignment: A transmitter may emit a signal with a wavelength slightly different than the expected one. Some operators use signal lockers to check the transmitted wavelength and if necessary correct it. However, this failure could be included and detected by the failure management.

These four failures cover most of the failures that may occur in transparent networks and are important concepts that will be used in the problem formulation and computation of the algorithm.

C. Example of Failures

As discussed previously, transparent optical networks are more vulnerable to failures than opaque networks. Opaque networks monitor the signal quality at the regenerators and other network components performing optical-to-electrical signal conversion. At these nodes, the signal quality can be measured by calculating the BER and performing some error control on the digital signal. Conversely, transparent networks do not perform any electrical conversion and, therefore, they can only rely on the information obtained from the optical analog signal by the monitoring equipment. Another disadvantage of transparent networks is that the failure may have a greater impact, as there are no transparency boundaries supported by optoelectronic regenerators.

This effect is shown in the following example of Fig. 1 as an attack. An attacker inserts optical power at a wavelength that is already used ($\lambda 2$). This attack will cause an increase of the optical power at that wavelength that will disturb neighboring channels. For example, when traversing an optical amplifier such as Erbium-doped fiber amplifier (EDFA), the gain that $\lambda 2$ channel will experience will be greater than the gain of $\lambda 1$ channel (case *a* of Fig. 1). Even after filtering channel $\lambda 1$ at the wavelength demultiplexer, there is some residual optical power at $\lambda 2$ higher than the one specified in the system, so it can degrade the performance of its neighboring channels (case *b* of Fig. 1). When there are optical switches, crosstalk is very critical. In our example, $\lambda 2$ channel of fiber N_f could be disturbed by $\lambda 2$ channel of Fiber 1 due to crosstalk (case *c* of Fig. 1). The degree of crosstalk is closely related to the optical power pumped by the attacker.

III. Problem Formulation

Before introducing the failure location algorithm, we will introduce the problem abstraction considered by the algorithm. The algorithm is based on the established channels. One channel is a unidirectional connection between two network nodes. A channel is considered as an ordered set of network components. These network components can be optical equipment or monitoring equipment. The optical equipment can have different alarm capabilities depending on which failures they are able to mask, so that the monitoring equipment following on that specific channel will not be able to detect that failure.

In this paper, several failures have been studied, as well as the behavior of network elements when the failures occur. Based on this behavior, we have defined different alarming properties.

- Power dropping masking: This property specifies whether the optical component masks any important drop of the optical power to any other monitoring equipment that follows it on the channel. For example, a regenerator will mask the power drop that occurred before the regenerator to any other component located after it on that channel.
- Misalignment masking: This property specifies whether the network component masks the wavelength misalignment failure to the network components that follow it on the channel. For example, a wavelength converter will mask any wavelength misalignment occurring at any optical component located before it on that channel (except if it uses the four-wave mixing (FWM) effect).
- IBJ masking: This property specifies whether the optical component masks the IBJ to the network components that follow it on the channel. For example, some regenerators are able to suppress crosstalk caused by IBJ.
- Out-band jamming masking: This property specifies whether the optical component masks the out-band jamming to the network components that follow it on the channel. For example, a filter should be able to eliminate the out-band signal when having a bandpass cutting it off.

A. Component Classification

As already mentioned before, the network components can be classified into two different categories: *optical components* and *monitoring equipment*. The former takes care of the transmission of the optical signal, whereas the latter takes care of the optical signal motoring. The *monitoring components* are able to send alarms when the optical signal is degraded and do not mask any failure since they receive the optical signal through a tapping coupler. On the other hand, the *optical components* are able to mask failures (summarized in Table II). For example, a filter is able to remove the nondesired out-band signal and, therefore, mask any out-band jamming that may have occurred before the filter. Another example is the amplifier without power

TABLE II
MASKING RELATIONSHIPS OF THE OPTICAL COMPONENTS

Optical Component	Power Drop	Wavelength Misalignment	In-band Jamming	Out-band Jamming	Category
Optical Fiber	No	No	No	No	O_0
Transmitter/Receiver	No	No	No	No	O_0
Filter	No	No	No	Yes[a]	O_2
Switch	No	No	No	No	O_0
Coupler	No	No	No	No	O_0
Converter/Regenerator	Yes	Yes[c]	Yes[b]	Yes	O_1
Amplifier	Yes[d]	No	No	No	O_3

[a]Masking will occur when the filter bandwidth is sharp enough to pass the signal and block the out-band signal. [b]Some techniques can suppress crosstalk. [c]Except when it is based on the FWM effect. [d]True when there is no power monitoring at the input.

monitoring: any power drop that may occur before the amplifier will be masked since the amplifier will give at the output the required signal power. Most of the passive components such as optical fiber, couplers, etc., do not mask any problem. Based on their masking properties, the optical components can be classified into different categories.

- **Optical components**: Let $\mathbf{O}$ denote the set of optical components in the network.
  - The $\mathbf{O_0}$ **masking components** are the optical components that are not able to mask any failure such as, for example, an optical fiber.
  - The $\mathbf{O_1}$ **masking components** are the optical components able to mask all kinds of failures. For example, an optical regenerator with crosstalk suppression capabilities and not based on FWM property.
  - The $\mathbf{O_2}$ **masking components** are the optical components able to mask out of band jamming, such as an optical filter.
  - The $\mathbf{O_3}$ **masking components** are the optical components able to mask power drops, such as an optical amplifier when it does not have power monitoring capabilities at its input.
- **Monitoring components**: The monitoring components are classified based on the failures they are able to detect. Let $\mathbf{V}$ denote the set of monitoring components in the network.
  - Let $\boldsymbol{V_1}$ denote the set of monitoring components able to detect just unexpected power variations such as PM.
  - Let $\boldsymbol{V_2}$ denote the set of monitoring components able to detect unexpected power variations as well as out-band jamming such as OSNR.
  - Let $\boldsymbol{V_3}$ denote the set of monitoring components able to detect unexpected power variations as well as in-band and out-band jamming such as BER.
  - Let $\boldsymbol{V_4}$ denote the set of monitoring components able to detect unexpected power variations, as well as wavelength misalignment

B. Channel Definition

The proposed algorithm is based on the established channels through the network instead of the network topology by itself. Each channel $CH_i = \{comp_j\}$ is an ordered list of network components. A component is identified by two numbers: the former gives the type of component (or category) and the second classifies the component within this category. The channels are considered here as unidirectional and, hence, bidirectional channels are equivalent to a pair of unidirectional channels. The algorithm uses a function $Pos(comp_j, CH_i)$ that returns the position of $comp_j$ within channel CH_i if the component belongs to the channel or 0, otherwise.

C. Domain Definition

The algorithm uses a function called *Domain*(*comp*), which is defined as the set of network elements that will send an alarm when a given optical component *comp* fails. This function is based on the fact that when a failure occurs it propagates along the path until the far end receiver or until it is masked by a certain component, while triggering the alarms of the monitoring equipment able to detect this failure. This function is applied to the different failures presented in Section II-B. Hence, four different kinds of *Domain* have been distinguished for every network component based on the nature of the failure.

- $PDomain(e_1)$ is the set of monitoring equipment whose alarms are expected when the network element e_1 suffers a power decrease or cut. These elements are any $\mathbf{V}$ monitoring equipment that follows e_1 in at least one channel and do not have any O_1 or O_3 component between them. Mathematically, $PDomain(e_1)$ can be expressed as follows: $PDomain(e_1) = \{e_2 \in V | e_1 P e_2 = 1\}$, where $e_1 P e_2 = 1$ if and only if
  - e_2 is a $\mathbf{V}$ monitoring equipment;
  - $\exists CH_i \in CH$ with $0 < Pos(e_1, CH_i) < Pos(e_2, CH_i)$;
  - $\forall e_j$ with $Pos(e_1, CH_i) < Pos(e_j, CH_i) < Pos(e_2, CH_i) e_j \notin O_1, O_3$.
- $MDomain(e_1)$ is the set of monitoring equipment whose alarms are expected when network element e_1 suffers a wavelength misalignment. These elements are any V_4 monitoring equipment that follows e_1 in at least one channel and do not have any O_1 component between them. Mathematically, $MDomain(e_1)$ can be expressed as follows: $MDomain(e_1) = \{e_2 \in V_4 | e_1 M e_2 = 1\}$ where $e_1 M e_2 = 1$ if and only if
  - e_2 is a V_4 monitoring equipment;
  - $\exists CH_i \in CH$ with $0 < Pos(e_1, CH_i) < Pos(e_2, CH_i)$;
  - $\forall e_j$ with $Pos(e_1, CH_i) < Pos(e_j, CH_i) < Pos(e_2, CH_i) e_j \notin O_1$.
- $IBJDomain(e_1)$ is the set of monitoring equipment whose alarms are expected when in network element e_1 an IBJ occurs. This IBJ can be caused by intra-channel crosstalk, in-band insertion of power, etc. The elements of the domain are any V_3 monitoring equipment that follows e_1 in at least one channel and do not have any O_1 component between them, where this M1 component can be regenerator or wavelength converter with IBJ suppression capabilities. Mathematically, $IBJDomain(e_1)$ can be expressed as follows:

$IBJDomain(e_1) = \{e_2 \in V_3 | e_1 IBJ e_2 = 1\}$ where $e_1 IBJ e_2 = 1$ if and only if
- e_2 is a V_3 monitoring equipment,
- $\exists CH_i \in CH$ with $0 < Pos(e_1, CH_i) < Pos(e_2, CH_i) e_j \notin \mathrm{O}_1$

- $OBJDomain(e_1)$ is the set of monitoring equipment whose alarms are expected when in network element e_1 an out-band jamming (OBJ) occurs. This out-band jamming can be caused by nonlinearities, interchannel crosstalk, etc. The elements of this domain are any V_2 or V_4 monitoring equipment that follows e_1 in at least one channel and do not have any O_1 or O_2 component between them. Mathematically, $OBJDomain(e_1)$ can be expressed as follows: $OBJDomain(e_1) = \{e_2 \in V | e_1 OBJ e_2 = 1\}$, where $e_1 OBJ e_2 = 1$ if and only if
  - e_2 is a V_2 or V_3 monitoring equipment;
  - $\exists CH_i \in CH$ with $0 < Pos(e_1, CH_i) < Pos(e_2, CH_i)$;
  - $\forall e_j$ with $Pos(e_1, CH_i) < Pos(e_j, CH_i) < Pos(e_2, CH_i) e_j \notin \mathrm{O}_1, \mathrm{O}_2$.

D. Mismatching Thresholds for Lost/False Alarm

When a failure occurs, monitoring equipment able to detect this failure sends alarms to the network manager providing information on the detected misbehavior. However, some of the alarms may not be generated or may be lost, and some others may be false alarms which are not related with the failure(s) that occurred in the network. To cope with this nonideal scenario of lost and false alarms, we introduce two *alarm mismatching thresholds*, which are two parameters that reflect the reliability of the management channel and of the management functions of the equipment. They are denoted by m_1 and m_2 and give the maximum number of, respectively, lost and false alarms that are tolerated. We denote by m the total mismatching threshold, i.e., $m = m_1 + m_2$. The availability to cope with the nonideal scenario is crucial so that in any alarm combination, the human manager will get a possible failure scenario.

IV. Fault Location Algorithm

A. Inputs and Output of the Algorithm

The algorithm has the following inputs.
- The set of established channels $\mathbf{CH} = \{CH_i\}$, which is updated whenever there is a new channel established or a channel is removed.
- The set of received alarms $\mathbf{R} = \{a_i\}$ by the network manager. Every time there is a new alarm, the algorithm delivers a new result based on the updated $\mathbf{R}$. The alarms are considered to have minimal content such as the monitoring equipment that generated it and the related effect shown in Table II.
- The mismatching thresholds are m_1 and m_2 which give the number of allowed lost and false alarms, respectively.

The output of the algorithm is the network component or the smallest set of network components that, when suffering from a given failure, will cause the alarms of set $\mathbf{R}$ to go out accepting the mismatching values set by the network manager. Although the ideal scenario would be to present to the network manager a single network element as the faulty candidate, this is not realistic. The reason is that the monitoring equipment has some cost and placement constraints that limit the surveillance of the signal. For example, the signal dropped at an OADM traverses an amplifier, a demultiplexer, a filter and after the receiver the BER of the signal is monitored. Between these network elements it is difficult to monitor the signal (due to cost and/or practical issues) and, therefore, if there is a failure in any of these components, all of them will be presented as faulty candidates and, therefore, the cardinality of the resulting set of faulty candidates is not 1.

B. Algorithm Description

The transparent failure location algorithm (TFLA) scheme is shown in Fig. 2 and the pseudocode is presented in the Appendix. The target of the TFLA developed in this paper is to minimize the computation time required to give the results to the human manager when receiving alarms. The goal was achieved by building a binary tree based on the established channels and the network components so that when alarms are received the tree should simply be traversed.

While the TFLA algorithm developed in this paper uses some of the ideas presented in [7] for locating single and multiple faults in opaque optical networks, it involves a new network model and problem formulation, already presented in the previous section. The new network model focuses on transparent networks and their vulnerability, easy propagation and difficult detection of failures. Apart from the failure diagnosis, a new module that proposes an optimal placement of new monitoring equipment, from the failure location point of view has been included.

The TFLA has two main parts: A precomputation phase (PCP) and a core phase (CP); and a third monitoring equipment placement phase (MEPP) that is a particular extension of the algorithm that proposed optimal placement of new monitoring equipment (further explained in Section IV-C). The PCP gathers most of the complexity of the algorithm so that the CP has minimum complexity in order to deliver the TFLA result as fast as possible. Another advantage is that the PCP part is executed only when there is a change on the set of established channels $\mathbf{CH} = \{CH_i\}$, not when the alarms are received which minimizes the time the algorithm needs to deliver results to the human manager. The multiple fault location problem has been shown to be NP-complete already in the ideal scenario [2]. Nevertheless, the size of the computation that has to be carried out when a new alarm reaches the manager has been kept small despite the potentially large size of the network, as in the herein proposed algorithm.

This section describes how the algorithm works together with a simple example shown in Fig. 3. Based on the set of established channels $\mathbf{CH} = \{CH_i\}$ and the mismatching thresholds m_1 and m_2 set by the manager, the PCP is executed.

- ***Compute domains***: In this phase the four domains presented in Section III-C are computed for all the optical components of the established channels. Hence, at the end of this module, *PDomain*(*comp*),

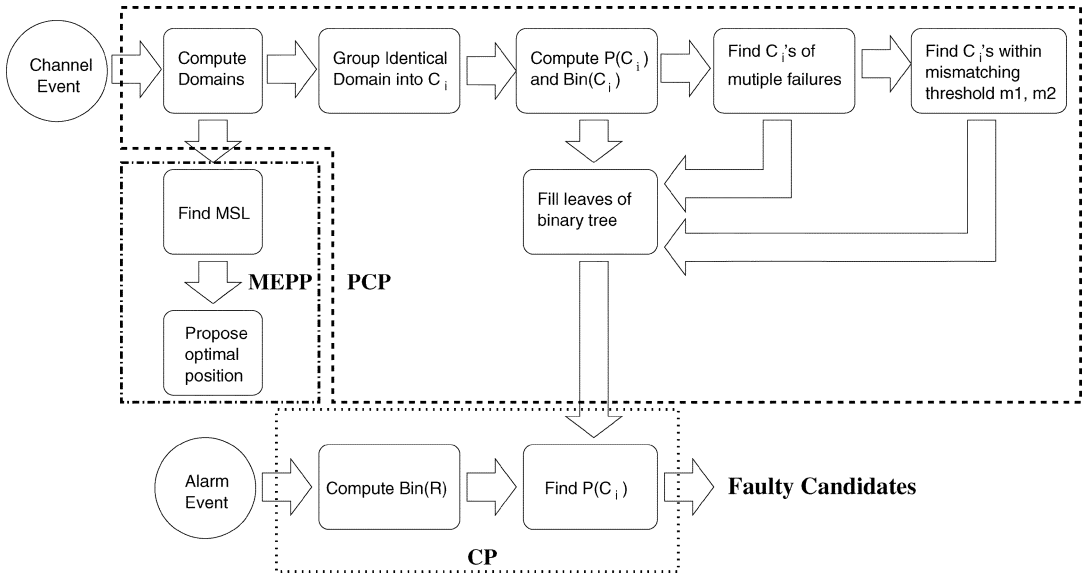

Fig. 2. Transparent failure location algorithm (TFLA) scheme. The PCP builds the binary tree, the CP traverses the tree based on the received alarms. The MEPP performs optimal placement of new monitoring equipment.

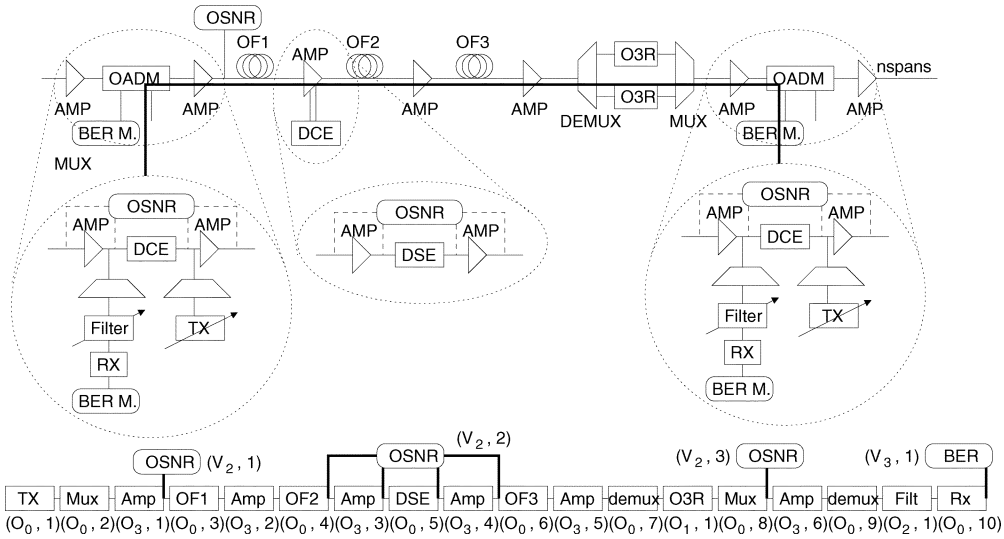

Fig. 3. Example of the modeling of a single connection between two OADMs of a ring with three fiber spans and optical regeneration. Each OADM consists of a preamplifier and postamplifier and a dispersion compensator equalizer (DCE); a demultiplexer, a tunable filter, and a receiver to drop the desired signal; a tunable transmitter and a multiplexer to add the signal; and optical signal-to-noise ratio (OSNR) and BER monitors. Each pair of OADM is interconnected by several optical fiber (OF) spans which may include optical regeneration (O3R) and dispersion suppression (DSE).

MDomain(*comp*), *IBJDomain*(*comp*), and *OBJDomain*(*comp*) are found for $\forall comp \in \mathbf{O}$. Each of these domains are sets of monitoring equipment and can be expressed as $\{v_i \in \mathbf{V}\}$. In our example, some domains are: $IBJDomain(\mathrm{O}_0, 9) = \{(V_3, 1)\}$, $IBJDomain(\mathrm{O}_3, 6) = \{(V_3, 1)\}$, $IBJDomain(\mathrm{O}_3, 5) = \mathrm{null}$ (since the O3R has IBJ suppression capabilities), $OBJDomain(\mathrm{O}_0, 4) = \{(V_2, 2)\}$, etc.

- ***Group identical domains into C_i***: This module groups equal sets obtained at the previous module into equivalent classes $C_1, C_2, \ldots, C_m$ with $m < 4n$ (with n being the cardinality of $\mathbf{V}$). In our example, we could group all the domains equal to $\{(V_3, 1)\}$, into C_1, the domains equal to $\{(V_2, 2)\}$, into C_2, etc.
- ***Associate binary vectors to each C_i***: Based on an ordered list of the monitoring equipment, a binary vector can be associated to each class: $Bin(C_i)$. Hence, the size of the binary vectors is the total number of monitoring equipment in the established channels. The jth component of $Bin(C_i)$ is equal to 1 if the associated monitoring equipment belongs to C_i and to 0, otherwise. In our example, $Bin(C_1) = (0001)$, $Bin(C_2) = (0100)$, etc.
- ***Find $Bin(C_i)$ associated to multiple failures***: Considering the case where two failures may happen in a short interval of time, the alarms related to both failures arrive intermingled to the manager and the algorithm should be able to cope with this. In this case, the domains of simultaneous failures should be computed which is equivalent to computing the union of each single failure domain,

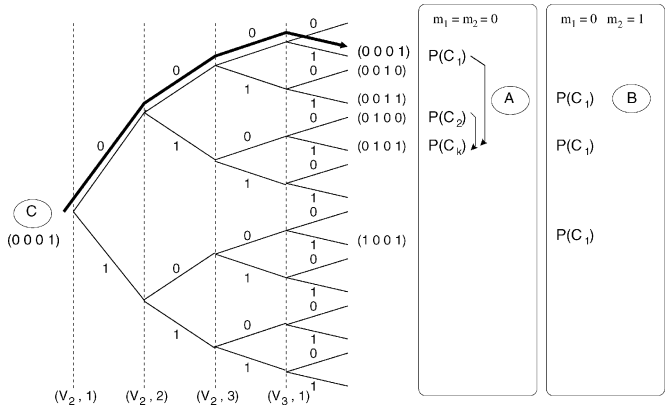

Fig. 4. Binary tree of the example with four monitoring equipment [(V_2,1), (V_2,2), (V_2,3), (V_3,1)] and some of the binary vectors. Step A shows how in an ideal scenario with no false or lost alarms ($m_1 = m_2 = 0$) the binary vector of a double failure is computed. Step B shows how the binary vectors associated to a failure scenario are computed when accepting 0 lost alarms ($m_1 = 0$) and one false alarm ($m_2 = 1$). Finally, step C shows how to traverse the tree when receiving an alarm from (V_3,1).

and which at the same time is equivalent to computing $Bin(C_k) = Bin(C_i \cup C_j) = Bin(C_i) \vee Bin(C_j)$, where $\vee$ stands for the point-wise OR operation. If $Bin(C_k)$ is equal to the binary vector associated to single failures, we can discard it if we assume that one failure is more likely than two failures. Hence, we will keep only the $Bin(C_k)$ different from the ones associated with single failures. In our example, $Bin(C_k) = Bin(C_1) \vee Bin(C_2) = (0\,1\,0\,1)$.

- ***Store the sets $P(C_i)$***: The set $P(C_i)$ refers to the set of elements (single failure scenario) or set of pair of elements (multiple failure scenario) with their j-*domain* that are associated with C_i (j-*domain* being *PDomain, MDomain, IBJDomain*, or *OBJDomain*). In other words, $P(C_i) = \{comp \in V | j\text{-}domain(comp) = C_i\}$ for single failures or

$$P(C_i) = \{(comp_k, j)(comp_l, m) | j\text{-}domain(comp_k) \cup m\text{-}domain(comp_l) = C_i\}$$

for multiple failures. In our example, $P(C_1) = \{IBJ(\mathrm{O}_3, 6), IBJ(\mathrm{O}_0, 9) \ldots\}$.

- ***Build a binary tree***: A binary tree is built with a depth equal to the number of monitoring equipment. The leaves corresponding to $Bin(C_i)$ following the path from the root to the leaves, point to the associated set $P(C_i)$. In our case, the binary tree is shown in Fig. 4.
- ***Nonideal scenario***: The binary tree can be viewed as a particular block error-correcting code, whose codewords have the property that the logical OR of any two codewords is another codeword. One empty leaf of the tree corresponds to an erroneous word, and we should find the leaf whose codeword has a minimal Hamming distance with the empty one. This module finds the binary vectors that have a minimal distance given the mismatching thresholds m_1 and m_2. For example, for $m_1 \neq 0$ and $m_2 = 0$, we accept m_1 lost alarms, i.e., the binary vectors that fall within this margin from the correct codewords are the binary vectors having a "0" when $Bin(C_i)$ has "1" in at most m_1 positions. In our example, and considering $m_1 = 0$ and $m_2 = 1$, it means that we accept one false alarm, i.e., the binary vector (*1 0 0 1*) could be the failures of $P(C_1)$ if alarm from (V_2, *1*) was false. This is shown in step B of Fig. 4.

All these steps can be computed before receiving any alarm so that the major computational complexity is placed in this PCP phase.

The core module of the algorithm works as follows: Once the manager receives alarms from the network, denoted as the set $\mathbf{R}$, the corresponding binary vector is computed $Bin(\mathbf{R})$ (in the previous example, if an alarm is received from (V_3, *1*), the corresponding vector is (*0 0 0 1*) as shown in Fig. 4). The binary tree is traversed from the root to the leaves (step C of Fig. 4). The set pointed by the leaf $P(C_i)$ will give the component(s) with the corresponding failures that justify the received alarms $\mathbf{R}$ (in our example, at least the IBJ failure of the components (O_3, *6*) and (O_0, *9*)].

C. Optimal Placement of Monitoring Equipment

A second problem that was studied is the optimal location for new monitoring equipment. We define *optimal location* as the best-effort positioning of the monitoring equipment that minimizes the number of network elements that are candidates to have a failure; i.e., that minimizes the result given by the TFLA.

For this purpose the TFLA was extended with a new module called MEPP in Fig. 2. The MEPP works as follows.

- When computing the domains of all the optical components, we store the tuple (X_i, Y_j), where X_i is a transmitter or the first optical component right after a monitoring equipment, and Y_j is the following monitoring equipment. Let us define a segment as a pair (X_i, Y_j) and let us denote by L_{ij} the length of the segment (X_i, Y_j); i.e., the number of elements of the segment (X_i, Y_j). This number is related to the number of network components that are candidates to be faulty.
- Find the segment (X_a, Y_b) with $\max\{L_{ij}\}$ for all i, j (which is the so-called MSL, standing for maximum segment length).
- By definition, the optimal position for a new monitoring equipment will be the one that divides the series (X_a, Y_b) in two series (X_a, Y_c), and (X_{c+1}, Y_b) with L_{ac}, and L_{c+1b} as similar as possible. In this way, after including this monitoring equipment in this position, the different domains of the optical components can be recomputed and will be reduced. Hence, the network components that are candidates to be faulty will be reduced.

D. Implementation of the TFLA

This algorithm has been implemented in Java so that it can be easily integrated in Web-based management systems.

The precomputation part of the algorithm, which contains most of the complexity, should be executed when there is a change in the established channels of the network topology. On the other hand, the core part, which has a polynomial complexity, should be run periodically or any time there is a new set

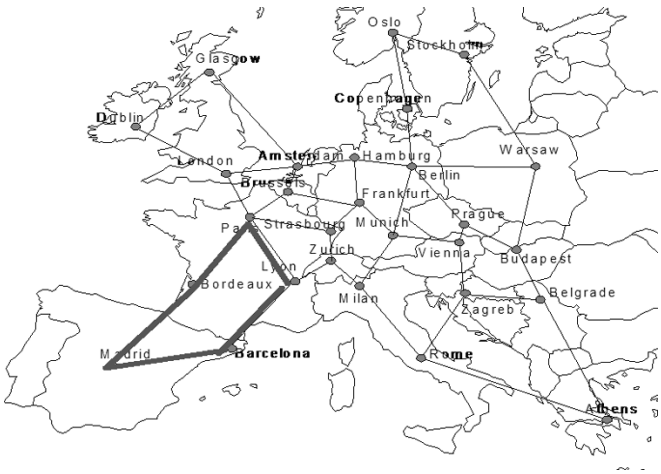

Fig. 5. Basic reference topology of the COST 266 Pan-European network with the considered transparent ring.

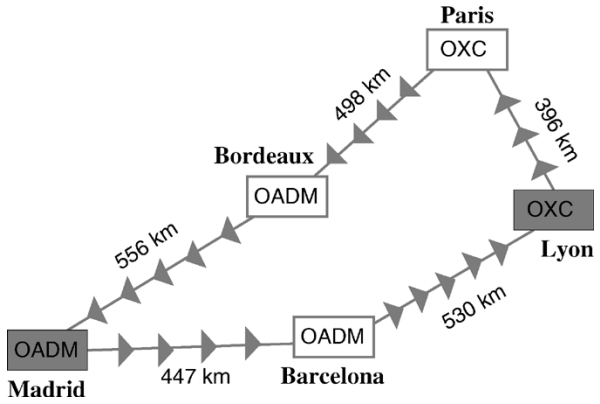

Fig. 6. Considered transparent ring including the amplifiers and the regeneration nodes needed. The number of amplifiers depends on the distance between intermediate nodes, whereas the regeneration (shown in bright color) depends on the overall ring length.

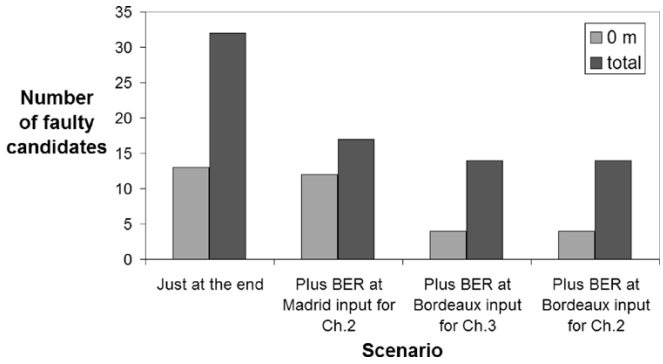

Fig. 7. Comparative graph showing the decrease of the cardinality of the set of faulty candidates when new BER monitors are included at different locations. If no mismatching is allowed (0 m) the number of faulty candidates is lower than when one lost or false alarm is allowed (total).

of received alarms. Every time the network manager identifies a fault and repairs it, the alarms related to that fault should be deleted.

The alarms that are received by the management system may contain different information such as origin of the alarm, type of alarm, time when the alarms was generated, etc. The proposed algorithm requires only the origin of the alarm and the type of alarm. The time when the alarm was generated is not used so that clock precision and synchronization are not required by the management system. Therefore, the proposed algorithm is able to cope with alarms that arrive in an intermingled manner.

V. Simulation Results

The simulations targeted two objectives: 1) the failure locating capability of the TFLA for different number and different types of monitoring equipment and 2) optimal placement of the monitoring equipment for two different scenarios: channel-based and topology-based. The former is presented in Section V-A and the latter in Section V-B.

A. Failure Location

The algorithm has been run on the Pan-European topology network [8] within a ring between Madrid, Barcelona, Lyon, Paris, and Bordeaux (Figs. 5 and 6) that is assumed to be transparent. OADMs are located at the cities of Madrid, Barcelona,and Bordeaux, whereas OXCs are located at Paris and Lyon. The architecture of OXCs and OADMs is wavelength selective [9]. The number of amplifiers needed for each link depends on the distance between the cities shown in Fig. 6. Due to the overall ring length, optical regeneration is needed in some nodes (Barcelona, Paris, and Bordeaux).

We have studied how the number of candidates to have a failure reduces based on the used monitoring equipment. Three different channels have been considered: Ch. 1 from Barcelona to Madrid, Ch. 2 from Barcelona to Bordeaux via Madrid, and Ch. 3 from Madrid to Paris via Bordeaux. Different scenarios have been tested and compared.

- Scenario 0: Initially, BER monitors have been considered at the receiver site, whereas within the channel there is other monitoring equipment (either PMs) or OSAs depending on the case).
- Scenario 1: Scenario 0 plus an extra BER monitoring of Ch. 2 is added at the input of Madrid.
- Scenario 2: Scenario 1 plus an extra BER monitoring of Ch. 3 is added at the input of Bordeaux.
- Scenario 3: Scenario 2 plus an extra BER monitoring of Ch. 2 is added at the input of Bordeaux.

Extra BER monitoring can be introduced by tapping the optical signal and selecting the channel of interest.

First, the TFLA was run for the scenario where the PMs are at the receiver side of each channel. The number of faulty candidates with new BER monitor equipment included in the channels was compared and plotted in Fig. 7. In this case, faulty candidates refer to one or several network components that when failure cause the received alarms accepting the given mismatching threshold, i.e., considering single and multiple failures. This figure shows that the number of faulty candidates when new BER monitor equipment is included in the channel, decreases depending on its location and the already existing monitoring equipment. Due to the fact that the goal is to study the impact of the monitoring equipment, we considered the particular scenario of accepting one lost alarm ($m_1 = 1$) and no false alarm ($m_2 = 0$). Hence, total mismatching threshold is equal to $m = m_1 + m_2 = 1$. The figure shows the number of

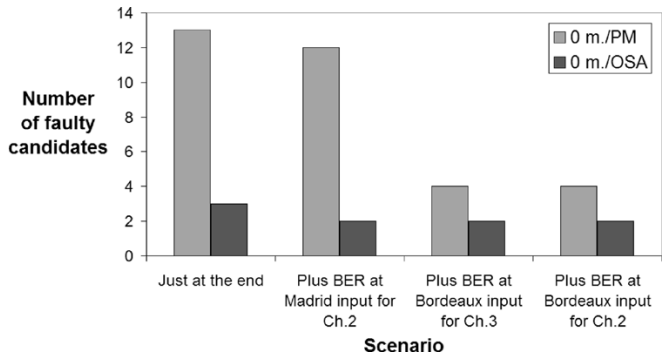

Fig. 8. Comparative graph showing the difference in the cardinality of the set of faulty candidates when power monitors (PMs) are replaced by OSAs in the four different scenarios (each scenario having one more monitoring equipment than the previous one).

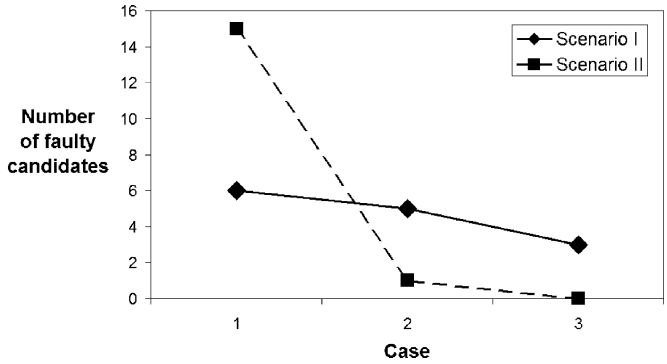

Fig. 9. Decrease in the number of optical components that are candidate to have a failure when including new monitoring equipment for two scenarios: when receiving one and two alarms at different points of the ring.

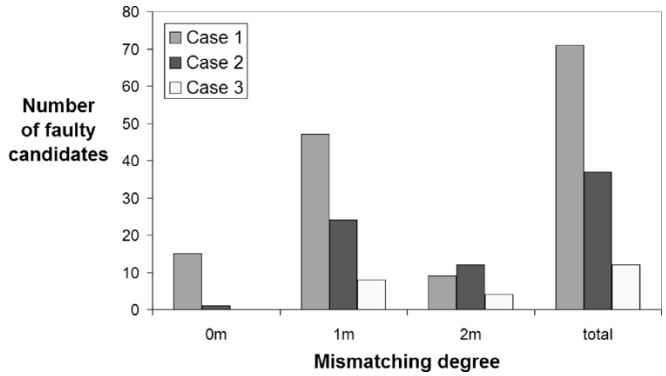

Fig. 10. Decrease of optical components that are candidates to have a failure for the three cases accepting $m = 0$, 1, or 2 lost and/or false alarms. Total shows the cardinality of the set of faulty candidates that are delivered. Although it can be observed that in this particular scenario, there are more candidates when accepting one false or lost alarms, than when accepting two, the importance of the result is based on the total number of delivered candidates.

elements that explain every received alarm (zero mismatching) and the total number of elements that cope with the given mismatching. We should clarify that the reason why the number of candidates do not reach one is because there are several network components that do not allow including monitoring equipment between them and, therefore, some of their failures cannot be distinguished. For example, at the end of the channel there is an amplifier, a demultiplexer, and a receiver and in between them no monitoring equipment is included and, therefore, the three of them will be candidates to have a failure in some scenarios.

A second study compared the variation of the number of faulty candidates when OSAs were used in the network instead of the PMs. The TFLA result, plotted in Fig. 8, shows that when using OSAs the number of elements that could have a failure decreases considerably in all the scenarios, as OSA are able to better distinguish between different failures. Therefore, this result leaves to network operators the decision to invest more (OSAs are more expensive than PMs) in order to better locate the failure (less cardinality).

B. Monitoring Equipment Optimal Location

The study of the optimal location for new monitoring equipment targets finding the location where new monitoring equipment should be placed so that it minimizes the nonmonitored areas. This study has been done either based on the connections required by the existing traffic demands ("established channels-based") or using the operator's network topology ("network topology-based"). The former depends on the traffic demands and the channels established in a certain time, whereas the latter depends on the topology independently on the demands and the established connections.

1) Established Channels Based: For long-term channels, the extended TFLA was run on the same network shown in Fig. 6. Three different channels have been considered: Ch. 1 from Barcelona to Madrid, Ch. 2 from Barcelona to Bordeaux via Madrid, and Ch. 3 from Madrid to Paris via Bordeaux (a total of 43 optical components are considered).

Three cases have been compared.

Case 1) A single monitoring equipment is installed at the end of each channel.

Case 2) One monitoring equipment is installed at the location proposed by TFLA, which is at Madrid's node.

Case 3) One new monitoring equipment (one more than Case 2) is installed at the location proposed by TFLA, which is at the output of Bordeaux's node. This proposed location is expected since the monitoring equipment that monitors the output of Ch. 2 does not monitor the quality of Ch. 3.

The TFLA was run for the three cases considering that there are no false or lost alarms. The number of optical components that could be faulty was studied for two scenarios.

- Scenario I: when receiving an alarm from the receiver for the channel dropped at Bordeaux.
- Scenario II: when receiving two alarms issued by the monitoring equipment located when dropping Ch. 1 at Madrid and Ch. 2 at Bordeaux.

Fig. 9 shows how the number of optical components that are delivered as candidate to have a failure is dropped when two extra monitoring equipment are installed.

Observe that for Case 3 and Scenario II there are no optical components delivered, which means that either there has been lost and/or false alarms. In our next study, plotted in Fig. 10, we compared the results for a mismatching threshold (i.e., false and lost alarms) equal to 0, 1 or 2. In particular, for Case 3 and Scenario II, we see that solution is given when at least one lost or false alarm is accepted. Fig. 10 shows the decrease of number

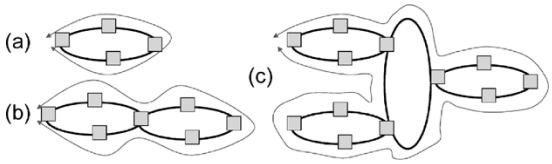

Fig. 11. Example of different ring topologies (a) single ring, (b) double ring, and (c) triple ring with the longest channel.

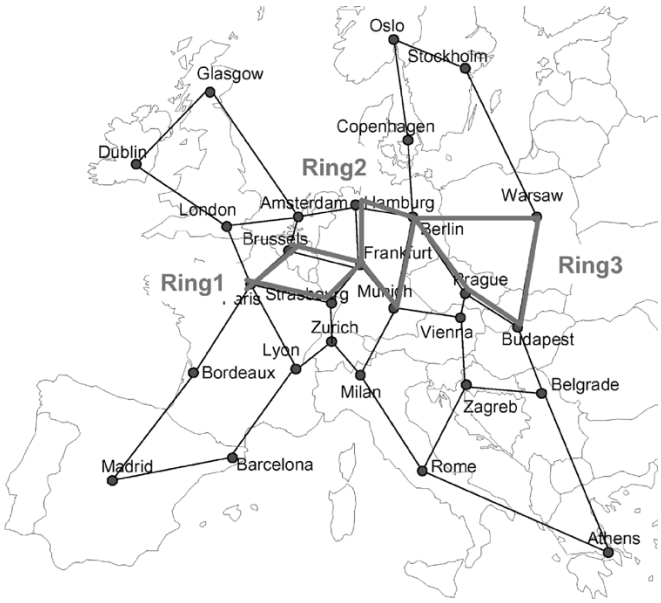

Fig. 12. Pan-European network with three rings.

of candidates when new monitoring equipment is installed in the places proposed by TFLA.

2) Topology-Based: The previous work shows the improvement on the failure location when new monitoring equipment is located with the proposed TFLA based on the established channels. However, network operators may be more interested in the location of new monitoring equipment based on the *network topology* rather than the channel-based approach. The reason is that the established channels are not fixed and may change with time and, hence, if we had optimized the monitoring equipment location for a particular set of established channels, it will not be optimal if the set changes.

The proposed TFLA could be used for any topology if we are able to find the longest channel that can be established in the given topology. For example, when studying ring topologies it can be done, as shown in Fig. 11. Based on this idea, we simulated the rings highlighted in Fig. 12. The fiber lengths in kilometers between the cities belonging to the rings are given in Table III. Fiber spans have been assumed to be 100 km long.

Three scenarios, the schemes presented in Fig. 11, have been tested.

- Scenario 1: Single ring (Ring 1 in Fig. 12).
  Paris – 4 spans – Brussels – 5 spans – Frankfurt – 3 spans – Strasbourg – 6 spans – Paris.

  In this scenario, there are 57 network elements. Initially, only one monitoring equipment is considered and, hence, all the optical components will be candidates to have a failure. Fig. 13 shows the decrease of the number of candidates when new monitoring equipment is added in the positions predicted by the algorithm. After having added four monitoring equipment, the number of candidates has decreased to 1/4 of the candidates delivered when having a single monitoring equipment.
- Scenario 2: Double ring (Ring 1 and Ring 2 in Fig. 12).
  Paris – 4 spans – Brussels – 5 spans – Frankfurt – 6 spans – Hamburg – 4 spans – Berlin – 8 spans – Munich – 5 spans – Frankfurt – 3 spans – Strasbourg – 6 spans – Paris.

  In this scenario, there are 119 optical components. Again, no monitoring equipment has been considered within the ring and, therefore, the maximum segment length is the total number of components. In order to decrease to 1/4, Fig. 13 shows that three monitoring equipment should be installed.
- Scenario 3: Triple ring: Ring 1 and Ring 3 interconnected through Ring 2.
  Paris – 4 spans – Brussels – 5 spans – Frankfurt – 6 spans – Hamburg – 4 spans – Berlin – 8 spans – Warsaw – 9 spans – Budapest – 7 spans – Prague – 5 spans – Berlin – 8 spans – Munich – 5 spans – Frankfurt – 3 spans – Strasbourg – 6 spans – Paris.

  In this scenario, there are 193 optical components. Again, no monitoring equipment has been considered within the ring. Fig. 13 confirms that to decrease the maximum segment length to 1/4 of its initial value, we should install three monitoring equipment, and to decrease it to 1/8 of its initial value, we should install seven monitoring equipment.

In general, the problem of minimizing the maximum segment size is a partition problem with rate 2. For all these scenarios with n rings, in order to decrease the maximum segment length to $1/2^n$ of its original value, $2^n - 1$ monitoring equipment

TABLE III
FIBER LENGTHS BETWEEN THE CITIES OF THE RINGS SHOWN IN FIG. 12

Frankfurt-Munich	456	Paris-Brussels	393	Paris-Strasburg	600
Munich-Berlin	757	Berlin-Prague	420	Strasburg-Frankfurt	271
Budapest-Warsaw	819	Prague-Budapest	668	Brussels-Frankfurt	474
Warsaw-Berlin	775	Berlin-Hamburg	381	Frankfurt-Hamburg	592

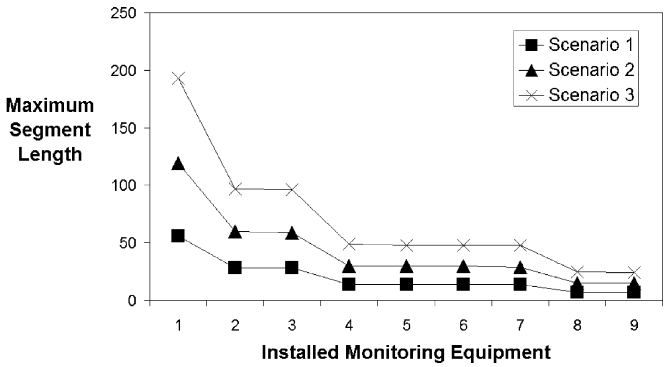

Fig. 13. Decrease of the maximum segment length as a function of the installed monitoring equipment. This segment length is directly related to the size of domains for different failures of optical components.

should be installed (the location is given by the extended TFLA and it is in the middle of the longest segment).

VI. Conclusion

In this paper, we have investigated general failure management issues in transparent optical networks such as the kind of failures that may occur, how they can be detected, how they affect other connections, etc. A failure location algorithm for transparent optical networks has been described. This algorithm concentrates most of its complexity in a precomputational phase so that when alarms are issued, the algorithm only deals with the traversing of a binary tree. The algorithm can cope with four types of failures: power, wavelength misalignment, IBJ, and out-band jamming. The algorithm has also been extended to find the best location for new monitoring equipment so that failures can be more precisely identified. The algorithm has been run on a Pan-European network and it has been shown that the number of faulty candidates decreases when one adds new monitoring equipment in the location(s) predicted by the algorithm. This study was done with two different approaches: one based on the established channels, which depend on the traffic demands; and a second approach based on the network topology.

Appendix

```
TFLA pseudocode
//single failure and ideal scenario
k = 1; C = null(C_0); MSL = null
For each established channel CH_k = {comp_i}
 i = 1;
 For each comp_i of CH_k
  Compute or Update(if comp_i ∈ CH_j with
  j < k) PDomain(comp_i)
   if found a segment longer than MSL
    update MSL
   if PDomain(comp_i) = C_a ∈ C_n
    update P(C_a)
   else
    include C_{n+1} = PDomain(comp_i)
    compute P(C_{n+1})
  Compute or Update(if comp_i ∈ CH_j with
  j < k) IBJDomain(comp_i)
    if found a segment longer than MSL
    update MSL
   if IBJDomain(comp_i) = C_a ∈ C_n
    update P(C_a)
   else
    include C_{n+1} = IBJDomain(comp_i)
    compute P(C_{n+1})
  Compute or Update(if comp_i ∈ CH_j
  with j < k) OBJDomain(comp_i)
    if found a segment longer than MSL
    update MSL
   if OBJDomain(comp_i) = C_a ∈ C_n
    update P(C_a)
   else
    include C_{n+1} = OBJDomain(comp_i)
    compute P(C_{n+1})
  Compute or Update(if comp_i ∈ CH_j with
  j < k) MDomain(comp_i)
    if found a segment longer than MSL
    update MSL
   if MDomain(comp_i) = C_a ∈ C_n
    update P(C_a)
   else
    include C_{n+1} = MDomain(comp_i)
    compute P(C_{n+1})
 i++;
k++;
Find binary vectors for each C_a ∈ C_n :
: Bin(C_a)
Fill leaves of binary tree with P(C_a)
Propose location of new equipment based on
MSL.


// Multiple failures scenario
i = 2;
while new binary vectors are found
 if (i == 2)
  for all Bin(C_a) and Bin(C_b) ≠ Bin(C_a)
   if Bin(C_c) = Bin(C_a) OR Bin(C_b) is a new
    vector
    update P(C_c)
    fill new leaf with P(C_c)
   else
    update existing P(C_c)
 if (i == 3)
  for all Bin(C_a), Bin(C_b) ≠ Bin(C_a) and
  Bin(C_c) ≠ Bin(C_a), Bin(C_b)
   if Bin(C_d) = Bin(C_a) OR Bin(C_b) OR Bin(C_c)
   is a new vector
    update P(C_d)
    fill new leaf with P(C_d)
   else
    update existing P(C_d)
 i++;


// nonideal scenario coping with m1 lost
alarms and m2 false alarms
for each Bin(C_a)
 find binary vectors BinV where
  Bin(C_a) XOR BinV has a number of
  ones ≤ m1+m2
  if BinV has at most m1 zeros at the
   positions where Bin(C_a) has ones,
   and has at most m2 ones at the
   positions where Bin(C_a) has zeros then
   include P(C_a) at branch BinV of binary
   tree.


//Core Phase
When alarms R are received
Compute Bin(R)
Traverse the binary tree and find the
 associated P(C)s.
```

```
Return to the manager the network
 components that are candidates to
 have a failure with their failure (either
 P, IBJ, OBJ, or M).
```

ACKNOWLEDGMENT

The authors would like to acknowledge the constructive comments of the reviewers that helped to improve the presentation of this paper.

REFERENCES

[1] M. Medard, S. R. Chinn, and P. Saengudomlert, "Node wrappers for QoS monitoring in transparent optical nodes," *J. High Speed Netw.*, vol. 10, pp. 247–268, 2001.

[2] N. S. V. Rao, "Computational complexity issues in operative diagnosis of graph-based systems," *IEEE Trans. Comput.*, vol. 42, pp. 447–457, Apr. 1993.

[3] R. Habel, K. Roberts, A. Solheim, and J. Harley, "Optical domain performance monitoring," in *Proc. Optical Fiber Commun. Conf.*, vol. 2, 2000, pp. 174–175.

[4] S. K. Shin, K. J. Park, and Y. C. Chung, "A novel optical signal-to-noise ratio monitoring technique for WDM networks," in *Proc. Opt. Fiber Commun. Conf. OFC*, Baltimore, MD, Mar. 2000, pp. 182–184.

[5] K. Mueller *et al.*, "Application of amplitude histograms for quality of service measurements of optical channels and fault identification," in *Proc. ECOC*, Madrid, Spain, Sep. 1998, pp. 707–708.

[6] I. Shake, H. Takara, S. Kawanishi, and Y. Yamabayashi, "Optical signal quality monitoring method based on optical sampling," *Electron. Lett.*, vol. 34, no. 22, p. 2152, Oct. 1998.

[7] C. Mas and P. Thiran, "An efficient algorithm for locating soft and hard failures in WDM networks," *IEEE J. Sel. Areas Commun. (Special Issue on Protocols and Architectures for Next-Generation WDM Optical Networks)*, vol. 18, pp. 1900–1911, Oct. 2000.

[8] S. De Maesschalck, C. Mauz, D. Colle, C. Gauger, T. Cinkler, F. Matera, B. Mikac, R. Inkret, and D. Schupke, "Reference scenario for a Pan-European network," COST 266 Rep., 2002.

[9] C. Mas, I. Tomkos, and O. K. Tonguz, "Optical network security: A failure management framework," in *Proc. ITCom*, Sep. 2003, pp. 230–241.

Carmen Mas (M'00) received the Telecommunications Engineering degree from the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 1995 and the Ph.D. degree from the Swiss Federal Institute of Technology, Lausanne (EPFL), Switzerland, in 2000.

In 1996, she became a Research Assistant at the Institute of Computer Communications and Applications, EPFL, where she was a Teaching Assistant in several courses and coordinated the participation in the COBNET European project implementing the management platform of an optical access network. In January 2000, she joined Intracom S.A, Greece, as Project Coordinator, where she participated and lead various tasks in several IST and Eurescom projects. In October 2002, she joined the Athens Information Technology (AIT) Center, Athens, Greece, as a Research Scientist. Since January 2004, she has been an Assistant Professor at the AIT. She is author and coauthor of more than 25 publications related to optical and mobile communications. Her research interests are related to optical network security, constrained based routing, protection and restoration, routing and signaling, and network control and management.

Dr. Mas is member of the Optical Society of America (OSA). She is member of the Technical Committee for the IEEE ICTON Conference. She has reviewed papers of the IEEE TRANSACTIONS ON NETWORKING, the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, ECOC, GLOBECOM, ICC, OFC, etc.

Ioannis Tomkos is an Associate Professor at the Athens Information Technology (AIT) Center, Athens, Greece, and an Adjunct Faculty member at Carnegie-Mellon University, Pittsburgh, PA. He serves as the Associate Dean of AIT and the Head of the High-Speed Networks and Optical Communications (NOC) Group. Previous professional positions held are with the University of Athens, as a Research Fellow (1996–1999) and with Corning Inc., as a Senior Scientist (2000–2002). He is the Chairman of the European Research Project COST 291, within which more than 25 EU University Research Centers participate. He is also a Reviewer for European research projects. He serves as a chairman or member of several technical program committees for the major international conferences in the areas of telecommunications/networking. He has coauthored over 100 articles, published in international journals and conference proceedings. He holds two patents.

Dr. Tomkos serves as the Vice-Chair of the International Optical Networking Technical Committee of the IEEE.

Ozan K. Tonguz (S'86–M'00) was born in Nicosia, Cyprus, in May 1960. He received the B.Sc. degree from the University of Essex, Colchester, U.K., in 1980, and the M.Sc. and Ph.D. degrees from Rutgers University, New Brunswick, NJ, in 1986 and 1990, respectively, all in electrical engineering.

He is currently a tenured Full Professor in the Department of Electrical and Computer Engineering, Carnegie Mellon University (CMU), Pittsburgh, PA. Before joining CMU in August 2000, he was with the Electrical and Computer Engineering Department, State University of New York at Buffalo (SUNY). He joined SUNY in 1990 as an Assistant Professor, where he was granted early tenure and promoted to Associate Professor in 1995, and to Full Professor in 1998. Prior to joining academia, he was with Bell Communications Research (Bellcore) between 1988–1990, doing research in optical networks and communication systems. He is author or coauthor of more than 150 technical papers in IEEE journals and conference proceedings, his contributions in optical networks and wireless networks are internationally acclaimed. He has published in the areas of optical networks, wireless communications and networks, and high-speed networking. He is the author of *Ad Hoc Wireless Networks: A Communication-Theoretic Perspective* (New York: Wiley, 2005). He was also the architect of the "High Performance Waveform (HPW)" that was implemented in Harris RF Communications' AN/PRC-117f UHF band man-pack tactical radio. His industrial experience includes periods with Bell Communications Research, CTI, Inc., Harris RF Communications, Aria Wireless Systems, Clearwire Technologies, Nokia Networks, Asea Brown Boveri (ABB), General Motors (GM), and Intel. He currently serves as a consultant for several companies, law firms, and government agencies in U.S. and Europe in the broad area of telecommunications and networking. He is also a Co-Director (Thrust Leader) of the Center for Wireless and Broadband Networking Research, Carnegie Mellon University. More details about his research interests, research group, and publications can be found at http://www.ece.cmu.edu/~tonguz/. His current research interests are in optical networks, wireless networks and communication systems, high-speed networking, and satellite communications.

Dr. Tonguz, in addition to serving on the Technical Program Committees of several IEEE conferences (such as INFOCOM, GLOBECOM, ICC, VTC) and symposia in the area of wireless communications and optical networks, currently serves or has served as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, the *IEEE Communications Magazine*, and the IEEE JOURNAL OF LIGHTWAVE TECHNOLOGY. He was a Guest Editor of a special issue of the IEEE JOURNAL OF LIGHTWAVE TECHNOLOGY and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (Special Issue on Multiwavelength Optical Networks and Technology), published in 1996.