Failure Location in Transparent Optical Networks: The Asymmetry Between False and Missing Alarms

Hung X. Nguyen and Patrick Thiran

School of Computer and Communication Sciences, EPFL
CH-1015 Lausanne, Switzerland
{hung.nguyen, patrick.thiran}@epfl.ch

Abstract. Failure location in transparent optical networks is difficult because of corrupted alarms and the large amount of alarms that a failure can trigger. One problem that network operators often face is how to set the thresholds in monitoring devices. Setting the thresholds low results in false alarms, whereas setting them high presents the risk of missing a significant degradation in network performance because of missing alarms. In this work, we show that for a network with binary alarms (alarms are either present or not), there is an asymmetry between false and missing alarms. We prove that false alarms can be corrected in polynomial time but the correction of missing alarms is NP-hard. Because of this asymmetry between false and missing alarms, false alarms have a lesser effect on the accuracy of the diagnosis results than missing alarms do. Network operators therefore, when allowed, should set the threshold low to favor false alarms.

Keywords: Optical Networks, Network Measurements, Failure Location, Complexity Theory.

1 Introduction

Transparent optical networks (TONs), where data travels along lightpaths without any optical-to-electrical conversion, will be increasingly important in future high speed networks due to their large transmission bandwidth, lower cost and transparency to different signal formats and protocols. Similar to opaque networks, transparent optical networks are vulnerable to failures such as fiber cuts, hardware malfunctions, etc. Moreover, there are new types of failures [1] and attacks [2] that are unique to transparent optical networks, e.g. failures related to subtle changes in signal power such as optical signal-to-noise ratio, cross-talk, and Kerr effects. Since the optical signals are not regenerated as in opaque networks, failures in all optical networks are more difficult to detect and isolate without significantly affecting the overall network performance. Good fault management is therefore essential to ensure the continuous functioning of such networks. When a failure occurs at the physical layer, the lightpaths that are interrupted have to be restored as soon as possible to limit the damage and so that higher layers do not see the failure and do not start their own restoration mechanisms. In the meantime, the failure has to be located and repaired. Protection and restoration mechanisms for optical networks is an active field of research. This paper focuses on the failure location problem where the root cause of a network failure has to be identified.

Failures are located from the alarms received by the management system. A single failure can trigger many alarms from different monitors [3]. When there are two or more simultaneous failures, the alarms arrive intermingled to the management system, thus the problem of locating the failures becomes very difficult. Failures are less rare than one might expect; [4] has recently reported failure rates of 1 per year, per 300km of fiber. Submarine cables, which are vulnerable to damage from submarines, anchors and fishing gears, have to be repaired once every five weeks [5]. Markopoulou et al. reported in [6] that about 11% of the failures at the optical layer in the Sprint IP backbone are multiple failures. In real optical networks, the observation of the network state is also frequently disturbed by the presence of corrupted alarms. Corrupted alarms are those that unexpectedly arrive at the management system when they should not (false alarms) or those that do not arrive at the manager when they should (missing alarms). In Wavelength Division Multiplexing (WDM) networks, network operators have the option of trading false alarms for missing alarms or vice versa by tuning the parameters of monitoring devices. Let us illustrate the scenario by an example using the model for WDM networks in [3], shown in Figure 1. In this example, the network contains a set of optical components at the WDM layer such as optical transmitters (marked Tx in Figure 1), optical receivers (Rx), multiplexers (MUX), demultiplexers (DEMUX), add/drop filters (ADF), switches, and optical fibers (OF). Assume that in this network transmitter Tx3 sends an optical signal to Receiver Rx4, but that the laser is slightly detuned, resulting in a shifted emitted wavelength. The quality of the signal will be degraded because of interferences with other wavelengths. To detect such a soft failure, the network needs to have some devices to monitor the signal quality. These monitors can be devices at the WDM layer or devices at the upper layers. For example, monitoring components at the SDH layer count the number of errored blocks over a time window of 15 minutes or 24 hours. The error counter is reset at each new time window. Whenever the number of errored blocks exceeds a threshold, an alarm ("Degraded Signal" or "Excessive Error") is sent. The threshold values recommended in the ITU standard G.806 [7] can have any value in the range $10^{-5} \dots 10^{-3}$ for Excessive Error alarms, and in the range $10^{-8} \dots 10^{-5}$ for Degraded Signal alarms. Setting the threshold high will increase the probability of missing alarms and decrease the probability of false alarms; setting the threshold low, on the contrary, will increase the probability of false alarms and decrease the probability of giving missing alarms. Similar examples can be found in most monitoring devices at the WDM layer [8].

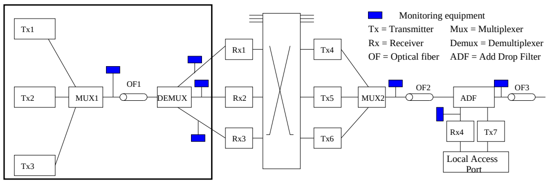


Fig. 1. Example of a WDM network with monitoring equipment using the model in [3].

1.1 Related Work

The importance of failure monitoring in optical communication networks has generated a wide body of approaches to solve it. They differ in the information they require from the monitoring tools (timestamps, failure probabilities), the way they collect this information (via passive or active monitoring), the methodology they use for making a location (expert system or case-based rules, abstract network model or black box learning), etc (see [9] for a complete review). In this paper, We use the model based approach of [3] where a transparent optical network is modelled as a directed deterministic dependency graph. The dependency relations are dictated by the established light paths in the network. There is also much research dealing with monitoring the performance of transparent optical networks. Recent progress in optical performance monitoring can be found in [8]. Other researchers, e.g. [10], have proposed to use active probes as tools to monitor and diagnose failures in transparent optical networks. A detailed survey of the existing commercial optical equipment and monitoring devices in transparent optical networks is given in [3].

Accounting for the effects of noisy alarms is a significant challenge in network failure location. Although many researchers [3, 11, 12] have suggested that failure location algorithms must be able to cope with erroneous alarms, most location algorithms today have avoided the issue of alarm uncertainty because of the complexity of covering all possible failures and all possible alarm uncertainties. A few works [3, 11, 12] in the literature incorporate missing and false alarms into fault location. In [11], Yemini et al. only consider single failures. In [12], Steinder et al. use failure probabilities of network components and the probabilities of corrupted alarms to develop a belief network to solve the failure location problem. In [3], Mas et al. develop a fault location algorithm capable of handling multiple failures and erroneous alarms in opaque optical networks without using probabilities. However, the approach in [3] requires considering all different combinations of failures and corrupted alarms in the network and therefore requires an exponential location time (or an exponential memory space).

1.2 Our Contributions

In this paper, we first mathematically formulate the failure location problem as a maximum likelihood inference problem in Section 2. We then show in Section 3 that the failure location problem is equivalent to the famous NP-hard set cover problem [13]. The benefits of proving the equivalence of the two problems are two-fold. First, the results enable us to adapt existing set cover algorithms in the literature to solve the failure location problem in optical networks. Second, linking the failure location problem to the set cover problem allows us to discover that false and missing alarms do not have equal effects on the failure location. We show in Section 4 that false alarms can be corrected in polynomial time, but that correcting missing alarms is NP-hard. The rather surprising advantage of false alarms over missing alarms, in terms of time-complexity, carries directly to the accuracy of the failure location: a polynomial time failure location algorithm is more accurate when most of the corrupted alarms are false than when most of the corrupted alarms are missing. Our studies on real network topologies in Section 5 confirm the advantages of tilting thresholds towards low values, so that corrupted alarms are rather false than missing. We conclude the paper in Section 6.

2 Network Model and Problem Setting

2.1 Network Model

Optical communication networks consist of passive optical components taking care of optical signal transmissions and of monitoring elements taking care of failure reporting [3]. A fault at an optical component not only results in faulty or abnormal behavior at that component, but can also cause the faulty component to transmit abnormal signals to other components. This manifestation is called fault propagation. Monitoring devices are used to detect abnormal transmitted signals [8]. A fault at one component can cause multiple monitors at various points in the network to ring alarms [3]. Failures of monitoring devices can result in corrupted alarm but do not interfere with the signal transmission.

Specifically, we model the network by a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ where each node $v \in \mathcal{V}$ of the graph represents an optical component, and the directed edge $(u, v) \in \mathcal{E}$ represents the fact that a faulty signal can be sent directly from u to v. The faulty signal that propagates from a node u to a node v does not cause v to be faulty. However, it may propagate further from v to other nodes directly connected to v, and so on. The signal propagation, and hence the fault propagation of the network, is determined by a set of channels, where each channel is equivalent to an established lightpath in the network. A fault at one node in a channel will propagate to all other nodes that follow it on the channel. We denote by $\mathcal{C}$ the set of optical components and by $\mathcal{M}$ the set of monitors. The *domain* of an optical component $v \in \mathcal{V}$, $Domain(v)$, is defined as the set of monitors that will ring alarms when v fails. Let us also denote the set of all ringing monitors by $\mathcal{M}_R \subseteq \mathcal{M}$ and the set of all silent monitors by $\mathcal{M}_S = \mathcal{M} \backslash \mathcal{M}_R$. For a subset $\mathcal{C}'$ of $\mathcal{C}$, we call $\mathcal{M}_{\mathcal{A}}(\mathcal{C}')$ the alarms that should be fired when all components of $\mathcal{C}'$ fail, i.e., $\mathcal{M}_{\mathcal{A}}(\mathcal{C}') = \bigcup_{c \in \mathcal{C}'} Domain(c)$, if all alarms are perfect. If some of the alarms are corrupted, i.e., provide wrong information, $\mathcal{M}_{\mathcal{A}}(\mathcal{C}') \neq \mathcal{M}_R$. The set of false alarms when all components of $\mathcal{C}'$ are diagnosed as faulty is given by $\mathcal{M}_F(\mathcal{C}') = \mathcal{M}_R \backslash \mathcal{M}_A(\mathcal{C}')$. Similarly, the set of missing alarms when all components of $\mathcal{C}'$ are diagnosed as faulty is given by $\mathcal{M}_M(\mathcal{C}') = \mathcal{M}_S \cap \mathcal{M}_A(\mathcal{C}')$.

2.2 Problem setting

A location algorithm needs to determine the root cause of a system disorder based on the observed alarms by returning the most probable explanation(s) for the observed alarms to the network manager. Given the set of ringing alarms $\mathcal{M}_R$ and the set of silent alarms $\mathcal{M}_S$, the solution to a failure location problem is a set of components $\mathcal{C}'$ that maximizes the likelihood of occurrence of $\mathcal{C}'$. The maximum likelihood failure location problem is best explained in term of probabilities as

$$\max_{\mathcal{C}' \subseteq \mathcal{C}} Prob(\mathcal{C}' | \mathcal{M}_R, \mathcal{M}_S) = \max_{\mathcal{C}' \subseteq \mathcal{C}} Prob(\mathcal{M}_R, \mathcal{M}_S | \mathcal{C}') Prob(\mathcal{C}') / Prob(\mathcal{M}_R, \mathcal{M}_S). \tag{1}$$

Denoting by $|\mathcal{C}|$ the cardinality of the set $\mathcal{C}$, if we assume that all optical components can fail with the same probability p independently of each other, that a monitor can give a missing alarm with probability p_m and a false alarm with probability p_f, then $Prob(\mathcal{C}') = p^{|\mathcal{C}'|}(1-p)^{|\mathcal{C}|-|\mathcal{C}'|}$ and $Prob(\mathcal{M}_R, \mathcal{M}_S | \mathcal{C}') = p_f^{|\mathcal{M}_F(\mathcal{C}')|}(1-p_f)^{|\mathcal{M}_S|-|\mathcal{M}_M(\mathcal{C}')|} p_m^{|\mathcal{M}_M(\mathcal{C}')|}(1 -$

$p_m)^{|\mathcal{M}_R|-|\mathcal{M}_F(\mathcal{C}')|}$. In the formula for $Prob(\mathcal{M}_R, \mathcal{M}_S|\mathcal{C}')$, the first term $p_f^{|\mathcal{M}_F(\mathcal{C}')|}$ comes from false alarms, the second term $(1-p_f)^{|\mathcal{M}_S|-|\mathcal{M}_M(\mathcal{C}')|}$ from the silent monitors that are not missing alarms, the third term $p_m^{|\mathcal{M}_M(\mathcal{C}')|}$ from missing alarms and the last term $(1-p_m)^{|\mathcal{M}_R|-|\mathcal{M}_F(\mathcal{C}')|}$ from ringing monitors that are not false alarms. We have made the implicit assumptions that given the set of faulty optical components $\mathcal{C}'$ the alarm status of monitoring devices are conditionally independent.

The probabilities p, p_m and p_f are difficult to obtain and are generally not available in practice. Therefore, the maximization problem in (1) cannot be solved analytically as is and requires some approximations. We propose a heuristic to solve the maximization problem in (1) by first minimizing the number of corrupted alarms $|\mathcal{M}_M(\mathcal{C}')| + |\mathcal{M}_F(\mathcal{C}')|$ and then minimizing the number of failures $|\mathcal{C}'|$. In other words, the failure location problem can be separated into two steps. The first step is to identify and correct corrupted alarms, which we call the Error Correction (EC) problem. The second step is to identify the failures, which we call the Multiple Fault (MFAULT) location problem, without corrupted alarms. For a logical development of the paper, we first present the MFAULT problem in Section 3 and then present the EC problem in Section 4.

3 The Failure Location Problem With Perfect Alarms

In this section, we study the failure location problem in the ideal scenario where there are no corrupted alarms. The objective of the MFAULT problem is to cover all ringing alarms but not silent alarms with the smallest number of failure candidates. The MFAULT problem can be formulated as follows. We want to find a subset $\mathcal{C}'$ of $\mathcal{C}$ such that the number of failures $|\mathcal{C}'|$ is minimized and there are no false alarms, which we can write as

$$\mathcal{M}_F(\mathcal{C}') = \emptyset, \tag{2}$$

and no missing alarm, which is to say that

$$\mathcal{M}_M(\mathcal{C}') = \emptyset. \tag{3}$$

The MFAULT is equivalent to the famous set cover problem (SC) [15]. The SC problem is a known NP-complete problem and can be defined as follows [13]: Given a finite set $\mathcal{S}$, a collection $\mathcal{X}$ of subsets of $\mathcal{S}$, we need to determine a subset $\mathcal{X}' \subseteq \mathcal{X}$ such that $|\mathcal{X}'|$ is minimized and $\bigcup_{X\in\mathcal{X}'} X = \mathcal{S}$.

Theorem 1. *Any instance of the MFAULT problem can be mapped into an instance of the SC problem and vice versa.*

The MFAULT problem therefore is NP-complete. In optical networks, failure location needs to be fast so that repair actions can be done swiftly. For this reason, we choose to adapt the greedy approximation algorithm for the set cover problem [14] to solve the MFAULT problem. This algorithm is fast and yet is the best polynomial time approximation algorithm for the SC problem (and hence the MFAULT problem) in terms of the worst case performance. The MFAULT approximation algorithm presented below is a greedy algorithm that chooses at each iteration the failure candidate whose domain contains the largest number of ringing alarms.

The MFAULT algorithm

- *Step 1*: Initialize $\mathcal{C}'$ to an empty set: $\mathcal{C}' = \emptyset$.
- *Step 2*: While $\mathcal{M}_R \neq \emptyset$
  1. Find a component $c \in \mathcal{C}$ and $\mathit{Domain}(c) \subseteq \mathcal{M}_R$ that minimizes $|\mathcal{M}_R \setminus \mathit{Domain}(c)|$.
  2. Add c to the solution $\mathcal{C}'$, $\mathcal{C}' = \mathcal{C}' \cup \{c\}$.
  3. Update the sets: $\mathcal{M}_R = \mathcal{M}_R \setminus \mathit{Domain}(c)$ and $\mathit{Domain}(c_i) = \mathit{Domain}(c_i) \setminus \mathit{Domain}(c)$ for all $c_i \in \mathcal{C}$.
- *Step 3*: Output $\mathcal{C}'$.

4 The Failure Location Problem with Corrupted Alarms

The task of failure location is more difficult when there are corrupted alarms as in this case it amounts to both correcting the corrupted alarms and localizing the faulty components. In this section, we only address the Error Correction (EC) problem that amounts to finding a set of components $\mathcal{F}_D \subseteq \mathcal{C}$ that minimizes the number of corrupted alarms $|\mathcal{M}_F(\mathcal{F}_D)|+|\mathcal{M}_M(\mathcal{F}_D)|$. Once the identified corrupted alarms are corrected, the MFAULT problem of Section 3 is solved and the minimal set of faulty components is located.

4.1 When There Are Only False Alarms

When there are false alarms only, which corresponds to the scenario where threshold values in monitoring devices are set low, the error correction problem can be stated as follows. Given a set of ringing alarms $\mathcal{M}_R$, some of them may be false alarms, we need to determine a set of network components $\mathcal{F}_D \subseteq \mathcal{C}$ whose failures would minimize the number of false alarms $|\mathcal{M}_F(\mathcal{F}_\mathcal{D})|$ and satisfy Condition (3), i.e., $\mathcal{M}_M(\mathcal{F}_\mathcal{D}) = \emptyset$. Condition (3) guarantees that there are no missing alarms. We call this problem the False Alarm (*FALARM*) problem. The FALARM problem can be solved in *polynomial time* by the following FALARM algorithm, which returns a set of identified false alarms $\mathcal{M}_F(\mathcal{F}_D)$.

The FALARM algorithm

- *Step 1*: Initialize $\mathcal{F}_D$ to an empty set: $\mathcal{F}_D = \emptyset$.
- *Step 2*: Loop through all nodes in $c \in \mathcal{C}$ and check the condition $\mathit{Domain}(c) \subseteq \mathcal{M}_R$. If this condition is satisfied for c, then add c to $\mathcal{F}_D$.
- *Step 3*: Output $\mathcal{M}_F(\mathcal{F}_D)$.

We now prove that the above algorithm works correctly. Step 2 ensures that $\mathcal{F}_D$ verifies Condition (3), and thus that there is no missing alarm. By construction, Step 2 also implies that $\mathcal{F}_D$ is the largest subset of $\mathcal{C}$ that satisfies (3), as otherwise there would be a node c', $c' \notin \mathcal{F}_D$ with $\mathit{Domain}(c') \cap \mathcal{M}_S = \emptyset$ because of (3), which would in turn imply that $\mathit{Domain}(c') \subseteq \mathcal{M} \backslash \mathcal{M}_S = \mathcal{M}_R$, a contradiction. Consequently any feasible solution $\mathcal{U}$ of the FALARM problem must be a subset of $\mathcal{F}_D$, whence

$$\mathcal{M}_\mathcal{A}(\mathcal{U}) = \bigcup_{c \in \mathcal{U}} \mathit{Domain}(c) \subseteq \bigcup_{c \in \mathcal{F}_D} \mathit{Domain}(c) = \mathcal{M}_A(\mathcal{F}_D)$$

and thus $\mathcal{M}_F(\mathcal{F}_D) \subseteq \mathcal{M}_F(\mathcal{U})$. This shows that $\mathcal{F}_D$ is the set of nodes whose failures give the least number of false alarms, and justifies the answer in Step 3.

4.2 When There Are Only Missing Alarms

We now consider the dual case where there are only missing alarms. This scenario happens when threshold values in monitoring devices are set high. In this case, we need to determine a set of network components $\mathcal{F}_D \subseteq \mathcal{C}$ whose failures would produce the smallest set of missing alarms, i.e., minimizes $|\mathcal{M}_M(\mathcal{F}_\mathcal{D})|$ and satisfies Condition (2), i.e., $\mathcal{M}_F(\mathcal{F}_\mathcal{D}) = \emptyset$. Condition (2) is to guarantee that there are no false alarms.

We call this problem the Missing Alarm (*MALARM*) problem. The MALARM problem can be shown to be NP-complete by a reduction from the the red-blue set cover problem [16]. The red-blue set cover problem is defined as follows. Given a finite set $\mathcal{S}$, which contains two disjoint subsets $\mathcal{R}$ and $\mathcal{B}$ ($\mathcal{R} \cup \mathcal{B} = \mathcal{S}$ and $\mathcal{R} \cap \mathcal{B} = \emptyset$) and a collection $\mathcal{X}$ of subsets of $\mathcal{S}$, we need to determine a subset $\mathcal{X}' \subseteq \mathcal{X}$, such that every element of $\mathcal{B}$ belongs to at least one member of $\mathcal{X}'$ and the number of elements of $\mathcal{R}$ that are covered by members of $\mathcal{X}'$ is minimized. The proof is given in [15].

4.3 Approximation algorithm for the error correction problem

In real networks, one can never be sure that the corrupted alarms are only false or only missing. It is therefore important to have an algorithm for the error correction problem that works when there are both false and missing alarms. Finding an algorithm for the EC problem is not easy for the following reasons. The red-blue set cover problem is not only NP-hard, it is also much harder to approximate than the set cover problem [16]. To date, there is no known approximation algorithm with a finite bound for the red-blue set cover problem in the literature. The Error Correction (EC) algorithm below greedily tries to cover as many ringing alarms and as few silent alarms as possible at each iteration by picking a component c whose domain has the smallest number of silent monitors, i.e., c minimizes $|\mathcal{M}_S \cap Domain(c)|$. Although we cannot provide a bound on the performance of the EC algorithm, our experiments in Section 5 show that the EC algorithm performs quite well on real network topologies.

The EC algorithm

```
– Step 1:
    1. Initialize $\mathcal{F}_D$ to an empty set: $\mathcal{F}_D = \emptyset$.
    2. Calculate $\mathcal{M}_S \cap Domain(c_i)$ for each component $c_i \in \mathcal{C}$.
    3. Find $c$ that minimizes $|\mathcal{M}_S \cap Domain(c)|$.
– Step 2: While $|\mathcal{M}_R \cap Domain(c)| - |\mathcal{M}_S \cap Domain(c)| \geq 0$
    1. Add $c$ to $\mathcal{F}_D$: $\mathcal{F}_D = \mathcal{F}_D \cup \{c\}$.
    2. Update the sets: $\mathcal{M}_R = \mathcal{M}_R \backslash Domain(c)$, $\mathcal{M}_S = \mathcal{M}_S \backslash Domain(c)$ and $Domain(c_i) = Domain(c_i) \setminus Domain(c)$ for all $c_i \in \mathcal{C}$.
    3. Recalculate $\mathcal{M}_R \cap Domain(c_i)$ and $\mathcal{M}_S \cap Domain(c_i)$ for each components $c_i \in \mathcal{C}$.
    4. Find $c$ that minimizes $|\mathcal{M}_S \cap Domain(c)|$.
– Step 3: Output $\mathcal{M}_F(\mathcal{F}_\mathcal{D})$ and $\mathcal{M}_M(\mathcal{F}_\mathcal{D})$.
```

The EC algorithm has the following notable features. When all corrupted alarms are false alarms, we have $\mathcal{M}_S \cap Domain(\{c_i\}) = \emptyset$ and hence $|\mathcal{M}_R \cap Domain(c_i)| \geq |\mathcal{M}_S \cap Domain(c_i)|$ for components c_i that are faulty. Therefore, the EC algorithm is equivalent to the FALARM algorithm in the sense that it adds to the set $\mathcal{F}_D$ all the components c that satisfies the condition $Domain(c) \subseteq \mathcal{M}_R$. When all corrupted alarms are missing alarms, the EC algorithm greedily tries to minimize the number of missing alarms.

5 Experimental Evaluation

We evaluate the effectiveness of our failure location algorithms (the MFAULT and EC algorithms) in 4 benchmark network topologies [10]: NSFNET, ARPA2, Smallnet and Bellcore. We particularly evaluate the effect of false and missing alarms on the accuracy of the failure location algorithm. Due to space constraints, we only present here the results on the NSFNET topology. Similar results are obtained in other topologies. We first describe the specific parameter settings in Section 5.1 and then show the results of our evaluations in Section 5.2 and 5.3.

5.1 Simulation Settings

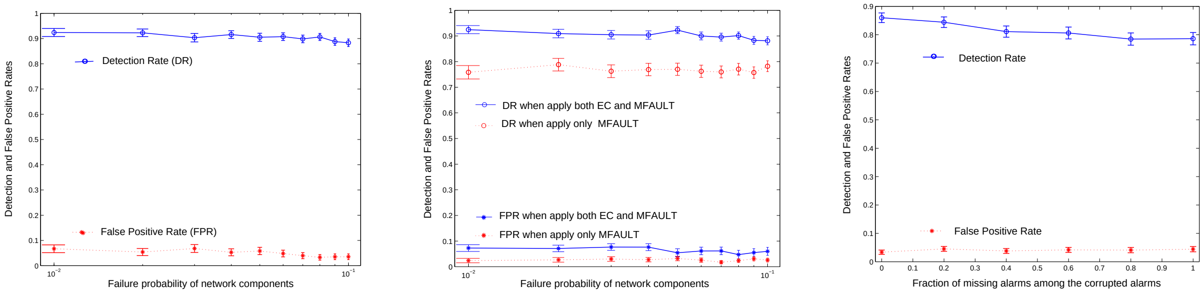
The performance of the algorithms are evaluated in terms of two metrics: the detection rate (DR), which is the percentage of components that are correctly diagnosed as faulty, and the false positive detection rate (FPR), which is the percentage of components that are working correctly but are diagnosed as being faulty. With $\mathcal{F}$ denoting the set of the actual faulty components, and $\mathcal{C}'$ the set of components identified as faulty by a location algorithm, these two rates are given by [12]:

$$\text{DR} = \frac{|\mathcal{F} \cap \mathcal{C}'|}{|\mathcal{F}|} \text{ ; FPR} = \frac{|\mathcal{C}' \backslash \mathcal{F}|}{|\mathcal{C}'|}.$$

To create plausibly realistic failure scenarios in each topology, we first fix the number of channels (lightpaths) to 10% (which is a reasonable approximation for the utilization of current optical networks) of the total number of source and destination pairs in the topology. For each channel, the source and the destination are chosen uniformly. We assume that the routing path of each channel is determined by a shortest path routing algorithm. Monitors are placed at all active input ports of network nodes, that is, ports traversed by a lightpath. To quantify the corrupted alarms, we use two metrics: the missing alarm ratios MR, i.e., the ratio of the number of generated alarms that were lost to the number of all generated alarms, and the false alarm ratio FR, i.e., the ratio of the number of false alarms to the number of all received alarms.

5.2 Effectiveness of the Failure Location Algorithm

Figure 2(a) plots the Detection Rate (DR) and False Positive Rate (FPR) when applying the EC and MFAULT algorithms to locate failures in the NSFNET topology with 20 channels when there are no corrupted alarms, i.e., $MR = 0$ and $FR = 0$. In this case, the failure location algorithm reduces to the MFAULT algorithm. We observe that the failure location algorithm achieves very accurate results with a Detection Rate above 90% and a False Positive Rate below 8%. Another interesting observation is that the DR



(a) when $MR = FR = 0$.

(b) When $MR = FR = 0.01$.

(c) When the nature of the alarms chages.

Fig. 2. Performance of the failure location algorithm on the NSFNET topology with 20 channels when there are no corrupted alarms and when there are corrupted alarms.

and FPR do not change much with the failure probability of network components. This observation suggests that our failure location algorithm performs well for small and large failure probabilities of network components.

Figure 2(b) plots the performance of the failure location algorithm when $MR, FR > 0$. To evaluate the effectiveness of the EC algorithm, we also plot the results when applying only the MFAULT algorithm in the non-ideal scenarios. We observe that when there are corrupted alarms, the EC algorithm helps improve the accuracy of the overall failure location by a large margin. The results demonstrate that even though the number of corrupted alarms is small, their effect on the failure location algorithm is substantial and cannot be neglected. Figure 3(b) also shows that in the non-ideal scenario, the False Positive Rate is higher than in the ideal scenario. This observation is explained by the fact that the EC algorithm is an approximation algorithm and its solution is not optimal.

5.3 Effect of False and Missing Alarms

We now evaluate the impact of false and missing alarms on the failure location algorithm. To compare the effect of false and missing alarms, we fix the total number of corrupted alarms, i.e., $MR + FR$ is fixed, but not the nature, i.e., MR and FR change. We run simulations on the NSFNET topology with 20 channels. The component failure probability is fixed at 0.01. The average number of monitors in this setting is 40 monitors. The average number of corrupted alarms is kept at 0.8 alarms (2% of the number of monitors). We vary the fraction of missing alarms among the corrupted alarms from 0 to 1, where 0 means there is no missing alarms and 1 means all corrupted alarms are missing alarms. The results are plotted in Figure 2(c).

We observe that as the fraction of missing alarms increases, the DR of the failure location algorithm decreases rapidly whereas the FPR does not change much. These results follow from our theoretical studies in Section 4 that when the majority of corrupted alarms are false alarms, these alarms can be corrected exactly by the EC algorithm; whereas when the majority of corrupted alarms are missing these alarms are only corrected approximately by the EC algorithm. We would like to emphasize here that the asymmetry between missing and false alarms is not an artifact of our EC algorithm. This asymmetry comes from the fact that false alarms are easier to correct than missing alarms, which we have solidly proved in Section 4.

6 Conclusions

We studied the failure location problem in transparent optical networks with noisy alarms. Is it better to have false or missing alarms? We showed that the former are preferable to the latter, both in terms of accuracy and of time complexity of the alarm correction. Quite surprisingly, false alarms can be corrected in polynomial time, but correcting missing alarms is NP-hard. We believe that network management and failure location algorithms should therefore put a strong bias in favor of false alarms over missing alarms, especially in large scale systems.

References

1. Kartalopoulos, S.V.: Fault Detectability in DWDM: Toward Higher Signal Quality and System Reliability. Wiley-IEEE Press (2001)
2. Medard, M., Marquis, D., R.A.Barry, S.G.Finn: Security issue in all-optical networks. IEEE Network **10** (1997) 42–48
3. Mas, C., Nguyen, H., Thiran, P.: Failure location in WDM networks. In: Optical WDM Networks: Past Lessons and Path Ahead. Kluwer Academic Publishers (2004)
4. De Maesschalck, S.M., et al.: Pan-european optical transport networks: an availability based comparison. Photonic Network Communication **5(3)** (May 2003) 203–225
5. Submarine Networks. FibreSystems **3** (1999) 26
6. A.Markopoulou, et al. Characterization of Failures in an IP Backbone. In: Proceedings of the IEEE INFOCOM'04. (2004)
7. I.T.U-T Rec G.806: Characteristics of Transport Equipment - Description Methodology and Generic Functionality (2000)
8. Kilper, D., et al.: Optical performance monitoring. Journal of Lightwave Technology **22** (Jan 2004) 294–304
9. Mas, C., Thiran, P.: A review on fault location methods and their application. Optical Networks Magazine **2** (2001) 1900–1911
10. Zeng H., et al.: Monitoring cycles for fault detection in meshed all-optical networks. In: Proceedings of IEEE ICPP'04. (2004)
11. Yemini, S., S.Kliger, Mozes, E., Yemini, E., Oshie, D.: High speed and robust event correlator. IEEE Communications Magazine **34** (1996) 82–90
12. Steinder, M., Sethi, A.S.: Increasing robustness of fault localization through analysis of lost, spurious, and positive symptoms. In: Proceedings of the IEEE INFOCOM, New York (2002)
13. Garey, M.R., Johnson, D.S.: Computers and Intractibility: A guide to the theory of NP-completeness. W. H. Freeman (1979)
14. Hochbaum, D., et al.: Approximation Algorithms for NP-Hard Problems. PWS Publishing Company, Boston, MA (1997)
15. lcawww.epfl.ch/nguyen/NguyenOptical05.pdf.
16. Carr, R.D., Doddi, S., Konjevod, G., Marathe, M.: On the red-blue set cover problem. In: Proceedings of Symposium on Discrete Algorithms. (2000)