

Efficient Alarm Management in Optical Networks

Sava Stanic¹, Suresh Subramaniam¹, Hongsik Choi², Gokhan Sahin¹, and Hyeong-Ah Choi²

¹Department of Electrical & Computer Engineering

²Department of Computer Science

The George Washington University

Washington, DC 20052

e-mail: {stanic,suresh,hongsik,sgokhan,choi}@seas.gwu.edu.

Abstract

As the capacity of optical transport networks increases, rapid fault identification and localization become increasingly important. These problems are more challenging than in traditional electronic networks because of optical transparency. In a transparent optical network which does not regenerate optical signals, a fault may propagate to various parts of the network from the origin, and multiple alarms can be generated for a single failure. Efficient alarm management and filtering requires a careful selection and placement of network monitoring equipment. In this paper, we survey the capabilities of current optical monitoring equipment and formulate a problem of selecting monitors to be placed throughout the network. Simulation results suggest that the number of monitors and generated alarms can be significantly reduced if monitor locations are selected judiciously.

1 Introduction

Today's optical networks are capable of carrying large amounts of data. Commercial systems have already been deployed with a per-fiber capacity of over 1.6 Terabits per second. This is equivalent to 25 million simultaneous telephone conversations. In lab settings, traffic throughputs of the order of 10 Terabits per second over a single optical fiber have been achieved. As optical network technology advances and higher bandwidth is demanded, the amount of data transmitted over a single optical fiber is expected to increase even further. Due to such high data rates, even a short service disruption may cause a large amount of data to be affected. Many different types of service disruptions occur frequently in practice. They include bending or cutting of fiber, equipment failure, and human error. Besides faults, optical networks are vulnerable to sophisticated attacks that may not be possible in electronic networks [7]. Therefore,

it is of critical importance for such networks to have fast and effective methods for identifying and locating network failures. This is especially important for the physical layer, where any physical failure should be detected, located, and corrected before it is noticed by upper layer protocols. In this paper, we use the terms fault and failure interchangeably, even though a failure may occur due to an attack on the physical infrastructure rather than faulty equipment.

Fault detection mechanisms in optical networks depend on alarms generated by different types of network monitoring equipment in response to unexpected events. Depending on the placement and capabilities of these monitoring devices, the network fault manager may receive a large number of redundant alarms for some network failures, while it may not receive any alarms for other network failures. In order for a fault detection and localization mechanism to be fast and effective, it is important to reduce the number of redundant alarms received to the smallest possible number, while providing fault detection capability over the largest possible set of network failures. This will reduce alarm processing time as well as ambiguity in fault localization. Thus, a judicious placement of network monitoring equipment is essential for fast and effective fault detection and localization.

Related work on fault diagnosis and localization include [3, 4, 5, 6, 2, 8]. The problem of identifying faults assuming that a fault propagates downstream on all lightpaths from the point of fault origin is considered in [2, 3, 4, 5]. In [2], a central manager is assumed, and an algorithm for single fault identification is presented. The central manager periodically tests all source and destination powers using the routing table information. If some node's power is out of expected bounds, the possible source of the fault is identified. In [3, 4, 5], fault identification through filtering alarms is discussed. Using a fault identification tree of depth equal to the number of alarming components, the set of potential fault sources is narrowed down. A survey of fault detection capability at each layer is presented in [6]. Approaches to

the fault location problem are also classified. A problem on monitor placement was considered in [8]. In [8], the authors show that a wavelength to be used for probing other nodes from a monitor node is highly likely to be available in dynamic traffic conditions. Based on this, it is claimed that fault detection and identification can be done successfully with high probability with a small number of monitor nodes. A heuristic algorithm for monitor placement that is based on clustering is then proposed.

In this paper, we consider a fault propagation model similar to the ones considered earlier in [2, 3, 4, 5]. As far as we are aware, except for [8], there are no papers in the literature on the placement of monitoring equipment in optical networks. Based on a survey of monitoring capability available in the optical components in the market, we formulate a monitor placement problem and present a solution. The traffic and fault propagation model we use are different from the one used in [8].

The rest of the paper is organized as follows. Section 2 provides a summary of the physical optical layer and commonly used optical monitoring devices. It specifies the set of alarms that are commonly provided by each monitoring device. Section 3 describes the advantages of optimally placing monitors, and a problem is formulated. In Section 4, we present an optimal monitor placement scheme assuming that the monitoring equipment generates a single type of alarm. Section 5 shows a simple illustrative example of how the scheme works. Numerical results on monitor placement on example networks and traffic sets are presented in Section 6. The paper concludes with a summary of advantages achieved by use of optimal monitoring equipment placement, and considers possible extensions of this work.

2 Physical Layer

In optical networks, the physical layer generally consists of several basic network components. Optical components are passive or active. Passive optical components do not have monitoring equipment capable of detecting and reporting alarms. Active optical components, on the other hand, usually have monitoring equipment and are therefore capable of reporting alarms to the network manager. We first review the available optical layer monitors, and then summarize the alarming capabilities of the common active optical components.

2.1 Physical Layer Monitoring Capability

Different network layers provide different monitoring capabilities. While the optical physical layer has monitoring capability to detect hard-failures, which are the result of total service disruption, it is unable to detect soft-failures resulting from slow degradation of the transmission quality.

There are two basic monitor types at the physical layer that provide information about physical network status, namely, optical power meter and optical spectrum analyzer. Both monitors generate alarms when the input power is outside specified threshold levels. An optical power meter generates an alarm when the aggregate power at its input is outside specified threshold levels. The optical power meter can be used on a fiber basis, in which case we will refer to it as an aggregate power monitor (APM), or on an individual wavelength basis, in which case we will refer to it as a single wavelength power monitor (WPM). An optical spectrum analyzer is capable of monitoring the power level of each active wavelength on the fiber. It generates an alarm for a specific wavelength whose power is outside specified threshold levels. We will refer to optical spectrum analyzers as spectrum power monitors (SPMs). Table 1 summarizes the alarm characteristics for these monitor types.

Table 1. Alarm Characteristics for Optical Power Meter and Optical Spectrum Analyzer

Monitoring Device	Monitoring Capabilities	Possible Fault type	Alarm Type Reported	Alarm Description
Aggregate Optical Power Meter	Total optical power Level on the fiber	One or more upstream nodes are transmitting at a power out of specified range	Aggregate optical power out of specified range	Aggregate input power alarm is active when aggregate optical input power is outside of specified range
Optical Spectrum Analyzer	Power level for each wavelength on the fiber	Upstream node is transmitting at a power out of specified range	Specific wavelength power out of specified range	Wavelength input power alarm is active for specific wavelength when the optical power is outside of specified range

2.2 Optical Network Components and a Fault-Propagation Example

This section summarizes the physical layer monitoring capabilities of commonly used optical network components. Although monitoring capabilities differ slightly from manufacturer to manufacturer, Table 6 provides the most common alarming capabilities of currently available optical network components.

Some of the listed components may also have upper layer monitors, such as BER, that are ignored in this paper since we only consider physical layer monitors here. Also, some components generate temperature alarms which, although useful for reporting the local status of a device, do not provide information on propagated hard failures and are therefore also ignored in this paper. Besides temperature information, the only two other physical monitor types are ag-

gregate power meter and optical spectrum analyzer. Both of these monitors provide information on hard-failures in a network and their placement should be optimized in a given network.

We next illustrate how a failure may generate multiple alarms in a network on the example network shown in Figure 1. We make the following assumptions for this example:

1. Monitoring equipment within network devices never fails. This assumption is required in order to have reliable set of alarms based on which component failure can be localized.
2. In this example we consider only hard failures, and therefore only single wavelength power monitors (WPM), aggregate power monitors (APM), and spectrum power monitors (SPM) are considered. WPMs report alarms for a single wavelength, APMs report power sum of all wavelengths on a single fiber but do not differentiate between different wavelengths, and SPMs monitor and report power level of each wavelength separately. All other component monitoring devices such as temperature monitors are ignored since they do not directly detect hard failures in devices.
3. Each of the following optical component modules has a set of monitoring devices which we consider in the following example. We assume that each component module has maximum monitoring capability and that alarm reporting by each device module can be turned on or off dynamically by the network manager in order to minimize redundant alarms while maximizing fault detection capability in a given network. The following list identifies the set of monitoring devices for each component.

(a) Optical Transmitter Module

(a-i) Output WPM

(b) Optical Receiver Module

(b-i) Input WPM

(c) Mux

(c-1) Per Input Port WPM

(c-ii) Output SPM

(d) Demux

(d-i) Input SPM

(d-ii) Per Output Port WPM

(e) Optical Switch

(e-i) Per Input Port SPM

(e-ii) Per Output Port SPM

(f) Protection Switch

(f-i) Per Input Port APM

(f-ii) Output APM

(g) Wavelength Converter (optical)

(g-i) Input SPM

(g-ii) Output SPM

(h) EDFA

(h-1) iInput APM

(h-ii) Output APM

(h-iii) Pump Laser WPM

4. It is assumed that devices are capable or reporting following alarm types based on the measurements reported by their monitors. Furthermore, it is assumed that network manager is capable of dynamically configuring component modules to report only specified fault types while filtering others.

A Network Example Illustrating Fault Propagation:

In the following example we consider the small network shown in Figure 1. In order to illustrate the fault propagation, we assume that following light-paths are established in the network:

Duplex connection between Host 1 and Host 3:

- *LP1:* Host1 → SW1 → L1 → SW2 → L2 → EDFA1 → L3 → WC1 → L4 → SW3 → Host3

- *LP2:* Host3 → SW3 → L13 → WC2 → EDFA2 → L15 → SW2 → L16 → SW1 → Host1

Duplex connection between Host 2 and Host 4:

- *LP3:* Host2 → SW2 → L2 → EDFA1 → L3 → WC1 → L4 → SW3 → L5 → SW4 → Host4

- *LP4:* Host4 → SW4 → L12 → SW3 → L13 → WC2 → L14 → EDFA2 → L15 → SW2 → Host2

If we assume full monitoring capability on each device, then a single component failure will generate large number of alarms. To illustrate this, we consider the failure of EDFA1 in the figure, in which case the following alarms will be generated based on our assumptions.

Alarms generated when EDFA1 fails:

- a. EDFA1 generates EDFA output failure alarm
- b. Wavelength Converter 1 generates Input power out of range on the input wavelengths corresponding to LP1 and LP3
- c. Switch SW3 generates Input power out of range for input port for link L4 corresponding to LP1 and LP3
- d. Host3 generates Receiver input power out of range
- e. Switch SW4 generates Input power out of range on input port for link L5 corresponding to the wavelength for LP3
- f. Host4 generates Receiver input power out of range.

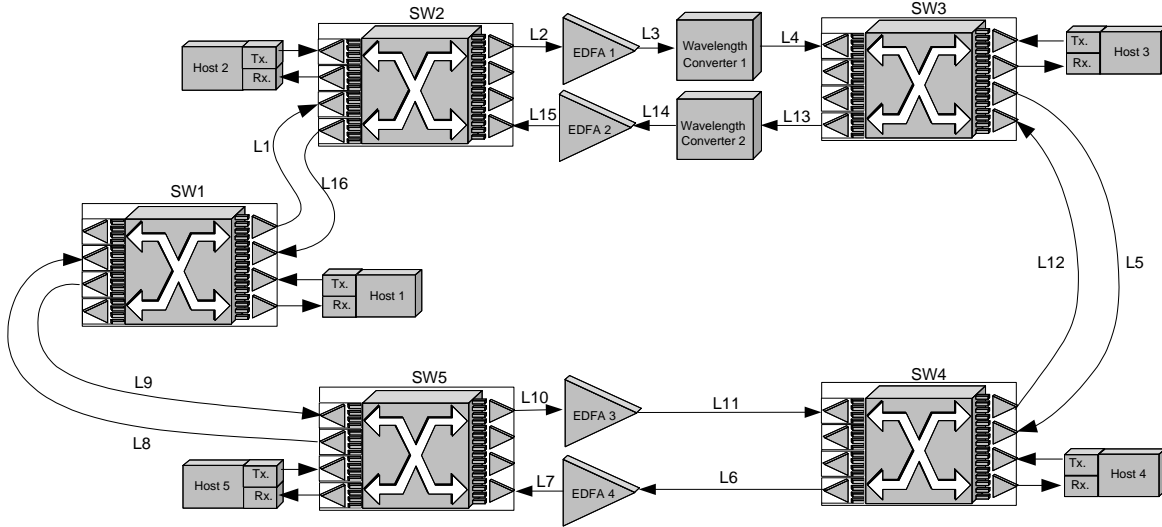


Figure 1. An example network illustrating fault propagation.

3 Optimal Monitor Placement and Problem Formulation

All networks require some form of a fault management system which, besides other functions, is capable of detecting and locating failures in a network. The function of such a system is to process alarms received from network components, and based on this information determine all possible locations of failure. Its effectiveness is measured by the speed with which it is able to process the received alarms, as well as by its ability to unambiguously provide fault source location.

Depending on the type of monitoring equipment used, its placement, network type, and network topology, different alarm types may be received by the fault manager. Some of the received alarms may be redundant, while in some cases, no alarms may be generated for a fault. By careful placement of network monitors, it is possible to achieve maximum fault-detection coverage while reducing redundant alarms. Therefore, optimal placement of monitoring components will improve speed and effectiveness with which the fault-manager is able to locate a network failure. Although similar placement optimization problems have been solved for many different applications they cannot be applied directly to optical networks. This is primarily due to the transparency characteristic of optical networks.

In transparent optical networks, faults propagate in the optical domain, while alarms are generated and processed in the electrical domain. A single fault can propagate throughout an optical network and generate many simultaneous

alarms. This complicates the problem of accurately locating the source of the fault. Therefore, we need to take the fault propagation model for a given network into account when determining the optimal monitor placement, in order to reduce the number of redundant alarms that are sent to the fault manager.

In this paper, we develop a scheme for the optimal placement of monitors in an optical network. Our network and traffic model is an arbitrary mesh network with a static set of lightpaths. The fault propagation model we assume is that a fault propagates in the downstream direction of all the lightpaths that pass through the source of the fault. This assumption is consistent with the one used in [2, 3, 4, 5]. Thus, every downstream monitor on every lightpath passing through the fault location is assumed to report an alarm for this fault. We believe this model to be reasonable in a transparent optical network. Nevertheless, other appropriate models can easily be incorporated into the problem formulation. As two other examples, one may consider: (a) a second-order fault propagation model in which the lightpaths which intersect with the lightpaths that pass through the fault origin can also be assumed to propagate the fault, and (b) a fault propagation model in which there are some masking components [5] which do not propagate the fault further downstream. In the remaining sections of the paper, we only consider the placement of aggregate power monitors at the input ports of a node. The problem we address here is informally stated below.

The Power Monitor Placement Problem: Given a mesh network and a set of lightpaths, and assuming the fault prop-

agation model above, determine the number and placement of the minimum number of monitors required to achieve the same level of fault localization as the network with monitors placed at every input port.

The goal is to develop an algorithm that minimizes the number of monitors while maximizing fault coverage, i.e., the number of fault scenarios which can be localized or whose origin can be inferred. Note that the above problem formulation considers a static set of lightpaths, and is more appropriate for a network provisioning or design application. For dynamic traffic, one must, of course, deploy all monitoring equipment at network design time. In this situation, our problem formulation is useful in the following sense. A solution to the monitor placement problem for a particular set of lightpaths at some instant of network operation can now be interpreted as the set of monitors that must be “turned on”, i.e., configured to report alarms to the network manager. Minimizing the number of alarms reported to the network manager without compromising on fault coverage is crucial to the rapid localization of faults as well as the stability of management systems against ever-increasing amounts of alarm data [9].

4 A Solution Approach

In our approach, we assume that only aggregate power monitors are used in a network. We assume that any input port of a network node may be assigned an aggregate power monitor. Our algorithm determines the optimal placement of aggregate-power monitors in network components on a per-port basis.

Our proposed power-monitor placement algorithm consists of two phases. The first phase is a preprocessing phase. During this phase, a fault-reporting *alarm matrix* is formed by considering fault propagation in a given network and determining the set of alarms reported for the failure of each network component. Each matrix row represents a binary vector of alarms that are reported by the monitors for a specific failure scenario, a 1 denoting a reported alarm and a 0 denoting no alarm. The alarm vector is determined for each failure scenario by using information about the network topology and the established lightpaths. Initially, we assume that every used input port on a network node is assigned a power monitor. Therefore, the resulting alarm matrix represents an “upper bound” on fault reporting for each network node. After such a matrix is formed, row-wise redundant information is removed by deleting all zero-vector rows and by grouping all identical rows into a single row. This is because, if a row consists of all zeros then no monitor detects the fault corresponding to that row. If two rows are identical, then the set of alarms reported for the two corresponding fault scenarios are identical, and therefore these faults cannot be unambiguously determined to have

occurred.

The second phase of the algorithm is the monitor placement optimization phase. During this phase, the optimal placement of power monitors is determined. The optimal placement of power monitors is determined by eliminating redundant monitors from the upper-bound fault-reporting alarm matrix that was constructed during the preprocessing phase. This corresponds to the removal of the maximum number of matrix columns (monitors) such that two row-wise constraints are met; namely, (a) a column may be removed only if after such removal none of the matrix rows become zero-vectors, and (b) all matrix rows remain distinct. By removing all possible columns under these two constraints, we can remove redundant monitors and therefore achieve the optimal monitor placement in a given network. The next section provides a simple example that illustrates the application of this algorithm in a small network.

5 A Simple Optimal Monitor Placement Example

In this example we consider a simple network with eight monitor-less optical nodes as shown in Figure 2, and show how our algorithm can be used to determine the optimal placement of aggregate-power monitors. We assume only single node-fault scenarios.

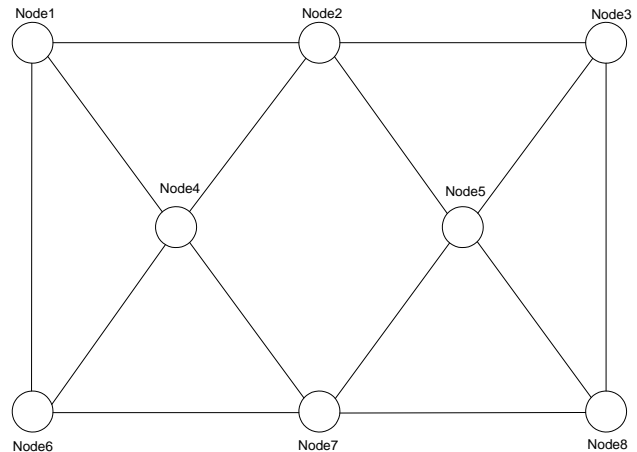


Figure 2. An example network for the power monitor placement problem.

It is assumed that the following three lightpaths *LP1*, *LP2*, and *LP3* have been established in the network shown above:

LP1: Node1 → Node2 → Node3,

LP2: Node1 → Node4 → Node2 → Node5 → Node3,
and

LP3: Node6 → Node4 → Node2 → Node5 → Node8.

Using this information about established lightpaths, we can simplify the network graph as shown in Figure 3.

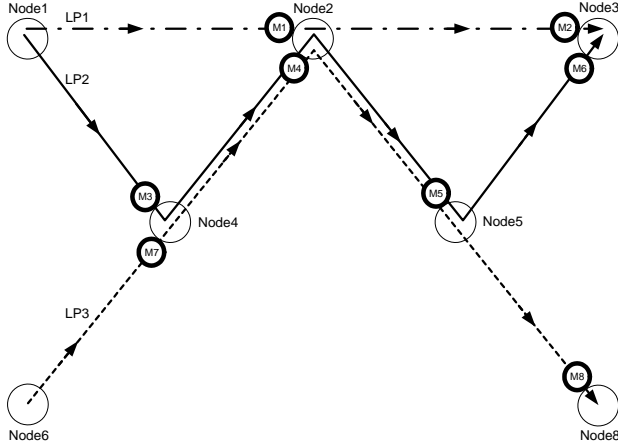


Figure 3. Three lightpaths in a network.

We start solving the optimal monitor placement problem by determining the upper-bound placement scenario. This results in the placement of aggregate power monitors on every currently used input port of monitor-less network nodes. We label these monitors M_1, \dots, M_8 as shown in Figure 2.

Using the information about established lightpaths, network topology, and monitor placement, we create the alarm matrix as shown in Table 2.

Table 2. Alarm Matrix

Faults	M1	M2	M3	M4	M5	M6	M7	M8
FN1	1	1	1	1	1	1	0	0
FN2	0	1	0	0	1	1	0	1
FN3	0	0	0	0	0	0	0	0
FN4	0	0	0	1	1	1	0	1
FN5	0	0	0	0	0	1	0	1
FN6	0	0	0	1	1	0	1	1
FN7	0	0	0	0	0	0	0	0
FN8	0	0	0	0	0	0	0	0

To remove redundant information from the alarm matrix, we remove all zero-vector rows and group all identical rows into single row. This results in the simplified alarm matrix shown in Table 3. In this case, faults in nodes 3, 7, and 8

cannot be identified because no alarms are reported. All other node faults can be unambiguously located because no two sets of alarms are identical.

Table 3. Simplified Alarm Matrix

Faults	M1	M2	M3	M4	M5	M6	M7	M8
FN1	1	1	1	1	1	1	0	0
FN2	0	1	0	0	1	1	0	1
FN4	0	0	0	1	1	1	0	1
FN5	0	0	0	0	0	1	0	1
FN6	0	0	0	1	1	0	1	1

Finally, redundant monitors (matrix columns) can be removed under the two constraints:

1. None of the matrix rows can be zero vectors.
2. All matrix rows must remain distinct.

Using these constraints, we can reduce the above matrix to the optimal alarm matrix as shown in Table 4.

Table 4. Optimal Alarm Matrix

Faults	M2	M4	M6
FN1	1	1	1
FN2	1	0	1
FN4	0	1	1
FN5	0	0	1
FN6	0	1	0

We have removed redundant aggregate-power monitors $M_1, M_3, M_5, M_7,$ and M_8 from the network, and therefore reduced the number of alarms that need to be processed by the network fault manager. We have also achieved over 60% cost savings in network monitoring equipment. The resulting optimal monitor placement is shown in Figure 4.

6 Experimental Results

We have formulated the problem of minimizing the number of monitors to be placed in the network as a mixed integer-linear program (MILP). We have used CPLEX, a commercially available optimization software, to solve the MILP. In this section we present numerical results on the number of monitors required with the CPLEX solution, as well as with a naive approach for monitor placement. The network topology we assumed for the simulation was the

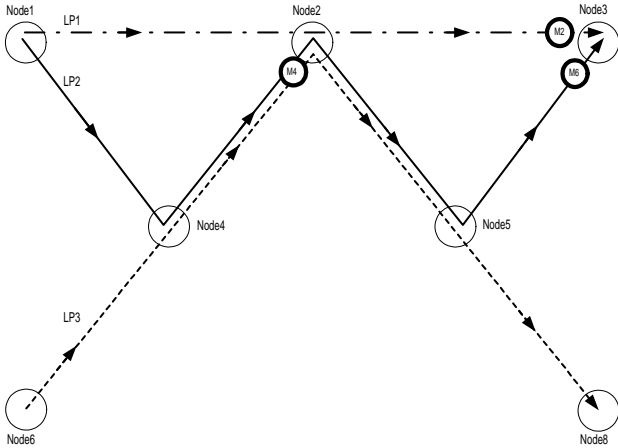


Figure 4. Optimal monitor placement for the example.

NSFnet topology shown in Figure 5. This network has 42 directed links and 182 ordered pair of nodes. The simulation results are given in Table 5. We assumed only single node-fault scenarios in our experiments. Note, however, that the problem formulation and the solution approach themselves do not depend on any specific fault model. The fault model affects only the alarm matrix that is generated. Furthermore, only aggregate power monitors at node input ports are assumed.

In the table, we show the number of monitors to be placed for the MILP solution obtained through CPLEX¹ for various lightpath set sizes. For each set size, we generated 100 random sets picked using a uniform distribution for the sources and destinations, and both average and worst-case results over these 100 sets are presented. Also shown in the table are the maximum number of possible monitor locations (Naive), i.e., the number of active input ports, for the various lightpath set sizes. It can be seen that the CPLEX solution provides significant reductions in the number of monitors required for all lightpath set sizes. The reduction in the number of monitors to be placed through optimization becomes more pronounced for large lightpath set sizes. For example, in the case 160 lightpaths, the naive approach requires 42 monitors, whereas the optimal solution requires only 6 monitors on the average. Interestingly, the number of required monitors slightly decreases as the lightpath set size becomes large. This is because the number of faults that can be distinguished by a full set of monitors itself becomes small due to the large number of lightpaths and the

¹In some instances, we have used a constrained version of the MILP formulation, so some of the CPLEX results we present may be improved further.

assumed fault propagation model.

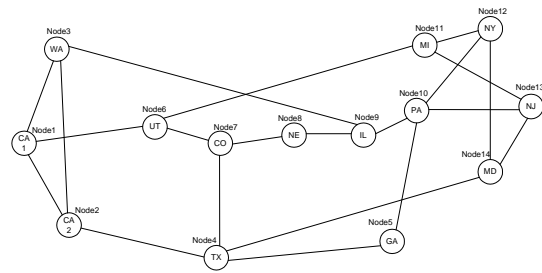


Figure 5. The NSFnet topology.

7 Conclusions and Future Work

In this paper, we presented the problem of optimal monitor placement in optical networks. We first described the types of optical monitoring equipment that are available, and the types of alarms that are generated by these equipments as well as by monitors within typical optical networking components. A simple example was given to illustrate the potential cost savings by optimally placing monitors, and an approach to placing monitors was presented. We have also presented performance results through a mixed integer-linear program (MILP) formulation of the problem, which resulted in significant reductions in the number of monitors required.

This work may be extended in the following ways. First, one may consider various other kinds of monitoring equipment and fault propagation models. Designing efficient heuristic algorithms for monitor placement with provable worst-case guarantees is another possible topic for future study.

Acknowledgement

This work was supported in part by the DARPA under Grant N66001-00-18949 (co-funded by NSA), by the NSF under grants ANI-9973098 and ANI-9973111, and by the DISA under an NSA-LUCITE contract.

References

- [1] M. R. Garey and D. J. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness* (Freeman, New York, 1979).
- [2] I. Katzela, G. Ellinas, W. S. Yoon, and T. E. Stern, "Fault diagnosis in optical networks", *Journal of High Speed Networks*, vol. 10, no. 4, 2001, pp. 269-91.

[3] C. Mas, O. Crochat, and J.-Y. Le Boudec, "Fault Localization in an Optical Network," *All-Optical Networking: Architecture, Control, and Management Issues (VV09), SPIE'98 Voice, Video, and Data Communications*, November, 1998.

[4] C. Mas and J.-Y. Le Boudec, "An alarm filtering algorithm for optical communication networks", *Proc. Management of Multimedia Networks and Services, IFIP/IEEE TC6/WG6.4/WG6.6 International Conference*, 1998, pp. 205-18.

[5] C. Mas and P. Thiran, "An Efficient Algorithm for Locating Soft and Hard Failures in WDM Networks," *IEEE J. Select Areas Commun.*, vol. 18, no. 10, pp. 1900-1911, Oct. 2000.

[6] C. Mas and P. Thiran, "A review on fault location methods and their application to optical networks", *Optical Networks Magazine*, pp. 73-87, Jul./Aug. 2001.

[7] M. Medard, D. Marquis, R. A. Barry, and S. G. Finn, "Security issues in all-optical networks," *IEEE Network*, vol. 11, no. 3, pp. 42-48, May-June 1997.

[8] W. Tao and A. K. Somani, "Attack monitoring and monitor placement in all-optical networks," *Proc. Gigabit Networking Workshop*, Anchorage, Alaska, in conjunction with INFOCOM '01.

[9] R. D. Gardner and D. A. Harle, "Pattern discovery and specification techniques for alarm correlation," *Network Operations and Management Symposium*, 1998, pp. 713-722.

[10] E. Horowitz, S. Sahni, and S. Rajasekaran, "Computer algorithms," Computer Science Press, New York, 1997.

Table 5. Number of Monitors

LPs	Naive Avg.	Naive Max.	optimal Avg.	optimal Max.
5	9.65	13	6	10
10	16.95	22	8	12
15	22.37	28	8	11
20	23.89	28	7	11
25	30.2	35	7	10
30	32.8	39	7	10
35	34.51	39	7	10
40	36.08	40	7	10
45	37.45	41	7	10
50	38.56	41	7	10
55	39.2	42	7	9
60	39.48	42	7	9
65	40.34	42	7	9
70	40.67	42	6	8
75	40.8	42	6	9
80	41.2	42	6	9
85	41.14	42	6	9
90	41.3	42	6	9
95	41.5	42	6	8
100	41.74	42	6	8
105	41.66	42	6	8
110	41.87	42	6	8
115	41.86	42	6	8
120	41.9	42	6	8
125	41.91	42	6	9
130	41.93	42	6	8
135	41.95	42	6	8
140	41.98	42	6	8
145	41.98	42	6	8
150	42.0	42	6	7
155	41.99	42	6	8
160	42.0	42	6	8
165	42.0	42	6	8
170	42.0	42	6	8
175	42.0	42	5	8
180	42.0	42	5	7
182	42.0	42	5	8

Table 6. Fault Monitoring Capabilities of Optical Components

Optical Device	Set of Monitors Reporting Alarm	Fault Type Reported by device to Network Manager
Optical Transmitter Module	(Output WPM) is out of range	Transmitter output power out of range
Optical Receiver Module	(Input WPM) is out of range	Receiver input power out of range
Mux	(Output SPM, wavelength x) is out of range	Mux device failure
	Input wavelength x WPM and (Output SPM, wavelength x)	Input power out of range on wavelength x
	(Output SPM, wavelength x) > Input wavelength x WPM	Crosstalk on wavelength x
Demux	Output wavelength x WPM	Demux device failure
	(Input SPM, wavelength x) and Output wavelength x WPM	Input power out of range on wavelength x
	Output wavelength x WPM > (Input SPM, wavelength x)	Crosstalk on wavelength x
Optical Switch	(Input SPM, port y, wavelength x) is out of valid range	Input power out of range on wavelength x on input port y
	(Output SPM, port y, wavelength x) is out of valid range	Switch Failure
	If (Input SPM, port y, wavelength x) is much larger than (Output SPM, port g(y), wavelength f(x)) but within valid range, where g() is port mapping function and f(x) is wavelength mapping function	Misrouting of wavelength x on port y
	If (Input SPM, port y, wavelength x) is less than (Output SPM, port g(y), wavelength f(x)) but input is within the valid range;	Crosstalk on output port g(y), wavelength f(x)
Protection Switch	Input x APM	Redundancy switch performed from input x to input y due to loss of signal on input x
	Output APM	Protection switch failure
	(Output APM) and (Input x APM)	Protection switch failure
Wavelength Converter (optical)	(Output SPM, wavelength f(x)) is out of range for (Input SPM, wavelength x) within the range. Where f() is the wavelength conversion function.	Wavelength converter failure
	(Input SPM, wavelength x) and (Output SPM, wavelength f(x)) are both out of range.	Input power out of range on the input wavelength x
	If (Input SPM, wavelength x) is greater than (Output SPM, wavelength f(x)) but within the range	Wavelength conversion error
	If (Input SPM, wavelength x) is less than (Output, SPM, wavelength f(x)) but within the range	Crosstalk on wavelength x
EDFA	Input APM and Output APM	Input power out of range
	Output APM	EDFA failure
	Laser Pump Output WPM	EDFA pump failure