

Fault and Attack Management in Optical Networks

Amitangshu Pal¹, Amitava Mukherjee², Mrinal Kanti Naskar³

¹Dept. of ECE, University of North Carolina at Charlotte, NC 28223, USA

amitangshupal@yahoo.co.in

²IBM India Pvt. Ltd., Calcutta 700091, India, amitava.mukherjee@in.ibm.com

³Dept. of ETCE, Jadavpur University, Calcutta 700032, India, mrinalnaskar@yahoo.co.in

Abstract—This paper proposes fault(attack) detection and localization scheme to handle multiple failures(attacks) in the optical network using wavelength-division multiplexing (WDM) technology. This proposed scheme is two-phased scheme containing (a) the detection of faults(attacks) through monitoring devices raising alarms (fault or attack detection) and (b) subsequently the localization of these faults or attacks (fault or attack localization) by invoking an algorithm. The later phase will obtain a set of potential faulty(attacked) nodes (links). Next the scheme locates the exact faulty(attacked) node(link) by the process of sending and receiving signals. I have demonstrated the performance of the scheme on 14-node NSFNet and 28-node EuroNet. Next I have compared this scheme with an existing algorithm [1] for locating faulty nodes (links). The proposed scheme outperforms the existing one.

Index Terms— Fault(Attack) Detection, Fault(Attack) localization, Optical Network

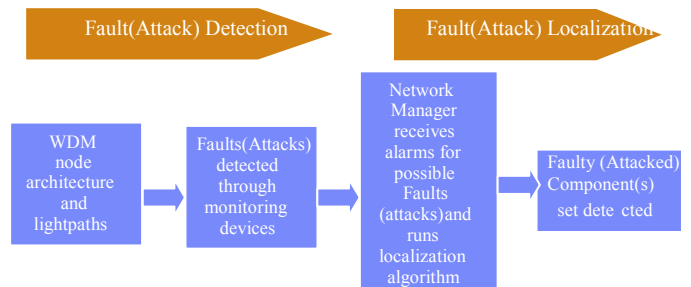
I. INTRODUCTION

High capacity optical networks are immensely used in industries due to its large transmission bandwidth and low cost. But these networks are also vulnerable to failures (like malfunctions of optical devices, fiber cuts, soft failures i.e., the impairment due to subtle changes in signal power such as degrading signal to noise ratio (SNR), etc) and different kinds of attacks (like service disruption, eavesdropping etc). One of the most important requirements to ensure high speed optical network survivable is to manage fault(attack) detection and fault(attack) localization. A single failure(disruption) can cause million of dollars of revenue lost right from corporate to service providers. So, the fault and attack management is essential to ensure uninterrupted services to users.

The management system involves in detecting faults(disruptions) in the network and alerting ‘manager’ through alarms triggered by monitoring devices when disruption happens. If a certain parameter is being monitored and its value falls outside a preset range, the network equipment and/or monitoring device generates an alarm. Again, monitoring devices raise alarm if link (e.g., fibre cut) gets damaged. Consider a situation that we may monitor the

power level of an incoming signal and if we see the power level drop below a certain range we may declare a loss of signal (LOS) and consequently monitoring devices raise alarms. Fault and attack management is an important management function that is responsible for fault and attack detection, localization and recovery. In this work I have discussed only fault (attack) detection and localization and the block diagram of the proposed scheme is shown in Figure 1.

Fig.1. Proposed fault detection and localization scheme



In optical network due to transparent characteristics of the network, a fault(disruption) propagates through out the network when it occurs. As a result whenever there is a failure or attack, for example, in a node, all the lightpaths passing through this node get disrupted and monitoring elements (monitoring devices and/or self alarmed optical devices e.g. Transmitter, Receiver, etc.) placed in the path raise alarms. Thus a single failure(disruption) may generate multiple alarms. In the case of multiple failures(disruptions) occurred in a number of nodes or in links simultaneously the raised alarms are intermingled and thus make the detection and localization process complex. Both single and multiple failures and attacks are detected through monitoring devices by raising alarms. To make the fault and attack management system cost effective the number of monitoring elements would be minimized and that will be spanned across the entire network.

The first phase of the proposed scheme detects the failure(s) and attack(s) in the network components. The monitoring devices are placed optimally across network. When any disruption occurs they will trigger alarms for probable

failure(s) and attack(s) in the network. In the second phase, the localization algorithm when it is invoked to locate faults or attacks gives a set of probable faulty(disrupted) components. In real scenario corrupted alarms (false alarms and miss alarms) arise in the network and make the localization process more difficult. The false alarms and missed alarms could be controlled by tuning the threshold values of the monitoring equipments and eventually the cardinality of the set of faulty (or attacked) components lowers down. In this paper, monitor and monitoring device has been used interchangeably.

A. Motivation

For critical business application running on optical networks, the 99.999% uptime of services is a must. This requirement corresponds to the connection downtime of less than five minutes per year. Hence, alerting manager appropriately through alarms triggered from upcoming faults(attacks) and consequently detecting and localizing faults(attacks) are prime activities in the network management. Fault(attack) diagnosis and localization is an interesting problem and hence it is an active field of research. Earlier works on these research areas have motivated us to work further.

Different approaches were used to solve the problem. In [4] Stanic et al. used approximation method to reduce the number of monitors and thus make the system cost effective. Another approximation algorithm was shown in [5] to reduce the number of monitoring elements. In [8] authors showed that the optimal monitor placement (reduction) is an NP hard problem. For solving the fault (attack) localization problem different scholars have taken different assumptions. In [16] only single failure is considered while in [1], [17]-[18] multiple simultaneous faults are considered. Also in [1], [10] false alarms and miss alarms are considered. In [7], authors have shown that false alarms can be corrected in polynomial time but the correction of miss alarms is NP-hard. In [20],[21],[22] algorithm for multiple attack localization and identification in all-optical networks has been presented. Since multiple fault(attack) detection with or without miss alarms or false alarms are NP-hard problems, none of the solutions obtained by approximation methods are working appropriately. Depending upon the network condition, resource available and customer demand the best possible fault(attack) management system is required.

B. Contribution

In this paper, the scheme has been divided into two phases namely i) fault(attack) monitoring: monitoring devices

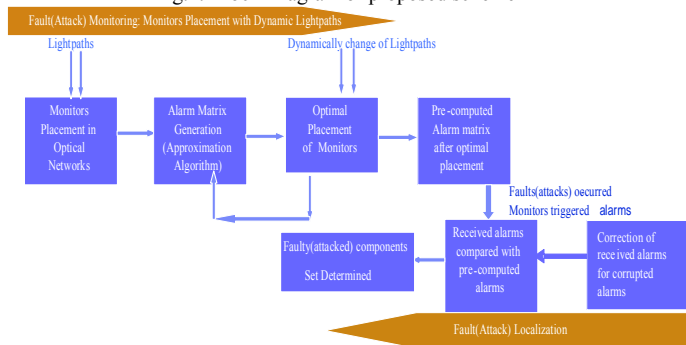
placement with dynamic lighpaths and ii) fault localization. The block diagram of the proposed scheme is shown in Figure2.

Dynamic scenario means that a set of lighpaths is added to a network at any point of time while a set of lighpaths would be cut off when disruption happens in the network or the traffic load increases. This dynamic scenario keeps the network running normal during survivable period to cater users' requirements. Firstly the total number of monitoring devices to be placed in the network has been minimized to make this placement cost effective. The placement of monitors in the network is posed as a NP-hard problem. Next an approximation algorithm has been proposed to place monitors in an optimal way that would be spanned across the network to cover the failures (disruption) of components when single/multiple simultaneous failures(disruptions) occurred. The dynamically change of lighpaths would be input to approximation algorithm until the placements of monitoring devices would optimal one and is almost independent of the change network scenarios. The pre-computed alarm matrix is the output of approximation algorithm, for optimal placement of monitoring devices.

Secondly, failures(disruptions) are located from the received alarms. Raising false alarms and miss alarms from faulty (disrupted) components are frequent features in the network. After receiving alarms from monitoring devices, irrespective of types of alarms, localization algorithm is invoked and compares received alarms with pre-computed alarm matrix generated in the monitor placement phase. This comparison will produce a set of probable faulty(disrupted) components. Next I have proposed a scheme to locate the exact faulty(disrupted) component by the process of sending and receiving signals. In this work, I have also compared performance this scheme with the algorithm given in [1] and discussed why this work is acceptable in real life scenario. In summary, the two-phased scheme has four important features i) minimizing the number of placement of monitoring devices, ii) reuse the previously placed monitors when network scenario changes, iii) the localization of multiple simultaneous faults(attacks) and iv) handling the effect of false and miss alarms in the network.

Section II explains different types of faults and attacks in optical networks. Section III describes network model and notations. Section IV discusses the proposed scheme. Section V presents simulation performance. Section VI concludes the work.

Fig.2. Block Diagram of proposed scheme



II. Faults and Attacks in Optical Networks

Different kinds of failures (such as link failures, node failures etc) degrade the performance of the network. In most cases ink failures occur because of fiber cuts. This is the most likely failure event. The next most likely failure event is the failure of active components inside the network equipment such as transmitters, receivers or controllers. Moreover, failure of controllers does not affect traffic but only impacts management visibility into the network. Node failures are other possible failures of the network. Entire central offices can fail, usually because of catastrophic events such as fires or

flooding. These events are rare, but they cause widespread disruption when they occur.

We can explain attacks from two different viewpoints, one from attacker's perspective and another from management's perspective. From the attacker's perspective attacks can be broadly categorized into service disruption and eavesdropping. In service disruption method the attacker can gain access to the network by implementing in-band and out-of-jamming attack method. For in-band-jamming attacks the attacker use to take the advantage of specific characteristics of some components such as gain saturation of optical amplifiers. At the input of an optical amplifier the attacker increase the power of one channel with respect to other. As a result the output of some channels will be too low or too high. This attacking signal will propagate through the network. In out-of-band jamming attack the attacker may use transmission effects such as Raman effects to degrade the performance of the network. Eavesdropping is the technique of gaining access to the network by unauthorized observation. From management's perspective attacks can be broadly classified into direct and indirect attacks. Direct attacks can be directly implemented on different physical components such as taps, fibers etc. In case of indirect attack method the attacker takes the advantages of possible vulnerabilities of network components and other transmission effects (e.g., crosstalk effects) to gain access to the network.

So there some differences between faults and attacks. Those are as follows.

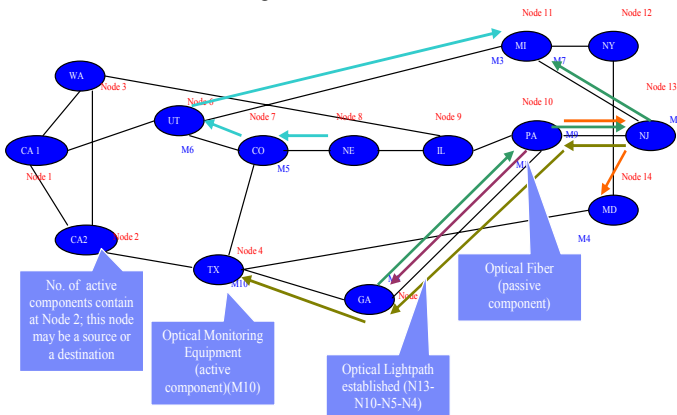
- i) Faults occur mainly due to natural fatigue and ageing of optical devices and components. Faults seldom occur in a network. But attacks appear or disappear sporadically in the network.
- ii) If a fault occurs in a device then it will remain disabled until it will be repaired again. On the other hand attack will appear and disappear sporadically.

III NETWORK MODEL AND NOTATIONS

A. Network Model

We model the network by a directed graph $G = (V, E)$ where each node $v \in V$ of the graph represents an optical component, and the directed edge $(u, v) \in E$ represents a directed lightpath from u to v . A fault(disruption) occurred at a node or a fibre-cut will disrupt the connectivity and

Fig.3. Reference NSFNet



disconnect all lightpaths passing through node or in link. Figure 3 shows 14-node NSFnet which is the backbone network for US. The Fig. 3 is self-explained.

In Fig.3, lightpaths passing through different cities has been shown. Let us consider that fault occurs in GA. Then this fault(disruption) will propagate to TX-CA2 and M9, M8 will raise an alarm. On the other hand the fault(attack) will also propagate to through the lightpath PA - NJ - MI marked in green. Thus M1, M2 and M6 will also raise alarm. In this way, a single fault(disruption) generates multiple alarms.

B. Notations, Definitions, and Preliminaries

In the discussion I have used the following notations throughout the paper. LP is the set of lightpaths. C is the set of all components. R is the set of all rows(components).in the Alarmmatrix. M is the set of all monitors. M_t is the set of all triggering alarms. M_s is the set of all silent alarms. H is the set of all hit values. FC is the set of probable faulty(attacked) components. Different notations have been shown in Table I.

TABLE I
NOTATIONS

LP	← the set of lightpaths
C	← set of all components
R	← set of all rows indicating components
M	← set of all monitors
M_t	← set of all triggering alarms
M_s	← set of all silent alarms
H	← set of all hit values
FC	← set of probable faulty (disrupted) components

Here in this discussion I have defined the term *Domain* of the faulty(disrupted) component(s) by the set of monitors which generate alarm on failure(attack). Domain can be expressed by the Boolean relation. Let (C_i, LP_i) be the position of the component C_i in the lightpath LP_i . Now a monitor $M_k \in M$ will be in the domain of (C_i) for $C_i \in C$ if the following conditions will be satisfied.

- i) if $LP_i \in LP$ and $LP_j \in LP$ such that $C_i \in LP_i$ and $M_k \in LP_j$ then $\exists i$ and j for which $LP_i = LP_j$
- ii) $\exists LP_i \in LP$ such that position $(C_i, LP_i) < \text{position}(M_k, LP_i)$ where position (X, L) gives the distance of X from the source of lightpath L.

IV. PROPOSED SCHEME

B. Fault(Attack) Monitoring: Monitors Placement with Dynamic Lightpaths

Monitors initially are placed to all possible number of locations so that the failures(attacks) can be detected and located for all components distinctly [4]. In Fig. 3, M1 - M11 i.e., 11 monitoring devices are placed to achieve maximum

coverage. I have proposed a greedy algorithm which determines the optimal number of monitors from the set of monitors in such a way that failures(disruptions) can be located for all components (i.e., for a node or a link) distinctly and no component (i.e., a node or a link) remains unattended i.e., if a fault(disruption) occurs in a component it must not remain undetected. The algorithm is described below [5] [19].

Algorithm for Choosing Optimal Monitors

```

Initialize an empty set S=∅
While (for any Ri,Rj∈R, Ri≠Rj such that i≠j){
  ∀Mp∈M and Mp∉S
  Hp←hit value of (Mp)
  if (Hr>Hq∀Hq∈H and r≠q){
    S=S∪Mr
  }
}
Output S

```

We explain this algorithm using Table II.

In Table II, ‘1’ denotes that if a node fails(is attacked) the

TABLE II
ALARM MATRIX FOR REFERENCE NETWORK

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11
ND4	0	0	0	0	0	0	0	1	0	0	0
ND5	1	1	0	0	0	1	0	1	1	0	0
ND6	0	0	1	0	0	0	0	0	0	0	0
ND7	0	0	1	0	1	0	0	0	0	1	1
ND8	0	0	0	0	0	0	0	0	0	0	1
ND10	0	1	0	1	0	1	1	1	1	0	0
ND13	0	0	0	1	0	1	0	0	0	0	0

monitor with ‘1’ triggers an alarm. The matrix has been called as alarm matrix is generated based on the Reference Network shown in Fig.3. The set of monitors which generate alarm on failure is called *Domain* of the faulty(disrupted) component(s). For the sake of simplicity to explain the algorithm, we take the set {M1, M2, M6, M8, M9} that is the domain of ND5 (node 5).

We reduce the number of monitoring devices by applying the approximation algorithm [5]. The main objective is to determine the optimal number of placement of monitors such that no component has null (empty) domain i.e., at least one monitor will raise alarm when the component fails(is attacked) and the components have distinct domains. To implement the above algorithm, first calculate the *hit value* of every column of the alarm matrix. Two different factors have been considered while calculating the hit value of a monitor. Hit value of a column is calculated on the basis of two following factors.

1. We cannot have all-zero rows. So, a column (monitor) is given weight, which gives first 1 to each row.
2. The rows, which have same binary patterns, form a group. The selected column divides some of such groups into distinguishable subgroups. The column, which divides more

groups into more equal (in length) distinguishable subgroups, is given more weight.

The general expression of hit value calculation for jth monitor (M_j) is given by

$$\text{Hit_value}(M_j) = [\sum_{(i=1 \text{ to } R)} (B)] + \sum_{(i=1 \text{ to } p)} (N_i - \text{abs}(N_{1,i} - N_{0,i})) \forall j$$

Where (B) = 1 if the jth column gives the first 1 to ith row
= 0 otherwise

N_i the total number of 0 and 1 in the ith group

N_{1,i} the total number of 1 in the ith group

N_{0,i} the total number of 0 in the ith group

We are choosing the monitors with maximum Hit values one by one as those monitors are optimal monitors(the proof is given on the Appendix). I explain the hit value calculation with the help of Table II.

First, the rows having all zero patterns have been deleted. Now from the above expression of hit value we have hit value of M1= 1+ (7-(6-1)) =3 [as M1 assigns first 1 to ND5 and divides a group of 7 rows having same pattern into two subgroups of 1 and 6 rows]. Similarly hit values of M2=5, M3=6, M4=5, M5=2, M6=6, M7=2, M8=7, M9=4, M10=2, M11=4.

As M8 has the highest Hit value (7) it is chosen first. Now two groups are formed for the selected column M8:

- {ND4, ND5, ND10} having pattern 1 and
- {ND6, ND7, ND8, ND13} having pattern 0

In the next iteration the hit value of M1= (3-(2-1)) + (4-(4-0)) =2 [as M1 does not assign first 1 to any row and does not divide second group into subgroups, but divides the first group {ND4, ND5, ND10} into two subgroups {ND5} and {ND4, ND10}]. Similarly the hit values of M2=2, M3=6, M4=5, M5=3, M6=5, M7=2, M9=2, M10=3, M11=6. So, M3 is selected next.

This selection process continues until domain patterns for all components are distinct. In the pre-computing stage, these domain patterns (see Table III) are stored and used to locate failure(attack) at the time of failure(attack) by comparing the received alarms patterns and stored domain patterns. So, proceeding on in this way the reduced alarm matrix is generated that is shown in Table III.

B. Detecting Single and Multiple Fault(s) and Attack(s)

When one or more monitors raise alarm, the network manager comes to know that there are some faults or attacks in the network. This stage is called Fault Detection stage. So the function of this stage is to make the network manager alert about a possible failure or attack in the network, so that he can run the fault localization algorithm (described later) to localize the faulty (disrupted) components.

C. Locating Single and Multiple Fault(s) and Attack(s)

When there is any fault(disruption) occurred in any component(s) some monitors which are in the domain of that component(s) will trigger alarms. But networks are frequently interrupted with corrupted alarms namely false and miss alarms. If an alarm would be triggered in non-failure(non-attacked) state then this corrupted alarm is supposed to be

false alarm. False alarm corresponds to the scenario where threshold values in the monitoring devices are set low. If an alarm would not be triggered in failure(attack) state then the corrupted alarm is supposed to be miss alarm. Miss alarm corresponds to the scenario where threshold values in the monitoring devices are set high. So, setting the threshold value high will increase the probability of the number of miss alarms and decrease the probability of that of false alarms. On the other hand setting the threshold value low will increase the probability of the number of false alarms and decrease the probability of that of miss alarms.

It is therefore very important to have an algorithm for the correction of false alarms and miss alarms. The fault localization algorithm (which also takes care for corrupted alarms) for the single fault and multiple faults(disruptions) is described below.

Algorithm for Locating Single fault and attack

```

Set_of_singlefault_attack(){
  Initialize an empty set FC=∅
  Search  $\forall C_i \in C$  such that Domain (Ci) = Mr
  Incorporate Ci to the set FC
  FC=FC $\cup$ {Ci}
  for (i=1 to |Mr|){
    Dr = Mr\Mr(i) where Mr(i)∈Mr
    Search  $\forall C_j \in C$  such that Domain (Cj) = Dr
    Add Cj to FC; FC=FC $\cup$ {Cj};
  }
  for (i=1 to |Ms|){
    Br = Mr $\cup$ Ms(i) where Ms(i) ∈Ms
    Search  $\forall C_j \in C$  such that Domain (Cj) = Br
    Add Cj to FC
    FC=FC $\cup$ {Cj}
  }
  for ( i=1 to |Mr|){
    Gr = Mr\Mr(i) where Mr(i)∈Mr
    for (k=1 to |Ms|){
      Lr = Gr $\cup$ Ms(k) where Ms(k) ∈ Ms
      Search  $\forall C_j \in C$  such that Domain (Cj) = Lr
      Add Cj to FC
      FC=FC $\cup$ {Cj}
    }
  }
  Output set FC;
}

```

Algorithm for Locating Multiple faults and attacks

```

Set_of_multiple_fault_attack(){
  Initialize an empty set FC=∅
  Multiplefault_attack(Mr)
  for ( i=1 to |Mr|){
    Dr = Mr\Mr(i) where Mr(i)∈Mr
    Multiplefault_attack(Dr)
  }
  for (i=1 to |Ms|){
    Br = Mr $\cup$ Ms(i) where Ms(i)∈Ms
    Multiplefault_attack(Br)
  }
}

```

```

}
for (i=1 to |Mr|){
  Gr = Mr\Mr(i) where Mr(i) ∈ Mr
  for (k=1 to |Ms|){
    Lr = Gr $\cup$ Ms(k) where Ms(k)∈Ms
    Multiplefault_attack(Lr)
  }
}
Output set FC;
}
Multiplefault_attack(set Mr){
  for (i=1 to |C|){
    search for a component Ci∈C such that Domain (Ci)⊆ Mr
    incorporate Ci to S
    FC=FC $\cup$ {Ci}
  }
}
}

```

We are explaining the localization algorithm by assuming that there may be maximum one false alarm and one miss alarm in the network i.e. we are considering four cases mentioned below:

- i) No false alarm and no miss alarm
- ii) One false alarm and no miss alarm
- iii) No false alarm and one miss alarm
- iv) One false alarm and one miss alarm

In case i) single or multiple fault(disruption) can be detected easily. For other cases many combinations may be possible. Moreover when network intercepts multiple failures(disruptions) at particular point of time, the triggered alarms are intermingled. We obtain a set of probable faulty(disrupted) components as an output of the algorithm

TABLE III
MULTIPLE FAULTS

	M8	M3	M6	M11	M1
ND4	1	0	0	0	0
ND5	1	0	1	0	1
ND6	0	1	0	0	0
ND7	0	1	0	1	0
ND8	0	0	0	1	0
ND10	1	0	1	0	0
ND13	0	0	1	0	0
RAL	1	1	1	0	0

from which the manager has to detect faulty(disrupted) component or components(the proof of surely getting the faulty or disrupted components in FC is shown in the Appendix). I am explaining the algorithm using Table III.

Let us consider at any time the *received alarm* (RAL) has been noticed {1 1 1 0 0} i.e. M3, M6, M8 has raised alarm but M1 and M11 are silent. Here M_r = {M3, M6, M8} and M_s = {M1, M11}. For case i) it is assumed that there are only correct alarms, hence ND5, ND7 and ND8 can be excluded from probable faulty(disrupted) components set. This is because if ND5 fails(is disrupted) then monitor M1 triggers alarm. But in the received alarm it shows that M1 is silent. So,

in general, if there is no alarm triggered from a monitor in the received alarm then the components having that monitor in their domain can be excluded i.e., for any component $C_i \in C$ if $\text{Domain}(C_i) \subseteq M_r$ then C_i is included in the probable faulty(disrupted) component (FC) set. As $\text{Domain}(ND4) \subseteq M_r$, $\text{Domain}(ND6) \subseteq M_r$, $\text{Domain}(ND10) \subseteq M_r$, $\text{Domain}(ND13) \subseteq M_r$, $\{ND4, ND6, ND10, ND13\}$ should be included in FC. Therefore, $FC = \{ND4, ND6, ND10, ND13\}$. RAL is obtained by performing logical OR operation on ND4, ND6, ND10 and ND13 rows [19]. This set strictly includes the probable faulty(disrupted) components for any number of simultaneous failures(attacks).

For case ii), iii), iv) the same concept has been used. Only difference is that there is a possibility of fault(attack) in other components which have not been included in FC because of false alarm and miss alarms. These components would be considered and consequently included in the set. For achieving this we have to consider many other combinations of received alarm patterns.

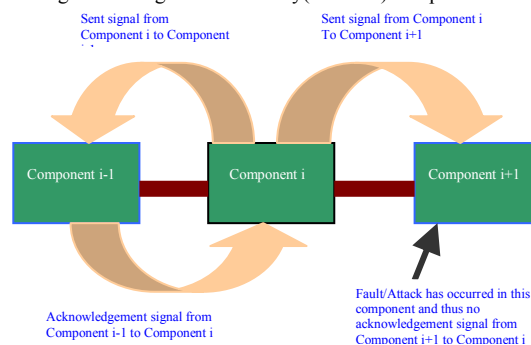
For case ii) we have to make all combination of received alarm pattern considering that there is one false alarm in the network i.e. any one of $M_r = \{M3, M6, M8\}$ has raised an alarm falsely. So we have to eliminate that false alarm from M_r . If D_r is the set of ringing alarms after elimination of false alarm then $D_r = M_r \setminus M_r(i)$ where $M_r(i) \in M_r$. If we eliminate M3 from M_r then the received alarm pattern will be (1 0 1 0 0) i.e. the '1' corresponding to M3 should be replaced by a '0'. Similarly if we eliminate M6 and M8 from M_r then we will get the pattern (1 1 0 0 0) and (0 1 1 0 0) respectively. So, in the above mentioned received alarm pattern three more patterns should be considered. They are $\{(1 1 0 0 0), (1 0 1 0 0), (0 1 1 0 0)\}$. When the pattern is (1 1 0 0 0) then $D_r = \{M3, M8\}$ and as $\text{Domain}(ND4) \subseteq D_r$ and $\text{Domain}(ND6) \subseteq D_r$, ND4 and ND6 should be included in FC. Similarly for the patterns (1 0 1 0 0) and (0 1 1 0 0) we have to include $\{ND4, ND10, ND13\}$ and $\{ND6, ND13\}$ in FN. So, $FC = FC \cup \{ND4, ND6\} \cup \{ND4, ND10, ND13\} \cup \{ND6, ND13\} = \{ND4, ND6, ND10, ND13\}$.

For case iii) there is one miss alarm but no false alarm in the network i.e. any one of $M_s = \{M1, M11\}$ has failed to raise an alarm i.e. any one of M_s should be included in M_r . If B_r is the set of ringing alarms after inclusion of missed alarms then $B_r = M_r \cup M_s(i)$ where $M_s(i) \in M_s$. If M1 has missed the alarm then we have to replaced the '0' corresponding to M1 in RAL by '1' i.e. we will get the pattern (1 1 1 0 1). Similarly if M11 will miss the alarm then we will get the pattern (1 1 1 1 0). So we have two more combinations of received alarm pattern. They are $\{(1 1 1 1 0), (1 1 1 0 1)\}$. For pattern (1 1 1 1 0) $B_r = \{M3, M6, M8, M11\}$ and as $\text{Domain}(ND4) \subseteq B_r$, $\text{Domain}(ND6) \subseteq B_r$, $\text{Domain}(ND7) \subseteq B_r$, $\text{Domain}(ND8) \subseteq B_r$, $\text{Domain}(ND10) \subseteq B_r$ and $\text{Domain}(ND13) \subseteq B_r$, $\{ND4, ND6, ND7, ND8, ND10, ND13\}$ should be included in FC. Similarly for the pattern (1 1 1 0 1), $\{ND4, ND5, ND6, ND10, ND13\}$ should be included in FC. So $FC = FC \cup \{ND4, ND6, ND7, ND8, ND10, ND13\} \cup \{ND4, ND5, ND6, ND10, ND13\} = \{ND4, ND5, ND6, ND7, ND8, ND10, ND13\}$.

For case iv) there are one false alarm and one miss alarm in the network i.e. any one of $M_r = \{M3, M6, M8\}$ has raised an

alarm falsely and at the same time any one of $M_s = \{M1, M11\}$ has failed to raise an alarm. So we have to exclude one of (M3, M6, M8) from M_r and include any one of (M1, M11) to M_r and thus get the set $H_r = M_r \setminus M_r(i) \cup M_s(k)$ where $M_r(i) \in M_r$ and $M_s(k) \in M_s$. If M3 has falsely raised an alarm and M1 has missed the alarm then in RAL the '1' corresponding to M3 will be replaced by '0' and the '0' corresponding to M1 will be replaced by '1'. So we will get the pattern (1 0 1 0 1). Similarly if M3 is false alarm and M11 is missed alarm then we will get the pattern (1 0 1 1 0). So in case iv) we have to consider eight more patterns of RAL. They are $\{(0 1 1 1 0)[M8 \text{ is false alarm and } M11 \text{ is missed alarm}], (0 1 1 0 1)[M8 \text{ is false alarm and } M1 \text{ is missed alarm}], (1 0 1 1 0), (1 0 1 0 1), (1 1 0 1 0)[M6 \text{ is false alarm and } M11 \text{ is missed alarm}], (1 1 0 0 1)[M6 \text{ is false alarm and } M1 \text{ is missed alarm}]\}$. For the pattern (0 1 1 1 0), $H_r = \{M3, M6, M11\}$ and so $\{ND6, ND7, ND8, ND13\}$ should be included in FC. So, proceeding on in this way we will get $FC = \{ND4, ND5, ND6, ND7, ND8, ND10, ND13\}$.

Fig4. Locating the exact faulty(attacked) component



D. Locating the exact faulty(disrupted) component(s)

To locate the exact faulty(disrupted) component(s) the network manager has to send signals to the component(s) which are in FC. If he does not get any acknowledgement signal from that component then he can confirm that the component is faulty (or disrupted), otherwise that component is alright. In Figure 4

the Component i-1 and Component i+1 are the probable faulty(disrupted) components which we got from the attack localization algorithm discussed above. Now the network manager has to confirm which the exact faulty(disrupted) component is. He will send a signal from Component i to Component i-1 as well as to Component i+1. Now if he will get an acknowledgement signal from Component i-1 then he can confirm that Component i-1 is in order. On the other hand if he will not get any acknowledgement signal from Component i+1 then he can say that Component i+1 is faulty(disrupted) and the traffics passing through this component should be rerouted to get rid of the damages in the network.

E. Regeneration of Lightpaths after Single or Multiple Fault(Attack) localization

Lightpaths which are passing through the faulty(attacked) components are added further by the process of their regeneration. This regeneration process is performed so that the new generated path will be the shortest path between the source and destination, and the number of lightpaths is kept more or less stable.

When new lightpaths are generated in the place of dropped lightpaths for passing through the faulty(disrupted) components the topology of the network will change accordingly. The regeneration of these lightpaths has sometimes changed the number of monitor devices spanned across network. We can use the algorithm described below to protect this anomaly and keep a provision of adding new monitors in the network as and when it is required. It leads to update the set of monitoring devices using the same algorithm described early. So the flexibility of the network can be increased with a provision of adding minimum number of new monitor devices.

Algorithm for updating the monitors after fault(attack) localization

```

Initialize an empty set  $T = \emptyset$ 
 $S \leftarrow$  set of all optimal monitoring devices that are already taken
Update alarmmatrix()
 $T = T \cup S$ 
while (for any  $R_i, R_j \in R, R_i = R_j$  such that  $i \neq j$ ) {
     $\forall M_p \in M$  and  $M_p \notin T$ 
     $H_p \leftarrow$  hit ratio of ( $M_p$ )
    if ( $H_r > H_q \forall H_q \in H$  and  $r \neq q$ ) {
         $T = T \cup M_r$ 
    }
}
Output T

```

V. SIMULATION PERFORMANCE

To evaluate the effectiveness of the proposed scheme I have implemented them in different network topologies such as EuroNet and NSFNet. I have shown results on EuroNet only that has 28 physical nodes.

Fig.5. Number of elements in faulty set vs. load

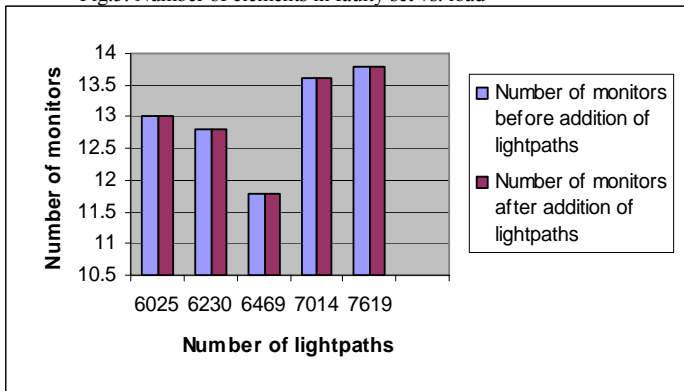


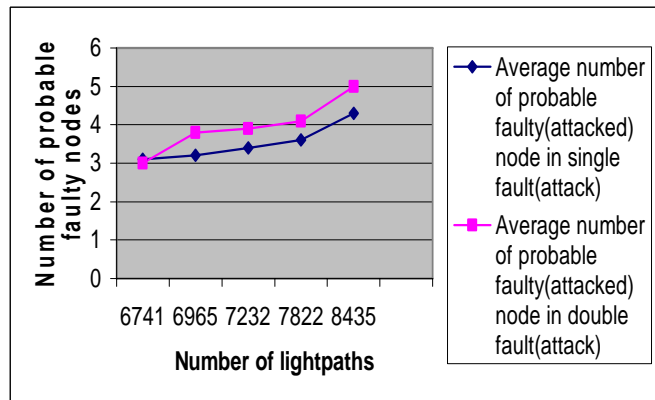
Fig. 5 shows that the number of monitoring devices changes with the increase of lightpaths i.e., the change of traffic load in the network. New lightpaths are added to a network when its

traffic increases rapidly or in the regeneration process when any nodes come under faults.

To make this traffic-intensive network survivable we need to add more monitoring devices attached to critical nodes in the network. But in order to make the scheme scalable and cost effective we must make sure that this number of adding new devices is least. It is clear from Fig. 5 that when more lightpaths are added the number of monitors required is not changed. I have increased the number of lightpaths by 10% to 12% the number of monitors in the network has more or less remained same. Therefore, we can mention that the algorithm is scalable.

Fig. 6 shows that the cardinality of the set of possible faulty(attacked) nodes in the case of single and double faults(attacks) varies marginally with the change of the number of lightpaths. This figure represents the output set of fault(attack) localization algorithm i.e., the set of probable faulty(attacked) nodes in the network for single/double faults(attacks). From Fig. 6 it is clear that the cardinality of the set increases with the increase of lightpaths. In the case of single fault(attack) the number of probable faulty(attacked) nodes increases very slowly while in double faults(attacks) the set cardinality increases little more higher when the number of

Fig.6. Number of elements in faulty set vs. load



lightpaths increases.

Fig. 7 shows that the number of monitoring devices remains more or less same with the change of lightpaths in three different situations namely a) during a single fault(attack), b) after single fault(attack) and c) after addition of a new monitor (node) in the network. This graph clearly indicates that the optimal placement of monitoring devices through the proposed scheme caters different conditions of network with the change of traffic loads. The optimal number of monitoring devices lies within 15 to 16 for 28 physical nodes (locations) placed in EuroNet. Like Fig.7, Fig. 8 shows similar scenario in the case of double faults(attacks). In this case, the number of monitoring devices lies within 15 to 16.

Fig.7. Number of monitor in different load before single fault, after single fault and after addition of a new node

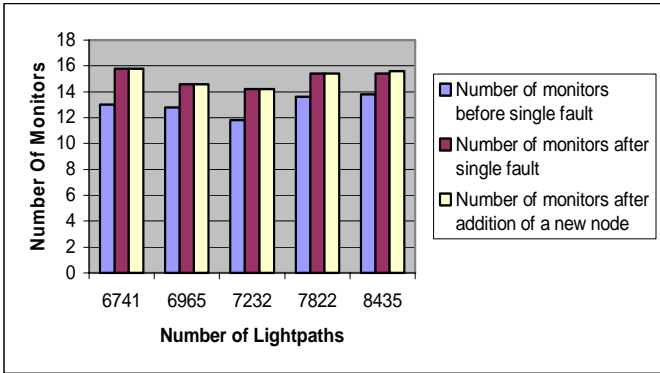
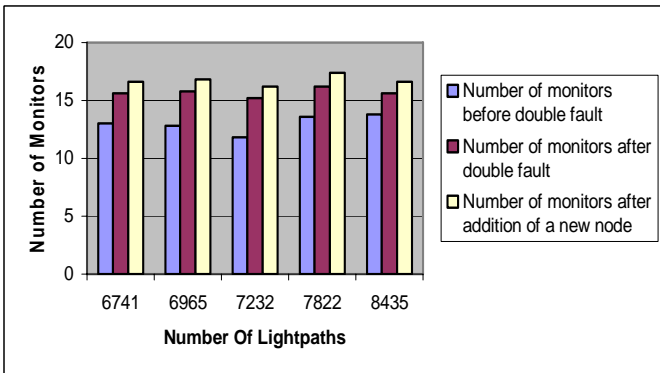


Fig. 8: Number of monitor in different load before double fault, after double fault and addition of a new node



From Fig. 7 and Fig. 8, it is clear that after addition of an extra node in the network with change of lightpaths during single/double fault(attack), the number of devices is varying within 15 to 17 i.e., effectively one extra monitoring device is required in EuroNet. Thus the dynamic nature of the network is achieved and the cost has also been reduced as the number of monitor devices is kept within the optimal figure obtained through their initial placements by the scheme.

C. Comparison between the proposed scheme and algorithm discussed in [1]

I have compared the proposed scheme with the algorithm given in [1] specifically on the fault localization i.e., how the cardinality of the set of faulty nodes varies in both schemes showing side by side. The comparisons have been done on the network of [1] and the results have been shown in Fig. 9 and Fig. 10 for single and double fault(s) respectively.

It has been seen that the cardinality of the set is less in the proposed algorithm than that of other algorithm stated in [1]. The proposed scheme locates the exact faulty component(s) in single or double fault(s). Thus according to the proposed scheme the cardinality of the faulty set is 1(for single fault) and 2(for double fault) against the number of physical nodes varies from 10 to 13 in the network. This cardinality set generated from the other algorithm [1] is higher in both cases.

Fig.9. Comparison of single fault

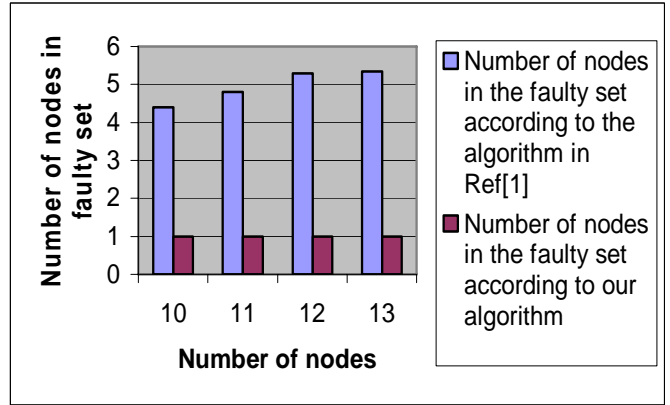
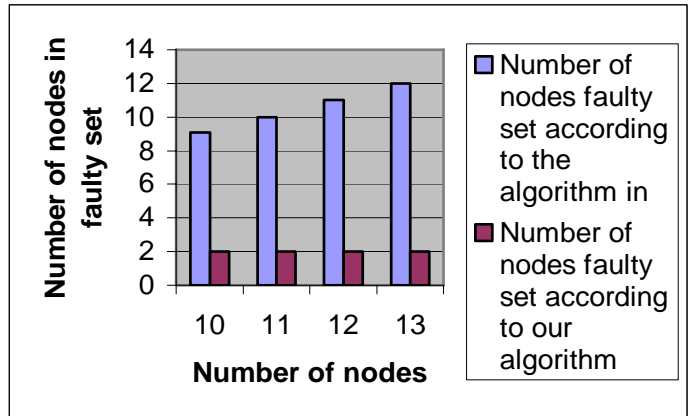


Fig. 10. Comparison of double fault



Therefore, this proposed algorithm performs better in locating faults than existing one [1].

VI. CONCLUSION

In this paper two-phased scheme containing (a) the detection of faults(attacks) through monitoring devices raising alarms (fault or attack detection) and (b) subsequently the localization of these faults and attacks (fault or attack localization) has been presented by invoking an algorithm and then by sending and receiving signals. I have shown the performance of the scheme on 28-node EuroNet and also compared fault localization scheme with an existing algorithm [1]. Clearly, it has been found that the proposed algorithm outperforms the existing one in the case locating faulty components in the network.

APPENDIX

Theorem 1:- The monitors with highest hit values will give optimal result i.e. those monitors will divide more groups into more distinguishable subgroups.

Proof:- The general expression of hit value calculation for jth monitor (M_j) is given by

$$\text{Hit_value}(M_j) = \left[\sum_{(i=1 \text{ to } R)} (B) \right] + \sum_{(i=1 \text{ to } p)} (N_i - \text{abs}(N_{1,i} - N_{0,i})) \quad \forall j$$

Where (B) = 1 if the jth column gives the first 1 to ith row
= 0 otherwise

N_i the total number of 0 and 1 in the ith group

$N_{1,i}$ the total number of 1 in the ith group

$N_{0,i}$ the total number of 0 in the ith group

We are giving weight to those monitors whose Hit values are maximum.

The first term ($\sum_{(i=1 \text{ to } R)} (B)$) is giving weight to those monitors which are giving first 1 in each row because we cannot have all 0 rows.

The second term ($\sum_{(i=1 \text{ to } p)} (N_i - \text{abs}(N_{1,i} - N_{0,i}))$) will be maximum if $\text{abs}(N_{1,i} - N_{0,i})$ will be minimum. I am proving this (for optimal monitors $\text{abs}(N_{1,i} - N_{0,i})$ will be minimum) with the help of Fig 11. Let the total number of component in the network is N_0 . Now the most optimal monitor divides N_0 into N_1 (number of components whose entry in the Alarmmatrix is 0) and N_2 (number of components whose entry in the Alarmmatrix is 1). Similarly the next optimal monitor divides N_1 into N_3 and N_4 and N_2 into N_5 and N_6 . This process will go on until the domains of all the components are distinct. Now we will reduce the number of optimal monitors i.e. the height of the tree (in Fig 11) as small as possible. Now for any number of components P_i the height of the tree is given by $\text{Height}(N_i) = \text{Max}\{\text{Height}(N_j), \text{Height}(N_k)\} + 1$.

Now for all N_i, N_j, N_k $\text{Height}(N_i) \propto N_i, \text{Height}(N_j) \propto N_j, \text{Height}(N_k) \propto N_k$.

Now, $\text{Height}(N_i)$ will be minimum

$$\Rightarrow \text{Max}\{\text{Height}(N_j), \text{Height}(N_k)\} \text{ will be minimum}$$

$$\Rightarrow \text{Max}\{N_j, N_k\} \text{ will be minimum}$$

Now as $N_i = N_j + N_k$, so $\text{Max}\{N_j, N_k\}$ will be minimum if and

only if $\text{abs}(N_j - N_k)$ will be minimum i.e. N_j and N_k should be as close as possible. Thus our motivation has been fulfilled and the theorem has been thus proved.

Theorem 2:- In the fault(attack) localization algorithm we will surely get the exact faulty(disrupted) components in the Faulty Component(FC) set.

Proof:- Suppose among all the nodes of the set $C = \{C_1, C_2, \dots, C_b, \dots, C_n\}$, C_f is the faulty(disrupted) component. Let M_r consists of all the ringing monitors $M_1, M_2, \dots, M_i, M_j, M_k, \dots, M_m$. Now I am discussing case i), case ii), case iii) and case iv) separately. For case i) there are no false alarm and no miss alarm. So, all the monitors which are in the domain of C_f will be in M_r i.e. $\text{Domain}(C_f) \subseteq M_r$. So, we will get the component C_f in the set FC .

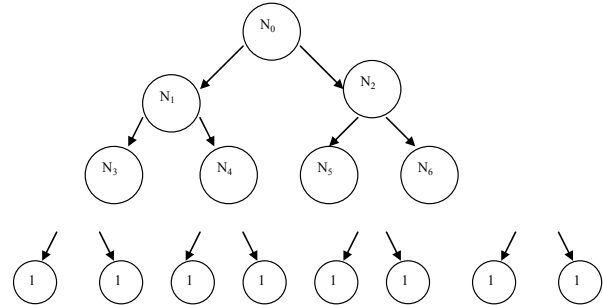
Now in case ii) there is one false alarm and no miss alarm in the network. Let M_i is the false alarm which is in M_r . Now in

the localization algorithm we are doing $D_r = M_r \setminus M_i(i)$ where $M_r(i) \in M_r$. So, M_i will be eliminated from D_r as $M_i \in M_r$. Now $\text{Domain}(C_f) \subseteq D_r$ and so we will get C_f in the set FC . In case iii) there is one miss alarm and no false alarm in the network. Let M_j is the miss alarm which is in M_s . Now in the localization algorithm we are doing $B_r = M_r \cup M_s(i)$ where $M_s(i) \in M_s$. So, M_j will be included in B_r as $M_j \in M_s$. Now $\text{Domain}(C_f) \subseteq B_r$ and so we will get C_f in the set FC . In case iv) there is one false alarm and one miss alarm in the network. Let M_i is the false alarm which is in M_r and M_j is the miss alarm which is in M_s . Now in the localization algorithm we are doing $L_r = M_r \setminus M_i(i)$ where $M_r(i) \in M_r$ and $G_r = L_r \cup M_s$ where $M_s(i) \in M_s$. So, M_i will be eliminated from G_r as $M_i \in M_r$ and M_j will be included in G_r as $M_j \in M_s$. Now $\text{Domain}(C_f) \subseteq G_r$ and so we will get C_f in the set FC . So in any of the four cases the localization algorithm will give C_f in the set FC . Thus the theorem can be proved.

REFERENCES

- [1] C. Mas and P. Thiran, "An Efficient Algorithm for Locating Soft and Hard Failures in WDM Networks", IEEE Journal of Selected Areas of

Fig 11: Topology of a network of N_0 components



- Communications, Vol. 18, No. 10, Oct 2000, pp 1900-1911.
- [2] I. Katzela, G. Ellinas, W. S. Yoon, T. E. Stern, "Fault Diagnosis in optical networks", Journal of High Speed Networks, Vol. 10, no. 4, 2001, pp. 269-91.
- [3] R. H. Deng, A. A. Lazar, W. Wang, "A probabilistic Approach to Fault Diagnosis in Linear Lightwave Networks". IEEE JSAC Vol. 11, No. 9, pp 1438-1448.
- [4] S. Stanic, S. Subramaniam, H. Choi, G. Sahin and H.-Ah Choi, "On Monitoring Transparent Optical Networks", Proceeding of the International Conference on Parallel Processing Workshops (ICPPW), 2002.
- [5] P. Nayek, S. Pal, B. Choudhury, A. Mukherjee, D. Saha and M. Nasipuri, "Optimal Monitor Placement Scheme for Single Fault Detection in Optical Network", 7th International Conference on Transparent Optical Networks ICTON 2005, Barcelona, Spain, July 3-7, 2005.
- [6] Mas, C., Nguyen, H., Thiran, P.: Failure location in WDM networks. In: Optical WDM Networks: Past Lessons and Path Ahead. Kluwer Academic Publishers (2004)
- [7] H. Nguyen, P. Thiran "Failure Location in Transparent Optical Networks: The Asymmetry Between False and Missing Alarms" Proceedings of The 19th International Teletraffic Congress (ITC19), Beijing, China, August 2005

- [8] N. S. V. Rao. Computational Complexity Issues in Operative Diagnosis of graph-based Systems. *IEEE Transactions on Computers*, 42(4):447–457, April 1993.
- [9] S. Abek H. Hegerin and B. Neumair. *Integrated Management of Networked Systems*. Morgan Kaufmann Publishers, 1998.
- [10] R. Gardner and D. Harle. Alarm Correlation and Network Fault Resolution using Kohonen Self-Organising Map. *Globecom 97 proceedings*, pages 1398–1402, 1997.
- [11] C. Rodriguez, S. Rementeria, J. I. Martin, A. Lafuente, J. Muguerza, and J. Perez. A Modular Neural Network approach to Fault Diagnosis. *IEEE Transactions on Neural Networks*, 7(2):326–340, March 1996.
- [12] C. S. Li and R. Ramaswami. Fault Detection and Isolation in transparent All-Optical Networks. *IBM Research Report, RC-20028*, April 1995.
- [13] C. Wang and M. Schwartz. Fault Detection with Multiple Observers. *IEEE INFOCOM Proc.*, pages 2187–2196, 1992.
- [14] A.T. Bouloutas, G. W. Hart, and M. Schwartz. Fault Identification Using a FSM model with Unreliable Partially Observed Data Sequences. *IEEE Transactions on Communications*, 41(7):1074–1083, July 1993.
- [15] Carmen Mas and P. Thiran. A review on fault location methods and their application to optical networks. *Optical Networks Magazine*, 2(4), July/August 2001.
- [16] N. S. V. Rao. On Parallel Algorithms for Single-Fault Diagnosis in Fault Propagation Graph Systems. *IEEE Transactions on Parallel and Distributed Systems*, 7(12):1217–1223, December 1996.
- [17] J. Kleer and B.C. Williams. *Diagnosing multiple faults-Artificial Intelligence*, volume 32. Elsevier Science Publishers, 1987.
- [18] Y. Y. Yang and R. Sankar. Automatic failure isolation and reconfiguration. *IEEE Network*, pages 44–53, September 1993.
- [19] S. Pal, P. Nayek and A. Mukherjee, “Fault Localization Scheme for Multiple Failures in Optical Networks”, *Proceeding of SNCNW 2006*, Lule, Sweden
- [20] R. Rejeb, M. S. Leeson, and R. J. Green, “Cost Optimization Method for Multiple Attack Localization and Identification in All-Optical Networks”, *ICTON 2005*, pages 101-106
- [21] R. Rejeb, M. S. Leeson, and R. J. Green, “Fault and Attack Management in All-Optical Networks”, *IEEE Communications Magazine*, November 2006, pages. 79-86
- [22] R. Rejeb, M. S. Leeson, and R. J. Green, “Multiple Attack Localization And Identification in All-Optical Networks”, *Opt. Switching and Net.*, vol. 3, no. 1, 2006, pp. 41-49