Optical Switching and Networking 8 (2011) 46–55

Contents lists available at ScienceDirect

Optical Switching and Networking

journal homepage: www.elsevier.com/locate/osn

Minimal monitor activation and fault localization in optical networks

Amitangshu Pal [a], Amitava Mukherjee [b,*], Mrinal K. Naskar [c], Mita Nasipuri [a]

[a] Department of CSE, Jadavpur University, Calcutta 700 032, India
[b] IBM India Pvt. Ltd., Salt Lake, Calcutta 700091, India
[c] Department of ETCE, Jadavpur University, Calcutta 700 032, India

ARTICLE INFO

Article history:
Received 28 July 2009
Received in revised form 11 June 2010
Accepted 22 June 2010
Available online 24 July 2010

Keywords:
Optical network
Fault detection
Fault localization
Optimal monitor placement

ABSTRACT

The scheme for efficient, accurate and scalable monitoring and localizing faults is necessary for transparent optical networks. Optical transparency makes the monitoring and localization process difficult in the optical layer as failures in physical layer propagate and subsequently generate multiple alarms throughout the network. Moreover, failures in physical layer could be detected and located in optical layer before they are propagated to the upper layer. So, a fast and scalable monitoring and fault localization scheme are required to offer a secure and resilient network. In this paper we propose a fault management scheme that handles multiple failures in the optical network using wavelength-division multiplexing (WDM) technology. It consists of a two-phase scheme, namely (a) fault *detection* which detects faults by raising alarms of the monitoring devices and (b) fault *localization* that subsequently localizes these faults by invoking an algorithm. The latter phase obtains a set of potential faulty nodes (links). Next, we locate the exact position of faulty node (link) by transmitting the signal through it. We demonstrate the performance of this proposed scheme on a 28-node EuroNet.

1. Introduction

High capacity optical network is immensely used in industries due to its large transmission bandwidth and low cost. But these networks are also vulnerable to failures (such as malfunctioning of optical devices, fibre cuts, soft failures, i.e., the impairment due to subtle changes in signal power like degrading signal-to-noise ratio (SNR), etc.). One of the most important requirements to ensure survivable high speed optical network is to manage fault detection and its localization. A single failure can cause millions of dollars of revenue loss right from corporate users to service providers. Consequently, fault management is essential to ensure uninterrupted services to users. Faults (like link and/or node failures, etc.) occur mainly due to natural fatigue and ageing of optical devices and components (i.e., transmitters, receivers or controllers). Besides failures there are different types of disruptions (i.e., impairment, attack, etc.) that degrade and disrupt the performance of the network. If a fault occurs in a device it remains disabled until it is repaired again.

The management system involves in detecting faults in the network and alerting 'manager' through alarms triggered by monitoring devices when fault 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 a link (e.g., fibre cut) gets damaged. When the power level of an incoming signal drops below a certain range it causes a loss of signal (LOS) and monitoring equipments raise alarms. Fault management is an important management function that is responsible for fault detection, localization and recovery. In this work we discuss only detection of faults and their localization. The block diagram of the proposed scheme is shown in Fig. 1.

* Corresponding author.
E-mail addresses: amitangshupal@yahoo.co.in (A. Pal), amitava.mukherjee@in.ibm.com (A. Mukherjee), mrinalnaskar@yahoo.co.in (M.K. Naskar), nasipuri@vsnl.com (M. Nasipuri).

1573-4277/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.osn.2010.06.002

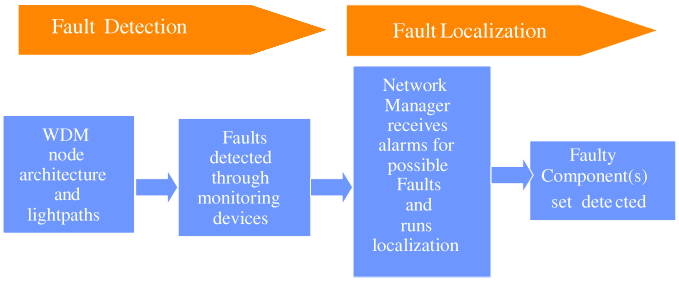

Fig. 1. Proposed fault detection and localization scheme.

Whenever there is a failure in a node, all the lightpaths passing through that node get disrupted and monitoring elements (monitoring devices and/or self-alarmed optical devices e.g., transmitter, receiver, etc.) placed in the path triggered alarms. Thus, a single failure may generate multiple alarms. In the case of multiple failures occurred in a number of nodes or in links simultaneously the raised alarms are intermingled and thus make the detection and subsequent localization process complex. Both single and multiple failures are detected through monitoring devices by triggering alarms. In order to develop 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. This will reduce alarm processing time as well as ambiguity in fault localization. Thus in our work we assume that monitors are placed at all nodes. During runtime, as the traffic changes, it is necessary to identify the minimum number of monitors to be turned ON so that failures can be localized using the currently established lightpaths.

The first phase of our proposed scheme is thus to select the monitoring devices that should be turned ON, and detects the failure(s) in the network components. As mentioned earlier this selective monitor activation has the advantages of reduced alarms processing time and thus has enhanced fault localization capability in a shorter time. In the second phase, the localization algorithm is invoked to locate faults and gives a set of apparent faulty components. In real scenario corrupted alarms (false alarms and miss alarms) may be triggered in the network to make the localization process more difficult. The false alarms and miss alarms are controlled by tuning the threshold values of the monitoring equipments. Lastly, the network manager sends test signals to the apparent faulty components and will locate the exact faulty components based on the acknowledgements. In this paper, we interchangeably use monitor and monitoring device.

1.1. Motivation

For critical business application running on optical networks, the 99.999% uptime of services is a critical requirement. This requirement corresponds to the connection downtime of less than five minutes per year. Hence, alerting manager appropriately through alarms triggered from upcoming faults and consequently detecting and localizing faults are prime activities in the network management. Fault diagnosis and localization is an interesting problem and hence it is an active field of research. Stanic et al. [1,2] used approximation method to reduce the number of monitors and thus make the system cost effective. Another approximation algorithm was shown in [3] to reduce the number of monitoring elements. A number of approaches based on graph theory were investigated in the context of fault diagnosis. In [4,5], authors proposed a parallel approach based on zero-time and nonzero-time systems and discussed an approach for single fault diagnosis. In [4], author showed that the optimal placement of monitors is an NP-hard problem. Several authors considered different assumptions for solving the fault localization problem. In [5,6] only single failure was assumed while in [7–9] multiple simultaneous faults were considered. In [6], fault manager checked periodically powers of all source and destination nodes by using the routing table information. If power level of some of nodes was out of expected bounds, that node was identified as a possible faulty node. In [10], the authors proposed fault identification algorithm through filtering alarms. The authors used the fault identification tree of depth equal to the number of alarming components to narrow down the potential faulty sources. In [11,12], a fault detection scheme was presented which is based on decomposition of network topology into monitoring cycles. The authors used a heuristic scheme for constructing of monitoring cycle cover that minimized cycle overlap for a given network topology. In [13], a hierarchically distributed monitoring model was proposed where the network topology is logically partitioned into monitoring domains, each of which is assigned a hierarchy level. Every monitoring domain is assigned a local fault manager responsible for computing the optimal set of activated monitors and performing the fault localization for all components within its domain, which enables distributed optimization of monitor activation and fault localization. In [14], an adaptive technique for fault diagnosis using "probes" was presented in which probes are established sequentially, each time using information about already established probes. While the sequential probing helps to achieve adaptive it also increases the fault localization time. In [7,15,16] false alarms and miss alarms were considered. In [15], authors showed that false alarms could be corrected in polynomial time but the correction of miss alarms is NP-hard. In [17], the authors propose an approach that equips only a few nodes with monitors and then based on the locations of monitors a heuristic approach is proposed for constructing monitoring cycles.

In our approach (follows our previous work described in [18–20]) we assume that all nodes are equipped with

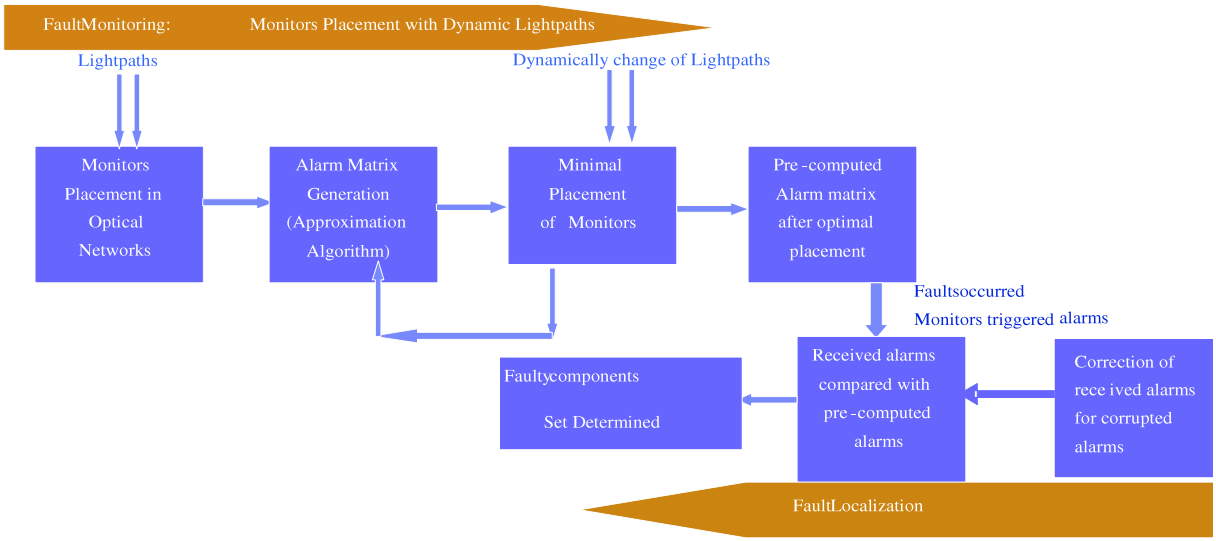

Fig. 2. Different stages of our proposed scheme.

monitors and reduce fault localization time with a minimal number of monitors activated. Most of the earlier research work posed the problem as monitor placement problem. But in real-life networks having the topology with dynamic nature that would be changed with traffic volumes, we assume monitors placed at all nodes in those networks. In our proposed fault detection and localization scheme, the activation of placed monitors is minimal based on traffic demand where fault propagates monitors from a source through those downstream in the network. A mechanism of locating the exact faulty components is also mentioned in this paper.

1.2. Our contribution

Dynamic scenario means that a set of lightpaths is added to a network at any point of time while a set of lightpaths are cut off due to some unexpected events like damage of fibre, failure of equipment, etc. First, we minimize the total number of monitoring devices to be activated in the network. The activation of monitors in the network (same as optimal monitor placement in literature) is proven to be a NP-hard problem. We propose an approximation algorithm in selecting the minimum number of monitors that should be activated such that all the faults can be detected. The pre-computed alarm matrix is the output of the approximation algorithm for optimal placement of monitoring devices.

Second, failures are located from the received alarms. After receiving alarms from monitoring devices, irrespective of types of alarms, localization algorithm is invoked and it compares received alarms with pre-computed alarm matrix generated in the monitor placement phase. This comparison will produce a set of apparent faulty components. Next, we have proposed a scheme to locate the exact location of faulty component(s) by the process of sending and receiving signals. In summary, the two-phased scheme has four important features (i) minimizing the number of monitoring devices that need to be activated, (ii) in case of change in network topology, some new monitors are turned ON while some are turned OFF, (iii) locating and subsequently localizing multiple simultaneous faults and (iv) handling the effect of false and miss alarms in the network. The different stages of our proposed scheme are shown in Fig. 2.

The rest of the paper is organized as follows. Section 2 describes network model and notations. Section 3 discusses our proposed scheme. Section 4 presents simulation performance. Finally we conclude our work in Section 5.

2. Network model and notation

2.1. 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 occurred at a node or a fibre cut will disrupt the connectivity and disconnect all lightpaths passing through node or in link. Fig. 3 shows a 14-node NSFnet. We denote ND as the set of optical components and M as the set of monitors.

In Fig. 3, we show lightpaths passing through different cities. Let us consider that fault occurs in TX. Then this fault will propagate through the paths TX–CO–UT (marked in light blue), TX–MD (marked in light green), TX–MD–NY (marked in dark gray) and TX–MD–NJ (marked in orange), and consequently M_1, M_2, M_6, M_8 and M_9 will trigger alarm. In this way, a single fault generates multiple alarms.

2.2. Notations, definitions, and preliminaries

In our discussion we use the following notations throughout the paper as shown in Table 1.

We define the term *domain*of the faulty component(s) by the set of monitors which generate alarms on failures.

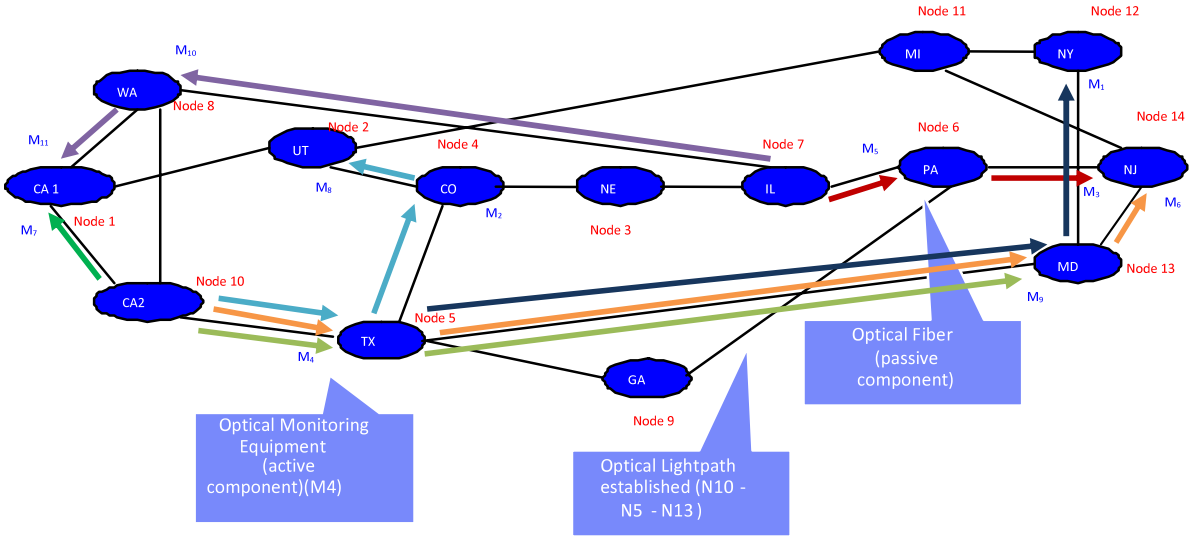

Fig. 3. Reference NSFNet. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Table 1
Notation.

LP	← the set of lightpaths
ND	← set of all components
R	← set of all rows indicating components
M	← set of all monitors
M_r	← set of all triggering alarms
M_s	← set of all silent alarms
H	← set of all hit values
FC	← set of probable faulty components

Domain can be expressed by a Boolean relation as follows. Let the term *position* (ND_i, LP_j) is defined as the distance of ND_i from the source of lightpath LP_j. Now $M_k \in M$ ($k \in [1, |M|]$) will be in the domain of (ND_i) for $ND_i \in ND$ if the following conditions are satisfied.

(i) if $ND_i \in LP_j$ and $M_k \in LP_j$ i.e., both ND_i and M_k belongs to the same lightpath.
(ii) $\exists LP_j \in LP$ such that *position* (ND_i, LP_j) $<$ *position* (M_k, LP_j) i.e., M_k is in the downstream of ND_i in lightpath LP_j.

3. Proposed scheme

3.1. Fault monitoring: minimal monitor activation with dynamic lightpaths

Monitors are initially placed to all possible locations so that the failures can be detected and located for any components distinctly [3]. In Fig. 3, M_1–M_{11} i.e., 11 monitoring devices are placed to achieve maximum coverage. We propose a greedy algorithm which determines the optimal number of monitors from the set of monitors in such a way that failures 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 occurs in a component it must not remain undetected. The algorithm is described below [3,18–20].

Algorithm for minimal monitor activation.

1. Initialize an empty set $S = \varnothing$
2. While (for any $R_i, R_j \in R$, $R_i = R_j$ such that $i \neq j$){
3. $\forall M_p \in M$ and $M_p \notin S$, $p \in [1, |M|]$
4. $H_p \leftarrow$ hit value of (M_p).
5. if ($H_r > H_q \; \forall H_q \in H$ and $r \neq q$){
6. $S = S \cup M_r$
7. }
8. }
9. Output S

We explain our algorithm using Table 2. In Table 2, '1' denotes that if a node fails the monitor with '1' triggers an alarm. The matrix we call 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 component(s). As an example in Fig. 3, the set $\{M_1, M_2, M_6, M_8, M_9\}$ is the domain of ND_5 (node 5).

We reduce the number of monitors by applying the approximation algorithm [3]. The main objective is to determine the optimal number of monitors such that no component has null (empty) domain i.e., there is at least one monitor which raises alarm when the component fails and the components have distinct domains. To implement the above algorithm we calculate the *hit value* of every column of the alarm matrix. Hit value of a column is calculated on the basis of following two factors.

1. We cannot have all zero rows. So, a column (monitor) is given a weight, which assigns 1 initially 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 subgroups into more equal (in length) distinguishable subgroups, is assigned more weight.

Table 2
Alarm matrix for reference network.

	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}
ND_4	0	0	0	0	0	0	0	1	0	0	0
ND_5	1	1	0	0	0	1	0	1	1	0	0
ND_6	0	0	1	0	0	0	0	0	0	0	0
ND_7	0	0	1	0	1	0	0	0	0	1	1
ND_8	0	0	0	0	0	0	0	0	0	0	1
ND_{10}	0	1	0	1	0	1	1	1	1	0	0
ND_{13}	1	0	0	0	0	1	0	0	0	0	0

The general expression for evaluating the hit value for the jth monitor (M_j) is given by

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

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

N_i: total number of 0's and 1's in the ith group

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

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

P: Number of groups having the same alarm pattern.

The monitors with maximum hit values are selected one by one as they are optimal one. We explain the calculation of hit value with the help of Table 2.

First, the rows having all zero patterns are deleted. These rows correspond to the nodes that are either ending lightpath nodes or idle nodes, i.e. these nodes are not taking part in any lightpath. For example in Fig. 3, Node 1, Node 2, Node 12, Node 14 are end lightpath nodes and Node 3, Node 9, Node 11 are idle nodes. So, the rows correspond to these nodes are deleted in Table 2. Failures in these nodes cannot be detected in our scheme. We calculate hit value for $M_1 = 2 + (7 - (5 - 2)) = 6$ [as M_1 assigns first 1 to ND_5 and ND_{13} and divides a group of 7 rows having same pattern into two subgroups of 2 and 5 rows]. Similarly hit values for $M_2 = 6, M_3 = 6, M_4 = 3, M_5 = 3, M_6 = 9, M_7 = 3, M_8 = 9, M_9 = 6, M_{10} = 3, M_{11} = 6$. As M_8 (chosen randomly between M_6 and M_8) has the highest Hit value (9) it is taken first. Two groups are formed for the selected column M_8: {ND_4, ND_5, ND_{10}} having pattern 1 and {ND_6, ND_7, ND_8, ND_{13}} having pattern 0.

In the next iteration the hit value for $M_1 = 1 + (3 - (2 - 1)) + (4 - (3 - 1)) = 5$ [as M_1 does not assign first 1 to any row and divides first group {ND_4, ND_5, ND_{10}} into two subgroups {ND_5} and {ND_4, ND_{10}} and second group {ND_6, ND_7, ND_8, ND_{13}} into two subgroups {ND_6, ND_7, ND_8} and {ND_{13}}]. Similarly the hit values for $M_2 = 2, M_3 = 6, M_4 = 2, M_5 = 3, M_6 = 5, M_7 = 2, M_9 = 2, M_{10} = 3, M_{11} = 6$. So, M_3 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 3) are stored and used to locate failure at the time of fault by comparing received alarms patterns with stored domain patterns. So, proceeding on in this way the reduced alarm matrix is generated that is shown in Table 3.

Table 3
Reduced alarm matrix.

	M_8	M_3	M_6	M_{11}	M_1
ND_4	1	0	0	0	0
ND_5	1	0	1	0	1
ND_6	0	1	0	0	0
ND_7	0	1	0	1	0
ND_8	0	0	0	1	0
ND_{10}	1	0	1	0	0
ND_{13}	0	0	1	0	1
RAL	1	0	1	0	0

Significance of Hit_value: We discuss the significance of Hit_value with the help of Fig. 4. In Fig. 4, first monitor M_8 divides all the nodes into two subgroups. Similarly, the other monitors divide all the nodes into different subgroups so that each node failure gives a distinct alarm pattern. The term Hit_value is the sum of two arguments. The first term (B) gives priority to the monitors that give first 1 to any node. As an example if we would choose $\{M_8, M_3, M_6, M_{10}, M_1\}$ instead of $\{M_8, M_3, M_6, M_{11}, M_1\}$ then we would not get any alarm in case of failure in ND_8. Thus failure of ND_8 would remain unattended. Thus our scheme gives some priority to M_{11} as it gives first 1 to ND_8.

The second term in the expression of *Hit_value* gives more weight to the monitor that divides a group of nodes into more equal length subgroups. As an example M_8 divides all the nodes into two subgroups of length 4 (ND_6, ND_7, ND_8, ND_{13}) and 3 (ND_4, ND_5, ND_{10}). Thus the scheme gives more weight to M_8. This can be observed from Fig. 4 that the number of alarms required to detect failures in all the nodes is the height of the tree. Now, the height of the tree will be small if the monitors divide the nodes into two subgroups with equal length (or almost equal). This is the significance of the second term.

Theoretical bounds on number of monitors: The theoretical bound of number of monitors are hard to get and strongly dependent on the Alarm Matrix. It can be seen from Fig. 4 that the minimal number of is equal to the height of the binary tree. Now if we assume that there are n nodes in a network, then in the best case i.e., the minimum height a binary tree is $\log_2(n)$ and in worst case, i.e. the maximum height of a binary tree is n. Thus on an average, the height (number of monitors) of the tree is $1/2(\log_2(n) + n)$.

3.2. Detecting single and multiple fault(s)

When one or more monitors raise alarm, the network manager comes to know that there are one or more faults occurred in the network. This stage is called Fault Detection

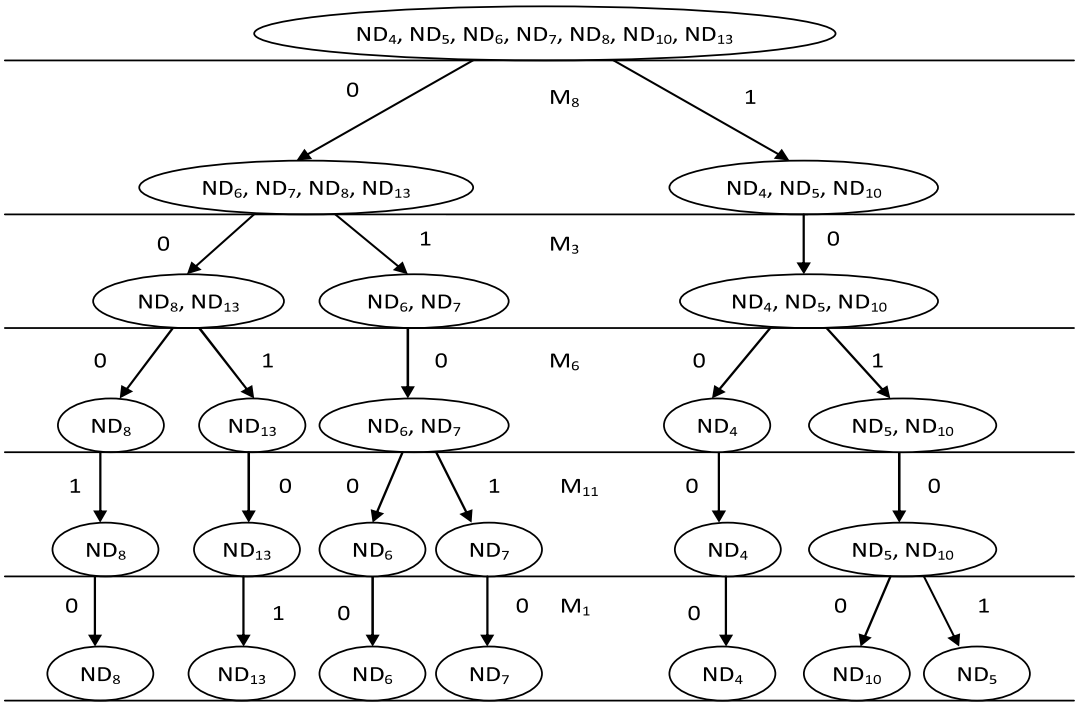

Fig. 4. Monitor selection based on Hit_value.

stage. The function of this stage is to make the network manager alert about a possible failure in the network, one can run the fault localization algorithm (described latter) to localize the faulty components.

3.3. Locating single and multiple fault(s)

When there is any fault occurred in any component(s) some monitors which are in the domain of that component(s) trigger alarms. But networks are frequently interrupted with corrupted alarms namely false and miss alarms. If an alarm is triggered in non-failure 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 is not to be triggered in the failure 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. The fault localization algorithm (which also takes care for corrupted alarms) for the single and multiple faults is described below.

Algorithm for locating single fault

1. Set_of_singlefault(){
2. Initialize an empty set FC $= \varnothing$
3. Search $\forall C_i \in C$ such that Domain $(C_i) = M_r$ /∗ Checks when there is no false alarm and no missed alarm ∗/
4. Incorporate C_i to the set FC
5. FC = FC $\cup$ C_i
6. for ($i = 1$ to $|M_r|$) {
7. $D_r = M_r \setminus M_r(i)$ where $M_r(i) \in M_r$
8. Search $\forall C_j \in C$ such that Domain $(C_j) = D_r$ /∗ Checks when there is one false alarm and no missed alarm ∗/
9. Add C_j to FC
10. FC = FC $\cup$ $\{C_j\}$
11. }
12. for ($i = 1$ to $|M_s|$){
13. $B_r = M_r \cup M_s(i)$ where $M_s(i) \in M_s$
14. Search $\forall C_j \in C$ such that Domain $(C_j) = B_r$ /∗ Checks when there is no false alarm and one missed alarm ∗/
15. Add C_j to FC
16. FC = FC $\cup$ $\{C_j\}$
17. }
18. Output set FC
19. }

Algorithm for locating multiple faults

1. Set_of_multiple_fault(){
2. Initialize an empty set FC $= \varnothing$
3. Multiplefault(M_r) /∗ Checks when there is no false alarm and no missed alarm ∗/
4. for ($i = 1$ to $|M_r|$){
5. $D_r = M_r \setminus M_r(i)$ where $M_r(i) \in M_r$
6. Multiplefault(D_r) /∗ Checks when there is one false alarm and no missed alarm ∗/
7. }
8. for ($i = 1$ to $|M_s|$){
9. $B_r = M_r \cup M_s(i)$ where $M_s(i) \in M_s$

10. Multiplefault(B_r) /* Checks when there is no false alarm and no missed alarm */
11. }
12. Output set FC;
13. }
14. Multiplefault(set M_r){
15. for ($i = 1$ to $|C|$){
16. search for a component $C_i \in C$ such that Domain $(C_i) \subseteq M_r$ /* Condition of checking multiple faults */
17. Incorporate C_i to S
18. FC = FC $\cup$ $\{C_i\}$
19. }
20. }

From these two algorithms (algorithm for single fault and double fault), it can be observed that the main difference between these two algorithms lie in lines 3, 8, 14 for single fault and in line 16 for double fault. In case of single fault, the scheme checks whether the domain of a component is equal to M_r, D_r or B_r or not, where in case of multiple faults the scheme checks whether the domain of a component is a subset to M_r, D_r or B_r or not. As an example if we assume that there is no false alarm or missed alarm and at any time the network manager gets that M_8 and M_6 have raised alarms. So, if there is only a single failure, it can be seen from Table 3 that ND_{10} is faulty (as Domain(ND_{10}) $= \{M_8, M_6\}$). Whereas if we consider multiple faults then we can say that ND_{10} as well as ND_4 may be faulty (as Domain (ND_{10}) and Domain (ND_4) are subsets of $\{M_8, M_6\}$). Next we explain the details of single and double faults location algorithm considering false and missed alarms.

We consider three cases to explain the localization algorithm by assuming maximum or false alarm and one miss alarm in the network:

(i) No false alarm and no miss alarm.
(ii) One false alarm and no miss alarm.
(iii) No false alarm and one miss alarm.

In case (i) single or multiple faults can be detected easily. Moreover when network intercepts multiple faults at particular point of time, the triggered alarms are intermingled. Localization algorithm is invoked and obtains a set of apparent faulty components from which faulty component or components have to be. We explain our algorithm using Table 3.

Let us consider at any time the *received alarm* (RAL) has been noticed {1 0 1 0 0} i.e., M_6 and M_8 have raised alarm but M_1, M_3 and M_{11} are silent. Here $M_r = \{M_6, M_8\}$ and $M_s = \{M_1, M_3, M_{11}\}$. Case (i) assume only correct alarms, hence ND_5, ND_6, ND_7 and ND_8 can be excluded from the set of probable faulty components. This is because if ND_5 fails then monitor M_1 triggers alarm. But in the received alarm it shows that M_1 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 $ND_i \in ND$ if Domain (ND_i) $\subseteq M_r$ then ND_i is included in the probable faulty component (FC) set. As Domain (ND_4) $\subseteq M_r$, Domain (ND_{10}) $\subseteq M_r$, $\{ND_4, ND_{10}\}$ is included in FC. Therefore, FC = $\{ND_4, ND_{10}\}$. RAL is obtained by performing *logical OR operation* on ND_4 and ND_{10} rows [19]. This set strictly includes the probable faulty components for any number of simultaneous failures.

Case (ii) makes all combination of received alarm patterns considering one false alarm in the network i.e., any one of $M_r = \{M_6, M_8\}$ has raised an alarm false. 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 M_6 is eliminated from M_r the received alarm pattern will be (1 0 0 0 0) i.e., the '1' corresponding to M_6 is replaced by a '0'. Similarly if M_8 are eliminated from M_r then we get the patterns (0 0 1 0 0) respectively. So, in the above mentioned received alarm pattern two other patterns need to consider. They are (1 0 0 0 0) and (0 0 1 0 0). When the pattern is (1 0 0 0 0) then $D_r = \{M_8\}$, and Domain (ND_4) $\subseteq D_r$, ND_4 is included in FC. Similarly for the patterns (0 0 1 0 0), $\{ND_{13}\}$ contain in FC. Hence, FC = FC $\cup$ $\{ND_4, ND_{13}\}$ = $\{ND_4, ND_{10}, ND_{13}\}$.

In case (iii) there is one miss alarm but no false alarm in the network i.e., any one of $M_s = \{M_1, M_3, M_{11}\}$ 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 M_1 has raised miss alarm then we have to replace the '0' corresponding to M_1 in RAL by '1' i.e., we will have the pattern (1 0 1 0 1). Similarly if M_{11} and M_3 will trigger miss alarm then we will find the pattern (1 0 1 1 0) and (1 1 1 0 0) respectively. Then we have three other combinations of received alarm patterns that are {(1 1 1 0 0), (1 0 1 1 0)} and {10101}. For pattern (1 1 1 0 0)$B_r = \{M_3, M_6, M_8\}$ and Domain (ND_4) $\subseteq B_r$, Domain (ND_6) $\subseteq B_r$, Domain (ND_{10}) $\subseteq B_r$ and Domain (ND_{13}) $\subseteq B_r$, $\{ND_4, ND_6, ND_{10}, ND_{13}\}$ should be included in FC. Similarly for the pattern (1 0 1 1 0) and (1 0 1 0 1), $\{ND_4, ND_8, ND_{10}, ND_{13}\}$ and $\{ND_4, ND_5, ND_{10}, ND_{13}\}$ is included in FC. Hence, FC = FC $\cup$ $\{ND_4, ND_5, ND_6, ND_8, ND_{10}, ND_{13}\}$ = $\{ND_4, ND_5, ND_6, ND_8, ND_{10}, ND_{13}\}$.

3.4. Locating the exact faulty component(s)

To locate the exact faulty component(s), the network manager has to send signals from any component that is not in FC to the component(s) which are in FC. If no acknowledgement signal comes from that component then the component is faulty. We call these signals active signals as these signals are only used to know that whether the components are active or not. This sending and receiving of active signaling is only necessary only when there is a fault in the network (i.e., when monitors raise alarm) and these signals are only sent to the components which are in FC. So, sending signals to the components in FC will be performed on demand, not regularly. These signaling are only being used for testing the components in FC and we have activated minimal monitors in the network to reduce the components in FC, thus reducing the overhead of sending these testing signals. The algorithm is described below.

Algorithm for locating the exact faulty component(s)

1. For each component $ND_i \in ND${
2. Send signal to ND_i from any $ND_j \notin$ FC

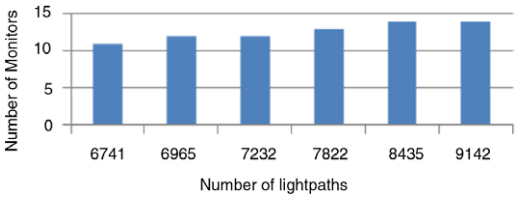

Fig. 5. Number of monitors in faulty set vs. load.

3. if (receive acknowledgement signal from ND_i){
4. $FC = FC \setminus ND_i$
5. }
6. }
7. Output FC

Consider an example that $FC = \{ND_4, ND_5, ND_6, ND_8, ND_{10}, ND_{13}\}$ and let us assume that ND_4 and ND_{13} are actually faulty. So, to check whether ND_4 is actually faulty or not, ND_2 can send an active signal. As ND_4 is faulty, ND_2 does not get any acknowledgement. Similarly active signal from ND_{14} to ND_{13} do not get an acknowledgement. On the other hand active signals from ND_9, ND_7, ND_7, ND_1 to ND_5, ND_6, ND_8, ND_{10} respectively receives acknowledgements, that confirms the fact that these node are in order. Thus the scheme outputs ND_4 and ND_{13} as the actually faulty component.

Generally optical networks provide backup paths as rerouting after failure is detected is too slow and lots of packets will be lost by this time. So, after fault localization, lightpaths passing through the faulty components are sent through the back up paths. This changes the network topology and so the number and position of monitors that should be activated needs to be changed. Thus algorithm for minimal monitor activation is called after detection of each fault.

4. Simulation results

To evaluate the effectiveness of our scheme we have implemented them on a standard network topology named EuroNet topology which consists of 28 nodes. All lightpaths are established using shortest path routing between node pairs. 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. For Fig. 5. we have used centralized algorithm for minimal activation of monitors as described in Section 3.1. As shown from Fig. 5, the number of monitors required to cover the whole network is in between 11 and 14 as the number of lightpaths changes from 6741 to 9142. New lightpaths are continuously being added in the network to meet traffic demand. But from Fig. 5, it is evident that even if the number of lightpaths is increased by around 40%, we need 2–3 extra monitors to maintain full fault localization coverage. So, requirement of turning the monitors ON and OFF is not very frequent unless there is any fault in the network.

Fig. 6 shows that the cardinality of the set of possible faulty nodes in the case of single and double faults varies marginally with the change of the number of lightpaths. This figure represents the output set of fault localization algorithm (described in Section 3.3) i.e., the set of probable faulty nodes in the network for single/double faults. From Fig. 6 it is clear that the cardinality of the set increases with the increase of lightpaths. In the case of single fault the number of probable faulty nodes increases very slowly while in double faults the set cardinality increases little more higher when the number of lightpaths increases. The results suggest that even if the number of lightpaths is increased from 6741 to 9142, the number of probable faulty nodes lies between 3 and 5.

Fig. 7 shows that the number of monitoring devices changes very little with the change of lightpaths in three different situations namely (a) before any fault, (b) after single fault and (c) after double fault. This graph clearly indicates that the minimal activation of monitoring devices through our scheme caters different conditions of network with the change of traffic loads. The optimal number of monitoring devices lies within 11 to 16 for 28 physical nodes (locations) placed in EuroNet. After the faults in the network, we have added extra lightpaths to meet traffic demand. To make this traffic-intensive network survivable we add more monitoring devices attached to critical nodes in the network. Fig. 7 shows that the number of monitors added in the network is 2–3 even after single and double faults.

4.1. Effectiveness of activating minimal number of monitors

In this section we highlight the effectiveness of activating minimal monitors. For explaining this we take the help of the network topology given in [7] where some

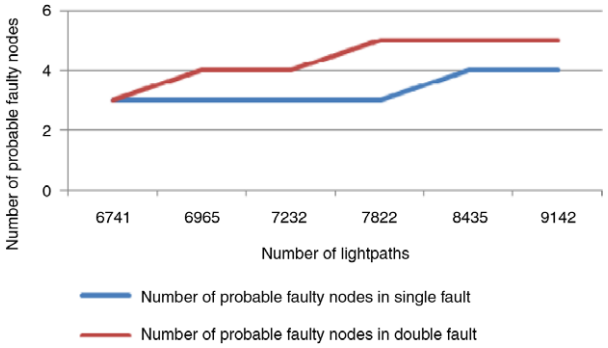

Fig. 6. Number of elements in faulty set vs. load.

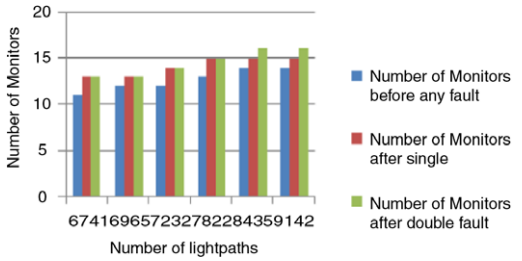

Fig. 7. Number of monitors under different loads before single fault, after single fault and after addition of a new node.

monitors are placed (monitors are placed randomly as this paper does not address monitor placement problem). We call this scenario '*Scenario* 1'. On another scenario, named '*Scenario* 2', we activate the necessary monitors based on our scheme on the same topology. In [7] the authors mainly make a binary tree that keeps all types of alarm patterns and in case of failure the network manager matches the alarm pattern with the leaves of the binary tree to track the faulty nodes. This approach eventually gives the same faulty component set as our scheme if the monitoring locations are same for the two schemes. In our scheme monitoring location are chosen intelligently before localization, the cardinality set of the faulty components is much lesser in our scheme.

The cardinality of FC in Scenario 1 and Scenario 2 are shown in Figs. 8 and 9 for single and double fault(s) respectively. The red bar is the output of our fault localization algorithm (before sending active signals) in Scenario 2 and the blue bar is the number of nodes in FC after sending active signals. The cardinality of the set is lower in Scenario 2 than that of Scenario 1. In Scenario 2 before sending active signals the cardinality of FC is 3–4 (for single fault) and 4–6 (in case of double fault) and after sending active signals the cardinality of the faulty set is 1 (for single fault) and 2 (for double fault) against the number of physical nodes that are active varies from 10 to 13 in the network. On the other hand the cardinality set generated in Scenario 1 is higher in both cases. Therefore, we must say that activation of minimal monitors reduces the size of FC, thus reduces the localization time.

5. Conclusion

In this paper we have presented a two-phased scheme containing (a) the detection of faults through monitoring devices raising alarms (fault detection) and (b) subsequently the localization of these faults (fault localization)

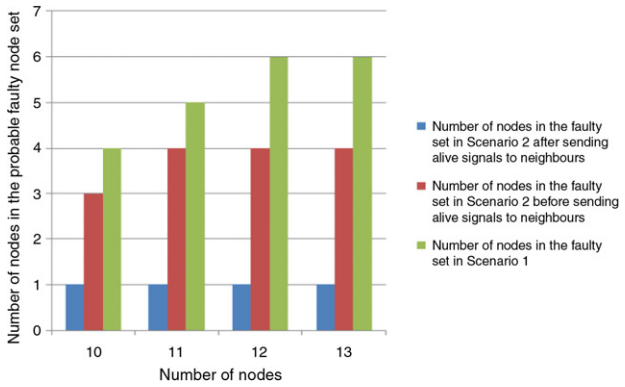

Fig. 8. Comparison of single fault. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

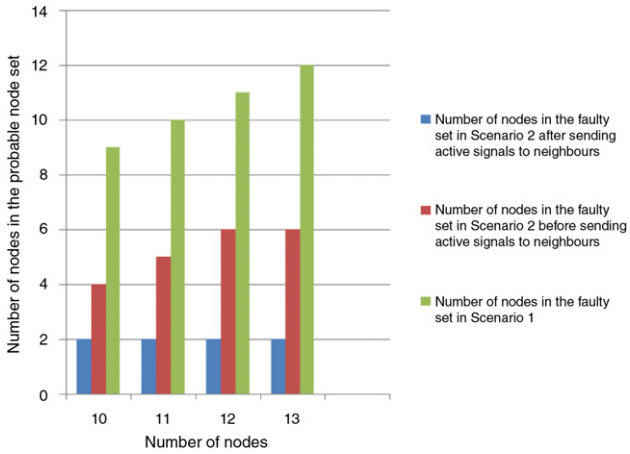

Fig. 9. Comparison of double faults. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

by invoking an algorithm and then by sending and receiving signals. We presented the problem of optimal monitor activation in optical networks. The problem of minimizing the number of activated monitors was proven to be NP-hard, and a heuristic algorithm that gave good performance in our experiments was also presented. A localization algorithm based on the alarm pattern is also presented. We showed the performance of our scheme on 28-node EuroNet and also compared the effectiveness of fault localization scheme before and after activating minimal monitors across the network. Clearly, activating minimal monitors gives much better performance that reduces alarm processing time as well as ambiguity in fault localization.

References

[1] S. Stanic, S. Subramanium, H. Choi, G. Sahin, H.-Ah. Choi, On monitoring transparent optical networks, in: Proceeding of the International Conference on Parallel Processing Workshops, ICPPW, 2002.

[2] Sava Stanic, Gokhan Sahin, Hongsik Choi, Suresh Subramaniam, Hyeong-Ah Choi, Monitoring and alarm management in transparent optical networks, in: Broadband Communications, Networks and Systems, 2007, BROADNETS 2007, 10–14 September, 2007, pp. 828–836.

[3] P. Nayek, S. Pal, B. Choudhury, A. Mukherjee, D. Saha, M. Nasipuri, Optimal monitor placement scheme for single fault detection in optical network, in: 7th International Conference on Transparent Optical Networks ICTON 2005, Barcelona, Spain, July 3–7, 2005.

[4] N.S.V. Rao, Computational complexity issues in operative diagnosis of graph-based systems, IEEE Transactions on Computers 42 (4) (1993) 447–457.

[5] 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) (1996) 1217–1223.

[6] I. Katzela, G. Ellinas, W.S. Yoon, T.E. Stern, Fault diagnosis in optical networks, Journal of High Speed Networks 10 (4) (2001) 269–291.

[7] C. Mas, P. Thiran, An efficient algorithm for locating soft and hard failures in WDM networks, IEEE Journal on Selected Areas in Communications 18 (10) (2000) 1900–1911.

[8] J. Kleer, B.C. Williams, Diagnosing multiple faults, in: Artificial Intelligence, vol. 32, Elsevier Science Publishers, 1987.

[9] Y.Y. Yang, R. Sankar, Automatic failure isolation and reconfiguration, IEEE Network (1993) 44–53.

[10] C. Mas, J.-Y. Le Boudec, An alarm filtering algorithm for optical communication networks, in: Proc. Management of Multimedia Networks and Services, IFIP/IEEE TC6/WG6.4/WG6.6 International Conference, 1998, pp. 205–218.

[11] H. Zeng, C. Huang, A. Vukovic, M. Savoie, Fault detection and path performance monitoring in meshed all-optical networks, in: IEEE Globecom'04, Dallas, November 2004.

[12] H. Zeng, C. Huang, A. Vukovic, A novel fault detection and localization scheme for meshed all-optical networks based on monitoring-cycles, Photonic Network Communications 11 (3) (2006) 277–286.

[13] S. Stanic, S. Subramaniam, A comparison of flat and hierarchical fault-localization in transparent optical networks, in: Optical Fiber Communication Conference and Exposition and The National Fiber Optic Engineers Conference, OFC/NFOEC, 2008.

[14] Y. Wen, V.W.S. Chan, L. Zheng, Efficient fault-diagnosis algorithms for all-optical WDM networks with probabilistic link failures, Journal of Lightwave Technology 23 (2005) 3358.

[15] H. Nguyen, P. Thiran, Failure location in transparent optical networks: the asymmetry between false and missing alarms, in: Proceedings of 19th International Teletraffic Congress, ITC19, Beijing, China, August 2005.

[16] C. Mas, I. Tomkos, O. Tonguz, Failure location algorithm for transparent optical networks, IEEE Journal on Selected Areas in Communications 23 (2005) 1508–1519.

[17] S.S. Ahuja, S. Ramasubramanian, M. Krunz, SRLG failure localization in all-optical networks using monitoring cycles and paths, in: Proceedings of INFOCOM 2008, Phoenix, AZ, USA, 13–18 April, 2008, pp. 181–185.

[18] A. Pal, A. Paul, A. Mukherjee, M.K. Naskar, M. Nasipuri, Fault detection and localization scheme for multiple failures in optical network, in: Proceedings of ICDCN 2008, Kolkata, India, pp. 464–470.

[19] A. Pal, A. Paul, A. Mukherjee, M.K. Naskar, Fault and attack management in optical networks, in: Proceedings of IEEE ANTS 2007, Mumbai, India.

[20] S. Pal, P. Nayek, A. Mukherjee, Fault localization scheme for multiple failures in optical networks, in: Proceeding of SNCNW 2006, Lule, Sweden.