Fault and Attack Management in Optical Network

A.Pal[1], A. Paul[1], A. Mukherjee[2] and M. K. Naskar[3]
[1]Dept. of CSE, Jadavpur University, Calcutta 700 032, India; e-mail: amitangshupal@yahoo.co.in and arghyadip.paul@yahoo.co.in
[2]IBM India Pvt Ltd, Salt Lake, Calcutta 7000 091, India e-mail: amitava.mukherjee@in.ibm.com
[2]Royal Institute of Technology, Stockholm 16440, Sweden, email: amitava@kth.se
[3]Dept. of ETCE, Jadavpur University, Calcutta 700 032, India; e-mail: mrinalnaskar@yahoo.co.in

***Abstract*— This paper proposes a scheme containing (a) the detection of faults or attacks through monitoring devices raising alarms and (b) the localization of them by invoking an algorithm. We demonstrate the performance of this scheme on EuroNet.**

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 (e.g. 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 (e.g. service disruption, eavesdropping etc.). One of the most important requirements to ensure the survivability of high speed optical network is to manage faults or attacks detection and their localization. A single failure (attack) can cause millions of dollar of revenue lost right from corporate to service providers. So, the fault and attack management is essential to ensure uninterrupted services to users. In this work we discus fault (attack) detection and localization and the block diagram of our proposed scheme is shown in Fig. 1.

Whenever there is a failure or an attack, for example, on a

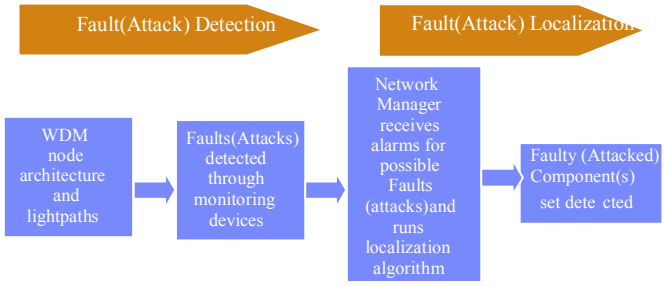

Fig. 1 Proposed fault detection and localization scheme

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. 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 our proposed scheme detects the failure(s) or attack(s) in the network components. The monitoring devices are placed optimally across network.

In the second phase, the localization algorithm, when it is invoked to locate faults, 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 fault 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 disrupted) components lowers down. In this paper, we interchangeably use monitor and monitoring device. In this paper, our scheme is divided into two phases namely i) fault (attack) monitoring: monitoring devices placement with dynamic lightpaths and ii) fault localization. The building blocks of our proposed scheme are shown in Fig. 2.

Dynamic scenario means that a set of lighpaths is added to a network at any point of time while a set of lightpaths would be

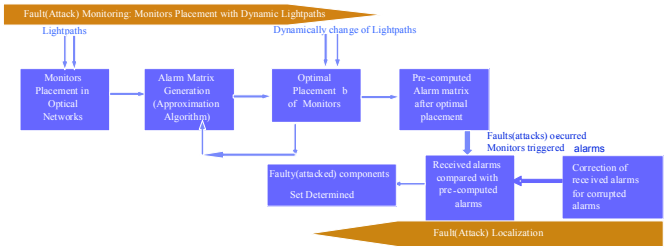

Fig. 2 Block Diagram of proposed scheme

cut off when disruption or failure happens or the traffic load increases. This dynamic scenario keeps the network running normal during survivable period to cater users' requirements. Firstly, we minimize the total number of monitoring devices to be placed in the network to make this placement cost effective. The placement of monitors in the network is posed as a NP-hard problem. We propose a heuristics to place monitors in an optimal way that would be spanned across the network to cover the failures (disruptions) of components when single/multiple simultaneous failures (disruptions) occurred. The dynamic change of ligthpaths would be input to approximation algorithm until the placements of monitoring devices would optimal one and is almost independent of the change of network scenarios. The pre-computed alarm matrix is the output of approximation algorithm, for optimal placement of monitoring devices [1]. Secondly, failures (or attacks) are located from the received alarms. 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 we propose a scheme to locate the exact faulty (disrupted) components by the process of sending and receiving signals. In this work, we have also compared performance of our scheme [2] with that of the algorithm stated in [3].

II. Proposed Scheme

Fig. 3 shows 14-node NSFnet which is the backbone network for US. We denote C the set of optical components and M the set of monitors. The Fig. 3 is self-explained.

A. Fault(Attack) Monitoring: Monitor Placement with Dynamic Lightpaths

In Fig. 3, M1 – M11 i.e., 11 monitoring devices are placed to

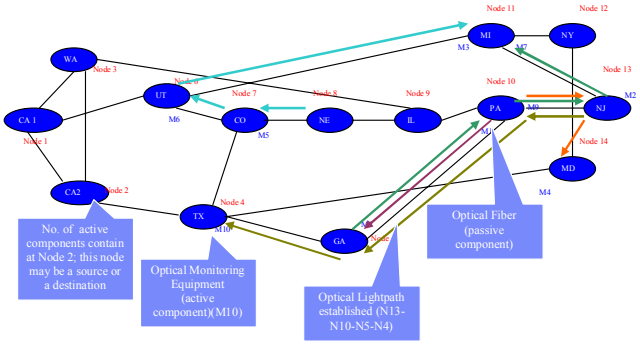

Fig.3. Reference NSFNet

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 (disruptions) can be located for all components (i.e., for a node or a link) distinctly. The algorithm is described in detail in [1].

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

When there is any fault (attack) 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-disrupted) 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 (disrupted) 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 and vice versa. The fault localization algorithm (which also takes care for corrupted alarms) for the single fault and multiple faults (attacks) is described in detail [2].

III. SIMULATION PERFORMANCE

We have shown results on EuroNet only that has 28 physical nodes. Fig. 4 shows that the number of monitoring devices changes with the increase of lightpaths. Fig. 5 shows that the cardinality of faulty (disrupted) set increases with the increase of lightpaths in the case of different scenarios. In Fig. 6, we have compared our scheme with the algorithm given in [3] specifically on the fault localization.

IV. Conclusion

In this paper we have presented two-phased scheme and

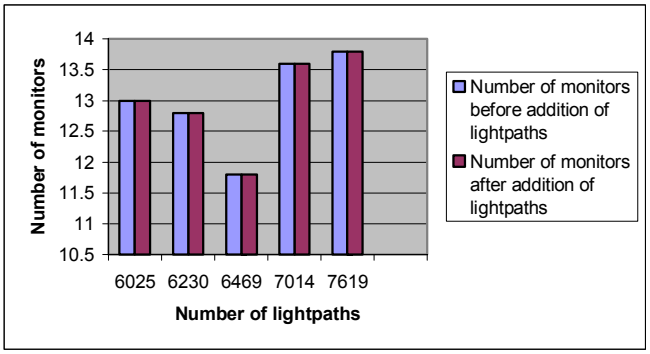

Fig.4 Number of monitors in different network load

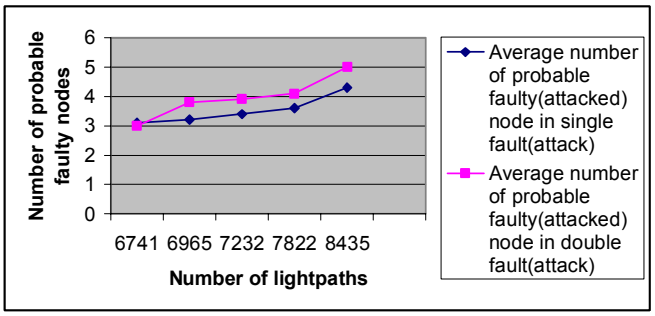

Fig.5. Number of elements in faulty set vs. load

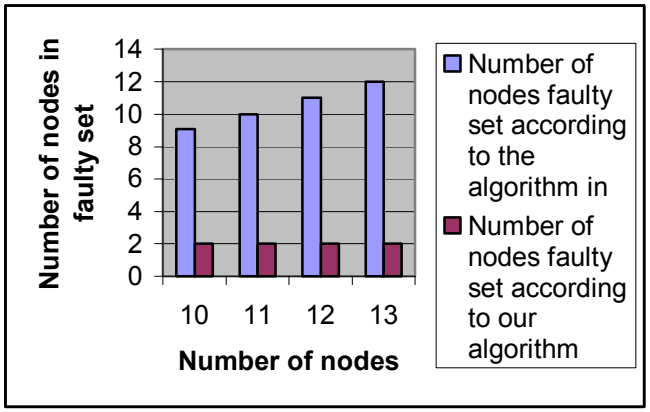

Fig.6. Comparison for the case of double faults (attacks)

shown its performance on 28-node EuroNet, and compared our scheme with an existing algorithm [3] too.

References

[1] 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.

[2] S. Pal, P. Nayek and A. Mukherjee, "Fault Localization Scheme for Multiple Failures in Optical Networks", Proceeding of SNCNW 2006, Lule, Sweden

[3] C. Mas and P. Thiran, "An Efficient Algorithm for Locating Soft and Hard Failures in WDM Networks", IEEE Journal of Selected Areas of Communications, Vol. 18, No. 10, Oct 2000, pp 1900-1911.