5.1 FAULT DETECTION AND LOCALIZATION

At different protocol layers, link failures can be detected. Generally, the detection time is much longer for an upper layer protocol when compared with the optical/physical layer scheme. It is needed to focus on optical layer monitoring schemes where a link failure can be detected by a special device called monitor for reducing the detection time. A channel based monitoring scheme requires a large number of monitors because it requires one monitor for each wavelength channel. Though link based monitoring scheme is more scalable, still it requires one monitor per link (Bin Wu et al 2008).

When compared with the fault localization, fault detection is easier and faster. Fault localization is the process of finding a minimum set of potential failed network resources based on the alarms generated in the fault detection phase. Fault localization in general network has been studied exclusively for many years in various areas and thus it is not a new problem. It has been studied in the areas like power distribution systems, electrical circuits, industrial control systems, and in communication networks. On the other hand, due to the lack of electrical terminations or the excessive cost and the difficulty in implementation, the existing fault localization schemes for traditional networks cannot be applied to the WDM networks directly. (Hongqing Zeng et al 2005).
In all-optical WDM networks, the network edge routers may be able to detect the existence of a fault whenever a link is damaged or a channel is disconnected. But, it is not possible to indicate the exact location of the fault. At this time, no advanced optical technique is introduced.

5.2 Failures in WDM Networks

Failures in all optical WDM networks can be classified into two categories according to the scale of their effect (Ramamurthy et al 1999). The first one is the wavelength level failure which affects the quality of transmission of each individual light path. The second one is the fiber level failure which affects all light paths on an individual fiber. A very short disruption of service caused by a network fault may lead to a very high data loss in such networks. Thus it is essential to ensure continuous and reliable network operation. Numerous schemes have been proposed for such networks to improve the network survivability (Ramamurthy et al 2003), where fault detection and localization is the vital part but has received disproportional attention.

Black Box based and network-model based methods have been proposed due to inability of applying conventional fault localization methods to optical networks (Carmen Mas and Patrick Thiran 2001). In WDM networks with the function of dynamic wavelength switching, routing to end users and every new light path provisioning may initialize a new training or learning process. In applied network models, the approaches include probabilistic reasoning systems, finite state machine models and deterministic fault-propagation models are accurate for static networks but for WDM networks with dynamic light path provisioning, the network model has to be changed dynamically. This is extremely difficult and time-consuming, if not impossible, and thus makes such approaches unable to detect and locate the network faults within the strict time-constraint.
The capability of the network to endure the failures is known as fault tolerance. When a link tends to fail, then all its constituent fibers also fails. Each and every connection which utilizes these fibers is rerouted and a wavelength will be assigned. Primary path is a light path which carries traffic during normal operation. In case of a failure, the traffic is rerouted. The large amount of traffic on these networks against the traditional copper links makes the fault tolerance as a major issue.

It is necessary to design an efficient algorithm for fault identification in the optical network. In addition to this, an algorithm to analyze the information of the alarms generated by the components of an optical network in the presence of a fault. It uses the alarm correlation in order to reduce the list of suspected components shown to the network operators.

5.3 EXISTING MODELS TO THE RELATED PROPOSED WORK

All the optical network services became feasible due to availability of ultra long reach transport. Faults are unavoidable in any communication networks and systems. Quick detection and isolation of the fault is essential for the robustness and reliability of both the network and the services carried over it.

Hongqing Zeng and Changcheng Huang (2004) proposed a mechanism for fault detection and path performance monitoring based on decomposing AONs into monitoring cycles. The authors developed two monitoring cycle finding algorithms which are heuristic depth first searching (HDFS) and shortest path Eulerian matching (SPEM). The HDFS and SPEM algorithms are developed for finding monitoring cycles in AONs. The two
algorithms are compared with respect to the maximum and average number of wavelengths occupied by monitoring in nodes and links. The hop count parameter is not considered in this scheme. When all links in the network have more occupied wavelength, hop count consideration is important.

Satyajeet S. Ahuja et al (2008) have considered the problem of fault localization in all-optical networks. They described a fault localization mechanism that uniquely determines SRLG failures by using monitoring cycles and paths. They have provided necessary and sufficient conditions on (1) the requirements of the fault localization set; (2) network connectivity for localizing failures with one monitoring location; (3) the placement of monitoring locations to obtain a solution. They developed an $O(k|L|)$ algorithm to calculate the minimum number of required monitoring locations to localize all possible failures involving up to k links. They described an ILP formulation and a heuristic approach to find the set of cycles that can localize SRLG failures using a single monitoring location.

Bin Wu et al (2008) developed a new monitoring trail (m-trail) concept considering various optical layer monitoring schemes for fast link failure localization in WDM mesh networks. When m-trail compared with the existing monitoring cycle (m-cycle), the m-trail provides a more flexible and general all-optical monitoring structure for fast link failure localization, with the objective of minimizing the total monitoring cost. Minimizing the total monitoring cost results in fewer fault management efforts, and thus enhance the scalability of the network. Both in cycle based and link based monitoring, the m-cycle design algorithms do not attain the joint optimization.

Yonggang Wen et al (2005) investigated the fault diagnosis problem for all-optical wavelength-division multiplexing (WDM) networks. They developed a run length probing algorithm for failure
localization to minimize the diagnosis effort (e.g., the average number of probes) to locate failures, by sending the optical probe signals sequentially along with a set of designed lightpaths and the network state is inferred from the result of this set of end-to-end measurements. Generally, the run length probing system uses a centralized fault management agent in which the agent communicates with all the network nodes through a reliable out-of-band control channel. There is a possibility of overhead for agent and agent failure in centralized management. Also this scheme is not advantageous as dependencies among failures in different wavelength channels are not considered in the wavelength level implementation.

Carmen Mas and Patrick Thiran (2000) proposed an algorithm for locating multiple failures at the physical layer of a WDM network. The proposed scheme handles missing and false alarms. The nonpolynomial computational complexity of the problem is pushed ahead into a precomputational phase, which is done off-line, when the optical channels are set up or cleared down. This results in fast on-line location of the failing components upon reception of the ringing alarms.

Hongqing Zeng et al (2005) designed a End-End protocol where the source node of each light-path keeps sending hello packets to the destination node exactly following the path for data traffic. The destination node generates an alarm once a certain number of consecutive hello packets are missed within a given time period. Then the network management unit collects all alarms and locates the faulty source based on the network topology, as well as sends fault notification messages via control plane to either the source node or all upstream nodes along the light-path. Large number of hello packets is used to identify the fault in this system. This results in message overhead problem.
In the previous End-End scheme message overhead is the major problem, since every node in the network sends the control packets for identification of fault. This problem can be solved and performance can be improved by the proposed FLAC scheme. In this scheme, message overhead is reduced for identification of fault in the optical path.

5.4 PROPOSED SCHEME

The objective of the proposed scheme is to identify the faults in the network and also to collect the failure information so that in future data transmission in the failed path can be rerouted.

5.4.1 Fault Detection and Localization Mechanism

The proposed mechanism can perform detection and localization of a fault on a light path. The fault detection phase detects the fault by raising the alarms signals. The localization phase will obtain a set of potential faulty links. The standard NSFnet topology (14nodes – 19 links) is taken into simulation design consideration. Assume the links are bidirectional. The length of each link is assumed one unit. ie. Hop count of each light path is the sum links in that path from source to destination. All nodes in the network has monitoring capability for creating the control signals whenever the fault occurs. The light path for normal data transfer is established as per RFTR algorithm .In the light path, the intermediate nodes at the distance of hopcount/3 between source and destination are activated for generating control signal whenever the fault occurs. For example, If the light path has hop count of 10, then the intermediate nodes 3 & 6 are activated to act as intermediate destination nodes. The intermediate control nodes send control packets are sent towards upstream. This algorithm detects the failed connections and tries to reroute data stream through an alternate path. The
destination node knows the source node and the setup route before an interruption occurs. When the destination does not receive expected data stream for the given time interval, then the connection gets interrupted. Immediately, the proposed algorithm will be activated by the destination. The operation of proposed algorithm is given below.

A Link Failure Alarm (LFA) signal is disseminated towards the upstream neighbor backwardly by the destination. The alarming signal is a small control packet which notifies the upstream node of data disruption. The alarming signal traverses through the secured control network (OSC's). If the recipient of LFA has not received the data in advance, it passes the LFA to its upstream neighbor in the path. Otherwise, if the recipient of LFA is also a recipient of data, a reply signal REP is sent to the downstream sender. Once the REP is received, the node will activate a restoration protocol to reroute the affected traffic through an alternate by the link restoration. Then the location of the failed connection is identified and it is transmitted to the entire nodes of the network. This is essential in order to maintain correct routing tables and also to prevent blocking of forthcoming calls by the failed connection. Moreover, by notifying the location of the failure, this could accelerate the restoration of longer disconnected light paths, even before they activate any restoration/localization process.

5.4.2 Fault Detection and Localization Algorithm

Initial conditions

1. Each link in the network is bidirectional.
2. Each link carries same number of wavelengths.
3. Light path setup is created based on RFTR algorithm.
4. Length of each link is one unit.

5. Fault link is randomly selected at the network.

6. Intermediate destination nodes are activated at the distance of hopcount/3. Where, hopcount = Total no. of links in selected light path.

7. Let $LP_1, LP_2, LP_3 \ldots LP_m$ be the set of light paths created by RFTR algorithm from the source(S) to destination(D) and $n_{11}(S), n_{12}, n_{13}, \ldots n_{ik}(D)$ be the set of nodes along the selected route ($LP_1$).

8. The final destination $n_k$ and the intermediate destination nodes $d_1, d_2, d_3, d_4 \ldots$ are activated at the distance interval of hopcount/3.

9. Under the selected path $LP_1$, the source $n_{11}$ sends data packets in fixed time intervals $\delta$. The sequence of packets $p_1, p_2, \ldots, p_k$ with time intervals $t, t+\delta, t+2\delta, \ldots, t+k\delta$ are sent from source(S) to destination(D).

10. When a $k/2$ number of consecutive packets are missed within a given time threshold $t$, then the nearest destination to fault link detects a fault on the light path.

11. The destination ($n_f$) nearest to fault link sends the probe packet towards the source.

   If $n_f$ has not received the data within the time interval $t$, then

   11.1 $n_f$ raises alarm signal and informs to NMS

   11.2 $n_f$ transmit packet towards to $n_j$, where $j=f-1$

   11.3 If $n_j$ does not receive the data before $t$, then
11.3.1 It does not send a REP packet to $n_i$, where $i=j+1$.

11.3.2 The node $n_i$ triggers recovery scheme for path restoration.

11.2.3 $n_j$ information is flooded through the network.

11.4 Else

11.4.1 $j=j-1$

11.4.2 Repeat the step 4.2

11.4 End If

12. End If

Figure 5.1 Functions of Link Failure Detection Algorithm

Figure 4.1 shows the functions of the proposed link failure detection algorithm. As shown in the figure, the alarming signal, Link Failure Alarm (LFA) is sent back towards the source from the intermediate destination node until it reaches the upstream node of the fault link. In
response, the RFTR algorithm is activated to implement the path recovery scheme.

5.4.3 Alarm Correlation Mechanism

The components able to send alarm can be divided in the following groups:

- Self alarmed ($G_1$) – When the failed component sends alarm.
- Out-alarmed ($G_2$) – When the component alarms informing that other component is not working correctly.

The components are said to be alerting components (A) when they send the alarm signal to network administrator during the occurrence of fault. On the other hand, the components which are not able to send alerts are named as Non-alerting components (P). The components that can able to send alert signal can be divided into following groups.

5.4.3.1 Active Components

The network components that can send alert to the administrator when they are not working properly.

5.4.3.2 Passive Components

The network components that can send alerts when some external event occurs, that is, they send alerts for the manager informing an abnormal condition in some point of the channel, even when they are not responsible for the problem.
5.4.3.3 Masking Components

The components of this group can mask the alerts sent by previous components, since the channel is an ordered sequence of components.

When a fault occurs, in order to identify which network component is damaged and which node it belongs each network component has a unique identification. In the network model used here, this identification is composed by a string of four fields \( f_1, f_2, f_3, f_4 \). These fields are having the following:

\[ f_1 : \text{It can assume the following values.} \]
\[ 0 \text{ – non-alarming component;} \]
\[ 1 \text{ – Self alarmed;} \]
\[ 2 \text{ – Out-alarmed;} \]
\[ 3 \text{ – Masking;} \]

\[ f_2 : \text{It indicates the node number.} \]

\[ f_3 : \text{It is always 0 for a local node.} \]

\[ f_4 : \text{It identifies the position of the component inside the node.} \]

The value of this field \( f_4 \) varies according to the component:

\[ \text{LAP} = 0 \text{ (Local Access Port);} \]
\[ \text{ADF} = 1 \text{ or 2 (Add/ Drop Filter);} \]
\[ \text{RX} = 1 \text{ or 2 (Receiver);} \]
\[ 3R = 4 \text{ or 5(Re-generator/Re-shaper/Re-timing) amplifier;} \]
\[ \text{TX} = 5 \text{ or 6(Transmitter);} \]
\[ \text{PS} = 3 \text{(Protection Switches);} \]
5.4.4 Alarm Correlation Algorithm

At the physical route domain, all network components that belong to any channel are numbered as \(C_1, C_2\) … and associated to each one of the alarm components of the respective alarms that will be sent to the network management server (NMS) if they fail.

Let \(S_i\) denotes the suspected list of components.

1. Server receives alarm \(a\) from the component \(C_i\).
2. If \(a = G_1\) then
   2.1 Add \(C_i(a)\) to \(S_i\).
3. Else If \(a = G_2\) then
   3.1 For each channel \(CH_i\)
3.1.1 Add $C_1(a)$ to $S_1$.

3.2 For each component $C_k(a), k \neq 1$

3.2.1 If $AD_k = PD(i)$, then where $AD_k$ is alarm domain and $PD$ is the route domain,

3.2.1.1 Add $C_k(a)$ to $S_1$.

3.2.2 Else

3.2.2.1 Drop the alarm $a$

3.2.3 End if

3.3 End For

4. End If

5.5 SIMULATION SETUP

By using ns2 simulator, the performance of the proposed algorithms is simulated as follows.

5.5.1 Simulation Model

The proposed algorithm is simulated with 14 nodes topology. The other simulation parameters are similar to the simulation parameters of previous algorithm defined in the last chapter. For the experimental setup, a dynamic traffic model is constructed in which connection requests arrive at the network according to an exponential process with an arrival rate $r$ (call/seconds). The session holding time is exponentially distributed with mean holding time $s$ (seconds).
The performance of proposed Fault Localization and Alarm Correlation algorithm (FLAC) with an extensive simulation study based upon the ns-2 network simulator. The Optical WDM network simulator (OWns) patch in ns2 is used to simulate 14-Nodes topology (Figure 4.2). Various simulation parameters are given in Table 4.1

In the experimental setup, multiple link failures are considered. The performance result of FLAC is compared with End-to-End scheme.

### 5.5.2 Performance Metrics

By using the above simulation setup, the following performance metrics have been evaluated

- Average Fault Detection Time
- Detection Accuracy
- Recovery Time

![Figure 5.3 14-nodes Topology](image)
Figure 5.4 25-nodes Topology

5.6 SIMULATION RESULTS AND OBSERVATIONS

The constructed model is simulated with increasing number of failures as 1, 2, 3, & 4 in the network and the corresponding blocking probability, end to end delay and network throughput are observed.

Figure 5.5 shows the average fault detection time obtained by proposed FLAC algorithm compared with End-to-End scheme under 14 nodes topology. It shows that FLAC has average fault detection time is 16% less than the End-to-End algorithm, when number of failures increases. The simulated results for Average fault detection time Vs no. of faults are tabulated in the Table 5.2.
Figure 5.5 14 nodes – No. of Failures Vs Average Fault Detection Time

Figure 5.6 25 nodes – No. of Failures Vs Average Fault Detection Time

Figure 5.6 shows the average fault detection time obtained by proposed FLAC algorithm compared with End-to-End scheme under 25 nodes topology. It shows that the proposed FLAC scheme has average fault
detection time is 19% less than the End-to-End scheme, when number of failures increases. The simulated results for Average fault detection time Vs no. of faults are tabulated in the Table 5.2.

**Table 5.1 Simulation Results - Average fault detection time Vs no. of faults**

<table>
<thead>
<tr>
<th>No. of faults</th>
<th>Average fault detection time (s)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>14 nodes topology</td>
<td>25 nodes topology</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FLAC End to End</td>
<td>FLAC End to End</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0.6734 0.7572</td>
<td>0.9620 1.12554</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0.7101 0.9505</td>
<td>1.0144 1.3578</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1.5794 2.0213</td>
<td>2.2563 3.1610</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2.2296 2.4501</td>
<td>3.1851 3.5727</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2.3975 2.8066</td>
<td>3.7107 4.3805</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5.7 and 5.8 shows the detection accuracy obtained for different number of faults under 14 nodes and 25 nodes topology respectively. The proposed FLAC scheme has averagely 13% more detection accuracy than End-to-End scheme under both 14 and 25 nodes topology.

**Figure 5.7 14 nodes – No. of Failures Vs Detection Accuracy**
Figure 5.8 represents the detection accuracy obtained for different number of faults under 25 nodes topology.

Figure 5.8 25 nodes – No. of Failures Vs Detection Accuracy

The following Table 5.3 shows the simulated results for detection accuracy against varying faults under 14 node and 25 nodes topology.

<table>
<thead>
<tr>
<th>No. of faults</th>
<th>Detection Accuracy</th>
<th>14 nodes topology</th>
<th>25 nodes topology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FLAC</td>
<td>End to End</td>
</tr>
<tr>
<td>1</td>
<td>0.8484</td>
<td>0.7813</td>
<td>0.8248</td>
</tr>
<tr>
<td>2</td>
<td>0.8712</td>
<td>0.7982</td>
<td>0.8371</td>
</tr>
<tr>
<td>3</td>
<td>0.7852</td>
<td>0.6749</td>
<td>0.7852</td>
</tr>
<tr>
<td>4</td>
<td>0.7576</td>
<td>0.6206</td>
<td>0.7876</td>
</tr>
<tr>
<td>5</td>
<td>0.7299</td>
<td>0.6045</td>
<td>0.7299</td>
</tr>
</tbody>
</table>

Figure 5.9 shows the recovery time obtained by proposed FLAC algorithm compared with End-to-End scheme under 14 nodes topology. It shows that the proposed FLAC scheme has averagely 21% lesser recovery time.
than End-to-End scheme, when number of failures increases. The simulated results for recovery time Vs no. of faults are tabulated in the Table 5.4.

![Fault Vs Recovery Time](image)

**Figure 5.9 14 nodes – No. of Failures Vs Recovery Time**

Figure 5.10 shows the recovery time obtained by proposed FLAC algorithm compared with End-to-End scheme under 25 nodes topology. It shows that the proposed FLAC scheme has averagely 25% lesser recovery time than End-to-End scheme, when number of failures increases. The simulated results for recovery time Vs no. of faults are tabulated in the Table 5.4.
The following Table 5.4 shows the simulated results for recovery time against varying faults under 14 node and 25 nodes topology.

**Table 5.3 Simulation Results - Recovery Time Vs No. of Faults**

<table>
<thead>
<tr>
<th>No. of faults</th>
<th>Recovery Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>14 nodes topology</td>
</tr>
<tr>
<td></td>
<td>FLAC</td>
</tr>
<tr>
<td>1</td>
<td>0.8081</td>
</tr>
<tr>
<td>2</td>
<td>1.0852</td>
</tr>
<tr>
<td>3</td>
<td>1.5895</td>
</tr>
<tr>
<td>4</td>
<td>2.5675</td>
</tr>
<tr>
<td>5</td>
<td>2.8770</td>
</tr>
</tbody>
</table>

---

Figure 5.10 25 nodes – No. of Failures Vs Recovery Time

The following Table 5.4 shows the simulated results for recovery time against varying faults under 14 node and 25 nodes topology.
5.7 CONCLUSION

This chapter proposes the implementation of Fault Localization and Alarm Correlation (FLAC) algorithm for the fast detection of fault in the optical WDM networks. The proposed FLAC algorithm is simulated under 14 nodes and 25 nodes topology. The proposed algorithm produces reduced average fault detection time, recovery time and improved detection accuracy, which is compared with existing End to End algorithm.