Abstract- It is an essential requirement to provide resilience against failures in high speed networks. In next generation optical networks it is required to protect and restore high capacity WDM networks from the failures. There are number of techniques available like Quick detection, identification and restoration which make networks more strong and consistent even though the failures cannot be avoided. Hence, we are required to develop fast, efficient and dependable fault localization or detection mechanisms. In this paper a new technique to localize faults in WDM networks is presented which can identify the location of a failure on a failed light path. Initially this technique detects the failed connection and then attempts to reroute data stream through an alternate path. In addition to this, an algorithm is presented which tries 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. By using these techniques blocking probability and delay can be reduced while throughput can be enhanced.

Keywords- Blocking probability, Delay, Fault Localization, WDM Networks.

1. Introduction

A) Wavelength Division Multiplexing (WDM)

Optical wavelength division multiplexing (WDM) networking is being recognized as an efficient technique for upcoming wide area network environments, because of its impending ability to meet the increasing demands of low latency communication and high bandwidth [1]. The basic property of single mode optical fiber is well known to us, that the optical fiber consists of enormous low loss bandwidth of several tons of Terahertz. But the single channel transmission is limited to only a small fraction of the fiber capacity due to the dispersive effects and shortcomings in optical device technology. Hence, the use of the wavelength division multiplexing (WDM) technology is an optional choice to get the full advantage of fiber potential [2]. WDM allows several signals to be carried independently along the same fiber provided each signal uses a different wavelength. As a result same fiber can be shared by many connections [3].

B) Types of WDM Networks

• WDM (wavelength division multiplexing): carries two to four wavelengths per fiber. The original WDM systems were dual-channel 1310/1550 nm systems. WDM systems are comparatively inexpensive and also more flexible.

• CWDM (coarse wavelength division multiplexing): carries four to eight wavelengths per fiber and in some cases even more wavelengths. This type of multiplexing is used for short to medium haul networks (regional and metropolitan area). This type of multiplexing is the cheapest among the three.

• DWDM (dense wavelength division multiplexing): can carry eight or more wavelengths. This type of multiplexing is very much flexible and also provides more number of options and interfaces. But this type of multiplexing is very expensive when compared with the other two.

C) Advantages of WDM

• Due to the reuse of the existing fiber cables, it increases the transmission capacity.

• It ensures scalability along with cost-effectiveness.

• The optical components are comparatively more reliable than the corresponding electronic component.
• Since newer optical network elements are commercially available, the incorporation of these elements into the network allows a smoother evolution of an all-optical network.

• Repeaters designed from the development of the fiber optic amplifiers are capable of amplifying many light wavelengths simultaneously, in turn increasing the feasibility.

• Submarine cables and extending the lifetime of cables where all fibers are used, are the two existing applications of WDM.

II. Problem Definition

A) 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. We 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 [4].

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 [5].

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.

III. Related Work

Michael T. Frederick and Arun K. Somani [6] have presented an L+1 fault tolerance which is used for the recovery of optical networks from single link failures without the allocation of valuable system resources. While the approach in its simplest form performs well against the existing schemes, the flexibility of L+1 leave many options to examine possible ways to further increase performance.

Muriel M’edard [7] has described that the protection routes are pre-computed at a single location and thus it is centralized. Before the restoration of the traffic, some distributed reconfiguration of optical switches is essential. On the other hand, restoration techniques depend upon distributed signaling between nodes or on the allocation of a new path by a central manager.

Joon-Young Kim, Sil-Gu Mun, Ju-Hee Park, Jin-Serk Baik and Chang-Hee Lee [8] have proposed and demonstrated a simple WDM-PON architecture that provides protection for both the feeder fiber and distribution fiber with a minimum addition of losses in the transmission path. In order to provide the protection function, they have used 1 x 2 optical switches or Ethernet switches at each ONU and OLT. In addition, the fault localization is implemented by using a tunable optical time domain reflectometer (OTDR) realized by a Fabry-Perot laser diode (F-P LD) and a tunable filter.

Hongqing Zeng, Alex Vukovic, Changcheng Huangb, Heng Huaa and Michel Savoiea [9] have presented a wavelength-routing fault detection scheme for concatenated in which pilot tones are added to wavelength channels as identifiers (CIDs) at input ports. Their scheme is applied to an AON testbed. The pilot tones are tracked and form the concatenated wavelength-routing fault detection scheme. The pilot tones and associated power penalty results are investigated by them.

Hongqing Zeng, Alex Vukovic, and Changcheng Huang [10] have described and analyzed an end-to-end lightpath fault detection scheme in data plane with the fault notification in control plane. Their effort is mainly focused on reducing the fault detection time. Their performance evaluation shows that their protocol can achieve fast fault detection,
and at the same time, the overhead brought to the user data by hello packets is negligible.

IV. Possible Solution - Fault Localization and Alarm Correlation

A) Detection and Localization Algorithm

In this section, a Link Failure Detection Algorithm which can identify the location of a failure on a lightpath is given. This algorithm detects the failed connections and tries to reroute data stream through an alternate path. Because of the short interval time of establishing a lightpath, we assume that a failure occurs during data transfer. This shows that 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, this algorithm will be activated by the destination. The operation of this algorithm is given below.

A Link Failure Alarm (LFA) signal is disseminated toward 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 (OSCs). If the recipient of LFA has not received the data before, 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 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.

Fig. 1: Shows the functions link failure detection algorithm

1) Algorithm

Let \( n_1, n_2, \ldots, n_k \) be the set of nodes along the route from the source \( n_1 \) to the destination \( n_k \).

1. The source \( n_i \) sends data packets in fixed time intervals \( \delta \). Source sends packets \( p_1, p_2, \ldots, p_k \) at time \( t, t+\delta, \ldots, t+k\delta \).
2. The destination \( n_k \) checks the packet sequence numbers \( s_1, s_2, \ldots, s_k \) of the packets.
3. When a \( k/2 \) number of consecutive packets are missed within a given time threshold \( t \), the destination detects a fault on the light path.
4. If \( n_k \) not received the data within the time interval \( t \), then
   1. \( n_k \) raises LFA and transmit backwards to \( n_j \), where \( j = k-1 \)
   2. if \( n_j \) received the data before \( t \), then
      1. It sends a REP packet to \( n_j \), where \( i = j+1 \).
      2. The \( n_j \) starts a recovery scheme for restoration
      3. The \( n_j \) information is flooded through the network.
   3. Else
      1. \( j = j-1 \)
      2. Repeat the step 1.2
   4. End if
5. End if

Fig. 1 shows the functions of this link failure detection algorithm. As shown in the figure, the alarming signal Link Failure Alarm (LFA) is sent back towards the source till it reaches the first recipient of data and it returns the REPLY (REP) signal is returned to the sender. In response, the RFTR scheme [11] is activated to avoid the failed link and restore the connection through a backup path.

B) Alarm Correlation

The components able to send alarm can be divided in the following groups:
A1 – When the damaged component sends an alarm;
A2 – When the component alarms informing that other component is not working correctly.

1) Alarm Correlation Algorithm

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

- \( f_1 \): It can assume the following values: 0 – non-alarming component; 1 – Self alarmed; 2 – Out-alarmed; 3 – Failure masking.
- \( f_2 \): It indicates the node number.
- \( f_3 \): It is always 0 for a local node.
- \( f_4 \): It identifies the position of the component inside the node. The value of this field varies according to the component: \( \text{LAP} = 0 \) (Local Access Port); \( \text{ADF} = 1 \text{ or } 2; \text{RX} = 4 \text{ or } 5; \text{3R amplifier} = 4 \text{ or } 5; \text{TX} = 5 \text{ or } 6; \text{PS} = 3. \)

2) 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 [12].

Let \( S_1 \) denote the suspected list of components.

1. Server receives alarm \( a \) from the component \( C_i \).
2. If \( a = A1 \) then
   2.1 Add \( C_i \) to \( S_1 \).
3. Else if \( a = A2 \) then
   3.1 For each channel \( C_{i1} \)
      3.1.1 Add \( C_{i1} \), \( k \neq 1 \)
   3.2 For each component \( C_k \), \( k \neq 1 \)
      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 \( C_k \) to \( S_1 \)
3.2.2 Else
   3.2.2.1 Drop the alarm \( a \)
3.2.3 End If
4. End if

V. Conclusion

Quick detection, identification and restoration make networks more strong and consistent even though the failures cannot be avoided. Hence, it is necessary to develop fast, efficient and dependable fault localization or detection mechanisms. In this paper a new fault localization algorithm for WDM networks which can identify the location of a failure on a failed lightpath is presented. This algorithm detects the failed connection and then attempts to reroute data stream through an alternate path. One assumption that a failure happens during the data transfer mode due to the short interval time of establishing a lightpath is taken. This implies that the destination node is aware of the source node and the setup route before an interruption of service occurs. The algorithm will be activated once a connection is disrupted. This happens when the destination does not receive expected data stream any longer. 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 is also presented. This algorithm uses the alarm correlation in order to reduce the list of suspected components shown to the network operators. By using these algorithms blocking probability and delay can be reduced while getting higher throughput.

VI. References


