ISSN: 2229-6948 (ONLINE)
DOI: 10.21917/ijct.2010.0014

FAULT LOCALIZATION AND ALARM CORRELATION IN OPTICAL WDM NETWORKS

G.Ramesh[1] and S.SundaraVadivelu[2]
[1]*Department of Information Technology, KLN College of Engineering, Madurai, Tamil Nadu, India*
Email: ramesh6_2000@yahoo.com
[2]*Department of Electronics and Communication Engineering, SSN College of Engineering, Chennai, Tamil Nadu, India*
Email: sundaravadivelus@hotmail.com

Abstract
For several high speed networks, providing resilience against failures is an essential requirement. The main feature for designing next generation optical networks is protecting and restoring high capacity WDM networks from the failures. 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 we propose a new fault localization algorithm for WDM networks which can identify the location of a failure on a failed lightpath. Our algorithm detects the failed connection and then attempts to reroute data stream through an alternate path. In addition to this, we develop 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. By our simulation results, we show that our proposed algorithms achieve less blocking probability and delay while getting higher throughput.

Keywords:
Alarm Correlation, Blocking Probability, Delay, Fault Localization, WDM Networks.

1. INTRODUCTION

1.1. WAVELENGTH-DIVISION-MULTIPLEXING (WDM) NETWORKS

Wavelength division multiplexing (WDM) is the concurrent transmission of multiple streams of data with the help of the special properties of fiber optics [1]. The ability of transferring huge amount of data at high speeds by the users over large distances is offered by the WDM networks.

WDM is considered as the most talented technology for the backbone of future next generation internet [2]. In WDM all optical networks, data is routed through optical channels called light paths. Without the wavelength conversion ability, the light path establishment requires same wavelength to be utilized along the entire route of the light path which is commonly referred to the wavelength continuity constraint. WDM enables the employment of a substantial portion of the available fiber bandwidth by allowing many independent signals with different wavelength to be transmitted simultaneously on one fiber [3].

The routing and detection of these signals can be obtained independently since the wavelength estimates the communication path by acting as the signature address of the origin, destination or routing. Hence, the wavelength selective components are necessary for allowing the transmission, recovery or routing of specific wavelengths.

1.2. 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.

1.3. FAULT TOLERANT IN WDM NETWORKS

Failures in WDM networks may seriously damage the end user applications because each light path can carry a large amount of traffic. Failures in all optical WDM networks can be classified into two categories according to the scale of their effect [6]. The first one is the wavelength level failure which affects the quality of transmission of each individual lightpath. The second one is the fiber level failure which affects all the lightpath on an individual fiber. Failures can lead to a severe data loss because each lightpath is estimated to operate at a rate of several gigabytes per second.

The capability of the network to endure the failures is known as fault tolerance. Due to the node failure or link failure, failure arises. 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.

Our objective is to detect the exact location of the failed connection and to reroute the data stream through an alternate path. Apart from this, we like to analyze the information of the alarms generated by the components of an optical network and to reduce the list of suspected components.

In this paper we propose a new fault localization scheme, which functions in the WDM layer. In this work, we propose a new algorithm which can identify the location of a failure on a failed lightpath. In addition to this, we develop an algorithm to analyze the information of the alarms emitted by the components of an optical network, in the presence of a fault.

2. RELATED WORK

Bin Wu, Pin-Han Ho and Kwan L. Yeung [4] have considered an optical layer monitoring schemes for fast link failure localization in WDM mesh networks. They have proposed a new concept for monitoring trail (m-trail) which differs from the existing monitoring cycle (m-cycle) concept by removing the cycle constraint. Their numerical result shows that the m-trail based scheme significantly outperforms its m-cycle based counterpart.

Hongqing Zeng, Alex Vukovic, and Changcheng Huang [5] 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.

Michael T. Frederick and Arun K. Somani [7] 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 [8] 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.

Hongsik Choi, Suresh Subramaniam and Hyeong-Ah Choi [9] have considered the network survivability which is a critical requirement in the high-speed optical networks. A failure model is considered so that any two links in the network may fail in an random order. They have presented three loop back methods of recovering from double-link failures. Only the first two methods require the identification of the failed links. But pre-computing the backup paths for the third method is more complex than the first two methods. The double link failures are tolerated by the heuristic algorithm which pre-computes the backup paths for links.

Yufeng Xin, Jing Teng, Gigi Karmous-Edwards, GeorgeN.Rouskas and Daniel [10] have studied the important fault management issue which concentrates on the fast restoration mechanisms for Optical Burst Switched (OBS) networks. The OBS network operates under the JIT signaling protocol. The basic routing mechanism is similar to the IP networks, where every OBS node maintains a local forwarding table. The entries in the forwarding table consist of the next hop information for the bursts per destination and per FEC (Forward Equivalent Class). Based on looking up the next-hop information in their forwarding tables, OBS nodes forwards the coming burst control packets and set up the connections. The connection set up process is signified by the burst forwarding or burst routing.

Jian Wang, Laxman Sahasrabuddhe and Biswanath Mukherjee [11] have considered the fault-monitoring functions which are usually provided by the optical-transmission systems. In order to measure the bit error rate in the wavelength channels using SONET framing, the B1 bit in the SONET overhead can be used. Moreover, to detect certain failures like fiber cut in other formatted optical channels, the optical power loss can be used. Optical-Electrical-Optical (OEO) conversion is used before each OXC port because most of the OXCs use electronic switching fabric. Therefore, faults can be detected on link-by-link basis. Both the end nodes of the failed link can detect the fiber cut for all-optical switches.

Joon-Young Kim, Sil-Gu Mun, Ju-Hee Park, Jin-Serk Baik and Chang-Hee Lee [12] 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 Vukovica, Changcheng Huangb, Heng Huaa and Michel Savoiea [13] have presented a wavelength-routing fault detection scheme for concatenated optical cross connects (OXCs) in all-optical networks (AONs), 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.

3. PROPOSED FAULT LOCALIZATION AND ALARM CORRELATION

3.1. DETECTION AND LOCALIZATION ALGORITHM

In this section, we propose a Link Failure Detection Algorithm which can identify the location of a failure on a lightpath. Our proposed 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, our algorithm will be activated by the destination. The operation of our 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 lightpaths, even before they activate any restoration/localization process.

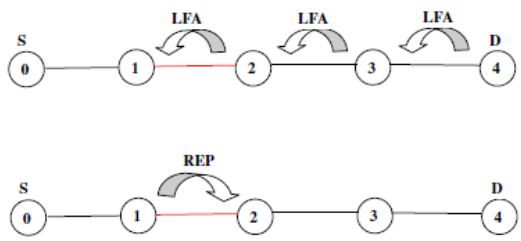

Fig.1. Functions of Link Failure Detection Algorithm

1) Algorithm

Let $n_1, n_2, \cdots, n_k$ be the set of nodes along the route from the source n_1 to the destination n_k.

1. The source n_1 send data packets in fixed time intervals δ. Source sends packets $p_1, p_2, \cdots, p_k$ at time $t1, t1+\delta, t+2\delta, \cdots, t+k\delta$.
2. The destination n_k checks the packet sequence numbers $s_1, s_2, \cdots, s_k$ 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
   - 4.1 n_k raises LFA and transmit backwards to n_j, where $j = k-1$
   - 4.2 If n_j received the data before t, then
     - 4.2.1 It send a REP packet to n_i, where $i = j+1$.
     - 4.2.2 The n_i starts a recovery scheme for restoration
     - 4.2.3 n_j information is flooded through the network.
   - 4.3 Else
     - 4.3.1 $j = j-1$
     - 4.3.2 Repeat the step 1.2
   - 4.4 End If
5. End If

Fig. 1 shows the functions of our 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 [14] is activated to avoid the failed link and restore the connection through a backup path.

3.2. ALARM CORRELATION

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

- A1 – When the damaged component send alarm;
- A2 – When the component alarms informing that other component is not working correctly.

Alarm Correlation Algorithm

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 $(f1, f2, f3, f4)$ having the following meaning for a local node:

$f1$: It can assume the following values: 0 – non-alarming component; 1 – Self alarmed; 2 – Out-alarmed; 3 – Failure masking.

$f2$: It indicates the node number.

$f3$: It is always 0 for a local node.

$f4$: It identifies the position of the component inside the node. The value of this field varies according to the component: $LAP = 0$ (Local Access Port); ADF = 1 or 2 ; RX = 1 or 2 ; 3R amplifier = 4 or 5 ; TX = 5 or 6 ; PS = 3 .

Algorithm

At the physical route domain, all network components that belong to any channel are numbered as $C1, C2, \cdots$ 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_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* $C_i(a)$ *to* S_1
3. *Else* If a = A2 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

3.4 *End* For

4. *End* If

4. SIMULATION RESULTS

4.1. SIMULATION MODEL AND PARAMETERS

In this section, we examine the performance of our Fault Localization and Alarm Correlation algorithm (FLAC) with an extensive simulation study based upon the ns-2 network simulator [15]. We use the Optical WDM network simulator (OWNs) patch in ns2, to simulate an 8-Node topology (Fig.3). Various simulation parameters are given in Table.1.

Table.1. Simulation Parameters

Topology	Mesh
Total no. of nodes	8
Link Wavelength Number	8
Link Delay	10ms
Wavelength Conversion Factor	1
Wavelength Conversion Distance	8
Wavelength Conversion Time	0.024
Link Utilization sample Interval	0.5
Traffic Arrival Rate	0.5
Traffic Holding Time	0.2
Packet Size	200
No. of Session-traffics	4
Max Requests Number	50
No. of Link Failures	1,2,3 and 4

In our experiments, we use a dynamic traffic model 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).

In our experiments, we will consider multiple link failures. We vary the number of link failures as 1, 2, 3 and 4. The connection requests are distributed randomly on all the network nodes. In all the experiments, we compare the results of FLAC with End-to-End [5] scheme.

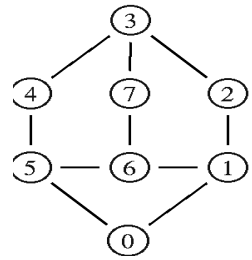

Fig.2. 8-Node Topology

4.2. PERFORMANCE METRICS

In our experiment, we measure the blocking probability, end-to-end delay and throughput.

Blocking Probability: It is the ratio of number of rejected requests to the total number of requests sent**.**

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Throughput: It is the number of packets received successfully.

Channel Utilization: It is the ratio of bandwidth received into total available bandwidth for a traffic flow.

4.3. RESULTS

Our simulation results for the number of failures are presented in Table.2.

Table.2. Simulation Results

No. Of Failures	Blocking Probability		Delay		Throughput	
	FLAC	End-To-End	FLAC	End-To-End	FLAC	End-To-End
1	0.5432	0.686667	1.0966	2.32457	732	427
2	0.6178	0.716666	1.7354	3.09908	642	281
3	0.6805	0.785714	2.2553	4.72548	564	152
4	0.7416	0.823636	4.4825	6.57268	405	104

Our simulation results for the various rates are presented in Table.3.

Table.3. Simulation Results

Rate (Mb)	Blocking Probability		Delay		Utilization	
	FLAC	End-To-End	FLAC	End-To-End	FLAC	End-To-End
2	0.01	0.15	200.8101	258.462486	0.034098	0.015658
4	0.122075	0.2093846	165.6041	243.106743	0.030568	0.01366
6	0.304862	0.4923077	101.2084	230.450229	0.024459	0.006868
8	0.507692	0.6967554	59.88886	152.666943	0.017623	0.002062

4.3.1. Based on Failures:

In the initial experiment, we vary the number of failures as 1, 2, 3 & 4 and measure the blocking probability, end-to-end delay and Throughput.

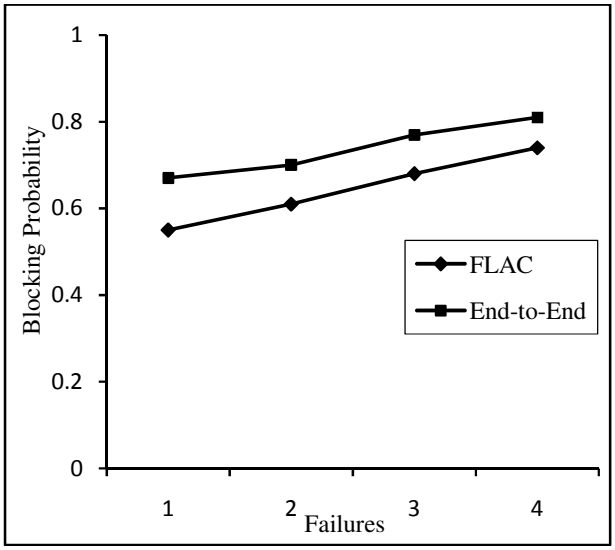

Fig.3. No. of Failures Vs Blocking Probability

Fig.3 shows the blocking probability obtained with our FLAC algorithm compared with End-to-End scheme. It shows that the blocking probability is significantly less than the End-to-End, when number of failures increases.

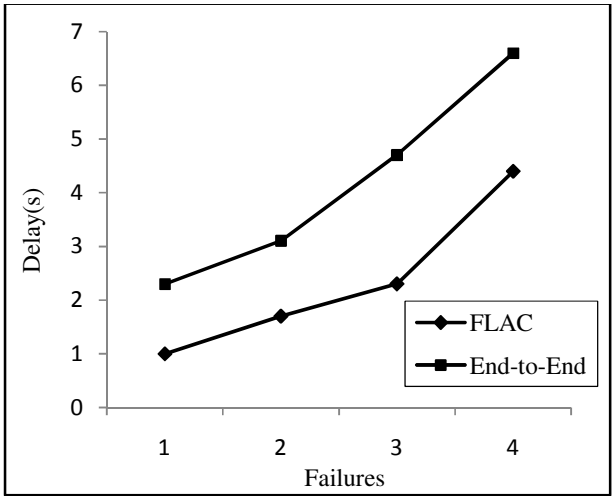

Fig.4. No. of Failures Vs Delay

Fig.4 shows the end-to-end delay occurred for the number of failures. It shows that the delay of FLAC is significantly less than the End-to-End scheme.

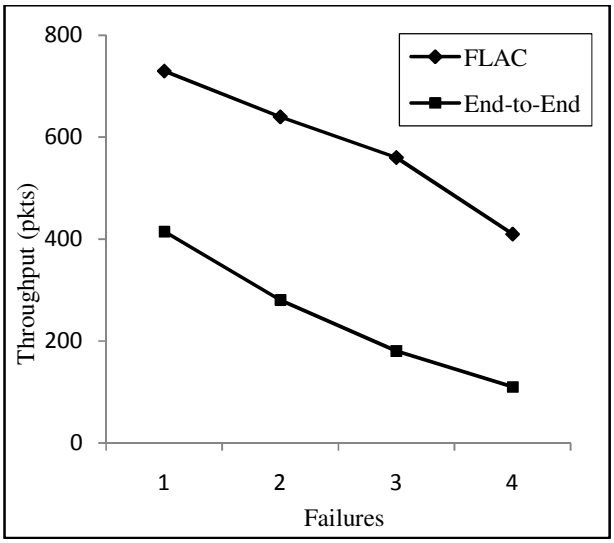

Fig.5. No. of Failures Vs Throughput

Fig. 5 shows the throughput occurred for various failures. As we can see from the figure, the throughput is more in the case of FLAC when compared to End-to-End scheme.

4.3.2. Based on Rate:

In the next experiment, we vary the traffic rate as 2Mb, 4Mb….8Mb and measure the blocking probability, end-to-end delay and channel utilization.

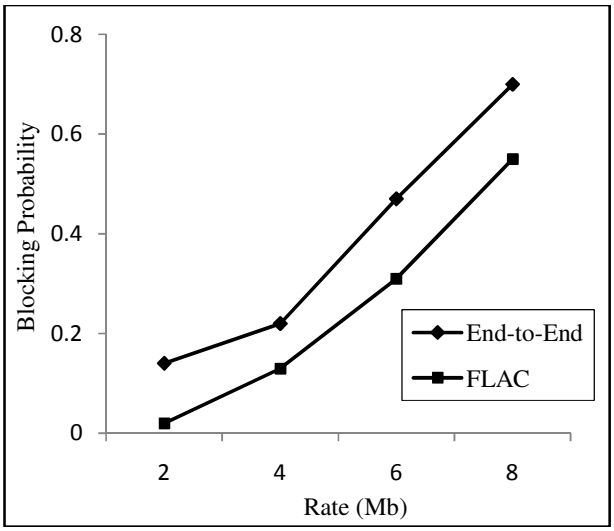

Fig.6. Rate Vs Blocking Probability

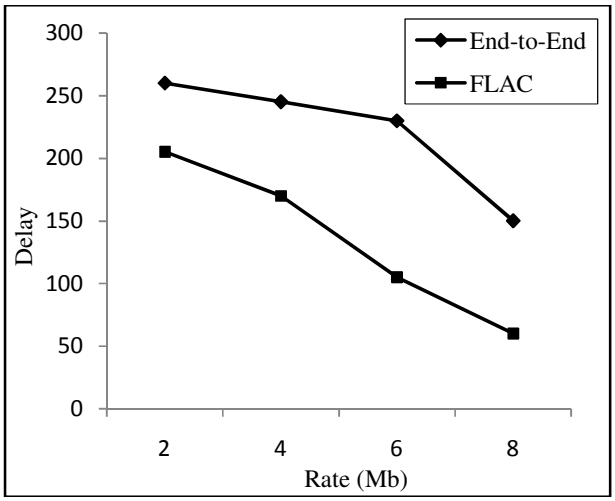

Fig.7. Rate Vs Delay

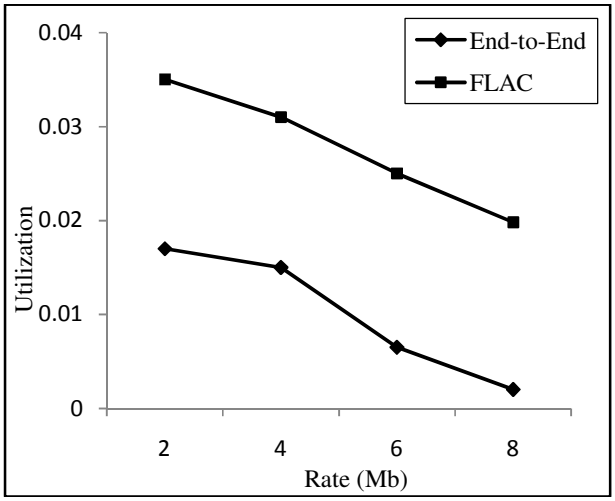

Fig.8. Rate Vs Utilization

Fig.6 shows the blocking probability obtained with our FLAC algorithm compared with End-to-End scheme. It shows that the blocking probability is significantly less than the DPBR, as rate increases.

Fig.7 shows the end-to-end delay occurred for various rates. It shows that the delay of FLAC is significantly less than the End-to-End scheme.

Fig.8 shows the channel utilization obtained for various rate. It shows that FLAC has better utilization than the End-to-End scheme.

5. 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 we have proposed a new fault localization algorithm for WDM networks which can identify the location of a failure on a failed lightpath. Our algorithm detects the failed connection and then attempts to reroute data stream through an alternate path. We have assumed that a failure happens during the data transfer mode due to the short interval time of establishing a lightpath. 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, we have developed an algorithm to analyze the information of the alarms generated by the components of an optical network, in the presence of a fault. The algorithm proposed uses the alarm correlation in order to reduce the list of suspected components shown to the network operators. By our simulation results, we have shown that our proposed algorithms achieve less blocking probability and delay while getting higher throughput. As a future work, we will consider the link failures while establishing the light path.

REFERENCES

[1] Canhui (Sam) Ou Hui Zang ,Narendra K. Singhal, Keyao Zhu, Laxman H. Sahasrabuddhe, Robert A. Macdonald, And Biswanath Mukherjee, "Sub path Protection For Scalability And Fast Recovery In Optical WDM Mesh Networks", IEEE Journal On Selected Areas In Communications, Vol. 22, No. 9, November, 2004.

[2] Vinh Trong Le, Son Hong Ngo, Xiao Hong Jiang, Susumu Horiguchi and Yasushi Inoguchi, "A Hybrid Algorithm for Dynamic Lightpath Protection in Survivable WDM Optical Networks", IEEE, 2005

[3] Sateesh Chandra Shekhar, "Survivable Multicasting in WDM Optical Networks", August, 2004.

[4] Bin Wu, Pin-Han Ho and Kwan L. Yeung, "Monitoring Trail: a New Paradiagm for Fast Link Failure Localization in WDM Mesh Networks", IEEE Global Telecommunications Conference, 2008, IEEE GLOBECOM 2008.

[5] Hongqing Zeng, Alex Vukovic, and Changcheng Huang, "A novel end-to-end fault detection and localization protocol for wavelength-routed WDM networks", submitted in the Communications Research Centre, Canada.

[6] S.Ramamurthy, Laxman Sahasrabuddhe, and Biswanath Mukherjee, "Survivable WDM Mesh Networks", Journal of light wave technology, Vol. 21, No. 4, April, 2003.

[7] Michael T. Frederick and Arun K. Somani, "A single-fault recovery strategy for optical Networks using sub graph routing", The International Journal of Computer and Telecommunications Networking, Vol. 50, Issue 2 February, 2006.

[8] MurielM´edard, "Network Reliability and Fault Tolerance", IEEE Transactions on Vol. 50, Issue 1, pp. 85 – 91, March, 2001.

[9] Hongsik Choi, Suresh Subramaniam, and Hyeong-Ah Choi, "On Double-Link Failure Recovery in WDM Optical Networks", INFOCOM Vol. 2, on pp. 808-816, 2002

[10] Yufeng Xin, Jing Teng, Gigi Karmous-Edwards, George N. Rouskas and Daniel Stevenson, "Fault Management with Fast Restoration for Optical Burst Switched Networks", IEEE, 2004.

[11] Jian Wang, Laxman Sahasrabuddhe and Biswanath Mukherjee, "Fault Monitoring and Restoration in Optical WDM Networks", National Fiber Optic Engineers Conference NFOEC 2002.

[12] Joon-Young Kim, Sil-Gu Mun, Ju-Hee Park, Jin-Serk Baik and Chang-Hee Lee, "Protection and Fault Localization in a WDM-PON", Korea Advanced Institute of Science and Technology.

[13] Hongqing Zeng, Alex Vukovica, Changcheng Huangb, Heng Huaa and Michel Savoiea, "Wavelength-routing fault detection in an AON testbed utilizing concatenated pilot tones", submitted in the Communications Research Centre, Canada.

[14] G.Ramesh and S.Sundara Vadivelu, "A Reliable and Fault-Tolerant Routing for Optical WDM Networks", International Journal of Computer Science and Information Security, December, 2009.