Proactive Fault Localization and Alarm Correlation in DWDM Networks

Prerna Shukla, Gupteswar Majhi, Yogesh Kumar
Centre for Development of Telematics
Mehrauli, New Delhi, India
prerna@cdot.in, majhig@cdot.in,yogeshk@cdot.in

***Abstract*—"Proactive Fault Localization and Alarm Correlation in DWDM Networks" approach proposes a new fault localization algorithm for DWDM networks where every entity of DWDM network participates in correlation of alarms and thus reduces the list of suspected components shown to the network operators.**

***Keywords*— OTN, DWDM, OTS, OMS, OCH, RCA**

I. Introduction

For several high-speed networks, providing resilience against failures is an essential requirement. Quick fault detection and identification make networks stronger and more consistent. Hence, it is necessary to develop swift, efficient, and less complex fault localization or detection mechanisms. Traditionally NMS was flooded with alarms in case of network fault as individual device components start raising their alarms. With this new correlation approach, device component level alarms are handled locally, and NMS is notified with lesser no of events resulting a clear and focused NMS flow.

In this paper we are presenting a proactive alarm correlation approach that provides fast, efficient and dependable fault localization or detection mechanisms. With predefined data, our algorithm detects the root cause of fault first and then attempts to suppress other generated faults within network element. It uses the alarm correlation to reduce the list of suspected components shown to the network operators.

Our simulation results suggest that proposed algorithms achieve accuracy, faster identification of the root cause and less complexity at management layer. This algorithm introduces intelligence in DWDM/OTN components for Root Cause Analysis

A. OTN and Optical Layers

We depict the typical network layer hierarchy in DWDM networks .In an 80 Tera bit DWDM network , a fiber can have up to eighty wavelength .Every wavelength is converted in to OTN4. One OTN4 can have maximum ten 10G Ethernet /OTN2/STM16 clients. In Fig. 1 We assume that for each fiber, there are 'W' wavelengths which are converted into OTN4 signals. Average 'X' OTN2 circuits traverse each OTN4 link. End users connect their OTN2 clients to the termination point of light paths to utilize the end-to-end bandwidth assigned from underlying optical infrastructure.

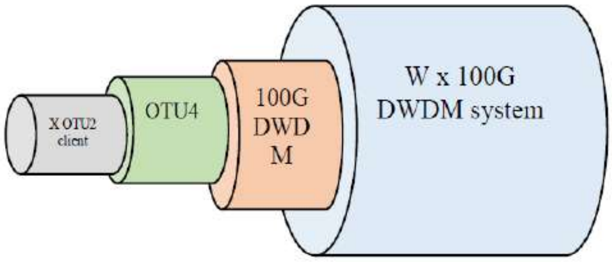

Fig. 1. Network layers of OTN based DWDM system

B. ALARM Propagation in a typical linear DWDM Network

This section talks about DWDM fault scenarios and alarm detection at various sections in such scenario. Backward and forward direction alarm indication in client layer, OTU, OCH, OMS and OTS layer is also covered. Alarms combination for a fault is unique so root cause analysis of every fault can be performed. Three nodes and linear topology is considered. Three nodes ROADM1, ILA1 and ROADM2 are connected in linear fashion ,Channels 1 and 2 are pass through channels from R1 and R2.Channel 3 is add/drop from R1 and R2. OTN client is transported between R1 and R2.

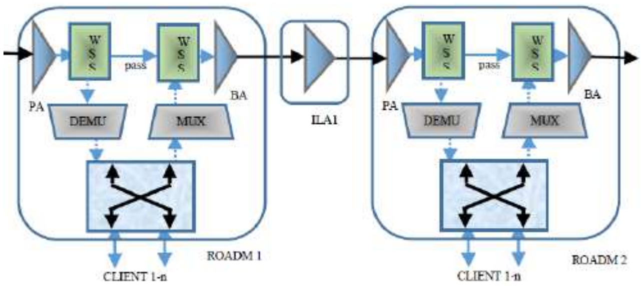

Fig. 2. R1, I1 and R2 in linear topology

TABLE I. Provides an overview of the fault scenarios which are possible in DWDM system. It also covers alarms detected and indicated at R1, I1 and R2 .Fault scenarios can be uniquely identified from different alarms occurring at different stages.

Sr No	Fault Case(Root Cause)	OTS	OMS	OCH	OTU Line	Client	Card
1.	Fiber break(Between R1 and I1)	ROADM1					
		OTS_BDI_P[1] OTS_BDI_O[1]			OTUk_BDI[2]		
		ILA1					

		OTS_LOS_P OTS_LOS_O	OMS_BDI_P				
		ROADM2					
			OMS_FDI_P		LOS_IP[2]	AIS[3]	
2.	Fiber break(Between I1 and R2)	ROADM1					
					OTUk_BDI[2]		
		ILA1					
		OTS_BDI_P[1] OTS_BDI_O[1]					
		ROADM2					
		OTS_LOS_P OTS_LOS_O			LOS_IP[2]	AIS[3]	
3.	Bidirectional Fiber break(Between R2 and I1)	ROADM1					
			OMS_FDI_P		LOS_IP[2]	AIS[3]	
		ILA1					
		OTS_LOS_P OTS_LOS_O	OMS_BDI_P				
		ROADM2					
		OTS_LOS_P OTS_LOS_O			LOS_IP[2]	AIS[3]	
4.	Fiber break(Before R1)	ROADM1					
		OTS_LOS_P OTS_LOS_O					
		ILA1					
		ROADM2					
				OCH_FDI_P[5] OCH_FDI_O[5]			
5.	Node Power Failure(I1)	ROADM1					
		OTS_LOS_P OTS_LOS_O			LOS_IP[2]	AIS[3]	
		ILA1					
		ROADM2					
		OTS_LOS_P OTS_LOS_O			LOS_IP[2]	AIS[3]	
6.	Amplifier failure(R2 PA)	ROADM1					
					OTUk_BDI[2]		
		ILA1					
			OMS_BDI_P				
		ROADM2					
			OMS_LOS_P		LOS_IP[2]	AIS[3]	
7.	PA to OSC fiber break/ connection is improper(R1 PA2) or OSC to BA fiber break/	ROADM1					
		ILA1					
		OTS_LOS_O					
		ROADM2					
			OMS_FDI_O				

	connection is improper(R1)						
8.	Fault in Amplifier (R2 PA)	ROADM1					
					OTUk_BDI[2]		
		ILA1					
			OMS_BD_P				
		ROADM2					
			OMS_LOS_P		LOS_IP[2]	AIS[3]	
9.	Amplifier Card failure(R2 PA) / Jacked OUT	ROADM1					
					OTUk_BDI[2]		
		ILA1					
		ROADM2					
				OCH_LOS_P[2]	LOS_IP[2]	AIS[3]	CARD_ABSENT
10.	Amplifier Failure (R1 BA2)	ROADM1					
		OTS_BDI_P[1]			OTUk_BDI[2]		
		ILA1					
		OTS_LOS_P	OMS_BDI_P				
		ROADM2					
			OMS_FDI_P	LOS_IP[2]	AIS[3]		
11.	Amplifier Card (R1 BA) / Jacked OUT	ROADM1					
		OTS_BDI_P[1] OTS_BDI_O[1]			OTUk_BDI[2]		CARD_ABSENT
		ILA1					
		OTS_LOS_P OTS_LOS_O	OMS_BDI_P				
		ROADM2					
			OMS_FDI_P	LOS_IP[2]	AIS[3]		
12.	Pre Amplifier Failure (R1 PA)/	ROADM1					
			OMS_LOS_P				
		ILA1					
		ROADM2					
				OCH_FDI_P			
13.	Amplifier to WSS(R2) fiber connection is improper	ROADM1					
					OTUk_BDI[2]		
		ILA1					
		ROADM2					
				OCH_LOS_P on all channels	LOS_IP[2]	AIS[3]	
14.	WSS(R1 TX) incoming add port fiber break/ misconnection/ misconfiguration	ROADM1					
			OMS_BDI_P		OTUk_BDI		
		ILA1					
			OMS_PMI OMS_BDI_P				
		ROADM2					
			OMS_FDI_P		LOS_IP[2]	AIS[3]	
15.	WSS Jack Out	ROADM1					
		OTS_BDI_P			OTUk_BDI[2]		CARD_ABSENT
		ILA1					
		OTS_LOS_P	OMS_BDI_P				
		ROADM2					
			OMS_FDI_P			AIS[3]	
16.	MPN failure Or Jack Out (R1)	ROADM1					
							CARD_ABSENT

		ILA1					
		ROADM2					
				Chnl3 OCH_ OCI	LOS_IP	AIS[4]	
17.	MPN to WSS (R1) fiber break/ misconnection	ROADM1					
					OTUk_ BDI		
		ILA1					
		ROADM2					
				Chnl3 OCH_ OCI	LOS_IP	AIS[4]	
18.	Muxponder failure Or Jack Out (R2)	ROADM1					
		ILA1					
		ROADM2					
							CARD_ ABSENT
19.	Line Tx(R1) Fault	ROADM1					
					TX FAULT		
		ILA1					
		ROADM2					
				Chnl3 OCH_ OCI	LOS_IP	AIS[4]	
20.	WSS to MPN(R2) fiber break/ misconnection	ROADM1					
					OTUk_ BDI		
		ILA1					
		ROADM2					
					LOS_IP	AIS[4]	
21.	Client fiber break /Misconnection	ROADM1					
						LOS_IP	
		ILA1					
		ROADM2					
						AIS	
22.	Client TX(R1) Fault	ROADM1				TX FAULT	
		ILA1					
		ROADM2					

Note[1]- Alarms will be visible only if backward direction supervisory link is up.
Note[2]- Alarms on line of all MPN/TPN line cards which are affected by a fault in corresponding OTS/OMS section.
Note[3]- Alarms on all clients of all MPN/TPN card which are affected by a fault corresponding in OTS/OMS section.
Note[4] -Alarms on all clients of a single MPN card.
Note[5] -Alarms on all channel which are passing through a node.
*Detected alarm are in orange color
*Forward indication alarms are in green color
*Backward indication alarms are in blue color
* Root cause of an event is in red color

II. CORRELATION DIAGRAM AND PROPOSED ALARM CORRELATION ALGORITHM

In previous section we have seen that how a failure in a network can generates and propagates faults in other layers in forward and backward direction. In most approaches all alarms and indication were reported to NMS for RCA of fault. In this paper we propose a Novel Alarm Correlation algorithm that simplifies root-cause analysis by implementing RCA in DWDM nodes itself. The flow of our proposed alarm correlation algorithm is illustrated in Fig. 3.

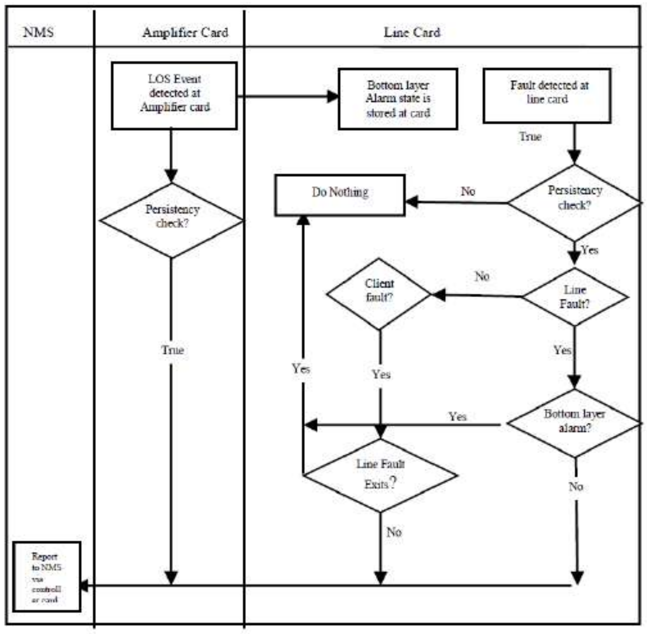

Fig. 3. Alarm correlation algorithm

Unlike the traditional algorithm, in our model correlation granularity is reduced to card level. Proposed proactive model of alarm correlation has multiple layers of masking and suppression that starts from device and reaches to controller card.

Muxponder carries predefined alarm relational data as well as ability to correlate and suppress alarms while Amplifier also has ability to propagate its fault towards Muxponder. With this new approach Muxponder acts intelligently and correlate alarms of top layer according to bottom layer alarms and thus reduced complexity at management layer. This model works in two phases –

A. Before fault

As soon as card is initialized and configured ,control plane relational information is transferred to card via controller card. This data includes configuration status of its corresponding bottom layer and alarm correlation model for its bottom layer alarms. Configuration status data at Muxponder consists of following information.

- Client layer is aware of OTU server layer
- OTU server layer is aware of its corresponding OCH ,OMS and OTS layer

Alarm correlation data is created by categorization of alarms by layers and assigning priority as a first step and then alarms are correlated intra-layer and then inter- layer. This model can be classified in two parts -

1- **Optical layer alarm relational data for Inter node Masking** -An alarm in any of the optical layers such as OTS, OMS and OCH can be masked according to predefined correlation data available at controller.

2- **Electrical and optical layer alarm relational data for Intra node Correlation and Suppression** - It can be further divided into two levels-

A-Electrical Alarm correlation at device level-This is in general provided by device.

B-Electrical and optical layer alarm correlation - Bottom layer electrical Alarm suppression according to top layer optical/electrical alarms-

i- Correlation between client ,ODU and OTU server layer

ii- Correlation between OTU server layer and OMS/OTS layer

B. After fault –

After fault, correlation is done on every entity depending on predefined data. Any alarm is forwarded to management layer only when if it is not belonging to any bottom layer alarm. This process involves diverse actions on different entity-

1) Link failure action on Muxponder and Amplifier

As a common example of link failure scenario if there is fiber cut event, amplifier reports this event immediately to Muxponder card, but this event is reported to NMS only after persistency check. Muxponder will also receive events at OTU and client layer. Persistency check will also happen at Muxponder for its events .After persistency check correlation of alarm will happen at Muxponder card. As a result of correlation algorithm Muxponder events will not be forwarded to controller. To handle toggling of any event at Amplifier card a toggling detection algorithm is applied, so that if frequent toggling is occurred event is not forwarded to corresponding top layer entities.

2) At Controller layer –

Alarm is masked at controller layer as predefined relation and only root cause of an event is reported as unmasked. Alarm is masked at controller layer if any high priority alarm is reported.

3) At NMS –

Only single alarm will be reported as root cause of alarm by a node. All other will be reported as masked or will be suppressed at node/card itself. At NMS there is no need to perform alarm correlation for a node/sub-network.

III. EXPERIMENT SCENARIOS

In this section, we would like to demonstrate the algorithm in lab environment. These tests are performed at our test bed in C-DOT DWDM lab. From the test results, we illustrate the alarm correlation diagram. The network topology is depicted in Fig. 4. We simulate three sites called A, B and C. Site A, has ROADM capability. A Muxponder can take maximum 10 clients of 10g data rate. This ROADM can multiplexed / de multiplexed maximum 80. Site B is in line amplifier .Site C is ROADM node. Site R1, R2 have two shelves that operate in DWDM and OTN layer separately. Site I1 is single shelf node which provides inline amplification functionality. There are two fibers which connect node R1-I1 and node I1-R2. OTN client is transported between R1 and R2.

Case 1-Fiber cut between ILA1 and R2-

When fiber is cut between I1 and R2 following action takes place-

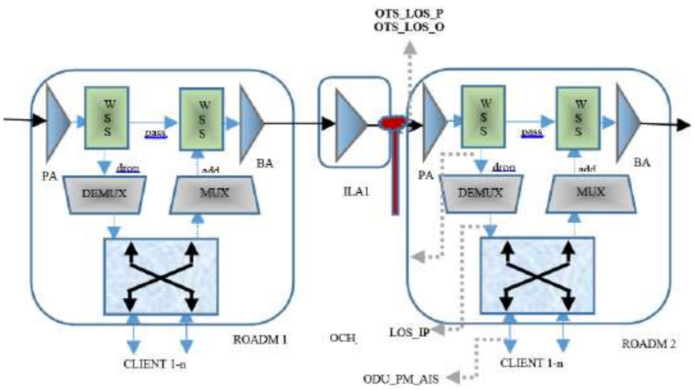

Fig. 4. Fault propagation when there is fiber cut between I1 and R2

At Muxponder- Muxponder receives OTS_LOS_P event indication. Muxponder detects OTN_LOS at line side and ODU_PM_AIS at client side. Muxponder suppress OTN_LOS and ODU_PM_AIS by not reporting these alarms to controller.

At Controller-Controller receives OTS_LOS_P and OCH_LOS_P of all OCH section .Controller masks OCH alarms and sends only OTS_LOS_P alarm to NMS.

At NMS- Only OTS_LOS_P alarm is displayed.

Case 2-Fiber cut between R1 and ILA1 and-

When fiber is cut between R1 and I1following action takes place- **Alarms at ILA1**

At Controller-Controller sends only OTS_LOS_P alarm to NMS.

At NMS- Only OTS_LOS_P alarm is displayed from I1.

Alarms at R2

At Muxponder- Muxponder receives OTS_LOS_P event indication. Muxponder detects OTN_LOS at line side and

ODU_PM_AIS at client side. Muxponder suppress OTN_LOS and ODU_PM_AIS by not reporting these alarms to NMS.

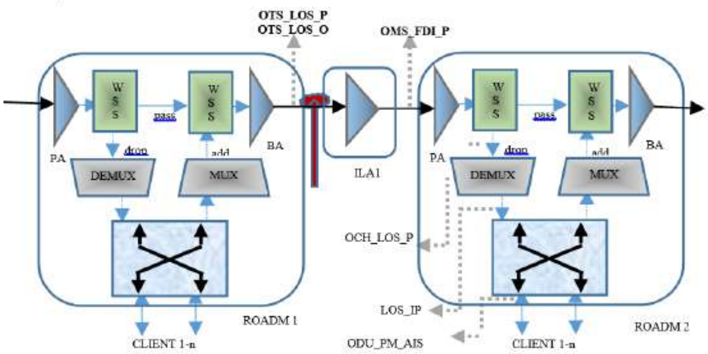

Fig. 5. Fault propagation when there is fiber cut between R1 and I1

At Controller-Controller receives OTS_LOS_P and OCH_LOS_P of all OCH section .Controller masks OCH alarms and sends only OTS_LOS_P alarm to NMS. OTS_LOS_P alarm is masked as soon as it receives OMS_FDI_P from ILA1.

At NMS- Only OMS_FDI_P alarm is displayed from R2.

From above test result it is demonstrated that correlation of alarm is performed by proactive distributed correlation system and only one alarm is reported as root cause of event.

A. Abbreviations and Acronyms

BA	-	Booster Amplifier
CSCC	-	Central Supervisory Controller Card
NE	-	Network Element
NMS	-	Network Management System
OA	-	Optical Amplifier
OMUX	-	Optical Multiplexer
PA	-	Pre-amplifier
TE	-	Terminal Equipment
RCA	-	Root Cause Analysis

IV. CONCLUSION

In this paper, we have described a root cause analysis technique that exploits a relationship that commonly exists between multiple layers in a network elements

This technique uses pre-existing control plane relational information data in the node without any extra data collection procedure. The algorithm we use is efficient and time saving and does not impose any overhead at the time of fault. The algorithm is a generalized and expandable and agnostic to node components, nodes and networks.

ACKNOWLEDGMENT

The product and approach mentioned here is an inspiration of our visionary director Dr. Pankaj Dalela.

REFERENCES

[1] Sava Stanic, , Suresh Subramaniam, , Gokhan Sahin, and Hyeong-Ah Choi, "Active Monitoring and Alarm Management for Fault Localization in Transparent All-Optical Networks", IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 7, NO. 2, JUNE 2010 (spatial database to handle big data)

[2] Te-Lung Liu, Hui-Min Tseng, Hui-Min Chen, Jen-Wei Hu, Chu-Sing Yang and C. Eugene Yeh, "Design of Alarm Management System in Hybrid IP/Optical Networks 2009 International Conference on Advanced Information Networking and Applications Workshops

[3] G.Ramesh and S.SundaraVadivelu, " Fault Localization and Alarm Correlation in Optical WDM Networks" International Journal of Information and Communication Engineering 6:2 2010

[4] Yekta Turk, Engin Zeydan, Fatih Mercimek, and Engin Danisman. "Unified and Automated Fault Management Platform for Optical Networks"