ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

August 2009, 16(4): 23–28
www.sciencedirect.com/science/journal/10058885

The Journal of China Universities of Posts and Telecommunications

www.buptjournal.cn/xben

Fault management: analysis of fault location algorithm in optical network

ZHENG Yan-lei (✉), HUANG Shan-guo, ZHANG Xian, GU Wan-yi

School of Telecommunication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract

This article proposes a new fault location mechanism in optical network. In this mechanism, a network alarm packet format with time-stamp is introduced to implement fast restoration. In locating the fault, the existing schemes are usually complex and inaccessible when solving the multifailure location problem. For multifailures, the proposed mechanism using time-stamps is more efficient in locating the fault and decreasing computational complexity.

Keywords fault location, alarming packet, time-stamp, optical network

1 Introduction

By 2000, wavelength division multiplexing (WDM) technology, which really improves the transmission capacity of a single fiber, has been applied substantially in backbone optical networks. One optical cable contains 8–64 fibers, and the number of fibers in transcontinental cables that use ribbon structure can reach several hundred. If four or more optical carrier signals are used in one fiber, this fiber can carry data information as many as *T* bit/s. Moreover, inexpensive devices such as semiconductor optical amplifier and wavelength converter also facilitate the rapid development of WDM technology.

Because of large data-carrying capacity in WDM networks, a single failure may result in large amounts of data loss. How to guarantee network survivability has received much attention [1]. Survivability represents the ability to protect and restore the data in optical network after node(s) and/or link(s) fail. Till now, many kinds of protection/restoration mechanisms have been proposed, but their realizations depend in part on the triggering of fault alarms and corresponding detection of the fault location [2–3]. If a failure occurs in the network without being detected or the failure cannot be localized exactly according to the alarm packet, it will lead to network's inability to start the normal protection/restoration mechanism. Hence, fault detection and location has a direct impact on network survivability [4].

Fault location problem in optical network is difficult to deal with, because when network failures (e.g. optic fiber breaks) happen, all related nodes and detection points will report alarms (namely, just one single failure will trigger large amounts of alarms) [5]. When many alarms reach the manager through the management communication network, it is difficult to locate the multifailures exactly without much troublesome manual checking and measuring [6].

In this article, the authors propose a fault localization model to solve the above problems. In this model, the central management system judges the fault location, whereas the distributed network elements report the alarm in formations. The manager can detect the fault(s) location using network topology and alarm packet analysis.

In the following sections, the authors first explain basic concepts and properties that will be used in the proposed model (Sect. 2), and then introduce fault management system, analyze the alarm packet format used between the manager and elements when using distributed alarm system (Sect. 3). By analyzing the fault alarm phenomena, Sects. 4 and 5 formalize the fault location algorithm mathematically. In Sect. 6, a concrete network scenario is used to depict the whole fault location process. Finally, conclusions are presented in Sect. 7.

Received date: 02-07-2008
Corresponding author: ZHENG Yan-lei, E-mail: leonard.zheng@gmail.com
DOI: 10.1016/S1005-8885(08)60243-5

2 The model of fault location algorithm

Network is usually depicted as many nodes connecting with each other by links. By analyzing the alarm packets reported by the network elements, the network manager can locate multifailures [5–7]. In this section, we will define and regulate the terms that will be used in fault location management model.

2.1 Network components

In WDM network, typical network components include transmitter, receiver, optical add-drop multiplexer, optical cross connection, etc. According to the ITU-T G.7710 Rec., network components can be classified into two categories in fault management: active component and passive component. An example of a passive component is optical fiber [8]. Active components work based on electrical needs. This category includes many components such as transceiver, optical cross connect (OXC), (de) multiplexer, etc. Obviously, as the managed objects, only active components can send alarm information to the manager directly.

2.2 Alarm type and failure source points

Alarms are messages sent to the manager by network elements to inform an abnormal condition (e.g. values of the component out of range or missing). Passive components cannot give any information to the manager. For active ones, there are two kinds of alarms: self-alarm and out-alarm.

1) Optical fiber break is one of the most frequently occurring failures in optical network [3]. Though fibers will not send alarms when broken, the active components after it will be triggered to report alarms till the end of the channel. According to the classification of alarm types [8], these alarms are defined as out-alarm, because the components send alarms after the failure occurs.

2) Node failure is viewed as the second frequent failure. For example, the physical distortion caused by hardware aging of the input and output ports of OXC will result in alarm for degradation in signal qualities of all the channels. In addition, some failures caused by equipment abnormal value, such as temperature and the optical signal power, will also trigger alarm report. These kinds of alarms as classified as self-alarm.

In terms of severity, alarms can be divided into normal alarms and severe alarms. M1 and M2 are used below to identify them: ‘M1’ means the normal working interval. The parameter will report normal alarm when the value is deviated from the interval, but the component still works; ‘M2’ means the working interval. The parameter will report severe alarm when the value is deviated from this interval, and then the component will stop working and try to start backup equipment.

2.3 Downstream and upstream

For a given node S_n in one channel following the data transmission direction, the nodes before S_n are called upstream nodes, whereas the nodes after it are called downstream ones.

2.4 Grouping and unidirectional channel

The failure of one network component may affect its downstream node till the end of the channel, or there is one node terminating its effect [9]. Group is defined as the set of active components sending alarms because of a failure in one channel. It can be easily concluded that the components falling into the group are out-alarm components.

The WDM channels defined in this article are unidirectional, which denoted by C_i and expressed as:

$$C_i = \{S_l\,|_{l=\text{number}}\} \tag{1}$$

The Group is an order decided by alarm packets [9]:

$$G = \{P_1, P_2, \ldots, P_n\} \tag{2}$$

If one chooses one active component and denotes its position as *P*, then the first one in the group is called P_1 and the rest may be deduced by analogy. There is difference between *P* and the alarm origin S_l: the former one is decided by concrete alarms and groups, whereas the latter is a unique identification of the network components. The expression of *P* position is,

$$P_i < P_j, P_i + n = P_j\,|;\quad 1 \leqslant i < j \in N, N = (1, 2, \ldots, n) \tag{3}$$

2.5 Time-stamp

The time-stamp adopted in this article is used as an important parameter to localize failures. Alarm packets will be sent to the network management center, whereas the arrival sequences of them cannot be obtained easily as the alarms downstream nodes report maybe reach the management system earlier than the upstream does. Therefore, the time when the failure happens is considered rather than the time when the alarm packet reaches the network management. When the network management system receives the alarm packets, it will choose one benchmark time and extract the failure time from every alarm packet. The smaller value of