Reliability Issues in an All-Optical Direct-Access Network Architecture

Liuyang Li, Sun-il Kim, and Steven S. Lumetta
CS and ECE Dept., University of Illinois at Urbana-Champaign
Coordinated Science Laboratory, 1308 W. Main St., Urbana, IL 61801
{*lli,sunilkim,lumetta*}*@uiuc.edu*

1 Introduction

A robust optical access architecture for a wavelength division multiplexing (WDM) mesh local or metropolitan area network (LAN/MAN) was introduced in [1]. This architecture provides low-cost access to shared wavelengths in optically transparent networks in a flexible and efficient manner, and provides robustness to single link and single node failures through a recovery protocol implemented in hardware. Faults affecting the availability of the recovery service thus affect the reliability of the networks. In this paper, we present a study of the reliability of the hardware implementation and its interaction with the access architecture.

Investigation of reliability of the opto-electronic hardware design and the all-optical network architecture, and their impact on each other has not been given much attention. We consider a model with two levels of network services. The first level of service refers to the normal network operation (access protocol). The second level of service consists of the protection scheme that is needed for handling a link or a node failure in the network which disrupts the first level of service (recovery protocol). A hardware fault may affect the access protocol, immediately disrupting the network service. On the other hand, some faults have no effect on the access protocol, but may effectively disable the protection service. *Dormant fault* refer to component faults that have no impact on the normal operation of the network, but can potentially bring down the protection service. In order to further guarantee highly reliable network services, we must understand how the network architecture and the hardware interact when hardware component faults are introduced.

We first proceed with a brief description of the access architecture and the hardware implementation. In Section 3, we provide a preliminary set of results from performing fault injection on gate-level electronics using our Optical Network and Device Simulator (ONDS), a discrete event simulator. We conclude with a discussion of future works.

This work is funded by NSF ANI 01-21662 ITR

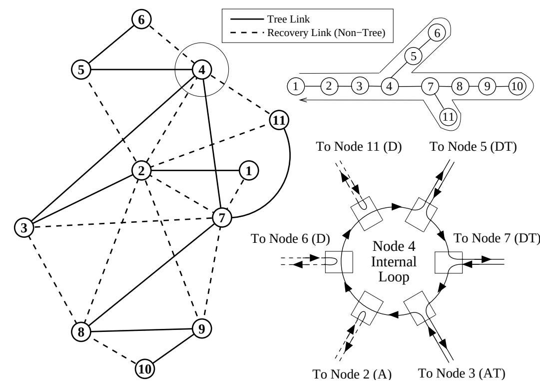

Figure 1. Access Route on NJ LATA

2 Architecture and Implementation

The access architecture allows low-cost access to a shared-wavelength without affecting other lightpaths in WDM systems. A detailed description of medium access control (MAC) protocol is out of the scope of this paper, and can be found in [1]. We explain how the shared wavelength access route is selected and configured in this section.

The architecture utilizes a depth first search (DFS) tree to build the access route, and is applicable to arbitrary link(or node)-redundant mesh networks. Links on a node are labeled as either ancestor(A) or descendant (D) depending on the relative order of the current node in the DFS tree. If a link is a part of the DFS tree that makes up the access route, it is labeled as a tree link (T). Figure 1 shows an example of a collection route and the link labeling on node 4 of the New Jersey Local Access Transport Area network (NJ LATA).

As shown in the, links on a node are interconnected in a ring called the *node internal loop*, which can be preconfigured by setting up the photonic crossconnects (PXCs) on the node. The white boxes in the figure represent *access protocol units* (APU). The APU is an opto-electronic device that we designed to execute the recovery protocol in a distributed manner in the event of a link or a node

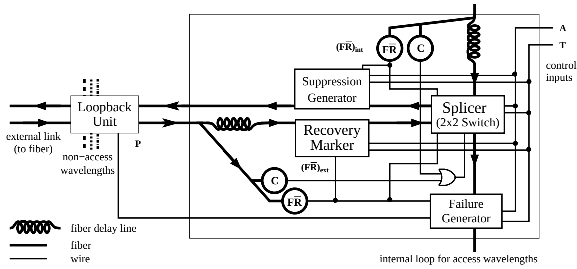

Figure 2. Access Protocol Unit Design

failure. APU's are attached at the ends of all links in the network. The block diagram of the APU is shown in Figure 2. The central component of the APU is the splicer, which contains a 2×2 optical switch. The configuration of the splicers on a link determines the inclusion of the link in the access route. The other four components—loopback unit, failure generator, suppression generator and recovery marker—participate in the recovery process by generating failure/recovery signals and by looping back broken connections. A detailed description of these electro-optical components are elided for brevity.

3 Simulation and Fault Injection

ONDS, a discrete event simulator, was built to simulate the access architecture. In addition to simulating the access architecture, ONDS simulates the behavior of the APU in detail. For example, signals between electronic logic gates and optical devices are explicitly simulated, supporting a wide range of experiments.

Logic gate faults were introduced to the ONDS through fault injection to study the robustness of the access architecture and the hardware implementation. Three fault types—stick high, stick low, and uncertain output—for the gates were examined. Different modes of a fault occurrence, i.e, static, transient, and chronic, were also considered. We first study the impact of a component fault on the normal operation of the network. We then test the impact of dormant faults, which had no impact on the normal service, on the protection service. The root node of the DFS tree monitors control signals on the access wavelength at the end of the access route in the current fault detection scheme.

Results from our investigation are shown in figure 3. Percentage are over faults injections of each type for every logic gate output in the APU. The majority of the logic gate faults have no impact on the normal operation of the network, where about 5.9% of the total number of faults cause a service disruption. Only 2.1% of the faults cause network failures and cannot be detected. It is interesting to note that 94.1% of the faults have no impact on the access route op-

Network Service (Normal Operation of the Access Route)

	Failure Modes			Average
	Static	Chronic	Transient	
Network Failure	8.2%	5.1%	4.3%	5.9%
Detectable	5.9%	2.8%	2.6%	3.8%
Non−Detectable	2.3%	2.3%	1.7%	2.1%
Dormant−no impact	91.8%	94.9%	95.7%	94.1%
Detectable	6.6%	4.9%	4.9%	5.5%
Non−Detectable	85.2%	90.0%	90.8%	89.7%

Effect of Non−Detectable Dormant Faults on Protection Service (Recovery Protocol)

Detectable		Non−Detectable	
Static fault	20% failure	Static fault	7% failure
Chronic fault	95% failure	Chronic fault	94% failure
Transient fault	95% failure	Transient fault	94% failure

Figure 3. Two-Level Service Model

eration. However, most of the dormant faults prevent the recovery protocol from successfully reconstructing the access route when a link or a node fails. Most of these faults are also non-detectable.

4 Conclusions and Future Work

Studying the interaction of the protocol and the hardware implementation under different failure modes using the two level service model enables us to gain a deeper understanding of the issues that need to be considered in designing reliable optical networks.

Some of the faults that cause network failures cannot be detected. Most of the dormant fault are also non-detectable and most of these faults lead to failure of the protection service. Efficient mechanisms to detect these faults are therefore necessary.

We are currently looking at tradeoffs in two possible detection mechanisms, one at the hardware level and a second at the protocol level, that can substantially raise the coverage rate of hidden fault detection. Fault localization is also very important and needs to be addressed.

We have tested logic gate faults for which the characteristics such as the mean time to failure are relatively well known. We are currently investigating impact of optical device faults, such as signal degradation and crosstalk, on the two level of services that are present in our architecture and in other similar systems.

References

[1] M. Médard, S. S. Lumetta, and L. Li, "A Network Management Architecture for Robust Packet Routing in Optical Access Networks", to appear in *IEEE Journal on Selected Areas in Communications*, exp. May 2002.