Fault/Attack Tolerant Recovery Mechanism Under SRLG Constraint in the Next Generation Optical VPN

Jin-Ho Hwang[1], Ju-Dong Shin[1], Mi-Ra Yun[1], Jeong-Nyeo Kim[2], Sang-Su Lee[2], and Sung-Un Kim[3,⋆]

[1] Pukyong National University, 599-1 Daeyeon 3-Dong Nam-Gu, Busan, 608-737, Korea
{jhhwang, jdshin, eggshape}@mail1.pknu.ac.kr
[2] Electronics and Telecommunications Research Institute, 161 Gajeong-Dong, Yuseong-Gu, Daejeon, 305-350, Korea
{jnkim, sangsu}@etri.re.kr
[3] Pukyong National University, 599-1 Daeyeon 3-Dong Nam-Gu, Busan, 608-737, Korea
kimsu@pknu.ac.kr

Abstract. A "Virtual Private Network (VPN) over Internet" has the benefits of being cost-effective and flexible. However, given the increasing demands for high bandwidth Internet and for reliable services in a "VPN over Internet," an IP/GMPLS over DWDM backbone network is regarded as a very favorable approach for the future "Optical VPN (OVPN)" due to the benefits of transparency and high data rate. Nevertheless, OVPN still has survivability issues such that a temporary fault can lose a large amount of data in seconds, moreover unauthorized physical attack can also be made on purpose to eavesdrop the network through physical components. Therefore fault/attack tolerant recovery mechanism that considers physical components is needed because optical network has vulnerabilities involved in the intrinsic characteristics, and these characteristics possibly menace reliable services in OVPN. Thus in this paper, with considering fault/attack in the next generation OVPN, we propose a recovery mechanism under shared risk link group (SRLG) constraint for network survivability by means of the classification of optical components and shared risk levels.

1 Introduction

As the Internet and optical network technology advances, the IP over DWDM has been envisioned as the most promising solution for the next generation optical Internet (NGOI). Especially, core transport networks in NGOI are currently in a transition period evolving from SONET/SDH-based time division multiplexed (TDM) networks utilizing a single wavelength to dense-wavelength

⋆ Corresponding Author.

M. Freire et al. (Eds.): ECUMN 2004, LNCS 3262, pp. 386–396, 2004.

division multiplexed (DWDM) networks with the multiple wavelengths strictly for fiber capacity expansion. On purpose to control for both optical and electronic networks, generalized multi-protocol label switching (GMPLS) has shown up and is currently under standardization at the Internet engineering task force (IETF)[1][2]. Therefore IP/GMPLS over DWDM network is emerging as a dominant technology for use in the next generation backbone network.

VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The primary advantages of "VPN over Internet" are cost-effectiveness and flexibility while coping with the exponential growth of Internet. However, the current disadvantages are the lack of sufficient quality of service (QoS) and provision of adequate transmission capacity for high bandwidth services. For resolving these problems, OVPN over the next generation optical Internet (NGOI)[3] has been suggested for supporting a variety of guaranteed high bandwidth-needed services in OVPN, but it still needs to provide optical QoS provisioning as described in[4], and the network survivability.

For the network survivability in OVPN, sequential procedures such as fault/attack detection, localization and recovery, are the most important issues because a short service disruption in DWDM networks carrying extremely high data rates causes loss of vast traffic volumes. In addition, the existing schemes for fault/attack management may no longer have access to the overhead bits that are otherwise used in legacy networks to transport supervisory information. Eventually, unlike in the case of the existing network, the new survivability mechanism considering intrinsic OVPN features is necessary to provide network survivability[5][6][7][8][9]. GMPLS can manage fault/attack in OVPN. It provides detection, localization, notification and recovery mechanism. When fault/attack or signal degradation is detected, the localization procedure gets started immediately by link management protocol (LMP) that runs between adjacent nodes. Thereafter, the notification procedure is started by resource reservation protocol (RSVP-TE), and determined recovery scheme transfers the traffic to a backup path.

Recently, a key feature of GMPLS is the backup path establishment that keeps physical-diversity (which is also called by physical-disjoint). It is also a dominant issue in OVPN backbone network. In OVPN, each link set up in one lightpath may cross one or more optical components, where the fault/attack of optical components may result in the potential failure of the link. A component here essentially presents any part or site involved in the integrity of the links and associated with a shared risk group (SRG) defined as resource groups having shared risk in common [10][11][12].

In this paper, we ramify SRG with considering the coverage of fault/attack and optical components in OVPN, and propose fault/attack tolerant recovery mechanism to guarantee the physical-diversity under SRLG constraint. Thereafter, we simulate and analyze the performance of the proposed recovery mechanism in the aspect of survivability[13][14].

The rest of this paper is organized as follows: section 2 describes OVPN structure and network survivability issues. In section 3, fault/attack classification for SRG is presented in the viewpoint of survivability, and SRG is defined in accordance with the coverage of fault/attack. In section 4, we illustrate the proposed recovery mechanism under SRLG constraint, and evaluate for the performance through simulation in section 5. Finally, some concluding remarks are made in Section 6.

2 OVPN Structure and Network Survivability Issues in OVPN

2.1 OVPN Structure

The suggested OVPN structure in figure 1 consists of the customer sites in the electric domain and the DWDM network in the optical domain. The external customer sites based on IP network aggregate (or de-segregate) IP packets at customer edge (CE) nodes and the internal OVPN backbone network composed of the provider edge (PE) nodes and the provider (P) core nodes forwards data traffic between the customer sites without electronic-optic-electronic (E-O-E) conversions[4].

An established lightpath between the CE1 and the CE2 may cross a number of intermediate P nodes interconnected by fiber segments, amplifiers and optional taps. The optical components that constitute a P node, in general, include an optical switch, a demultiplexer comprising of signal splitters and optical filters, and a multiplexer made up of signal combiners. A P node may also contain a transmitter array (Tx) and a receiver array (Rx) enabling local add/drop of the wavelengths.

In this structure, we can describe three management sections taking into consideration resource types (optical components) and the coverage of fault/attack effects.

• *Optical Channel Section*(OCh) : Channel management section for one lightpath established between CE nodes.
• *Optical Multiplexing Section*(OMS): Link management section for one link between adjacent nodes. This includes Optical Amplifier Section (OAS) and Fiber Intrusion Section (FIS).
• $P(or PE)$ *Node Section* : Node management section including demux, optical switch and mux that are divided and managed by sub management sections, i.e. Demultiplexing Section (DS), Switching Section (SS) and Multiplexing Section (MS).

2.2 Network Survivability Issues in OVPN

The ramification of network survivability in OVPN backbone network is depicted in figure 2. Fault survivability contains fault management for a sudden fault of

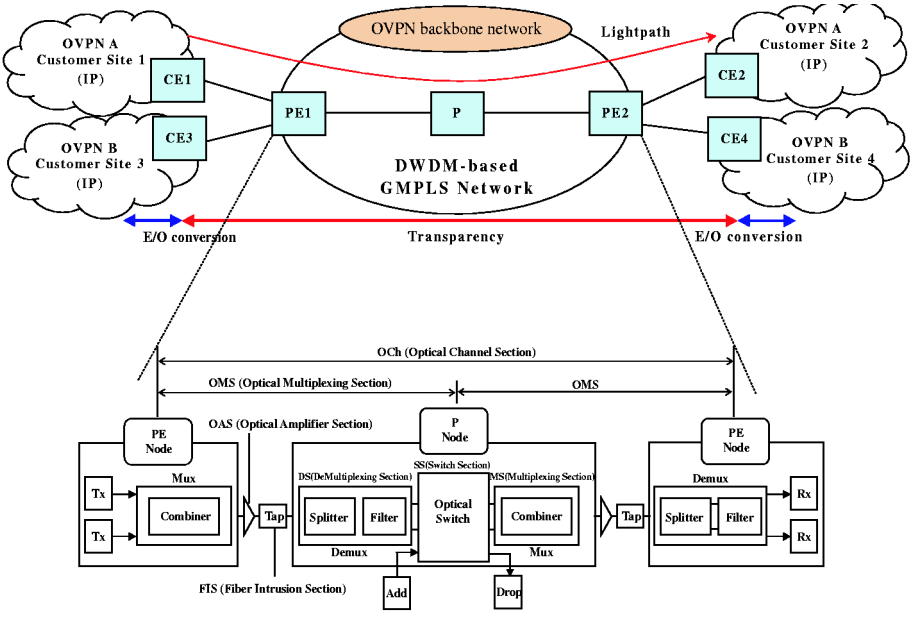

Fig. 1. OVPN Structure

optical components and signal degradation management. Also, attack survivability is divided into physical attack management and logical attack management depending on attack methods. Especially, physical attack in optical domain needs to be managed in optical layer because it causes signal degradation by maliciously using intrinsic characteristics of optical components[6][7][8][9]. However, logical attack is defined as an unauthorized person's network access on purpose to modify or to eavesdrop information, and has to be dealt by quantum-cryptography, but it is beyond the scope of this paper.

In order to manage fault/attack, the sequential mechanism is needed as follows: detect fault/attack as soon as possible (detection), separate fault/attack from normal traffic (localization), and notify fault/attack to network elements which are responsible for network management (notification) and recover traffic to avoid fault/attack (protection/restoration).

3 Fault/Attack Classification for SRG

3.1 Fault/Attack Classification

OVPN backbone network has many fault possibilities due to vulnerable characteristics of optical components used in DWDM network, so short and sporadic failures of network elements may cause a large amount of data loss. In fault survivability, the physical fault (or hard fault) on optical components has to be considered firstly. It causes failure in all optical channels that are going through

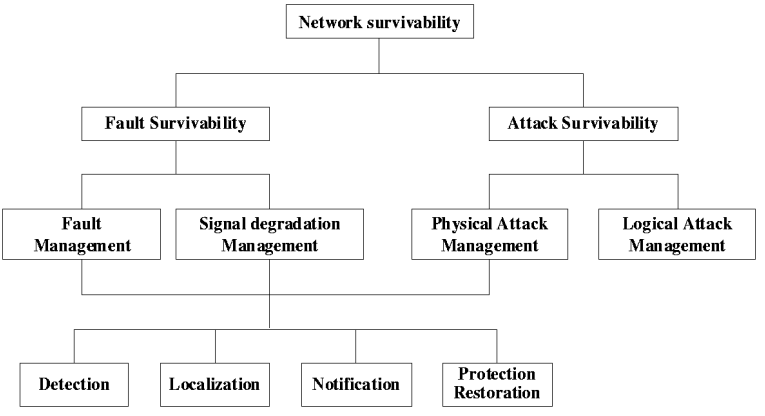

Fig. 2. Network Survivability in OVPN

a link or in a specified optical channel. The coverage of fault is specified depending on the optical components. Resource types and the coverage of fault are summarized in figure 3.

On the other hand, optical components such as optical fiber or erbium-doped fiber amplifier (EDFA) can be used by first attack point to cause signal degradation or to eavesdrop information. For example, gain competition attack causes signal degradation in optical channels that are going through a link by using intrinsic feature of EDFA as mentioned in[8]. With reference to the OVPN structure shown in figure 1, we categorize attack issues at two functional levels, and they are summarized in figure 3 [6][7].

• *Direct attack* : there are certain physical link elements with their own peculiar characteristics that are more likely to be exploited by an intruder as direct attack ports.
• *Indirect attack*: there are certain optical components (P or PE node) that are unlikely to be attacked directly either because a direct attack is too complicated to generate the desired effect or because the ports are not easily accessible to the potential intruders.

As the aspect of the above, in OVPN backbone network, a single fault or attack has various coverage of effect (OCh, OMS, node) depending on resource types or fault/attack types. Thus recovery mechanism needs to be done by making common risk group to avoid common fault/attack. In the following subsection, we define SRG according to the analysis of fault/attack coverage.

3.2 SRG Definition

A SRG is defined as a group of links or nodes that share a common risk component, whose fault/ attack can potentially cause the failure of all the links or nodes in the group. When the SRG is applied to the link resource, it is referred

Category	*Resource type*	*Fault possibility*	*Attack possibility*		*SRG*	
Path (OCh)	Transmitter	Laser or laser driver electronic problem	Signal Degradation with high power laser	Direct Attack	Channel	SRLG
		Pump laser temperature due to high current				
	Receiver	Out of range power or unacceptable input optical power	Unauthorized access to information			
Link (OMS)	Fiber (FIS)	Fiber damaging or cutting	Fiber cut or optical power reduction		Fiber	
			Tapping only or jamming only			
			Tapping & Jamming			
	Amplifier (OAS)	Amplifier optical path failure (due to fiber cutting)	Gain Competition due to local attack		Conduit	
		Passive component failure with in the amplifier	Gain Competition due to remote attack			
		Pump laser or Pump laser driver electronic problem	Crosstalk due to high power signal			
	Conduit	Conduit damaging or cutting	Conduit cut or optical power reduction			
Node (OXC)	Demux (DS)	Electronic driver failure at Demux or Optical filter failure	Intentional crosstalk using high power signal	Indirect Attack	SRNG	
		Out of range power or unacceptable input optical power				
	Switch (SS)	Electronic driver failure at switch, Misrouting	Intentional crosstalk using high power signal			
		Input power is over/under threshold or out of range	Unauthorized access to information using crosstalk			
	Mux (MS)	Electronic driver failure at Mux or Optical filter failure	Intentional crosstalk propagation from preceding devices			
		Out of range power or unacceptable input optical power				

Fig. 3. Fault/Attack classification for SRG

to SRLG. For example, all fiber links that go through a common conduit under the ground belong to the same SRLG, because the conduit is a shared risk component whose failure, such as a cut, may cause all fibers in the conduit to be broken. This SRLG is introduced in the GMPLS and can be identified by a SRLG identifier, which is typically a 32-bit integer. On the other side, the SRG is applied to the node, and it is referred to SRNG[15][16]. SRNG has to be controlled by a network manager, because it may affect the whole network survivability.

In this paper, in accordance with resource types and coverage of fault/attack effects, we suggest that the SRLG has three levels as follows:

• *SRLG in channel level* : sub-channels that are aggregated in one established channel (lightpath) have the same risk level. This SRLG information can be applied to routing constraint via multiple domains.
• *SRLG in fiber level* : a fiber that connects two nodes is composed of more than one optical channel, and these optical channels have the same risk level with failures in fiber level (such as FIS, OAS).
• *SRLG in conduit level* : a fiber group that connects different nodes can have physical structure bundled by a conduit. Thus fibers in conduit have the same risk level with failure in conduit level.

Figure 4 illustrates a simple example of the proposed SRLG concept. The upper plane is logical topology controlled by GMPLS and the lower plane is

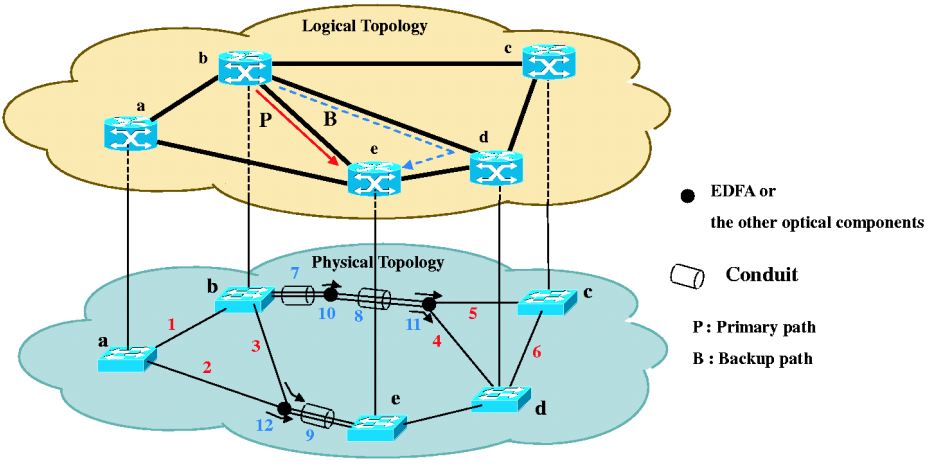

Fig. 4. SRLG example

the physical topology in which optical components (i.e., fiber, conduit, EDFA, etc.) are deployed. To provide physical-diversity of a primary path and a backup path, SRLG should be considered in the physical topology. Let us assume the physical topology consists of 5 nodes, 6 links, 3 conduits and 3 EDFAs. These uniquely have SRLG identifiers in fiber level and in conduit level. When there is a connection request between node b and node e, b-e (P in figure 4) can be a primary path by shortest path first (SPF) algorithm, and there could be two candidates for a backup path, b-a-e and b-d-e. If we only look at the logical topology, both the two backup paths can be allowed. However, If the backup path resolves b-a-e, the primary path and the backup path that go through the same conduit can fail at the same time by one single fault or physical attack in conduit 9, so the determined backup path is b-d-e (B in figure 4). Consequently, in order to make a network survivable against failure generated by fault or physical attack, the SRLG constraint should be imposed on the selection of backup path.

According to the description above, SRLG is the most important criteria concerning the constrained-based path computation of optical path. By applying the SRLG criteria to the constraint-based path computation, one can select a path taking into account diversity of physical resources and logical structure.

4 Recovery Mechanism Under SRLG Constraint

As discussed earlier, in order to achieve fault/attack tolerant recovery mechanism, the backup path has to keep physical-diversity with a primary path, because the failure of optical components as presented in figure 3 results in the potential failure of the link. Thus the recovery mechanism considering SRLG is essentially needed for network survivability in OVPN. On the other hand, a node

failure is actually just a special case of SRNG where links are placed in groups based on whether or not they share a common node. A network manager should control it to avoid the service disruption of the whole network survivability.

In designing recovery mechanism under SRLG constraint, we raised three goals as follows: i) approximately 100% recovery capability and high-speed recovery. ii) almost the same blocking probability compared SPF algorithm with SRLG constraint with SPF algorithm without SRLG constraint. iii) less computational complexity for a backup path.

In order to achieve our goals, the recovery mechanism needs 1:1 path protection, SPF algorithm, SRLG constraint and First-Fit algorithm as wavelength assignment scheme.

The notations used in this paper are as follows:

- $G(N, L)$: The given network, where N is the set of nodes and L is the set of links.
- M: The set of source-destination connection request pairs.
- C_{ab}^{l} : The link cost between link pair (a, b) where (a, b)$\in$(s, d)/M.
- $sr1g_{ab}^{l}$: The set of SRLG IDs in a link pair (a, b) where (a, b)$\in$(s, d)/M.
- $srlg_{sd}^{p/ab}$: The set of SRLG IDs used in a primary path (s, d) where (s, d)$\in$M.
- $R(l)$: The number of currently available wavelengths on a link l where l$\in$L.
- N_c : The total number of connection requests.
- N_f : The total number of failed connections.
- N_s : The total number of successfully established connections.
- N_d : The total number of service disruptions, when a primary path is failed, and there is no backup resource available, then the service on this primary path will be disrupted. If the failed path is a backup path in the running state, the service on this path will also be disrupted.

The procedure, how to find a primary path and a backup path, is described as follows:

STEP 1: Correlate the network resources and compute C_{ab}^{l} for all (a, b) included in G(N,L).

STEP 2: Wait for a request between a (s, d) pair as the current demand where (s, d)$\in$M.

(a) If it is a connection request, go to STEP 3.

(b) If it is a connection release request, go to SETP 7.

STEP 3: Route the request for a primary path between node s and node d selected by SPF algorithm.

SETP 4: SRLG identifiers are correlated between end nodes. Update $srlg_{sd}^{p/ab}$.

SETP 5: Update link cost : C_{ab}^{l}:[$(srlg_{ab}^{l} \in srlg_{sd}^{p/ab})\cup$(R(l)=0)].

STEP 6: Reserve the resource for the request as a backup path between node s and node d selected by SPF algorithm, go to STEP 8.

SETP 7: Release the primary path and the backup path pair (s, d).

STEP 8: Update the network resource states, go to STEP 1.

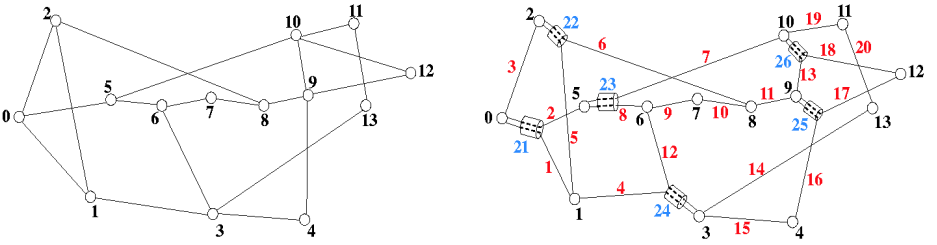

Fig. 5. NSFnet logical topology vs. physical topology considering arbitrary SRLG identifiers

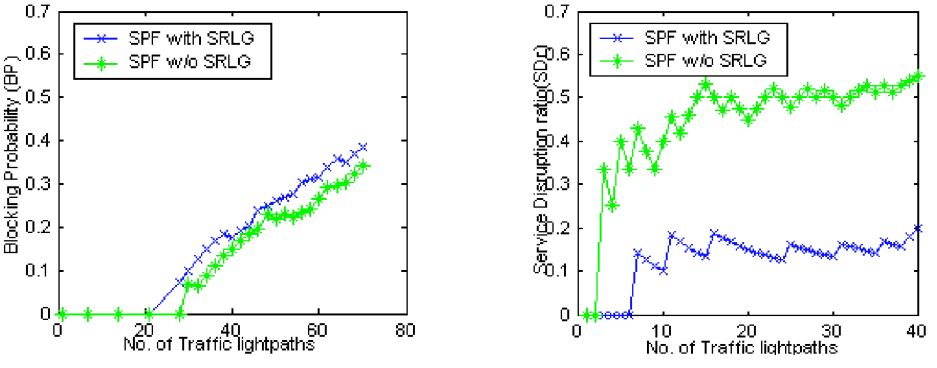

Fig. 6. Blocking probability vs. service disruption ratio as a function of number of traffic lightpaths

The STEP 5 is the most important step because it updates the cost of all links depending on the condition, C_{ab}^{l}:[$(srlg_{ab}^{l} \in srlg_{sd}^{p/ab})$∪(R(l)=0)] which means whether or not the backup path has the same risk in common with the primary path and there are available wavelengths in the link. The recovery mechanism provides very fast and simple to satisfy the goals and is evaluated by blocking probability and service disruption ratio (SD_r) as the performance evaluation metrics, and these are defined as $BP = N_f/N_c$ and $SD_r = N_d/N_s$, respectively. The metrics show performance evaluation results in the viewpoint of survivability in the next section.

5 Numerical Results

In this section, simulation is carried out to evaluate the performance of the recovery mechanism described in section 4. To prove the efficiency, we analyze the results of blocking probability and service disruption ratio with or without SRLG constraint.

The topology used in simulation is NSFnet and we allocate arbitrary conduit level in the physical topology, which is composed of fiber groups. The numbers on a fiber or on a conduit are unique IDs for fiber level SRLG and conduit level SRLG.

The assumptions for the simulation are as follows: i) the physical topology consists of 14 nodes, 20 links and 6 conduits as shown in Figure 5. ii) links are bi-directional, each link has two fibers to different directions and the number of wavelengths per a fiber is 8. iii) all nodes have wavelength converters. iv) the topology is static and is not reconfigured during the simulation. v) connection requests arrive in sequence.

The numerical results of blocking probability and service disruption ratio are plotted as a function of the number of traffic lightpaths in figure 6.

In the case of the blocking probability, SPF with SRLG is slightly higher than SPF w/o SRLG. However, the service disruption ratio guarantees that the recovery mechanism recovers the failed traffic approximately 85% with failed backup paths for a single conduit level failure. Thus, the results of the recovery mechanism confirm better performance in the viewpoint of survivability. However, there is a tradeoff between blocking probability and service disruption ratio as considering SRLG constraint in physical topology.

Acknowledgment. This work was supported by grant No.(R01-2003-000-10526-0) from Korea Science and Engineering Foundation.

References

1. E. Mannie et al.: Generalized Multi-Protocol Label Switching (GMPLS) Architecture, draft-ietf-ccamp-gmpls-archtecture-07.txt, Internet Draft, Work in progress, May 2003.
2. A. Banerjee, et al.: Generalized multiprotocol label switching: an overview of signaling enhancements and recovery techniques, IEEE Commun. Mag., vol.39, no.7, pp.144-151, Jan. 2001.
3. Hamid Ould-Brahim et al.: Service Requirements for Optical Virtual Private Networks, draft- ouldbrahim-ppvpn-ovpn-requirements-01.txt, Internet Draft, Work in progress, July 2003.
4. Mi-Ra Yoon et al.: Optical LSP Establishment and a QoS Maintenance Scheme Based on Differentiated Optical QoS Classes in OVPNs, Photonic Network Commun., vol.7, no.2, pp.161-178, March 2004.
5. Jing Zhang et al.: A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges, IEEE Network, vol.18, no.2, pp.41-48, March/April 2004.
6. Sung-un Kim and David H. Su: Modeling Attack Problems and Protection Schemes in All-Optical Transport Networks, Optical Network Magazine, vol.3, no.4, pp.61-72, July/Aug. 2002.
7. Sung-un Kim and David H. Su: A Framework for Managing Faults and Attacks in All-Optical Transport Networks, DISCEX 2001, June 2001.
8. Muriel Medard et al.: Security Issues in All-Optical Networks, IEEE Networks, vol.11, no.3, pp.42-48, May/Jun 1997.

9. M. Medard, R. Chinn, Saengudomlert: Attack Detection in All-Optical Networks, Technical Digest of Optical Fiber Conference (OFC), 1998.
10. Panagiotis Sebos et al.: Auto-discovery of Shared Risk Link Groups, Optical Fiber Communication Conference, 2001.
11. D. Papadimitriou et al.: Inference of Shared Risk Link Groups, draft-many-inference-srlg-02.txt, Internet Draft, Nov. 2001.
12. Eiji Oki et al.: A disjoint path selection scheme with Shared Risk Link Groups in GMPLS Networks, IEEE Communications letters, vol.6, no. 9, pp.406-408, Sep. 2002.
13. Yun Wang et al.: Dynamic Survivability in WDM Mesh Networks under Dynamic Traffic, Photonic Network Commun., vol.6, no.1, pp.5-24, July 2003.
14. Guido Maier, Achille Pattavina, et al.: Optical Network Survivability: Protection Techniques in the WDM Layer, Photonic Network Communications, vol.4, no.3/4, pp. 251-269, July/Dec. 2002.
15. Sebos, P. et al.: Effectiveness of shared risk link group auto-discovery in optical networks, Optical Fiber Communication Conference and Exhibit, pp.493-495, 2002.
16. Haibo Wen et al.: Dynamic RWA Algorithms under Shared-Risk-Link-Group constraints, IEEE 2002 International Conference on, vol. 1, pp.871-875, July 2002.