論文2003-40TC-10-9

차세대 광 인터넷 백본망에서 망생존성을 위한 Fault/Attack Management 프레임워크

(Fault/Attack Management Framework for Network Survivability in Next Generation Optical Internet Backbone)

金 成 筠 *, 李 俊 源 **

(Sung Un KIM and Joon Won LEE)

요 약

인터넷 트래픽의 폭발적인 증가로 인한 높은 대역폭의 요구와 광 네트워크 기술이 발전되면서 DWDM 네트워크가 국가적 혹은 범세계적인 차세대 광 인터넷(NGOI) 백본망의 대안으로 인식되고 있다. 이러한 DWDM 네트워크 기반의 NGOI에서는 RWA(Routing and Wavelength Assignment) 문제와 생존성이 중요한 이슈가 되고 있다. 특히 높은 데이터 전송율을 가지는 DWDM 네트워크에서 일어나는 짧은 서비스 파괴는 막대한 트래픽 손실을 야기하므로, AOTN에서의 fault/attack 검출, 지역화, 그리고 회복 스킴은 가장 중요한 이슈 중 하나가 된다. 본 논문에서는 다양한 광 백본망 소자들의 fautl/attack 취약성 분석을 통한 fault/attack 관리 모델을 제안하고, IP/GMPLS over DWDM 내의 제어프로토콜인 Extended-LMP (Link Management Protocol)와 RSVP-TE+(Resource ReSerVation Protocol-Traffic Engineering)를 이용하여 fault/attack 회복 절차를 제시한다.

Abstract

As optical network technology advances and high bandwidth Internet is demanded for the exponential growth of internet traffic volumes, the Dense-Wavelength Division Multiplexing (DWDM) networks have been widely accepted as a promising approach to the Next Generation Optical Internet (NGOI) backbone networks for nation wide or global coverage. Important issues in the NGOI based on DWDM networks are the Routing and Wavelength Assignment(RWA) problem and survivability. Especially, fault/attack detection, localization and recovery schemes in All Optical Transport Network(AOTN) is one of the most important issues because a short service disruption in DWDM networks carrying extremely high data rates causes loss of vast traffic volumes. In this paper, we suggest a fault/attack management model for NGOI through analyzing fault/attack vulnerability of various optical backbone network devices and propose fault/attack recovery procedure considering Extended-LMP(Link Management Protocol) and RSVP-TE+(Resource ReserVation Protocol-Traffic Engineering) as control protocols in IP/GMPLS over DWDM.

Keywords : Next Generation Optical Internet Backbone, Network Survivability, DWDM, Fault/Attack Management, Protection/Restoration, LMP, GMPLS, AOTN

* 正會員, 釜慶大學校 電子컴퓨터情報通信工學部
(Div. of Electronic, Computer and Telecommunication Engineering, Pukyung National University)
** 正會員, 安東大學校 電子情報産業學部
(School of Electronics & Information Engineering, Andong National University)

※ 본 연구는 한국과학재단 목적기초연구(R01-2003-000-10526-0) 지원으로 수행되었음.
接受日字:2003年9月7日, 수정완료일:2003年10月10日

Ⅰ. 서 론

차세대 광 인터넷에 대한 연구는 광 전송 기술 분야와 멀티미디어 서비스의 QoS(Quality of Service) 보장 및 트래픽 제어를 위한 제어프로토콜 분야에서 활발한 연구가 이루어지고 있다. 특히 차세대 광 인터넷의 백본망은 TDM(Time Division Multiplexing)에 기반한 SONET/SDH(Synchronous Optical NETwork/Synchronous Digital Hierarchy)에서 WDM 기반인 AOTN(All-Optical Transport Network)으로 급격한 발전을 이루고 있으며, 패킷 스위칭 외에 time-slot, 파장(wavelength) 혹은 파장군(waveband), 물리적 포트 혹은 파이버 스위칭 등 다양한 인터페이스들을 포괄하는 GMPLS(Generalized Multi-Protocol Label Switching) 제어프로토콜 기술이 연구되면서, IP/GMPLS over DWDM 프레임워크로 표준화되고 있다[1]. 그러나 AOTN에서 사용되는 광소자의 일시적인 장애는 전송용량에 비례한 많은 데이터 손실의 원인이 될 수 있고, 더욱이 핵심 전송망으로 비권한자의 침입이 가능할 경우에는 망 생존성(Network survivability)에 심각한 영향을 미칠 수 있어 신뢰성 있는 서비스 제공에 결정적인 결함을 초래하게 된다. 결과적으로 AOTN이 차세대 광 인터넷 백본망으로서 원활한 멀티미디어 서비스의 전개를 위해서는 망 생존성 보장 기술의 제공이 중요한 이슈가 된다[2].

현재 망 생존성 보장을 위한 연구 분야로는 광 성능 모니터링(Optical Performance Monitoring : OPM) 기술, fault/attack의 지역화(localization) 알고리즘, 망 회복과 관련된 보호(protection) 및 복구(restoration) 스킴의 적용 기술, fault/attack 관리를 위한 제어프로토콜 연구 등 다양한 분야에서 이루어지고 있으나, 이들 대부분이 O-E-O 변환이 있는 electro-optic 망에 기반한 연구였다. 그러나 AOTN에서 발생되는 fault/attack은 electro-optic 망과는 달리 광소자의 특성에 따라 망에 미치는 영향력이 다르며, 투명(transparency)한 데이터 전달 특성으로 인해 새로운 형태의 관리 기술이 요구되고 있다. 특히 MIT(Massachusetts Institute of Technology) 및 미국방성 DARPA(Defense advanced Research Projects) 과제를 통해 physical attack 가능성과 그 심각성이 보고되었으나[3-5], 이에 대한 적극적인 해결방안은 아직 제시되지 못하고 있다. 따라서 본 논문에서는 다양한 광소자의 fault/attack 취약성의 분석 및 검출 기술과 fault/attack 관리 모델을 제안하고, 차세대 광 인터넷 백본망 프레임워크인 IP/GMPLS over DWDM의 LMP+&RSVP-TE+를 이용한 fault/attack recovery 절차를 제시한다. 이를 위해 Ⅱ장에서는 차세대 광 인터넷 백본망의 망 생존성 보장을 위해 광소자별 fault/attack 가능성 분석과 검출 및 회복 스킴을 정의하고, Ⅲ장에서는 AOTN 구조와 fault/attack 관리를 위한 시스템 모델을 제시한다. Ⅳ장에서는 제시된 fault/attack 관리 시스템과 GMPLS 제어프로토콜과의 접목을 통해 망 생존성 회복 절차인 검출 및 지역화, 통지(notification), 그리고 보호/복구 절차를 제시한다. 마지막으로 Ⅴ장에서는 본 연구의 결론과 향후 연구 추진 사항에 대해 서술한다.

Ⅱ. AOTN의 망 생존성

AOTN에서의 망 생존성 보장은 <그림 1>과 같이 fault survivability와 attack survivability로 분류된다. 전자의 fault survivability는 광소자들의 갑작스런 결함에 대한 관리와 전송손실 요인으로 인한 광신호의 품질 저하(Signal Degradation : SD)에 대한 관리로 나뉘며, 후자의 attack survivability는 공격자의 목적에 따라 physical attack, logical attack의 관리로 분류된다. 특히 AOTN에서의 physical attack은 비권한자가 물리적 접근을 통해 서비스 파괴, 서비스의 품질 저하를 목적으로 전송 매체로 사용되는 광 파이버나 기타 다양한 광소자들의 동작 특성을 교묘하게 이용하는 새로운 형태의 공격 유형이다. 게다가 EDFA(Erbium Doped Fiber Amplifier)나 PXC(Photonic Crossconnect) 등 AOTN의 광소자들이 non-regeneration 시스템으로 구성되면서,

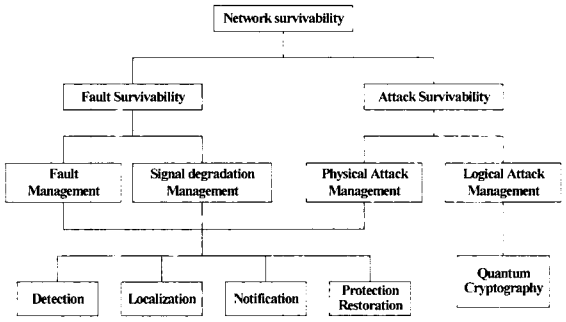


그림 1. AOTN의 망 생존성 분석
Fig. 1. Analysis of the network survivability of AOTN.

기존의 오버헤드 비트(overhead bit)를 이용한 전송 관리 정보(transport supervisory information)의 사용이 더 이상 유효하지 않아 fault/attack 관리에 많은 문제점을 드러내고 있다. Physical attack과는 다르게 비권한자가 정보의 획득 및 획득된 정보를 조작할 목적으로 망에 접근하는 것이 logical attack이다. 물리적 접근 방법인 탭핑(tapping)이나 재밍(jamming)을 통해 정보를 획득/조작하는 logical attack의 가장 큰 문제점은, 광 도메인에서의 검출이 곤란하다는 것과 짧은 순간의 접근으로도 많은 양의 정보가 외부로 누출 될 위험이 있다는 것이다. 따라서 비권한자의 정보 획득/조작을 막기 위해서는 물리적 레벨보다는 상위 레벨에서의 암호화 과정과 안전한 키 분배 방식이 제공되어야 할 것이다. 특히 양자현상을 이용한 양자 키 분배방식(quantum cryptography)의 도입은 logical attack에 대한 뛰어난 보안성을 제공할 수 있을 것으로 예상한다[6].

위에서 서술된 것처럼 AOTN은 광소자들이 가지는 여러 형태의 fault/attack 가능성으로 인해 망 생존성에 심각한 위해 요소들을 가지고 있다. 따라서 본 장에서는 AOTN 구성소자들의 fault/attack 가능성 및 영향에 대한 분석과 이를 검출하기 위한 광 성능 모니터링 기술 및 회복 스킴의 적용을 제시한다.

1. Fault Survivability

<그림 2>는 AOTN을 구성하는 핵심소자와 fault/attack의 관리구간을 나타낸다. 광신호의 전달 매체인 광 파이버와 탭(tap), 광신호의 감쇄를 보상하기 위한 광 증폭기, 그리고 AOTN 노드로 구성되며, AOTN 노드는 파장다중화를 위한 Mux/Demux, 광경로의 스위칭을 위한 PXC, 그리고 엑세스 망과의 접근을 위한 Tx/Rx(혹은 add/drop port)로 구성된다.

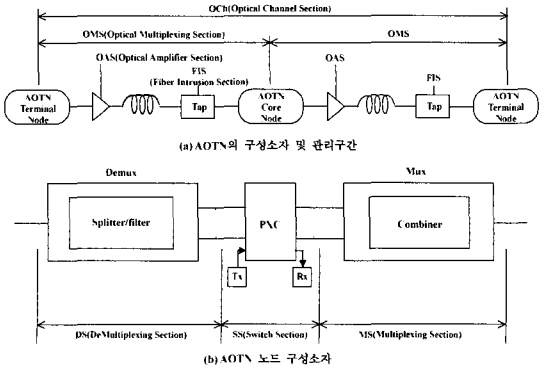


그림 2. AOTN 구성소자 및 fault/attack 관리구간
Fig. 2. AOTN components and management sections for fault/attack.

Fault survivability에서 가장 먼저 고려되는 것은 광소자들의 물리적 고장으로 인한 장애이다. <그림 2>에서 언급된 광소자들은 전원 모듈이나 제어모듈 등 내부적으로 다양한 sub-system으로 구현되며, 이들의 물리적 고장은 광소자들의 오동작이나 동작불능을 유발하게 되며, 그 영향이 미치는 범위에 따라 다음의 세가지 레벨로 분류된다. 첫째, OCh 구간(Optical Channel section)은 AOTN terminal 노드 사이에 설립되는 하나의 광경로에만 영향을 미치며, 광경로에 대응되는 파장을 송·수신하는 레이저(혹은 add port)나 광 수신기(혹은 drop port)의 고장이 원인이 된다. 둘째로는, OMS 구간(Optical Multiplexing Section)으로 노드간에 파이버의 단절이나 광 증폭기 고장이 원인이 되며, DWDM 기술을 사용하기 때문에 그 링크를 거치는 모든 파장에 장애를 유발한다. 셋째, Demux, PXC, Mux로 구성되는 AOTN 노드 구간은 망 핵심 소자로써 해당 노드를 통과하는 모든 광경로에 영향을 주며, 가장 심각한 고장으로 여겨진다.

그리고 이들 구간 내에서 공격과 관련하여 OAS (Optical Amplifier Section)와 FIS(Fiber Intrusion Section), 그리고 AOTN 노드의 DS(Demultiplexing Section), SS(Switching Section), MS(Multiplexing Section), TS (Transmission Section), RS(Reception Section)의 세부구간으로 분석될 수 있으며, 이에 대한 내용은 2.2에서 다루고 있다.

AOTN에서 발생하는 장애의 다른 종류로써 환경적 요인이나 광소자의 자체적 손실요인에 의한 신호의 품질 저하를 고려할 수 있다. 예를 들면, EDFA에서 발생되는 ASE(Amplified Spontaneous Emission) 잡음이나 레이저의 RIN(the Relative Intensity Noise)과 같이 가우시안 과정으로 취급될 수 있는 신호의 랜덤한 파동에 기인한 잡음들, 광 파이버에서의 전송 손실(attenuation)이나 색분산(chromatic dispersion), 그리고 비선형 현상(non-linear effect)으로 인한 펄스 모양의 왜곡, 파장들간의 간섭으로 인한 crosstalk 등 다양한 불안 요소에 의해 신호의 품질은 영향을 받게 된다[7, 8]. 따라서 fault survivability를 위해서는 광소자의 고장에 대한 관리와 함께 SD 관리를 위한 신호 품질 측정 기술이 요구된다. 기존의 전송망인 SONET/SDH에서의 신호 품질 측정은, 전기적인 레벨에서 ES(Error Seconds), SES (Severely Errored Seconds), UAS(UnAvailable

Secocnds)와 같은 성능 파라메터들로 측정되었다. 특히 SONET/SDH는 section, line, path layer에서의 에러를 측정하기 위해 자신의 프레임 구조에 B1, B2, B3와 같은 오버헤드를 첨가하고, 각 세그먼트의 단말에서 전기적인 변환을 통해 오버헤드에 대한 정보를 읽을 수 있었기 때문에 성능 측정이 용이하였다. 그러나 DWDM 기반의 AOTN에서는 중간 노드의 데이터에 대한 접근이 없어 광채널의 상태를 평가할 수 없으며, fault/attack의 빠르고 정확한 검출을 위해서는 광 도메인에서의 성능 모니터링 기술이 요구된다. 이에 T1X1.5에서는 OPM 문제를 해결하기 위해서 ITU-T draft recommendation G.798과 G.874에 포함되었던 일부 광 성능 파라메터(Optical Performance Parameter : OPP)에 대한 연구를 진행하고 있으며[9], <표 1>은 OPM 기능을 수행하기 위해 요구되는 OPP를 요약한 것이다.

표 1. 광 도메인에서의 OPP와 OPM 기술의 종류

Table 1. Technologies for OPP and OPM in optical domain.

종류	전송 손실요인	광 성능 파라메터 (OPP)	광 성능 모니터링 기술 (OPM)
Noise	ASE noise Crosstalk Laser noise Reflections Jitter	Composite optical power level Composite optical power deviation	Optical Power Level monitoring
		Channel optical power Channel optical power deviation OSNR(Optical Signal-to-Noise Ratio) OSNR drift Wavelength identification Wavelength drift	Optical Spectrum Analysis monitoring
Distortion	Chromatic dispersion Filtering effect PMD Nonlinearity	Q-factor Q-factor drift Eye diagram Eye diagram drift	Q-factor monitoring based on eye diagram

본 논문에서는 OPM 기술을 통해 측정된 OPP 값을 기반으로 광소자의 고장과 SD를 검출하기 위해서 다음의 네 가지 OPM 기술을 사용한다.

(a) Optical Power Level(OPL) 모니터링 기술

광파이버로 전송되는 광신호의 전체 전력을 측정하며, DWDM 시스템에서 가장 쉽게 사용되는 모니터링 기술이다. 광신호의 세기(strength)는 DWDM 시스템의 성능에 직접적으로 영향을 주는 중요한 파라메터이고, 링크 상의 LOL(Loss Of Light)를 빠르게 검출할 수 있다. 따라서 광소자의 입출력 포트에서 composite optical power를 측정/비교함으로써, 광소자 고장 검출과 시스템의 안정성을 모니터링 한다.

(b) Optical Spectrum Analysis(OSA) 모니터링 기술

DWDM 시스템은 채널에 해당하는 다수의 파장이 다중화 되어 전송되기 때문에, 각 채널의 상태를 모니터링 하기 위한 파장별 광전력(optical power)의 모니터링이 요구된다. OSA는 각 파장에서의 결합/분기(add/drop) 정보나 특정 파장의 LOL 검출이 가능하고, channel power measurement, OSNR(Optical Signal-to-Noise Ratio) 측정 등 다양하게 응용이 된다. 특히 EDFA의 경우, 평탄한 이득 특성이 제공되는지를 모니터링 하기 위해서는 파장별 분석이 필요하다. 그러나 OSA는 파장별 OSNR, wavelength identification 등의 측정이 가능하지만, 광파이버에 존재하는 분산이나 비선형 특성으로 인한 신호의 왜곡을 측정하기에는 제한이 따른다. 따라서 이를 해결하기 위해 다음의 Q-factor 모니터링 기술을 사용한다.

(c) Q-factor 모니터링 기술

Q-factor는 광 시스템에서 OSNR을 결정하고 BER을 추정할 수 있는 새로운 품질 평가 파라메터로, 광 시스템을 통계적 가우시안 잡음으로 가정했을 때의 SNR을 측정한 값이며, eye diagram의 측정값이 기반이 된다. 특히 BER을 추정할 수 있으므로, 왜곡으로 인한 SD를 검출하기에 용이하다.

(d) Indirect 모니터링 기술

직접적으로 광신호의 형태나 파워를 감지하지 않고, 망 요소들의 LOL이나 온도 변화, 주파수 편향 정도, sub-system의 동작상태와 같은 특징적인 징후를 감시하는 방식으로, 광 시스템이 잘 동작하고 있는지를 판별할 수 있다. 특히, 송신기나 EDFA의 펌핑(pumping)을 위해 사용되는 레이저의 온도변화는 송출되는 광신호의 품질과 직결된다.

<표 2>는 각 구간별 광소자들에 대한 세부적인 fault 가능성 분석과 검출을 위한 모니터링 방법, 그리고 회복 스킴을 요약하였다.

<표 2>에서 분석된 바와 같이 광소자의 고장은 각 소자의 입력/출력 포트에서의 광전력을 비교함으로써 검출할 수 있다. 만약 입력이 α(단, α는 시스템이 허용하는 임계치 이상의 값), 출력이 0일 경우, 광소자의 고장으로 간주되며, 입력이 0이고 출력도 0일 경우는, 업

스트림 광소자의 고장 전파로 인한 LOL로 분석된다. 이와 달리 SD의 검출은 제시된 OPM 기술로 측정된 OPP 값과 시스템이 요구하는 최저 혹은 최고 임계치 값을 주기적으로 비교함으로써 SD 발생을 검출할 수 있다[10].

표 2. AOTN에서의 Fault 가능성 분석 및 검출, 회복 스킴

Table 2. Analysis, detection, and recovery schemes of the fault possibility in AOT.

	구간	광소자	fault 가능성 분석	광 모니터링 기술	회복 스킴
Fault	OMS	Fiber	물리적 힘에 의한 파이버의 절단	-	Link disjointed GMPLS recovery
		EDFA	EDFA 내의 수동소자 fault	OPL (input:α, output:0)	
			펌프 레이져 또는 펌프 레이져의 드라이버 문제		
	AOTN 노드	Demux	Demux, 광필터의 물리적 드라이버 fault 혹은 misrouting	OSA (input:α, output:0)	Node disjointed GMPLS recovery
		PXC	물리적인 드라이버 문제 혹은 misrouting		
		Mux	Optical combiner의 물리적인 드라이버 fault		
	OCh	Transmitter (or Add port)	레이저 또는 레이저 드라이버의 전기적 문제, 레이저의 온도 상승	OPL, Indirect (temperature)	GMPLS recovery or Resource provisioning
		Receiver (or Drop port)	광수신기의 내부적 결함	Indirect	
SD	전송 손실 요인으로 인한 광신호의 감쇄			OPL, OSA Q-factor	Link or Node disjointed GMPLS recovery

2. Attack Survivability

미 국방성의 DARPA와 MIT에서는, AOTN에서 비권한자의 탭핑/재밍을 통한 공격 취약성과 이에 따른 심각성을 제시하였다. 이 보고서에 따르면 광 시스템의 물리적 접근을 통한 광 파이버에서의 비선형 현상 유발이나 WDM 채널간의 crosstalk 등과 같은 전송 손실요인들로 인해 다른 광신호 품질에 심각한 영향을 주거나 정보를 획득할 수 있게 되는데, 특히 광 증폭기로 사용되는 EDFA와 광필터로 구현되는 AOTN 노드는 SD를 유발하거나, 비권한자에게 정보를 유출할 수 있는, 공격에 매우 취약한 소자로 소개되고 있다[3, 5]. 이처럼 광소자의 시스템 패널티(system penalty)를 이용한 AOTN의 공격은 공격자가 광소자의 동작특성을 교묘히 이용함으로써 신호에 대한 SD를 유발하거나 탭핑을 통한 정보획득의 한 수단으로 사용될 수 있음을 보여주며, 공격 구간에 따라서 direct attack, indirect attack, 그리고 pseudo attack으로 분류된다[2].

AOTN에서 사용되는 각 소자들은 침입자의 물리적 접근을 통해 공격 가능한 포트처럼 직접적으로 활용되는데, 특히 광 파이버나 탭은 공격자의 접근이 용이하기 때문에 SD유발에 매우 취약하며, 공격자의 정보획득을 위한 최초의 침입 포트로도 활용된다. 이처럼 광소자에 직접 접근하여 일련의 공격활동이 이루어지는 것을 direct attack이라 한다. 이와는 다르게, AOTN 노드는 물리적으로 공격자가 쉽게 접근하기 어렵기 때문에, SD나 정보획득을 목적으로 direct attack과 같은 공격활동을 하기가 곤란하다. 그러나 Demux, PXC, Mux에서 사용되는 광필터의 crosstalk 특성을 간접적으로 이용하는 공격이 가능하며, 이를 통해 SD나 정보획득의 공격이 이루어질 수 있는데, 이를 indirect attack이라 한다. 그리고 동적 재구성이 가능한 AOTN에서의 광신호 품질은, 물리적인 망 토폴로지에 따라 달라질 수 있다. 특히 OADM(Optical Add/Drop Multiplexer)이나 PXC의 결

표 3. AOTN에서의 Attack 가능성 분석 및 검출, 회복 스킴

Table 3. Analysis, detection, and recovery schemes of the attack possibility in AOTN.

종류	구간	attack 가능성 분석	광 모니터링 기술	회복 스킴
Direct Attack (OMS)	FIS	Fiber cut or optical power reduction	-	GMPLS recovery
		*Tapping only	difficult	Semantic level
		*Tapping & Jamming	difficult	Semantic level
		Jamming only (high power injection)	Q-factor	GMPLS recovery
	OAS	Gain competition due to local attack	OSA (per channel input/output power)	Power equalization GMPLS recovery
		Gain competition due to remote attack		
		Crosstalk due to high power signal		
Indirect Attack (AOTN 노드)	DS	Intentional crosstalk	OSA	Power equalization
	SS	Intentional crosstalk	OSA	Power equalization
		*Unauthorized access to information using crosstalk	difficult	Semantic level
	MS	Intentional crosstalk propagation	OSA	Power equalization
Pseudo Attack (OCh)	TS	Optical power deviation due to input optical power	OPL	-
	RS	Optical power deviation due to output optical power	OPL	-

합/분기 포트에서 일부 파장이 결합 또는 분기될 때, 다른 파장들의 신호 품질에 미소한 영향을 미치게 되고, 이 같은 예외적 현상은 공격자에 의한 침입은 아니지만, 침입 감시 알고리즘에 의해 공격이 이루어진 것처럼 인식될 수 있다. 이러한 현상을 pseudo attack이라 부르며, 망 토폴로지를 적합하게 구현하거나 사용 파장들에 대한 정보를 실시간으로 주고받음으로써 전체 또는 부분적으로 극복이 가능한 요소이다.

AOTN에서 가능한 공격은 <표 3>에서 분석된 바와 같이, 높은 세기의 광신호 삽입으로 한정된 이득을 여러 파장이 공유함으로써 발생되는 EDFA의 gain competition[13]이나 AOTN 노드에서의 crosstalk 특성을 이용하여 SD를 유발하는 physical attack, 그리고 물리적인 파이버 탭핑을 통한 광신호 획득이나 WDM 채널간의 crosstalk 성분을 획득하는 logical attack(<표 3>에서 *로 표시)의 2가지 유형으로 분석된다. 이것은 공격자가 공격한 포트의 위치를 정확히 찾아내어 사용자 트래픽과 분리시킴으로써 해결될 수 있어서 physical attack은 2.2에서 제시된 SD 관리와 동일한 검출/회복 스킴이 적용될 수 있다. 그러나 이와 달리 logical attack은 검출이 힘들뿐만 아니라 semantic 레벨에서의 보안이 요구되기 때문에 보안 수준이 높은 암호화 알고리즘과 quantum cryptography 기술을 활용한 양자 키 분배 방식의 병행적 사용이 필요하다.

Ⅲ. Fault/Attack Management System 모델

제안되는 차세대 광 인터넷 구조는 <그림 3>과 같이 두 개의 기능적 도메인으로 고려된다[11]. 외부 도메인은 패킷 헤더 정보를 기반으로 하는 기존의 상업적인 전기 도메인(LAN, MAN, ATM등)들이고, 차세대 광 인터넷 백본망인 내부 도메인은 광소자 기술로 구현된 광 제어 도메인이다. Ingress 노드로 유입되는 다양한 IP 트래픽들은 GMPLS의 optical-LSP(Label Switched Path)를 따라 Egress 노드로 전송된다. 이때 코어(core) 노드는 광 스위칭에 기반 하여 O-E-O 변환 없는 데이터 포워딩(forwarding)만을 담당하며, Egress 노드는 전송된 트래픽들을 엑세스망에 따라 다시 분리하여 최종 목적지로 전달된다.

이 같은 차세대 광 인터넷 백본망의 fault/attack 관리 모델은 다음의 세 부분으로 나뉜다. 첫째, Fault/Attack

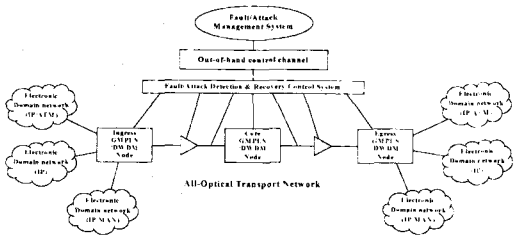


그림 3. 차세대 광 인터넷 백본망의 fault/attack 관리 모델

Fig. 3. Fault/attack management model of Next Generation Optical Internet Backbon.

D&RCS(Detection&Recovery Control System)은 광 계층과 매우 가깝게 위치하며, 임의의 fault/attack으로부터 적절한 회복 스킴을 제공하기 위해서, 상위 단계에 fault/attack 발생 사실을 통지하는 기능을 담당한다. 둘째, out-of-band 제어 채널은 Fault/Attack Management System과 Fault/Attack D&RCS 간의 양 방향 인터페이스를 제공한다. 마지막으로, Fault/Attack Management System은 fault/attack 회복을 위한 일련의 제어를 담당한다. 본 장에서는 fault/attack 관리 모델에 요구되는 Fault/Attack Management System 및 제어프로토콜과 이들의 기능적 모델을 제시한다[12].

1. Fault/Attack Detection & Recovery Control System(D&RCS)

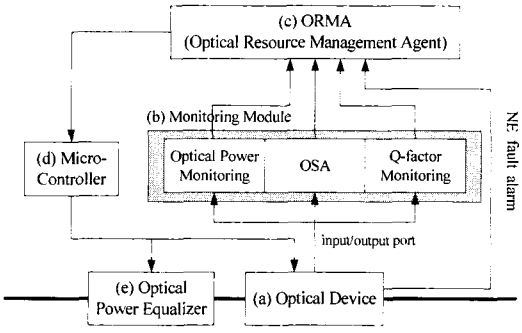


그림 4. Fault/Attack D&RCS의 구조

Fig. 4. Structure of fault/attack D&RCS.

망 생존성 보장에 있어서 중요한 이슈 중 하나는 fault/attack 검출 기술이며, 코어 노드에서의 데이터 접근이 불가능한 AOTN에서는 광 도메인에서의 빠르고 정확한 fault/attack 검출이라는 주요한 문제점을 극복해야하며, 이를 위해서는 앞서 살펴본 OPM 기술을 필요

로 한다. 본 논문에서는 <그림 4>와 같이 OPM 기술을 적용할 수 있는 Fault/Attack D&RCS를 제안하며, 그 구성요소는 다음과 같다.

(a) Optical Devices(광소자) :
<그림 2>에서 나타난 Mux, Demux, PXC, EDFA, Tx, Rx 등의 소자들이며, 동일한 기능의 광 소자들은 하나의 ORMA(Optical Resource Management Agent)에 의해 제어된다

(b) Monitoring Module(모니터링 모듈) :
광소자 및 광신호의 상태를 측정하기 위한 모니터링 장비로써, 광소자의 입출력 포트를 탭핑하여 Optical power level, OSA, Q-factor 모니터링 등의 방식으로 OPP 정보를 측정, 이를 ORMA(Optical Resource Management Agent)에게 전달한다. 그러나 OPM이 적용될 수 없는 일부 소자(광 수신기)에서는 indirect 모니터링 기술이 적용되어 sub-system의 장애를 NE fault alarm을 통해 보고할 수 있다.

(c) ORMA(Optical Resource Management Agent) :
모니터링 모듈에서 제공하는 OPP 정보를 기반으로 자신이 관리하는 광자원의 상태정보를 유지하며, Micro-Controller를 통한 직접적인 광소자의 제어를 담당한다. 최초 시그널링 절차를 통해 전달된 각 파장 혹은 광링크에서 요구하는 OPP의 임계치 정보를 유지하고, 이 값을 모니터링 모듈에서 주기적으로 전달되는 OPP와 비교함으로써 광소자의 고장 및 SD 발생 여부를 판단한다. 그리고 out-of-band 제어 채널을 통해 SF(Signal Failure), SD의 발생을 Fault/Attack Management System에게 알린다.

(d) Micro-Controller
ORMA의 요구에 따른 광소자의 실질적인 물리적 제어를 담당한다. 특히 fault/attack 관리와 관계하여 EDFA의 펌프 레이저 제어를 통한 이득 조절, Optical Power Equalizer의 제어 등 다변적인 망 상황에 능동적으로 대처할 수 있다.

(e) Optical Power Equalizer
광소자로 입력되는 각 채널의 입력 파워가 균일하도록 제어하는 기능을 담당하며, 특히 높은 세기의 방해파 삽입을 통해 이루어지는 physical attack에 대해서 시스템적으로 상당한 보안성을 제공할 수 있다. 예를 들면, EDFA의 gain competition이나 핵심 소자인 AOTN 노드에서의 crosstalk과 같은 physical attack의 취약성에 대해 시스템 레벨에서의 능동적인 관리를 가능하게 한다.

2. Out-of-band 제어 채널

DWDM 기반의 AOTN에서는 이웃한 노드와 여러 개의 파이버로 연결되고, 각 파이버는 수 백개 이상의 파장을 전달할 수 있다. 이를 효율적으로 관리하기 위한 제어 채널로써, IETF(the Internet Engineering Task Force)에서는 GMPLS의 링크 관리 프로토콜인 LMP (Link Management Protocol)를 정의하고 있다[15]. LMP는 이웃한 노드 간에 out-of-band 제어 채널을 통해 데이터 링크와 관련된 제어정보를 주고받을 수 있으나, 두 이웃 노드를 연결하는 DWDM 광 링크의 구조 및 상태 정보를 알기 위해서는 Fault/Attack D&RCS와의 정보 교환이 요구된다. 따라서 본 논문에서는 fault/attack 관리를 위한 out-of-band 제어 채널로써 LMP, 그리고 LMP를 전송장비 OLS(Optical Line System) 사이로 확장한 LMP-WDM[16]이 상호 동작되는 모델(이하 LMP+라 명칭)을 제안한다.

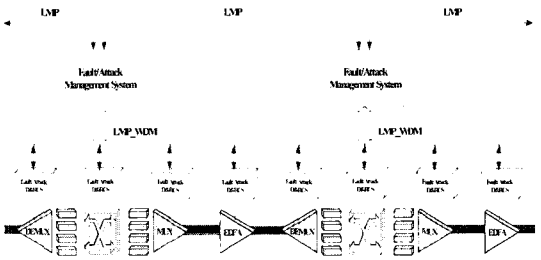


그림 5. LMP+ 모델
Fig. 5. LMP+ mode.

제안된 LMP+는 <그림 5>와 같이 노드-노드 간의 LMP와 노드-Fault/Attack D&RCS 간의 LMP-WDM이 상호 동작하는 모델로 광 도메인과 제어 평면을 연결하는 기능이 LMP-WDM을 통해 구현되며, LMP-WDM을 통해 수집된 광링크의 정보를 기반으로 LMP는 GMPLS 시그널링과 라우팅에 사용되는 TE(Traffic Engineering) 링크 형성 및 fault/attack 관리를 위한 이웃한 노드간의 제어 정보의 전달을 수행한다. 즉, Fault/Attack D&RCS 내의 ORMA에서 유지되는 광자원의 상태정보가 LMP-WDM을 통해 Fault/Attack Management System에 전달되고, 이것은 LMP를 통해 fault/attack 관리 기능을 수행할 수 있다.

3. Fault/Attack Management System

AOTN 노드는 광 스위치로 유입되는 트래픽을 스위

칭 테이블에 따라 파장(혹은 파장군) 및 공간 스위칭을 담당하는 데이터 평면(data plane)과 시그널링/라우팅 및 시스템 관리를 담당하는 제어 평면(control plane)으로 나뉜다. 분산형 Fault/Attack Management System의 기능적 블록을 <그림 6>과 같이 나타낼 수 있는데[13], 제어 평면에서는 라우팅을 위한 IP Routing Agent, 시그널링을 위한 GMPLS Signaling Agent, 링크 관리를 위한 LMA(Link Management Agent), DWDM 링크 자원의 정보 유지를 위한 LRMA(Link Resource Management Agent), 그리고 fault/attack의 전반적인 제어를 위한 Fault/Attack MA(Management Agent)로 세분화되며, 각 기능 블럭들은 fault/attack 관리를 위해 상호 유기적으로 동작된다.

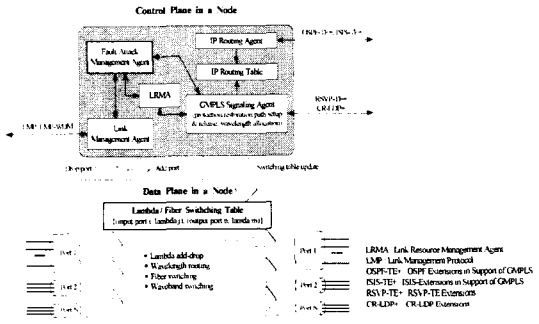


그림 6. AOTN 노드의 기능 블록도
Fig. 6. Functional blocs of AOTN node.

각 기능 블럭들의 동작을 살펴보면, 먼저 제어 평면 내의 Fault/Attack MA(Management Agent)는 LMP-WDM 제어 채널로 전달된 광소자 및 DWDM 링크의 상태 정보를 광 스위치의 분기 포트(drop port)를 통해 수신하고, fault/attack 종류에 따른 적절한 회복 스킴 제공을 위한 시스템의 전반적인 제어 절차를 제공한다. 만일 Fault/Attack D&RCS로부터 LMP-WDM 제어채널을 통해 SF/SD 알람을 수신하게 되면, 최초 Fault/Attack MA는 LMA에서 제공되는 LMP와 LMP-WDM을 통해 fault/attack 지역화 절차를 수행한다. 이웃 노드 및 Fault/Attack D&RCS와의 정보 교환을 통해 지역화 절차가 종결되면, Fault/Attack MA는 LMA에서 제공되는 상태정보를 바탕으로 LRMA에 저장된 DWDM 광링크 자원에 대한 정보를 업데이트 한다. 이후 GMPLS Signaling Agent는 시그널링 프로토콜인 RSVP-TE+(혹은 CR-LDP+)를 이용하여 fault/attack이 발생됐음을 회복에 책임이 있는 노드들에게 알려 주면, 이 노드들의 Fault/Attack MA는 광경로에 따라 제공되어야 할 회복 스킴을 적용하게 된다. 이처럼 fault/attack 검출에서부터 회복까지의 데이터 처리 과정은 다양한 Fault/Attack Management System의 상호 협력적인 과정으로 이루어지고, 이를 위한 제어프로토콜의 절차는 4장에서 다루고 있다.

Ⅳ. Fault/Attack Recovery 절차

GMPLS로 제어되는 광 전송망에서, 데이터 평면에서 발생한 장애를 회복하기 위한 요구 절차로 P. Czezowski와 T. Soumiya는 <그림 7>과 같이 장애 검출단계(T1), 지역화 및 분리단계(T2), 장애 통지 단계(T3), 회복 스킴 적용단계(T4), 그리고 정상 상태 진입(T5)의 다섯 단계로 제시하였다[17]. 본 논문에서는 이 같은 recovery 절차를 다음의 세 가지로 요약된다. 첫째로, 시스템 레벨에서 처리되는 장애 검출단계, 둘째로는 GMPLS 링크 관리 프로토콜인 LMP+를 통한 fault/attack 지역화 및 분리단계, 마지막으로는 GMPLS 시그널링 프로토콜로 사용되는 RSVP-TE+에 의해 제공되는 fault/attack 통지, ingress노드와 egress노드에 기반한 end-to-end GMPLS 보호/복구 스킴 적용 및 정상 상태 진입이다.

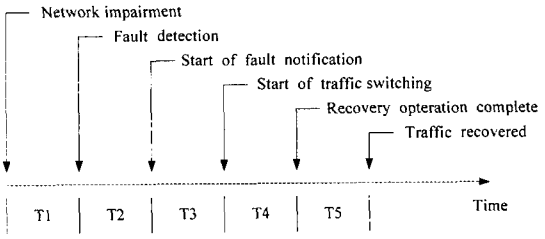
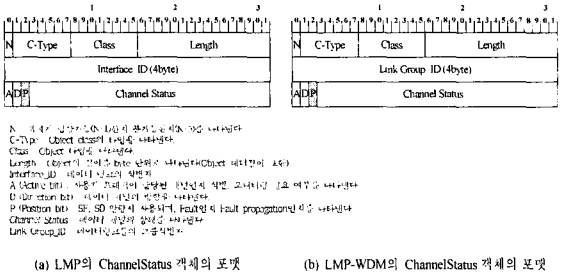


그림 7. Recovery의 시간적 절차 모델
Fig. 7. Timing procedure model for recovery.

본 논문의 3.1에서 제시된 Fault/Attack D&RCS의 도입을 통해 다양한 fault/attack을 광 도메인에서 검출할 수 있는 방법이 이미 제시되었다. 따라서 본 장에서는 fault/attack 지역화 및 분리를 위한 LMP+와 장애 통지 및 회복 스킴의 적용을 위한 RSVP-TE+ 절차를 제시하도록 한다.

1. Fault/Attack Localization

LMP는 ChannelStatus 메시지 교환에 기반한 장애 관리 절차를 바탕으로 망에서 발생한 fault/attack의 지역화를 제공한다[14]. 이때 사용되는 ChannelStatus 메시지는 하나 혹은 그 이상의 데이터 채널들의 상태를 이웃 노드에 통지하기 위해 사용되며, 포맷은 <그림 8(a)>와 같이, 장애가 발생한 데이터 링크의 식별자(Interface_ID), 데이터 링크의 상태(Signal Failure, Signal Degradation, 그리고 Signal OK) 및 데이터 채널의 방향을 나타낸다. 그리고 LMP-WDM에서는 <그림 8(b)>처럼 Link Group_ID를 새롭게 정의하며, 데이터 링크를 위한 개별적인 ChannelStatus 객체 대신 데이터 링크들의 그룹을 사용함으로써 fault/attack 발생에 의한 제어 트래픽의 양을 줄이기 위해 사용된다[15, 16].



(a) LMP의 ChannelStatus 객체의 포맷 (b) LMP-WDM의 ChannelStatus 객체의 포맷

그림 8. ChannelStatus 객체의 포맷
Fig. 8. Format of the ChannelStatus objec.

ChannelStatus 메시지의 교환은 물리적으로 2가지 의미를 가진다. ChannelStatus 메시지를 전달하는 매체 혹은 데이터 링크에서 fault/attack이 발생했음을 보고하는 경우와 이전 소자(혹은 광 파이버)의 fault/attack으로 인한 LOL 검출과 같이 업스트림에서 발생한 fault/attack의 전파로 인해 다운스트림 측에서도 fault/attack 발생을 보고하는 경우이다. 이 두 경우의 차이점은 광소자의 입/출력 성능 모니터링 기술(2.1에서 소개)을 통해 구분가능하며, DWDM 광 링크 구간에서의 보다 정확한 지역화를 위해서는, 장애와 장애 전파의 정확한 의미를 제어 평면에 전달해야할 필요가 있다. 따라서, 본 논문에서는 <그림 8>의 Channel Status 필드 중 1비트를 P 비트(Position bit)로 활용할 것을 제안한다. 제안된 P비트는 LMP-WDM과 LMP에 모두 사용되는데, P비트가 0이면, 관리되는 구간에서의 fault/attack이 발생했음을 나타내고, P비트가 1이면, 장애 전파를 의미한다. 만약 LMP-WDM Link_Group ChannelStatus 객체의 P비트가 0이면, 모니터링 되는 광소자에서 fault/attack이 일어났음을 의미하고, P비트가 1이면, 업스트림 소자의 장애로 인한 전파임을 나타낸다. 마찬가지로 LMP ChannelStatus 객체에서의 P비트가 0이면, 그 노드가 관리하는 OLS에서의 fault/attack임을, P비트가 1이면 업스트림 노드의 전파임을 나타낸다.

<그림 9>는 제안된 LMP+ 모델에서 ChannelStatus 메시지와 Channel Status 필드의 P비트를 사용한 fault/attack 지역화 알고리즘이며, <그림 10(a)>는 Fault/Attack D&RCS를 통해 모니터링 가능한 소자(EDFA)에서 fault/attack이 발생했을 경우, (b)는 OPM이 적용되지 않은 광 파이버에서 fault/attack이 발생했을 때의 지역화 절차 예이다. LMP+ 모델에서 각 노드의 LMA를 데이터의 전달방향에 따라 U-LMA(Upstream-LMA), D-LMP(Downstream LMA)라 하고, LMA와 Fault/Attack D&RCS 간의 LMP-WDM 제어 채널을 업스트림에서부터 각각 LMP-WDM session1, session2, session3로 가정한다.

Phase 1: LMP-WDM localization
1) fault/attack을 검출한 Fault/Attack D&RCS가 ChannelStatus 메시지 전달
 · 광소자 fault/attack일 경우 P 비트 0
 · fault/attack으로 인한 propagation일 경우 P 비트 1
2) 각 LMA는 ChannelStatusAck 메시지로 응답
3) LMP-WDM correlation
 · P 비트를 통해 LMP-WDM session 내 결함 광소자의 위치 확인
4) ChannelStatus 메세지를 통해 각 Fault/Attack D&RCS에게 상태 정보를 전달
5) LMP-WDM localization 절차 완료

Phase 2: LMP localization
1) fault/attack을 검출한 D-LMA가 U-LMA로 ChannelStatus 메시지 전달
 · 자신의 LMP-WDM session 내에서 fault/attack이 발생하면 P 비트 0
 · 그렇지 않으면(failure propagation) P 비트 1
2) ChannelStatus 메시지를 수신한 U-LMA는 ChannelStatusAck 메시지로 응답
3) LMP correlation
 · LMP-WDM session의 상태 정보 및 D-LMA가 전달한 상태 정보 확인
 · (a)의 경우: U-LMA 내 EDFA failure
 · (b)의 경우: U-LMA와 D-LMA 사이 구간(광 파이버)에서 failure
4) ChannelStatus 메시지를 통해 D-LMA에게 상태 정보를 전달
5) LMP localization 절차 완료

그림 9. LMP+ localization 알고리즘
Fig. 9. Localization algorithm for LMP+.

<그림 10>의 예에서 살펴본 바와 같이 제안된 LMP+ 모델에서의 지역화 알고리즘은 LMP-WDM 지역화와

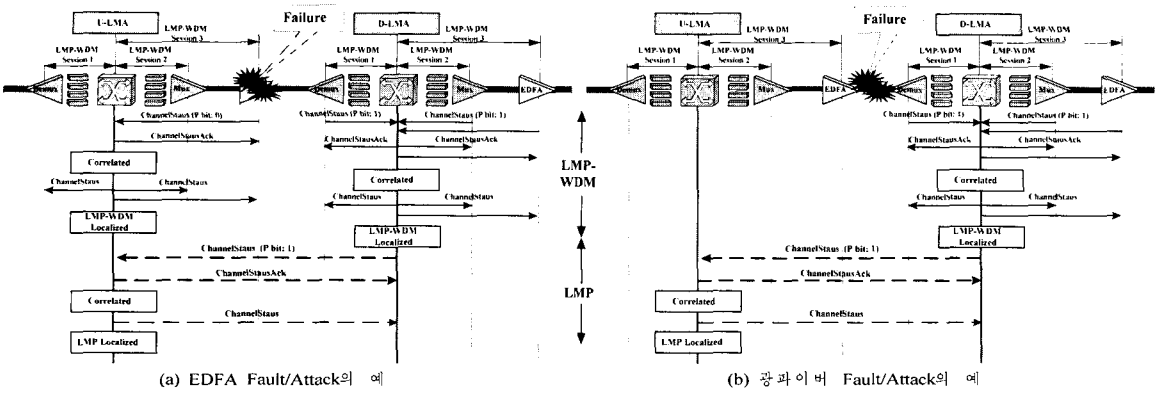


그림 10. LMP+를 사용한 fault/attack 지역화 및 장애 고립 절차
Fig. 10. Fault/attack localization procedure using LMP.

LMP 지역화의 두 가지 과정으로 동작되며, 이를 통해 고장난 광소자의 위치나 공격 포인트를 정확하게 검출 및 지역화 할 수 있는 이점을 제공한다.

2. Fault/Attack Notification & Protection/Restoration

제안된 LMP+ 모델을 통해 fault/attack이 지역화 되면, 회복 스킴 수행에 책임이 있는 노드(ingress 또는 egress)로 RSVP-TE+의 Notify 메시지를 통해 fault/attack 발생을 알리며, 이 메시지를 통해 fault/attack 상태 및 제어 정보, 그리고 fault/attack이 발생한 O-LSP의 식별자 등이 전달된다[19]. 이후 해당 O-LSP에게 보호 및 복구의 회복 스킴이 적용되며, 그 절차는 <그림 11>과 같다.

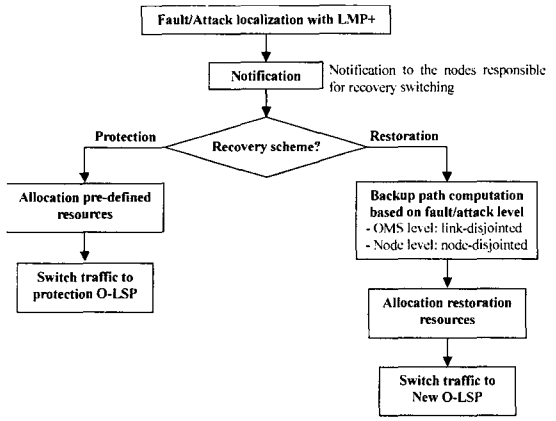


그림 11. Fault/Attack 회복을 위한 시그널링 절차
Fig. 11. Signaling procedure for recovering fault/attack.

먼저 보호 스킴의 경우, 미리 설정된 backup path로 트래픽을 스위칭하기 위해서 ingress와 egress 노드 간에 switchover request/response를 나타내는 Notify request object를 PATH/Resv 메시지에 넣어 교환한다[17, 18]. 이렇게 백본망의 터미널 노드인 ingress-egress 간에 protection switching을 위한 정보 전달이 완료되면 backup path로 트래픽을 스위칭한다. 보호를 위한 backup path 요구는 시그널링 프로토콜인 RSVP-TE+의 PATH 메시지 내에 <그림 12>에 제시된 protection 객체를 통해 이루어진다. GMPLS의 protection path는 working path 설립시 이루어지며, 이때 protection 객체의 S(Secondary bit)와 P(Protecting bit)비트를 사용하여 요구되는 O-LSP가 working path인지 backup path인지를 나타낼 수 있다[18]. 예를 들어, 1:1 보호의 경우 working path는 "S(0), P(0)"이며, backup path는 "S(0), P(1)"로 요구된다. 그리고 1+1 보호의 경우에는 working path는 "S(0), P(0)", fault/attack 발생 후 요구되는 backup path는 "S(1), P(0)"로 요구된다. 이외에도 "LSP Falgs"에서 정의되는 다양한 보호/복구를 위한 working, backup path의 요구를 제공할 수 있다.

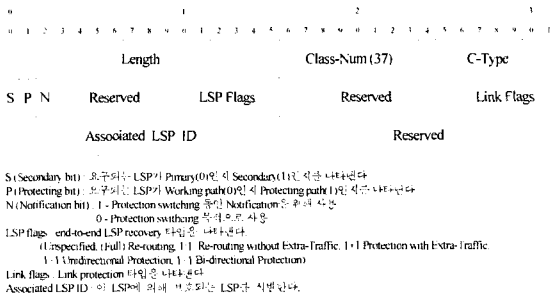


그림 12. Protection 객체의 포맷
Fig. 12. Format of the protection object.

망 장애 발생후 동적인 backup path를 할당하는 복구 스킴의 경우, Notification 이후 fault/attack 레벨에 기준(2.1에서 제시)한 backup path 계산이 이루어진다. 이 과정에서 working path에 영향을 받지 않도록 OMS 레벨의 fault/attack 발생시 link-disjointed backup path, AOTN 노드 레벨의 fault/attack 발생 시에는 node-disjointed backup path가 계산된다. 이후 RSVP-TE+를 통한 자원 예약이 수행되고, 새로운 O-LSP로 해당 트래픽을 스위칭함으로써 복구 절차가 완료된다.

V. 결 론

본 논문에서는 차세대 광 인터넷 백본망인 AOTN에서의 광소자별 fault/attack 가능성 분석을 토대로 망 생존성 보장에서 요구되는 fault/attack 관리 모델을 제시하였다. 세부적으로는 분산형 관리에 적합한 Fault/Attack D&RCS와 out-of-band 제어 채널로 동작되는 LMP+ 모델을 통해 fault/attack 관리에 필요한 광 도메인에서의 fault/attack 검출 및 지역화 절차를 제시하였다. 그리고 RSVP-TE+ 통한 Fault/Attack 통지 및 보호/복구 과정의 흐름을 마지막으로 살펴보았다. 이와 같이 본 논문에서 제시된 fault/attack management 프레임워크는 fault survivability 뿐만 아니라, attack survivability까지 보장 가능한 관리절차를 제시함으로써, 차세대 광 인터넷 백본망인 AOTN에서 신뢰성 있는 서비스를 제공할 수 있을 것으로 기대되며, 향후 다양한 광소자들의 동작 특성이 고려된 fault/attack 가능성과 제어 프로토콜의 구체적인 기능 제시와 fault/attack 관리 모델의 구현을 통한 시뮬레이션 등의 연구가 지속적으로 이루어져야 할 것이다.

참 고 문 헌

[1] Bala Rajagopalan, James Luciani, et al., "IP over Optical Networks: A Framework," Internet Draft, draft-ietf-ipo-framework-04.txt, April 2003.

[2] Jigesh K. Patel, Sung-Un. Kim, David. H. Su, "Modeling Attack Problems and Protection Schemes for All-Optical Transport Networks," Optical Network Magazine, 3(4), pp. 61-72, July/August 2002.

[3] Muriel Medard, Douglas Marquis, et al., "Security Issues in All-Optical Networks," IEEE Network, 11(3), pp. 42 -48, May/Jun 1997.

[4] M. Medard, D. Marquis, S.R. Chinn, "Attack Detection Methods for All-Optical Networks," NDSS '98, the Internet Society's Symposium on Network and Distributed System Security, 1998.

[5] http://www.ll.mit.edu/aon/

[6] Nicolas Gisin, et al., "Quantum cryptography," Reviews of Modern Physics, 74, pp. 145-195, January 2002.

[7] C. P. Larsen, P. O. Andersson, "Signal Quality Monitoring in Optical Networks," Optical Network Magazine, 1(4), pp. 17-23, October 2000.

[8] Stefano Binetti, Svetlana Chemiakinal, Roberto Sabella, "Impact of Fiber Non-linearity in high Capacity WDM Systems and in Cross-Connceted Backbone Networks," Photonic Network Communications, 3(3), pp. 237-243, July 2001.

[9] Harish Jayaram, "Proposed Optical Performance Monitoring Parameters for OTN," Contribution to T1 standards project, September 2001.

[10] Stanic, S. Subramaniam, et al., "On Monitoring Transparent Optical Networks," Proceedings of the International Conference on Parallel Processing Workshops(ICPPW'02), pp. 18-21, August 2002.

[11] Jae-Dong Lee, Sung-Un Kim, et al., "Differentiated Wavelength Assignment with QoS Recovery for DWDM Next Generation Internet Backbone Networks," Photonic Network Communications, 5(2), pp. 163-175, March 2003.

[12] David. H. Su, Sung-Un. Kim, et al., "Attack Management for All-Optical Transport Networks," Proceedings of Wisa 2002, Vol.3, pp. 405-422, August 2002.

[13] Youngtak Kim, et al., "GLASS (GMPLS Lightwave Agile Switching Simulator) - A Scalable Discrete Event Network Simulator for GMPLS-based Optical Internet," http://dns.antd.nist.gov/glass/, white paper.

[14] Eric Mannie, et al., "Generalized Multi-Protocol

Label Switching(GMPLS) Architecture," Internet Draft, draft-ietf-ccamp-gmpls-architecture-07.txt, May 2003.

[15] J. Lang, "Link Management Protocol(LMP)," Internet Draft, draft-ietf-ccamp-lmp-08.txt, March 2003.

[16] A. Fredette, J. Lang, "Link Management Protocol(LMP) for DWDM Optical Line Systems," Internet Draft, draft-ietf-ccamp-lmp-wdm-01.txt, September 2002.

[17] P. Czezowski, T. Soumiya, "Optical Network Failure Recovery Requirements," Internet Draft, draft-czezowski-optical-recovery-reqs-00.txt, October 2002.

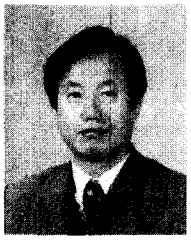
[18] J. P. Lang, Y. Rekhter, "RSVP-TE Extensions in support of End-to-End GMPLS-based Recovery," Internet Draft, draft-lang-ccamp-gmpls-recovery-e2e-signaling-01.txt, May 2003.

[19] L. Berger, "Generalized Multi-Protocol Label Switching(GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering(RSVP-TE) Extensions," RFC 3473, January 2003.

저 자 소 개

金 成 賛(正會員)

1982년 12월~1985년 9월 : 한국 전자통신연구원, 연구원. 1985년 10월~1995년 8월 : 한국통신 연구개발본부, 연구실장. 1990년 8월 : 프랑스 국립 파리 7 대학교 정보공학과 석사. 1993년 8월 : 프랑스 국립 파리 7 대학교 정보공학과 박사. 2000년 8월~2001년 7월 : 미국 NIST 초빙 연구원, DARPA 과제 수행. <주관심분야 : Optical Network, NGN, 광 생존성, RWA, GMPLS, 프로토콜 엔지니어링>



李 俊 源(正會員)

1976년 2월 : 서울대학교 전자공학과 졸업(학사). 1992년 8월 : 충북대학교 전산과 졸업(석사). 1997년 8월 : 충북대학교 전산과 졸업(박사). 1977년~1979년 : 삼성전기 근무. 1980년~1998년 : 한국전자통신연구원 근무(초고속망 연구실장). 1987년~1989년 : 미국 AT&T Bell 연구소 방문 연구원. 1998년 3월~현재 : 안동대학교 정보통신 전공 조교수. 2001년 1월~현재 : 솔루넷(주) 대표이사. <주관심분야 : 정보통신 표준, 초고속 정보통신망, 인터넷 주문>