차세대 광 인터넷 백본망에서 망생존성을 위한 Fault/Attack Management 프레임워크

*신주동, 김성운, 황진호, **한종욱, 손승원
*부경대학교 정보통신공학과, **한국전자통신연구원
e-mail : *jdshin@mail1.pknu.ac.kr, kimsu@pknu.ac.kr, jhhwang@korea.com, {hanjw, swsohn}@etri.re.kr*

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

**Ju-Dong Shin, Sung-Un Kim, Jin-Ho Hwang, **Jong-Wook Han, Seung-Won Sohn
*Dept. of Telecommunication Engineering, PuKyong Nat'l University,
Electronics and Telecommunications Research Institute

Abstract

As optical network technology advances, the Dense-Wavelength Division Multiplexing(DWDM) networks have been widely accepted as a promising approach to the Next Generation Optical Internet (NGOI) backbone networks. Especially, a fault/attack management scheme in NGOI backbone networks 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 backbone networks and propose a fault/attack recovery procedure in IP/GMPLS over DWDM.

Ⅰ. 서론

최근 급속하게 증가하는 인터넷 트래픽을 고속 대용량의 광 통신망을 통해 전달할 수 있는 차세대 통신 네트워크의 패러다임으로 IP/GMPLS over DWDM 모델의 표준화 연구가 국내외에서 활발하게 진행되고 있다. 이 모델은 DWDM(Dense Wavelength Division Multiplexing) 기술을 이용한 풍부한 대역 제공 능력과 기존 IP의 범용성, 그리고 단일 제어평면인 GMPLS(Generalized Multi-Protocol Label Switching)가 결합된 경제적이고 효율적인 네트워크로 주목받고 있다[1]. 그러나 광 파이버, 광 증폭기, 포토닉 스위치 등의 non-regeneration 시스템이 사용되기 때문에, 기존의 오버헤드 비트를 이용한 전송 관리 정보가 더 이상 유효하지 않아 장애 관리에 많은 어려움을 지니게 된다. 특히 광소자의 일시적 장애로 인한 서비스 파괴, DARPA(Defense Advanced Research Projects) 과제를 통해 보고된 물리적 공격 가능성과 이들의 심각성은 차세대 광 인터넷(NGOI: Next Generation Optical Internet)에서의 신뢰성 있는 서비스 제공에 결정적인 결함을 초래하며, 이에 대한 적절한 대처 방안이 절실하게 요구되고 있다[2-3]. 따라서 본 논문에서는 NGOI 백본망에서의 생존성 보장을 위한 fault/attack 관리 모델 및 회복 절차를 제시한다. 이를 위해 본 논문의 구성은 다음과 같다. 먼저, 2장에서는 전광 전달망(All Optical Transport Network: AOTN)인 NGOI 백본망의 fault/attack 관리 모델을 제안하고, 3장에서는 GMPLS의 링크 관리 프로토콜과 시그널링 프로토콜을 이용한 fault/attack의 회복 절차를 제시한다. 마지막으로 5장에서는 결론 및 향후 연구방향을 제시한다.

본 연구는 한국전자통신연구원 수행과제(과제번호: 0701-2003-0019) 연구비에 의해 연구되었음

II. Fault/Attack 관리 모델

제안되는 NGOI 구조는 그림 1과 같이 두 개의 기능적 도메인으로 분류된다. 외부 도메인은 패킷 헤더 정보를 기반으로 하는 기존의 상업적인 전기 도메인(LAN, MAN, ATM등)이며, NGOI의 백본망인 내부 도메인은 광소자 기술로 구현된 AOTN이다. 특히 AOTN에서는 포토닉 스위치의 사용으로 인한 투명한(transparent) 데이터 전달 특성을 가진다[2, 4].

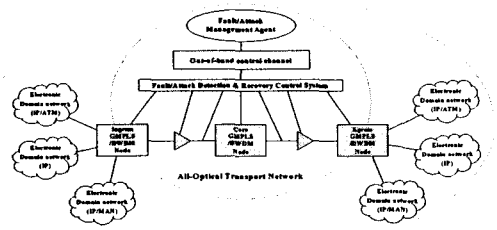


그림 1. NGOI 백본망의 fault/attack 관리 모델

이 같은 NGOI 백본망에서의 fault/attack 관리 모델은 다음의 세 부분으로 분석된다. 첫째, Fault/Attack D&RCS(Detection & Recovery Control System)는 광 계층과 매우 가깝게 위치하여 fault/attack 발생 사실을 상위 단계에 통지하거나 상위 단계의 제어에 따른 물리적인 회복을 담당한다. 둘째, out-of-band 제어 채널은 Fault/Attack MA(Management Agent)와 Fault/Attack D&RCS 간의 양방향 인터페이스를 제공한다. 마지막으로, Fault/Attack MA는 fault/attack 회복을 위한 일련의 제어를 담당한다.

2.1 Fault/Attack D&RCS

광 도메인에서의 fault/attack 검출 및 광소자의 능동적인 제어를 수행하기 위해 본 논문에서는 그림 2와 같이 구성된 Fault/Attack D&RCS를 제안하며, 그 구성은 다음과 같다.

(a) Optical Devices(광소자)
(b) Monitoring Module(모니터링 모듈) : OPL(Optical Power Level), OSA(Optical Spectrum Analysis), Q-factor 등 광 성능 모니터링 기술 적용[5]
(c) ORMA(Optical Resource Management Agent) : 광자원의 상태정보 유지 및 광소자의 제어 담당
(d) Micro-Controller : 광소자의 물리적 제어를 담당
(e) Optical Power Equalizer : 입력 파워를 제어, 광전력의 변동으로 인한 장애 및 물리적 공격에 대한 능동적 대처가 가능

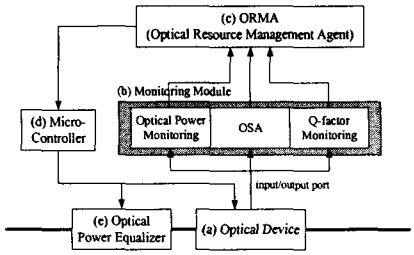


그림 2. Fault/Attack D&RCS의 구조

Fault/Attack D&RCS는 각 소자의 동작이나 광신호 품질을 모니터링 하여 fault/attack 조건을 검출하며, 본 논문의 2.2에서와 같은 out-of-band 제어 채널을 통해 관리 시스템에게 공격 상태를 보고하거나 광소자들의 회복을 위한 제어를 담당한다.

2.2 Out-of-band 제어 채널

IETF(the Internet Engineering Task Force)에서는 광 링크로 연결된 이웃한 노드간에 링크와 관련한 제어 정보를 주고받기 위해 out-of-band 제어 채널인 링크 관리 프로토콜(Link Management Protocol: LMP)을 정의하고 있다[6]. 그러나 LMP 만으로는 두 이웃 노드를 연결하는 DWDM 시스템의 광 링크 구조 및 상태 정보를 전달할 수 없으며, 이에 Fault/Attack D&RCS와의 정보 교환을 목적으로 하는 LMP-WDM의 도입이 요구된다[7]. 본 논문에서는 그림 3과 같이, fault/attack 관리를 위한 out-of-band 제어 채널로써 LMP와 LMP-WDM이 상호 동작되는 모델(이하 LMP+라 명칭)을 제안한다.

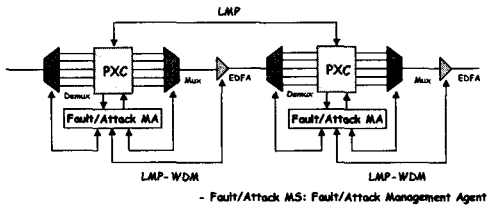


그림 3. LMP+ 모델

LMP+ 모델은 광 도메인과 전기적 제어 평면이 LMP-WDM을 통해 연결되는데, LMP-WDM을 통해 수집된 광 링크의 정보를 기반으로 GMPLS의 TE(Traffic Engineering) 링크 형성 및 fault/attack 관리를 위한 이웃한 노드간의 제어 정보의 전달이 수행된다.

2.3 Fault/Attack Management Agent

Fault/Attack MA(Management Agent)는 제어 채널

인 LMP+로 전달된 광소자 및 DWDM 링크의 상태 정보를 광 스위치의 분기 포트(drop port)를 통해 수신하고, fault/attack 종류에 따른 적절한 회복을 위한 시스템의 전반적인 제어 절차를 제공한다.

III. Fault/Attack 회복 절차

GMPLS로 제어되는 광 전송망에서, 데이터 평면에서 발생한 장애를 회복하기 위한 요구 절차는 다음의 세 가지로 요약된다. 첫째, 시스템 레벨에서 처리되는 fault/attack 검출단계, 둘째, LMP+를 통한 fault/attack 지역화 및 분리단계, 마지막으로는 RSVP-TE+에 의한 fault/attack 통지와 ingress-egress 간의 보호/복구(protection/restoration) 스킴의 적용을 통한 및 정상 상태 진입 단계이다.

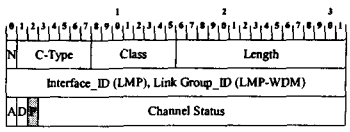
3.1 Fault/Attack 검출

광소자의 장애는 각 소자의 입력/출력 포트에서의 광전력을 비교함으로써 검출한다. 예를 들면, 입력 파워가 'α'(단, 'α'는 시스템이 허용하는 임계치 이상의 값), 출력 파워가 '0'일 경우에는 광소자의 고장으로 간주되며, 입력 파워가 '0', 출력 파워도 '0'일 경우에는 업스트림 광소자의 고장 전파로 인한 LOL(Loss Of Light)로 분석될 수 있다. 또한 환경적 요인이나 물리적 공격으로 인한 신호 품질 감쇄의 경우는 광 성능 모니터링으로 측정된 광 성능 파라메터 값과 시스템이 요구하는 최저(혹은 최고) 임계치 값을 비교함으로써 신호 품질 감쇄의 검출이 가능하다.

3.2 Fault/Attack 지역화 및 분리

LMP+는 ChannelStatus 메시지 교환을 통해 망에서 발생한 fault/attack 지역화 및 분리 (localization and isolation) 메커니즘을 제공한다. 이때 사용되는 ChannelStatus 메시지는 하나 혹은 그 이상의 데이터 채널들의 상태를 이웃 노드에 통지하기 위해 사용되며, 포맷은 그림 4와 같이, Interface_ID(LMP) 혹은 Link Group_ID(LMP-WDM), Channel Status 및 데이터 채널의 방향 등을 나타낸다[6-7]. 특히 LMP-WDM에서는 Interface_ID 대신 새롭게 정의된 Link Group_ID를 사용하여 제어 트래픽의 양을 줄일수 있다.

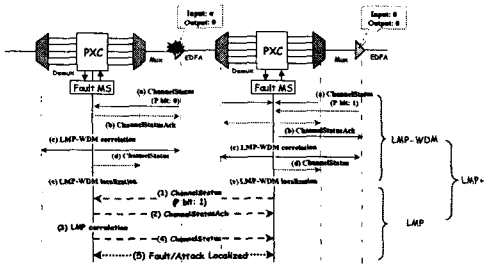
LMP+ 모델에서 ChannelStatus 메시지의 교환은 물리적으로 2가지 의미를 가진다. ChannelStatus 메시지를 전달하는 광소자나 링크에서 fault/attack이 발생했음을 보고하는 경우, 그리고 업스트림에서 발생한 fault/attack의 전파로 인해 다운스트림 측에서 fault



N : 객체가 협상가능(N=1)한지 불가능한지(N=0)를 나타낸다
C-Type : Object class의 타입
Class : Object 타입
Length : Object의 길이(Object 헤더길이 포함).
Link Group_ID : 데이터링크들의 그룹식별자
A (Active bit) : 사용자 트래픽이 할당된 채널인지 식별, 모니터링 필요 여부를 나타낸다.
D (Direction bit) : 데이터 채널의 방향을 나타낸다.
P (Position bit) : SF, SD 알람이 사용되며, Fault인지 Fault propagation인지를 나타낸다
Channel Status : 데이터 채널의 상태를 나타낸다.

그림 4. ChannelStatus 객체의 포맷

/attack 발생을 보고하는 경우이다. 이 두 경우의 차이점은 3.1에서도 살펴보았듯이 광소자의 입/출력 포트에서의 광 성능 모니터링을 통해 구분 가능하며, DWDM 광 링크 구간에서의 보다 정확한 지역화를 위해서는, 이들 두 경우의 정확한 의미를 제어 평면에 전달해야할 필요가 있다. 따라서, 본 논문에서는 기존의 Channel Status 필드 중 1비트를 P비트(Position bit)로 활용할 것을 제안한다. 제안된 P비트는 LMP-WDM과 LMP에 모두 사용되며, P비트가 '0'이면 관리되는 구간에서의 fault/attack이 발생했음을 나타내고, P비트가 '1'이면 전파에 의한 fault/attack 임을 의미한다. 그림 5는 제안된 LMP+ 모델에서 ChannelStatus 메시지와 Channel Status 필드의 P비트를 사용한 지역화 알고리즘으로, LMP-WDM 지역화와 LMP 지역화의 두 가지 과정으로 상호 동작되며, 이를 통해 고장난 광소자의 위치까지도 정확하게 검출 및 지역화 할 수 있다.



Phase 1: LMP-WDM 지역화
(a) Fault/Attack D&RCS의 ChannelStatus 메시지 전달
(b) LMA의 ChannelStatusAck 응답
(c) LMP-WDM correlation
(d) 각 Fault/Attack D&RCS에게 상태 정보 전달
(e) LMP-WDM 지역화 절차 완료

Phase 2: LMP 지역화
(1) D-LMA가 U-LMA로 ChannelStatus 메시지 전달
(2) U-LMA의 ChannelStatusAck 메시지 응답
(3) LMP correlation
(4) D-LMA에게 상태 정보 전달
(5) LMP 지역화 절차 완료

그림 5. LMP+ 지역화 과정 및 알고리즘

3.3 Fault/Attack 통지 및 보호/복구

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/attack의 발생을 알리며, 이 메시지를 통해 fault/attack 상태 및 제어 정보, 그리고 fault/attack이 발생한 O-LSP(Optical-Label Switched Path)의 식별자 등이 전달된다[8-10]. 이후 해당 O-LSP에게 보호 및 복구의 회복 스킴이 적용되며, 그 절차는 그림 6과 같다.

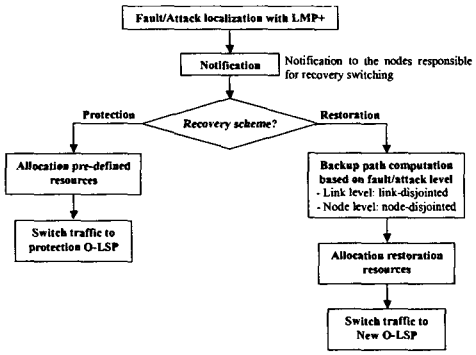


그림 6. Fault/Attack 회복 시그널링 절차

먼저 보호(protection) 스킴의 경우, 미리 설정된 대체 경로(backup path)로 트래픽을 스위칭하기 위해서 ingress와 egress 노드간에 'switchover request /response'를 나타내는 'Notify request object'를 PATH/Resv 메시지에 넣어 교환한다. 이렇게 백본망의 터미널 노드인 ingress-egress 간에 보호 스위칭을 위한 정보 전달이 완료되면, 대체 경로로 트래픽을 스위칭한다. 보호를 위한 대체 경로의 요구는 최초 O-LSP 셋업시 RSVP-TE+의 PATH 메시지 내에 protection 객체를 통해 이루어진다[9].

망 장애 발생후 동적인 대체 경로를 할당하는 복구(restoration) 스킴의 경우, Notification 이후 fault/attack 종류에 따른 대체 경로의 계산이 이루어진다. 이 과정에서 fault/attack이 발생한 경로에 영향을 받지 않기 위해서 링크 레벨의 fault/attack 발생 시에는 link-disjointed 대체 경로로, 노드 레벨의 fault/attack 발생 시에는 node-disjointed 대체 경로를 계산한다. 이후 RSVP-TE+를 통한 자원 예약이 수행되고, 새로운 대체 경로로 해당 트래픽을 스위칭 함으로써 복구 절차가 완료된다.

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 현재 각광받고 있는 NGOI 백본망인 AOTN에서의 fault/attack 관리 모델과 fault/attack 검출 및 지역화 절차를 제시하였다. 또한 GMPLS 시그널링 프로토콜을 통한 fault/attack 통지 및 보호/복구 과정의 흐름을 마지막으로 살펴보았다. 이와 같이 본 논문에서 제시된 fault/attack 관리 프레임워크는 NGOI 백본망에서 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.

참고문헌

[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] 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.

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

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

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

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

[9] 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.

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