情 報 保 護 學 會 誌
第 13 券 第 1 號, 2003. 2

전광 전달망(AOTN)에서의 물리적 보안 관리

김 성 운*, 신 주 동**, 한 종 욱***

요 약

차세대 광 인터넷 백본망 기술은 WDM(Wavelength Division Multiplexing)기반의 고속 대용량 전광 전달망인 AOTN (All-Optical Transport Network)으로 발전하고 있고, 가입자의 원활한 멀티미디어 서비스의 제공을 위한 망 생존성 보장이 중요한 이슈로 부각되고 있다. 특히 광소자의 고유한 특성을 교묘히 이용하는 물리적 공격은 AOTN의 투명한 데이터 전달 특성으로 인해 기존의 오버헤드를 이용한 관리 시스템이 더 이상 유효하지 않아, 새로운 검출/회복 메커니즘이 요구된다. 본 고에서는 AOTN에서 발생 가능한 공격 유형을 광소자별로 분석하고, 광 레벨에서의 공격 검출과 회복 메커니즘을 소개한다. 이를 바탕으로 공격관리 시스템(Attack Management System: AMS)의 제어 모델을 기술한다.

Ⅰ. 서 론

광 인터넷 백본망 기술은 TDM(Time Division Multiplexing) 기술에 기반한 단일파장의 SONET/SDH에서 WDM 기술을 사용하는 광 전달망으로 발전해 가고 있다. 특히 DWDM(Dense WDM) 기반의 전광 전달망인 AOTN은 대용량의 고속 전송 서비스를 제공하기 때문에, 광 링크나 광 증폭기, 광 회선분배기(Optical Cross-connect: OXC), OADM(Optical Add/Drop Multiplexer) 등 광소자의 일시적 장애 또는 이에 대한 의도적인 공격으로 인해 많은 데이터가 손실될 수 있고, 이것은 망 생존성(network survivability)에 치명적인 문제를 초래할 수 있다. 따라서 광대역 초고속의 AOTN이 백본망으로서 차세대 멀티미디어 서비스의 원활한 전개를 위해서는 망 생존성의 보장(즉, 망 장애로부터 사용자 트래픽을 보호하고, 의도적인 공격으로 인한 서비스의 단절로부터 사용자 트래픽을 보호하는 시스템의 능력으로 정의)이 가장 핵심적인 기술로 대두되고 있다. 현재 차세대 광 인터넷 백본망 구현을 위해 미국에서는 Internet 2 프로젝트를 수행하고 있고, 캐나다에서는 WDM을 이용한 광 전달망에서 IP를 구현하기 위한 CA*net3가 연구중이며, 유럽에서도 전광 전달망 구현을 위해 TF-TANT(Task Force-Testing of Advanced Networking Technologies) 프로젝트가 수행되고 있다. AOTN 생존성에 관한 연구는 MIT(Massachusetts Institute of Technology) 및 미국방성 DARPA(Defense Advanced Research Projects Agency)과제 등으로 학계 및 연구계에서 많은 연구가 시작되었으나, 기존의 망 관련 프로토콜 기술, WDM 기술, 광소자 관련 기술, 보안 관련 기술 등 다양한 분야의 내용과 연관되기 때문에 상업화 및 실제 시스템 적용에 많은 연구와 개발 노력이 요구되고 있다.

백본망인 AOTN을 통해 전송되는 광신호는 간단한 감쇄에서부터 복잡한 비선형 효과(nonlinear effect)나 분산(dispersion) 등 다양한 손실요인에 노출되어 있다. 이러한 손실요인들은 광 전달매체 또는 능동/수동 소자들의 고유한 특성으로 인해 악의적인 공격자의 공격에 이용될 수 있는데, 일반적으로 매체를 직접 공격하는 물리적 공격들에 대해서는 현재의 광 검출 기술로 발견하고 교정할 수 있으나, 광소자들의 특성을 교묘히 이용한 공격은 광소

* 부경대학교 정보통신공학과 (kimsu@pknu.ac.kr)
** 부경대학교 정보통신공학과 (jdshin76@korea.com)
*** 한국전자통신연구원 정보보호연구본부 (jwhan@etri.re.kr)

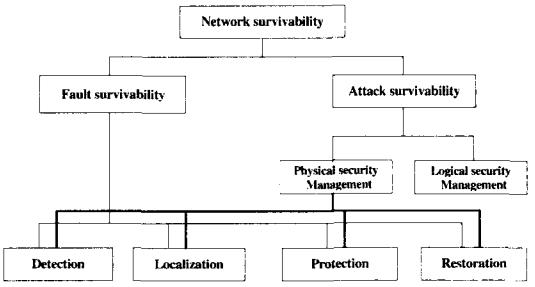
자에 대한 전문지식을 바탕으로 하는 검출 스킴과 회복 스킴이 필요하다. 특히 AOTN의 광/전 변환(optical/electronic conversion)이 없는 투명한(transparent) 데이터 전달 특성은 오버헤드 비트(overhead bit)를 이용한 중간 노드에서의 데이터 모니터링과 재생이 불가능하기 때문에, 광 레벨에서 공격을 검출하기 위해서는 새로운 검출 메커니즘과 각 공격 유형에 대응되는 회복 메커니즘의 도입이 필요한 것이다. 본 고에서는 AOTN에서 발생 가능한 물리적 공격 유형에 대한 분석과, 공격 유형별 검출/회복 메커니즘을 소개하고, AOTN의 구조와 생존성 문제에 관련하여, IP/GMPLS(Generalized-MPLS) over WDM 제어 프로토콜을 이용한 공격관리 시스템의 모델을 기술한다.

II. AOTN에서의 생존성 이슈

고속 대용량의 DWDM 기술이 인터넷 백본망 기술로 자리를 확고히 함에 따라, 백본망에서의 생존성 보장이 중요한 이슈로 부각되고 있다. 즉, 가입자에게 안정적인 서비스를 제공하기 위해서 시스템 관리자는 망에서 발생하는 장애나 공격을 신속히 인지하고, 정상적인 트래픽과 분리시키며, 파괴된 트래픽에 대한 복구를 제공해야한다. 이를 위해 시스템 관리자는 장애나 공격에 대한 정확한 분석과 망 관리 시스템을 통한 적절한 대응책이 요구되는데, 일반적으로 AOTN에서의 생존성 이슈는 그림 1과 같이 장애에 대한 생존성 보장(fault survivability)과 의도적 공격에 대한 생존성 보장(attack survivability)으로 분석된다.[1]

장애에 대한 생존성 보장은 망에서 사용되는 능동소자의 갑작스런 고장으로 발생하는 시스템 동작 불능과 점진적인 신호 품질의 저하에 대응하는 것으로, 전자를 hard failure, 후자를 soft failure라고 부르며, 어떠한 광소자의 장애에도 강건한 시스템의 구현을 그 목적으로 한다.

반면 공격에 대한 생존성 보장은 크게 물리적 공격에 대한 보안문제와 논리적 공격에 대한 보안 문제로 해석된다. AOTN에서 물리적 공격이란, 비권한자가 물리적 접근을 통해 서비스 파괴, 서비스 품질 저하 등을 목적으로, 광 전송 매체로 사용되는 광파이버나 기타 다양한 광 소자들이 가지는 고유한 광학 특성을 이용하는 공격 유형으로, 기존의 전기적



[그림 1] AOTN의 망 생존성

망이나 electro-optic 망에서 취급되는 공격 유형과는 다른 형태로 분류된다. 특히 광/전 변환이 없는 투명한 데이터 전송 특성으로 인해 기존망에서 사용되던 오버헤드 비트를 사용한 전송 관리 정보(transport supervisory information)를 더 이상 사용할 수 없게 됨에 따라, 새로운 형태의 검출 메커니즘과 각 공격 유형에 대응되는 회복 메커니즘의 도입이 필요하다.

위와는 다르게 비권한자는 정보의 획득/조작을 목적으로 망에 접근할 수 있는데, AOTN의 특성상 짧은 순간의 접근으로 많은 양의 정보가 외부로 누출될 위험이 있다. 탭핑(tapping)이나 재밍(jamming)을 통해 정보를 획득/조작하는 논리적 공격의 가장 큰 문제점은 광 레벨에서의 검출이 어렵다는 것이다. 그러나 본 고에서 제시하는 검출 메커니즘(3.3에서 설명)과 향후 암호화 기술로 주목받고 있는 양자 암호화(quantum cryptography) 기술의 도입으로 극복될 수 있으리라 전망한다.

관리 시스템이 위와 같은 장애/공격으로부터 생존성을 보장하기 위해서 제공해야 하는 메커니즘은 다음과 같다.

첫째, 보호(protection) 메커니즘은 망에서 주경로(primary path)가 할당될 때, 파장이나 파이버와 같은 여분의 망 자원을 사용하여 백업 경로(backup path)를 미리 할당하고, 장애/공격이 검출되면, 트래픽 복구를 위해 미리 할당된 백업 경로로 트래픽을 스위칭함으로써 생존성을 보장하는 메커니즘이다.

둘째, 검출(detection) 메커니즘은 일반적으로 보호/복구에 앞서 수행되며, 망 생존성에서 중요한 메커니즘이다. 특히 전광 전달망을 통해 전달되는 데이터 스트림은 중간 노드에서 광전 변환 없이 전달되기 때문에 각 세그먼트 사이의 신호 품질을 모

니터링 하기란 쉽지 않다. 그러나, 파이버의 절단이나 노드 장애에 의한 LOS(Loss Of Signal) 등 일반적인 결함은 광 모니터링 방법으로 발견할 수 있다. 하지만 앞서 언급한 물리적인 공격에 대해서는 현재의 간단한 모니터링 방법으로 검출하기가 어려운 상황이다.

셋째, 장애 고립(localization or isolation) 메커니즘은 검출 메커니즘에 의해 망 내에서 장애/공격이 발생했음을 인지한 후, 그 위치를 관리 시스템에 통보하는 메커니즘이며, 이것의 가장 중요한 목적은 문제의 광소자를 사용자 트래픽과 분리하는 데 있다.

마지막으로 복구(restoration) 메커니즘은 장애/공격이 발생한 후, 전체적인 망 상황을 고려하여 동적으로 백업 경로를 할당하는 메커니즘이다. 보호 메커니즘은 광 경로를 할당하면서 미리 백업 경로를 할당하기 때문에 자원의 효율성이 매우 떨어지는데 반해, 복구 메커니즘은 장애 발생 후, 여분의 자원을 백업 경로로 활용하므로 자원을 효율적으로 사용할 수 있다. 그러나 전체적인 망 상황을 지속적으로 모니터링해야 하고, 백업 경로를 할당하는 절차를 수행해야 하기 때문에 복구 시간이 늦다는 것이 단점이다.

현재 많은 연구 기관에서 AOTN의 생존성 연구가 진행되고 있으나, 고려되어야 할 이슈들이 산재해 있고, 현 시점에서 보안 문제를 해결하는 데에는 기술적으로 부족하다. 특히 AOTN에서의 물리적 공격에 대한 연구는 아직 초보단계이며, 기존의 전기적 망에서 존재하는 논리적 보안문제 또한 고려되어야 한다. 본 고에서는 AOTN에서 가능한 물리적 공격 유형들을 분석하고, 이를 검출 관리할 수 있는 시스템을 분석한다.

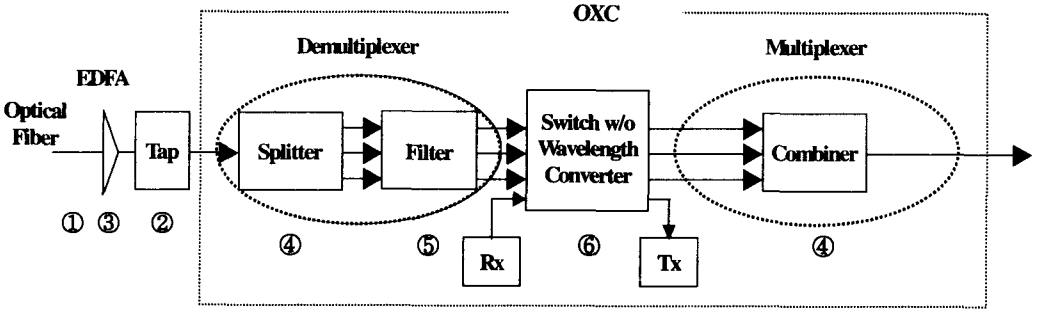
Ⅲ. 물리적 공격 가능성과 관리기술

3.1 물리적 공격 가능성

AOTN은 그림 2와 같이, 설정된 광경로에 따라 파장을 스위칭하는 광 회선분배기, 전송되는 광신호를 일괄적으로 증폭시키는 광 증폭기, 그리고 광신호를 전달하기 위한 광 파이버와 탭으로 구성되며, 광 회선분배기는 광 역다중화기/광 스위치/광 다중화기로 세분화된다. 그리고 파장의 선택성을 높여주기 위한 광 필터가 부가적으로 사용된다. 그러나 광소자들이 가지는 다양한 시스템 패널티(system penalty)는 침입자의 공격 포트로 이용된다. 즉, 석영계 광섬유에서 발생되는 색분산, PDL(Polarization Dependant Loss), 비선형 현상과 광 증폭기의 ASE(Amplified Spontaneous Emission) 잡음, 그리고 광 필터에 의한 crosstalk 현상들은 시스템에서 광신호의 감쇄와 왜곡의 원인이 되며, 공격자는 이런 요소들을 교묘하게 이용하여 서비스를 파괴하고, 신호의 품질을 저하시키며, 사용자 정보를 획득하는 포트로 활용된다.

3.1.1 광 파이버 (공격 포트①)

공격자가 광 파이버나 탭에 직접 접근할 수 있다면, 시스템은 공격으로부터 취약하게된다. 예를 들면, 공격자가 파이버에 접근하여 의도적으로 파이버를 절단할 수 있는데, 이것은 기존의 검출 메커니즘이나 센서를 사용하여 쉽게 검출할 수 있고[2-3], 파이버를 견고하게 제작하여 미연에 방지할 수 있다. 그러나 가장 우려되는 것은, 고도의 장비를 갖춘 숙련된 공격자일 경우, 파이버의 탭핑이나 파이버의 밴딩(bending)을 통해 광신호의 일부 모드를 유출



〔그림 2〕 AOTN의 구성 소자와 공격 포트

또는 삽입시켜 공격할 경우이다. 특히 임계치 이상의 높은 전력이 파이버 내로 삽입될 경우, 광 파이버에서 발생되는 비선형 현상은 다른 광신호에 영향을 미친다. 또한 탭을 통해 획득한 광신호는 공격자에 의해 정보 내용이 조작될 수 있다. 이런 형태의 공격은 검출하기가 매우 어렵고, 그 영향이 망 전체에 전파되기 때문에, 그 심각성이 매우 크다.

3.1.2 탭 (공격 포트②)

탭을 제공하는 목적은 쉬운 모니터링과 망의 확장에 따른 자원의 증가에 유연하게 대처할 수 있는 효율적인 결합 포트를 제공하기 위함이다. 그러나 탭의 사용은 삽입 손실의 발생과 외부로의 정보 유출이 우려되는데, 일반적인 시스템에서 발생하는 삽입 손실은 광 증폭기를 통해 보상되지만, 광 증폭기 또한 공격에 취약한 소자(3.1.3에서 설명)이므로 다른 형태의 공격 취약성을 추가적으로 감수해야만 한다. 탭을 통해서 비권한자가 광신호에 접근하는 것은, 광소자의 특성 또는 광신호의 전력 변화 등 임의의 공격에 무방비 상태로 노출되어 있는 것과 같다. 이것으로부터 손실을 최소화하기 위해서는 시스템 내의 탭 수를 최소화하거나, 공격자의 직접적인 접근을 막기 위한 물리적인 보안 대책이 강구되어야 한다. 특히 탭을 이용한 재밍 공격은 검출하기가 매우 어렵기 때문에 적절한 회복을 위해서는 논리적 레벨에서의 회복이나 공격에 취약한 장비를 교체함으로써 극복될 수 있다.

3.1.3 광 증폭기 (공격 포트③)

전송거리에 따른 광전력의 감쇄를 보상하기 위해 사용되는 광 증폭기는 레이저의 원리를 이용한 SOA (Semiconductor Optical Amplifier)와 증폭재료인 어븀(erbium)을 코어에 직접 도핑시켜서 증폭이득을 얻는 EDFA(Erbium Doped Fiber Amplifier)가 사용되는데, 높은 증폭이득과 낮은 crosstalk 특성을 갖는 EDFA가 더욱 실용적인 것으로 보고된다. 그러나 EDFA도 다른 종류의 광 증폭기와 마찬가지로 ASE 잡음으로 인한 채널 간 간섭과, 증폭 이득의 불균형으로 야기되는 이득 경쟁(gain competition)에 취약하다. 광 증폭기는 공격 신호와 사용자 신호를 구별하지 않고 증폭대역 내의 모든 파장을 증폭시키는데, 모든 파장에서 광 증폭기의 한정된 이득(광신호를 증폭시키는 여기 상태의 어븀이온)을 공유하게 된다. 공격자는 높은 전력의 광신호를 광 증폭기 내에 삽입함으로써 공격 신호보다 낮은 전력인 사용자 신호에게 제공되어야 할 증폭이득을 빼앗게 되고, 이로 인해 사용자 신호의 증폭이득이 감소하게 된다. 그리고 AOTN의 투명한 데이터 전달 특성으로 인해 여러 단의 광 증폭기를 거치면서 공격 신호는 지속적으로 증가하는 반면 사용자 신호는 점차 감소하게 된다.[4]

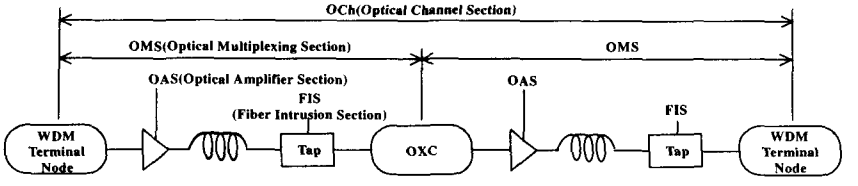
DWDM 시스템은 채널 수가 많을 경우 이득 경쟁이 지배적으로 나타나며, 채널 수가 적을 때에는 crosstalk 현상이 지배적이다. 그리고 높은 데이터율로 광신호가 전송될 때 crosstalk 현상은 더 이상 나타나지 않고 이득 경쟁만 나타난다.[5-6] 공격자는 광 증폭기의 특성을 이용하여 일부 채널의 전송을 방해하거나, 망에서 제공하는 전체 서비스를 파괴하게 된다.

3.1.4 광 스플리터/컴바이너 (공격 포트④)

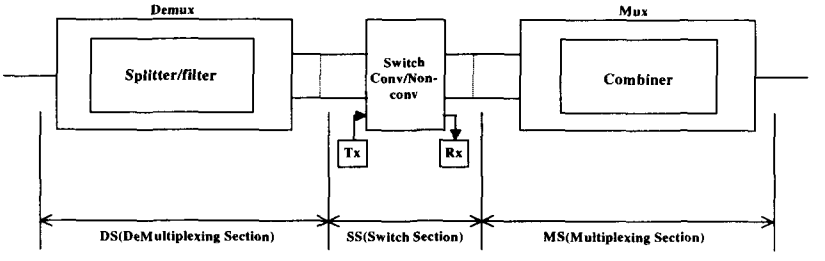
일반적인 광 역다중화기는 스플리터와 광 필터로 구성되거나 광 필터를 응용하여 구현된다. 그리고 스플리터와 컴바이너는 삽입 손실로 인해 광전력의 일부가 손실된다. 이들은 광 필터와 기능적으로 유사하며, 광 필터는 crosstalk를 유발하는 공격에 취약하다.

3.1.5 광 필터 (공격 포트⑤)

성능이 좋은 광 필터는 낮은 삽입 손실과 온도변화에 의한 특성 변화가 없어야 한다. 특히 DWDM 시스템은 채널 간격이 좁기 때문에 이를 필터링 할 수 있는, 좁은 통과대역 특성을 가진 광 필터가 요구된다. 그렇지만 실제 시스템에서는 이상적인 광 필터를 구현할 수 없기 때문에, 어느 정도의 채널 간 crosstalk는 시스템 내에서 감수해야 하며, 특히 채널 간격이 아주 가까운 DWDM 시스템에서 사용되는 대부분의 광 소자들은 어떤 형태로든 crosstalk를 유발하게 된다. crosstalk는 인접 채널과의 간섭현상으로, 광신호의 품질을 저하시키며, 비권한자의 접근으로 인한 정보 유출에 결정적인 기여를 한다. 결과적으로 의도적인 높은 전력 신호는 높은 crosstalk로 나타나고, 다른 합법적인 사용자들의 서비스를 파괴한다. 이런 형태의 공격은 광 레벨에서 쉽게 검출 할 수 없고, 높은 품질의 광 필터를 사용하거나, 필터링 전후에 전력 등화(power



(a) AOTN의 공격관리 구간



(b) 광 회선분배기 내 공격관리 구간

〔그림 3〕 물리적 공격관리 구간

equalization)와 같은 예방 조치가 필요하다.

3.1.6 광 스위치 (공격 포트⑥)

광 스위치 역시 불완전한 파장 선택 스위칭으로 인해 crosstalk가 발생한다. 간섭 신호가 최초 주 신호에 나타날 때를 1차 crosstalk라고 하고, 이 신호가 다시 다음의 스위치에서 crosstalk에 영향을 받으면 이를 2차 crosstalk라고 한다. 광신호는 네트워크에서 다수의 스위치와 여러 노드를 거치면서, crosstalk의 정도는 더욱 복잡하게 된다.[7-8]

합법적인 사용자 신호는 송신기의 전력 레벨 변화에 의해 위협 받을 수 있고, 의도적인 crosstalk는 망에서 제공되는 서비스를 파괴하거나 또는 광전력 감지 기술을 활용하는 비권한자가 사용자 정보에 접근할 수 있는 기회를 제공한다. 전력 등화를 통해 전자의 의도적인 crosstalk를 제거할 수 있으나, 후자의 비권한자의 정보 접근을 검출하는 것은 현재 기술로 매우 어렵다. 그리고 파장 변환기를 사용하는 non-blocking 스위치는 잡음, 삽입 손실, PDL과 관계된 추가적인 crosstalk를 유발하여 공격에 더욱 취약해진다.

3.2. 물리적 공격관리

그림 3의 (a)는 AOTN의 기능적 레벨에 따른 공격관리 구간을, (b)는 광 회선분배기의 공격관리 구간을 분석한 것이다. 광 소자의 특성과 공격자의 공격 유형에 따라 직접적인 공격(direct attack), 간접적인 공격(indirect attack), 그리고 의사 공격(pseudo attack)의 세 가지 유형으로 분류되며, 각 공격 유형에 따른 검출 메커니즘과 회복 메커니즘은 표 1, 2, 3과 같이 요약된다.

3.2.1 직접적인 공격(Direct attack)의 관리

AOTN에서 사용되는 광 소자들은 물리적 공격에 대해 3.1에서 설명된 바와 같이 고유한 취약특성을 나타내는데, 각 소자들은 침입자가 공격 가능한 포트처럼 직접적으로 활용된다. 이것은 물리적 계층 또는 그 상위 계층에서의 복잡한 관리 수단이 요구되며, 직접적 공격에 따른 공격 검출과 분리 메커니즘, 그리고 회복 메커니즘은 표 1로 요약된다.

3.2.2 간접적인 공격(Indirect attack) 의 관리

AOTN의 광 회선분배기와 같은 일부 구간은 물리적으로 침입자가 쉽게 접근하기 어렵기 때문에, 공격자가 서비스 파괴나 정보획득 등의 목적으로 표 1과 같은 일련의 공격활동을 하기가 곤란하다. 그러나 광 필터의 crosstalk 특성을 이용하는 간접적 공격은 직접적인 공격보다 성공하기는 어려우나, 일단 공격이 가해진다면, 이에 대한 검출이나 분리, 그리고 복구는 직접적인 공격보다 더욱 복잡하며,

〔표 1〕 직접적인 공격 유형과 관리 기능

구간	공격 유형	검출 메커니즘	회복 메커니즘
FIS	탭을 통한 비권한자의 정보 접근	탭의 전후를 통한 지속적인 평균 전력 레벨의 모니터링	물리적 보안대책 제공(3.1.2)
	탭핑과 재밍에 의한 광신호의 품질 저하	의사 공격인지 직접적 공격인지 판단하기가 곤란	논리적(전기적) 레벨에서의 회복 메커니즘이 요구
	재밍에 의한 정보변경	광 레벨에서 검출이 곤란	
OAS	근거리 소자를 통한 이득 경쟁	광전력 모니터링 또는 채널상태 테스트(in-situ channel equality test)[1]	전력 등화(power equalization) 스킴
	원거리 소자를 통한 이득 경쟁		
	crosstalk특성을 이용한 공격	광/전 변환없이 검출하기가 곤란 (연속적인 BER 측정을 통한 검출)	광 증폭기 입력단에서의 전력 등화 스킴
OCh	채널 공격	광채널의 품질 테스트나 광/전 변환을 통한 검출	GMPLS 보호/복구 또는 TCP 전송 기반의 IP 복구 메커니즘
OMS	물리적인 파이버 단절	OTDR(Optical Time Domain Reflectometer)을 이용한 검출	DLP(Dedicated Line Protection), OULSR (Optical Unidirectional Line-Switched Ring), SLP(Shared Line Protection), WSHR(shared line-switched WDM Self-Healing Ring) 등의 장애 제어 메커니즘

〔표 2〕 간접적인 공격 유형과 관리 기능

구간	공격 유형	검출 메커니즘	회복 메커니즘
DS	의도적인 crosstalk를 이용한 공격	광/전 변환을 통한 검출 메커니즘	전력 등화 메커니즘
SS	의도적인 crosstalk를 이용한 공격	광/전 변환을 통한 검출 메커니즘	전력 등화 메커니즘과 dilation
	결합/분기 포트를 통한 비권한자의 정보접근	지속적인 광전력 레벨의 모니터링	논리적 레벨에서의 회복 메커니즘
MS	이전 구간에서의 의도적 공격으로 인한 crosstalk 전파	광/전 변환을 통한 검출 메커니즘	전력 등화 메커니즘

〔표 3〕 의사 공격 유형과 관리 기능

구간	공격 유형	검출 메커니즘	회복 메커니즘
TS	결합 신호로 인한 광전력 변동	광전력 모니터링	결합 포트의 차단 또는 전력 등화 메커니즘
RS	분기 포트를 통한 비권한자의 정보접근 또는 광전력 변동으로 인한 신호의 품질감쇄	검출이 곤란	분기 포트의 제한 또는 전력 등화 메커니즘

비용 또한 많이 소요된다. 광 회선분배기 내에서 발생할 수 있는 간접적 공격과 관련된 이슈는 표 2와 같이 요약된다.

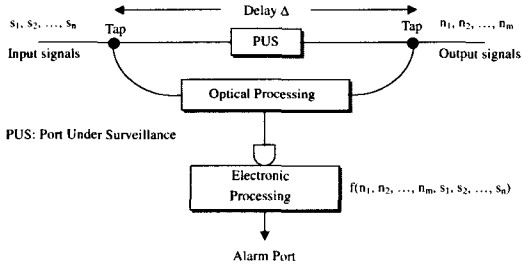
3.2.3 의사 공격(Pseudo attack)의 관리

동적 재구성이 가능한 AOTN에서의 광신호 품질은, 물리적인 망 토폴로지에 따라 달라진다. 특히 OADM에서 일부 파장이 결합/분기 될 때, 다른 파장들의 신호품질에 미소한 영향을 미치게 되고, 이 같은 예외적 현상은 공격자에 의한 침입은 아니지만, 침입 감시 알고리즘(intrusion surveillance algorithm)에 의해 공격이 이루어진 것처럼 인식될 수 있다. 이러한 현상을 의사 공격(pseudo attack)이라 부르며, 망 토폴로지를 적합하게 구현함으로써 전체 또는 부분적으로 극복이 가능한 요소로 분석된다. 표 3은 의사 공격과 관련한 관리 이슈를 요약한 것이다.

3.3 공격 검출 시스템

광소자들의 공격을 검출하기 위해 Medard[4]는

그림 4와 같은 공격검출 스킴을 제안하였다. 관측되는 장비 PUS(Port Under Surveillance)는 공격에 취약한 광소자가 되며, 입력과 출력의 탭에서 분리된 신호들은 PUS가 가지는 고유한 지연과 매칭시키기 위한 광 처리(Optical Processing) 장치와 연결된다. 이렇게 탭에 의해 생성된 새로운 경로의 신호는 전기적 처리(Electronic Processing) 장치에서 함수 $f(n_1,\cdots, n_m, s_1,\cdots, s_n)$의 전기적 신호로 변환된다. 전기적 처리 장치는 물리적인 공격을 검출하기 위해 수신된 신호들을 처리하고, 함수 $f(n_1,\cdots, n_m, s_1,\cdots, s_n)$를 어떤 형태의 파라미터에 비추어 PUS의 동작 상태를 측정하여, 출력된 f의 값에 따라 경고(alarm)의 가동 유무를 결정한다. 그러나 이 스킴은 신호 처리 함수 f의 최적화 문제가 남아있고, 특정 PUS의 공격 형태에 따른 광 처리장치와 전기적 처리장치의 신호처리에 대한 명확한 구현을 제공하지 못하는 한계를 가진다.



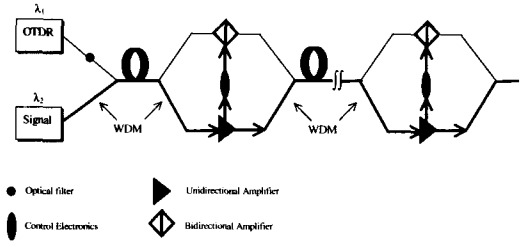
〔그림 4〕 공격 검출 스킴

공격 검출과 회복기능을 쉽게 지원하기 위해서는, 광신호로 전달된 정보를 참조하는 정보 내용의 관리(information content management)와 광전력 관리(power management)로 요약되며, 두 카테고리를 결합시킴으로써 AMS(Attack Management Surveillance)의 시스템적 돌파구를 제시할 수 있다. 따라서 AMS는 광전력 모니터링 시스템과 정보 변경 검출 시스템의 두 카테고리로 분류된다.

3.3.1 광전력 모니터링 시스템

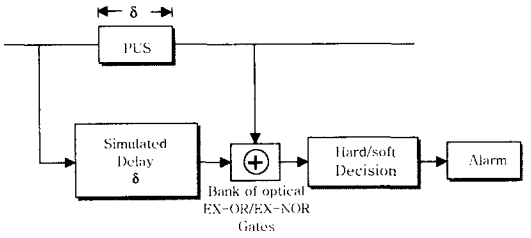
효율적인 광전력 모니터링 기술은 광소자들의 상태를 진단하는데 큰 도움을 준다. 이것은 공격으로 인한 PUS의 장애들을 진단할 수 있고, 비권한자에 의한 광신호 유출을 감지할 수 있으며, 연속적인 변경에 대한 실마리를 제공할 수 있다. 광전력 모니터링 기술은 AOTN에서 중요한 기술로 많은 연구가 있었고, 다음과 같은 모니터링 기술들이 보고된다. Matsuoka[9]는 높은 비트율 신호로 변조되는 펌프 레이저 다이오드 기술을 제안하였고, Angellieri[10]는 EDFA에서 수 백 bps의 원격신호에 의한 레이저 변조를 제안하였으며, Ellis[11]는 광 증폭기의 자연 방출(spontaneous emission) 변조를 제안하였다. 그러나 이 방식들은 개별적인 EDFA 감시는 가능하나, 파이버 절단 위치를 진단할 수 없는 단점이 있다.

위의 방식과는 다르게 증폭된 관리 신호(amplified supervisory signal)[12]나 후향 산란방식(back-scattered)의 OTDR[13]을 사용하는 방식이 보고되었으나, 반대 방향으로 경로 제공을 위한 광서큘레이터(optical circulator)의 추가적인 사용은 시스템 비용을 증대시킨다. 그리고 MacKichan[14]은 펄스 펌프 레이저(pulsed pump laser)가 탑재된 OTDR의 사용을 제안하였다. 그러나 이 방식도 거리가 먼 포트 간에 상업적인 OTDR을 사용할 수 없는 것이 단점이다. Lai[15]는 WDM OTDR 기술의 사용을 제안하였다. 이 스킴의 기본적인 원리는 그림 5과 같이 WDM 다중화기에 의해 λ_2의 전송신호와 λ_1의 OTDR 신호가 합쳐진다.



〔그림 5〕 광전력 모니터링 시스템

파이버의 절단과 모든 단 방향(아이솔레이터를 사용하기 때문에) EDFA의 상태를 모니터링하기 위해, OTDR의 파장이 입/출력 WDM에 의해서 주 EDFA를 통과 한다. 방향성 보호 광 증폭기(그림 5의 상위 증폭기)는 OTDR의 동작 범위를 증가 시키기 위해서 입/출력 WDM 사이에 삽입되고, 양방향 보호 증폭기의 펌프 레이저는 주 증폭기의 펌프 레이저가 고장을 일으켰을 때, 교체하여 사용된다. 그러므로, 이 스킴은 OTDR 신호(trace)를 사용한 광전력의 모니터링과 주 EDFA의 보호를 동시에 수행할 수 있다.



〔그림 6〕 정보 변경 검출 시스템

3.3.2 정보변경 검출 시스템

광소자에 대한 비권한자(공격자) 접근은, 잠정적으로 사용자 트래픽의 정보 내용에 접근하고, 임의로 변경할 수 있는 기회를 제공하게 된다. 그림 6과 같은 시스템을 구현함으로써 임의적인 데이터의 변경을 온라인 상에서 모니터링/검출이 가능하다.

이 스킴은 기본적으로 하나의 EX-OR 게이트 또는 EX-NOR 게이트를 비교기로 사용하며, 검출은 hard decision과 soft decision의 두 가지 형태로 동작된다. hard decision 스킴은 비교기에서 한 비트씩 비교되고, 경고 또는 정정 메커니즘은 모든 에러에서 일어난다. 그리고 Soft Decision 스킴에서는 단지 미리 결정된 수의 비트 열(128비트 혹은 1024비트 등)에서 에러가 발생할 때 경고가 동작된다. 분명한 것은 soft decision 스킴은 구현이 더 간단하다는 것이다.

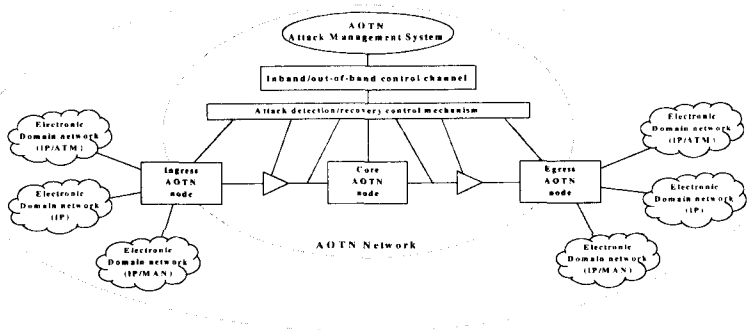
이와는 다르게 OCDMA(Optical Code Division Multiple Access) 기술을 이용함으로써 공격자의 정보 접근을 예방하는 기술도 제안되었다.[16-18] 그러나 이 기술은 높은 비트율에 적용하기 위해서 시스템의 구현이 점점 더 복잡해진다는 단점이 있다.

Ⅳ. 물리적 공격관리 시스템

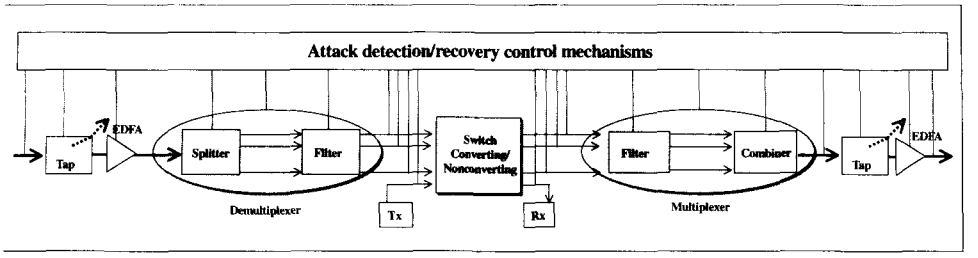
4.1 AOTN 공격관리 시스템의 구조

그림 7은 AOTN의 공격관리 시스템(Attack Management System: AMS) 구조를 나타내며, 두 개의 기능적 도메인으로 고려된다. 외부 도메인은 전기적인 제어 도메인으로서, 패킷 헤더 정보를 기반으로 라우팅(routing)과 포워딩(forwarding) 기능을 수행한다. 반면 내부 도메인은 광 제어 도메인으로서, 두 도메인의 경계면에 위치한 에지(edge) 노드는 광 소자 기술에 기초하여, 하위 계층의 스위칭 기능과 광 데이터의 전송을 위한 파장 할당 기능 등을 수행한다. 즉, 기존의 상업적인 전기 도메인들(LAN, MAN, ATM 등과 같은)의 다양한 IP 트래픽들이 Ingress 노드로 유입되고, 목적지인 Egress 노드로 광 데이터 패킷을 전달하기 위한 기본적 라우팅 기능이 수행된다. 노드를 통해 광 패킷들을 간단하게 전달하기 위해서, MPλS (Multi-Protocol Lambda Switching) 혹은 MPLS(Multi-Protocol Label Switching)를 확장한 GMPLS 기술이 에지 노드 사이에서 사용되는데, MPλS /GMPLS에서의 광 채널들은 MPLS의 레이블과 유사하다. 이렇게 조합된 광 데이터 패킷들은 소스 노드에서 코어 노드를 통해 목적지 노드로 전송된다. 목적지의 Egress 노드는 전송된 트래픽들을 엑세스망에 따라 다시 분리하고 최종 목적지로 전달된다.

그림 7에서 알 수 있듯이, 공격관리 스킴은 망 공격을 관리하기 위해 다음의 3단계의 데이터 처리과정으로 나뉜다. 첫째, 공격 검출과 회복 제어 평면(Attack Detection/Recovery Control Plane: AD/RCP)은 광 계층과 매우 가깝게 위치하며, 임



〔그림 7〕 AOTN의 공격관리 시스템 구조



〔그림 8〕 AD/RCM과 광소자들 간의 상호작용

의의 공격으로부터 적절한 회복 스킴을 제공하기 위해서 상위 단계에 침입 사실을 통지하는 기능을 담당한다. 둘째, in-band 혹은 out-of-band 제어 채널을 통해 AOTN 공격관리 커널과 AD/RCP 간의 양 방향 인터페이스를 제공한다. 그림 8은 AD/RCP에서 각 소자를 제어하기 위한 포트들과의 연결을 자세하게 나타낸다. 공격 검출/회복 제어 메커니즘(Attack Detection/Recovery Control Mechanism: AD/RCM)은 모든 광소자의 동작 조건을 모니터링하고, 광소자의 공격 조건을 검출하며, in-band/out-of-band 제어 채널을 통해 관리 시스템에게 공격 상태를 보고한다. 마지막으로, AMS는 공격 받은 소자들의 회복을 위해 시스템 제어를 담당한다.

4.2 공격관리

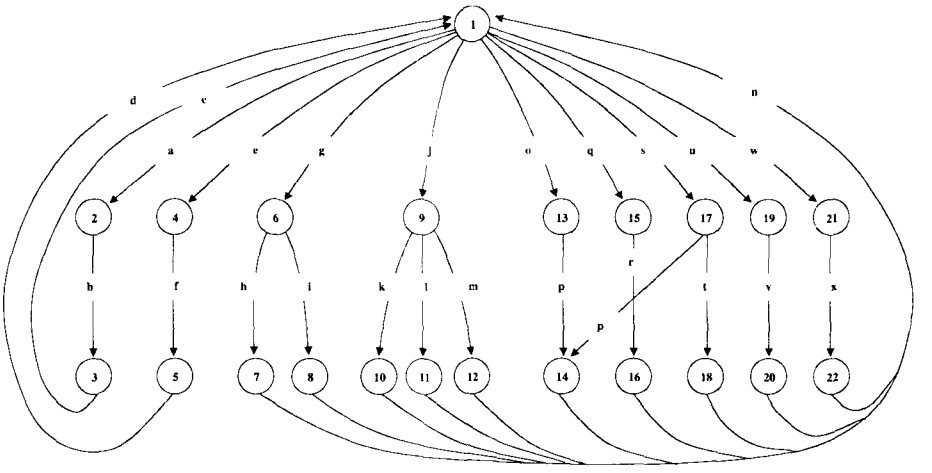
그림 7, 8과 같은 플랫폼에서, 공격관리 문제는 그림 9와 같은 입/출력 유한 상태 기계(Input/ Output Finite State Machine: I/OFSM)로 표현되며, 이 모델은 3장에서 분석된 공격 유형의 검출, 회복 스킴에 각각 대응된다. 또한 AMS와 AD/RCM 간의 공격관리를 위해 요구되는 제어 과정을 모두 고려한 것이다(공격관리 기능을 요약한 표 1, 2, 3과 표 4, 5를 참고). I/OFSM은 공격관리 대상(Attack Management Objects: AMO)에 따른 공격 시나리오를 다루고, AMO들에게서 관찰될 수 있는 특성들을 묘사하기 위한 체계적인 모델을 제공한다.

그림 9에서 주어진 I/OFSM 모델은 각 공격 문제와 관련된 9개의 중요한 상태(OCh_공격상태, OMS_공격상태, OAS_공격상태, FIS_공격상태, DS_공격상태, MS_공격상태, SS_공격상태, TS_공격상태, RS_공격상태)로 구성되며, 각 공격관리를 위한 I/OFSM 모델의 상태 천이에 대한 자세한 설명은 다음 소절에서 자세히 기술한다.

4.2.1 직접적인 공격(Direct attack)의 관리

가. OCh 공격관리 : IP/GMPLS over WDM 프레임워크는 보호/복구 절차에 따라 OMS 계층에서의 파이버 보호/복구와 OCh 계층에서의 채널 보호/복구, 그리고 IP/GMPLS 계층에서의 보호/복구의 세가지 스킴을 제공한다. 본 고에서는 공격에 의한 망 장애를 극복하기 위해서, OMS 계층의 파이버 보호/복구와 IP/GMPLS 계층에서의 채널 복구 스킴을 사용한다. 특히 CR-LDP(ConstRaint-based Label Distribution Protocol)와 RSVP-TE(Resource reSerVation Protocol-Traffic Engineering)와 같은 제어평면의 시그날링에 기반한 GMPLS 복구 스킴의 변형(그림 9의 state 3)은 OCh 공격 회복(attack recovery)에 적용된다.
검출기(detector)가 광경로 상에서 어떤 형태의 공격을 감지할 때마다, 정보화된 AMS는 광경로, 즉 λ-LSP(λ-Label Switching Path)의 연결을 해제하고 새로운 λ-LSP로 리라우팅하기 위해서 AOTN의 Ingress와 Egress 노드에 제어정보를 전달한다. 이 스킴에서 AD/RCM은 각 능동 소자의 검출/모니터링 정보를 AMS로 전달하기 위해 감시 채널(supervisory channel)을 사용한다.

나. OMS 공격관리 : 파이버 구간은 파장 당 많은 TDM 채널들로 구성되며, 높은 속도의 광신호를 전달하는 구간이다. OMS 공격 회복 스킴들은 다중화된 신호 레벨에서 동작하므로, 공격받은 구간에 존재하는 모든 광경로들에 대한 회복이 요구된다. 일반적으로 링형 망에서는 WSHR(WDM Self-Healing Ring) 기반의 SLS(Shared Line-Switched) 스킴이 사용되는데,



〔그림 9〕 I/OFSM 모델

〔표 4〕 I/OFSM 모델에서의 공격 유형별 입/출력

입/출력	식별자
OCh_공격_검출/OCh_공격처리_지시	a
IP/GMPLS_회복메커니즘_요구/IP/GMPLS_회복메커니즘_지시	b
IP/GMPLS_회복완료_통지/공격관리_초기화_요구	c
OMS_회복완료_통지/공격관리_초기화_요구	d
파이버 단절_검출/OMS_공격처리_지시	e
OMS_회복메커니즘_요구/OMS_회복메커니즘_지시	f
OAS_공격_검출/OAS_공격처리_지시	g
OAS_이득경쟁_회복메커니즘_요구/OAS_전력등화_지시 또는 OAS_광증폭기 교체_지시	h
OAS_crosstalk_회복메커니즘_요구/OAS_전력등화_지시	i
FIS_공격_검출/FIS_공격처리_지시	j
FIS_정보접근_회복메커니즘_요구/FIS_정보접근보호_지시	k
FIS_광신호 품질 저하_회복메커니즘_요구/FIS_논리적 회복메커니즘_지시	l
FIS_비권한자의 정보변경_회복메커니즘_요구/FIS_논리적 회복메커니즘_지시	m
회복완료_통지/공격관리_초기화_요구	n
DS_공격_검출/DS_공격처리_지시	o
의도적 crosstalk_회복메커니즘_요구/전력등화_지시	p
MS_공격_검출/MS_공격처리_지시	q
의도적 crosstalk 전파_회복메커니즘_요구/MS_전력등화_지시	r
SS_공격_검출/SS_공격처리_지시	s
비권한자의 정보접근_회복메커니즘_요구/논리적 레벨_회복메커니즘_지시	t
TS_공격_검출/TS_공격처리_지시	u
TS_광전력 변동_회복메커니즘_요구/TS_전력등화_지시 또는 TS_공격포트 차단_지시	v
RS_공격_검출/RS_공격처리_지시	w
RS_분기 포트를 통한 비권한자의 정보접근 또는 광전력 변동으로 인한 신호의 품질 감쇄_회복메커니즘_요구/RS_공격포트 제한_지시 또는 RS_전력등화_지시	x

(표 5) I/OFSM에서의 공격 유형별 상태

상 태	식별자
공격관리_준비상태	1
OCh_공격상태	2
OCh_IP/GMPLS_회복_처리상태	3
OMS_공격상태	4
OMS_회복_처리상태	5
OAS_공격상태	6
OAS_이득경쟁_회복_처리상태	7
OAS_crosstalk_회복_처리상태	8
FIS_공격상태	9
FIS_비권한자의 정보접근_회복_처리상태	10
FIS_광신호 품질 저하_회복_처리상태	11
FIS_비권한자의 정보변경_회복_처리상태	12
DS_공격상태	13
DS_의도적 crosstalk_회복_처리상태	14
MS_공격상태	15
MS_의도적 crosstalk 전파_회복_처리상태	16
SS_공격상태	17
SS_비권한자의 정보접근_회복_처리상태	18
TS_공격상태	19
TS_광전력 변동_회복_처리상태	20
RS_공격_상태	21
RS_분기 포트를 통한 비권한자의 정보접근 또는 광전력의 변동으로 인한 신호의 품질 감쇄_회복_처리상태	22

메쉬(mesh) 망은 여러 개의 링 집합으로 재구성하여 WSHR의 확장을 적용할 수 있다. 따라서 파이버 단절과 관련한 장애는 감시 채널을 사용한 WSHR 시그널링과 제어 스킴을 적용하여 회복된다.

다. OAS 공격관리 : 광 증폭기는 공격에 의한 파라메터의 교묘한 조작(광 증폭기의 이득 경쟁과 crosstalk를 이용한 조작)으로 성능이 좌우될 수 있기 때문에, OAS는 공격자의 손쉬운 공격 대상이 된다. 본 고에서 제시한 I/OFSM 모델에서 OAS 공격관리는, 모니터링 장비에 의해 OAS 공격이 검출되면, OAS_공격상태로 천이(입/출력 "g"를 통해 상태 1에서 상태 6으로 천이)된다. 이득 경쟁으로 인한 공격(입/출력 "h"를 통한 상태 7로 천이)은 3.2.1에서 제시한 모니터링 알고리즘을 통해 광 도메인에서 검출이 가능하지만, 의도적 crosstalk로 인한 공격(입/출력 "i"를 통한 상태 8로 천이)은 채널 간의 SNR (Signal to Noise Ratio)을 분석해야 되기 때문에, 광/전 변환이 요구된다. 그리고 AD/RCM 계층에서는 공격 포트의 위치를 검출하고, AMS는 각 공격 유형에 대응되는 회복 메커니즘을 제어하게 된다. 모든 회복 메커니즘이 완료가 되면 공격관리가 초기화(입/출력 "n"을 통해 상태 1로 천이)된다.

라. FIS 공격관리 : 광 파이버는 WDM 신호의 전송 기반으로, 공격자가 FIS에 접근한다는 것은, 직접적 공격으로 인한 서비스 파괴나 정보 유출에 심각한 위협이 된다. AD/RCM에서 FIS 공격이 검출되면, FIS_공격상태로 천이(입/출력 "j"를 통해 상태 9로 천이)되고, 각 공격 특성에 따라 탭핑과 재밍을 통한 비권한자의 정보접근, 광신호의 품질저하, 사용자 정보변경(상태 10, 11, 12)으로 분류된다. 특히 탭핑과 재밍에 의한 광신호의 변경이나 정보변경은 광전력 모니터링만으로 검출이 어렵기 때문에, 3.3.2에서 기술한 정보변

경 검출 시스템을 이용하여 검출하고, 논리적(전기적)인 레벨에서의 회복 메커니즘이 요구된다.

4.2.2 간접적인 공격(Indirect attack)의 관리

가. DS 공격관리 : 광 역다중화기는 그림 3과 같이 스플리터와 부가적으로 사용되는 광 필터로 구성된다. 특히 이 포트에서 가능한 공격 유형은 crosstalk를 이용한 간접적 침입으로, DS_공격상태로 천이(입/출력 "o"를 통해 상태 13으로 천이)되고, AD/RCM 계층은 전력 관리 스킴을 사용하여 검출과 복구를 담당(입/출력 "p"를 통해 상태 14로 천이)한다.

나. MS 공격관리 : 이전의 구간(DS와 SS)에서 공격으로 인한 crosstalk 전파는 비권한자의 침입으로 간주하여 MS_공격상태로 천이(입/출력 "q"를 통해 상태 15로 천이)된다. 그리고 전력 관리 스킴을 통해 회복(입/출력 "r"을 통해 상태 16으로 천이)된다.

다. SS 공격관리 : 광 스위치로 유입되는 채널간의 높은 crosstalk는 BER 저하와 정보 도청의 위험이 있다. 광 스위치 구간의 간접적 공격이 검출되면, SS_공격상태로 천이(입/출력 "s"를 통해 상태 17로 천이)된다. 의도적 crosstalk로 인한 서비스 파괴/품질저하일 경우, DS의 회복메커니즘과 동일하게 처리(입/출력 "p"를 통해 상태 14로 천이)되고, 결합/분기 포트를 통한 비권한자의 정보 획득이 감지될 경우 논리적 레벨의 보안(입출력 "t"를 통해 상태 18로 천이)이 요구된다.

4.2.3 의사 공격(Pseudo attack)의 관리

가. TS 공격관리 : AOTN에서는 광신호의 전력 변동으로 인한 시스템 성능 저하가 발생하는데, 이로인해 TS 구간에서 삽입되는 채널의 전력 조절이 요구된다. 전력 관리 스킴은 전력의 변동을 검출하고, 삽입되는 채널의 전력 레벨을 임계치 이하로 유지한다. 이 구간에서 검출되는 의사 공격은 전력 관리 또는 결합 포트의 차단(입/출력 "u", "v"에 의해 상태 19와 20으로 천이)으로 회복된다.

나. RS 공격관리 : 특정 RS에서 의도되지 않은 정보 접근은 침입 감시 알고리즘에 의해 의사 공격으로 검출되며, 전력 관리 또는 분기 포트를 제한(입/출력 "w", "x"를 통해 상태 21, 22로 천이)함으로써 회복된다.

V. 결 론

광신호는 AOTN의 다양한 손실요인에 의해 감쇄와 왜곡을 경험한다. 특히 전송매체나 광소자의 고유한 특성들은 비양심적 공격자로부터 공격 가능성을 제공하게되고, AOTN의 투명한 데이터 전달 특성으로 인한 새로운 검출 및 회복 스킴이 요구된다. 본 고에서는 분류된 direct, indirect, pseudo 공격에 기초하여 공격 유형별 검출/회복 메커니즘과 검출 시스템, 그리고 IP/GMPLS over WDM에 기반한 AMS의 개념적 모델과 동작을 정의하여 물리적 공격에 대한 생존성 보장의 대안을 기술하였다. 그러나 차세대 광 인터넷 백본망에서 보안 취약성 해결하기 위해서는 AOTN의 기본적인 모델 연구와 광소자 및 구현 기술 연구가 요구되며, 이를 바탕으로 한 물리적 장치들의 보안 취약성을 분석하고 체계적인 검출 스킴과 회복을 위한 제어 프로토콜의 지속적인 연구가 요구된다.

참 고 문 헌

[1] Jigesh K. Patel, Sung-Un. Kim, David H. Su, "Modeling Attack Problems and Protection Schemes for All-Optical Transport Networks", *Optical Network Magazine*, vol 3, no 4, July/August, 2002.

[2] J.P. Hazan,; M. Steers; G. Delmas; J. L.Nagel, "Buried Optical Fibre Pressure Sensor for Intrusion Detection", *Proceedings of 1989 International Carnahan Conference on Security Technology*, pp. 149-154, 1989.

[3] B. Griffiths, "Developments in and Applications of Fibre Optic Intrusion Detection Sensors", *Proceedings of 29th Annual 1995 International Carnahan Conference on Security Technology*, Institute of Electrical and Electronics Security

Technology, pp. 325-330, 1995.

[4] M. Medard, R. Chinn, Saengudomlert, "Attack Detection in All-Optical Networks", *Technical Digest of Optical Fiber Conference (OFC)*, pp. 272-273, 1998.

[5] R. Ramaswami, P. A. Humblet, "Amplifier Induced Crosstalk in Multichannel Optical Networks", *IEEE Journal of Lightwave Technology*, vol. 8, no. 12, pp. 1882-1896, Dec 1990.

[6] E. Desurvire, "Erbium-Doped Fiber Amplifiers: Principles and Applications", *John Wiley & Sons*, NY, 1994.

[7] J. Zhou, R. Cadeddu, E. Casaccia,C. Cavazzoni, and M. J. O'Mahony, "Crosstalk in Multiwavelength Optical Cross-Connect Networks", *IEEE Journal of Lightwave Technology*, vol. 14, no. 6, pp. 1423-1435, June 1996.

[8] L. Gillner, C. P. Larsen, and M. Gustavsson," Scalability of Optical Multiwavelength Networks: Crosstalk Analysis", *IEEE Journal of Lightwave Technology*, vol. 17, no. 1, pp. 58-67, Jan 1999.

[9] S. Matsuoka, Y. Yamabayashi, and K. Aida, "Supervisory Signal Transmission Methods for Optical Amplifier Repeater Systems," *Technical Digest, GLOBECOM*, pp. 903.2.

[10] M. Angellieri, et al., "Low bit-rate Service Channel for Remote Monitoring of EDFA in-line Repeaters Obtained by Modulation of the Active Fiber Gain," *Technical Digest, Optical Amplifiers and Their Applications*, pp. THA3.

[11] A. D. Ellis, W. A. Stallard, and D. J. Maylon, "Supervisory System for Cascaded Semiconductor Laser Amplifier Repeaters," *Electronics Letters*, vol. 25, pp. 309-311, 1989.

[12] Y. Sato, Y. Yamabayashi, and K. Aoyama, "Supervisory Channel Using Fiber Brillouin Amplifiers for Er-doped Fiber Amplifier Transmission Systems," *Technical Digest, Optical Amplifiers and Their Applications*, pp. THA2, 1992.

[13] Y. Sato and K. Aoyama, "Optical Time Domain Reflectometry in Optical Transmission Lines Containing in-line Er-Doped Fiber Amplifiers," *IEEE Journal of Lightwave Technology*, vol. 10, no. 1, pp. 78-83, Jan 1992.

[14] J. C. MacKichan, J. A. Kitchen, and C. W. Pitt., "Innovative Approach to Interspan Fiber Break Location in Fiber Amplifier Repeatered Communication Systems," *Electronics Letters*, vol. 28, pp. 626-628, 1992.

[15] Y. W. Lai, Y. K. Chen, and W. I. Way, "Novel Supervisory Technique Using Wavelength Division Multiplexed OTDR in EDFA Repeatered Transmission Systems," *IEEE Photonics Technology Letters*, vol. 6, no. 3, pp. 446-449, Mar 1994.

[16] D. Benhaddou, Al-Fuqaha, and G. chaudhry, "New Multiprotocol WDM/CDMA-based Optical Switch Architecture", *Proceedings of 34th Annual Simulation Symposium*, pp.285-291, 2001.

[17] J. Wu, and C. L. Lin, "Fiber-Optic Code Division Add-Drop Multiplexers", *IEEE Journal of Lightwave Technology*, vol.18, no.6, pp.819-824, June 2000.

[18] P. R. Prucnal, M. A. Santoro, and T. R Fan, "Spread Spectrum Fiber-Optic Local Area Network Using Optical Processing", *IEEE Journal of Lightwave Technology*, vol. LT-4, no. 5, pp. 547-554, May 1986.

[19] 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.

〈著 者 紹 介〉

김 성 운 (Kim Sung-Un)

1982년 12월~1985년 9월 : 한국전자통신연구원, 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
관심분야 : DWDM optical network, RWA, QoS, GMPLS, protocol engineering

신 주 동 (Shin Ju-Dong)

2001년 2월 : 부경대학교 정보통신공학과(공학사)
2001년 3월~현재 : 부경대학교 정보통신공학과 석사과정
관심분야 : DWDM optical network, Optical network security, GMPLS

한 종 욱 (Han Jong-Wook)

1989년 2월 : 광운대학교 전자공학과(공학사)
1991년 2월 : 광운대학교 대학원 전자공학과(공학석사)
2001년 2월 : 광운대학교 대학원 전자공학과(공학박사)
1991년~현재 : 한국전자통신연구원 정보보호연구본부 선임연구원
관심분야 : Optical security, Network security