광전달망 계층 암호화 기술 표준화 동향

윤지욱 한국전자통신연구원 광네트워크연구실 책임연구원

1. 머리말

광전달망 계층 암호화 기술은 OTN(Optical Transport Network)을 통해 전송되는 데이터의 기밀성(Encryption)과 신뢰성(Authentication)을 보장해주는 기술이다. 현재 ITU-T SG15에서 표준기술을 개발하고 있다. 해당 기술은 기존 네트워크 계층 암호화 기술인 IPsec 기술, 데이터 링크 계층 암호화 기술인 MACsec 기술과 비교해 높은 데이터 처리율과 매우 낮은 지연시간을 제공한다. 또한 IP 패킷과 이더넷 프레임 외에도 FC, SONET/SDH, Infiniband 등 다양한 클라이언트 신호를 동시에 수용할 수 있다는 장점을 가진다. 이러한 장점을 바탕으로, 광전달망 계층 암호화 기술은 '외부 해킹에 민감하면서도 대용량 또는 저지연 특성이 요구되는 서비스'를 제공하기 위한 요소기술로 주목받고 있다. 주된 활용 분야로는 5G 기반 대용량 실감 서비스, 자율주행, 주식거래 등이 꼽힌다.

광전달망 계층 암호화 기술은 크게 ITU-T G.709 표준[1] 기반 OTN 프레임을 사용하는 OTNsec(OTN security) 암호화 기술, 그리고 ITU-T G.709.1 표준[2] 기반 Flexible OTN 프레임을 사용하는 FlexOsec(Flexible OTN security) 암호화 기술로 구분된다.

이번 원고에선 광전달망 계층에서의 암호화 기술을 제공하기 위한 세부적인 오버헤드 규격이 제정된, FlexOsec 암호화 기술을 중심으로 고찰해 본다.

2. OTNsec 암호화 기술

2.1 표준화 동향

OTNsec을 구현하기 위해 사용되는 암호화 정보는 ODUk 오버헤드를 통해 전송되며, 세부적인 오버헤드 규격은 OTNsec을 지원하는 벤더 자체 규격을 따른다[3]. <표 1>은 OTN 프레이머 칩 또는 OTN 전송/스위칭 장치를 생산하는 국내외 주요 업체들이 제안하고 있는 OTNsec 규격을 보여준다. 현재 OTN 프레이머 칩 형태로 상용화된 제품은 마이크로칩(Microchip)과 아카시아(Acacia) 두 업체가 제공하고 있다.

국내 업체에선 상용 OTN 프레이머 칩을 기반으로 FPGA를 이용한 자체 솔루션을 개발해 자사 제품에 적용하고 있다. 이들 솔루션들은 국내 환경에 맞게 AES-256(Advanced Encryption Standard)과

<표 1> 국내외 주요 업체별 OTNsec 제안 방식

업체	암호화 계층	SFH 오버헤드	프레임 형태	SFC 오버헤드	프레임 형태	기타
Microchip (Microsemi)	ODUk, ODUCn	PSI (MFAS[251:255])	256-다중 프레임	ODUk 오버헤드 8/16바이트	단일 프레임 또는 2-다중 프레임	30-비트 크기의 Life cycle
Acacia	ODUk, ODUCn	ODUk 오버헤드와 MFAS	2-다중 프레임	ODUk 오버헤드 16바이트	단일 프레임	MFAS 비트 "0"을 SFH indicator로 사용
Huawei	ODUk, ODUCn	ODUk 오버헤드	4/8/16-다중 프레임	ODUk 오버헤드	4/8/16-다중 프레임	SFH와 SFC를 동일한 ODUk 오버헤드를 이용해 전송
우리넷	ODUk, ODUCn	PSI (MFAS[251:255])	256-다중 프레임	ODUk 오버헤드 8/16바이트	단일 프레임 또는 2-다중 프레임	Microsemi 칩을 기반으로 국내시장에 맞게 변경
코위버	ODUk, ODUCn	ODUk 오버헤드와 MFAS	2-다중 프레임	ODUk 오버헤드 16바이트	단일 프레임	Acacia 칩을 기반으로 국내시장에 맞게 변경

출처: 한국전자통신연구원 자체 작성

<표 2> 광전달망에서의 보안 애플리케이션

애플리케이션 종류	상세 분류
Client end to end security	Client end to end security with CPE
	Client end to end security without CPE
	DC, content or mobile service provider client end to end security
Service provider CPE end to end security	Service provider CPE end to end security
OTN link/span security	OTN link/span security
	OTN link/span leased fiber security
OTN second operator security	OTN leased service security
Access link/span security	Client access link/span security
OTN end to end security	OTN end to end security with CPE
	OTN end to end security without CPE
	DC, content or mobile service provider OTN end to end security
Service provider path end to end security	Service provider path end to end security

출처: ITU-T, 'Optical transport network security,' G.Suppl.76, 2021. 문서를 기반으로 한국전자통신연구원 자체 작성

LEA-256(Lightweight Encryption Algorithm) 암호화 알고리즘을 지원한다. OTNsec 암호화 기술을 규정하고 있는 ITU-T G.Suppl.76 표준은 OTN 계층(ODUk, ODUCn, FlexO)에서 클라이언트 데이터의 기밀성과 신뢰성을 보장하기 위한 다양한 애플리케이션과 사용 사례만을 규정하고 있다. 다만 별도의 암호화 알고리즘은 정의하지 않고 상용 알고리즘 사용을 권고한다[4].

국외에선 주로 NIST(미국 국립표준기술연구소, National Institute of Standards and Technology)가 개발한 대칭 키 암호화 표준인 AES 알고리즘을 사용한다. 국내에선 AES 알고리즘과 함께 LEA 알고리즘 또는 ARIA(Academy, Research Institute, Agency) 알고리즘을 사용한다. 암호화 운영 모드는 기밀성과 무결성을 동시에 제공하는 GCM(Galois Counter Mode) 또는 CCM(Counter with CBC-MAC)을 사용한다. <표 2>는 G.Suppl.76 표준에서 정의하고 있는 광전달망에서의 보안 애플리케이션 종류를 보여준다.

3. FlexOsec 암호화 기술

3.1 표준화 동향

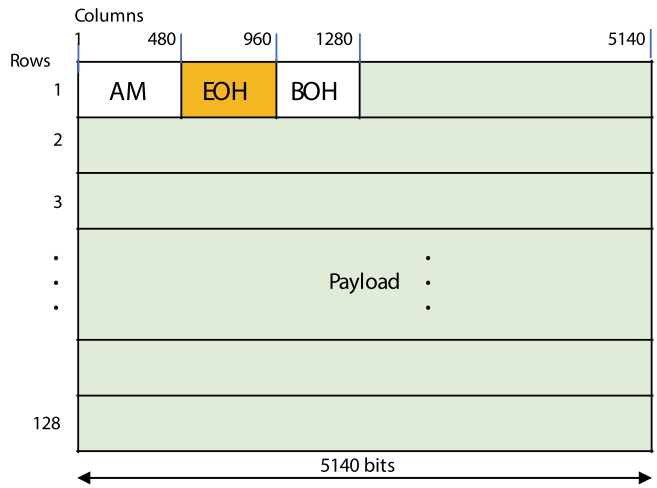
FlexOsec 암호화 기술은 광섬유나 보안성을 제공하지 않는 단-대-단 광라인 시스템 또는 광네트워크로 연결된 FlexO(Flexible OTN) 인터페이

스 양단 간 보안 통신을 제공하기 위해 사용되며, FlexO 프레임의 암호화와 인증 기능을 제공한다. FlexOsec 암호화 기술은 ITU-T G.709.1 표준에서 규정하고 있다. FlexOsec 기능을 구현하기 위한 암호화 정보는 [그림 1]의 FlexO 프레임 오버헤드 중 EOH(Extended Overhead) 영역을 통해 전송된다. FlexO 프레임 오버헤드는 총 1,280비트로 구성되며, 이들 오버헤드 중 480비트 크기의 EOH 영역을 암호화 및 인증에 사용한다.

EOH 영역을 필드별로 자세히 살펴보면 [그림 2]와 같다. EOH 영역은 크게 FlexOfec(Flexible OTN forward error correction) 오버헤드, Regen(Regeneration) 오버헤드, FlexOsec 오버헤드로 구성된다.

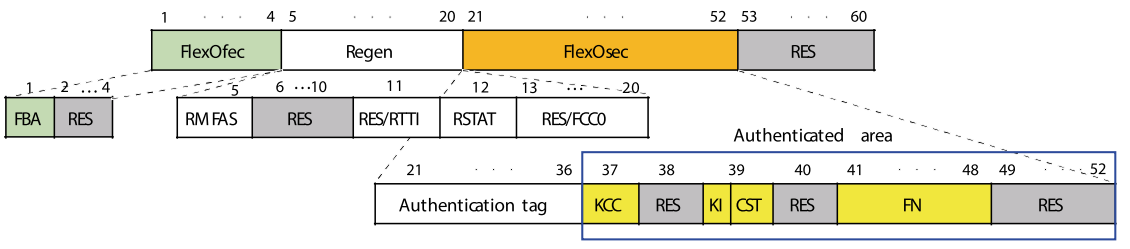
FlexOfec 오버헤드는 FBA(FEC Block Alignment)와 RES(Reserved)로 구성된다. FlexO 표준은 400Gb/s 이상의 고속신호 전송을 위한 표준으로 G.709.3에서 정의하고 있는 SC-FEC(StairCase FEC)를 사용한다[5].

Regen 오버헤드는 FlexO regeneration 기능에 사용되며, RMFAS(Regen Muti-Frame Alignment Signal), RTTI(Regen Trail Trace Identifier), RSTAT(Regen Status), FCC0(FlexO Regen Communication Channel)로 구성된다. FlexO 인스턴스가 총 n개로 구성될 경우, RTTI와 FCC0는 첫 번째 인스턴스에만 존재하고 다른 인스턴스에서



출처: ITU-T, "Flexible OTN common elements," G.709.1 (03/2024), 2024.

[그림 1] Flexible OTN 프레임 구조



출처: ITU-T, "Flexible OTN common elements," G.709.1 (03/2024), 2024. 문서를 기반으로 한국전자통신연구원 자체 제작

[그림 2] Extended Overhead 구조

<표 3> FlexOsec에서 정의하고 있는 CST값

CST bits[1:6]	설명
000000	No source FlexOsec
000001	GCM-AES-256 FlexOsec without OH encryption
000010-110111	Code-points reserved for future standardized cryptographic cipher suites for use with FlexO
111000-111110	Reserved codes for proprietary use
111111	Reserved for future maintenance signal

출처: ITU-T, "Flexible OTN common elements," G.709.1 (03/2024), 2024.

는 해당 비트를 RES로 처리한다.

FlexOsec 오버헤드는 AT(Authentication tag), Authenticated 영역으로 구성되며, FlexO 프레임에 적용되는 8개의 다중 프레임을 사용하지 않고 단일 프레임으로 동작한다. AT는 비트 단위 FlexO 프레임의 무결성 전송을 보장하기 위해 사용되는 영역이다. 이는 KI(Key Index), CST(Cipher Suite Type), FN(Frame Number)값을 이용해 BOH(Basic OverHead), EOH 일부 영역(769~960비트) 및 페이로드 전 영역에 대해 FlexO 인스턴스별로 계산된다. 생성된 AT값은 해당하는 프레임의 다음 프레임에 삽입돼 전송된다.

FlexOsec 암호화 기능을 위해 새롭게 정의된 Authenticated 영역은 KCC(Key exchange Communication Channel), KI, CST, FN으로 구성된다. 이 중 KCC 사용은 선택사항으로서, FlexOsec 인터페이스 양 종단 간 벤더, 운용자 또는 유저별로 정의된 key 합의 프로토콜을 인-밴드 방식으로 교환하기 위한 것이다.

KI는 FlexOsec 인터페이스 양 종단에서 동일한 key값을 가지도록 조율하는 인-밴드 메커니즘에 사용된다. KI값은 소스에서 key change 또는 key roll 이벤트가 발생할 때마다 1씩 증가한다.

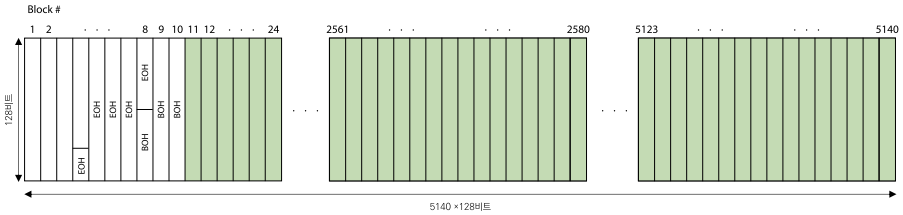
FlexOsec 오버헤드 기능은 단일 프레임으로 동작한다. 이 때문에 4개의 다중 프레임으로 동작하는 FlexOsec 프레임이 연속하는 4개의 FlexOsec 프레임을 전송하는 동안, KI값은 늘어나지 않고 이전 값을 유지한다. 이후, FN[63, 64] = "00"인 FlexO 다중 프레임 경계에서 KI값을 "1"씩 증가시킨다.

CST는 향후 FlexOsec 암호화 기술이 널리 사용될 경우, 벤더별 또는 애플리케이션별로 사용되는 다양한 암호화 알고리즘들을 구분하기 위해 사용되는 값이다. 현재는 GCM-AES-256(Galois/Counter Mode-Advanced Encryption Standard) 알고리즘만 정의돼 있다. <표 3>은 FlexOsec에서 정의하고 있는 CST값을 보여준다.

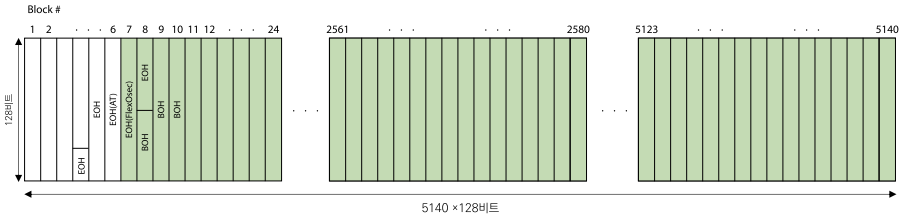
FN은 FlexOsec 인터페이스 양 종단에 있는 Invocation 카운터값 동기화에 사용된다. FN값은 매 FlexO 프레임마다 "1"씩 증가하며, key값이 변경될 경우 "0"으로 초기화된다.

3.2 암호화 알고리즘

현재 FlexOsec 암호화 및 인증에는 GCM-AES-256 FlexOsec 알고리즘이 사용되고 있다. n개의 FlexO 인스턴스로 구성된 FlexO 프레임에 대한 암호화는 FEC 정합 및 FlexO-x 인터페이스 인터리빙 이전에 FlexO 인스턴스별로 수행되며, [그림 3]의 (a)와 같이 FlexO 프레임의 AM(Alignment Marker), EOH 오버헤드, BOH 오버헤드를 제외한 페이로드 전 영역에 걸쳐 수행된다.



(a) FlexO 프레임 암호화 영역



(b) FlexO 프레임 인증 영역

출처: ITU-T, "Flexible OTN common elements," G.709.1 (03/2024), 2024.

[그림 3] 128비트 형태의 FlexO 프레임

FlexOsec 인증은 FlexO 프레임이 FlexOsec 인터페이스를 통해 전송되기 직전 수행되며, [그림 3]의 (b)와 같이 EOH 오버헤드 일부분(769~960비트)과 BOH 오버헤드 및 페이로드 전 영역에 걸쳐 수행된다.

4. 맺음말

이번 원고에선 광전달망 계층에서의 암호화 기술 표준화가 어떻게 진행되고 있는지 고찰해 봤다. 시장에 출시되고 있는 광전달망 장비들은 대부분 OTNsec 암호화 기능을 제공하고 있으나, 공통된 표준규격이 없어 타사 장비와의 연동에 잠재적 문제점을 갖고 있다. 현재 클라우드 서비스 활성화와 AI의 눈부신 발전으로 인해 실시간 대용량 서비스 수요가 빠르게 늘어나고 있다. 이에 적합한 FlexOsec 암호화 기술에 대한 요구 역시 증가하고 있다. FlexOsec 암호화 기술은 현재 ITU-T G.709.1 문서를 기반으로 구체적인 오버헤드 규격에 대한 합의가 이뤄진 상태다. 향후 산업계를 중심으로 상용 시스템 적용이 예측된다.

※ 본 연구는 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행됨(No. 2019-0-00002, 광 클라우드 네트워킹 핵심기술 개발).

참고문헌

[1] ITU-T, 'Interfaces for the optical transport network Amendment 3,' G.709/Y.1331 (2020) Amd.3 (03/2024), 2024.
[2] ITU-T, 'Flexible OTN common elements,' G.709.1 (03/2024), 2024.
[3] ICNF, '광전달망 계층 암호화 표준 기술 동향,' 산업융합네트워크포럼 표준기술 동향 분석서, 2020.
[4] ITU-T, 'Optical transport network security,' G.Suppl.76 (12/2021), 2021.
[5] ITU-T, 'Flexible B100G long-reach interfaces,' G.709.3 (03/2024), 2024.