EPON MAC 계층의 안전한 데이터 전송을 위한 인증 및 키관리 프로토콜

정회원 강 인 곤*, 이 도 훈*, 이 봉 주**, 김 영 천***

An Authentication and Key Management Protocol for Secure Data Exchange in EPON MAC Layer

In-kon Kang*, Do-hoon Lee*, Bong-ju Lee**, Young-chon Kim*** *Regular Members*

요 약

IEEE 802.3ah에서 표준화가 진행되고 있는 EPON은 하나의 OLT와 다수의 ONU가 수동소자에 의해 트리 구조로 연결되므로 도청, 위장, 가용성 등의 보안 위협을 포함한다. 본 논문에서는 EPON에서 보안 위협으로부터 망을 보호하고 안전한 데이터 전송을 보장하기 위하여 MAC 계층에서 인증 및 비밀성 서비스를 제공하는 보안 프로토콜을 설계하였다. 설계된 보안 프로토콜은 효율적인 키관리를 위하여 공개키 기반 인증 및 키관리 프로토콜을 이용하며, 비밀성 서비스를 위하여 최근 표준화된 AES의 Rijndael 알고리즘을 채택하였다. 제안된 인증 및 키관리 프로토콜은 인증과 공개키 교환을 동시에 수행하며, 공개 난수를 전송하여 공통의 암호키를 생성하는 안전한 프로토콜이다. 키관리의 구현을 위하여 인증 및 공개키 교환 절차, 세션키 변경 절차, 키복구 절차 등을 제안하였다. 제안된 프로토콜을 검증하기 위하여 알려진 세션키, 전향적 비밀성, 마지키 공유, 키손상 위장 등의 안전성을 분석하였다.

ABSTRACT

An EPON which is going on standardization in IEEE 802.3ah, is tree topology consists of a OLT and multiple ONU using passive optical components, so this network is susceptible to variable security threats - eavesdropping, masquerading, denial of service and so on. In this paper, we design a security protocol supporting authentication and confidentiality services in MAC layer in order to prevent these security threats and to guarantee secure data exchange The designed security protocol introduce public-key based authentication and key management protocols for efficient key management, and choose Rijndael algorithm, which is recent standard of AES, to provide the confidentiality of EPON Proposed authentication and key management protocols perform authentication and public-key exchange at a time, and are secure protocols using derived common cipher key by exchanging public random number To implement the designed security protocol, we propose the procedures of authentication and public-key exchange, session key update, key recovery. This proposed protocol is verified using unknown session key, forward secrecy, unknown key-share, key-compromise impersonation

I. 서 론

최근 HDTV, 화상 회의 등 사용자의 멀티미디어 서비스의 수요가 증가함에 따라 고속 기간망과 사용자 사이에 고도화된 FTTH(Fiber-To-The-Home) 구축이 절실히 요구된다. 이러한 요구를 경제적으로 수용하기 위하여 PON(Passive Optical Network)에 대한 연구가 활발하게 진행되고 있다. PON은 송신

* 국가보안기술연구소(firefly@etri.re.kr, dohoon@etri.re.kr), ** 전북대학교 영상공학과 (bjlee@networks.chonbuk.ac.kr),
*** 전북대학교 컴퓨터공학과 (yckim@moak.chonbuk.ac.kr)
논문번호 020280-0619, 접수일자 2002년 6월 19일

측과 수신측 사이에 수동소자로 구성된 점대다점(point-to-multipoint) 광전송망이다 PON은 초고속 기간망에 연결되는 OLT(Optical Line Termination)와 가입자망에 연결되는 ONU (Optical Network Unit)로 구성되며, OLT는 다수의 ONU가 하나의 광섬유를 통해 공유하는 트리구조를 갖는다[1,2,3].

PON을 기반으로 한 고속 가입자망은 APON (ATM over PON)과 EPON (Ethernet PON)에 대한 연구가 가장 활발하게 진행되고 있으며, APON은 유럽의 통신사업자들의 모임인 FSAN(Full Service Access Network)에 의해 소개된 이후 ITU-T G.983 시리즈로 표준화되었다 그러나 IP 기술의 발달으로 인터넷 트래픽의 95%가 이더넷 프레임으로 통해 전달되고 이더넷의 고속 전송기술의 발달로 기가급 으로 증가함에 따라 APON을 가입자망으로 채택할 경우 IP와 ATM 프로토콜 변환에 따른 오버헤드, 상대적으로 낮은 대역폭, IP 기반의 다양한 서비스를 수용하지 못하는 문제점이 야기된다. 이러한 문제점을 해결하기 위하여 기존의 이더넷 기반구조를 수용하면서 기가비트 이상의 고속 가입자망을 경제적으로 구축할 수 있는 EPON에 대한 논의가 활발하게 진행중이며, IEEE의 802.3 EFM(Ethernet in the First Mile) SSG에서 2003년 9월을 목표로 표준화를 추진하고있다[2,3,4]

EPON은 하나의 OLT에 16~32개의 ONU가 수동소자를 이용하여 트리구조를 갖는다 이 구조에서는 OLT에서 ONU로 전송되는 하향스트림은 수동소자에 의해 분배되므로 모든 ONU에 브로드캐스트되고, 각 ONU에서는 필터를 통하여 자신의 ID와 일치하는 프레임만 받아들인다 상향스트림은 다수의 ONU들이 시간을 공유하여 데이터를 전송한다 하향스트림의 경우에는 전송되는 스트림이 모든 ONU에 도착하므로 데이터의 도청, 위장, 서비스 거부 공격 등의 보안 위협이 존재한다. 이러한 보안상의 문제점을 해결하기 위하여 EPON에서의 인증, 데이터의 암호화, 키관리 프로토콜 등의 보안 서비스가 요구된다.

본 논문에서는 EPON에서 요구되는 보안서비스를 식별하기 위하여 EPON의 구조적인 보안 위협을 분석하였으며, EPON에 적합한 보안서비스를 구현하기 위하여 필요한 암호 알고리즘의 선택을 위한 분석, 인증 및 키관리 프로토콜을 제안하였다.

암호 알고리즘은 기가비트 이상을 전송하는 고속의 기간통신망에 사용될 수 있도록 고속 암복호 속도와 구현이 간단한 비밀키 알고리즘이 선택되어야 한다. 기존의 미국 국가의 표준으로 채택되어 널리 통용되던 DES는 1998년을 기점으로 표준 사용 기한이 만료되었고, Triple DES는 2003년으로 만료될 예정이므로 2003년에 표준화를 목표로 진행하고 있는 EPON에 사용하기에는 부적합하다 따라서 2001년에 표준화가 완료된 AES의 알고리즘을 채택하는 것이 효율적이고 안전하다. AES의 알고리즘은 DES와 같은 블록 알고리즘으로서 2000년 10월에 Rijndael 알고리즘으로 채택되었고 128비트의 블록 길이와 128, 192, 256 비트의 키 길이를 지정할 수 있다. 따라서 암호 알고리즘의 선택을 위하여 AES를 EPON 시스템에 적용 가능한지를 분석하는 것에 대한 연구와 암호 또는 복호에 사용되는 동일한 키의 생성, 키 동기 메카니즘, 키복구 알고리즘 등에 대한 연구가 반드시 필요하다

EPON에서 하나의 OLT와 다수의 ONU가 암복호 통신으로 안전하게 데이터를 전송하기 위해서는 상호간의 인증 절차를 통한 인증 프로토콜이 요구된다. 또한, 공통키를 유도하기 위한 공개키 기반의 안전한 메카니즘, 인증서와 공개키를 공유하기 위한 절차, 세션 중에 새로운 암복호 키로 갱신하기 위한 키교환 절차, 세션키가 손상되어 암복호 동기가 일치하지 않을 경우 새로운 키로 복구하기 위한 절차도 반드시 요구된다. 본 논문에서는 EPON 시스템의 MAC 계층에서 안전한 데이터 통신을 보장하기 위하여 요구되는 인증 및 키관리 프로토콜을 제안하였으며, 제안된 프로토콜의 안전성을 검증하기 위하여 알려진 세션키, 전향적 비밀성, 미지키 공유, 키손상 위장 등의 안전성 분석을 실시하였다.

본 논문의 구성은 1장 서론에 이어, 2장에서는 EPON의 구조에 대한 소개와 구조에서 포함할 수 있는 보안 위협을 분석하고 이에 대한 보안서비스를 도출하였다. 3장에서는 AES의 표준 알고리즘으로 채택된 Rijndael 알고리즘에 대하여 기술하였으며, EPON에서 이 알고리즘의 적용 가능성 분석을 실시하였다. 4장에서는 인증 및 키관리 프로토콜에 대하여 제안하였고 제안된 프로토콜에 대한 안전성 분석을 실시하였다 마지막으로 5장에서는 결론을 기술하였다.

Ⅱ. EPON 시스템의 보안요구사항 분석

본 장에서는 EPON의 구조에 대하여 기술하고, EPON 구조에서의 가능한 보안 위협에 대하여 보안서비스의 요구조건에 대하여 논의하였다.

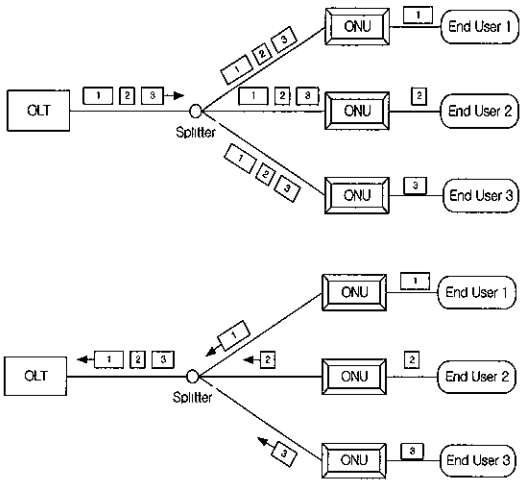


그림 1 EPON 시스템의 상향 및 하향스트림

1. EPON 시스템의 구조

PON은 하나의 OLT와 다수의 ONU가 트리구조 형태로 구성되며, OLT와 ONU 사이에는 광섬유와 수동소자인 분배기(splitter) 및 결합기(coupler)로 구성된다[4] 그림 1에는 EPON 구조에서 상향스트림(upstream)과 하향스트림(downstream)을 나타내었다

그림 1에 나타난 것처럼 EPON은 기간망에 연결되는 하나의 OLT와 가입자망에 연결되는 최대 32개의 ONU로 구성된다 OLT에서 ONU로 전송되는 하향스트림은 수동 분배기에 의해서 모든 ONU에 전송되며, 각 ONU는 필터를 통하여 수신지가 자신의 주소와 동일한 프레임을 수신한다 ONU에서 OLT로 전송되는 상향스트림은 광매체를 공유하므로 MAC(Media Access Control) 스케줄링 알고리즘에 의하여 시간을 분할하여 프레임을 전송한다. EPON의 구조를 제공하는 계층 모델(layer model)은 그림 2와 같다

EPON은 그림 2에서 나타난 것처럼 Ethernet

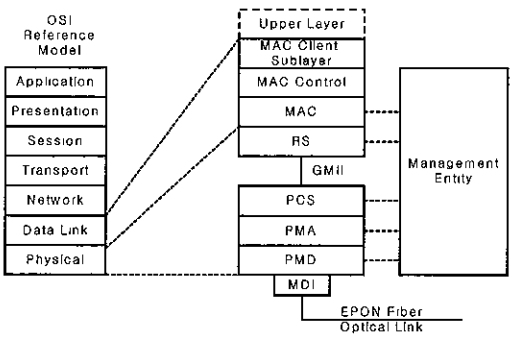


그림 2 EPON 계층 모델

CSMA/CD와 마찬가지로, 계층 2까지 만을 포함한다. 물리계층은 PMD(Physical Medium Dependent), PMA (Physical Medium Attachment), PCS (Physical Coding Sublayer), RS (Reconciliation)을 포함하며, MAC 계층에서 보내는 프레임을 광섬유를 통해 전송하고 흐름제어나 8B/10B 코딩 등의 역할을 수행한다. 데이터 링크 계층은 MAC (Media Access Control), MAC Control, MAC 서브계층을 포함하며, OLT와 ONU와의 통신 채널을 설정하거나 ONU의 매체접근제어 또는 대역할당하는 기능을 수행한다.

2 EPON의 보안 위협 분석

EPON은 IP 기반에서 제공되는 다양한 서비스를 수용하므로 음성, 비디오, 데이터 등의 다양한 형태의 정보가 전송된다 이러한 정보는 초고속 가입자망을 이용하는 개인, 기업, 은행, 정부 등에서 전송되는 중요한 정보가 포함될 것이 예상되므로 전송정보에 대한 필수적인 보안이 요구된다 이러한 요구를 만족하는 보안서비스를 제공하기 위하여 가장 먼저 EPON의 구조에 포함된 보안 위협을 분석하여야 한다

EPON의 보안 위협은 다른 전송망과 같이 비밀성, 무결성, 가용성을 저해하는 정보의 도청, 위장, 서비스 거부 등과 같은 보안위협이 존재한다 각각의 위협은 EPON 구조의 보안 취약점에 기인한 것으로 다음과 같다

1) 정보의 도청 위협(Eavesdropping) 전송 매체를 공유하는 EPON의 구조에서는 하향스트림 또는 상향스트림에 대한 도청의 위협이 존재한다. OLT에서 ONU로 전송되는 하향스트림은 수동소자인 분배기에 의해 모든 ONU에 도달되고, 각 ONU에서 필터에 의해 자신의 ONU ID와 일치하는 수신지를 갖는 프레임만을 수신하게 된다. 만약 임의의 ONU가 무조건모드(promiscuous mode)로 설정되어 있거나 수신 필터의 ID 테이블을 조작하여 다른 ONU의 ID로 설정해 놓는다면 OLT의 전송의 도와는 상관없이 두 개 이상의 ONU에서 같은 프레임을 수신할 수 있다 상향스트림은 하향스트림과 달리 구조적의 보안 취약점은 없으므로 도청을 수행하기는 어렵다 그러나 망의 토폴로지에 따라 상향스트림의 반향파장(reflected wavelength)을 수신하거나 수동소자인 결합기에 비인가된 접속을 통해 불법적인

도청이 가능하다.

2) 위장 위협(Impersonation) · EPON은 OLT와 ONU 사이의 데이터 전송을 위하여 초기에 등록(initial registration) 과정을 수행한다. 등록은 OLT에서 ONU를 탐색(discovery)하고 탐색된 ONU에 대하여 논리적인 ONU ID를 부여하는 절차로 진행된다 또한 초기 등록 이후에 추가적인 등록(late registration) 절차를 수행하므로써 새로운 ONU의 등록과 통신을 보장하고 있다 그러나 EPON의 구조적인 취약점으로 인해 임의의 ONU에서는 모든 접속된 ONU에 대한 MAC 주소를 쉽게 취득할 수 있으며, 불법 등록 프레임을 생성하여 OLT로 전송하므로써 쉽게 불법적인 ONU로 위장할 수 있다. 위장된 ONU에서는 다른 ONU에서 보내는 것으로 위장하여 불법적인 데이터를 전송하는 것이 가능하다 이와 같은 위장을 통하여 운용 및 관리에 관련된 프레임을 송신할 경우에 더욱 위협적이다

3) 서비스 거부 위협(Denial of Service) : ONU에서 OLT로 전송하는 상향스트림의 경우 다양한 기법으로 하나의 광섬유를 공유한다 가장 간단한 공유 기법은 고정 대역할당 방식으로 모든 ONU에게 전송시간을 동일하고 할당하여 사용하는 것이다 그러나 전송 효율을 증가시키기 위하여 동적 대역할당 방식을 채택하는데, 일반적으로 동적 대역할당 방식은 전송 요구가 많은 ONU에게 많은 대역을 할당하는 기법을 채용한다. 이와같이 동적 대역할당 기법을 채용할 경우, 임의의 ONU 사용자가 비정상적으로 많은 트래픽을 발생시킨다면 다른 ONU는 정상적으로 대역을 할당받지 못하게 되고 경우에 따라서는 전혀 서비스를 받지 못하게 된다 하향스트림에서는 상향스트림의 경우와 달리 쉽지는 않다 그러나 불법적인 의도를 가진 사용자가 OLT로 위장하여 ONU에게 대역할당을 위한 제어 프레임을 변조하여 대역을 할당하지 않는다면 모든 ONU는 상향스트림을 전혀 전송하지 못하는 서비스 거부 상태가 된다

정보의 도청, 위장, 서비스 거부 외에도 EPON은 이더넷을 기반으로 하므로 IP를 기반 네트워크에서 가지는 많은 위협이 존재한다. 그러나 본 논문에서는 EPON 만이 가지는 구조적 취약점을 분석하였으며, IP 기반 네트워크에서 발생할 수 있는 위협들에 대한 보안서비스는 EPON 외의 상위 계층에서 제공하는 것을 가정하였다

2 보안 서비스

EPON의 구조적인 취약점으로 인한 정보의 도청, 위장, 서비스 거부 등의 보안 위협에 대한 대응으로 보안 서비스가 요구된다. 일반적으로 네트워크에서 제공되는 보안서비스는 정보의 비밀성(confidentiality), 무결성(integrity), 인증(authentication), 접근제어(access control), 부인봉쇄(non-repudiation), 가용성(availability) 등이 있다. 그러나 EPON은 계층 2만을 포함하며 Gbps 이상의 고속으로 데이터를 전송해야하는 조건을 가지므로 상위계층에서 이루어져야 할 보안서비스와 EPON에서 제공해야할 보안서비스를 적정한 수준에서 절충안(trade-off)를 선택해야 한다. 표 1에는 EPON의 보안위협과 보안서비스의 상관관계를 나타내었다.

표 1 EPON의 보안위협과 보안서비스의 상관관계

서비스 \ 위협	정보의 도청	위장	서비스 거부
비밀성	V	V	
인증		V	V
가용성			V

표 1에 나타난 것처럼 EPON의 보안위협에 따라 요구되는 보안서비스는 비밀성, 인증, 가용성 등이다. 비밀성 서비스는 평문에 대한 암호화에 의해 이루어 질 수 있으며, 암호화는 암호 키를 기반으로 특정한 암호 알고리즘을 포함하는 함수를 통해 전송되는 평문 데이터를 암호문 데이터로 변형하는 것으로 암호 키와 적용 알고리즘을 보유하고 있는 OLT 또는 ONU 만이 평문을 획득할 수 있다 비밀성 서비스는 암호화를 통해 불법적으로 정보를 도청하는 것으로부터 보호할 수 있을 뿐만 아니라 위장으로부터 보호할 수 있다.

인증 서비스는 정보 또는 자원을 사용하기 전에 권한을 획득하는 것으로 위장에 대한 위협으로부터 보호할 수 있는 서비스이다. OLT에서 ONU에 대한 인증을 수행하므로써 ONU의 위장을 방지할 수 있으며, ONU에서 OLT에 대한 인증을 수행하므로써 OLT의 위장을 방지할 수 있다. 인증 서비스는 위장에 대한 위협 뿐만아니라 합법적인 사용자들만을 망 자원을 사용하게 함으로써 불법적인 사용자에

의한 서비스 거부에 대한 위협을 차단하는 기반 서비스를 제공한다. 인증 서비스는 ONU와 OLT 모두 인증하는 상호 인증을 수행하며, 암호 알고리즘과 인증서를 기반으로 인증 서비스를 수행하는 것이 안전한 방법이다

가용성 서비스는 서비스 거부와 같은 위협으로부터 항상 망과 자원이 이용 가능하도록 제공하는 서비스이다 인증 서비스가 제공되는 환경에서 정당한 사용자가 서비스 거부 공격을 수행하는 것은 암호를 통한 보안 서비스의 범위를 벗어난다 서비스 거부 공격에 대한 대응은 특정한 ONU에서 트래픽이 비정상적으로 범람할 지라도 다른 ONU가 서비스를 제공받을 수 있도록 강건한(robustness) 동적 대역 할당 프로토콜에서 해결되어야 할 범위이다

Ⅲ. AES 암호 알고리즘

EPON에 적합한 암호 알고리즘은 구현이 간단하고 고속처리가 가능하며 MAC 계층에서 모든 처리가 가능한 요구조건을 만족해야 한다 암호화 시스템은 비밀키 암호 시스템과 공개키 암호 시스템으로 나누어진다. 일반적으로 비밀키 암호 시스템은 속도가 빠르고 안전하지만 키관리가 어렵다는 단점을 가지며, 공개키 암호 시스템은 확장성과 키관리가 용이하지만 속도가 느리다는 단점을 가지고 있다 따라서 최근에는 비밀키와 공개키의 장점을 수용하는 하이브리드 암호 시스템이 이용되고 있으며, 하이브리드 암호 시스템은 공개키를 이용하여 키 공유 및 관리를 수행하고 공통키(또는 세션키)를 생성하여 비밀키 알고리즘으로 암복호를 수행하는 방법을 채택하고 있다[5,6]

가장 널리 사용되는 비밀키 암호 알고리즘에는 1977년 미국의 국가 암호 표준으로 채택된 DES (Data Encryption Standard)와 3-DES에 기초를 두고 있다. 그러나 1998년 DES는 이미 표준 사용기한이 만료되었고, 3-DES는 2003년에 만료될 예정이며, 최근 DES challenge III에서 22시간 15분 만에 해독되는 등 알고리즘의 계속적인 사용에 문제점이 나타나고 있다[7].

이러한 문제점을 해결하기 위하여 미국 NIST (National Institute of Standards and Tech- nology)에서는 새로운 AES(Advanced Encryption Standard)를 위한 알고리즘을 공모하여 Rijndael 알고리즘이 채택되었다[8]. AES의 표준으로 선정된 Rijndael 알고리즘은 알려진 공격에 강하고, 다양한 플랫폼에서 빠르고 간단한 코드로 구현될 수 있으며, 단순한 구조를 갖는 특징을 갖는다. 이러한 AES 블록 암호 알고리즘은 EPON 암호 알고리즘의 요구조건에 부합된다. 또한 차세대 초고속 광 가입자망에서 사용될 암호 알고리즘으로 최근에 채택된 표준 암호 알고리즘을 수용하는 것이 바람직할 것으로 판단된다.

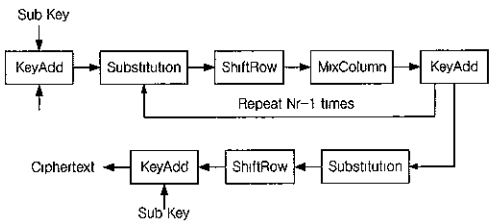
AES의 암호 알고리즘으로 채택된 Rijndael 알고리즘은 가변 블록 길이와 가변 키 길이를 갖는 반복구조의 블록 암호방식이며 블록 길이와 키 길이는 128, 192, 256 비트로 독립적으로 지정될 수 있다 라운드 수(Nr)는 블록 길이(Nb)와 키 길이(Nk)에 따라 결정되며, 이들 사이의 관계를 표 2에 나타내었다.

표 2 EPON의 보안위협과 보안서비스의 상관관계

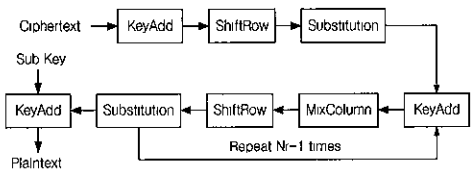
키 길이 \ 블록길이	Nb=4 (128 bits)	Nb=6 (192 bits)	Nb=8 (256 bits)
Nk=4(128bits)	Nr=10	Nr=12	Nr=14
Nk=6(192bits)	Nr=12	Nr=12	Nr=14
Nk=8(256bits)	Nr=14	Nr=14	Nr=14

표 2에 나타난 것처럼 키 길이가128 비트이고 블록 길이가 128 비트이면 10 라운드가 필요하다

Rijndael 알고리즘의 암호화 및 복호화 블록도는 그림 3과 같다. 평문(Plaintext)이 입력되면 가장 먼저 키 값과 입력 데이터는 XOR 연산을 수행한다



(a) 암호화 블록도



(b) 복호화 블록도

그림 3 Rijndael 알고리즘의 암복호 블록도

다음으로 ByteSub를 통하여 바이트 치환을 수행한

후, ShiftRow를 통하여 라운드 서브 키와 함께 XOR 연산을 한 후 다시 ByteSub에 되돌아가서 (Nr-1)번 이 과정을 반복 수행한다. 마지막으로 MixColumn이 생략된 최종 라운드를 통과하여 암호문(Ciphertext)이 출력된다 복호화는 암호화 블록도와 반대로 진행된다 암호화 블록과 복호화 블록의 진행 순서는 역순이지만 블록의 구조 자체는 서로 다른 구조로 설계되어 있다.

Rijndael 알고리즘은 구조가 간단하고 병렬처리가 가능하므로 기가비트 이상의 속도를 제공하는 EPON에서 구현은 어렵지 않을 것으로 판단되며, 상용 제품도 출시되고 있는 실정이다[9]. 표 3에는 상용 제품의 구현 사례를 나타내었으며, FPGA 또는 ASIC으로 구현시 128 비트 ECB(Electronic Codebook) 모드 운용할 경우 암복호 속도를 나타내었다.

표 3 AES 암호 알고리즘 하드웨어 구현 사례

Core / Target	STANDARD core Lowest Gatecount	FAST core High Speed/ Low Latency	PIPELINED core Ultra High Speed
Xilinx FPGA (Vertex E-8)	300 Mbps	1190 Mbps	> 10 Gbps
Xilinx FPGA (Vertex II-5)	470 Mbps	1700 Mbps	> 16 Gbps
ASIC (0 18um CMOS)	> 500 Mbps	> 2 Gbps	> 25 Gbps

Ⅳ. 인증 및 키관리 프로토콜

본 장에서는 EPON에 적합한 인증 및 키관리 프로토콜을 제안하였으며, 제안된 프로토콜을 검증하기 위하여 안전성 분석을 수행하였다. 본 장에서 사용되는 기호에 대한 설명은 다음과 같다.

P_A, P_B : A와 B의 공개키
S_A, S_B A와 B의 비밀키
n : 매우 큰 솟수 값(prime number)
nA, nB . n 보다 작은 랜덤 정수(random number)
O 덧셈에 대한 항등원
G : $nG = O$를 만족하는 유한체 타원곡선의 가장 작은 값
K_{AB} · A와 B가 데이터 암복호에 사용하는 공통키
C_A 공개키를 포함한 A의 공개키 인증서

1 공통키 생성 메카니즘

하이브리드 암호 체계에서는 공개키 교환을 통하여 암호측과 복호측이 동일한 공통키를 공유하고 공통키를 이용하여 비밀키 암호 알고리즘을 이용한다. 따라서 공개키를 교환으로 공통키를 생성하는 메카니즘이 필요하다.

공통키 생성을 위한 키 교환 방법은 Diffie-Hellman 또는 RSA가 가장 널리 사용 되었지만, Diffie-Hellman은 응답 공격(reply attack)에 취약한 단점을 갖고 있으며 RSA(Rivest-Shamir-Adleman)는 최근에 강도를 향상시키기 위하여 키의 길이를 증가시켜 고속망에 사용하기에는 부적합하다[5,6]. 이에 대한 대안으로 ECC(Elliptic Curve Cryptography)가 사용될 수 있으며, ECC는 RSA에 비해 상대적으로 키 길이가 작으며 처리 오버헤드가 적다 따라서 ECC 상에서 Diffie-Hellman 키 교환 프로토콜을 변형한 공통키 생성을 위한 방법을 제안하였다.

OLT와 ONU 중 하나가 공통키를 생성하기 위하여 OLT를 A로 정의하고 ONU 중 하나를 B로 정의하자. 먼저 유한체 위의 타원곡선을 선정하고, 임의의 큰 솟수 n를 선택한다. 공개키 연산을 위하여 $nG = O$를 만족하는 생성자 G를 계산한다 A의 공개키는 P_A와, B의 공개키 P_B는 식 (1)과 식 (2)와 같이 정의된다

$$A\text{의 공개키} \quad P_A = S_A \times G \tag{1}$$

$$B\text{의 공개키} \quad P_B = S_B \times G \tag{2}$$

초기에 A와 B는 공개키를 교환하여 상대방의 공개키를 교환한다 상대방의 공개키가 교환된 후에는 필요에 따라 세션을 위한 공통키를 생성하는데, 공통키 생성 절차는 그림 4와 같다

그림 4와 같이 랜덤 정수의 교환이 이루어진 다음에 생성된 공통키 K_{AB}는 A측과 B측이 식 (3)에 나타난 바와 같이 동일한 값이므로 공통의 세션키로 사용할 수 있다.

$$\begin{aligned} K_{AB} &= n_A P_B + S_A(n_B G) \\ &= n_A(S_B G) + n_B(S_A G) \\ &= S_B(n_A G) + n_B P_A \end{aligned} \tag{3}$$

A와 B에서 공통키를 생성하기 위해서는 상대방의 공개키와 랜덤 정수를 공유해야 한다 공개키의

공유는 인증 및 공개키 교환 프로토콜을 통해 이루어지며, 랜덤정수의 공유는 키교환 프로토콜에 의해 이루어진다.

A (OLT)	Public domain	B (ONU)
A의 초기상태 S_A, P_A, P_B		B의 초기상태 S_B, P_B, P_A
랜덤 정수 생성 n_A $n_A \times G$ 계산		
	n_AG 전송 ---▶	
		랜덤 정수 생성 n_B $n_B \times G$ 계산 공통 세션키 계산 $K_{AB=S_B}(n_AG)+n_BP_A$
	n_BG 전송 ◀---	
공통 세션키 계산 $K_{AB=n_A}P_B+S_A(n_BG)$		

그림 4 공통키 생성 절차

2. 인증 및 공개키 교환 절차

인증 및 공개키 교환은 ONU가 OLT에 등록된 후에 인증 절차를 수행한다. 인증절차를 수행하는 과정에는 인증서를 교환하는데 인증서에는 공개키를 포함하고 있다. 인증 및 공개키 교환 절차는 그림 5와 같다.

ONU에서 통신을 개설하기 위해서는 OLT에 등록하는 절차를 수행하며, 등록 절차가 완료되면 ONU는 논리적인 PHY ID를 할당받는다. 등록 절차를 마친 후에 OLT(A)와 ONU(B)는 상호 인증을 수행하게 되는데, 전송되는 내용과 절차는 다음과 같다.

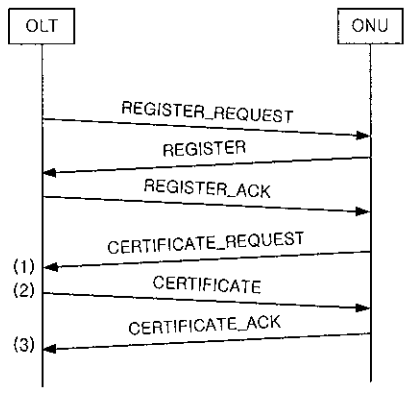


그림 5 인증 및 공개키 교환 절차

1) ONU(B) → OLT(A) . $\{B, A, N_B, C_B\}$
2) OLT(A) → ONU(B) . $\{A, B, N_A, C_A\}$
3) ONU(B) → OLT(A) · $\{B, A, E_{K_{AB}}\{N_A, N_B\}\}$

공개키 인증서 C_A에는 ID, 공개키, 공개키의 서명값 등의 정보를 포함하고 있다. 이 공개키 인증서는 OLT와 ONU 각각에 자신의 인증서을 가지고 있으며, 인증서의 초기 발급은 신뢰기관(Trusted Third Party)에 의존한다고 가정한다. 인증서에 대한 검증은 별도의 인증서버(Authentication Server)를 두고 인증과정 중에 온라인으로 접속하여 수행하거나, 초기 장비 설치시 인증서를 검증하기 위한 별도의 프로그램 및 키를 오프라인으로 주입할 수 있다. EPON에서는 별도의 인증서버를 운용하는 것은 많은 오버헤드를 가지므로 오프라인 주입이 효율적이다고 판단된다.

3. 키교환 절차

OLT와 ONU 사이에 초기 등록이 완료된 후에는 동일한 공통키를 갖게 된다. 그러나 키의 안전성 또는 멀티캐스트 등의 요구로 인하여 세션 중에 키를 변경해야 하는 요구가 발생하게 된다. 이러한 요구가 발생하였을 경우 OLT에서 ONU에게 키를 변경하기 위한 메시지를 전송하고 정확한 시간에 키를 변경해야 한다. 키교환 절차를 그림 6에 나타내었다.

세션 중간에 새로운 공통키를 생성하기 위해서는 상대의 공개키과 랜덤 정수가 필요하다. 그러나 공개키는 변하지 않고 초기 등록 후 인증 과정에서 교환하였으므로 새로운 공통키를 생성하기 위해서는 암호화된 랜덤 정수만을 교환한다. NEW_KEY_REQUEST에 OLT에서 생성한 랜덤 정수 n_A를 공개 랜덤 정수 n_AG로 변환하여 전송한다.

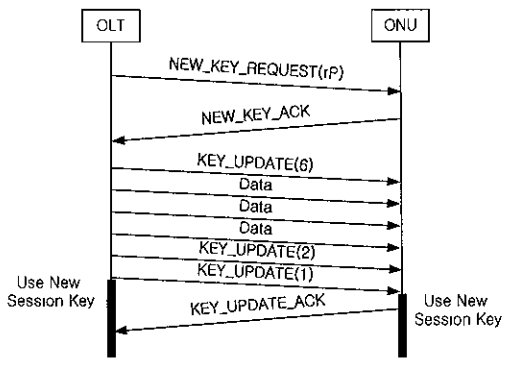


그림 6 키교환 절차

ONU에서는 요구 메시지를 수신한 후에 공통키를 정상적으로 생성한 상태와 n_BG를 전송한다 전송된 메시지에 의하여 그림 4에 나타난 것처럼 OLT와 ONU는 새로운 공통키 K_{AB}를 생성한다

생성된 공통키는 암복호 패킷에 대하여 정확히 동기되어야 한다. 암복호에 사용되는 키의 동기는 정확한 시간을 이용하기도 하는데, EPON에서는 정확한 시간을 이용한 키동기는 패킷의 중간에 키가 변경될 수 있으므로 부적합하다. EPON 시스템에 적합한 키동기는 전송되는 패킷 기점으로 키가 변경되고 동기될 수 있도록 해야한다 따라서 KEY_UPDATE 메시지에 키변경이 될 때까지 전송될 패킷의 수의 정보를 전송하는 N-To-Go 메카니즘을 제안하였다. N-To-Go 메카니즘은 KEY_UPDATE 메시지 중 하나가 전송되지 않거나 데이터 패킷의 손실이 있더라도 이 프로토콜에는 복구할 수 있는 기능이 있다. 예를 들어, KEY_UPDATE(6)를 전송한 후에 데이터 패킷 중 하나가 손실되거나 KEY_UPDATE(2) 또는 KEY_UPDATE(1) 메시지를 수신하여 새로운 공통키로 변경된다.

4 키복구 절차

키복구 절차란 암호측과 복호측의 키가 일치하지 않을 경우 이를 발견하여 양측이 동일한 키를 갖도록 재설정해주는 프로시쥬어이다 제안된 EPON에서의 암호는 MAC 계층에서 이루어지므로 암호 패킷에 대한 FCS(Frame Check Sequence)는 물리계층에 전송하기 전에 계산하여 부가하며, 수신된 암호패킷은 FCS를 검사하여 전송 중 에러를 검사하고 복호화 후에 새로운 FCS를 재계산하여 프레임 뒤에 부가하게 된다 따라서 EPON에서 전송과정 중에는 암복호가 정상적으로 수행하고 있는지를 자동적으로 검출할 수 있는 방법이 없다 따라서 주기적으로 일정한 패턴을 가진 프레임을 전송하여 암복호가 정상적으로 이루어지고 있는지를 검사하는 방법으로 키동기 불일치를 탐지한다 키동기 불일치가 발생하게 되면, 키복구를 수행하는데 키 복구는 새로운 공통키를 생성하기 위한 랜덤 정수를 교환하므로써 이루어진다. 키복구 절차는 그림 7과 같다.

그림 7에 나타난 거처럼 KEY_SYNC_REQUEST 메시지를 OLT에서 주기적으로 전송하는데, OLT에서 전송한 이 메시지를 ONU에서 복호하여 정상적이면 KEY_SYNC_ACK 메시지로 응답하고, 비정상적이면 KEY_SYNC_NACK를 응답한다.

OLT에서 KEY_SYNC_NACK 메시지를 수신하면 키동기가 불일치하다고 인식하고 키복구 절차를 수행한다. 키복구 절차는 새로운 공통키를 생성하기 위하여 공개 랜덤 정수를 KEY_RESYNC_REQUEST 메시지에 실어 보낸다 ONU에서는 공통키를 생성한 후에 자신이 생성한 공개 랜덤 정수를 KEY_RESYNC_ACK를 통해 전송하여 OLT에서도 새로운 공통키가 생성되도록 한다.

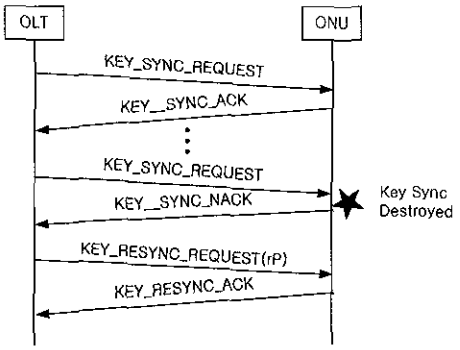


그림 7 키복구 절차

5. 프로토콜의 안전성 분석

제안된 프로토콜은 공격자가 프로토콜에 참여하여 비밀키를 획득할 수 있는 능동적인 공격(active attack)에 대하여 인증 및 공통키 생성 프로토콜의 안전성을 분석[10]을 수행하였다

1) 알려진 세션키(known session keys)

알려진 세션키는 이전 세션에 사용되었던 세션키를 알고 있는 공격자에 대한 안전성을 분석하는 것이다. 제안된 프로토콜은 새로운 세션을 위한 공통키를 생성하기 위하여 새로운 랜덤 정수를 상호 간에 교환하므로 이전 세션에 사용되었던 공통키가 알려졌을지라도 새로운 세션에는 영향을 받지 않는다.

공격자 C가 이전 세션에 대한 공통키 값을 알고, A인 것처럼 가장하는 시나리오를 고려해 보면 다음과 같다

(1) A→B A, B, n_AG

(2) B 공통키 계산, $K_{AB}=S_B(n_AG)+n_BP_A$

(3) B→A B, A, n_BG

(4) A : 공통키 계산, $K_{AB}=n_AP_B+S_A(n_BG)$

(5) C(A')→B A, B, n_AG

(6) B n_B' 생성, $n_B'G$ 계산

(7) B . 공통키 계산, $K_{AB}=S_B(n_AG)+n_B'P_A$

(8) B→C(A') $B, A, n_B'G$

(9) C(A') . 계산된 공통키 $K_A'B$ 사용불가능

위의 시나리오에서 공격자 C는 (1)-(4)를 통하여 공통키 생성하는 방법과 n_AG, K_{AB}를 알고 있다고 가정하였으므로, (5)-(8) 과정을 거쳐 A인 것처럼 위장할 수 있다. 그러나 (6) 과정에서 B는 A로부터 동일한 랜덤 정수를 수신했을지라도 새로운 랜덤 정수 n_B'를 생성하며, n_B'G를 계산하여 새로운 공통키 $K_{A'B}$를 생성한다 과정 (9)에서 공격자가 이미 알려진 K_{AB}를 사용하여 A인 것처럼 위장하는 것은 공통키 값이 서로 다르므로 불가능하다. 또한, 공격자 C는 A의 비밀키 S_A와 A의 랜덤 정수 n_A를 알지 못하므로 K_{AB}를 계산할 수 없다. 따라서 제안된 프로토콜은 알려진 세션키에 대한 안전성이 보장된다

2) 전향적 비밀성(forward secrecy)

전향적 비밀성은 장기간 사용 등으로 비밀키가 노출되어도 이전 세션에 영향을 받지 않는 안전성을 분석하는 것이다 제안된 프로토콜은 비밀키가 노출된 경우에도 공개 영역에서 획득한 공개 난수 값 n_AG, n_BG로부터 nA, nB를 계산할 수 없으므로 이전 세션에 사용된 공통키를 계산할 수 없다. 따라서 전향적 비밀성에 대한 안전성이 보장된다

3) 미지키 공유(unknown key-share)

미지키 공유는 키 공유 대상을 속이는 공격에 대하여 안전성을 분석하는 것이다. 즉, 공격자 C가 네트워크의 중간에서 A와 B사이에서 전송되는 공개키를 가로채고 신뢰기관으로부터 공개키 인증서를 새로이 발급 받은 후에 중계하므로써 A 또는 B가 상대와의 통신이 정상적으로 이루어지고 있다고 위장하는 것에 대한 안전성을 보장하는 것이다

본 논문에서는 EPON은 가입자와 기간 통신망을 연결하는 액세스 망으로 온라인 상의 신뢰기관이 없고 초기 인증서 발급시에 공개키와 공개키에 대한 인증서를 ONU와 OLT에 오프라인으로 입력하는 것을 제안하였다 제안된 가정하에서 공격자 C는 중간에서 공개키를 가로채어 새로운 인증서를 발급받는 것이 불가능하며, EPON의 트리 구조에서는 OLT와 ONU 사이에 오직 능동 소자만 존재하므로 가로채어 재전송하는 것이 구조적으로 불가능하게 되어 있다 따라서 제안된 EPON 구조의 인증 과정 중에서는 미지키 공유에 대한 안전성이 보장된다.

4) 키손상 위장(key-compromise impersonation)

키손상 위장은 비밀키 정보가 노출되어 공격자가 위장하는 공격에 대하여 안전성을 분석하는 것이다 즉, OLT 또는 임의의 ONU의 비밀키가 노출되어 공격자 C가 다른 OLT 또는 ONU로 위장하는 것에 대한 안전성을 보장하는 것이다

임의의 ONU를 B(i)라 하고, B(i)의 비밀키 $S_{B(i)}$가 노출되어 공격자 C가 B(j)인 것처럼 위장하는 경우를 고려해 보자 공격자 C가 B(j)로 위장할 경우 초기 등록과정과 인증 절차를 수행하는데, 인증 프로토콜에서는 B(j)로 위장하기 위해서는 B(j)의 공개키와 공개키에 대한 인증서를 OLT로 전송해야 한다. 그러나 공격자 C는 공개키 B(j)에 대한 올바른 인증서를 생성할 수 없으므로 B(j)로 위장하는 것은 불가능하다. 따라서 제안된 프로토콜은 키손상 위장에 대한 안전성을 보장한다

Ⅳ. 결 론

본 논문에서는 광가입자망의 표준으로 추진되고 있는 EPON에서 요구되는 MAC 계층의 보안 프로토콜을 제안하였다 제안된 프로토콜은 AES의 Rijndael 암호 알고리즘을 이용하고 공개키 기반 키 교환을 통해 공통키를 생성하는 하이브리드 인증 및 암호 프로토콜이다 암호 및 인증을 위하여 공개키와 랜덤 정수를 이용한 공통키 생성, 공개키 인증서를 기반으로 하는 인증 및 공개키 교환, N-To-Go 메카니즘을 이용한 키동기, 주기적인 검사 패턴을 이용한 키일치 및 키복구 등을 EPON에 적합하도록 제안하였다. 제안된 프로토콜의 안전성을 검증하기 위하여 알려진 세션키, 추후 비밀성, 미지키 공유, 키손상 위장 등에 대하여 안전성 분석을 실시하여 프로토콜의 안전성을 검증하였다

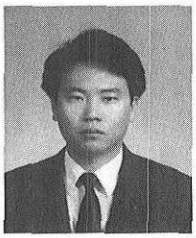
EPON은 다른 광가입자망에 비하여 경제적이고 효율적으로 초고속 가입자망을 구축할 수 있다는 장점을 가지므로 표준화와 함께 광대역을 요구하는 IP 기반의 가입자망에 급속히 상용화될 것이 예측된다. 따라서 EPON에 대한 보안 프로토콜의 규격을 제정하고 구현하는 것은 매우 절실한 연구과제이다. 앞으로는 본 연구를 기반으로 EPON에서 상용화할 수 있는 안전한 데이터 전송을 보장하는 보안 MAC 계층 설계에 대한 연구를 추진할 예정이다

참 고 문 헌

[1] U Killat, editor "Access to B-ISDN via PONs ATM Communication in Practices", John Wiley & Sons Ltd & B G. Teubner, 1996

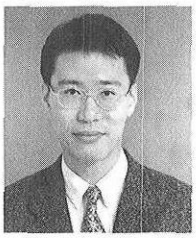
[2] ITU-T Recommendation G.PONB - Draft D, "ATM PON Specification," April 1997.
[3] ITU-T Recommendation G.983, "High Speed Optical Access Systems Based on Passive Optical Network (PON) Techniques," ITU-T Study Group 15, Feb. 1998.
[4] IEEE 802.3ah Ethernet in the First Mile Task Force
[5] 강주성, 박상우, 박춘식, 지성택, 천정희, 한재우, 현대암호학, 제2판, 한국전자통신연구원, 1999.
[6] William Stallings, Cryptography and Network Security, 2nd Edition, Prentice-Hall, 1999.
[7] http://www.rsa.com/rsalabs/des3/, January, 1999.
[8] FIPS 197, Specification for the Advanced Encryption Standard(AES), NIST, Nov. 2001.
[9] http://www.heliontech.com/core2.htm
[10] Simon Blake-Wilson, Don Johnson, Alfred Menezes, "Key Agreement Protocols and their Security Analysis," 6th IMA Conference on Cryptography and Coding, LNCS1355, pp. 30-45, 1997.

강 인 곤(In-Kon Kang) 정회원



1990년 2월 : 전북대학교 컴퓨터공학과 졸업
1992년 2월 : 전북대학교 컴퓨터공학과 석사
2003년 2월 : 전북대학교 컴퓨터공학과 박사 예정
1996년 1월~2000년 10월 : 국방과학연구소 선임연구원
2000년 2월~현재 : 국가보안기술연구소 선임연구원
<주관심 분야> 네트워크 보안, 인터넷

이 도 훈(Do-Hoon Lee) 정회원



1989년 2월 : 한양대학교 전산학과 졸업
1991년 2월 : 한양대학교 전산학과 석사
1991년 2월~2000년 1월 : 국방과학연구소 선임연구원
2000년 2월~현재 : 국가보안기술연구소 선임연구원
<주관심 분야> 컴퓨터 통신, 네트워크 보안

이 봉 주(Bong-Ju Lee) 정회원

1995년 8월 : 전북대학교 물리학과 졸업
1998년 2월 : 전북대학교 영상정보공학과 석사
1999년 3월~현재 : 전북대학교 영상공학과 박사과정
<주관심 분야> 이동통신, 위성통신, 인터넷, 보안

김 영 천(Young-Chon Kim) 정회원
한국통신학회 논문지 제19권 제2호 참조
현재 : 전북대학교 컴퓨터공학과 교수