특 집

광 가입자망에서의 인증 및 링크 보안

Authentication and Link Security in Optical Access Networks

김 아 정

세종대학교 전자정보통신공학부

I. 서 론

정보 통신 및 정보화 기술의 활용이 증가됨에 따라 가입자망에서 까지 광대역의 통신망 기술을 요구하게 되었고 이러한 가입자망에서의 대역폭 문제만큼이나 심각하게 통신 보안의 문제가 대두되고 있다. 무선 LAN이나 이동 무선 네트워크의 경우 특성상 제3자의 도청 방지등 보안이 절실히 필요하지만, 현재 상용화된 시스템에서는 보안에 대한 위험성들이 많이 지적되고 있는 실정이다. 차세대 광 가입자망 구현 방식으로서 주목받고 있는 수동형 광가입자망(PON)의 경우도 하나의 OLT에 수동소자를 이용해 다수의 ONU를 연결한 트리 구조를 형성해 토폴로지 상 무선 통신과 같이 broadcast and select의 원리를 따르고 있으므로 보안의 문제는 심각하며 이러한 문제는 공중망에 진입해 시장이 성장하는데 큰 걸림돌이 될 수 있는 상황이다.

보안이나 privacy 서비스를 논의할 때 생각할 수 있는 것이 암호 기술이라 할 수 있다. 암호 기술은 흔히 생각하는, 평문을 해독 불가능하게 하는 암호화와 수신자가 평문으로 복원하는 복호화에 연관된 기밀성(confidentiality) 보장 뿐만 아니라 데이터가 전송 중에 그 내용이 변경되었는지를 확인할 수 있는 무결성(integrity) 보장, 전송된 문서의 출처 및 무결성을 확인할 수 있는 메시지 인증, 전송한 사용자가 실제 정당한 사용자인지를 판별하는 사용자 인증, 서비스를 받거나 제공하고서도 부인하는 것을 방지하는 부인봉쇄(nonrepudiation) 등 많은 기술의 형태로 존재한다.

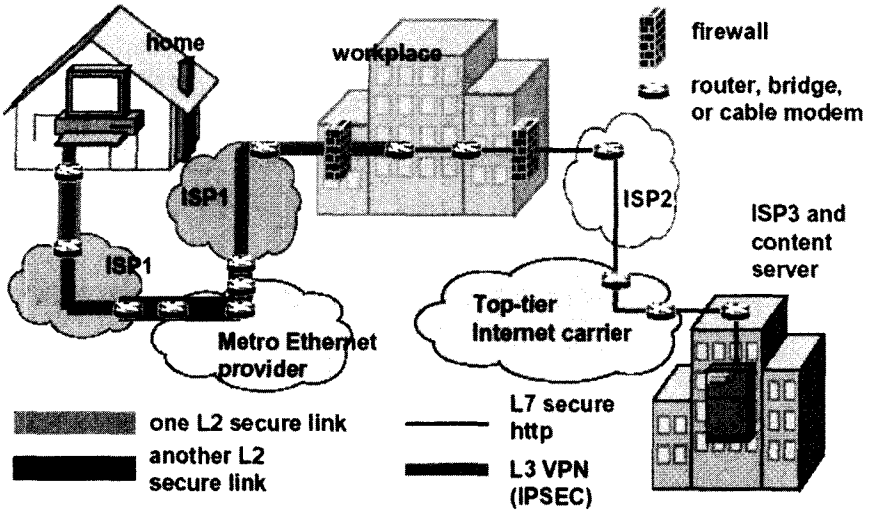
본 논문에서는 기존의 시스템에서 정의된 보안 시스템 구조와 메커니즘 분석을 통하여 가입자망 시스템에서의 인증 및 privacy 메커니즘을 이해하며, 이를 바탕으로 차세대 광가입자망에서 요구되는 보안 시스템의 요구 사항을 Ethernet PON 기반의 광대역 광 가입자망을 중심으로 전망해보고자 한다.

II. 본 론

1. 보안 위협과 보안 서비스

보안이란 일종의 위험 관리에 관한 문제로서 항상 위험억제와 그에 따른 시스템 복잡성 및 비용 증대의 양면에 대한 고려를 하여 그 사이의 최적화를 이끌어내야 한다. 따라서 시스템이 지닌 보안의 위협 요소를 분석해 보안 서비스의 수준을 정하는 것이 시스템 설계의 중요 요소라 하겠다. <그림 1>은 현재 전체 통신망에서 각 layer가 담당하는 보안 링크를 나타낸다. Spanning Tree 등 많은 프로토콜이 IPsec과 같은 layer 3 보안만으로는 보호되지 않고 링크 영역상 각기 다른 책임과 요구사항이 적용되기 때문에 link layer의 보안을 부가함으로써 L2 carrier에 부가가치를 창출할 수 있다.

PON의 토폴로지에 있어 downlink에서는 broadcast로 인해 다른 ONU의 도청의 위험이 존재하고 uplink에서는 점대다점 구조로 인해 인증받지 못한 ONU의 자원 접근이나 다른 ONU의



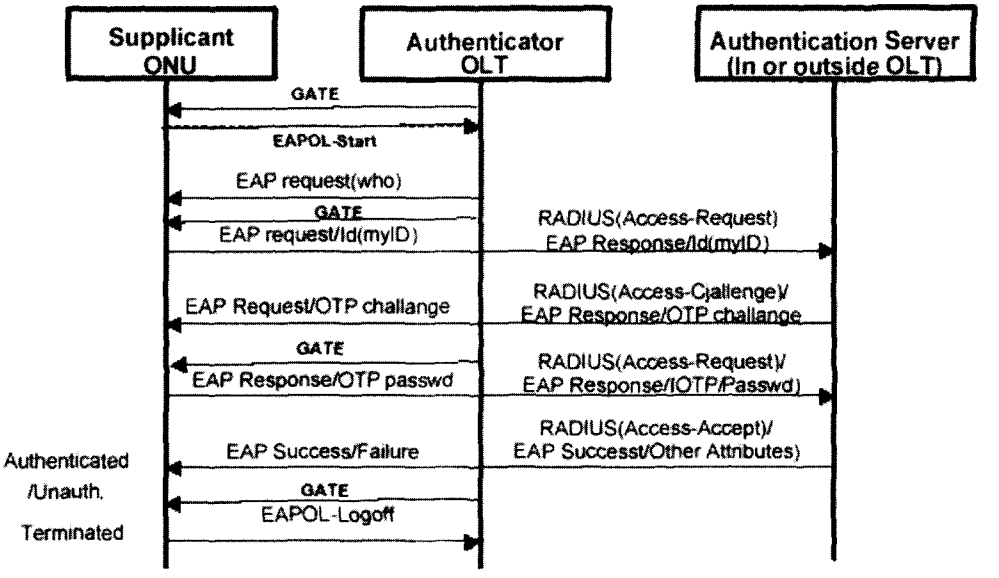
Source: Cisco.com

〈그림 1〉 통신망에서의 layer별 보안

변장(impersonation)의 위험이 있다. 데이터 암호화를 통해서 이러한 shared medium을 점대점 링크의 집합으로 변환시킬 수 있다. 암호화를 통해 downlink상의 도청과 uplink의 변장을 방지할 수 있고 인증을 수행할 수 있는데 EPON에서는 MPCP(multipoint control protocol)와 같은 링크 control에 대한 트래픽과 OAM packet 역시 보호되야 할 필요성이 있다. 따라서 PON에서 중심이 되어야 할 보안 서비스 이슈들은 ONU 인증, encryption, 그리고 키관리 등을 들 수 있다. 인증을 통해 자원 접근을 콘르롤하고 상하향 데이터의 encryption을 통해 도청방지와 비인증 ONU의 변장을 방지하여 메시지나 메시지 근원에 대한 무결성을 보장할 수 있다. 이러한 인증과 encryption에 사용되는 파라미터가 암호화 키인데 이 키의 운용과 교환방식에 따라 암호화 방안의 키관리 flow와 스케쥴링이 달라진다.

2. 인증

현재 EPON의 표준화를 담당하는 IEEE 802.3 ah에서는 보안 이슈를 다루지 않고 있기 때문에 EPON의 MAC layer에서 따로 인증 메커니즘을 고안하여 수행하지는 않고 기존의 성립되어 있는 프로토콜을 차용할 것으로 보인다. 이 때 ITU-T 계열의 인증 표준인 X.509 보다는 IEEE 802.1x가 유력하다. 802.1x는 MAC 상위에서 포트를 기반으로 한 네트워크 access control 메커니즘을 정의한 것으로, 802.1d를 위해 고안되었으나 Ethernet, Token Ring 및 802.11 무선 랜 등에서도 사용되고 있다. 802.1x는 자체적으로 인증 프로토콜을 가지고 있진 않으며 인증에 필요한 패킷들을 전송하는 전송 메커니즘을 정의하고 있다. 802.1x상에서 인증 알고리즘으로는 Kerberos over 802.1x와 unspecified authentication over 802.1x 등을 들 수 있는데 이러한 방법을 EPON에 적용시킨 예를 〈그림 2〉에서 보이고 있다. 여기서 ONU와 OLT 사이에서는 EAPoL(Extensible Authentication Protocol over LAN) 패킷 형태를 사용하고 OLT와 인증 서버 사이에서는 EAP 패킷 형태를 사용하게 된다. 802.1x의 동작원리를 PON 시스템에 적용해보면, ONU와 같은 supplicant 시스템의 인증메시지는 OLT에 해당하는 Authenticator 시스템의 uncontrolled port를 통해서 back end 시스템의 authentication server 시스



〈그림 2〉 EAP 기반의 인증 절차도

템에 전달된다. 이 때, supplicant 시스템과 authentication 시스템 사이의 패킷은 EAP 형태인데, MAC layer 상위에서 EAP을 사용할 수 있게 하였다. Authenticator 시스템은 supplicant 시스템을 인증한 후에 controlled port를 unblock 하게 되고 이후 전송 패킷들이 controlled port를 통해서 네트워크로 전송된다.

L2에서 access control 을 위해서 802.1x는 RADIUS와 함께 네트워크 사용자가 네트워크에 접근할 수 있도록 해주는 역할을 한다. 다른 메커니즘이 없이도 802.1x를 이용해서 네트워크에 접근 가능하게 할 수 있으며, 사용자를 추가적으로 구분하여 다른 서비스를 제공하기 위해서는 또 다른 메커니즘이 필요하다. 즉, 802.1x는 광링크에 대한 접근제어 기능을 하며, 인증 프로토콜은 PAP(Password Authentication Protocol), CHAP(Challenge-Handshake Authentication Protocol), EAP 등에 의존할 것이다.

그러나 802.1x는 802.11에서의 pre-authentication에서 보듯 802 네트워크에 그대로 적용시키기에는 부적절한 면이 있어 EPON 등의 802 네트워크를 위한 적절한 인증 아키텍처를 필요로 한다. 또한, 한 domain 또는 여러 domain에서 여러 access technology를 사용하는 환경에서는 802.1x를 그대로 적용하기에 힘들기 때문에 상위계층에서 인증 메커니즘을 (재)설계하는 것이 바람직하다고 생각된다. 즉, 802.1x는 heterogeneous network에서는 여러 technology 간의 hand off나 여러 사용자에 차별화 된 서비스를 제공하기 위한 메커니즘으로서는 적합하지 않다. 다음은 layer 2에서 802.1x와 상위계층에서 authentication mechanism을 조합해서 이용하는 시나리오를 보이고 있다.

- 시나리오 1:
  무료의 local access를 위한 L2 인증+과금성의 서비스나 global Internet에의 access를 위한 high layer authentication
- 시나리오 2:
  무료 local service가 존재하지 않는 공중망에서의 L2 인증+호텔등 무료 intranet이 가능한 곳을 위한 higher layer 인증.

과금성의 video service의 경우 video providing server에서의 인증이 이루어지므로 이때 가입자망에서의 인증은 전자의 경우를 적용할 수 있다.

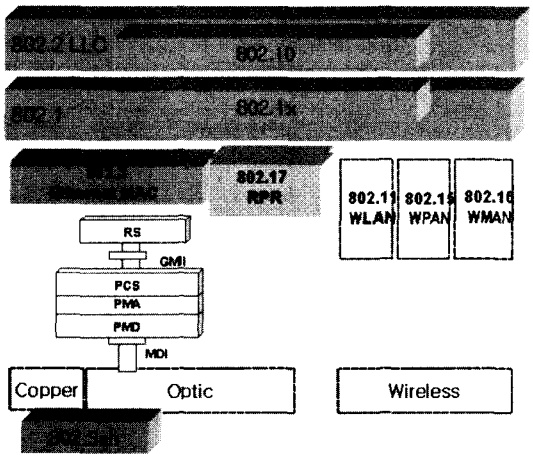
EPON에서의 인증 절차를 보면, ONU가 등록을 하고 LLID(logical link ID)를 부여받은 후에 인증을 하는 것을 고려해 볼 수 있다. 이 방안은 등록자의 신뢰성을 확인하지 않은 채로 아이디를 부여하고 전체 스케쥴링 절차가 증가한다는 점이 있으나 등록시에 발생하는 충돌로 인한 손실에는 영향을 받지 않는다는 장점이 있다. 사용자 인증을 한 후, 인증받은 ONU만 등록시키는 방안도 고려할 수 있으나 이 방안은 등록시도시 충돌이 발생할 경우 인증요청과 인증절차 자체가 충돌될 수 있어 비효율적이다. 따라서 ONU 등록 후 인증 challenge에 따른 grant를 받아 인증 절차를 수행하고 인증 acknowledge를 받은 후 신규나 갱신을 위한 키를 생성 분배함으로써 보안 기본 절차를 수행한다. 키의 갱신 시 ONU와 OLT의 키 동기를 위한 방법으로는 키 분배 acknowledge를 하는 hand shaking 방법, OLT가 갱신 몇 프레임 전부터 갱신 키로 전환 시점까지 보낼 패킷 수를 switch-key 메시지에 담아 보내 갱신 시기를 알리는 방법, 또는 switch-key 표시 bit으로 toggling하는 방법 등을 들 수 있다.

3. Privacy

현재 802.1x 표준 지원 장비를 도입하고 있는 무선 랜의 경우 사용자 인증과 접속 보안만을 취급할 뿐 일단 접속한 사용자에 대한 보안은 지원하지 못하고 있어 무선 랜에 접속해 네트워크 환경을 검색하면 같은 AP에 접속된 다른 사용자의 정보가 그대로 노출되는 위험성이 있는데 같은 원리로 EPON에서도 암호화에 대한 지원이 필요하다.

암호화에 있어 기능은 인증뿐 아니라 기밀성과 무결성 보장 등을 들 수 있으나 그 중 네트워크 상에서의 기능상 비중은 오히려 메시지나 메시지의 근원이 변조되지 않았는가에 관한 무결성에 대한 중요도가 더 크다 하겠다.

IEEE 802 LANs and MANs 표준 산하에는 이러한 호환성있는 data link layer security protocol과 이에 연관된 보안 서비스를 위한 Secure



〈그림 3〉 layering model

Data Exchange(SDE) protocol을 802.10에서 규정하고 있으나 현재 Cisco Internetwork Operating System에서 SDE의 SAID(Security Association Identifier) field를 VLAN ID로 차용하여 쓸 뿐 data link security를 위해 802.10을 사용하는 상용 시스템은 없는 상황이다. 〈그림 3〉은 여러 네트워크를 포함한 layering model과 그 관계를 나타낸다. SDE는 Logical Link Control(LLC) sublayer로서 Medium Access Control(MAC) sublayer의 상위 layer에서 connectionless service를 제공하는데 SAID와 키 등을 관장하는 SMIB(Security Management Information Base)와 연동하여 SDE PDU에 대한 프로세싱과 데이터의 전송을 수행하기도 한다. 그러나 EPON에 802.10을 적용할 경우 802.10 header와 ICV(Integrity Check Value) 추가에 따른 fragmentation이 불가피하거나 MAC sublayer에서 이를 적용할 경우 Ethernet type을 이용해 designator를 명시해야 하므로 Ethernet type을 사용하는 대부분의 Ethernet frame은 frame conversion을 필요로 한다. 따라서 EPON 에서는 802.11i와 같이 자신의 MAC의 특징을 고려한 고유의 보안 대책을 강구할 것으로 보인다.

이 때 privacy layer를 sub-RS layer에 두는 경우와 sub-MAC layer에서 수행하는 경우

를 고려할 수 있다. Sub-MAC layer의 경우는 보안에 관계된 정보를 frame 안에 tag의 형태로 전송하는 방식으로 최대 패킷 사이즈의 제한을 받게 되어 VLAN의 경우와 같이 최대 패킷 사이즈 수정을 필요로 한다. Sub-RS layer의 경우는 preamble에 보안 정보를 포함하므로 frame 크기 제한을 받지 않으나 designator, 무결성 보장 등을 가용한 한 두 바이트에 담기에는 제한이 있을 것으로 보인다. 또한 이 경우는 MAC frame 전체를 암호화하게 되는데 MAC address를 암호화하여 기밀성을 보장시킬 수 있으나 MAC address를 암호화함으로써 management 문제나 비호환성 문제 등 그 부작용이 심각하여 bridged network에서는 문제를 야기시킬 수도 있을 것으로 보인다.

〈표 1〉은 여러 네트워크에서의 보안 서비스에 대한 비교 분석이다. ATM을 기반으로 한 APON에서 사용되고 있는 암호화 방안은 churning으로 3bytes 크기의 암호화 키가 사용된다. 이 방법은 2초마다 키값이 갱신되어야 하는 암호능력을 가지고 있으며 상대적으로 간단한 알고리즘이므로 622Mbps APON의 고속지원에 사용되었다. 키 값은 ONU에서 만들어져 각 OLT에게 제공되며 이 값과 주기적으로 갱신되는 키값들은 OAM cell의 payload 부분에 넣어져 전달된다. APON의 경우, 당시 암호화 기술의 한계와 고속지원의 가능성으로 인하여 3bytes의 churning 키를 OAM cell에 넣어 사용하였으나 이 방식은 현 기술 수준 상 암호화 강도가 미약하다는 한계가 있다.

현재 컴퓨터의 계산능력을 보거나, 기가비트 이더넷의 경우는 622Mbps의 전송속도를 갖는 APON에 비해 상대적으로 고속이라는 점을 고려하면 APON의 암호화 방안을 따르는 것은 기술적으로 비효율적일 수 밖에 없다. EPON에서 채택할 가능성인 높은 encryption 방안은 symmetric 방법인 AES(Advanced Encryption Standard)로 이는 Rijndael 알고리즘에 의해 구체화된다. AES는 키를 갱신해야 하는 주기가 $3*10^{17}$년 정도인 강력한 암호화 방안으로 특히

〈표 1〉 여러 네트워크에서의 보안 서비스 비교

	802.16 WBA	DOCSIS	802.15 WPAN	802.11 WLAN
Authentication	- shared key - open system	X.509	TLS-like public key mutual authentication	- open system - shared key - ULA
Encryption algorithm	DES	3-DES	RSA	AES, WEP, WEP2
Encrypted range	MAC PDU	MAC PDU	MAC PDU(data and commanc)	MSDU
Privacy sublayer	Sub-MAC	Sub- MAC	Sub- MAC	Sub-MAC
Security associate information header	- EC(1bit) : enc.on/off - EKS(2bits) : key index	- Key-seq(4bits) - Version(4bits) - Enable(1bit) ; - Toggle(1bit) - SAID(14bits)	Becon - SSID, MIC command - SSID, counter, IV, MIC data - SSID, IV,, MIC	WEP/WEP2 - IV(3bytes) - Key ID(2bits) - MIC(4bytes)
Characteristic	More directional, wider range that 802.11	Multiple level of protection	Complexity, power contraint	Easy man-in-the-middle attack

기가비트 이상의 고속의 망을 위하여 제안되었다. 이는 블록 단위로 데이터를 encryption하며 이 때 블록의 크기는 128bits이고 사용되는 키의 길이는 128, 192 혹은 256bits가 된다. 보통 hybrid encryption 방식을 택하여 shared key를 만들기 위한 목적으로 공개키를 키분배하여 session key를 update하기도 한다.

암호 모드에 대해서는 여러 가능성이 있는데 그 중 OCB(Offset Code Book) mode는 무결성 알고리즘이 내장되어 있어 privacy와 무결성을 함께 보장할 수 있고 병렬 프로세싱이 가능하다는 등 장점을 가지고 있으나 IEEE 외부의 지적재산권의 문제가 걸려 있고, 그 외 CTR mode 등도 고려되고 있다.

Ⅲ. 결 론

현재 EPON에서의 보안 이슈는 EPON의 표준화를 수행하고 있는 802.3ah의 영역 밖으로 간주되어 새로이 link security라는 study group을 형성한 채 task force 승인을 목적으로 활동중이다. 그 이전에는 각 시스템 vendor에서 각기 보안 솔루션을 제공할 것인데 이에 대해 상호 호환성 문제가 대두될 것으로 예상되며 이는 시장 형성의 걸림돌로 작용할 가능성도 있다.

현재 link layer의 보안 필요성을 가장 먼저 절감을 해 고안, 검토 중인 802.11 WLAN의 해결책을 바탕으로 전개되리라 본다. 인증, 기밀성, 무결성 보장을 위해 상향/하향 링크의 사용자 데이터의 암호화 문제가 중요하므로 강력하고 효율적인 암호화 키 방안의 선택과 효과적인 운용이 필요하다. 비디오 서비스와 같은 종류의 멀티캐스트 서비스는 일반적으로 서비스 제공자가 higher layer에서 암호화하여 MTU의 셋톱 박스에서 복호화하므로 central office에서 L2 encryption을 할 필요는 없을 것으로 보여지나 기타 멀티캐스트 전송에 대한 것도 해결해야 할 보안 이슈 중 하나로 보여진다. 같은 키를 공유하고 있는 멀티캐스트 그룹으로 부터의 탈퇴는 다른 모든 그룹원에게 키를 갱신함으로써 이루어지는데 이에 대한 운용 또한 고려해야 할 이슈이다.

참 고 문 헌

〔1〕 IEEE p802. 1X, D10, January, 2001
〔2〕 IEEE Std 902. 11eS/D1, March 2001
〔3〕 IEEE 802.3ah EFM presentations
〔4〕 RFC 2284, "PPP Extensible Authentication Protocol".
〔5〕 J. Daemen, V. Rijmen, AES Proposal : Rijndael, 1999
〔6〕 J. Daemen, V. Rijmen, AES Proposal : Rijndael, 1999
〔7〕 P. Rogaway, OCB Mode-Proposal to NIST for a block-cipher mode of operation which simultaneously provides privacy and authenticity, 2001
〔8〕 A. J. Menezes, "Handbook of Applied Cryptography", CRC Press, 1997

저 자 소 개

金 娥 正

1988년 2월 서울대. B.S, 1995년 6월 Northwestern Univ. M.S., 1996년 12월 Northwestern Univ. Ph.D., 1997년 1월~1998년 : Norwestern Univ. 전자컴퓨터 공학과, associate researcher, 1998년 4월~2003년 2월 : 삼성종합기술원 i-networking랩, 전문연구원, 2003년 3월~현재 : 세종대학교 전자정보통신공학부 광공학과 조교수, 〈주관심분야 : 광대역 통신망, 광통신시스템, 광소자〉