[4-37]

수동 광 네트웍에서의 링크 레이어 보안 프로토콜의 구축

김아정, 박태성^
세종대학교 전자정보통신공학부
akim@sejong.ac.kr tspark@samsung.co.kr

Link layer security protocol in passive optical networks

Ajung Kim and Taesung Park^
Sejong Univ., Samsung Elec.^

요 약

차세대 통신망 중 효율적이고 경제적인 가입자망으로 각광받는 수동형 광 통신망은 점대 다의 트리형 토폴로지로 인해 기밀성이나 사용자 인증등 보안에 취약점을 안고 있어 보안 레이어의 정립을 필요로 하고 있다. 본 논문에서는 이더넷을 기반으로 한 Giga bps 급 이더넷 수동 광 통신망을 중심으로 가능한 보안 공격과 그에 대해 요구되는 보안 시스템의 요구 사항을 규정하고 이를 바탕으로 Ethernet bridge 와 연동하여 적용할 수 있는 port base 의 인증 절차와 메커니즘을 제안한다. 또한 암호화에 관계된 동작을 sub-MAC layer 에서 수행하는 보안 레이어의 설계과 메커니즘을 제안 분석한다. 이는 물리계층에서의 구현 방법에 비해 기존 네트웍 운영에 큰 부작용을 초래하지 않으면서 메세지 인증을 가능하게 하고 MAC 의 기능과 연동하여 flexibility 를 제공한다.

I. 서론

차세대 통신은 가입자 망에서의 대역폭 병목현상을 제거하기 위하여 가입자단까지 광 선로를 설치하는 광 가입자망 (Fiber To The X)을 요구하게 되었는데, 저비용의 광 가입자망 구축에 수동 전송 특성을 갖는 수동형 광통신망(PON)이 망 구성과 유지 측면에서 경제적이고 효율적인 광 가입자망 구현 방식으로서 각광받고 있다.

수동형 광가입자망 (PON)의 경우도 하나의 OLT 에 수동소자를 이용해 다수의 ONU 를 연결한 트리 구조를 형성해 토폴로지 상 무선 LAN 이나 이동통신에서와 같이 [1] broadcast and selection 의 원리를 따르고 있으므로 보안의 문제는 심각하며 이러한 문제는 공중망에 진입해 시장이 성장하는데 큰 걸림돌이 될 수 있는 상황이다.

보안이나 privacy 서비스를 논의하는데 있어 암호기술은 암호화와 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 [2].

Ethernet PON 의 국제 표준 기구인 IEEE 802.3ah 에서는 이러한 암호화를 담당하는 privacy layer 를 물리계층인 sub-RS layer 에 구축하자는 안이 있었다[3]. Sub-RS layer 의 경우는 preamble 에 보안 정보를 포함하는데 designator, 무결성 보장 등을 가용한 한 두 바이트에 담기에는 제한이 있을 것으로 보이며, 또한 이 경우는 MAC frame 전체를 암호화하게 되는데 MAC address 를 암호화하여 기밀성을 보장시킬 수 있으나 MAC address 를 암호화함으로써 management 문제나 비호환성 문제 등 그 부작용이 심각하여 bridged network 에서는 문제를 야기시킬 수 도 있을 것으로 보인다.

본 논문에서는 보안 시스템 구조와 메커니즘 분석을 통하여 차세대 광가입자망에서 요구되는 보안 시스템의 요구 사항을 Gigabit Ethernet PON (GE-PON)을 기반으로 한 광가입자망을 중심으로 정의하고 이를 바탕으로 GE-PON 에 적용할 수 있는 port base 방식의 인증을 제안하고 sub-MAC layer 에 privacy layer 를 구현하는 안을 제안 분석한다.

II. 본론

PON 의 토폴로지에 있어 downlink 에서는 broadcast 로 인해 다른 ONU 의 도청의 위험이 존재하고 uplink 에서는 점대다점 구조로 인해 인증받지 못 한 ONU 의 자원 접근이나 다른 ONU 의 변장(impersonation)의 위험이 있다. 데이터 암호화를 통해서 이러한 shared medium 을 점대점 링크의 집합으로 변환시킬 수 있다. 암호화를 통해 downlink 상의 도청과 uplink 의 변장을 방지할 수 있고 인증을 수행할 수 있는데 EPON 에서는 MPCP(multipoint control protocol)와 같은 링크 control 에 대한 트래픽과 OAM packet 역시 보호되야 할 필요성이 있다. 따라서 PON 에서 중심이 되어야 할 보안 서비스 이슈들은 ONU 인증, encryption, 그리고 키관리