2계층 보안을 위한 MACsec 어댑터

정낙주** · 서종균** · 한기천** · 김창수* · 정회경*

*배재대학교 · **(주)유비테크

MACsec Adapter for 2 Layer Security

Nahk-Ju Jeong* · Jong-Kyoun Seo* · Ki-Cheon Han* · Chang-Su Kim* · Hoe-Kyung Jung*

*PaiChai University · **UbiTech Co

E-mail : njjeong@gmail.com, {ice9422, kchan153}@naver.com, {MIE-ddoja, hkjung}@pcu.ac.kr

요 약

MACsec은 Layer 2에서 동작하는 암호화 기능이다. 최근 대두가 되고 있는 IoT(사물인터넷)와 같은 대규모 산업 분야의 장치들이 네트워크와 연결되면서 인터넷 트래픽이 급속도로 증가하고 있으며, 다양한 인터넷을 통한 공격의 위기에 놓여있다. 때문에 현재와 같이 트래픽이 증가하고 복잡해지는 상황에 특정 부분만이 아닌 트래픽 전체를 보호하는 MACsec 기술이 관심을 받고 있다.

이에 본 논문에서는 Layer 2 보안 기술인 MACsec을 기존 Layer2 네트워크에 간편하고 쉽게 추가할 수 있는 기술인 MACsec 어댑터를 설계한다.

ABSTRACT

MACsec is a cryptographic function that operates on Layer 2. As industries such as IoT(Internet of Things) devices are receiving attention recently are connected to the network and Internet traffic is increasing rapidly. Because of today, Becoming the increase in traffic and complex situations to protect the overall traffic, not just certain parts. The MACsec technology has received attention.

In this paper, Layer 2 security technology to MACsec. Design the technology MACsec adapter that can easily and readily added to existing Layer 2 network.

키워드

Encryption, ethernet, MACsec, L2 Security

Ⅰ. 서 론

인터넷을 통한 해킹, 정보 유출, 네트워크 공격과 같은 뉴스들이 연일 보도되고 있다. 이러한 네트워크를 통한 공격 및 정보 유출은 일부 악성 해커들뿐 아니라 적대적인 국가에 의해서도 발생할 수 있다. 최근에는 M2M이나 IoT와 같은 산업 분야의 장치들이 네트워크에 연결되면서 악의적으로 공격할 수 있는 취약점이 급격히 증가하고 있어서 네트워크에 대한 잠재적인 위협은 급속도로 증가되는 추세이다[1]. 때문에 이러한 상황에서 국가나 기업은 정보를 보호하고 네트워크를 안전하게 유지하기 위해서 많은 노력을 기울이고 있다. 데이터를 보호하기 위해서 기존에는 애플리케이션에서 직접 지원하는 SSL, TLS, SSH 등의 방법들이 많이 사용되었으나, 최근에는 특별한 보안 규칙없이 네트워크 전체의 모든 트래픽을 보호할 수 있는 방법들이 인기가 증가하고 있다. 이 논문에서는 MACsec 기능을 이용하여 L2에서 네트워크 트래픽 전체를 암호화 할 수 있는 어댑터 개발에 대한 내용을 다룬다[2-4].

Ⅱ. 시스템 설계

2.1 MACsec 어댑터 설계

기존에 캐리어 이더넷을 위한 MACsec 보안기

능은 해외의 네트워크 장비사에서 L2 스위치로 제공되고 있다. 이러한 MACsec기능을 지원하기 위한 Cisco, 주니퍼 네트워크 등의 장비는 MACsec의 지원을 위하여 RADIUS와 같은 인증 서버의 지원이 필요한 구조로 설계되어 있다. 이러한 구조는 대형 시스템에서 고비용을 투자하기에는 문제가 없지만, 기존 시스템을 재설계해야 하는 문제가 있다. 본 논문에서 구현하고 있는 MACsec 어댑터는 기존에 L2 네트워크 망이 구축된 상황에서 간단하게 L2의 보안 기능만을 향상시키기 위해서 적용할 수 있는 모델이다.

그림 5는 본 논문에서 설계된 MACsec 어댑터의 하드웨어 구조를 보여준다. 어댑터는 관리용 이더넷 포트 1개와 MACsec PHY 에 연결된 4개의 이더넷 포트를 가지고 있다. MACsec PHY의 이더넷 포트 중 2개는 L2 스위치의 WAN 입력을 위한 MACsec이 적용되지 않는 Normal 포트로 사용되며, 나머지 2개의 포트는 암/복호화를 위한 MACsec 포트로 사용된다. 본 논문에서 구현된 MACsec 어댑터 장비는 최대 2개의 L2 스위치 장비에 연결 될 수 있으며, 관리용 포트는 로컬망에서 MACsec 어댑터 장비에 대한 상태 모니터링 및 MACsec PHY 칩을 제어하는 역할을 담당한다.

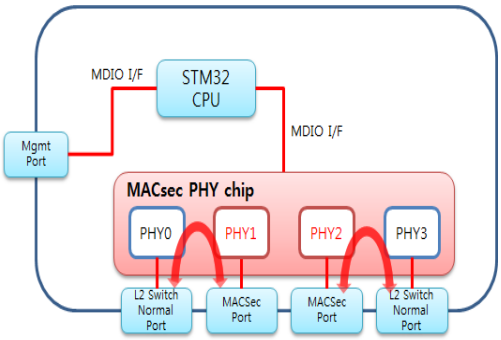

그림 1. MACsec Adapter H/W 구조도

그림 5에서 MACsec PHY를 기반으로 L2 암호화 통신을 하기 위해서는 외부에서 PHY 칩에 대한 보안 설정을 할 수 있어야 한다. 본 어댑터의 구현에서는 이 부분을 Cortex-M 계열 프로세서인 STM32F407을 사용한다. 이 프로세서에는 리눅스 계열 운영체제를 사용하여 PHY 칩을 제어할 수 있도록 한다. PHY 칩을 제어하기 위해서는 MDIO 인터페이스가 필요하며, STM32 계열 프로세서는 1개의 MDIO 인터페이스를 지원하고 있다. 그러나, 본 논문의 어댑터는 관리용 이더넷 포트를 위한 PHY 와 MACsec PHY 두 개와 연결이 필요하다. 그래서, MACsec PHY의 연결을 GPIO를 이용하여 별도로 구현한다.

그림 6은 본 논문에서 설계된 MACsec 어댑터 초기화 과정이다.

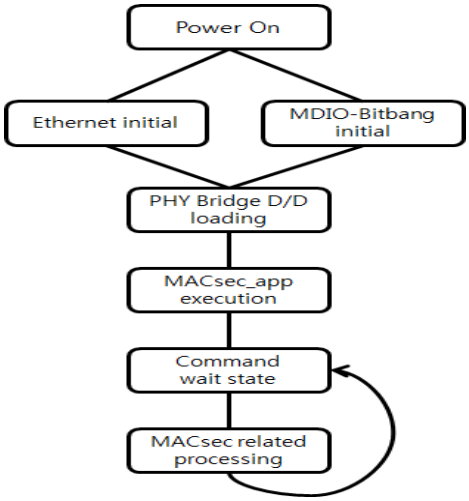

그림 2. MACsec Adapter의 흐름도

전원이 인가되면 관리를 위한 이더넷 포트를 초기화 하고, MACsec PHY 칩 제어를 위한 MDIO-Bitbang 디바이스 드라이버를 초기화 한다. 다음으로 MACsec PHY 칩 제어 응용프로그램과 MDIO-Bitbang 드라이버를 연결하기 위한 PHY Bridge 디바이스 드라이버를 커널에 등록 시킨다. 마지막으로 MACSec 설정을 위한 응용 프로그램인 MACsec_app을 실행한다.

MACsec_app 응용 프로그램은 MACsec PHY 칩을 초기화 한 후 보안키를 등록하고 SC(Secure Channel)를 생성한다. 생성된 SC에 대해서 보안키를 기반으로 데이터 암/복호화를 수행한다. 모든 MACsec PHY칩에 대한 설정이 완료되면 MACsec_app 제어 프로그램은 명령 대기 상태로 들어가 제어 및 상태 조회 등에 사용할 수 있다.

Ⅲ. 고찰 및 결론

최근 네트워크는 IoT의 확대와 LTE 네트워크와 같은 고속의 무선 기술들이 등장하면서 트래픽이 급격히 증가하고 보안 위협은 급속도로 증가하고 있다. 현재까지 대부분 네트워크 계층에서 전송되는 데이터의 보안 및 인증을 위해서 IP 보안 프로토콜인 IPsec 이나 어플리케이션 레벨의 보안 기능을 사용하여 암호화를 제공하고 있다. 그러나 이러한 기술들은 Layer 3에서 이루어지는 기술들로 Layer 2 프로토콜인 ARP, DHCP, Link Aggregation, Spanning Tree Protocol 등에 대한 공격에 대해서 방어할 수 없는 상태이다. 주요 네트워크 장비 업체들은 MACsec을 지원하는 스위치를 개발하여 RADIUS 시스템과 연동하여 서비스를 제공하고 있다. 이러한 시스템은 전체 시스템을 재구축해야하므로 많은 비용이 들어가게 된다. 본 논문에서는 MACsec 기능을 제공하는 PHY Chip을 이용하여 어댑터 형태로 MACsec 기능을

설계하였다. 또한 MACsec 어댑터를 이용하면 기존 L2 장비를 그대로 사용하면서 L2 보안을 위한 어댑터 형태로 MACsec 기능을 제공할 수 있다.

ACKNOWLEDGMENTS

This work (Grants No. C0297232) was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2015.

참고문헌

[1] Y. H. Kim, J. G. Yang and H. B. Kim, "Trends and threats of M2M / IoT," Korea Institure of Information Security & Cryptology, Vol. 24, No. 6 pp. 48-59, 2014.12

[2] IEEE Std. 802.1AE, Media Access Control (MAC) Security, IEEE, 2006.

[3] IEEE Std. 802.1AEbw, Media Access Control (MAC) Security, IEEE, 2013.