JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 5 : 972~978 May. 2016

레이어 2 보안을 위한 MACsec 어댑터 구현

정낙주[1] · 박병돈[1] · 박한수[2] · 서종균[2] · 한기천[2] · 정회경[1*]

Implementation of MACsec Adapter for Layer 2 Security

Nahk-Ju Jeong[1] · Byung-Don Park[1] · Han-Su Park[2] · Jong-Kyoun Seo[2] · Ki-Cheon Han[2] · Hoe-Kyung Jung[1*]

[1*]Department of Computer Engineering, Paichai University, Daejeon 35345, Korea
[2]Ubiquitous Technology Co, Daejeon 34126, Korea

요 약

MACsec 은 Layer 2에서 동작하는 암호화 기능으로, IEEE 802.1AE에서 정의하고 있는 국제 표준이다. 최근 주목을 받고 있는 IoT(사물인터넷) 와 같은 산업 분야의 장치들이 네트워크에 연결되면서 인터넷 트래픽이 급격히 증가하고 있으며, 다양한 인터넷 공격의 위기에 노출되고 있다. 기존의 네트워크 보안 기술들은 IPsec과 같이 Layer 3에서 이루어지는 경우가 많았다. 그러나 현재와 같이 트래픽이 급격히 증가하고 복잡해지는 상황에서는 특정 응용이나 프로토콜에 대한 보안 대신에 트래픽 전체를 보호하는 기능에 관심을 갖게 된다. 이러한 기술로 등장한 것이 Layer 2에서 트래픽 전체를 보호하는 기술인 MACsec 기술이다. 본 논문에서는 Layer 2 보안 기술인 MACsec을 기존 Layer 2 네트워크에 간편하고 쉽게 추가할 수 있는 기술로서 MACsec 어댑터를 제안한다. 그리고 MACsec의 특징 및 장점을 기술하고 실제 제품을 구현하여 시험을 진행한다.

ABSTRACT

MACsec is a cryptographic function that operates on Layer 2, the international standard defined in the IEEE 802.1AE. As industries such as IoT(Internet of Things) devices are receiving attention recently are connected to the network and Internet traffic is increasing rapidly, and is exposed to the risk of a variety of Internet attacks. Traditional network security technologies were often made in Layer 3, such as IPsec. However, to be increased as rapidly as the current traffic situation is complicated, and became interested in the security function of protecting the entire traffic instead of for a specific application or protocol. It appeared as these technologies is technology MACsec technology to protect all traffic in Layer 2. In this paper, we propose a Layer 2 security technology adapter MACsec MACsec a technology that allows you to simply and easily add them to the existing Layer 2 networks.

키워드 : 암호화, 캐리어 이더넷, MACsec, L2 보안

Key word : Encryption, Carrier ethernet, MACsec, L2 Security

Received 21 March 2016, **Revised** 24 March 2016, **Accepted** 08 April 2016

* **Corresponding Author** Hoe-Kyung Jung(E-mail:hkjung@pcu.ac.kr, Tel:+82-42-520-5640)
Department of Computer Engineering, Paichai University, Daejeon 35345, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.5.972 print ISSN: 2234-4772 online ISSN: 2288-4165

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. 이러한 상황에서 국가나 기업은 정보를 보호하고 네트워크를 안전하게 유지하기 위해서 많은 노력을 기울이고 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[1-3].

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. 가장 일반적인 네트워크 보안 프로토콜은 Layer 3에서 동작하는 IPsec일 것이다. IPsec은 매우 인기가 많은 프로토콜이지만 암호화 기능을 수행하는 엔진이 별도로 필요해서 암호화 비용이 많이 발생하는 문제가 있다. 또한 IPsec은 L2 기반 프로토콜인 ARP, DHCP, Link Aggregation, Spanning Tree Protocol 등에 대한 프로토콜에 대한 암호화를 지원하지 못하는 문제가 있다[4-6].

최근 캐리어 이더넷 L2 VPN 과 같은 서비스가 도입되면서, L2 에서의 암호화 기능은 사용하기 쉽고 오버헤드가 적으면서도 쉽게 확장할 수 있는 방향으로 발전하고 있다. IEEE는 802.1AE 표준으로 L2에서의 암호화 기능과 키 관리 기능인 MACsec 기능을 정의하고 있다[7].

본 논문에서는 MACsec 기능을 이용하여 L2에서 네트워크 트래픽 전체를 암호화 할 수 있는 어댑터 개발에 대한 내용을 다룬다.

Ⅱ. MACsec의 개요

네트워크에서 키 관리를 위한 KeySec과 함께 L2에서의 암호화 기술인 MACsec은 L2 이더넷 네트워크에서 데이터의 안전성과 기밀성을 보장하기 위한 보안 솔루션이다.

MACsec은 L2 이더넷 프레임을 DMAC (Destination MAC)과 SMAC(Source MAC) 다음부터 암호화 한다. 기본적인 이더넷 프레임 구조에 암호화를 위해 MACsec 파라미터를 포함한 보안 태그(SecTag:Security Tag)가 추가되며, 프레임의 뒤에 암호화 기법으로 생성하는 무결성 체크 값(ICV:Integrity Check Value)이 추가된다. L2 프레임의 마지막에 들어가는 FCS(Frame Check Sequence)는 ICV까지 반영하여 다시 계산된다. MACsec에서 실제 데이터 부분인 Payload를 암호화 할 것인가는 옵션 사항으로 암호화하지 않을 수도 있다. 그러나, 이 부분이 암호화 되지 않더라도 SecTag와 ICV를 사용하여 데이터의 무결성은 보장된다. 그림 1은 일반적인 이더넷 프레임과 MACsec이 적용된 이더넷 프레임의 모습을 보여준다.

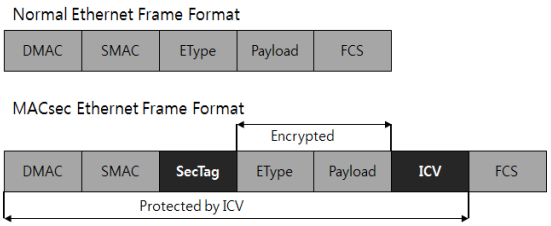

Fig. 1 Traditional MACsec Frame Format

전통적인 MACsec은 Port를 기반으로 네트워크를 보호한다. 즉, 네트워크 내부의 여러 장치들에 대해서 두 장치 사이에서만 기능을 지원한다. 이러한 기능을 Port 기반의 MACsec이라고 하며, hop-by-hop 보안 기능을 제공한다. 그림 2는 캐리어 이더넷 시스템에서 모든 물리적인 링크를 보호하기 위한 MACsec의 적용 예를 보여주고 있다.

Fig. 2 Structure Secured Hop-by-Hop with MACsec

본 논문에서 개발하는 MACsec 어댑터는 그림 2의 기본적인 MACsec 암호화 기법 외에 VLAN(Virtual Local Area Network)환경에서도 end-to-end로 어댑터

를 적용할 수 있도록 하는 VLAN Tag Bypass 기능을 지원하도록 한다.

이 기능을 지원하기 위해서는 칩셋 레벨에서 설정이 가능해야 하며 이러한 기능을 지원하는 MACsec 칩셋으로 Vitesse의 VSC8584를 사용한다.

전통적인 MACsec은 VLAN 태그를 인식하지 못한다. 그리고 해당 부분도 프레임 데이터의 일부로 판단하여 전체를 보호하기 위해서 SecTag로 감싸게 된다. Vitesse의 VSC8584를 사용하여 개발하는 어댑터는 VLAN 태그를 인식도록 설정할 수 있어서 태그를 건너뛰어서 실제 데이터 부분만 SecTag로 보호하게 된다. 이로 인해 L2에서 hop-by-hop 구간에서의 데이터 보호뿐 아니라 end-to-end에서의 데이터 보호가 가능하다. 그림 3는 이러한 VLAN 태그를 Bypass하는 기능을 표시한다.

이러한 VLAN 태그의 Bypass 기능을 사용하게 되면 그림 2에서 표현된 것처럼 모든 포트에 MACsec 어댑터를 적용하지 않아도 된다.

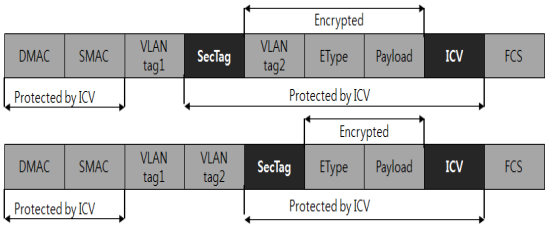

Fig. 3 MACsec Frame Format including VLAN Tag Bypass

그림 4는 그림 2에서 보여줬던 Hop-by-Hop 보안 적용 방식을 그림 4의 VLAN에서의 Tag Bypass 기능이 적용된 MACsec을 적용하여 end-to-end 보안 적용 방식으로 변경한 모습을 보여준다.

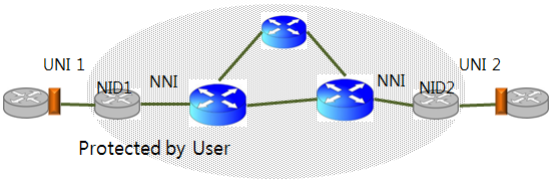

Fig. 4 Structure Secured End-to-End with MACsec

Ⅲ. MACsec 어댑터 설계 및 구현

3.1. MACsec 어댑터 설계

기존에 캐리어 이더넷을 위한 MACsec 보안기능은 L2 스위치로 제공되고 있다. 이러한 MACsec기능을 지원하기 위한 장비는 MACsec의 지원을 위하여 RADIUS와 같은 인증 서버의 지원이 필요한 구조로 설계되어 있다. 고비용 투자가 가능한 대형 시스템에서는 비용적인 문제가 없지만, 기존 시스템을 재설계해야하는 문제가 있다.

이를 해결하기 위해 기존의 L2 구축된 네트워크에서 L2의 보안 기능만을 향상시키기 위해서 적용할 수 있는 모델을 제안한다. 제안하는 모델은 추가적인 투자나 시스템 재설계를 진행하지 않아도 되는 이점이 있다.

그림 5는 본 논문에서 구현된 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 제어한다.

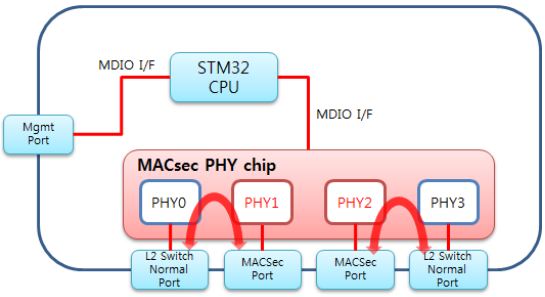

Fig. 5 MACsec Adpater H/W Structure

그림 5에서 MACsec PHY를 기반으로 L2 암호화 통신을 위해서는 외부에서 PHY 칩에 대한 보안 설정이 가능해야 한다. 어댑터의 구현은 Cortex-M 계열 프로세서인 STM32F407을 사용한다. 리눅스 계열 운영체제를 사용하여 PHY 칩을 제어할 수 있도록 하고 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. 이를 위해 MACsec PHY의 연결을 GPIO를 이용하여 별도로 구현한다.

그림 6은 본 논문에서 구현된 MACsec 어댑터 초기화 과정이다.

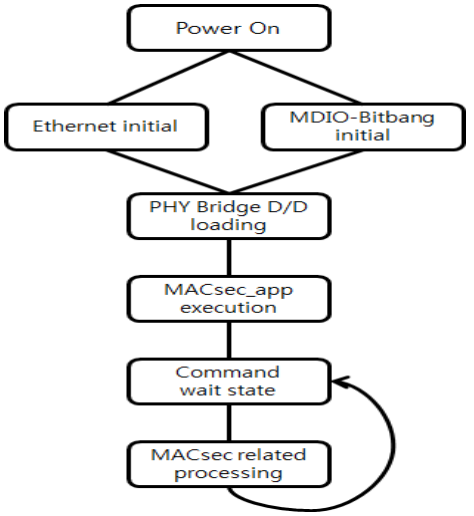

Fig. 6 MACsec Adapter Initial Flow-Chart

전원이 인가되면 관리를 위한 이더넷 포트를 초기화하고, 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.

본 논문에서 개발하는 어댑터를 실제 네트워크에 연결하면 그림 7과 같은 연결 모습을 갖게 된다.

그림 7은 기존 서비스 제공 사업자가 L2 네트워크를 구축한 상태이다. 네트워크에는 보안 기능이 추가되어 있지 않은 상태였다. L2 보안을 적용하기 위해서 사용자가 직접 네트워크의 양 끝단에 본 논문에서 제안하는 어댑터를 적용한 모습을 보여준다. 기존 네트워크에서 L2 보안을 제공하지 않았어도 손쉽게 보안 기능을 추가할 수 있다.

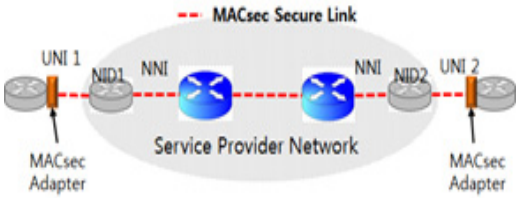

Fig. 7 Image of MACsec Adapter applied to The Existing Network

3.2. MACsec 어댑터 구현

구현된 MACsec 어댑터는 그림 8과 같다.

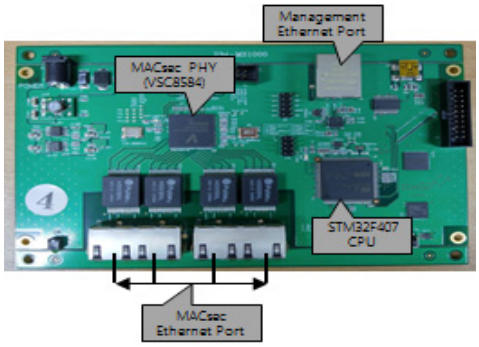

Fig. 8 Real Image of MACsec Adapter

그림 8은 MACsec PHY에 4개의 포트가 연결되어 있으며, 이 포트의 두 개는 WAN을 위한 이더넷 포트로 사용하고 나머지 두 개는 MACsec 보안 포트로 사용한다. 어느 포트를 MACsec 보안을 위해서 사용할 것인가는 소프트웨어로 설정할 수 있다.

본 논문에서 구현된 MACsec 어댑터 설정 프로그램 구성도는 그림 9와 같다.

위 프로그램은 세 가지 모듈로 구성된다.

- MACsec 제어 프로그램
  - ✓ MACsec PHY 칩 초기화

- ✓ MACsec 암호 설정 기능
- ✓ MACsec 채널 설정 기능
- ✓ MACsec PHY 상태 모니터 기능

• PHY bridge 디바이스 드라이버
- ✓ MACsec 제어 프로그램과 MDIO 드라이버 연결
- ✓ PHY read/write 명령을 디바이스 드라이버로 전달

• MACsec phy 칩 디바이스 드라이버
- ✓ PHY에 대한 read/write 기능 수행

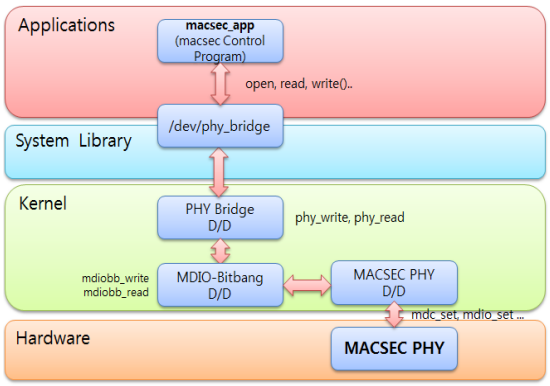

Fig. 9 MACsec Software Block Diagram

3.3. MACsec 어댑터 성능 시험

그림 10은 구현된 MACsec 어댑터의 기능을 검증하기 위한 실험 시나리오이다.

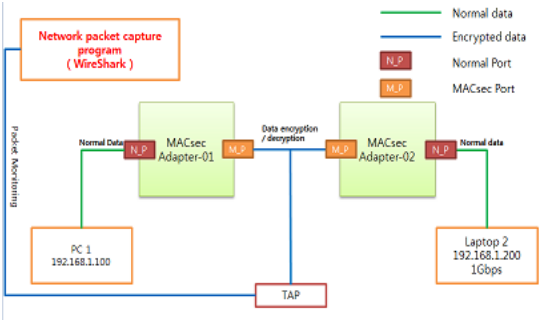

Fig. 10 Scenario of MACsec Operation Test

MACsec 어댑터 장비 1대와 PC 1대를 WAN 포트에 연결하고, MACsec 포트는 상대방 MACsec 어댑터 장비의 MACsec 포트에 연결한다. 그리고 WAN 포트를 노트북에 연결한다. 이때, 출력되는 패킷이 암호화된 패킷인지 확인하기 위해서 MACsec 포트의 LAN 선을 TAP(Test Access Point) 장비에 연결한 후 Wireshark과 같은 네트워크 모니터링 프로그램을 통해서 암호화가 정상적으로 이루어지는지 확인한다. 그림 11은 실제 MACsec 동작 테스트 환경이다.

그림 12는 평문 데이터와 MACsec이 적용된 패킷을 캡처한 화면이다.

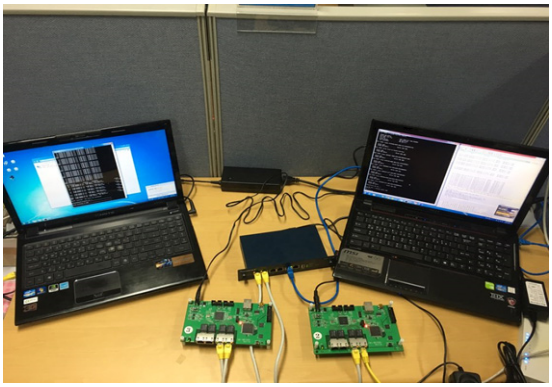

Fig. 11 MAcsec Operation Test

MACsec 동작 테스트는 ping 명령어를 이용하여 테스트를 진행 하였다. MACsec을 적용하지 않았을 경우에는 출발지 주소 / 목적지 주소가 IP 주소 형태로 모니터링 되며, 패킷 타입은 ICMP로 출력된다. MACsec을 적용한 후 캡처한 화면에서는 출발지 / 목적지 주소가 MAC 주소로 나오며, 이더넷 타입이 MACsec type (0x88e5)로 나오며, 데이터들이 암호화 되어있는 것을 확인할 수 있다.

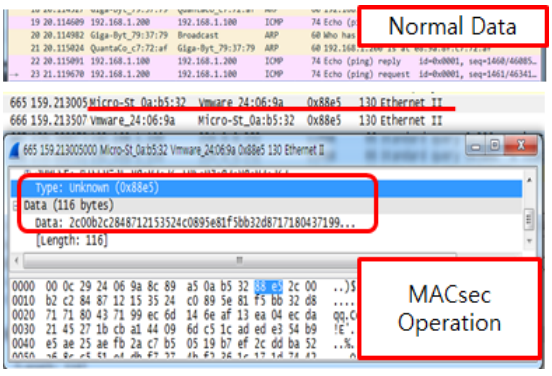

Fig. 12 Screenshot of MACsec Packet

Table. 1 MACsec Performance Test

Method	Throughput(Mbps)		
	Non-applied	MACsec	
		(GCM-AES-128)	(GCM-AES-256)
TCP	920	902	900
UDP	818	797	791

표 1은 MACsce 어댑터 실험 결과를 정리한 것이다. 본 논문에서 MACsec 어댑터는 128암호화 방식(GCM-AES-128)과 256bit(GCM-AES-256)을 적용하여 Throughput을 통한 성능 검증을 하였으며, MAcsec 암호화를 통한 속도 저하 1~2% 수준으로 성능 저하가 거의 없음을 알 수 있다.

- test program: iperf
- 수행횟수: 10회

Ⅳ. 결 론

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. 이에 IEEE는 IEEE 802.1AE로 데이터 링크 계층의 보안 기술인 MACsec에 대해 표준화를 진행하고 있으며, 이를 통해 데이터 링크 계층을 이용한 통신서비스에서의 기밀성, 데이터 무결성, 인증을 제공한다. 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 MACsec을 지원하는 어댑터를 개발하여 기존 L2 네트워크에 장착하여 Layer 2 보안 기능을 제공할 수 있도록 하였다.

본 논문에서는 MACsec 기능을 제공하는 PHY Chip을 이용하여 어댑터 형태로 MACsec 기능을 구현하고, 128bit/256bit 으로 MACsec 암호화 및 성능 시험을 진행하였다. 본 논문에서 개발한 MACsec 어댑터를 이용하면 기존 L2 장비를 그대로 사용하면서 L2 보안을 위한 어댑터 형태로 MACsec 기능을 제공할 수 있음을 알 수 있다.

향후 연구로는 다양한 실험을 통해 효율성을 검증하고 상용화 진행이 필요한 것으로 사료된다.

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.

REFERENCES

[1] Y. H. Kim, J. G. Yang and H. B. Kim, "Trends and threats of M2M / IoT," *Korea Institute of Information Security & Cryptology*, vol. 24, no. 6 pp. 48-59, Dec. 2014.

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

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

[4] T. K. Kang, T. S. Jung, J. H. Yoo, “Carrier ethernet technology and standard status.” ETRI ettrends, vol. 24, no. 3 pp. 78-90, June 2009.

[5] H. Altunbasak, S. Krasser, H. Owen, J. Grimminger, H. Huth. and J. Sokol, "Securing Layer 2 in Local Area Networks," *Networking-ICN 2005*, vol. 3421 pp. 699-706, April 2005.

[6] IEEE Std. 802.1X-2010, Standard for Local and metropolitan area networks - Port-Based Network Access Control, IEEE, 2010.

[7] microsemi. Quad Port Dual Media QSGMII/SGMII GbE PHY with Intellisec and VeriTime[Internet]. Available: http://www.microsemi.com.

정낙주(Nahk-Ju Jeong)

1992년 충남대학교 컴퓨터공학과(공학사)
1995년 충남대학교 컴퓨터공학과(공학석사)
2015년 ~ 현재 배재대학교 컴퓨터공학과(박사과정)
2015년 ~ 현재 ㈜유비테크 연구소장
※관심분야 : 임베디드 시스템, IoT, 모바일 보안

박병돈(Byung-Don Park)

1985년 충남대학교 전자교육공학과(공학사)
2007년 충남대학교 정보통신공학과(공학석사)
2016년 ~ 배재대학교 컴퓨터공학과(박사과정)
※관심분야 : IoT, 네트워크

박한수(Han-Su Park)

2011년 한밭대학교 컴퓨터공학과(공학사)
2014년 한밭대학교 컴퓨터공학과(공학석사)
2012년 ~ 현재 (주)유비테크 부설연구소 과장
※관심분야 : 임베디드 시스템, IoT, 모바일 보안

서종균(Jong-Kyoun Seo)

1998년 건양대학교 정보통신공학과(공학사)
2014년 충남대학교 산업시스템공학과(공학석사)
2003년 ~ 현재 (주)유비테크 부설연구소 부장
※관심분야 : 유무선 통신, 네트워크 보안

한기천(Ki-Cheon Han)

1986년 광운대학교 전자계산학과(공학사)
1998년 광운대학교 전자계산학과(공학석사)
1998년 한국전자통신연구원 선임연구원
2003년 ~ 현재 (주)유비테크 대표
※관심분야 : 임베디드 시스템, 유무선 통신, 네트워크 보안

정회경(Hoe-Kyung Jung)

1985년 광운대학교 컴퓨터공학과(공학사)
1987년 광운대학교 컴퓨터공학과(공학석사)
1993년 광운대학교 컴퓨터공학과(공학박사)
1994년 ~ 현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 멀티미디어 문서정보처리, XML, SVG, Web Services, Semantic Web, MPEG-21, Ubiquitous Computing, USN