http://dx.doi.org/10.7236/JIIBC.2013.13.2.77
JIIBC 2013-2-11

WiMax2 PKMv2 암호화 계층의 검증 및 성능 평가 테스트베드의 구축

Implementation of Verification and Evaluation Testbed of WiMax2 PKMv2 Encryption Layer

김장현*, 서효중**

Jang-Hyun Kim, Hyo-Joong Suh

요 약 모바일 인터넷 통신 표준인 WiMax2는 PKMv2 프로토콜을 이용한다. PKMv2는 키에 기반한 암호화를 사용하여 통신 기지국과 단말간의 데이터를 보호한다. 따라서 WiMax2 단말 또는 기지국을 개발하는 경우 PKMv2 프로토콜을 구현하여야만 하며, 상호 동작에 대한 적합성 테스트를 통과하여야 한다. 또한 저성능 프로세서를 이용하는 단말의 경우 암호화 모듈의 처리 성능이 WiMax2 통신의 데이터 처리 능력에 병목이 될 수 있으므로 해당 프로세서에서의 암호화 모듈 처리 성능의 적절성을 측정하여야 한다. 본 논문은 이러한 경우에 사용할 수 있는 WiMax2 PKMv2에 따르는 동작성 시험 및 성능 측정 테스트베드를 구현하였다.

Abstract PKMv2 security protocol was adopted by the WiMax2 mobile internet communication standard. A base station and a mobile station protect communication data using key based encryption according to the PKMv2 protocol. Consequently, each development of a base station and/or mobile station includes implement of the PKMv2 protocol, and the station must qualifies various interoperable tests. Furthermore, communication bandwidth of the station can be limited by the encryption module when the station implemented based on a low-performance processor. Thus, a correspondence measurement of the encryption module must be carried on the target processor. In this paper, we implement a testbed which affords throughput measurement as well as the interoperable tests by PKMv2.

Key Words : WiMax2, PKMv2, encryption test, Testbed

Ⅰ. 서 론

유비쿼터스 환경이 급속히 확장되어가고 있는 최근에 다양한 휴대 인터넷 기술은 스마트폰, 넷북 등 여러 기기에 수용되어 보급되고 있다. 이러한 무선통신의 대표적인 표준으로 WiMax(Worldwide Interoperability for Microwave Access)[1]나 LTE(Long Term Evolution)[2]를 들 수 있다. 휴대 인터넷은 개방되어 있는 무선 환경의 특성상 인증 및 보안을 반드시 필수로 하며, 프로토콜에서 보안 계층을 규정하여 기기와 기지국 간 안전한

*준회원, 가톨릭대학교 컴퓨터공학과
**정회원, 가톨릭대학교 컴퓨터정보공학부(교신저자)
접수일자 2013년 2월 8일, 수정완료 2013년 3월 8일
게재확정일자 2013년 4월 12일

Received: 8 February 2013 / Revised: 8 March 2013 / Accepted: 12 April 2013
**Corresponding Author: hjsuh@catholic.ac.kr
Dept. of Computer Science and Information Engineering, the Catholic University, Korea

통신을 보장하고 있다. WiMax 포럼은 WiMax 통신 표준을 따르는 기기들을 상호 호환을 보장하는 인증 체계를 두고 있으며, WFDCL (WiMax Forum Designated Certification Laboratories)와 WCB(WiMax Certification Bodies)[3]를 두어 WiMax 기기간의 상호 동작을 시험하고 인증을 부여하여 상호 호환을 보장하고 있다.

하지만 이러한 인증 기관에서의 인증 절차는 높은 시간당 비용이 부과되며, 절차적인 방법으로 인증의 항목별 통과 또는 실패 여부만을 테스트하므로, 항목 시험과 디버깅이 병행되는 프로토콜의 개발 진행 단계에서의 테스트과정과 큰 차이가 있다. 따라서 WiMax 관련 기기를 개발하기 위해서는 우선 표준 프로토콜에 따르는 기기를 시험 기기를 이용하여 자체 내에서 통신 시험을 진행하여야 되며[4], 이러한 내부적 시험을 완료한 후에 앞서 이야기한 공인 인증 기관에서의 인증 절차를 밟게 된다.

WiMax2의 보안 계층에 해당되는 프로토콜은 PKMv2[5]를 따르게 되는데, 이 보안 계층을 구현하여야만 기지국(base station)과 단말(mobile station) 사이의 접속 인증 및 데이터 전송을 구현할 수 있으므로 단말 또는 기지국의 개발에 있어서 이러한 보안 계층의 구현과 시험은 데이터 전송을 위한 가장 기본적인 부분이다.

본 연구는 이러한 필요성에 입각하여 단말 또는 기지국 개발 과정에서 WiMax2 PKMv2 프로토콜을 준수하여 동작하는지 시험할 수 있는 테스트베드를 구현함으로써 WiMax2 단말 또는 기지국을 개발하는 데 사용할 수 있도록 하고, 구현한 보안 계층에 문제가 있는지 전송 절차와 데이터를 감시할 수 있도록 하며, 또한 저전력 단말과 같이 낮은 성능의 프로세서를 사용한 기기에 개발된 보안 계층을 적용하는 데 있어서 WiMax2 데이터 대역폭을 및도는 병목의 발생 가능성 여부를 시험할 수 있도록 하는 것이다.

구현한 테스트베드는 WiMax2 보안 층에서 단말과 기지국이 서로 암호화를 하기 위한 키를 교환하고, 테스트베드의 단말기와 기지국 사이에 교환되는 데이터를 암호화 및 복호화 하며 테스트 대상 기기의 암호화 모듈이 정상적인 동작을 하는 지를 확인한다. 또한 테스트 데이터의 메시지 전달 과정을 모니터링 할 수 있도록 하여 테스트 기기의 암호화 모듈이 비정상 데이터를 생성할 경우 이에 대한 보고를 할 수 있도록 하였으며, 대상 장치의 암호화 및 복호화 처리 능력을 측정하여 대상 기기에서 발생할 수 있는 암호화 처리부분에 의한 데이터 병목 현상을 확인할 수 있도록 구성하였다.

본 논문의 구성은 다음과 같다. 우선, 2장에서 WiMax2 보안 층의 동작 메커니즘과 키 교환 동작 및 구현을 간략히 기술하고 PKMv2의 동작을 요약한다. 3장에서는 PKMv2 검증 테스트베드의 구성을 기술하고, 4장에서는 테스트베드의 성능을 평가한다. 마지막으로 5장에서 결론을 맺는다.

II. WiMax2 보안 층의 동작 메커니즘

WiMax2의 PKMv2를 따르는 보안 층 메커니즘은 인증 단계와 인증 후 암호화에 사용할 키를 생성하고 관리하는 단계로 구성되어 있다. 단말기과 기지국은 처음 통신 연결 개시 과정에서 해당하는 통신사의 허용된 단말기인지 인증(authentication)하는 과정을 진행 한다. 인증 완료 후에 실질적으로 암호화를 담당하는 키를 단말기과 기지국 사이에서 생성 및 교환하고 차후 이 키에 기반하여 데이터의 암호화 및 복호화를 수행한다[5].

인증 과정은 EAP(Extensible Authentication Protocol)[6] 기반 인증 방식, RSA[7] 기반 인증 방식, EAP 기반 인증과 RSA 기반 인증이 동시에 사용 되는 경우, 총 세 종류의 인증 방식이 있다. EAP와 RSA방식 모두 우선 키 생성에 필요한 데이터들을 단말기에 보내게 되며, EAP 기반 인증 방식을 사용한 경우는 인증 절차를 진행하여 단말기는 기지국으로부터 EAP 프로토콜을 통해 MSK(Master Session Key)을 받게 된다. RSA 기반 인증 방식을 이용할 경우에는 인증 절차를 진행한 후에 단말기는 기지국으로부터 RSA 프로토콜을 통해 Pre-PAK(primary authorization key)을 받게 된다. EAP 기반 인증과 RSA 기반 인증이 동시에 사용 될 경우 기지국은 MSK, Pre-PAK에 대한 각각의 인증을 단말기에 전송한다. 단말기는 기지국으로부터 받은 MSK, 또는 Pre-PAK으로부터 인증키 AK (Authorization key)를 유도하고 키 교환 절차를 완료한다.

인증의 첫 단계인 키 교환이 완료된 후 기지국과 단말기는 이 키를 이용하여 PKMv2 3-way handshake 절차를 진행함으로서, 실질적으로 통신 데이터의 암호화에 사용하는 TEK (Traffic Encryption Key)를 생성하고 단말기는 기지국 상호간에 이 TEK를 공유하게 된다. 그

림 1은 WiMax2 기지국과 단말기간의 PKMv2 3-way handshake 과정을 도시한 것이다.

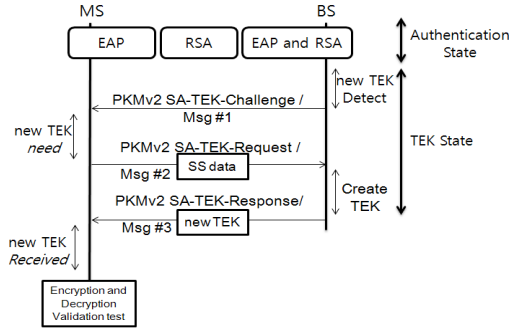

그림 1. WiMax2 PKMv2프로토콜 인증 및 TEK 생성
Fig. 1. Authentication and TEK generation of the WiMax2 PKMv2

기지국과 단말기 사이의 3-way handshake 과정은 크게 AAI-PKM-RSP (PKMv2 SA-TEK-Challenge), AAI-PKM-REQ (PKMv2 SA-TEK-Request), AAI-PKM-RSP (PKMv2 SA-TEK-Reponse)으로 나눌 수 있다. 첫 번째로 우선 기지국으로부터 TEK 가 새로 생성될 필요가 있거나 갱신되었음을 알리는 PKMv2 SA-TEK-Challenge 메세지를 단말기가 받게 된다. 두 번째로 메시지를 받은 단말기는 TEK를 갱신받기 위해 PKMv2 SA-TEK-Request 메시지를 기지국으로 보내 TEK 갱신을 요구하고, 세 번째로 기지국은 다시 단말기로 PKMv2 SA-TEK-Reponse를 보내 TEK를 생성하여 공유하게 된다.

이와 같이 여러 단계를 거쳐 생성한 TEK은 기지국과 단말기 간의 데이터를 암호화할 때 사용하게 된다. 본 논문에서 구현한 테스트베드는 테스트베드 내의 가상의 기지국을 구현하여 미리 정한 키를 기지국과 단말기 사이에 공유하도록 하였으며. 초기 인증 절차를 완성하고 이 후로부터 이루어지는 PKMv2 3-way handshake 교환 단계로부터 TEK의 생성 및 생성된 TEK를 이용한 데이터의 암호화와 복호화 부분을 모두 진행한다.

III. WiMax2 테스트베드 구현

1. 테스트베드 동작 형태

본 논문에서 구현한 테스트베드는 WiMax2 프로토콜 진행 및 암호화 계층에 해당되는 모듈의 검증과 성능을 확인하는데 그 목표가 있다. 따라서 이러한 소프트웨어 계층을 테스트하기 위해 실제 기지국과 무선 통신을 구축하여야 할 필요가 없으며, 물리 계층에 해당되는 RF 부분은 TCP/IP 프로토콜을 이용하도록 하였다. 따라서 테스트베드는 독립적인 유무선 네트워크로 연결된 PC를 이용하여 기지국과 단말 역할을 수행하도록 하거나, 한 대의 피씨에서 기지국과 단말에 해당되는 가상머신을 구축하여 TCP/IP 통신을 이용한 메시지 교환을 하도록 구현할 수 있다. 이러한 방법은 물리적인 무선 계층 환경과 무관하게 상위 계층 프로토콜 부분만을 독립적으로 테스트할 수 있는 장점을 가지며, 특히 단말 개발에 있어서 단말을 직접 PC와 USB 또는 이더넷 등으로 연결하여 TCP/IP 연결을 경유할 수 있도록 하여 무선 계층과 분리하여 테스트 할 수 있으므로, 개발 단말에서 무선 계층의 영향 없이 소프트웨어 검증과 성능 측정을 시험할 수 있게 한다[8][9].

그림 2는 간편하게 한 대의 PC를 이용하여 VMWare[10]를 이용한 가상머신으로 구축한 일례로, 한 대의 리눅스 가상머신은 기지국 역할을 수행하도록 하고, 복수 개의 리눅스 가상머신을 단말 역할을 수행하도록 구성한 것이다. 우선 기지국 역할을 하는 리눅스 가상머신 서버가 가동 된 상태에서 단말 역할을 하는 가상머신을 실행하여 기지국과 장치 간에 TCP 연결을 시킨다. 이 TCP 연결이 설정되면 사용자는 기지국과 장치 간에 PKMv2 프로토콜에 따른 암호화 및 복호화 메커니즘을 실행할 수 있다. 또한 연결을 진행하는 단계와 데이터의 암호화 및 복호화 내용은 실시간으로 모니터링 및 로깅 됨으로써 정확한 데이터의 전달과 오류의 발생을 확인할 수 있다.

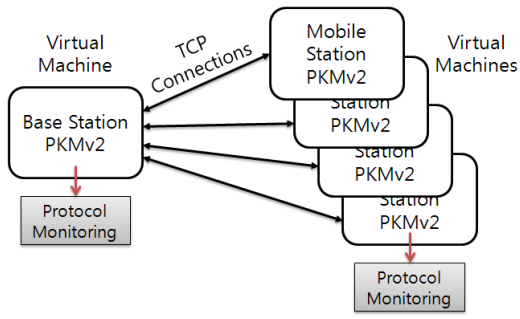

그림 2. 가상 머신을 이용한 테스트베드의 간단한 구축형태
Fig. 2. Simple implement of a testbed using virtual machines

다음 그림 3은 WiMax2 PKMv2에 따르는 인증 및 각 단계에 대응하여 테스트베드에 구현되어 있는 프로그램 모듈을 도시한 것이다.

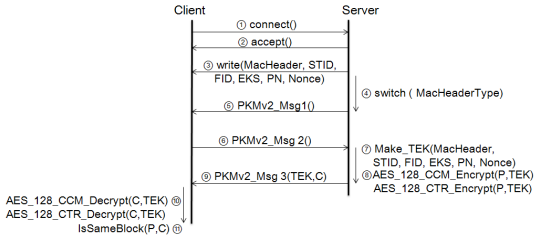

그림 3. 테스트베드에서 WiMax2 PKMv2 진행 절차
Fig. 3. Procedure of the WiMax2 PKMv2 in the testbed

기지국 역할을 하는 서버와 단말기의 역할을 하는 클라이언트는 ①과 ②와 같이 TCP/IP 를 통해 서로 연결되며 테스트를 시작한다. TEK의 생성 및 교환 알고리즘에 필요한 데이터와 키들은 미리 구성하거나 생성하며, TEK를 생성하기 위한 키는 ③과 같이 서버와 클라이언트 간에 서로 공유하도록 한다. 그 다음 서버는 ④에서 앞으로 보낼 패킷의 종류를 파악하고, ⑤에서 PKM Msg #1를 보내도록 한다. PKM Msg #1를 받은 클라이언트는 TEK 생성 요청을 위해 서버로 ⑥과 같이 PKM Msg #2를 보낸다. 클라이언트로부터 PKM Msg #2를 받은 서버는 ⑦과 같이 Make_TEK 함수를 통해 임의로 정한 데이터들로 TEK를 생성하고, ④에서 파악한 패킷 종류에 따라 ⑧번처럼 AES_128_CCM 방식 또는 AES_128_CTR 방식으로 패킷을 암호화한다. TEK 생성과 패킷 암호화가 다 끝나면 서버는 클라이언트로 ⑨와 같이 PKM Msg #3를 보내는 동시에 TEK와 암호화된 패킷을 보낸다. 클라이언트가 서버로부터 PKM Msg #3과 TEK, 암호화된 패킷을 받게 되면 ④에서 파악한 패킷 종류에 따라 ⑩번처럼 AES_128_CCM 방식 또는 AES_128_CTR 방식으로 암호화된 패킷을 복호화하고, 최종적으로 ⑪번의 IsSameBlock 함수를 사용하여 수신된 패킷의 암호화 및 복호화 과정이 제대로 되었는지 검증하고 모니터링한다.

2. PKMv2 암호화 검증 프로그램

테스트베드에서 개별적으로 기지국과 단말의 역할을 수행하는 프로그램은 각각 하나의 서버와 여러 클라이언트로 구성되는데, 서버는 기지국에 대응되며 클라이언트는 단말의 역할을 수행하는 형태가 된다. 서버와 클라이언트는 임의로 정한 키를 인증 절차로 공유하고, 3-way handshake 및 PKM 과정을 수행하여 TEK를 생성하고, 이 TEK를 이용하여 데이터의 암호화를 하게 된다. 이러한 절차와 단계에 있어서 테스트베드는 각 단계별 진행 상황과 전송 데이터에 대해 모니터링 및 로깅을 제공하며, 처리 데이터의 전송률을 측정한다.

그림 4는 이러한 프로토콜 모니터링 내용을 표시한 것으로, 서버와 클라이언트 사이에서 진행하는 프로토콜의 단계별 진행 상황과, 암호화되어 송수신된 패킷의 원 데이터와 복호화 된 데이터이다. 만약 수신된 패킷의 복호화에 실패한 경우 상세한 오류 내용을 확인할 수 있다.

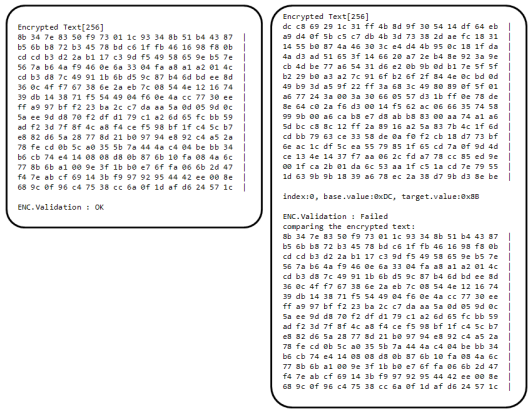

그림 4. 패킷 모니터링: 성공 및 실패한 경우
Fig. 4. Packet monitoring: success and failure cases

IV. 성능 평가

무선 통신 기지국 또는 단말을 개발할 때, 기지국의 경우 단말 몇 대의 동시 연결과 데이터 전송을 수용할 수 있도록 할 것인지 성능 기준을 설정하여야 하며, 단말의 경우에도 물리계층의 최대 전송 대역폭을 충분히 활용할 수 있는 데이터 처리 능력을 보일 수 있는지 검증하여야만 한다. 이러한 기지국 또는 단말은 전용 임베디드 시스템으로 구성되며, 특히 단말의 경우 낮은 성능의 메모리와 프로세서를 사용하는 것이 일반적이다. 하지만 무선 통신 대역폭은 OFDM(Orthogonal Frequency Division

Multiplexing)[11] 기술 등으로 지속적으로 데이터 전송 능력을 확대하고 있으며, 따라서 소프트웨어 프로토콜 처리 능력이 데이터 전송의 병목으로 작용할 수 있다.

본 논문에서 구축한 테스트베드의 경우 앞서 제시한 바와 같이 물리 계층 부분을 분리한 형태로도 시험할 수 있는 환경을 제공하므로, 프로토콜 처리 및 암호화 계층의 소프트웨어적인 처리 능력을 측정할 수 있다. 테스트베드에서 측정 가능한 최대 처리 능력은 테스트베드가 구축되는 시스템의 성능에 따라 달려 있으므로, 요구 성능에 적합하게 테스트베드의 사양을 구성할 수 있다. 표 1은 본 논문의 구현에서 사용한 테스트베드의 하드웨어 및 운영 환경 사양으로 일반적인 데스크톱 시스템에 사용되는 것이다.

표 1. 구현한 테스트베드의 시스템 사양
Table 1. System specification of the testbed

Testbed system specification	
Processor	Pentium 4 3GHz
Main memory	2 GB
Host OS	Windows XP
Virtual machine OS	VMWare, Ubuntu 10.04

암호화 및 복호화 패킷 처리량의 성능 측정은 기지국과 단말을 모두 동일 기기에 수행시키고 물리적인 네트워크 어댑터를 경유하지 않도록 동일 머신 내에서 TCP로 연결하여 동작시켰으며, 리눅스의 time.h 라이브러리의 clock_gettime 함수를 사용하여 프로토콜 암호화 및 복호화 시간을 측정하였다. 송수신 패킷의 길이는 64~256바이트를 적용하였으며, 동일 패킷 길이에 대하여 10,000개의 패킷을 반복하여 송수신하였다. 실험 결과, 논문에서 구축한 테스트베드의 경우 표 2와 같은 처리율을 보여주었다.

표 2. 구현한 테스트베드의 프로토콜 처리율 측정치
Table 2. Measured throughput of the testbed

Packet size(bytes/packet)	Throughput(Mbytes/sec)
64	209.72
128	486.24
256	1209.46
512	3355.44

측정 결과에 따르면, 논문에서 구축한 테스트베드의 암호화 및 복호화 처리율은 WiMax2의 최대 전송률을 크게 상회하고 있으므로 WiMax2 통신 단말의 개발에 따른 암호화 및 복호화 검증을 위한 동작을 수행하기 위해 충분함이 확인 되었으며, 필요에 따라서 보다 고성능의 프로세서 및 메모리를 채용한 기기로 테스트베드를 구축한다면 더욱 높은 측정 한계를 보여줄 것으로 판단된다.

V. 결 론

본 논문은 WiMax2 기지국 또는 단말 개발 시에 사용할 수 있는 암호화 및 복호화 검증 및 성능평가 테스트베드를 구축하였다. 본 연구에서 개발된 테스트 베드는 WiMax2 PKMv2 보안 층의 구현을 검증할 수 있고, 높은 비용이 들어가는 WiMax2의 공인 인증 절차 이전에 내부 개발 과정에서 사용되어 신뢰성 있는 테스트 환경을 제공하게 될 것이다. 또한 WiMax2 기기의 프로토콜 계층상에서 암호화 및 복호화 부분의 최대 데이터 처리 능력과 병목 현상을 감지할 수 있어, 점차 고속화되는 무선 통신 물리 계층의 대역폭 확장에 대응하는 암호화 계층의 성능 개선 진단 요구의 역할도 할 수 있을 것이다.

현 WiMax2 구축 확산의 가장 큰 걸림돌은 PKMv2의 복잡한 인증과 암호단계이다. 다행히, PKMv2보다는 훨씬 간단한 PKMv3가 곧 개발될 전망이다. PKMv3는 간단한 인증 메커니즘으로 WiMax2의 상호 연동성을 크게 향상시킬 것으로 보인다. 향후 PKMv3에 대응한 인증 과정에 필요한 암호화 및 성능 평가 테스트베드로의 확장을 수행할 예정이다.

참 고 문 헌

[1] "IEEE Std. 802.16e-2005", Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, IEEE, 2006.

[2] D. Astely, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom, S. Parkvall, "LTE: the evolution of mobile broadband", IEEE Communications Magazine, Vol. 47. No. 4, pp. 44-51, 2009.

[3] Daan Pareit, Bart Lannoo, Ingrid Moerman, Piet Demeester, "The History of WiMAX: A Complete Survey of the Evolution in Certification and Standardization for IEEE 802.16 and WiMAX", IEEE Communications Surveys & Tutorials, Vol. 14, No. 4, pp. 1183-1211, 2012.

[4] Yu-Doo Kim, Il-Young Moon, "Design of Testbed for Performance Evaluation of Peer-to-Peer Protocols in Mobile Networks", Journal of Korean Institute of Information Technology, Vol. 8, Issue 10, pp. 159-166, Oct. 2010.

[5] David J, Jesse W., "Overview of IEEE 802.16 Security", IEEE Security and Privacy, Vol. 2, No. 3, pp. 40 - 48, 2004.

[6] J. Arkko, V. Lehtovirta, P. Eronen, Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'), IETF Trust, 2009.

[7] Steve Burnett, Stephen Paine, The RSA Security's Official Guide to Cryptography, McGraw-Hill, 2001.

[8] Dae-Woo Choi, "Implementation of a Testbed for Wireless Sensor Network, Journal of the Korea Academia-Industrial cooperation Society", Vol.12, No.1, pp. 445-450, 2011.

[9] Xiao-Lei Zhang, Ye Wang, Jang-Geun Ki, Kyu-Tae Lee, "Simulation model of a multihomed node with WiMAX and WLAN", The Journal of the Institute of Webcasting, Internet and Telecommunication, Vol. 10, Issue 3, pp. 111-119, 2010.

[10] Rosenblum, Mendel. "VMware's Virtual Platform ™", Proc. Hot Chips, pp.185-196, 1999.

[11] Ye Geoffrey Li, Orthogonal Frequency Division Multiplexing for Wireless Communications, Springer-Verlag Berlin, 2009.

저자 소개

김 장 현(준회원)

- 2013년 ~ 현재 : 가톨릭대학교 컴퓨터공학과 석사과정
- 2013년 : 가톨릭대학교 컴퓨터정보공학 학사

<주관심분야 : 모바일 시스템, 내장형 시스템, 이동 통신>

서 효 중(정회원)

- 2003년 ~ 현재 : 가톨릭대학교 컴퓨터정보공학부 부교수
- 2000년 ~ 2003년 : 지씨티리서치 연구원
- 2000년 : 서울대학교 컴퓨터공학 박사
- 1994년 : 서울대학교 컴퓨터공학 석사
- 1992년 : 서울대학교 학사

<주관심분야 : 컴퓨터 구조, 컴퓨터 시스템, 내장형 시스템, 이동 통신>