JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 11 : 2014~2020 Nov. 2016

GNU Radio 기반 블루투스 통신 취약점 분석

김태용[1*] · 이훈재[2]

Vulnerability Analysis of Bluetooth Communication based on GNU Radio

Tae-Yong Kim[1*] · Hoon-Jae Lee[2]

[1*]Division of Computer Engineering, Dongseo University, Pusan 47011, Korea
[2]Division of Computer Engineering, Dongseo University, Pusan 47011, Korea

요 약

일반적으로 스마트 도어락을 이용한 공공 시설물 관리 시스템은 블루투스 무선 통신 구간에서 항상 보안 취약점을 가지게 된다. 특히 인증 절차 과정에서 비밀키와 같은 중요한 정보를 교환할 때는 주로 무선 구간에서 공격자에 노출될 위험이 높다. 그러므로 무선 구간에서 교환되는 정보는 적절하게 암호화되어 전송될 필요가 있다. 지하철 환기구와 같은 공공 시설물 관리 시스템의 보안 취약점을 분석하기 위해서 GNU Radio 플랫폼과 HackRF 장비의 도입을 통해 소프트웨어적 전력분석 공격이 효율적으로 수행 가능함을 확인하였다. 실험장비를 통해 얻어진 무선 패킷은 패킷 타입, CRC, 데이터 길이 및 데이터 등으로 간단하게 디코딩할 수 있으며 이는 보안취약점 개선에 활용될 예정이다.

ABSTRACT

In general, automatic access control management system using smart door-lock must be always exposed to security vulnerability during wireless communication based on Bluetooth. In particular, important information such as a secrete key can be exposed to the attacker when the authentication protocol has been operating in the wireless section. Therefore important information exchanged in the radio section needs to be properly encrypted. In order to analyze security vulnerability for automatic access control management system of public facilities such as subway vent, GNU Radio platform and HackRF device will be considered and experimented. Proposed experimental system to perform software based power analysis attack could be very effectively applied. As a result, important information such as packet type, CRC, length of data, and data value can be easily decoded from wireless packet obtained from HackRF device on GNU Radio platform. Constructed experimental system will be applied to avoid some security problems.

키워드 : GNU Radio 플랫폼, 출입관리, 스마트 도어락, 전력분석, 프로토콜 분석, HackRF

Key word : GNU Radio platform, Access control, Smart door-lock, Power analysis, Protocol analysis, HackRF

Received 30 October 2016, **Revised** 01 November 2016, **Accepted** 08 November 2016

* **Corresponding Author** Tae-Yong Kim(E-mail:tykimw2k@dongseo.ac.kr, Tel:+82-51-320-1738)
Division of Computer Engineering, Dongseo University, Pusan 47011, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.11.2014 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

오늘날, 블루투스 통신기능은 컴퓨터, 스마트폰, 아이팟, 태블릿 PC, 스피커, 게임 컨트롤러 등 거의 모든 기기에 내장되어 사용되고 있다. 또한 사실 부정한 목적으로 이들 블루투스 기기에 대한 해킹 사례들은 꾸준히 보고되고 있다.

사진, 전자메일, 텍스트 등과 같은 기본 정보를 블루투스 통신 기반에서 교환하는 과정 중에 부정한 목적으로 공격을 당하면 공격대상의 장치 제어 및 이러한 장치에 불필요한 정보를 전송하여 정보 손상을 유도 시키는 행위도 가능하다.

블루투스 해킹을 위해서는 블루투스에 내장된 보안 기능을 이해할 필요가 있으며, 이에 따른 취약점 분석을 통해 보다 안전한 블루투스 통신을 보장할 수 있다. 일반적으로 근거리 통신을 목적으로 하는 블루투스는 2.485GHz의 주파수 대역에서 초당 1600홉에 해당하는 주파수 호핑 확산 스펙트럼을 사용한다[1]. 통신 범위는 10m 이내의 거리에서 가능하지만 특수 안테나를 사용하면 더 넓은 통신 커버리지를 달성하는 것도 가능하다.

두 개의 블루투스 장치를 연결하는 과정을 페어링이라고 부르며 임의의 검색 가능한 블루투스 장치는 이름, 클래스, 서비스 목록 및 기술정보 등을 전송하게 된다[1]. 페어링이 완료되면 이들 블루투스 기기는 미리 공유된 비밀키 또는 링크키를 교환한 뒤에 다음 연결에서 디바이스를 식별할 목적으로 이 정보를 저장하게 된다.

일반적으로 그림 1에서의 블루투스 장치 스택의 모든 프로토콜을 사용할 필요가 없다. 블루투스 스택은 데이터 통신 이외에도 다양한 용도로 블루투스 기능을 사용할 수 있도록 개발되고 있으며 일반적인 응용 프로그램은 이 스택 중 하나의 수직 슬라이스를 사용하고 있다[1].

블루투스 보안은 몇 가지 기술을 기반으로 한다. 첫 번째로는 주파수 호핑을 들 수 있다[1]. 마스터와 슬레이브 디바이스끼리는 주파수 호핑 알고리즘을 공유하고 다른 디바이스는 이를 알지 못한다. 둘째, 페어링 과정에서는 사전 공유키 인증 또는 암호화 (128 비트)를 사용한다. 블루투스에 대한 세 가지 보안 모드는 다음과 같다.

- 보안 모드 1 : 활성 보안.
- 보안 모드 2 : 서비스 수준의 보안을 제공한다. 중앙 집중식 보안 관리자 인증, 구성 및 권한 부여를 처리하며 사용자가 활성화되지 않을 수 있다. 디바이스 수준의 보안은 제공하지 않는다.
- 보안 모드 3 : 장치 수준의 보안을 제공한다. 인증 및 암호화는 비밀키를 기반으로 항상 낮은 수준의 보안 연결에 적용된다.

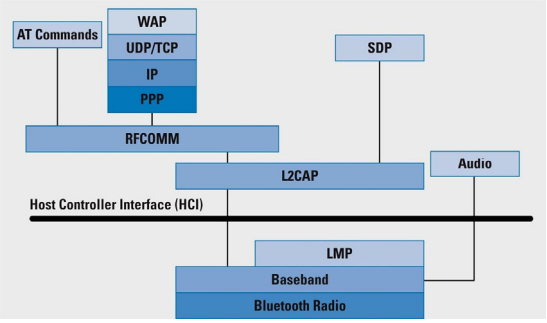


Fig. 1 Bluetooth layer protocols

그러나 기본적으로 제공되는 보안모드만으로는 기본적인 취약점을 보완하기 힘들며 통신거리 범위 내에서는 통신 중에 발생하는 신호원에 대한 보안대책은 거의 어려운 상태이다.

본 연구에서는 소프트웨어에 기반하여 무선통신 시스템을 용이하게 구축할 수 있는 GNU Radio[2] 플랫폼을 이용하였다. 블루투스 무선신호 공격에 필요한 전력 샘플링 과정과 신호 추정에 요구되는 신호처리 과정을 자동화 시킬 수 있는 효율적인 방안을 연구하고 그 활용 범위를 확인하였다.

Ⅱ. 연구 배경

공공시설물 중 하나인 지하철 환기구는 차단시설이 미비하고 인도와 똑같은 높이의 환구로 설치되어 있어 일반인이 쉽게 접근할 수 있어 불법 침입사건 및 안전사고의 주요 요인이 되고 있다[3].

부산시에서 운영하는 공공 인프라에 대한 출입관리 시설 현황을 살펴보면 부산 시내 도시철도 1-4호선에 설치된 환풍구는 총 832곳으로서 지표면에서 0.2-0.7m 가량인 배기구가 464곳을 차지하고 있다(그림 2 참조).

따라서 시설물 관리 권한이 없는 일반 시민이 접근할 수 있는 시설물이 안전과 동떨어진 상황에서 전통적인 시설물 관리 절차에 따라 방치되고 있어 보다 체계적이고 안전한 방법으로 시설물 관리를 수행할 필요가 있다.

최근에는 전통적인 물리보안 산업이 컴퓨터, 네트워크상의 정보를 보호하는 IT 정보보안 기술과의 접목을 통해 차세대 고부가가치 융합보안 서비스 산업으로 급부상하고 있다[4]. 따라서 공공 시설물 운영에 따른 출입관리 시설에 대한 IoT 기반의 출입관리 시스템을 구축하고 정보보안 기술의 접목을 통하여 시민의 안전을 확보하면서 체계적이고 효율적인 출입관리 시스템 구축이 시급하다.

본 연구에서는 블루투스 근거리 통신을 활용한 스마트폰 인증키 기반 출입관리 시스템을 설계하고 중앙시스템을 거친 인증만으로 지하공동구 개폐기 사용이 가능하도록 하여 높은 보안설정과 출입 인력에 대한 관리가 가능한 통합 출입관리 시스템을 설계하고 있다[3].

Fig. 2 Door-lock system exposed subway vent

Ⅲ. 블루투스 기반 출입관리 시스템

3.1. 시스템 요구사항

일반적으로 지하철 환기구의 특수 환경을 고려할 때 네트워크/전력선 인프라의 부재, 시설물의 디지털 도어락 이용을 위한 리더기가 야외에 노출되어 있는 등의 문제점 등이 먼저 개선될 필요가 있다.

대다수의 시설물 관리 대상은 그림 2와 같이 야외에 단순 노출된 상태로서 시설물 관리사무소에서 키를 수령 받은 관리자만 접근할 수 있어야 하지만 일반인도 이러한 시설물에 접근 가능한 상태이다.

시설물 관리자가 관리 사무소에 직접 방문하지 않고 인증 시스템을 통해 실시간으로 인증키를 발급받고 시설물에 접근 가능하도록 하여 업무의 효율성과 비인가자의 접근을 통제할 수 있도록 시스템을 재설계할 필요가 있다.

3.2. 블루투스 기반 출입관리 시스템

출입관리 시스템 서버는 HTTP, MQTT 프로토콜을 이용하여 Push 형태의 데이터를 전달하는 서버로서 출입요청 및 허가, 이력관리 등을 위한 데이터 전달, 암호화 인증 역할을 수행한다. 그림 3에 나타낸 것처럼 모바일 App은 출입관리 시스템 서버와 게이트웨이 역할을 하며 출입 도어락 제어 인증 및 긴급 출입요청, 출입자 위치정보 등을 제공한다[3].

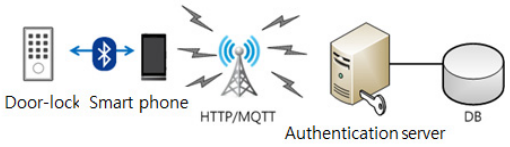


Fig. 3 Access control system based on Bluetooth

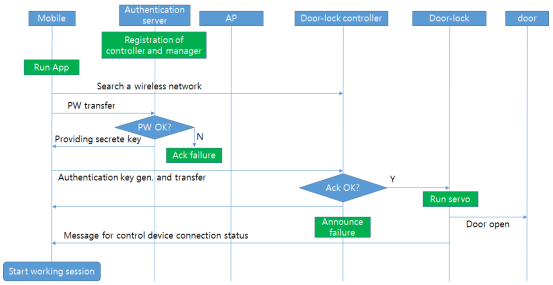


Fig. 4 Authentication procedure of smart door-lock

출입 인증 모바일 App 및 출입관리 서버가 만족하여야 하는 기본 요구사항을 간략하게 정리하면 다음과 같다[3].

- 모바일 App: 출입자 인증 기능, 출입/점검 이력 전송 등
- 스마트 도어락: 블루투스 통신(세션 제어), 서보 모터 구동, 내장된 암호 모듈 등

• 출입관리(Web 서비스): 관리자 등록, 출입 이력관리, 점검 이력, 스마트 도어락 상태 및 모니터링 등

그리고 스마트 도어락 시스템에서 요구되는 기본적인 인증 절차는 그림 4에 나타내었다[3].

기존 공공 시설물의 도어락 대체를 위해 암호화 모듈이 장착된 슬라이드형 스마트 도어락 시스템을 개발하고 있다. 그러나 작업인증 절차를 위해 송수신하는 무선 데이터에 대한 보안 취약점을 개선하기 위해서는 실제 무선 데이터를 송수신하는 과정을 모니터링하고 실제 나타나는 취약점 분석을 통해 적용하고자 하는 암호 알고리즘의 보안성 검증이 필요하다.

Ⅳ. GNU Radio를 이용한 신호계측

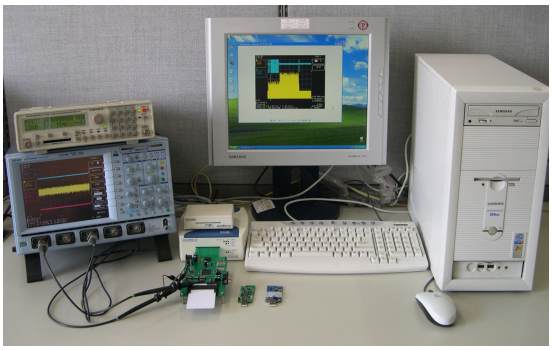
4.1. 전력신호를 이용한 공격 시스템

GNU Radio[2]는 1998년에 시작된 GNU의 대표적인 정규 프로젝트로서 소프트웨어에 기반한 무선 통신시스템을 연구하고 제작하기 위한 툴킷이다. 이것은 USRP(Universal Software Radio Peripheral) 또는 HackRF와 같은 범용 무선장치를 이용하여 강력한 신호처리 소프트웨어를 통하여 다양한 분야의 응용이 가능하다. 일반적으로 전력분석공격은 알고 있는 평문값 및 중간 암호값과 추정된 마스터 키(비밀키)로부터 생성된 숨겨진 값을 입력받아 연산하는 시점에서 해밍무게/해밍거리에 따른 차분전력/상관성분석이 이루어진다[5-7]. 따라서 암호연산 결과 값과 연산중에 측정된 전력신호의 상관도를 분석함으로써 숨겨진 값을 탐색할 수 있고, 탐색된 이 값을 통해 비밀키를 추정할 수 있다.

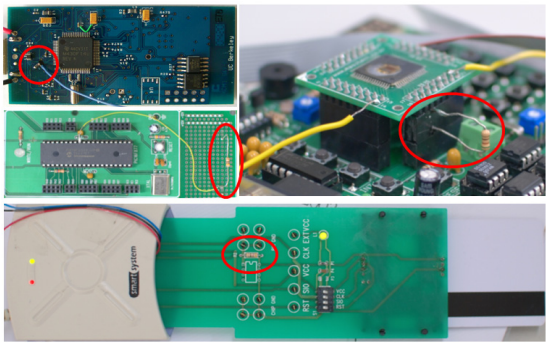
그러나 그림 5에서와 같이 통상적인 전력분석 공격을 위한 고가의 측정 장비들(고해상도를 가진 디지털 오실로스코프, 분석 에뮬레이터, 디지털 함수 발생기, 정밀 프로브 등)을 이용하여야만 하고, 다량의 전력샘플 채집과 장시간의 연산수행을 통해 원하는 값을 탐색하여야만 하는 문제가 있다.

4.2. GNU Radio 기반 전력분석 시스템 구축

암호장치에서 그림 6과 같은 암호화 연산을 수행하는 과정에서 첫 번째 라운드의 SubBytes() 함수의 출력값 생성 시점에 맞춰 공격한다고 가정한다[7].



(a)



(b)

Fig. 5 General power signal analysis for attacking (a) Experimental environment for power analysis attack (b) Resistance insertion for measure power consumption

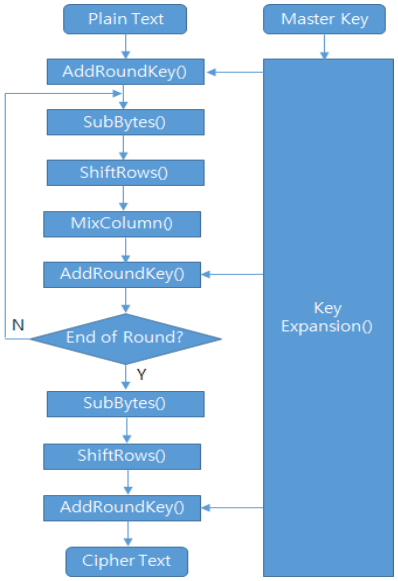


Fig. 6 Operation for AES encryption algorithm

이때 전력분석에 필요한 전력수집은 HackRF 또는 USRP와 같은 범용 무선장치를 이용하여 디지털 오실로스코프를 대신하여 이용 가능하다. 실험에서는 1MHz-6GHz 동작범위의 신호를 수신 가능하며 20Mps의 신호 샘플링이 가능한 HackRF 장치를 통해 원하는 신호를 채집하였다.

이후 GNU Radio 플랫폼에서 전력분석 공격을 위한 실험 시스템은 다음과 같은 절차를 통하여 신호처리를 하여 추정된 전력신호와 측정된 전력신호간의 상관도 분석 등을 수행하거나 프로토콜 분석을 통해 비밀키를 추정할 수 있다[8].

- Step 1: 범용 무선장치를 이용하여 전력신호 수집을 위한 인터페이스 설정
- Step2: GNU Radio에서 범용 무선장치 인터페이스를 통해 전력신호(power traces)를 수집하고 큐에 저장
- Step 3: 큐에 저장된 전력신호를 구간 단위로 임의의 추정 키를 대입 연산하여 SBOX에 대입하여 출력 값을 도출
- Step 4: 도출된 값을 토대로 SPA 또는 신호 상관도를 계산하여 추정키를 계산하고 전체 키를 얻을 수 있을 때까지 Step 2로 되돌아 가서 이 과정을 반복
- Step 5: 최종 키 수열을 획득

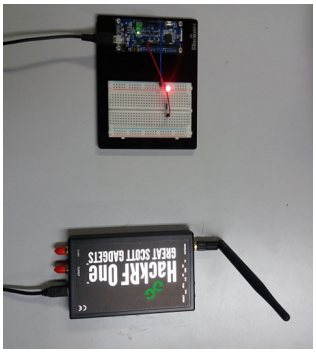
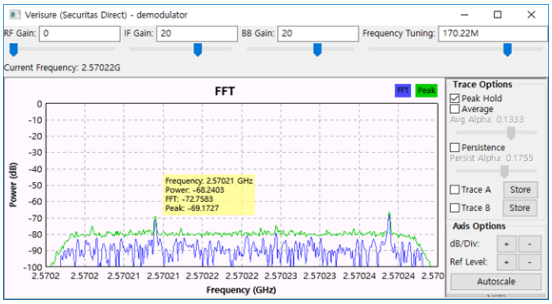


Fig. 7 Experimental environment using HackRF

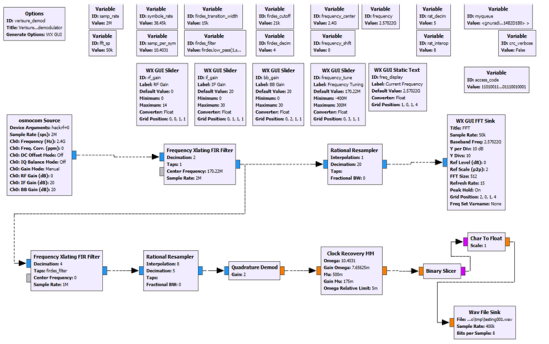
4.3. 실험결과

실험은 그림 7에서와 같이 블루투스 4.0으로 동작하는 Bluinno 장치를 대상으로 스마트폰에서 제어신호를 송신하고 이를 주고받는 과정을 HackRF 장치를 이용하여 무선 패킷을 캡처하여 신호를 분석하였다.

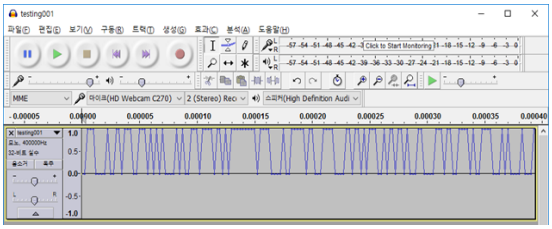
그림 8 (a)에서와 같이 장치 사이의 무선신호는 대역통과필터를 거쳐 주파수 신호 분석이 가능하다. 유효대역 내에서 강한 전력신호의 주파수 위치를 나타내는 구간을 확인할 수 있으며 전력신호 분석을 위한 공격대상 주파수를 선택할 수 있다.



(a)



(b)



(c)

Fig. 8 Signal analysis GNU Radio platform and HackRF (a) Observed power spectrum using BPF (b) Signal flow diagram on GNU Radio companion (c) Time signal plot using Audacity utility

그리고 선택한 주파수의 신호를 대상으로 GNU Radio 플랫폼에서 원하는 신호를 비트 레벨로 변환하여 wav 형식의 파일로 저장한다(그림 8(b) 참고). 다음 절차로 그림 8(c)에서와 같이 Audacity 오디오 툴에서 이

신호를 관측하게 되면 신호의 비트 패턴 분석을 할 수 있다. 이 과정에서 무선 패킷의 기본 구조에 해당하는 동기화 패턴, CRC, 신호 데이터 등의 정보를 얻을 수 있다. 이와 같이 공격대상 장치의 전력신호 분석을 통해 동작 프로토콜 등을 확인할 수 있으며, 저장된 wav 형식의 파일을 대상으로 프로토콜을 구체적으로 분석하면 그림 9와 같이 무선 패킷의 길이, PID, CRC 및 데이터 등을 분석할 수 있어 암호통신 과정에서의 비밀키 등을 확인하는데 유용하다는 것을 확인할 수 있었다.

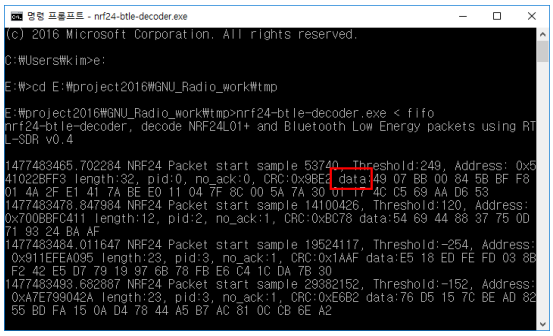


Fig. 9 Analysis result for Bluetooth protocol

V. 결 론

공공 시설물 관리를 위해 암호화 통신이 가능한 스마트 도어락 시스템 구축 과정에서 안전한 데이터 통신을 보장하기 위해서는 인증 프로토콜의 안전성을 고려하여야 한다. 통신과정에서 암호화 통신에 따른 취약점 분석과 공격자에 대한 대책을 세우기 위해 GNU Radio 플랫폼과 HackRF 장비를 이용하여 무선 데이터의 취약점 분석을 위한 기본 실험을 수행하였다.

구축된 전력분석 실험 시스템은 통상적으로 이용되는 고가의 전력분석 공격 시스템을 대신하여 무선 데이터의 효율적인 채집과 프로토콜 분석에 이용 가능하다는 것을 확인하였다.

ACKNOWLEDGMENTS

This work (Grants No. C0400192) was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2016.

REFERENCES

[1] Bluetooth SIG official site. [Internet]. Available: http://www.bluetooth.org/.

[2] GNU Radio site. [Internet]. Available: http://gnuradio.org/.

[3] T. Y. Kim and D. S. Lee, “System design for access to subway vent based bluetooth smart door-lock,” *in Proceeding of the 40th Annual Conference of KIICE*, pp. 63-65, October 2016.

[4] S. T. Bae and J. K. Kim, “IoT development and security paradigm,” *KISTEP R&D InI*, vol. 14, pp. 44-57, 2016.

[5] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” *Advances in Cryptology, CRYPTO'99*, LNCS 1666, pp. 388-397, August 1999.

[6] P. Kocher et al., “Introduction to differential power analysis,” *Journal of Cryptographic Engineering*, vol. 1, no. 1, pp. 5-27, April 2006.

[7] Y. G. Park, H. R. Kim, H. J. Lee, D. C. Park, and U. Y. Pak, “A software power analysis countermeasure using secrete intermediate key,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 17, no. 12, pp.2883-2890, December 2013.

[8] T. Y. Kim and H. J. Lee, “Software power analysis countermeasure using GNU Radio antenna,” *in Proceeding of the 40th Annual Conference of KIICE*, pp. 70-71, October 2016.

김태용(Tae-Yong Kim)

1993년 부경대학교(공학사)
1997년 오카야마대학(공학석사)
2001년 오카야마대학(공학박사)
2002년~현재 동서대학교 컴퓨터공학부 교수
※관심분야 : 위성통신, 마이크로파 회로해석 및 설계, 마이크로 센서 응용, 센서 네트워크

이훈재(Hoon-Jae Lee)

1985년 경북대학교(공학사)
1987년 경북대학교(공학석사)
1998년 경북대학교(공학박사)
1987년~1998년 국방과학연구소
2002년~현재 동서대학교 컴퓨터공학부 교수
※관심분야 : secure communication system, side-channel attack, USN RFID security