논문 18-43-04-15 The Journal of Korean Institute of Communications and Information Sciences '18-04 Vol.44 No.04
https://doi.org/10.7840/kics.2018.43.4.723

경량 보안 프로토콜 구현

유 기 순◆, 김 성 준*, 박 원 규*, 장 민 호**, 임 대 운°

Implement of Lightweight Security Protocol

Ki-soon Yu◆, Sung-joon Kim*, Won-kyu Park*, Min-Ho Jang**, Dae-woon Lim°

요 약

IoT 기반 서비스는 이기종 기기 및 어플리케이션을 활용함으로써 보안위협에 노출 될 가능성이 높다. 본 논문에서는 IoT 서비스 통신 데이터에 대한 정보 누출 및 위·변조를 방지하고자 경량 보안 프로토콜을 제안한다. 제안된 경량 보안 프로토콜은 SHA256-HMAC, PRESENT, LEA 알고리즘을 기반으로 사용자 인증, 메시지 인증, 메시지 암호화 기능을 지원하여 도청으로 인한 통신 데이터의 누출 방지 및 위·변조의 위협을 줄 일 수 있다. 하지만, 프로토콜의 헤더로 인해 데이터 전송률이 낮아진다는 문제점과 인증 및 암호 알고리즘의 연산으로 통신 시간이 증가한다는 문제점이 있다.

Key Words : IoT Security, PRESENT, LEA, Lightweight Encrypt, Authentication

ABSTRACT

Services based on IoT are more to be exposed to security threats by utilizing heterogeneous devices and applications. In this paper, lightweight security protocol is proposed to prevent information leakage and the forgery of communication data for IoT service. The proposed lightweight security protocol supports user authentication, message authentication, and message encryption based on the SHA256-HMAC, PRESENT, and LEA algorithms thereby preventing leakage of communication data and threat of tampering due to eavesdropping. However, there are some problems that the data transmission rate is lowered due to the header of the protocol and the communication time is increased due to the operation of the authentication and encryption algorithm.

Ⅰ. 서 론

네트워크를 통해 유기적으로 연결된 이기종의 IoT 기기는 스마트홈, 의료, 제조, 자동차, 에너지 등 다양한 산업 분야에서 활용되고 있다.[1] 더불어 보안기능을 지원하지 않는 IoT 기기로 인해 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)에 대한 침해 가능성 또한 높아지고 있다. 특히, IoT 기반 의료서비스에서 암호화되지 않은 진료 정보가 누출될 경우 개인 생체정보 누출로 인한 프라이버시 침해를 야기할 수 있다. 이러한 보안 위협에 대응하기 위해 초경량, 저전력, 저성능의 특징을 지닌 IoT 기기에 기존 보안기술을 적용하는데 한계가 있다.[2,3] 이에 본 논문에서는 IoT 기기 간 전송되는 개인 정보 및 주요 정보의 누출을 예방하고자 기존 보안기술을 개선하여 IoT 환경에 적합한 경량 암호 프로토콜을

※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW중심대학지원 사업의 연구결과로 수행되었음(2016-0-00017)
◆ First Author : Department of Information Communication Engineering, Dongguk University, ykscj29@naver.com, 학생회원
° Corresponding Author : Department of Information Communication Engineering, Dongguk University, daewoonlim@gmail.com, 종신회원
* Department of Information Communication Engineering, Dongguk University, happygrounds@naver.com, wku0905@gmail.com
** School of Electrical and Electronic Engineering, Ulsan College, mhjang@uc.ac.kr, 종신회원
논문번호 : KICS2017-04-114, Received April 18, 2017; Revised March 2, 2018; Accepted March 5, 2018

제안한다.

Ⅱ. 관련연구

2010년 블루투스 Special Interest Group은 기존의 블루투스보다 전류 소모량을 줄일 수 있는 블루투스 4.0을 발표하였다. Bluetooth Low Energy(BLE)는 기존의 블루투스 전류 소모량을 최대 10분의 1 수준으로 줄여 장기간 무선 통신이 가능하다.[4]

<그림 1>은 BLE 스택을 보여준다. PHY(Physical Layer)는 패킷 송수신 기능을 담당한다. LL(Link Layer)은 Advertiser, Scanner, Initiator와 같은 RF 상태를 제어한다. HCI(Host Controller Interface)는 Host영역과 Controller영역을 연결하는 역할을 한다. L2CAP(Logical Link Control and Adaptation Protocol)는 상위 레벨의 통신서비스 품질을 보증하기 위한 QoS(Quality of Service)를 지원하고, 패킷 분배 및 재조합의 기능을 지원한다. SMP(Security Manager Protocol)는 보안과 관련된 것으로 AES-128 엔진을 기반으로 보안 기능을 제공한다. ATT(Attribute Protocol)는 기기 간 연결이 설정된 후 클라이언트와 서버의 통신을 위한 비보존성 규약을 설정한다. GAP(Generic Access Profile)는 Pairing과 Bonding(Linker)을 통해 기기 간 연결을 담당한다. GATT(Generic Attribute Profile)는 통신 데이터의 구조 통신 방법에 대해 정의한다.[5]

BLE는 통신상의 보안 강화를 위해 SMP를 통해 보안 서비스를 제공하고 있다. 본 논문에서는 IoT 기기에서 BLE 통신을 하는 어플리케이션에 적용 가능한 경량 보안 프로토콜을 설계 및 구현하고 그 결과를 평가한다.

Ⅲ. 경량 보안 프로토콜 설계

3.1 프로토콜 기능

본 논문에서 제안하는 경량 보안 프로토콜은 인증 및 메시지 암호 기능을 제공한다. 기능에 따라 비보안 모드, 인증 모드, 암호 모드, 인증 및 암호 모드로 4가지의 통신모드를 지원한다. 이를 위해 갱신키(Update Key)와 세션키(Session Key)를 사용한다. 갱신키의 역할은 <표 1>과 같이 사용자 인증을 위해 사용된다. 사용자 인증은 제3자가 네트워크상에서 공격자가 정당한 사용자로 위장하는 것을 방지하기 위한 것으로, 두 기기사이에 새로운 세션이 맺어졌을 때 사용자 인증을 수행한다. 세션키는 두 기기 간의 보안통신 시 메시지 인증 및 메시지 암호화에 사용된다.

표 1. 키 종류
Table 1. Type of keys

Type	Use
Update Key	User Authentication
Session Key	Message Authentication, Message Encryption

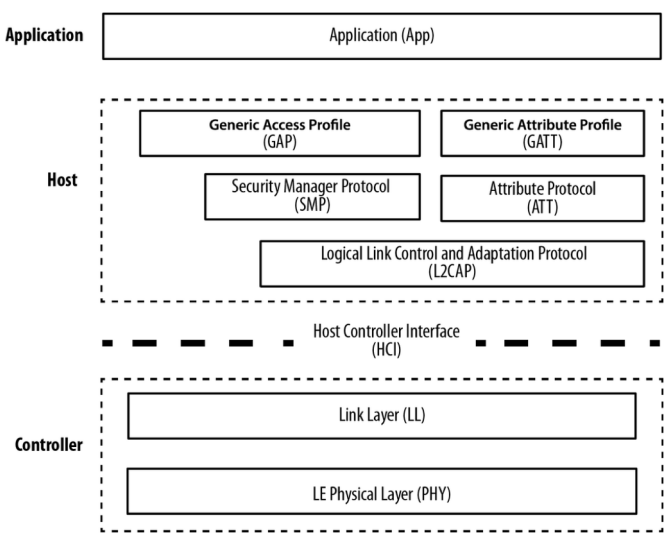

그림 1. BLE 스택
Fig. 1. The stack of BLE

비보안 모드는 보안기능 없이 통신하는 모드로 메시지 전송효율이 다른 모드에 비해 높지만 메시지의 누출 및 위·변조와 같은 보안위협에 취약하다.

인증 모드는 메시지 인증을 하는 것으로 통신 메시지에 대한 HMAC의 일부를 인증토큰으로 사용한다. 인증토큰을 통해 네트워크에서 발생할 수 있는 메시지의 위·변조를 방지할 수 있다. HMAC 생성은 SHA256 알고리즘을 사용한다.

암호 모드는 통신 메시지의 누출을 방지하기 위해 메시지를 암호화 한다. 이때, IoT 기기에서 암호로 인한 부하를 줄이고자 경량 암호 알고리즘인 PRESENT와 LEA를 이용한다.[6,7]

인증 및 암호 모드는 메시지에 대한 인증과 암호 기능을 모두 지원하는 것으로 메시지에 대한 무결성 및 기밀성을 지원한다.

3.2 경량 보안 프로토콜 구조

<그림 2>는 경량 보안 프로토콜의 계층 구조를 보여준다. 상위 계층(High Layer)은 입력 받은 메시지에 상위 계층 헤더를 붙여 세그먼트로 만들고, 메시지의 전송 실패나 예상하지 못한 오류 메시지를 제어한다. 하위 계층(Low Layer)은 상위 계층에서 전달 받은 세그먼트를 인증 및 검증하고 암호 및 복호화하는 기능을 제공한다.

입력받은 메시지는 각 계층을 거쳐 프레임으로 만들어진다. 발신부에서는 프레임의 페이로드보다 긴 메시지를 BLE가 전송할 수 있도록 여러 프레임으로 나누어 전송한다. 이를 수신한 수신부는 여러 프레임을 조립하여 세그먼트의 형태로 복원하여 상위 계층으로 전달한다.

<그림 3>은 세그먼트의 구조를 보여준다. Type에 따라 요청과 응답 세그먼트가 구분된다. HL SEQ는

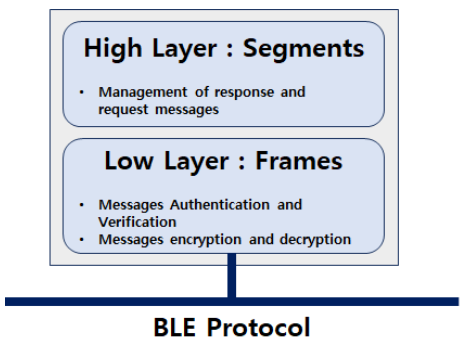

그림 2. 경량 보안 프로토콜 계층구조
Fig. 2. The structure of lightweight security protocol

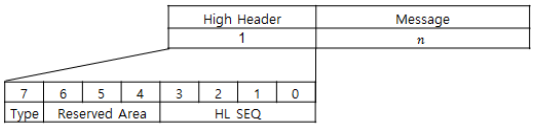

그림 3. 세그먼트 구조
Fig. 3. The structure of a segment

요청 세그먼트의 순번(Sequence)으로 발신자는 해당 순번으로 요청 세그먼트에 대한 응답 세그먼트를 정상적으로 수신하였는지 판단하게 된다. 순번의 범위는 0~15번이다.

<그림 4>는 상위 계층의 통신과정을 보여준다. 통신 당사자는 각자 요청 세그먼트의 순번을 관리한다. 요청 세그먼트를 전송 한 후 요청한 순번에 대한 응답 세그먼트를 일정 시간동안 기다린다. 그동안 다른 요청 세그먼트는 전송할 수 없지만, 수신한 요청 세그먼트에 대한 응답 세그먼트는 전송 할 수 있다. 일정 시간동안 요청 세그먼트에 대한 응답 세그먼트를 수신하지 못하면 동일한 순번으로 다른 요청 세그먼트를 전송하고, 응답 세그먼트를 수신하게 되면 순번을 1씩 증가 시켜 다음 요청 세그먼트를 전송한다.

<그림 5>는 프레임의 구조를 보여준다. 프레임은 4바이트의 헤더와 최대 16바이트의 페이로드 부분으로 이루어진다. 우선 프레임의 헤더를 살펴보면 Mode는 통신모드를 뜻하는 것으로 현재 통신하고 있는 모드로 설정하게 된다. Ack는 프레임 전송에 대한 수신 응답을 뜻하는 것으로, 수신한 프레임에 대한 응답으로 Ack 값을 1로 하여 전송한다. LL SEQ는 전송 프레임의 순번으로 프레임 전송의 성공여부와 관계없이 프레임 전송 시 계속해서 1씩 증가하며 범위는 0~31이다. Function Code는 세그먼트의 구분자를 나타내는 것으로 상위 계층에서 처리해야 할 메시지와 그보다

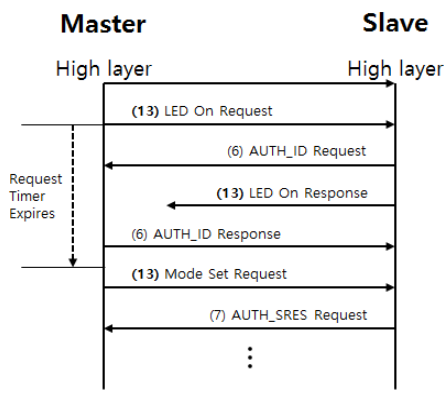

그림 4. 상위 계층 통신과정
Fig. 4. The communication on the high layer

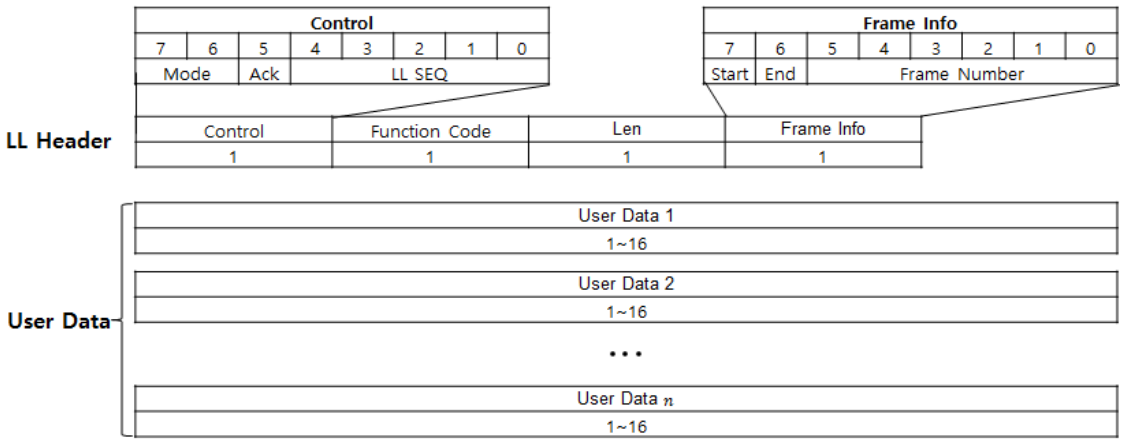

그림 5. 프레임 구조
Fig. 5. The structure of a frame

높은 서비스 계층에서 처리해야 할 내용을 구분해 준다. Len은 인증과 암호화 전의 세그먼트의 길이를 나타낸다. 이를 통해 수신해야하는 프레임의 개수 예측할 수 있다. Frame Info는 전송한 프레임에 대한 정보로 몇 번째 프레임인지에 대한 정보를 나타낸다. User Data는 세그먼트가 들어갈 영역으로 크기가 최대 16바이트이다. 그러므로 세그먼트의 길이가 16이상일 경우 여러 개의 세그먼트는 여러 User Data 블록으로 나누어지고 각 블록은 하위 계층 헤더와 연접하여 하나의 프레임으로 만들어져 전송된다. 이 때 Frame Info를 통해 전송하고 수신 프레임을 관리 할 수 있다.

<그림 6>은 하위 계층의 통신과정을 보여준다. 통신 당사자는 각자 전송 프레임의 순번을 관리한다. 프레임 전송 후 전송한 순번에 대한 응답(Ack)을 일정 시간동안 기다린다. 그동안 다른 프레임은 전송할 수 없다. 발신자는 일정시간동안 전송 프레임에 대한 응답을 받지 못한 경우 해당 통신 메시지 전송이 실패한 것으로 보고 상위 계층 메시지 전송 실패를 알린다. 세그먼트가 여러 프레임으로 전송되는 경우 해당 세그먼트와 관련한 모든 프레임을 수신하면 조립하여 상위 계층으로 전달한다.

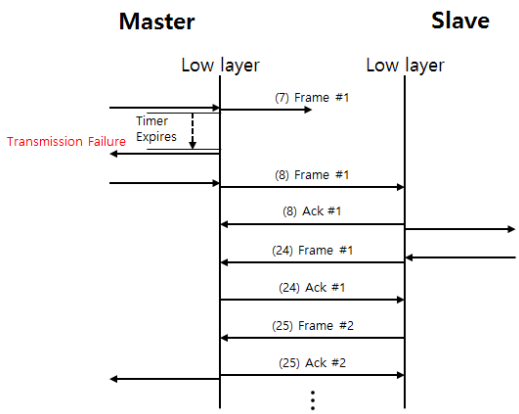

그림 6. 하위 계층 통신과정
Fig. 6. The communication on the low layer

Ⅳ. 경량 보안 프로토콜 구현

4.1 하드웨어 구성 및 개발환경

본 논문에서는 경안 보안 프로토콜 구현하고 그 결과를 확인하기 위해 <표 2>와 같은 하드웨어로 테스트 환경을 구성하였다.

Keil 컴파일러를 이용해 기존 nRF51822에서 BLE 통신을 지원하는 소프트웨어에 경량 보안 프로토콜을 적용하였다. BLE 통신을 하는 어플리케이션에 경량 보안 프로토콜을 적용하였다. 보안통신이 정상적으로 이루어지는지 확인하기 위해 J-Link RTT Viewer를 사용하였다.

표 2. 개발환경
Table. 2. Development Environment

Item	Model
Bluetooth	Bluetooth v4.2
Smart Phone	Samsung Galaxy A5
Application	Android 6.0 (Marshmallow)
Control Board	nRF51822
Software Compiler	Keil μVision5® IDE
Log	J-Link RTT Viewer V5.12f

4.2 구현결과

어플리케이션과 IoT 기기는 BLE 연결이 완료 된 후 갱신키를 이용해 사용자 인증을 수행하고, 세션키를 생성한다. 갱신키는 두 기기에 안전한 방법으로 저장되어 있는 것으로 가정하고, 본 논문에서는 갱신키의 생성 및 분배방법에 대해 언급하지 않는다.

사용자 인증 및 세션키 생성과정은 다음과 같다.

1) 인증 요청자는 요청자의 아이디를 보낸다.
2) 인증 검증자는 랜덤넘버를 보낸다.
3) 인증 요청자와 인증 검증자는 갱신키를 이용해 요청자의 아이디와 랜덤넘버에 대한 HMAC을 생성한다.
4) HMAC의 왼쪽 32비트를 인증토큰으로 사용한다.
5) 나머지는 비트 중 일부분을 세션키로 사용한다.

위 과정을 거친 후 통신모드를 설정하게 되고 통신모드에 따라 메시지 인증 및 메시지 암호화를 수행한다.

<표 3>은 경량 보안 프로토콜 적용한 프로그램과 미적용 프로그램의 실행파일 크기를 보여준다.

<그림 7>은 경량 암호 프로토콜의 테스트 환경을 보여준다.

<표 4>는 길이가 10바이트와 20바이트인 메시지를 각각 1회 송·수신하는데 소요된 시간과 평균 소모 전류를 모드별로 보여준다.

경량 보안 프로토콜을 적용한 경우 헤더 추가 및 응답 전송으로 인해 메시지 전송 시간이 증가한다.

특히, 20바이트의 메시지는 경량 보안 프로토콜을 적용하지 않은 경우 한 번의 통신으로 전송 가능하지만 경량 보안 프로토콜을 적용하면 두 번에 걸쳐 메시지를 전송하므로 경량 보안 프로토콜 미적용의 경우보다 4~5.5배 수행 시간이 느려진다.

표 3. 경량 보안 프로토콜 모듈 크기
Table. 3. The size of lightweight security protocol

Item	Size of IoT Software
Non Protocol	98,304 byte
Protocol	147,456 byte

암호 모드에서는 암호 알고리즘으로 인한 수행 시간 차이가 크다. 메시지의 기밀성을 보장하면서도 통신의 지연을 줄이 수 있는 경량 암호 알고리즘의 사용이 필요하다는 것을 알 수 있다.

소모 전류는 메시지 통신 시 소비한 전류를 평균한 것으로 통신 시간이 증가함에 따라 소모 전류 역시 증가함을 알 수 있다.

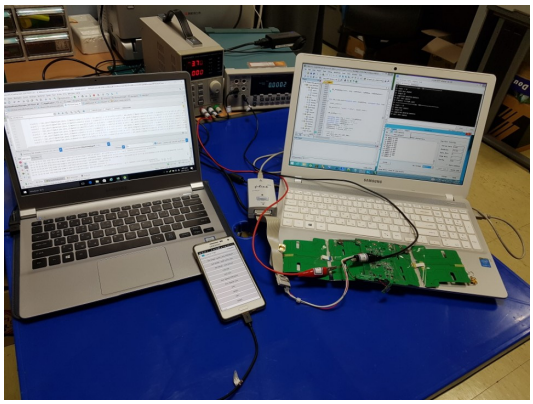

그림 7. 테스트베드
Fig. 7. Testbed

Table 4. Test result

Communication Mode		10 byte			20 byte		
		Length of Message	Performance Time (ms)	Operating Current (A)	Length of Message	Performance Time (ms)	Operating Current (A)
Non Protocol		10	411.20	0.09	20	414.03	0.09
Non Secure		15	812.09	0.19	25	1639.04	0.35
Authentication Only		19	825.85	0.19	33	1664.31	0.35
Encryption Only	PRESENT	20	1012.68	0.28	32	2247.29	0.67
	LEA	20	848.15	0.18	40	1668.74	0.35
Authentication and Encryption	PRESENT	20	1655.10	0.53	40	2236.19	0.74
	LEA	20	1230.88	0.31	40	1654.96	0.36

V. 결 론

본 논문에서는 IoT 환경에서 발생할 수 있는 보안 문제에 대응하고자 경량 보안 프로토콜을 제시하였다. 제안한 경량 보안 프로토콜은 SHA256-HMAC, PRESENT, LEA 알고리즘을 바탕으로 사용자 인증, 메시지 인증, 메시지 암호화 기능을 지원한다. 이를 통해 도청으로 인한 통신 메시지의 누출을 방지하고 통신 중 발생 할 수 있는 메시지 위·변조의 위협을 줄 일 수 있다.

하지만 프로토콜의 헤더로 인해 통신 데이터가 증가하여 데이터 전송률이 낮아진다는 문제점 가지고 있다. 이를 보완하기 위해 헤더 크기를 줄일 수 있는 연구가 필요하다.

References

[1] J. Jeon, N. Gim, T. Bak, H. Gang, and C. Pyo, "IoT devices product and technology trends," *J. KICS,* vol. 31, no. 4, pp. 44-52, Apr. 2014.

[2] J. Gim and S. Jin, "IoT security technology for security threats in second connection environment," *J. KICS,* vol. 34, no. 3, pp. 57-64, Mar. 2017.

[3] N. Gang, "IoT convergence services security requirements," *J. KICS,* vol. 32, no. 12, pp. 45-50, Dec. 2015.

[4] K. Byeon, S. Lim, B. Le, and J. Yun, *Bluetooth low energy wireles technology*, Hongrung Publishing Company, 2014.

[5] R. Davidson, K. Townsend, C. Wang, and C. Cufi, *Getting Started with Bluetooth Low Energy*, pp. 15-33, O'Reilley Publishing Co., 2014.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," *CHES 2007, Springer*, vol. 4727 LNCS, pp. 450-466, 2007.

[7] D. Hong, J.-K. Lee, D.-C. Kim, D. Kwon, K. H. Ryu, and D.-G. Lee, "LEA: A 128-Bit block cipher for fast encryption on common processors," *Inf. Secur. Appl., Springer*, vol. 8267, pp. 3-27, 2014.

유 기 순 (Ki-soon Yu)

2007년 2월 : 안동대학교 컴퓨터공학과 학사

2015년 2월 : 동국대학교 정보보호학과 석사

2015년 3월~현재 : 동국대학교 정보통신공학과 박사과정

<관심분야> 암호학, 제어시스템보안,

김 성 준 (Sung-joon Kim)

2011년 3월~현재 : 동국대학교 컴퓨터공학부 정보통신공학 전공 학사과정

<관심분야> 암호학, 소프트웨어공학, 임베디드 시스템

박 원 규 (Won-kyu Pim)

2011년 3월~현재 : 동국대학교 컴퓨터공학부 정보통신공학 전공 학사과정

<관심분야> 암호학, 소프트웨어공학, 임베디드 시스템

장 민 호 (Min-Ho Jang)

2002년 8월 : 연세대학교 전기전자공학부 공학사
2004년 8월 : 서울대학교 전기컴퓨터공학부 공학석사
2009년 2월 : 서울대학교 전기컴퓨터공학부 공학박사
2009년 3월~2011년 8월 : 삼성전자 DMC연구소 책임연구원
2011년 9월~현재 : 울산과학대학교 전기전자공학부 부교수
<관심분야> 디지털통신, 이동통신시스템, 오류정정 부호, OFDM, 암호학, 정보보호

임 대 운 (Dea-woon Lim)

1994년 8월 : KAIST 전기및전자공학사 학사
1997년 2월 : KAIST 전기및전자공학사 석사
2002년 8월 : 서울대학교 전기컴퓨터공학부 박사
1995년 9월~2002년 8월 : LS산전 중앙연구소 선임연구원
2006년 9월~현재 : 동국대학교 정보통신공학과 부교수
<관심분야> 암호학, 제어시스템보안