Regular paper | Journal of the KIECS. pp. 1077-1082, vol. 14, no. 6, Dec. 31. 2019, t. 98, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2019.14.6.1077

무선 RFID 환경에서 해시코드를 이용한 EPC 코드 보안

이철승*

Security Authentication Technique using Hash Code in Wireless RFID Environments

Cheol-Seung Lee*

요 약

컴퓨팅 기술과 네트워킹의 발달은 4차 산업혁명의 근본이 되는 기술로 발달하여, 유비쿼터스 환경을 제공하게 되었다. 유비쿼터스 환경에서는 각종 디바이스나 사물에 접근과 접속이 활발하게 진행될 수 있도록, 사물인터넷 환경이 이슈과 되고 있으며, 무선 식별코드를 사용하는 RFID 시스템은 RFID 태그를 사물에 장착하여 제품의 생산, 유통과 같은 SCM 관리에 매우 효율적으로 응용되고 있다. EPCglobal에서 RFID 시스템 표준화 연구와 각종 보안 연구를 진행하고 있다. RFID 시스템은 무선 환경기술을 사용하기 때문에 유선상의 문제점보다 더 많은 보안 위협요소가 존재하게 된다. 특히, 기밀성, 불구분성, 전방향 안전성을 제공하지 못한다면 4차 산업혁명 시대에 각종 위협에 노출될 수 있을 것이다. 이에 본 연구는 EPCgolbal의 표준방법을 분석하고, 연산량을 고려할 수 있는 해시코드를 이용한 RFID 보안 기법을 제안한다.

ABSTRACT

The development of computing technology and networking has developed into a fundamental technology of the Fourth Industrial Revolution, which provides a ubiquitous environment. In the ubiquitous environment, the IoT environment has become an issue so that various devices and the things can be actively accessed and connected. Also, the RFID system using the wireless identification code attaches an RFID tag to the object, such as the production and distribution of products. It is applied to the management very efficiently. EPCglobal is conducting a research on RFID system standardization and various security studies. Since RFID systems use wireless environment technology, there are more security threats than wire problems. In particular, failure to provide confidentiality, indistinguishability, and forward safety could expose them to various threats in the Fourth Industrial Revolution. Therefore, this study analyzes the standard method of EPCgolbal and proposes RFID security method using hash code that can consider the amount of computation.

키워드

RFID System, EPC Code, Hash Function, Security
RFID 시스템, EPC 코드, 해시 함수, 보안

* 교신저자 : 광주여자대학교 교양과정부
• 접 수 일 : 2019. 10. 06
• 수정완료일 : 2019. 11. 10
• 게재확정일 : 2019. 12. 15
• Received : Oct. 06, 2019, Revised : Nov. 10, 2019, Accepted : Dec. 15, 2019
• Corresponding Author : Cheol-Seung Lee
Dept. of Liveral Arts, Kwangju women's University
Email : cyberec@kwu.ac.kr

Ⅰ. 서 론

ICT(: Information and Communications Technologies) 산업의 급변화로 정보통신기술의 융합을 통한 새로운 산업혁명인 4차 산업혁명이 전세계의 화두가 되고 있다. 4차 산업혁명의 다양한 기술 중 무선통신환경을 이용하는 유비쿼터스 컴퓨팅 환경은 각종 디바이스, 네트워크 및 소프트웨어 기술의 융합 환경을 필요로 하며, IOT(: Internet of Things) 기술 분야 중 사물을 식별하는 RFID(: Radio Frequency Identification) 기술은 산업 전 영역에 응용되고 있으며, 무한한 경쟁력을 갖추고 있다. 하지만 RFID 기술의 무분별한 사용으로 RFID태그에 부착된 정보의 유출이나, 고유한 식별자 ID(: IDentifier) 유출 그리고 공격자의 공격으로 인한 각종 보안 위협요소(스니핑, 스푸핑, 재전송 공격, 서비스 거부 공격, 위치 트래킹)가 존재하여 무선통신 기술을 사용하는 유비쿼터스 환경에서 반드시 해결해기 위한 예방과 대책들이 필요하다.

Ⅱ. 관련연구

2.1 RFID 시스템

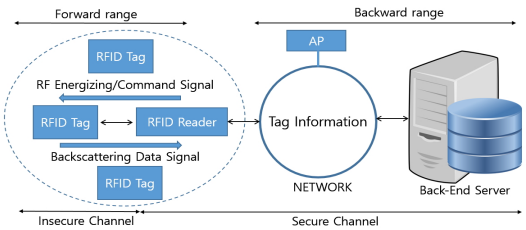

그림 1. RFID 시스템
Fig. 1 RFID system

그림 1과 같이 RFID 시스템은 무선주파수를 이용하여 컨트롤러가 인식 후, 분석하여 RFID 태그의 정보를 획득 하는 방식으로, RFID 태그, RFID 리더 그리고 데이터를 저장하는 Back-end Server가 결합되어있는 시스템이다[1].

RFID 태그는 전력 공급방식에 따라, (능동형, 수동형) 트랜스폰더라고도 불리며, 무선통신을 수행하기 위해 안테나와 인증을 하기 위한 연산 정보가 내장된 마이크로 칩으로 구성되어 있고, 특정 개체의 고유 식별자 ID와 정보를 RRID 리더에게 송신하는 역할을 한다.

RFID 리더는 RFID 태그로부터 송신된 고유한 정보를 식별하는 장치로 트랜시버라고 하고, RF 모듈, 제어장치 및 무선 주파수를 사용하여 RFID 태그에게 신호를 송·수신하는 장치로 구성된다. RFID 태그로부터 수신 된 정보는 Back-end Server에게 송신하고, 필요한 정보를 다시 수신하는 역할을 한다.

Back-end Server는 RFID 리더로 부터 수신된 정보를 저장하고, 적법한 데이터 인지 확인하는 인증 절차를 수행한다. Back-end Server는 수신 정보의 적절한 필터링을 수행하기 위해 Savant, ONS(: Object Naming Services), PML(: Project Markup Language)로 구성된 미들웨어이다[2].

2.2 EPCglobal의 RFID 정보서비스

RFID 시스템은 EPCglobal, 유비쿼터스 ID 센터에서 표준화를 진행하고 있다. EPCglobal에서는 GS1(: Global Standard Number 1)의 EPC(: Electronic Program Code) 체계를 전망했다. EPC는 특정제품의 다양한 정보를 식별할 수 있는 RFID 기반 산업의 표준 인프라를 수행하고 있다. RFID 정보서비스 EPCIS(: EPC Information Service)는 미들웨어가 제공하는 ALE(: Application Level Event)를 수집하여, 유통, 문류등의 응용 서비스 시스템 구축하여 서버와 공유한다.

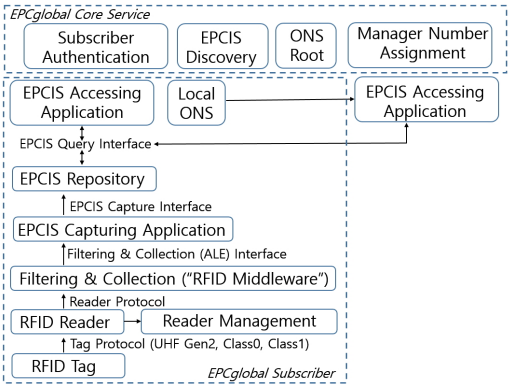

그림 2. EPCglobal의 RFID 정보서비스
Fig. 2 RFID information service of EPCglobal

그림 2는 EPCglobal의 RFID 정보서비스를 보이고 있다. RFID 태그와 RFID 리더 사이에 태그 프로토콜로 UHF 대역의 Class 1 Generation2가 Class0, Class1을 통합하여 EPCglobal의 EPCIS 정보서비스를 제공하고 있다[3].

2.3 EPC 코드

EPC는 EAN(: European Article Number)과 UCC(: Uniform Code Council)가 공동 제안한 RFID 체계로 위조, 유효기관리, 재고관리 및 상품추적 등의 공급망 관리 효과를 누릴 수 있는 코드를 말한다.

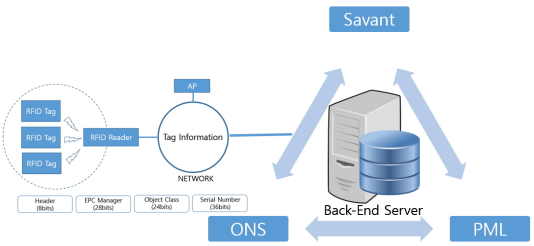

그림 3. EPC code와 back-end server
Fig. 3 EPC code and back-end server

Header는 기존 정의된 다른 코드버전 넘버와 호환이 될 수 있는 헤더이며, 이 헤더를 EPC 코드의 전체 길이, 식별코드, 필터 값 정의를 한다. Header는 가변 길이 값을 가지며 2bit일 경우 3개, 8bit의 경우 63개의 값을 가진다. EPC Manager는 EAN 회원기관이 할당하며, 영문, 숫자 조합으로 28bit 길이로 약 2억 6천만 개의 벤더의 정보를 식별해주는 식별코드이다. Object Class는 상품 품목 코드에 해당하며, 24bkt의 용량으로 6개의 숫자, 문자 조합하여 약 1천 6백만 개 상품을 구분할 수 있는 일련번호로 구성 되어 있다. Serial Number는 상품의 고유 식별번호로, 36blt의 숫자, 문자 조합하여 680억개의 상품을 부여할 수 있다.

EPCglobal은 미들웨어 기술 체계를 구축하는 요소로 EPC, Savant, ONS, PML등을 구성하여 Back-end Server 시스템을 구축하고, 인터넷 망에 연동되어 지속적으로 발생되는 데이터를 수집, 제어, 관리를 하는 응용 서비스를 제공한다. 또한 다양한 RFID 리더 인터페이스, 코드, 네트워크 연동 등 다양한 Application에 대해 상호 운용성을 보장할 수 있도록 관리한다[4-6].

2.4 무선 RFID 보안 요소

RFID 시스템은 무선 환경을 사용하고 있기 때문에 유선상의 보안 문제점보다 더 많은 보안 위협요소가 존재하게 된다. RFID 보안 시스템을 구성하기 위해서는 시스템의 연산량과 메모리 자원을 고려해야 하고, 대칭 키 암호화 기법이나, 보안성이 우수한 공개키 암호화 기법을 적용하기에는 많은 문제점이 존재한다. 따라서 RFID 환경에서 효율성과 안전성을 제공하기 위해서는 해시 함수와 XOR 연산을 수행하는 RFID 인증 프로토콜이 있으나, 보안성 문제는 여전히 존재하며, RFID 정보서비스 보안 요구사항으로 상호인증, 무결성, 기밀성, 접근제어, 불구분성, 전방향 안전성이 있으며, 특히! 기밀성, 불구분성, 전방향 안전성이 제공 되어야 한다[7].

III. 무선 RFID 시스템 해시 보안

최근 RFID 시스템의 응용 및 활용분야가 점차 확대됨에 따라 RFID 보안은 중요한 이슈이다. RFID 보안 위협요소로는 RFID 태그에 부착된 소유물의 정보가 유출되는 경우와 RFID 태그의 직접적인 식별 정보와 고유한 ID가 유출되어 공격자로부터 보안 위협이 존재한다. 3장에서 해시 함수와 기 연구된 RFID 시스템의 XOR 기반 기법과 해시를 이용한 기법을 소개하고 문제점을 분석하도록 한다.

3.1 해시 함수

일방향 해시 함수는 임의의 길이를 가진 입력 값을 받아 해시 함수 h()를 통해 고정된 크기의 출력값을 유지하는 암호화 기법을 말한다. 해시함수의 특징은 주어진 key값 k에 대해 h(k) 형태로 해시 함수를 수행 한 후, 0부터 배열의 크기 -1 사이의 결과값을 배열 인덱스로 저장하는 방식으로 역방향으로 입력값 $h(k_n-1)$을 구할 수 없다.

해시함수의 일반적으로 사용되는 입력 길이는 128bit, 160bit, 192bit, 256bit 등이며, 대표적인 일방향 해시함수는 MD5, SHA-1 알고리즘을 사용했으나, 동일한 출력 값, 즉 출동이 발생할 수 있어 SHA-2 등이 주로 이용되고 있다[8].

표 2. SHA 알고리즘
Table 2. SHA algorithm

Algorithm	Message	Block	Result	Strength
SHA-1	$< 2^{64}$	512bit	160bit	0.625
SHA-256	$< 2^{64}$	512bit	256bit	1
SHA-384	$< 2^{128}$	1024bit	384bit	1.5
SHA-512	$< 2^{128}$	1024bit	512bit	2

3.2 RFID 시스템의 XOR 및 해시기법

무선 RFID 시스템의 보안 기법들은 다양한 상호 인증프로토콜 관련연구와 연산량을 줄이면서 보안성을 유지할 할 수 있는 XOR 기반 기법과 해시함수를 이용한 기법들이 지속적으로 연구되고 있다. 그림 5는 RFID 시스템의 XOR 기반 기법과 해시함수를 이용한 보안기법들을 보이고 있으며, 3,3절에서는 논문에 배경이 된 해시 락 기반 ID 변형기법에 대해 기술한다.

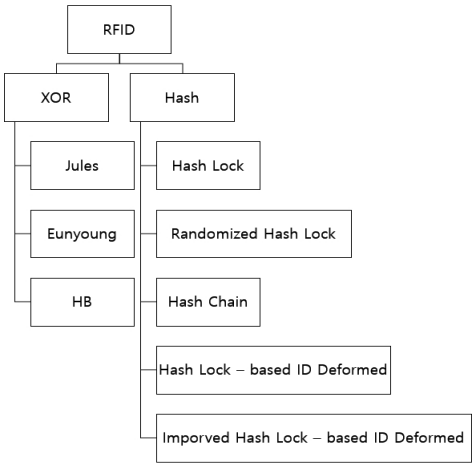

그림 4. RFID 시스템의 XOR 및 해시기법
Fig. 4 XOR and hash techniques of RFID system

3.3 해시 락 기반 ID 변형 기법

해시함수 기반의 대표적인 해시 락 기법은 저렴한 비용과, RFID 태그에서 리소스 제한의 문제점을 개선하기 위해 사용되는 기법이며, 해시 락 기반의 ID 변형 기법은 RFID 태그안의 해시함수가 들어있다고 가정하며, 매 세션마다 ID 변형을 위해 해시 연산을 수행하게 되는 기법을 말한다.

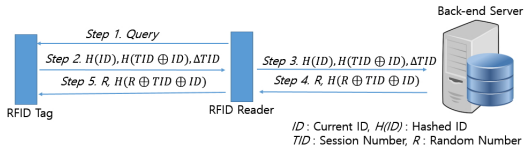

그림 5. Hash-Lock 기반 ID 변형기법
Fig. 5 Hash-Lock based ID deformed

그림 5의 해시 락 기반 ID 변경기법의 수행절차를 보이고 있다. RFID 리더가 태그에게 *Query*를 보낸 후, RFID 태그는 현재의 *ID*값을 해시한 $H(ID)$, 현재의 인증 세션번호인 *TID* 값에 가장 최근에 성공한 인증 세션번호 LST(: Last Session Number)를 제외한 $\triangle TID$, 그리고 $H(TID \oplus ID)$를 RFID 리더에게 전송한다.

RFID 리더는 $H(ID), H(TID \oplus ID), \triangle TID$ 값을 Back-end 서버에 저장하게 되며, Back-end 서버는 데이터베이스 안의 $H(ID)$ 값이 저장되어 있는 해시 테이블을 찾아낸다. 다른 값과 해시 테이블에 저장되어 값의 일치 여부를 확인한 후, 임의의 난수 R을 생성하여 테이블 해시 테이블을 갱신하고, 새로운 키 값 $H(R \oplus ID)$를 가지는 새로운 해시 테이블을 갱신하여 함께 보관한다.

그 후 R값과 $H(R \oplus TID \oplus ID)$값을 함께 RFID 리더에게 송신하고, RFID 리더는 R, $H(R \oplus TID \oplus ID)$를 RFID 태그에게 송신한다. RFID 태그는 이전에 수신 된 R값을 자신의 TID값, ID와 함께 XOR 연산을 수행하고, 수신된 $H(R \oplus TID \oplus ID)$ 값과 일치여부를 확인한 후, $ID = TID \oplus ID$로 변경한다[9].

3.4 해시 락 기반 ID 변형 기법의 문제점

해시 락 기반 ID 변형 기법은 Back-end 서버의 계산량이 가볍고 기밀성과 재전송 공격의 안전성을 보장하게 된다. 하지만 불구분성을 보장하지 못한다는 문제점이 존재한다.

첫 번째 동일한 $H(ID)$값의 송신은 공격자로부터 RFID 태그의 위치추적이 될 수 있다. 두 번째 $\triangle TID$값의 일정한 증가는 RFID 태그의 다음 응답정보 일부를 예측할 수 있게 된다. 세 번째 임의의 RFID 리더가 지속적으로 태그에게 *Query*를 전송하게 되면 $\triangle TID$값이 증가하게 되어, 다른 RFID 태그와 구분이 가능하게 된다. 네 번째 정상적인 RFID리

더의 송신 값을 가로 챈 후, 공격자는 임의로 생성한 *R=0*값과 이를 이용해서 계산된 $H(R \oplus TID \oplus ID)$ 값을 RFID 태그에게 송신 시 RFID 태그는 정상적인 값으로 인지하게 되며, ID를 변경하지만, *R*값이 0이기 때문에 원래의 *ID*를 유지하게 된다. 이처럼 Back-end 서버에 저장된 정보와 RFID 태그에 저장되어 있는 정보의 불일치 문제로 인해 불구분성과 전방향 안전성을 보장하지 못한다.

Ⅳ. 제안기법

RFID 시스템의 보안 기법들은 아직 연구해야할 과제가 많으며, 해시 락 ID 변형 기법의 문제점을 분석하여 본 절에서는 연산량을 줄이고, 강력한 보안을 제공하기 위해 기밀성, 불구분성, 전방향 안전성을 고려한 해시된 RFID 보안기법을 제안한다.

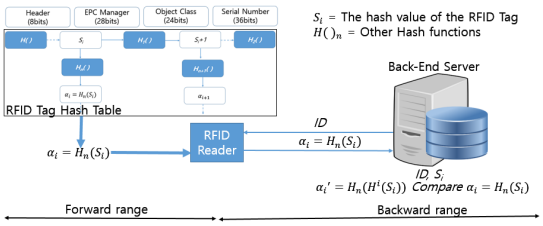

그림 6. 제안기법
Fig. 6 Proposed technique

RFID 시스템의 보안을 위해서는 ID 익명화를 통해 관련된 정보유출을 막아, RFID 태그의 위치추적을 피하는 방법과 공개키 암호화 알고리즘을 사용할 수 있지만, 공개키 암호화 기법의 경우 많은 양의 연산량을 고려해야하며 이는 RFID 태그의 비용 증가로 인해 경제성면에서 적절하지 않다.

그림 6은 RFID 태그는 해시함수 *H(), Hn()*을 가지고 있고, Back-endd 서버는 태그 *T*에 대한 각각의 식별정보 *ID*값과 임의로 생성된 RFID 태그의 해시된 비밀값 S_i 값을 데이터베이스에 저장하며, 각 태그에는 S_i를 가지고 있다고 가정한다. 태그가 읽혀지는 횟수인 *n*값이 정해지면 T의 범위는 *1<=T<=m* 이다. RFID 리더가 Query를 전송할 때 마다 태그는 현재 자신의 비밀값 $\alpha_i = H_n(S_i)$를 RFID 리더에게 송신한다.

RFID 태그는 자신의 비밀값을 스스로 갱신하기 위해 $S_{i+1} = H(S_i)$를 계산하고, RFID 리더는 $\alpha_i = H_n(S_i)$를 Back-end 서버에 송신한다. Back-end 서버는 모든 *1<=T<m*과 *1<=i<=n*에 대해서 $\alpha_i' = H_n(H^i(S_i))$를 계산하여 수신된 α_i와 일치하는 S_i 값을 찾아낸다. S_i 값으로 *ID*를 찾을 수 있고 Back-end 서버는 RFID 리더에게 ID 식별정보를 전송한 후 세션을 종료한다.

Back-end 서버는 데이터베이스 안에 저장된 모든 비밀값을 계산하여, 특정 RFID 태그가 어떤 해시 테이블에 속해 있는지 알아낼 수 있지만, RFID 태그의 개수 m이 증가하면 연산의 문제점이 발생할 수 있다.

제안기법은 현재의 비밀값 S_i를 해시함수 $H_n()$로 계산한 값을 RFID 리더에게 송신하기 때문에 연산과정이 단순하며, 공격자의 특정값 입력을 통한 공격이 어려우며, RFID 태구 외부에서 내부정보 값을 업데이트 하는 방식이 아니며, RFID 태그가 자신의 정보를 지속적으로 갱신하는 방법의 수행으로 스니핑 공격에 안전할 수 있다. 이로인해 기밀성과 불구분성을 보장할 수 있고, 해시 함수를 이용하여 계산하기 때문에 공격에 의해 내부 정보가 유출되는 경우라도 해시함수의 특성에 전방향 안전성을 보장할 수 있다.

Ⅴ. 결 론

ICT 산업의 급변화로 정보통신기술의 융합을 통한 새로운 산업혁명인 4차 산업혁명의 큰 패러다임 속에 무선으로 사물을 식별하는 RFID기술은 IOT 기술중 대표적인 인식기술로 산업 전 분야에 응용되고 경쟁력을 갖추고 있다. 하지만 RFID의 무분별한 사용으로 태그에 부착된 정보의 유출이나, 고유한 ID 유출 그리고 공격자의 공격으로 인한 각종 보안 위협요소가 존재하여, 유비쿼터스 환경에서 해결해야 할 문제이다. RFID 보안 시스템을 구성하기 위해서는 시스템의 연산량을 고려해야 하고, 보안성이 우수하고 무거운 보안기법을 적용하기에는 많은 문제점이 존재한다. 특히, 기밀성, 불구분성, 전방향 안전성을 제공하지 못한다면 다양한 문제점을 야기할 것이다.

이에 본 논문은 EPCglobal의 RFID 정보 서비스와 RFID 해시 보안을 분석하고, Hash-Lock 기반 ID 변

형 기법을 모델로 한, 해시코드를 이용한 EPC 코드 보안을 제안하였다..

제안 인증기법은 해시함수의 특성을 이용하여, 연산량을 줄인 단순한 프로토콜로 RFID 태그 스스로 내부 정보를 갱신하도록 구성되어졌다. 이를 통해 기밀성, 불구분성, 그리고 전방향 안전성을 보장하는 RFID 시스템이라 할 수 있다. 향후 4차산업혁명 시대에 RFID 시스템의 확장성을 고려하여, 각종 보안 알고리즘 연구와 RFID 시스템의 개선된 연구가 필요하게 될 것 이다.

감사의 글

"본 연구결과는 2019학년도 광주여자대학교 교내연구비 지원에 의하여 연구되었음".

(KWUI19-041)

References

[1] J. Jung, H. Lee, and Y. Kim, "High Speed Collision Avoidance Algorithm for Active RFID Network System," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 6, June 2016, pp. 581-590.

[2] R. Weinstein, "A Technical Overview and Its Application to the Enterprise," *IT Professional, IEEE Computer Society*, vol. 7, issue 3, June 2005, pp. 27-33.

[3] H. Chow, K. Choy, W. Lee, and K. Laub, "Design of a RFID case-based Resource Management System for Warehouse Operations," *J. of International Expert System with Applications*, vol. 20, issue 4, May 2006, pp. 561-576.

[4] C. Floerkemeier, D. Anarkat, T. Osinski, and M. Harrison, "PML Core Specification 1.0," *Auto-ID Center Recommendation*, Sept. 2003, pp. 5-25.

[5] U. Karthaus and M. Fischer, "Fully integrated passive UHF RFID transponder IC with 16.7-uW minimum RF input power," *J. of IEEE Journal for Solid-state Circuits*, vol. 38, no. 10, Oct. 2003, pp. 1602-1608.

[6] H. Yoon, M. Mohaisen, K. Chang, J. Bae, and G. Choi, "Performance Analysis of Wireless Communications between Tag and Reader in EPCglobal Gen-2 RFID System," *J. of Korean Institute of Electromagnetic and Engineering and Science*, vol. 18, no. 124, 2007, pp. 1047-1056.

[7] K. Han and G. Yim, "Design of an RFID Authentication Protocol Using Nonlinear Tent-Map," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 10, Aug. 2014, pp. 1145-1152.

[8] C. Lee "A Study on Effective using Security Routing based on Mobile Ad-hoc Networks," *Int. J. of Security and Its Application*, vol. 9, no. 7, 2015, pp. 141-152.

[9] C. Lee "Security Authentication Technique using Hash Code in Wireless RFID Environments," Int. *J. of Grid and Distributed Computing*, vol. 11, no. 10, 2018, pp. 93-102.

저자 소개

이철승(Cheol-Seung Lee)

2001년 광주대학교 공과대학 컴퓨터학과 졸업 (공학사)
2003년 조선대학교 대학원 컴퓨터공학과 졸업 (공학석사)
2008년 조선대학교 대학원 컴퓨터공학과 졸업(공학박사)
2012년 ~ 광주여자대학교 교양과정부 교수
※ 관심분야 : MANET Security, Android Security Wireless Network Security