논문 16-41-05-11 The Journal of Korean Institute of Communications and Information Sciences '16-05 Vol.41 No.05
http://dx.doi.org/10.7840/kics.2016.41.5.581

프라이버시 보호를 위한 RFID 인증 프로토콜의 안전성 분석과 개선

김 지 예◆, 원 동 호°

Security Analysis and Improvements of Authentication Protocol for Privacy Protection in RFID Systems

Jiye Kim◆, Dongho Won°

요 약

RFID(Radio Frequency IDentification) 기술은 지난 10년간 유통, 의료 등 여러 분야에 적용되었으며 향후 더 광범위하게 보편화될 것으로 기대된다. 그러나 태그와 리더는 무선 주파수를 이용하여 서로 통신하기 때문에 메시지 도청이나 변조에 안전하지 않다. 따라서 RFID 시스템은 예상되는 공격에 대응하기 위하여 보안 기술을 적용해야 한다. 2013년에 Oh 등은 태그와 리더 간 상호 인증 프로토콜을 제안하였다. 이 프로토콜은 프라이버시 보호를 위하여 태그의 위치 추적 문제를 해결하도록 설계되었으며 이를 위해서 태그는 대칭키 암·복호화와 XOR 연산만 수행하므로 효율적이다. 그러나 이 프로토콜에서는 모든 리더와 태그가 같은 키를 사용하고 있고 그 키는 장기간 갱신되지 않기 때문에 공격자에게 쉽게 노출될 수 있다. 우리는 이 키가 한 번 공격자에게 노출되면 대량의 태그에 대한 위장 공격이나 위치 추적이 가능하다는 것을 발견하였다. 본 논문에서는 발견된 취약점을 분석하고 안전성이 개선된 프로토콜을 제안한다. 또한 태그의 자원 제한적인 특성을 고려하여 제안 프로토콜이 연산량과 메시지 전송량 측면에서 효율적임을 보인다.

Key Words : RFID(Radio Frequency IDentification), Security, Privacy, Authentication Protocols

ABSTRACT

RFID(Radio Frequency IDentification) is a key technology in ubiquitous computing and is expected to be employed in more fields in the near future. Nevertheless, the RFID system is vulnerable to attacks by eavesdropping or altering of the messages transmitted in wireless channels. In 2013, Oh et al. proposed a mutual authentication protocol between a tag and a reader in RFID systems. Their protocol is designed to resist location tracking for privacy protection. However, all tags and readers use only one network-wide key in their protocol and tags are usually vulnerable to physical attacks. We found that their protocol is still vulnerable to tag/reader impersonation attacks and location tracking if an attacker obtains the network-wide key from a tag. In this paper, we propose a security improved authentication protocol for privacy protection in RFID systems. In addition, we demonstrate that the proposed scheme is efficient in terms of computation and communication costs.

※ 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.R0126-15-1111, 클라우드 보안을 위한 위험기반 인증·접근제어 프레임워크 및 보안상태 점검기술 개발)

◆ First Author : College of Information & Communication Engineering, Sungkyunkwan University, jykim.isg@gmail.com, 학생회원
° Corresponding Author : College of Information & Communication Engineering, Sungkyunkwan University, dhwon@security.re.kr, 종신회원

논문번호 : KICS2016-04-001, Received April 14, 2016; Revised May 3, 2016; Accepted May 3, 2016

Ⅰ. 서 론

RFID(Radio Frequency IDentification)는 모든 개체에 마이크로 칩을 내장한 태그(Tag)를 부착하고 리더(Reader)가 일정한 주파수 대역을 이용해 무선 통신으로 개체의 정보를 자동으로 인식하고 감지하는 센서 기반 기술이다[1-4]. RFID 기술의 적용은 국방, 의료, 유통, 제조업, 서비스 산업 등 다양한 분야에서 보편화되고 있으며 향후 더 광범위하게 우리의 생활을 바꾸어 놓을 것으로 기대된다[5-8]. 그러나 RFID 시스템에서 태그와 리더는 무선 주파수를 이용하여 서로 통신하기 때문에 다른 무선 통신과 마찬가지로 공격자의 메시지 도청이나 변조에 의한 스푸핑 공격(Spoofing Attacks), 재전송 공격(Replay Attacks), 서비스 거부 공격(Denial-of-service Attacks) 등에 취약할 수 있다[12,13]. 그 뿐 아니라 RFID 태그는 대량의 사물에 부착되어 배포되기 때문에 그 내부에 저장된 정보는 공격자의 물리적 공격에 안전하지 않다[7]. 따라서 RFID 시스템은 메시지의 기밀성과 무결성, 서비스의 가용성과 같은 보안 요구사항을 달성하기 위하여 보안 기술을 적용해야 한다. 인증 프로토콜은 가장 필수적이고 적용 가능한 보안 기술 중 하나로[16] 최근까지 RFID 시스템의 구성 요소 간 상호 인증 기술이 중요하게 연구되고 있다[1].

2012년 Bae는 RFID 시스템에서 프라이버시가 보호된 인증 프로토콜(DAP3-RS)을 제안하였다[5,9]. Bae는 고정된 태그 ID 전송에 의한 태그 위치 추적 문제와 같은 기존 프로토콜의 취약점을 해결하고자 리더와 태그의 난수를 AES 암호 기술로 암호화하여 인증 과정에 이용하였다[5,9]. 그러나 2013년에 Oh 등은 Bae의 프로토콜이 여전히 태그의 위치 추적 공격에 취약하며 메시지 재전송 등을 통한 위장 공격에도 안전하지 못하다는 것을 지적하였다[5]. 그들은 이러한 취약점들이 개선된 태그와 리더 간 상호 인증 프로토콜을 제안하였는데, 이 프로토콜은 리더와 태그가 상호 인증을 위하여 각자 생성한 랜덤 넘버를 서로 교환하여 이용한다. 이 과정에서 태그는 대칭키 암·복호화와 XOR 연산만을 수행하기 때문에 효율적이다.

그러나 Oh 등의 프로토콜에서는 모든 리더와 태그가 같은 암·복호화 키를 저장하고 있고 그 키는 태그의 수명 내내 갱신되지 않는 값(long-term key)이기 때문에 공격자에게 쉽게 노출될 수 있다. 더구나 RFID 시스템에서 태그는 물리적 공격에 취약하기 때문에 공격자가 태그 중 하나를 물리적으로 탈취하여 내부에 저장된 키를 추출할 수 있다[7]. 우리는 Oh 등의 프로토콜에서 공격자가 일단 키를 한 번 알아내면 메시지 도청을 통하여 다른 태그 또는 리더로 위장할 수 있다는 것을 발견하였다. 또한 이런 경우 태그의 식별 정보가 공격자에게 노출되기 때문에 태그의 위치 추적이 여전히 가능하였다. 이러한 공격들은 단 한 개의 태그만 훼손되어도 공격자가 도청 가능한 범위 내 있는 모든 태그들에 대하여 수행 가능하기 때문에 더욱 심각하다.

본 논문에서는 Oh 등의 프로토콜을 살펴보고 보안 취약점을 분석한다. 그리고 발견한 취약점을 제거하여 안전성이 개선된 프로토콜을 제안한다. 이를 위하여 제안 프로토콜에서는 각 태그에 고유한 키를 부여하고 그 키를 서버의 태그 정보 데이터베이스에서 관리한다. 또한 태그의 식별 정보 노출과 위치 추적으로 인한 프라이버시 침해를 방지하기 위하여 매 통신 세션마다 변경되는 동적 ID를 사용하였다. 추가적으로 네트워크 범용 키가 공격자에게 노출되어도 그것을 이용하여 훼손되지 않은 다른 태그의 통신을 공격할 수 없도록 설계하였다. 또한 태그의 제한된 하드웨어 자원을 고려하여[10] Oh 등의 프로토콜과 마찬가지로 대칭키 암호 기술을 이용한 암·복호화와 XOR 연산만을 사용하도록 설계하였다.

본 논문은 다음과 같이 구성된다. Ⅱ장에서 RFID 시스템의 구성과 보안 요구사항을 살펴본다. Ⅲ장에서는 Oh 등의 프라이버시 보호를 위한 RFID 인증 프로토콜을 리뷰하고, Ⅳ장에서는 그 취약점을 분석한다. Ⅴ장에서 우리가 제안하는 스킴을 단계별로 상세히 설명한다. Ⅵ장과 Ⅶ장에서는 제안 프로토콜을 안전성과 효율성 측면에서 분석한다. 마지막으로 Ⅷ장에서는 본 논문의 결론을 맺는다.

Ⅱ. 배경 지식

본 장에서는 일반적인 RFID 시스템의 구성과 동작 원리, 그리고 RFID 인증 프로토콜이 만족해야 하는 보안 요구사항에 대하여 살펴본다.

2.1 RFID 시스템

RFID 시스템은 일반적으로 리더, 태그, 그리고 태그 정보 데이터베이스를 관리하는 서버로 구성된다[1,2,5-7]. 리더는 소형 단말기 또는 고정된 장치로[1] 여러 장소에 설치되며 무선 주파수를 통하여 태그로 신호를 전달하고 태그로부터 필요한 정보를 수신한다[7]. 태그는 식별 가능한 고유의 ID를 가지며 각 개체에 하나씩 부착된다[1]. 태그는 리더나 서버에 비하여 연

산 처리 능력이나 저장 용량 등과 같은 자원이 제한적이다[6,10]. 서버는 태그 정보 데이터베이스를 관리하며 리더에 의해 수집된 태그의 정보는 유무선 네트워크를 통하여 서버로 전송된다[1]. 일반적으로 RFID 시스템에서 서버는 자원의 제약이 없다고 가정한다[1].

RFID 시스템에서 서버와 리더 간의 채널은 일반적으로 안전한 채널(Secure Channel)이며 리더와 태그 간의 채널은 안전하지 않은 공개 채널(Insecure Channel)로 가정한다[6]. 리더가 먼저 태그에게 질의(Query) 정보를 전송하면 태그는 자신의 고유한 ID를 리더에게 전송한다. 리더는 태그로부터 수집한 정보를 데이터베이스를 관리하는 서버에게 전송한다[1,6,7,15]. 서버는 태그로부터 수집한 정보를 응용 시스템이 요구하는 의미 있는 정보로 재구성하거나[7] 리더에게 태그 정보를 알려준다[6].

2.2 RFID 인증 프로토콜 보안 요구사항

RFID 시스템에서 태그와 리더 간의 통신은 공격자가 전송되는 메시지를 도청 또는 변조할 수 있는 공개 채널로 가정한다. 따라서 RFID 인증 프로토콜은 공격자가 메시지의 도청이나 변조를 통하여 공격에 필요한 정보를 알아낼 수 없어야 한다. 일반적으로 RFID 시스템의 인증 프로토콜은 다음과 같은 보안 요구사항을 고려하여 설계되어야 한다.

2.2.1 스푸핑 공격에 안전

스푸핑 공격은 공격자가 정당한 통신 주체 중 하나, 즉 서버, 리더, 또는 태그로 위장하여 인증에 필요한 정보나 유용한 정보를 얻어내는 것을 의미한다[2,6,7].

2.2.2 중간자 공격에 안전

RFID 시스템에서 중간자 공격(Man-In-The-Middle Attacks, MITM Attacks)이란 공격자가 통신하고 있는 리더와 태그 사이에 정당한 통신 주체처럼 위장하여 끼어들어 메시지를 조작하거나 공격에 필요한 정보를 얻어내는 공격이다[7].

2.2.3 재전송 공격에 안전

재전송 공격은 공격자가 태그나 리더 간에 전송되는 메시지를 저장하였다가 다음 통신에서 이를 재전송하여 정당한 태그나 리더로 인증 받는 공격이다[2,6].

2.2.4 태그 익명성

태그 익명성(Tag Anonymity)이란 ID와 같은 태그의 고유 식별 정보가 평문 형태로 전송되거나 태그와 리더 사이의 메시지를 이용하여 쉽게 계산되지 않아야 함을 의미한다[2,6,11].

2.2.5 위치 추적에 안전

위치 추적(Location Tracking)은 RFID 시스템에서 리더가 통신을 요청하는 질의 메시지를 브로트캐스트 할 때마다 태그가 변하지 않는 고정된 응답을 할 경우 이를 이용하여 해당 태그의 위치를 추적하는 것이다[3,5]. 공격자는 여러 지역에 불법 리더기를 설치하고 어떤 태그의 이동 경로를 추적한다[2]. 만약 사용자가 태그를 부착된 상품을 소지하고 있을 경우 태그의 위치 추적을 통하여 사용자의 프라이버시를 침해 할 수 있다[6,7,14]. 위치 추적 문제를 해결하기 위해서는 리더가 통신을 요청할 때마다 태그는 다른 값으로 응답하도록 설계되어야 한다[7].

2.2.6 물리적 공격에 안전

물리적 공격이란 태그의 메모리 내 정보를 추출하는 공격 기법으로 RFID 시스템에서 태그는 물리적 공격에 취약하다[7]. 물리적 공격으로 태그 내 저장된 비밀값이 노출된다면 대량의 태그 정보나 전체 시스템의 안전에 영향을 미칠 수 있다[7]. 보안 프로토콜은 그 자체만으로는 물리적 공격을 완전히 방어할 수 없지만 한 개 또는 소수(少數)의 태그가 물리적 공격에 훼손되더라도 훼손되지 않은 태그나 전체 네트워크은 안전하도록 설계되어야 한다.

2.2.7 위장 공격에 안전

위장 공격(Impersonation Attacks)이란 상대방이 공격자를 해당 RFID 시스템의 정당한 태그 혹은 리더로 여기도록 속이는 것을 의미한다[2].

2.2.8 상호 인증

상호 인증(Mutual Authentication)은 RFID 시스템에서 리더와 태그 모두 정당한 통신자인지 명시적인 인증을 통해서 확인하는 과정이다[2,17]. 태그와 리더 사이에 공유한 비밀값을 확인하거나 서로 동일한 값을 생성함으로써 상대방을 인증한다[2].

Ⅲ. Oh 등의 프라이버시 보호를 위한 RFID 인증 프로토콜

본 장에서는 Oh 등이 제안한 프라이버시 보호를 위한 RFID 인증 프로토콜을 살펴본다. 그림 1은 Oh 등의 프로토콜의 수행 과정을 나타낸다. 프로토콜의 명확한 설명을 위하여 논문 전체에서 사용한 표기들을 표 1과 같이 정리하였다.

표 1. 표기법
Table 1. Notations

Notations	Descriptions
Svr	Server
Rdr_j	j-th reader
Tg_i	i-th tag
[ ]	Database of Svr
x_s	Secret value known to only Svr
ID_i	Identity of Tg_i
DID_i, $\mathfrak{DID}_i$	Dynamic ID of Tg_i
$TagInfo_i$	Information of Tg_i
K	Network-wide symmetric key shared between tags and readers
K_i	Symmetric key shared between only Svr and Tg_i, $K_i = h(ID_i \| x_s)$
RN_i, RN_j	Random number of Tg_i and Rdr_j
$h(\bullet)$	One-way hash function
$c = ENC_k(m)$	Encryption of a plaintext m using a symmetric key k
$m = DEC_k(c)$	Decryption a ciphertext c using a symmetric key k
$\oplus$	XOR operation
$\|$	Concatenation operation
$=?$	Verification operation
$\{m\}$	m is the message transmitted in an insecure channel.
(m)	m is the message transmitted in a secure channel.

리더와 태그가 설치되는 초기화 단계에서 리더 Rdr_j와 태그 Tg_i에 대칭키 K를 각각 저장한다.

초기화 단계 이후 리더 Rdr_j가 자신의 무선 범위 내에 질의 메시지를 브로드캐스트하면 인증 과정이 다음과 같이 수행된다 (Step 1~6) (그림 1). 이 때 서버 Svr와 리더 Rdr_j 간은 안전한 채널, 리더 Rdr_j와 태그 Tg_i 간은 공개 채널로 통신한다고 가정한다.

Step 1: 리더 Rdr_j는 랜덤 넘버 RN_j를 생성한 후 RN_j을 프로토콜의 초기화 단계에 설치했던 키 K를 이용하여 암호화한다.

$$C_j = ENC_K(RN_j) \tag{1}$$

리더 Rdr_j는 자신의 무선 범위 내에 질의 메시지 {Query, C_j}를 브로드캐스트한다.

Step 2: 태그 Tg_i는 리더 Rdr_j로부터 질의 메시지 {Query, C_j}를 수신하면 자신의 랜덤 넘버 RN_i를 생성한 후 키 K를 이용하여 C_j를 복호화한다.

$$RN_j' = DEC_K(C_j) \tag{2}$$

태그 Tg_i는 RN_j'를 키로 이용하여 자신의 랜덤 넘버 RN_i, 자신의 ID ID_i, 그리고 RN_j'를 암호화한다.

$$C_i = ENC_{RN_j'}(RN_i \| ID_i \| RN_j') \tag{3}$$

태그 Tg_i는 리더 Rdr_j에게 응답메시지 $\{C_i\}$를 전송한다.

Step 3: 리더 Rdr_j는 자신이 생성했던 랜덤 넘버 RN_j를 키로 이용하여 C_i를 복호화한다.

$$RN_i^* \| ID_i^* \| RN_j' = DEC_{RN_j}(C_i) \tag{4}$$

리더 Rdr_j은 태그 Tg_i를 인증하기 위하여 자신이 생성했던 랜덤 넘버 RN_j와 태그 Tg_i의 응답메시지에 포함되었던 RN_j'의 값을 비교한다. 만약 이 두 값이 동일하다면 리더 Rdr_j는 안전한 채널을 통하여 서버 Svr에게 태그 Tg_i의 ID ID_i^*을 전송하고, 그렇지 않다면 인증 과정을 중단한다.

Step 4: 서버 Svr는 리더 Rdr_j로부터 ID_i^*를 수신하면 그것을 이용하여 자신의 데이터베이스에서 태그 Tg_i의 정보 $TagInfo_i$를 찾고 안전한 채널을 통하여 리더 Rdr_j로 전송한다.

Step 5: 리더 Rdr_j는 태그 Tg_i로부터 수신한 RN_i^*와 자신의 랜덤 넘버 RN_j를 XOR 연산한다.

$$V = RN_i^* \oplus RN_j \tag{5}$$

리더 Rdr_j는 메시지 $\{V\}$를 태그 Tg_i로 전송한다.

Step 6: 태그 Tg_i는 리더 Rdr_j로부터 메시지 $\{V\}$를 수신하면 자신의 랜덤 넘버 RN_i와 리더 Rdr_j로부터 수신했던 RN_j'를 XOR 연산한다.

$$V' = RN_i \oplus RN_j' \tag{6}$$

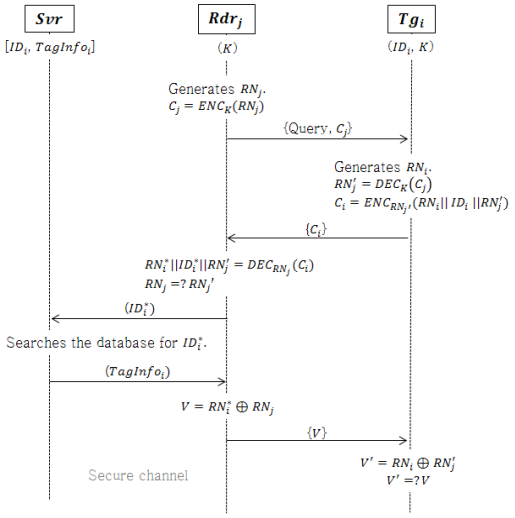


그림 1. Oh 등의 프라이버시 보호를 위한 RFID 인증 프로토콜
Fig. 1. Oh et al.'s authentication protocol for privacy protection in RFID system

태그 Tg_i는 리더 Rdr_j의 인증을 위하여 V'와 V의 값을 비교한다. 만약 이 두 값이 동일하면 태그 Tg_i의 리더 Rdr_j 인증이 성공적으로 완료된다. 반면 두 값이 동일하지 않다면 인증 실패로 프로토콜은 중단된다.

Ⅳ. Oh 등의 프로토콜의 취약점 분석

Oh 등의 RFID 인증 프로토콜은 리더와 태그 각각 생성한 랜덤 넘버를 이용하여 상호 인증하고 있으며 이를 위하여 태그는 대칭키 암·복호화와 XOR 연산만을 수행하기 때문에 연산량 측면에서 효율적이다. 그러나 이 프로토콜에서 키 K는 모든 리더와 태그에 광범위하게 저장되고 시스템의 수명 내내 갱신되지 않는 값(long-term key)이기 때문에 공격자에게 노출될 위험이 크다. 더구나 일반적으로 RFID 시스템에서 태그는 물리적 공격에 취약하다[7]. 따라서 공격자는 대량의 객체에 부착되어 배포된 태그 중 하나를 물리적으로 탈취하여 내부에 저장된 키 K를 추출할 수 있다. 공격자에게 키 K가 한 번 노출되면 메시지 도청을 통하여 태그들의 ID를 알아내거나 위치를 추적할 수 있다. 또한 정당한 태그나 리더로 인증받도록 상대 통신자를 속이는 위장 공격이 가능하다. 이러한 공격들은 공격자가 키 K를 얻기 위하여 훼손한 태그 뿐 아니라 도청 가능한 범위 내 있는 모든 태그들에 대하여 수행 가능하다는 점에서 더욱 심각하다.

4.1 태그의 식별 정보 노출

Oh 등의 프로토콜에서 공격자가 키 K를 알아내고 리더와 태그들 사이에 송수신되는 메시지를 도청한다면 해당 태그들의 ID를 복구할 수 있다. 예를 들어, 공격자가 태그 Tg_i로부터 키 K를 알아낸 뒤 리더 Rdr_j와 다른 태그 Tg_{i+1} 사이에 전송되는 메시지 {Query, C_j}와 $\{C_{i+1}\}$를 도청했다고 가정하자. 그림 2와 같이, 공격자는 키 K를 알고 있기 때문에 메시지 {Query, C_j}의 C_j를 복호화할 수 있다.

$$RN_j = DEC_K(C_j) \tag{7}$$

그런 다음 공격자는 키 RN_j를 계산하였기 때문에 태그 Tg_{i+1}의 응답 메시지 $\{C_{i+1}\}$도 복호화할 수 있다.

$$RN_{i+1} \| ID_{i+1} \| RN_j = DEC_{RN_j}(C_{i+1}) \tag{8}$$

따라서 공격자는 태그 Tg_{i+1}의 ID ID_{i+1}를 얻을 수 있으며 태그 Tg_{i+1}에 대한 익명성을 제공하지 못한다.

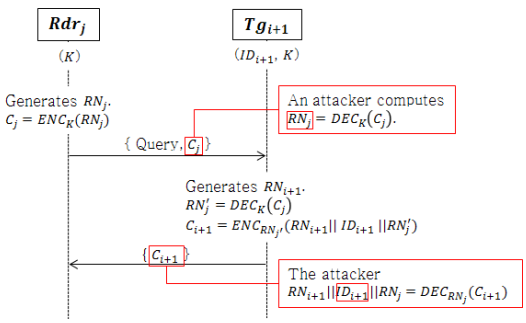


그림 2. Oh 등의 RFID 인증 프로토콜 상에서의 태그 ID 추출 과정
Fig. 2. Attacker's tag ID extraction in Oh et al.'s authentication protocol

4.2 태그의 위치 추적

Oh 등의 프로토콜에서 리더의 질의 메시지에 대한 태그 Tg_{i+1}의 응답 메시지는 랜덤 넘버를 포함한 암호문이므로 매 통신 세션마다 변경된다. 그러나 그림 2에서 살펴본 것처럼 공격자가 키 K를 알면 리더와 태그 사이에 교환되는 메시지를 도청하여 태그 ID를 알아낼 수 있다. 따라서 만약 공격자가 여러 지역에 설치된 리더기 근처에서 송수신되는 메시지를 도청하

여 태그 ID를 복구하는 과정을 반복한다면 태그 Tg_{i+1}의 위치 추적이 가능하다.

4.3 태그 위장 공격

그림 2에서 살펴본 것처럼 공격자가 키 K를 알면 리더와 태그 사이에 교환되는 메시지를 도청하여 태그 ID를 알아낼 수 있다. 이와 연계한 공격으로 공격자는 키 K와 태그 ID를 이용하여 정당한 태그로 위장할 수 있다. 예를 들어, 키 K와 태그 Tg_{i+1}의 ID ID_{i+1}를 알고 있는 공격자는 리더 Rdr_j로부터 질의 메시지 {Query, C_j}를 수신했을 때 다음과 같이 C_a를 생성한다.

$$RN_j = DEC_K(C_j) \tag{9}$$

$$C_a = ENC_{RN_j}(RN_a \| ID_{i+1} \| RN_j) \tag{10}$$

공격자가 응답 메시지 {C_a}를 리더 Rdr_j로 전송하면 리더 Rdr_j는 다음과 같이 공격자를 정당한 태그 Tg_{i+1}로 인증한다.

$$RN_a^* \| ID_{i+1}^* \| RN_j' = DEC_K(C_a) \tag{11}$$

$$RN_j = ? RN_j' \tag{12}$$

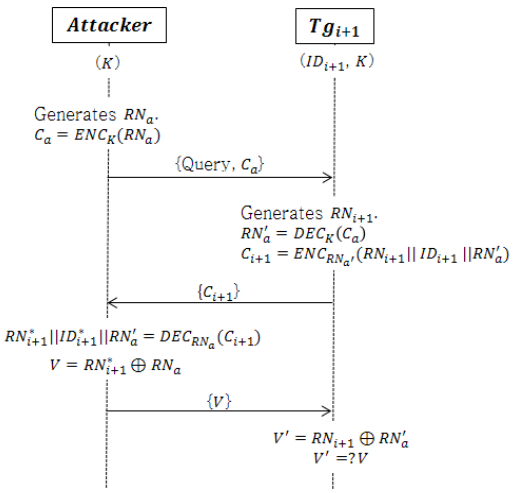


그림 3. Oh 등의 RFID 인증 프로토콜 상에서의 리더 위장 공격 과정
Fig. 3. Reader Impersonation attacks in Oh et al.'s authentication protocol

4.4 리더 위장 공격

만약 공격자가 i-번째 태그 Tg_i로부터 키 K를 알아냈다고 가정하자. 공격자는 그림 3와 같이 키 K를 이용하여 태그 Tg_i 외 다른 태그들에게 정당한 리더처럼 위장할 수 있다. 공격자는 인증 과정을 시작하기 위하여 랜덤 넘버 RN_a를 생성한 다음 이미 획득한 키 K를 이용하여 그것을 암호화한다.

$$C_a = ENC_K(RN_a) \tag{13}$$

공격자가 질의 메시지 {Query, C_a}를 브로드캐스트하면 공격자의 무선 범위 내 태그 Tg_{i+1}은 랜덤 넘버 RN_{i+1}을 생성하고 키 K로 C_a를 복호화한다.

$$RN_a' = DEC_K(C_a) \tag{14}$$

태그 Tg_{i+1}가 RN_a'를 키로 하여 자신의 랜덤 넘버 RN_{i+1}, 자신의 ID ID_{i+1}, 그리고 수신한 RN_a'를 암호화한 다음 그 결과값 C_{i+1}를 응답메시지로 공격자에게 전송한다.

$$C_{i+1} = ENC_{RN_a'}(RN_{i+1} \| ID_{i+1} \| RN_a') \tag{15}$$

키 RN_a'는 공격자가 생성한 랜덤 넘버이기 때문에 공격자는 C_{i+1}를 복호화할 수 있다. 복호화 결과로부터 태그 Tg_{i+1}의 ID와 Tg_{i+1}로부터 정당한 리더로 인증받는데 필요한 랜덤 넘버 RN_{i+1}^*를 추출할 수 있다.

$$RN_{i+1}^* \| ID_{i+1}^* \| RN_a' = DEC_{RN_a'}(C_{i+1}) \tag{16}$$

공격자는 태그 Tg_{i+1}로부터 수신한 RN_{i+1}^*과 자신이 생성한 RN_a를 XOR 연산한 다음 그 결과를 태그 Tg_{i+1}에게 전송한다.

$$V = RN_{i+1}^* \oplus RN_a \tag{17}$$

태그 Tg_{i+1}는 V값을 검증하고 공격자를 정당한 리더로 인증하게 된다.

Ⅴ. 제안 프로토콜

이 장에서는 이전 Ⅳ장에서 살펴본 취약점을 개선한 프라이버시 보호를 위한 RFID 인증 프로토콜을 제

안한다. 제안 프로토콜은 스푸핑 공격, 중간자 공격, 재전송 공격과 같이 RFID 인증 프로토콜에 가능한 공격에 대하여 안전해야 한다. 또한 위장 공격에 대응하기 위하여 태그와 리더 간의 상호 인증 과정을 제공해야 한다. 사용자의 프라이버시를 보호하기 위해서 태그의 익명성을 제공해야 할 뿐 아니라 태그의 위치 추적이 불가능해야 한다. 추가적으로 제안 프로토콜에서는 공격자가 한 개 또는 소수의 태그로부터 비밀값을 알아낸다 하더라도 그것을 이용하여 훼손되지 않은 태그의 통신을 공격하거나 전체 네트워크의 보안을 위협할 수 없도록 설계되어야 한다.

제안 프로토콜은 크게 초기화 단계와 인증 단계로 구성되며 본 장에서는 제안 프로토콜의 각 단계의 수행 과정을 상세히 설명한다.

5.1 초기화 단계

프로토콜의 초기화 단계는 서버, 리더, 그리고 태그에 인증 시 필요한 정보를 설치하는 단계로 다음 과정을 단 한 번 수행한다 (Step I-1~I-3).

Step I-1: 모든 리더와 태그는 키 K를 공유한다.

Step I-2: 태그 Tg_i를 위하여 랜덤 넘버 rn_i을 생성한 후 Tg_i의 ID ID_i와 rn_i의 연접한 값을 해쉬 연산하여 동적 ID DID_i를 계산한다.

$$DID_i = h(ID_i \| rn_i) \tag{18}$$

태그 Tg_i의 고유한 키 K_i를 생성하기 위하여 태그 Tg_i의 ID ID_i와 서버의 비밀값 x_s를 이용하여 $h(ID_i \| x_s)$를 계산한다. 일방향 해쉬 함수의 특성에 따라 서버를 제외한 다른 통신자나 공격자가 K_i로부터 ID_i나 x_s을 유도하는 것은 불가능하다.

$$K_i = h(ID_i \| x_s) \tag{19}$$

태그 Tg_i에 앞서 생성한 DID_i와 K_i를 저장한다.

Step I-3: 비밀값 x_s를 서버 Svr에 저장한다. 이 x_s는 서버 외 다른 통신자에게는 공유하지 않는다.

또한 서버 Svr는 자신이 관리하는 태그 정보 데이터베이스에 태그들의 ID와 태그 정보 뿐 아니라 동적 ID 정보를 추가한다. 예를 들어, 태그 Tg_i를 위하여 태그 Tg_i의 ID ID_i, 동적 ID DID_i, 그리고 태그 정보 $TagInfo_i$를 서버의 데이터베이스에 추가한다.

5.2 인증 단계

이 단계에서는 리더와 태그가 상호 인증한 후 다음 통신 세션을 위하여 태그의 동적 ID를 갱신한다. 기존의 가정과 마찬가지로 서버와 리더 간은 안전한 채널로 통신하며, 리더와 태그 간은 공개 채널로 통신한다. 리더의 질의 메시지에 대하여 무선 통신 범위 내에 존재하는 태그가 응답하면 인증 단계가 시작된다 (Step A-1~A-6). 그림 4는 제안 프로토콜의 인증 단계를 나타낸다.

Step A-1: 리더 Rdr_j는 랜덤 넘버 RN_j를 생성한 후 그것을 프로토콜의 초기 단계에 설치된 키 K와 함께 XOR 연산을 수행한다.

$$V = K \oplus RN_j \tag{20}$$

리더 Rdr_j는 자신의 무선 범위 내 모든 태그에게 질의 메시지 {Query, V}를 브로드캐스트한다.

Step A-2: 태그 Tg_i가 메시지 {Query, V}를 수신하면 자신의 키 K_i를 이용하여 $V_i = K_i \oplus V$를 수행한다.

그런 다음 태그 Tg_i는 자신의 키 K_i를 이용하여 V_i을 암호화한다.

$$C_i = ENC_{K_i}(V_i) \tag{21}$$

태그 Tg_i는 리더 Rdr_j에게 응답 메시지 {DID_i, C_i}를 전송한다.

Step A-3: 리더 Rdr_j가 태그 Tg_i로부터 메시지 {DID_i, C_i}를 수신하면 안전한 채널을 통하여 DID_i를 서버 Svr로 전달한다.

Step A-4: 서버 Svr는 DID_i로 자신의 데이터베이스를 검색하여 태그 Tg_i의 ID ID_i와 태그 정보 $TagInfo_i$를 찾는다.

서버 Svr는 자신의 비밀값 x_s와 ID_i를 연접한 결과를 XOR 연산하여 키 K_i'를 생성한다.

$$K_i' = h(x_s \| ID_i) \tag{22}$$

서버 Svr는 태그 Tg_i의 태그 정보 $TagInfo_i$와 키 K_i'를 안전한 채널을 통해 리더 Rdr_j로 전송한다.

Step A-5: 리더 Rdr_j는 C_i를 서버 Svr로부터 수신한 키 K_i'를 이용하여 복호화한다.

$$V_i^* = DEC_{K_i'}(C_i) \tag{23}$$

리더 Rdr_j는 키 K_i'와 V를 XOR 연산한 결과값 $(K_i' \oplus V)$과 복호화 결과값인 V_i^*를 비교한다. 만약 두 값이 같다면 응답 메시지 $\{DID_i,\ C_i\}$의 송신자는 정당한 태그 Tg_i라는 것을 의미한다. 만약 두 값이 다르다면 인증 실패로 인증 단계는 중단된다.

리더 Rdr_j은 다음 통신 세션을 위하여 태그 Tg_i의 동적 ID를 갱신한다. 태그 Tg_i의 새로운 동적 ID $\mathcal{DID}_i$는 다음과 같이 현재의 동적 ID DID_i와 키 K_i'를 연접한 값을 해쉬 연산하여 생성한다.

$$\mathcal{DID}_i = h(DID_i \| K_i') \tag{24}$$

리더 Rdr_j은 태그 Tg_i의 키 K_i'를 이용하여 V_i^*와 $\mathcal{DID}_i$를 암호화한다.

$$C_j = ENC_{K_i'}(V_i^* \| \mathcal{DID}_i) \tag{25}$$

리더 Rdr_j는 태그 Tg_i의 새로운 동적 ID $\mathcal{DID}_i$를 서버 Svr와 태그 Tg_i가 공유하도록 서버 Svr에게는 DID_i와 $\mathcal{DID}_i$를, 태그 Tg_i에게는 암호화된 메시지 $\{C_j\}$를 전송한다.

Step A-6: 태그 Tg_i는 리더 Rdr_j로부터 메시지 $\{C_j\}$를 수신하면 자신의 키 K_i를 이용하여 C_j를 복호화한다.

$$V_i^* \| \mathcal{DID}_i = DEC_{K_i}(C_j) \tag{26}$$

태그 Tg_i는 메시지 $\{C_j\}$의 송신자가 정당한 리더임을 인증하기 위해서 V_i^*와 V_i의 값을 비교한다. 만약 두 값이 같다면 메시지 $\{C_j\}$의 송신자는 태그 Tg_i의 키 $K_i(=K_i')$을 보유한 정당한 리더이다. 그러나 두 값이 다르다면 리더의 인증은 실패하고 인증 단계는 중단된다.

태그 Tg_i은 자신의 동적 ID DID_i를 $\mathcal{DID}_i$로 교체한다. 한편 서버 Svr 또한 자신의 태그 정보 데이터베이스에서 태그 Tg_i의 동적 ID 정보를 DID_i에서 $\mathcal{DID}_i$로 변경한다.

Ⅵ. 제안 프로토콜의 안전성 분석

본 장에서는 Ⅱ장에서 기술했던 보안 요구사항을 중심으로 제안 프로토콜의 안전성을 논한다. 표 2는 제안 프로토콜의 안전성을 기존 Oh 등의 프로토콜과 비교한 결과를 나타낸다.

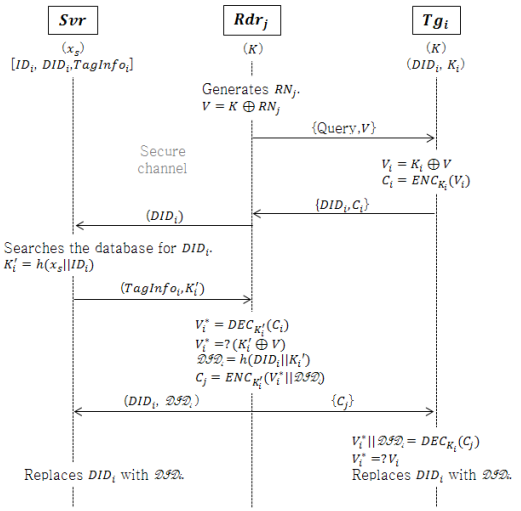


그림 4. 제안 프로토콜의 인증 단계
Fig. 4. Authentication phase of the proposed protocol

6.1 상호 인증

RFID 시스템에서 상호 인증은 태그와 리더가 서로 공유한 비밀값을 확인하거나 동일한 값을 생성함으로써 상대방이 정당한 통신자인지 확인하는 과정이다[2]. 제안 프로토콜에서 리더는 메시지 $\{DID_i,\ C_i\}$를 수신하면 메시지 송신자가 정당한 태그 Tg_i임을 인증하기 위하여 키 K_i를 이용하여 암호문 C_i를 복호화한다. 만약 복호화된 평문 V_i^*와 $(K_i' \oplus V)$의 계산값이 일치한다면 메시지 $\{DID_i,\ C_i\}$를 보낸 상대방은 정당한 태그 Tg_i이다. 제안 프로토콜의 초기화 단계에 따라 서버와 태그 Tg_i만이 키 K_i 값을 알고 있기 때

문에 서버 아니면 태그 Tg_i만이 $V_i^*(= V_i = K_i' \oplus V = K_i \oplus V)$를 계산할 수 있기 때문이다. 한편 태그 Tg_i는 메시지 $\{C_j\}$를 수신하면 메시지 송신자가 정당한 리더임을 인증하기 위하여 키 K_i를 이용하여 C_j를 복호화한다. 만약 복호화된 평문 $V_i^* \| \mathcal{DID}_i$에서 V_i^*와 V_i의 값이 동일하다면 메시지 $\{C_j\}$를 보낸 상대방은 정당한 리더이다. 왜냐하면 제안 프로토콜의 초기화 단계에서 서버와 태그 Tg_i만이 키 K_i를 공유하였기 때문에 서버 또는 서버와 안전한 채널로 통신하는 리더만이 $V_i(= K_i \oplus V)$ 값을 계산하고 암호문 C_j를 생성할 수 있기 때문이다.

6.2 물리적 공격에 안전

제안 프로토콜에서는 공격자가 어떤 태그 내부에 저장된 비밀값을 알아내도 그것을 이용하여 다른 태그의 통신을 효과적으로 공격할 수 없다. 예를 들어, 공격자가 태그 Tg_i로부터 비밀값 K, DID_i, 그리고 K_i를 추출한 다음, 리더 Rdr_j와 (Tg_i가 아닌) 다른 태그 Tg_{i+1} 간에 송수신되는 메시지를 도청했다고 가정하자. 우선 태그 Tg_{i+1}로부터 리더 Rdr_j에게 전송되는 응답 메시지 $\{DID_{i+1}, C_{i+1}\}$는 태그 Tg_i의 세 비밀값을 이용하여 공격이 불가하다. 왜냐하면 DID_{i+1}는 태그 Tg_{i+1}의 동적 ID이고 C_{i+1}는 태그 Tg_{i+1}의 키 K_{i+1}를 이용하여 암호화되었기 때문에 태그 Tg_i의 세 비밀값과 아무런 관련이 없기 때문이다. 마찬가지로 리더 Rdr_j로부터 태그 Tg_{i+1}에게 전송되는 메시지 $\{C_j'\}$ 또한 키 K_{i+1}를 이용하여 암호화되었기 때문에 태그 Tg_i의 세 비밀값을 이용하여 의미있는 공격을 수행할 수 없다. 한편 키 K는 시스템의 모든 태그와 리더가 사용하는 범용 키이기 때문에 공격자는 리더 Rdr_j로부터 브로드캐스트되는 질의 메시지 {Query, V}를 도청하면 $V \oplus K$를 계산함으로써 리더 Rdr_j의 랜덤 넘버 RN_j를 알아낼 수 있다. 그러나 RN_j만으로는 다른 공격에 필요한 정보를 얻어낼 수 없을 뿐 아니라 RN_j는 매 세션 새로 생성된다. 따라서 제안 프로토콜은 한 개 또는 소수의 태그가 훼손되더라도 훼손되지 않은 다른 태그나 시스템 전체의 안전에는 영향을 미치지 않는다.

6.3 위장 공격, 스푸핑 공격, 그리고 중간자 공격에 안전

제안 프로토콜은 태그와 리더 간의 상호 인증 과정을 제공하므로 공격자는 태그나 리더로 위장할 수 없다. 만약 공격자가 물리적인 태그 탈취 등을 통하여 태그 Tg_i 내부에 저장된 비밀값 K, DID_i, 그리고 K_i를 알게 된다고 하더라도 공격자는 태그 Tg_i 외 다른 태그로 위장할 수 없다. 그러므로 제안 프로토콜은 위장 공격에 기반한 스푸핑 공격이나 중간자 공격에도 안전하다.

표 2. 프라이버시 보호를 위한 RFID 인증 프로토콜의 안전성 비교
Table 2. Security comparison of the proposed protocol

Security attacks and features	Oh et al's protocol[5]	The proposed protocol
Spoofing Attacks	Partially	Yes
MITM Attacks	Partially	Yes
Replay Attacks	Yes	Yes
Tag Anonymity	Yes	Yes
Location Tracking	Partially	Yes
Physical Attacks	No	Yes
Impersonation Attacks	Partially	Yes
Mutual authentication	Yes	Yes

Yes : The protocol resists the attacks or provides the functionality; No : The protocol does not resist the attacks or provide the functionality; Partially: 'Yes' under the condition that the network-wide key K has not been exposed to an attacker.

6.4 태그 익명성과 위치 추적 방지

태그 익명성이란 태그 ID가 공격자에게 노출되지 않아야 함을 의미한다. 제안 프로토콜에서 태그는 자신의 ID 대신 동적 ID를 사용한다. 다음 통신 세션을 위한 태그 Tg_i의 동적 ID $\mathcal{DID}_i$는 태그 Tg_i의 고유한 키 $K_i'(= K_i)$와 현재 통신 세션의 동적 ID DID_i를 연접한 값을 해쉬 연산하여 생성된다. 일방향 해쉬 함수의 특성에 따라 공격자는 $\mathcal{DID}_i$로부터 DID_i나 K_i', 또는 ID_i를 유도할 수 없다. 또한 태그의 동적 ID는 매 통신 세션 마다 변경되고 서버와 해당 태그만 그 값을 공유하기 때문에 제안 프로토콜은 공격자의 태그 위치 추적에 안전하다.

6.5 재전송 공격

제안 프로토콜에서 공격자가 리더와 태그 Tg_i 사

이에 전송되는 메시지 {Query, V}, {DID_i, C_i}, 또는 {C_j}를 도청하였다가 다른 통신 세션에 다시 전송하더라도 리더 또는 태그 Tg_i처럼 위장하거나 인증에 필요한 정보를 얻을 수 없다. 메시지 {DID_i, C_i}와 {C_j}는 태그 Tg_i와 서버만이 알고 있는 키 K_i를 이용하여 암호화된 암호문일 뿐 아니라 암호화되기 전의 평문이 매 통신 세션마다 새로 생성되는 랜덤 넘버를 포함하고 있기 때문에 재전송 공격이 불가능하다.

Ⅶ. 제안 프로토콜의 효율성 분석

본 장에서는 제안 프로토콜의 효율성을 연산량과 메시지 전송량 측면에서 분석 및 비교하였다.

표 3은 제안 프로토콜과 Oh 등의 프로토콜[5]을 연산량 측면에서 분석한 결과를 나타낸 것이다. 표 3은 두 프로토콜에서 수행된 연산의 종류와 수행 횟수를 나타낸다. 우선 서버에서의 연산량은 제안 프로토콜이 $1S+1H$, Oh 등의 프로토콜이 $1S$이고, 리더에서의 연산량은 제안 프로토콜이 $1R+1E+1D+1H+2X$, Oh 등의 프로토콜이 $1R+1E+1D+1X$이다. 그러나 RFID 시스템에서 자원 제한적인 노드는 태그이기 때문에 우리는 서버나 리더보다 태그 상에서의 연산량에 더 집중할 필요가 있다. 태그에서의 연산량은 제안 프로토콜에서 $1E+1D+1X$이고, Oh 등의 프로토콜에서 $1R+1E+1D+1X$으로 제안 프로토콜의 연산량이 더 작다. 이것은 개선된 안전성을 감안한다면 연산량 측면에서 제안 프로토콜이 Oh 등의 프로토콜보다 더 효율적이라는 것을 의미한다.

메시지 전송량 측면에서 제안 프로토콜에서 리더와 태그 사이에 전송되는 메시지의 총 수는 3개로 Oh 등의 프로토콜에서의 메시지 수와 같다.

표 3. 프라이버시 보호를 위한 RFID 인증 프로토콜의 연산량 비교
Table 3. Computation cost comparison of the proposed protocol

Communication parties		Oh et al's protocol[5]	The proposed protocol
Tag	Tg_i	$1R+1E+1D+1X$	$1E+1D+1X$
Reader	Rdr_j	$1R+1E+1D+1X$	$1R+1E+1D+1H+2X$
Server	Svr	$1S$	$1S+1H$

R: Random number;
E: Symmetric encryption;
D: Symmetric decryption;
X: XOR operation; H: Hash operation;
S: Search

Ⅷ. 결 론

본 논문에서는 프라이버시 보호를 위하여 기존에 제안된 RFID 인증 프로토콜이 암호 해독(Cryptanalysis)이나 물리적 공격 등을 통하여 한 개의 태그로부터 비밀값이 노출되는 경우 다른 태그의 통신이나 전체 시스템의 안전성이 위협받을 수 있음을 보였다. 본 논문에서는 이러한 문제를 해결하기 위하여 서버가 각 태그를 위한 고유의 암호키와 동적 ID를 관리하는 프로토콜을 제안하였다. 제안 프로토콜은 RFID 시스템에서 예상되는 위장 공격, 스푸핑 공격, 중간자 공격, 재전송 공격에 안전하다. 또한 사용자의 프라이버시를 보호하기 위해서 태그의 익명성을 제공할 뿐 아니라 위치 추적이 불가능하다. 제안 프로토콜은 개선된 안전성에도 불구하고 태그의 연산량 측면에서 기존 프로토콜보다 더 효율적이다.

References

[1] R. S. Ahn, E. J. Yoon, K. D. Bu, and I. G. Nam, "Secure and efficient DB security and authentication scheme for RFID system," *J. KICS*, vol. 36, no. 4C, pp. 197-206, Nov. 2011.

[2] D. H. Jeon, H. M. Kim, H. J. Kwon, and S. J. Kim, "Hash-based mutual authentication protocol for RFID environment," *J. KICS*, vol. 35, no. 1B, pp. 42-52, Oct. 2010.

[3] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," *Security in Pervasive Computing,* Springer, vol. 3450, pp. 70-84, Boppard, Germany, 2005.

[4] J. S. Kim, J. K. Park, and Y. T. Shin, "RFID-Based automatic inspection system design and implementation for manufacturing and retail industry," *J. KICS*, vol. 39, no. 1C, pp. 97-105, Jan. 2014.

[5] S. Oh, C. Lee, T. Yun, K. Chung, and K. Ahn, "Improved authentication protocol for privacy protection in RFID systems," *J. KICS*,

vol. 38, no. 1, pp. 12-18, Jan. 2013.

[6] E. J. Yoon and K. Y. Yoo, "Patient authentication system for medical information security using RFID," *J. KICS*, vol. 35, no. 6B, pp. 962-969, Jun. 2010.

[7] W. Che, S. Kim, Y. Kim, T. Yun, K. Ahn, and K. Han, "Design of PUF-Based encryption processor and mutual authentication protocol for Low-Cost RFID authentication," *J. KICS*, vol. 39, no. 12B, pp. 831-841, Dec. 2014.

[8] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," *Security in Pervasive Computing,* Springer, pp. 201-212, Boppard, Germany, 2004.

[9] W. S. Bae, "Design of an authentication protocol for privacy protection in RFID systems," *J. Digital Policy and Management*, vol. 10, no. 3, pp. 155-160, Apr. 2012.

[10] K. H. Chung, K. Y. Kim, S. J. Oh, J. K. Lee, Y. S. Park, and K. S. Ahn, "A mutual authentication protocol using key change step by step for RFID systems," *J. KICS*, vol. 35, no. 3B, pp. 462-473, Mar. 2010.

[11] B. Toiruul, K. O. Lee, H. J. Lee, Y. H. Lee, and Y. Y. Park, "Mutual-authentication mechanism for RFID systems," *Mobile Ad-hoc and Sensor Networks,* Springer, pp. 449-460, Hong Kong, China, Dec. 2006.

[12] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. Areas in Commun.,* vol. 24, no. 2, pp. 381-394, 2006.

[13] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID systems and security and privacy implications," *Cryptographic Hardware and Embedded Systems-CHES 2002,* Springer, pp. 454-469, Redwood Shores, CA, USA, Aug. 2002.

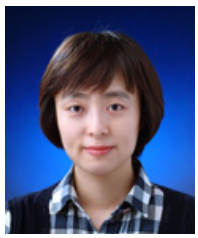
[14] J. Saito, J. C. Ryou, and K. Sakurai, "Enhancing privacy of universal re-encryption scheme for RFID tags," *Embedded and Ubiquitous Computing,* Springer, pp. 879-890, Aizu-Wakamatsu City, Japan, Aug. 2004.

[15] S. Kim, K. Lee, S. Kim, and D. Won, "Security analysis on anonymous mutual authentication protocol for RFID tag without back-end database and its improvement," *World Acad. Sci. Eng. Technol.*, vol. 59, pp. 460-464, Nov. 2009.

[16] K. Rhee, J. Kwak, W. S. Yi, C. Park, S. Park, H. Yang, S. Kim, and D. Won, "Efficient RFID authentication protocol for minimizing RFID tag computation," *Advances in Hybrid Inf. Technol.,* Springer, pp. 607-616, Jeju Island, Korea, Nov. 2006.

[17] M. Aigner and M. Feldhofer, "Secure symmetric authentication for RFID tags," *Telecommun. Mob. Comput.,* Graz, Austria, 2005.

김 지 예 (Jiye Kim)



1999년 2월 : 성균관대학교 정보공학과 학사

2007년 2월 : 이화여자대학교 컴퓨터교육학 석사

1999년~2013년 : (주)팬택 소프트웨어 개발 그룹

2013년 9월~현재 : 성균관대학교 전자전기컴퓨터공학과 박사과정

<관심분야> 암호이론, 보안 프로토콜, 무선 센서 네트워크 보안 등

원 동 호 (Dongho Won)

1976년 2월 : 성균관대학교 전자공학과 학사

1978년 2월 : 성균관대학교 전자공학과 석사

1988년 2월 : 성균관대학교 전자공학과 박사

1982년~2015년 : 성균관대학교 교수

2015년~현재 : 성균관대학교 행단석좌교수

<관심분야> 암호이론, 정보시스템 보안 등