논문 2009-46CI-1-1

RFID/USN 환경을 위한 개선된 인증 프로토콜

(Improved Authentication Protocol for RFID/USN Environment)

안 해 순*, 부 기 동**, 윤 은 준***, 남 인 길****

(Hae-Soon Ahn, Ki-Dong Bu, Eun-Jun Yoon, and In-Gil Nam)

요 약

최근 Shin과 Park은 RFID/USN 환경에서의 해쉬 함수와 배타적논리합(XOR) 연산을 이용한 인증 프로토콜을 제안하였다. 본 논문에서는 Shin과 Park이 제안한 인증 프로토콜이 스푸핑 공격, 위치 트래킹 공격, 태그 키 유출 공격에 취약하며 태그 익명성을 제공하지 않음을 증명하며, 공격들에 안전한 RFID/USN 환경을 위한 개선된 인증 프로토콜을 제안한다. 결론적으로 제안한 프로토콜은 기존의 방법과 비교하여 안정성뿐만 아니라 통신라운드 수 또한 줄여주어 통신 효율성도 보장 할 수 있다.

Abstract

Recently, Shin and Park proposed an authentication protocol using the hash function and the XOR operation in RFID/USN environment. However, Shin and Park's proposed authentication protocol is vulnerable to spoofing attack and location tracking attack and tag key exposure attack, and it does not provide tag anonymity. In this paper, we propose an improved authentication protocol for the RFID/USN environment that can withstand those attacks. The proposed authentication protocol provides more improved secrecy and communication efficiency because it decreases the communication rounds compared with the Shin and Park's protocol.

Keywords : RFID/USN, 인증, 프로토콜, 해쉬함수, 프라이버시

Ⅰ. 서 론

RFID(Radio Frequency IDentification) 기술은 USN(Ubiquitous Sensor Network) 기술과 더불어 유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경 실현을 위한 중요한 핵심 기술로 가장 주목을 받고 있는 기술이다[1~3]. RFID 시스템은 무선 주파수를 이용하여 물리적인 접촉 없이 태그(Tag)에 저장된 정보를 비접촉 방식으로 읽거나 정보를 기록할 수 있는 자동 인식(Automatic Identification) 시스템이다[1~3].

이러한 RFID 시스템의 장점은 기존의 바코드(Bar Code) 시스템이나 자기 인식 장치들이 지니고 있는 일회성 저장 문제를 해결하여 주어, 교통카드, 출입구 보안 및 출결 카드 분야를 포함한 상거래와 직접적인 관련이 있는 물류관리, 재고관리, 항만관리, 동물관리 등 물류 및 유통 분야 등 다양한 분야에 관리 자동화를 위해 활용되어 지고 있다[1~6].

RFID 시스템은 리더(Reader), 태그(Tag) 그리고 백-엔드 데이터베이스(Back-end Database)의 3가지 구성요소로 이루어 져있다. 리더와 백-엔드 데이터베이스의 연산 능력에 비해 RFID 태그는 연산 능력이 떨어지며, 객체를 유일하게 식별하기 위한 정보만을 가지며, 정보

* 학생회원, 대구대학교 대학원 컴퓨터정보공학과
(Dept. of Computer Information Engineering, Graduate School, Daegu University)
** 정회원, 경일대학교 컴퓨터공학부
(School of Computer Engineering, Kyungil University)
*** 정회원, 경북대학교 전자전기컴퓨터학부
(School of Electrical Engineering and Computer Science, Kyungpook National University)
**** 정회원-교신저자, 대구대학교 컴퓨터·IT공학부
(School of Computer & Information Technology, Daegu University)
접수일자: 2008년12월10일, 수정완료일: 2009년1월13일

노출, 위치 추적 등으로 인한 개인의 프라이버시(Privacy) 침해를 유발할 수 있는 문제점을 지니고 있다[1~19].

현재 RFID/USN 환경에서 발생할 수 있는 프라이버시 침해 문제를 해결하기 위해 지금까지 많은 연구자들에 의해 해쉬-락 기법, 확장된 해쉬-락 기법, 해쉬-기반 ID 변형 기법, 개선된 해쉬-기반 ID 변형 기법, 블로커 태그를 이용한 기법, 해쉬-체인 기법 등 다양한 RFID 인증 프로토콜(Authentication protocol)들이 최근까지 개발되어져 오고 있다[4~20].

하지만 현재까지 제안되어져 오고 있는 대부분의 RFID 인증 프로토콜들은 태그의 재사용이 불가능하거나, 태그의 위치추적으로 위치 트래킹 공격(Location tracking attack)이 쉬우며, 재전송 공격(Replay attack)이나 스푸핑 공격(Spoofing attack)에 취약하는 등 다양한 보안 취약점과 프라이버시 침해 문제들을 가짐을 많은 연구자들에 의해 발견되어 지고 있다[7~20].

2007년에 Shin과 Park은 유비쿼터스 환경을 실현하기 위한 기술 중의 하나인 RFID 시스템에서의 RFID 태그의 특성을 고려한 RFID 환경 및 USN(Ubiquitous sensor network) 환경을 위한 해쉬 함수와 배타적논리합(XOR) 연산을 이용한 SPRFID 인증 프로토콜을 제안하였다[14]. 그들은 제안한 SPRFID 인증 프로토콜의 안전성 분석을 통하여 재전송 공격, 스푸핑 공격, 위치 트래킹 공격, 태그 키 유출 공격(Key exposure attack) 등에 안전함을 주장하였다[14].

본 논문에서는 Shin과 Park이 제안한 SPRFID 인증 프로토콜이 그들의 주장과는 달리 여전히 스푸핑 공격, 위치 트래킹 공격, 태그 키 유출 공격에 취약하며 태그 익명성(Anonymity)을 제공하지 않음을 증명한다[17~18]. 더 나아가 위와 같은 공격들에 안전한 RFID/USN 환경을 위한 개선된 인증 프로토콜을 제안한다. 결론적으로 제안한 프로토콜은 기존의 방법과 비교하여 안정성뿐만 아니라 통신라운드 수 또한 줄여주어 통신 효율성도 보장 할 수 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 RFID 시스템과 일반적인 RFID 인증 프로토콜들이 만족해야 할 보안 요구사항에 관해 설명한다. Ⅲ장에서는 SPRFID 인증 프로토콜을 소개하며, Ⅳ장에서 SPRFID 인증 프로토콜의 보안 취약점들을 증명한다. Ⅴ장에서는 본 논문에서 제안한 개선된 RFID 인증 프로토콜을 기술하고, Ⅵ장과 Ⅶ장에서 각각 안전성과 효율성을 분석한다. 최종적으로 Ⅷ장에서 결론을 맺는다.

Ⅱ. 배경 지식

본 장에서는 RFID 시스템과 일반적인 RFID 인증 프로토콜들이 만족해야 할 보안 요구사항에 관해 설명한다.

1. RFID 시스템 환경

본 절에서는 RFID 시스템 환경에 관해 기술한다. 일반적으로 RFID 시스템은 다음과 같은 가정들 하에 운영된다.

(1) RFID 시스템은 그림 1과 같이 백-엔드 데이터베이스 서버, RFID 리더(Reader), RFID 태그(Tag)들의 3종류의 컴포넌트들로 구성되어 진다[1, 20~22].

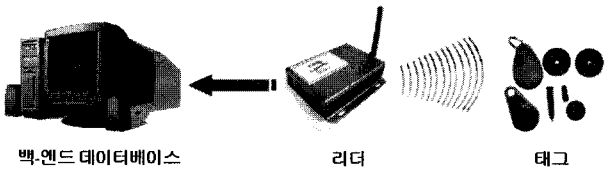


그림 1. RFID 시스템
Fig. 1. RFID system.

(2) 백-엔드 데이터베이스 서버는 각 태그를 위한 *ID*와 제품 정보 등 필요한 정보 집합을 관리하고 있다.

(3) 각 태그는 읽고 쓰기가 가능한 메모리를 내장하고 있다. 리더와 태그 사이의 채널은 안전하지 않으며 모든 통신 메시지들은 공격자에 의해 엿보기나 수정이 가능하다.

2. 보안 요구사항들[4~20]

본 절에서는 RFID 시스템 환경에서의 보안 요구사항들을 기술한다. 일반적으로 RFID 시스템에서 다음의 세가지 속성에 의해 프라이버시(Privacy)를 정의하고 있다.

(1) 태그 익명성(Tag anonymity): 태그의 *ID*는 평문 형태로 전송 되지 않아야 하며, 또한 태그와 리더 사이의 통신 채널 상으로부터 쉽게 계산되어지지 않아야만 된다.

(2) 위치 프라이버시(Location privacy): 태그와 리더 사이의 통신 메시지 내용으로부터 태그의 ID를 추적(Trace)할 수 없어야 한다. 만약 공격자(Attacker)가 임의의 통신 메시지 내용이 특정한 태그로부터 송신되어 졌음을 구분할 수 있다면 해당 공격자는 태그의 위치를 추적할 수 있게 된다.

또한, 다양한 보안 위협들로부터 안전하기 위해 RFID 시스템에서는 다음과 같은 공격들에 대해 견고하여야 한다.

(3) 재전송 공격(Replay attack): 공격자는 태그와 리더 사이의 모든 통신 메시지들을 도청할 수 있으며 더 나아가 해당 공격자가 도청한 메시지들의 재전송을 통하여 합법적인 태그 또는 리더로 위장하여 인증을 받을 수 있다.

(4) 스푸핑 공격(Spoofing attack): 일반적으로 태그와 리더 사이의 통신 채널은 안전하지 않은 공개 무선 채널이기 때문에, 공격자는 쉽게 송수신되는 모든 통신 메시지들을 엿볼 수 있다. 이에 공격자는 정당한 통신 당사자로 위장하여 태그와 리더간의 인증과정을 통과할 수 있다.

(5) 위치 트래킹 공격(Location tracking attack): 위치 트래킹 공격은 공격자가 태그의 위치변화를 감지함으로 인해 태그 소유자의 이동 경로를 파악하여 사용자의 프라이버시(privacy)를 침해하는 공격이다. 일반적으로 RFID 시스템에서의 위치 트래킹 공격은 동일한 태그로부터 나오는 응답들을 모두 수집하여, 그 응답이 가지고 있는 연관성을 파악하여 응답들에 대한 링크를 통해 공격이 이루어진다.

Ⅱ. SPRFID 인증 프로토콜

본 장에서는 Shin과 Park이 제안한 SPRFID 인증 프로토콜에 관해 설명한다[14]. 표 1은 본 논문에서 사용되어 지는 시스템 파라미터들을 보여준다.

SPRFID 인증 프로토콜에서 RFID 백-엔드 데이터베이스와 리더 간에 사전에 안전한 세션키 sk가 설정 되어 있음을 가정하며, 각 태그의 비밀 키 k는 백-엔드 데이터베이스에 등록되어 있음을 가정한다. 그림 2는 SPRFID 인증 프로토콜의 구성과 동작 과정을 보여주

표 1. 시스템 파라미터
Table 1. System parameters.

기호	의미
Tag	RFID 태그
$Reader$	RFID 리더
DB	백-엔드 데이터베이스
$query$	태그의 응답을 요청하는 리더의 요청
ID	태그에게 할당된 고유 정보
k	Tag와 DB간에 공유된 비밀 키
sk	$Reader$와 DB간에 공유된 비밀 세션 키
$E(\cdot)$	대칭키 암호 시스템(symmetric key cryptosystem)
$h(\cdot)$	안전한 일방향 해쉬 함수(secure one-way hash function)
$prng(\cdot)$	의사난수생성기(pseudo random number generator)
r	리더가 매 세션마다 생성하여 태그에게 전송하는 랜덤 값
t	태그가 매 세션마다 생성하여 리더에게 전송하는 랜덤 값
$\oplus$	배타적 논리합(XOR; eXclusive OR) 연산
$\|$	연접 연산(concatenation) 연산
$A \rightarrow B : X$	X가 A에서 B로 전송

며, 다음의 7단계를 거쳐 인증 과정이 이루어진다.

(1) 리더 → 태그: $query$
리더는 태그에게 질의인 $query$를 전송한다.

(2) 태그 → 리더: ID
리더로부터 $query$를 수신한 태그는 자신의 ID를 리더에게 전송한다.

(3) 리더 → 백-엔드 데이터베이스: $E_{sk}(ID)$
리더는 백-엔드 데이터베이스와 설정된 세션 키 sk를 사용하여 태그의 ID를 암호화하여 $E_{sk}(ID)$를 백-엔드 데이터베이스에게 전송한다.

(4) 백-엔드 데이터베이스: → 리더: $E_{sk}(k, ID)$
백-엔드 데이터베이스는 리더로부터 전송받은 $E_{sk}(ID)$을 세션 키 sk를 사용하여 복호화 한 후 ID 태그의 비밀 키 k를 세션 키 sk로 암호화하여

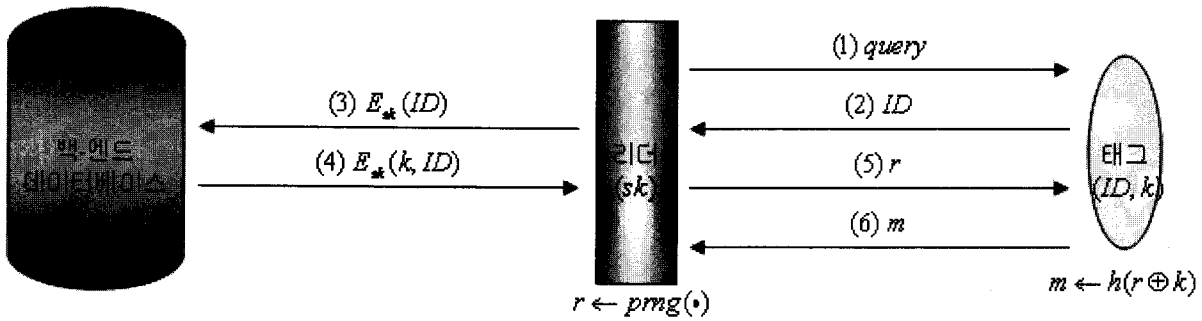


그림 2. SPRFID 인증 프로토콜
Fig. 2. SPRFID authentication protocol.

$E_{sk}(k, ID)$을 리더에게 전송한다.

(5) 리더 → 태그: r
리더는 백-엔드 데이터베이스로부터 수신한 $E_{sk}(k, ID)$을 복호화하여 태그의 비밀 키 k를 저장하고 태그에게 랜덤 값 r을 전송한다.

(6) 태그 → 리더: m
태그는 수신한 랜덤 값 r과 자신의 비밀 키 k를 이용하여 $m = h(r \oplus k)$을 계산하여 리더에게 전송한다.

(7) 리더는 $m' = h(r \oplus k)$을 계산하여 수신한 m과 동일한지를 비교한다. 만약 두 값이 같으면 태그를 인증하고, 다르면 인증을 중단한다.

III. SPRFID 인증 프로토콜의 취약점

본 장에서는 Shin과 Park이 제안한 SPRFID 인증 프로토콜이 스푸핑 공격, 위치 트래킹 공격, 태그 키 유출 공격에 취약하며 태그 익명성을 제공하지 않음을 증명한다.

1. 스푸핑 공격

SPRFID 인증 프로토콜에서 태그는 리더를 전혀 인증하지 않기 때문에 공격자가 리더로 위장하여 아래와 같은 과정을 통해 스푸핑 공격을 성공할 수 있다.

(1) 공격자 → 태그: $query$
공격자는 태그에게 $query$를 전송한다.

(2) 태그 → 공격자: ID
공격자로부터 $query$를 수신한 태그는 자신의 ID를 공격자에게 전송하게 된다.

(3) 공격자 → 태그: r^*
공격자는 백-엔드 데이터베이스와 인증 과정을 무시하고 랜덤 값 $r^* \leftarrow prng(\cdot)$를 생성하여 태그에게 전송한다. 물론 r^*는 이전 세션에서 도청한 r을 이용하여 재전송 공격을 수행하여도 된다.

(4) 태그 → 공격자: m^*
태그는 수신한 랜덤 값 r^*와 자신의 비밀 키 k를 이용하여 $m^* = h(r^* \oplus k)$을 계산하여 공격자에게 전송하게 된다.

(5) 공격자는 m^*를 수신한 후 세션을 종료한다.

위 단계 (4)에서 태그는 공격자가 합법적인 리더이며 백-엔드 데이터베이스로부터 올바른 자신의 비밀 키 k를 수신하여 소유하고 있는지 여부를 전혀 확인하지 않고 m^*를 최종 전송하게 된다. 따라서 공격자는 태그에게 합법적인 리더로 가정하여 쉽게 스푸핑 공격을 성공

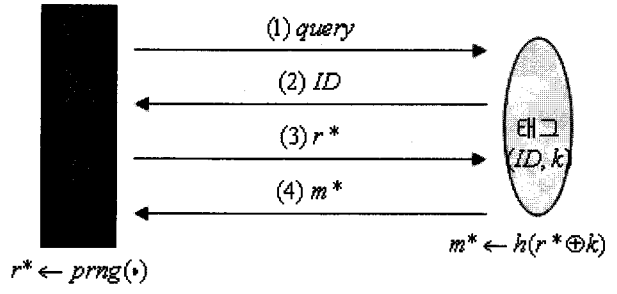


그림 3. 스푸핑 공격
Fig. 3. Spoofing attack.

할 수 있다. 그림 3은 SPRFID 인증 프로토콜에 대한 스푸핑 공격에 대한 예를 보여주고 있다.

2. 위치 트래킹 공격

SPRFID 인증 프로토콜에서 임의의 공격자가 이전 세션의 단계 (2)에서 태그가 전송한 ID를 도청하여 소유하고 있다고 가정하자. ID는 공개된 통신 채널을 통해 전송됨으로 공격자는 쉽게 획득할 수 있다. 그러면 해당 공격자는 임의의 세션에서 리더로 위장하여 다음과 같은 과정을 수행하여 위치 트래킹 공격을 성공할 수 있다.

(1) 공격자 → 임의의 태그들: $query$

공격자는 임의의 태그들에게 $query$를 브로드캐스팅(broadcasting)한다.

(2) 임의의 태그들 → 공격자: ID_i

공격자로부터 $query$ 수신한 임의의 태그들은 응답 메시지로 자신의 ID_i를 공격자에게 전송하게 될 것이다.

(3) 공격자는 임의의 태그들로부터 전송받은 ID_i를 이용하여 이전 세션에서 도청한 ID와 동일한 ID_i가 있는지를 아래와 같은 검증 연산을 수행하여 일치하는 ID_i 값을 검색한다.

```
For (i = 1 to n)
{
  If(이전에 도청한 ID == 수신한 ID_i)
  {
    print(위치 트래킹 공격 성공);
    return( Tag_i and ID_i );
  }
  Else print(해당 ID가 존재하지 않음);
}
```

만약 일치하는 ID_i 값이 검색되면 공격자는 그 일치하는 ID_i를 전송한 태그가 이전 세션에서 도청한 ID를 전송한 태그와 동일한 태그임을 알게 되어 태그의 위치변화를 쉽게 감지할 수 있다. 이로 인해 태그 소유자의 이동 경로를 쉽게 파악하여 사용자의 프라이버시(privacy)를 침해할 수 있음으로 SPRFID 인증 프로토콜은 위치 트래킹 공격에 취약함을 알 수 있다. 그림 4는 SPRFID 인증 프로토콜에 대한 위치 트래킹 공격에 대한 예를 보여주고 있다.

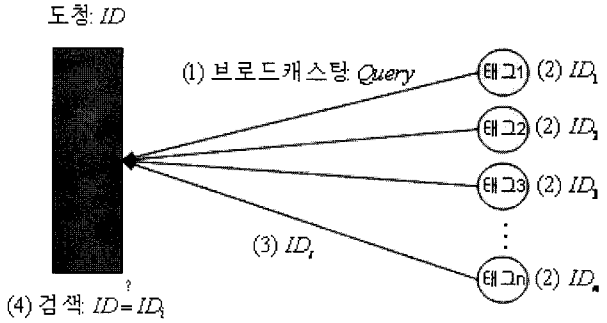


그림 4. 위치 트래킹 공격
Fig. 4. Location tracking attack.

3. 태그 키 유출 공격[18]

SPRFID 인증 프로토콜의 단계 (3)에서 임의의 태그에 대한 비밀 키 k를 획득하기 위한 악의적인 목적을 가진 리더가 존재한다고 가정할 때, 해당 리더는 아래와 같은 태그 키 유출 공격을 수행하여 간단히 태그의 비밀 키 k를 획득한 후 해당 태그로의 스푸핑 공격 등을 수행 할 수 있다.

악의적인 리더는 공개된 통신 채널로부터 임의의 태그들에 대한 ID_i 값들을 획득한다. 여기에서 $1 \le i \le n$. 악의적인 리더는 아래 (1)~(3)의 과정을 모든 태그들에 대해 수행하여 ID_i와 k_i 쌍을 획득한다.

(1) 악의적인 리더 → 데이터베이스: $E_{sk}(ID_i)$

악의적인 리더는 백-엔드 데이터베이스와 설정된 세션 키 sk를 사용하여 수집한 태그들의 ID_i를 암호화하여 $E_{sk}(ID_i)$를 백-엔드 데이터베이스에게 전송한다.

(2) 백-엔드 데이터베이스 → 공격자: $E_{sk}(k_i, ID_i)$

백-엔드 데이터베이스는 악의적인 리더로부터 전송받은 $E_{sk}(ID_i)$을 세션 키 sk를 사용하여 복호화 한 후 ID_i 태그의 비밀 키 k를 세션 키 sk로 암호화하여 $E_{sk}(k_i, ID_i)$을 악의적인 리더에게 전송하게 된다.

(3) 악의적인 리더는 백-엔드 데이터베이스로부터 수신한 $E_{sk}(k_i, ID_i)$을 복호화하여 태그의 비밀 키인 k_i를 획득한다.

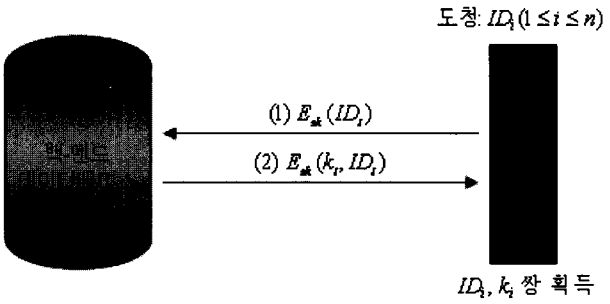


그림 5 태그 키 유출 공격
Fig. 5. Tag key exposure attack.

결론적으로 악의적인 리더는 ID_i와 k_i 쌍을 이용하여 자유롭게 태그로 위장하여 스푸핑 공격 등을 수행할 수 있다. 따라서 SPRIFD 인증 프로토콜은 태그 키 유출 공격에 취약하다. 그림 5는 SPRFID 인증 프로토콜에 대한 태그 키 유출 공격에 대한 예를 보여주고 있다.

4. 태그 익명성 문제

태그 익명성(Tag anonymity)을 제공하기 위해서는 태그와 리더의 통신에서 해당 태그에게 할당된 고유한 식별자인 ID가 노출되지 않아야한다. 즉, 태그의 정보는 데이터베이스와 태그만이 식별할 수 있는 형태로 전송되어야 한다. 하지만 SPRFID 인증 프로토콜의 단계 (2)에서 태그가 전송한 ID 자체가 해당 태그에게 할당된 고유한 식별자임을 쉽게 알 수 있다. 임의의 공격자는 공개된 통신 채널을 통해 ID를 쉽게 획득할 수 있음으로 SPRFID 인증 프로토콜은 태그 익명성을 제공하지 않음을 알 수 있다.

Ⅳ. 제안한 RFID 인증 프로토콜

본 장에서는 SPRFID 인증 프로토콜에서의 스푸핑 공격 및 위치 트래킹 공격에 대한 취약점을 제거하고 태그 익명성을 제공하는 개선된 RFID/USN 환경에 적합한 인증 프로토콜을 제안한다. 제안한 프로토콜에서는 스푸핑 공격 및 위치 트래킹 공격에 안전하기 위해 태그 측에서도 리더와 마찬가지로 임의의 랜덤 값을 생성하도록 설계하였다.

SPRFID 인증 프로토콜과 마찬가지로 RFID 백-엔드 데이터베이스와 리더 간에 사전에 안전한 세션키 sk가 설정 되어 있음을 가정하며, 각 태그의 비밀 키 k는 백-엔드 데이터베이스에 등록되어 있음을 가정한다. 그림 6은 제안한 RFID 인증 프로토콜의 구성과 동작 과정을 보여주며, 다음의 5단계를 거쳐 인증 과정이 이루어진다.

(1) 리더 → 태그: $query$, r
리더는 랜덤 값 r을 생성한 후, 태그에게 $query$와 함께 r을 전송한다.

(2) 태그 → 리더: m, t
태그는 랜덤 값 t를 생성한 후, 리더로부터 수신한 r과 자신의 ID 및 비밀 키 k을 이용하여 랜덤 해쉬 값 $m = h(ID||k||r||t)$을 계산한 후, m과 t를 리더에게 전송한다.

(3) 리더 → 백-엔드 데이터베이스: $E_{sk}(m,t,r)$
리더는 백-엔드 데이터베이스와 설정된 세션 키 sk를 사용하여 태그로부터 수신한 m과 t 그리고 자신이 생성한 r을 암호화하여 $E_{sk}(m,t,r)$를 백-엔드 데이터베이스에게 전송한다.

(4) 백-엔드 데이터베이스: → 리더: $E_{sk}(r,info)$

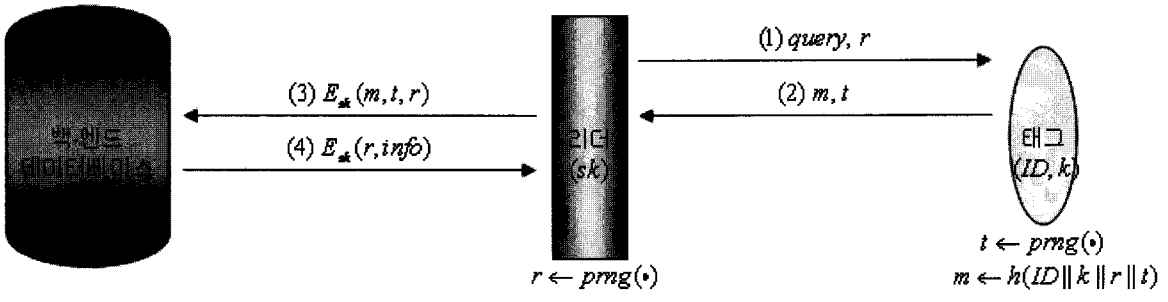


그림 6. 제안한 RFID 인증 프로토콜
Fig. 6. Proposed RFID authentication protocol.

백-엔드 데이터베이스는 리더로부터 전송받은 $E_{sk}(m,t,r)$을 세션 키 sk를 사용하여 복호화 한 후, $m' = h(ID||k||r||t)$을 계산하여 자신의 데이터베이스 내에 저장하고 있는 모든 ID와 k 쌍을 이용하여 리더로부터 수신한 m 값과 아래와 같은 검증 연산으로 비교하여 일치하는 ID와 k 쌍을 검색한다.

계산된 m' ?= 수신한 m

만약 일치하는 값이 검색되지 않으면, 오류(error) 메시지를 리더에게 전송하고, 일치하는 값이 검색되면 태그를 인증하고 태그에 대한 상품 관련정보(related information)인 $info$를 리더가 생성한 랜덤 값 r과 함께 세션 키 sk로 암호화하여 $E_{sk}(r,info)$을 리더에게 전송한다.

(5) 리더는 백-엔드 데이터베이스로부터 수신한 값이 오류일 경우, 태그와의 통신을 중단하고, 정상적인 인증이 되었을 경우에서는 백-엔드 데이터베이스로부터 수신한 $E_{sk}(r,info)$을 복호화하여 r과 $info$를 얻는다. 상호인증을 위해 복호된 r이 자신이 생성한 랜덤 값 r과 동일한지를 검증한다. 만약 동일한 r이 맞으면, 리더는 태그에 관한 상품 관련정보인 $info$를 이용하여 상품에 대한 요금부과와 같은 원하는 작업을 수행한다.

V. 안전성 분석

본 장에서는 제안한 RFID 인증 프로토콜에 대한 보안성 분석을 한다. 먼저, 제안한 인증 프로토콜의 안전성 분석을 위해 필요한 중요한 보안 항목을 다음과 같이 정의한다[23~24].

[정의 1]. 강력한 비밀 키(k와 sk)는 높은 엔트로피(entropy)를 가지는 값으로써 다항식 시간(polynomial time) 내에 추측되어 질 수 없다.

[정의 2]. 안전한 일방향 해쉬 함수(secure one-way hash function) $y = h(x)$에서, 주어진 x를 이용하여 y를 계산하는 것은 쉽지만, 주어진 y를 이용하여 x를 계산하는 것은 어렵다.

위의 [정의 1]과 [정의 2]를 기반으로 제안한 프로토콜은 다음과 같이 재전송 공격, 스푸핑 공격, 위치 트래킹 공격, 태그 키 유출 공격에 안전하며 태그 익명성을 제공한다.

1. 재전송 공격(Replay attack)

제안한 프로토콜의 임의의 세션에서 공격자가 리더와 태그 사이에서 전송되는 정보를 모두 도청한 후, 다음 세션에서 정당한 리더나 태그로 위장을 시도하는 재전송 공격을 수행한다고 가정하자. 제안한 프로토콜에서는 매 세션마다 리더가 생성하는 새로운 랜덤 값 r과 태그가 생성하는 새로운 랜덤 값 t를 이용하여 백-엔드 데이터베이스에 의해 인증을 수행하기 때문에, 과거에 공격자에 의해 재전송된 랜덤 값들은 백-엔드 데이터베이스의 인증 과정 중에 쉽게 검출된다. 즉, 이전 세션의 랜덤 값을 알고 있는 공격자라 하더라고 새로운 세션에서의 랜덤 값을 알지 못하면 리더에게 정당한 태그인 것처럼 위장하여 속이는 것은 불가능하다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

2. 스푸핑 공격(Spoofing attack)

제안한 프로토콜에서 공격자가 백-엔드 데이터베이스와 태그 간에 공유된 비밀 키인 k를 얻을 수 있으면, 리더 또는 태그로의 스푸핑 공격을 성공할 수 있다. 하지만 제안한 프로토콜에서 공개 통신 채널 상으로 전송되는 정보들인 $\{m, t, r\}$을 이용하여, 공격자는 백-엔드 데이터베이스와 태그 내에 각각 안전하게 저장하고 있는 비밀 키인 k를 직접적으로 얻을 수 있는 방법이 없다. 또한 송수신되는 통신 메시지 $m = h(ID||k||r||t)$ 내의 비밀 키인 k는 태그의 ID 및 랜덤 값 t와 r 그리고 안전한 일방향 해쉬 함수에 의해 보호되어져 있다. 따라서 제안한 프로토콜은 스푸핑 공격들에 대해 안전하다.

3. 위치 트래킹 공격(Location tracking attack)

제안한 프로토콜에서는 SPRFID 인증 프로토콜과 달리 태그 측에서도 랜덤 값 r을 생성하여 인증에 이용한다. 즉, 태그의 비밀 키 k와 ID 및 두 개의 랜덤 값 t와 r에 의해 계산된 $m = h(ID||k||r||t)$은 매 세션마다 변경되기에 공격자는 현재 세션에서 태그의 응답이 과거 세션에 도청한 응답과 동일한지를 비교할 수 없다. 즉, 매 세션마다 서로 다른 랜덤 값 t와 r을 생성함으

로, 매 세션마다 서로 다른 두 개의 응답이 동일한 태그로부터 송신된 것인지 여부를 쉽게 구별할 수 없게 된다. 이로 인해, 공격자는 태그의 이동경로를 쉽게 추적을 할 수 없을 뿐만 아니라, 특정한 태그를 식별할 수 없기에 위치 트래킹 공격을 수행 할 수 없다. 결론적으로 제안한 프로토콜은 사용자의 프라이버시 보호할 수 있다. 따라서 제안한 프로토콜은 위치 트래킹 공격에 안전하다.

4. 태그 키 유출 공격(Tag key exposure attack)

제안한 프로토콜에서는 SPRFID 인증 프로토콜과는 달리 리더는 백-엔드 데이터베이스로부터 수신한 $E_{sk}(r,info)$로부터 태그의 비밀 키 k에 관한 어떠한 정보도 얻을 수 없다. 따라서 제안한 프로토콜은 SPRFID 인증 프로토콜에 취약했던 태그 키 유출 공격에 안전하다.

5. 태그 익명성(Tag anonymity)

제안한 프로토콜에서 리더는 임의의 랜덤 값 r을 생성하여 태그에게 전송하고, 태그는 수신한 r과 자신이 생성한 임의의 랜덤 값 t 그리고 태그의 비밀 키인 k를 이용하여 안전한 일방향 해쉬 함수의 도움으로 $m = h(ID||k||r||t)$을 계산한 후 리더에게 전송한다. 이로 인해, $m = h(ID||k||r||t)$을 도청한 공격자는 태그의 비밀 키인 k를 알지 않고서는 태그의 ID를 추측할 수 없을 뿐만 아니라 일방향 해쉬 함수의 성질에 의해 m으로부터 태그의 정보를 직접적으로 얻을 수 없다. 따라서 제안한 프로토콜은 태그 익명성을 제공한다.

표 2는 제안한 프로토콜과 SPRFID 인증 프로토콜과의 안전성을 비교 및 분석한 표이다. 표 2와 같이 제안한 프로토콜은 SPRFID 인증 프로토콜과 비교하여 스푸핑 공격, 위치 트래킹 공격 그리고 태그 키 유출 공격 등에 안전할 뿐 만 아니라 태그 익명성도 보장하여 줌으로써 보다 강한 보안성을 제공함을 알 수 있다.

표 2. 보안성 비교
Table 2. Comparison of security.

프로토콜 / 공격유형	SPRFID 인증 프로토콜[14]	제안한 RFID 인증 프로토콜
재전송 공격	안전하지 않음	안전함
스푸핑 공격	안전하지 않음	안전함
위치 트래킹 공격	안전하지 않음	안전함
태그 키 유출 공격	안전하지 않음	안전함
태그 익명성	제공 안함	제공함

VI. 효율성 분석

본 장에서는 제안한 인증 프로토콜과 SPRFID 인증 프로토콜과의 효율성 측면에서 비교 및 분석한다. 표 3은 제안한 프로토콜과 SPRFID 인증 프로토콜과의 효율성을 비교 및 분석한 표이다.

제안된 인증 프로토콜은 SPRFID 인증 프로토콜과 비교하여 태그 측에서 하나의 랜덤 값 생성이 요구되며, 백-엔드 데이터베이스 측에서 n번의 해쉬 연산이 요구된다. 이러한 추가적인 연산은 SPRFID 인증 프로토콜이 가지는 4가지 보안 취약점들을 제거하기 위해 필요한 연산들이며, 태그와 달리 데이터베이스는 높은 시스템 성능과 연산 능력을 가짐으로 n번의 해쉬 연산을 통한 태그 인증은 빠른 시간 내에 이루어 질 수 있다. 더 나아가, 제안한 인증 프로토콜은 6번의 통신 라운드를 수행하는 SPRFID 인증 프로토콜과 달리 4번의 통신 라운드만을 수행하여 표 3과 같은 모든 보안 속성들을 만족할 수 있음으로, SPRFID 인증 프로토콜과 비교하여 높은 통신 효율성을 보장함을 알 수 있다. 결론적으로 제안된 인증 프로토콜은 강화된 보안성을 제공하면서 보다 높은 통신 효율성을 제공함을 알 수 있다.

표 3. 효율성 비교
Table 3. Comparison of efficiency.

프로토콜 / 비교요소	SPRFID 인증 프로토콜[14]			제안한 RFID 인증 프로토콜		
	DB	리더	태그	DB	리더	태그
랜덤 값	0	1	0	0	1	1
대칭키 암호 연산	2	2	0	2	2	0
해쉬 연산	0	1	1	n	1	1
XOR 연산	0	1	1	0	0	0
통신 라운드 수	6			4		

n : 백-엔드 데이터베이스에 저장된 최대 태그수

Ⅶ. 결 론

본 논문에서는, 최근 Shin과 Park이 제안한 RFID/USN 환경에서의 해쉬 함수와 배타적논리합(XOR) 연산을 이용한 SPRFID 인증 프로토콜이 그들의 주장과는 달리 여전히 스푸핑 공격, 위치 트래킹 공격, 태그 키 유출 공격에 취약하며 태그 익명성을 제공하지 않음을 증명하였다. 또한 위와 같은 보안 취약점들을 제거하기 위해 공격들에 안전한 개선된 RFID/USN 환경을 위한 인증 프로토콜을 제안하였다. 결론적으로 제안한 RFID 인증 프로토콜이 SPRFID 인증 프로토콜과 비교하여 안정성뿐만 아니라 통신라운드 수 또한 줄여주어 통신 효율성도 보장 할 수 있음을 증명하였다. 향후 연구로는 전방향 보안성을 고려한 RFID 상호 인증 프로토콜 개발을 통한 실용적인 RFID 시스템 개발에 목표를 둔다.

참 고 문 헌

[1] F. Klaus, "RFID handbook," Second Edition, Jone Willey & Sons, 2003.

[2] S. A. Weis, "Security an privacy in radio-frequency identification devices," MS Thesis. MIT. May, 2003.

[3] 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 2003, LNCS 2802, pp. 201-212, Springer-Verlag Heidelberg, 2004.

[4] S. E. Sarma, S. A. Weis, D. W. Engels. "RFID systems, security & privacy implications," White Paper MIT-AUTOID-WH_014, MIT AUTO-ID CENTER, 2002.

[5] A. Juels and R. Pappu, "Squealing euros: privacy protection in RFID-enabled banknotes," In proceedings of Financial Cryptography-FC'03, Vol. 2742 LNCS, pp. 103-121, Springer-Verlag, 2003.

[6] A. Juels, R. L. Rivest, M Szydlo "The blocker tag: selective blocking of RFID tags for consumer privacy," In Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103-111, 2003.

[7] S. Junichiro, H. Jae-Cheol and S. Kouichi, "Enhancing privacy of universal re-encryption scheme for RFID tags," EUC 2004, Vol. 3207 LNCS, pp. 879-890, Springer-Verlag, 2004.

[8] S. A. Weis, S. Sarma, R. Rivest, D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212, Springer-Verlag, 2004.

[9] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain based forward-secure privacy protection scheme for low-cost RFID," Proceedings of the SCIS 2004, pp. 719-724, 2004.

[10] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, "분산 데이타베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜," 한국정보처리학회 논문지C, 제12-C권, 제03호, pp. 309-316, 2005.

[11] 양형규, 안영화, "유비쿼터스 컴퓨팅 환경에 적합한 RFID 인증 프로토콜에 관한 연구," 전자공학회 논문지, 제42권, 제CI-1호, pp. 45-50, 2005.

[12 최은영, 최동희, 임종인, 이동훈, "저가형 RFID 시스템을 위한 효율적인 인증 프로토콜," 정보보호학회논문지, 제15권, 제05호, pp. 59-71, 2005.

[13] 이영진, 정윤수, 서동일, 이상호, "부분ID를 이용한 읽기전용 RFID태그 인증프로토콜," 한국정보처리학회 논문지 C, 제13-C권, 제05호, pp. 595-600, 2006.10.

[14] 신진섭, 박영호, "RFID/USN에서의 EXOR과 해쉬함수를 이용한 인증 프로토콜," 한국산업정보학회 논문지, 제12권, 제02호, pp. 24-29, 2007.6.

[15] 김대중, 전문석, "일회성 난수를 이용한 안전한 RFID 상호인증 프로토콜 설계," 정보과학회논문지, 정보통신, 제35권, 제03호, pp. 243-250, 2008.

[16] 강수영, 박종혁, 이덕규, "유비쿼터스 환경에서의 RFID 보안 기술 및 산업 동향에 관한 고찰," 보안공학연구논문지, Vol. 5, No. 2, pp. 53-68, 2008.5.

[17] 김현석, 김주배, 한근희, 최진영 "정형검증을 통한 RFID 보안프로토콜 분석 및 구현," 정보과학회논문지, 시스템 및 이론, 제35권, 제07호, pp. 332-339, 2008.8.

[18] 김경신, 김세일, 천지영, 이동훈, "경량 RFID 시스템에서의 안전한 상호 인증 기법," 한국정보과학회 가을 학술발표논문집, Vol. 35, No. 2(D), pp. 29-34, 2008.10.

[19] 강부중, 임을규, "RFID 시스템을 위한 상호 인증 프로토콜," 보안공학연구논문지, Vol. 5, No. 4, pp. 13-22, 2008.11.

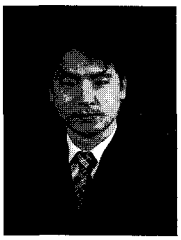
[20] 김진목, 유황빈, "유비쿼터스 환경에서 Pre-Distribution을 기반으로 한 안전한 RFID 시스템," 전자공학회논문지, 제42권, 제CI-6호, pp. 29-36, 2005.

[21] 오선문, 강대성, "NMF와 LDA 혼합 특징추출을 이용한 해마 학습기반 RFID 생체 인증 시스템에

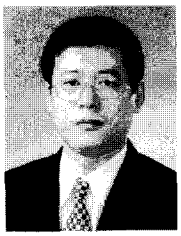
관한 연구," 전자공학회논문지, 제43권, 제SP-4호, pp. 46-54, 2006.
[22] 박인정, 현택영, "RFID를 이용한 작업관리 시스템," 전자공학회논문지, 제44권, 제CI-2호, pp. 31-36, 2007.
[23] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," CRC Press, New York, 1997.
[24] B. Schneier, "Applied cryptography protocols," Algorithms and Source Code in C, 2nd edn. John Wiley, Chichester, 1995.

저 자 소 개

안 해 순(학생회원)
1996년 경일대학교 컴퓨터공학과 (공학사)
2001년 경일대학교 컴퓨터공학과 (공학석사)
2009년 대구대학교 컴퓨터정보공학과 (박사수료)
2004년~2008년 경일대학교 컴퓨터공학부 전임강사
2008년~현재 대구대학교 교양교직부 컴퓨터과정 초빙교수
<주관심분야: 데이터베이스, 정보보안, 정보검색, 모바일 GIS, 데이터베이스 보안, RFID 보안>



윤 은 준(정회원)
1995년 경일대학교 졸업 (공학사)
2003년 경일대학교 컴퓨터공학과 (공학석사)
2007년 경북대학교 컴퓨터공학과 (공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2009년~현재 경북대학교 전자전기컴퓨터학부 연구교수
2007년~현재 보안공학연구지원센터 보안공학논문지 편집위원
<주관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜>



부 기 동(정회원)
1984년 경북대학교 전자공학과 (공학사)
1988년 경북대학교 전자공학과 (공학석사)
1996년 경북대학교 전자공학과 (공학박사)
1983년~1985년 포항종합제철 시스템개발실
2001년~2002년 일본 게이오대학 방문교수
1988년~현재 경일대학교 컴퓨터공학부 교수
<주관심분야: 데이터베이스, GIS, 시멘틱 웹, 데이터베이스 보안, RFID 보안>

남 인 길(정회원)
1978년 경북대학교 전자공학과 (공학사)
1981년 영남대학교 전자공학과 (공학석사)
1992년 경북대학교 전자공학과 (공학박사)
1978년~1981년 대구은행 전산부
1980년~1990년 경북산업대학 부교수
1990년~현재 대구대학교 컴퓨터·IT공학부 교수
<주관심분야: 데이터베이스, 데이터마이닝, 데이터베이스 보안, RFID 보안>