情報保護學會論文誌
第17卷 第 5號, 2007. 10

비밀정보 동기화에 기반한 Strong RFID 인증 프로토콜*

하 재 철,[1†] 김 환 구,[1‡] 하 정 훈,[2] 박 제 훈,[2] 문 상 재[2]
[1]호서대학교, [2]경북대학교

A Strong RFID Authentication Protocol Based on Synchronized Secret Information*

JaeCheol Ha,[1†] HwanKoo Kim,[1‡] JungHoon Ha,[2] JeaHoon Park,[2] SangJae Moon[2]
[1]Hoseo University, [2]Kyungpook National University

요 약

최근 Lee 등에 의해 비밀 정보 동기화에 기반한 RFID 인증 프로토콜이 제안되었다[8]. 본 논문에서는 이 프로토콜이 공격자가 악의적인 랜덤 수를 전송함으로써 합법적인 태그로 리더를 속일 수 있는 스푸핑 공격(spoofing attack)에 취약함을 보이고자 한다. 또한 논문에서는 위장공격을 방어할 뿐만 아니라 RFID시스템에서 최근 이슈화 되고 있는 backward untraceability는 물론 forward untraceability를 만족하는 인증 프로토콜을 제안하고자 한다. 특히 제안하는 프로토콜 II는 데이터베이스에서 동기화된 태그를 인증하는데 필요한 연산량을 3회의 해쉬 연산(비동기화된 태그의 경우 평균 $\lceil m/2 \rceil \cdot 2+3$번, m은 태그 수)으로 줄일 수 있어 대형 RFID 시스템에 적합하다.

ABSTRACT

Lee et al. recently proposed an RFID mutual authentication scheme based on synchronized secret information. However, we found that their protocol is vulnerable to a spoofing attack in which an adversary can impersonate a legal tag to the reader by sending a malicious random number. To remedy this vulnerability, we propose two RFID authentication protocols which are secure against all possible threats including backward and forward traceability. Furthermore, one of the two proposed protocols requires only three hash operations(but, $\lceil m/2 \rceil \cdot 2+3$ operations in resynchronization state, m is the number of tags) in the database to authenticate a tag, hence it is well suitable for large scale RFID systems.

Keywords : *RFID System, Authentication protocol, Indistinguishability, Backward untraceability, Forward unraceability*

Ⅰ. 서 론

RFID(Radio Frequency Identification) 시스템은 태그와 리더(Reader) 그리고 데이터베이스로 구성되며 리더와 태그간의 무선 통신을 통한 비접촉식 자동식별 기술로서 빠른 식별 능력, 소형화 등의 많은 장점을 가

접수일: 2007년 7월 24일; 채택일: 2007년 8월 13일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음. (IITA-2007-C1090-0701-0026).
† 주저자, jcha@hoseo.edu
‡ 교신저자, hkkim@hoseo.edu

지고 있다. 이와 같은 장점으로 바코드를 대체할 수단으로 인식되었고, 물류망 관리, 재고 관리, 쇼핑 센터 등 산업 전반에 걸쳐 현재 이용되고 있다[1].

그러나 태그와 리더간의 무선 통신으로 인해 태그의 정보 노출의 위협이 있으며, 악의적인 공격자는 도청, 스푸핑(spoofing) 공격, 재생(replay) 공격, 비동기(desynchronization) 공격 등을 통해 태그 소유자의 프라이버시를 침해하고 소유자의 위치를 추적할 수 있게 되었다.

RFID 시스템에서 태그와 리더간의 안전한 통신을 위한 다양한 인증 방법들이 제안되었다[2-5]. 기존의 방법들은 해쉬 함수를 이용하거나 재암호화 하거나 혹은 XOR과 같은 간단한 함수를 사용하는 것들 이었다[6-9]. 이 중에서 해쉬 함수에 기반한 방법들이 많이 제안되었으며 지금도 태그나 데이터베이스의 계산 부하 및 저장 공간을 최소화하기 위한 연구들이 진행 중에 있다. 특히 분산 환경을 고려한 RFID 시스템이 제안되기도 하였지만 대부분의 프로토콜이 고정 ID를 사용하게 되는 조건이 데이터베이스에서 연산량이 많아지는 결과를 초래하거나 일부 보안 조건을 만족하지 못하는 경우도 있었다[4, 10-11].

기존에 제안된 인증 시스템 중에서 Lee 등은 비밀 정보를 동기화시켜 인증을 수행하는 방법을 제안하였다[8]. 이 인증 방법에서 저자들은 완전한 추적 불가능(untraceability)을 제공하기 위해 태그의 indistinguishability와 forward security(backward untraceability)를 정의하였고 이를 만족하는 프로토콜을 제안하였다. 그러나 본 논문에서 이 프로토콜이 공격자가 악의적인 랜덤수를 전송함으로써 합법적인 태그로 리더를 속일 수 있는 스푸핑 공격(spoofing attack)에 취약함을 보이고자 한다. 나아가 본 논문에서는 위장 공격을 비롯한 현재 제시된 대부분의 공격을 방어할 뿐만 아니라 backward untraceability의 대칭 개념인 forward untraceability를 만족하는 프로토콜을 제안하고자 한다. 특히 제안 프로토콜 Ⅱ는 이전 세션에서 정상적인 상호 인증이 수행된 경우에는 다음 세션에서 데이터베이스에서 검색 시간을 크게 줄일 수 있어 태그의 수가 많은 대형 RFID 시스템에 유용하다.

Ⅱ. 비밀정보 동기화에 기반한 RFID 인증

2.1. 용어 및 표기

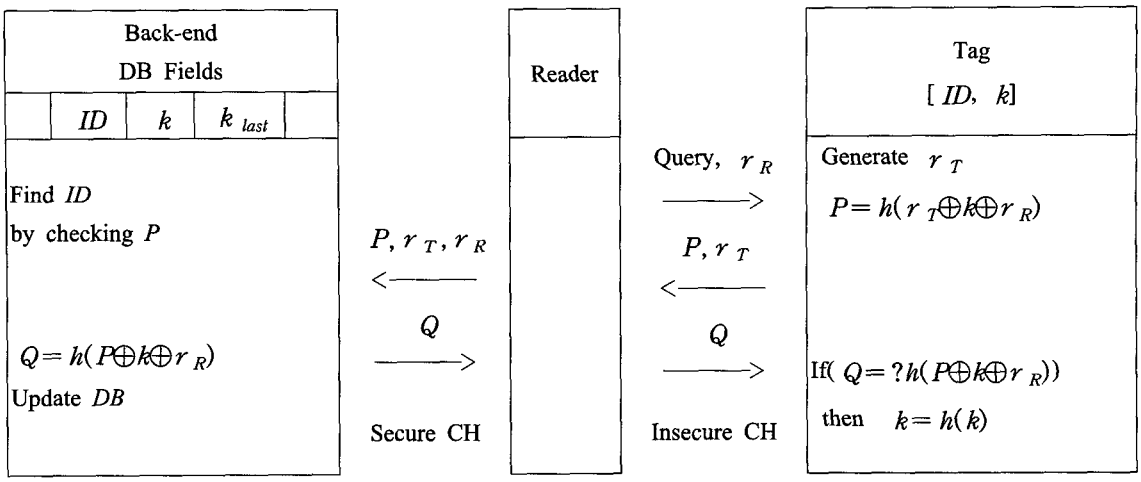
Lee 등이 제안한 비밀정보 동기화에 기반한 인증 프로토콜과 본 논문에서 제안하는 프로토콜에서 사용될 용어 및 표기는 다음과 같다.

- T : 태그
- R : 리더
- B : back-end 서버, 태그에 대한 DB 저장
- $h(\ )$: 해쉬 함수
- ID : EPC(Electronic Product Code)와 같은 태그의 고유 ID
- k : T와 B간의 동기화된 비밀정보, 비밀 키라고도 표현함
- k_{last} : T와 B간에 이전 세션에서 사용된 공통 비밀정보
- k_{next} : T와 B간에 다음 세션에서 사용될 갱신된 비밀 정보
- r_R : 리더가 발생하는 랜덤수
- r_T : 태그가 발생하는 랜덤수
- $L(Q)$, $R(Q)$: 정보 Q의 왼쪽 절반 혹은 오른쪽 절반
- $SYNC$: 상호 인증이 정상적으로 종료되었는지 나타내는 1비트 정보
- $\oplus$: 비트 XOR
- $\|$: 연접(concatenation)

2.2. Lee 등의 RFID 인증 방식

다음은 Lee 등이 제안한 비밀정보 동기화에 기반한 인증 프로토콜의 절차이며 이를 도식화 한 것이 [그림 1]이다[8]. 데이터베이스와 태그는 사전에 비밀정보 k를 공유하고 있다. 그리고 데이터베이스는 각 태그들의 비밀 정보를 저장하는 k 필드를 가지고 있고 이전 세션의 비밀 정보를 저장하는 k_{last} 필드를 가지고 있다.

- 1단계 : 리더는 질의(Query)와 랜덤수 r_R을 태그에 보낸다.



〔그림 1〕 비밀정보 동기화에 기반한 인증 프로토콜

- 2단계 : 태그는 랜덤수 r_T를 발생하고 인증 메시지 $P=h(r_T \oplus k \oplus r_R)$를 리더에게 보낸다.
- 3단계 : 리더는 P, r_T 그리고 r_R을 데이터베이스에게 보내고 데이터베이스는 태그를 인증한 후 $Q=h(P \oplus k \oplus r_R)$를 리더에게 보낸 후 데이터베이스를 갱신한다.
- 4단계 : 리더는 Q값을 태그에게 보내게 되고 태그는 이 값을 인증함으로써 데이터베이스를 인증한다. 이후에 태그는 자신의 비밀 정보 $k=h(k)$를 갱신하여 데이터베이스와 동일한 비밀정보를 유지한다.

2.3. 취약점 분석

Lee 등이 제안한 프로토콜은 그 동안 태그와 데이터베이스간의 인증 문제를 포함하여 비동기 문제를 해결하면서 indistinguishability와 forward security를 제공한다. 그러나 다음과 같은 시나리오에 의해 정당한 태그로 가장한 공격자에 의해 스푸핑 공격이 가능하다. 이 공격에서 공격자는 도청을 할 수 있으며 악의적인 임의의 메시지를 만들어 태그로 전송할 수 있다고 가정한다.

- 1단계 : 공격자는 도청을 통해 리더가 보내는 r_R, 그리고 태그가 전송하는 r_T과 P를 도청한다. 이때 관계식은 아래와 같다

$$P=h(r_T \oplus k \oplus r_R) \quad (1)$$

- 2단계 : 공격자는 다음 세션에서 임의의 r_R'가 오면 태그를 가장하여 $r_T'=r_T \oplus r_R \oplus r_R'$과 $P'=P$를 리더에게 보내게 된다.
- 3단계 : 이 경우 데이터베이스는 이전 세션에서 k의 갱신 유무에 상관없이 인증과정을 통과하게 된다. 왜냐하면 데이터베이스에서는 r_R', r_T'과 P'만을 이용하여 다음 등식이 성립하는지를 검사하기 때문이다.

$$P' = ?\, h(r_T' \oplus k \oplus r_R') \quad (2)$$

이때 r_T'을 조작하여 보냈기 때문에 실제는 아래 등식을 검사하게 되는 것이다.

$$P' = ?\, h(r_T \oplus r_R \oplus r_R' \oplus k \oplus r_R')$$
$$= h(r_T \oplus r_R \oplus k) = P \quad (3)$$

따라서 이 등식은 식 (1)과 같아져 정당한 태그로 인증하게 된다. 만약 이전 세션에서 데이터베이스의 갱신이 있었다면 공격자가 보낸 정보에 포함된 k는 데이터베이스의 k_{last} 필드에 있을 것이고 갱신이 없었다면 k 필드에 있을 것이다. 따라서 공격자는 도청을 통하여 수집한 정보로 정당한 태그로 인증받는 스푸핑 공격이 가능하다.

또한 이 공격은 이전 세션에서 도청한 r_R, P와 Q을 통해서도 위장 공격이 가능하다. 여기에서 $Q=h(P \oplus k \oplus r_R)$ 관계가 성립한다. 이 경우 다음 세션에서 처음 리더로부터 질의(Query)와 r_R'을 받

은 후 r_T'값을 $r_T' = P \oplus r_R \oplus r_R'$로 위조하고 $P' = Q$을 그대로 리더에게 보내면 인증과정을 통과할 수 있다. 즉, 데이터베이스에서는 다음 등식이 성립하는지만 검사하므로 공격자는 이 과정을 통과하게 된다.

$$P' = ? h(r_T' \oplus k \oplus r_R') \quad (4)$$

이때 r_T'을 조작하여 보냈기 때문에 실제는 아래 등식을 검사하게 되는 것이다.

$$P' = ? h(P \oplus r_R \oplus r_R' \oplus k \oplus r_R')$$
$$= h(P \oplus r_R \oplus k) = Q \quad (5)$$

이와 같은 위장 공격은 전달되는 메시지만 도청해도 그 이후 세션에서 계속해서 공격을 시도할 수 있다.

Lee 등이 제안한 프로토콜은 forward security를 부분적으로 만족한다. 즉, 어느 시점에 비밀 키가 노출되면 비밀 키 k가 갱신되기 전까지는 위치 추적이 가능하다는 의미에서 부분적으로만 만족한다고 하고 있다. 그런데 문헌 [12]에서 저자들은 forward security뿐만 아니라 backward security의 중요성을 기술하고 있다. 엄밀한 의미에서 forward security는 backward untraceability를 의미하며 비밀 키가 노출된 이전의 정보를 가지고 위치추적을 할 수 있는 특성으로 정의되고 backward security는 forward untraceability를 의미하며 비밀 키가 노출된 이후의 정보를 가지고 위치추적을 할 수 있는 특성으로 정의된다.

그러나 Lee 등이 제안한 방식은 forward untraceability를 만족하지 못한다. 그 이유는 비밀 정보가 $k = h(k)$형태로 갱신되기 때문에 한번 k가 노출된 이후에도 새로운 k를 공격자가 유추해 낼 수 있기 때문이다. 유추된 k는 P를 만드는데 사용되므로 랜덤수 r_T와 r_R을 알면 위치 추적이 가능하므로 forward untraceability를 만족한다고 볼 수 없다.

Ⅲ. 비밀정보 동기화에 기반한 strong 인증 프로토콜

본 논문에서는 위에서 분석한 내용을 토대로 보안성이 강화된 strong한 인증 프로토콜을 제안한다. 기존 비밀정보 동기화에 기반한 제안된 인증 프로토콜은 다음과 같은 프로토콜 설계상의 문제점이 있으므로 제안할 프로토콜의 설계에서는 최소한 이러한 문제점을 해결하고자 한다.

첫째, 해쉬 함수 내에서 생기는 ⊕연산 때문에 생기는 위장 공격을 방어할 수 있도록 가급적이면 해쉬 함수내에서는 연접연산(||)을 사용하였다. 단, 연접에 따른 해쉬 함수내의 연산량을 줄이기 위해 ⊕연산이 아닌 다른 연산자를 사용할 수 있지만 앞장에서 설명한 위장공격은 불가능해야 한다.

둘째, 태그에서 수행하는 $P = h(r_T \oplus k \oplus r_R)$의 계산구조와 데이터베이스에서 인증을 위해 계산하는 $Q = h(P \oplus k \oplus r_R)$구조를 달리함으로써 (4)식에 의한 두 번째 위장 공격도 방어할 수 있도록 하였다. 또한 태그가 데이터베이스를 인증할 경우 r_R이 인증 요소로 입력될 필요는 없으며 태그에 의해 생성된 r_T를 인증하는 것이 시도 응답형(challenge-response) 인증에 부합된다.

셋째, 태그와 데이터베이스 간에 동기화되는 비밀정보 k를 갱신할 경우, k에 대한 한 번의 노출이 있더라고 이후의 갱신된 k값을 가급적 계산하기 힘들도록 하여 forward untraceability를 만족하는 구조로 설계한다.

넷째, 비동기화(desynchronization) 공격에도 데이터베이스와 태그간의 동기를 회복할 수 있도록 해야 하며 가급적 태그와 데이터베이스에서의 계산량을 최소화하도록 설계한다.

제안 프로토콜 I은 Lee 등의 프로토콜이 가지는 문제점을 개선한 것으로 [그림 2]와 같으며 각 단계를 기술하면 다음과 같다. 단, 태그는 사전에 ID와 자신의 비밀 키 k를 발급받아 저장해 둔다. 여기서 ID는 고정값이지만 k는 인증 과정을 거치면서 갱신되는 비밀 정보이다.

- 1단계 : 리더는 질의(Query)와 랜덤수 r_R을 태그에 보낸다.
- 2단계 : 태그는 랜덤수 r_T를 발생하고 P를 계산하여 리더에게 보낸다.
- 3단계 : 리더는 데이터베이스에 관련정보를 안전하게 보내고 데이터베이스는 자신이 가진 ID와 k와 k_{last} 필드에 있는 값들을 대입하여 계산한 결과를 수신한 P와 비교함으로써 ID를 찾고 인증을 수행한다. 그리고 Q을 계산하여 리더에게 보낸 후 k를 갱

신한다.

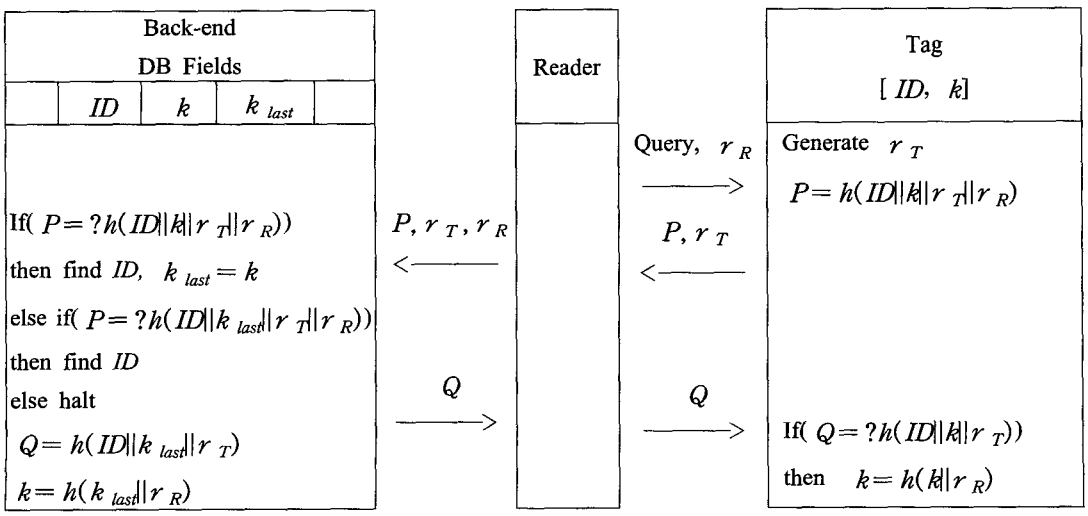
- 4단계 : 리더는 Q을 태그에게 보내고 태그는 이를 검증함으로써 데이터베이스를 인증한다.

인증 프로토콜 I에서는 안전성 측면에서 볼 때 다양한 공격위협으로부터 안전할 수 있지만 단점은 데이터베이스에서 태그의 ID를 찾는데 많은 시간이 필요하다는 점이다. 즉, m개의 태그가 있을 때를 가정하면 Lee 등의 방식이나 제안 방식 I에서는 ID를 찾는데 이전 세션에서 동기화가 잘된 경우에는 평균 $\lceil m/2 \rceil$ 번의 해쉬 연산이 필요하다. 만약, 동기화가 이루어지지 않은 경우에는 k필드와 k_{last} 필드에 대해 모든 검색을 수행해야 하므로 평균 m번의 해쉬 연산이 필요하다. 이점은 대용량의 태그를 가진 경우에는 데이터베이스에 상당한 부담이 될 수 있다. 예를 들어 대형 매장에서 동시에 수십 ~ 수백 개의 제품을 인식해야 할 경우에는 안전성과 더불어 꼭 해결해야 할 문제가 데이터베이스에서의 ID 검색 문제이다.

본 논문에서는 Ha 등이 제안한 상호인증 프로토콜[13]을 개선한 인증 프로토콜 II를 제안한다. 원래 문헌 [13]에서의 인증프로토콜은 고정 ID를 이용하는 것이 아니라 ID값을 계속해서 갱신하는 형태로 제안된 것이다. 제안 프로토콜 II에서는 고정된 ID를 가지면서도 데이터베이스에서 태그의 검색시간을 줄이기 위해 개선한 것이다. 기본 아이디어는 데이터베이스쪽에서 효과적인 ID검색을 위해 다음 세션에서 비교에 사용될 $k_{next} = h(ID||k)$를 미리 계산하여 둔다는 점이다. 따라서 태그는 이전 세션에서 k값이 정상적으로 갱신되었다면 $SYNC$값은 "0"이 되고 다음 세션에서는 $P = h(ID||k)$를 계산하여 보내게 된다. 이 경우 정당한 태그라면 데이터베이스내에서는 해쉬 연산없이 단순히 P와 k_{next} 값의 비교만으로 ID를 찾을 수 있다. 하지만 이전 세션에서 비동기화가 발생하여 만약 k값이 갱신이 되지 않았다고 해서 이전 세션과 동일한 P를 보낼 수는 없다. 그 이유는 이전 세션과 동일한 P를 보내게 되면 위치 추적이 되기 때문이다. 따라서 이전 세션에서 동기화가 어긋난 경우($SYNC = 1$)에는 $P = h(ID||k||r_T)$를 보내어 위치 추적을 불가능하게 해야 한다.

제안 프로토콜 II는 제안 프로토콜 I이나 Lee 등의 프로토콜이 가지는 데이터베이스에서의 태그 검색 부하가 많은 점을 개선한 것으로 [그림 3]과 같이 요약할 수 있으며 각 단계를 기술하면 다음과 같다. 여기서 $SYNC$ 신호는 상호인증이 정상적으로 이루어진 것인지 확인하는 정보로서 정상적으로 인증이 되면 "0", 그렇지 않으면 "1"의 값을 가진다.

- 1단계 : 리더는 질의(Query)와 랜덤수 r_R을 태그에 보낸다.
- 2단계 : 태그는 랜덤수 $SYNC$에 따라 P와 $L(Q)$를 계산하여 리더에게 보낸다.
- 3단계 : 리더는 데이터베이스에 관련정보를 안전하



〔그림 2〕 비밀정보 동기화에 기반한 Strong 인증 프로토콜 I

게 보내고 데이터베이스는 자신이 가진 k_{next}과 P가 동일한지 확인하여 ID를 찾는다. 이 비교 단계에서 찾지 못하면 ID와 k의 쌍 혹은 ID와 k_{last}의 쌍을 r_T와 함께 해쉬 함수의 입력으로 한 연산을 수행하여 P와 비교함으로써 ID를 찾아낸다. 이후 $L(Q)$값을 검증하고 $R(Q')$을 태그에게 보낸 후 k값과 k_{next} 값을 갱신한다.

- 4단계 : 리더는 $R(Q')$을 태그에게 보내고 태그는 이를 검증함으로써 데이터베이스를 인증한다. 이 과정이 성공적이면 $k=h(k\|r_R)$와 같이 비밀 정보를 갱신하고 $SYNC$값을 "0"으로 하여 인증이 정상적으로 종료된 정보를 저장한다.

Ⅳ. 제안 인증 프로토콜 분석

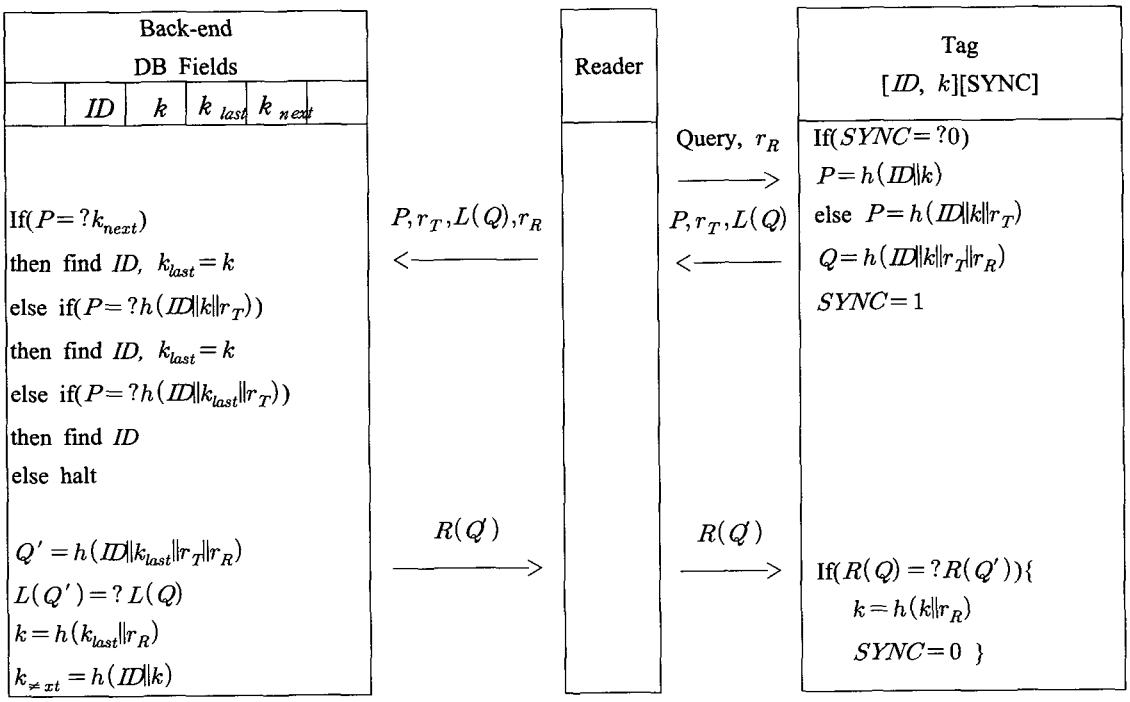
본 장에서는 Ⅲ장에서 제안된 상호 인증 프로토콜의 안전성과 구현의 효율성을 분석하고자 한다. 먼저 안전성을 분석하기 위해서는 공격자의 공격 능력을 가정할 필요가 있는데 본 논문에서는 공격자의 능력이 도청이 가능할 뿐 아니라 메시지에 대한 인터럽트 혹은 블로킹이 가능하다고 가정한다. 또한, 도청된 메시지를 분석한 후 일부 메시지를 변조하여 태그나 리더로 보낼 수 있다고 본다. 향후의 공격 기술의 발전에 따라서는 일부 태그를 손상시킬 수도 있으며 태그의 비밀 정보를 물리적인 방법으로 공격할 수 있을 것이라 가정한다.

4.1. 안전성

4.1.1. 도청

안전성을 분석하는데 가장 기본적인 요소는 도청에 대한 방어 능력이다. 공격자가 리더와 태그간의 정보는 도청할 수 있다고 보지만 이를 통하여 유용한 비밀 정보를 얻을 수 없도록 해야 한다. 제안한 프로토콜 Ⅰ과 Ⅱ에서는 태그와 리더가 발생하는 랜덤수를 제외한 모든 정보는 일방향 해쉬함수 연산을 거쳐 전송되는 정보이므로 전송 정보를 도청하더라도 ID나 비밀키 값들을 계산할 수 없어 안전하다.

4.1.2. 스푸핑 공격



〔그림 3〕 데이터베이스 검색이 효과적인 strong 인증 프로토콜 II

스푸핑 공격은 공격자가 정당한 리더 혹은 태그로 위장하여 상대방을 속이거나 유용한 정보를 얻어내는데 목적이 있다. 이 공격이 성공하기 위해서는 공격자는 상대방의 시도(challenge)에 정당한 응답(response)을 생성해 낼 수 있어야 한다. 제안한 프로토콜 Ⅰ에서 공격자는 올바른 리더로 가장하여 태그를 속이기 위해서는 정확한 Q값을 계산해야 하지만 ID나 비밀키 k를 알지 못하면 생성할 수 없다. 또한 태그로 위장하고자 하는 경우에는 올바른 P값을 전송해야 하지만 이 역시 ID나 비밀키 k를 알지 못하면 계산할 수 없어 안전하다. 제안한 프로토콜 Ⅱ에서도 공격자는 올바른 리더로 가장하여 태그를 속이기 위해서는 정확한 $R(Q')$값을 계산해야 하지만 ID나 비밀키 k를 알지 못하면 생성할 수 없다. 그리고 태그로 위장하고자 할 때에도 올바른 P와 $L(Q)$를 전송해야 하지만 이 역시 ID나 비밀키 k를 알지 못하면 계산할 수 없어 안전하다.

4.1.3. 위치 추적

위치 추적 공격은 공격자가 특정한 태그로부터 동일한 정보나 특정 태그를 구별할 수 있는 정보를 찾아 태그 소유자의 위치를 추적하는 공격이다. 제일 쉽게 생각할 수 있는 위치 추적은 태그로부터 매 세션마다 동일한 정보가 나오는 RFID 시스템은 위치 추적이 가능하다고 본다. 또한 랜덤한 두개의 태그를 두고 이들을 구별해 낼 수 없으면 indistinguishability를 만족하며 태그의 위치 프라이버시를 보장받을 수 있다. 제안된 프로토콜 Ⅰ과 Ⅱ에서는 매 세션마다 P나 $L(Q)$값이 새롭게 갱신되므로 이전 세션과 동일한 값을 전송하지 않으며 일방향 해쉬 함수를 사용하기 때문에 공격자는 매 세션마다 나오는 정보로 위치를 추적할 수 없다.

4.1.4. 비동기화 공격

공격자가 전송 메시지를 블로킹하여 정상적인 인증 과정을 방해했을 경우, 태그와 데이터베이스는 비동기 상태에 빠질 수 있다. 이러한 문제를 해결하기 위해 태그는 최소한 이전 세션에서 사용된 비밀 정보 k_{last}를 저장하고 있어야 한다. 그 이유는 데이터베이스가 태그보다 항상 먼저 키를 갱신하도록 되어 있어 데이터베이스는 갱신을 했지만 태그가 키 갱신을 못했을 경우만 고려하면 된다. 이 경우에 대비하여 제안된 프로토콜 Ⅰ과 Ⅱ에서는 비동기화를 방어하기 위해 k_{last}를 저장하여 동기를 회복하고 있다. 특히, 프로토콜 Ⅱ에서는 이전 세션이 정상 종료된 경우, 데이터베이스에서는 저장해 둔 $k_{\neq xt}$와 $P=h(ID\|k)$값을 비교하여 쉽게 태그를 찾아낸다. 그러나 전송 메세지가 블로킹되는 경우는 블로킹 부분에 따라 데이터베이스에서의 검색 요소가 달라진다. 즉, 프로토콜 Ⅱ에서 태그와 리더간의 두 번째 메시지 중 $P=h(ID\|k)$가 블로킹되면 데이터베이스와 태그는 모두 비밀정보 갱신을 하지 않게 되고 다음 세션에서 $P=h(ID\|k\|r_T)$가 전송되므로 데이터베이스는 모든 ID와 k 쌍에 대해 r_T를 검증하는 해쉬 연산을 수행해야 한다. 이때는 평균 $\lceil m/2 \rceil$ 번의 해쉬 연산이 필요하다. 두 번째는 태그와 리더간의 세 번째 메세지가 블로킹되어 데이터베이스에서는 비밀정보 갱신을 했고 태그에서는 갱신을 하지 못한 경우를 살펴보자. 이때 다음 세션에서는 $P=h(ID\|k\|r_T)$가 전송되므로 데이터베이스에서 ID와 k 쌍에 대해 r_T를 검증하면 ID를 찾을 수 없고, ID와 k_{last} 쌍에 대해 r_T를 검증하는 경우에만 태그를 찾을 수 있다. 따라서 이 경우에는 태그 검색을 위해 평균 $m+\lceil m/2 \rceil$ 번의 해쉬 연산이 필요하다.

4.1.5. 물리적 공격

태그에 대한 물리적 공격으로 인해 태그의 ID와 k에 관한 정보가 노출되었고 이전에 도청된 정보를 가지고 있다고 하더라도 위치를 추적할 수 없는 성질이 backward untraceability이고 물리적인 비밀 정보 노출 이후에도 계속해서 태그가 사용되어 위치가 추적되는 것이 forward untraceability인데 프로토콜 Ⅰ과 Ⅱ에서는 Lee 등에 제안한 프로토콜과 마찬가지로 비밀 정보가 노출된 시점 이전에 한번이라도 k가 갱신되면 위치 추적이 불가능하므로 backward untraceability는 부분적으로 만족한다고 하고 있다.

또, forward untraceability 측면에서 보면 Lee 등이 제안한 방식은 비밀 정보가 $k=h(k)$형태로 갱신되기 때문에 한번 k가 노출된 이후에도 계속해서 k를 공격자가 유추해 낼 수 있기 때문에forward untraceability을 만족하지 못한다. 그러나 제안된 프로토콜 Ⅰ과 Ⅱ

에서는 비밀 키 k를 $k=h(k\|r_R)$로 갱신하도록 하였다. 그 이유는 특정 태그의 ID와 k가 노출된 이후에도 연속적으로 모든 r_R값을 알고 있으면 forward 위치추적이 가능하지만 한번이라도 r_R값을 알지 못하면, 즉 k를 갱신하는 체인이 끊기면 다음 세션의 k를 유추할 수 없도록 하기 위해서이다. 따라서 제안된 프로토콜 I과 II는 특정 태그의 r_R 값을 연속적으로 도청할 수 있는 시점까지만 forward 위치추적이 가능하므로 부분적으로 forward untraceability를 만족한다고 할 수 있다.

상기한 바와 같이 RFID 시스템에 대해 안전성 측면에서 기존의 방식과 제안 방식을 비교한 것이 표 1이다. 표에서 보는 바와 같이 Dimitriou와 같은 방식[5]은 정상적으로 세션이 종결되지 못하면 다음 세션에서 태그가 동일한 정보를 전송하는 형태라 위치 추적이 되는 대표적인 사례이고 비동기화가 발생했을 경우 태그를 더 이상 사용할 수 없는 상황도 발생한다. Rhee 등의 방식[4]은 매 세션마다 고정된 ID를 사용하는데 태그가 한번 비밀 키를 노출하게 되면 도청된 정보를 이용하여 위치추적이 가능하므로 backward untraceability와 forward untraceability를 만족하지 못한다. Lee 등의 방식에서는 비동기화 문제를 해결하기 위해 동기화된 비밀 정보를 사용하지만 상기한 바와 같이 스푸핑 공격과 태그가 물리적 공격을 당했을 경우 forward untraceability를 만족하지 못한다.

4.2. 효율성

제안된 동기화된 비밀 정보에 기반한 인증 프로토콜을 효율성 면에서 비교한 것이 [표 2]이다. 비교 요소는 태그와 데이터베이스에서의 연산량, 데이터 저장 공간 그리고 통신량이다. 여기에서는 m개의 태그가 있고 각 정보들은 L비트로 구성되어 있다고 가정하자 단, 비교하고자 하는 프로토콜들의 연산량중에서 태그가 랜덤 수를 생성할 때 필요한 계산량은 공통적으로 생략하였다. 그 이유는 태그에 랜덤 수 생성기를 별도로 두는 방법도 있으며 논문 [4]에서 밝힌 바와 같이 해쉬 함수를 이용할 수도 있지만 그 생성방법은 선택적 요소이기 때문이다. Dimitriou와 같은 방식[5]은 안전성은 부족하지만 데이터베이스와 태그의 계산량은 비교적 적다. Lee 등의 방식에서 태그에서 필요한 연산은 3번으로 비교적 적다. 그러나 태그를 찾기 위해 데이터베이스에서는 평균 $\lceil m/2 \rceil$ 번의 해쉬 연산이 필요하므로(비동기 상태에서는 평균 $m+\lceil m/2 \rceil$ 번) 데이터베이스에서 필요한 해쉬 연산은 평균 $\lceil m/2 \rceil+2$번이다. 제안 프로토콜 I에서의 연산량은 Rhee 등의 방식이나 Lee 등의 방식과 거의 비슷하다. 그러나 제안 프로토콜 II에서는 데이터베이스에서 연산하는 연산량을 획기적으로 줄일 수 있는데 정상 상태에서는 단지 3번의 해쉬 연산량만 필요하다. 그 이유는 특정 태그를 찾기 위해서 모든 태그에 대해 해쉬 연산을 할 필요가 없고 단지 저장 값과의 비교만 필요하므로 연산량을 줄일 수 있다. 그러나 제안 프로토콜 II에서도 비동기화가 발생하면 다음 세션에서 정당한 태그를 찾아 동기를 회복하는데 평균 $\lceil m/2 \rceil \cdot 2+3$번의 해쉬 연산이 필요하다.

제안 프로토콜 I에서는 태그는 ID를 저장하기 위한 $2L$ 비트의 저장 공간을 필요로 하는 반면, 데이터베이스는 $3L\times m$의 저장 공간을 필요로 한다. 이것은 소요되는 메모리와 각 연산량 측면에서 Lee 등의 프로토콜과 동일하다. 그러나 제안 프로토콜 II에서는 데이터베이스에서 추가적으로 k_{next}를 저장해야 하므로 태

〔표 1〕 안전성 비교

(○: 안전, ×: 불안전, △ : 부분만족)

구 분	Dimitriou[5]	Rhee 등[4]	Lee 등[8]	제안방식 I	제안방식 II
재생 공격	○	○	○	○	○
스푸핑 공격	○	○	×	○	○
위치추적 공격	×	○	○	○	○
비동기 공격	×	○	○	○	○
backward untraceability	△	×	△	△	△
forward untraceability	△	×	×	△	△

〔표 2〕 연산량 비교

(m: DB에 저장된 ID 수, L : 데이터 단위 비트)

구 분	Dimitriou[5]	Rhee 등[4]	Lee 등[8]	제안방식 I	제안방식 II
DB 해쉬 연산	4	$\lceil m/2 \rceil + 1$	$\lceil m/2 \rceil + 2$[1]	$\lceil m/2 \rceil + 2$[1]	3[2]
T 해쉬 연산	4	2	3	3	3
DB 메모리(비트)	$2L \times m$	$L \times m$	$3L \times m$	$3L \times m$	$4L \times m$
T 메모리(비트)	L	L	$2L$	$2L$	$2L+1$
통신량	$5L$	$4L$	$4L$	$4L$	$4L$

1) 비동기화 발생시 동기회복을 위해서는 평균 $m + \lceil m/2 \rceil + 2$번

2) 비동기화 발생시 동기회복을 위해서는 평균 $\lceil m/2 \rceil \cdot 2 + 3$번

그당 L비트씩 늘어나며 태그에서는 $SYNC$ 정보를 저장해야 하므로 1비트씩 늘어난다.

따라서 제안 프로토콜 I과 II는 안전도면에서도 strong한 프라이버시를 제공하고 있으며 특히 프로토콜 II에서는 데이터베이스에서의 연산 시간이 줄게 되어 태그가 많은 대용량 RFID 시스템이나 동시 접속이 많은 시스템에 적합하다.

V. 결 론

최근 RFID 시스템의 보안 요구 사항이 스푸핑 공격과 같은 위장 공격이나 indistinguishability 등을 넘어 forward untraceability까지 요구되면서 보다 암호학적으로 strong한 프로토콜을 필요로 하고 있다. 본 논문에서 데이터베이스와 태그가 동일한 비밀 키를 저장하면서 동기화를 통해 상호 인증을 하는 프로토콜 중에서 기존 프로토콜이 가지는 취약점을 분석하고 보다 강인한 특성을 지닌 인증 방식을 제안하였다. 제안 프로토콜 I과 II는 현재까지 제시된 RFID의 보안 위협 중에서 스푸핑 공격, 비동기 공격에 안전함은 물론 태그 소유자의 위치 프라이버시를 보장하는 indistinguishability를 만족하며 나아가 부분적으로 backward untraceability와 forward untraceability를 만족하는 강력한 인증 방식이다. 특히 제안 프로토콜 II는 데이터베이스에서 저장 공간이 더 필요하기는 하지만 태그 인증을 위한 연산시간을 크게 줄일 수 있어 대용량의 RFID 시스템에 적합하다.

참고문헌

[1] Auto-ID Center, *"860MHz-960MHz Class I Radio Frequency Identification Tag Radio Frequency and logical Communication Interface Specification Proposed Recommendation Ver. 1.0.0, Technical Report, MIT-AUTOID-TR-007"*, AutoID Center, MIT, 2002.

[2] S. Lee, Y. Hwang, D. Lee and J. Lim, "Efficient Authentication for Low-cost RFID Systems", *ICCSA'05*, LNCS 3480, pp. 619-627, Springer-Verlag, 2005.

[3] M. Ohkubo, K. Suzuki and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID," *In proceedings of the SCIS'04*, pp. 719-724, 2004.

[4] K. Rhee, J. Kwak, S. Kim and D. Won, "Challenge-Response Based on RFID Authentication Protocol for Distributed Database Environment", *SPC'05*, LNCS 3450, pp. 70-84, Springer-Verlag, 2005.

[5] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks." *Security and Privacy for Emerging Areas in Communications Networks-2005*, pp. 59-66, Sept., 2005.

[6] J. Saito, J. Ryou and K. Sakurai, "Enhancing Privacy of Universal Reencryption Scheme for RFID Tags," *EU- 2004*, LNCS 3207, pp. 879-890, Springer- Verlag, 2004.

[7] P. Peris-Lopez, J. C. Hermandez-Castro, J. M. Estevez-Tapaidor, A. Ribagorda, "EMAP: An efficient Mutual-Authentication Protocol for Low-cost RFID tags," *Proceedings of OTM Federated Conferences and Workshop: IS Workshop*, Nov., 2006.

[8] S. Lee, T. Asano and K. Kim. "RFID Mutual Authentication Scheme based on Synchronized Secret Information." *Proceedings of the SCIS'06*, 2006. available at http://caislab.icu.ac.kr/Paper/paper_files/2006/SCIS_Lee.pdf

[9] 최은영, 이수미, 임종인, 이동훈, "분산시스템 환경에 적합한 효율적인 RFID 인증시스템", *한국정보보호학회논문지*, 제 16권, 제 6호, pp. 25-35, 2006. 12.

[10] 하재철, 하정훈, 박제훈, 김환구, 문상재, "분산 환경에 적합한 저비용 RFID 인증 프로토콜", *한국정보보호학회하계학술대회 논문집*, 제 17권 제1호, pp.78-83, 2007. 6.

[11] 박정수, 최은영, 이수미, 이동훈, "저가형 RFID 시스템에 강한 프라이버시를 제공하는 자체 재암호화 프로토콜", *한국정보보호학회논문지*, 제 16권, 제 4호, pp. 3-12, 2006. 8.

[12] C. H. Lim and T. K. Kwon, "Strong and Robust RFID Authentication Enabling perfect Ownership Transfer," *ICICS'06*, LNCS 4307, pp. 1-20, Springer-Verlag, 2006.

[13] J. C. Ha, J. H. Ha, S. J. Moon and C. Boyd, LRMAP: Lightweight and Re- synchronous Mutual Authentication Protocol for RFID System, *ICUCT 2006*, LNCS 4412, Dec., 2006.

〈著者紹介〉

하 재 철 (JaeCheol Ha) 종신회원
1989년 2월: 경북대학교 전자공학과 졸업
1993년 8월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2006년 1월: 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2006년 7월~2006년 12월: QUT in Australia 연구 교수
2007년 3월~현재: 호서대학교 정보호호학과 부교수
2002년 3월~현재: 한국정보보호학회 이사
<관심분야> 정보보호, 네트워크 보안, 스마트카드 보안

김 환 구 (HwanKoo Kim) 종신회원
1987년 2월: 경북대학교 수학과 졸업
1991년 2월: 경북대학교 대학원 수학과 이학석사
1998년 5월: U. of Tennessee-Knoxville, 수학과, Ph. D.
2002년 3월~현재: 호서대대학교 정보보호학과 교수
2004년 3월~현재: 한국정보보호학회 이사
<관심분야> 평가 및 인증, 암호학

하 정 훈(JungHoon Ha) 학생회원
2002년 2월: 경북대학교 전자·전기공학부 졸업
2004년 2월: 경북대학교 전자공학과 석사
2007년 8월: 경북대학교 전자공학과 박사
2007년 9월~현재: 삼성전자 연구원
<관심분야> 정보보호, 네트워크 보안

박 제 훈 (JeaHoon Park) 학생회원
2004년 2월: 경북대학교 전자·전기공학부 졸업
2006년 2월: 경북대학교 전자공학과 석사
2006년 3월~현재: 경북대학교 전자공학과 박사과정
<관심분야> 정보보호, 네트워크 보안, 스마트카드 보안

문 상 재 (SangJae Moon) 종신회원
1972년 2월: 서울대학교 공업교육(전자전공)과 학사
1974년 2월: 서울대학교 전자공학과 석사
1984년 6월: 미국 UCLA 전기공학과 박사
1984년 7월~1985년 6월: UCLA Postdoctor 근무
1984년 7월~1985년 6월: 미국 OMNET 컨설턴트
1997년 9월~1998년 8월: 경북대학교 전자전기공학부 학부장
1974년 12월~현재: 경북대학교 전자전기컴퓨터공학부 교수
2000년 8월~현재: 경북대학교 이동네트워크 정보보호기술 연구센터장
2002년 2월~현재: 한국정보보호학회 명예회장
<관심분야> 정보보호, 디지털 통신, 이동 네트워크