情報保護學會論文誌
第18卷 第1號, 2008. 2

검색 정보 사전 동기화를 이용한 저비용 RFID 인증 방식*

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

Low-cost Authentication Protocol Using Pre-synchronized Search Information in RFID System*

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

요 약

최근 유비쿼터스 분산 환경에 적합한 해쉬 기반의 효율적인 RFID 인증 프로토콜들이 제안되었다. 분산 환경에 적합하기 위해서는 고정된 ID를 사용하는 것을 일반적인 특징으로 하는데, 기존 방식들은 ID를 Back-end DB에서 검색하는데 시간이 많이 소요되거나 안전성 측면에서 몇 가지 취약점을 가지고 있다. 본 논문에서는 분산 환경에 적합하도록 고정 ID를 사용하면서 DB에서 ID 검색이 용이한 RFID 인증 프로토콜을 제안하고자 한다. 제안 프로토콜의 특징은 DB가 다음 세션의 ID 검색을 용이하게 하기 위해 이전 세션에서 미리 검색 정보를 저장하여 둔다는 점이다. 제안 프로토콜에서는 태그와 DB간의 비동기 현상이 일어나지 않을 경우, 태그와 DB가 각각 단 3번씩의 해쉬 연산만으로 상호 인증을 수행할 수 있다.

ABSTRACT

Recently, many hash-based authentication protocols were presented to guarantee mutual authentication between tag and DB in RFID system. To be suitable for distributed DB environment, one generally uses fixed constant value as a tag ID. However, some existing protocols have security flaws or heavy computational loads in DB in order to search a tag ID. We propose a secure authentication protocol which is suitable for distributed DB environment by using unchangeable tag ID. The storage method of pre-synchronized information in DB at previous session is core idea of our proposal which gives low-cost ID search of DB at next session. In normal synchronization state, our protocol only requires 3 hash operations in tag and DB respectively.

Keywords : *RFID System, Authentication protocol, Indistinguishability, Traceability*

접수일: 2007년 9월 29일; 채택일: 2007년 12월 5일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음. (IITA-2008-C1090-0801-0026).
† 주저자, jcha@hoseo.edu
‡ 교신저자, jcha@hoseo.edu

Ⅰ. 서 론

RFID 시스템은 RFID 태그와 리더 그리고 Back-end 데이터베이스(DB)로 구성된 개체를 인식하는 시스템으로서 소형성, 저가, 그리고 내장성 등의 장점을 갖추고

있다. 최근에는 리더와 태그 사이의 무선 통신을 통한 개체 인식 방식이 주류를 이루면서 바코드 시스템을 대체할 방법으로 각광받고 있다[1, 2]. 그러나 태그와 리더 간의 무선 구간은 RF 신호를 이용하게 되고 이로 인해 안전성이 위협받고 있다. RFID 시스템에서 안전성을 위협하는 요소는 개인 프라이버시 정보의 노출, 스푸핑(spoofing) 공격, 위치 추적 그리고 비동기화(desynchronization) 공격 등이 대부분이다.

RFID 시스템의 안전성 문제를 해결하기 위해 리더와 태그간의 다양한 인증 방법들이 제안되었다. 해쉬 함수를 이용하거나[3-9] 재암호화 방법[10] 혹은 +, ⊕, ∧, ∨ 연산을 사용하는 방법[11, 12]들이 있다. 이 중에서 해쉬 함수에 기반한 방법들이 많이 제안되었는데 이는 태그의 안전도를 보장하면서 계산 부하 및 저장 공간을 최소화하기에 적합한 암호기술로 평가되고 있기 때문이다.

기존에 제안된 인증 시스템 중에서 유비쿼터스 분산 환경에 적합하게 설계된 것으로 Rhee 등이 제안한 CRAP(Challenge-Response Based Authentication Protocol)방식[7]과 Choi 등이 제안한 OHLCAP(One-way Hash Based Low-Cost Authentication Protocol) 방식[8]이 있다. 분산 환경에 적합하기 위해서는 고정된 ID를 사용하는 것을 특징으로 하는데 이것 자체가 DB에서 ID를 검색하는 시간을 많이 소비하거나 안전성 측면에서 몇 가지 취약점을 가지게 된다. 또한, 문헌 [7]이나 [8]에서는 상호 인증을 수행하므로 DB가 태그의 ID를 인증하는 것은 물론 태그가 DB를 인증한다. 태그가 DB를 인증하는 이유는 추후 태그의 사용을 중지할 필요성이 있거나 인증 후의 추가 서비스에 의해 태그 메모리에서 데이터를 읽고 쓰는데 필요한 명령어의 객체를 인증할 경우와 같은 확장적 요소가 필요하기 때문이다. 하지만 단순히 DB가 태그를 인식만 하는 경우에는 굳이 DB 인증을 하지 않아도 된다.

본 논문에서는 먼저 분산 환경에 적합한 RFID 인증 시스템 중 CRAP 방식과 OHLCAP 방식을 분석한다. 분석 결과 CRAP 방식은 안전도 측면에서는 문제가 없지만 DB에서 ID를 찾기 위한 계산량이 너무 많으며, OHLCAP 방식은 안전성에 몇 가지 위협이 존재한다. 본 논문에서는 기존 프로토콜 분석 결과를 기반으로 고정 ID를 사용하면서 DB에서 ID 검색이 용이하며, 재동기화 기능을 활용하여 분산 환경에 적용할 수 있는 RFID 인증 프로토콜을 제안하고자 한다. 제안 프로토콜의 핵심은 DB가 다음 세션에서 태그 ID 검색을 용이하게 하기 위해 이전 세션에서 미리 검색 정보를 저장하여 둔다는 점이다. 제안 프로토콜은 안전성면에서 정보 노출 공격, 스푸핑 공격, 위치 추적은 물론 전송 메시지의 유실시 발생하는 비동기화 문제도 해결하였다. 계산의 효율성 면에서는 태그와 DB간의 비동기 현상이 일어나지 않을 경우, 태그와 DB가 각각 단 3번씩의 해쉬 연산만으로 태그 검색 및 상호 인증을 수행할 수 있어 대형 RFID 시스템에서 유용하게 사용할 수 있다.

Ⅱ. 기존의 분산 환경형 RFID 인증 방식

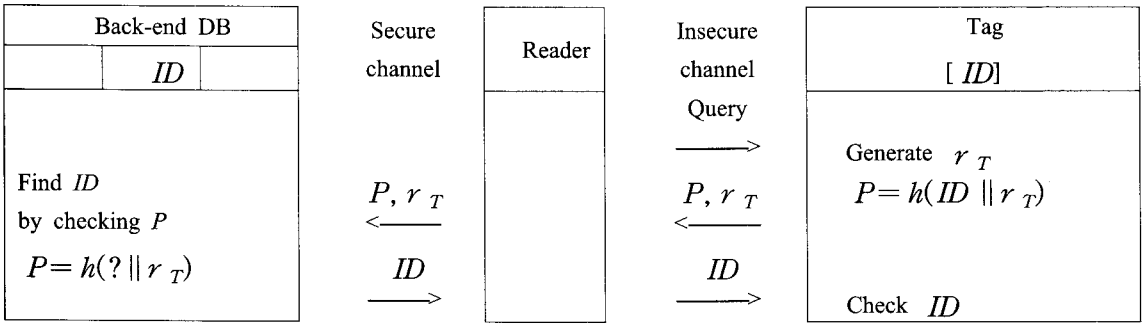
2.1. 용어 및 표기

기존의 논문을 분석하거나 제안하는 프로토콜 설명을 위해 사용될 용어 및 표기는 다음과 같다.

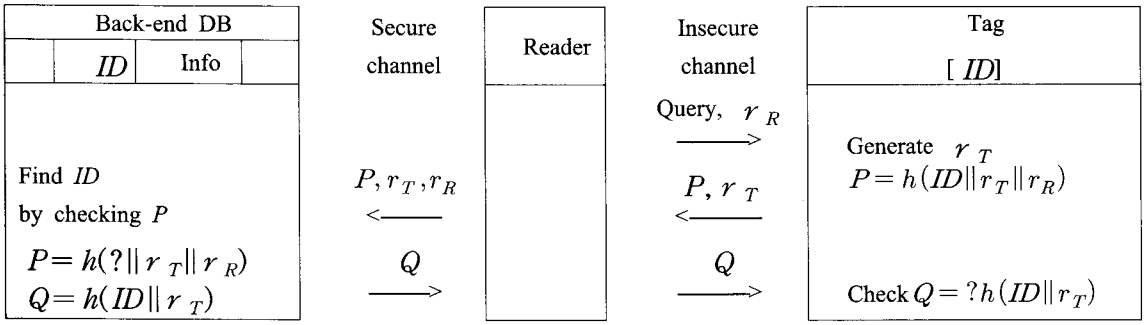
- $h(\ )$: 해쉬 함수
- ID : 태그를 인식할 수 있는 고유한 비밀 정보. 단, ID값은 해쉬 함수의 입력으로 사용될 경우 전수조사 공격 등에 대응할 수 있을 정도의 충분한 랜덤성과 길이를 가져야 하며 DB에서 EPC(Electronic Product Code)와 연동하여 사용할 수도 있음.
- S : 하나의 태그와 데이터베이스간 고유 비밀 키
- GI_i : i 번째 그룹 인덱스
- K : 모든 태그와 데이터베이스간의 공통키
- c : 태그의 카운터
- r_R 혹은 r : 리더가 발생하는 랜덤 수
- r_T : 태그가 발생하는 랜덤 수
- $B_L(B_R)$: 메시지 B의 왼쪽(오른쪽) 반절
- x_p : 이전 세션의 x값
- x_c : 현재 세션의 x값
- ⊕ : 비트 XOR
- ‖ : 연접(concatenation)

2.2. Randomized Hash-Lock 인증 방식

이 인증 방식은 RFID 인증 방식 중 초기에 제안된 방식으로서 다양한 형태의 보안성 분석 과정에서 보안성은 거의 없다는 것이 밝혀졌다. 난수 기반 해쉬 락 인증 방식인 RHAP(Randomized Hash-Lock Authentication Protocol)방식을 도식화한 것이 [그림 1]이다[3].



〔그림 1〕 Randomized Hash-Lock 인증 프로토콜(RHAP)



〔그림 2〕 Challenge-Response 기반 인증 프로토콜(CRAP)

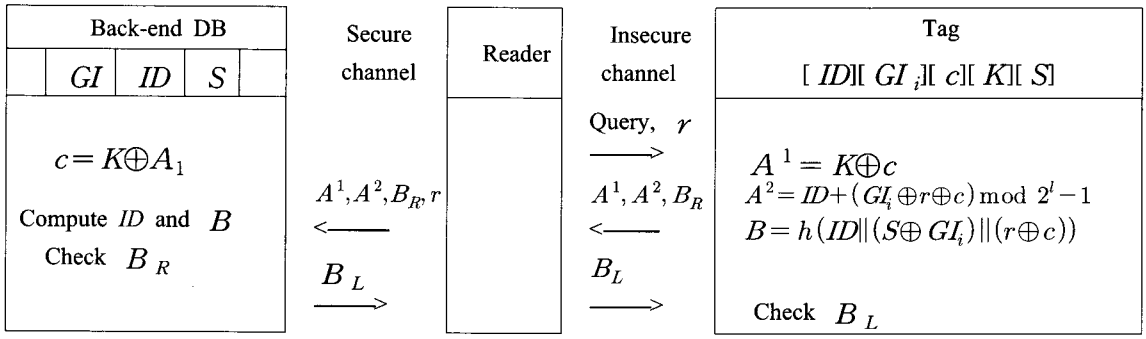
이 방식에서 태그가 난수를 발생하여 단지 한 번의 해쉬 연산을 통해 인증을 요청하지만 안전성을 보장할 수 없다. 첫째, 도청(eavesdropping)을 통해 ID 정보를 얻을 수 있으며, 둘째, 공격자가 이전에 사용한 P, r_T를 리더에게 보냄으로서 재생(replay)공격이 가능하다. 셋째, 공격자는 다른 태그 정보를 리더에게 보냄으로서 정당한 태그로 위장할 수 있으며, 넷째, 도청을 통해 위치 추적도 가능하다. 또한 계산량 측면에서 보면 태그의 연산량은 적지만 데이터베이스에서는 정당한 태그를 찾기 위해 평균 $\lceil m/2 \rceil$ 번의 해쉬 연산이 필요하다.

2.3. CRAP 인증 방식

Rhee 등이 제안한 시도-응답형 인증 프로토콜인 CRAP 인증 방식을 나타낸 것이 [그림 2]이며[7], 인증 절차를 간략히 기술하면 다음과 같다. 이 방식에서 데이터베이스는 단지 ID 목록만 가지고 있으며 태그 역시 자신의 ID 값만 저장하고 있다.

- 1단계 : 리더는 질의(Query)와 랜덤 수 r_R을 태그에 보낸다.
- 2단계 : 태그는 랜덤 수 r_T를 발생하고 인증 메시지 $h(ID \| r_R \| r_T)$를 리더에게 보낸다.
- 3단계 : 리더는 r_R, r_T 그리고 $h(ID \| r_R \| r_T)$를 데이터베이스에게 보내고 데이터베이스는 태그를 인증한 후 $h(ID \| r_T)$을 리더에게 보낸다.
- 4단계 : 리더는 $h(ID \| r_T)$ 값을 태그에게 보내게 되고 태그는 이 값의 정확성을 인증함으로써 데이터베이스를 인증한다.

이 인증 방식은 메모리 사용과 태그의 계산량 측면에서는 효율적인 방법이다. 그러나 데이터베이스에서는 태그의 인증을 위해 모든 ID를 검색해야 하므로 m개의 태그가 있다면 평균 $\lceil m/2 \rceil + 1$번의 해쉬 연산이 필요하여 태그가 많은 시스템에서는 데이터베이스에서의 부하가 많아지게 된다. 일반적으로 분산형 RFID 시스템을 사용하는 환경은 지역적으로 멀리 떨어져 있는 독립된 데이터베이스를 사용하거나 대용량의 태그를 분산 처리해야 하는 환경이다. 이러한 점을 고려하면 데이



〔그림 3〕 해쉬 기반의 저가형 RFID 인증 프로토콜(OHLCAP)

터베이스에서 계산량이 많다는 것을 분산 환경형이라고 하기에는 역설적인 측면을 가지고 있다.

2.4. OHLCAP 인증 방식

Choi 등이 제안한 해쉬 기반 인증 프로토콜은 초기화 단계와 상호 인증 단계로 이루어져 있으며 이를 나타낸 것이 [그림 3]이다[8].

■ 초기화 단계

- 데이터베이스 : m개의 태그를 n개의 그룹으로 나누고 각 그룹은 평균 n/m개의 태그를 가지게 구분한다. 데이터 필드는 $GI \| ID \| S \| Data$이며 모든 태그와 데이터베이스간의 공통 비밀 키로 K를 사용한다. 여기서 GI는 각 태그가 속한 그룹의 인덱스이다.
- 태그 : 각 태그 데이터 필드는 $ID \| GI_i \| c \| K \| S$이며 카운터는 리더로부터 질의를 받을 때마다 하나씩 증가시킨다.

■ 상호 인증 단계

- 1단계 : 리더는 랜덤 수 r을 발생하여 질의와 함께 태그에게 보낸다.
- 2단계 : 태그는 아래와 같은 연산을 수행하고 이 중에서 A^1, A^2, B_R을 리더에게 보낸다.

$A^1 = K \oplus c$,

$A^2 = (ID + (GI_i \oplus r \oplus c)) \bmod (2^l - 1)$,

$B = h(ID \| (S \oplus GI_i) \| r \oplus c)$

- 3단계 : 리더는 A^1, A^2, B_R, r을 데이터베이스에 보내고 데이터베이스는 다음 연산을 통해 태그의 ID를 찾는다. 데이터베이스가 찾은 ID를 이용하여 $B = h(ID \| (S \oplus GI_i) \| r \oplus c)$를 계산하고 전송된 B_R 값을 검사함으로써 태그를 인증한다. 태그 인증 후에는 B_L 값을 리더에게 보낸다.

$c = K \oplus A_1$,

$ID = (A^2 - (GI_i \oplus r \oplus c)) \bmod (2^l - 1)$,

$B = h(ID \| (S \oplus GI_i) \| r \oplus c)$

- 4단계 : 리더는 B_L 값을 태그에게 보내게 되고 태그는 이전에 계산된 값과 동일한지 여부를 확인함으로써 데이터베이스를 인증한다.

이 방식은 태그가 한 번의 해쉬 연산만 수행하므로 효과적인 인증 방법으로 제시되었으며 공격들로부터 모두 안전하다고 분석되었다. 그러나 최근 OHLCAP 프로토콜은 몇 가지 위치 추적 공격에 취약함이 발견되었다[13].

Ⅲ. OHLCAP에 대한 취약점 분석

이 장에서는 OHLCAP 인증 프로토콜의 안전성을 분석해 보기로 한다. 먼저, RFID 시스템에서는 위치 추적 공격이 아주 중요한 위협이므로 위치 추적 공격에 대한 안전성을 엄밀하게 정의할 필요가 있다. 위치 추적 공격은 공격자가 태그의 이전 이동 경로를 추적할 수 있는 공격으로서 이 공격을 방어하기 위해서는 RFID 태그의 응답이 공격자에게 랜덤하게 보여 다른 태그와의 구별이 불가능(indistinguishability)하여야 한다. 구별 불가능성은 임의의 두 개의 태그가 있을 경우 모든 세션에서 이 둘 중에서 특별한 하나를 찾아내는 공격이 불가능함을 의미한다[14]. 뿐만 아니라 어떤 태그가 공격자로부터 위치 추적을 피하기 위해서는 현재 세션에서 출력하는 정보가 이전 세션에서 출력된 정보와도 독립성을

유지해야 한다. 만약 태그의 현재 정보가 이전 정보와 연관성을 가지고 있다면 공격자는 이 연관성을 찾아냄으로써 다른 태그와 구별하고 위치를 추적할 수 있다. 즉, 현재 세션의 태그는 인접한 태그의 정보와 구별 불가능해야 함과 동시에, 이전 세션의 정보와도 연관성이 없어야 위치 추적에 안전하다고 할 수 있다. 따라서 현재 세션에서는 이전 세션과 동일한 정보 메시지나 연관성을 유추할 수 있는 메시지가 아닌 랜덤한 정보를 출력하여야 하며 다른 태그와도 구별되지 않아야 한다.

3.1. 카운터 정보를 이용한 위치 추적 공격

이 공격은 전송되는 메시지를 도청하면서 간단한 XOR 연산만으로 이전 세션에서 사용된 태그를 구별해냄으로써 태그의 위치를 추적하는 공격이다.

가정 1 : 공격자는 이전 세션에서 출력하는 정보 $A_p^1 = K \oplus c_p$를 도청하였다고 가정하자. 이후 공격자는 태그들이 출력하는 정보를 도청하여 $A_c^1 = K \oplus c_c$를 얻어 이 태그가 이전의 태그와 동일한 태그인지를 찾아내는 공격이다. 물론 카운터는 1이 증가하였으므로 $c_c = c_p + 1$이라 가정한다. 여기서 가정은 A_c^1와 A_p^1가 특정 태그의 연속적인 메시지라는 것을 이미 알고 있는 것은 아니며, 공격하고자 하는 특정한 태그의 A_c^1은 정해지고 A_p^1은 이전에 발생한 여러 개의 신호 중에서 공격자가 구별해야 할 메시지이다. ■

공격 1 : 공격자는 취득한 A_c^1 그리고 임의의 A_p^1, 이 두 메시지를 XOR 연산을 한다. 즉, $A = A_p^1 \oplus A_c^1 = c_p \oplus c_c$ 가 된다. 그 결과 이 식에서 K 성분은 상쇄되고 카운터와 관련한 정보만 가지게 된다. 따라서 현재 카운터는 이전 카운터 값에서 하나씩 증가한 값이므로 A값은 언제나 LSB(Least Significant Bit)로부터 1's-run을 갖게 된다. 따라서 공격자가 목표 태그의 이전 세션 정보를 알고 있다면 다음 세션에서 출력하는 정보가 1's-run을 가지는지 살펴봄으로써 추적하고자 하는 태그인지 구별할 수 있다. ■

예를 들면, $c_p = 1011010101$이라면 그 다음 세션의 $c_c = 1011010110$일 것이다. 이 경우 $A = c_p \oplus c_c = 0000000011$와 같이 LSB로부터 2비트의 1's-run을 가진다. 특히, $c_p = 1011010110$과 같이 최하위 비트가 0인 경우에는 공격 시의 A값은 항상 단지 1비트의 1's-run을 가지게 되므로 구별이 훨씬 쉽다. 따라서 공격자는 연속적인 태그의 출력 정보 A_p^1와 A_c^1를 도청할 수 있으면 위치 추적이 가능하다. 일반적으로 카운터 정보의 특성상 카운터 값이 큰 값을 사용할수록 동일하지 않은 태그는 1's-run을 가지지 않게 되고 동일한 태그는 다음 세션에서 반드시 1's-run을 가지게 된다. 특히, 카운터가 l비트이면 공격 대상 태그와 임의의 태그를 구별할 수 없는 확률은 $l/2^l$이 되므로 이는 l이 클 경우 무시할 만하므로 위치 추적의 정확성은 매우 높다. 즉, 이 확률은 1's-run이 있을 경우 잘못 판단하는 확률을 의미한다. 또한, 공격에 사용된 두 A^1값이 바로 직전 세션과 다음 세션의 값이 아니면 1's-run을 가지지 않는다. 그렇다고 하더라도 동일한 태그는 카운터 값의 변동이 적어 두 값의 XOR 결과는 해밍 웨이트(Hamming weight)가 작아 태그 식별 가능성은 상대적으로 매우 높다.

3.2. 악의적 랜덤 수 발생을 이용한 스푸핑 공격

이 공격에는 악의적인 리더가 보내는 랜덤 수를 위조하여 정확한 B_L 값을 태그에게 전송함으로써 정당한 리더로 가장하여 태그를 속일 수 있다.

가정 2 : 공격자는 특정한 태그의 이전 세션에서 리더가 전송한 r_p 값과 B_L 값을 알고 있다고 가정한다. 공격의 용이성을 위하여 r_p의 LSB가 0일 때 다음 세션에서 공격한다고 가정한다. ■

공격 2 : 공격자는 악의적인 리더로 가장하여 랜덤 수 $r_c = r_p + 1$와 같이 발생하여 공격하고자 하는 태그에게 보내게 된다. 즉, r_p의 LSB를 0에서 1로만 바꾸어 보낸다. 이 경우 태그는 적당한 응답을 보내게 되고 정당한 B_L이 오기를 기다리게 된다. 이때 공격자는 이전 세션에서 획득한 B_L을 보내게 된다. 태그는 B를 $h(ID \| (S \oplus GI) \| (r \oplus c))$로 계산하는데 카운터 c값이 1만큼 증가하게 되므로 이전 세션 c의 LSB가 0 이었다면 이전 세션이나 현재 세션의 $r \oplus c$ 값이 동일한 값이 되므로 B는 동일한 값으로 연산되어 리더는 이전의 B_L을 보내도 태그의 인증과정을 통과하게 된다. 따라서 성공

확률 1/2로 적법한 리더로 스푸핑 공격을 할 수 있다. ■

이외에도 문헌 [13]에서는 태그의 스푸핑 공격과 태그 ID 복구 공격 그리고 하나의 ID 공격에 의한 동일 그룹 내 ID 노출 문제 등을 지적하였다. 한편, OHLCAP은 문헌 [15]에서 위 프로토콜을 일부 수정하여 다시 제시된 바 있다. 개선된 프로토콜에서는 태그에서 A^1과 B를 계산하는 방식을 아래와 같이 변경하였다.

$$A^2=(ID\oplus r)+(GI_i\oplus r\oplus c)\bmod 2^l-1,$$

$$B=h(ID\|(S\oplus GI_i)\|(r\|c))$$

그러나 이 개선 프로토콜도 본 논문에서 제시한 공격 1을 방어할 수 없으며 공격 2를 변형하면 스푸핑 공격은 불가능하지만 위치를 추적을 할 수 있다. 즉, 공격자는 리더가 보내는 랜덤 수를 위조하여 특정 태그를 구별해 낼 수 있다.

가정 3 : 이 공격에서 공격자는 이전 세션에서 리더가 전송한 LSB가 0인 r_p 값과 A_p^2 값을 알고 있고 가정한다. ■

공격 3 : 다음 세션에서 공격자는 이 태그를 찾기 위해 리더로 가장하여 랜덤 수 $r_c=r_p+1$와 같이 발생하여 태그에게 보내게 된다. 즉, r_p의 LSB를 0에서 1로만 바꾸어 보낸 후 A_c^2를 도청하여 $A=A_p^2\oplus A_c^2$를 계산 후 이 값을 보고 동일 태그 여부를 판별한다. ■

개선된 OHLCAP에서 $A=A_p^2\oplus A_c^2$ 값은 카운터 값에 따라 달라지는데 c_p의 LSB가 0이었을 경우 A는 1이 되지만 c_p의 LSB가 1이었다면 A는 1이 되지 않는다. 따라서 공격하고자 하는 태그에 대해서는 A가 1이 될 확률은 1/2이므로 A_c^2를 도청하여 태그를 구별할 수 있다. 즉, r_p 값의 LSB가 0이었다면 특정 태그에 대해 악의적인 랜덤 수 발생으로 이전 태그임을 구별해 내는데 카운터 값의 홀·짝 수 여부에 따라 성공할 확률과 실패할 확률은 각각 1/2이다. 이 외에도 OHLCAP은 모든 태그가 동일한 공통 비밀 키 K를 사용하고 그룹 키 GI를 사용하게 됨으로써 인접 태그의 안전도에 영향을 받는 구조로 되어 있다는 점이 단점이다.

Ⅳ. 분산 환경에 적합한 RFID 인증방식 제안

4.1. 제안하는 RFID 인증 프로토콜

본 장에서는 분산 환경에 적합하면서도 데이터베이스에서 ID 검색 시간을 최소화할 수 있는 상호 인증 프로토콜을 제안하고자 한다. 제안하고자 하는 인증 프로토콜을 설계할 때 고려한 기본 조건은 아래와 같다.

① 고정 ID를 사용함으로써 분산 환경에 적합한 시스템

② 태그뿐만 아니라 DB에서도 태그를 검색하는 시간을 최소화

③ 위치 추적 공격을 비롯한 제반 공격에 대한 안전성(물리적 공격은 제외)

④ 비동기(desynchronization) 발생 시에도 동기 복구 기능

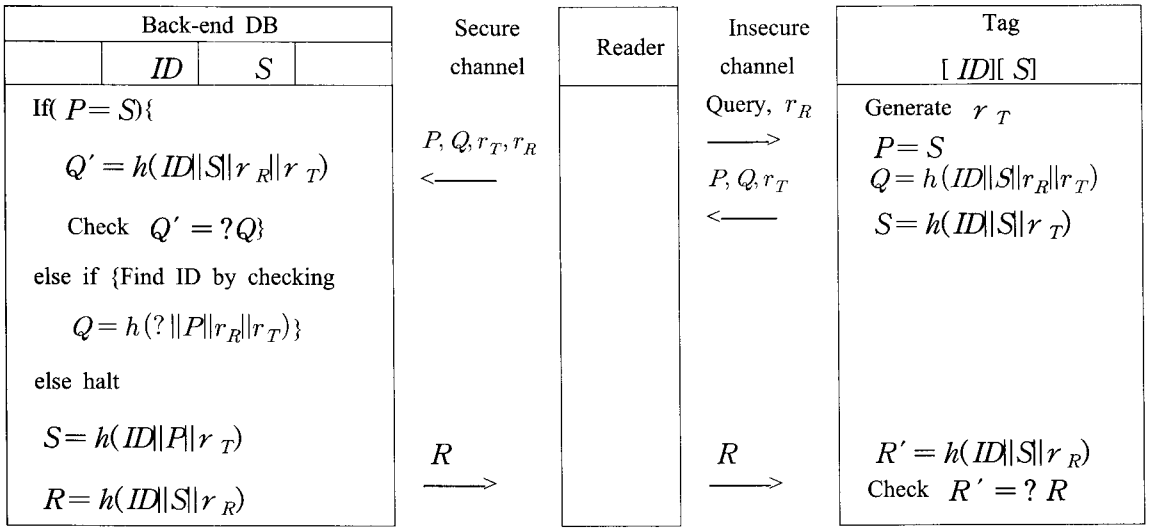
특히, 위 고려 사항 중에서 DB에서의 ID 검색 단계를 최소화할 수 있는 방법에 주안점을 두고 설계하였다. DB의 ID 검색을 최소화할 수 있는 방법의 핵심 아이디어는 다음 세션에서 태그가 보낼 메시지를 이전 세션에서 데이터베이스가 미리 저장하는 방식이다. 이전 세션에서 인증이 정확하게 이루어졌다면 다음 세션에서 태그는 이전 세션에서 저장되었던 태그 검색을 위한 정보 S를 보내고 데이터베이스는 S값의 검색을 통해 쉽게 ID를 찾도록 고안한 것이다. 즉, 다음 세션에서 데이터베이스의 ID 검색이 용이하도록 이전 세션에서 미리 동기화된 비밀 정보 S를 태그와 데이터베이스가 동시에 저장해 두는 방식이다. 또한, 제안 프로토콜에서 악의적이든 그렇지 않은 경우이든 이전 세션에서 비동기가 발생할 경우에는 리더가 보낸 정보 P, Q, r_R, r_T를 이용하여 ID를 찾고 전송된 P를 이용하여 S를 복구하도록 하였다. 이를 나타낸 것이 [그림 4]이다.

제안 프로토콜에서 태그는 사전에 ID와 자신의 비밀 키 S를 발급받아 저장해 둔다. 여기서 ID는 고정 값이지만 S는 인증 세션을 거치면서 변하는 값이다.

- 1단계 : 리더는 질의와 랜덤 수 r_R을 태그에 보낸다.

- 2단계 : 태그는 랜덤 수 r_T를 발생하고 P와 Q를 계산하여 리더에게 보내고 S를 갱신한다.

- 3단계 : 리더는 데이터베이스에 관련 정보를 안전하게 보내고 데이터베이스는 자신이 가진 S와 P를 비교하여 ID를 찾고 Q값을 검증함으로써 인증을 수행한다. 그리고 S를 갱신한 후 R을 계산하여 보낸다. 이때 이전 세션에서 동기화가 되지 않았다면 리더가 보낸 정보 P, Q, r_R, r_T를 이용하여 $Q=h(?\|P\|r_R\|r_T)$를 검사함으로써 ID를 찾아 인증을 수행한다. 즉, 전송 방해 등에



〔그림 4〕 제안하는 분산 환경에 적합한 인증 프로토콜

의해 이전 세션에서 DB에 대한 인증 과정 없음에도 태그가 무조건 S를 갱신하였다 가정하자. 그렇다면 다음 세션에서는 DB가 $Q=h(?\|P\|r_R\|r_T)$를 검사하여 ID를 찾고 동기를 복구하게 된다.

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

4.2. 제안 인증 프로토콜 분석

4.2.1 안전성

제안된 상호 인증 프로토콜의 안전성을 다음과 같이 분석하였고 분석결과를 정리한 것이 [표 1]이다.

〔표 1〕 안전성 비교 (○: 안전, ×: 불안전)

	RHAP[3]	CRAP[7]	OHLCAP[8]	제안 방식
도청 공격	×	○	○	○
재생 공격	×	○	○	○
스푸핑 공격	×	○	×	○
위치 추적 공격 (Indistinguishability)	×	○	×	○
비동기 공격	×	○	○	○
분산 환경	○	○	○	○

① 도청 공격

RHAP 프로토콜에서는 ID 값이 노출되어 도청공격에 취약하지만 나머지 방식에서는 해쉬 함수의 일방향성으로 인해 전송되는 정보로부터 ID나 비밀키 S를 계산할 수 없어 도청 공격에 안전하다. 다만 도청 정보는 직접적인 공격 수단이 아니라 다른 공격을 위한 정보 수집 차원의 공격이므로 도청에 기반한 다른 제반 공격에 주의해야 한다.

② 스푸핑 공격

제안 프로토콜에서 공격자가 올바른 리더로 가장하여 태그를 속이기 위해서는 올바른 R 값을 계산해야 하지만 ID나 비밀키 S를 알지 못하면 공격할 수 없다. 또한, 태그로 위장하고자 하는 경우에는 올바른 Q값을 전송해야 하지만 이 역시 ID나 비밀키 S를 알지 못하면 계산할 수 없어 안전하다.

③ 위치 추적

제안된 프로토콜은 매 세션마다 S값이 갱신되므로 매번 전송하는 P나 Q의 값이 랜덤하게 변경되어 이전 세션과 동일한 값을 전송하지 않는다. 따라서 공격자는 매 세션마다 나오는 정보로 위치를 추적할 수 없어 태그의 위치 프라이버시가 보장된다. 즉, 인접 태그와 혹은 이전 세션 값과의 구별 불가능성을 만족한다. 또한, 메시지 R도 역시 S와 r_R 값에 의해 매번 바뀌게 되어 위치 추적 공격은 불가능하다.

그러나 논문 [7]이나 [8]의 프로토콜이나 제안된 프

로토콜에서는 고정 ID를 사용하는데 고정 ID를 사용하는 대부분의 인증방식은 forward security를 만족하지 못한다. 이전의 모든 통신 메시지와 현재 시점에서 특정 태그의 ID와 S를 안다면 이전의 태그 위치를 추적할 수는 있다. 즉, 이전 세션에서 도청한 통신 메시지 정보(예, S, r_R, r_T, Q)를 가지고 절취한 ID값을 해쉬 함수에 입력하여 그 결과 $Q' = h(ID \| S \| r_R \| r_T)$와 도청한 Q를 비교한 후, 그 일치 여부에 따라 위치를 추적할 수 있다.

④ 비동기 공격

악의적인 공격자가 메시지 블로킹으로 정상적인 인증 과정을 방해했을 경우, 태그와 데이터베이스는 비동기 상태에 빠질 수 있다. 즉, 어떤 세션에서 태그는 S값을 갱신했지만 리더로 가는 정보가 블로킹되어 데이터베이스에서는 갱신하지 못했다고 가정하자. 그러나 이 경우에도 제안된 인증 프로토콜은 리더가 보낸 정보 P, Q, r_R, r_T를 이용하여 $Q = h(? \| P \| r_R \| r_T)$를 검사하여 ID를 찾고 전송된 P를 이용하여 S를 다시 재동기화할 수 있다. 따라서 제안된 프로토콜은 비동기 공격에도 강인하다.

⑤ 분산 환경에서의 적용

분산 환경하에서는 지역적으로 떨어져 있어 독립된 여러 대의 데이터베이스 서버를 가지고 있을 수 있다. 제안 방식의 경우 데이터베이스 A에서 인증을 수행한 태그가 데이터베이스 B가 있는 지역에 가서 인증을 수행한다고 가정하자. 이 경우 중앙 서버를 두지 않는다면 두 데이터베이스가 가지고 있는 S값이 다를 수밖에 없다. 하지만 이러한 문제 역시 위에서 언급한 비동기 공격과 동일한 상황이 되어 태그 ID를 가진 정당한 B라면 리더가 보낸 정보 P, Q, r_R, r_T를 이용하여 $Q = h(? \| P \| r_R \| r_T)$를 검사하여 ID를 찾고 S를 다시 재동기화하여 인증을 계속 수행할 수 있다.

⑥ DoS(Denial of Service) 공격

제안 프로토콜은 RHAP나 CRAP에서 가졌던 문제 중 데이터베이스에서 태그 검색 시간을 줄이는데 주안점을 두었으나 비동기화가 발생했을 때 동기를 회복하는데 걸리는 시간은 개선되지 않았다. 즉, 비동기화 발생 시 동기회복을 위해 서버에서 평균 $\lceil m/2 \rceil + 2$번의 해쉬 연산이 필요하다. 따라서 공격자가 임의의 질의만 전송하는 방법 등을 사용하여 악의적으로 대량의 비동기화를 발생시켜 DoS 공격을 할 수 있다. 이에 대한 대응책으로는 먼저 태그의 검색 시 서버의 성능을 고려하여 오버 헤드가 걸리지 않는 적당한 규모의 태그가 있는 시스템에 적용해야 하겠지만 다음과 같이 서버를 효과적으로 운영함으로써 해결할 수 있다.

첫째, 태그 규모가 큰 대형 RFID 시스템에 대한 DoS 공격에 대비하여 보안성을 해치지 않고 서버가 수용 가능한 일정한 개수의 태그를 그룹으로 묶고 태그에는 그룹 인덱스인 GI_i를 저장해 둔다. 그리고 GI_i 관련 정보를 전송함으로써 서버의 검색 범위를 줄이는 방법도 사용할 수 있다. 단, 그룹 인덱스 정보가 노출되더라도 그룹 내에 속한 태그끼리는 구별할 수 없도록 적절한 크기로 그룹화하는 것이 중요하다. 만약 그룹 인덱스 정보 노출이 안전성에 위협을 준다면 태그와 DB의 계산량은 증가하겠지만 태그가 $h(GI_i \| r_T \| r_R)$와 같은 정보를 보냄으로서 좀 더 안전하게 DoS 공격에 대비할 수도 있다.

둘째, 대형 RFID 시스템일 경우 분산 서버를 독립적으로 두어 운영한 후 정기적으로 혹은 비정기적으로 태그의 최신 S값만 메인 서버로 보내 업데이트하는 방법도 있다. 이 경우 단위 서버의 계산량을 감소시켜 DoS 공격에 대비할 수 있으며 일정 지역의 DoS 공격은 하나의 서버만 공격하므로 다른 서버에는 영향을 주지 않게 된다. 따라서 대형 태그 시스템에 대한 DoS 공격은 제안 프로토콜만으로는 완벽하게 해결할 수 없지만 그룹 인덱스를 두는 방식이나 분산 서버를 이용하여 해결할 수 있다.

4.2.2. 효율성

[표 2]는 데이터베이스와 태그에서의 연산량과 구현의 효율성을 기존 연구와 비교하여 정리한 것이다. 비교 요소는 태그와 데이터베이스에서의 연산량, 데이터 저장 공간 그리고 통신량이다. 여기에서는 m개의 태그가 있고 각 정보들은 L비트로 구성되어 있다고 가정하였다. 단, 비교하는 프로토콜들의 연산량 중에서 태그의 랜덤 수 생성에 필요한 계산량은 공통적으로 생략하였다. 그 이유는 태그에 랜덤 수 생성기를 별도로 두는 방법도 있고 논문 [7]에서 밝힌 바와 같이 해쉬 함수와 같은 방법을 이용할 수도 있지만 그 생성방법은 선택적이기 때문이다. 그러나 성능 비교 시 태그에서 랜덤 수가 필요한 프로토콜은 랜덤 수 생성을 위한 연산은 별도로 추가하여 비교해야 한다.

제안된 프로토콜은 정상적으로 인증 과정이 완료되었을 경우, 데이터베이스와 태그에서 각각 3번의 해쉬

〔표 2〕 연산량 비교
(m: DB에 저장된 ID 수, L : 데이터단위 비트)

	RHAP[3]	CRAP[7]	OHLCAP[8]	제안방식
DB 해쉬 연산	$\lceil m/2 \rceil$	$\lceil m/2 \rceil + 1$	1	3[1]
T 해쉬 연산	1	2	1	3
DB 메모리(비트)	$L \times m$	$L \times m$	$3L \times m + L$	$2L \times m$
T 메모리(비트)	L	L	$5L$	$2L$
통신량	$3L$	$4L$	$4L$	$5L$

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

연산을 수행한다. 이것은 CRAP 프로토콜이 인증을 위해 평균 $\lceil m/2 \rceil + 1$ 번의 해쉬 연산을 필요로 하는 것에 비해 상당히 효율적이다. 그러나 제안 프로토콜에서도 비동기화가 발생하면 다음 세션에서 정당한 태그를 찾아 동기를 회복하는데 평균 $\lceil m/2 \rceil + 2$번의 해쉬 연산이 필요하다.

태그는 ID을 저장하기 위한 $2L$ 비트의 저장 공간을 필요로 한다. 반면, 데이터베이스가 m개의 태그를 관리한다고 가정했을 때 데이터베이스는 $2L \times m$의 저장 공간을 필요로 한다. 그러므로 제안된 상호 인증 프로토콜은 분산 환경 하에서 제한된 메모리 공간을 지닌 RFID 시스템에 적합하고 매우 실용적이다. 인증을 위해 주고받는 통신량은 총 $5L$로서 타 방식에 비해 조금 많으나 구현 측면에서 큰 문제는 되지 않을 것으로 여겨진다.

V. 결 론

본 논문에서 분산 환경에 적합하고 RFID 시스템의 보안 요구 사항을 만족하는 효율적이고 실용적인 상호 인증 프로토콜을 제안하였다. 제안 프로토콜 설계 시 사용된 핵심 개념은 데이터베이스에서 이전 세션을 종료하기 전에 태그와 동기화된 값을 저장하도록 하여 다음 세션에서 태그 검색이 용이하도록 한 것이다. 제안 프로토콜은 태그 소유자의 위치 프라이버시가 보장되고, 스푸핑 공격 및 비동기 공격에도 강인한 특성을 지니고 있다. 특히, 데이터베이스가 분산된 환경에서 고정 ID를 사용하는 것이 효율적이나 이것 자체가 데이터베이스에서 태그 인증을 위해 많은 연산이 필요했던 기존 방식의 단점을 크게 개선하여 동기화 상태에서는 단 3번의 해쉬 연산으로 상호 인증을 수행할 수 있다.

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] International Standard ISO/IEC 18000-6: *Information technology- Radio frequency identification for item management-Part 6: Parameters for air interface communications at 860MHz to 960MHz,* 2004.

[3] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", *Security in Pervasive Computing 2003*, LNCS 2802, pp. 201-212, 2004.

[4] D. Henrici, and P. Müller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", *Proceeding of the Second*

IEEE Annual Conference on Pervasive Computing and Communication Security, pp. 149-153, 2004.

[5] 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.

[6] 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.

[7] 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.

[8] E. Choi, S. Lee, and D. Lee. "Efficient RFID Authentication Protocol for Ubiquitous Computing Environment", *EUC-2005*, LNCS 3823, pp. 945-954, Springer-Verlag, 2005.

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

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

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

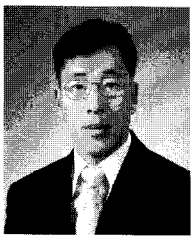
[12] 권대성, 이주영, 구본욱, "*경량 RFID 상호인증 프로토콜 LMAP, M²AP, EMAP에 대한 향상된 취약성 분석*", 한국정보보호학회논문지, 제 17권, 제 4호, pp. 103-113, 2007. 8.

[13] D. Kwon, D. Han, J. Lee, and Y. Yeom, "Vulnerability of an RFID Authentication Protocol Proposed in at SecUbiq2005", *EUC-2006*, LNCS 4097, pp. 262-270, 2006.

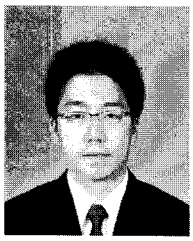
[14] A, Jules and S. A. Weis, "Defining Strong Privacy for RFID", *Cryptology ePrint Archive, Report 2006/137, Referenced 2006 at http://eprint.iacr.org,* 2006.

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

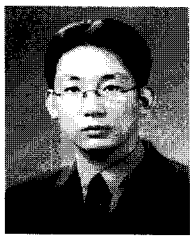
〈著者紹介〉



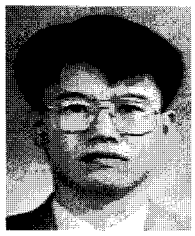
하 재 철 (JaeCheol Ha) 종신회원
1989년 2월 : 경북대학교 전자공학과 졸업
1993년 8월 : 경북대학교 전자공학과 석사
1998년 2월 : 경북대학교 전자공학과 박사
1998년 3월~2006년 1월 : 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년 3월~2007년 2월 : 나사렛대학교 정보통신학과 부교수
2006년 7월~2006년 12월 : QUT in Australia 연구 교수
2007년 3월~현재 : 호서대학교 정보호호학과 부교수
2002년 3월~현재 : 한국정보보호학회 이사
<관심분야> 정보보호,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



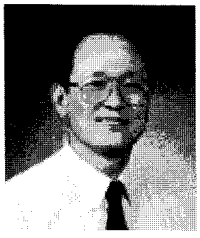
박 제 훈 (JeaHoon Park) 학생회원
2004년 2월 : 경북대학교 전자·전기공학부 졸업
2006년 2월 : 경북대학교 전자공학과 석사
2006년 3월~현재 : 경북대학교 전자공학과 박사과정
<관심분야> 정보보호, 네트워크 보안, 스마트카드 보안



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



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