저부하 및 재동기 특성을 가진 안전한 RFID 인증 프로토콜†

하정훈*, 조광현**, 하재철***, 문상재*

*경북대학교 전자공학과

**경북대학교 정보보호학과

***나사렛대학교 정보통신학과

Lightweight and Resynchronous Authentication Protocol for Secure RFID System

*JungHoon Ha, **KwangHyun Cho, ***JaeCheol Ha and *SangJae Moon

*School of Electrical Eng. & Computers Science, Kyungpook National Univ.

**Department of Information Security, Kyungpook National Univ.

***Department of Information and Communication, Korea Nazarene Univ.

요 약

RFID 시스템 상에서의 보안 문제를 해결하기 위한 다양한 노력에도 불구하고 대부분의 기존 연구들은 안전한 RFID 시스템을 위한 보안 요구 사항을 완벽하게 충족시키지 못하였다. 또한, 일부 시스템은 RFID 태그의 연산 능력만을 고려할 뿐 백엔드 데이터베이스(Back-end Database)의 연산 부하는 비교적 고려대상이 아니었다. 하지만, 실용적인 RFID 시스템 설계를 위해서는 제한된 능력을 지닌 RFID 태그뿐만 아니라 데이터베이스의 연산량 또한 고려되어야 한다. 따라서 본 논문에서는 이 두 개체의 연산 부하를 줄이기 위한 효율적인 프로토콜을 제시한다. 제안된 프로토콜은 위치 추적 방지, 데이터베이스와 태그간의 상호 인증을 보장하며 재생 공격 및 스푸핑 공격에도 강인한 특성을 지니고 있다. 특히, 통신 장애나 악의적인 공격에 의해 비동기상태가 발생할 경우에도 데이터베이스와 태그는 손쉽게 동기를 회복할 수 있다.

I. 서론

RFID(Radion Frequency Identification) 시스템은 RFID 태그라는 소형 장치를 이용하여 리더(Reader)와 태그간의 무선 통신을 통한 비접촉식 자동식별 기술로서 빠른 식별 능력, 소형화 등의 많은 장점을 가지고 있다. 이로 인해, 광학 바코드를 대체할 수단으로 인식되었고, 공급망 관리, 재고 관리 등 산업 전반에 걸쳐 현재 이용되고 있다.

그러나 태그와 리더간의 무선 통신으로 인해 태그의 정보가 쉽게 노출될 수 있고, 악의적인 공격자는 도청, 스푸핑(spoofing) 공격, 재생(replay) 공격, 비동기(desynchronization) 공격 등을 통해 태그 소유자의 개인 정보뿐만 아니라 위치를 추적할 수 있게 되었다.

따라서 이들 공격들을 막기 위한 대책으로 많은 대안이 제시되고 연구되었지만 대부분의 기존 연구들은 안전한 RFID 시스템을 위한 보안 요구 사항을 모두 만족하지는 못하였다. 또한, RFID 프로토콜 설계 시, 태그의 연산 능력을 고려할 뿐 백엔드 데이터베이스(Back-end Database)의 연산량

† 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.

은 비교적 고려 대상이 아니었다. 하지만, 실용적인 RFID 시스템을 위해서는 제한된 능력을 지닌 RFID 태그뿐만 아니라 데이터베이스의 연산량 또한 반드시 고려되어야 한다.

본 논문에서는 태그와 데이터베이스에서의 연산 부하를 줄이기 위한 효율적인 프로토콜을 제시한다. 제안된 프로토콜은 위치 추적 방지, 데이터베이스와 태그간의 상호 인증을 보장하며 재생 공격, 스푸핑 공격 및 비동기 공격에도 안전한 특성을 지니고 있다. 특히, 통신 장애나 악의적인 공격에 의해 데이터베이스와 태그간의 비동기 상태가 발생하는 경우에도 손쉽게 동기를 회복할 수 있다.

본 논문의 구성은 먼저 RFID 시스템의 구성요소와 안전한 RFID 시스템을 위한 보안 요구 사항을 정의한다. 3장에서는 기존의 인증 프로토콜 연구에 대한 기술과 더불어 문제점을 분석한다. 4장에서는 RFID 시스템을 위한 효율적인 상호 인증을 제안하고 안정성과 효율성에 대한 분석은 5장에서 제시한다. 끝으로, 6장에서는 결론을 맺는다.

II. RFID 시스템

1. 구성요소

1) RFID 태그

RFID 태그는 일반적으로 연산과 데이터 저장을 위한 마이크로 칩과 무선 통신을 위한 안테나 등으로 구성되어 있다. 전력 가동 방식에 따라 능동형과 수동형 태그로 나누어진다. 즉, 능동형 태그는 보드에 배터리가 부착되어 있는 반면, 수동형 태그는 내장된 배터리가 없으므로 리더로부터 전송되는 무선전파로부터 전력을 공급받는다.

2) RFID 리더

RFID 리더는 무선 인터페이스를 통해 태그에게 쿼리 신호를 보내고 태그로부터 수신된 정보를 데이터베이스에 전달, 데이터베이스로부터 전송된 인증 결과를 다시 태그에게 전달하는 중재자 역할을 한다. 리더로부터 태그로의 채널은 forward 채널로 정의되고, 반대로 태그로부터의 리더로의 채널은 backward 채널로 정의되며 이들 모두는 무선 통신을 기반하는 것으로 공격자의 도청이 가능한 안전하지 않는 채널이다.

3) 백엔드 데이터베이스

백엔드 데이터베이스는 리더로부터 수신된 정보를 바탕으로 태그의 인증을 담당하며 인증 후 상품 설명, 가격 등의 태그에 대한 서비스 정보를 리더에게 전송한다. 데이터베이스와 리더와의 채널은 일반적으로 안전한 채널로 규정된다.

2. 보안 요구 사항

안전한 RFID 시스템을 위해서는 다음의 공격들에 강인해야한다 [1, 2, 3].

1) 도청(Eavesdropping)

리더와 태그사이의 무선 통신으로 인해 공격자는 메시지를 도청할 수 있다. 도청한 내용을 바탕으로 공격자는 재생 공격, 스푸핑 공격 등을 시도하고 태그내의 유용한 정보나 비밀 정보 값을 알아 낼 수 있다. 따라서 RFID 시스템은 무선 통신에 의한 메시지 유출에 강인하게 설계되어야 한다.

2) 스푸핑(Spoofing) 공격

공격자는 공격 대상이 되는 태그에게 악의적인 쿼리(*Query*)를 전송함으로써 태그로부터의 응답 메시를 수집한다. 올바른 리더기를 가장하여 태그에게 쿼리를 보내고 태그로 수집된 정보를 바탕으로 차후 인증 프로토콜에 참여하여 불법적인 인증 시도를 한다. 따라서 이런 스푸핑 공격을 고려하여 RFID 시스템은 설계 되어야한다.

3) 위치 추적

위치 추적은 공격자가 태그의 위치를 파악함으로써 태그 소유자의 이동 경로를 알 수 있는 것으로 소유자의 프라이버시를 침해할 수 있다. 이런 위치 추적 방지를 위해 2가지 보안 요소를 정의한다. 첫 번째는 indistinguishability로, 이것은 어떤 특정 태그가 전송하는 메시지 값과 다른 태그와의 메시지 값을 공격자가 구분하기 힘듦을 나타내는 속성이다. 두 번째로 forward security는 태그에 저장되어 있는 비밀 데이터가 노출되더라도 공격자가 이를 이용하여 이전의 태그 위치를 추적할 수 없음을 정의한다.

4) 비동기(Desynchronization) 공격

데이터베이스와 태그간의 비동기는 시스템 통신 장애나 악의적인 공격 등으로 인해 두 개체 사이에 *ID* 업데이트가 정상적으로 이루어지지 않았을 경우 발생할 수 있다. 비동기 상태에 고착될 경우 정상적인 인증이 불가능하고 태그의 위치 추적 또한 가능할 수 있으므로 RFID 시스템은 비동기 발생 시 신속하게 재동기가 가능해야 한다.

III. RFID 인증의 기존 연구 분석

1. ID 변형 프로토콜

ID 변형 프로토콜은 Henrici와 Müller에 의해 제안된 것으로 매 세션마다 태그의 *ID*가 바뀌는 것을 특징으로 한다 [4]. 이로 인해, 재생 공격에는 안전하지만 악의적인 공격자가 올바른 리더인 척 하며 태그에게 접근하는 스푸핑 공격이 가능하다. 즉, 태그로부터 수집한 $H(ID), H(TID \oplus ID)$ 및 ΔTID 이용하여 다음 인증과정에 참가한다. 정상적인 리더로부터의 쿼리에 대한 응답으로 수집한 이들 메시지를 전송함으로써 인증 과정을 통과할 수 있다. 또한 공격자가 프로토콜의 마지막 메시지를 고의적으로 블록(blocking)할 경우, 태그는 그 메시지를 받을 수 없으므로 인증 실패로 간주하고 *ID*을 업데이트 하지 않는다. 따라서 다음 인증 세션 시에 태그는 이전 세션과 동일한 메시지 값을 전송하게 된다. 이로 인해 공격자는 태그의 위치를 추적할 수 있다.

2. 신청-응답 기반 인증 프로토콜

Rhee 등은 해쉬 함수(Hash Function)에 기반한 신청-응답(Challenge-Response) 프로토콜을 제안하였다 [5]. 그들의 프로토콜은 스푸핑 공격, 재생 공격에 강인하며 위치 추적 방지를 보장한다. 그러나 그들의 스킴(scheme)은 연산량 측면에서 비효율적이다. 즉, 백엔드 데이터베이스는 인증을 요청한 특정 태그를 찾기 위해서 데이터베이스에 저장된 모든 *ID* 값들을 비교, 해쉬 연산을 수행하는 전탐사법을 이용한다. 비록 해쉬 연산이 다른 암호학적 연산에 비해 비교적 적은 연산량을 필요로 하지만 빠른 인증을 필요로 하는 RFID 시스템에서는 적잖은 부담이 될 수 있다. 데이터베이스가 관리, 저장하는 태그의 수를 m개라 했을 때, 인증을 요청한 특정 태그의 *ID*을 찾기 위해 데이터베이스는 평균 $m/2$번의 해쉬 연산을 수행해야 한다.

3. 저비용 인증 프로토콜: LCAP

저비용 인증 프로토콜(LCAP)은 Lee 등에 의해 제안된 것으로 태그에서 단지 2개의 해쉬 연산만을 필요로 하므로 비교적 효율적이다 [6]. 그러나 안정성 측면에서, 그들의 스킴은 위치 추적에 취약한 특성을 지니고 있다. 즉, 통신 장애나 악의적인 공격에 의해 프로토콜의 마지막 메시지가 블로킹 되었을 경우, 태그는 *ID*을 업데이트 하지 않고 다음 인증 세션에 이전 세션과 동일한 메시지 값을 전송한다. 따라서 공격자는 지속적인 메시지 블로킹으로 태그 소유자의 행로를 파악할 수 있다. 특히, *ID* 업데이트 방식이 기존 *ID*와 공개되는 랜덤수와의 XOR로 이루어지므로 forward security를 만족하지 못한다.

4. 경량 신청-응답 프로토콜

최근에, Dimitriou는 경량 RFID 인증 프로토콜을 제안하였다 [7]. 그들의 스킴은 매 세션마다 업데이트 되는 비밀 값을 데이터베이스와 태그가 공유함으로써 위치 추적 방지와 태그 복제에 강인한 특성을 보인다. 그러나 악의적인 공격자에 의해 프로토콜의 마지막 메시지가 블로킹되어 태그가 그 메시지를 수신할 수 없을 경우, 태그와 데이터베이스는 비동기 상태에 빠지게 된다. 즉, 데이터베이스는 *ID*를 업데이트 하는 반면, 태그는 *ID*를 업데이트 하지 않고 다음 세션에서도 기존의 *ID*를 그대로 사용하게 된다. 공격자는 지속적인 블로킹으로 두 개체를 비동기 교착 상태에 빠뜨리고 태그의 위치를 추적할 수 있게 된다.

IV. 제안된 인증 프로토콜

이 장에서는 효율적이고 상호 인증을 보장하며 비동기 상태가 발생할 때 신속하게 재동기가 가능한 RFID 시스템에 대해 설명한다. 먼저 우리는 이 논문에서 사용되는 용어를 정의한다.

1. 용어 정의

T : RFID 태그

R : RFID 리더

DB : 백엔드 데이터베이스

ID : 태그의 고유 식별 정보, L bits

HID : *ID*의 해쉬된 값, L bits

PID : 이전 세션에 사용된 태그의 *ID*, L bits

r_R : 리더가 생성한 랜덤 수

r_T : 태그가 생성한 랜덤 수

Query : 리더에 의해 생성된 요청(Request)

SYNC : T와 DB가 동시에 *ID* 업데이트에 성공했는지를 체크하기 위한 변수

$H()$: 일방향 해쉬 함수, $H: \{0,1\}^* \rightarrow \{0,1\}^l$

$L(m)$: 입력 메시지 m의 왼쪽 반

$R(m)$: 입력 메시지 m의 오른쪽 반

$\|$: 두 입력 메시지의 연접

$=?$: 두 입력 정보의 비교

2. 시스템 모델과 가정

1) RFID 태그

T는 R의 *Query*에 대한 응답으로 *SYNC* 값에 따라 $P=H(ID)$ 또는 $P=H(ID\|r_T)$을 전송한다. 즉, 만약 시스템 통신 장애나 악의적인 공격 등으로 인해 프로토콜의 마지막 메시지를 태그가 수신하지 못하는 경우에는 *SYNC*는 1이 되고 다음 세션의 응답 값으로 $P=H(ID\|r_T)$을 전송한다. 반면에, 정상적인 인증 프로토콜이 완료된 경우에는 *SYNC* 값은 0이 되고, 다음 세션의 R로부터 온 *Query*의 응답 값으로 $P=H(ID)$을 전송한다.

2) RFID 리더

R는 자신이 생성한 랜덤 수 r_R와 함께 *Query*를 T에게 브로드캐스트하고 응답으로 T로부터 수신한 두 개의 해쉬 값과 r_T을 *DB*로 전달해주는 역할을 한다. *DB*가 T에 대한 인증을 마쳤을 경우에는 *DB*로부터 수신된 인증 결과 메시지를 T에게 전달한다.

3) 백엔드 데이터베이스

*DB*는 각 태그의 관리를 위해 *ID*, *HID* 그리고 *PID* 필드(field)를 가지고 있다. 이전 세션의 상태에 따라 *DB*는 현 세션을 위한 *ID*와 지난 세션에 해당되는 *PID*을 찾을 수 있다. 이것은 T로부터 수신하는 $P=H(ID)$ 또는 $P=H(ID\|r_T)$ 값을 데이터베이스의 *HID*, *PID* 필드내의 값들과 비교함으로써 가능하다. T을 인증한 후, *DB*는 태그의 *ID*을 업데이트하고 자신을 인증하기 위한 응답 메시지를 전송한다.

3. 프로토콜 설명

그림 1은 제안된 상호 인증 프로토콜 과정을 도식으로 보여준다.

제안된 상호 인증 프로토콜의 세부적인 절차는 다음과 같다.

i) R는 랜덤 수 r_R을 선택해서 *Query*과 함께 T에게 전송한다.

ii) T는 랜덤 수 r_T을 선택하고 *SYNC*의 값에 따라 P을 다르게 계산한다. 즉, *SYNC* 값이 0이면, $P=H(ID)$이고, 그렇지 않은 경우에는 $P=H(ID\|r_T)$이다. T는 $Q=H(ID\|r_T\|r_R)$을 계산하고 *SYNC* 값을 1로 둔다. T는 *Query*에 대한 응답으로 $L(Q), P$ 및 r_T을 R에게 전송한다.

iii) R은 T로부터 수신한 메시지, $L(Q), P$ 및 r_T을 단계 i)에서 생성한 r_R 함께 *DB*로 전달한다.

iv) *DB*는 수신한 P의 값에 따라 특정 태그의 *ID*를 찾는다. 먼저, *DB*는 수신한 $P=H(ID)$ 값을 *HID* 필드내의 값들과 비교한다. 일치되는 값이 발견될 경우 해당되는 그 *ID*가 인증을 요청한 태그의 *ID*가 된다.

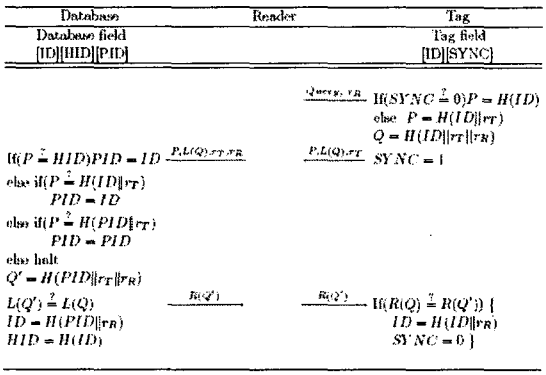

그림 1. 제안된 효율적인 상호 인증 프로토콜

한편, 일치되는 값을 발견할 수 없을 경우, 두 번째 검색과정으로 *DB*는 수신된 r_T과 *ID* 필드내의 값들을 이용해 $H(ID\|r_T)$을 계산하고 그 값을 수신한 P의 값과 비교한다. 이때 일치하는 *ID*에 해당되는 값이 인증을 요청한 태그의 *ID*가 된다. 이 경우는 이전 세션에서 R의 *Query* 에 대한 T의 응답 메시지가 공격자의 메시지 블로킹으로 인해 $P, L(Q), r_T$가 R에게 전송되지 못할 경우에 발생한다. 즉, 이전 세션에서 *DB*와 T 모두 인증 과정을 통과하지 못하고 *ID* 값을 업데이트하지 못해서 *SYNC* 값이 1인 경우이다.

위의 두 번째 경우에도 *ID*을 찾지 못하면 *DB*는 세 번째 검색과정으로 이전 세션의 태그 *ID*에 해당하는 *PID*와 수신한 r_T을 이용하여 $H(PID\|r_T)$을 계산하고 그 결과 값을 R로부터 전송된 P의 값과 일치유무를 확인함으로써 인증을 요청한 T의 *PID*을 발견하게 된다. 이 경우는 이전 세션에서 T의 응답에 대해 R의 두 번째 전송 메시지 $R(Q')$가 공격자의 메시지 블로킹으로 인해 이전 세션에서 *DB*는 *ID* 값을 갱신하지만 T는 인증 과정을 통과하지 못하고 *ID* 값을 업데이트하지

못하여 $SYNC$ 값은 1이 된 경우이다.

T의 ID 또는 PID을 찾은 DB는 태그의 인증을 위해 $Q' = H(PID \| r_T \| r_R)$와 $L(Q')$을 계산하고 다음 수식이 성립하는지 검증한다.

$$L(Q') = ?L(Q) \quad (1)$$

여기서, $L(Q)$는 R로부터 수신한 값이다. 수식 (1)이 만족되면, DB는 $R(Q')$을 계산, R에게 전송하고 ID을 업데이트 한다. 즉, $ID = H(PID \| r_R)$을 계산하고, 그 때 갱신된 T의 고유 식별 정보는 $ID = H(ID \| r_R)$이다.

v) R는 DB로부터 수신한 $R(Q')$을 T에게 전달한다.

vi) $R(Q')$의 정확성을 검증하기 위해, T는 단계 i)에서 계산된 Q 값을 이용하여 다음 수식을 통과하는지 확인한다.

$$R(Q') = ?R(Q) \quad (2)$$

수식 (2)이 통과되면 T는 자신의 고유 식별 정보를 $ID = H(ID \| r_R)$로 갱신하고 $SYNC$을 0으로 둔다.

V. 분석

1. 안정성

여기서는 제안된 상호 인증 프로토콜이 2장에서 소개된 RFID 시스템 보안 요구 사항을 만족하는지를 분석한다. 분석결과를 정리한 것이 표 1이다.

1) 도청

T의 비밀 정보를 얻기 위해서는 공격자는 도청으로 수집된 메시지들로부터 T의 ID을 복원해야 한다. 즉, $H(ID)$ 또는 $H(ID \| r_T)$로부터 공격자는 ID을 추측해야 하지만, 해쉬 함수의 일방향성 특성으로 인해 불가능하다. 공격자는 알려진 r_R 또는 r_T을 이용하여 적합한 $L(Q)$을 계산하는 공격을 수행할 수 있지만 이것 또한 해쉬 함수의 일방향성 특성으로 인해 불가능하다. 한편, 매 세션마다 ID가 갱신되므로 재생 공격도 불가능하다. 그러므로 제안된 상호 인증 프로토콜은 공격자의 도청으로 인한 공격에 강인한 특성을 보인다.

2) 스푸핑(Spoofing) 공격

공격자는 올바른 R인척하며 T의 응답 메시지를 수집한 후, T을 가장하며 인증 과정을 통과하려 한다. 하지만, T의 ID 값을 모른 채 해쉬 연산 결과 값인 P와 $L(Q)$을 계산하는 것은 해쉬 함수의 일방향성으로 인해 불가능하다. 따라서 제안된 프로토콜은 스푸핑 공격에 대해서 안전하다.

3) 위치 추적

제안된 프로토콜은 매 세션마다 ID 값이 갱신되므로 T의 위치 프라이버시가 보장된다. 즉, indistinguishability와 forward security를 만족한다. 이전 세션에서 성공적인 인증이 수행되었다고 가정하자. 현 세션의 인증을 위해서 T는 $Query$에 대한 응답으로 $H(ID)$ 값을 전송한다. 이 때 ID는 이전 세션의 성공적인 인증으로 인해 갱신된 값으로 $H(ID)$는 이전 세션의 해쉬 결과와는 다른 값을 가진다. 한편, 통신 장애, 공격자의 악의적인 메시지 블로킹 등으로 인해 비정상적으로 프로토콜이 완료되었을 경우, T는 $Query$에 대한 응답으로 $H(ID \| r_T)$을 전송한다. 비록 ID가 갱신되지 않더라도 r_T이 포함된 해쉬 값이 전송되므로 이전 세션의 응답과는 다른 해쉬 값이 전송된다. 즉, 프로토콜의 정상/비정상적인 인증 결과에 상관없이 indistinguishability를 만족한다.

제안된 프로토콜은 ID가 $H(ID \| r_R)$ 형태로 구성되어 있으므로 forward security를 만족한다. 즉, ID가 노출되더라도 그 이전의 $H(ID \| r_R)$에 해당되는 ID 값은 복원할 수 없다. 이것은 해쉬 함수의 일방형성 특성에 기인한다.

4) 비동기(Desynchronization) 공격

악의적인 공격자가 메시지 블로킹으로 정상적인 인증 과정을 방해했을 경우, T와 DB는 비동기 상태에 빠질 수 있다. 즉, 프로토콜의 두 번째 응답 메시지를 고의적으로 끊어 DB로 전달되는 메시지를 차단했을 경우, DB와 T는 모두 ID 업데이트에 실패하게 된다. 다음 세션의 인증 과정 시 T는 $H(ID \| r_T)$을 전송하더라도 DB는 ID필드를 통해 ID 값을 찾고 이후 업데이트를 수행한다. 한편, 공격자가 프로토콜의 마지막 단계인 T로 전송되는 메시지를 블로킹 했을 경우, DB는 ID 업데이트를 수행하지만 T는 그렇지 않다. 이 경우, 비동기가 발생하지만 다음 세션의 인증에서 DB는 PID 필드를 통해 ID 값을 손쉽게 발견, 이후 재동기가 가능하다. 따라서 제안된 프로토콜은 비동기 공격에도 강인하다.

표 1. 안전성 비교 (O: 안전, ×: 불안전)

	Henrici [4]	Rhee [5]	Lee [6]	Dimitriou[7]	제안된 스킴
재생 공격	O	O	O	O	O
스푸핑 공격	×	O	×	O	O
Indistinguishability	×	O	×	×	O
Forward security	×	×	×	O	O
비동기 공격	O	O	O	×	O
ID 갱신	O	×	O	O	O

2. 효율성

제안된 프로토콜의 효율성 정도를 분석하기 위해 우리는 앞서 소개된 기존 연구와의 연산량을 비교한다. 즉, 표 2는 *DB*와 *T*에서의 연산량을 기존 연구와 비교한 것이다. 제안된 프로토콜은 정상적으로 인증 과정이 완료되었을 경우, *DB*와 *T*에서 각각 3번의 해쉬 연산을 수행한다. 그러나 비동기 상태에서는 m번의 해쉬 연산을 필요로 한다. 이것은 Rhee의 프로토콜이 인증을 위해 $m/2+2$ 번의 해쉬 연산을 필요로 하는 것에 비해 상당히 효율적이다. *T*는 *ID*을 저장하기 위한 L 비트와 *SYNC* 위한 1 비트, 총 $L+1$ 비트의 저장 공간을 필요로 한다. 반면에, *DB*가 m개의 *T*을 관리한다고 가정했을 때 *DB*는 $3L \times m$의 저장 공간을 필요로 한다. 또한, 본 프로토콜은 무선 채널상의 통신량도 고려하여 설계되었다. 즉, 통신량을 줄이기 위해 *T*는 $L(Q)$을 전송하고 *R*는 $R(Q)$을 전송한다. 따라서 *T*에서 *R*로 전송되는 통신량은 $2.5L$이고 *R*에서 *T*로 전송되는 통신량은 $0.5L$이다. 그러므로 제안된 상호 인증 프로토콜은 제한된 메모리 공간을 지닌 RFID 시스템에 적합하고 실용적이다.

VI. 결론

우리는 본 논문에서 RFID 시스템의 보안 요구사항을 만족하면서 효율적이고 실용적인 상호 인증 프로토콜을 제안하였다. 태그 소유자의 위치 프라이버시가 보장되고 재생 공격, 스푸핑 공격 및 비동기 공격에도 강인한 특성을 지니고 있다. 특히, 통신 장애나 악의적인 공격에 의해 인증 과정이 비정상적으로 종료되었을 경우에도 태그와 데이터베이스 간에 동기 복구가 가능하다.

표 2. 연산량 비교 (m: *DB*에 저장된 *ID*의 수)

	Henrici [4]	Rhee [5]	Lee [6]	Dimitriou[7]	제안된 스킴
*DB*의 해쉬 연산	3	$m/2+2$	2	4	3
*T*의 해쉬 연산	3	2	2	4	3
*DB*의 메모리(비트)	$8L \times m$	$1L \times m$	$6L \times m$	$2L \times m$	$3L \times m$
*T*의 메모리(비트)	$3L$	$1L$	$1L$	$1L$	$1L+1$

참고문헌

[1] A. Juels. "RFID Security and Privacy: A Research Survey," *RSA Laboratories*, 2005.

[2] S. Lee, T. Asano and K. Kim. "RFID Mutual Authentication Scheme based on Synchronized Secret," Information. *In proceedings of the SCIS'06*, 2006.

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

[4] D. Henrici and P. Muller. "Hash-based Enhancement of Location Privacy for Radio Frequency Identification Devices using Varying Identifiers," *In proceeding of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp. 149-162, IEEE, 2004

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

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