논문 2009-46CI-5-7

TRMA: 2-라운드 RFID 상호 인증 프로토콜

(TRMA: Two-Round RFID Mutual Authentication Protocol)

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

RFID 시스템에서는 리더와 태그간의 통신이 안전하지 않은 채널에서 수행되므로 전송되는 데이터가 공격자에 의해 쉽게 도청당하고, 위조될 수 있다. 그러므로 인증은 안전성과 프라이버시를 제공하기 위해 RFID 애플리케이션에서 중요한 역할을 한다. 2006년에 Lee, Asano 그리고 Kim은 해쉬 함수와 동기화된 비밀 정보를 이용하여 RFID 상호 인증 프로토콜인 LAK 프로토콜을 제안하였다. 그러나 Cao와 Shen은 LAK 프로토콜이 재전송 공격에 취약하고 공격자가 태그를 위조할 수 있다고 증명하였다. 본 논문에서는 안전한 일방향 해쉬 함수를 기반으로 하는 간단한 2-라운드 RFID 상호 인증 프로토콜인 TRMA 프로토콜을 제안한다. 제안한 TRMA 프로토콜은 다양한 공격들에 대해 안전할 뿐만 아니라 RFID 태그와 리더 간의 통신을 2-라운드만 수행하여 안전한 상호 인증을 하고, 높은 통신 효율성도 제공한다.

Abstract

In RFID system, the communicated data can be easily eavesdropped and tampered with by an attacker because the communication between the reader and the tag is performed in an insecure channel. Therefore, authentication is an important role in RFID applications for providing security and privacy. In 2006, Lee, Asano and Kim proposed an RFID mutual authentication protocol (the LAK protocol) which utilizes a hash function and synchronized secret information. However, Cao and Shen showed that the LAK protocol is vulnerable to replay attack, and therefore an adversary can impersonate the tag. This paper proposes a new simple two-round RFID mutual authentication (TRMA) protocol based on secure one-way hash function. As a result, the proposed TRMA protocol not only can prevent various attacks and but also provides communication efficiency since they mutually authenticate by performing two-round between RFID tag and RFID reader.

Keywords : RFID, 상호 인증, 프로토콜, 해쉬 함수, 유비쿼터스

I. 서 론

유비쿼터스 컴퓨팅(Ubiquitous Computing) 네트워크 환경에서 RFID(Radio Frequency IDentification) 기술은 NFC(Near Field Communication) 통신 기술들 중에서 가장 전도유망한 기술 중의 하나이다. RFID 시스템은 개체 추적과 모니터링, 티켓팅, 공급 망 관리, 비 접촉식 지불 시스템과 같은 IT 애플리케이션 산업에서 엄청난 생산성 편의와 이익을 창출한다[1].

RFID 시스템은 태그(Tag), 리더(Reader), 그리고 백-엔드 데이터베이스(Back-end Database) 세 가지 요소로 구성된다. RFID 시스템에서의 태그와 리더 간의 통신은 안전하지 않은 채널에서 수행되므로 전송되는 데이터는 공격자에 의해 쉽게 도청당하고 위조될 수 있다. 그러므로 인증은 안전성과 프라이버시를 제공하기 위해 RFID 애플리케이션에서 중요한 역할을 한다[2~5, 10].

* 학생회원, 대구대학교 교양대학
(College of General Education, 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, 대구대학교 컴퓨터·IT공학부
(School of Computer & Information Technology, Daegu University)
접수일자: 2009년4월10일, 수정완료일: 2009년9월4일

인증(Authentication)은 통신 상대자의 식별을 요구할 때 합법적인지 여부를 증명하는 것을 의미한다. 만약 RFID 시스템에서 RFID 태그가 어떠한 인증도 수행하지 않고 리더에게 자신의 유일한 식별자 정보를 알려주게 되면 스푸핑 공격, 개인 정보 누출, 개체의 위치 트래킹 공격 등과 같은 다양한 프라이버시 침해 문제를 유발시킬 것이다[4~6, 10].

일반적으로 RFID 태그는 제한된 연산과 메모리 자원을 가지고 있는 저비용이므로 대칭 키 알고리즘과 공개 키 알고리즘과 같은 표준 동기화 연산은 수행할 수 없다. 따라서 대부분의 RFID 프로토콜들은 효율성과 안전성을 동시에 제공하기 위해서 해쉬 함수(Hash Function)와 난수 생성기(Random Number Generator)를 기반으로 한다[7~23].

2006년에 Lee, Asano 그리고 Kim은[8] 해쉬 함수와 동기화된 비밀 정보를 이용하여 RFID 상호 인증 프로토콜인 LAK 프로토콜을 제안하였다. Chien과 Huang[9]도 난수 생성기를 기반으로 Lee 등이 제안한 LAK 프로토콜과 유사한 경량 RFID 인증 프로토콜을 제안하였다. 하지만 Cao와 Shen[10]은 LAK 프로토콜이 재전송 공격이에 취약하며, 공격자가 합법적인 태그로 위조할 수 있음을 증명하였다. 즉, 공격자는 리더와 태그 간의 통신을 도청하여 나중에 재전송 공격을 수행할 때 인증 정보를 복사할 수 있음을 증명하였다.

현재까지 제안된 많은 RFID 인증 프로토콜들은 RFID 태그와 리더 간의 상호 인증을 제공하기 위해서 3-라운드(Three-Round) 통신 모델을 기반으로 한다. 만약 동일한 보안성과 통신 효율성을 제공하는 2-라운드(Two-Round) 기반의 RFID 상호 인증 프로토콜을 구현할 수 있다면, 경량 RFID 프로토콜을 기반으로 다양한 애플리케이션에서 더욱 효율적으로 사용될 수 있을 것이다. 따라서 본 논문에서는 위와 같은 연구 동기를 기초로 안전한 일방향 해쉬 함수 기반의 새로운 간단한 2-라운드 RFID 상호 인증 프로토콜인 TRMA를 제안한다. 제안한 TRMA 프로토콜은 RFID 태그와 리더 간의 통신을 2-라운드만 수행하여 안전한 상호 인증을 하기 때문에 여러 공격에도 보호될 뿐만 아니라 기존 기법들과 비교하여 통신 효율성 면에서도 우수하다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 관련연구로서 RFID 시스템과 RFID 상호 인증 프로토콜에 필요한 보안 요구사항에 대하여 기술하고, Ⅲ장에서는 LAK-RFID 상호 인증 프로토콜에 대하여 간단하게 재검토한다. Ⅳ장에서는 제안한 2-라운드 RFID 상호 인증 프로토콜인 TRMA 프로토콜에 대해 기술하고, Ⅴ장에서는 보안성 분석, Ⅵ장에서는 효율성 분석에 대해 각각 토의한다. 마지막 Ⅶ장에서는 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 RFID 시스템과 RFID 상호 인증 프로토콜이 충족해야 할 보안 요구사항 및 본 논문에서 사용되는 용어들에 대해 설명한다.

1. RFID 시스템

RFID 시스템은 RFID 태그(Tag), RFID 리더(Reader), 백-엔드 데이터베이스(Back-end Database)인 세 가지 컴포넌트로 구성된다[2, 10]. 그림 1은 RFID 시스템의 구조를 보여준다.

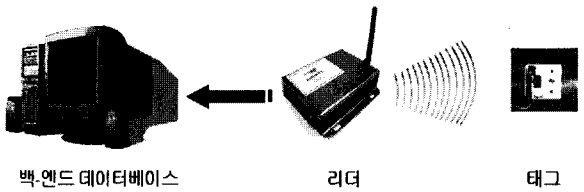

그림 1. RFID 시스템 구조
Fig. 1. Architecture of RFID system.

(1) RFID 태그

RFID 시스템에서 하나의 개체에 부착되어 있는 식별 장치로서, 리더가 질의하면 태그는 자신에게 저장된 식별정보인 ID를 안전하지 않은 무선 통신 채널을 통해 리더에게 전송한다.

(2) RFID 리더

RFID 태그와 통신하는 장치로서 리더가 태그에 질의하여 수집된 정보를 백-엔드 데이터베이스에게 전송한다. 리더는 소형 단말기 또는 고정된 장치일 수 있다.

(3) 백-엔드 데이터베이스

RFID 태그와 연관된 제품 정보, 트래킹 로그 또는 키 관리 정보를 레코드 형태로 저장한다. 정당한 리더로부터 수신된 임의의 태그에 관한 정보를 이용하여 해당 태그의 정당성을 식별하는 기능을 수행한다.

2. 보안 요구사항

RFID 태그가 어떠한 인증도 없이 RFID 리더에게 자신의 유일한 식별자 정보를 알려주면 스푸핑 공격, 재전송 공격, 상호 인증, 개인 정보 누출, 개체의 위치 트래킹 공격과 같은 프라이버시 문제를 발생시킬 것이다[3~6]. 따라서 RFID 시스템은 다음과 같은 보안 문제점들을 고려하여 설계되어야 한다.

(1) 스푸핑 공격

공격자가 정당한 태그로 위장하여 리더에게서 인증에 필요한 정보를 획득하고, 정당한 리더나 태그로 인증 받는 공격을 의미한다.

(2) 재전송 공격

스푸핑 공격의 일종으로 이전에 태그와 리더 사이의 전송된 메시지를 재전송함으로써 공격자가 태그를 위조한다.

(3) 상호 인증

클라이언트와 서버 둘 다 같은 프로토콜 내에서 서로 인증되는 것을 의미한다.

(4) 정보 누출

개체에 부착된 태그의 비밀 정보를 어떤 공격자에 의해 해독될 수 있는 것을 말한다.

3. 용어 정의

본 논문에서 사용할 용어들의 표기법 및 정의는 표 1과 같다.

표 1. 용어 정의
Table 1. Notations.

기호	의 미
T	RFID 태그
R	RFID 리더
DB	백-엔드 데이터베이스(Back-End Database)
$query$	태그의 응답을 요청하는 리더의 요청
k	태그 T의 현재 비밀 값
$klast$	태그 T의 이전 비밀 키
K	DB 내의 태그 T에 대한 현재 비밀 값의 필드
$Klast$	DB 내의 태그 T에 대한 이전 비밀 값의 필드
TID	태그 T의 아이디 값
RID	리더 R의 아이디 값
$TIDS$	DB 내의 태그 T에 대한 식별 필드
$Data$	DB 내의 태그 T에 대한 제품 정보 필드
$h(\cdot)$	안전한 일방향 해쉬 함수(Secure One-Way Hash Function)
$PRNG$	의사난수생성기(Pseudo Random Number Generator)
N_R	리더가 생성한 난수
N_T	태그가 생성한 난수
$\oplus$	배타적 논리합(XOR; eXclusive OR) 연산
$\|$	연접(Concatenation) 연산

III. LAK-RFID 상호 인증 프로토콜

본 장에서는 Lee, Asano 그리고 Kim이 제안한 LAK-RFID 상호 인증 프로토콜에 대해 간단하게 검토해 본다[8]. 그림 2는 LAK 프로토콜의 처리 과정을 보여주고, 각 단계별로 상세한 설명은 다음과 같다.

Step 1. 리더 R은 난수 생성기를 사용하여 난수 N_R을 생성하고, 태그에게 전송한다.

Step 2. 리더로부터 난수 N_R 값을 수신한 태그는 난수 N_T를 생성하고, $c1 = h(N_t \oplus k \oplus N_R)$을 계산한다. 태

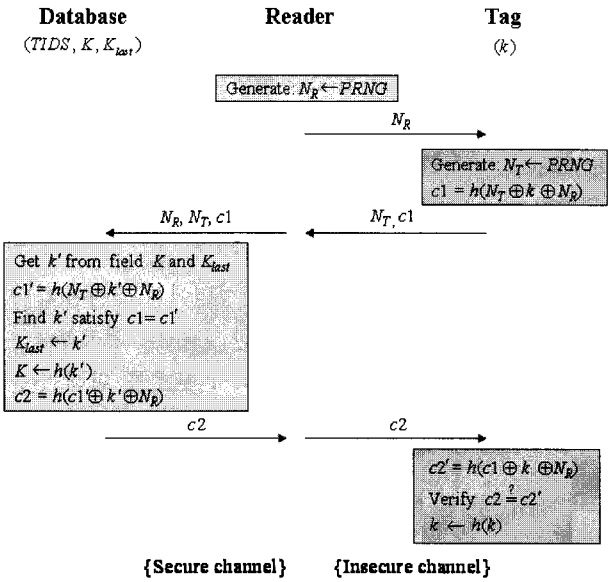

그림 2. LAK-RFID 상호 인증 프로토콜
Fig. 2. LAK-RFID mutual authentication protocol.

그는 리더에게 $\{N_T, c1\}$을 전송한다.

Step 3. 리더는 태그로부터 수신한 메시지에 자신이 생성한 난수와 함께 $\{N_T, c1, N_R\}$을 DB로 전송한다.

Step 4. DB는 리더로부터 $\{N_T, c1, N_R\}$을 수신하고, 태그의 식별자를 찾기 위해 태그의 현재 비밀 값 필드와 이전 비밀 값 필드로부터 태그의 현재 비밀 값인 k'을 가져온다. 수신한 N_T와 N_R을 이용하여 $c1' = h(N_t \oplus k' \oplus N_R)$을 계산하고, $c1 = c1'$을 만족하는 k'을 찾게 되면 DB는 태그와 리더를 인증하고, k'은 이전 비밀 값 필드 K_{last}에 $h(k')$은 현재 비밀 값 필드 K에 복사된다. 마지막으로 DB는 $c2 = h(c1' \oplus k' \oplus N_R)$을 계산하고, $c2$를 리더에게 전송한다. 만약 k'을 DB 내의 현재 비밀 값의 필드 K가 아닌 이전 비밀 값의 필드 K_{last}에서 찾았다면, DB는 정보를 업데이트 하지 않고, 통신을 중단한다.

Step 5. 리더는 $c2$를 태그에게 전송한다.

Step 6. 리더로부터 $c2$를 수신한 태그는 자신이 저장하고 있던 $c1$과 N_R을 사용하여 $c2' = h(c1 \oplus k \oplus N_R)$을 계산한다. 태그는 $c2 = c2'$가 일치하는지 검사하고, 일치하면 태그는 리더와 인증하고, k를 $h(k)$로 갱신한다.

Ⅳ. 제안한 TRMA 프로토콜

본 장에서는 안전한 일방향 해쉬 함수 기반의 새로운 간단한 2-라운드 RFID 상호 인증 프로토콜인 TRMA 프로토콜을 제안한다. 제안한 TRMA 프로토콜은 RFID 태그와 리더 간의 2-라운드만을 수행하여 상호 인증을 성취하기 때문에 여러 공격에도 안전할 뿐만 아니라 기존 기법들과 비교하여 통신 효율성면에서도 우수하다. 저비용 RFID 태그를 위해 제안한 TRMA 프로토콜은 태그의 위조를 방지하고, 프라이버시 보호를 위해 단순한 XOR 알고리즘과 안전한 일방향 해쉬 함수를 사용한다. 태그는 태그와 리더 둘 다에 저장된 자신들의 리더 식별자(ID)에 의해 검증된 리더들의 식별이 가능하도록 하기 위해서 태그의 메모리에 사전에 검증된 리더의 식별자(ID)를 저장하는 것이 중요하다.

제안한 TRMA 프로토콜에서는 백-엔드 데이터베이스, 리더 그리고 태그는 XOR 연산과 일반적인 일방향 해쉬 함수인 $h(\bullet): \{0,1\}^* \rightarrow \{0,1\}^1$을 수행한다. 리더와 태그는 각각 난수 생성기를 가지고 있다. 128비트 크기인 두 개의 비밀 값인 리더 식별자와 태그 식별자는 태그의 비휘발성 메모리에 저장되어 있다. 리더 식별자는 리더를 식별하기 위해 사용되고, 태그 식별자는 태그를 식별하기 위해 사용된다. 그리고 백-엔드 데이터베이스는 RFID 태그 식별자와 각 태그의 제품 정보를 저장하고 있는 태그 식별자들의 필드와 데이터를 가지고 있다. 태그 식별자와 각 태그의 데이터를 초기 정보로 각각 설정한다.

그림 3은 제안한 TRMA 프로토콜의 처리 과정을 보여주며 각 단계별로 상세한 설명은 다음과 같다.

Step 1. 리더는 128비트 난수 N_R을 생성하고, $c1 = RID \oplus N_R$, $c2 = h(RID \| N_R)$을 계산한다. 리더는 태그에게 $\{query, c1, c2\}$를 전송한다.

Step 2. 리더로부터 $\{query, c1, c2\}$를 수신한 태그는 다음과 같이 태그에 미리 저장된 $c1$과 RID를 XOR 연산을 수행하여 난수 N_R을 찾아낸다.

$$c1 \oplus RID = RID \oplus N_R \oplus RID = N_R$$

태그는 N_R과 RID를 이용하여 $c2 = h(RID \| N_R)$을 계산하고, $c2 = c2'$를 검사한다. 만약 $c2$와 $c2'$가 일치한다면 태그는 리더를 인증한다. 그러면 태그는 128비트 랜

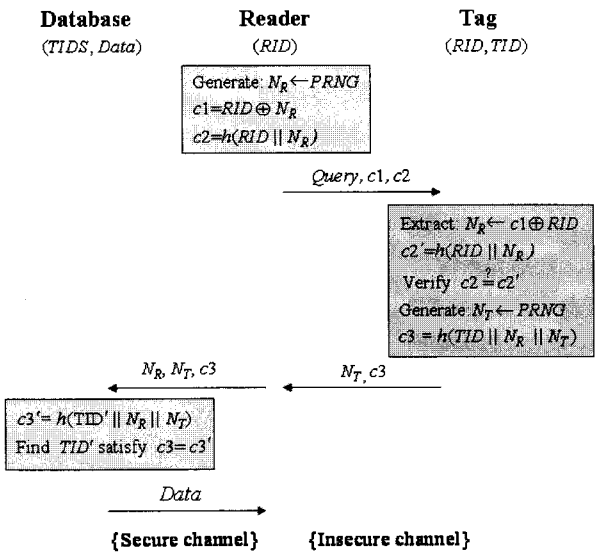

그림 3. 제안한 TRMA 프로토콜
Fig. 3. Proposed TRMA protocol.

덤 난수 N_T를 생성하고, $c3 = h(TID \| N_R \| N_T)$를 계산한다. 마지막으로 태그는 $\{N_T, c3\}$을 리더에게 전송하고, $c2$와 $c2'$가 일치하지 않는다면 통신을 중단한다.

Step 3. 리더는 태그로부터 수신한 메시지에 난수 N_R을 붙여서 $\{N_T, c3, N_R\}$을 DB로 전송한다.

Step 4. DB는 리더로부터 $\{N_T, c3, N_R\}$을 수신하고, 태그의 식별자를 찾기 위해 $c3' = h(TID' \| N_R \| N_T)$를 계산하고, $c3 = c3'$을 만족하는 DB내의 태그 식별자 필드를 검색한다. 만약 DB가 일치된 태그 식별자를 찾는다면, 태그와 리더를 인증하고, 리더에게 데이터를 전송한다. 일치된 태그 식별자를 찾지 못하면 DB는 통신을 중단한다.

Step 5. 리더는 수신된 데이터로부터 필요한 제품 정보를 사용한다.

V. 안전성 분석

본 장에서는 제안한 TRMA 프로토콜의 안전성에 대해 분석한다. 프로토콜 분석에서 필요로 하는 안전성[24]은 다음과 같이 정의된다.

[정의 1]. 리더와 태그의 강력한 비밀 키들 (RID, TID)은 다항식에서 추측될 수 없는 높은 엔트로피 $S(K)$ 값이다.

[정의 2]. 안전한 일방향 해쉬 함수 $y = h(x)$에서 주어진 x로 y를 계산하는 것은 쉽고, 주어진 y로 x를 계산하는 것은 어렵다.

위에서 정의된 것을 고려하여 다음과 같은 이론들이 제안한 TRMA 프로토콜의 안전성 분석에 사용된다.

[정리 1]. 제안한 TRMA 프로토콜은 스푸핑 공격에 안전하다.

증명 : 태그와 백-엔드 데이터베이스 사이에서의 상호 비밀 키 값인 태그 식별자 TID는 스푸핑 공격을 예방할 때 사용된다. 비합법적인 공격자는 상호 비밀 키인 태그 식별자 TID를 가지고 있지 않으므로 인증을 하기 위해 태그나 백-엔드 데이터베이스를 위조할 수 없다. 또한 리더와 태그 사이에서의 상호 비밀 키 값인 리더 식별자 RID도 스푸핑 공격을 예방할 때 사용된다. 비합법적인 공격자는 상호 비밀 키인 리더 식별자 RID를 가지고 있지 않으므로 인증을 하기 위해 리더나 태그를 위조할 수 없다. 따라서 제안한 TRMA 프로토콜은 스푸핑 공격에 안전하다.

[정리 2]. 제안한 TRMA 프로토콜은 재전송 공격에 안전하다.

증명 : 공격자가 리더로부터 $c1 = RID \oplus N_R$과 $c2 = h(RID \| N_R)$를 가로채고, 리더로 위장한다고 가정하자. 그러나 공격자는 $c3 = h(TID \| N_R \| N_T)$를 정확하게 계산할 수 없거나 비밀 키 값을 정확하게 예측하지 못하고 전송하게 된다. 비록 공격자가 태그의 검증 절차를 통과할 수 있다 할지라도 리더와 백-엔드 데이터베이스 사이에서는 안전한 채널 상에서 인증 단계들이 수행되므로 검증 절차를 통과할 수 없다. 따라서 공격자는 재전송 공격에 성공할 수 없다. 반면에 공격자가 태그로부터 난수 값 N_T와 $c3 = h(TID \| N_R \| N_T)$를 가로채고, 태그로 위장한다고 가정하자. 같은 이유로 공격자는 $c1 = RID \oplus N_R$로부터 정확한 난수 값 N_R을 얻지 못한다면 백-엔드 데이터베이스는 리더에게 데이터를 전송할 수 없을 것이다. 따라서 제안한 TRMA 프로토콜은 재전송 공격에 안전하다.

[정리 3]. 제안한 TRMA 프로토콜은 상호 인증을 제공한다.

증명 : 제안한 프로토콜의 Step1에서 합법적인 리더만이 $c1 = RID \oplus N_R$과 $c2 = h(RID \| N_R)$를 계산할 수 있기 때문에 태그는 $c2 ? = c2'$을 검사하여 리더를 인증할 수 있다. Step 4에서도 합법적인 태그만이 $c3 = h(TID \| N_R \| N_T)$를 계산할 수 있으므로 백-엔드 데이터베이스가 $c3 ? = h(TID' \| N_R \| N_T)$를 검사하여 태그를 인증할 수 있다. 따라서 제안한 TRMA 프로토콜은 상호 인증을 제공한다.

[정리 4]. 제안한 TRMA 프로토콜은 정보 누출을 방지한다.

증명 : 공격자가 Step 1에서 리더로부터 $c1 = RID \oplus N_R$

과 $c2 = h(RID \| N_R)$을 가로채고, Step 2에서는 태그로부터 난수 값 N_R과 $c3 = h(TID \| N_R \| N_T)$를 가로챈다고 가정하자. 그러나 공격자는 $c1$, $c2$, $c3$으로부터 리더 식별자인 RID 값을 얻을 수 없다. 즉, 난수 N_R을 알지 못한다면 공격자는 $c1$으로부터 정확한 리더 식별자인 RID 값을 추출할 수 없다. 또한 안전한 일방향 해쉬 함수의 정의 2에 따라 공격자는 $c2$와 $c3$으로부터 리더 식별자 RID 값과 태그 식별자 TID 값을 얻을 수 없다. 따라서 제안한 TRMA 프로토콜은 정보 누출에 안전하다.

[정리 5]. 제안한 TRMA 프로토콜은 위치 트래킹 공격에 안전하다.

증명 : 위치 트래킹 공격은 공격자가 개체에 부착된 특별한 태그의 위치를 추적하는 것을 말한다. 제안한 프로토콜에서 난수와 태그 식별자 TID에 의해 계산된 해쉬 값 $c3 = h(TID \| N_R \| N_T)$는 각 세션마다 항상 변하기 때문에 공격자는 특별한 RFID 태그를 인증하기 위해 위치 트래킹 공격을 수행할 수 없다. 따라서 제안한 TRMA 프로토콜은 태그의 프라이버시가 안전한 일방향 해쉬 함수에 의해 보호되기 때문에 위치 트래킹 공격에 안전하다.

VI. 효율성 분석

본 장에서는 제안한 TRMA 프로토콜의 효율성을 분석한다. 표 2는 제안한 TRMA 프로토콜과 LAK 프로토콜의 효율성을 비교 및 분석한 표이다.

LAK 프로토콜의 DB 측에서는 $n+2$번의 해쉬 연산과 $2n+2$번의 XOR 연산이 요구되지만 제안한 TRMA 프로토콜은 n번의 해쉬 연산만 요구된다. 그러므로 제안한 TRMA 프로토콜이 LAK 프로토콜보다 훨씬 효율적이라는 것을 알 수 있다. LAK 프로토콜의 리더 측에서는 1번의 난수 생성 연산을 하고, 제안한 TRMA 프로토콜은 1번의 해쉬 연산, 1번의 XOR 연산, 1번의 난수 생성 연산을 한다. 그러나 리더는 태그보다 훨씬 더 강력하므로 리더는 1번의 해쉬 연산과 1번의 XOR 연산을 쉽게 수행할 수 있다. 또한 LAK 프로토콜의 태그 측에서는 3번의 해쉬 연산, 4번의 XOR 연산 그리고 1번의 난수 생성 연산을 수행하지만, 제안한 TRMA 프로토콜은 2번의 해쉬 연산, 1번의 XOR 연산 그리고 1번의 난수 생성 연산을 한다. 따라서 제안한 TRMA 프로토콜이 LAK 프로토콜보다 훨씬 더 효율적이라는 것을 증명하며, 제안한 TRMA 프로토콜이 경량 RFID 시스템에 더 쉽게 채택될 수 있다. 또한, 제안한 TRMA 프로토콜은 LAK 프로토콜과는 달리 더 적은 수의 통신 라운드를 사용한다. 위와 같은 이유로 본 논문에서 제안한 TRMA 프로토콜이 LAK 프로토콜보다 효율성 면에서도 훨씬 더 우수함을 명백하게 보여준다.

표 2. 효율성 분석
Table 2. A Comparison of efficiency.

	LAK 프로토콜[8]			제안한 TRMA 프로토콜		
	DB	리더	태그	DB	리더	태그
해쉬 연산	n+2	0	3	n	1	2
XOR 연산	2n+2	0	4	0	1	1
랜덤 값	0	1	1	0	1	1
통신 라운드 수	5			4		

n : 백-엔드 데이터베이스에 저장된 태그수

VII. 결 론

본 논문에서는, 안전한 일방향 해쉬 함수 기반의 새로운 2-라운드 RFID 상호 인증 프로토콜인 TRMA 프로토콜을 제안하였다. 제안한 프로토콜은 RFID 태그와 리더 간에 2-라운드 통신만을 수행하여 상호 인증을 수행하기 때문에 3-라운드를 요구하는 LAK 프로토콜과 비교하여 높은 통신 효율성을 제공할 뿐만 아니라, RFID 시스템 상에서 발생할 수 있는 다양한 공격들에 대해서도 안전하기에 RFID 기반 유비쿼터스 응용 환경에 효율적이고 안전하게 사용되어 질 수 있다.

참 고 문 헌

[1] D. Lin, H. G. Elmongui, E. Bertino, and B. C. Ooi, "Data management in RFID applications", International conference on database and expert systems applications, LNCS 4653, pp. 434-444, 2007.

[2] K.Finkenzeller, "RFID handbook: fundamentals and applications in Contactless smart cards and identification", (2nd ed.), Munich, Germany: Wiley, 2003.

[3] S. Garfinkel and B. Rosenberg, "RFID applications, security, and privacy", Boston, USA: Addison-Wesley, 2005.
[4] L.Srivastava, "Ubiquitous network societies: The case of Radio Frequency Identification, background paper", International telecommunication union (ITU)new initiatives workshop on ubiquitous network societies, Geneva, Switzerland, 2005.
[5] S.Shepard, "RFID: Radio Frequency Identification", New York, USA: Mc Graw Hill, 2005.
[6] S. A. Weis, S. E. Sarma, and R. L. Rivest, "Security and privacy aspects of low-cost Radio Frequency Identification systems", Proceedings of first international conference on security in pervasive computing. 2003.
[7] Y. C. Chen, W. L. Wang, and M. S. Hwang, "Low-cost RFID authentication protocol for anti-counterfeiting and privacy protection", Asian journal of health and information sciences, Vol. 1, No. 2, pp. 189-203, 2006.
[8] S. Lee, T. Asano, and K. Kim, "RFID mutual authentication scheme based on synchronized secret information", In proceedings of the SCIS'06, 2006.
[9] H. Y. Chien and C. W. Huang, "A lightweight RFID protocol using substring", EUC 2007, LNCS 4808, pp. 422-431, 2007.
[10] T. Cao and P. Shen, "Cryptanalysis of two RFID authentication protocols", International journal of network security, In press, 2008.
[11] D. N. Duc, J. Park, H. Lee, and K. Kim, "Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning", The 2006 Symposium on Cryptography and Information Security, 2006.
[12] A. D. Henrici and P. MÄuller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers", In the Proceedings of PerSec'04 at IEEE PerCom, 2004, pp. 149-153.
[13] S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography", Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, 2005, pp. 63-67.
[14] D. Molnar and D. Wagner, "Privacy and security in library RFID: issues, practices, and architectures", Conference on Computer and Communications Security-CCS'04, 2004, pp. 210-219.
[15] M. Ohkubo, K. Suzki, and S. Kinoshita, "Cryptographic approach to 'privacy friendly' tags", RFID Privacy Workshop, 2003.
[16] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment", International Conference on Security in Pervasive Computing-SPC 2005, 2005, pp. 70-84.
[17] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost RFID", Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, 2005.
[18] J. Yang, K. Ren, and K. Kim, "Security and privacy on authentication protocol for low-cost radio", The 2005 Symposium on Cryptography and Information Security, 2005.
[19] 양형규, 안영화, "유비쿼터스 컴퓨팅 환경에 적합한 RFID 인증 프로토콜에 관한 연구," 전자공학회 논문지 42권 CI 1호, pp.45-50, 2005
[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] 안해순, 부기동, 윤은준, 남인길, "RFID/USN 환경을 위한 개선된 인증 프로토콜," 전자공학회논문지, 제46권, 제CI-1호, pp. 1-10, 2009.
[24] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, "Handbook of applied cryptograph", CRC Press, New York, 1997.

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 교양대학 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 계약교수
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)-교신저자
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>