情報保護學會論文誌
第18卷 第5號, 2008. 10

# 데이터베이스에서의 태그 검색이 쉽고 안전한 RFID 상호인증 프로토콜*

권 혜 진†, 이 재 욱, 전 동 호, 김 순 자‡
경북대학교

# Easy to Search for Tags on Database and Secure Mutual Authentication Protocol for RFID system*

Hye-Jin Kwon†, Jae-Wook Lee, Dong-Ho Jeon, Soon-Ja Kim‡
Kyungpook National University

요 약

안전한 RFID 시스템을 위하여 현재까지 다수의 RFID 인증 프로토콜이 제안되었다. 이들은 어떤 암호학적 요소를 사용하느냐에 따라 크게 해시기반, 재 암호화 기반, XOR 기반으로 나눌 수 있다. 현재까지 알려진 대표적인 공격으로는 도청, 사칭, 위치추적공격 등이 있는데 기존에 제안된 프로토콜들은 이러한 공격에 안전하지 않거나, 데이터베이스의 태그 검색 과정이 비효율적이었다. 따라서 본 논문에서는 해시함수를 사용하여 알려진 공격에 안전하고 데이터베이스가 태그와 사전에 공유한 값을 통해 이전 세션의 상태를 파악하게 하여 태그 검색 과정이 비교적 간단한 프로토콜을 제안한다.

ABSTRACT

A great number of RFID authentication protocols have been proposed for the secure RFID system. These are typically divided into three types according to primitive that they use : Hash-based, Re-encryption based, and XORing-based protocol. The well-known attacks in RFID system are eavesdropping, impersonating, location tracking, and so on. However, existing protocols could not provide security against above attacks, or it was not efficient to search for tags on database. Therefore, in this paper we present a protocol which is secure against above attacks by using hash function and makes Database search tags easily by attaining the state information of previous session through the shared values with all tags and database.

**Keywords** : RFID system, Authentication protocol, privacy

## Ⅰ. 서 론

RFID(Radio Frequency Identification) 시스템은 무선채널을 통하여 태그를 식별하는 시스템이다. 이는 대개 데이터베이스, 리더, 태그로 구성되는데, 리더는 일정 영역 내에서 물리적 접촉 없이 태그로부터 메시지를 받아 그를 데이터베이스로 전송하고 데이터베이스는 그

접수일 : 2008년 4월 27일; 수정일 : 2008년 7월 1일;
채택일 : 2008년 7월 31일
* 본 연구는 경북대학교 2006년도 연구교수 연구비 지원에 의해 수행됨.
† 주저자, kelted@ee.knu.ac.kr
‡ 교신저자, snjkim@ee.knu.ac.kr

메시지를 토대로 태그를 식별한다. 리더가 피 식별 개체의 메시지를 무선으로 수신하는 특징으로 인하여 RFID 시스템은 현재 식별 시스템에서 통용되고 있는 바코드를 대체할 시스템으로 주목받고 있다[1-3]. 그러나 이러한 장점은 곧 RFID 시스템의 보안상 위협으로 이어진다. 리더와 태그간의 무선 통신은 유선 통신에 비해 도청되기 쉽고, 태그를 부착할 물품의 대량생산 환경에서 태그 칩 가격의 한계로 인해 일반 컴퓨터 통신과 같이 연산량이 많은 암호 요소를 쓸 수 없다. 이에 Weis 등은 유선 통신에서 통용되고 있는 공개키나 대칭키 암호보다는 연산량이 적으면서 암호학적 효과를 낼 수 있는 해시함수를 사용하여 통신되는 정보를 숨기는 프로토콜을 제안하였다[3]. 즉, 고유 식별자($ID$)와 키를 가진 태그는 리더의 요청에 $ID$대신, 자신의 고유키를 해시한 $metaID$를 전송한다. 리더는 이를 데이터베이스에 전송하여 그에 해당하는 $ID$와 키를 받아 태그를 식별한다. 이 프로토콜은 직접적인 정보 노출은 막았지만 매 세션 고정된 $metaID$를 전송하여 위치 추적(location tracking)이나 재전송공격, 사칭 등 여러 가지 보안상의 위협을 내포하였다. 이에 Ohkubo 등은 두 개의 해시함수를 사용한 해시 체인 프로토콜을 제안하였다[4]. 이 프로토콜은 $ID$와 비밀정보($s_i$)를 가진 태그가 두 개의 해시함수를 내장하였다고 가정하고, 하나의 해시함수($H$)는 $s_i$갱신에, 나머지 함수($G$)는 갱신된 $s_i$보호에 이용하였다. 태그가 자신의 비밀정보를 갱신함으로써 불구분성이 지켜졌지만, 데이터베이스가 태그의 갱신된 정보를 저장하지 않아 재전송공격을 통한 사칭에 안전하지 못하였으며, 태그 검색 과정이 비효율적이었다. 그 후 Henrici와 Muller는 태그 검색 시에 데이터베이스의 부하를 줄이고 재전송 공격을 차단하기 위해 데이터베이스 역시 태그의 정보를 갱신하는 프로토콜을 제안하였다[5]. 그러나 공격자가 리더와 태그사이에서 메시지 차단을 할 경우 불구분성이 만족되지 않아 위치추적에 안전하지 않았다. 이를 개선하여 Yoo 등에 의해 이전 세션의 상태에 따라 메시지를 다르게 보내는 상태기반 RFID 프로토콜이 제안되었으나 이는 태그에서 리더로 가는 첫 번째 메시지가 유실 될 경우 더 이상의 인증이 불가능하였다[6]. 이에 Ha 등이 LRMAP를 제안하였는데 이 프로토콜은 리더와 태그간의 통신 중 어느 부분이 차단되더라도 그 다음 세션에서 인증이 가능하게 설계되었다[7]. 그러나 이 프로토콜은 이전세션이 비정상 종료되었다면 다음번 통신에서 데이터베이스는 태그를 식별하기 위해 평균 ($m$+3)번($m$: $DB$가 저장하고 있는 태그의 $ID$개수)의 해시 연산이 요구되어 비효율적인 면이 있다. 이에 본 논문에서는 기존 공격방법에 안전하며, 이전 세션이 비정상종료 되었을 경우 데이터베이스에서 평균 ($\sqrt{m}$+5)번의 해시를 통해 해당 태그를 찾을 수 있는 프로토콜을 제안한다.

## Ⅱ. 연구배경

### 2.1 보안 요구 조건[2,8-9]

RFID 시스템의 보안상 취약점은 데이터베이스 관리상의 문제, 기존 유선 통신($DB \leftrightarrow R$)에서의 문제와 무선통신($R \leftrightarrow T$)으로 인한 문제, 저가 태그의 사용으로 인한 문제(고급 암호요소 사용불가, 물리적 공격에 취약) 등으로부터 발생한다. 또한 RFID의 특징에 의해 위치추적과 개인 정보 노출이라는 개인 프라이버시에 대한 새로운 보안상 취약점을 가지게 된다. 이 절에서는 이러한 다양한 종류의 위협과 그로부터 안전하기 위해 필요한 조건을 기술한다. 단, 본 논문에서는 데이터베이스와 리더는 태그에 비하여 가격적 제약이 약하다고 간주하고 $DB, R$ 각 개체와 그들 간의 통신은 안전하다고 가정한다.

- 정보 노출(Information leakage)에 안전 : RFID 시스템에서 리더와 태그 간의 통신은 무선으로 이루어지고, 또한 태그는 리더의 요청을 받으면 리더에 대한 인증과정 없이 응답을 하게 된다. 따라서 공격자는 별 다른 노력 없이 쉽게 정당한 태그의 응답을 얻을 수 있다. 그러므로 안전한 RFID 시스템은 공격자가 정당한 메시지를 얻더라도 그로부터 어떠한 유용한 정보도 얻을 수 없게 설계되어야 한다.

- 재전송 공격(Replay attack) 및 사칭(Impersonate attack)에 안전 : 재전송 공격이란 과거에 정당한 개체간의 통신 메시지를 도청한 후, 이후에 그 메시지를 재사용하는 것을 뜻한다. 이 공격은 주로 사칭과 연결 되는데, 공격자는 이전 세션에서 도청한 메시지를 현재 세션에 사용함으로써 정당한 사용자로 사칭할 수 있다. 따라서 메시지는 세션마다 불규칙적으로 변경되어야 한다.

- 위치추적(Location tracking)에 안전 : 위치추적공

격은 공격자가 불법적인 리더를 여러 곳에 걸쳐 설치한 환경에서 특정 태그 소지자의 이동 경로를 추적하는 것을 말한다. 이는 아래의 두 가지 보안조건이 충족되지 않을 때 일어나게 된다.[8]

i) 불구분성(indistinguishability)
불구분성이란 태그에 대한 접근 권한이 없는 자가 태그의 메시지를 토대로 그 메시지의 출처를 알아내지 못하는 성질을 말한다. 이를 만족하기 위해서는 통신 중 특정 태그를 지칭하는 고정 메시지나 규칙적인 성질을 가지는 메시지 전송을 지양하여야한다.

ii) 전방향안전성(forward secrecy)
전방향안전성이란 공격자가 물리적 공격에 성공하여 태그의 현재 내부 비밀 정보를 알게 되었을 때라도 그를 이용하여 해당 태그의 과거 비밀 정보를 아는 것이 불가능하여, 태그 소지자의 과거 이동경로를 추측하지 못하는 것을 말한다.

즉, 위치추적공격에 안전하려면 리더와 태그와의 통신에서 오가는 메시지가 일정하거나 규칙적으로 생성되어 공격자가 메시지를 보고 태그를 쉽게 추측할 수 없어야 하고, 또한 현재의 정보를 토대로 이전의 정보를 추측할 수 없어야 한다.

- 비동기화유도 공격(Desynchronization attack)에 안전[9] : 태그의 비밀정보가 갱신되는 프로토콜에서 통신상의 문제가 발생할 경우, 데이터베이스와 태그사이에 내부 정보가 불일치할 수 있다. 이러한 점에 착안하여 공격자가 고의로 통신을 방해하여 데이터베이스와 태그의 정보 불일치를 유도하는 것을 비동기화유도 공격이라 한다. 이는 일종의 서비스 거부 공격(DoS, Denial of Service attack)으로 이러한 공격에 안전하려면 정보 불일치가 일어나더라도 그를 회복할 수 있도록 설계하여야 한다.

- 물리적 공격(Physical attack)에 안전 : 물리적인 공격은 통신내용이 아니라 태그 자체에 저장된 정보를 직접 해석하는 방법(프로브 공격)부터 통신장비 등에서 발생하는 전자파를 분석하는 공격(TEMPEST공격)까지 포함한다[2]. 이런 문제는 태그 가격의 제한으로 인해 암호화가 가능한 고가의 칩을 사용하기 힘든 점에서 나온다. 따라서 태그 자체에 중요한 정보를 저장하기보다 *ID*등의 최소한 정보만을 저장하여 인가된 리더만 그 태그의 정보를 얻게 하는 것이 안전하다.

### 2.2 효율성 측면의 요구 조건

- 데이터베이스에서 태그를 찾는 알고리즘의 효율성 : 이는 데이터베이스에서 저장하고 있는 태그의 *ID* 개수가 증가하더라도 데이터베이스의 식별 과정중의 계산량이 일정 수준 이하로 유지되어야 한다는 데이터베이스의 확장성(Scalability)과 관련된 문제이다[10]. RFID 시스템은 데이터베이스가 동시에 여러 태그를 인증하는 환경에 있는 시스템이므로, 안전한 인증방식도 중요하지만, 해당 태그를 빠르게 찾아 인증하는 것도 프로토콜 설계 시 중요한 고려 요소가 된다.

- 안전성을 지키는 범위 안에서, 통신되는 메시지는 짧을수록 효율적이며 태그가 부착될 상품이 대량 생산될 경우, 태그의 저가 형성이 중요하므로 저장 공간과 정보보호를 위한 암호 요소의 연산 양을 줄이는 것이 필요하다.

### 2.3 기존 RFID 인증 프로토콜의 취약점

RFID 특성상 태그마다 고유한 *ID*는 키 이상의 의미를 가진다. 이러한 *ID*를 갱신하지 않는 프로토콜은 갱신하는 것에 비하여 별다른 노력 없이 비동기화유도공격을 막을 수 있고 식별과정이 비교적 간단하나, 고정적인 *ID*를 이용한 메시지를 매 세션마다 불규칙적으로 변경할 수 있어야 재전송 공격, 사칭에 안전하고 불구분성을 만족한다. 그러나 이러한 문제를 해결하더라도 이미 *ID*가 노출된 경우에는 위치 추적을 피할 수 없다. 이에 비해 *ID*를 갱신하는 프로토콜의 경우, 데이터베이스에서의 태그 식별과정이 복잡하고 비동기화유도공격에 안전하기 위해서는 특별한 노력이 필요하다. 그러나 *ID*를 갱신하는 연산이 알려진 가운데, 그 역연산을 하는 것이 쉽지 않은 경우에 한해서는 전방향안전성을 보장할 수 있는 장점이 있다. 이에 본 절에서는 해시함수를 사용하며 *ID*를 갱신하는 LRMAP[7]와 *ID*를 갱신하지 않으면서 한 번의 해시만을 사용한 강화된 OHLCAP[9]을 소개하고 앞서 제시한 요구 조건을 기준으로 분석한다.

### 2.3.1 Lightweight and resynchronous mutual authentication protocol (LRMAP)[7]

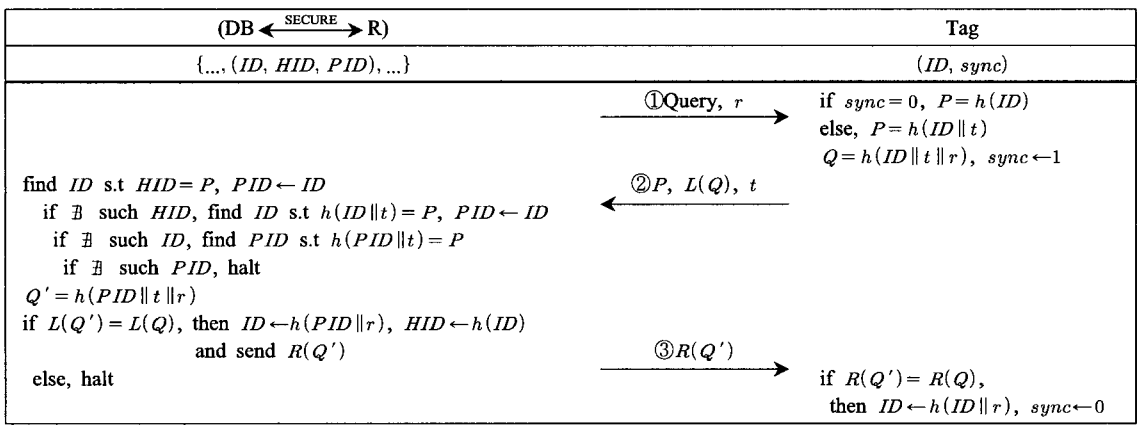
이 프로토콜은 Ha 등이 제안한 것으로 리더와 태그는 난수생성이 가능하며 태그는 해시까지 가능하여야 한다. 또한 리더와 데이터베이스의 통신은 안전하다고 가정한다. 리더의 난수 $r$과 함께 요청을 받은 태그는 난수 $t$를 생성하고, *sync* 값(이전 세션의 정상종료 여부를 나타냄)에 따라 메시지 쌍 $(P, L(Q), t)$중 $P$를 달리 생성한다. *sync*가 0인 경우 $(h(ID),\ h(ID\|t\|r),\ t)$를 생성하고, *sync*가 1인 경우 $(h(ID\|t),\ h(ID\|t\|r),\ t)$를 생성하며 이를 리더에게 전송한 후 *sync*를 1로 둔다.

메시지를 전송받은 리더는 그에 자신의 난수 $r$을 덧붙여 데이터베이스에 전송한다. 데이터베이스는 [그림 1]과 같이 수신한 메시지 중 $P$를 이용하여 메시지를 보낸 태그를 찾을 수 있다. 만일 이 과정에서 일치하는 값이 없다면 정당하지 않은 태그의 메시지로 간주하고 프로토콜을 종료시킨다. *ID*를 찾아 그를 *PID*로 대입하는 과정을 거쳤다면 $h(PID\|t\|r)$와 $L(Q)$가 일치하는지 확인한다. 일치하지 않는다면 프로토콜을 종료시키고, 일치한다면 태그가 리더를 인증할 수 있게 $R(h(PID\|t\|r))$을 전송하고, $h(PID\|r)$을 *ID*로, $h(ID)$를 *HID*로 갱신한다. 리더는 $R(h(PID\|t\|r))$을 태그에게 전송하고 태그는 그 값이 $R(Q)$와 일치한다면 다음 통신을 위해 $h(ID\|r)$를 *ID*로 갱신하고 *sync*를 0으로 두고, 일치하지 않는다면 종료한다.

이 프로토콜은 *ID*를 갱신하며, 이전 세션의 통신 중 메시지 유실이 발생하여 데이터베이스와 태그의 정보가 일치하지 않더라도 정보 차이를 회복 할 수 있도록 설계되었고, 앞에서 제시한 보안 요구조건을 모두 만족한다.

효율성 측면에서 볼 때, 데이터베이스와 태그의 정보가 일치되어 있을 경우에는 데이터베이스의 계산량이 문제가 되지 않는다. 그러나 이전 세션이 비정상 종료된 경우 태그는 $h(ID\|t)$를 보내지만 데이터베이스는 리더로부터 받은 태그의 해시 값이 $h(ID)$, $h(ID\|t)$, $h(PID\|t)$ 중 어느 것에 해당하는 값인지 알 수 없기 때문에, 비정상 종료된 경우라도 먼저 데이터베이스내의 *HID* 리스트에서 일치하는 값이 있는지 검색하게 되는데 이는 태그 식별과정의 비효율성을 초래한다.

예를 들어, 이전 세션에서 데이터베이스의 마지막 메시지가 리더에서 태그로 가는 도중(③번 과정) 차단되었다고 가정하면 데이터베이스는 해당 태그의 현재 *ID*는 *PID*필드에 대입하고, *ID* 필드를 $h(ID\|r)$로 갱신한 상태이지만, 태그는 인증 메시지를 받지 않았으므로, *ID*를 갱신시키지 않고 그대로 둔다. 리더의 다음 요청이 있을 때, 비동기 상태이기 때문에 태그는 $h(ID)$를 보내는 대신 불구분성을 만족시키기 위해 $h(ID\|t)$를 보낸다. 이 값은 현재 데이터베이스의 상태로서는 $h(PID\|t)$이지만 데이터베이스는 먼저 자신의 *HID* 리스트에서 일치하는 데이터가 있는지 검색한다. 만일 일치하는 데이터가 없다면 일치하는 데이터가 나올 때까지 데이터베이스내의 모든 *ID*에 대해 $h(ID\|t)$를 구해서 비교한다. 또 다시 일치하는 데이터가 없다면 모든 *PID*에 대해 $h(PID\|t)$를 계산한 후 *ID*를 찾게 된다. 따라서 비동기시 데이터베이스가 태그를 찾는 과정은 평균 $m$+3번의 해시를 하게 되어 비효율적이다.




[그림 1] Lightweight and resynchronous mutual authentication protocol.

### 2.3.2 Enhancement of One-way Hash based Low-Cost Authentication Protocol[9]

이 프로토콜은 $ID$를 갱신시키지 않고, 한 번의 해시만을 사용한 인증 프로토콜이다. 리더의 난수 $r$과 함께 요청을 받은 태그는 난수 $t$를 생성하고, 메시지 쌍 ($A^1$, $A^2$, $R(B)$)을 ($K \oplus t$, $GI+(r \oplus t)$, $R(h(ID\|GI\|r\|t))$)와 같이 생성한 후 리더에게 전송한다. 태그로부터 메시지를 전송받은 리더는 자신의 난수 $r$과 함께 데이터베이스에 전송한다. 데이터베이스는 $A^1 \oplus K$를 하여 $t$를 계산하고, $A^2-(r \oplus t)$를 계산하여 $GI$를 계산한다. $GI$-group 내에서 $R(B)$와 일치하는 $R(h(ID\|GI\|r\|t))$이 나올 때까지 계산한다. 일치하는 $R(h(ID\|GI\|r\|t))$이 있다면 $L(h(ID\|GI\|r\|t))$을 리더에게 전송하고, 일치하는 값이 없다면 프로토콜을 종료한다. 리더는 메시지를 태그에게 전송하고, 태그는 수신한 메시지가 $L(B)$와 일치하는 지 확인한다([그림 2]).

이 프로토콜은 매 세션 난수에 의해 메시지가 변하므로 재전송공격이나 사칭, 불구분성에 안전하나 $ID$를 생신하지 않기 때문에 어떤 공격으로 인해 현재 $ID$가 노출 될 경우 그 이전의 이동 경로가 파악되어 전방향안전성을 제공하지 않는다. 또한 효율성 측면에서 데이터베이스는 리더로부터 메시지를 받을 경우마다 태그를 파악하기 위하여 평균 ($\sqrt{m}/2$)번의 해시를 하여야 한다.

## Ⅲ. 제안하는 프로토콜

이 장에서는 2장에서 제시한 RFID 시스템의 여러 가지 요구조건을 바탕으로 안전하고, 데이터베이스에서의 태그 인식시간이 짧은 프로토콜을 제안한다[그림 3]. 먼저 데이터베이스와 리더는 안전한 채널 상에서, 리더와 태그는 안전하지 않은 무선 채널 상에서 통신한다고 가정한다. 또한 리더와 태그는 난수생성이 가능하며, 태그는 이에 추가적으로 해시와 덧셈이 가능하여야 한다.

### 3.1 용어정리

이 절에서는 여기서는 제안 기법에 사용하게 될 용어

| (DB ⟵SECURE⟶ R) | | Tag |
|---|---|---|
| $\{K\} \cup \{..., (GI, ID), ...\}$ | | $(GI, ID, K)$ |
| | ① Query, $r$ ⟶ | $A^1 = K \oplus t$<br>$A^2 = GI+(r \oplus t)$<br>$B = h(ID\|GI\|r\|t)$ |
| $t = A^1 \oplus K$, $GI = A^2-(r \oplus t)$,<br>search $ID$ s.t. $R(h(ID\|GI\|r\|t)) = R(B)$ in $GI$-gr<br>if 」 such $ID$, send $L(B)$<br>else, halt | ⟵ ② $A^1$, $A^2$, $R(B)$ | |
| | ③ $L(B)$ ⟶ | check $L(B)$ |

[그림 2] Enhancement of one-way hash based low-cost authentication protocol

| (DB ⟵SECURE⟶ R) | | Tag |
|---|---|---|
| $\{K_0, K_1\} \cup \{..., (GI, ID, HID, PID), ...\}$ | | $(K_0, K_1, GI, ID, k)$ |
| | ① Query, $r$ ⟶ | if $k=0$, $S_{ID} = h(ID)$<br>else, $S_{ID} = h(ID\|t)$<br>$S_t = K_k \oplus t$, $A_t = h(K_k\|t)$,<br>$S_{GI} = GI+(r \oplus t)$, $k \leftarrow 1$ |
| find $k \in \{0, 1\}$ s.t $L(h(K_k\|S_t \oplus K_k)) = L(A_t)$<br>if ∃ such $k$, then $t \leftarrow S_t \oplus K_k$. else, halt<br>$GI = S_{GI}-(r \oplus t)$<br>if $k=0$, find $ID$ s.t $HID = S_{ID}$ in $GI$-gr, $PID \leftarrow ID$<br>else, find $ID$ s.t $h(ID\|t) = S_{ID}$ in $GI$-gr, $PID \leftarrow ID$<br>if ∃ such $ID$, find $PID$ s.t $h(PID\|t) = S_{ID}$<br>if ∃ such $PID$, halt<br>$A_R = h(PID\|GI\|r)$, $ID \leftarrow h(PID\|r)$, $HID \leftarrow h(ID)$ | ⟵ ② $S_t$, $L(A_t)$, $S_{GI}$, $S_{ID}$ | |
| | ③ $L(A_R)$ ⟶ | if $L(h(ID\|GI\|r)) = L(A_R)$,<br>then $ID \leftarrow h(ID\|r)$, $k \leftarrow 0$ |

[그림 3] 제안하는 프로토콜.

를 설명한다.

| | |
|---|---|
| $DB$ | : 백 엔드 데이터베이스 |
| $R$ | : 리더 |
| $T$ | : 태그, $m$개 |
| $r$ | : 리더가 생성한 난수 |
| $t$ | : 태그가 생성한 난수 |
| $h()$ | : 해시함수. $h:(0,1)^* \rightarrow (0,1)^l$ |
| $ID$ | : 태그의 식별정보, $l$-bit, $m$개 |
| $PID$ | : 태그의 바로 이전 $ID$ |
| $HID$ | : $ID$의 해시 값 |
| $GI$ | : 그룹의 식별정보, $l$-bit, $\sqrt{m}$개 |
| $K_0$, $K_1$ | : $DB$와 모든 태그의 공통 비밀정보, $l$-bit |
| $S_x$ | : $x$를 찾는데 필요한 정보 |
| $A_x$ | : $x$를 인증하는데 필요한 정보 |
| $L()$, $R()$ | : 메시지의 왼쪽(오른쪽) 절반 |
| $\|\|$ | : 연접 |
| $+$ | : $2^l-1$을 법으로 한 덧셈 |
| $\oplus$ | : 2을 법으로 한 덧셈 |

### 3.2 제안하는 프로토콜

제안하는 프로토콜은 태그가 이전 통신의 종료 상태(정상이면 $K_0$, 비정상이면 $K_1$)를 알 수 있게 함으로써 재전송 공격(replay attack)과 사칭(impersonate)에 안전하고 불구분성(indistinguishability)을 만족하며, 또한 이를 데이터베이스 역시 그를 알아 이전 세션이 비정상적으로 종료된 경우에도 태그를 인식하는 시간이 기존의 상태를 기반으로 한 프로토콜보다 상대적으로 줄어들게 설계하였다. 또한 제안하는 프로토콜은 $ID$를 갱신하는데, 갱신 시에 이전 세션의 $ID$에 리더의 난수 $r$을 연접하여 해시를 하므로 물리적 공격에 의해 현재의 $ID$를 알고 있더라도 일방향 해시함수의 성질에 의해 이전 $ID$를 알 수 없으므로 전방향안전성(forward secrecy)이 보장되도록 설계한다.

1. 리더는 태그에게 난수 $r$과 함께 질의를 보낸다.
2. 태그는 난수 $t$를 생성하고, $k$를 체크한다.
   - $k=0$ : $S_t = K_0 \oplus t$, $L(A_t) = L(h(K_0 \| t))$, $S_{GI} = GI + (r \oplus t)$, $S_{ID} = h(ID)$를 생성하고
   - $k=1$ : $S_t = K_1 \oplus t$, $L(A_t) = L(h(K_1 \| t))$, $S_{GI} = GI + (r \oplus t)$, $S_{ID} = h(ID \| t)$를 생성하여

   생성된 모든 메시지를 리더에게 전송한 후, $k$를 1로 둔다.
3. 리더는 태그로부터 받은 메시지를 자신의 난수 $r$과 함께 데이터베이스에게 전송한다.
4. 리더로부터 메시지를 전송받은 데이터베이스는 태그의 난수 $t$를 구해야 하는데, 먼저 이전세션이 정상종료 되었다고 가정하고 $S_t \oplus K_0$를 계산하여 $h(K_0 \| S_t \oplus K_0)$의 왼쪽 부분과 $L(A_t)$이 일치하는지 비교한다.
   - 일치한다면 이전 세션이 정상적으로 종료되었고($K = K_0$) 태그가 선택한 난수 $t$가 $S_t \oplus K_0$라는 것을 알 수 있고, 태그가 속한 그룹의 $ID$를 구하게 된다.
   - 일치하지 않는다면 $h(K_1 \| S_t \oplus K_1)$를 계산하고, 그 왼쪽부분과 $L(A_t)$의 일치여부를 판단한다.
     - 일치한다면 이전 세션이 비정상적으로 종료되었고($K = K_1$), 태그가 선택한 난수 $t$가 $S_t \oplus K_1$라는 것을 알 수 있다.
     - 일치하지 않는다면 $K_0$, $K_1$를 알지 못한 누군가에 의해 보내진 메시지로 간주하고 세션을 종료시킨다.

   태그가 보낸 $t$를 찾았다면 $S_{GI} - (r \oplus t)$를 계산하여 태그가 속한 그룹의 식별정보($GI$)를 찾고, $S_{ID}$를 이용하여 그 그룹($GI$-group)내에서 아래와 같이 태그를 검색한다.
   - 만약 $K = K_0$라면, 해당 그룹 안에서 $S_{ID}$와 일치하는 $HID$가 있는지를 검색하여 $ID$를 찾아 $PID$필드에 대입한다.
   - 그렇지 않다면($K = K_1$인 경우), 데이터베이스는 이전 세션이 비정상 종료 되었다는 것은 알지만 정확히 어디에서 통신 이상이 발생하여 비정상 종료 된 것인지는 모른다. 즉, 통신 차단이 발생된 곳이 ②번인지 ③번인지 알 수 없기 때문에 이 두 가지 경우 모두 고려하여 $ID$를 검색해야 한다.
     - 먼저 데이터베이스는 이전 세션에서 ②번 과정 중 메시지가 차단되었다고 가정하고 해당 그룹 내의 $ID$에 대해 $S_{ID}$와 일치하는 $h(ID \| t)$ 값이 나올 때까지 해시를 한다. 일치하는 $ID$가 있다면 이전 세션은 ②번 과정에서 비정상 종료되었다는 것을 알 수 있고, 그 $ID$를 $PID$필드

에 대입하고 검증단계로 넘어간다.

- 만약 그룹 안에서 $S_{ID}$와 일치하는 $h(ID\|t)$ 값이 없다면 그룹 내의 $PID$에 한하여 $h(PID\|t)$를 계산하여 $S_{ID}$와 일치하는지 검사한다. 일치하는 데이터가 있다면 이전 세션이 ③번 과정에서 비정상 종료되었다는 것을 의미하므로 검증 단계로 넘어가고, 없다면 정당한 사용자에 의한 메시지가 아니라고 판단하여 세션을 종료 한다.

$S_{ID}$를 이용하여 $ID$를 찾은 경우 태그에게 전송할 인증 값 $L(A_R)=L(h(PID\|GI\|r))$를 생성하여 전송한 후, $ID$를 $h(PID\|r)$로, $HID$를 $h(ID)$로 갱신한다.

5. 리더는 $L(A_R)$를 전달한다.
6. 태그는 전달 받은 $L(A_R)$와 $L(h(ID\|GI\|r))$가 일치한다면 $ID$를 $h(ID\|r)$로 갱신하고, 정상 종료되었다는 것을 저장하기위해 $k$를 0로 바꾼다.

### 3.3 제안 프로토콜 분석

이 절에서는 앞서 소개된 여러 가지 RFID 요구조건을 바탕으로 제안 프로토콜의 안전성과 효율성에 대하여 분석 한다.

#### 3.3.1 보안 분석

- **정보 노출에 대한 안전** : 제안한 프로토콜은 통신 과정에서 $ID$를 직접 노출시키지 않고, 일방향 해시함수를 사용하여 인가된 사용자만이 해당 태그의 $ID$를 알아 낼 수 있도록 하였다. 인가되지 않은 사용자가 메시지를 보고 $ID$를 알아낼 확률은 $2^{-l}$로서 희박하다고 볼 수 있다.

- **재전송 공격 및 사칭에 대한 안전** : 통신되는 메시지 $S_t=K_k\oplus t$, $L(A_t)=L(h(K_k\|t))$, $S_{GI}=GI+(r\oplus t)$, $S_{ID}=h(ID)$ 또는 $h(ID\|t)$, $r$, $L(A_R)$는 모두 난수이거나 난수와 결합되어 생성된 메시지다. 다음 세션에서의 메시지는 새롭게 생성된 난수와 태그정보가 결합되어 생성되기 때문에 이전에 도청한 메시지로는 정당한 개체로 인증 받을 수 없으므로 사칭이 불가능하다[표 1].

- **위치추적에 대한 안전**

i) 불구분성 : 리더의 요청에 대한 태그의 응답은 $S_t=K_k\oplus t$, $L(A_t)=L(h(K_k\|t))$, $S_{GI}=GI+(r\oplus t)$와 이전 세션이 정상 종료 되었을 경우는 $h(ID)$, 비정상 종료 되었을 경우는 $h(ID\|t)$이 된다. 이전 세션의 통신 정상 여부와 관계없이 메시지는 이전 세션과 동일하거나 규칙적으로 변하는 것이 아니므로 공격자가 설령 과거 통신내용을 모두 알고 있는 상황이더라도 현재 통신 중인 태그가 어떤 특정 태그라고 단정할 수 없다.

ii) 전방향안전성 : 공격자가 태그와 $DB$의 통신 상태를 전반적으로 알 수 있는 환경에서, 태그의 현재 $ID$가 노출된 상황을 가정하더라도 제안 프로토콜에서는 공격자가 태그의 이동경로를 유추할 수 없다. $ID$갱신 알고리즘을 보면 현재의 $ID$는 $h(PID\|r)$로 생성된다. 태그의 과거 이동경로를 유추하려면 $PID$를 알아야 하는데, $ID$와 $r$을 아는 상황에서 $PID$를 구하는 것은 일방향 해시함수에서 프리이미지를 구할 수 있는 문제의 어려움과 같으므로, 본 프로토콜의 전방향 안전성은 일방향 해시함수의 프리이미지를 찾는 문제가 어려운 범위 내에서 보장된다. (단, 연속적인 통신 차단이 일어난 경우, 통신 차단

[표 1] 제안하는 프로토콜과 기존 프로토콜의 안전성 비교

○ : 안전, × : 불안전

| | Henrici et al.'s AP[5] | 상태기반 인증프로토콜[6] | EOHLCAP[9] | LRMAP[7] | 제안하는 프로토콜 |
|---|---|---|---|---|---|
| 재전송 공격 | ○ | ○ | ○ | ○ | ○ |
| 사칭 | × | ○ | ○ | ○ | ○ |
| 불구분성 | × | × | ○ | ○ | ○ |
| 전방향 안전성 | × | × | × | ○ | ○ |
| $ID$ 갱신 | ○ | ○ | × | ○ | ○ |
| 비동기화유도공격 | ○ | × | ○ | ○ | ○ |

기간 동안 태그의 $ID$는 갱신되지 않으므로 태그에 물리적 공격을 가하여 갱신되지 않은 $ID$를 알아낸다면 차단 기간 동안의 위치는 추적가능하다. 그러나 이는 해당 태그가 이동할 수 있는 영역의 전 리더가 통신 차단이 발생하여야 가능하므로 아주 낮은 확률을 지닌다고 간주한다.)

- **비동기화유도 공격에 대한 안전** : 제안하는 프로토콜에서는 공격자가 고의로 통신을 차단하더라도 정당한 태그라면 항상 인증 받을 수 있다.
공격자가 ②번($T \rightarrow R$)과정에서 통신을 차단한 경우, 태그와 데이터베이스의 정보가 일치하지만 태그는 전송한 메시지에 대한 응답을 받지 못하였으므로 다음 세션에서 $S_{ID}$를 $h(ID)$대신 $h(ID\|t)$로 만들고, $S_t = K_1 \oplus t$, $L(A_t) = L(h(K_1\|t))$, $S_{GI} = GI + \oplus t)$과 함께 보낸다. 이 메시지를 받은 데이터베이스는 $S_t$와 $L(A_t)$로부터 $K$값이 $K_1$임을 알 수 있게 된다. 따라서 데이터베이스는 $GI$-group내에 있는 $ID$에 대해 평균 $(5+\sqrt{m}/2)$번의 해시($h(ID\|t)$)를 하여 수신된 $S_{ID}$와 비교해 $ID$를 찾을 수 있다.
③번(마지막 과정, $R \rightarrow T$)에서 통신이 차단된 경우, 데이터베이스는 해당 태그의 $ID$를 갱신하지만 태그는 $ID$를 갱신하지 못한다. 즉, 태그의 $ID$는 데이터베이스의 $PID$이다. 이런 상태에서 태그가 리더의 요청을 받을 경우, 태그는 ②번에서 종료된 경우와 같이 $S_t = K_1 \oplus t$, $L(A_t) = L(h(K_1\|t))$, $S_{GI} = GI$, $+(r \oplus t)$, $S_{ID} = h(ID\|t)$를 전송한다. 데이터베이스는 $S_t$와 $L(A_t)$로부터 이전 통신이 비정상 종료되었다는 것을 알고, 우선 $GI$-group내에 있는 $ID$에 대해 $h(ID\|t)$와 $S_{ID}$를 비교하지만 일치하는 값을 찾을 수 없다(해시 충돌이 발생하지 않는다는 가정 하에). 그렇다면 데이터베이스는 $GI$-group내에 있는 $PID$에 대해 평균 $(5+3\sqrt{m}/2)$의 해시 $h(PID\|t)$를 하여 $S_{ID}$와 비교 후 $ID$를 찾는다.
즉, 어느 과정에서 통신이 차단되더라도 정당한 태그인 경우에는 데이터베이스와의 비동기를 회복할 수 있기 때문에 비동기화유도 공격에 안전하다.

- **태그 인식의 오류** : 데이터베이스가 리스트 순서대로 태그를 검색하며 그 리스트 중 $j$번째에 위치하는 $jTag$가 메시지 $(S_t, L(A_t), S_{GI}, S_{ID})$를 보냈다고 가정하자. 이 경우 만약 $jTag$와 같은 그룹안의 어떤 $iTag(i<j)$가 $jTag$가 보낸 $S_{ID}$와 일치하는 해시 값을 가진다면 데이터베이스는 $jTag$를 $iTag$로 인식하게 된다. RFID 시스템이 올바르게 운영되려면 위와 같은 경우의 확률이 낮아야한다. 이 확률을 구하기 위해 데이터베이스에서 저장하고 있는 태그의 $GI(l$-bit) 개수를 $\sqrt{m}$, 한 그룹 안의 $ID(l$-bit) 개수를 $\sqrt{m}$(즉, 총 태그 개수 $m$), 가능한 해시 값을 $M=2^l$라 두고, 이전 세션 통신이 정상적으로 끝날 확률을 $p_1$, ②번 과정에서 차단될 확률을 $p_2$, ③번 과정에서 차단될 확률을 $p_3$라 하자.
첫째, 이전 통신이 정상 종료된 $jTag$가 $iTag(i<j)$로 잘못 식별 될 경우는 $jTag$가 보낸 $S_{ID}$가 $iHID$ ($iTag$의 $HID$)와 같을 때이다. 이 확률은 $p_1\left(1-\exp(-\frac{(j-1)^2}{2M})\right)$이 된다.
둘째, 이전 통신이 ②번 과정에서 차단된 $jTag$가 메시지를 보내 식별을 요할 때, 다른 태그로 식별되지 않으려면 $S_{ID}$와 같은 $h(iID\|t)(i<j)$가 없어야 한다. 따라서 $jTag$가 임의의 다른 태그로 잘못 식별될 확률은 $p_2\left(1-\exp(-\frac{(j-1)^2}{2M})\right)$이 된다.
셋째, 이전 통신이 ③번 과정에서 차단된 $jTag$가 데이터베이스의 식별을 요할 때, 다른 태그로 인식될 경우는 임의의 $iTag$에 대한 $h(iID\|t)$와 $S_{ID}$가 같거나, $i<j$인 $iTag$에 대한 $h(iPID\|t)$과 $S_{ID}$이 같은 경우이다. 따라서 이 확률은 $p_3\left(1-\exp(-\frac{(\sqrt{m}+j-1)^2}{2M})\right)$와 같다.
임의의 태그가 다른 태그로 인식될 확률은 평균
$\sum_{j=1}^{\sqrt{m}} \frac{1}{\sqrt{m}}\{p_1(1-\exp(-(j-1)^2/2M)) + p_2(1-\exp(-(j-1)^2/2M)) + p_3(1-\exp(-(\sqrt{m}+j-1)^2/2M))\}$
이 된다. 따라서 고정된 $M=2^l$에 대해 위의 확률을 고려한 정도의 태그($m$개)만을 사용할 수 있다.

### 3.3.2 효율성 분석

제안 프로토콜은 리더의 메시지가 들어왔을 때 이전의 통신이 정상적으로 종료된 경우 [표 2]과 같이 4번의 해시를 통해 해당 태그를 식별할 수 있으며, 이전 세션이 비정상 종료 된 경우에는 데이터베이스 역시 이전 통신이 비정상 종료되었다는 것을 알 수 있어 데이터베

〔표 2〕 제안하는 프로토콜과 기존 프로토콜의 효율성 비교

| | Henrici et al.'s AP[5] | 상태기반 인증프로토콜[6] | EOHLCAP[9] | LRMAP[7] | 제안하는 프로토콜 |
|---|---|---|---|---|---|
| 데이터베이스의 해시횟수 | 3 | 정상일 경우 2<br>비정상일 경우 평균 $\sqrt{m}+1$ | $\frac{\sqrt{m}}{2}$ | 정상일 경우 3<br>비정상일 경우 평균 $m+3$ | 정상일 경우 4<br>비정상일 경우 평균 $\sqrt{m}+5$ |
| 태그의 해시횟수 | 3 | 4 | 1 | 3 | 4 |
| 데이터베이스의 저장량 | $10l \cdot m$ | $3l \cdot m$ | $2l \cdot m + l$ | $4l \cdot m$ | $4l \cdot m + 2l$ |
| 태그의 저장량 | $3l$ | $3l+1$ | $3l$ | $l+1$ | $4l+1$ |
| 태그의 메시지 길이 | $3l$ | $2.5l$ | $2.5l$ | $2.5l$ | $3.5l$ |

$m$: $DB$가 소유한 태그의 $ID$개수

이스가 소유하고 있는 $ID$의 개수를 $m$이라 할 때, 평균 ($\sqrt{m}+5$)번(최악의 경우$2\sqrt{m}+5$)의 해시를 통해 태그를 식별할 수 있다. 이는 비정상 종료 시에 평균 ($m+3$)(최악의 경우 $2m+3$)번의 해시를 하는 LRMAP에 비해 상당히 효율적이라고 할 수 있다. 그러나 태그의 해시 횟수 및 저장량, 데이터베이스의 저장량, 통신되는 메시지양이 기존의 프로토콜에 비해 증가하여 향후 이를 개선하기 위한 노력이 필요하다.

## Ⅳ. 결 론

본 논문에서는 RFID 시스템의 보안상 문제점을 알아보고, 그를 해결하기 위해 제안된 기존의 해시 기반 인증 프로토콜을 소개하고 분석하였다. 그러나 기존 프로토콜은 대표적으로 위치 프라이버시(Location privacy)를 보장하지 못하거나, 데이터베이스에서의 태그 식별이 비효율적이었다. 따라서 본 논문에서는 해시함수와 그룹아이디를 사용하며, 태그의 식별정보를 갱신하여 기존에 알려진 공격에 안전하며, 데이터베이스와 모든 태그 간에 공유된 $K_0$와 $K_1$값을 통하여 데이터베이스 역시 이전 통신의 정상 종료 여부를 판단 할 수 있어 데이터베이스에서의 해시 연산량이 감소한 프로토콜을 제안하였다.

안전하며 데이터베이스에서의 연산량이 감소한 반면, 태그의 메시지 양과 저장량이 늘어났으며, 또한 이전 세션이 비정상 종료 된 경우 정확히 어느 과정에서 비정상적으로 종료된 것인지는 확인이 불가능하기 때문에 향후 이를 개선하면 데이터베이스에서의 태그 식별이 더욱 쉬워질 여지가 있다.

## 참고문헌


[1] K. Finkenzeller, *RFID Handbook*, John Wiley & Sons, 1999.

[2] 이용한, 김지영, 정지훈, "무선인식 (RFID) 개인정보보호에 관한 국내외 동향 조사연구", *한국유통물류진흥원*, 2006. 6.

[3] S A 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] M. Ohkubo, K. Suzuki and S. Kinoshita, "Efficient Hash-Chain Based RFID Privacy Protection Scheme", *In Privacy Workshop at the Sixth International Conference on Ubiquitous Computing (UbiComp 2004)*, 2004.

[5] D. Henrici, P. Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. PERCOMW'04*, pp. 149-153

[6] 유성호, 김기현, 황용호, 이필중, "상태기반 RFID 인증 프로토콜", *한국정보보호학회*, pp. 57-68, 2004.

[7] JeaCheol Ha, JungHoon Ha, SangJae Moon, and Colin Boyd, "LRMAP : Lightweight and Resynchronous Mutual Authentication Protocol

for RFID System", *Ubiquitous Convergence Technology*, 2007.

[8] M. Ohkubo, K. Suzuki, and S. Kinoshita, "A Cryptographic Approach to "Privacy- Friendly" tag", *RFID Privacy Workshop*, 2003

[9] JeaCheol Ha, SangJae Moon, Juan Manuel-Gonzalez Nieto, and Colin Boyd, "Security Analysis and Enhancement of One-Way Hash based Low-Cost Authentication Protocol (OHLCAP)", *SSDU 2007*, LNCS, 2007.

[10] G. Avoine, P. Oechslin, "A Scalable and. Provably Secure Hash-based RFID Protocol", *IEEE PerSec 2005*, March 2005.

[11] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, "Universal re-encryption for mix-nets", *Proc. of 2004 RSA Conference*, 2004.

[12] Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai, "Enhancing privacy of universal re-encryption scheme for RFID tags", *Embedded and Ubiquitous Computing EUC*, pp. 879-890, 2004.

[13] A. Juels. "Minimalist cryptography for Low-Cost RFID Tags", *In The Fourth International Conferece on Security in Communication Networks-SCN 2004, vol.3352 LNCS*, pp. 149-164, 2004.

## 〈著者紹介〉

**권 혜 진 (Hye-Jin Kwon) 학생회원**
2007년 2월 : 경북대학교 수학과 학사
2007년 3월~현재 : 경북대학교 정보보호학과 석사과정
<관심분야> RFID보안, 무선랜보안, 정보보호

**이 재 욱 (Jae-Wook Lee) 학생회원**
2001년 2월 : 경북대학교 전자공학과 학사
2003년 2월 : 경북대학교 전자공학과 석사
2003년 3월~현재 : 경북대학교 전자공학과 박사과정
<관심분야> RFID보안, 무선랜보안, 정보보호

**전 동 호 (Dong-Ho Jeon) 학생회원**
2000년 2월 : 밀양대학교 컴퓨터공학과 학사
2002년 2월 : 경북대학교 정보통신학과 석사
2002년 3월~현재 : 경북대학교 정보보호학과 박사과정
<관심분야> 스마트카드, 무선랜보안, 정보보호

**김 순 자 (Soon-Ja Kim) 종신회원**
1975년 2월 : 경북대학교 수학 교육학과 학사
1977년 2월 : 경북대학교 수학과 석사
1988년 2월 : 계명대학교 수학과 박사
1993년 4월~현재 : 경북대학교 전자·전기 공학부 교수
<관심분야> 정보보호 및 보안기술, 정보보호 응용기술