DBpia



# 효율성을 고려한 해시 함수 기반의 안전한 RFID 인증 프로토콜

정회원 김 익 수*

# Hash Function-based Secure Authentication Protocol for Improving Efficiency in RFID System

Ik-Su Kim* *Regular Member*

요 약

안전한 유비쿼터스 환경 구축을 위해 RFID 시스템 인증 프로토콜들이 제안되어 왔다. 하지만 기존 프로토콜들은 최근의 다양한 공격 방법들에 적절히 대응하지 못하거나, 대량의 태그를 인증하기 위해 많은 해시 연산을 필요로 하기 때문에 효율성의 문제가 있다. 이에 본 논문에서는 효율성을 고려한 해시 함수 기반의 안전한 RFID 인증 프로토콜을 제안한다. 제안하는 인증 프로토콜은 공격자에 의한 수동적 공격과 능동적 공격에 안전하며, 태그와 데이터베이스는 상호 인증에 각각 두 번과 세 번의 해시 연산만을 필요로 한다. 따라서 대량의 태그를 처리해야 하는 데이터베이스와 저가의 태그로 구성된 RFID 시스템 환경에 효과적으로 동작한다.

**Key Words** : RFID, Authentication, Hash Function, DoS Attack, Spoofing Attack

ABSTRACT

Many RFID authentication protocols have been proposed to build a secure ubiquitous environment. However, existing protocols do not respond recent attacks appropriately and they perform many hash operations to authenticate a large number of tags. In this paper, we propose a hash function-based secure authentication protocol for improving efficiency in RFID system. The proposed protocol is safe to passive attacks and active attacks, and requires only 2 hash operations in a tag and 3 hash operations in a database. Accordingly, the proposed protocol is very effective in RFID system environment which is composed to low-cost tags and a database handling many tags.

## Ⅰ. 서 론

최근 유비쿼터스 환경 구축을 위해 RFID(Radio Frequency Identification) 시스템을 이용하여 개체를 식별하고 인증하는 연구가 활발히 진행되고 있다. RFID 시스템은 사용자의 개입 없이 무선 주파수를 이용하여 개체에 대한 정보를 읽거나 기록하는 자동인식 기술 시스템으로 바코드 시스템을 대체할 방법으로 주목받고 있다[1,2]. RFID 시스템은 크게 태그와 리더, 태그에 대한 정보를 보관하는 데이터베이스로 구성되는데, RFID 시스템에서 사용되는 태그는 저장과 연산능력을 가지는 하드웨어 칩으로서 가격이 저렴하며, 물리적인 접촉 없이 리더에 의해 식별이 가능하여 기존의 바코드 식별 방법에 비해 속도가 빠르다는 장점이 있다. 하지만 RFID 시스템은 무선 주파수를 이용하기 때문에 공격자에 의한 불법 행위가 가능하다는 문제가 있다. 예를 들면, 태그와 리더 사이에 전송되는 정보를 공격자가 도청함으로써 태그의 위치 추적이 가능하며, 획득한 정보를 재생하거나 새로운 메시지를 생성하여 전송

* (주)유빗(iksuplorer@nate.com)
논문번호 : KICS2008-11-490, 접수일자 : 2008년 11월 6일, 최종논문접수일자 : 2009년 3월 12일



www.dbpia.co.kr

함으로써 정당한 태그 혹은 리더로 위장할 수 있다.

지금까지 RFID 시스템에서 발생할 수 있는 문제들을 해결하기 위한 많은 연구가 진행되어 왔다[3-9]. 기존 연구들의 특징은 RFID 시스템에 사용되는 태그가 저장과 연산능력에 한계가 있기 때문에 단순한 연산자 및 해시함수를 이용하여 개체를 식별하고 인증한다. 하지만 기존 알고리즘들은 최근의 다양한 공격 방법들을 반영하지 못하거나, 대량의 태그를 인증하기 위해 많은 검색 시간을 요구한다[10,11].

이에 본 논문에서는 효율성을 고려한 해시 함수 기반의 안전한 RFID 인증 프로토콜을 제안한다. 제안 프로토콜은 난수와 ID의 해시 연산을 통해 인증하기 때문에 공격자에 의한 수동적 공격과 능동적 공격에 안전하다. 특히, 제안 프로토콜에서는 데이터베이스가 ID의 위치 정보를 이용하여 ID를 탐색하기 때문에 등록된 태그의 수가 증가하더라도 단지 세 번의 해시 연산만을 통해 태그를 인증할 수 있다. 결국, 확장성 측면에서 기존 프로토콜과 달리 전체 해시 연산수가 태그의 수에 종속되지 않기 때문에 태그의 수가 급속히 증가하는 유비쿼터스 환경에서 효율적이며, 특히 서비스 거부 공격에 의해 발생할 수 데이터베이스의 부하를 크게 감소시킬 수 있는 장점이 있다.

본 논문의 구성은 다음과 같다. 2장과 3장에서는 RFID 시스템과 RFID 시스템을 보호하기 위한 기존의 인증 프로토콜들을 소개한다. 4장에서는 본 논문에서 제안하는 인증 프로토콜을 기술하며 안전성과 효율성을 평가한다. 마지막으로 5장에서는 결론을 맺는다.

## Ⅱ. RFID 시스템

RFID 시스템은 태그, 리더, 데이터베이스로 구성된다. 일반적으로 태그는 식별 및 인증을 위해 개체에 부착되는 마이크로칩으로서 리더의 질의에 따라 저장된 정보를 전송한다. 태그는 자체적으로 전력을 보유하는지 여부에 따라 능동형 태그와 수동형 태그로 분류된다.

능동형 태그는 자체 내장된 배터리를 통해서 전력을 공급하지만 자체 배터리를 내장하기 위한 비용으로 태그의 가격은 증가하며, 태그의 수명은 배터리의 방전 시간에 종속된다는 단점이 있다. 반면, 수동형 태그는 전력 공급을 위한 별도의 배터리가 포함되지 않으며, 리더로부터 수신한 전자기파로부터 유도된 전류를 전원으로 사용한다. 태그의 전송 능력이 낮기 때문에 근거리 통신에만 응용 가능하며, 능동형 태그에 비해 가격이 저렴하다는 장점이 있다.

리더는 태그와 직접적으로 데이터를 송수신하는 장치로서 태그에게 데이터를 요청하고 태그로부터 수신한 정보를 데이터베이스에게 전달한다. 아울러 전력 공급 능력이 없는 수동형 태그에게는 전자기파를 통해 전력을 공급하는 역할을 한다.

데이터베이스는 태그에 관련된 정보를 저장하고 관리하며, 리더로부터 수신된 정보를 통해 태그의 식별 및 인증 작업을 수행한다.

RFID 시스템에 있어서 태그와 리더는 무선 주파수를 이용하여 상호 간에 정보를 교환하기 때문에 도청과 같은 수동적 공격에 매우 취약하며, 재생공격 및 반사공격, 스푸핑 공격, 서비스 거부 공격과 같은 능동적 공격에 취약하다.

- 도청 공격: 도청은 수동적인 공격 방법으로서 공격자가 리더와 태그 사이에 교환되는 메시지를 불법으로 획득하는 공격이다. 도청된 메시지는 공격자에 의해 분석되며, 매 도청 시 동일한 메시지가 전송될 경우 특정 태그를 식별할 수 있기 때문에 공격자는 태그 소유자의 위치를 추적할 수 있다.
- 재생 공격 : 재생 공격은 공격자가 태그와 리더 간에 전송되는 메시지를 도청하여 저장한 후 저장된 메시지를 차후에 재전송함으로써 인증에 성공한다. 이 공격은 태그와 리더 간에 항상 동일한 메시지를 전송할 때 발생한다.
- 반사 공격 : 반사공격은 공격자가 한 개체로부터 생성된 메시지를 저장하고 다시 그 개체에게 재전송하여 인증을 통과하는 방법이다. 시도-응답 프로토콜에서는 신뢰되는 두 개체가 인증 과정에 사용하기 위한 동일한 키 K를 공유하며, 서로 간의 식별을 위해 난수를 생성한다. 개체 A가 난수 $N_1$을 전송하면 개체 B는 암호 값 $E(N_1, K)$와 난수 $N_2$로 응답한다. 개체 A는 개체 B로부터 수신한 $E(N_1, K)$와 자신이 계산한 암호 값을 비교함으로써 개체 B를 인증한다. 인증에 성공하면 개체 A는 $E(N_2, K)$를 개체 B에게 전송하며, 개체 B는 수신한 $E(N_2, K)$와 자신이 계산한 암호 값을 비교하여 개체 A를 인증한다.

  공격자는 공유키 K를 모르기 때문에 송신 개체가 전송한 난수의 암호 값을 송신 개체에게 전송할 수 없다. 하지만, 공격자는 송신 개체가



www.dbpia.co.kr

보낸 난수에 대한 암호 값을 알기 위해서 수신한 난수를 송신 개체에게 재전송하고, 이를 수신 개체의 난수로 인식한 송신 개체는 이에 대한 암호 값을 공격자에게 전송하게 된다. 암호 값을 수신한 공격자는 이 암호 값을 다시 송신 개체에게 전송함으로써 타당한 개체로 가장할 수 있다.

- 스푸핑 공격 : 스푸핑 공격은 공격자가 정당한 리더 혹은 태그로 위장하여 인증을 통과하는 방법으로 앞서 기술한 재생공격과 반사공격은 일종의 스푸핑 공격이다. 재생공격과 반사공격이 불가능할 경우에는 트래픽 분석을 통해 전송되는 메시지에 포함된 태그의 ID나 난수 혹은 키를 예측하여 메시지를 생성해야 한다.
- 서비스 거부 공격 : 서비스 거부 공격은 RFID 시스템이 정상적으로 작동하지 못하도록 많은 메시지를 생성하여 전송함으로써 태그와 리더, 데이터베이스에게 많은 연산을 유발한다.

## Ⅲ. 기존의 RFID 시스템 인증 프로토콜

기존의 RFID 시스템 인증 프로토콜과 제안하는 프로토콜을 설명하기 위해 사용될 용어 및 표기 방법은 다음과 같다.

h() : 해시 함수
ID : 태그에 할당되는 고유정보
P : 데이터베이스에 저장된 ID의 위치
RR : 리더가 생성하는 난수
RT : 태그가 생성하는 난수
⊕ : 비트 XOR 연산
‖ : 연접 연산

Hash-Lock 인증 프로토콜은 해시 함수를 이용하여 리더와 태그간의 인증을 수립하는 대표적인 방법으로 인증 방식이 단순하여 저가의 태그에 적합하다. 하지만 인증과정에서 태그가 항상 고정된 h(key) 값을 리더에게 전송하기 때문에 공격자는 도청을 통해 쉽게 태그를 식별하여 위치를 추적할 수 있다.

RHAP(Randomized Hash-Lock Authentication Protocol)는 Hash-Lock 인증 프로토콜이 항상 고정된 값을 전송하는 문제를 해결하기 위해 난수 생성기를 사용한다[3]. 그림 1은 RHAP에 의한 리더와 태그 간의 인증 과정을 나타낸다. 태그와 데이터베이스는 각각 인증에 필요한 태그의 ID를 저장하고 있으며, 인증 과정은 부여된 번호 순서에 따라 이루어진다.

RHAP에서 태그는 난수를 생성하고 ID 연접하여 해시 연산을 수행하며, 이 결과를 전송하기 때문에 4단계에서 공격자가 태그의 위치를 추적하는 것을 막을 수 있다. 하지만 이 과정에서 공격자가 메시지를 획득할 경우 재생공격을 통해 정당한 태그로의 위조가 가능해진다. 예를 들어 공격자가 메시지를 획득한 후, 차후에 이 메시지를 리더에 전송할 경우에 리더는 데이터베이스에 등록된 태그로 인식하게 된다. 또한 8단계에서는 ID 정보가 평문으로 전송되기 때문에 도청을 통한 태그의 위치 추적이 가능하다. 아울러 데이터베이스에 ID가 존재하는지의 여부를 조사하기 위해서는 최악의 경우에 n번의 해시 연산을 통해 해당 ID가 존재하는지를 검사해야 하기 때문에 대량의 태그가 등록된 데이터베이스 환경에는 적합하지 않다.

Kim 등은 RHAP에 내재된 취약점을 개선하여 위치 추적 및 재생, 스푸핑, 반사 공격에 안전한 인증 프로토콜을 제안하였다[9]. 이 프로토콜은 그림 2에서 알 수 있듯이 리더와 태그간의 인증 과정에서

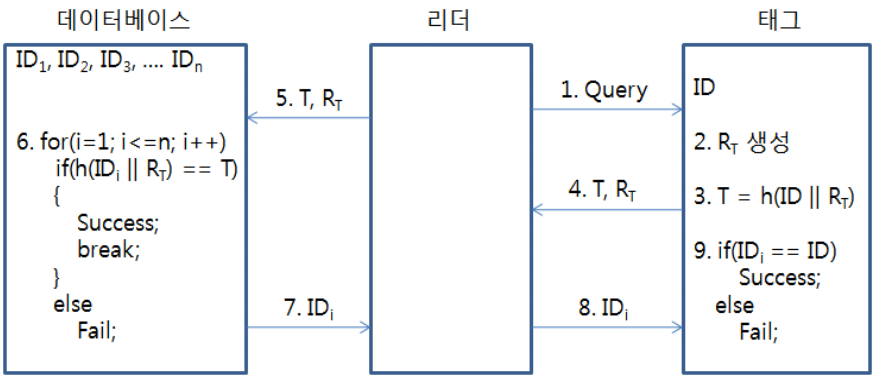


그림 1. RHAP에 의한 리더와 태그 간의 인증 과정



www.dbpia.co.kr

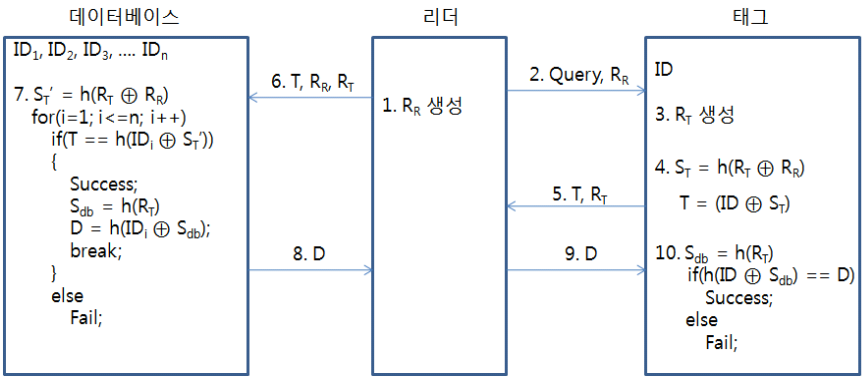


그림 2. Kim 등이 제안한 프로토콜에 의한 리더와 태그 간의 인증 과정

ID 정보가 난수와 함께 XOR 연산 및 해시 연산이 이루어져 전송되기 때문에 공격자에 의한 불법 행위로부터 안전하다. 하지만 데이터베이스와 태그가 상호 인증을 수행하기 위해서는 최악의 경우 n+7번의 해시 연산을 필요로 한다.

CRAP(Challenge-Response based Authentication Protocol)는 Kim 등이 제안한 인증 프로토콜과 같이 리더와 태그간의 인증 과정에서 ID 정보가 난수와 함께 연접 연산 및 해시 연산이 이루어져 전송되기 때문에 공격자에 의한 불법 행위로부터 안전하다[6]. 그림 3은 CRAP에 의한 인증 과정을 나타낸다. 인증에 필요한 해시 연산의 수는 최악의 경우 데이터베이스가 n+1번을 수행하며, 태그는 2번의 연산을 필요로 한다. 즉, Kim 등이 제안한 인증 프로토콜과 비교하여 CRAP은 데이터베이스와 태그에서의 해시 연산이 각각 2번 감소한다는 것을 알 수 있다.

요약하면, 앞선 인증 프로토콜들은 데이터베이스가 보유해야 하는 태그의 ID 수가 증가함에 따라 수행되어야 할 해시 연산이 증가하며, 특히 서비스 거부 공격에 의해 리더가 대량의 메시지를 수신할 경우에는 데이터베이스의 인증 절차에 필요한 n번 이상의 해시 연산으로 인해 서비스 질이 크게 감소될 수 있다.

## Ⅳ. 효율성을 고려한 안전한 RFID 시스템 인증 프로토콜

본 장에서는 공격자에 의한 수동적 공격과 능동적 공격에 안전하고, 인증 과정에 필요한 해시 연산의 수를 최소화함으로써 기존 프로토콜의 효율성을 개선한 인증 프로토콜을 기술한다.

### 4.1 제안하는 인증 프로토콜

안전성을 고려한 기존 RFID 시스템 인증 프로토콜의 가장 큰 문제점은 데이터베이스가 태그를 인증하는 과정에서 최악의 경우 n번 이상의 해시 연산을 요구한다는 것이다. 즉, 태그와 리더 간에 전송되는 ID 정보가 공격자에게 노출되는 것을 막기 위해 ID

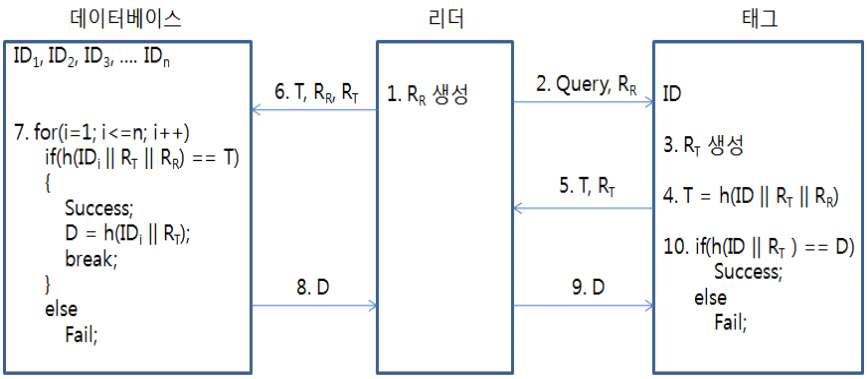


그림 3. CRAP에 의한 리더와 태그 간의 인증 과정



www.dbpia.co.kr

정보와 난수를 연접 연산과 해시연산을 수행한 후 전송하기 때문에, 데이터베이스는 태그를 인증하기 위해서 태그로부터 전달된 난수와 데이터베이스에 저장된 ID 리스트에 대해 동일한 연접 연산과 해시 연산을 수행한 후 서로의 값을 비교해야 한다.

이러한 문제점을 보완하기 위해 제안 프로토콜은 그림 4와 같이 ID 정보와 ID의 위치를 나타내는 위치 정보를 태그와 데이터베이스에 함께 보관한다.

제안 프로토콜은 리더와 태그 간의 상호 인증을 위해 다음 과정을 거친다.

1단계 : 리더가 난수 $R_R$을 생성한다.
2단계 : 리더가 태그에게 질의와 난수 $R_R$을 전송한다.
3단계 : 태그가 난수 $R_T$를 생성한다.
4단계 : 태그는 도청에 의한 불법행위를 방지하기 위해 ID와 난수 $R_T$, $R_R$을 연접한 후 해시 연산을 수행하여 메시지 T를 생성한다.
5단계 : 태그가 리더에게 T, P, $R_T$를 전송한다.
6단계 : 리더가 데이터베이스에게 T, P, $R_T$, $R_R$을 전송한다.
7단계 : 데이터베이스는 수신한 P값을 통해 ID의 위치를 찾고 해당 위치의 $ID_i$와 난수 $R_T$, $R_R$을 연접한 후 해시 연산을 수행한다. 생성된 해시 값과 리더로부터 수신한 T값을 비교하여 일치할 경우 태그가 인증되며, 검색된 $ID_i$와 난수 $R_T$를 연접한 후 해시 연산을 수행하여 메시지 D를 생성하며, $P_i$를 갱신한다.
8단계 : 데이터베이스가 리더에게 D를 전송한다.
9단계 : 리더가 태그에게 D를 전송한다.
10단계 : ID와 난수 $R_T$를 연접한 후 해시 연산을 수행한다. 생성된 해시 값과 리더로부터 수신한 D값을 비교하여 일치할 경우 리더가 인증되며, P가 갱신된다.

### 4.2 인증 프로토콜의 안전성

앞서 살펴본 바와 같이 RFID 시스템의 태그와 리더는 무선 주파수를 이용하여 상호 간에 정보를 교환하기 때문에 도청에 의한 위치 추적과 같은 수동적 공격에 매우 취약하며, 재생공격 및 반사공격, 스푸핑 공격, 서비스 거부 공격과 같은 능동적 공격에도 취약하다. 그 외에 리더와 데이터베이스 사이의 유선 통신 채널에서도 유사하고 다양한 공격들이 발생 가능한데 고속의 유선 통신 채널에서는 강력한 보안 솔루션 적용이 가능하기 때문에 안전하다고 가정하여, 본 절에서는 태그와 리더 간의 취약한 무선 채널에서 발생할 수 있는 공격에 대해서만 안전성 평가를 수행하였다.

- 위치 추적 : 태그의 위치를 추적하기 위해서는 공격자가 5와 9단계에서 전송되는 메시지 T와 D를 도청해야 한다. 하지만 이 메시지들은 태그와 리더가 생성하는 난수 $R_T$, $R_R$에 의해 항상 변하는 해시 값이기 때문에 공격자는 특정 태그를 식별할 수 없으며 결국 태그의 위치를 추적할 수 없다.
- 재생 공격 : 태그와 리더 간에 전송하는 메시지를 공격자가 도청하여 저장하고 차후에 재생할 경우, 재생된 메시지에 포함된 난수는 리더가 새로 생성한 난수와 다르기 때문에 7단계에서의 $h(ID_i \| R_T \| R_R) == T$ 는 성립하지 않아 인증에 실패한다.
- 반사 공격 : 반사 공격에 안전한 인증 프로토콜

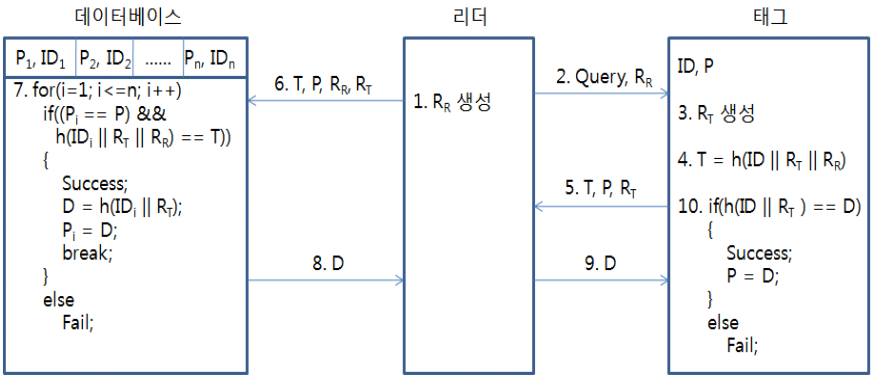


그림 4. 제안 프로토콜에 의한 리더와 태그 간의 인증 과정



www.dbpia.co.kr

은 상호 간에 암호 값을 생성하는 방법이 달라야 한다. 앞서 기술한 시도-응답 프로토콜에서 반사 공격은 두 개체가 시도에 대해 동일한 방법 E(N, K)을 사용하여 응답을 하기 때문에 발생한다. 하지만 제안 프로토콜에서는 개체 간에 응답을 생성하기 위해 서로 다른 $h(ID_i \| R_T \| R_R)$과 $h(ID_i \| R_T)$를 사용하기 때문에 반사 공격이 이루어질 수 없다.

- 스푸핑 공격 : 공격자가 리더로 가장하기 위해서는 올바른 D 값을 계산해야 하며, 태그로 가장하기 위해서는 올바른 T 값을 계산해야 한다. 제안 프로토콜에서 비록 난수 $R_R$과 $R_T$가 평문의 형태로 전송되지만, 메시지 T와 D는 난수와 ID의 연접 연산 및 해시 연산을 통해 생성되기 때문에 ID를 모르는 상태에서 공격자가 올바른 T와 D 값을 계산할 수 없다.
- 서비스 거부 공격 : 서비스 거부 공격을 막기 위해서는 공격자의 물리적인 접근을 차단해야 하지만 이는 정상적인 사용자의 서비스 역시 불가능하게 만든다. 결국 서비스 거부 공격은 정상적인 사용자의 서비스를 제공하기 위한 환경에서는 피할 수 없는 공격이다. 공격자가 서비스 거부 공격을 수행하여 데이터베이스의 해시 연산수를 최대한 증가시키기 위해서는 데이터베이스에 저장되지 않은 ID 정보로 구성된 대량의 인증 요청을 전송해야 한다. 이러한 상황에서 기존의 인증 프로토콜들은 차후 살펴볼 효율성 평가에 근거하여 n번 이상의 해시 연산을 요구하지만, 제안 프로토콜은 ID 정보의 유무를 확인하기 위해 1번의 해시 연산만을 요구하기 때문에 서비스 거부 공격에 더 안전하다.

### 4.3 인증 프로토콜의 효율성 평가

제안하는 인증 프로토콜의 효율성을 평가하기 위해 상호 인증 과정에 필요한 태그와 데이터베이스의 해시 연산수, 메모리 사용량을 기존 인증 프로토콜과 비교하였다. 그리고 효율성 평가에 있어서 데이터베이스는 n개의 태그 정보를 저장하고 있으며, 인증에 필요한 각 정보들은 L비트의 길이를 갖는다고 가정한다.

표 1과 같이 RHAP는 전체적인 해시 연산수와 메모리 사용량에 있어서 타 인증 프로토콜보다 효율적이지만, 앞서 기술했듯이 ID 정보가 도청에 의해 쉽게 유출될 수 있기 때문에 안전하지 못하다. 반면, Kim 등이 제안한 프로토콜과 CRAP은 공격자의 불법행위에 안전하지만, 데이터베이스에 등록된 태그의

표 1. 인증 프로토콜 효율성 평가

| | RHAP | Kim 등 | CRAP | 제안 프로토콜 |
|---|---|---|---|---|
| 데이터베이스 해시 연산 | n번 | n+3 | n+1 | 3 |
| 태그 해시 연산 | 1 | 4 | 2 | 2 |
| 데이터베이스 메모리 사용량 | n×L | n×L | n×L | n×2L |
| 태그 메모리 사용량 | L | L | L | 2L |

수가 증가함에 따라 태그를 인증하기 위해 데이터베이스에서 최악의 경우 n번 이상의 해시 연산이 요구된다. 하지만 제안 프로토콜은 ID의 위치 정보를 통해 ID를 찾아 인증을 수행하기 때문에 태그의 수에 상관없이 항상 2번의 해시연산만으로도 태그의 인증이 가능하다. 그런데 제안 프로토콜은 다른 알고리즘과 달리 데이터베이스에서 ID의 위치를 검색하기 위한 추가적인 연산이 발생한다. n개의 ID 위치 정보를 저장하고 있는 데이터베이스에서 특정 ID를 검색하기 위한 알고리즘으로써 순차검색 알고리즘을 이용할 경우에는 최대 n번, 이진검색 알고리즘을 이용할 경우에는 log2n 번의 검색 작업이 필요하다. 용이한 효율성 평가를 위해 제안 프로토콜이 ID 검색에 해시 알고리즘을 사용한다고 가정하면, 데이터베이스에서는 1번의 추가적인 해시 연산을 필요로 하기 때문에 최대 3번의 해시 연산만이 필요하다. 이는 확장성 측면에서 기존 프로토콜과 달리 제안 프로토콜에서의 전체 해시 연산수가 태그의 수에 종속되지 않기 때문에 태그의 수가 급속히 증가하는 유비쿼터스 환경에서 효율적이다 할 수 있다. 아울러 태그 상에서의 인증 과정을 고려하면 2번의 해시 연산만을 필요로 하기 때문에 저가로 생산된 태그에 적합하다.

각 태그의 정보를 저장하기 위한 데이터베이스 메모리 사용량에 있어서는 태그의 수가 증가함에 따라 2배씩 증가하며, 태그의 메모리에 ID 위치 정보를 저장하기 위해 추가적인 L비트를 요구하지만, EPC(Electronic Product Code)의 표준에 따라 태그 ID의 길이가 96 비트를 따르기 때문에 다른 프로토콜에 비해 구현상의 비용이 크게 증가하지 않는다.

## V. 결 론

최근 들어 유비쿼터스 환경 구축을 위해 RFID 시스템에 관한 연구가 진행되고 있다. 하지만 RFID 시스템은 태그와 리더 간에 무선 주파수를 이용하기 때문에 보안상 매우 취약하다. 이에 안전한 유비



www.dbpia.co.kr

퀴터스 환경 구축을 위해 RFID 시스템 인증 프로토콜들이 제안되어 왔지만 이들은 최근의 다양한 공격 방법들에 적절히 대응하지 못하거나, 대량의 태그를 인증하기 위해 많은 해시 연산을 필요로 하기 때문에 효율성의 문제가 있다.

이에 본 논문에서는 대량의 태그가 등록된 데이터베이스의 효율성을 개선하기 위한 해시 함수 기반의 안전한 RFID 인증 프로토콜을 제안하였다. 제안 프로토콜은 데이터베이스가 ID의 위치 정보를 이용하여 ID를 탐색하기 때문에 등록된 태그의 수가 증가하더라도 단지 세 번의 해시 연산만을 통해 태그를 인증할 수 있다. 특히, 기존 프로토콜들에서는 공격자가 태그를 가장하여 대량의 인증 정보를 전송할 경우에, 데이터베이스는 등록된 모든 ID에 대해 해시 연산을 수행하기 때문에 데이터베이스의 부하가 크게 증가하지만 제안 프로토콜은 ID 탐색을 위한 한 번의 해시 연산만을 수행하기 때문에 부하를 크게 줄일 수 있다. 그리고 태그의 ID가 난수와 연접 및 해시 연산을 통해 전송되기 때문에 메시지의 추측이 불가능하여 위치 추적, 재생, 반사, 스푸핑 공격에 안전하다. 비록 제안 프로토콜은 기존 프로토콜과 비교하여 구현에 있어서 추가적인 메모리 비트를 요구하지만 그 비용이 크게 증가되지 않으며, 인증에 소요되는 해시 연산의 수와 서비스 거부 공격이 발생했을 때 수행되는 해시 연산의 수를 고려하면 그 비용은 큰 문제가 되지 않는다고 판단된다.

## 참 고 문 헌


〔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 System", Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212, 2004.

〔4〕 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.

〔5〕 S. Lee, Y. Hwang, D. Lee, and J. Lim, "Efficient Authentication for Low-cost RFID Systems", ICCSA'05, LNCS 3480, pp. 619-627, 2005.

〔6〕 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, 2005.

〔7〕 E. Choi, S. Lee, and D. Lee, "Efficient RFID Authentication Protocol for Ubiquitous Computing Environment", EUC-2005, LNCS 3823, pp. 945-954, 2005.

〔8〕 A. Juels and R. Pappu, "Squealing euros: Privacy Protection in RFID-Enabled Banknotes", In proceedings of Financial Cryptography-FC'03, LNCS 2742, pp. 103-121, 2003.

〔9〕 김배현, 유인태, "반사공격에 안전한 RFID 인증 프로토콜", 한국통신학회논문지, 제 32권, 제 3호, pp. 348-354, 2007.

〔10〕 하재철, 하정훈, 박제훈, 김환구, 문상재, "분산 환경에 적합한 저비용 RFID 인증 프로토콜", 한국정보보호학회하계학술대회 논문집, 제 17권, 제 1호, pp. 78-83, 2007.

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



**김 익 수** (Ik-Su Kim) 정회원

2000년 2월 숭실대학교 컴퓨터학과 학사

2002년 2월 숭실대학교 컴퓨터학과 석사

2008년 2월 숭실대학교 컴퓨터학과 박사

2006년~2009년 (주)스카이컴 과장

<관심분야> 시스템 보안, 네트워크 보안, 모바일 보안, 시스템 소프트웨어




www.dbpia.co.kr