반사공격에 안전한 RFID 인증 프로토콜

정회원 김 배 현*, 유 인 태**

RFID Mutual Authentication Protocol Against Reflection Attack

Baehyun Kim*, Intae Ryoo** ***Regular Members***

요 약

RFID(Radio Frequency Identification) 시스템은 유비쿼터스 컴퓨팅 환경에서 주목 받는 기술이다. RFID 시스템은 물류, 유통, 의료 등 다양한 분야에 적용 가능하지만 프라이버시 침해 문제가 존재하기 때문에 이를 해결하기위한 많은 연구가 이루어지고 있다. 그러나 기존의 RFID 인증 프로토콜은 프라이버시 침해나 효율성에서 여전히 문제점들을 가지고 있다. 따라서 본 논문에서는 프라이버시 보호를 위한 기존의 인증 프로토콜보다 안전성이 개선된 RFID 상호 인증 프로토콜을 제안한다. 제안하는 인증 프로토콜은 상호인증이 가능하고 위치 추적, 스푸핑 공격, 반사 공격에 안전하다.

Key Words : RFID, Mutual Authentication, Reflection Attack

ABSTRACT

RFID system is emerging new technology for ubiquitous computing environment. RFID system, however, provides privacy problems while the technology offers incredible rich opportunities for applications in the filed of logistics, distribution, and medical services, etc. Many researches have been conducted in order to solve this problem, but the current RFID authentication protocols are still insufficient for settling the privacy problem in the point of view of privacy intrusion and system efficiency. The purpose of this paper is to present a RFID mutual authentication protocol which improves safety level, compared with current authentication protocols. The proposed authentication protocol can provide mutual authentication services, and is secure against location tracing, spoofing, reflection attack.

Ⅰ. 서 론

유비쿼터스 컴퓨팅 환경의 실현을 위한 핵심 기술로 RFID 시스템이 주목을 받고 있다. RFID 시스템은 태그에 저장된 정보를 무선 주파수를 이용하여 비접촉 방식으로 읽거나 정보를 기록할 수 있는 자동인식(Automatic Identification) 기술이다. RFID를 이용하면 기존의 바코드(Barcode) 시스템을 대체할 수 있다. RFID 시스템은 바코드 시스템이 가지고 있는 일회성 문제를 해결할 수 있기 때문에 물류 및 유통 관리의 자동화뿐만 아니라 의료, 금융, 교통 등 다양한 분야에 활용이 가능하다. 그러나 RFID 태그는 객체를 유일하게 식별하기 위한 정보를 가지고 있기 때문에 개인정보의 노출, 위치 추적 등의 프라이버시 침해를 유발할 수 있다는 문제점이 있다[1,2,6].

RFID의 프라이버시 침해 문제를 해결하기위한 많은 연구가 진행되어 왔다. 대표적인 기존의 연구는 해시함수, 암호학적 알고리즘 또는 단순한 연산자를 사용하는 다양한 기법들이 제안되었다[2,3,4,5]. 본 논문에서는 RFID의 프라이버시 침해 문제를 해결하기위해 해시함수를 이용한 효율적인 상호인증

* 호원대학교 사이버수사경찰학부 (bhyunkim@khu.ac.kr), ** 경희대학교 전자정보대학 (itryoo@khu.ac.kr)
논문번호 : KICS2006-12-519, 접수일자 : 2006년 12월 5일, 최종논문접수일자 : 2007년 3월 19일

기법을 제안한다.

본 논문의 구성은 다음과 같다.

2장에서는 RFID 시스템의 구성요소와 보안 고려사항에 대하여 기술하고3장에서는 기존RFID 인증 프로토콜을 기술한다. 4장에서는 본 논문에서 제안하는 RFID 상호 인증 프로토콜을 기술하고 안전성과 효율성을 분석한다. 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. RFID 시스템

RFID 시스템의 구성요소와 보안관련 문제에 대하여 알아본다.

2.1. RFID 시스템 구성요소

RFID 시스템은 3가지 구성요소인 태그(Tag), 리더(Reader), 그리고 백-엔드 데이터베이스(Back-end Database)로 구성된다.

- 태그(Tag): 태그는 RFID 시스템에서 리더의 질의에 태그에 저장된 식별정보를 무선 통신을 사용하여 전송한다. 태그의 구성은 무선 통신을 위한 안테나와 연산을 수행하고 정보를 저장하는 마이크로 칩으로 이루어져있다. 태그는 전력을 공급받는 방법에 따라 능동형 태그(Active Tag)와 수동형 태그(Passive Tag)로 구분된다.
  - ✓ 능동형 태그: 능동형 태그는 자체 내장된 배터리를 통해서 전력을 공급한다. 자체 내장된 배터리를 사용하기 때문에 원거리 정보 전송이 가능하다. 하지만 자체 배터리가 내장되어 있어서 태그의 가격이 비싸며, 태그의 수명도 배터리에 종속적이라는 단점을 갖는다. 능동형 태그는 토목·건축분야, 의료분야 등에 사용된다.
  - ✓ 수동형 태그: 수동형 태그는 리더로부터 수신한 전자기파에 의해 유도된 전류를 전원으로 사용한다. 태그의 전송 전력이 리더에 비해 낮기 때문에 근거리 통신에 이용된다. 수동형 태그는 배터리를 내장하고 있지 않기 때문에 능동형 태그보다 가격이 싸며, 태그의 수명이 반영구적이다. 수동형 태그는 물류관리, 전자상거래, 교통 분야, 전자물체감시 시스템 분야 등에 사용된다.
- 리더(Reader): 리더는 태그가 전송하는 데이터를 수신하여 태그를 인식하거나 태그에 새로운 정보를 다시 쓰는 역할을 수행하는 장치이다. 리더가 태그에 무선 통신을 사용하여 태그에 정보를 요청하고 받은 정보를 데이터베이스에 전송한다. 리더는 수동형 태그에 RF 신호를 전송하여 전력을 공급한다.
- 백-엔드 데이터베이스(Back-end Database): 백-엔드 데이터베이스는 태그에 관련된 정보를 저장하고 관리하며, 연산 능력이 낮은 태그 또는 리더를 대신하여 복잡한 연산을 대신 수행하기도 한다. 즉, 데이터베이스는 정당한 리더로부터 전송된 임의의 태그의 정보를 통해서 개체를 식별하는 기능을 수행한다.

본 논문은 RFID 시스템의 리더와 백-엔드 데이터베이스 사이의 통신 채널이 공격자로부터 안전하다고 가정한다.

2.2 RFID 시스템의 보안 고려사항

RFID 시스템의 보안 취약점을 알아보고 이를 바탕으로 RFID 인증 프로토콜을 설계하기위한 보안 고려사항에 대하여 알아본다.

RFID 시스템의 태그-리더 구간은 무선 통신 구간이기 때문에 다음과 같은 보안 취약점을 가지고 있다.[6,9]

- 도청(Eavesdropping): RFID 시스템의 태그와 리더간은 무선통신을 전제로 하고 있다. 따라서 공격자가 리더를 갖고 태그를 스캔하는 적극적 공격과, 리더와 태그 간에 전송되는 데이터를 도청하는 수동적 공격이 가능하다. 도청을 통해서 얻은 정보는 공격에 활용될 수 있다.
- 트래픽 분석(Traffic Analysis): 공격자는 도청을 통해 얻은 트래픽을 분석하면 여러 가지 정보를 알아낼 수 있다.예를 들어 그 지역에서 어느 정도의 트래픽이 존재하는지, 어느 정도의 물품이 존재하고, 빠져나가는지에 대해서 알 수 있다.또한, 트래픽 분석을 통해서 위치 추적(Location Tracking)이 가능하다. 비록 패킷 내용이 암호화되어 있더라도 같은 비트 패턴의 태그가 이동하는 것을 알 수 있기 때문에 태그의 움직임을 알 수 있다.
- 스푸핑 공격(Spoofing Attack): 공격자는 도청한 정보를 이용하여 임의의 태그에게 자신이 정당한 리더인 것처럼 가장하여 태그 정보를 얻거나, 임의의 리더에게 자신이 정당한 태그인 것처럼 가

장하여 리더에게 거짓 정보를 보낼 수 있다.

- 서비스 거부 공격(Denial of service Attack): 서비스 거부 공격은 RFID 시스템이 작동을 못하도록 하는 위협이다. 예를 들어, 공격자는 RFID 시스템이 사용하는 주파수 영역을 교란하는 방해전파를 발산하여 통신이 불가능하게 할 수 있다. 또한, 리더와 태그 간에 질의/응답(Query/Response) 메커니즘을 이용하여 공격자가 리더를 가지고 수많은 질의를 리더 및 태그에게 보내면 리더와 태그는 많은 질의에 대하여 응답을 하게 된다. 이는 너무 많은 계산이 요구하게 되어, 리더와 태그가 정상적인 기능을 하지 못하도록 하는 결과를 초래한다.
- 물리적 공격(Physical Attack): 태그는 제한된 생산가격으로 인해 고가의 시스템에 사용되는 고가의 메모리나 칩을 사용하기가 힘들다. 따라서 프로브 공격이나 TEMPEST 공격 등에 취약하다.

이와 같은 RFID 시스템의 보안 취약점으로부터 안전한 인증 프로토콜을 설계하기 위한 고려사항은 다음과 같다[9].

- 상호인증: RFID 시스템이 통신하는 상대에 대한 인증 절차가 없다면, 공격자는 리더나 태그를 위조하는 것이 가능하다. 또한 통신하는 태그나 리더 중 하나만을 인증하는 일방향 인증일 경우에도 인증되지 않은 다른 하나에 대해서는 위조하는 것이 가능하기 때문에 스푸핑 공격(spoofing attack)과 재전송 공격(replay attack)에 안전하지 않다. 따라서 태그와 리더가 상호 인증을 해야만 스푸핑 공격 방지, 재전송 공격 방지를 할 수 있다.
- 위치추적 방지: RFID 시스템의 태그가 가지고 있는 정보를 이용하여 위치 추적이 가능하다. 그러나 정당하지 않은 시스템에 의한 태그의 이동 경로를 파악하는 것이 불가능해야 한다.

Ⅲ. 기존 RFID 인증 프로토콜

기존에 제안된 RFID 인증 프로토콜에 대하여 알아본다.

3.1 KILL 명령어

MIT의 Auto_ID 센터(현재 EPCglobal)에서 제안한 방식으로 태그는 8비트의 패스워드를 내장하고 있다가 동일한 패스워드와 Kill 명령이 수신되면 태그 내부의 회로들이 완전히 단락 되어,태그의 모든 기능을 중지시켜 다시 사용할 수 없도록 하는 것이다. 한 번 중지된 태그는 되살릴 수 없기 때문에 태그를 재사용할 필요가 있는 분야에서는 적용이 불가능하다. 이 방식은 현재 EPC 클래스 1 태그와 ISO 18000 Part 6 Type C 태그에 기본 기능으로 내장되고 있다.

3.2 해시-락(Hash Lock) 인증 프로토콜

해시-락 RFID 인증 프로토콜은 해시 함수를 한 번만 사용하기 때문에 저가로 구현 가능하다. 이 방식에서 태그는 기본적으로 잠김 상태에 있으며, 태그가 사용하는 난수 형태의 키에 대한 해시 값 metaID을 DB와 태그에 저장한다. 리더가 태그에게 Query를 보내면 태그는 metaID를 전송한다. 리더는 DB에서 이 metaID에 해당되는 ID와 키를 가져와서 태그에게 키만을 전송한다. 태그는 키에 대한 해시 값을 계산하여 자신의metaID와 일치하는 경우에만 잠김 상태에서 빠져나와 자신의 ID를 리더에게 전송한다. 이 방식은 태그가 가지는 metaID가 항상 일정하기 때문에 위치 추적이 가능하다는 단점을 가지고 있으며 공격자가 태그의 metaID를 입수하여 정당한 리더에게 재사용(replay)하여 보내는 경우 리더는 올바른 키를 공격자에게 보내게 되는 위험이 있다.

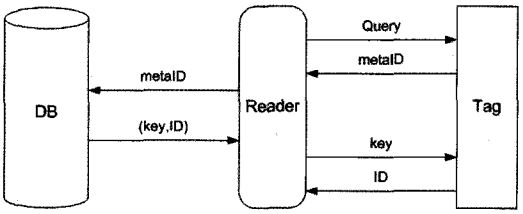

그림 1. 해시-락 인증 프로토콜

3.3 확장된 해시-락(Randomized Hash Lock) 인증 프로토콜

확장된 해시-락 인증 프로토콜은 해시-락 방식에서 metaID가 항상 동일한 값을 가지는 문제점을 해결하기 위해 난수 R을 사용한다. 태그는 의사난수 생성기(RNG: Random Number Generator)를 가지며, 생성한 난수와 자신의 ID로 해시 값을 계산하여 리더로 전송하기 때문에 항상 해시 값이 변하게 된다. 리더는 태그로부터 전달된 해시 값과 난수를 가지고 서버로부터 모든 태그의 ID를 받아서 해시

값을 계산하여 리드로부터 수신한 해시 값과 일치되는 태그의 ID를 찾은 후 태그로 전송한다. 이 방식은 해시-락 방식의 metaID에 대한 추적을 피할 수 있으나 태그에 의사난수생성기를 내장하여야 하며 서버/리더기의 계산량이 많아진다는 부담이 있다. 또한 공격자가 R, $h(ID_K||R)$ 메시지를 재전송할 경우, 정당한 태그로 가장할 수 있는 스푸핑 공격이 가능하고 마지막 단계에서 리더가 태그에게 전송하는 ID_k가 노출된다.

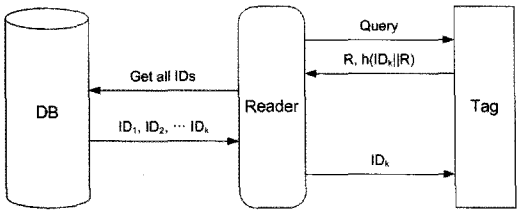

그림 2. 확장된 해시-락 인증 프로토콜

3.4 해시 체인(Hash-chain) 인증 프로토콜

해시 체인 인증 프로토콜은 두 개의 해시함수 H와 G를 사용하여 해시체인을 구성하며, 태그가 초기에 정보 S_i를 가진다. 태그는 리더와의 i번째 통신에서 $Ai=G(S_i)$를 보내고 자신의 정보는 $S_i+1=H(S_i)$로 갱신하여 보안을 유지한다. 태그가 리더에게 응답할 때는 H 함수를 사용하고, 태그의 Si값을 갱신하기 위해서는 G함수를 사용하여 세션마다 다른 A_i값을 전송하므로 위치 추적 공격에 안전하다. 그러나 백-엔드 시스템에서의 계산량이 많고 2개의 해시 함수를 사용한다는 점이 확장된 해시-락 인증 프로토콜에 비해 부담이 된다.

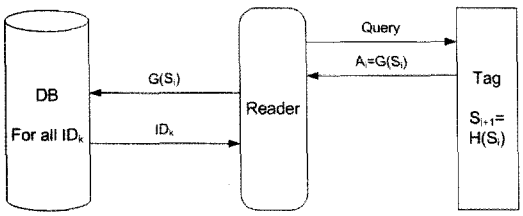

그림 3. 해시 체인 인증 프로토콜

3.5 재 암호화 방식(re-encryption)

재 암호화 방식은 ElGamel 공개키 암호화 알고리즘을 기반으로 하고 있으며, 유로화 지폐에 RFID 태그를 내장하기 위해 사용되는 방식이다. 이 방식은 태그가 전송하는 ID의 암호문 c를 임의의 난수 r과 공개키를 이용하여 새로운 암호문(c')으로 변형하는 것이다. 즉, r에 의해 ID에 대한 여러 개의 암호문이 생성가능하기 때문에 사용자의 추적이 불가능하다. 이 방식은 리더나 백-엔드 시스템에서 고유 ID를 암호화하여 태그에 저장하기 때문에 공개키를 알고 있는 믿을만한 리더나 백-엔드 시스템만이 태그 정보를 확인할 수 있다.

Ⅳ. 제안 프로토콜

본 장에서는 Ⅱ장 2절의 RFID 인증 프로토콜 설계 시 고려사항을 바탕으로 RFID 상호 인증 프로토콜을 제안하고 안정성을 분석한다.

4.1 제안 인증 프로토콜의 구성

제안하는 RFID 상호 인증 프로토콜의 전체적인 구성과 동작은 그림 4와 같다.

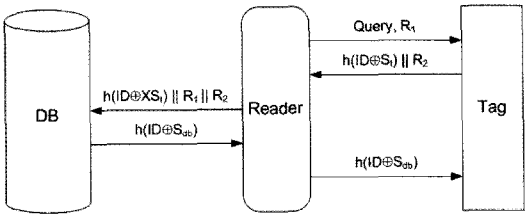

그림 4. 제안 인증 프로토콜

〔용어정의〕

- Query: 태그의 응답을 요청하는 리더의 요청
- ID:태그에 할당된 고유정보
- ||: 연접
- h(): 일 방향 해시
- R_1: 리더가 생성한 난수
- R_2: 태그가 생성한 난수
- S_t: $h(R1 \oplus R2)$
- S_{db}: $h(R2)$

본 논문에서 제안하는 프로토콜의 인증과정은 다음과 같다. 리더는 태그를 인증하기위해 난수 R_1을 생성하여 Query와 함께 태그로 전송한다. 태그는 Query를 수신한 후, 리더를 인증하기 위한 R_2를 생성한다. 그리고 태그는 R_1와 R_2를 이용하여 S_t를 계산하고, R_2와 함께 리더에게 전송한다. 리더는 수신한 "$h(ID \oplus S_t) \parallel R_2$" 메시지에 R_1을 연접하여 DB에게 전송한다. DB는 수신한 R_1과 R_2를 이용하여 S_t'를 계산한 후, 수신한 St와 비교한다. S_t'와 S_t가 일치하면, DB에 저장되어 있는 ID를 이용하여 수

신된 $h(ID \oplus S_t)$와 일치하는 값을 찾는다. 수신된 $h(ID \oplus S_t)$와 DB에서 계산된 $h(ID \oplus S_t)$'가 일치하지 않는다면, Error 메시지를 전송한다. 수신된 $h(ID \oplus S_t)$와 DB에서 계산된 $h(ID \oplus S_t)$'가 일치한다면 리더가 인증된다. 그리고 DB는 R_2를 이용하여 S_{db}를 계산한 후, 리더가 DB를 인증하기 위한 $h(ID \oplus S_{db})$ 메시지를 리더에게 전송한다. 리더는 Error메시지를 수신한 경우, 태그와 통신을 중단하고 $h(ID \oplus S_{db})$ 메시지를 수신한 경우 태그에게 전송한다. 태그는 $h(ID \oplus S_{db})$ 메시지를 수신하면, 자신이 저장하고 있는 R_2와 자신의 ID를 이용하여 $h(ID \oplus S_{db})$'를 계산한다. 수신된 $h(ID \oplus S_{db})$와 계산된 $h(ID \oplus S_{db})$'이 일치하면, DB가 인증된다.

Step 1. 리더 -> 태그: Query, R_1
Step 2. 태그 → 리더: $h(ID \oplus S_t) \parallel R_2$
Step 3. 리더 → 백-엔드 DB: $h(ID \oplus S_t) \parallel R_2 \parallel R_1$
Step 4. DB → 리더: R_1과 R_2를 이용하여 S'를 계산
- $h(ID \oplus S_t) \neq h(ID \oplus S_t)$' 이면, Error 메시지를 전송
- $h(ID \oplus S_t)$ = 계산된 $h(ID \oplus S_t)$ 이면, $h(ID \oplus S_{db})$ 메시지 전송

Step 5. 리더 → 태그: $h(ID \| R_2)$
Step 6. 태그: 태그는 $h(ID \| S_{db}) = h(ID \| S_{db})$' 이면, 리더 인증

4.2 안전성 분석

제안하는 인증 프로토콜의 안정성은 RFID 인증 프로토콜 설계 시 고려사항을 고려하여 분석한다.

본 논문에서 리더가 태그를 인증할 뿐만 아니라, 태그가 리더를 인증하는 상호 인증 프로토콜을 제안하였다. 제안된 상호 인증 프로토콜은 재전송 공격, 스푸핑 공격 등뿐만 아니라, 반사공격에도 안전하다.

- 상호인증: 리더의 태그 인증은 step 1에서 리더가 전송한 랜덤 값 R_1에 대한 step 2의 "$h(ID \oplus S_t)$" 메시지에 의해 이루어진다. 태그의 리더 인증은 태그가 생성한 R_2에 대한 step 5의 "$h(ID \oplus S_{db})$"메시지에 의해 이루어진다.
- 재전송 공격 방지: step 2의 "$h(ID \oplus S_t) \parallel R_2$" 메시지의 값이 매번 변화하기 때문에 재전송 공격에 안전하다.
- 위치 추적 방지: step2에서 $h(ID \oplus S_t)$의 S_t 와 step 5에서 $h(ID \oplus S_{db})$의 S_{db}가 매 세션 마다 변하기 때문에 공격자가 특정 태그를 식별할 수 없어 위치 추적에 안전하다.

해시함수는 익명성, 무결성, 인증성 등의 보안 서비스를 제공하지만 기밀성을 제공하지 않는다. 따라서 스푸핑 공격의 일종인 반사공격(reflection attack)에도 취약하다.

일반적으로 시도-응답(challenge-response) 프로토콜을 상호인증으로 확장하면 난수 r_1은 서버에 대한 시도, 난수 r_2는 클라이언트에 대한 시도로 사용된다(그림 5). 하지만, 클라이언트와 서버 간에 1개 이상의 세션을 동시에 여는 것이 가능하기 때문에 공격자는 정당한 클라이언트를 가장하는 반사공격에 노출될 수 있다. 그림 5에서 공격자가 클라이언트로 가장하여 서버와 함께 상호 인증 프로토콜을 시작하였다고 가정하다. 서버로부터 r_2를 받은 공격자는 대칭키를 모르기 때문에 응답 $H(r_2)$를 보낼 수 없다. 그러나 공격자가 두 번째 세션을 열어 client, r_2를 시도로 보낸다. 서버가 응답 $H(r_2)$를 보내면, 두 번째 세션을 일방적으로 종료하고 서버로부터 응답으로 받은 $H(r_2)$를 첫 번째 세션의 응답으로 보내면 처음 세션의 인증 과정을 통과할 수 있다. 반사공격이 가능한 근본적인 원인은 클라이언트와 서버가 난수 r에 대한 응답을 모두 동일한 방식인 H(r)로 계산하기 때문이다.

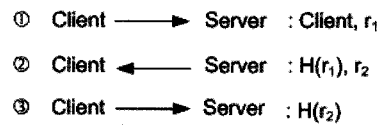

그림 5. 단순 상호인증 프로토콜

- 반사공격 방지: 본 논문에서 제안하는 RFID 상호 인증 프로토콜은 이러한 반사공격에 안전하도록 하기위해, 시도(challenge)나 응답(response)을 리더와 태그 간에 구별할 수 있는 방식을 사용한다. 제안된 상호인증 프로토콜에서 태그가 리터에게 보내는 메시지 $h(ID \oplus S_t)$의 S_t는 R_1과 R_2로 해시 연산을 수행하며, 리더가 태그에게 보내는 메시지 $h(ID \oplus S_{db})$의 S_{db}는 R2로 해시 연산을 수행한다. 즉 $h(ID \oplus S_t)$와 $h(ID \oplus S_{db})$가 서로 다른 방식으로 해시 값을 계산하도록 하였기 때문에 반사공격에 안전하다.

4.3 효율성 분석

본 논문에서 제안하는 인증 프로토콜의 효율성 분석하기 위해 랜덤 해시-락 기법과 인증시간을 비교해보았다. 그림 6은 검색할 ID의 개수가 각각 5,000개, 10,000개 50,000개, 100,000개 일 때 인증 시간을 보여준다. 제안 인증 프로토콜은 안정성을 증가시키기 위해 랜덤 해시-락 기법에 비해 3회 더 많은 연산을 수행한다. 그러나 랜덤 해시-락 기법은 ID를 검색하기 위해 DB에서 리더로 모든 ID를 전송해야 하지만, 제안 인증 프로토콜은 ID가 저장되어 있는 DB에서 검색을 수행하기 때문에 모든 ID를 리더로 전송하는 시간을 줄일 수 있다. 따라서 제안 인증 프로토콜이 랜덤 해시-락 기법에 비해 전체적인 인증 시간이 감소한다는 것을 알 수 있다.

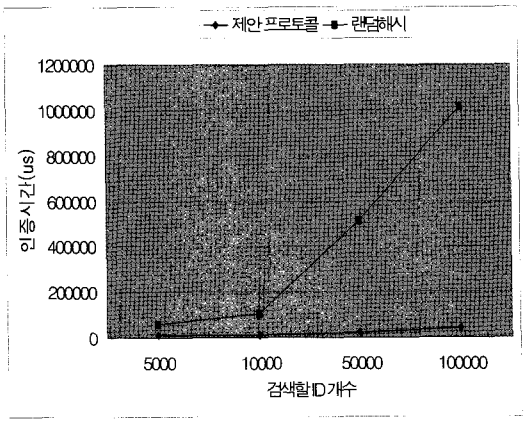

그림 6. 랜덤 해시와 제안 인증 프로토콜의 인증 시간 비교

V. 결 론

RFID 시스템은 물류, 유통, 의료, 금융 등 다양한 분야에서 자동 인식 기술로 활용 가능하기 때문에 향후 도래할 유비쿼터스 컴퓨팅 환경의 핵심 기술로 주목 받고 있으며 국내외에서 많은 연구가 행해지고 있다. 그러나 무선통신 환경을 기반으로 하는 RFID 시스템은 안전한 인증 프로토콜이 적용되지 않을 경우, 개인정보의 노출, 위치 추적 등의 프라이버시 침해를 유발할 수 있다는 문제점이 있다. 기존의 RFID 시스템을 위한 많은 인증 프로토콜이 연구되었지만, 프라이버시 침해나 효율성에서 여전히 문제점들을 가지고 있다.

본 논문에서는 기존의 RFID 인증 프로토콜을 분석하였고, 이를 바탕으로 해시를 이용한 RFID 상호 인증 프로토콜을 제안했다. 제안된 인증 프로토콜은 위치 추적, 재전송 공격, 스푸핑 공격에 안전할 뿐만 아니라 단순한 상호 인증 방식에서 취약했던 반사공격에도 안전하다. 또한 제안된 인증 프로토콜과 기존 랜덤 해시-락 기법의 인증 시간을 비교를 통해 제안된 인증 프로토콜이 더욱 효율적임을 확인하였다. 따라서 제안된 인증 프로토콜은 RFID 시스템뿐만 아니라 유비쿼터스 컴퓨팅 환경의 다양한 분야에 적용이 가능할 것으로 기대된다.

참 고 문 헌

[1] A. Juels, R. L. Rivest, M Szydlo "The Blocker Tag: Selective Blocking of RFID Tags for consumer Privacy", In Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp.103-111, 2003.

[2] S. A. Weis, S. E. Sarma, R. L. Rivest, D. and W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, Springer-Verlag, 2004.

[3] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID", Proceedings of the SCIS 2004, pp.719-724, 2004.

[4] S. E. Sarma, S. A. Weis, D. W. Engels. "RFID systems, Security & Privacy Implications", White Paper MIT-AUTOID-WH_014, MIT AUTO-ID CENTER, 2002.

[5] A. Juels and R. Pappu, "Squealing euros: Privacy protection in RFID-Enabled banknotes", In proceedings of Financial Cryptography-FC'03, vol. 2742 LNCS, pp.103-121, Springer-Verlag, 2003.

[6] S. Junichiro, R. Jae-Cheol and S. Kouichi, "Enhancing privady of Universal Re-encryption scheme for RFID Tags", EUC 2004, Vol. 3207 LNCS, pp.879-890, Springer-Verlag, 2004.

[7] F. Klaus, "RFID Handbook", second edition, Jone Willey & Sons, 2003.

[8] 양형규, 안영화, "유비쿼터스 컴퓨팅 환경에 적합한 RFID 인증 프로토콜에 관한 연구", 전자공학회논문지 42권 CI 1호, pp. 45-50, 2005.
[9] 최은영, 최동희, 임종인, 이동훈, "저가형 RFID 시스템을 위한 효율적인 인증 프로토콜" 정보보호학회논문지 15권 5호, pp.59-71, 2005.

김 배 현 (Baehyun Kim) 정회원

1995년 2월 : 호원대학교 전자계산학과 졸업
1997년 2월 : 수원대학교 전자계산학과 석사
2003년 2월 : 경희대학교 컴퓨터공학과 박사수료
2004년~2007년 : 한신대학교 정보통신공학과 겸임교수
2007년 3월~현재 : 호원대학교 사이버수사경찰학부 연구교수
<관심분야> Mobile IP, 차세대 인터넷, 네트워크 보안,

유 인 태 (Intae Ryoo) 정회원

1995년 2월 : 연세대학교 전자공학과 졸업
1989년 2월 : 연세대학교 전자공학과 석사
1994년 2월 : 연세대학교 전자공학과 박사
1997년 8월 : 동경대학 전자정보통신전공 Ph.D
1999년 : 삼성전자 정보통신총괄 선임연구원
1999년~ 현재: 경희대학교 전자정보대학 부교수
<관심분야> 인터넷, 네트워크 보안, 무선 LAN, IPT