행렬기반 RFID 인증 프로토콜에 대한 연구

이수연* · 안효범**

요 약

최근 RFID/USN 환경에서 정보보호는 네트워크 보안 및 RFID 정보보호 기술로 구분될 수 있다. 특히, 저가의 RFID 시스템에 개인 프라이버시 보호를 위한 인증 프로토콜 설계가 활발히 연구되고 있다. 그러나, 저가의 RFID 태그의 생산과 사용자 프라이버시 보호를 위한 안전한 인증 프로토콜의 개발은 미흡한 실정이다. 따라서, 본 논문에서는 기존의 인증 프로토콜보다 RFID 태그에서 계산량을 감소시키고 통신 오버헤드를 감소시키므로 개인 프라이버시 보호를 위한 효율적인 행렬기반 RFID 인증 프로토콜을 제안하였다.

A Study on Secure Matrix-based RFID Authentication Protocol

Su Youn Lee* · Hyo Beom Ahn**

ABSTRACT

Recently, the security for RFID/USN environment is divided into network security and RFID security. The authentication protocol design for RFID security is studied to protect user privacy in RFID system. However, the study of efficient authentication protocol fot RFID system is not satisfy a security for low-cost RFID tag and user privacy. Therefore, this paper proposes a secure matrix-based RFID authentication protocol that decrease communication overhead and computation. In result, the Matrix-based RFID authentication protocol is an effective authentication protocol compare with HB and HB^+ in traffic analysis attack and trace location attack.

Key words : RFID, Matrx, Authentication Protocol

* 백석대학 컴퓨터정보학부
** 공주대학교 정보통신학부

1. 서 론

유비쿼터스 컴퓨팅(Ubiquitous Computing) 기술은 먼저 인식정보를 제공하는 RFID(Radio Frequency IDentification)를 중심으로 발전하였다. RFID 시스템은 무선 주파수를 이용하여 물리적인 접촉 없이 개체에 대한 정보를 읽거나 기록하는 자동 인식 시스템이다.

그러나, RFID 시스템을 이용한 개체인식 기술은 리더와 태그 사이에 물리적인 접촉 없이 인식 가능하고 이로 인한 과도한 정보 노출을 포함한 사용자의 프라이버시 침해를 유발시킨다는 문제점을 가지고 있다.

따라서, RFID 기술을 여러 응용 분야에 적용하기 위해서는 태그에 저장된 정보를 보호하고 임의의 태그에 대한 추적 방지 등과 같은 보안 문제를 해결할 수 있는 인증 프로토콜에 대한 연구가 활발히 진행 중이다. 이에 기존에 무선환경에서 제공하던 보안 프로토콜의 고려할 수 있으나 RFID 태그가 낮은 가격으로 공급되어져야하기 때문에 자원의 소모가 적으면서도 안전한 암호 알고리즘의 개발과 아울러 최소의 자원을 사용하면서도 안전한 프로토콜의 개발이 필수적이다[1].

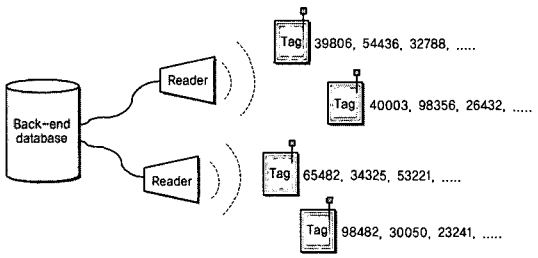
이제까지 제안된 대부분의 인증 프로토콜은 RFID 태그에 하드웨어적인 제약사항을 만족시키지 못했다. 따라서, 본 논문에서는 태그와 리더간에 쌍방향 인증을 위해 최소의 자원을 활용하고 사용자의 프라이버시 공격을 방지할 수 있는 행렬 기반의 RFID인증 프로토콜을 제안하고자한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 RFID 시스템 개요와 태그와 리더간의 위협요소 및 보안 방안을 간략히 설명하고 3장에서 지금까지 제안된 RFID 인증 프로토콜에 대해 설명한다. 4장에서는 제안하고자하는 인증 프로토콜에 대해 구체적으로 설명하고 5장에서는 제안된 인증 프로토콜과 기존의 인증 프로토콜을 비교·분석한다. 마지막으로 6장에서는 결론을 맺는다.

2. RFID 시스템 개요

2.1 리더-태그 구성요소

RFID 시스템은 크게 두 가지 부분으로 나눌 수 있다. '리더-태그 시스템'과 '백엔드 시스템'이다. 리더-태그 시스템은 태그에 기록되어 있는 비트로 표시된 정보를 리더가 읽어와 응용 프로그램에 넘겨주고 응용프로그램이 리더에게 명령하여 태그에 새로운 비트로 표시된 정보를 기록하는 부분을 의미한다. 구성요소는 (그림 1)과 같다.



(그림 1) RFID 시스템의 리더-태그 구성요소

태그(Tag)는 실제 물체에 부착하는 것으로 칩과 안테나를 가지고 있으며 적게는 64비트에서 많게는 8천비트 정도까지 정보를 담을 수 있다. 값싼 RFID 시스템 구현을 위해서 태그의 가격을 저렴하게 만드는 것이 중요하다. 따라서, 태그는 하드웨어적으로 상당히 제한적일 수 밖에 없으며 간단한 몇 가지 명령을 수행할 수 있을 정도이다.

리더(Reader)는 태그의 정보를 읽어들이는 장치로 정보를 응용프로그램에 전송하는 역할과 응용프로그램에게 명령을 받아 태그에 정보를 기록하기 위하여 명령어를 주파수 형태로 변환하여 전송하는 역할을 한다.

2.2 리터-태그 위협요소 및 보안 요구사항[2]

RFID 시스템은 그 편리함에도 불구하고 개인정보나 보안에 대해 취약한 것이 사실이다. 바코

드 시스템과 비교하여 시야가림에 대한 문제가 없어졌지만 그 시야가림의 문제로 인하여 RFID 태그는 항상 도청자에 의해 읽혀질 수 있는 가능성이 높다. 특히, 리더-태그에서의 보안 문제는 태그에 탑재될 수 있는 하드웨어적 기술의 한계가 지나치게 낮고 태그에 담겨진 정보를 불법적으로 엿듣거나 정보에 대한 변조를 시도할 수 있는 가장 빠르고 손쉬운 부분이기 때문이다. 다음은 태그-리더 통신상에서 발생할 수 있는 위협요소와 보안요구사항이다.

- 도청(Eavesdropping) : 태그와 리더간의 통신방식은 무선이므로 공격자는 쉽게 통신 내용을 엿들을 수 있다. 따라서, 도청한 내용에 따라 태그에 저장된 비밀 정보를 알아내는 것을 불가능하게 해야 한다.
- 재전송 공격(replay attack) : 수동적 공격자가 리더와 태그 사이의 통신을 도청한 후 이를 재전송하므로 정당한 태그로 인증받으려는 공격이다. 따라서, 도청한 내용을 이용하여 리더가 정당한 태그로 인증할 수 있는 새로운 값을 생성하는 것은 불가능 해야한다.
- 스푸핑 공격(spoofing attack) : 공격자가 정당한 RFID 리더로 위장하여 태그로부터 인증에 필요한 정보를 획득하고 이를 이용하여 정당한 태그로 인증 받는 공격이다. 따라서, 공격자가 위장된 리더가 태그의 응답정보를 통해 태그안의 비밀정보를 아는 것이 불가능해야 하며 세션마다 태그의 응답이 변화될 수 있도록 난수 등을 이용한 프로토콜이 설계되어져야 한다.
- 트래픽 분석 공격(Traffic analysis attack) : 공격자가 도청을 통해서 얻은 내용을 분석하므로 리더의 질의에 대한 태그의 응답을 예측하여 태그의 이동경로를 트래킹할 수 있는 공격이다. 이를 방지하기 위해 서로 다른 두 개의 응답이 동일한 태그에서 나온 것인지 아닌지를 구별하는 것이 불가능해야 한다.
- 위치 트래킹 공격(Location tracking attack) : 공격자가 공격자 혹은 악의적인 리더가 태그의 위치변화를 감지하므로 태그 소유자의 이동경로를 파악하는 공격방법으로 사용자의 프라이버시를 침해하는 유형중의 하나이다. 따라서 이를 방지하기 위해서는 매 세션마다 갱신되는 RFID 태그의 ID를 사용하므로 공격자로부터 프라이버시를 보호하여야 한다.

2.3 리더-태그 보안 방안

최근의 RFID에 대한 보안 대책은 리더와 태그 사이의 보안 기술에 초점이 맞추어져 있다. 이전 절에서 설명한 위협요소에 대한 보안 방안에 대한 기술은 3가지 분야로 분류할 수 있다[3].

- 인증 및 접근제어 기술

태그와 리더는 서로를 인증하여 신뢰하는 경우에만 올바로 동작을 보장할 수 있다. 이는 접근제어와도 동일한 개념이다. 사용자만이 태그에 접근할 수 있으며 태그를 잠그거나(Lock) 해제(Unlock)할 수 있어야한다. 현재 논의되고 있는 기술로는 '해쉬 기반(Hash-based) 접근 제어[3]'나 '냄덤(Randomized) 접근제어[3]' 방법이 제안되었다.

- 도청 방지 기술

정당한 사용자에 의하여 전송된 태그의 정보는 제 3자가 엿들을 수 없으며 도청 당한 경우에는 정확히 무슨 정보인지 알 수 없어야한다. 이를 위한 방법으로는 '고요한 트리워킹(Silent Tree-walking)[3]'이나 '랜덤 트리워킹(Randomized Tree-walking)[3]' 같은 방법이 있다. 그 외에는 '비밀키 암호화 방식'을 사용하여 암호화된 데이터를 전송하는 방법이나 공개키 암호화 방식을 사용하여 암호화 된 정보를 태그에 기록하는 '재암호화(Re-Encryption) 방법[3]' 등이 있다.

• 정보차단을 위한 물리적 방법

어느 누구도 태그의 정보를 알 수 없도록 태그의 정보를 막는 방법이다. 물리적인 방법으로 '킬 태그(Kill Tag)' 방법이나 '패러데이 우리(Faraday Cage)', '방해 전파(Active Jamminig)'을 쓰는 방법과 '차단자 태그(Blocker Tag)'를 사용하는 방법이 있다.

3. 기존의 RFID 인증 프로토콜

RFID 시스템에서는 리더를 소유한 공격자는 물리적인 접촉없이 태그의 정보를 읽는 것이 가능하므로 사용자가 알지 못하는 사이에 태그의 정보가 유출되거나 태그의 식별 정보를 이용한 사용자 위치 추적 등이 가능하게 된다. 이러한 문제를 해결하기 위해 사용자의 프라이버시를 보호할 수 있는 RFID 인증 프로토콜이 제안되었다. 본 절에서는 지금까지 제안된 사용자 프라이버시를 해결하기 위한 인증 프로토콜을 살펴보고자 한다. 인증 프로토콜 접근 방식에 따라 3가지로 분류 할 수 있다.

3.1 해쉬 기반

해쉬 기반 기법은 해쉬 함수의 일방향성(One way property)을 이용하여 태그의 정보를 보호하는 기법이다. 그러나 RFID 시스템에서는 공격자가 리더와 태그의 통신을 도청하기 쉽기 때문에 채널에서 얻은 정보를 이용하여 재사용 공격과 스푸핑 공격을 수행할 수 있다.

Weis 등이 제안한 기법[3]이며 태그를 잠그고 풀기 위하여 리더가 랜덤한 키를 해쉬하여 데이터베이스에 저장하고 이를 태그의 메타 ID로 사용한다. 그러나, 이 기법에서는 태그가 고정된 값 메타 ID를 리더에게 전송하기 때문에 위치 추적이 가능하다. 이를 보완하기 위해 랜덤 접근 기법(RHLK)이 제안되었다. 태그는 메타 ID뿐만 아니라 난수 R과 자신의 임의의 여러 개의 ID 중에서 (ID_k를 사용하여 생성한 $h(ID_k \| R)$을 리더에게 전송한다. 개선된 기법에서 태그는 임의의 난수를 사용하기 때문에 위치추적이 불가능하다. 이외에서도 Dirk Henrici와 Paul Muller는 [4]에서 해쉬에 기반하여 ID를 갱신하므로 위치트래킹 공격을 방지하는 프로토콜을 제안하였다. 그러나, 이 프로토콜은 인증이 완료될 경우 ID가 갱신되므로 위치트래킹 공격에 안전하게 보이나 태그와 데이터베이스 사이에 정상적이지 않은 인증의 경우 태그는 항상 동일한 h(ID)를 응답하므로 공격자는 태그의 위치를 트래킹 할 수 있다는 문제점을 갖는다. 또한, Ohkubo 등은 위치트래킹 공격에 안전하며 전방위 안정성도 보장되는 해쉬체인 프로토콜[5]을 제안하였다. 두 개의 해쉬 함수를 이용하여 태그의 정보를 보호하는 방법으로 EPC(Electronic Product Code)에 적용하기 쉬운 기법이다. 이 기법에서는 리더의 질의에 대해 태그는 매번 다른 응답을 하므로 공격자는 태그의 이동경로를 파악할 수 없게 된다. 또한, 그 세션에서 해쉬 함수의 값이 노출되더라도 해쉬 함수의 일방향 성질에 의해서 이전의 세션에 대한 정보를 얻을 수 없다. 이러한 성질로 인해 사용자의 프라이버시를 보호할 뿐만 아니라 사용자의 위치 정보를 보호할 수 있다. 그러나, 이 기법에서는 데이터베이스의 해쉬 연산량이 태그의 수에 비례한다는 취약점을 갖는다.

3.2 재 암호화 기반

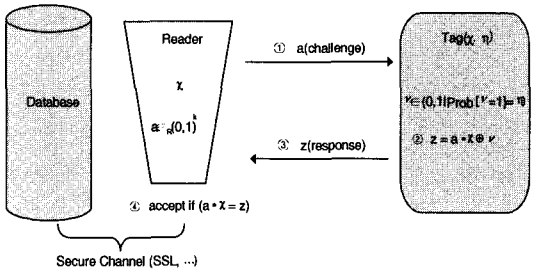
RFID 시스템에서 리더의 질의에 태그가 매번 다른 값을 전송하므로서 사용자의 위치 정보가 노출되는 것을 막을 수 있다. 재 암호화 기법이란 태그의 정보를 재 암호화하여 리더의 질의에 대해서 항상 다른 값으로 응답하는 기법이다. 재 암호화 기법은 많은 연산량을 필요로 하기 때문에 제

한된 자원을 가진 태그가 수행하기 어렵다. 따라서, 태그를 대신하여 데이터베이스나 리더 등을 사용하여 재 암호화 과정이 이루어진다. Satio 등에 의해서 제안 기법[6]인 Universal 재 암호 기법은 재 암호화 과정이 일어날 때 공개키 없이 임의의 랜덤값을 사용하여 재 암호화가 이루어지는 기법이다. 그러나, 태그의 정보에 재 암호화 과정이 여러 번 일어나더라고 단 한 번의 복호화 과정으로 원래의 메시지를 복원할 수 있다. Juels 등에 의해서 제안 기법[7]인 Privacy Protection in RFID-enabled Banknotes는 Euro 화폐에 태그를 적용하여 불법 거래시 화폐의 흐름을 추적하기 위해 제안되었다. 그러나, 악의적인 상인이 화폐에 재 암호화 과정을 수행하지 않거나 시스템의 오류로 재 암호화 과정이 수행되기 전에 리더와 태그 사이의 통신이 끊길 경우 태그는 일정한 기간 동안 고정된 값을 리더에게 전송하게 되고 사용자의 위치 추적이 가능하다는 문제점이 있다.

3.3 XOR 기반

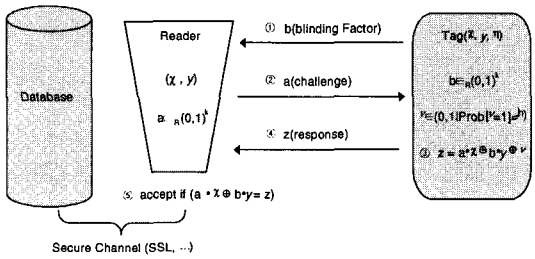
해쉬 기반과 재 암호화 기반의 기법들은 최소한의 연산만을 수행하는 태그가 사용되는 환경에 적용하기에는 적합하지 않다. XOR 기반의 기법은 해쉬 기반의 기법보다 더 단순한 비트 연산을 사용하여 RFID의 프라이버시를 보호하는 기법으로 최저가의 RFID태그에 적용 가능한 기법이다. 따라서, 본 논문에서 제안한 행렬 기반 인증 프로토콜은 XOR 기반으로 개발된 프로토콜이다.

Juels는 사용자의 프라이버시를 보호하며 최소한의 암호학적 함수를 사용하는 기법을 제안하였다[8]. 제안된 기법은 간단한 비트 연산인 XOR 연산을 사용한다. 리더로부터 임의의 값들을 받아서 그것을 이용하여 다음 세션에 사용될 값들을 갱신하므로 공격자가 태그를 추적하지 못하도록 한다. 또한, Juels에 의해 2005년에 제안된 HB 프로토콜[9]은 1비트로 상대방을 인증하는 기법이다(그림 2).



(그림 2) HB 프로토콜

이 기법은 수동적인 공격자에 대해서 안전할 수 있으나 공격자가 a값을 자신에게 유리하게 선택하여 리더에게 전송한다면 응답 값 z에서 x에 대한 값을 알아낼 수 있다. 따라서, Juels는 능동적인 공격에 안전한 HB^+기법을 제안하였다[10](그림 3). 이 기법은 리더와 태그 간에 추가적으로 y라는 비밀값을 서로 저장하고 이전 기법과 달리 b라는 임의의 값을 태그가 전송하는 기법이다.



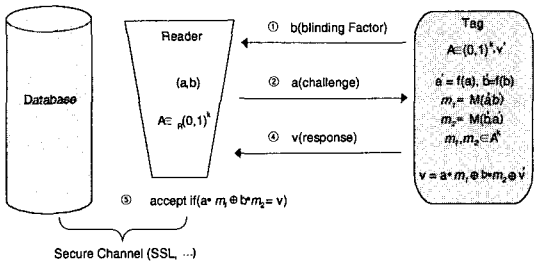
(그림 3) HB^+ 프로토콜

하지만 제안된 기법은 1비트의 값으로 태그를 인증하는 것이기 때문에 그를 관리하는 환경에서는 오류 발생의 확률이 많다. 그러므로 다수의 태그 정보를 다루는 환경에서 사용하기에는 부적합하며 이 기법은 안전성 측면에서 취약성을 갖는다[10].

4. 제안된 인증 프로토콜

사용자의 프라이버시를 보호할 수 있는 인증

프로토콜은 태그의 식별정보가 직접 전송되지 않고 매 세션마다 전송되는 인증 정보를 변경하므로 위치 추적이나 트래픽 분석 공격에 대해 안전성을 제공한다. 따라서, 본 논문에서 제안하는 인증 프로토콜은 비트 연산을 기반으로 태그에 최소한의 연산을 수행하게하며 Jules가 제안한 HB^+ 문제점인 1비트 값으로 태그를 인증하므로 발생되는 오류 발생 확률이 높은 것을 해결한 행렬을 기반으로 하는 인증 프로토콜을 제안하고자 한다. (그림 4)는 제안 프로토콜의 상호 인증 단계이다.



(그림 4) 상호 인증 프로토콜

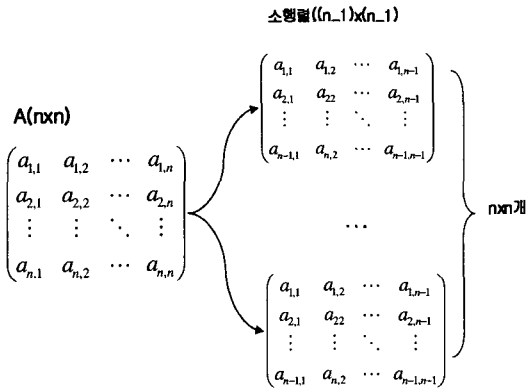
우선, RFID 태그와 리더간에 비밀 정보 행렬 (A) n × n(= k비트)를 공유하고 이전에 사용된 v 값인 v′을 저장한 상태에서 인증 프로토콜이 수행된다.

① 먼저, 능동적인 공격에 안전하게 설계하기 위해 태그가 리더에서 랜덤 값 b를 전송한다.

② 리더는 b 값을 받아 저장하고 랜덤 값 a를 전송한다. a 값을 받은 태그는 a, b를 이용하여 행렬 A의 소행렬 위치를 함수(f)를 사용하여 계산한다. 즉, a′ = f(a), b′ = f(b)이다. 여기서, 함수 f()는 랜덤 값 a, b가 n보다 작거나 같다는 조건을 만족시키기 위해 사용한다. 그리고 리더와 공유한 비밀정보(A)로부터 소행렬 $m_1 = M(a',b')$와 $m_2 = M(b',a')$를 생성한다. 소행렬 m_1, m_2를 이용하여 상호간에 받은 랜덤 값 a와 b 값과 XOR 연산을 한 후 v′와 XOR 연산을 한 값 v를 리더에게 전송하고 v′에 v를 저장한다.

③ 리더는 전송받은 v를 DB로부터 비밀정보 A를 가져와 자신이 보내고 받은 a, b와 함수(f)를 이용하여 소행렬 m_1, m_2를 계산한다. 그 후 소행렬 값과 랜덤 값 그리고 저장된 이전에 사용된 v인 v′을 이용하여 v를 계산하고 일치여부를 확인하여 상호 인증을 수행한다. 일치가 확인되면 v′에 계산된 v를 저장한다.

제안 프로토콜은 상호인증이 가능하며 비밀 정보 m_1, m_2가 행렬 A로부터 변경되므로 능동적 공격을 방지 할 수 있다. 또한, 복잡성을 늘이기 위해 비밀정보 A의 크기 k비트를 증가시키면 n×n만큼의 소행렬을 생성할 수 있으므로 복잡도를 높일 수 있다. (그림 5)는 n × n 행렬 A로부터 (n-1) × (n-1)의 소행렬을 2n개 얻을 수 있다는 것을 보인다.



(그림 5) 소행렬의 생성

5. 제안된 인증 프로토콜 비교 · 분석

본 장에서는 제안 된 인증프로토콜을 기존 XOR 기반의 HB[9]와 HB^+ [10]인증 프로토콜과 안정성과 효율성 측면에서 비교 · 분석하였다.

5.1 안정성

제안 프로토콜은 이전에 제안된 방식과는 다르게 공유된 비밀 정보를 노출시키지 않고 비밀정보 행렬(A)로부터 m_1과 m_2를 통신 시점에서 생성하기 때문에 제 3자가 트래픽 분석을 통해 비밀정보에 대한 수집 공격을 어렵게 한다. 즉, 비밀 정보행렬(A) n × n비트 중 (n-1) × (n-1) 비트, 즉 n^2-2n+1 비트를 전송함으로써 2n-1 만큼의 비트가 제 3자로부터 감춰지게 됨으로 트래픽 분석을 통해 2n-1 비트를 얻어 내기 힘들다. 또한, 비밀 정보는 a와 b에 의해 계산된 비밀 정보 m_1과 m_2는 통신을 할 때 마다 변경되고 또한 이전에 사용된 v′의 정보를 XOR 연산을 통해 v를 생성함으로써 a, b를 수집하더라고 동일한 v를 동일한 v값을 얻을 수 없다.

제안 프로토콜은 비밀 정보행렬(A)를 이용하여 리더와 태그가 동일한 v를 생성해야 하기 때문에 m_1과 m_2 소행렬을 생성해야 하고 이전의 v′값을 통해 동일한 v값을 생성해야 하기 때문에 리더와 태그간의 상호인증을 수행할 수 있다.

〈표 1〉 안정성 비교 · 분석

구분	HB	HB$^+$	제안 프로토콜
트래픽 분석	X	X	○
재전송 공격	X	○	○
스푸핑 공격	X	○	○
위치추적 공격	X	X	○

5.2 효율성

제안된 프로토콜은 HB와 HB$^+$에 비해서는 XOR 연산이 많으나, HB와 HB$^+$에서처럼 여러 번의 라운드에 걸쳐 통신을 하지 않기 때문에 통신오버헤드는 줄어들게 된다. 또한, XOR연산에도 HB와 HB$^+$는 각 라운드마다 오류를 첨부한 z를 생성하기 위하여 XOR 연산을 수행한다. 이 측면에서 보면 HB와 HB$^+$의 XOR 연산량은 라운드 수(r)와 같게 된다. 제안된 인증 프로토콜은 한번의 v를 계산하기 위한 XOR 연산 2번을 사용함으로 상대적으로 연산량을 감소시킬 수 있다. 그러나 이전의 HB보다는 저장해야 하는 비밀정보의 크기가 크다는 문제를 가진다(HB$^+$는 두 개의 비밀정보 x, y를 사용함으로 비밀정보가 k비트라면 4 * n비트의 공간이 필요하다). 즉, 저장 공간은 일반적인 k비트(n × n행렬)의 비밀정보를 가진다면, 제안된 프로토콜은 소행렬이 (n-1)×(n-1)비트의 크기를 가져야 함으로 2n-1비트의 저장 공간을 더 요구한다.

〈표 2〉 계산량 비교 · 분석

	HB	HB$^+$	제안 프로토콜
통신오버헤드	1+r	2+r	3
XOR 연산량	r	r	2

r : 라운드의 횟수를 의미한다.

6. 결 론

본 논문에서는 HB와 HB$^+$의 트래픽 분석공격의 약점을 해결하기 위하여 행렬기반의 키 생성을 통한 인증 및 트래픽 분석을 어렵게 하기 위한 방법을 제안했다. 제안 인증 프로토콜은 비밀정보를 HB나 HB$^+$처럼 통신시 전체를 공개하지 않고 일부만을 키로 사용하여 최대한 비밀정보를 감추기 위하여 행렬의 소행렬 생성방법을 적용하였고, 이를 통해 상호인증과 트래픽 분석 그리고 위치추적을 방지를 XOR연산 만을 통해 구현될 수 있는 새로운 RFID 인증 프로토콜이다. 그러나, 기존의 XOR을 이용한 HB보다는 비밀 정보를 저장할 공간이 요구되는 단점이 있으나 HB에서 제공되지 않는 트래픽 분석과 위치 추적 그리고 다수의 태그를 다룰 수 있는 응용에서 사용될 수 있는 방법이다. 향후 연구 과제는 외부에 비밀정보를 유출되지 않도록 하는 더욱더 안전한 인증 프로토콜에 대한 연구가 요구된다.

참 고 문 헌

[1] S. E. Sarma, "Towards the fivecent tag", MIT Auto ID Center, Technical Report MIT-AUTOID-WH-006.2001.(http://autoidcenter.org)

[2] 정병호, "RFID/USN 환경에서의 정보보호", 제9회 정보보보심포지움, pp. 447-463, 2004.

[3] S. A. Weis, S. E. Sarma and D. W. Engels, "Security and privacy Aspects of Low Cost Radio Frequency Identification System", First International Conference on Security in Pervasive Computing, 2003. (http://theory.lcs.mit.edu/sweis/spc-rfid.pdf)

[4] D. Herinici, and P. Muller, "Hash based enhancement of location privacy for radio frequency identification devices using varying identifiers", Per-Sec'04, pp. 149-153, March 2004.

[5] M. Ohkubo, K. Suxuki and S. Kinoshita, "Efficient Hash-Chain Based RFID Privacy Protection Scheme", Ubcomp 2004 workshop.

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

[7] A. Jule, "Minimalost cryptography for Low Cost RFID Tag", The Fourth International Conference on Security in Communication Networks SCN2004, Vol. 3352 LNCS, pp. 149-164, Sep 2004.

[8] A. Jule, "Authentication Pervasive Devices with Human Protocols", To appear Crypto 2005, Aug 2005.

[9] A. Jule and R. Pappu, "Squealing euros: Privacy protection in RFID-enable banknote", In proceedings of Financial Cryptography -FC'03, Vol. 2742 LNCS, pp. 103-121, Sep. 2003.

[10] H. Gilbert, M.Robshaw and H.Sibert, "An Active Attack Against HB+ D-A probably Secure Lightweigh Authentication Protocol". (http://eprint.iacr.org/2005/237)

[11] 최은영, 이동훈,"RFID 정보보호 기술 동향", 정보처리학회지, 제12권, 제5호, 2005.

[12] A. Juela, R. L. Riverst and M. Szydlo, "The Blocker Tag:Selective Blocking of RFID Tags for Consumner Privacy", 8th ACM Conference on Computer and Communication Security. pp. 103-111, ACM Press. 2003.

[13] 김동서, 박종서, "RFID/USN 보안 연구대상 및 향후 추세", 정보보호학회지, 제15권, 제1호, 2005.

[14] 강전일, 박주성, 양대헌, "RFID 시스템에서의 프라이버시 보호기술", 정보보호학회지, 제14권, 제6호, 2004.

이 수 연

1990년 단국대학교 전산학과 학사
1993년 단국대학교 전산통계학과 석사
2003년 성균관대학교 전기전자 및 컴퓨터공학부 박사
1997년~현재 백석대학 컴퓨터정보학부 교수

안 효 범

1992년 단국대학교 전자계산학과 (이학사)
1994년 단국대학교 전산통계학과 대학원 석사(이학석사)
2002년 단국대학교 전산통계학과 대학원 박사(이학박사)
1997년~2005년 천안공업대학 정보통신과 부교수
2005년~현재 공주대학교 정보통신학부 교수