견고한 행렬기반 RFID 상호인증 프로토콜

정회원 윤 은 준*, 하 경 주**, 유 기 영***°

Robust Matrix-based RFID Mutual Authentication Protocol

Eun-Jun Yoon*, Kyeoung-Ju Ha**, Kee-Young Yoo***° *Regular Members*

요 약

2006년에 Lee와 Ahn은 기존의 HB와 HB+ RFID 인증 프로토콜들이 가지는 보안취약점들을 해결한 행렬기반의 RFID 인증 프로토콜을 제안하였다. 그들이 제안한 프로토콜은 RFID 태그측의 계산량을 감소시켜줄 뿐만 아니라, 통신 오버헤드를 줄여주며, 사용자 프라이버시 보호 등의 장점을 제공한다. 하지만, 본 논문에서는 먼저 Lee와 Ahn이 제안한 프로토콜이 그들의 주장과는 달리 RFID 리더를 태그가 인증을 하지 않는 상호인증 문제로 인하여 다양한 공격들에 취약함을 지적하고, 이러한 문제점들을 해결한 상호인증을 제공하는 개선된 행렬기반 RFID 인증 프로토콜을 제안한다. 결론적으로 제안한 RFID 인증 프로토콜은 Lee와 Ahn의 프로토콜과 비교하여 강한 보안성을 제공할 뿐만 아니라, 통신 라운드 수 또한 줄여주었기 때문에 높은 효율성을 보장할 수 있다.

Key Words : RFID, Security Analysis, Mutual Authentication, Matrix, Protocol

ABSTRACT

In 2006, Lee and Ahn proposed a matrix-based RFID authentication protocol which eliminates the security problems in HB and HB+ RFID authentication protocols. Their proposed protocol provides the following three merits: (1) it reduces the computational costs of the RFID tag. (2) it reduces the communication overhead between the reader and the tag. (3) it protects the user privacy. However, this paper points out that Lee and Ahn's proposed protocol is insecure to various attacks because it does not provide mutual authentication which the RFID tag does not authenticate the legality of the RFID reader unlike their claims. In addition, this paper proposes an improved matrix-based RFID mutual authentication protocol that can provide the mutual authentication. As a result, the proposed protocol not only can provide strong security and but also guarantee high efficiency because it reduces the communication rounds compare with Lee-Ahn's protocol.

Ⅰ. 서 론

최근 RFID(Radio Frequency IDentification) 기술은 센서 네트워크(Sensor Network) 기술과 더불어 유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경 실현을 위한 중요한 핵심 기술로 주목을 받고 있다. RFID 시스템의 일반적인 정의는 무선 주파수를 이용하여 물리적인 접촉 없이 태그(Tag)에 저장된 정보를 비접촉 방식으로 읽거나 정보를 기록할 수 있는 자동 인식(Automatic Identification) 시스템을 의

※ 본 연구는 2단계 두뇌한국 21 프로젝트(2008)의 연구결과로 수행되었습니다.
* 경북대학교 전자전기컴퓨터학부(ejyoon@tpic.ac.kr),
** 대구한의대학교 모바일콘텐츠학부(kjha@dhu.ac.kr)
*** 경북대학교 컴퓨터공학과 정보보호연구실(yook@knu.ac.kr) (°: 교신저자)
논문번호 : KICS2008-06-259, 접수일자 : 2008년 6월 25일, 최종논문접수일자 : 2008년 10월 7일

미한다. 이러한 RFID 시스템의 장점은 기존의 바코드(Bar Code) 시스템이 지니고 있는 일회성 저장 문제를 해결하여 주어, 물류, 유통, 의료, 금융, 교통 등 다양한 분야에 관리 자동화를 위해 활용되어 질 수 있다[1][2][3].

일반적으로 RFID 시스템은 3가지 구성요소인 리더(Reader), 태그(Tag) 그리고 백-엔드 데이터베이스(Back-end Database)로 구성되어진다. 리더와 백-엔드 데이터베이스의 연산 능력에 비해 RFID 태그는 연산 능력이 떨어지며, 객체를 유일하게 식별하기 위한 정보만을 가지며, 정보 노출, 위치 추적 등의 프라이버시 침해를 유발할 수 있는 문제점을 지니고 있다[4][5][6].

최근까지 RFID의 프라이버시 침해 문제를 해결하기위한 많은 인증 프로토콜(Authentication Protocol)들이 제안되어져 오고 있다[7-12]. 일반적으로 RFID 인증 프로토콜은 접근 방식에 따라 해쉬 기반, 재 암호화 기반, XOR 기반의 3가지로 분류되어진다[4,5,6,7-12]. 특히 XOR 기반의 기법은 다른 두 기법과 비교하여 단순한 비트 연산만을 사용하여 RFID의 프라이버시를 보호하는 기법으로 최저가의 RFID 태그에 적용 가능한 기법으로 사용된다. 2005년에 Juels[10][11]가 제안한 HB 프로토콜과 HB^+ 프로토콜은 대표적인 XOR 기반 RFID 인증 프로토콜들이다. 하지만 HB와 HB^+프로토콜들은 1비트의 값으로 태그를 인증하는 기법으로 오류 발생 문제와 다수의 태그 정보를 다루는 환경에서 트래픽 분석공격 문제 등의 안전성 측면에서 취약성을 가짐을 Gilbert 등[12]은 증명하였다.

최근 Lee와 Ahn[13]은 기존의 HB와 HB^+ RFID 인증 프로토콜들이 가지는 보안 취약점들을 해결한 행렬기반의 새로운 RFID 인증 프로토콜을 제안하였다. 그들이 제안한 프로토콜은 비트 연산을 기반으로 RFID 태그측의 계산량을 감소시켜줄 뿐만 아니라, 통신 오버헤드를 줄여주며, Jules[11]가 제안한 HB와 HB^+ 프로토콜들의 문제점인 1비트 값으로 태그를 인증하므로 발생되는 오류 발생 확률이 높아지는 문제점을 해결하며, 트래픽 분석공격에 안전하고, 사용자 프라이버시 보호 기능 제공 등의 많은 장점을 가진다.

그럼에도 불구하고, 본 논문에서는 Lee-Ahn이 제안한 RFID 인증 프로토콜이 그들의 주장과는 달리 RFID 리더를 태그가 인증을 하지 않는 상호인증(Mutual Authentication) 문제점으로 인해 트래픽 분석 공격(Traffic Analysis Attack), 위치 트래킹 공격(Location Tracking Attack), 서비스 거부 공격(Denial of Service Attack)등에 취약함을 지적하고, 이러한 취약점들을 해결한 상호인증을 제공하는 개선된 행렬기반 RFID 상호인증 프로토콜을 제안한다[14-16]. 결론적으로 제안한 RFID 인증 프로토콜은 Lee와 Ahn의 프로토콜과 비교하여 보다 강한 보안성을 제공할 뿐만 아니라, 시스템 전체의 통신 라운드 수 또한 줄여주었기 때문에 보다 높은 통신 효율성을 보장할 수 있다.

본 논문의 구성은 다음과 같다. 먼저 Ⅱ장에서는 Lee와 Ahn이 제안한 행렬기반 RFID 인증 프로토콜에 대해 설명하며 Ⅲ장에서는 그들 프로토콜의 보안 취약점들을 설명한다. Ⅳ장에서는 제안하고자 하는 인증 프로토콜에 대해 구체적으로 설명하고 Ⅴ장에서는 제안된 인증 프로토콜과 기존의 인증 프로토콜들을 안정성과 효율성 측면에서 비교·분석한다. 마지막으로 Ⅵ장에서는 본 논문의 결론을 맺는다.

Ⅱ. Lee와 Ahn의 프로토콜

본 장에서는 Lee와 Ahn[13]이 제안한 행렬기반의 RFID 인증 프로토콜을 간략히 설명한다.

인증 프로토콜을 수행하기 전인 초기화 단계에서 RFID 태그와 리더간에는 $n \times n$ 크기 비밀 행렬 A (=k비트)와 이전 세션에서 계산된 랜덤 값 v'를 공유하고 있다. 여기에서 비밀행렬 A의 크기 k비트를 증가시켜 $n \times n$ 갯수 만큼의 소행렬을 생성하여 A의 복잡도와 안전성을 보장한다.

그림 1은 Lee와 Ahn이 제안한 RFID 인증 프로토콜의 인증 과정을 보여주며, 아래와 같은 단계로 인증 프로토콜이 수행된다.

Step 1. Reader → Tag: query
Reader는 감응 인식 범위 내에 Tag가 존재하면 query를 Tag에게 전송한다.

Step 2. Tag → Reader: b (blinding factor)
Tag는 랜덤 값 $b \in_R (0,1)^k$를 생성한 후 Reader에게 전송한다.

Step 3. Reader → DB: b (blinding factor)
Reader는 DB에게 랜덤 값 b를 전달한다.

Step 4. DB → Reader: a (challenge)
DB는 b값을 받아 저장하고, 랜덤 값 $a \in_R (0,1)^k$를 생성한 후 Reader에게 전송한다.

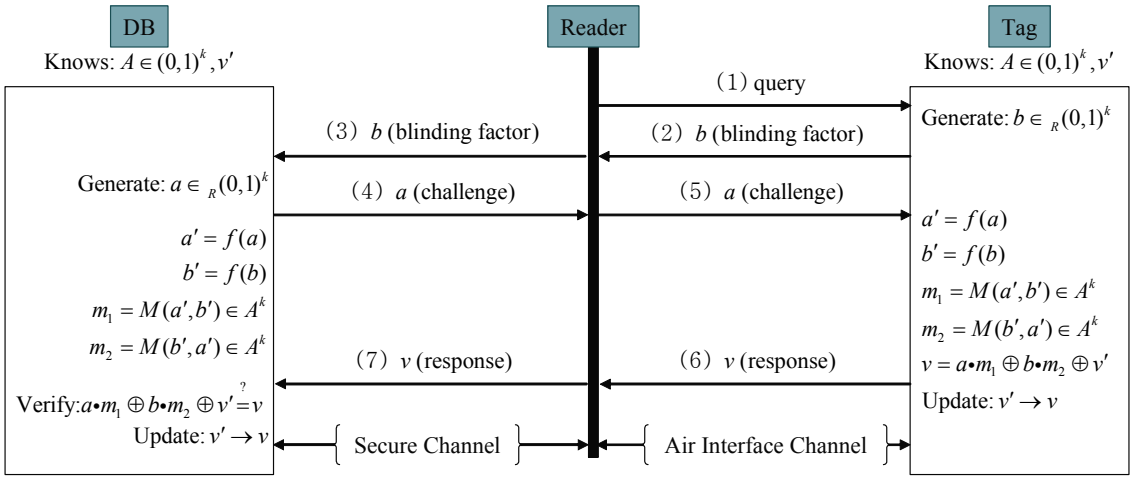

그림 1. Lee와 Ahn의 행렬기반 RFID 인증 프로토콜

Step 5. Reader → Tag: a (challenge)
Reader는 Tag에게 랜덤 값 a를 전달한다.

Step 6. Tag → Reader: v (response)
Tag는 랜덤 값 a와 b를 이용하여 행렬 A의 소행렬 위치를 함수 $f()$를 사용하여 $a' = f(a)$과 $b' = f(b)$을 각각 계산한다. 여기서, 함수 $f()$는 랜덤 값 a와 b가 n보다 작거나 같다는 조건을 만족시키기 위해 사용한다. 계속해서, Reader와 공유한 비밀 행렬 A로 부터 소행렬 $m_1 = M(a', b')$과 $m_2 = M(b', a')$를 생성한다. 생성된 소행렬 m_1과 수신한 랜덤 값 a를 $a \bullet m_1$과 같이 AND 연산하고, 소행렬 m_2와 생성한 랜덤 값 b를 $b \bullet m_2$와 같이 AND 연산한다. 마지막으로, 공유하고 있는 v'과 함께 XOR 연산을 하여 $v = a \bullet m_1 \oplus b \bullet m_2 \oplus v'$를 계산 한 후 v를 Reader에게 전송하고 Tag내의 v'위치에 v를 저장한다.

Step 7. Reader → DB: v (response)
Reader는 DB에게 v를 전달한다.

Step 8. DB는 전송받은 v를 검증하기 위해 랜덤 값 a와 b를 이용하여 행렬 A의 소행렬 위치 $a' = f(a)$과 $b' = f(b)$을 각각 계산한다. 계속해서, DB내에 저장된 비밀 행렬 A로부터 소행렬 $m_1 = M(a', b')$와 $m_2 = M(b', a')$를 생성한 후, 생성된 소행렬 m_1과 랜덤 값 a를 $a \bullet m_1$과 같이 AND 연산하고, 소행렬 m_2와 생성한 랜덤 값 b를 $b \bullet m_2$와 같이 AND 연산한다. 마지막으로, 공유하고 있는 v'과 함께 XOR 연산을 하여 $a \bullet m_1 \oplus b \bullet m_2 \oplus v'$를 계산 한 후 수신한 v와 일치하는 지를 검증한다. 만약 두 값이 동일하면 Reader는 Tag를 인증하고, DB내의 v'위치에 v를 저장한다.

Ⅲ. 보안 취약점 분석

본 장에서는 Lee와 Ahn이 제안한 행렬기반 RFID 인증 프로토콜이 상호인증을 제공하지 않음으로 인해, 트래픽 분석 공격(Traffic Analysis Attack), 위치 트래킹 공격(Location Tracking Attack), 서비스 거부 공격(Denial of Service Attack)등에 취약함을 보인다[14-16].

제안한 공격에서 공격자 Adv(Reader)는 이전 세션에서 도청한 v'을 사용하는 임의의 세션에서 Reader로 위장하여 다음과 같은 공격을 먼저 수행한다.

Step 1. Adv(Reader) → Tag: query
리더로 위장한 Adv(Reader)는 query를 Tag에게 전송한다.

Step 2. Tag → Adv(Reader): b (blinding factor)
Tag는 랜덤 값 $b \in_R (0,1)^k$를 생성한 후 리더로 위장한 Adv(Reader)에게 전송한다.

Step 3. Adv(Reader) → Tag: a (challenge)
Adv(Reader)는 Tag로부터 수신한 랜덤 값 b를 a로 두고, Tag에게 a를 전달한다. 즉, 두 랜덤 값 b와 a

가 동일한 값이 되도록 Adv(Reader)는 Tag로부터 수신한 값을 반사(Reflection) 시킨다.

Step 4. Tag → Adv(Reader): v (response)
Tag는 a, b를 이용하여 $a'=f(a)$과 $b'=f(b)$을 각각 계산한 후, $m_1=M(a',b')$와 $m_2=M(b',a')$를 생성하게 된다. 이후, Tag는 a', b', m_1, m_2와 저장된 v'을 이용하여 $v=a \bullet m_1 \oplus b \bullet m_2 \oplus v'$를 계산 한 후 v를 Adv(Reader)에게 전송하고 Tag내의 v'위치에 v를 저장하게 된다.

Step 5. 공격자 Adv(Reader)는 수신한 v (response)를 저장한다.

위 Step 3에서 공격자 Adv(Reader)는 Tag로부터 수신한 랜덤 값 b를 자신의 challenge인 a로 만들어 Tag에게 전송하였기에, Step 4에서 Tag가 계산한 $a'=f(a)$와 $b'=f(b)$은 결론적으로 b'의 하나의 동일한 값이 되며, 더 나아가 $m_1=M(a',b')$과 $m_2=M(b',a')$ 또한 $M(b',b')$의 하나의 동일한 값이 됨을 알 수 있다. 결론적으로, Tag가 Adv(Reader)에게 전송하게 되는 v값은 다음과 같이 이전 세션에서 갱신된 v'과 동일한 값임을 쉽게 알 수 있다.

$$\begin{aligned} v &= a \bullet m_1 \oplus b \bullet m_2 \oplus v' \\ &= b \bullet m_2 \oplus b \bullet m_2 \oplus v' \\ &= v' \end{aligned}$$

따라서 공격자 Adv(Reader)는 위 Step 5에서 수신하여 저장된 v를 이용하여 다음과 같이 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등을 수행한다.

(1) 트래픽 분석 공격: 공격자 Adv(Reader)는 위와 같은 공격 방법으로 수집한 Tag의 응답(Response) v가 이전에 도청한 v'과 동일한지를 쉽게 비교할 수 있다. 만약 v'과 동일한 v를 발견하면 공격자는 해당 Tag의 응답을 예측하게 되어 태그의 이동경로를 트래킹 할 수 있다. 즉 서로 다른 두 개의 응답 v와 v'이 동일한 Tag에서 나온 것인지를 쉽게 구별할 수 있음으로 트래픽 분석 공격에 취약하게 된다.

(2) 위치 트래킹 공격: 공격자는 응답 v와 v'이 동일한 Tag를 다른 위치상에서 발견하였다면 이는 Tag의 위치변화 또한 감지하게 되어 Tag 소유자의 이동경로를 쉽게 파악케 하여 사용자의 프라이버시를 침해할 수 있는 위치 트래킹 공격에도 취약하게 된다.

(3) 서비스 거부 공격: Tag는 Reader를 인증하지 않고 수신한 a를 합법적인 Reader가 보낸 것임을 단순히 믿기에, Tag 자신이 보낸 a값을 b로 두어 반사시킨 것임을 전혀 알지 못한 상태에서 v를 계산하여 응답으로 Adv(Reader)에게 전송하고 Tag 자신의 이전 랜덤 값 v'을 v로 갱신하게 된다. 하지만 Reader내의 DB는 여전히 이전 세션에 갱신된 v'값을 저장하고 있기에 합법적인 Reader가 인증요청을 할 경우 DB는 자신이 계산한 $a \bullet m_1 \oplus b \bullet m_2 \oplus v'$가 Tag를 거쳐 Reader로부터 수신한 $v^*=a \bullet m_1 \oplus b \bullet m_2 \oplus v$와 같지 않음을 검증하게 되어 해당 Tag를 인증하지 못하게 된다. 따라서 합법적인 Tag는 이후의 모든 서비스를 거부 받게 되는 서비스 거부 공격에 취약하게 된다.

위와 같은 공격방법들은 일반적으로 RFID 시스템의 사용 용도에 따라 취약정도는 달라 질 수 있다. 예를 들어 125 KHz나 13.56 MHz의 주파수 대역을 가지는 단거리 RFID 시스템의 경우 Tag와 Reader 간의 인식 거리가 매우 짧기 때문에 정상적인 리더가 공존하는 환경에서는 제안한 공격방법들이 적용되기 어려울 수 있다. 하지만 EPC Gen2 RFID Reader와 같은 900MHz 주파수 대역을 가지는 RFID 시스템은 최대 100미터까지 장거리인식이 가능함으로 얼마든지 제안한 공격이 가능할 것이다. 따라서 위와 같은 보안 요구사항들은 RFID 인증 프로토콜에서 반드시 만족되어야 한다.

Ⅳ. 제안 프로토콜

본 장에서는 Ⅲ장에서 보여준 Lee와 Ahn이 제안한 프로토콜의 보안 취약점들을 해결한 안전한 행렬기반 RFID 상호인증 프로토콜을 제안한다.

제안한 프로토콜의 상호인증 과정을 수행하기 전에 초기화 단계에서 Tag와 Reader간에는 $n \times n$ 크기 비밀 행렬 A(=k비트)와 비밀값 x를 공유하고 있다고 가정한다. Lee와 Ahn의 프로토콜과는 달리 x는 공유 비밀값으로 어떠한 경우에도 갱신되지 않는다.

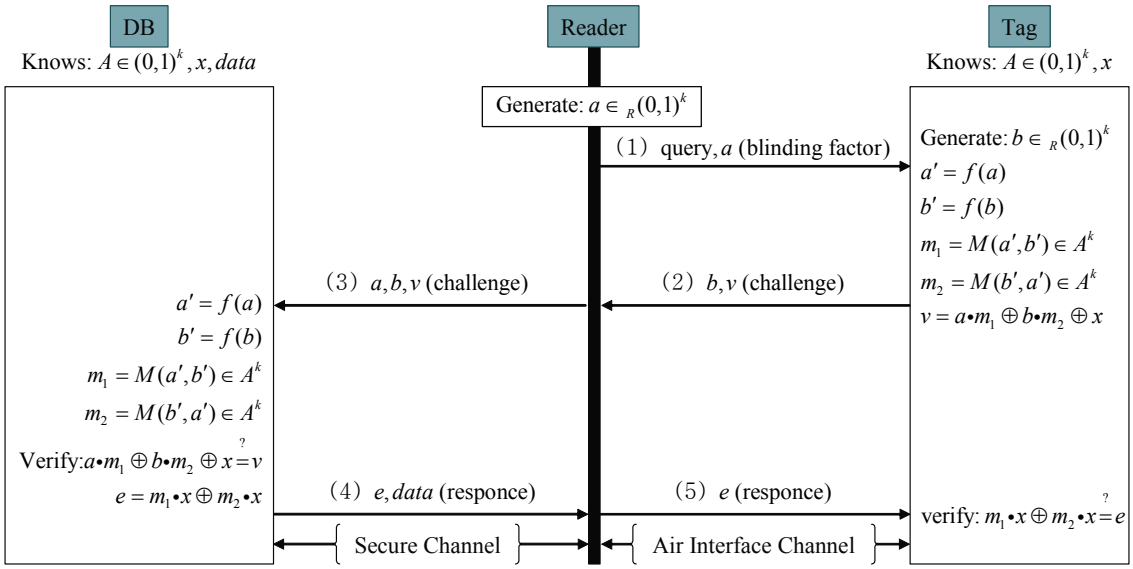

그림 2. 제안한 행렬기반 RFID 상호인증 프로토콜

그림 2는 제안한 프로토콜의 상호인증 단계를 보여주며, 아래와 같이 수행된다.

Step 1. Reader → Tag: query, a (blinding factor)
Reader는 감응 인식 범위 내에 Tag가 존재하면 랜덤 값 $a \in_R (0,1)^k$를 생성하여 query와 함께 Tag에게 전송한다.

Step 2. Tag → Reader: b, v (challenge)
Tag는 Reader로부터 query와 a를 수신한 후, 랜덤 값 $b \in_R (0,1)^k$를 생성한다. a와 b를 이용하여 행렬 A의 소행렬 위치를 함수 $f()$를 사용하여 $a' = f(a)$과 $b' = f(b)$을 각각 계산한다. 계속해서, Reader와 공유한 비밀 행렬 A로부터 소행렬 $m_1 = M(a', b')$와 $m_2 = M(b', a')$를 생성한다. 생성된 소행렬 m_1과 수신한 랜덤 값 a를 $a \bullet m_1$과 같이 AND 연산하고, 소행렬 m_2와 생성한 랜덤 값 b를 $b \bullet m_2$와 같이 AND 연산한다. 마지막으로, 공유 비밀값 x와 함께 XOR 연산을 하여 $v = a \bullet m_1 \oplus b \bullet m_2 \oplus x$를 계산 한 후 b와 함께 Reader에게 전송한다.

Step 3. Reader → DB: a, b, v (challenge)
Reader는 DB에게 자신이 생성한 랜덤 값 a와 Tag로부터 수신한 b와 v를 전달한다.

Step 4. DB → Reader: e, $data$ (response)
DB는 전송받은 v를 검증하기 위해 a와 b를 이용하여 행렬 A의 소행렬 위치 $a' = f(a)$과 $b' = f(b)$을 각각 계산한다. 계속해서, DB내에 저장된 공유 비밀 행렬 A로부터 소행렬 $m_1 = M(a', b')$와 $m_2 = M(b', a')$를 생성한 후, 생성된 소행렬 m_1과 랜덤 값 a를 $a \bullet m_1$과 같이 AND 연산하고, 소행렬 m_2와 랜덤 값 b를 $b \bullet m_2$와 같이 AND 연산한다. 마지막으로, DB에 저장된 Tag들의 공유 비밀값 x를 이용하여 XOR 연산을 하여 $a \bullet m_1 \oplus b \bullet m_2 \oplus x$를 계산 한 후 수신한 v와 일치하는 x가 존재하는 지를 검증한다. 만약 DB내의 모든 Tag들의 x를 이용하여 검증하여도 동일한 두 값이 존재하지 않으면, DB는 Tag가 가짜 Tag 또는 위조된 Tag로 인식하여 통신을 종료한다. 두 값이 동일하게 되는 x를 찾게 되면 DB는 Tag를 인증하게 되며 상호인증을 수행하기 위해 공유 비밀값 x와 계산된 소행렬 m_1과 m_2를 이용하여 $e = m_1 \bullet x \oplus m_2 \bullet x$를 계산한 후, Reader가 필요로 하는 정보인 Tag의 $data$ 정보와 함께 Reader에게 전송한다.

Step 5. Reader → Tag: e (response)
Reader는 DB로부터 수신한 $data$를 이용하여 필요한 정보를 획득하고, Tag에게 e를 전달한다.

Step 6. Tag는 공유 비밀값 x와 소행렬 m_1이용하여 $m_1 \cdot x$와 같이 AND 연산하고, 공유 비밀값 x와 소행렬 m_2를 이용하여 $m_2 \cdot x$와 같이 AND 연산한다. 마지막으로, 두 값을 XOR 연산을 하여 $m_1 \cdot x \oplus m_2 \cdot x$를 계산 한 후, 수신한 e와 동일한지를 검증한다. 만약 두 값이 동일하면 Reader는 Tag를 인증하게 되어 상호인증이 이루어지게 된다.

V. 안전성과 효율성 분석

본 장에서는 제안한 행렬기반 RFID 상호인증 프로토콜에 대한 안전성과 효율성을 분석한다.

5.1 안전성 분석

제안한 프로토콜은 다음과 같이 상호인증을 명시적으로 제공함으로 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 안전하다.

(1) 상호인증(Mutual Authentication): 상호인증은 Tag와 Reader 모두 상대 통신 당사자가 합법적인지를 명시적인 인증을 통해 확인하는 것이다.

제안한 프로토콜의 Step 4에서 Reader는 Tag로부터 수신한 v가 Reader 자신이 계산한 $a \cdot m_1 \oplus b \cdot m_2 \oplus x$와 동일한지를 검증하며, Step 6에서 Tag는 Reader로부터 수신한 e가 Tag 자신이 계산한 $m_1 \cdot x \oplus m_2 \cdot x$와 동일한지를 검증한다. 이로 인해 Tag와 Reader 사이에 공유된 비밀값 x를 모르는 한 공격자는 Tag 또는 Reader로 위장 공격을 수행할 수 없게 된다. 또한 제안한 프로토콜에서 사용되는 공유된 비밀값 x는 추측이 불가능한 비트 길이의 의미가 없는 랜덤 값을 사용함으로 공격자가 dictionary attack과 같은 불법적인 Reader에 의한 트랜잭션 트래킹 공격을 수행하여 공유된 비밀값 x를 추측할 수 없다. 따라서 제안한 프로토콜은 안전한 상호인증을 제공한다.

(2) 도청 공격(Eavesdropping Attack): 도청공격은 공격자가 Tag와 Reader간에 송수신되는 모든 통신 내용을 엿들은 후 Tag에 저장된 비밀 정보를 알아내고자 하는 공격이다.

제안한 프로토콜에서 공격자는 송수신되는 통신 메시지 a, b, e, v를 도청할 수 있다. 하지만 도청한 내용으로부터 공격자는 Tag와 Reader의 DB 간에 공유된 비밀 행렬 A와 비밀값 x를 구할 수 없다. x를 얻기 위해서는 공격자가 $v = a \cdot m_1 \oplus b \cdot m_2 \oplus x$와 $e = m_1 \cdot x \oplus m_2 \cdot x$로부터 소행렬 m_1과 m_2를 구할 수 있어야 한다. m_1과 m_2를 구하기 위해서는 비밀 행렬 A를 알아야 한다. 하지만 비밀 행렬 A는 Tag와 DB측에서 내부적으로 활용되어 지며 공개된 통신 채널로 전송되어 지지 않기에, 공격자는 A를 얻을 수 없기 때문에 소행렬 m_1과 m_2 또한 구할 수 없다. 또한 e와 v에 있는 m_1과 m_2 각각 비밀값 x로 암호화된 형태를 가짐으로 e와 v로부터 공격자는 x를 모르는 한 m_1과 m_2 또한 구할 수 없다. 따라서 제안한 프로토콜은 도청 공격에 안전하다.

(3) 재전송 공격(Replay Attack): 재전송 공격은 수동적 공격자가 과거에 Reader와 Tag 사이에 통신한 내용들을 도청한 후 이를 재전송하여 합법적인 Tag로 인증 받으려는 공격이다.

제안한 프로토콜에서는 매 세션마다 새로운 랜덤 값 a와 b를 생성하여 상호인증을 수행하기 때문에 과거에 공격자에 의해 재전송된 랜덤 값들은 Tag와 Reader간의 상호인증 과정 중에 쉽게 검출된다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

(4) 스푸핑 공격(Spoofing Attack): 스푸핑 공격은 공격자가 정당한 Tag로 위장하여 Reader로부터 인증에 필요한 정보를 획득하거나 또는 정당한 Reader로 위장하여 Tag로부터 인증에 필요한 정보를 획득하고 이를 이용하여 정당한 Tag 또는 Reader로 인증 받는 공격이다.

제안한 프로토콜에서 공격자가 Reader와 Tag간에 공유된 비밀 행렬 A와 비밀값 x를 얻을 수 있으면 스푸핑 공격을 수행할 수 있다. 하지만 공격자는 Reader와 Tag내에 각각 안전하게 저장하고 있는 A와 x를 얻을 수 있는 방법이 없다. 또한 송수신되는 통신 메시지 e와 v내의 비밀값 x는 랜덤 값 a와 b, 소행렬 m_1과 m_2에 의해 보호되어 있다. 따라서 제안한 프로토콜은 스푸핑 공격에 안전하다.

(5) 트래픽 분석 공격(Traffic Analysis Attack): 트래픽 분석 공격은 공격자가 도청을 통해서 얻은 내용을 분석하여 Reader의 질의에 대한 Tag의 응답을 예측하여 Tag의 이동경로를 트래킹 할 수 있는 공격이다.

제안한 프로토콜에서는 랜덤 값 a와 b에 의해 계산된 m_1과 m_2는 매 세션마다 변경되기에 공격자는

현재 세션에서 Tag의 응답 v_{now}가 이전에 도청한 응답 v_{old}과 동일한지를 비교할 수 없다. 즉, 2^v 비트의 경우의 수로 v를 생성할 수 있음으로 매 세션마다 서로 다른 두 개의 응답 v_{now}와 v_{old}이 동일한 Tag에서 나온 것인지를 쉽게 구별할 수 없음으로 태그의 이동경로를 쉽게 트래킹 할 수 없다. 따라서 제안한 프로토콜은 트래픽 분석 공격에 안전하다.

(6) 위치 트래킹 공격(Location Tracking Attack): 위치 트래킹 공격은 공격자가 Tag의 위치변화를 감지함으로 인해 Tag 소유자의 이동 경로를 파악하여 사용자의 프라이버시를 침해하는 공격이다.

제안한 프로토콜에서는 위 트래픽 분석 공격과 마찬가지로 랜덤 값 a와 b에 의해 계산된 m_1과 m_2는 매 세션마다 변경되기 때문에 공격자가 특정한 Tag를 식별할 수 없어 위치 트래킹을 할 수 없기에 사용자의 프라이버시 보호할 수 있다. 따라서 제안한 프로토콜은 위치 트래킹 공격에 안전하다.

(7) 서비스 거부 공격(Denial of Service Attack): 서비스 거부 공격은 Reader 또는 Tag가 정당한 통신 상대방의 인증 요청임에도 불구하고 공격자에 의한 많은 계산이 요구되는 데이터 송신, 이전 세션에서 갱신되는 값들을 올바른 값으로 갱신되지 못하도록 방해하는 등 Reader와 Tag가 정상적인 서비스와 기능을 수행 하지 못하도록 하는 공격이다.

제안한 프로토콜에서는 Reader와 Tag간에 XOR 기반의 연산만을 이용하여 상호인증을 함으로 많은 계산이 요구되지 않는다. 또한 매 세션마다 Reader와 Tag간에 상호인증 완료 후 갱신되는 값이 전혀 없다. 따라서 제안한 프로토콜은 서비스 거부 공격에 안전하다.

표 1은 제안한 프로토콜과 XOR 연산 기반의 프로토콜들인 HB, HB$^+$ 그리고 Lee와 Ahn의 프로토콜과의 안전성을 비교·분석한 표이다. 표 1과 같이 제안한 프로토콜은 기존의 프로토콜과 비교하여 상호인증을 명시적으로 제공함으로 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 안전함을 알 수 있다.

5.2 효율성 분석

표 2는 제안한 프로토콜과 Lee와 Ahn의 프로토콜과의 효율성을 비교·분석한 표이다. 표 2와 같이 Lee와 Ahn이 제안한 프로토콜과 비교하여 행렬 연산량은 동일하며, XOR 연산이 DB측과 Tag측에 각각 1번씩 더 수행되며, AND 연산도 DB측과 Tag측에 각 2번씩 더 수행된다. 이러한 추가적인 XOR 연산과 AND 연산은 Lee와 Ahn의 프로토콜이 가지는 보안 취약점들을 제거하기 위해 필요한 연산들로 결론적으로 Lee와 Ahn의 프로토콜과 비교하여 동일한 통신 효율성을 보장함을 알 수 있다. 더 나아가 제안한 프로토콜은 표 1과 2에서 각각 보여주는 것처럼 명시적인 상호인증을 제공함으로 인해 다양한 공격에 안전할 뿐만 아니라 Tag의 쓰기 연산을 요구하지 않으며, 통신 라운드 수 또한 2번을 줄여주어 안전성과 효율성 모두를 보장해 준다.

표 1. 관련 프로토콜들과의 안전성 비교·분석

공격	HB	HB$^+$	Lee-Ahn 프로토콜	제안 프로토콜
상호인증	×	×	×	○
도청공격	○	○	○	○
재전송공격	○	○	○	○
스푸핑 공격	×	○	○	○
트래픽 분석 공격	×	×	×	○
위치 트래킹 공격	×	×	×	○
서비스 거부 공격	○	○	×	○

표 2. 관련 프로토콜들과의 효율성 비교·분석

효율성	Lee-Ahn 프로토콜			제안 프로토콜		
	DB	Reader	Tag	DB	Reader	Tag
행렬 연산량	2	0	2	2	0	2
XOR 연산량	2n	0	2	2n+1	0	3
AND 연산량	2n	0	2	2n+2	0	4
랜덤값 생성수	1	0	1	0	1	1
Tag 쓰기연산	필요			불필요		
통신 라운드수	7			5		

n: DB에 저장된 Tag의 수

Ⅵ. 결 론

본 논문에서는 최근에 Lee와 Ahn에 의해 제안된 행렬기반의 RFID 인증 프로토콜을 분석하여 상호인증을 제공하지 않음으로 인해 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 취약함을 지적하였다. 더 나아가 이러한 보안 문제점을 해결

할 수 있는 상호인증을 제공하는 한 개선된 행렬기반 RFID 상호인증 프로토콜을 제안하였다.

결론적으로 제안한 프로토콜은 Lee와 Ahn의 프로토콜과 비교하여 DB와 태그에서의 1~2회의 XOR연산과 AND 연산만을 추가로 수행하여 상호인증을 제공케 하여 위와 같은 다양한 공격에 대해 안전하도록 개선하였다. 또한 과거에 제안된 HB와 HB^+ 그리고 Lee와 Ahn의 프로토콜과 비교하여 Tag의 쓰기 연산 부담을 없애고 통신 라운드 수도 줄여 줌으로써 효율성 측면에서도 더 개선되거나 큰 차이를 보이지 않음으로 최저가의 RFID Tag에 안전하고 효율적으로 적용 가능한 프로토콜이다.

향후 연구 과제로는 제안한 프로토콜을 실제 RFID 시스템 환경에서 구현하여 암호학적 공격뿐만 아니라 프로브 공격이나 TEMPEST 공격 등과 같은 물리적 공격에 대한 안전성 분석 및 실험에 대한 연구도 진행되어야 할 것이다.

참 고 문 헌

〔1〕 M. Weiser, "Some Computer Science Problems in Ubiquitous Computing", *Communications of the ACM*, July 1993.

〔2〕 M. Weiser, "Ubiquitous Computing", *Nikkei Electronics*, pp.137-143, December 1993.

〔3〕 S. E. Sarma, "Towards the Fivecent Tag", MIT Auto ID Center, *Technical Report MIT-AUTOID-WH-006.2001*. (http://autoid center.org)

〔4〕 A. Juels, R. L. Rivest, and 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.

〔5〕 S. A. Weis, S. E. Sarma, R. L. Rivest, and D. 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.

〔6〕 S. Junichiro, R. Jae-Cheol and S. Kouichi, "Enhancing Privacy of Universal Re-encryption Scheme for RFID Tags", *EUC 2004*, Vol. 3207 LNCS, pp.879-890, Springer-Verlag, 2004.

〔7〕 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.

〔8〕 M. Ohkubo, K. Suxuki and S. Kinoshita, "Efficient Hash-Chain Based RFID Privacy Protection Scheme", *Ubcomp 2004 workshop*.

〔9〕 A. Jule, "Minimalist Cryptography for Low Cost RFID Tag", *The Fourth International Conference on Security in Communication Networks SCN2004*, Vol. 3352 LNCS, pp.149-164, Sep 2004.

〔10〕 A. Jule, "Authentication Pervasive Devices with Human Protocols", *To appear Crypto 2005*, Aug 2005.

〔11〕 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.

〔12〕 H. Gilbert, M.Robshaw and H.Sibert, "An Active Attack Against HB^+ - A probably Secure Lightweight Authentication Protocol", (*http://eprint.iacr.org/2005/237*)

〔13〕 이수연, 안효범, "행렬기반 RFID 인증 프로토콜에 대한 연구", *정보·보안논문지*, 제6권, 제1호, 2006.

〔14〕 정병호, "RFID/USN 환경에서의 정보보호", *제9회 정보보호심포지움 SIS 2004*, pp.447-463, 2004.

〔15〕 최은영, 이동훈, "RFID 정보보호 기술 동향", *정보처리학회지*, 제12권, 제5호, 2005.

〔16〕 강전일, 박주성, 양대헌, "RFID 시스템에서의 프라이버시 보호기술", *정보보호학회지*, 제14권, 제6호, 2004

윤 은 준 (Eun-Jun Yoon) 정회원

1995년 2월 경일대학교 공학사 졸업
2003년 2월 경일대학교 컴퓨터 공학과 공학석사
2007년 2월 경북대학교 컴퓨터 공학과 공학박사
2007년 3월~2008년 2월 대구 산업정보대학 컴퓨터정보계열 전임강사
2008년 3월~현재 경북대학교 전자전기컴퓨터학부 BK21 박사후연구원
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

하 경 주 (Kyeoung-Ju Ha) 정회원

1991년 2월 경북대학교 컴퓨터 공학과 공학사
1993년 2월 경북대학교 컴퓨터 공학과 공학석사
1996년 2월 경북대학교 컴퓨터 공학과 공학박사
1996년~1999년 ETRI 부호기술 연구부 선임연구원
1999년 3월~현재 대구한의대학교 모바일콘텐츠학부 부교수
<관심분야> 정보보호, 시각암호, 스테가노그라피

유 기 영 (Kee-Young Yoo) 정회원

1976년 2월 경북대학교 수학과 이학사
1978년 2월 한국 과학 기술원 컴퓨터 공학과 공학석사
1992년 2월 미국 뉴욕 Rensselaer Polytechnic Institute 컴퓨터 과학과 이학박사
1978년 3월~현재 경북대학교 컴퓨터공학과 교수
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜