행렬기반 RFID 인증 프로토콜에 관한 연구

신효영* · 정계동**
*경복대학교
**광운대학교

A study on the matrix-based RFID authentication protocol

Hyo-Young Shin* · Kye-Dong Jung**
*Kyungbok University
**Kwang-woon University
E-mail : hyshin@kbu.ac.kr

요 약

최근 RFID 시스템을 물류, 유통 분야를 비롯한 여러 분야에서 활용하기 위해RFID 시스템에 대한 정보보호에 대한 연구가 활발히 진행되고 있다. 본 논문에서는 기존에 제안된 행렬기반 RFID 인증 프로토콜이 갖는 단점을 개선하고, 행렬을 이용하여 성능이 향상된 인증 프로토콜을 제안한다. 제안된 인증 프로토콜은 상호인증을 제공하고, 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격 등에도 강하며, 백엔드 데이터베이스의 부하를 줄여 시스템 효율이 우수한 장점을 갖는다.

ABSTRACT

Recently, research on security of RFID system has been conducted actively in order to utilize RFID system in various fields including distribution and logistics. This paper suggests an authentication protocol which supplement the flaws of previous RFID authentication protocols and we improved its performance using matrix-based authentication. The suggested authentication protocol provides mutual authentication, protects from wiretapping attack, replay attack, spoofing attack, and traffic analysis attack and so on, and reduces overload of back-end database so that has efficient performance.

키워드
RFID, 인증, 행렬, 정보보호

Ⅰ. 서 론

RFID(Radio Frequency Identification)는 모든 사물에 전자 태그를 부착하고 무선 통신 기술을 이용하여 사물의 정보 및 주변 상황정보를 감지할 수 있는 기술이다[1].

RFID 시스템은 가까운 거리의 통신으로 사물을 인지할 수 있으므로 물류, 유통, 재고관리 등에 유용한 도구로 사용되고 있다.

RFID 시스템은 태그, 리더, 데이터베이스의 3가지 요소로 구성된다. 태그는 자신만의 고유한 ID를 갖고 태그가 부착된 사물에 대한 정보 요청이 있으면 자신의 ID 정보를 알려주는 기능을 한다. 태그는 전원공급 방식에 따라 수동형과 능동형으로 분류할 수 있다[2,8].

리더는 태그들로부터 ID를 수집하여 태그를 인

식하거나 태그에 새로운 정보를 다시 쓰는 역할을 수행한다. 리더는 태그로부터 받은 정보를 데이터베이스에 전송하는 기능도 수행한다.

데이터베이스는 태그에 관련된 정보를 저장하고 관리하는 역할을 수행한다. 데이터베이스는 연산능력이 낮은 리더나 태그를 대신하여 연산을 수행하기도 하며 리더로부터 수신한 태그의 정보를 통해 태그를 식별하고 수신한 정보의 정확성을 판별하는 역할을 수행한다.

적절한 정보보호 기능을 구현하지 않은 RFID 시스템은 도청, 트래픽 분석, 스푸핑, DoS 등의 공격에 취약할 수 있다. 이러한 공격으로 사용자 정보를 비롯한 민감한 자료가 유출될 수 있으므로 안전한 접근제어와 인증과정을 통한 시스템 보호장치가 필요하다.

RFID 시스템 보안을 위해 기존에 제안된기술에는 물리적 보안을 위해 킬 태그, 페러데이 케이지, Active Jamming, Blocking 태그 등이 있으며, 도청방지를 위해 silent tree-walking, 재암호화 방법 등이 있다. 인증 및 접근제어를 위해 해쉬함수, 암호 알고리즘을 이용하는 방법과 XOR 연산을 이용하는 방법들이 제안되었다[5,6,7].

지금까지 제안된 대부분의 인증 프로토콜은 백엔드 데이터베이스가 태그를 인증하기 위해 데이터베이스에 저장된 모든 태그의 식별정보를 확인해야 하는 절차가 포함되어 있어서 데이터베이스에 많은 연산량을 요구하는 단점이 있다.

Lee와 Ahn은 기존의 HB와 HB+ 인증 프로토콜의 보안취약점을 보완하기 위해 행렬기반의 RFID 인증프로토콜을 제안하였다[9]. 제안된 프로톨은 태그의 계산량을 감소시켰고, 통신 부하가 줄었으며, 사용자 프라이버시 등의 장점을 제공한다. Yoon등은 Ha 등은 앞서 제안된 행렬기반프로토콜이 트래픽분석 공격과 같은 다양한 공격에 취약함을 지적하고 상호인증이 가능한 프로토콜을 제안하였다[10]. 그러나 이 인증방법은 데이터베이스에서 모든 태그에 대한 연산을 요구하여 태그 수 증가에 따라 데이터베이스 시스템에 부하가 증가되는 단점이 있다.

본 논문에서는 미리 계산된 검증값을 데이터베이스에 저장하여 인증과정에서 백엔드 데이터베이스의 연산량을 줄여서 전체적인 RFID 시스템의 성능을 향상시키기 위한 인증 프로토콜을 제안한다. 제안된 프로토콜은 상호인증을 제공하고, 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격 등에도 강하며 시스템 효율이 우수한 장점을 갖는다.

II. 관련 연구

RFID 시스템의 구조와 보안 요구사항 기존에 수행된 관련 연구들은 다음과 같다.

2.1 Lee와 Ahn의 프로토콜

Lee와 Ahn은 행렬을 기반으로 하는 RFID 인증 프로토콜을 제안하였다. 인증프로토콜을 수행하기 전의 초기화 단계에서 태그와 리더 사이에는 비밀 행렬 $A(n\times n)$와 이전 세션에서 계산된 랜덤 값 v'를 공유하고 있다. 이 프로토콜에서는 비밀 행렬 A의 크기 k비트를 증가시켜 $n\times n$ 개수의 소행렬을 생성시켜 복잡도를 높일 수 있다.

그림 1은 Lee와 Ahn이 제안한 인증 프로토콜의 인증과정을 보여준다. 이는 상호인증을 제공하지 않아 트래픽분석공격, 위치트래킹공격, 서비스 거부공격 등에 취약함을 보인다[5].

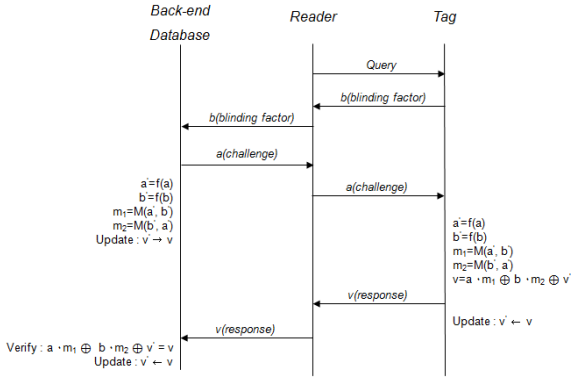

그림 1. Lee와 Ahn의 행렬기반 RFID 인증 프로토콜

2.2 Yoon, Ha, Yoo의 상호인증 프로토콜

Yoon, Ha, Yoo는 Lee 와 Ahn이 제안한 프로토콜의 보안 취약점을 해결하기 위해 상호인증이 가능한 프로토콜을 제안하였다.

이 프로토콜에서는 초기화 단계에서 태그와 리더 사이에는 비밀 행렬 $A(n\times n)$와 비밀값 x를 공유하고 있다고 가정한다. 그림 2는 상호인증 프로토콜의 단계를 보여준다.

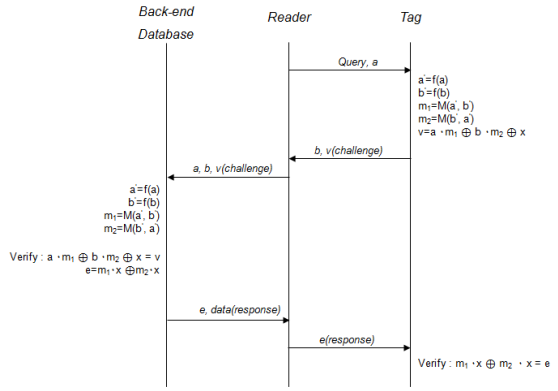

그림 2 행렬기반 RFID 상호인증프로토콜

이 인증 프로토콜은 상호인증을 제공하여 트래픽 분석공격을 비롯한 보안 문제점을 해결하였다. 그러나 데이터베이스에 저장된 태그들의 비밀값

x를 모두 대입하는 연산을 수행하여 수신된 v값과 일치하는지를 모든 인증 과정에서 수행해야한다. 이러한 부하는 시스템이 확장되어 태그 수가 증가할 수록 부하가 증가되는 단점이 있다.

III. 제안 프로토콜

3.1 용어 정의

제안 프로토콜에서 사용하는 용어들을 다음과 같이 정의한다.

· *Query* : 태그의 응답을 요청하는 리더의 질의어

· *TID* : 태그의 *ID*

· $\oplus$: 배타적 논리합 연산

3.2 초기화 단계

제안한 프로토콜을 실행하기 전에 데이터베이스, 리더, 태그에서 초기화해야할 사항들은 다음과 같다.

① 모든 태그에 자신의 식별자로 비밀정보인 *TID* 값을 저장한다.

② 모든 태그와 데이터베이스는 비밀 키 정보인 x 값을 공유한다.

③ 태그와 데이터베이스 간에는 $n \times n$ 크기 비밀 행렬 A(=k 비트)를 공유한다.

④ 데이터베이스에는 모든 태그의 식별자인 *TID* 값과 *TID*별로 할당된 비밀키 정보 x값을 저장한다.

3.3 제안 프로토콜 실행 절차

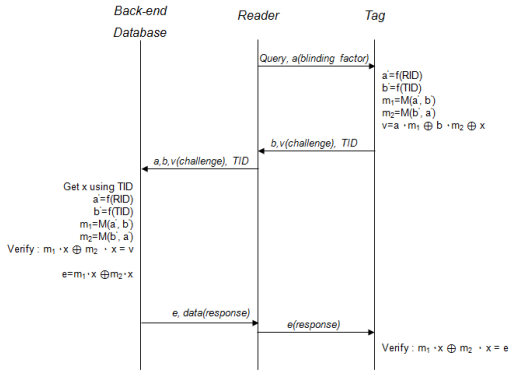

그림 3 제안 프로토콜 구조

단계 1. 리더 → 태그 : $Query, a(blinding\,factor)$

리더는 질의어와 함께 랜덤값 $a \in_R (0,1)^k$를 생성하여 태그로 전송한다.

단계 2. 태그 → 리더 : b, v, TID

태그는 리더로부터 질의어와 a를 수신한 후 행렬 A의 소행렬 위치 $a' = f(RID)$, $b' = f(TID)$를 계산한다. 여기서 함수 $f()$는 a와 b가 n보다 작거나 같다는 조건을 만족시키기 위하여 사용한다. 데이터베이스와 공유한 비밀행렬 A로부터 소행렬 $m_1 = M(a', b')$과 $m_2 = M(b', a')$를 생성한다. 생성된 소행렬 m_1과 수신한 a를 $a \bullet m_1$과 같이 AND 연산하고, 소행렬 m_2와 b를 $b \bullet m_2$와 같이 AND 연산한다. 마지막으로 공유 비밀값 x와 XOR 연산을 하여 $v = a \bullet m_1 \oplus b \bullet m_2 \oplus x$를 계산한 후 리더로 *TID*와 함께 전송한다.

단계 3. 리더 → 데이터베이스 : a, b, v, *TID*

리더는 태그로부터 수신한 v를 a, b, *TID*와 함께 데이터베이스로 전송한다.

단계 4. 데이터베이스 → 리더 : $e, data$

데이터베이스는 저장된 x 값 중에서 리더로부터 수신한 *TID*에 해당하는 x를 찾는다. 이후 소행렬 위치를 $a' = f(a)$, $b' = f(b)$계산하고, 소행렬 $m_1 = M(a', b')$과 $m_2 = M(b', a')$를 생성한다.

$a \bullet m_1 \oplus b \bullet m_2 \oplus x$를 계산하여 수신한 v와 일치하는지 검증한다. 만일 일치하지 않으면 데이터베이스는 이를 가짜 태그로 판단하고 통신을 종료한다.

두 값이 일치하는 경우 상호인증을 수행하기 위해 데이터베이스는 계산된 m_1과 m_2를 이용하여 $e = m_1 \bullet x \oplus m_2 \bullet x$를 계산한 후 리더로 전송한다. 이 과정을 알고리즘으로 기술하면 다음과 같다.

x = xValue[TID] // Get x using TID
$a' = f(a)$
$b' = f(b)$
$m_1 = M(a', b')$
$m_2 = M(b', a')$
$e = m_1 \bullet x \oplus m_2 \bullet x$
If $(a \bullet m_1 \oplus b \bullet m_2 \oplus x) == v$
  Send e To Reader
Else
  Send Error Message

단계 5. 리더 → 태그 : e

리더는 데이터베이스로부터 수신한 e 값을 태그로 전송한다.

단계 6. 태그

태그는 공유 비밀값 x와 소행렬 m_1, m_2를 이

용하여 $e' = m_1 \bullet x \oplus m_2 \bullet x$를 계산한다. e'와 수신한 e가 동일하면 태그는 리더를 인증하게 되어 상호 인증이 이루어진다.

V. 결 론

RFID 시스템은 물류시스템의 자동화를 비롯하여 통신, 의료, 환경, 국방 분야 등 그 사용이 증가하고 있다. RFID 시스템의 사용확대를 위해 정보보호에 대한 연구 또한 활발히 진행되고 있으며, 인증 및 접근제어를 위해서 해쉬함수, 암호 알고리즘을 이용하는 방법과XOR 연산을 이용하는 방법들이 제안되었다.

기존 연구에서 Lee와 Ahn은 행렬기반 인증프로토콜을 제안하였고, Yoon, Ha, Yoo은 행렬기반의 상호인증 프로토콜을 제안하였다. 그러나 Lee와 Ahn의 프로토콜은 상호인증을 제공하지 않아 트래픽분석공격, 위치트래킹공격, 서비스거부공격 등에 취약함을 보인다.

Yoon, Ha, Yoo의 인증프로토콜은 상호인증을 제공하여 도청공격 등 보안성 면에서 기존의 Lee와 Ahn의 프로토콜을 보완하였으나, 백엔드 데이터베이스에게 부하를 많이 주는 단점을 가지고 있다. 백엔드 데이터베이스에 저장된 공유 비밀값 x를 이용하여 XOR 연산을 하여 수신한 v와 일치하는 x가 존재하는 지를 검증하기 위해서는, 백엔드 데이터베이스에 등록된 모든 태그들을 검색하여 검증하기 위한 연산을 수행해야한다. 이러한 작업은 태그의 수가 증가하여 시스템이 확장될 수록 데이터베이스시스템에대한 부하가 증가하는 문제가 발생한다.

본 논문에서는 태그 ID를 이용하여 데이터베이스에서 공유된 비밀값을 효율적으로 검색할 수 있는 인증프로토콜을 제안하였다. 제안 프로토콜에서는 태그 ID를 인덱스로 사용해 공유된 비밀값을 직접 접근할 수 있으므로 데이터베이스의 부하없이 직접 검증연산을 수행할 수 있으며, 태그의 수가 아무리 증가하여도 데이터베이스 시스템에 미치는 부하의 영향이 적은 장점을 가질 수 있다.

제안된 인증 프로토콜에 대한 안전성과 효율성 분석을 향후 연구에서 진행할 예정이다. 제안된 알고리즘에 대한 상호인증, 도청공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 대한 안전성을 분석하고, 제안 프로토콜의 행렬 연산량, XOR 연산량, AND 연산량, 랜덤 값 생성수, 통신 라운드 수 면에서의 효율성도 분석할 것이다.

제안된 인증 프로토콜은 안전성 면에서 기존 프로토콜 보다 안전하거나 비스한 안전성을 유지하며, 데이터베이스 시스템의 부하를 줄여주어 안전성과 효율성면에서 우수한 기능을 제공할 것으로 기대된다.

참고문헌

[1] R. Chandramouli, T. Grance, R. Kuhn, "Security Standards for the RFID Market ", IEEE Security & Privacy, Dec. 2005.

[2] Christian Flockermeier, Sanjay Samara, "An Overview of RFID System Interfaces and Reader Protocols", 2008 IEEE International Conference on RFID, pp.232-pp.240, April, 2008

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

[4] A. Jules, R. L. Rivest, and M. Szydlo " 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] H. Gillbert, M. Robshaw, H. Sibent, "Active attack against HB+: a probably secure lightweight authentication protocol", Electronics Letters, 13th October, vol. 41, No. 25, 2005.

[6] S. L. Garfinkel, A. Jules and R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions", IEEE Security and Privacy, vol. 3, pp.34-43, May/June 2005.

[7] Lars Kulseng, Zhen Yu, Yawen Wei, Young Guan, "Lightweight Secure Search Protocols for Low-cost RFID Systems, 29th International Conference on Distributed Computing Systems, 2009.

[8] Simon L. Garfinkel, Ari Juels, Ravi Pappu, "RFID Privacy: An overview of problems and proposed solutions", IEEE Security & Privacy, May/June, 2005.

[9] 이수연, 안효범, “행렬기반 RFID 인증 프로토콜에 대한 연구”, 정보·보안논문지, 제6권, 제1호, 2006.

[10] 윤은준, 하경주, 유기영, “견고한 행렬기반 RFID 상호인증 프로토콜”, 한국통신학회논문지, Vol. 33, No. 11, 2008.

[11] 최은영, 최동희, 임종인, 이동훈, “저가형 RFID 시스템을 위한 효율적인 인증 프로토콜, 정보보호학회논문지, 제 15권, 제5호, 2005.

[12] 김익수, “효율성을 고려한 해시함수 기반의 안전한 RFID 프로토콜”, 한국통신학회논문지, 제34권 4호, pp.428-434, 2009.

[13] 이향진, 신동휘, 전길수, “RFID 프라이버시 보호기술 및 표준화 동향”, 정보보호학회지, 제18권 제4호, 2008.