난수를 이용한 RFID 태그와 리더의 보안 인증 프로토콜

배우식*

An Authentication Protocol for the Security of RFID Tags and Readers using Random Number

Bae Woo Sik*

요 약 RFID 시스템은 태그와 리더사이의 무선통신 기술을 통해 사물의 정보를 감지하는 기술로 다양한 분야에 사용범위가 확장되고 있다. 그러나 무선으로 통신을 하므로 보안상 많은 취약점이 존재한다. 최근까지 RFID의 보안 및 안정성 문제를 해결하기 위하여 수많은 연구가 진행되고 있다. 본 논문에서는 여러 보안문제 중 프라이버시 보호를 위한 기존 기법의 취약점을 보완하여 태그가 리더로부터 수신한 해시 값과 난수 값을 기반으로 설계한 인증 프로토콜을 제안한다. 제안을 바탕으로 구현 할 때 태그와 리더간 그리고 리더와 DB 간에 각종 공격에 안전하다. 아울러 최근 제안된 타 프로토콜에 비해 보안성은 강력해지며 태그의 연산량은 줄이고 RFID시스템을 구현할 수 있는 프로토콜이다.

주제어 : 인증 프로토콜, 프라이버시 보호, RFID 보안, RFID 인증

Abstract A RFID system is a technology for detecting information on an object through wireless communication between a tag on the object and a reader, and its applications are being expanded to various areas. Because of its wireless communication, however, there are many vulnerabilities in security. Until now, many studies have been executed in order to solve problems related to the security and stability of RFID. In order to resolve vulnerabilities in existing security methods for privacy protection, this study proposed an authentication protocol that uses hash values received from tags and random numbers. When the proposed protocol was implemented, it was safe from various types of attacks between tag and reader and between reader and DB. Furthermore, compared to recently proposed protocols, it could implement a RFID system with enhanced security and less computation in tags.

Key Words : Authentication Protocol, Privacy Protection, RFID Security, RFID Authentication

1. 서론

RFID(Radio Frequency Identification)는 전자태그를 물품에 부착하여 기존의 IT시스템과 실시간으로 정보를 교환, 처리할 수 있는 기술을 말한다. RFID는 높은 인식률, 비 접촉형 인식매체, 도달거리, 다른 통신망과의 연계 및 통신 가능성 등의 확장성으로 인해 특히 물류, 유통, 군사, 식품안전 및 의료분야 등 산업전반에 막대한 파급효과를 끼칠 전망이다. 특히 의료 분야에서는 매년 약물의 잘못된 포장 등으로 많은 사람이 죽거나 부작용에 시달리고 있는 문제를 볼 때 자동으로 약품의 정보를 알 수 있다면 좀더 정확한 투약이 될 것이며 이러한 시스템에 보안 분야의 문제가 발생할시 프라이버시 침해로 문제가 될 수 있다[8].

*아주자동차대학
논문접수: 2012년 5월 4일, 1차 수정을 거쳐, 심사완료: 2012년 5월 21일

1.1 연구 배경 및 필요성

그러나, RFID 시스템은 그 편리성에도 불구하고 무선 구간의 비접촉식 인식시스템이라는 특징 때문에 안정성과 프라이버시 보호 측면에서 문제점을 지니고 있다.[7] 보안상 안전하지 않는 태그를 사용하는 경우 물리적 공격, 위조, 스푸핑, 도청, 트래픽 분석, DOS 공격 등에 의한 보안적 취약점에 노출되어 진다. 이러한 취약점을 방지하기 위해 태그에 저장 관리되는 식별 정보를 보호하기 위한 다양한 방법이 제안되고 있다[2][4][6]. 하지만 대부분의 프로토콜이 태그에서의 연산이 과중하여 태그 제작시 비용증가를 불러오게 되어 RFID 시스템의 도입이 지연되고 있다. 따라서 연산량을 줄이고 보안성은 보장되는 프로토콜의 설계가 무엇보다 중요하다.

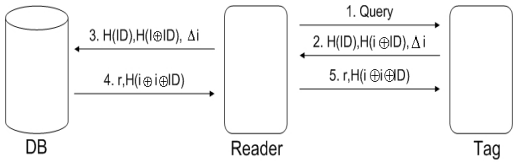
1.2 학문적 기여

본 논문에서는 RFID의 프라이버시 문제를 해결하기 위해 기존에 제안된 해시관련 기법[1][3][5] 등에서 해결하지 못한 문제점을 보완하여 보다 안전하고 효율적으로 사용자의 프라이버시를 보호할 수 있는 인증프로토콜을 제안한다. 타 프로토콜에 비해 태그에서의 연산은 줄였으며 매 세션마다 동일한 데이터가 아닌 새로운 데이터가 전송되어 보안성을 높였다. 이로 인하여 RFID시스템에 적용할시 저가로 태그를 제작할 수 있으며 리더에서 생성한 해시함수와 난수를 이용하여 공격자의 공격에 대응함으로써 추후 예상되는 각종공격에 보안성을 제공하여 안전한 RFID 시스템이 되도록 하는 프로토콜이다.

2. 관련 연구

2.1 해시 기반 ID변형기법

해시 기반 ID 변형기법[5]은 ID가 인증 세션마다 바뀌므로 변형되는 ID를 저장하고 있는 데이터베이스가 존재해야만 하는 문제점이 있다. 본 프로토콜은 매 세션마다 태그의 ID가 난수 R에 의해 갱신되므로 재전송 공격으로부터 안전하다. 그러나 공격자가 태그로부터 H(ID), H(i⊕ID), Δi를 획득하고, 정당한 태그가 다음 인증세션을 수행하기 전에 정보들을 리더의 질의에 대한 응답으로 전송하면 프라이버시를 침해받을 수 있는 문제가 있다. 다음의 [그림 1]은 해시기반 ID변형기법의 구조도 이다.



[그림 1] 해시 기반 ID 변형 기법

2.2 Ahn-Bu외 2명의 프로토콜

본 인증 프로토콜은[1] 비교적 복잡한 연산을 수행한다. 태그에서 해시연산 3회, 난수생성 1회, 쓰기연산이 필요하며, 리더에서는 난수 1회, DB에서 해시연산이 2n+2회의 연산이 필요하고 태그에서의 해시 연산이 $S_T = h(0 \| ID \| N_T \| N_R)$로 복잡하게 이루어진다. 타 인증 프로토콜에 비해 비트가 많은 데이터의 전송과 연산이 이루어지며 $S_T = h(1 \| ID \| N_T \| N_R)$, $S_T = h(2 \| ID \| N_T \| N_R)$ 값을 계산하여 저장하기 때문에 해시 전 0,1,2를 알아낼 경우 태그로 위장하여 도청공격 또는 DB에서 최종처리 된 $ID_{new} = h(2 \| ID \| N_T \| N_R)$ 값도 알아낼 수 있기 때문에 리더로 가장한 각종공격자의 공격의 위험성이 있는 문제가 있다.

2.3 Lee외 2명의 프로토콜

본 상호인증 프로토콜은[3] 태그에서 다양한 연산을 요구하는데 해시연산 2회, 쓰기동작 2회, XOR연산 2회의 연산이 필요하다. 특이한 점은 기존의 리더에서 태그에게만 보내던 Query를 태그의 ID를 유지하는 DB에게도 동시에 보냄으로써 DB도 난수 값을 생성하게 된다. 이로 인하여 태그에서의 쓰기 동작이 2회가 발생하며 인증 단계가 증가하는 단점이 있다.

3. 제안하는 인증 프로토콜

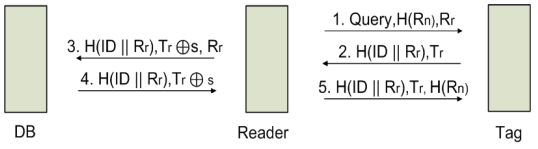
3.1 구조

본 논문의 제안 프로토콜의 리더는 난수 생성기를 갖고 있으며, 리더가 처음 태그에게 질의를 할 때 난수와 해시된 값을 함께 전송하고, 태그는 리더로부터 수신한 난수와 해시 값을 자신이 가지고 있는 ID와 해시한 값을 이용하여 매 세션마다 다르게 응답함으로써 재전송 공격과 스푸핑 공격에 대하여 안전하다. 제안프로토콜에서

데이터베이스는 태그의 ID와 관련 데이터를 저장하고 있으며, 리더를 인증하기 위한 비밀키 확인과 해시함수 1회의 연산만을 이용하여 태그를 인증한다.

제안 프로토콜에서 사용되는 파라미터는 다음과 같으며, [그림 2]는 제안하는 프로토콜의 기본구조를 나타낸 것이다.

[파라미터]
- Query : 질의, 태그의 응답을 요청
- ID : 태그 고유의 정보
- H( ) : 해시함수 연산
- H(R_n) : 리더가 태그에게 전송하는 해시된 리더코드
- s : 리더와 DB간의 공유된 비밀 키
- R_r : 리더가 생성한 난수
- T_r : 태그가 생성한 난수
- $\oplus$:배타적 논리합(XOR)
- || : 연접(Concatenate function)



[그림 2] 제안 프로토콜의 구조

3.2 제안 프로토콜의 인증과정

[Step 1] 리더는 태그에게 Query와 H(R_n)R_r를 함께 브로드캐스팅 한다.

create H(R_n), R_r
send Query, H(R_n), R_r to tag

[Step 2] 태그는 ID와 자신이 가지고 있던 ID를 연접한 후 해시하고 난수를 생성하여 Query에 대한 응답으로 리더에게 전송한다.

Tag receive Query, H(R_n), R_r
compute
A1 = $H(ID \| R_r)$
create T_r
send A1, T_r to Reader

[Step 3] 리더는 $H(ID \| R_r)$ $T_r \oplus$s, R_r를 백-엔드 데이터베이스로 전송한다.

Reader receive A1, T_r
send A1, $T_r \oplus$s, R_r to Database

[Step 4] 백-엔드 데이터베이스는 $T_r \oplus$s값을 확인한 후 임시메모리에 이동시킨 다음 저장된 ID를 해시한 값과 리더로부터 수신한 $H(ID \| R_r)$를 비교하여 태그를 인증한다.

Database receive A1, $T_r \oplus$s, R_r
compute
$H(ID \| R_r)$
Database search $H(ID \| R_r)$
if found $H(ID \| R_r)$
A2 = $H(ID \| R_r)$
if A1 = A2
send A2, $T_r \oplus$s to Tag
else
End of Present Session
else
End of Present Session

인증이 성공하면 $H(ID \| R_r)$ $T_r \oplus$s를 리더에게 전송한다.

[Step 5] 태그는 자신의 ID와 인증세션에서 생성된 $H(ID \| R_r)$와 리더로 부터 수신된 $H(ID \| R_r)$ T_r, H(R_n)를 확인하여 인증을 성공적으로 종료한다.

Tag receive A2, T_r
if A2 = $H(ID \| R_r)$ T_r, H(R_n)
End of Present Session

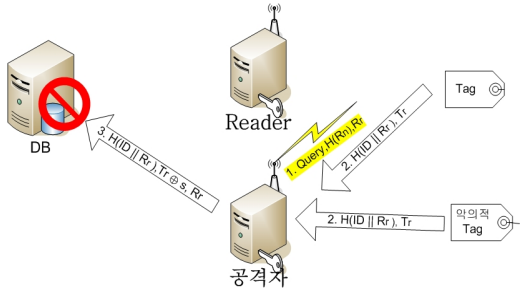
3.3 제안 프로토콜의 안전성

3.3.1 스푸핑 공격에 대한 안전성

스푸핑 공격은 공격자가 정당한 태그로 위장하여 리더로부터 인증에 필요한 정보를 알아내거나 정당한 리더로 위장하여 인증에 필요한 태그의 정보를 알아내는 공

격방법이다.

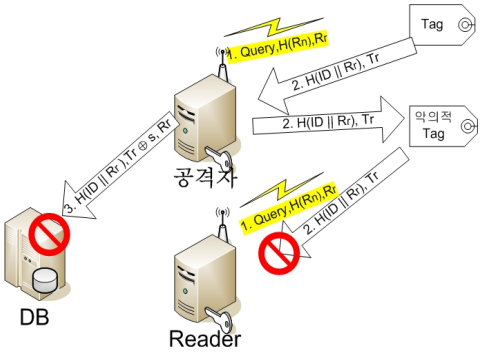
본 제안프로토콜은 공격자가 정당한 리더로 가장하여 $H(R_n)R_r$를 전송하면, $H(R_n)R_r$를 획득할 수 있으나 악의적인 태그에 넣어 응답으로 보내지게 되면 다음세션에서 사용하는 난수가 달라지며 세션이 바뀐 후의 정보 $H(R_n)R_r$ 로는 인증을 할 수가 없으며 데이터베이스에서 $H(ID \| R_r)\ T_r$s를 계산하는 과정에서 위장한 태그를 확인할 수 있어 [그림 3]과 같이 스푸핑 공격이 DB의 거부로 불가능 하게 된다.



[그림 3] 스푸핑 공격 거부

3.3.2 재전송 공격에 대한 안전성

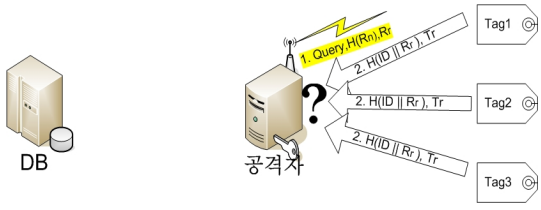
제안 프로토콜에 정당한 리더로 가장한 공격방법으로 공격자는 이전 세션에서 도청으로 $H(R_r)R_r$, $H(ID \| R_r)\ T_r$를 획득할 수 있지만 정당한 리더의 Query와 $H(R_n)R_r$는 매 세션마다 변하기 때문에 $H(ID \| R_r)\ T_r$도 매 세션마다 바뀌게 된다. 그러므로 공격자는 도청으로 획득한 $H(R_r)R_r$, $H(ID \| R_r)\ T_r$를 [그림 4]처럼 다음 세션에서는 응답으로 사용할 수 없으므로 재전송 공격에 안전하다.



[그림 4] 재전송 공격 거부

3.3.3 트래픽 분석과 위치 추적에 대한 안전성

공격자가 Query와 $H(R_r)R_r$를 태그에게 전송하여도 이후 세션에서는 DB에서의 인증이 필요하여 매 세션마다 변하는 응답을 전송하므로 [그림 5]와 같이 공격자는 트래픽 분석이 불가능하고 태그의 위치도 추적할 방법이 없게 된다.



[그림 5] 위치추적 공격 안전성

3.4 제안 프로토콜의 효율성

기존의 제안 프로토콜과 효율성을 비교하기 위하여 태그, 리더, 데이터베이스의 연산량을 [표 1]과 같이 비교하였다. 데이터베이스 및 리더의 연산보다 태그에서의 연산이 많을 경우 효율성이 떨어진다고 할 수 있다. 제안한 프로토콜의 태그는 인증세션 동안 해시함수 1회 리더는 난수 1회의 연산만을 수행하므로 연산부담도 크지 않으며 보안성을 충족하고 타 프로토콜에 비해 효율이 우수하며 저가의 태그에 적용이 가능하다.

[표 1] 제안프로토콜의 효율성

	해시기반 ID변형기법	Ahn-Bu외 2명의 프로토콜	Lee외 2명의 프로토콜	제안프로토콜
태그 연산량	해시3회	난수 1회 해시 3회 쓰기 1회	해시 2회 쓰기 2회 XOR 2회	해시1회
리더 연산량	-	난수 1회	난수 1회	난수1회
DB연산량	해시3회 난수1회	해시 2n+2	난수 1회 해시 1회	해시1회

4. 결론

최근 들어 바코드를 대체하여 모든 산업 분야에서 RFID 시스템의 구축이 진행되기 시작하였다. 귀중품 관리, 의료용 제품관리, 진품인증 및 각종 제품관리에 편리

성 향상으로 확산되어 지고 있다. 그러나 시스템 구성상 무선으로 데이터를 읽어 들이는 특성 때문에 보안적인 측면에서 프라이버시 노출 문제에 대한 해결이 있어야 하는 부분이 있다. 기존에 제안된 프로토콜들은 보안상 취약 하거나 태그에서의 연산이 많아 실제로 구현하기에 어려움이 있으며 태그제작 비용이 상승하는 문제가 있다. 본 논문에서 제안한 인증 프로토콜은 태그가 리더로부터 수신한 난수 및 해시된 리더코드로 부터 매 세션마다 다른 응답을 전송할 수 있도록 했다. 이로 인하여 타 프로토콜에 비해 구현에서 리더의 추가적인 해시 연산을 요구 하지만 그 비용은 크게 증가 하지 않는다. 아울러 태그의 연산량을 해시 1회로 줄여 안정성을 제공하며, 보안적인 측면에서도 공격자의 재전송 공격, 스푸핑 공격, 위치추적 등에 안전한 인증 프로토콜로써 RFID 시스템에 적용시 안전성과 효율성을 충족할 수 있다.

참 고 문 헌

[1] 안해순, 부기동, 윤은준, 남인길 “강력한 보안성을 제공하는 RFID 상호 인증 프로토콜” 정보처리학회논문지 C 제16.C권 제3호 pp.325-334, 2009.

[2] 원태현, 유영준, 천지영, 변진욱, 이동훈,“온라인 백-엔드 데이터베이스가 없는 안전한 RFID 상호 인증 프로토콜”, 정보보호학회논문지, 제20권, 제1호, pp. 63-72, 2010.

[3] 이승민, 김은환, 전문석 “모바일 RFID를 위한 보안 RFID 상호인증 프로토콜 설계” 한국통신학회논문지 10-2 Vol. 35 No.2 pp.183-190, 2010.

[4] 주학수, “RFID 시스템의 보안 및 프라이버시 보호를 위한 기술 분석”, 전자정보센터, 2004.

[5] Gildas Avoine and Philippe Oechslin "RFID Traceability : A Multilayer Problem", Financial Cryptography, March 2005.

[6] Jun Zhou; Yongjun Xu; Xiaowei Li; Inst. “Reconfigurable and scalable security module of active RFID for security-sensitive applications” Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference, pp.135-140, April 2010

[7] X. Lin, R. Lu, D. Kwan and X. Shen. REACT: An RFID-based Privacy-preserving Children Tracking Scheme for Large Amusement Parks. Computer Networks 54(2010) 2744-2755

[8] Yu YC, Hou TW, Chiang TC."Low Cost RFID Real Lightweight Binding Proof Protocol for Medication Errors and Patient Safety" 2 April 2010 / Accepted: 14 June 2010 Springer Science+Business Media, LLC 2010

배 우 식

- 1997년~현재 아주자동차대학
- 2006년 백석대학교 정보기술대학원 (공학석사)
- 2012년 충북대학교 대학원 컴퓨터교육과(교육학박사)
- 2009년~2010년 한국산학기술학회 이사역임
- 2010년~현재 한국융합학회 총무이사
- 2010년~현재 중소기업정보기술융합학회 이사
- 관심분야 : RFID 보안, 무선 네트워크, 암호 프로토콜/알고리즘, 정보시스템
- E-Mail : bws@motor.ac.kr