RFID 시스템 보안 강화를 위한 비공개 코드 기반의 인증 프로토콜

장봉임* · 김용태** · 정윤수*** · 박길철****

Authentication Protocol of Private Code-based for Advanced Security of RFID System

Bong-Im Jang* · Yong-Tae Kim** · Yoon-Su Jeong *** · Gil-Cheol Park****

이 논문은 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(2009-0074117)

요 약

최근 산업 및 생활 전반에 걸쳐 RFID(Radio Frequency IDentification)의 사용은 증가 추세에 있으며, 더욱 확대될 전망이다. 그러나 RFID는 인증과정에서 도청, 재전송 공격, 스푸핑 공격(Spoofing attack), 위치 추적 공격 등의 악의적인 위협으로부터 취약하다. 특히 저가형 RFID태그에는 기존의 다른 시스템에서 사용되던 인증 프로토콜의 적용이 어려운 실정이다. 따라서 본 논문에서는 RFID 프라이버시 보호를 위한 효율적인 인증 프로토콜 기법을 제안한다. 제안 기법은 기존의 기법에 비해 전송 데이터의 검증과정을 강화하여 도청이나 스푸핑 공격으로부터 안전하며, 태그의 연산 작업을 최소화하여 저가형 태그로의 적용이 유용하다. 또한 통신 라운드 수를 줄여 통신의 효율성을 보장하는 장점을 가진다.

ABSTRACT

The use of RFID recently tends to increase and is expected to expand all over the industry and life. However, RFID is much vulnerable to the malign threats such as eavesdropping, replay attack, spoofing attack, location tracking in the process of authentication. In particular, it is difficult to apply authentication protocol used in the other previous system to low-priced RFID tag. After all, this paper suggests the scheme of efficient authentication protocol for RFID privacy protection. Compared to the previous scheme, suggested scheme reinforces the checking process of transmission data and is secure from eavesdropping and spoofing attack. It minimizes the operation work of the tag and is very useful to apply to the low-priced tag. It also has the merit to confirm the efficiency of communication by reducing the communication rounds.

키워드

RFID 시스템, 인증 프로토콜, 해쉬 함수, 보안

Key word

RFID System, Authentication Protocol, Hash Function, Security

* 한남대학교 멀티미디어학과 박사과정

** 한남대학교 멀티미디어학부 강의전담교수 (교신저자)

*** 충북대학교 전자계산학과 네트워크 보안연구실

**** 한남대학교 멀티미디어학부 교수

접수일자 : 2009. 08. 25

심사완료일자 : 2009. 09. 21

Ⅰ. 서 론

RFID 시스템은 유비쿼터스 컴퓨팅 환경을 위한 기술 중에서 가장 주목받는 기술이며, 다양한 산업 분야에서 응용되어 이용되고 있다. 또한 RFID 기술은 물리적 또는 시각적 접촉과 무관하게 주변 환경의 사물을 인식하는 획기적인 기술이다[1].

최근까지 제품의 인식 방법으로 바코드가 이용되어 져 왔으나, 현재는 RFID가 제품 인식을 위한 기술로 인식되고 있으며 그 사용 범위가 다양한 분야로 확대되고 있다[2]. 그리고 RFID 시스템은 바코드 시스템보다 효율적인 식별 체계 구축이 가능하므로 바코드 시스템을 대신하여 유통, 물류 산업, 실시간 재고관리, 자동 품질관리 등의 다양한 분야에서 이용이 예측된다[3,4,5].

RFID는 데이터 전송을 위해 무선 주파수 통신을 사용하므로 정보 노출, 위치 추적, 위조 및 서비스 장애와 같은 보안 및 사용자 프라이버시 침해를 유발할 수 있는 단점이 존재한다[6]. 이러한 문제를 해결하기 위해 현재까지 많은 연구가 진행되었지만 여전히 위치 추적 공격, 재전송 공격, 스푸핑 공격 등의 취약점이 존재하며, 최근의 RFID 환경은 수동형 태그의 효율적인 에너지 사용을 위해 태그 연산 작업의 최소화가 가능한 인증 프로토콜을 요구하고 있다.

그러므로 본 논문에서는 기존 방법들의 문제점을 분석하여 개선된 효율적인 인증 방법의 제안으로 RFID 인증의 취약점을 보완한다.

본 논문의 구성은 다음과 같다. 2장에서는 RFID 시스템의 구성 요소와 RFID 인증에서 요구되는 보안 요소들을 기술한 후 기존의 프라이버시 침해 방지 프로토콜 기법들을 분석한다. 3장에서는 개선된 인증 프로토콜을 제안하고, 4장에서는 제안한 기법의 보안성 및 효율성을 비교 분석한다. 마지막으로 5장에서 결론과 향후 연구 방향을 제시한다.

Ⅱ. 본 론

본 장에서는 RFID 시스템의 구성요소에 대해 기술하고, RFID 시스템에서 상호 인증을 위한 다양한 프로토콜 기법들을 비교 검토한다.

2.1 RFID 시스템 구성요소

RFID는 사물의 자동 인식을 위해 무선 주파수를 이용하는 기술로 사물에 부착하는 RFID 태그(Tag) 부분과 태그의 정보를 취득하는 리더(Reader), 그리고 데이터의 저장과 관리를 담당하는 백엔드 데이터베이스(Backend Database)로 구성된다.

RFID 태그는 마이크로칩과 안테나 코일로 구성되고 마이크로칩은 기본적인 연산 및 데이터를 저장하는 역할을 담당하며, 안테나 코일은 리더와 통신을 담당한다. 또한 태그의 전력 공급 방식에 따라 능동형 태그(Active tag)와 수동형 태그(Passive tag) 그리고 능동형과 수동형의 중간 형태인 반능동형 태그(Semi-Active tag)로 구분된다.

능동형 태그는 배터리가 내장되어 있으며 인식거리가 길고 가격이 비싸다. 수동형 태그는 내장 배터리가 없으며 인식거리가 짧아 근거리 데이터 통신에 사용된다. 반능동형 태그는 기존의 수동형 태그에 자체 전원 공급을 위한 얇은 전지를 부가하여 수동형 태그의 최대 문제점인 인식률을 개선하고 부착물체의 영향을 보완한 형태이다[7].

RFID 리더는 RF모듈, 제어장치(Control unit), 안테나로 구성되며, 무선 주파수를 이용해 태그와 통신을 수행한다. RFID 리더는 태그로부터 인증을 위한 데이터를 수신하고, 수신한 데이터를 백엔드 데이터베이스에 전송하거나 백엔드 데이터베이스로부터의 전송 결과를 다시 태그에게 전달하는 역할을 통해 사물에 대한 정보를 수집한다. 이러한 과정은 안전하지 않은 무선 주파수를 기반으로 수행하기 때문에 악의적인 공격자로부터의 침입 위험이 항시 존재한다.

백엔드 데이터베이스는 태그와 관련된 데이터를 저장하고 관리하는 장치로 계산능력이 제한된 태그나 리더를 대신해 복잡한 계산을 수행하는 역할로, 이미 저장되어 있는 인증 정보를 통해 리더로부터 전송된 태그 데이터를 인증한다. 일반적으로 리더와 백엔드 데이터베이스 사이의 채널은 안전하다고 가정한다.

2.2 인증 보안요소

태그와 리더 사이의 통신은 무선 통신으로 공격자의 침입이 가능한 불안전한 채널이므로, 태그와 리더 사이의 인증을 위협하는 여러 위험 요소들이 존재한다. RFID 시스템 환경에서의 위협 요소들로는 도청,

재전송 공격, 스푸핑 공격 그리고 위치 추적 공격 등이 있다.

첫 번째, 도청은 악의적인 의도를 가진 공격자가 RFID 태그와 리더 사이의 통신이 무선 채널임을 이용해 둘 사이의 통신 내용을 도청하는 것이다[2]. 따라서 RFID 통신에서는 정보가 공격자에게 도청되었더라도 중요한 정보가 유출되지 않도록 인증 프로토콜을 설계해야 한다.

두 번째, 재전송 공격은 공격자가 태그와 리더 사이에서 도청한 통신 메시지들을 저장해 두었다가 정당한 메시지로 위장하여 재전송함으로써 합법적인 메시지로 인증되는 공격 방법이다[8].

세 번째, 스푸핑 공격은 공격자가 정당한 통신자로 위장하여 정당하지 않은 정보를 정당한 것으로 속여 태그와 리더간의 잘못된 인증이 이루어질 수 있도록 위협하는 공격을 말한다[9].

마지막으로 위치 추적 공격은 공격자가 태그의 위치 변화를 감지하여 태그 소유자의 이동 경로를 파악하는 태그 소유자 프라이버시 침해 공격이다[10]. 일반적으로 RFID 시스템 상에서의 위치 추적은 특정 태그가 전송하는 메시지를 모두 수집한 후 그 메시지들이 갖고 있는 연관성을 파악하여 메시지들에 대한 링크를 통해 공격이 이루어지므로 이를 방지하기 위해서는 각 태그들이 전송하는 메시지의 구별을 불가능 상태로 만들어 추적하지 못하도록 해야 한다.

2.3 기존 해쉬 기법의 인증 종류와 특성

현재까지 RFID 시스템 사용자의 프라이버시 보호와 태그와 리더간의 상호 인증을 위한 다양한 프로토콜 기법들이 제안되었다. 특히 RFID 태그의 제한된 연산능력으로 인해 해쉬 함수와 같은 가벼운 연산법을 사용하는 프로토콜들이 연구되고 있다.

Stephen등이 제안한 해쉬-락 기법(Hash-Lock)은 저비용 태그 자원의 제한 문제 해결을 위해 태그에 해쉬 함수만 구현한 간단한 프로토콜이다[2]. 해쉬-락 기법은 해쉬 함수 처리한 값인 metaID를 저장하여 인증과정에 사용하는 방식으로, 그림 1은 해쉬-락 기법의 동작 절차를 나타낸다.

그림 1에서와 같이 리더가 태그에게 질의를 전송하면 태그는 자신의 키(key)를 이용하여 해쉬 함수 연산을 수행하고 생성한 metaID=h(key)를 리더에게 전송한다. 리더는 데이터베이스로부터 해당 키를 추출한 후, 추출된 키를 태그에게 전송한다. 태그는 전송받은 키를 이용하여 metaID를 생성하고, 자신의 metaID값과의 일치여부를 확인한다.

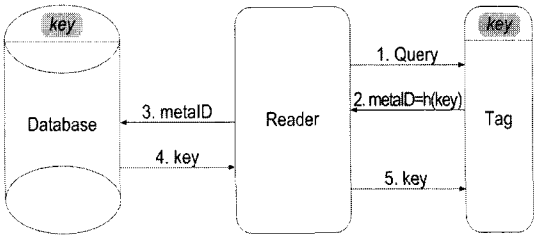

그림 1. Hash-Lock 기법의 인증 과정
Fig 1. Authentication process of Hash-Lock scheme

해쉬-락 기법은 태그에서 랜덤하게 선택된 키의 해쉬 값인 metaID를 전송함으로써 key값의 노출을 방지한다는 장점이 있지만, 고정된 metaID의 사용으로 매회 같은 값이 전송되므로, 태그의 추적이 가능하다. 또한 암호화 과정 없이 데이터를 넘겨주어 도청의 위험이 존재한다.

난수적 해쉬-락 기법은 태그의 위치 추적 방지를 위하여 난수 생성기를 이용하는 기법이다.

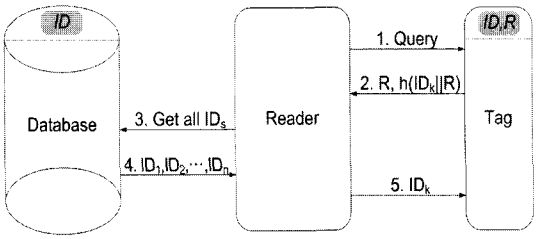

그림 2. 난수적 Hash-Lock 기법의 인증 과정
Fig 2. Authentication process of randomized Hash-Lock scheme

그림 2에서와 같이 난수적 해쉬-락 기법은 질의를 받은 태그가 생성한 난수 R과 ID를 이용하여 해쉬 함수 연산을 수행한 후 그 결과 값과 난수 R을 리더에게 전송한다. 리더는 DB로부터 모든 ID를 전송받고, 전송된 ID와 난수 R을 해쉬 함수 처리하여 태그에서 전송된 ID와 일치하는 ID를 다시 태그에게 전송하여 일치여부를 확인하는 기법이다.

난수적 해쉬-락 기법은 태그가 난수 생성기를 가지고 있다고 가정하고 난수 R을 생성해 태그의 응답을 랜덤화 한다. 따라서 난수를 이용해 매번 다른 결과 값을 전달하므로 위치 추적 문제가 해결되는 반면, 악의적인 리더가 태그로부터 R값과 h(IDk ‖ R)값을 획득하여 재전송 공격이 가능하며 스푸핑 공격에도 취약하다는 문제점이 있다. 특히, 마지막 단계에서 태그가 리더에게 ID를 전송함으로써 ID의 유출이 손쉽게 이루어질 수 있다는 단점을 가진다.

일회성 난수를 이용한 인증 프로토콜 기법은 일회성 난수를 이용하여 상호 인증을 하는 기법[11]으로 기존의 연구들이 리더에서 태그에게만 전송하던 질의를 DB에게도 동시에 전송하며, DB도 난수를 생성한다는 차이점을 갖는다. 일회성 난수를 이용한 인증 프로토콜 기법의 인증 과정은 그림 3과 같다.

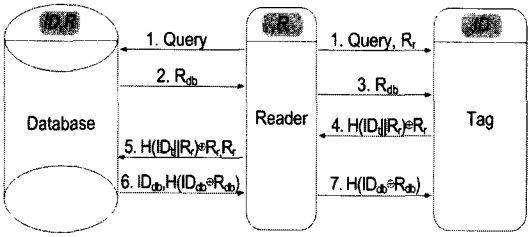

그림 3. 일회성 난수를 이용한 기법의 인증 과정
Fig 3. Authentication process of scheme using one time random number

그림 3에서 보는 것과 같이 리더는 난수 Rr을 생성하여 태그에게 전송하고, DB로부터 전송된 난수 Rdb를 수신한 리더는 난수 Rdb를 다시 태그에게 전송한다. 태그가 리더로부터 수신한 Rr과 자신의 IDt를 해쉬 함수 처리하여 리더에게 전송하면, 리더는 자신의 난수 Rr과 태그로부터 수신한 계산 값을 DB에게 전송한다. DB는 난수 Rr과 자신의 IDdb에 의해 계산된 값과 리더에게 전송받은 값을 비교하여 일치여부를 판단한 후, 자신이 생성한 난수 Rdb와 IDdb의 계산 값을 리더에게 전송한다. 리더가 DB로부터 전송받은 값을 다시 태그에게 전송하면, 태그는 자신의 IDt로 같은 계산을 실행하여 전송받은 값과의 일치여부를 판단한다.

일회성 난수를 이용한 인증 프로토콜 기법은 리더와 DB에서의 난수 값 생성으로 매번 다른 데이터를 송수신하여 재전송 공격을 방지하고, 위치 추적 공격에도 안전하다는 장점이 있다. 그러나 연산능력이 제한되는 태그에게 해쉬 연산과 XOR 연산을 2회씩 실행시킴으로써 태그가 다소 많은 임무를 갖게 된다는 단점이 있다. 또한 통신 라운드 수의 추가로 인한 처리 시간 증가에 따른 태그의 에너지 소모 증가로 저가형 태그로의 적용에 유용하지 못하다.

Ⅲ. 제안 시스템

본 논문에서는 비공개 코드(Private Code)를 사용하여 기존 기법들의 단점을 보완하고 태그의 연산을 최소화하면서 보안을 강화시키는 효율적인 인증 프로토콜을 제안한다.

3.1 제안 프로토콜을 위한 시스템 계수

본 논문에서 제안한 인증 프로토콜을 설계하기 위한 가정은 다음과 같다.

[가정1] 태그는 해쉬 함수와 XOR 연산을 수행한다.
[가정2] 태그와 리더, DB는 사전에 안전한 비밀 코드 값으로 사용하는 비공개 코드(PrC)를 공유한다.
[가정3] 리더와 DB는 난수 생성기를 통해 난수를 생성한다.

본 논문에서 제안한 프로토콜의 처리 절차를 나타내기 위해서 사용되는 용어 및 표기 방법은 다음의 표 1에서 정의한다.

표 1. 용어 정의
Table 1. Definitions of terms

용어	정의
h( )	해쉬 함수
⊕	XOR연산
PrC	사전에 저장된 안전한 비공개 코드 값
Rr	리더가 생성한 난수
Rd	DB가 생성한 난수
CP	h(PrC ‖ Rr) 연산 결과 값
CPL	CP를 전체 길이의 세 부분으로 나눈 왼쪽 n비트 값
CPM	CP의 가운데 n비트 값
CPR	CP의 오른쪽 n비트 값

3.2 제안 프로토콜의 실행 과정

본 논문에서 제안한 프로토콜의 인증 과정은 그림 4와 같다. 리더가 난수 R_r을 생성한 후 태그에게 R_r과 질의를 전송하고, 동시에 DB에게도 R_r을 전송하면, 태그는 R_r과 사전에 저장되어 있던 PrC값을 연접 해쉬 함수 처리한 값의 왼쪽 n비트 값 CP_L을 리더에게 전송한다. CP_L을 전송받은 리더는 사전에 저장하고 있던 PrC값과 R_r을 연접 해쉬 함수 처리하여 태그로부터 전송된 정보와의 일치여부를 검증한 후 정당한 정보로 판정되면, CP'의 가운데 n비트 값 CP_M을 DB에게 전송한다. 리더로부터 값을 전송받은 DB는 전송된 정보의 정당성을 전 단계와 같은 방법으로 검증한 후 일치하는 값으로 판정되면, 자신의 난수 R_d를 생성하고 R_d값과 검증 값의 오른쪽 n비트 값인 CP_R을 XOR하여 리더에게 전송한다. 리더는 DB로부터 전송받은 값을 태그에게 전송하고, 태그는 그 값을 검증 연산 처리하여 전송된 정보의 일치여부를 판정한다.

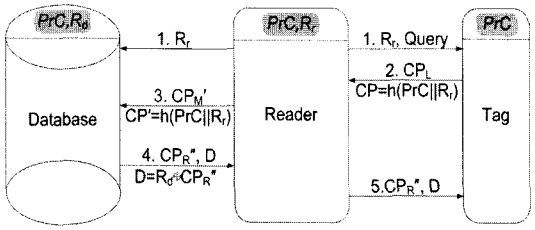

그림 4. 제안 기법의 인증 과정
Fig 4. Authentication process of suggested scheme

세부 실행단계는 아래와 같이 총 5단계로 이루어지며, 세부 동작 과정은 그림 5와 같다.

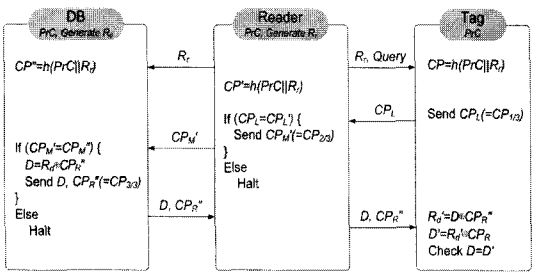

그림 5. 제안 기법의 세부 동작 과정
Fig 5. Detail authentication process of suggested scheme

[단계1] 리더는 태그의 존재가 인식되면 난수 R_r을 생성한 후 질의와 생성한 난수 R_r을 태그에게 전송하고, 동시에 난수 R_r을 DB에게도 전송한다. 이와 같은 과정을 표식화 하면 아래와 같다.

Reader → Tag : Query, Rr

Reader → DB : Rr

[단계2] 태그는 리더에게 전송받은 난수 R_r과 이미 저장되어 있던 비공개 코드 값 PrC를 해쉬 함수 처리 ($CP=h(PrC \| R_r)$)하여 CP값을 생성한 후 CP값의 왼쪽 n비트 값 CP_L을 리더에게 전송한다. 단계2는 아래와 같이 표식화 된다.

Tag : h(PrC ‖ Rr)

Tag → Reader : CPL

[단계3] 리더는 자신의 비공개 코드 값 PrC와 난수 R_r을 연접 해쉬 함수 처리한 결과 값 CP'의 CP_L'와 태그로부터 송신된 CP_L을 비교하여 값의 일치 여부로 태그 정보의 정당성을 확인한다. 값이 일치하면 CP' 결과 값의 가운데 n비트 값 CP_M'를 DB에게 전송한다. 단계3 과정의 표식화는 아래와 같다.

Reader : CPL = CPL'

Reader → DB : CPM'

[단계4] DB는 자신의 비공개 코드 값 PrC와 리더로부터 전송받은 난수 R_r을 단계3과 같은 방법으로 처리한 CP''의 CP_M''를 통해 리더로부터 송신된 태그 정보의 정당성을 확인한다. 확인 결과, 자신의 연산 값과 전송받은 값이 일치하면 CP''의 오른쪽 n비트 값인 CP_R''와 자신이 생성한 난수 R_d를 이용하여 $D=R_d \oplus CP_R''$의 연산을 수행한 후 연산 결과 값 D와 CP_R''를 리더에게 전송한다. 단계4 과정의 표식화는 아래와 같다.

DB : $CP_M' = CP_M''$, $R_d \oplus CP_R''$

DB → Reader : D, CP_R''

[단계5] 리더는 DB로부터 전송받은 D와 CP_R''를 태그에게 전송한다. 태그는 리더로부터 전송된 D와 CP_R''로부터 DB의 난수 값인 R_d'를 획득하고, 자신의 CP_R로 $R_d' \oplus CP_R$ 연산을 수행하여 D'를 생성한 후, D=D' 검증을 통해 인증을 수행한다. 단계5 과정의 표식화는 아래와 같다.

Reader → Tag : D, CP_R''

Tag : $R_d' = D \oplus CP_R''$, $R_d \oplus CP_R'' = R_d' \oplus CP_R$

Ⅳ. 보안 및 효율성 분석

본 장에서는 기존 기법과 제안 기법의 보안성 및 효율성을 비교 분석한다.

4.1 보안성 분석

본 절에서는 도청 및 재전송 공격, 스푸핑 공격, 위치 추적 공격 등의 RFID 시스템 인증 보안 요소를 기반으로 제안 기법의 보안성을 분석하였다.

첫째, 제안 기법은 리더와 DB에서 매 회 난수를 발생시키고, Private Code와 난수를 해쉬 함수 처리한 값만 전송하므로 코드 값 도청 공격으로부터 안전하며, 리더가 생성한 난수는 DB에서 다시 한 번 검증 절차를 거쳐 재전송된 난수 값을 검출하므로 재전송 공격으로부터도 안전하다. 또한 단계별로 전송 값을 달리하여 검증하고, 전송 시 연산 처리된 값만 전송되므로 일회성 난수를 이용한 기법보다 재전송 공격으로부터 더욱 안전하다.

둘째, CP값은 난수를 포함한 $h(PrC \| R_r)$로 얻어지는 안전한 일방향 해쉬 함수로 처리되며, 비록 공격자가 전송 값인 CP_L, CP_R 값을 취득했어도 그 값은 완전한 정보가 아니다. 그러므로 정당한 통신자로 위장한 악의적인 태그가 사용한 값은 다음 인증 과정에서 사용할 수 없게 되어 스푸핑 공격으로부터 차단된다.

셋째, 제안 기법은 해쉬-락 기법과는 달리 리더와 DB에서 난수를 발생시키므로 매 세션 다른 전송 값을 사용하게 된다. 따라서 현재 세션의 전송 값과 도청한 값이 동일하지 않아 태그가 어느 위치에 있는지 추적할 수 없으므로 위치 추적 공격으로부터 안전하다.

위와 같이 기존 기법과 제안 기법을 비교 분석한 결과, 해쉬-락 기법은 도청, 재전송 공격, 스푸핑 공격, 위치 추적 공격으로부터 모두 취약하며, 난수적 해쉬-락 기법은 위치 추적 공격에는 안전하나 다른 공격에는 취약하다. 일회성 난수를 이용한 기법은 위 두 기법에 비해 크게 개선되었지만, 연산 처리되지 않은 값을 전송하므로 재전송 공격에 노출될 위험이 있다.

그러나 본 논문에서 제안한 기법은 표 2에서와 같이 네 가지 공격으로부터 모두 안전함을 볼 수 있다.

표 2. 보안성 분석
Table 2. Security analysis

프로토콜 \ 비교요소	도청	재전송 공격	스푸핑 공격	위치추적 공격
Hash-Lock 기법	취약	취약	취약	취약
난수적 Hash-Lock 기법	취약	취약	취약	안전
일회성 난수를 이용한 기법	안전	보통	안전	안전
제안 기법	안전	안전	안전	안전

4.2 효율성 분석

본 절에서는 기존 기법과 제안 기법의 효율성을 비교 분석하였으며, 그 결과는 표 3과 같다.

표 3. 효율성 분석
Table 3. Efficiency analysis

프로토콜 \ 비교요소		난수 생성	해쉬 연산	XOR 연산	데이터 검증	통신 라운드수
Hash-Lock 기법	DB	-	-	-	-	5
	리더	-	-	-	-	
	태그	-	2	-	-	
난수적 Hash-Lock 기법	DB	-	-	-	-	5
	리더	-	1	-	-	
	태그	1	1	-	-	
일회성 난수를 이용한 기법	DB	1	1	1	1	7
	리더	1	-	-	-	
	태그	-	2	2	-	
제안 기법	DB	1	1	1	1	5
	리더	1	1	-	1	
	태그	-	1	2	1	

첫째, 태그 존재 인식 시 리더가 DB와 태그에게 난수를 동시에 전송하므로, 태그와 DB가 동일하게 연산을 시작한다. 따라서 DB의 연산 및 검증 과정의 작업시간 단축 효과가 있다.

둘째, 기존 기법에서의 태그 난수 생성 과정을 제거하고, 태그의 해쉬 연산 처리 과정을 감소시켜 수동형 태그

에서의 보다 효율적인 에너지 활용이 가능하다.

셋째, 사전에 태그, 리더, DB에 Private Code를 입력시켜, 검증 절차의 간소화와 검증 값의 정확도를 향상시켰다.

넷째, 전송 값 검증 과정에서 단계별로 검증 값을 달리하여 데이터 유출 방지 효과가 뛰어나다.

마지막으로, 통신 라운드 수를 감소하여 공격자로부터의 침입을 최소화하였으며, 그에 따른 에너지 소모의 감소로 통신의 효율성을 보장한다.

V. 결 론

최근 RFID 시스템이 다양한 분야에서 이용 및 활성화되면서 RFID 시스템의 취약점인 프라이버시 침해 문제가 핵심 이슈로 등장하고 있다. RFID 시스템은 무선 주파수 통신을 사용하므로 악의적인 공격자에 의한 리더와 태그간의 정보 유출 문제가 발생한다. 또한 일반 인증 시스템은 연산능력이 제한되는 저가형·수동형 태그로의 적용이 어려워 태그 연산 작업의 최소화가 가능한 인증 프로토콜이 요구된다. 이러한 문제점을 해결하고자 본 논문에서는 기존의 기법들을 보완한 효율적인 RFID 인증 프로토콜을 제안하였다.

제안한 기법은 매 세션마다 난수를 새로 발생시키고, 전송 데이터의 검증과정을 강화하여 도청이나 스푸핑 공격, 위치 추적 공격으로부터 안전하다. 또한 사전에 태그, 리더, DB에 Private Code를 입력시켜 검증 절차를 강화하고 인증 과정을 간소화 하였으며, 이전 기법에 비해 태그의 연산 작업을 최소화 하였다. 결과적으로 전체 통신 라운드 수의 감소로 태그의 통신 효율성이 증대되어 저가형·수동형 태그로의 적용이 기대된다.

향후, 제안한 인증 시스템이 휴대폰, PDA등과 접목된 모바일 RFID 시스템에도 적용될 수 있도록 모듈 형태로의 구현에 대한 연구가 필요하다.

참고문헌

[1] G. Avoine and P. Oechslin, "RFID Traceability: A Multilayer Problem", *In Proceeding of the Financial Cryptography* '05 - FC'05, LNCS 3570, pp.125-140, 2005.

[2] Stephen A. Weis, Sanjay 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, 2004.

[3] Klaus Finkenzeller, *RFID Handbook,* Second Edition, John Wiley& Sons, 2003.

[4] S. Sarma, S. Weis and D. Engels, "Radio-Frequency identification: security Risks and Challenges", *RSA Laboratories Cryptobytes,* Vol.6, No.1, pp.2-9, 2003.

[5] S. E. Sarma, S. A. Weis and D. W. Engels, "RFID systems, security & privacy implications", *Cryptographic Hardware and Embedded Systems-CHES 2002,* LNCS 2523, pp.454-469, 2003.

[6] A. Juels, "RFID Security and Privacy: A Research Survey", *IEEE Journal on Selected Areas in Communications,* Vol. 24, Issue:2, pp.381-394, 2006.

[7] 정재영, 여준호, 이형섭, 표철식, "센서 태그 기술 동향", 전자통신동향분석 제22권 제3호, pp.38-45, 2007.

[8] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID Attacks", *Proc. Int'l Workshop on RFID Technology,* pp.73-86, 2008.

[9] Erol Ozan and Gaétan Hains, "Development of a Framework for the Enterprise RFID Defense System Architecture", *Technical Report TR- LACL-2009-1,* Laboratory of Algorithmics, Complexity and Logic(LACL) University Paris 12(Paris Est), pp.1-14, 2009.

[10] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador and Arturo Ribagora, "RFID Systems: A Survey on Security Threats and Proposed Solutions", *PWC 2006,* LNCS 4217, pp.159-170, 2006.

[11] 김대중, 전문석, "일회성 난수를 이용한 안전한 RFID 상호인증 프로토콜 설계", 정보과학회논문지:정보통신 제35권 제3호, pp.246- 247, 2008.

저자소개

장봉임(Bong-Im Jang)

2003 한남대학교 멀티미디어학과 공학석사
2008~현재 한남대학교 멀티미디어학과 박사과정

※관심분야 : RFID/USN, 센서 웹, 멀티미디어, 웹서비스

김용태(Yong-Tae Kim)

1984 한남대학교 계산통계학과 학사
1988 숭실대학교 전산학과 공학석사

2008 충북대학교 전산학과 이학박사
2002~2006 (주)가림정보기술 이사
2006~현재 한남대학교 멀티미디어학부 강의전담교수
※관심분야 : 모바일 웹서비스, 정보보안, 센서 웹, 모바일 통신보안, 멀티미디어

정윤수(Yoon-Su Jeong)

2000 충북대학교 전산학과 석사
2008 충북대학교 전자계산학 이학박사

※관심분야 : 센서 보안, 암호 이론, Network Security, 이동통신 보안

박길철(Gil-Cheol Park)

1983 한남대학교 계산통계학과 학사
1986 숭실대학교 전산학과 공학석사

1998 성균관대학교 정보공학과 박사
2006 UTAS, Australia 교환교수
1998~현재 한남대학교 멀티미디어학부 교수
※관심분야 : multimedia and mobile communication, network security