韓國 컴퓨터情報學會 論文誌
第12卷 第6號, 2007. 12.

2007-12-6-2-3

RFID 시스템의 개선된 인증 프로토콜

이 상 렬*

Enhanced Authentication Protocol of RFID System

Sang-Ryul Lee*

요 약

기존의 바코드(Bar code) 시스템에 비하여 RFID(Radio Frequency Identification) 시스템은 저장능력이 뛰어나고 사물에 비접촉성을 갖는 장점이 있다. 그러나 RF(Radio Frequency) 신호를 이용하여 통신을 하기 때문에 전송되는 정보를 누구나 손쉽게 수신할 수 있어 시스템 보안과 개인의 프라이버시를 침해하는 문제점을 갖고 있다. 본 논문에서는 도청, 재전송, 스푸핑(Spoofing) 그리고 위치추적과 같은 공격에 안전하며 리더(Reader)와 태그(Tag) 간에 상호 인증을 효율적으로 할 수 있는 RFID 시스템을 제안한다. 제안한 시스템은 앞으로 유비쿼터스(Ubiquitous) 환경에서 다양한 분야에 활용될 수 있을 것이다.

Abstract

There is an advantage that RFID system is better than previous bar code system in storage ability and noncontact property. But, everyone can easily receive the transmitting information by using RF signal. So, there is a problem that system security and personal privacy are threatened. In this paper, I propose RFID system that is secure against attacks like eavesdropping, replay, spoofing and location tracking and can efficiently provide mutual authentication services between reader and tag. The proposed RFID system can be used in various sections of ubiquitous computing environment.

▸ Keyword : RFID System, Authentication Protocol, Privacy

• 제1저자 : 이상렬
• 접수일 : 2007.10.4, 심사일 : 2007.10.28, 심사완료일 : 2007.11.28.
* 상지영서대학 인터넷정보과 교수

Ⅰ. 서 론

미래는 점차 유비쿼터스 컴퓨팅 환경으로 변화해갈 것이다. 유비쿼터스 컴퓨팅 환경에서는 모든 사람과 사물이 네트워크로 연결되어 원하는 일을 언제 어디서나 할 수 있게 된다. RFID는 이러한 유비쿼터스 컴퓨팅 환경에 있어 가장 핵심적인 기술로서 앞으로 물류는 물론 금융, 의료, 통신, 교육, 건설, 국방, 소방, 문화 등 인간 생활 전반에 걸쳐 폭넓게 사용될 것이다.

RFID 시스템의 태그는 정보를 읽거나 기록할 때 RF 신호를 이용하고 메모리를 내장하고 있음으로 바코드보다 인식 가능한 거리도 길고 많은 정보를 저장할 수 있다. 하지만 RF 신호는 누구나 손쉽게 수신할 수 있기 때문에 정보의 노출을 피할 수 없다. 따라서 태그 사용자는 자신도 모르게 리더를 가진 공격자들에게 태그의 정보를 노출하게 된다. 특히 태그의 고유 식별 번호가 노출될 경우 자신의 현재 위치가 추적되어 개인의 프라이버시가 침해될 수 있다[1,2,3]. 따라서 RFID 시스템이 상용화되기 위해서는 이러한 문제점들을 반드시 조속히 해결해야 한다.

그동안 이런 문제점을 해결하기 위하여 여러 가지 연구 결과가 발표되었다. 그 대표적인 것으로 물리적 접근방법과 암호학적 접근방법이 있다. 물리적 접근방법에는 킬(Kill) 명령을 이용하는 방식[4,5]과 암호학적 접근방법에는 해쉬 함수를 기반으로 하는 해쉬 락[6], 랜덤 해쉬 락[7], 해쉬 체인 방식[8]과 재 암호화 방식, XOR 기반 등의 방식이 있다. 그러나 이러한 방식들은 제각기 약간의 문제점들을 갖고 있다. 문제점들의 유형으로는 암호키가 쉽게 노출되어 도청이 가능하고 인증 세션(Session) 때마다 동일한 정보가 전송되기 때문에 한번 전송된 메시지를 공격자가 재전송할 위험이 있고 그로 인하여 위장 태그 또는 위장 리더가 발생될 수 있어 스푸핑 및 사용자의 위치가 추적되는 위험이 있다.

따라서 본 논문에서는 전송 정보의 보안과 개인의 프라이버시를 보호하기 위하여 도청, 재전송, 스푸핑 그리고 위치추적과 같은 공격에 안전하며 리더와 태그 간에 상호 인증을 효율적으로 할 수 있는 RFID 시스템을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 일반적인 RFID 시스템의 구성과 기존의 RFID 인증 프로토콜들의 특징 및 문제점에 대해 살펴본다. 3장에서는 기존의 RFID 시스템의 문제점을 해결할 수 있는 새로운 시스템을 제안하고 4장에서는 제안한 시스템의 안전성과 효율성에 대해 분석한다. 끝으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 RFID 시스템 구성

일반적인 RFID 시스템은 태그, 리더 그리고 백-앤드 데이터베이스(Back-end database)로 구성된다[9,10]. 〔그림 1〕에서 전방위 영역(Forward range)은 리더가 태그에게 질의를 보낼 수 있는 물리적 범위를 의미한다. 반대로 후방위 영역(Backward range)은 태그가 리더에게 질의에 대한 응답을 보낼 수 있는 물리적 범위를 의미한다. 태그에 배터리를 내장하지 않은 RFID 시스템의 경우 리더는 태그에게 에너지를 전달해야하는 필요성에 의하여 필드의 범위가 넓어질 수밖에 없고 태그는 리더에게 전달받은 에너지를 이용하여 리더에게 응답하기 때문에 그 범위가 좁을 수밖에 없다. 따라서 전방위 영역은 후방위 영역보다 범위가 넓다. 전방위 영역에 포함된 Tag1과 Tag2는 리더가 전송하는 신호를 모두 수신할 수 있지만 후방위 영역 안에 있는 Tag1만이 그에 대한 응답 신호를 전송할 수 있다. 일반적인 RFID 시스템에서는 RF 신호를 이용하는 리더와 태그 사이의 통신은 도청 가능한 불안전한 채널(Insecure channel) 그리고 유선을 이용하는 리더와 백-앤드 데이터베이스 사이의 통신은 안전한 채널(Secure channel)이라 가정한다.

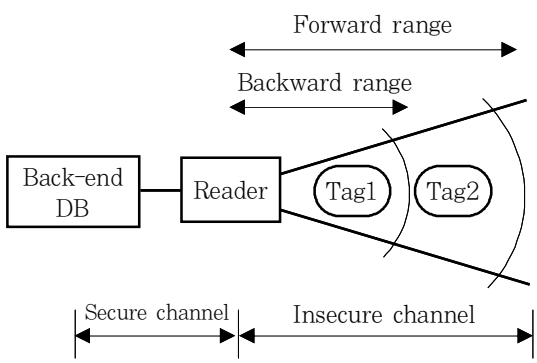

그림 1. RFID 시스템 구성도
Fig. 1. Structure of RFID system

(1) 태그

태그는 리더의 요청에 대하여 태그의 식별 정보를 송신하는 것으로 트랜스폰드(Transponder)라고도 하며 마이크로 칩과 안테나로 구성된다.

전원 공급 방법에 따라 능동형 태그(Active Tag)와 수동

형 태그(Passive Tag)로 크게 분류한다. 능동형 태그는 전원을 내장한 것이 특징으로 배터리를 내장하고 있어 수동형 태그보다 긴 거리의 데이터 전송거리를 갖는 것이 특징이지만 비싼 것이 단점이다. 수동형 태그는 리더로부터 유도전류에 의해 전원을 공급받아 사용하는 것으로 현재 가장 경쟁적으로 개발하고 있는 태그이다.

태그에서 사용하는 메모리는 RAM, OTP(One Time Programmable user memory), EEPROM, FRAM 등이 있다. 그 중에서 FRAM은 전력 소모 면에서도 EEPROM과 몇 배나 차이가 나기 때문에 사실상 RFID 시스템에서는 FRAM을 사용할 것으로 결정되었으나 다른 회로와의 결합 문제로 현재 사용하지 못하고 있는 실정이다.

(2) 리더

리더는 태그의 식별 정보를 수신하여 태그를 인식하는 장치로서 트랜시버(Transceiver)라고도 하며 정보를 응용프로그램에게 전송하는 역할과 응용프로그램으로부터 명령을 받아 태그에 정보를 기록하기 위하여 명령어를 주파수 형태로 변환하여 전송하는 역할을 한다.

RFID 시스템에서 사용하는 주파수의 경우 크게 세 가지 정도로 나눌 수 있다. 각각의 용도에 따라 100~500KHz, 10~15MHz, 850~950Mhz/2.4~5.8GHz로 나눌 수 있는데 그 중에서 일찍부터 관심을 끌었던 주파수는 125KHz, 13.56MHz, 2.45GHz이다. 주파수의 특성에 따라 태그의 데이터를 읽어 들이는 속도나 거리 그리고 가격의 차이가 발생하며 주파수가 높을수록 이 세 가지 특성이 모두 높아진다.

(3) 백-앤드 데이터베이스

백-앤드 데이터베이스는 리더가 수집한 태그에 관한 정보(예를 들어, 상품관련 정보, 로그기록 정보, 리더의 위치정보 등)를 저장하고 관리하며 리더 또는 태그 대신 복잡한 연산을 수행하는 안전한 서버이며 리더에게 수집된 정보의 진위 여부를 판별해 주는 역할을 수행한다.

2.2 기존의 RFID 인증 프로토콜

RFID 시스템에서 사용자의 프라이버시 보호를 위하여 그동안 제안된 기법들은 킬 태그(Kill Tag), Faraday Cage, Active Jamming 등 물리적 접근방법과 해쉬 함수 기반, 재암호화, XOR 기반 등 암호학적 접근방법으로 크게 두 가지로 분류된다. 이 절에서는 이러한 여러 가지 기법들 중에서 물리적 접근방법인 킬 태그 방식과 암호학적 접근방법인 해쉬 함수 기반 방식의 특징과 문제점을 살펴보고자 한다.

2.2.1 킬 태그 방식

킬 태그 방식은 MIT의 Auto-ID 센터(현재 EPCglobal)에서 제안한 방법으로 태그 설계 시 8비트의 암호를 포함하고 있으며 태그는 이 패스워드와 'Kill'명령을 받으면 자신의 모든 기능을 중지시킨다. 태그는 내부에 단락회로가 있기 때문에 이를 단절시킴으로서 'Kill'명령을 실행하게 되는데 한 번 죽은 태그는 다시 살릴 수 없다. 이런 경우 태그를 재사용할 필요가 있는 분야에서는 사용이 불가능하다. 물론 읽기 및 쓰기가 가능하도록 설계된 태그의 경우 플래그(Flag) 비트를 이용하여 태그를 죽였다 다시 살릴 수도 있을 것이다. 수많은 제품에 사용될 태그라는 것을 감안하고 보안을 생각한다면 8비트의 암호는 문제가 있으며 128비트 이상을 암호로 사용해야 하지만 이는 태그에 상당한 부담을 주게 된다. 그렇다고 태그마다 다른 암호를 사용한다면 이를 저장하는 것도 문제가 될 것이다.

이러한 킬 태그 방식은 RFID 태그를 단순히 무력화 시킬 수 있을 뿐이지 개개인의 프라이버시를 보호하기 위한 해결책이 될 수 없다.

2.2.2 해쉬 함수 기반 방식

(1) 해쉬 락(Hash lock) 방식

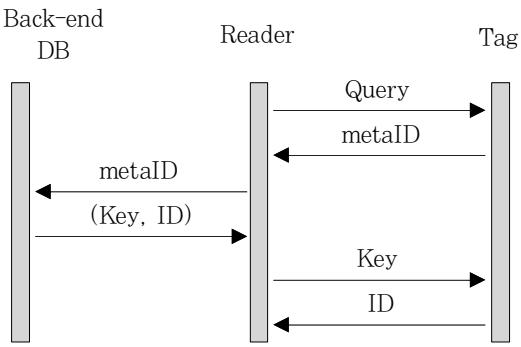

그림 2. 해쉬 락 인증 프로토콜
Fig 2. Authentication protocol of hash lock

〔그림 2〕와 같은 해쉬 락 방식의 인증 프로토콜에서는 초기에 태그는 metaID=h(Key)와 자신의 ID를 보관하고 있으며 DB는 모든 태그의 metaID에 대한 ID와 Key를 보관하고 있다. 리더가 태그에게 Query를 보내면 태그는 리더에게 metaID를 전송한다. 리더는 DB에게 metaID를 전송하여 태그의 ID와 Key를 알아낸 후 태그에게 Key를 전송한다. 상호 인증 방법에 있어 태그는 h(Key)를 계산하여 metaID와 일치하면 리더를 인증하게 되고 자신의 ID를 리더에게 전송

한다. 리더는 태그로부터 수신한 ID가 DB에서 받은 ID와 일치하면 태그를 인증하게 된다.

하지만 태그의 항상 일정한 metaID에 대한 Key와 ID가 마지막 단계에서 노출되기 때문에 위장 리더가 metaID에 대한 응답으로 이전에 도청한 Key를 재전송하여 태그로부터 인증을 받을 수 있고 또한 위장 태그가 이전에 도청한 metaID와 ID를 리더에게 재전송하여 리더로부터 인증을 받을 수 있다. 따라서 리더와 태그 모두 상호 인증의 신뢰성에 문제가 발생하게 된다. 그리고 태그는 항상 일정한 metaID를 리더에게 전송하기 때문에 태그의 위치가 추적될 수 있다.

(2) 랜덤 해쉬 락(Randomized Hash lock) 방식

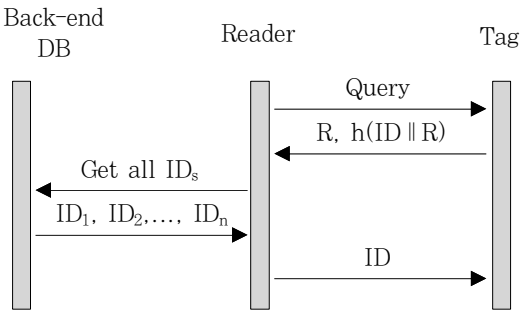

그림 3. 랜덤 해쉬 락 인증 프로토콜
Fig. 3. Authentication protocol of randomized hash lock

〔그림 3〕과 같은 랜덤 해쉬 락 방식의 인증 프로토콜은 해쉬 락 방식에서 항상 일정한 metaID를 사용함으로써 발생되는 문제점을 해결하기 위하여 의사난수생성기(Pseudo Random Number Generator)를 이용하여 생성한 난수 R을 이용한다. 초기에 태그는 자신의 ID만을 보관하고 있으며 DB는 모든 태그의 ID를 보관하고 있다. 리더가 태그에게 Query를 보내면 태그는 리더에게 R과 h(ID‖R)를 전송한다. R은 전송 때마다 바뀜으로 h(ID‖R)는 항상 다른 값이 전송된다. 리더는 DB로부터 모든 ID를 받아와 각 ID에 대한 h(ID‖R)를 계산하여 태그로부터 받은 h(ID‖R)와 일치된 값을 찾아 태그의 ID를 알아낸 후 태그에게 이를 전송한다. 상호 인증 방법에 있어 리더는 일치된 ID를 찾아냄으로써 태그를 인증하게 되고 태그는 리더로부터 받은 ID가 자신의 ID와 일치할 경우 리더를 인증하게 된다.

하지만 이 방식은 위장 태그가 이전에 도청한 R, h(ID‖R) 메시지를 재전송할 경우 리더를 속일 수 있기 때문에 리더가 태그를 인증하는 데는 문제가 발생한다. 또한 태그의 ID가 노출되는 문제점도 있고 태그에 의사난수생성기를 내장해야 하고 정당한 ID를 찾기 위해 리더의 계산량이 많아진다는 단점이 있다.

(3) 해쉬 체인(Hash chain) 방식

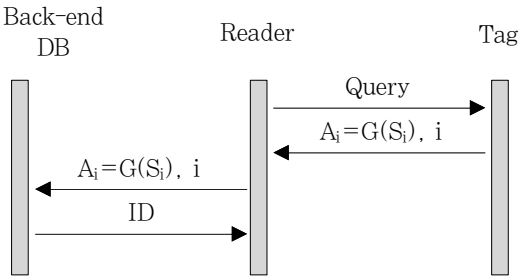

그림 4. 해쉬 체인 인증 프로토콜
Fig. 4. Authentication protocol of hash chain

〔그림 4〕와 같은 해쉬 체인 방식의 인증 프로토콜은 두개의 해쉬 함수 H와 G를 이용하여 리더의 질의에 응답한다. 초기에 태그와 DB는 태그의 ID와 S를 보관하고 있다. 리더가 태그에게 i번째로 Query를 보내면 태그는 $A_i=G(S_i)$, i 메시지를 리더에게 보낸다. 그리고 태그는 i번째 통신 후에는 S값을 $S_{i+1}=H(S_i)$로 변경시킨다. 리더는 $A_i=G(S_i)$, i 메시지를 DB에게 보내고 DB는 모든 S에 대하여 $G(S_i)$를 계산하여 A_i와 일치하는 값을 찾아 ID를 알아내고 이를 리더에게 전송한다.

상호 인증 방법에 있어 리더는 DB로부터 ID를 받음으로써 태그를 인증하게 되지만 태그가 리더를 인증하는 절차는 없다. 또한 위장 태그가 $A_i=G(S_i)$, i 메시지를 재전송할 경우 리더를 속일 수 있기 때문에 리더가 태그를 인증하는 데도 문제가 발생한다. 그리고 태그는 두개의 해쉬 함수를 사용하고 DB는 모든 S에 대하여 i번의 해쉬 함수 G를 계산해야하기 때문에 태그와 DB에 많은 부담을 주게 된다.

III. 제안하는 시스템

이 장에서는 제안하는 RFID 시스템이 보안을 유지하기 위한 요건을 설명하고 이를 만족하는 인증 프로토콜을 제안한다.

3.1 제안하는 RFID 시스템의 보안 요건

RFID 시스템에서는 리더와 태그 사이가 RF 신호를 이용함으로 채널이 불안전하다. 따라서 RFID 시스템이 안전해지기 위해서는 다음과 같은 공격으로부터 안전해야 한다[11,12]. 이러한 공격으로부터 완전히 안전하여야만 리더와 태그 간에 상호 인증이 가능하다.

(1) 도청(Eavesdropping) 공격

RFID 시스템에서 도청 공격이란 공격자가 리더와 태그 사이에 주고받는 정보를 엿듣는 공격 방법이다. 도청으로부터 얻은 정보는 또 다른 공격에 이용될 수 있다.

(2) 재전송(replay) 공격

RFID 시스템에서 재전송 공격이란 공격자가 리더와 태그 사이에 주고받는 정보를 도청한 후 이를 재 전송함으로써 정당한 태그나 리더로 인증 받으려는 공격 방법이다.

(3) 스푸핑(Spoofing) 공격

RFID 시스템에서 스푸핑 공격이란 공격자가 정당한 리더나 태그로 위장하여 상대방으로부터 인증에 필요한 정보를 습득하고 이 정보를 이용하여 정당한 태그나 리더를 속이는 공격 방법이다. 일반적으로 스푸핑 공격은 자신이 공격을 당하고 있는지도 모른 채 오랜 시간을 보낼 수 있기 때문에 더욱 위험하다.

(4) 위치 추적(Location tracking) 공격

RFID 시스템에서 위치 추적 공격이란 공격자가 리더와 태그 사이에 주고받는 정보를 분석하여 동일한 태그에서 전송되는 정보의 패턴을 알아내어 태그의 위치 정보 등을 알아내는 공격 방법이다.

3.2 제안하는 RFID 시스템의 인증 프로토콜

본 논문에서 제안하는 RFID 시스템은 유효한 태그의 ID를 보관하고 있는 백-앤드 데이터베이스와 태그의 자료를 읽어내는 리더 그리고 태그로 구성된다. 데이터베이스와 리더 사이는 안전한 채널로 연결되어 있고 리더와 태그 사이는 안전하지 않은 채널로 이루어져 있으며 초기에 태그는 자신의 ID, key, cnt 값을 갖고 있으며 DB는 모든 태그의 ID와 key 값을 갖고 있다고 가정한다.

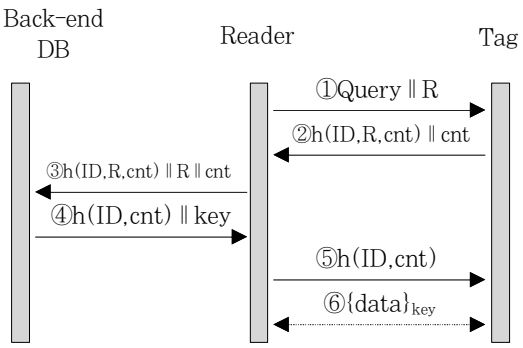

그림 5. 제안 시스템의 인증 프로토콜
Fig. 5. Authentication protocol of the suggested system

〔시스템 계수〕
- ID : 태그의 고유 인식 번호
- R : pseudo random number
- cnt : counter
- key : 태그와 DB가 초기에 공유하고 있는 대칭키
- h() : one way hash function
- ‖ : 문자열 연접

제안한 시스템의 인증 프로토콜은 〔그림 5〕에서 보는 바와 같이 인증은 ①~⑤단계에서 이루어지며 ⑥단계에서 암호화된 자료가 전송된다. 상세 내용은 다음과 같다.

① (리더→태그) : 리더는 임의 난수 R을 생성하여 Query 명령과 함께 태그에게 전송한다.

② (태그→리더) : Query 명령을 수신한 태그는 자신의 ID와 R 그리고 보관중인 cnt를 이용하여 h(ID, R, cnt)를 계산하여 cnt와 함께 리더에게 보낸다. 그리고 cnt를 1증가하여 저장해 둔다.

③ (리더→DB) : 리더는 태그로부터 받은 h(ID, R, cnt)와 cnt 그리고 자신이 생성한 R을 데이터베이스로 보낸다.

④ (DB→리더) : 데이터베이스는 R과 cnt를 이용하여 보관중인 ID들로부터 h(ID, R, cnt)와 일치하는 ID를 찾는다. 일치하는 ID가 있다면 데이터베이스는 비로소 태그를 인증하게 되고 h(ID, cnt)를 계산하여 대칭키 key와 함께 리더에게 전송한다. 만일 일치하는 ID가 없다면 오류 메시지를 리더에게 전송한다.

⑤ (리더→태그) : 리더는 오류 메시지를 수신할 경우에는 태그와의 통신을 중단하고 h(ID, cnt)를 정상적으로 수신한 경우에는 이를 태그에게 전송한다. 태그는 수신한 h(ID, cnt)와 자신이 계산한 h(ID, cnt)를 비교하여 일치하면 데이터베이스를 인증할 수 있게 된다.

⑥ (리더↔태그) : 리더와 태그는 data를 전송할 때 대칭키 key로 암호화하여 {data}key 을 상호 전송한다. 만일 공격자가 이를 도청하더라도 해독할 수 없다.

Ⅳ. 제안하는 시스템의 분석

이 장에서는 3장에서 제안한 인증 프로토콜이 기능적인 면에서 안전성이 보장되는가 그리고 성능적인 면에서 효율성 즉 인증 속도는 기존의 다른 시스템의 인증 프로토콜과 비교하여 어떠한가를 분석해본다.

여러 가지 공격 형태로부터 시스템의 안전성은 제안한 프로토콜을 단계별로 상세히 분석함으로써 증명해보이고 시스템의 효율성은 제안한 프로토콜에서 인증 속도에 영향을 미치는 해쉬 함수와 난수 생성기의 실행 횟수를 시스템의 각 구성 요소들 별로 계산해봄으로써 기존의 다른 시스템과 비교분석해본다.

4.1 안전성 분석

이 절에서는 제안하는 시스템이 3.1절의 제안하는 RFID 시스템의 보안 요건을 얼마나 충족시키는지를 분석해본다.

(1) 도청 공격에 대한 안전성

공격자가 〔그림 5〕에서 ①, ②, ⑤ 내용을 도청하더라도 통신내용 중 유일한 비밀정보인 태그의 ID가 해쉬 함수로 보호되고 있기 때문에 이를 알아낼 수 없다. 따라서 제안하는 시스템은 상호 인증과정에서 도청 공격에 안전하다. 또한 상호 인증 이후에도 리더와 태그는 대칭키 key를 이용하여 비밀통신을 하기 때문에 도청 공격에 안전하다.

(2) 재전송 공격에 대한 안전성

매 인증 세션마다 R값이 변경됨으로 〔그림 5〕에서 ②는 항상 새로이 생성되어야 한다. 따라서 위장 태그가 정상 태그의 ID를 알지 못하고는 ②를 재전송할 수 없다. 또한 위장 리더가 이전 인증 세션의 ①, ②, ⑤ 내용을 모두 도청하여 보관하고 있더라도 ②의 내용이 매 인증 세션마다 변경됨으로 이전에 보관한 것을 재사용할 수 없다.

(3) 스푸핑 공격에 대한 안전성

위장 태그가 리더에게 정상 태그로 보이기 위해서는 〔그림 5〕의 ②를 생성할 수 있어야하는데 위장 태그는 정상 태그의 ID를 알 수 없기 때문에 ②를 생성할 수 없다. 만일 ②를 재전송하더라도 ⑤에서 정상 태그의 ID를 알 수 없음으로 ⑥에서 계속적인 비밀 통신은 불가능하다. 그리고 위장 리더가 태그에게 정상 리더로 보이기 위해서는 ②에 대한 ⑤를 응답해야하는데 위장 리더는 태그의 ID를 모름으로 ⑤를 생성할 수 없다. 또한 매 인증 세션마다 R이 바뀜으로 ⑤를 재전송할 수도 없다. 따라서 위장 리더는 존재할 수 없다.

(4) 위치추적 공격에 대한 안전성

태그는 매 인증 세션마다 다른 R을 사용하여 해쉬 값을 계산하여 ②를 리더에게 보내기 때문에 태그의 위치정보를 추적할 수 없다. 또한 공격자가 이전 인증 세션에서 전송한 ①을 반복하여 재전송 하더라도 ②는 매번 다른 내용이 전송됨으로 태그의 위치정보를 추적해낼 수 없다.

(5) 상호인증

〔그림 5〕에서 리더는 태그에게 ①을 전송한 후 데이터베이스로부터 ④를 정상적으로 수신하게 되었을 때 태그를 인증하게 된다. 또한 태그는 리더에게 ②를 전송한 후 리더로부터 ⑤를 정상적으로 수신하게 되었을 때 리더를 인증하게 된다. 따라서 제안 시스템은 리더와 태그 간에 상호 인증이 가능하다.

〔표 1〕은 각 인증 프로토콜들에 대해서 공격자의 공격 유형에 따라 안전도는 어떠하며 리더와 태그 간의 상호 인증 여부는 어떠한가를 보여준다. 이 표에서 보듯이 제안 시스템이 모든 면에서 우월함을 알 수 있다.

표 1. 기존 시스템과 안전성 비교분석
Table 1. Comparison and analysis of the stability with other systems

항목 / 프로토콜	공격 유형에 따른 안전성				상호 인증
	도청	재전송	스푸핑	위치 추적	
해쉬 락	불안전	불안전	불안전	불안전	불가능
랜덤 해쉬 락	불안전	불안전	불안전	안전	일방향 가능
해쉬 체인	불안전	불안전	불안전	안전	불가능
제안 시스템	안전	안전	안전	안전	가능

4.2 효율성 분석

인증 프로토콜의 효율성을 분석하기 위하여 RFID 시스템의 구성 요소들의 연산량을 조사해보았다. 연산량은 해쉬 함수의 실행 횟수와 난수 생성기의 실행 횟수를 계산하였다. 제안 시스템에서는 태그에서는 해쉬 함수가 2회 실행되었고 난수 생성은 하지 않았다. 리더에서는 난수 생성을 1회만하여 랜덤 해쉬 락보다 월등히 연산량이 적다. 그리고 데이터베이스에서는 해쉬 함수가 태그의 수 절반정도로 랜덤 해쉬 락과 비슷하며 해쉬 체인보다는 i배나 적은 횟수이다.

〔표 2〕는 각 인증 프로토콜들에 대해서 태그, 리더 그리고 DB의 연산량을 비교분석한 결과이다. 종합적으로 제안 시스템의 효율성은 태그와 리더의 부담을 줄이고 데이터베이스의 부담도 최소화 시켰다.

표 2. 기존 시스템과 효율성 비교분석
Table 2. Comparison and analysis of the efficiency with other systems

항목 / 프로토콜	연산량		
	태그	리더	DB
해쉬 락	해쉬함수 : 1회	-	-
랜덤 해쉬 락	해쉬함수 : 1회 난수생성 : 1회	해쉬함수 : 태그수/2회	-
해쉬 체인	해쉬함수 : 2회	-	해쉬함수 : (태그수/2)*i회
제안 시스템	해쉬함수 : 2회	난수생성 : 1회	해쉬함수 : (태그수/2)+1회

V. 결론

향후 RFID 시스템은 현재의 바코드 시스템을 대체할 것으로 예상된다. 그러나 RFID 시스템은 근원적으로 몇 가지 문제점을 갖고 있는데 이를 해결해야만 앞으로 상용화가 가능할 것이다. RFID 시스템에서는 리더와 태그 간의 통신이 RF 신호를 이용하기 때문에 아무나 손쉽게 통신 내용을 수신할 수 있음으로 도청에 취약하고 이미 한번 전송된 내용을 재전송함으로써 비정상적인 태그나 리더가 정상적인 것으로 위장하기도 쉽고 태그를 소유한 사용자의 위치를 추적할 수 있는 문제점을 갖고 있다.

그동안 이러한 문제점들을 보완한 여러 가지 연구 결과가 발표되었으나 각기 약간의 문제점들을 갖고 있었다. 그 중에서 해쉬 락 방식은 도청, 재전송, 스푸핑, 위치추적 공격에 모두 불안전하였으며 이를 개선한 랜덤 해쉬 락 방식과 해쉬 체인 방식은 위치추적에는 안전하나 다른 부분에서는 불안전했다. 그리고 상호 인증 부분에서는 해쉬 락 방식과 해쉬 체인 방식은 양방향 모두 인증이 불가능하였고 랜덤 해쉬 락 방식은 태그가 리더만 인증할 수 있는 일방향 인증만 가능하였다.

본 논문에서는 기존 RFID 시스템의 인증 프로토콜의 이러한 문제점들을 개선한 새로운 RFID 시스템을 제안하였다. 제안한 시스템은 안전성 면에서 ID를 해쉬 함수로 항상 보호하고 있음으로 도청이 불가능하며 인증 세션 때마다 교환되는 메시지를 항상 다르게 했기 때문에 리더나 태그로 위장한 공격자가 한번 보낸 메시지를 재전송할 수 없다. 또한 매번 다른 메시지의 전송으로 태그의 위치를 추적할 수 없어 개인의 프라이버시도 보호할 수 있다. 그리고 상호 인증을 할 수 있음으로 위장 태그나 위장 리더가 제안 시스템 내에서는 동작할 수 없다. 또한 제안 시스템의 효율성 측면에서는 시스템 구성 요소들의 능력을 고려하여 연산기능이 떨어지는 태그에는 부담을 줄였고 데이터베이스와 리더의 부담은 최소화시켰다.

본 논문의 결과는 유비쿼터스 환경에서 RFID 태그를 이용한 다양한 분야에 활용될 수 있을 것으로 기대한다. 그리고 본 논문에서는 데이터베이스와 리더 사이가 안전한 채널이라고 가정하였으나 앞으로 이 채널도 불안전한 것으로 가정한 연구가 필요할 것으로 사료된다.

참고문헌

〔1〕 H. Knospe and H. Pob, "RFID Security", Information Security Technical Report, Vol.9, No.4, pp.39-50, 2004

〔2〕 S. A. Weis, "Security and Privacy in Radio-Frequency Identification Devices", Master's thesis, MIT, 2003

〔3〕 S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID Systems, Security & Privacy Implications", White Paper, Auto-ID Center, MIT, 2002

〔4〕 Ari Juels, Ronald L. Rivest, and Michael Szydlo, "The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy", 8th ACM Conference on Computer and Communications Security, Vol.10, pp.103-111, 2003

〔5〕 S. E. Sarma, S. A. Weis, and D. W. Engels,

"Radio-frequency identification systems", Workshop on Cryptographic Hardware and Embedded Systems, CHES02, LNCS 2523, Springer-Verlag, pp.454-469, 2002

〔6〕 S. A. Weis, "Radio-frequency identification security and privacy", Master's thesis, MIT, 2003

〔7〕 S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", In First International Conference on Security in Pervasive Computing 2003, Springer-Verlag, LNCS 2802, pp.201-212, 2004

〔8〕 M. Ohkubo, K. Suzuki, and S. Kmoshita, "A Cryptographic Approach to 'Privacy-Friendly' tag", RFID Privacy Workshop, Nov 2003

〔9〕 K. Finkenzeller, RFID Handbook, John Wiley and Sons, pp.2-10, 1999

〔10〕 D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers", Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp.219-224, 2004

〔11〕 A. Juels, "RFID Security and Privacy: A Research Survey", IEEE journal on selected areas in communications, Vol.24, No.2, pp.381-394, 2006

〔12〕 S. Lee, T. Asano and K. Kim, "RFID Mutual Authentication Scheme based on Synchronized Secret", Information, In proceedings of the SCIS'06, 2006

저 자 소 개

이상렬

1981 한양대학교 전자공학과 학사
1983 한양대학원 전자공학과 석사
2005 한양대학원 전자공학과 박사
1997~현재 상지영서대학 인터넷정보과 교수
〈관심분야〉 컴퓨터통신, 시스템 및 네트워크 보안