공개 채널 기반의 RFID 상호인증 시스템 설계

종신회원 윤 은 준*, 정회원 유 기 영**°

A Design of RFID Mutual Authentication System based on Open Channel

Eun-Jun Yoon* *Lifelong Member*, Kee-Young Yoo**° *Regular Member*

요 약

일반적인 RFID 시스템에서는 리더와 백 엔드 데이터베이스 사이의 통신 채널을 안전한 채널로 가정하고 있다. 하지만 응용 환경에 따라 리더와 데이터베이스 사이의 통신 채널이 리더와 태그 간의 통신 채널처럼 안전하지 않은 채널을 통하여 메시지를 송수신 하게 되는 경우가 얼마든지 존재한다. 본 논문에서는 데이터베이스, 리더 그리고 태그 간의 모든 통신 채널이 안전하지 않은 공개 채널임을 가정하여 공개 채널 기반의 안전한 RFID 상호인증 프로토콜을 제안한다. 제안한 프로토콜은 공개된 채널 상에 송수신되는 모든 통신 메시지의 인증과 무결성을 보장하기 위해 안전한 일방향 해쉬 함수를 사용하였다. 또한 상호인증 후 데이터베이스와 태그가 다음 세션을 위해 기존의 비밀키를 새로운 비밀키로 각각 갱신하도록 하여 전방향 안전성을 제공하도록 설계하였다.

Key Words : RFID, Authentication, Ubiquitous Security, Protocol, One-Way Hash Function

ABSTRACT

General RFID system has assumed that the communication channel between reader and back-end database is secure channel. However, the reader can be communicated with the database through insecure channel like the communication channel between the reader and the tag according to application environment. In this paper, we propose a new secure RFID mutual authentication protocol based on open network channel which assumed that all communication channels between the database, the reader and the tag are insecure communication channels. The proposed protocol uses a secure one-way hash function to provide authentication and integrity against all communication messages which exchanged on the open channels. In addition, we designed that the proposed protocol can provide forward secrecy by performing the database and the tag update their old secret key with a new secret key after finished mutual authentication.

Ⅰ. 서 론

RFID(Radio Frequency IDentification) 기술은 현재 유비쿼터스 산업 기반에서 가장 광범위하게 사용되어 지고 있다. RFID 기술은 무선 주파수를 이용하여 움직이는 물체를 인식, 추적, 분류 및 인식기 간의 데이터 통신을 수행하는 자동 데이터 수집 기술로써, 현재 국내에서는 교통카드, 출입구 보안 및 출결 카드 등 근접식 RFID가 주로 활용되고 있으며, 많은 연구로 인해 물류 및 유통 분야까지

※ 이 논문은 2008년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음 (KRF-2008-521-D00367)
* 경북대학교 전자전기컴퓨터학부 (ejyoon@knu.ac.kr)
** 경북대학교 컴퓨터공학과 정보보호연구실 (yook@knu.ac.kr) (°:교신저자)
논문번호 : KICS2009-07-275, 접수일자 : 2009년 7월 27일, 최종논문접수일자 : 2009년 9월 7일

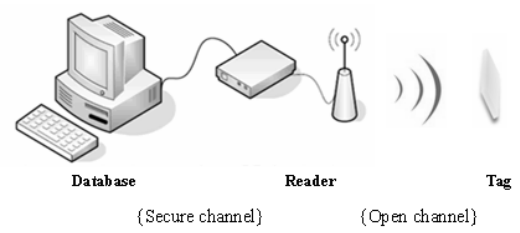


그림 1. 일반적인 RFID 시스템의 구조

빠르게 응용 및 확산되고 있다[1].

그림 1은 기본적인 RFID 시스템의 네트워크 구조를 보여준다. 그림 1에서 보여주는 것과 같이 RFID 시스템은 태그(Tag), 리더(Reader), 그리고 백-엔드 데이터베이스(Back-end Database:DB)의 3가지 구성요소로 구성된다[2]. RFID 시스템에서 인증(Authentication)은 프라이버시 침해와 다양한 공격들을 막기 위한 아주 중요한 보안기법이다. Weis 등이 제안한 RFID 인증 프로토콜을 시작으로 그동안 많은 연구자들에 의해 안전성과 효율성을 고려한 RFID 인증 프로토콜들을 제안하여 오고 있다. 하지만 지금까지 제안되어져오고 있는 RFID 인증 프로토콜들은 Reader와 DB 사이의 통신 채널을 안전한 채널(Secure Channel)로 가정하고 Reader와 Tag간의 인증을 안전하게 수행하는 방법들에 관한 연구를 해왔다[3]-[16].

RFID 시스템 응용 환경에 따라 Reader와 DB 사이의 통신 채널이 Reader와 Tag 간의 통신 채널처럼 안전하지 않은 채널(Insecure Channel)을 통하여 메시지를 송수신 하게 되는 경우가 얼마든지 존재한다. 예를 들면, 휴대폰, PDA와 같은 모바일 장치(Mobile Device)들에 Reader가 장착되어 무선 네트워크(Wireless Network)를 통하여 DB와 기밀 정보를 송수신하게 된다면 얼마든지 공격자(Attacker)가 개입되어 송수신되는 메시지에 대한 기밀성(Confidentiality)과 무결성(Integrity)을 저해할 수 있다. 만약 이러한 환경에서 기존의 RFID 인증 프로토콜들을 적용하게 된다면 DB와 Reader 간의 통신 채널이 안전하지 않음으로 인해 Reader와 Tag 간의 통신 채널에서 발생할 수 있는 도청 공격(Eavesdropping Attack), 재전송 공격(Repaly Attack), 스푸핑 공격(Spoofing Attack) 등 다양한 공격들에 취약할 수 있다. 이러한 이유로 DB와 Reader 간에도 안전한 상호인증을 수행할 수 있는 보안 프로토콜 개발이 아주 중요하다.

본 논문에서는 DB, Reader 그리고 Tag 간의 모든 통신 채널이 안전하지 않은 공개 채널(Open Channel)임을 가정하여 공개 채널 기반의 안전한 RFID 상호인증 프로토콜을 제안한다. 제안한 프로토콜은 공개된 채널 상에 송수신되는 모든 통신 메시지의 인증(Authentication)과 무결성(Integrity)을 보장하기 위해 안전한 일방향 해쉬 함수(Secure One-way Hash Function)를 사용하였다. 또한 상호인증 후 DB와 Tag가 다음 세션을 위해 기존의 비밀키(Secret Key)를 새로운 비밀키로 각각 갱신하도록 하여 전방향 안전성(Forward Secrecy)을 제공하도록 설계하였다. 결론적으로 제안한 공개 채널 기반의 RFID 상호인증 프로토콜은 Reader, DB, Tag 모두 안전한 상호인증(Mutual Authentication)을 수행할 수 있어 다양한 RFID 시스템 환경에 실용적으로 사용되어 질 수 있다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 관련연구로써 RFID 시스템에 대한 소개와 제안한 공개 채널 기반의 RFID 상호인증 프로토콜에서 필요한 보안요구 사항들을 정의하며, 3장에서는 제안하는 공개 채널 기반의 안전한 RFID 상호 인증 프로토콜에 대한 동작과정을 구체적으로 설명하고, 4장과 5장에서는 안정성과 효율성을 각각 분석한다. 마지막으로 6장에서는 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

2.1 RFID 시스템의 구성요소

일반적으로 RFID 시스템은 태그(Tag), 리더(Reader), 그리고 백-엔드 데이터베이스(Back-end Database)의 3가지 구성요소로 구성되며 이들 구성요소의 기능은 다음과 같다[1],[11],[15].

2.1.1 태그(Tag)

Tag는 무선 통신을 수행하기 위한 안테나와 인증관련 연산을 수행하고 필요한 정보를 Tag 내에 저장하는 마이크로 칩으로 구성되어진다. Reader가 질의를 하면 Tag는 자신에게 저장된 식별정보 등을 무선 통신 채널을 통해 Reader에게 전송한다. 일반적으로 Tag는 전력을 공급받는 방법에 따라서 능동형 태그(Active Tag)와 수동형 태그(Passive Tag)로 구분된다.

2.1.1.1 능동형 태그(Active Tag)

능동형 Tag는 Tag 자체에 내장된 배터리를 이용하여 전력을 공급받게 된다. 능동형 Tag는 자체에

내장된 배터리 사용으로 인해 수십미터 이상의 원거리 정보 전송도 가능한 장점을 가진다. 하지만 Tag 자체에 배터리가 내장되어 있어서 Tag의 가격이 비싸며, Tag의 수명 또한 배터리에 종속적이라는 단점을 갖는다. 능동형 Tag는 토목, 건축, 의료 분야 등에 응용되고 있다.

2.1.1.2 수동형 태그(Passive Tag)

수동형 Tag는 RFID Reader가 송신해주는 전자기파에 의해 유도된 전류를 전원으로 사용하여 필요한 정보를 Reader로 전송한다. 따라서 Tag의 전송 전력이 Reader에 비해 상대적으로 낮기 때문에 근거리 정보 전송에 이용된다. 수동형 Tag는 배터리를 자체 내장하고 있지 않기 때문에 능동형 Tag보다 가격이 싸며, Tag의 수명이 반영구적인 장점을 가진다. 수동형 Tag는 물류관리, 전자상거래, 교통, 전자물체감시 시스템 분야 등에 응용되고 있다.

2.1.2 리더(Reader)

Reader는 Tag가 전송하는 데이터정보를 수신하여 Tag를 인식하거나 Tag에 필요한 새로운 정보를 다시 쓸 수 있게 해주는 역할을 수행하는 Tag 인식 장치이다. Reader는 무선 통신 채널을 통하여 Tag에게 필요한 정보를 요청하거나 Tag로 부터 수신한 정보를 데이터베이스에 전송하여 필요한 정보를 수신하게 된다.

2.1.3 백-엔드 데이터베이스(Back-end Database)

Back-end Database(DB)는 Tag에 관련된 다양한 정보를 데이터베이스 내에 저장 및 관리하며, 상대적으로 연산 능력이 떨어지는 Reader 또는 Tag를 대신하여 복잡한 연산을 대신 수행하여 필요한 정보를 제공하여 준다. 일반적으로 RFID 시스템에서 DB는 정당한 Reader로부터 송신된 임의의 Tag에 관한 정보를 수신하여 이를 이용하여 해당 Tag의 정당성을 식별하는 기능을 수행한다.

2.2 제안한 RFID 시스템의 보안 고려사항

본 논문에서 제안한 RFID 시스템 통신 환경은 그림 2와 같다. 즉, Tag와 Reader간의 통신 채널외에 추가적으로 Reader와 DB간의 통신 채널 또한 안전하지 않은 공개된 통신 채널(Open communication channel로 가정함으로 Reader와 DB 사이의 보안도 고려하여야 한다. 따라서 제안한 RFID 시스템에서는 다음과 같은 보안 문제들을 고려하여 설계되어져야 한다[5],[10],[11].

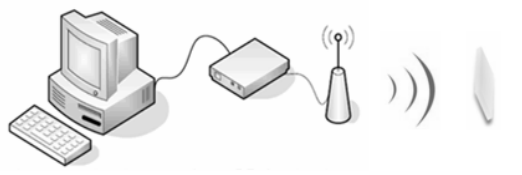


그림 2. 제안한 RFID 시스템의 구조

2.2.1 상호인증(Mutual Authentication)

상호인증은 Tag, Reader 그리고 DB 모두 상대 통신 당사자가 합법적인지를 명시적인 인증을 통해 확인하여 안전한 인증을 수행하는 것이다.

2.2.2 도청 공격(Eavesdropping Attack)

도청 공격은 공격자가 Tag와 Reader간에 또는 Reader와 DB간에 송수신되는 모든 통신 내용을 엿들은 후 Tag 또는 DB내에 저장된 비밀 정보를 알아내고자 하는 공격이다.

2.2.3 재전송 공격(Replay Attack)

재전송 공격은 수동적 공격자가 과거에 Reader와 Tag 사이 또는 Reader와 DB 사이에 통신한 내용들을 도청한 후 이를 재전송하여 합법적인 Tag, Reader 또는 DB로 인증 받으려는 공격이다.

2.2.4 스푸핑 공격(Spoofing Attack)

스푸핑 공격은 공격자가 정당한 Tag로 위장하여 Reader로부터 인증에 필요한 정보를 획득하거나, 정당한 Reader로 위장하여 Tag 또는 DB로부터 인증에 필요한 정보를 획득하거나, 또는 정당한 DB로 위장하여 Reader로부터 인증에 필요한 정보를 획득하여 이를 이용하여 정당한 Tag, Reader 또는 DB로 인증 받는 공격이다.

2.2.5 트래픽 분석 공격(Traffic Analysis Attack)

트래픽 분석 공격은 공격자가 도청을 통해서 얻은 내용을 분석하여 Reader의 질의에 대한 Tag의 응답을 예측하여 Tag의 이동경로를 추적할 수 있는 공격이다.

2.2.6 위치 트래킹 공격(Location Tracking Attack)

위치 트래킹 공격은 공격자가 Tag의 위치변화를 감지함으로 인해 Tag 소유자의 이동 경로를 파악하여 사용자의 프라이버시를 침해하는 공격이다.

2.2.7 서비스 거부 공격(Denial of Service Attack)

서비스 거부 공격은 Reader, Tag 또는 DB가 정당한 통신 상대방의 인증 요청임에도 불구하고 공격자에 의한 많은 계산이 요구되는 데이터 송신, 이전 세션에서 갱신되는 값들을 올바른 값으로 갱신되지 못하도록 방해하는 등 Reader, Tag 또는 DB가 정상적인 서비스와 기능을 수행 하지 못하도록 하는 공격이다.

2.2.8 전방향 안전성(Forward Secrecy)

전방향 안전성은 공격자에게 현재 세션에서 DB와 Tag간에 공유된 비밀키 값이 누출되더라도 해당 비밀 값을 이용하여 과거에 사용된 비밀 값을 유도하거나 메시지 무결성을 저해하지 않아야 하는 보안성을 의미한다. 즉, RFID Tag는 폐기 되어질 수 있기에 공격자에 의해 쉽게 획득되어 부채널 공격(Side-Channel Attack)등을 통해 Tag 내에 저장된 비밀키 값이 유출될 수 있다. 따라서, DB와 Tag는 상호인증을 수행 후 다음 세션을 위해 서로의 비밀 값을 안전하게 갱신하여 트래픽 분석 공격이나 위치 트래킹 공격 등을 방어할 수 있어야 한다.

Ⅲ. 제안하는 프로토콜

본 장에서는 제안한 공개 채널 기반의 RFID 상호인증 프로토콜 소개한다. 표 1은 제안한 프로토콜에서 사용되어 지는 시스템 파라미터를 보여준다.

그림 3은 제안한 공개채널 기반의 RFID 상호인증 프로토콜의 세부 동작과정을 보여주며 다음과 같이 총 6단계로 수행되어 진다.

표 1. 시스템 파라미터

기호	의미
$Query$	Tag의 응답을 요청하는 Reader의 요청
ID	Tag에게 할당된 고유 정보
K	Reader와 DB의 공유 비밀키
$H(\cdot)$	안전한 일방향 해쉬 함수
$PRNG(\cdot)$	의사난수 생성 함수 (Pseudo Random Number Generator)
R	Reader가 매 세션마다 생성하여 Tag에게 전송하는 난수
T	Tag가 매 세션마다 생성하여 Reader에게 전송하는 난수
$Info$	제품의 자세한 정보
$\oplus$	비트 단위 배타적 논리합(XOR) 연산
$\|$	연접(Concatenation) 연산

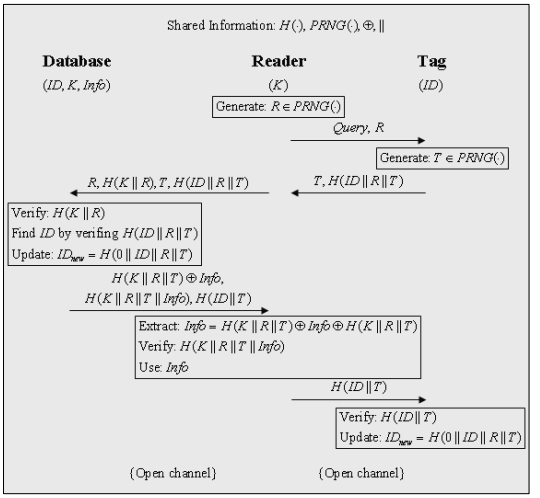


그림 3. 제안한 RFID 상호인증 프로토콜

(1) Reader → Tag : $Query$, R

Reader는 감응 인식 범위 내에 Tag가 존재하면 난수 $R \in PRNG(\cdot)$을 생성하여 $Query$와 함께 Tag에게 전송한다.

(2) Tag → Reader : T, $H(ID\|R\|T)$

Tag는 R을 수신 후, 임시저장소에 R을 저장한다. Tag는 난수 $T \in PRNG(\cdot)$를 생성하여 자신의 ID와 기 저장된 R을 이용하여 $H(ID\|R\|T)$을 계산하여 T와 함께 Reader에게 전송한다.

(3) Reader → DB : R, $H(K\|R)$, T, $H(ID\|R\|T)$

Reader는 자신이 생성한 난수 R과 데이터베이스와 공유하고 있는 비밀키 K를 이용하여 $H(K\|R)$을 계산한 후, R과 $H(K\|R)$ 그리고 Tag로부터 수신 한 T와 $H(ID\|R\|T)$을 DB에게 전송한다.

(4) DB → Reader : $H(K\|R\|T) \oplus Info$, $H(K\|R\|T\|Info)$, $H(ID\|T)$

DB는 Reader와 공유하고 있는 비밀키 K와 수신한 R을 이용하여 $H(K\|R)$을 계산한 후 수신한 $H(K\|R)$와 일치 여부를 비교한다. 만약 두 값이 일치한다면, DB는 Reader를 인증하게 되고 계속해서 Tag 인증을 수행한다. 그렇지 않다면 인증과정을 중지한다. DB는 자신의 ID 테이블에 저장된 n개의 Tag ID들과 수신한 R과 T를 이용하여 $H(ID\|R\|T)$을 각 Tag에 대해 계산한 후, Tag로부터 수신 한 $H(ID\|R\|T)$와 일치하는 ID를 찾는다.

만약 두 값이 일치하는 해쉬 값을 찾았다면, DB는 Tag를 인증하게 되고 해당 ID를 이용하여 Tag와 상호인증 메시지를 계산한다. 그렇지 않다면 인증과정을 중지한다. Reader가 DB 자신을 인증한 후 필요로 하는 Tag에 관한 제품의 자세한 정보를 담고 있는 $Info$를 활용 할 수 있도록 상호인증을 위한 $H(K\|R\|T)\oplus Info$와 $H(K\|R\|T\|Info)$를 계산한다. 또한 Tag가 DB 자신을 인증한 후 다음 세션에서 인증을 위해 사용되는 새로운 비밀키로 갱신할 수 있도록 상호인증을 위한 $H(ID\|T)$를 계산한다. 마지막으로 DB는 $H(K\|R\|T)\oplus Info$, $H(K\|R\|T\|Info)$ 그리고 $H(ID\|T)$를 Reader에게 전송하고 새로운 비밀값인 $ID_{new}=H(0\|ID\|R\|T)$를 계산하여 이전의 ID를 갱신한다.

(5) Reader → Tag : $H(ID\|T)$

Reader는 DB와 공유하고 있는 비밀키 K와 자신이 생성한 난수 R 그리고 Tag로부터 수신한 난수 T를 이용하여 $H(K\|R\|T)$를 계산한 후, DB로 부터 수신한 $H(K\|R\|T)\oplus Info$을 이용하여 $H(K\|R\|T)\oplus Info\oplus H(K\|R\|T)$와 같이 XOR 연산을 수행하여 제품에 대한 정보인 $Info$를 얻는다. 계속해서 Reader는 $H(K\|R\|T\|Info)$를 계산한 후, DB로 부터 수신한 $H(K\|R\|T\|Info)$와 일치 여부를 비교한다. 만약 두 값이 일치한다면, Reader는 DB를 인증하게 되고 $Info$ 정보를 활용한다. 그렇지 않다면 인증과정을 중지한다. Reader는 DB로부터 수신 한 $H(ID\|T)$를 Tag에게 전송한다.

(6) Tag: $H(ID\|T)$ 검증

Tag는 $H(ID\|T)$을 수신한 후, 자신의 ID와 자신이 생성한 난수 T를 이용하여 $H(ID\|T)$을 계산한 후, Reader로부터 수신 한 $H(ID\|T)$와 일치 여부를 비교한다. 만약 두 값이 일치한다면, Tag는 Reader를 인증하게 되고 다음 세션을 위해 새로운 비밀값인 $ID_{new}=H(0\|ID\|R\|T)$를 계산하여 이전의 ID를 갱신한다. 그렇지 않다면 인증과정을 중지한다.

Ⅳ. 안전성 분석

본 장에서는 제안한 공개채널 기반의 RFID 상호인증 프로토콜에 대한 안전성을 분석한다. 먼저, 제안한 인증 프로토콜의 안전성 분석을 위해 필요한 중요한 보안 항목을 다음과 같이 정의한다[17],[18].

정의 1. 강력한 비밀 키(ID와 K)는 높은 엔트로피(entropy)를 가지는 값으로써 다항식시간(Polynomial time) 내에 추측되어 질 수 없다.

정의 2. 안전한 일방향 해쉬 함수(Secure One-way Hash Function) $y=H(x)$에서, 주어진 x를 이용하여 y를 계산하는 것은 쉽지만, 주어진 y를 이용하여 x를 계산하는 것은 어렵다.

위의 정의 1과 2를 기반으로 제안한 프로토콜은 다음과 같이 상호인증을 명시적으로 제공하며, 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 안전하며 전방향 안전성을 제공한다.

4.1 상호인증(Mutual Authentication)

제안한 프로토콜의 단계 4에서 DB는 자신이 계산한 $H(K\|R)$이 Reader로부터 수신한 $H(K\|R)$와 동일한지를 검증하여 Reader를 인증하고, 자신이 계산한 $H(ID\|R\|T)$가 Reader로부터 수신한 $H(ID\|R\|T)$와 동일한지를 검증하여 Tag를 인증한다. 단계 5에서 Reader는 DB로부터 수신한 $H(K\|R\|T\|Info)$이 자신이 계산한 $H(K\|R\|T\|Info)$와 동일한지를 비교하여 DB를 인증한다. 단계 6에서 Tag는 Reader로부터 수신한 $H(ID\|T)$가 자신이 계산한 $H(ID\|T)$와 동일한지를 검증하여 Reader와 DB를 인증한다. DB와 Reader 사이에 공유된 비밀키 K와 Tag와 DB 사이에 공유된 비밀키 값 역할을 하는 ID를 모르는 공격자는 DB, Reader 또는 Tag로 위장하여 스푸핑 공격 등을 수행할 수 없게 된다. 따라서 제안한 프로토콜은 상호인증을 제공한다.

4.2. 도청 공격(Eavesdropping Attack)

제안한 프로토콜에서 공격자는 송수신되는 통신 메시지 $\{Query,\ R,\ T,\ H(ID\|R\|T),\ H(K\|R\|T),\ \oplus Info,\ H(K\|R\|T\|Info),\ H(ID\|T)\}$를 모두 도청할 수 있다. 하지만 도청한 내용으로부터 공격자는 Tag와 DB 간에 공유된 비밀키 값 역할을 하는 ID를 구할 수 없다. 즉, ID를 얻기 위해서는 공격자가 도청한 메시지 $H(ID\|R\|T)$ 또는 $H(ID\|T)$로부터 ID를 구할 수 있어야 한다. 하지만 안전한 일방향 해쉬 함수의 성질과 충분한 보안 강도를 만족하는 비트 길이를 가지는 비밀키 값인 ID에 의해 공격자는 $H(ID\|R\|T)$와 $H(ID\|T)$로부터 ID를 얻는 것은 불가능하다. 또한 비밀 값인 ID는 Tag와 DB

측에서 내부적으로 활용되어 지며 공개된 통신 채널로 전송되어 지지 않기에 공격자는 ID를 직접적으로 구할 수 없다. 또한 도청한 내용으로부터 공격자는 DB와 Reader 간에 공유된 비밀키 K를 구할 수 없다. 즉, K를 얻기 위해서는 공격자가 도청한 메시지 $H(K\|R\|T)\oplus Info$ 또는 $H(K\|R\|T\|Info)$로부터 K를 구할 수 있어야 한다. 하지만 안전한 일방향 해쉬 함수의 성질과 충분한 보안 강도를 만족하는 비트 길이를 가지는 비밀키인 K에 의해 공격자는 $H(K\|R\|T)\oplus Info$와 $H(K\|R\|T\|Info)$로부터 K를 얻는 것은 불가능하다. 따라서 제안한 프로토콜은 도청 공격에 안전하다.

4.3 재전송 공격(Replay Attack)

제안한 프로토콜에서는 매 세션마다 Reader가 생성하는 새로운 난수 R과 Tag가 생성하는 새로운 난수 T를 이용하여 DB, Reader 그리고 Tag 간의 상호인증을 수행하기 때문에, 과거에 공격자에 의해 재전송된 난수 값들은 Tag와 Reader 그리고 DB간의 상호인증 과정 중에 쉽게 검출된다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

4.4 스푸핑 공격(Spoofing Attack)

제안한 프로토콜에서 공격자가 DB와 Tag 간에 공유된 비밀키 값인 ID를 얻을 수 있으면, DB 또는 Tag로의 스푸핑 공격을 수행할 수 있다. 하지만 공격자는 DB와 Tag 내에 각각 안전하게 저장하고 있는 비밀키 값인 ID를 직접적으로 얻을 수 있는 방법이 없다. 또한 송수신되는 통신 메시지 $H(ID\|R\|T)$와 $H(ID\|T)$ 내의 비밀키 값인 ID는 난수 R과 T 그리고 안전한 일방향 해쉬 함수에 의해 보호되어져 있다. 제안한 프로토콜에서 공격자가 DB와 Reader 간에 공유된 비밀키 값인 K를 얻을 수 있으면, DB 또는 Reader 로의 스푸핑 공격을 수행할 수 있다. 하지만 공격자는 DB와 Reader 내에 각각 안전하게 저장하고 있는 비밀키 값인 K를 직접적으로 얻을 수 있는 방법이 없다. 또한 송수신되는 통신 메시지 $H(K\|R\|T)\oplus Info$와 $H(K\|R\|T\|Info)$ 내의 비밀키인 K는 난수 R과 T 그리고 안전한 일방향 해쉬 함수에 의해 보호되어져 있다. 따라서 제안한 프로토콜은 스푸핑 공격들에 대해 안전하다.

4.5 트래픽 분석 공격(Traffic Analysis Attack)

제안한 프로토콜에서는 난수 R과 T에 의해 계산된 $H(ID\|R\|T)$와 $H(ID\|T)$는 매 세션마다 변경되기에 공격자는 현재 세션에서 Tag의 응답 $H(ID\|R\|T)_{now}$가 과거 세션에 도청한 응답 $H(ID\|R\|T)_{old}$와 동일한지를 비교할 수 없다. 즉, 매 세션마다 서로 다른 난수 R과 T를 생성함으로, 매 세션마다 서로 다른 두 개의 응답 $H(ID\|R\|T)_{now}$와 $H(ID\|R\|T)_{old}$이 동일한 Tag로부터 송신된 것인지 여부를 쉽게 구별할 수 없음으로, Tag의 이동경로를 쉽게 추적을 할 수 없다. 따라서 제안한 프로토콜은 트래픽 분석 공격에 안전하다.

4.6 위치 트래킹 공격(Location Tracking Attack)

제안한 프로토콜에서는 위 트래픽 분석 공격과 마찬가지로 난수 R과 T에 의해 계산된 $H(ID\|R\|T)$와 $H(ID\|T)$는 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.

4.7 서비스 거부 공격(Denial of Service Attack)

제안한 프로토콜에서는 Reader와 Tag 간에 일방향 해쉬 함수 기반의 연산만을 이용하여 상호인증을 수행함으로, Tag 측에 서비스 거부 공격을 수행할 만큼의 많은 연산량을 요구하지 않는다. 또한 매 세션마다 DB와 Tag 간에 안전한 검증을 통한 상호인증을 완료 후에 다음 세션에서 사용되어 지는 새로운 비밀키 값인 $ID_{new}=H(0\|ID\|R\|T)$으로 갱신되어지기 때문에 공격자에 의한 서비스 거부 공격은 쉽게 발견되어 질수 있다. 따라서 제안한 프로토콜은 서비스 거부 공격에 안전하다.

4.8 전방향 안전성(Forward Secrecy)

기존에 제안되어진 많은 RFID 인증 프로토콜이 매 세션마다 동일한 비밀키 값인 하나의 ID만을 이용하여 상호인증을 수행한다. 이로 인해, 공격자가 폐기되어진 RFID Tag로부터 부채널 공격(Side-Channel Attack)등을 통해 Tag 내에 저장된 비밀키 값인 ID를 획득하였을 때, 과거에 해당 Tag와 Reader 간에 통신된 모든 메시지들에 대한 무결성과 기밀성은 보장되어 질 수 없게 된다. 하지만, 제안한 프로토콜에서는 DB와 Tag간에 상호인증을 수행한 후에 DB와 Tag가 서로 이전의 비밀 값인 ID를 다음 세션을 위해 새로운 비밀 값인 $ID_{new}=H(0\|ID\|R\|T)$로 각자 갱신하여 사용함으로, 공격자

표 2. 제안한 프로토콜의 안전성 분석

프로토콜 / 공격유형	해쉬 락[2],[3]	랜덤 해쉬락[7]	해쉬 체인[8]	제안 프로토콜
DB와 Tag 상호인증	○	○	×	○
DB와 Reader 상호인증	×	×	×	○
도청 공격	×	×	×	○
재전송 공격	×	×	○	○
스푸핑 공격	×	×	×	○
트래픽 분석 공격	×	○	○	○
위치 트래킹 공격	×	○	○	○
서비스 거부 공격	○	○	○	○
전방향 안전성	×	×	×	○

○ : 제공/안전, × : 제공안함/안전안함

표 3. 제안한 프로토콜의 효율성 분석

시스템 객체 / 연산종류	Tag	Reader	DB
해쉬 연산량	3	3	n+5
XOR 연산량	0	1	1
난수 생성수	1	1	0
Reader와 Tag간 통신메시지	$1Q+2R_n+2h()$		
Reader와 DB간 통신메시지	$2R_n+5h()$		
Reader와 Tag간 통신라운드	3		
Reader와 DB간 통신라운드	2		
전체 통신라운드수	5		
Tag의 쓰기연산	필요		

n : DB에 저장된 태그의 개수, Q : 쿼리(Query) 개수
$h()$: 해쉬 연산 값 개수, Rn : 일회성 난수 개수

가 현재의 비밀키 값인 $ID_{new}=H(0\|ID\|R\|T)$를 알더라도 안전한 일방향 해쉬 함수의 성질에 의해 과거에 사용된 비밀키 값인 ID를 얻을 수 없으며 Tag의 과거 메시지들을 추적할 수 없다. 따라서 제안한 프로토콜은 전방향 안전성을 제공한다.

표 2는 제안한 프로토콜과 해쉬 연산 기반의 프로토콜들인 해쉬락, 랜덤해쉬락 그리고 해쉬체인 프로토콜과의 안전성을 비교·분석한 표이다. 표 2에서 보여주는 것과 같이 제안한 프로토콜은 기존의 프로토콜과 비교하여 DB와 Reader 간의 상호인증 뿐만아니라 DB와 Tag 간에도 상호인증을 명시적으로 제공하며, 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 안전할 뿐만 아니라 전방향 안전성을 제공함을 알 수 있다. 결론적으로 제안한 프로토콜은 보다 강한 보안성을 제공함을 알 수 있다.

V. 효율성 분석

본 장에서는 제안한 RFID 상호인증 프로토콜에 대한 효율성을 분석한다. 표 3은 제안한 프로토콜의 효율성을 분석한 표이다.

표 3과 같이 제안한 프로토콜은 태그 측의 해쉬 연산량은 상호인증을 위한 해쉬 연산 2번과 전방향 안전성을 제공하기 위한 비밀키 값 갱신에 대한 해쉬 연산 1번을 포함한 총 3번이 요구되며, Reader 측의 해쉬 연산량은 상호인증과 제품에 대한 정보를 얻기 위한 해쉬 연산 3번이 요구되며, DB측의 해쉬 연산량은 상호인증을 위한 해쉬 연산 n+4번과 전방향 안전성을 제공하기 위한 비밀키 값 갱신에 대한 해쉬 연산 1번을 포함한 총 n+5번이 요구된다. 또한, Tag측의 XOR 연산은 전혀 요구되지 않으며, Reader와 DB가 제품에 대한 정보 송수신을 위해 각각 1번의 XOR 연산을 요구한다. 제안한 프로토콜은 Reader와 Tag 측에서 각각 생성한 난수 R과 T를 이용하여 안전한 상호인증을 수행함을 보안성 분석을 통하여 증명하였다. Reader와 Tag 사이에 송수신되는 통신 메시지수는 $1Q+2R_n+2h()$이며, Reader와 DB 사이에 송수신되는 통신 메시지수는 $2R_n+5h()$이다. 이는 강한 보안성을 제공하는 것과 견주어 볼 때 경량의 통신 트래픽이 요구됨을 알 수 있다. Reader와 Tag 사이의 통신 라운드수는 3라운드이며, Reader와 DB 사이의 통신 라운드수는 2라운드이다. 전체 통신 라운드수는 5라운드로 DB, Reader 그리고 Tag 모두 상호인증을 수행하는 것과 견주어 볼 때 효율적인통신라운드를 수행함을 알 수 있다. 제안한 프로토콜은 전방향 안전성을 제공하기 위해 Tag의 쓰기 연산을 필요로 한다. 물론 제안한 프로토콜이 전방향 안전성을 제공하지 않는 환경에 이용되어 진다면, 그림 4와 같이 DB와 Tag의 비밀키 값 갱신을 위한 Tag의 DB 인증 과정을 수행하지 않아도 됨으로 4번의 해쉬 연산량을 줄여 주고 전체 통신 라운드수 또한 4라운드만 필요하게 됨으로 더욱 효율적일 수 있다.

결론적으로 제안한 프로토콜은 표 2에서 보여주는 것처럼 명시적인 상호인증을 제공함으로 인해 다양한 공격에 안전하고 전방향 안전성을 제공할 뿐만 아니라 표 3과 같이 연산 오버헤드 또한 줄여

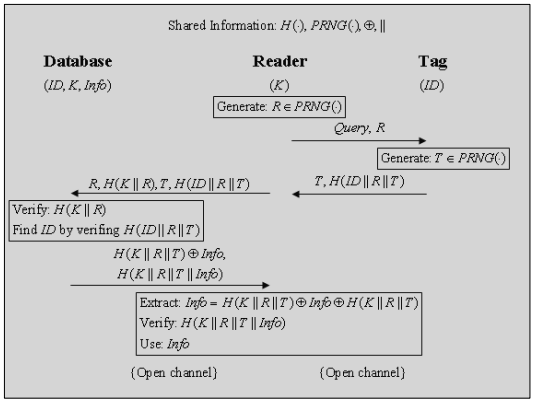


그림 4. 전방향 보안성을 제공하지 않는 제안한 RFID 상호인증 프로토콜

줌으로 안전성과 효율성 모두를 보장해 준다.

Ⅵ. 결론 및 향후연구

본 논문에서는 일반적인 RFID 인증 프로토콜들과는 달리 DB, Reader 그리고 Tag 간의 모든 통신 채널이 안전하지 않은 공개 채널임을 가정하여 공개 채널 기반의 새로운 RFID 상호인증 프로토콜을 제안하였다. 제안한 프로토콜은 공개된 채널 상에 송수신되는 모든 통신 메시지의 인증과 무결성을 보장하며 효율성을 제공하기 위해 안전한 일방향 해쉬 함수만을 사용하였다. 또한 상호인증 후 DB와 Tag가 다음 세션을 위해 기존의 비밀키를 새로운 비밀키로 각각 갱신하도록 하여 전방향 안전성을 제공하도록 설계하였다. 결론적으로 제안한 공개 채널 기반의 RFID 상호인증 프로토콜은 Reader, DB, Tag 모두 안전한 상호인증을 수행할 수 있어 현재의 RFID 기반의 모바일 환경 및 도래하는 유비쿼터스 컴퓨팅 사회에서의 다양한 RFID 시스템 환경에 실용적으로 사용되어 질 수 있을 것이다.

향후 연구로는 비동기화 유도 공격 및 태그 인식의 오류 확률 등을 고려한 보다 견고한 공개 채널 기반의 RFID 상호인증 프로토콜 개발과 DB내의 비밀 정보 유출로 인한 공격들에 안전할 수 있도록 최근에 연구되고 있는 안전한 키워드 검색(Keyword Search) 알고리즘을 DB에 적용하여 안전한 DB 보호 스킴을 적용한 완벽한 RFID 시스템 개발을 목표로 둔다. 더 나아가 제안한 RFID 상호 인증 프로토콜이 2장에서 정의된 공격들에 대해 안전하고 전방향 안전성을 보장함을 최근에 많은 보안 연구자들에 의해 사용되어 지는 정형적인 안전성 분석 방법들[19]-[22]을 기반으로 증명함을 목표로 두며, 또한 제안한 프로토콜을 실제 개발하여 그 실용성을 증명하는데 중점을 둔다.

참 고 문 헌

〔1〕 F. Klaus, “RFID handbook,” Second Edition, Jone Willey & Sons, 2003.

〔2〕 S. E. Sarma, S. A. Weis, and D. W. Engels. “RFID systems, security & privacy implications,” White Paper MIT-AUTOID-WH_014, MIT AUTO-ID CENTER, 2002.

〔3〕 S. A. Weis, “Radio-frequency identification security and privacy,” Master’s Thesis, M.I.T. 2003.

〔4〕 A. Juels and R. Pappu, “Squealing euros: privacy protection in RFID-enabled banknotes,” In proceedings of Financial Cryptography-FC’03, Vol. 2742 LNCS, pp. 103-121, Springer-Verlag, 2003.

〔5〕 A. Juels, R. L. Rivest, 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.

〔6〕 S. Junichiro, H. Jae-Cheol and S. Kouichi, “Enhancing privacy of universal re-encryption scheme for RFID tags,” EUC 2004, Vol. LNCS 3207, pp. 879-890, Springer-Verlag, 2004.

〔7〕 S. A. Weis, S. Sarma, R. Rivest, D. Engels, “Security and privacy aspects of low-cost radio frequency identification systems,” Security in Pervasive Computing 2003, Vol. LNCS 2802, pp. 201-212, Springer-Verlag, 2004.

〔8〕 M. Ohkubo, K. Suzuki, and S. Kinoshita, “Hash-chain based forward-secure privacy protection scheme for low-cost RFID,” Proceedings of the SCIS 2004, pp. 719-724, 2004.

〔9〕 양형규, 안영화, “유비쿼터스 컴퓨팅 환경에 적합한 RFID 인증 프로토콜에 관한 연구”, 전자공학회논문지 42권 CI 1호, pp. 45-50, 2005.

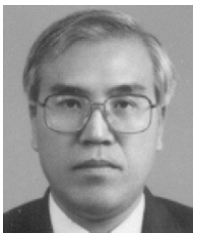
〔10〕 최은영, 최동희, 임종인, 이동훈, “저가형 RFID 시스템을 위한 효율적인 인증 프로토콜”, 정보보호학회논문지 15권 5호, pp. 59-71, 2005.

〔11〕 김배현, 유인태, "반사공격에 안전한 RFID 인증 프로토콜", 한국통신학회논문지 32권 3호, pp. 348-354, 2007.
〔12〕 김진목, 유황빈, "유비쿼터스 환경에서 Pre-Distribution을 기반으로 한 안전한 RFID 시스템", 전자공학회논문지, 제42권, 제CI-6호, pp. 29-36, 2005.
〔13〕 오선문, 강대성, "NMF와 LDA 혼합 특징추출을 이용한 해마 학습기반 RFID 생체 인증 시스템에 관한 연구", 전자공학회논문지, 제43권, 제SP-4호, pp. 46-54, 2006.
〔14〕 박인정, 현택영, "RFID를 이용한 작업관리 시스템", 전자공학회논문지, 제44권, 제CI-2호, pp. 31-36, 2007.
〔15〕 안해순, 부기동, 윤은준, 남인길, "RFID/USN 환경을 위한 개선된 인증 프로토콜", 전자공학회논문지, 제46권, 제CI-1호, pp. 1-10, 2009.
〔16〕 K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," Proc. of the SPC 2005, Vol. LNCS 3450, pp. 70-84, Springer-Verlag, 2005.
〔17〕 A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," CRC Press, New York, 1997.
〔18〕 B. Schneier, "Applied cryptography protocols," Algorithms and Source Code in C, 2nd edn. John Wiley, Chichester, 1995.
〔19〕 A. Juels and S. Weis, "Defining strong privacy for RFID," Cryptology ePrint Archive, Report 2006/137, 2006.
〔20〕 S. Vaudenay, "On privacy models for RFID," Proc. of the Asiacrypt 2007, Vol. 4833, pp. 68-87, Springer-Verlag, 2007.
〔21〕 I. Damgard and M. Ø. Pedersen, "RFID security: tradeoffs between security and efficiency," Proc. of the CT-RSA 2008, Vol. LNCS 4964, pp. 318-332, Springer-Verlag, 2008.
〔22〕 P. I. Paise and S. Vaudenay, "Mutual Authentication in RFID: Security and Privacy," Proc. of the CCS 2008, pp. 292-299, ACM, 2008.

윤 은 준 (Eun-Jun Yoon) 종신회원

1995년 2월 경일대학교 공학사
2003년 2월 경일대학교 컴퓨터공학과 공학석사
2007년 2월 경북대학교 컴퓨터공학과 공학박사
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2009년 3월~현재 경북대학교 전자전기컴퓨터학부 계약교수
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

유 기 영 (Kee-Young Yoon) 정회원



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