분산 데이터베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜

이 근 우[†] · 오 동 규[††] · 곽 진[†] · 오 수 현[†††] · 김 승 주[††††] · 원 동 호[††††]

요 약

최근 유비쿼터스 환경의 실현을 위한 핵심기술로서 RFID 시스템에 대한 연구가 활발히 진행되고 있다. 그러나 RFID 시스템이 가지고 있는 특성으로 인하여 사용자 프라이버시 침해 문제가 대두되고 있으며, 이를 해결하기 위한 프로토콜들이 개발되었다. 본 논문에서는 기존의 기법들이 가지고 있는 프라이버시 침해 문제를 분석하고 보다 안전하고 효율적으로 사용자의 프라이버시를 보호할 수 있는 인증 프로토콜을 제안한다. 또한 기존의 RFID 인증 기법들과 비교하여 제안하는 프로토콜이 안전하고 효율적임을 증명한다. 제안하는 프로토콜은 일방향 해쉬 함수와 난수를 이용한 Challenge-Response 방식에 기반하고 있으므로 공격자의 재전송 공격 및 스푸핑 공격 등에 안전하고, 분산 데이터베이스 환경에 적합하다.

키워드 : RFID 시스템, 인증 프로토콜, 일방향 해쉬 함수, 난수, Challenge-Response 방식

Challenge-Response Based Secure RFID Authentication Protocol for Distributed Database Environment

Keun-Woo Rhee[†] · Dong-Kyu Oh[††] · Jin-Kwak[†] · Soo-Hyun Oh[†††] · Seung-Joo Kim[††††] · Dong-Ho Won[††††]

ABSTRACT

Recently, RFID system is a main technology to realize ubiquitous computing environments, but the feature of the RFID system may bring about various privacy problem. So, many kinds of protocols to resolve this problem are researched. In this paper, we analyse the privacy problem of the previous methods and propose more secure and effective authentication protocol to protect user's privacy. Then we prove that the proposed protocol is secure and effective as we compare the proposed protocol with previous methods. The proposed protocol is based on Challenge-Response using one-way hash function and random number. The proposed protocol is secure against replay attack, spoofing attack and so on. In addition, the proposed protocol is proper for distributed database environment.

Key Words : RFID System, Authentication Protocol, One-way Hash Function, Random Number, Challenge-Response

1. 서 론

RFID(Radio Frequency Identification) 시스템은 무선 주파수를 이용한 자동인식기술로서 물리적 접촉 없이 개체의 정보를 읽거나 기록할 수 있는 시스템이다. 최근 들어 물류 및 유통 비용을 절감하기 위한 자동 인식 기술의 하나로 주목 받기 시작하면서 RFID 시스템에 대한 활발한 투자와 연구가 이루어지고 있으며, 기존의 바코드 방식이 물품 수명이 다할 때까지 평균 1회 정도 사용되는 것에 비해 물류 및 유통 과정에 RFID 시스템을 적용할 경우, 자동인식의 장점뿐만 아니라 태그 내의 정보를 이용한 지속적인 서비스가 가능하기 때문에 많은 기업들이 RFID 시스템에 관심을 보이고 있다[1].

하지만, RFID를 이용한 자동 인식 기술은 사용자도 모르게 개인의 정보 노출, 위치 추적 등의 프라이버시 침해 문제를 발생시킬 수 있다. 지금까지 이러한 프라이버시 침해 문제를 해결하기 위해 많은 연구가 진행되어 왔으며, 킬(Kill) 명령어 기법[1], 해쉬-락(Hash-Lock) 기법[1, 2, 3, 4], 확장된 해쉬-락 기법[1, 4], 외부 재 암호화 기법[5], 블로커태그(Blocker tag) 기법[6], 해쉬-체인(Hash-Chain) 기법[7], 그리고 해쉬 기반 ID 변형 기법[8] 등이 대표적인 예이다. 그러나 기존의 방법들은 태그의 재사용이 불가능하거나 재전송 공격, 스푸핑 공격 등에 취약하고 태그의 추적이 가능하므로 사용자 프라이버시 침해 문제를 해결하지 못하고 있다.

본 논문에서는 먼저 기존의 방법들이 가지고 있는 문제점

※ 이 논문은 2004년도 한국학술진흥재단의 지원에 의하여 연구되었음(KRF-2004-003-D00390).
† 준 회 원 : 성균관대학교 정보통신공학부 컴퓨터공학과
†† 준 회 원 : 성균관대학교 정보통신공학부 컴퓨터공학과
††† 정 회 원 : 호서대학교 컴퓨터공학부 교수
†††† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2004년 9월 17일, 심사완료 : 2005년 2월 14일

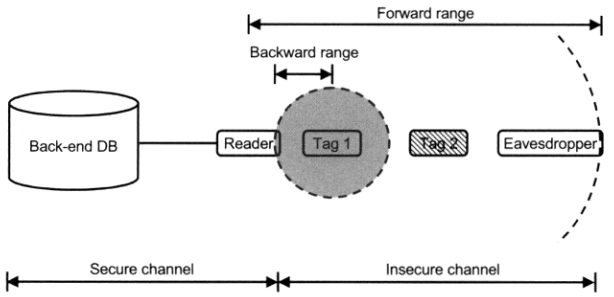
들을 분석하고, 해쉬 함수와 난수를 이용하여 태그가 리더에게 전송하는 정보를 변형함으로써 공격자에 의한 사용자 프라이버시 침해를 방지하며 도처에 분산된 데이터베이스, 리더, 태그가 존재하는 유비쿼터스 환경에 적용 가능한 RFID 인증 프로토콜을 제안한다. 또한 제안하는 프로토콜을 기존의 RFID 인증 기법들과 비교하여 제안 프로토콜의 안전성과 효율성을 증명한다.

본 논문의 구성은 다음과 같다. 2장에서는 RFID 시스템의 구성과 보안 요구사항에 대하여 설명하고, 3장에서는 기존에 제안된 RFID 시스템 보안 기법들의 문제점을 분석하며, 4장에서는 제안 프로토콜에 대하여 기술하고 안전성과 효율성을 분석한다. 마지막으로 5장에서 결론을 맺는다.

2. RFID 시스템

2.1 RFID 시스템의 구성

RFID 시스템은 일반적으로 태그, 리더, 그리고 백 앤드 데이터베이스로 구성되며, 각각의 구성과 기능은 다음과 같다. (그림 1)은 RFID 시스템의 구성에 대하여 나타낸 것이다.



(그림 1) RFID 시스템의 구성

2.2.1 태그(Tag)

태그는 RFID 시스템에서 리더의 요청에 대하여 사물, 동물, 사람 등의 식별 정보를 송신하는 것으로서 트랜스폰더(Transponder)라고도 한다. 태그의 구성은 무선 통신을 위한 결합장치(Coupling element)와 연산을 수행하고 정보를 저장하는 마이크로 칩으로 이루어져 있으며, 전력을 공급받는 방법에 따라 능동형 태그(Active tag)와 수동형 태그(Passive tag)로 분류한다.

- **능동형 태그(Active tag)** : 태그에 자체 내장된 배터리로부터 전력을 공급 받으며, 원거리 정보 전송이 가능하다. 그러나 배터리가 내장되어 있으므로 태그의 가격이 높으며, 태그의 수명이 배터리의 수명에 종속적이라는 단점이 있다. 능동형 태그는 주로 차량 타이어 압력감지시스템, 환자 관리 시스템 등에서 사용된다.
- **수동형 태그(Passive tag)** : 리더로부터 수신한 전자기파에 의한 유도 전류를 전원으로 사용하며, 태그의 전송 전력이 리더의 전송 전력에 비해 상대적(1/10 정도)으로 낮기 때문에 근거리 정보 전송에 주로 이용된다. 수동형 태그는 배터리를 내장하고 있지 않으므로 태그의 가격이 낮으며, 태그의 수명이 반영구적이라는 장점을 갖고 있기 때문에 물류관리 분야에 주로 사용된다.

2.1.2 리더(Reader)

리더는 태그가 송신한 식별 정보를 수신하여 태그를 인식하는 역할을 하는 장치로서 트랜시버(Tranceiver)라고도 한다. 리더는 태그에게 RF 신호(RF Signal : Radio Frequency Signal)를 전송하여 전력을 공급하고, 태그로부터 수신한 정보를 백-엔드 데이터베이스로 전송한다. 그리고 리더는 태그의 정보를 읽거나 기록할 수 있다.

2.1.3 백-엔드 데이터베이스(Back-end Database)

백-엔드 데이터베이스는 리더가 수집한 정보를 저장하며, 연산 능력이 낮은 태그 또는 리더를 대신하여 복잡한 연산을 수행한다. 또한 태그를 식별할 수 있는 정보를 저장하고 있으므로 리더가 태그로부터 수집한 정보의 진위를 판별하는 기능을 수행한다.

(그림 1)에서 전방위 영역(Forward range)은 리더가 RF 신호를 태그로 전송할 수 있는 영역이며, 후방위 영역(Backward range)은 태그가 리더의 요청에 대하여 자신의 정보를 전송할 수 있는 영역이다. 태그의 전송 능력이 리더의 전송 능력에 비해 상대적으로 낮기 때문에 후방위 영역은 전방위 영역에 비해 작다. 예를 들어서, 915 MHz의 주파수를 사용하는 RFID 시스템의 경우, 수동형 태그는 반경 3미터 정도의 후방위 영역을 가지지만, 리더의 전방위 영역은 반경 100미터에 이른다[4]. 그러므로 이러한 경우에는 리더의 주파수를 수신한 태그가 자신의 정보를 리더에게 전송하여도 리더가 인식하지 못하는 경우가 발생할 수 있다. 또한, 리더와 태그 간의 통신 채널은 RF 신호를 이용하므로 도청이 가능한 불안전한 채널이라 가정하고, 백-엔드 데이터베이스와 리더 간의 통신 채널은 안전한 채널이이라 가정한다.

2.2 RFID 시스템의 보안 요구사항

RFID 시스템은 물리적 접촉 없이 태그의 인식이 가능하다는 특징으로 인해 프라이버시 침해 문제를 발생시킬 수 있다. 특히, 리더와 태그 간의 통신은 불안전한 채널 상에서 이루어지므로 다음과 같은 공격자들의 공격에 대해 안전하게 설계되어야 한다[4].

2.2.1 도청자

도청자는 임의로 RFID 시스템 프로토콜에 참여하는 것은 불가능하지만 리더 또는 태그로부터 전송되는 정보를 도청 가능한 공격자로서 도청한 정보로부터 비밀 정보를 획득할 수 있으며, 또한 재전송 공격을 수행할 수 있다. 그러므로 RFID 시스템은 도청자가 도청으로 얻은 정보로부터 어떠한 비밀 정보도 유추하지 못하도록 설계되어야 하며, 또한 재전송 공격에 안전하도록 설계되어야 한다.

2.2.2 능동적 공격자

능동적 공격자는 RFID 시스템의 동작 과정에 능동적으로 참여가 가능한 공격자로서 태그에 대한 물리적 접촉은 불가능하지만 태그에게 질의하고 리더에게 응답하는 것이 가능하다. 그러므로 공격자는 정당한 리더로 가장하여 태그로부터 정보를 수집하고 이 정보를 이용하여 정당한 태그인 것처럼 가장하는 스푸핑 공격(Spoofing attacks)[1]을 수행할 수 있으며, 정당한 리더로 가장하여 태그에게 지속적인 질의를 하여 응답을 얻음으로써 태그의 위치를 추적할 수 있다. 그러므로 RFID 시스템은 능동적 공격자가 정당한 태그로부터 수집한 정보를 이용하여 정당한 태그로 가장하는 것이 불가능하도록 설계되어야 하며, 서로 다른 두 응답이 동일한 태그가 전송한 것임을 구별할 수 없도록 설계되어야 한다.

2.2.3 추적자

추적자는 트래픽 분석이 가능한 공격자로서 언제, 어디로, 어느 정도의 정보가 전송되었는지를 알 수 있다. 이러한 정보를 이용하여 추적자는 사용자의 위치를 추적할 수 있다. 그러므로 RFID 시스템은 서로 다른 두 응답이 동일한 태그가 전송한 것임을 추적자가 구별할 수 없도록 해야 한다.

2.2.4 방해자

방해자는 RFID 시스템의 동작과정에서 어떠한 정보도 수집할 수 없으나 정보 전송 방해 공격을 수행하여 메시지 유실과 같은 피해를 줄 수 있다. 방해자는 프라이버시 침해는 유발하지 않지만 시스템의 올바른 동작을 방해하므로, RFID 시스템은 방해자에 의한 정보 전송 방해 공격을 탐지 할 수 있어야 한다.

3. 관련 연구

RFID 시스템에서 리더와 태그 사이의 RF 신호를 이용한 정보 전달은 불안전한 채널 상에서 이루어지므로 2.2절에서 설명한 공격들에 노출되어 있다. 또한, 주로 물류 시스템에서 사용되는 저가의 RFID 시스템의 경우에는 태그의 가격 제한으로 인해 안전한 통신을 위한 암호화 기법을 적용하기가 어렵다는 문제가 존재한다. 이러한 문제를 해결하기 위해 그동안 다양한 보안 기법들이 연구되었다.

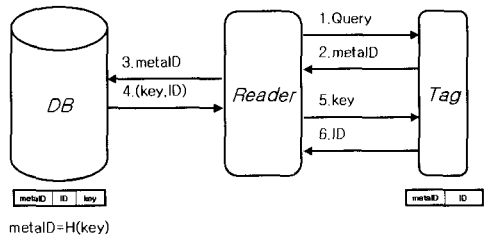
RFID 시스템의 물리적 보안 기법으로는 킬 명령어 기법[1], 패러데이 케이지(Faraday cage) 기법[9], 액티브 재밍(Active Jamming) 기법[6], 블로커 태그 기법[6] 등이 제안되었다. 그러나 물리적으로 RFID 시스템을 보호하는 기법들은 <표 1>에서 나타내고 있는 것과 같이 추가적인 장치가 필요하거나 보호 장치의 형태에 제한이 있고, 법적인 문제가 존재한다. 그러므로 현재 RFID 시스템에서는 암호학적인 방법을 이용한 인증 기법을 주로 연구하고 있으며, 현재까지 해쉬-락 기법[1, 2, 3, 4], 확장된 해쉬-락 기법[1, 4], 외부 재 암호화 기법[5], 해쉬-체인 기법[7], 해쉬 기반 ID 변형 기법[8], 개선된 해쉬 기반 ID 변형 기법[10] 등이 제안되었다. 그러나 지금까지 제안된 RFID 인증 기법들은 재전송 공격에 취약하거나, 위치정보를 노출시키는 등 많은 문제점을 가지고 있다. 본 장에서는 기존의 RFID 인증 기법들의 문제점에 대하여 분석한다.

〈표 1〉 RFID 시스템에서 물리적 보안 기법들의 문제점

보안 기법	문 제 점
킬 명령어 기법	• 태그의 재사용 불가능 • 'Kill' 명령 이행 검증의 어려움
패러데이 케이지 기법	• 'Faraday cage'의 형태가 제한적
액티브 재밍 기법	• 합법적 동작까지 방해하는 법적 문제 존재
블로커 태그 기법	• 별도의 블로커 태그 필요

3.1 해쉬-락 기법의 문제점

해쉬-락 기법[1, 2, 3, 4]의 경우 실제 ID의 노출을 방지하기 위하여 metaID를 이용하지만 metaID는 고정되어있기 때문에 공격자가 태그를 추적할 수 있고, 재전송 공격에 취약하다. 그리고 공격자가 정당한 리더로 가장하여 태그로부터 metaID를 수신하고, 이 metaID를 이용하여 태그로 가장해서 리더로부터 key를 획득하는 경우, 공격자는 다시 리더로 가장하여 태그로부터 ID를 알아낼 수 있다. 결국, 공격자는 metaID, key, ID를 모두 획득하게 되므로 정당한 태그로 완벽하게 가장할 수 있는 스푸핑 공격이 가능하다[1]. (그림 2)는 해쉬-락 기법의 동작과정을 나타낸 것이다.



(그림 2) 해쉬-락 기법

3.2 확장된 해쉬-락 기법의 문제점

확장된 해쉬-락 기법[1, 4]은 태그가 난수를 생성하여 매 세션마다 다른 응답을 리더에게 전송하는 방법을 이용한다. 그러나 ID_k를 불안전한 채널을 통해 전송하므로 여전히 위치 추적이 가능하며, 리더의 공격자가 질의에 대한 응답 R, $H(ID_k||R)$을 도청하여 재전송하는 경우 정당한 태그로 완벽하게 가장할 수 있으므로 재전송 공격에도 취약하다. 또한 공격자가 정당한 리더로 가장하여 태그로부터 R, $H(ID_k||R)$를 획득하는 경우 공격자는 리더의 질의에 대하여 이전에 획득한 R, $H(ID_k||R)$를 응답으로 전송하여 정당한 태그로 가장할 수 있다. (그림 3)은 확장된 해쉬-락 기법의 동작과정을 나타낸 것이다.

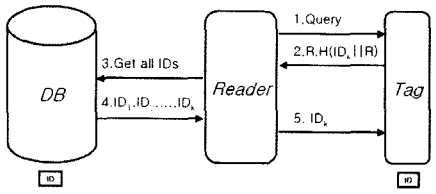
3.3 외부 재 암호화 기법의 문제점

외부 재 암호화 기법[5]은 공개키 암호화 기법을 이용하여 태그의 ID를 보호하기 때문에 이론적으로는 이전의 기법들보다 안전하지만, 공개키 암호화가 많은 연산량을 요구하기 때문에 태그의 자체적인 연산이 불가능하여 리더와 같은 외부 장치에 의해 공개키 암호화가 수행된다. 이 기법에서

는 암호화된 태그의 ID는 고정되어 있으므로 각 태그의 데이터는 자주 다시 기록되어야 한다는 문제점이 존재한다. 또한 재 암호화를 위한 외부 장치와 사용자의 행위가 필요하므로 유비쿼터스 환경에는 적합하지 않다.

3.4 해쉬-체인 기법의 문제점

두 개의 서로 다른 해쉬 함수를 이용하는 해쉬-체인 기법[7]은 리더의 질의에 대하여 항상 다른 응답을 하므로 공격자가 태그의 응답 $a_{t,i}$를 알고 있다고 하더라도 어떤 태그가 응답하였는지 알 수 없으며, 서로 다른 응답에 대해서 동일한 태그의 응답이라는 것도 알 수 없다. 그러나 공격자가 $a_{t,i}$를 재전송하는 경우 정당한 태그로 가장할 수 있으므로 해쉬-체인 기법은 재전송 공격과 스푸핑 공격에 취약하다. 또한 해쉬-체인 기법은 백-엔드 데이터베이스가 태그를 인증하려면 모든 태그에 대하여 해쉬 함수 연산을 i번 수행해야하므로 지나친 연산량 부담이 있으며, 태그가 2개의 서로 다른 해쉬 함수를 내장하고 있어야 하므로 태그의 가격이 상승한다. (그림 4)는 해쉬-체인 기법의 동작과정을 나타낸 것이다.



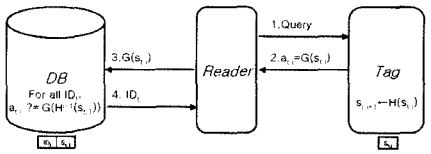
(그림 3) 확장된 해쉬-락 기법

3.5 해쉬 기반 ID 변형 기법의 문제점

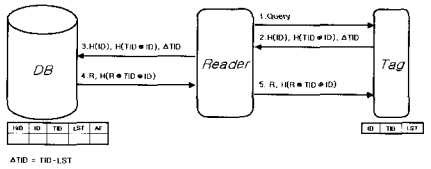
해쉬 기반 ID 변형 기법[8]은 해쉬-체인 기법과 유사하게 태그의 인증 정보인 ID를 매 세션마다 바꾸는 기법이다. 매 세션마다 태그의 ID가 난수 R에 의해 갱신되고, TID와 LST가 갱신되므로 공격자의 재전송 공격으로부터 안전하다. 그러나 공격자가 정당한 리더로 가장하여 태그로부터 H(ID), H(TID⊕ID), △TID를 획득하고, 정당한 태그가 다음 인증 세션을 수행하기 전에 이 정보들을 리더의 질의에 대한 응답으로 이용하면 공격자는 정당한 태그로 인증 받을 수 있다[10]. 그리고 공격자가 정당한 리더로 가장하여 H(ID), H(TID⊕ID), △TID를 획득하고 (그림 5)의 5번 과정에서 전송되는 정보를 태그에게 전송하지 않으면, 태그는 (그림 5)의 5번 과정의 정보가 유실되었다고 여겨 ID를 변형하지 않는다. 이 경우 공격자가 여러 개의 리더를 곳곳에 설치해두고 있다면 태그가 정당한 리더와 인증 세션을 수행하여 H(ID)가 갱신되기 전까지 H(ID)를 통해 태그의 위치를 추적할 수 있다. 또한 해쉬 기반 ID 변형 기법은 ID가 인증 세션마다 바뀌므로 변형되는 ID를 저장하고 있는 유일한 데이터베이스가 존재해야만 한다. 그러나 데이터베이스가 하나만 존재하는 경우 수많은 태그를 인증하기 위해서는 데이터베이스가 매우 많은 연산을 수행해야하며, 다양한 서비스 제공에 어려움이 생기게 된다. (그림 5)는 해쉬 기반 ID 변형 기법의 동작과정을 나타낸 것이다.

3.6 개선된 해쉬 기반 ID 변형 기법의 문제점

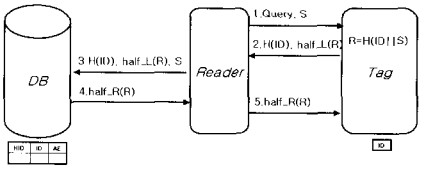
황영주 등은 스푸핑 공격에 취약한 해쉬 기반 ID 변형 기법을 개선한 RFID 인증 기법을 제안하였다[10]. 그러나 이 기법도 해쉬 기반 ID 변형 기법과 동일하게 인증 세션이 완전하게 종료된 이후에나 ID가 갱신되기 때문에 여러 개의 리더를 곳곳에 설치해놓은 공격자가 정당한 리더로 가장하여 H(ID), half_L(R)을 획득하고 half_R(R)은 전송하지 않는다면 공격자는 태그가 정당한 리더와 인증 세션을 수행하여 H(ID)가 갱신되기 전까지 H(ID)를 통해 태그의 위치를 추적할 수 있다. 그리고 이 기법도 변형되는 ID를 저장하고 있는 유일한 데이터베이스가 존재해야만 한다. (그림 6)은 개선된 해쉬 기반 ID 변형 기법의 동작과정을 나타낸 것이다.



(그림 4) 해쉬-체인 기법



(그림 5) 해쉬 기반 ID 변형 기법



(그림 6) 개선된 해쉬 기반 ID 변형 기법

다음 <표 2>는 기존 인증 기법들의 문제점을 정리한 것이다.

〈표 2〉 기존 인증 기법들의 문제점

보안 기법	문제점
해쉬-락 기법	• 위치정보 노출 • 재전송 공격 가능 • 스푸핑 공격 가능
확장된 해쉬-락 기법	• 재전송 공격 가능 • 스푸핑 공격 가능
외부 재 암호화 기법	• 외부 장치 필요
해쉬-체인 기법	• 서로 다른 해쉬 함수 사용으로 인한 태그 가격 상승 • 백-엔드 데이터베이스의 많은 계산량 요구
해쉬 기반 ID 변형 기법	• 스푸핑 공격 가능 • 위치정보 노출 • 태그의 변형되는 인증 정보를 소유한 유일한 데이터베이스 가정
개선된 해쉬 기반 ID 변형 기법	• 위치정보 노출 • 태그의 변형되는 인증 정보를 소유한 유일한 데이터베이스 가정

4. 제안 프로토콜

본 논문에서 제안하는 프로토콜은 기본적으로 Challenge-Response 방식을 이용하고 있다. 리더가 처음 태그에게 질의를 할 때 난수를 함께 전송하고, 태그는 리더로부터 수신한 난수와 자신이 생성한 난수를 이용하여 응답함으로써 기존 프로토콜들에서 문제점으로 지적되었던 재전송 공격과 스푸핑 공격에 대하여 안전하다. 그리고 저장되어 있는 ID를 변형하지 않으므로 해쉬 기반 ID 변형 기법과는 달리 데이터베이스들이 분산되어있는 유비쿼터스 환경에 적용이 가능하다는 장점을 가지고 있다.

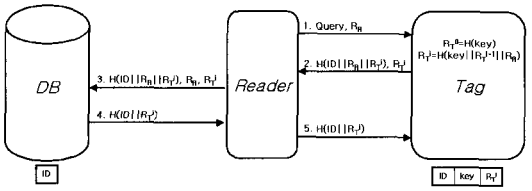
4.1 구조

제안 프로토콜에서 백-엔드 데이터베이스는 태그의 ID와 관련 데이터를 저장하고 있으며, 해쉬 함수 연산만을 이용하여 태그를 인증한다. 리더는 난수를 생성하는 것 이외의 연산이 필요하지 않으며, 태그와 백-엔드 데이터베이스 사이에서 전송되는 정보를 저장하기 위한 임시적인 메모리만이 요구된다.

제안 프로토콜에서 사용되는 파라미터는 다음과 같으며, (그림 7)는 제안하는 프로토콜의 기본 구조를 나타낸 것이다.

〔파라미터〕

- *Query* : 질의. 태그의 응답을 요청.
- *ID* : 태그 고유의 비밀 인증 정보. j 비트.
- *key* : 난수 생성을 위한 비밀정보. j 비트.
- $H(\ )$: 일방향 해쉬 함수. $H : \{0, 1\}^* \rightarrow \{0, 1\}^j$.
- R_R : 리더가 매 세션마다 생성하여 태그에게 전송하는 난수. n 비트.
- R_T : 태그가 생성하는 난수. 태그가 *key*와 이전 세션에서 생성한 난수와 R_R를 연접한 후 해쉬 함수 연산을 수행하여 생성. m 비트.
- $\|$: 연접(Concatenate function).



(그림 7) 제안 프로토콜의 기본 구조

4.2 인증 과정

- (Step 1 : 리더)
  리더는 태그들에게 *Query*와 난수 R_R를 함께 브로드캐스팅한다.
  리더 → 태그 : *Query*, R_R
- (Step 2 : 태그)
  태그는 자신이 생성한 난수 R_T^i를 R_R, *ID*와 연접한 후 해쉬하여, R_T^i와 함께 *Query*에 대한 응답으로 리더에게 전송한다.
  태그 → 리더 : $H(ID\|R_R\|R_T^i)$, R_T^i
  그러나, 저가의 태그 IC 칩을 구성하고 있는 게이트의 수는 7.5-15Kgates이고 이 중 암호 기술을 구현하기 위해 사용 가능한 게이트의 수는 2.5-5Kgates로서[11] 태그가 난수생성기를 이용하여 난수 R_T^i를 생성하기에는 태그의 게이트가 매우 부족하다. 그러므로 제안 프로토콜에서 태그는 *key*와 이전 세션에서 태그가 생성한 난수 R_T^{i-1}과 리더로부터 수신한 R_R을 연접한 후 해쉬 함수를 사용하여 새로운 난수 R_T^i를 생성한다. 처음 태그가 생산될 때 R_T^0는 $H(key)$이다.
  태그 : $R_T^0=H(key)$
  $R_T^i=H(key\|R_T^{i-1}\|R_R)$
- (Step 3 : 리더)
  리더는 R_R과 태그로부터 수신한 $H(ID\|R_R\|R_T^i)$, R_T^i를 백-엔드 데이터베이스로 전송한다.
  리더→백-엔드 데이터베이스 : $H(ID\|R_R\|R_T^i)$, R_R, R_T^i
- (Step 4 : 백-엔드 데이터베이스)
  백-엔드 데이터베이스에 저장된 모든 *ID*를 R_R, R_T^i와 연접하여 해쉬한 값과 리더로부터 수신한 $H(ID\|R_R\|R_T^i)$를 비교하여 태그를 인증한다.
  백-엔드 데이터베이스 :
  $$\text{계산된 } H(ID\|R_R\|R_T^i) \stackrel{?}{=} \text{수신한 } H(ID\|R_R\|R_T^i)$$
  인증이 성공하면 $H(ID\|R_T^i)$를 리더에게 전송한다.
  백-엔드 데이터베이스 → 리더 : $H(ID\|R_T^i)$
- (Step 5 : 리더, 태그)
  리더는 백-엔드 데이터베이스로부터 수신한 $H(ID\|R_T^i)$를 태그에게 전송한다.
  리더 → 태그 : $H(ID\|R_T^i)$
  태그는 자신의 *ID*와 인증 세션에서 생성한 R_T^i를 연접하여 해쉬한 값과 $H(ID\|R_T^i)$를 비교하여 백-엔드 데이터베이스를 인증하고 인증 세션은 성공적으로 종료된다.
  $$\text{태그 : 계산된 } H(ID\|R_T^i) \stackrel{?}{=} \text{수신한 } H(ID\|R_T^i)$$

4.3 제안하는 프로토콜의 안전성

기존의 인증 프로토콜들은 재전송 공격, 스푸핑 공격에 취약하였으며, 또한 공격자에 의한 추적이 가능하였다. 그러나 제안하는 프로토콜은 태그가 리더로부터 수신한 난수를 이용하여 세션마다 다른 응답을 하기 때문에 재전송 공격과 스푸핑 공격에 대하여 안전하며, 공격자에 의한 추적도 방지할 수 있다.

본 절에서는, 2.2절에서 설명한 공격자들의 공격에 대하여 제안 프로토콜이 어떻게 안전한가를 분석한다.

4.3.1 스푸핑 공격에 대한 안전성

공격자가 정당한 리더로 가장하여 *Query*와 함께 태그에게 난수 R_R'를 전송한다면, 태그로부터 $H(ID\|R_R'\|R_T^i)$, R_T^i를 획득할 수 있다. 그러나 다음 세션에서 정당한 리더가 *Query*,

R_R를 전송하는 경우 정당한 태그로 가장한 공격자는 $H(ID\|R_R\|R_T^i)$, R_T^i를 응답으로 전송해야하므로 태그로부터 획득한 정보 $H(ID\|R_R'\|R_T^i)$, R_T^i로는 스푸핑 공격이 불가능하다.

4.3.2 재전송 공격에 대한 안전성

정당한 리더가 *Query*와 함께 전송하는 난수 R_R는 매 세션마다 변하기 때문에 태그의 응답 $H(ID\|R_R\|R_T^i)$, R_T^i도 매 세션마다 바뀌어야 한다. 결국, 공격자는 도청으로 획득한 $H(ID\|R_R\|R_T^i)$, R_T^i를 다음 세션에서는 응답으로 사용할 수 없으므로 제안하는 프로토콜은 재전송 공격에 안전하다. 또한 프로토콜에서 공격자는 태그의 ID를 알 수 없으므로 매 세션마다 변하는 R_R에 대하여 정당한 응답 $H(ID\|R_R\|R_T^i)$를 생성하는 것은 계산상 불가능하다.

4.3.3 트래픽 분석과 위치 추적에 대한 안전성

공격자가 정당한 리더로 가장하여 지속적으로 고정된 R_R를 태그에게 전송하여도 태그는 난수 R_T^{i-1}과 공격자는 알 수 없는 ID를 이용하여 매 세션마다 변하는 응답 $H(ID\|R_R\|R_T^i)$를 전송하므로 공격자는 서로 다른 응답이 동일한 태그에 의한 것인지를 판별할 수 없다. 또한 공격자는 *key*값을 모르기 때문에 R_R, R_T^{i-1}를 도청하여도 다음 세션의 난수 $R_T^i=H(key\|R_T^{i-1}\|R_R)$가 어떤 태그에 의해 생성된 것인지 알 수 없다. 그러므로 공격자는 트래픽 분석이 불가능하고 태그의 위치도 추적할 수 없다.

4.4.4 정보 전송 방해에 대한 안전성

제안하는 프로토콜은 상호 인증을 제공하므로 정보 전송 방해 공격을 탐지할 수 있으며, 태그의 인증 정보 ID는 고정되어 있으므로 세션마다 ID가 변하는 해쉬 기반 ID 변형 프로토콜에서 발생 가능한 데이터베이스의 정보 유실은 일어나지 않는다.

<표 3>은 제안 프로토콜의 안전성을 기존의 RFID 인증 기법과 비교하여 나타낸 것이다. <표 3>에서 프로토콜이 위치 정보 노출에 대하여 '익명성(약)'을 보장한다는 것은 리더의 질의에 대한 태그의 응답으로부터 공격자가 태그의 실제 ID는 알 수 없으나, 하나의 태그가 각각의 인증 세션에서 서로 다른 응답을 하더라도 이러한 서로 다른 응답이 동일한 태그에 의한 것임은 알 수 있는 경우이다. 그러므로 프로토콜이 위치 정보 노출에 대하여 '익명성(약)'을 보장하지 않는 경우, 공격자는 태그의 실제 ID와 태그가 각각의 인증 세션에서 서로 다른 응답을 하더라도 이 응답들이 동일한 태그에 의한 것임을 알 수 있다. 반면, 프로토콜이 위치 정보 노출에 대하여 '익명성(강)'을 보장한다는 것은 리더의 질의에 대한 태그의 응답으로부터 공격자가 태그의 실제 ID는 물론 태그가 각각의 인증 세션에서 서로 다른 응답을 하는 경우 이러한 서로 다른 응답이 동일한 태그에 의한 것인지도 판별할 수 없는 경우이다. 그러므로 프로토콜이 위치 정보 노출에 대하여 '익명성(강)'을 보장하지 않는 경우, 공격자는 태그의 실제 ID는 알 수 없지만 태그가 각각의 인증 세션에서 서로 다른 응답을 하는 경우 이러한 서로 다른 응답이 동일한 태그에 의한 것임은 알 수 있다.

또한 인증 세션마다 태그의 인증 정보가 변형되는 해쉬 기반 ID 변형 기법과 개선된 해쉬 기반 ID 변형 기법을 제외한 나머지 기법들은 데이터베이스 내의 인증 정보가 고정되어 있으므로 정보 전송 방해 공격에 따른 데이터베이스의 정보 유실에 대하여 안전하다.

〈표 3〉 기존 기법들과 제안 프로토콜과의 안전성 비교

		해쉬-락 기법	확장된 해쉬-락 기법	해쉬-체인 기법	해쉬 기반 ID 변형 기법	개선된 해쉬 기반 ID 변형 기법	제안 프로토콜
스푸핑 공격		×	×	×	×	○	○
재전송 공격		×	×	×	○	○	○
트래픽 분석 공격		×	×	○	○	○	○
위치 정보 노출	익명성(약)	×	×	○	○	○	○
	익명성(강)	×	×	○	×	×	○
정보 전송 방해 공격		○	○	○	○	○	○

○ : 안전, × : 취약

제안하는 프로토콜은 (1)~(4)의 공격에 대하여 안전하므로 도청자, 능동적 공격자, 추적자, 방해자에 대해서 안전하다.

4.4 제안하는 프로토콜의 효율성

제안 프로토콜에서 태그는 해쉬 함수 연산만을 수행하므로 저가의 태그에서 구현하기에 적합하며, 인증 세션 동안 3회의 해쉬 함수 연산을 수행하므로 연산 부담도 크지 않다. 그리고 태그에 비해 상대적으로 연산 능력이 충분한 리더는 1회의 난수 생성 연산만을 수행하므로 쉽게 구현이 가능하다. 또한 백-엔드 데이터베이스는 태그를 인증하기 위해 백-엔드 데이터베이스에 저장된 모든 태그의 ID에 대하여 각각 1회의 해쉬 함수 연산을 수행해야하므로 태그 인증 과정에서 평균적으로 $\frac{\text{태그 } ID\text{의 수}}{2}$ 회의 해쉬 함수 연산을 수행하고, 태그가 백-엔드 데이터베이스를 인증할 수 있는 인증 정보 생성을 위해 1회의 추가적인 해쉬 연산을 수행한다. 이를 종합하면 백-엔드 데이터베이스는 평균적으로 $\frac{\text{태그 } ID\text{의 수}}{2}$ + 1 회의 해쉬 함수 연산을 인증 세션마다 수행하므로 백-엔드 데이터베이스의 연산 부담은 적다. 실제로 해쉬 함수 MD5는 소프트웨어적으로 구현할 경우 Intel의 90Mhz Pentium 프로세서에서 32.5Mb/s의 연산이 가능하고[12], 하드웨어적으로 구현할 경우 CAST Inc.의 제품의 경우 307Mb/s의 연산이 가능하므로[13] 백-엔드 데이터베이스는 태그의 수가 많더라고 고속으로 태그 인증을 수행할 수 있다.

인증 세션에서 요구되는 정보를 저장하기 위한 메모리량으로는 해쉬 함수 연산의 결과가 $m = n = j$ 라 가정한다면,

태그는 *ID, key*를 저장하기 위한 $2j$비트와 이전 세션에서 생성한 난수 R_T^{i-1}를 저장하기 위한 j비트의 고정된 메모리가 필요하다. 그리고 백-엔드 데이터베이스는 각 태그의 *ID*를 저장하기 위해 태그 1개 당 j비트의 메모리가 필요하다.

제안 프로토콜의 효율성을 기존의 RFID 인증 기법들과 비교하여 <표 4>에 정리하였다. 제안 프로토콜의 효율성을 기존의 RFID 인증 기법들과 객관적으로 비교하기 위하여 태그 인증에 사용되는 비밀 정보 ID, $S_{t,i}$, key는 모두 j비트라 가정하고 일방향 해쉬 함수는 $H : \{0, 1\}^* \rightarrow \{0, 1\}^j$라 가정한다. 또한 해쉬 기반 ID 변형 기법에서 TID와 LST는 각각 $\frac{1}{2}j$라 가정한다.

〈표 4〉 기존 기법들과 제안 프로토콜과의 효율성 비교

	메모리(비트)		연산량(회)			분산 데이터베이스 환경에의 적용 가능성
	태그	데이터베이스	태그	리더	데이터베이스	
해쉬-락 기법	2j	4j	해쉬 함수 : 1	-	-	○
확장된 해쉬-락 기법	j	j	난수 생성 : 1 해쉬 함수 : 1	해쉬 함수 : (태그의 수/2)	-	○
해쉬-체인 기법	j	2j	해쉬 함수 : 2	-	해쉬 함수 : (태그의 수/2) × i	○
해쉬 기반 ID 변형 기법	3j	8j	해쉬 함수 : 3	-	난수 생성 : 1 해쉬 함수 : 3	×
개선된 해쉬 기반 ID 변형 기법	j	6j	해쉬 함수 : 2	난수 생성 : 1	해쉬 함수 : 2	×
제안 프로토콜	3j	j	해쉬 함수 : 3	난수 생성 : 1	해쉬 함수 : (태그의 수/2) + 1	○

제안하는 프로토콜은 메시지 유실 방지를 위해 태그 1개당 2개의 행을 가지고 있는 해쉬 기반 ID 변형 기법과는 달리 태그의 ID가 고정되어 있기 때문에 데이터베이스는 태그 1개당 1개의 행만이 필요하다. 그러므로 데이터베이스의 총 정보량은 해쉬 기반 ID 변형 기법보다 매우 작다. 또한 제안 프로토콜은 변형되는 ID를 저장하고 있는 유일한 데이터베이스의 존재를 가정하고 있는 해쉬 기반 ID 변형 기법이나 개선된 해쉬 기반 ID 변형 기법과는 달리 분산된 데이터베이스가 존재하는 유비쿼터스 환경에도 적용할 수 있다는 장점이 있다.

예를 들어, 가전제품매장에서 TV를 구입한다고 가정하면, TV의 가격을 조회하여 대금을 지불하기 위해서 TV에 부착된 태그를 읽고 가전 매장의 판매정보 데이터베이스에 접속해야할 것이다. 그리고 구입한 TV가 고장 난 경우 AS센터에서는 TV의 AS기록을 조회하고 수리비용을 청구하기 위해 제조사의 AS 데이터베이스에 접속해야 할 것이다. 제안 프로토콜의 경우 태그의 인증 정보인 ID는 고정되어 있으므로 이러한 분산 데이터베이스 환경에 적용하기 쉽다. 그러나 ID가 지속적으로 갱신되는 해쉬 기반 ID 변형 기법이나 개선된 해쉬 기반 ID 변형 기법은 변형되는 ID를 저장하고 있는 유일한 데이터베이스가 존재해야 한다. 그러므로 실제 다양한 서비스를 제공하기 어려우며, 단일 인증 세션에서 적은 데이터베이스 연산량에도 불구하고 모든 태그에 대하여 데이터베이스가 유일하므로 실제로 수많은 태그의 다양한 서비스를 처리하기 위해서는 막대한 연산이 불가피하다.

5. 결 론

RFID 시스템은 유비쿼터스 컴퓨팅 환경을 실현시킬 수 있는 기술로 많은 연구가 진행되고 있다. 그러나 RFID 시스템의 자동 인식 특징은 생활의 편리함 뿐만 아니라 다양한 프라이버시 침해 문제도 발생시킬 수 있다. 이러한 문제를 해결하기 위해 지금까지 사용자의 프라이버시를 보호할 수 있는 방법에 대한 연구가 진행되어 왔으나 기존에 제안된 여러 보안 기법들은 여전히 안전성에 문제점을 가지고 있으며 실제 유비쿼터스 환경에 적용하기에는 많은 문제점들을 가지고 있다.

본 논문에서는 태그가 리더로부터 수신한 난수로부터 새로운 난수를 생성하여 매 세션마다 다른 응답을 전송할 수 있도록 함으로써 공격자의 재전송 공격, 스푸핑 공격, 위치 추적 등에 안전한 인증 프로토콜을 제안하였다.

제안하는 프로토콜은 안전성과 효율성뿐만 아니라 분산 데이터베이스 환경을 고려하고 있으므로 유비쿼터스 컴퓨팅 환경 실현을 위해 다양하게 활용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] S. A. Weis, S. 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, Springer-Verlag Heidelberg, 2004.

[2] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID Systems and Security and Privacy Implications", CHES 2002, LNCS 2523, pp.454-469, Springer-Verlag Heidelberg, 2003.

[3] S. E. Sarma, S. A. Weis, D. W. Engels. "RFID systems, Security & Privacy Implications", White Paper MIT-AUTOID-WH-014, MIT AUTO-ID CENTER, 2002.

[4] S. A. Weis, "Security an Privacy in Radio-Frequency Identification Devices" MS Thesis. MIT. May, 2003.

[5] A. Juels, R. Pappu, "Squealing Euros : Privacy protection in RFID-enabled banknotes", Financial Cryptography'03, LNCS 2742, pp.103-121, Springer-Verlag Heidelberg, 2003.

[6] A. Juels, R. L. Rivest, M Szydlo, "The Blocker Tag : Selective Blocking of RFID Tags for consumer Privacy",

Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp.103-111, ACM Press, 2003.

[7] 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.

[8] D. Henrici, and P. Müller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", Procedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops(PERCOMW'04), pp.149-153, IEEE, 2004.

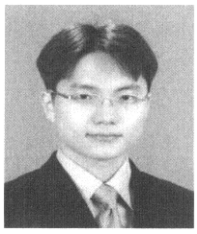
[9] mCloak : Personal/corporate management of wireless devices and technology, 2003. http://www.mobilecloak. com.

[10] 황영주, 이수미, 이동훈, 임종인, "유비쿼터스 환경의 Low-Cost RFID 인증 프로토콜", 한국정보보호학회 하계정보보호학술대회 논문집 Vol.14, No.1, pp.109-114, 2004.

[11] S. E. Sarma, S. A. Weis, and D. W. Engels, "Radio-Frequency Identification : Secure Risks and Challenges", RSA Laboratories Cryptobytes, Vol.6, No.1, pp.2-9, Spring 2003.

[12] J. D. Touch, "Performance Analysis of MD5", Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication, (SIGCOMM'95), pp.77-86, ACM Press, 1995.

[13] M. Y. Wang, C. P. Su, C. T. Huang, and C. W. Wu, "An HMAC processor with integrated SHA-1 and MD5 algorithms", Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair 2004, pp.456-458, IEEE Press, 2004.

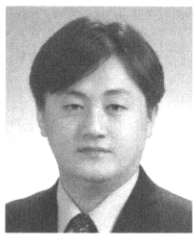


이 근 우

e-mail : kwrhee@dosan.skku.ac.kr
2004년 성균관대학교 정보통신공학부(학사)
2004년~현재 성균관대학교 대학원 컴퓨터공학과 석사과정
관심분야 : 유비쿼터스 센서네트워크 보안, RFID 보안

오 동 규

e-mail : dkoh@dosan.skku.ac.kr
2003년 성균관대학교 정보통신공학부(학사)
2003년~현재 성균관대학교 대학원 컴퓨터공학과 석사과정
관심분야 : RFID 보안



곽 진

e-mail : jkwak@dosan.skku.ac.kr
2000년 성균관대학교 생물기전공학과(학사)
2003년 성균관대학교 대학원 전기전자및컴퓨터공학부 컴퓨터공학전공(석사)
2003년~현재 성균관대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 암호 알고리즘/프로토콜, 유비쿼터스 보안

오 수 현

e-mail : shoh@office.hoseo.ac.kr
1998년 성균관대학교 정보공학과(학사)
2000년 성균관대학교 대학원 전기전자및컴퓨터공학부 컴퓨터공학전공(석사)
2003년 성균관대학교 대학원 전기전자및컴퓨터공학부 컴퓨터공학전공(박사)
2004년~현재 호서대학교 컴퓨터공학부 정보보호전공 전임강사
리즘/프로토콜, 유비쿼터스 보안

김 승 주

e-mail : skim@ece.skku.ac.kr
1994년 성균관대학교 정보공학과(학사)
1996년 성균관대학교 대학원 정보공학과(석사)
1999년 성균관대학교 대학원 정보공학과(박사)
1998년~2004년 한국정보보호진흥원(KISA) 팀장
2001년~현재 한국정보보호학회 논문지편집 위원
2002년~현재 한국정보통신기술협회(TTA) IT국제표준화 전문가
2004년~현재 성균관대학교 정보통신공학부 조교수
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호

e-mail : dhwon@dosan.skku.ac.kr
성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1985년~1986년 일본 동경공업대 객원연구원
1988년~2003년 성균관대학교 교학처장, 전기전자및컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장, 한국정보보호학회장
1996년~1998년 국무총리실 정보화추진위원회 자문위원
현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정통부지정 정보보호인증기술연구센터장
관심분야 : 암호이론, 정보이론, 정보보호이론