JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 2 : 357~364 Feb. 2015

안전한 RFID 환경을 위한 태그-리더 상호 인증 프로토콜

이영석[1*] · 최훈[2]

Tag-Reader Mutual Authentication Protocol for secure RFID environments

Young-seok Lee[1*] · Hoon Choi[2]

[1*]Department of Information Communication Engineering, Kunsan National University, Kunsan 573-701,Korea
[2]Department of Computer Science & Engineering, Chungnam National University, Daejeon 305-764, Korea

요 약

RFID 환경에서는 태그-리더 사이에 무선으로 데이터를 송수신하기 때문에, 공격자가 물리적인 제약없이 네트워크에 참가할 수 있어 도청 및 데이터 위·변조와 같은 다양한 공격 기법에 쉽게 노출될 수 있다. 또한, RFID 태그의 자원 제약성이 높아 외부 공격에 방어하기 위한 보안 기술을 적용하는 것이 쉽지 않다. 본 논문에서는 스푸핑 공격, 재전송 공격, 트래픽 분석 공격, 위치 트래킹 공격과 같은 외부 사이버 공격에 대해 안전하게 RFID 태그 정보를 보호하고, 다양한 외부 공격에 견딜 수 있는 새로운 태그-리더 상호 인증 프로토콜을 제안한다. 제안된 상호 인증 프로토콜의 성능 평가를 수행하고 시뮬레이션 결과를 제시한다.

ABSTRACT

Tags and Readers is receiving and sending the data using the wireless communication in the RFID environment. Therefore, it could allow an attacker to participate in the network without the physical constraints, which can be easily exposed to a variety of attacks, such as taps and data forgery. Also, it is not easy to apply the security techniques to defend external attacks because the resource constraints of RFID tags is high . In this paper, new tag-reader mutual authentication protocol is proposed to protect the external cyber attacks such as spoofing attacks, replay attacks, traffic analysis attacks, location tracking attacks. The performance evaluation of the proposed mutual authentication protocol is performed and the simulation results are presented..

키워드 : RFID, 태그, 리더, 상호 인증, 프로토콜

Key word : RFID, Tag, Reader, Mutual Authentication, Protocol

접수일자 : 2014. 11. 03 심사완료일자 : 2014. 12. 11 게재확정일자 : 2014. 12. 26

*** Corresponding Author** Young-seok Lee(E-mail:leeys@kunsan.ac.kr,Tel+82-63-469-4695
Department of Information Communication Engineering,Kunsan National University, Kunsan, 573-701 Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.2.357 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

RFID는 유비쿼터스 컴퓨팅(ubiquitous computing)의 실현을 위한 매우 중요한 기술 중 하나로 모든 개체에 마이크로 칩을 내장한 태그(tag)를 부착하고, 일정한 주파수 대역을 이용해 무선 통신으로 개체의 정보를 리더(reader)에서 자동으로 인식하고 감지하는 기술이다. 또한 단거리 무선 통신 기술 중에서 정보기술과 자동인식 및 데이터 획득 분야에서 빠른 성장세를 보이고 있으며, 출입 통제를 비롯한 출퇴근 관리, 물류 관리 및 주차 관리, 홈 오토메이션 등 산업 분야에서 새로운 대체 기술로서 주목을 받고 있다. 그러나, 무선 통신 채널을 이용하여 인증 절차를 거쳐야 하는 RFID 시스템의 특성으로 인해 상호 인증 과정에서 도청(eavesdropping attack), 스푸핑 공격(spoofing attack), 재전송 공격(replay attack), 서비스 거부 공격(denial of service attack), 위치 트래킹 공격(location tracking attack) 등 악의적인 위협요소들에 쉽게 노출될 수 있는 취약점을 포함하고 있다[1].

이와 같은 RFID 기술의 취약점들은 개인이나 조직의 보안과 프라이버시 보호에 심각한 문제를 발생시킬 수 있다. 따라서 태그와 리더의 정보를 저장하고 관리하는 백-엔드 데이터베이스(back-end database) 사이에 안전성을 보장할 수 있는 상호 인증기술이 중요하게 다루어지고 있으며, 최근 들어 RFID 시스템의 보안 취약성을 해결하기 위한 많은 연구가 수행되고 있다[2-4].

RFID 시스템은 그림 1에서 보듯이 리더(Reader), 태그(Tag) 그리고 백-엔드 데이터베이스(Back-end Database)의 3가지 구성 요소로 이루어 져있다.

그림 1. RFID 시스템 구성
Fig. 1 RFID System Architecture

리더와 백-엔드 데이터베이스의 연산 능력에 비해 RFID 태그는 연산 능력이 떨어지며, 객체를 유일하게 식별하기 위한 정보만을 가지며, 정보 노출, 위치 추적 등으로 인한 개인의 프라이버시(Privacy) 침해를 유발할 수 있는 문제점을 지니고 있다. 현재 RFID/USN 환경에서 발생할 수 있는 프라이버시 침해 문제를 해결하기 위해 지금까지 많은 연구자들에 의해 해쉬-락 기법, 확장된 해쉬-락 기법, 해쉬-기반 ID 변형 기법, 개선된 해쉬-기반 ID 변형 기법, 블로커 태그를 이용한 기법, 해쉬-체인 기법 등 다양한 RFID 인증 프로토콜(Authentication protocol)들이 최근까지 개발되고 있다[5-7].

하지만 현재까지 제안된 대부분의 RFID 인증 프로토콜들은 태그의 재사용이 불가능하거나, 태그의 위치 추적으로 위치 트래킹 공격이 쉬우며, 재전송 공격이나 스푸핑 공격에 취약하는 등 다양한 보안 취약점과 프라이버시 침해 문제들을 가짐을 많은 연구자들에 의해 발견되고 있다[8,9].

연구 [10]에서는 유비쿼터스 환경을 실현하기 위한 기술 중의 하나인 RFID 시스템에서의 RFID 태그의 특성을 고려한 해쉬 함수와 배타적 논리합(XOR) 연산을 이용한 RFID 인증 프로토콜을 제안하였다. 그렇지만, 스푸핑 공격, 위치 트래킹 공격, 태그 키 유출 공격에 취약하며 태그 익명성(Anonymity)을 제공하지 않고 있다. 연구[11]에서는 태그 키 유출 공격과 스푸핑 공격, 위치 트래킹 공격에 대응하기 위해 개선된 인증 프로토콜을 제안하였다. 그러나 취약점 증명과정에서 태그 키 유출 공격에 대해 모순점이 발견되었고, 개선된 프로토콜도 여전히 스푸핑 공격에 취약하다는 문제점이 있다.

본 논문에서는 기존에 제안된 인증 프로토콜의 문제점을 해결하고 RFID 리더와 태그 사이에 상호인증을 제공하는 새로운 인증 프로토콜을 제안하고 검증한다. 본 논문의 구성은 다음과 같다. 2장에서는 기존 RFID 인증프로토콜에 대해 살펴보고, 3장에서는 본 논문에서 제안한 프로토콜을 기술한다. 4장에서는 기존 인증 프로토콜들과 본 논문에서 제안한 프로토콜의 성능을 메모리 사용량 및 계산량의 관점에서에서 비교한다. 5장에서는 제안된 프로토콜과 기존 프로토콜들의 효율성을 분석하기 위해 시뮬레이션을 수행하고 성능 평가의 결과를 기술한다. 6장에서 결론을 제시한다.

Ⅱ. 관련 연구

2.1. 기존 인증 프로토콜

RFID 백-엔드 데이터베이스와 리더 간에 사전에 안전한 세션키 K_R가 설정되어 있음을 가정하며, 각 태그

의 비밀키 K_T는 백-엔드 데이터베이스에 등록되어 있음을 가정한다. 표 1은 본 논문에서 사용되는 시스템 파라미터를 보여준다. 그림 2는 기존 인증 프로토콜의 구성과 동작 과정을 보여주며, 7단계의 인증 과정이 수행된다[10].

표 1. 프로토콜 파라미터
Table. 1 Protocol parameters

기호	의미
ID_R	리더 식별자
ID_T	태그 식별자
K_R	데이터베이스와 리더간 공유 비밀키
K_T	데이터베이스와 태그간 공유 비밀키
$E_K()$	비밀키 암호
h()	해쉬함수
prng()	의사난수발생기
r	리더가 생성한 난수
t	태그가 생성한 난수
$\otimes$	배타적 논리합(XOR)
$\|\|$	연접 연산

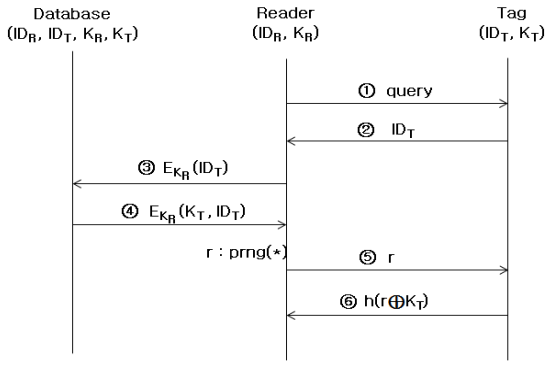

그림 2. 기존 인증 프로토콜
Fig. 2 Existing Authentication Protocol

(1) 리더는 태그에게 query를 전송한다.
(2) 리더로부터 query를 수신한 태그는 자신의 ID_T를 리더에게 전송한다.
(3) 리더는 백-엔드 데이터베이스와 설정된 세션 키 K_R를 사용하여 태그의 ID_T를 암호화하여 E_{KR} (ID_T)를 백-엔드 데이터베이스에게 전송한다.
(4) 백-엔드 데이터베이스는 리더로부터 전송받은 E_{KR} (ID_T)을 세션 키 K_R를 사용하여 복호화 한 후 ID_T태그의 비밀 키 K_T를 세션 키 K_R로 암호화하여 E_{KR} (K_T, ID_T)을 리더에게 전송한다.
(5) 리더는 백-엔드 데이터베이스로부터 수신한 E_{KR} (K_T, ID_T)을 복호화하여 태그의 비밀 키 K_T를 저장하고 태그에게 랜덤 값 r을 전송한다.
(6) 태그는 수신한 랜덤 값 r과 자신의 비밀 키 K_T를 이용하여 $h(r \oplus K_T)$을 계산하여 리더에게 전송한다.
(7) 리더는 $h(r \oplus K_T)$을 계산하여 수신한 $h(r \oplus K_T)$과 동일한지를 비교한다. 만약 두 값이 같으면 태그를 인증하고, 다르면 인증을 중단한다.

기존 인증 프로토콜에서 태그는 리더를 전혀 인증하지 않기 때문에 공격자가 리더로 위장하여 스푸핑 공격을 성공할 수 있다. 또한, 임의의 공격자가 이전 세션의 단계 (2)에서 태그가 전송한 ID_T를 도청하여 소유하고 있다고 가정하자. ID_T는 공개된 통신 채널을 통해 전송됨으로 공격자는 쉽게 획득할 수 있다. 그러면 해당 공격자는 임의의 세션에서 리더로 위장하여 위치 트래킹 공격을 성공할 수 있다. 그리고, 단계 (3)에서 임의의 태그에 대한 비밀 키 K_T를 획득하기 위한 악의적인 목적을 가진 리더가 존재한다고 가정할 때, 해당 리더는 태그 키 유출 공격을 수행하여 태그의 비밀 키 K_T를 획득한 후 해당 태그로의 스푸핑 공격 등을 수행 할 수 있다.

2.2. 개선된 인증 프로토콜

2.1절에서 제시한 인증 기법이 태그 키 유출 공격과 스푸핑 공격, 위치 트래킹 공격에 취약하다는 사실을 증명하고 개선된 인증 프로토콜을 제안하였다[11]. 그러나 취약점 증명과정에서 태그 키 유출 공격에 대해 모순점이 발견되었고, 개선된 프로토콜도 여전히 스푸핑 공격에 취약하다는 문제점이 있다.

개선된 인증 프로토콜과 마찬가지로 RFID 백-엔드 데이터베이스와 리더 간에 사전에 안전한 세션키 K_R가 설정 되어 있음을 가정하며, 각 태그의 비밀 키 K_T는 백-엔드 데이터베이스에 등록되어 있음을 가정한다. 그림 3은 개선된 RFID 인증 프로토콜의 구성과 동작 과정을 보여주며, 다음의 5단계를 거쳐 인증 과정을 수행한다.

(1) 리더는 랜덤 값 r을 생성한 후, 태그에게 ID_R와 함께 r을 전송한다.
(2) 태그는 랜덤 값 t를 생성한 후, 리더로부터 수신한 r과 자신의 ID_T 및 비밀 키 K_T을 이용하여 랜덤 해쉬 값 $h(ID_T || K_T || r || t)$을 계산한 후, $h(ID_T || K_T || r || t)$과 t를 리더에게 전송한다.

(3) 리더는 백-엔드 데이터베이스와 설정된 세션 키 K_R를 사용하여 태그로부터 수신한 $h(ID_T||\ K_T\ ||r||t)$과 t 그리고 자신이 생성한 r을 암호화하여 E_{KR} ($h(ID_T||\ K_T\ ||r||t)$, r, t)를 백-엔드 데이터베이스에게 전송한다.

(4) 백-엔드 데이터베이스는 리더로부터 전송 받은 E_{KR} ($h(ID_T||\ K_T\ ||r||t)$, r, t)을 세션 키 K_R를 사용하여 복호화 한 후, ($h(ID_T||\ K_T\ ||r||t)$, r, t)을 계산하여 자신의 데이터베이스 내에 저장하고 있는 모든 태그 ID와 비밀키 쌍을 이용하여 리더로부터 수신한 ($h(ID_T||\ K_T\ ||r||t)$, r, t)값과 아래와 같은 검증 연산으로 비교하여 일치하는 ID와 키 쌍을 검색한다. 만약 일치하는 값이 검색되지 않으면, 오류 메시지를 리더에게 전송하고, 일치하는 값이 검색되면 태그를 인증하고 리더가 생성한 랜덤 값 r과 함께 세션 키 K_R로 암호화하여 E_{KR} (r)을 리더에게 전송한다.

(5) 리더는 백-엔드 데이터베이스로부터 수신한 값이 오류일 경우, 태그와의 통신을 중단하고, 정상적인 인증이 되었을 경우에서는 백-엔드 데이터베이스로부터 수신한 E_{KR} (r)을 복호화하여 r을 얻는다. 상호 인증을 위해 복호된 r이 자신이 생성한 랜덤 값 r과 동일한지를 검증한다. 만약 동일한 r이 맞으면, 리더는 태그에 관한 원하는 작업을 수행한다.

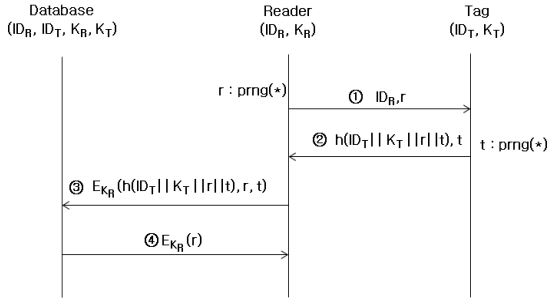

그림 3. 개선된 인증 프로토콜
Fig. 3 Enhanced Authentication Protocol

개선된 인증 프로토콜 역시 태그는 리더에 대한 인증을 하지 않기 때문에 악의적인 리더로의 위장이 가능하다. 만약 읽고 쓰기가 가능한 태그의 경우, 공격자는 악의적인 리더를 이용하여 인증과정을 무시하고 태그에게 직접적으로 요금을 부과하거나 부당한 명령을 전달할 수 있다.

Ⅲ. 상호 인증 프로토콜 설계

3.1. 프로토콜 절차

기존 인증 프로토콜의 문제점을 해결하면서 리더와 태그 사이에 상호 인증을 제공하는 새로운 프로토콜을 제안한다. 태그의 ID와 비밀 키는 안전하게 백-엔드 데이터베이스에 등록되어 있으며, 오직 태그와 데이터베이스만이 알고 있다고 가정한다. 또한 리더와 데이터베이스는 사전에 세션 키를 공유하고 있으며 안전한 통신 채널을 이용한다고 가정한다. 제안하는 상호 인증 프로토콜의 동작과정은 그림 4와 같다. 상호 인증 프로토콜은 6단계의 인증 절차를 포함한다.

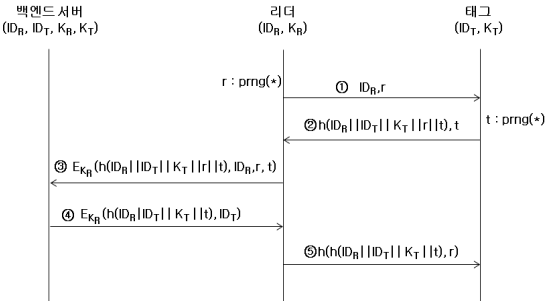

그림 4. 제안된 인증 프로토콜
Fig. 4 Proposed Authentication Protocol

(1) 리더는 랜덤 값 r을 생성한 후, 태그에게 ID_R와 함께 r을 전송한다.

(2) 태그는 난수 t를 생성하여 리더로부터 수신한 난수 r을 사용하여 인증메시지 $h(ID_R||ID_T||\ K_T\ ||r||t)$을 계산하여 t와 함께 리더에게 전송한다.

(3) 리더는 태그로부터 수신한 $h(ID_R||ID_T||\ K_T\ ||r||t)$과 t, 그리고 자신이 생성한 난수 r을 세션 키 K_R를 사용하여 암호화하여 백-엔드 데이터베이스에게 전송한다.

(4) 데이터베이스는 E_{KR} ($h(ID_R||ID_T||\ K_T\ ||r||t)$, ID_R,r, t)를 복호하여 저장된 태그들의 ID를 이용하여 다음을 만족하는 ID_T를 검색한다.

$$h(ID_R||ID_T||\ K_T\ ||r||t)$$

만일 일치되는 값이 없으면 리더에게 인증 실패 메시지를 전송하고, 일치되는 값이 있으면 태그를 인증하고 E_{KR} ($h(ID_R|ID_T||\ K_T\ ||t)$, ID_T)를 생성하여 리더에게 전송한다.

(5) 리더는 데이터베이스로부터 수신한 E_{KR} (h(ID_R||ID_T|| K_T ||t), ID_T)를 복호화하고 태그가 정당함을 인증한 후, h(h(ID_R||ID_T|| K_T ||t), r)를 계산하여 태그에게 전송한다.

(6) 태그는 자신의 비밀 키 K_T를 이용하여 h(h(ID_R||ID_T|| K_T ||t), r)을 계산하여 리더로부터 수신된 값과 일치하는지 확인한다. 일치하는 경우 정당한 리더로 인증하고, 일치하지 않을 경우 통신을 중단한다.

3.2. 안전성 분석

(1) 재전송 공격 : 제안하는 프로토콜에서 사용하는 인증 메시지에는 매 세션마다 리더와 태그가 생성하는 난수를 포함한다. 따라서 공격자가 이러한 인증 메시지를 도청하여 재전송 하는 경우에 백-엔드 데이터베이스에 의해 검출될 수 있다. 따라서 제안한 프로토콜은 재전송 공격에 대해 안전하다.

(2) 스푸핑 공격 : 스푸핑 공격은 태그의 비밀 키를 얻어 태그로 위장하거나 리더와 태그간의 상호인증이 이루어지지 않을 경우 악의적인 리더로 위장하는 것이다. 제안하는 프로토콜에서 전자의 경우, 태그의 비밀 키 k는 안전한 해쉬 함수에 의해 변형된 값으로 전송되므로 태그의 비밀 키는 보호된다. 후자의 경우, ②와 ⑤의 검증을 통해 리더와 태그간 상호인증을 제공하기 때문에 악의적인 리더로의 위장은 불가능하다.

(3) 태그의 익명성 : 제안하는 프로토콜에서 태그의 ID는 백-엔드 데이터 베이스와 태그만이 알고 있으며, 태그의 ID가 전송될 때에도 리더와 태그가 각각 생성한 난수 t, r과 함께 태그의 ID를 해쉬한 결과 값을 전송함으로써 태그의 익명성을 보장할 수 있다.

(4) 악의적인 리더 공모에 의한 위치 트래킹 공격 : 악의적인 리더들의 공모에 의해 태그에 대한 인증 메시지 ②를 획득하더라도 인증 메시지 ②는 태그가 생성한 난수 t로 인해 매 세션마다 변하는 정보이므로, 악의적인 리더들은 두 개의 다른 인증 메시지가 동일한 태그에 대한 인증 메시지인지 확인할 수 없다.

Ⅳ. 성능 분석

본 장에서는 기존에 제안된 인증 프로토콜들과 본 논문에서 제안한 프로토콜의 성능을 메모리 사용량 및 연산량의 관점에서 비교하고, 제안 프로토콜의 효율성에 대해 살펴 본다.

4.1. 메모리 사용량 비교

메모리 사용량에서 태그에 저장해야 하는 저장량을 비교하면, 기존 인증 프로토콜은 태그 ID에 해당하는 정보 t, 태그 비밀 키 k, 태그에서 생성한 해쉬 값 h, 태그에서 발생한 난수 r로 인하여 log(t) + log(k) + log(h) + log(r) = log(tkhr)의 저장량을 필요로 한다. 개선된 인증 프로토콜은 태그 ID에 해당하는 정보 t, 태그 비밀 키 k, 태그에서 생성한 해쉬 값 h, 리더에서 발생한 난수 r, 태그에서 발생한 난수 r로 인하여 log(t) + log(k) + log(h) + log(r) + log(r) = log($tkhr^2$)의 저장량을 필요로 한다. 본 논문에서 제안한 인증 프로토콜은 태그 ID에 해당하는 정보 t, 태그 비밀 키 k, 태그에서 생성한 해쉬 값 h, 리더에서 생성한 해쉬 값 h, 리더에서 발생한 난수 r, 태그에서 발생한 난수 r로 인하여 log(t) + log(k) + log(h) + log(r) + log(h) + log(r) = log(tkh^2r^2)의 저장량을 필요로 한다. 각 방식의 메모리 사용량이 표 2에 보여진다.

표 2. 메모리 사용량 비교
Table. 2 Comparison of Memory Usage

구분	기존인증 프로토콜	개선 프로토콜	제안 프로토콜
태그	log(tkhr)	log($tkhr^2$)	log(tkh^2r^2)
리더	log(ushr)	log($ushr^2$)	log(ush^3r^2)
백엔드 데이터베이스	nlog(tk)+ mlog(us)	nlog(tkhr)+ mlog(usr)	nlog(tkhr)+ mlog(ushr)

- t : RFID 태그 ID
- u : 리더 ID
- k : 데이터베이스와 태그 사이에 공유된 비밀 키
- s : 데이터베이스와 리더 사이에 공유된 비밀 키
- h : 해쉬 값(Hash value)
- r : 난수(Random number)
- n : 태그 개수
- m : 리더 개수

메모리 사용량에서 리더에 저장해야 하는 저장량을 비교하면, 기존 인증 프로토콜은 리더 ID에 해당하는 정보 u, 리더 비밀 키 k, 리더에서 생성한 해쉬 값 h, 리더에서 발생한 난수 r로 인하여 log(u) + log(k) + log(h)

+ log(r) = log(ukhr)의 저장량을 필요로 한다. 개선된 인증 프로토콜은 리더 ID에 해당하는 정보 u, 리더 비밀 키 k, 태그에서 생성한 해쉬 값 h, 리더에서 발생한 난수 r, 태그에서 발생한 난수 r로 인하여 log(u) + log(k) + log(h) + log(r) + log(r) = log(ukhr^2)의 저장량을 필요로 한다. 본 논문에서 제안한 인증 프로토콜은 리더 ID에 해당하는 정보 u, 리더 비밀 키 k, 태그에서 생성한 해쉬 값 h, 백-엔드 데이터베이스에서 생성한 해쉬 값 h, 리더에서 생성한 해쉬 값 h, 리더에서 발생한 난수 r, 태그에서 발생한 난수 r로 인하여 log(u) + log(k) + log(h) + log(h) + log(h) + log(r) + log(r) = log(ukh^{3}r^2)의 저장량을 필요로 한다.

데이터베이스에 저장해야 하는 저장량을 비교하면 기존 인증 프로토콜은 n개의 태그 ID에 해당하는 정보 t, 그리고 데이터베이스와 태그 사이에 공유된 비밀 키 k로 인해, nlog(t) + nlog(k) = nlog(tk)의 저장량이 필요하며, m개의 리더 ID에 해당하는 정보 u, 그리고 데이터베이스와 리더 사이에 공유된 비밀 키 s로 인하여 mlog(u) + mlog(s) = mlog(us)의 저장량을 필요로 한다. 따라서 기존 인증 프로토콜은 총 nlog(tk) + mlog(us)의 저장량을 필요로 한다. 개선된 인증 프로토콜을 살펴보면, n개의 태그 ID에 해당하는 정보 t, 데이터베이스와 태그 사이에 공유된 비밀 키 k, m2 연산을 위해 사용할 해쉬 값 h, 그리고 태그에서 발생한 난수 r로 인하여 nlog(t) + nlog(k) + nlog(h) + nlog(r) = nlog(tkhr)의 저장량이 필요하고, m개의 리더 ID에 해당하는 정보 u, 데이터베이스와 리더 사이에 공유된 비밀 키 s, 리더에서 발생한 난수 r로 인하여 mlog(u) + mlog(s) + mlog(r) = mlog(usr)의 저장량이 필요하다. 따라서, 개선된 인증 프로토콜은 총 nlog(tkhr) + mlog(usr)의 저장량을 필요로 한다. 제안된 인증 프로토콜을 살펴보면, n개의 태그 ID에 해당하는 정보 t, 데이터베이스와 태그 사이에 공유된 비밀 키 k, 태그에서 생성한 h(ID||k||r||t) 연산의 해쉬 값 h, 그리고 태그에서 발생한 난수 r로 인하여 nlog(t) + nlog(k) + nlog(h) + nlog(r) = nlog(tkhr)의 저장량이 필요하고, m개의 리더 ID에 해당하는 정보 u, 데이터베이스와 리더 사이에 공유된 비밀 키 s, Esk(h(ID||k||t), info) 연산을 위해 사용한 해쉬 값 h, 리더에서 발생한 난수 r로 인하여 mlog(u) + mlog(s) + mlog(h) + mlog(r) = mlog(ushr)의 저장량이 필요하다. 따라서, 본 연구에서 제안된 인증 프로토콜은 총 nlog(tkhr) + mlog(ushr)의 저장량을 필요로 한다.

4.2. 연산량 비교

기존 인증 프로토콜에서 태그의 계산량은 해쉬 연산 1회를 수행한다. 개선된 인증 프로토콜에서 태그 계산량은 난수 발생 1회와 해쉬 연산 1회로서 h + r 계산량을 필요로 한다. 제안된인증 프로토콜은 2h + r의 계산량을 갖는다. 이는 해쉬 함수 2회와 난수 발생 1회를 의미한다.

기존 인증 프로토콜에서 리더의 계산량을 살펴보면, 해쉬 함수 연산 1회, 난수 발생 1회, 암호화 연산 1회, 그리고 복호화 연산 1회로서 h + r + 2e의 계산량을 필요로 한다. 개선된 인증 프로토콜에서 리더 계산량은 난수 발생 1회와 암호화 연산 1회, 복호화 연산 1회로서 r + 2e의 계산량을 필요로 한다. 제안된 인증 프로토콜은 해쉬 함수 연산 1회, 난수 발생 1회, 암호화 연산 1회, 그리고 복호화 연산 1회로서 h + r + 2e의 계산량을 필요로 한다.

기존 인증 프로토콜에서 데이터베이스의 계산량을 살펴보면, 암호화 연산 1회와 복호화 연산 1회로서 2e의 계산량을 필요로 한다. 개선된 인증 프로토콜에서 데이터베이스의 계산량은 n/2h + 2e로서 저장된 n개의 태그 중에서 하나의 태그를 식별하기 위한 해쉬 계산량인 n/2h, 암호화 연산 1회와 복호화 연산 1회의 계산량이 2e로 구성된다. 제안된 인증 프로토콜은 저장된 n개의 태그 중에서 하나의 태그를 식별하기 위한 해쉬 계산량인 n/2h, 해쉬 함수 1회, 암호화 연산 1회, 그리고 복호화 연산 1회로서 총 (n/2+1)h + r + 2e의 계산량을 필요로 한다. 각 방식의 계산량을 비교하면 표 3과 같다.

표 3. 연산량 비교
Table. 3 Comparison of Operation Quantity

구분	기존 프로토콜	개선 프로토콜	제안 프로토콜
태그	h	h+r	2h+r
리더	h+r+2e	r+2e	h+r+2e
백엔드 데이터베이스	2e	n/2h+2e	(n/2+1)h+2e

- h : 해쉬 함수 연산
- r : 난수 발생 연산
- e : 암호화 또는 복호화 연산
- n : 태그 개수

Ⅴ. 성능 평가

제안하는 인증 프로토콜과 이전 인증 프로토콜들의 효율성을 분석하기 위해 시뮬레이션을 수행하였다. 시뮬레이션은 RFID 시스템 환경에서 기존 방식, 개선된 방식, 그리고 제안된 방식의 프로토콜을 메모리 사용량과 통신량 2가지 측면에서 비교한다. 시뮬레이션은 OPNET 17.1을 이용하여 수행되었고, 시뮬레이션을 위해 태그 데이터 전송율은 1Mbps로 가정하였고, 리더 데이터 전송율 11Mbps로 가정하였다. 태그의 전송 전력은 0.001W, 리더의 전송 전력은 0.005W, 태그의 타입은 수동형, 시뮬레이션 시간은 1hour로 산정하였다.

메모리 사용량과 통신량 비교 그래프는 표 2와 표 3을 참고하여 수행된 결과를 보여준다. 각 프로토콜 별 메모리 사용량에 대한 내용을 비교 그래프로 표현한다. 제안 프로토콜은 다른 프로토콜들에 비해 추가적으로 저장해야 하는 리더 ID, 세션키와 같은 추가적인 데이터가 필요하며, 그래프에서 보여주는 제안 프로토콜의 저장량은 X축의 태그 개수 n에 비례하며, 리더 ID, 세션키와 같은 데이터는 1천 만개 정도의 리더가 등록 되어 있다고 가정하였다. 여기서 메모리 사용량은 각 구성별로 나누어 그래프로 표현하였다.

리더의 메모리 사용량에 대한 그래프 그림 5는 태그의 개수 n에 상관없이 고정된 메모리 사용량을 보여준다. 기존 프로토콜의 메모리 사용량이 가장 적고 제안된 프로토콜 가장 많지만, 아주 근소한 메모리 사용량의 차이를 보인다.

그림 6을 보면 데이터베이스에서는 추가적인 저장량이 필요한 제안 프로토콜이 5GB 정도의 가장 많은 메모리 사용량을 가졌으며, 개선된 프로토콜과는 아주 근소한 메모리 사용량의 차이를 보인다.

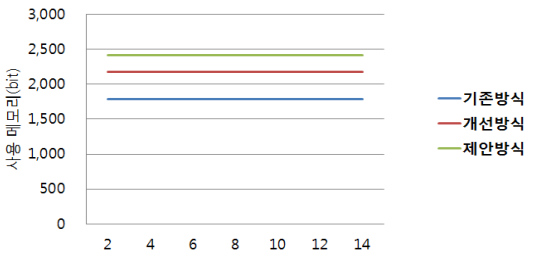

그림 5. 메모리 사용량 비교(리더)
Fig. 5 Comparison of Memory Usage for Reader

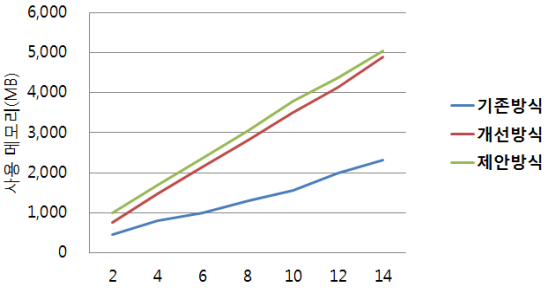

그림 6. 메모리 사용량 비교(데이터베이스)
Fig. 6 Comparison of Memory Usage for Database

기존 프로토콜은 단순한 인증 절차로 인하여 메모리 사용량이 낮음을 알 수 있다. 1억 4천개 정도의 태그를 저장하기 위한 제안 프로토콜의 저장량은 약 5GB 정도이며, 개선된 프로토콜 역시 약 5GB, SP-RFID 프로토콜은 약 2GB 정도의 저장량을 필요로 하는 것을 볼 수 있다. 데이터베이스의 메모리 사용량이 상대적으로 많다고 하지만 태그 개수가 1억개 일때 데이터베이스에 저장한다면 약 5GB 정도의 저장량이 필요하며 등록된 모바일 단말의 개수가 1천만대라고 해도 약 0.2GB 정도의 저장량을 필요로 하므로 총 5GB 정도의 저장량을 필요로 한다.

Ⅵ. 결 론

RFID 기술은 유비쿼터스 컴퓨팅 환경을 조성하기 위한 핵심 기술로써 산업에 전반적으로 활용되어 많은 이익을 남기고 있다. 그러나 이에 대한 역기능으로 RFID 시스템의 보안 위협으로 인해 더 큰 손해가 발생할 수 있다. 본 연구에서는 보다 안전한 RFID 시스템을 위하여 최근에 연구되었던 RFID 인증 기술을 분석하여 보다 안전한 통신을 위해 상호인증을 제공하는 RFID 인증 프로토콜을 제안하였다. 제안한 인증 프로토콜은 리더와 태그간 상호인증을 제공함으로써 악의적인 리더나 불법적인 태그로의 위장을 방지할 수 있으며, 손상된 리더에 대하여 태그의 비밀 키를 보호할 수 있다.

제안 프로토콜은 경량 프로토콜이므로 기존 저가의 수동형 태그에 적용가능하기 때문에, 기존의 대부분 RFID 인증 및 프라이버시 보호 서비스에 그대로 적용될 수 있을 것으로 기대된다.

감사의 글

"본 연구는 교육부와 한국연구재단의 지역혁신 인력양성사업으로 수행된 연구(No. 2013H1B8A 2032180)"결과 입니다.

REFERENCES

[1] A. Juels, "RFID Security and Privacy: AResearch Survey," *IEEE Journal on Selected Areas in Communications*, 24(2): 381-394, Feb.2006.

[2] Li Lu, Yunhao Liu and Xiang-Yang Li,"Refresh: Weak Privacy Model for RFID Systems", *IEEE INFOCOM 2010*.

[3] Taeyang Eom, Jeong-Hyun, "Performance Evaluation of Authentication Protocol for Mobile RFID Privacy", *Korean Institute of Communication and Information Sciences*, Vol. 36, No 6, 2011. 6.

[4] M. Ohkubo, K. Suzuki, and S. Kinoshita,"Hash-chain based forward-secure privacy protection scheme for low-cost RFID,"*Proceedings of the SCIS 2010*, pp. 719-724, 2010.

[5] J. Daemen, V. Rijmen, " The Design of Rijndeal," *AES-The advanced Encryption Standard*, Springer-Verlog, Berlin, Heidelberg, New York, 2009.

[6] D. Henrici and P. Müuller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers,"*Proceeding of the Second IEEE Annual Conference on Pervasive Computing and Communication Security*, pp. 149-153, Mar. 2008.

[7] Le, X.H., Lee, S. and Lee, Y.K. "Two-tier user authentication scheme for heterogeneous sensor network", *Proceedings of the 5th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, USA, 2009.

[8] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in SECON'07: *Proceedings of the 4th Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, June 2007.

[9] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proceedings of the Twelfth USENIX Security Symposium*. Washington, DC, USA: USENIX Association, Aug. 2003, pp. 15–28.

[10] Jin-seob Shin, Young-ho Park, "An Authentication Protocol using the EXOR and the Hash Function in RFID/USN," *Korea Society of Industrial Information Systems*, Vol. 12, No. 2, pp.24-29, 2007.6.

[11] Hae-Soon Ahn, Ki-Dong Bu, "Improved Authentication Protocol for RFID/USN Environment", *The Institute of Electronics and Information Engineers*, Vol.46, No. CI-1, 2009.1.

이영석(Young-seok Lee)

1992년 충남대학교 컴퓨터공학과 공학사
1994년 충남대학교 컴퓨터공학과 공학석사
2002년 충남대학교 컴퓨터공학과 공학박사
1994년 ~ 1997년 LG전자 연구원
2002년 ~ 2004년 한국전자통신연구원 선임연구원
2004년 ~ 현재 군산대학교 정보통신공학과 부교수
※관심분야 : 정보보안, 사물인터넷, 이동컴퓨팅

최 훈(Hoon Choi)

1983년 서울대학교 컴퓨터공학과 (학사)
1990년 Duke Univ. 전산학과 (석사)
1993년 Duke Univ. 전산학과 (박사)
1983년 ~ 1996년 한국전자통신연구원 선임연구원
1996년 ~ 현재 충남대학교 컴퓨터공학과 교수
※관심분야 : 모바일 컴퓨팅/분산 시스템 미들웨어, 운영체제