RFID 환경을 위한 해시기반 상호인증 프로토콜

정회원 전 동 호*, 김 해 문*, 권 혜 진*, 종신회원 김 순 자*

Hash-based Mutual Authentication Protocol for RFID Environment

Dong-ho Jeon*, Hae-moon Kim*, Hye-jin Kwon* *Regular Members,* Soon-ja Kim* *Lifelong Member*

요 약

최근, Ahn 등에 의해 RFID 환경에서 해시함수를 이용한 개선된 인증 프로토콜을 제안하였다. 그들이 제안한 프로토콜은 RFID 태그측의 계산량을 감소시켜줄 뿐만 아니라, 통신 오버헤드를 줄여주며, 사용자 프라이버시 등의 장점을 제공한다. 그러나 본 논문에서는 기존에 Ahn 등이 제안한 프로토콜은 태그가 리더와 데이터베이스를 인증 하지 않는 상호인증 문제로 인하여 다양한 공격들에 취약함을 지적하고, 이러한 문제점을 해결한 상호인증을 제공하는 개선된 상호인증 프로토콜을 제안한다.

Key Words : RFID, Mutual Authentication, Desynchronization Attack

ABSTRACT

Recently, Ahn et al proposed an improved authentication protocol using the hash function in RFID environment. Their proposed protocol provide the following three merits; it reduces the computational costs of RFID tag. itrfduces the communication overhead between the reader and the tag. it protects the user privacy. However, this paper points out that does not authenticate the legality of the RFID reader and database. this paper proposes an improved mutual authentication protocol that can provide the mutual authenticaion.

Ⅰ. 서 론

RFID(Radio Frequency Identification) 시스템은 무선 주파수를 이용하여 물리적 접촉없이 정보를 읽고 저장할 수 있는 기술이다. 바코드 시장을 대체할 기술로서 지나 10년 동안 꾸준하게 발전을 해왔으며 유통, 물류, 의료, 교육등의 분야에 적용되고 있다. RFID 시스템의 구성은 데이터베이스를 포함한 서버와 연결된 리더, 태그로 구성되어 있다. RFID의 비접촉 무선인식 기술은 기술적인 유용성은 뛰어나지만, 태그와 리더간의 통신이 무선 채널상에서 이루어지므로 공격자에 의해 태그정보가 노출되거나 사생활 침해 및 보안상의 취약점이 드러나게 되었다.[1] 이는 세계 각국에서 사생활 침해논란으로 인해 RFID 대중화의 저해요소로 작용되고 있다. 리더와 태그간의 무선 통신은 유선 통신에 비해 도청되기 쉽다. 이를 극복하기위해서 암호학적인 방법을 RFID 시스템에 추가하여 보안성을 높이는 연구가 계속 진행되어 왔다. 태그 가격의 한계로 인해 일반 컴퓨터 통신과 같이 연산량이 많은 암호요소를 쓸 수 없다. 이에 Weis 등은 유선 통신에서 통용되고 있는 공개키나 대칭키 암호보다는 연산량이 적으면서 암호학적 효과를 낼 수 있는 프로토콜을 제안하였다[2]. 그러나 이 프로토콜은 직접적인 정보노출은 막았지만 위치추적이나 재전송공격, 사칭 등 여러 가지 보안 사항들을 내포하였다. 이에 Ohkubo 등은 두 개의 해시 함수를 사용한 해시 체인 프로토콜을 제안하였다. 그러나 이 프로토콜은

* 경북대학교 전자전기컴퓨터학부 컴퓨터통신망연구실(jdh0692@korea.com, snjkim@ee.knu.ac.kr)
논문번호 : KICS2009-09-441, 접수일자 : 2009년 9월 30일, 최종논문접수일자:2010년 1월 6일

재전송 공격을 통한 사칭에 안전하지 못 할 뿐 만 아니라, 해당 태그를 인증하기 위해 데이터베이스의 부하가 많았다. 그 후 Henrici 와 Muller에 의해 태그의 *ID*를 갱신하는 프로토콜이 제안되었다[7]. 그러나 이는 공격자가 리더와 태그사이에서 메시지 차단을 할 경우 불구분성이 만족되지 않아 위치추적에 안전하지 않고, 리더에서 태그로 가는 마지막 메시지가 유실될 경우 정당한 태그라도 데이터베이스와 더 이상 인증을 할 수 없게 설계되었다. 위와 같은 보안 문제점들을 해결하기 위해 많은 연구자들에 의해 해시-락 기법, 확장된 해시-락, 해시기반 ID 변형 기법, 개선된 해시기반 ID변형기법 등 다양한 RFID 인증 프로토콜들이 최근까지 제안되어 왔다. 제안된 기법들은 다양한 보안 취약점을 가지고 있음이 많은 연구자들로부터 계속 발견되어 지고 있다[2]-[24].

최근에 Ahn등에 의해 제안된 ABYN 은 Shin과 Park에 의해 제안된 RFID 환경을 위한 해시함수와 배타적 논리합(xor)연산을 이용한 SP 프로토콜의 취약점을 개선한 프로토콜이다. Ahn등의 연구에서 SP 프로토콜은 스푸핑 공격, 위치트래킹 공격, 태그 키 유출 공격에 취약함을 보이고 태그의 익명성을 제공하지 않았음을 증명하였으며 취약성을 개선한 ABYN 프로토콜을 제안하였다[25],[27].

개선된 ABYN 프로토콜은 리더와 데이터베이스 인증과 데이터베이스에서 태그에 대한 인증만 이루어진다. 태그에서 데이터베이스와 리더에 대한 인증 과정이 없으므로 상호인증을 제공하지 않는다. 본 논문에서 태그에서 데이터베이스와 리더를 인증하는 프로토콜을 제안하고 인증 후 키를 갱신하는 과정을 통해 전 방향 안전성을 제공한다. 키 갱신 과정에서 일어날 수 있는 비 동기공격에 대한 취약성을 개선한다. 이를 통해 강한 인증과 프라이버시를 강화하는 RFID 환경에 적합한 RFID 상호인증 프로토콜을 제안한다. 또한 제안하는 프로토콜을 기존의 RFID 인증 기법들과 비교하여 제안 프로토콜의 안전성과 효율성을 분석한다.

본 논문의 구성은 다음과 같이 구성되어 있다. 2장에서는 RFID 시스템의 구성과 일반적인 RFID 인증프로토콜들이 만족해야 할 보안 요구사항에 대해 설명한다. 3장에서는 ABYN 인증 프로토콜을 소개하고 보안 취약성을 설명한다. 4장에서는 제안하는 개선된 상호인증 프로토콜을 소개한다. 5장에서는 제안 기법에 대한 안전성과 효율성을 살펴보고 6장에서 결론을 맺는다.

Ⅱ. 배경지식

2.1 RFID 시스템

본 절에서는 RFID 시스템의 환경에 대해 기술한다. RFID 시스템은 일반적으로 데이터베이스 서버, RFID 리더, RFID 태그로 구성되어 있다.

2.1.1 태그

태그는 RFID 시스템에서 리더의 요청에 대하여 식별정보를 송신하는 것으로서 트랜스폰더라고 한다. 태그의 구성은 무선통신을 위한 결합장치와 연산을 수행하고 정보를 저장하는 마이크로 칩으로 이루어져 있으며, 전력을 공급받는 방법에 따라 능동형 태그와 수동형 태그로 분류한다.

2.1.2 리더

리더는 태그가 송신한 식별정보를 수신하여 태그를 인식하는 역할을 하는 장치로서 트랜시버라고도 한다. 리더는 태그에게 RF신호를 전송하여 전력을 공급하고, 태그로부터 수신한 정보를 데이터베이스로 전송한다. 리더는 태그의 정보를 읽거나 기록할 수 있다.

2.1.3 데이터베이스

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

2.2 보안 요구 조건

본 절에서는 RFID 시스템의 태그와 리더는 무선주파수 통신을 사용하기 때문에 불법적인 3자의 공격에 취약할 수 있다. RFID 시스템에서 발생할 수 있는 보안 위협의 요구 조건에 대해 설명한다.

2.2.1 상호 인증(Mutual Authentication)

RFID 시스템에서 데이터베이스와 연결된 리더와 태그 모두 합법적인지를 명시적인 인증을 통해서 확인하는 과정이다. 태그와 리더간의 공유한 비밀값을 확인하여 인증하거나 동일한 값을 생성함으로써 상대방을 인증한다.

2.2.2 도청공격(Eavesdropping Attack)에 안전

도청공격은 공격자가 태그와 리더 간에 송수신되는 모든 통신 내용을 엿들은 후 태그에 저장된 비밀정보를 알아내고자 하는 공격이다. 도청을 통해

얻어지는 정보를 이용하여 태그에 대한 비밀 값들을 알아낼 수 없어야 한다.

2.2.3 정보 노출(Information leakage)에 안전

RFID 시스템에서 리더와 태그 간의 통신은 무선으로 이루어지고, 또한 태그는 리더의 요청을 받으면 리더에 대한 인증과정 없이 요청에 대한 응답을 하게 된다. 따라서 공격자는 별 다른 노력 없이 쉽게 정당한 태그의 응답을 얻을 수 있다. 그러므로 안전한 RFID 시스템은 공격자가 정당한 메시지를 얻더라도 그로부터 어떠한 유용한 정보도 얻을 수 없게 설계되어야 한다.

2.2.4 재전송 공격 (Replay attack) 및 사칭 (Impersonate attack) 에 안전

재전송 공격이란 이전 세션에 사용된 메시지를 공격자가 재사용하는 것을 말한다. 이 공격은 주로 사칭과 연관 되는데, 공격자는 이전 세션에서 도청한 메시지를 현재 세션에 사용함으로써 정당한 사용자로 사칭할 수 있다.

2.2.5 스푸핑 공격(Spoofing attack)에 안전

스푸핑 공격은 공격자가 정당한 리더 혹은 태그로 위장하여 상대방을 속이거나 유용한 정보를 얻어 공격이다. 이 공격이 성공하기위해서는 공격자는 상대방의 시도에 정당한 응답을 생성해 낼 수 있어야 한다.

2.2.6 위치추적(Location tracking)에 안전

위치추적공격은 공격자가 여러 지역에 걸쳐 불법적인 리더기를 설치한 상황에서 어떤 태그 소유자의 이동 경로를 추적하는 것을 말한다. 이는 아래의 두 가지 보안조건이 충족되지 않을 때 일어나게 된다.

2.2.6.1 불구분성(Indistinguishability)

불구분성이란 여러 통신 당사자들 중에서 도청된 메시지를 토대로 특정 통신자를 구별하지 못하는 성질을 말한다. 이를 만족하기 위해서는 통신 중 특정 태그를 지칭하는 고정 메시지나 규칙적인 성질을 가지는 메시지 전송을 지양하여야한다.

2.2.6.2 전방향 안전성(Forward secrecy)

전방향 안전성이란 공격자가 어떠한 공격의 성공으로 통신 당사자의 현재 비밀키가 노출되더라도 이전의 암호통신의 내용이 밝혀지지 않는 특성을 말한다. 즉, 전방향 안전성을 만족하려면 현재의 비밀키를 획득한 공격자가 이전의 도청된 메시지를 추측하여 특정한 태그임을 알 수 없어야 한다.

2.2.7 비동기화유도 공격 (Desynchronization attack:DoS)에 안전

데이터베이스와 태그사이에 정보 갱신이 이루어지는 프로토콜에서 공격자가 악의적으로 통신상의 메시지를 차단하거나 통신상의 문제가 발생할 경우 두 개체 사이에 정보 불일치가 일어 날 수 있다. 이러한 점에 착안하여 악의적으로 리더와 태그사이의 통신을 차단하여 정보 불일치를 유도하는 것을 비동기화유도 공격이라 한다. 이것은 일종의 서비스 거부 공격(DoS, Denial of Service attack)으로 이러한 공격에 안전하려면 정보 불일치가 일어나더라도 그를 회복할 수 있도록 설계되어야 한다.

Ⅲ. ABYN 프로토콜

3.1 ABYN 프로토콜

본 장에서는 최근에 Ahn등에 의해 제안된 ABYN 프로토콜을 간략히 설명한다. ABYN 프로토콜은 RFID 환경을 위해 해시함수와 XOR을 이용한 SP 프로토콜의 취약점을 개선한 프로토콜이다[25], [27]. Ahn등의 연구에서 ABYN 프로토콜은 인증 프로토콜을 수행하기전인 초기단계에서 데이터베이스와 리더간에 안전한 세션키 sk가 설정되어 있고, 태그와 리더에서 난수값을 생성하도록 설계되어 있다. 그림1은 Ahn등이 제안한 ABYN 프로토콜의 인증과정을 보여주며, 아래와 같은 단계로 인증프로토콜이 진행된다.

Step 1. Reader → Tag : r_R

리더는 태그를 인식하여 랜덤 값 r_R을 생성하여, Query와 함께 태그에게 전송한다.

Step 2. Tag → Reader : m, r_T

태그는 리더로부터 Query와 r_R를 수신한 후 , 랜덤값 r_T를 생성하고, 수신된 r_R값과 자신의 ID 및 데이터베이스와 공유 비밀값 k를 이용하여 랜덤 해시 값 $m=h(ID \| k \| r_R \| r_T)$을 계산한 후, r_T와 m 값을 리더에게 전송한다.

Step 3. Reader → DB : $E_{sk}(m, r_T, r_R)$

리더는 데이터베이스와 설정된 세션 키 sk를 사

용하여 태그로부터 수신한 m 과 r_T 그리고 자신이 생성한 r_R를 암호화하여 데이터베이스로 전송한다.

Step 4. DB → Reader : $E_{sk}(r_R, m, info)$

데이터베이스는 수신한 $E_{sk}(m, r_T, r_R)$를 세션키 sk를 사용하여 복호화 한 후, m'=$h(ID \| k \| r_R \| r_T)$를 계산하여 자신의 데이터베이스에 저장되어 있는 ID, k쌍을 이용하여 태그에 대한 검증과정을 거친다. 데이터베이스는 m'= $h(ID \| k_{new} \| r_R \| r_T)$값이 수신된 m값과 일치하면 태그를 인증하고 리더와 공유된 세션키 sk를 사용하여 $E_{sk}(r_R, m, info)$를 암호화 하여 리더에게 전송한다. 리더로부터 수신된 m 값과 일치하지 않는다면 오류 메시지를 리더에게 전송하고 종료한다.

3.2 ABYN 프로토콜 의 취약점

Ahn등의 연구에서 SP 프로토콜은 스푸핑 공격, 위치트래킹 공격, 태그 키 유출 공격에 취약함을 보이고 태그의 익명성을 제공하지 않았음을 증명하였으며 취약성을 개선한 ABYN 프로토콜을 제안하였다. 개선된 ABYN 프로토콜은 리더와 데이터베이스 인증과 데이터베이스에서 태그에 대한 인증만 이루어진다. 따라서, 태그에서 데이터베이스와 리더에 대한 인증과정이 없으므로 상호인증을 제공하지 않는다. 또한, 공격자가 물리적 공격을 통하여 태그의 위치를 추적할 수 있고 데이터베이스와 태그에게 정당한 리더로 가장하여 스푸핑 공격에 안전하지 않으므로 전방향 안전성을 제공하지 않는다.

3.2.1 상호인증

3.2.1.1 데이터베이스 와 리더간 인증

ABYN 프로토콜에서 데이터베이스는 리더와 사전에 공유된 세션키 sk를 이용하여 암호와와 복호화 과정이 이루어진다. 데이터베이스는 복호화 과정 $D_{sk}(E_{sk}(m, r_T, r_R))$을 통해 세션키 sk가 동일한 것으로 리더를 인증하게 되고 리더는 자신이 생성한 난수값 r_R을 데이터베이스에 전송하고 데이터베이스에서 수신한 값 $E_{sk}(r_R, info)$을 복호화하여 자신이 생성한 난수값 r_R이 일치하는지를 판단하여 데이터베이스를 인증하게 된다.

3.2.1.2 데이터베이스와 태그간 인증

데이터베이스에서 태그의 인증은 리더를 거쳐 수신된 암호화된 해시값 m=$h(ID \| k \| r_R \| r_T)$을 데이터베이스에서 복호화하여 자신이 해시한 값 m'= $h(ID \| k_{new} \| r_R \| r_T)$과 비교하여 일치하면 태그를 인증한다. 하지만 ABYN 프로토콜에서는 태그에서 데이터베이스를 인증하는 과정이 없으므로 태그는 정당한 데이터베이스인지 알지 못한다.

3.2.1.3 리더와 태그간 인증

ABYN 프로토콜에서 리더에서 태그를 인증하는 과정은 간접적으로 이루어진다. 태그에서 보낸 해시된 값 m=$h(ID \| k \| r_R \| r_T)$과 난수를 암호화하여 데이터베이스에 보내고 이를 수신한 데이터베이스는 복호화하여 태그가 전송한 값 m=$h(ID \| k \| r_R \| r_T)$과 자신이 해시한 값 m'= $h(ID \| k_{new} \| r_R \| r_T)$이 일치하면 리더가 생성한 난수 r_R와 상품정보 $info$를 암호화하여 리더에게 전송한다. 수신한 리더는 복호화하여 자신이 생성한 난수값 r_R과 일치하면 데이터베이스를 인증하며 이것은 간접적으로 태그를 인증한다. 그러나 태그에서 리더를 인증하는 과정이 없으므로 정당한 리더인지 알지 못한다.

3.2.2 전방향 안전성

RFID 인증 프로토콜이 전방향 안전성(Forward Secrecy)을 제공하기 위해서는 다음의 조건을 만족하여야 한다. 공격자가 임의의 태그를 탈취하여 태그내의 메모리에 저장된 중요한 정보들을 얻었더라도 과거에 해당 태그가 참여한 모든 통신 메시지를 이용하더라도 태그를 추적할 수 없어야 한다. ABYN 프로토콜은 전방향 안전성을 제공하지 않는다. 공격자가 임의의 태그를 탈취하여 메모리에 저장된 중요한 정보인 ID, k를 얻었으며 이전의 메시지들을 도청하였다고 가정하면 공격자는 다음의 과정을 통해 태그의 위치를 추적할 수 있다.

Step 1. Attacker → Tag : r_R

공격자는 도청을 통하여 이전의 통신 메시지 m*, r_T*, r_R*들을 획득하고 고정된 ID, k값을 물리적 공격을 통하여 얻었다고 가정한다. 공격자는 태그를 인식하여 랜덤 값 r_R을 생성하여, Query와 함께 태그에게 전송한다.

Step 2. Tag → Attacker : m, r_T

태그는 공격자로부터 Query와 r_R를 수신한 후 , 랜덤값 r_T를 생성하고, 수신된 r_R값과 자신의 ID 및 데이터베이스와 공유 비밀값 k를 이용하여 랜덤

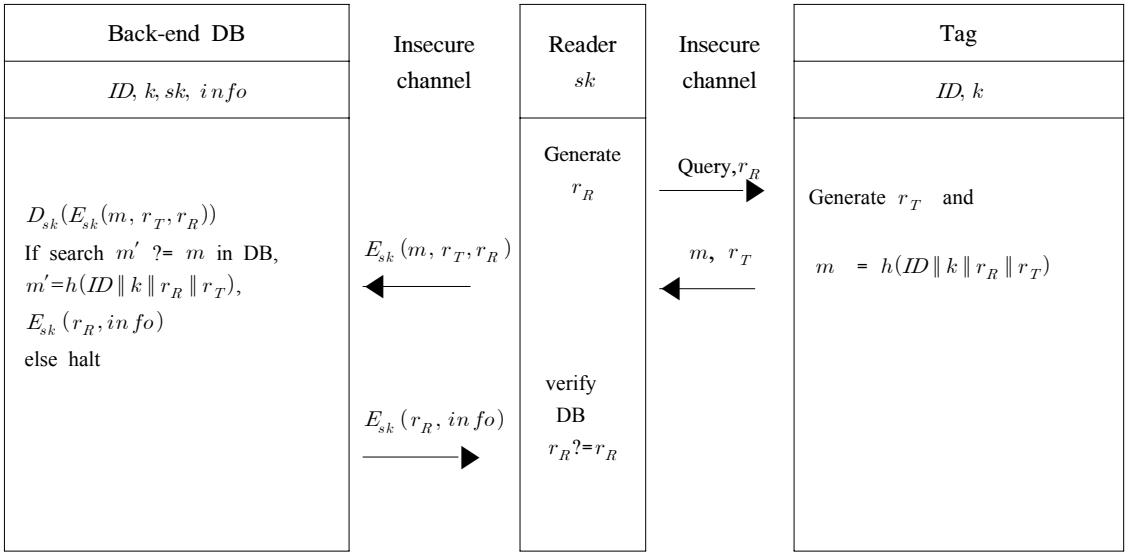

그림 1. ABYN 프로토콜

해시 값 $m=h(ID \| k \| r_R \| r_T)$을 계산한 후, r_T와 m 값을 공격자에게 전송한다.

Step 3. 위치추적

공격자는 태그에서 탈취한 ID, k값을 이용하여 현재의 해시된 값 $m=h(ID \| k \| r_R \| r_T)$을 연산할 수 있으며 이전에 도청을 통하여 획득한 메시지 m^*, r_T^*, r_R^*을 이용하여 $m^*=h(ID \| k \| r_R^* \| r_T^*)$ 값을 연산할 수 있다.

공격자는 도청을 통하여 과거의 모든 메시지에 대해 연산이 가능하므로 위치추적이 가능하다. 따라서 ABYN 프로토콜은 전방향 안전성을 만족하지 않는다.

Ⅳ. 제안하는 프로토콜

본 장에서는 RFID 시스템의 여러 가지 보안 요구조건을 바탕으로 데이터베이스와 리더뿐만 아니라 태그와 리더간의 인증을 포함하는 상호인증 프로토콜을 제안한다(그림 1). 여기에서 데이터베이스와 리더는 안전하지 않은 유선 채널이며 리더와 태그는 안전하지 않은 무선 채널 상에서 통신한다고 가정한다. 또한 리더와 태그는 난수생성이 가능하여야 하며, 데이터베이스와 리더는 세션키 sk를 공유하고 있고, 데이터베이스와 태그는 태그의 ID와 비밀키 k를 공유하고 있다. 제안하는 프로토콜은 데이터베이스에서 태그에 대한 인증과 리더에 대한 인증이 동시에 이루어지며 리더가 이전에 데이터베이스로 전송한 난수값을 확인하는 과정을 통해 이루어진다. 태그에 전송된 메시지를 통해 데이터베이스와 리더를 동시에 인증하게 되고 이후에 해시연산을 통해 키 업데이트가 이루어진다. 또한 데이터베이스에서 이전 세션의 태그의 키 값을 저장하고 있어 블로킹으로 인해 비동기 공격이 일어나더라도 이전 세션의 키 값을 찾아 상호인증을 가능하게 한다. 매 세션마다 태그와 데이터베이스에서 연산되는 r_T , r_R, k 값이 바뀌게 되므로 도청, 재전송 공격, 스푸핑 공격, 위치추적 공격, 서비스거부 공격에 안전하다. 태그의 ID, k 값이 노출되더라도 다음 세션에서 k 값이 업데이트 되므로 전방향 안전성을 만족한다.

4.1 용어정리

이 절에서는 여기서는 제안 기법에 사용하게 될 용어를 설명한다.

- DB : 백 엔드 데이터베이스.
- R : 리더.
- T : 태그.
- r_R : 리더가 생성한 난수
- r_T : 태그가 생성한 난수
- ID : 태그의 식별정보.
- k : Tag에 저장된 키 값
- $h()$: 해시연산
- m_L : 해시한 결과인 m의 좌측 절반
- k_{old} : DB에 저장된 태그의 이전 키값.

k_{new} : DB에 저장된 태그의 현재의 키값.
m_L : 해시한 결과인 m의 우측 절반
$\|$: 연접
$E_{sk}(\,)$: 세션키 sk를 이용한 대칭키 암호연산
$D_{sk}(\,)$: 세션키 sk를 이용한 대칭키 복호연산

4.2. 제안하는 프로토콜

제안하는 프로토콜은 그림 2에서 개선된 상호인증 프로토콜의 세부동작을 보여 준다. 데이터베이스와 리더사이의 채널은 안전하지 않은 채널(Insecure Channel)이며 리더와 태그 사이의 채널도 안전하지 않은 채널이라고 가정한다. 각각의 태그에 대하여 데이터베이스에 ID, 초기 인증키k_{new}, k_{old} , $info$값을 저장하고 태그에 ID, k 값을 저장한다. 리더와 데이터베이스는 세션키 sk를 공유하고 있다.

Step 1. Reader → Tag : r_R

리더는 태그를 인식하여 랜덤 값 r_R을 생성하여, Query와 함께 태그에게 전송한다.

Step 2. Tag → Reader : m_L, r_T

태그는 리더로부터 Query와 r_R를 수신한 후 , 랜덤값 r_T를 생성하고, 수신된 r_R값과 자신의 ID 및 데이터베이스와 공유 비밀값 k를 이용하여 랜덤 해시 값 m=$h(ID \| k \| r_R \| r_T)$을 계산한 후, r_T와 m 값의 왼쪽 절반인 m_L을 리더에게 전송한다.

Step 3. Reader → DB : $E_{sk}(m_L, r_T, r_R)$

리더는 데이터베이스와 설정된 세션키 sk를 사용하여 태그로부터 수신한 m_L 과 r_T 그리고 자신이 생성한 r_R를 암호화하여 데이터베이스로 전송한다.

Step 4. DB → Reader : $E_{sk}(r_R, m_R, info)$

데이터베이스는 리더로부터 수신한 $E_{sk}(m_L, r_T, r_R)$를 세션키 sk를 사용하여 복호화 한 후, m'_L= $h(ID \| k_{new} \| r_R \| r_T)$ 를 계산하여 자신의 데이터베이스에 저장되어 있는 ID, k_{new}, k_{old}쌍을 이용하여 태그에 대한 검증과정을 거친다. 데이터베이스는 m'_L= $h(ID \| k_{new} \| r_R \| r_T)$값이 수신된 m_L값 일치하면 태그를 인증하고 리더와 공유된 세션키 sk를 사용하여 $E_{sk}(r_R, m_R, info)$를 암호화 하여 리더에게 전송한다. 리더로부터 수신된 m_L 값과 일치하지 않는다면 m'_L=$h(ID \| k_{old} \| r_R \| r_T)$ 값과 비교하여 일치하는지 검증한다. 일치하면 태그를 인증하고 리

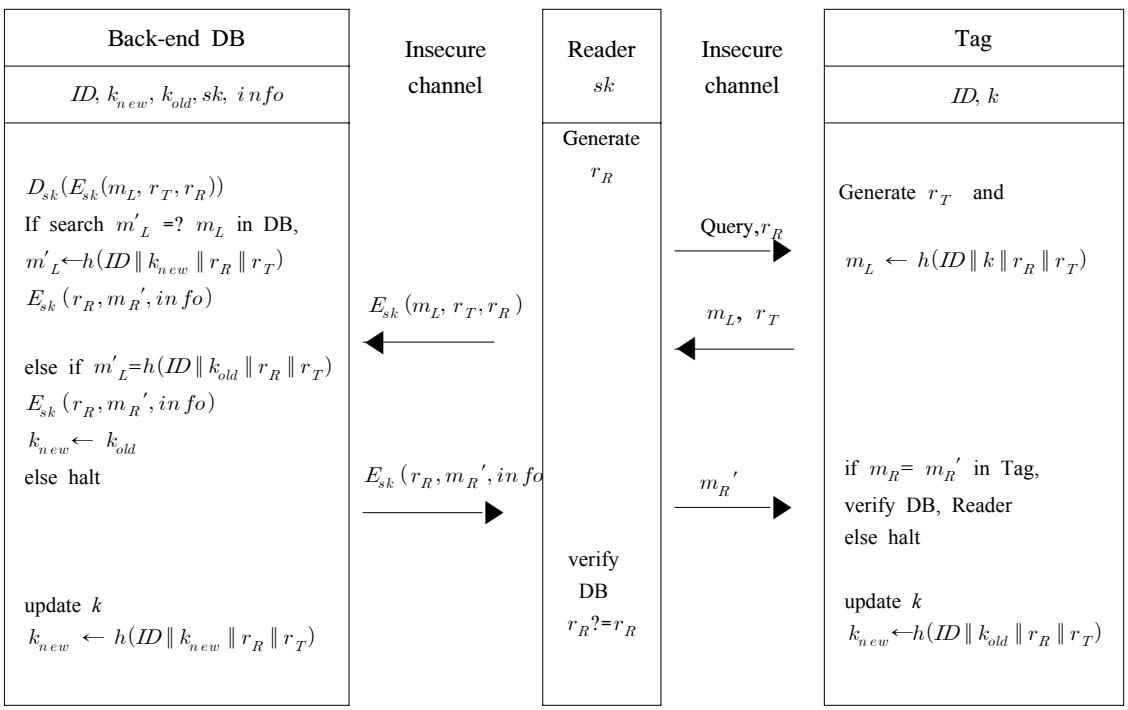

그림 2. 제안하는 프로토콜

더와 공유된 세션키 sk를 사용하여 해시한 메시지의 오른쪽 절반 m_R값과 리더가 생성한 r_R값, 태그에 대한 상품 관련 정보 $info$를 암호화 하여 $E_{sk}(r_R, m_R, info)$을 리더에게 전송한다. 다만 일치하는 값이 검색되지 않으면 오류메시지를 리더에게 전송한다. 이후 데이터베이스는 k_{old}값을 k_{new}값으로 변경하고 새로운 k_{new}값은 해시 연산 k_{new}= $h(ID \| k_{old} \| r_R \| r_T)$을 통해 갱신된다.

Step 5. Reader → Tag : $E_{sk}(r_R, m_R, info)$

리더는 데이터베이스에서 수신한 값이 오류이면 태그와의 통신을 중단하고, 정상적인 인증이 되었을 경우 수신된 $E_{sk}(r_R, m_R, info)$를 데이터베이스와 공유된 세션키 sk를 사용하여 복호화 연산 $D_{sk}(E_{sk}(r_R, m_R, info))$을 한다. 이전에 데이터베이스로 송신한 r_R값과 비교하여 일치하면 데이터베이스를 인증하고 m_R값을 태그에게 전송한다. 태그는 수신된 m_R값과 자신의 해시연산 결과값의 오른쪽 절반 m_R을 비교하여 일치하면 데이터베이스와 리더를 모두 인증하고 일치하지 않으면 종료한다. 태그에서 데이터베이스와 리더의 인증과정이 진행된 이후 해시연산 $k = h(ID \| k \| r_R \| r_T)$을 통해 태그에 저장된 키 값을 업데이트 한다.

Ⅴ. 제안 프로토콜 분석

본 장에서는 앞서 소개된 여러 가지 RFID 보안 요구조건을 바탕으로 Ⅲ장에서 제안한 상호 인증 프로토콜의 안전성과 구현의 효율성에 대하여 분석한다. 리더와 데이터베이스는 뿐만 아니라 리더와 태그도 안전하지 못한 채널이다. 공격자는 도청이 가능할 뿐 아니라 메시지에 대한 인터럽트도 가능하고 태그에 대한 물리적인 공격을 통한 ID, k의 탈취도 가능하다고 가정한다. 제안하는 프로토콜은 다음과 같이 상호인증을 통하여 재전송 공격, 스푸핑 공격, 위치추적 공격, 서비스거부 공격 등에 안전하고 전방향 안전성을 만족한다.

5.1 안전성 분석

5.1.1 상호인증 (Mutual Authentication)

상호인증은 참여하는 당사자가 각각 인증을 통해 서로가 합법적인지 확인하는 과정이다. 제안 프로토콜에서 상호인증은 데이터베이스에서 태그와 리더에 대한 인증, 태그에서 데이터베이스와 리더에 대한 인증, 리더에서 데이터베이스와 태그에 대한 인증을 모두 만족한다. 인증에 참여하는 세부분이 서로를 각각 인증한다. 제안한 프로토콜은 통신과정에서 ID를 직접 노출 시키지 않고, 데이터베이스와 공유 비밀 값 k와 랜덤 넘버 r_T, r_R를 사용하여 인가된 사용자만이 해당 태그의 ID, k를 알아 낼 수 있도록 하였다. 데이터베이스에서 매 세션마다 m_L= $h(ID \| k \| r_R \| r_T)$값과 일치하는 ID, k를 찾아서 태그를 인증하게 된다. 태그 자신이 연산한 결과가 m'_L=$h(ID \| k_{new} \| r_R \| r_T)$를 만족하는 값이면 데이터베이스를 인증한다. 따라서 제안한 프로토콜은 안전한 상호인증을 제공한다.

5.1.2 도청공격 (Eavesdropping Attack)

도청공격은 무선통신구간인 태그와 리더사이에 송수신되는 내용을 도청하여 태그에 대한 정보를 알아내는 공격이다. 제안한 프로토콜에서 공격자는 r_R, r_T, m_L, m_R를 도청할 수 있다. 하지만 공격자는 도청한 내용으로 일방향 해시함수의 특성상 역으로 연산을 하지 못하므로 태그의 비밀 값 ID, k에 대한 정보를 얻어낼 수 없다. 따라서 제안한 프로토콜은 도청공격에 안전하다.

5.1.3 재 전송공격 (Replay Attack)

재전송 공격은 공격자가 과거에 태그와 리더의 무선통신 구간에서 내용을 도청한 후 이를 재전송하여 합법적인 태그나 리더로 인증 받으려는 공격이다. 제안 프로토콜에 정당한 리더로 가장한 공격방법을 적용하면 공격자는 이전 세션에서 도청을 통하여 r_R, r_T, m_L, m_R를 얻을 수 있지만 이전 세션에서 태그에서 k값이 갱신되어 있고 태그에서 생성된 난수 r_T가 다르므로 이전의 m_L와 다르므로 정당한 리더로 인증되지 않는다. 또한 데이터베이스와 리더 사이에는 공유된 sk로 암호화하여 m_L를 전송하므로 공유된 sk를 알지 못하므로 리더를 가장할 수 없다. 공격자가 정당한 태그로 가장한 경우 매 세션마다 리더로부터 전송된 r_R값과 태그에서 생성된 r_T값을 m_L=$h(ID \| k \| r_R \| r_T)$연산에 사용되어 m'_L=$h(ID \| k_{new} \| r_R \| r_T)$값과 데이터베이스에서 일치하지 않으므로 가짜 태그 또는 공격 태그로 쉽게 검출된다. 따라서 제안한 프로토콜은 재 전송공격에 안전하다.

5.1.4 스푸핑 공격 (Spoofing Attack)

스푸핑 공격은 공격자가 정당한 태그로 위장하여

리더로부터 인증에 필요한 정보를 획득하거나 정당한 리더로 위장하여 태그로부터 인증에 필요한 정보를 획득하여 공격하는 방법이다. 제안 프로토콜에서는 공격자가 정당한 리더로 가장하여 태그를 속이기 위해서는 재전송 공격의 방법과 동일하게 올바른 $m_R=h(ID \| k \| r_R \| r_T)$값을 계산해야 하지만 ID, k값을 알지 못하면 정당한 리더로 인증 받을 수 없어 공격에 안전하다. 정당한 태그로 위장하는 경우, 이전 세션에서 도청으로 얻은 정보 m_L를 데이터베이스로 전송하여도 데이터베이스에서 $m'_L=h(ID \| k_{new} \| r_R \| r_T)$를 계산하는 과정에서 위장한 태그를 식별해 낼 수 있어 스푸핑 공격에 안전하다.

5.1.5 위치추적 공격 (Location Tracking Attack)

위치 추적 공격은 공격자가 태그의 위치변화를 감지하여 태그 소유자의 이동경로를 파악하여 사용자의 프라이버시를 침해하는 공격이다. 태그로부터 매 세션마다 동일한 정보가 나오는 RFID 시스템은 위치추적이 가능 하다. 랜덤한 두 개의 태그를 두고 이들을 구별해 낼 수 없으면 불구분성(indistinguishability)을 만족하며 태그의 위치 프라이버시를 보장받을 수 있다. 제안 프로토콜에서는 매 세션마다 r_R, r_T, k값에 의해 계산된 m_L 값이 계속해서 바뀌게 되어 이전 세션과 항상 다른 값을 전송하므로 공격자는 특정한 태그를 식별할 수 없으므로 위치추적에 안전하다.

5.1.6 서비스 거부 공격 (Dos Attack ; 비동기화 유도 공격(Desynchronization attack))

서비스 거부공격은 RFID시스템의 정상적인 작동을 방해하여 비동기화 문제를 일으키는 방법이다. 또한 악의적으로 리더와 태그사이의 통신을 차단하여 정보 불일치를 유도하는 것이 비동기화 유도공격이다. 제안 프로토콜에서 비동기화 유도공격을 시도하려면 안전하지 못한 태그와 리더 사이에서 m_L 값이 전송된 후 데이터베이스는 일치하는 태그 인증과정을 거친 후 k_{new}값이 갱신되고 기존 k_{new}의 값은 k_{old} 값으로 바뀌게 된다. 데이터베이스에서 태그로 전송되는 m_R를 가로채면 태그에서 k값은 갱신되지 않는다. 데이터베이스는 태그 인증 후 k_{new}, k_{old}값이 업데이트 되고 태그는 k값이 업데이트 되지 않은 비동기 상태가 된다. 그러나 공격받은 태그는 다음 세션에서 k값을 이용하여 연산한 결과인 m_L값을 리더에게 전송하면 데이터베이스에서 k_{new}값이 없을 경우 k_{old}값을 검색하여 인증과정을 거쳐 정상적인 k값을 갱신하는 과정이 진행된다. 따라서 m_R의 정보가 차단되더라도 다음 통신 세션에서 데이터베이스에 k_{old}값을 통하여 상호인증을 진행할 수 있어 비동기화 유도공격에 안전하다.

5.1.7 전방향 안전성 (Forward secrecy)

전방향 안전성은 공격자가 물리적인 공격을 통하여 어떤 태그의 ID, k값을 알아내더라도 이로부터 이전 세션의 정보를 획득할 수 없어야 한다. 제안 프로토콜에서는 공격자가 물리적 공격을 통하여 ID, k값을 알아내더라도 연속적으로 r_R, r_T값을 알고 있으면 전방향 위치 추적이 가능하지만 한번이라도 r_R, r_T값을 알지 못하면, 즉 k를 갱신하는 체인이 끊기면 이전 세션의 k를 유추할 수 없다. 특정 태그의 r_T값을 연속적으로 도청할 수 있는 시점까지만 전방향 위치 추적이 가능하므로 전방향 안전성을 만족한다고 할 수 있다.

표 1은 제안한 프로토콜과 SP 프로토콜, ABYN 프로토콜과의 안전성을 비교 분석한 표이다. Ahn 등의 연구에서 분석결과를 인용하면 SP 프로토콜은 각각의 공격에 취약함을 보였고 ABYN 프로토콜과 더불어 상호인증을 제공하지 않았다. 제안 프로토콜에서는 SP 프로토콜과 ABYN 프로토콜에서 제공하지 않았던 태그에서 데이터베이스와 리더에 대한 인증을 가능하게 하였다. 태그에서 물리적 공격등을 통하여 태그의 중요한 정보인 비밀값 ID, k를 공격자가 획득할 수 있다고 가정하였다. 이러한 환경에서 ABYN 프로토콜은 전방향 안전성을 제공하지

표 1. 안전성 비교

(O : 만족, X : 불만족)

		SP[25]	ABYN[27]	제안하는 프로토콜
DB	태그 인증	O	O	O
	리더 인증	O	O	O
리더	DB 인증	O	O	O
	태그 인증	X	O	O
태그	DB 인증	X	X	O
	리더 인증	X	X	O
재전송		X	O	O
스푸핑		X	O	O
위치추적		X	X	O
서비스거부		X	X	O
전방향 안전성		X	X	O

않아 이전 메시지에 도청을 통하여 태그 위치를 추적할 수 있었지만 제안 프로토콜에서는 상호인증 후에 비밀키 값이 갱신되므로 전방향 안전성을 만족한다. 또한 메시지 차단을 통한 서비스 거부 공격이 있더라도 데이터베이스에서 k_{old}값으로 태그에 대한 인증이 이루어진다. 결론적으로 표 1과 같이 ABYN 프로토콜과 비교하여 상호인증과 전방향 안전성을 제공함으로 재전송 공격, 스푸핑 공격, 위치추적, 서비스거부 공격 등에 안전함을 알 수 있다.

5.2 효율성 분석

본 절에서는 제안한 상호인증 프로토콜에 대한 효율성을 분석한다. 표 2는 제안한 상호인증 프로토콜과 SP, ABYN 인증 프로토콜과의 효율성을 분석한 표이다. 제안한 상호인증 프로토콜은 ABYN 인증 프로토콜과 비교하여 태그와 데이터베이스에서 각각 계산되는 추가적인 한 번의 해시연산들은 ABYN 프로토콜이 가지는 취약성인 태그의 전방향 보안성을 제공하기 위한 방법으로 사용되어 진다. ABYN 프로토콜과 비교하여 제안한 상호인증 프로토콜은 통신라운드 수가 증가하였으나 이것은 태그에서 리더와 데이터베이스를 인증하기 위한 방법으로 사용되어 진다. 제안된 상호인증 프로토콜은 ABYN 프로토콜과 비교하여 해시된 결과값의 절반만 사용하여 전송하므로 태그와 리더간의 전송이 효율적이다. 결론적으로 제안한 상호인증 프로토콜은 ABYN 인증 프로토콜과 비교하여 표 1에서 보여주는 것처럼 상호인증을 제공함으로 인해 다양한 공격에 안전하도록 하였다. 안전성을 보장하기 위해 추가된 해시연산은 ABYN 프로토콜과 비교하면 데이터베이스와 태그에서 2배로 증가되는 오버헤드가 발생한다. 데이터베이스는 시스템의 성능이 좋으므로 많은 연산이 가능하나 태그에서는 한 번 더 해시연산이 이루어지므로 오버헤드가 발생한다. ABYN 인증 프로토콜과 마찬가지로 해시연산이 태그에 포함되어 있다면 전력소비와 연산속도에서 느려지는 단점이 있다. 그러나 보안성 강화측면에서 장점을 제공한다.

표 2. 효율성 비교

(n : 태그의 개수)

효율성	SP 프로토콜[25]			ABYN 프로토콜[27]			제안하는 프로토콜		
	DB	Reader	Tag	DB	Reader	Tag	DB	Reader	Tag
난수 생성	0	1	0	0	1	1	0	1	1
대칭키 암호연산	2	2	0	2	2	0	2	2	0
해시연산	0	1	1	n	0	1	2n	0	2
XOR 연산	0	1	1	0	0	0	0	0	0
통신 라운드 수	6			4			5		

Ⅵ. 결 론

RFID 시스템에 대한 관심이 커지면서 RFID 보안 요구사항이 증대되고 있다. 본 논문에서 최근 Ahn 등이 의해 제안된 해시기반 RFID 인증 프로토콜을 분석하여 상호인증을 제공하지 않았으며 위치추적 공격에 취약하고 전방향 안전성을 제공하지 않았음을 지적하였다. 이러한 문제점을 해결하기 위해 RFID 환경을 위한 안전한 상호인증을 제공하는 개선된 상호인증 프로토콜을 제안하였다. 결론적으로 제안 프로토콜은 ABYN 프로토콜과 비교하여 데이터베이스와 태그에서 한 번의 해시연산의 추가로 비밀키를 업데이트하여 전방향 안전성을 제공하였고 리더에서 태그로의 통신라운드가 추가되어 안전한 상호인증을 제공하였다. 데이터베이스에서 키 갱신 과정에 이전의 키값을 저장하여 무선구간에서 비동기공격이 일어나더라도 다음 세션에서 동기를 회복할 수 있어 비동기 공격에도 안전하다. 안전한 상호인증을 위해 통신라운드 증가는 논리적으로 추가되어야 하고 1회 증가된 해시는 데이터베이스와 태그에서 오버헤드를 발생시키지만 보안성을 강화하는 측면에서 장점을 제공한다. 제안 프로토콜은 ABYN 프로토콜과 비교하여 비슷한 해시연산을 사용하면서도 데이터베이스와 리더, 태그에 각각 안전한 상호인증과 전방향 보안성을 제공하며 비동기 공격에도 안전하다.

참 고 문 헌

〔1〕 K. Finkenzeller, *RFID Handbook*, John Wiley & Sons, 1999.

〔2〕 S A Weis, S Sarma, R Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", *Security In Pervasive Computing 2003*, LNCS 2802, pp.201-212, 2004.

〔3〕 S. Junichiro, H. Jae-Cheol, and S. Kouichi, "Enhancing privacy of universal re-encryption

scheme for RFID tags," *EUC 2004*, LNCS 3207, pp.870-890, Springer-Verlag, 2004.

〔4〕 A.Juels and S. A. Weis, "Authenticating pervasive devices with human protocols", *Advances in Cryptogloy-Crypto '05*, LNCS 3126, pp.293-308, springer, 2005.

〔5〕 S.S Kumar and C. Paar, "Are standards compliant Elliptic Curve Cryptosystems Feasible on RFID?", *Proceedings of Workshop on RFID security*, Austria, July 2006.

〔6〕 M. Ohkubo, K. Suzuki and S. Kinoshita, "Efficient Hash-Chain Based RFID Privacy Protection Scheme", *Privacy Workshop at the Sixth International Conference on Ubiquitous Computing (UbiComp 2004)*, 2004.

〔7〕 D. Henrici,, P. Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", *Proc. Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. PERCOMW '04*, pp.149-153, 2004.

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

〔9〕 G. Avoine, P. Oechslin, "A Scalable and. Provably Secure Hash-based RFID Protocol", *IEEE PerSec 2005*, March 2005.

〔10〕 JeaCheol Ha, JungHoon Ha, SangJae Moon, and Colin Boyd, "LRMAP: Lightweight and Resynchronous Mutual Authentication Protocol for RFID System", *Ubiquitous Convergence Technology*, 2007.

〔11〕 A. Juels. "Minimalist cryptography for Low-Cost RFID Tags", *The Fourth International Conferece on Security in Communication Networks- SCN 2004*, LNCS 3352, pp.149-164, 2004.

〔12〕 D. N. Duc, J. park, H. Lee and K. Kim, "Enhancing Security of EPCgloabal Gen-2 RFID Tag against Traceability and Coning", *The 2006 Symposium on Cryptography and Information Security*, 2006.

〔13〕 A. Juels, "Strenthening EPC Tag against Cloning", *ACM Workshop on Wireless Security (WiSe)*, pp.67-76, 2005.

〔14〕 S. Karthikeyan, and M. Nesterenko, "RFID security without extensive cryptography", *Proc. 3rd ACM workshop on Security of ad hoc and sensor networks*, pp.63-67, 2005.

〔15〕 H-Y. Chien, and C-H. Chen, "Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards", *Computers Standard & Interfaces,* 29(2), pp.254-259, 2007.

〔16〕 J. Bringer, H. chabanne, and E. Dottax, "HB++: A Lightweight Authentication Protocol Secure against Some Attacks", *Proc. IEEE Int' Conf Pervasive Service, Workshop Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, 2006.

〔17〕 J. Munilla and A.Peinado, "HB-MP:A further step in the HB-family of lightweight authentication protocols", *Computer Networks*, 51(9): 2262-2267, June 2007.

〔18〕 P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "LMAP: A Real Lightweight Low-Cost RFID Tags", *Proc. Second Workshop RFID Security*, July, 2006.

〔19〕 P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "M2AP: A Minimalist mutual-Authentication Protocol for Low-Cost RFID Tags", *Proc. Int' Conf Ubiquitous Intelligence and Computing(UIC, 06)*, pp.912-923, 2006.

〔20〕 P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags", *Proc. OTM Federated Conf and Workshop: IS Workshop*, Nov. 2006.

〔21〕 H.-Y. Chien. "SASI: A New Ultra-lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", *IEEE Transactions on Dependable and Secure Computing,* 4(4), pp.337-340. Oct-Dec, 2007.

〔22〕 T. Li and R.H. Deng, "Vulnerability Analy-

sis of EMAP-an Effcinet RFID Mutual Authentication Protocol," *Proc. Second International Conference, Availability, Reliability, and Security (AReS'07)*, 2007.

〔23〕 T. Li and G. Wang, "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols," *Proc. 22nd IFIP TC-11 International Information Security Conference*, May 2007.

〔24〕 H.-Y. Chien and C.-W. Hung, "Security of Ultra-Lightweight RFID Authentication Protocols and Its Improvements," *ACM Operating System Rev*, 41(2), pp.83-86, July 2007.

〔25〕 신진섭, 박영호, "RFID/USN 에서의 EXOR과 해쉬함수를 이용한 인증 프로토콜," *한국산업정보학회논문지*, 12(20), pp.24-29, 2007.

〔26〕 권혜진, 이재욱, 전동호, 김순자, "데이터베이스에서 태그 검색이 쉽고 안전한 RFID 상호 인증 프로토콜," *한국정보보호학회논문지*, 18(5), pp. 125-134. 2008.

〔27〕 안해순, 부기동, 윤은준, 남인길, "RFID/USN 환경을 위한 개선된 인증 프로토콜," *전자공학회논문지*, 46(1), 제1호, pp.1-10. 2009.

전 동 호 (Dong-ho Jeon) 정회원

2000년 2월 밀양대학교 컴퓨터공학과 학사

2002년 2월 경북대학교 정보통신공학과 석사

2002년 3월~현재 경북대학교 정보보호학과 박사과정

<관심분야> RFID/USN, 정보보호, 네트워크 보안

김 해 문 (Hae-moon Kim) 정회원

2002년 2월 경북대학교 전자공학과 학사

2004년 8월 경북대학교 전자공학과 석사

2004년 9월~현재 경북대학교 전자공학과과 박사과정

<관심분야> 스테가노그라피, 정보보호, 네트워크 보안

권 혜 진 (Hye-jin Kwon) 정회원

2007년 2월 경북대학교 수학과 학사

2009년 2월 경북대학교 정보보호학과 석사

2009년 3월~현재 경북대학교 전자공학과 박사과정

<관심분야> RFID/USN, 스테가노그라피, 암호기술

김 순 자 (Soon-ja Kim) 종신회원

1975년 2월 경북대학교 수학교육학과 졸업

1977년 2월 경북대학교 수학과 석사

1988년 2월 계명대학교 수학과 박사

1993년 4월~현재 경북대학교 전자전기컴퓨터학부 교수

<관심분야> 정보보호 및 보안기술, 정보보호 응용기술