情報保護學會論文誌
第16卷 第3號, 2006. 6

안전하지 않은 채널에서의 RFID 프라이버시 보호에 관한 연구

박 장 수†, 이 임 영‡
순천향대학교 컴퓨터학부

A Study on RFID Privacy Protection in Insecure Channel

Jang-Su Park†, Im-Yeong Lee‡
Division of Computer Science & Engineering, Soonchunhyang Univ.

요 약

유비쿼터스 환경에서의 핵심 기술로써 RFID 기술은 중요한 위치를 차지하고 있다. RFID 기술은 작은 전자 태그를 사물에 부착하여 사물에 대한 정보나 주위 환경에 대한 다양한 정보를 제공해 주는 것으로 무선 인식 기술을 의미한다. 하지만 RFID는 물리적인 접촉 없이도 인식이 가능하다는 특징으로 인해 안전성과 프라이버시 측면에서 기존에 발생하지 않았던 문제점이 발생할 수 있어 이를 해결하기 위해 RFID 인증 기술에 대한 많은 연구가 진행 되고 있다. 현재 연구가 진행되고 있는 것은 데이터베이스와 리더사이의 통신이 안전한 통신 채널, 리더와 태그사이의 통신은 불안전한 통신 채널에서의 인증 기술을 적용한다. 하지만 본 논문에서는 데이터베이스와 리더사이의 통신도 안전하지 않은 통신 채널에서의 인증 프로토콜을 제안함으로써 정당한 객체에게만 정보를 제공하도록 하여 사용자의 프라이버시 침해 문제를 해결하고자 한다.

ABSTRACT

As a core technology in the ubiquitous environment, RFID (Radio Frequency Identification) technology takes an important role. RFID technology provides various information about objects or surrounding environment by attaching a small electronic tag on the object, thus, it means the remote control recognition technology. However, the problems which never happened before can be generated on the point of security and privacy due to the feature that RFID technology can recognize the object without any physical contact. In order to solve these problems, many studies for the RFID recognition technology are going on the progress. The currently running study is the secure communication channel between database and reader applying the recognition technology in the insecure communication channel between reader and tag. But, the purpose of this paper is to settle a privacy problem, which is insecurity of communication between database and reader channel by suggesting providing a user with authentication protocol in order to give information to an authorized entity.

Keywords : *RFID, Authentication(인증)*

Ⅰ. 서 론

유비쿼터스(Ubiquitous) 환경에서의 핵심 기술로 최근 많은 주목을 받고 있는 RFID(Radio Fre-

접수일: 2006년 2월 8일; 채택일: 2006년 4월 10일
† 주저자, pjswise@sch.ac.kr
‡ 교신저자, imylee@sch.ac.kr

quency IDentification)는 무선 주파수를 이용하여 물리적 접촉 없이 태그에 대한 정보를 읽거나 기록하는 자동 인식 기술 시스템이다. 이러한 RFID는 메모리를 가지고 있어 데이터의 읽기/쓰기가 가능하며, 이동 중 인식 가능하고, 여러 개의 Tag를 동시 사용 할 수 있다는 다양한 장점을 가지고 있어 앞으로의 활용 분야는 금융, 의료, 교통, 제조, 문화 등 다양한 분야에서의 사용으로 산업전반에서 혁신적인 발전을 이룩할 것으로 기대되고 있다.

하지만 RFID 태그가 모든 사물에 부착되어 일상화 될 경우, 식별정보가 쉽게 식별된다는 RFID의 기본적인 특징으로 인해 개인정보 침해 및 정보 유출에 따른 보안 문제가 중요한 사회적 이슈로 대두될 것이라 사료된다. 또한 안전성과 프라이버시 측면에서 기존에 발생하지 않았던 문제점이 발생할 수 있다. 그러므로 RFID 시스템을 사용하고자 할 때 보안 및 프라이버시 침해를 해결하는 방안에 대한 연구가 우선되어야한다 [1,2].

프라이버시 침해 문제를 해결하기 위한 방안으로 가장 활발하게 연구가 진행되는 것은 인증 기술을 적용시킴으로써 정당한 객체인 태그, 리더, 데이터베이스에게만 정보를 획득할 수 있도록 하고, 정당하지 않은 개체들에게 어떠한 정보도 획득할 수 없게 하여, 프라이버시를 보호하는 것이다. 그리고 현재 연구가 진행되는 것들은 데이터베이스와 리더사이의 통신은 안전하고, 태그와 리더사이의 통신은 불안전하다는 가정 하에 진행되고 있다 [1,3,4-9].

따라서 본 논문에서는 태그와 리더의 통신뿐만 아니라 데이터베이스와 리더의 통신도 불안전하다는 가정 하에 RFID의 프라이버시 문제를 해결하기 위한 인증 프로토콜을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 RFID 시스템 구성과 위협요소 및 고려사항을 기술하고, 3장에서는 RFID 프라이버시에 보호에 관한 기존의 연구를 분석한다. 4장에서는 2장에서 언급한 위협요소 및 고려사항에 대해 만족하며, 3장에서의 기존 방식 보다 효율적인 방식을 제안 한다. 마지막으로 5장에서는 결론으로 맺는다.

II. RFID 시스템 구성 과 위협요소 및 고려사항

본 장에서는 RFID 시스템의 일반적인 구성과 RFID 시스템에서의 위협요소 및 인증 프로토콜 설계시 고려사항에 대하여 알아본다.

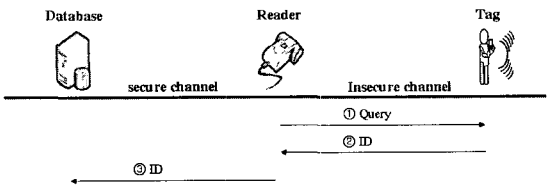

그림 1. 일반적인 RFID 시스템

1. RFID 시스템 구성

앞에서 언급 하였듯이 RFID는 RF(Radio Frequency)를 이용해 태그와 리더가 서로 정보를 주고받는 방식이다. 일반적인 RFID 시스템은 그림 1에서와 같이 다음의 세 가지 구성요소로 구성된다 [1,3,7,9,10].

- 태그(Tag) : IC 칩과 안테나로 구성되어 있고, 식별 정보를 가지고 있다. 일반적으로 전원의 유/무에 따라 능동형 태그(Active Tag)와 수동형 태그(Passive Tag)로 나뉘며 태그의 목적과 용도에 따라 형태가 다양하다.
- 리더(Reader) : 태그에 정보를 요청하며 태그에 데이터의 읽기/쓰기를 진행한다.
- 데이터베이스(Database) : 태그와 관련된 정보를 저장 관리한다.

2. 위협요소 및 고려사항

일반적으로 RFID 통신에서 데이터베이스와 리더 사이의 통신은 안전한 통신 채널을 이용하여 이루어지는 반면에, 태그와 리더 사이의 통신은 안전하지 않은 무선 통신을 사용한다. 하지만 본 논문에서는 데이터베이스와 리더사이의 통신도 안전하지 않은 통신 채널을 이용하기 때문에 각 통신에서의 공격자에 의한 도청 등 여러 공격 가능성이 존재하게 된다. 다음은 RFID 시스템에 대해 공격자가 행할 수 있는 공격 방법들에 대해 알아보고 이런 공격들에 대비하기 위한 RFID 인증 프로토콜을 설계함에 있어 위협요소 및 고려사항에 대하여 알아본다 [7,9].

2.1 위협 요소

- 도청(Eavesdropping) : 각 객체 사이의 통신 방식은 안전하지 않은 통신 채널로 이루어져있어 공격자는 쉽게 통신내용을 엿들을 수 있다.
- 통신내용 분석(Traffic Analysis) : 공격자는

도청을 통해서 얻은 내용을 분석하여 리더의 질의에 대한 태그의 응답을 예측할 수 있다.

- 재전송 공격(Replay Attack) : 도청된 내용을 정당한 객체(태그, 리더, 데이터베이스)에게 재전송함으로써 정당한 객체인 것처럼 가장할 수 있다.
- 위치 확인(Position Detection) : 공격자는 악의적인 리더로 태그의 식별 정보를 취득하여 어떤 태그의 정보인지 판단할 수 있다. 이는 태그 소유자의 위치를 파악하는 방법으로 사용자의 프라이버시를 침해하는 유형중의 하나이다.

2.2 고려사항

- 동기화(Synchronization) : 매 인증 세션마다 갱신되는 데이터들은 정당한 객체들 간의 서로 동기화가 유지되어야 한다.
- 익명성(Anonymity) : 공격자로 인해 도청된 태그는 어떤 태그로부터 데이터가 전송되었는지 확인할 수가 없어야 한다.
- 인증(Authentication) : 각 객체들 사이의 통신은 안전하지 않은 통신 채널을 이용하기 때문에 각 객체들간의 전송된 데이터가 정당한 객체로부터 전송되었는지 확인이 필요하다.
- 효율성(Efficiency) : 저가의 태그에서 연산 능력 및 저장 공간이 제한적인 것을 고려하여, 인증 프로토콜을 설계해야한다.

Ⅲ. 기존 RFID 인증 프로토콜

본 장에서는 기존에 제안된 RFD 인증 프로토콜에 대해 알아보고 2장에서 언급한 위협요소 및 고려사항을 바탕으로 분석한다.

1. Hash-Lock 프로토콜

Hash-Lcok 프로토콜은 MIT에서 제안된 방식으로 태그는 Key의 해쉬 값인 MetaID를 데이터베이스는 Key를 사전에 공유되었다고 가정하며, 인증 프로토콜은 그림 2와 같다. 리더는 태그에게 Query를 전송하면, 태그는 리더에게 MetaID를 전송한다. 태그에게 MetaID를 전송받은 리더는 데이터베이스에게 MetaID를 전송한다. 데이터베이스는 MetaID 값과 같은 ID와Key값을 검색하여 리더에게 전송하면 리더는 Key값만을 태그에게 전송한다. 태그는 리더로부터 전송받은 Key를 해쉬 연산하여 MetaID와 같은지 비교 후 같다면 ID를 리더에게 전송함으로써 모든 인증과정이 이뤄진다 [1].

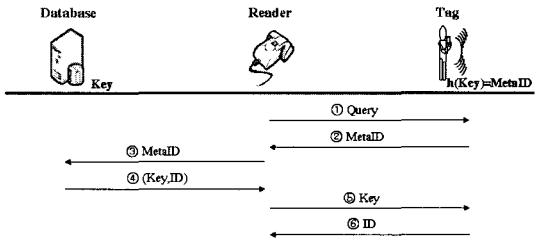

그림 2. Hash-Lock 프로토콜

Hash-Lcok 프로토콜은 일방향 해쉬 함수에 안전성을 기반 하여 제안 되었지만, 리더와 태그간의 통신은 도청이 가능하므로 특정 태그와 정당한 리더간의 통신을 도청한 공격자는 Key를 획득할 수 있으며, 획득한 Key를 태그에게 전송함으로써, 태그의 ID 정보를 얻을 수 있다. 또한 태그 인증시 이용되는 가상 ID인 MetaID를 생성하여 익명성을 보장하려고 하였지만, 매 세션 고정되어 있어 도청하는 공격자들의 재전송 공격이 가능하며, 태그로부터 같은 정보가 출력되어 해당 태그의 위치 확인이 가능하게 된다. 즉, 해쉬 연산을 한번 수행하여 저가의 태그에서의 효율성은 보장되지만, 보안상의 취약점을 내포하고 있다.

2. Hash-based ID Variation 프로토콜

Hash-based ID Variation 프로토콜은 식별 값으로 사용되는 ID를 매 세션 갱신시킴으로써 프라이버시 보호를 하고자 설계되었으며, 인증 프로토콜은 그림 3과 같다. 리더는 태그에게 Query를 전송하면 태그는 TID를 1증가시켜 h(ID), h(TID⊕ID), △TID(△TID= TID-LST)를 계산하여 리더에게 전송한다. 리더는 태그에게 전송받은 데이터를 데이터베이스에게 전송한다. 데이터베이스는 △TID에 LST를 더하여 새로운 TID를 획득 후 h(TID⊕ID)를 계산하여 태그로부터 전송되어진 데이터를 비교 후 같다면 정당한 태그로부터 전송되어졌다고 확인하고 랜덤수 RND를 생성하여 h(RND⊕TID⊕ID)를 계산하여 리더에게 전송한다. 리더는 데이터베이스로부터 전송받은 데이터를 태그에게 전송한다. 태그는 전송된 데이터를 확인하고 같다면 정당한 데이터베이스로부터 전송되어졌다고 인증한다 [3].

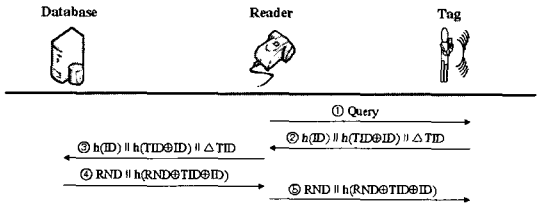

그림 3. Hash-based ID Variation 프로토콜

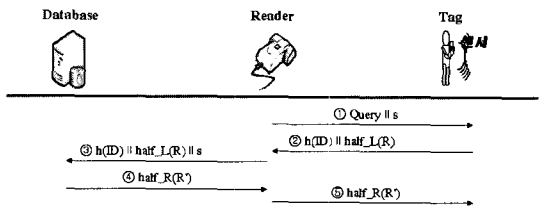

그림 4. Low-Cost 프로토콜

Hash-based ID Variation 프로토콜은 ID를 다양하게 하여 도청을 하는 공격자로부터 프라이버시 침해 및 재전송 공격에도 안전하다. 또한 정상적으로 세션이 종료되면 ID가 갱신되기 때문에 위치 확인이 불가능하다. 하지만 그림 3의 ②번 세션에서 악의적인 제 3자의 공격으로 세션이 차단될 경우 또는 네트워크 문제로 인해 세션이 비정상적으로 종료될 경우에는 ID 갱신이 되지 않아 태그는 같은 h(ID)를 출력하게 된다. 이는 태그의 위치 확인이 가능해짐으로 사용자의 위치 프라이버시 침해가 발생될 수 있다. 또한 ⑤번 세션에서 데이터가 전송이 안 될 경우 데이터베이스는 ID를 갱신시키고 태그는 ID를 갱신시키지 못하게 되므로 ID 갱신의 동기화 문제점이 발생된다.

3. Low-Cost 프로토콜

Low-Cost 인증 프로토콜은 검증 데이터로 쓰이는 데이터를 반으로 쪼개어 각각 이용함으로써 Hash-based ID Variation 프로토콜보다 효율성을 고려한 방식이다. 인증 프로토콜은 그림 4와 같다. 리더는 랜덤수 s를 생성하여 Query와 같이 태그에게 전송한다. 태그는 h(ID)와 $h(s \| ID)=R$을 계산한고 h(ID)와 half_L(R)을 연접하여 리더에게 전송한다.(R은 좌측(half_L(R))과 우측(half_R(R))로 구성된다.) 리더는 태그로부터 전송받은 데이터에 랜덤수 S를 연접하여 데이터베이스에게 전송한다. 데이터베이스는 데이터가 정당한 개체로부터 전송되었는지 확인하기 위해 $h(ID \| s)=R'$을 계산하여 R'의 좌측과 half_L(R)을 비교하여 같다면 R'의 우측을 리더에게 전송한다. 리더는 데이터베이스로 부터 전송받은 데이터를 태그에게 전송한다. 태그는 R'의 우측과 자기 자신의 생성한 half_R(R)을 비교함으로써 인증과정이 이뤄진다.

만약 값이 같다면 $ID \rightarrow ID \oplus (R \| R)$로 ID를 갱신시킨다[7].

Low-Cost 인증 프로토콜은 일방향 해쉬 함수 안전성에 기반 하여 도청을 하는 공격자로부터 프라이버시 보호를 제공하고, 랜덤수 s를 사용하여 재전송 공격에도 안전하다. 또한 정상적으로 세션이 종료될 경우 ID 갱신이 이뤄지기 때문에 위치 확인이 불가능하다. 하지만 Hash-based ID Variation 프로토콜과 마찬가지로 전 세션이 비정상적으로 종료될 경우 태그에서 출력되는 데이터는 h(ID)로 같은 데이터가 출력 되므로 사용자의 위치 확인이 가능하게 된다. 또한 마지막 세션에서 데이터가 전송이 안 될 경우 데이터베이스는 ID를 갱신하고, 태그에서는 ID를 갱신하지 못하게 되므로 ID 갱신의 동기화 문제점이 발생한다.

4. Mutual Authentication 프로토콜

Mutual Authentication 프로토콜은 앞에서 설명한 기존의 방식과는 달리 태그와 리더사이의 통신뿐만 아니라 리더와 데이터베이스사이의 통신도 안전하지 않다고 가정하에 프로토콜이 설계되었다. 인증 프로토콜은 그림 5와 같다. 리더는 랜덤수 r을 생성하여 데이터베이스와 사전에 공유한 k로 r을 해쉬 연산하여 S를 계산한다. 그리고 query와 연접하여 태그에게 전송한다. 태그는 리더로부터 S를 전송받아 ID를 계산하고 리더에게 전송한다. 리더는 태그로부터 전송받은 ID에 S와 r을 연접하여 데이터베이스에게 전송한다. 데이터베이스는 리더와 사전에 공유한 key k로 랜덤수 r을 해쉬하여 S와 같은지 비교 후 같다면 모든 태그의 k1, C 그리고 S를 XOR 연산을 하고 해쉬하여 ID와 같은 데이터를 찾아낸다. 그리고 ID와 같은 데이터의 k2를 해쉬하여 ID'를 계산하고 Data를 $h_k(S)$로 암호화하여 리더에게 전송한다. 리더는 $h_k(S)$로 복호화하여 DATA를 획득하고 ID'를 태그에게 전송한다. 태그는 k2를 해쉬

하여 ID'와 같은지 비교 후 같다면 k1, k2를 갱신시킴으로써 인증과정이 이뤄진다 [10].

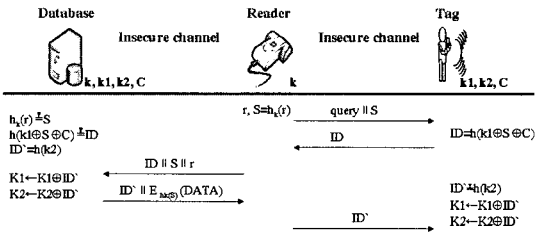

그림 5. Mutual Authentication 프로토콜

Mutual Authentication 프로토콜은 각 개체의 통신의 안전하지 않은 통신 채널을 이용하기 때문에 리더와 태그, 리더와 데이터베이스, 태그와 데이터베이스간의 각각의 인증과정이 이뤄져야하는데, 리더와 데이터베이스이 단방향 인증과, 데이터베이스와 태그 사이의 상호인증만이 이뤄지고 있다. 리더가 데이터베이스에게 전송하는 ID ‖ S ‖ r을 전송할 때 가로채어 차단할 경우 재전송 공격이 가능하다. 그리고 같은 ID가 전송되어 위치 확인도 가능하게 된다. 또한 k1,k2가 갱신되는데 갱신되는 과정에서 k1, k2의 동기화 문제가 발생될 수 있다.

Ⅳ. 제안방식

본 장에서는 기존 인증 프로토콜의 분석을 기반으로 하여 2장에서 언급한 위협요소에 안전하고 고려사항을 만족하는 상호 인증 프로토콜을 제안하고자 한다.

1. 가정사항

본 논문의 인증 프로토콜을 제안하기 위해 다음과 같은 사항을 가정한다.

- 태그는 전력을 공급하여 수행하는 수동형 스마트 태그 이다.
- 태그, 데이터베이스, 리더는 해쉬 함수와 XOR 연산을 수행할 수 있다.
- 태그와 데이터베이스는 태그의 비밀 ID(SIDi)를 사전에 공유한다.
- 태그와 데이터베이스는 태그마다 서로 값이 다른 패스워드(T_key)를 공유한다.
- 정당한 객체(태그, 데이터베이스, 리더)는 그룹키(G_key)를 공유한다.
- 데이터베이스와 리더사이의 통신은 안전하지 않은 통신 채널이다.
- 리더는 랜덤수를 생성할 수 있다.

2. 시스템 계수

다음은 본 프로토콜에 사용되는 시스템 계수이다.

- SID_i : Security ID로써 공개되지 않은 태그의 식별 값 ($i=(1,2,....,n)$, n:태그의 개수)
- T_key : 태그와 데이터베이스가 사전에 공유한 패스워드 ($i=(1,2,....,n)$, n:태그의 개수)
- G_key : 정당한 객체(태그, 데이터베이스, 리더)만이 소유하고 있는 그룹키
- $metaID$: 인증시 태그의 식별 데이터로 사용되는 가상 ID
- R : 리더에서 생성한 랜덤 수
- T_value : 정당한 태그로부터 데이터가 전송되었는지 확인하기 위한 데이터
- R_value : 정당한 리더로부터 데이터가 전송되었는지 확인하기 위한 데이터
- DB_value : 정당한 데이터베이스로부터 전송되었는지 확인하기 위한 데이터
- S : 리더에서 생성한 랜덤수 R을 해쉬 연산 하여 획득하는 값 ($S=h(R \| ts)$)
- ts : timestamp
- $h()$: 안전한 일방향 해쉬 함수
- $\oplus$: XOR 연산
- $\|$: 연접

3. 제안 프로토콜

본 논문의 제안방식1과 2는 각 객체 사이의 통신 채널은 안전하지 않으며, XOR 연산과 해쉬 연산으로 이뤄져 있다. 제안방식2는 제안방식1 보다 태그의 해쉬 연산 횟수를 1회 줄였다. 또한 데이터베이스의 해쉬 연산 횟수도 n+2에서 3회로 줄여 데이터베이스에서의 metaID값을 보다 빠르게 검색할 수 있도록 효율성을 고려하여 제안 하였다.

3.1 제안방식 1의 프로토콜 동작 과정

Step 1. 리더기는 랜덤수 R을 생성 후, $R \oplus G\_key = R\_value$, $h(R \| ts)=S1$를 계산하여 타임스탬프인 ts와 $query$와 연접하여 태그에게 전송한다.(①, ②)

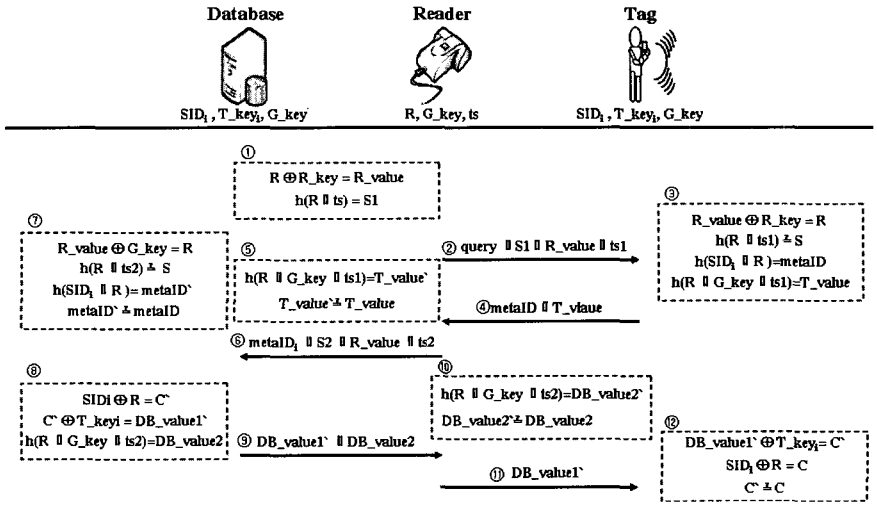

그림 6. 제안방식1 프로토콜

$$query \parallel S1 \parallel R\_value \parallel ts1$$

Step 2. 태그는 정당한 리더로부터 전송되었는지 확인하기 위하여 R_value에 G_key를 XOR연산을 취해 R을 획득하고 리더로부터 전송받은 $ts1$과 연접하여 해쉬를 취해 $S1$과 같은지 비교한다. 같다면 정당한 리더로부터 데이터가 전송되어졌다고 검증하고 $metaID, T_value$를 계산하여 리더에게 전송한다.(③, ④)

$$R\_value \oplus G\_key = R \ , \ h(R \parallel ts1) \stackrel{?}{=} S1$$
$$h(SID_i \parallel R) = metaID$$
$$h(R \parallel G\_key \parallel ts1) = T\_value$$

Step 3. 리더는 태그로부터 전송받은 데이터가 정당한 데이터인지 확인하기 위하여 T_value'를 계산하여 비교 후 같다면 정당한 태그로부터 전송되어졌다고 검증하여 $metaID$에 $S2, R\_value$ 그리고 $ts2$를 연접하여 데이터베이스에게 전송한다.(⑤, ⑥)

$$h(R \parallel G\_key \parallel ts1) = T\_value'$$
$$T\_value' \stackrel{?}{=} T\_value$$

Step 4. 데이터베이스는 정당한 리더에게 전송되었는지 확인하기 위하여 R_value에 G_key를 XOR 연산을 하여 R을 획득한다. 획득한 R에 $ts2$를 연접하여 해쉬 연산을 하여 $S2$와 같은지 비교한다. 만약 같다면 정당한 리더로부터 전송되어졌다고 검증하여 $metaID$를 확인하고 C, DB_value1', DB_value2를 계산하여 DB_value1', DB_value2을 리더에게 전송한다.(⑦, ⑧, ⑨)

$$R\_value \oplus G\_key = R \ , h(R \parallel ts2) \stackrel{?}{=} S2$$
$$all\ Tag \Rightarrow h(SID_i \parallel R) = metaID'$$
$$metaID' \stackrel{?}{=} metaID \ , \ SID_i \oplus R = C'$$
$$C' \oplus T\_key_i = DB\_value1'$$
$$h(R \parallel G\_key \parallel ts2) = DB\_vlaue2$$

Step 5. 리더는 데이터베이스로부터 전송받은 데이터가 정당한 데이터베이스로부터 전송되었는지 확인하기 위하여 DB_value2'를 계산하여 데이터베이스로부터 전송받은 DB_value2와 비교하여 같으면 DB_value1'을 태그에게 전송한다.(⑩, ⑪)

$$h(R \parallel G\_key \parallel ts2) = DB\_vlaue2'$$
$$DB\_value2' \stackrel{?}{=} DB\_value2$$

Step 6. 태그는 리더로부터 전송받은 DB_value1'이 정당한 데이터베이스로부터 전송되었는지 검증하기 위하여 DB_value1'에 T_key_i를 XOR 연산을 취해 C'를 획득한다. 획득한 C'와 태그가 생성한 C와 비교하여 서로 같다면 정당한 데이터베이스로부터 전송되어졌다고 판단되어 인증과정이 종료된다.(⑫)

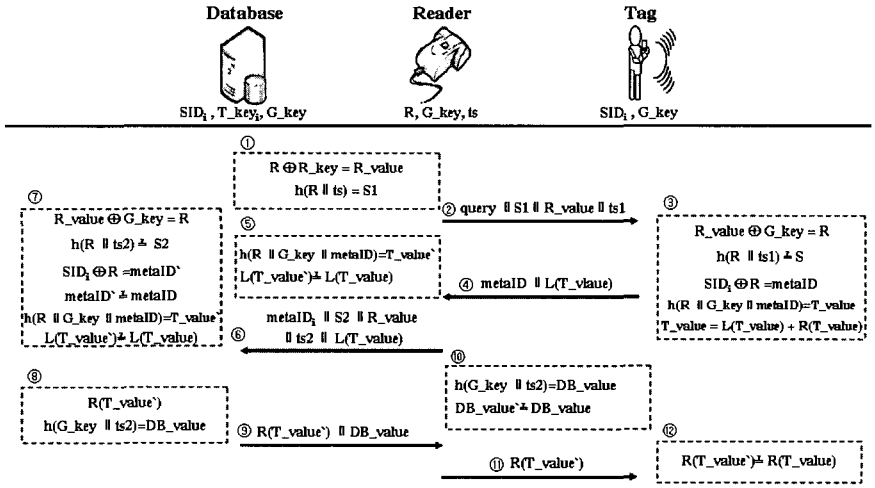

그림 7. 제안방식2 프로토콜

$$DB\_value1' \oplus T\_key_i = C'$$
$$SID_i \oplus R = C$$
$$C' \stackrel{?}{=} C$$

3.2 제안방식 2의 프로토콜 동작 과정

Step 1. 리더기는 랜덤수 R을 생성 후, $R \oplus G\_key = R\_value$, $h(R \| ts) = S1$를 계산하여 타임스탬프인 ts와 $query$와 연접하여 태그에게 전송한다.(①, ②)

$$query \| S1 \| R\_value \| ts1$$

Step 2. 태그는 정당한 리더로부터 전송되었는지 확인하기 위하여 R_value에 R_key를 XOR연산을 취해 R을 획득하고 리더로부터 전송받은 $ts1$과 연접하여 해쉬를 취해 $S1$과 같은지 비교한다. 같다면 정당한 리더로부터 데이터가 전송되어졌다고 검증되고, $metaID$, T_value를 계산하여 리더에게 전송한다.(③, ④)

$$R\_value \oplus G\_key = R \ , \ h(R \| ts1) \stackrel{?}{=} S1$$

$$SID_i \oplus R = metaID$$
$$h(R \| G\_key \| metaID) = T\_value$$
$$T\_value = L(T\_value) + R(T\_value)$$

Step 3. 리더는 태그로부터 전송받은 데이터가 정당한 데이터인지 확인하기 위하여 T_value'를 계산하여 $L(T_value)$와 비교 후 같다면 정당한 태그로부터 전송되어졌다고 검증하여 태그로부터 전송받은 데이터에 $S2$, R_value 그리고 $ts2$를 연접하여 데이터베이스에게 전송한다.(⑤, ⑥)

$$h(R \| G\_key \| metaID) = T\_value$$
$$L(T\_value)' \stackrel{?}{=} L(T\_value)$$

Step 4. 데이터베이스는 정당한 리더에게 전송되었는지 확인하기 위하여 R_value에 R_key를 XOR 연산을 하여 R을 획득한다. 획득한 R에 $ts2$를 연접하여 해쉬 연산을 하여 $S2$와 같은지 비교한다. 만약 같다면 정당한 리더로부터 전송되어졌다고 판단하여 $metaID$를 확인하고 $R(T\_value)'$, DB_value를 계산하여 리더에게 전송한다.(⑦, ⑧, ⑨)

$$R\_value \oplus R\_key = R \ , \ h(R \| ts2) \stackrel{?}{=} S2$$
$$all\ Tag \Rightarrow SID_i \oplus R = metaID'$$
$$metaID' \stackrel{?}{=} metaID$$
$$h(R \| R\_key \| metaID) = T\_value'$$
$$T\_value' = L(T\_value)' + R(T\_value)'$$
$$h(R\_key \| ts2) = DB\_value$$

Step 5. 리더는 데이터베이스로부터 전송받은 데

이터가 정당한 데이터베이스로부터 전송되었는지 확인하기 위하여 DB_value'를 계산하여 데이터베이스로부터 전송받은 DB_value와 비교하여 같으면 $R(T_value)'$을 태그에게 전송한다.(⑩, ⑪)

$$h(R\_key \| ts2) = DB\_vlaue'$$
$$DB\_value' \stackrel{?}{=} DB\_value$$

Step 6. 태그는 전송받은 $R(T_value)'$가 정당한 데이터베이스로부터 전송되었는지 확인하기 위하여 태그가 생성한 T_value의 우측 $R(T_value)$와 비교함으로써 인증과정이 종료된다.(⑫)

$$R(T\_value)' \stackrel{?}{=} R(T\_value)$$

4. 제안 프로토콜 분석

본 제안방식은 리더와 태그사이통신 뿐만 아니라 리더와 데이터베이스와의 통신도 안전하지 않지 않은 통신채널을 이용한다고 가정하에 프로토콜을 설계하였다. 따라서 모든 객체사이의 통신이 이뤄지기 전에 정당한 객체인지 확인하는 과정이 있어야 한다. 따라서 본 논문의 제안방식1과 제안방식2는 각 객체사이의 통신을 할 때 서로 정당한 객체인지 확인하는 과정이 있다.

- 도청에 대한 안전성 : 제안방식 역시 도청이 가능하다. 하지만 일방향성 해쉬 함수를 사용함으로써 도청된 데이터가 악의적인 제 3자에 의해 공격의 기본 정보로 활용할 수 없도록 제안하여 도청에 안전하다.
- 통신내용분석에 대한 안전성 : 일방향성 해쉬 함수와 XOR 연산의 조합으로 각 세션에서 정당한 개체(태그, 리더, 데이터베이스)들로 부터 출력되는 식별데이터를 예측할 수 없기 때문에 통신내용 분석에 안전하다.
- 재전송공격에 대한 안전성 : 태그의 출력이 랜덤수 R로 인해 매 세션 바뀌게 되고 타임스탬프를 사용하여 어느 정도의 시간 간격에서 오버되면 재전송 공격으로 판단할 수 있는 기준이 되어 재전송 공격에 안전하다.
- 위치확인에 대한 안전성 : 매 세션 태그의 식별데이터로 사용되는 *metaID*로 인해 위치 확인에 안전하다.
- 동기화 제공 : 본 제안방식에서는 갱신되는 값들이 없기 때문에 동기화에 대한 문제점이 발생하지 않는다.
- 익명성 제공 : 태그의 metaID를 이용하여 본 제안방식1과 제안방식2에서는 악의적인 제 3자에게 익명성을 제공한다.
- 효율성 제공 : 태그의 해쉬 연산이나 저장하고 있어야할 데이터는 기존의 방식과 차이는 없다. 하지만 제안 방식 1에서는 데이터베이스에서의 태그의 식별데이터를 확인하는 과정에서의 많은 연산이 필요하다.

본 제안방식1의 단점으로는 위에서 언급하였듯이 metaID값을 데이터베이스에서 확인하는 과정에서 태그의 개수만큼의 해쉬 연산 횟수를 취해야 하기 때문에 많은 연산을 필요로 하는 것이 단점이다. 그러나 기존의 데이터베이스들은 데이터의 검색 능력 및 연산 능력이 향상되어 있으므로 이는 크게 문제가 되지 않을 것이다. 또한 제안방식 2에서 서버에서의 태그의 식별값을 획득하는 과정에서 해쉬 연산 대신 XOR 연산을 통해 효율성 및 서버의 부하의 문제를 해결하였다.

표 1. 인증 프로토콜 분석

		도청	통신내용분석	재전송공격	위치확인	동기화	효율성	익명성
Hash-Lock 프로토콜		×	×	×	×	.	○	×
Hash-based ID Variation 프로토콜		○	○	○	△	×	△	△
Low-Cost 프로토콜		○	○	○	△	×	○	△
Mutual Authentication 프로토콜		○	○	○	○	×	△	○
제안방식	제안방식1	○	○	○	○	.	△	○
	제안방식2	○	○	○	○	.	○	○

표 2. 해쉬 연산의 횟수

		태그 해쉬 연산 횟수	리더 해쉬 연산 횟수	데이터베이스 해쉬 연산 횟수
Hash-Lock 프로토콜		1	0	1
Hash-based ID Variation 프로토콜		3	0	3
Low-Cost 프로토콜		2	0	3
Mutual Authentication 프로토콜		2	2	n+2
제안방식	제안방식1	3	4	n+2
	제안방식2	2	4	3

V. 결 론

언제, 어디서나 컴퓨팅능력이 편재되어있는 유비쿼터스 환경에서는 사용자에게 다양한 서비스를 제공하기 위해서 어쩔 수 없이 개인정보를 이용해야 하기 때문에 서비스를 이용하려고 하는 사용자의 프라이버시 침해 소지가 크다. 따라서 보안에 관한 연구가 반드시 뒤따라야 한다. 현재 연구가 진행 되고 있는 것들은 리더와 태그사이의 통신만 불안전하여 리더와 태그사이의 통신에서의 인증이 이뤄지고 있다. 그러나 본 논문에서는 리더와 태그사이의 통신뿐만 아니라 리더와 데이터베이스와의 통신도 안전하지 않다는 가정 하에 인증 프로토콜을 제시하여 태그-리더, 리더-데이터베이스, 데이터베이스-태그 각각의 객체사이의 인증을 할 수 있도록 제안하였다. 하지만 제안된 방식의 경우 물리적 공격 및 다양한 네트워크 공격에 취약할 수 있다. 따라서 향후 연구 방향으로는 보다 다양한 보안 위협에 대해 보안사항과 더불어 보다 현실적인 RFID 태그의 보안 서비스를 위한 인증 방식 연구가 지속적으로 수행되어야 할 것으로 사료된다.

참 고 문 헌

[1] S. Weis, "Security and Privacy in Radio-Frequency Identification Devices", Masters Thesis MIT, 2003.

[2] 정병호, 강유성, 김신효, 정교일, 양대헌, "RFID /USN 환경에서의 정보보호 소고", 한국통신학회지, 제 21권 5호, pp 728-741, 2004.

[3] D. Henrici and P. MÜller, "Hash-based enhancement of location privacy for radio-frequency identification de-vices using varying identifiers", Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp 219-224, 2004.

[4] M. Aigner and M. Feldhofer, "Secure Symmetric Authentication for RFID Tags" Telecommunication and Mobile Computing, 2005.

[5] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems using the AES Algorithm", In Conference of Cryptographic Hardware and Embedded Systems, pp 357-370, 2004.

[6] P. Golle, M, Jakobsson, A Juels and P. Syverson, "Universal re-encryption for mixnets", RSA Conference Cryptographers' Track '04, pp 163-178, 2004.

[7] 황영주, 이수미, 이동훈, 임종인, "유비쿼터스 환경의 Low-Cost RFID 인증프로토콜",한국정보보호학회 하계학술대회, pp 109-114, 2004.

[8] 이상진, 김진, 김광조, "저가형 RFID를 위한 효율적인 프라이버시 보호 기법", 한국정보보호학회 하계학술대회, pp 569-573, 2005.

[9] 유성호, 김기현, 황용호, 이필중, "상태기반 RFID 인증 프로토콜" 한국정보보호학회 논문지 제14권, 제6호, pp. 57-68, 2004.

[10] Jeongkyn Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and Kwangjo Kim, "Mutual Authentication Protocol for Low-cost RFID", Ecrypt Workshop, 2005.

〈著者紹介〉

이 임 영 (Lee, Im-Yeong) 정회원
1981년 8월 홍익대학교 전자공학과 졸업
1986년 3월 오사카대학 통신 공학 전공 석사
1989년 3월 오사카대학 통신공학 전공 박사
1989년 1월 ~ 1994년 2월 한국전자통신연구원 선임 연구원
1994년 3월 ~ 현재 순천향대학교 컴퓨터학부 교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안

박 장 수 (Park, Jang-Su) 학생회원
2004년 2월 : 순천향대학교 정보기술공학부 컴퓨터전공 졸업
2004년 3월 ~ 현재 순천향대학교 전산학과 석사 과정
〈관심분야〉 RFID 보안, 키 관리