Journal of Korea Multimedia Society Vol. 9, No. 5, May 2006(pp. 615-623)

ID 동기화를 가지는 RFID 인증 시스템

박장수[†], 이임영[††]

요 약

최근 다가오는 유비쿼터스 환경에서 RFID 기술은 중요한 위치를 차지할 것이라 예측되어진다. 이로 인해 RFID에 대해 많은 연구가 진행되고 있으며, 물류 유통 뿐만 아니라 금융, 의료, 교통, 문화 등 다양한 분야에서의 활용이 점차 증가되고 있다. 그러나 RFID 시스템에서의 태그와 리더 사이의 통신은 라디오 주파수인 무선통신을 사용하므로 악의적인 제 3자에 의해 식별 정보가 도청될 수 있다. 이러한 도청된 정보는 공격의 기본 정보로 사용되어 질수 있고 이는 사용자의 프라이버시 침해를 가져올 수 있어 사용자들의 RFID 사용을 기피하려고 하고 있다. 이러한 문제점을 해결하기 위해 ID 갱신을 하여 태그의 출력을 다르게 하는 많은 연구가 현재 진행되고 있다. 하지만 기존의 연구에서는 데이터베이스와 태그 사이의 ID 갱신과정에서 ID 동기화를 고려하지 않고 프로토콜이 설계되고 있다. 따라서 본 논문에서는 ID 동기화를 고려하여 RFID 인증 프로토콜을 제안하고자 한다.

RFID Authentication System with ID Synchronization

Jang-Su Park[†], Im-Yeong Lee[††]

ABSTRACT

It has been estimated that 'RFID' technology would be playing an important role in the incoming ubiquitous environment. For this reason, many studies on 'RFID' have been conducted and its application has been on the increase in various fields such as finance, medicine, transportation and culture as well as in logistics distribution. However, the communication between Tag and Reader in RFID system has been conducted by wireless communication of radio frequency so that the information on identification could be eavesdropped by the third party maliciously. Such eavesdropped information could be also used as basic information in attacking others; in this regard, it could impair the privacy of its users and the users have avoided using 'RFID.' To solve theses problems, many studies are being performed to different output of tags by renewing ID. However, protocols have been devised without considering an ID Synchronization in the ID renewal process between database and tag in the existing studies. In this regard, this study has suggested a RFID Authentication Protocol while considering the ID Synchronization.

Key words: RFID(무선인식기술), Authentication(인증), ID Synchronization(ID 동기화)

1. 서 론

현재 다가오는 유비쿼터스(Ubiquitous) 환경에서는 자율 컴퓨팅 기능을 갖는 기기 및 사물 등에 의하여 실시간 상황정보의 분석과 이를 통한 서비스가 이루어질 것이다. 이러한 유비쿼터스 환경에서의 핵심 기술로 현재 주목 받고 있는 기술이 RFID(Radio Frequency Identification)기술이다. RFID 기술은 작은 전자 태그를 사물에 부착하여 사물에 대한 정보나 주위 환경에 대한 다양한 정보를 제공해 주는 것으로

※ 교신저자(Corresponding Author) : 이임영, 주소 : 충남 아산시 신창면 읍내리 순천향 대학교(336-745), 전화 : 041) 542-8819, FAX : 041)530-1548, E-mail : imylee@sch.ac.kr
접수일 : 2005년 11월 14일, 완료일 : 2006년 1월 26일

[†] 순천향대학교 정보기술공학부
(E-mail : pjswise@sch.ac.kr)
[††] 순천향대학교 정보기술공학부

무선 인식 기술을 의미한다.

RFID는 물리적 접촉 없이도 인식이 가능하다는 특징으로 사용자에게 편리성을 제공하는 한편 안전성과 프라이버시 측면에서 기존에 발생하지 않았던 여러 문제점이 발생할 수 있다. 하나의 예로, 리더가 태그의 식별 정보를 요청하고 태그는 식별 정보를 그대로 리더에게 전송하는 경우, 태그와 리더 사이의 통신은 무선 주파수를 이용하기 때문에 식별 정보가 악의적인 제 3자에 의해 쉽게 도청이 가능하다. 또한 악의적인 제 3자는 도청한 정보를 이용하여 분석하면 어떤 태그의 정보라는 것을 확인할 수 있으며, 이는 사용자의 위치 확인이 가능하다. 따라서 사용자의 프라이버시 침해가 발생한다.

프라이버시 침해 문제를 해결하기 위한 방안으로 가장 활발하게 연구가 진행되는 것은 인증 기술을 적용시킴으로써 정당한 태그, 리더, 데이터베이스에게만 정보를 획득할 수 있도록 하여, 프라이버시를 보호하는 것이다. 하지만 저가의 태그는 제한적인 연산 능력과 저장 공간으로 인해 현재 사용되고 있는 대칭키 암호 알고리즘, 공개키 암호 알고리즘 같은 암호 알고리즘들의 사용은 불가능하다. 따라서 자원의 소모가 적으면서도 안전한 암호 알고리즘의 개발과 최소의 자원을 사용하면서도 안전한 프로토콜 개발에 대한 연구가 필요하다.

본 논문에서는 RFID의 프라이버시 문제를 해결하기 위한 기존의 방식들을 살펴보고, 이들의 문제점 분석을 통해 RFID 태그의 연산 능력 및 저장 공간을 고려하여 효율적이고 안전한 방식을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 RFID 시스템 구성과 위협요소 및 고려사항을 기술하고, 3장에서는 RFID 프라이버시에 관한 기존의 연구를 분석한다. 4장에서는 2장에서 언급한 위협요소 및 고려사항에 대해 만족하며, 3장에서의 기존 방식보다 효율적인 방식을 제안 한다. 마지막으로 5장에서는 결론으로 맺는다.

2. RFID 시스템 구성 과 위협요소 및 고려사항

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

2.1 RFID 시스템 구성

앞에서 언급 하였듯이 RFID는 RF(Radio Frequency)를 이용해 태그와 리더가 서로 정보를 주고받는 방식이다. 일반적인 RFID 시스템은 다음의 세 가지 구성요소로 구성된다[2,6,7,8,12].

- 태그(Tag) : IC 칩과 안테나로 구성되어 있으며, 식별 정보를 가지고 있고, 리더의 요청에 응답하여 정보를 전송한다.
- 리더(Reader) : 태그에 정보를 요청하며 태그에 데이터의 읽기/쓰기를 진행한다.
- 데이터베이스(Database) : 태그와 관련된 정보를 저장 관리한다.

2.2 위협요소 및 고려사항

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.

1) 위협 요소

- 도청(Eavesdropping) : 태그와 리더간의 통신 방식은 무선으로 이루어져있어 공격자는 쉽게 통신 내용을 엿들을 수 있고 도청된 정보는 공격의 기본 정보로 활용될 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 리더에게 재전송함으로써 정당한 태그인 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.
- 서비스 거부(Denial of Service) : RFID 시스템이 정상적으로 작동하지 못하도록 하기 위해 태그와 리더간의 RF통신에 특정 주파수를 갖는 방해전파를 방출하여 서비스를 이용하지 못하도록 하는 것이다.
- 물리적 공격(Physical Attack) : 사용되고 있는 태그를 훔치거나 파손시키는 등 물리적으로 이루어지는 공격들을 의미한다.

2) 고려사항

- ID 동기화(ID Synchronization) : 매 인증 세션마다 갱신되는 ID는 태그와 데이터베이스간의 서로 동기화를 유지하여야 한다.

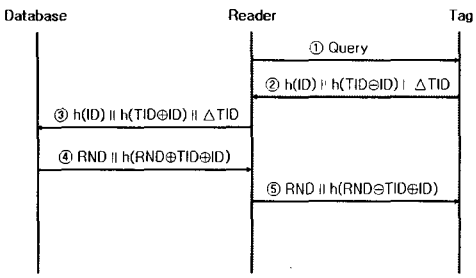

그림 1. Hash-based ID Variation.

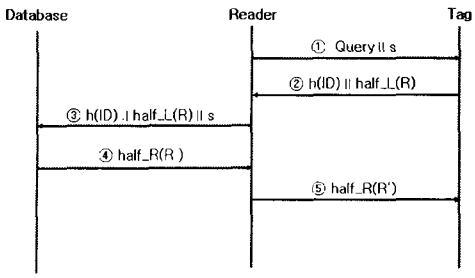

그림 2. Low-Cost.

• 익명성(Anonymity) : 태그와 리더간의 통신은 도청 될 수 있어, 어떠한 태그로부터 정보가 전송되는지 확인가능하다. 따라서 어떤 태그로부터 데이터가 전송되는지 공격자는 확인할 수가 없어야 한다.

• 효율성(Efficiency) : 저가의 태그에서 연산 능력 및 저장 공간이 제한적인 것을 고려하여, 인증 프로토콜을 설계해야한다.

위에서 설명한 위협 요소들 중에서 마지막에 언급한 물리적 공격과 서비스 거부는 RFID 시스템의 기계적/물리적 특성에 기인한 공격방법이며 인증 프로토콜 설계시 고려할 수 있는 사항이 아니므로 본 논문에서는 언급하지 않는다. 또한 고려사항에서의 ID 동기화는 반듯이 이뤄져야할 사항이다. 그 이유는 사용자의 프라이버시를 제공하기 위해 매 인증 세션마다 태그와 데이터베이스에서 ID를 갱신한다. 하지만 갱신된 ID를 태그와 데이터베이스간의 동기화를 제공 못한다면 다음 인증 세션에서 인증과정을 정확하게 수행을 하지 못하기 때문이다.

3. 기존의 RFID 인증 프로토콜

3.1 Hash-based ID Variation 프로토콜

Hash-based ID Variation 프로토콜은 인증 시 이용되는 ID값을 다양하게 함으로써 사용자의 프라이버시 보호를 제공하도록 제안되었다. 인증 프로토콜은 (그림 1)과 같다[2].

Hash-based ID Variation 프로토콜은 ID를 각 인증 세션마다 갱신시킴으로서, 도청에 안전하며, 재전송 공격에도 안전하다. 또한 정상적으로 세션이 종료되면 ID가 갱신되기 때문에 위치 확인이 불가능하다. 하지만 태그에서 전송되는 세션에서 악의적인 제 3자의 공격으로 세션이 차단되거나 네트워크 문제로 세션이 비정상적으로 종료될 경우에는 ID 갱신이 되지 않아 같은 h(ID)를 전송하게 된다. 이는 태그의 위치 확인이 가능해짐으로 사용자의 위치 프라이버시 침해가 발생될 수 있다. 또한 마지막 세션에서 데이터가 전송이 안 될 경우 데이터베이스는 ID를 갱신시키고 태그는 ID를 갱신시키지 못하게 되므로 ID 갱신의 동기화 문제점이 발생된다.

3.3 Low-Cost 프로토콜

Low-Cost 프로토콜은 앞에서 언급한 Hash-based ID Variation 프로토콜에 해쉬 연산을 1번 줄여 효율성을 증가시킨 프로토콜이다. 인증 프로토콜은 (그림 2)와 같다[12].

Low-Cost 프로토콜은 일방향 해쉬 함수를 이용하여 도청에 안전하고, 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 h(ID)로 같은 데이터가 전송 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.

3.4 상태기반 프로토콜

상태기반 프로토콜은 비정상적으로 세션이 종료될 경우에도 사용자의 위치 확인에 안전하게 하기위하여 제안된 프로토콜이다. 태그에는 전 세션이 상태를 나타내는 flag(초기값 0), Query(질의)를 받으면 1씩 증가하는 cnt, 비정상적으로 종료되었을 때 데이터베이스에서 태그를 검색할 수 있도록 사용되는 IK를 포함하고 있다. 인증 프로토콜은 전 세션이 정상적으로 종료되었는지, 비정상적으로 종료되었는지

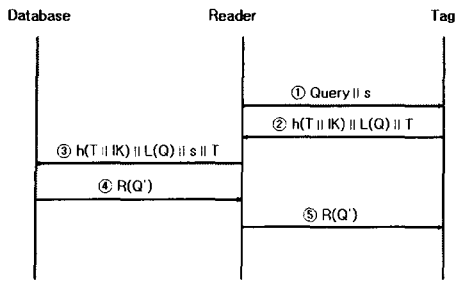

그림 3. 상태기반 flag=1인 경우

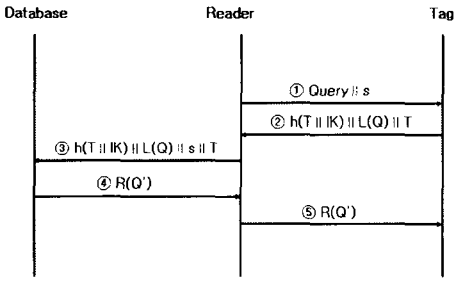

그림 4. 상태기반 flag=1인 경우

에 따라 (그림 3), (그림 4)와 같다[8].

상태기반 프로토콜은 flag를 두어 정상적으로 세션이 종료되지 않았을 때 사용자의 위치 확인에 안전하도록 제안을 두었다. 하지만 flag가 0인 프로토콜의 마지막 세션에서 차단되어 flag가 1인 프로토콜로 수행될 경우 동기화 되지 않은 상태에서 ID를 이용하기에 인증 프로토콜을 수행할 수가 없다.

4. 제안 방식

. 본 장에서는 기존 인증 프로토콜의 분석을 기반으로 하여 2장에서 언급한 위협요소 및 고려사항에 대해 만족하는 상호 인증 프로토콜을 제안하고자 한다.

4.1 가정 사항

본 논문의 제안 방식인 ID 동기화를 가지는 인증 프로토콜을 제안하기 위해 다음과 같은 사항을 가정한다.

- 태그는 전력을 공급하여 수행하는 수동형 스마트태그 이다.
- 태그와 데이터베이스는 해쉬 함수와 XOR 연산을 수행할 수 있다.
- 태그와 데이터베이스는 태그의 비밀 ID(초기값 SID_0)와 태그마다 서로 값이 다른 패스워드(T_key)를 사전에 공유한다.
- 태그와 데이터베이스는 정당한 리더만 가지고 있는 패스워드(R_key)를 공유한다.
- 데이터베이스와 리더사이의 통신은 안전한 채널(그림 5, 6)과 안전하지 않은 채널(그림 7, 8)을 각각 이용한다.
- 리더는 랜덤수를 생성할 수 있다.

4.2 시스템 계수

다음은 본 프로토콜에 사용되는 시스템 계수이다.

- SID_i : 인증을 위한 Security ID로써 공개되지 않은 각 태그의 식별 값 (i : 현재 세션, $i=0,1,2,.....,n$)
- SID_{i+1} : 다음 세션에서 사용되는 SID
- $count$: $query$(질의)를 받을 때 마다 1씩 증가하는 카운터 (초기 값=0)
- $flag$: 전 세션의 상태를 나타내는 값으로, 정상적으로 종료되었다면 0, 비정상적으로 종료되었다면 1로 상태를 표시 (초기 값=0)
- T_ID : $Temporary\ ID$로 비정상적으로 종료되었을 때 사용되는 태그의 임시 식별 값으로 $T_key \oplus R$로 연산하여 획득
- T_key : 태그마다 값이 다른 패스워드
- R_key : 정당한 리더가 소유하고 있는 패스워드로써 모든 리더는 같은 R_key를 갖으며, 정당한 태그와 데이터베이스도 소유
- R : 리더에서 생성한 랜덤수
- T_value : $SID_i \oplus T_key$의 연산으로 획득하는 값으로 정당한 태그로부터 데이터가 전송되었는지 확인하기 위한 데이터로 사용
- R_value : $R_{key} \oplus R$의 연산으로 획득하는 값으로 정당한 리더로부터 데이터가 전송되었는지 확인하기 위하여 사용
- $count\_state$: $flag=0$일때 $count \oplus T_value$과 $flag=1$일때 $count \oplus T_ID$의 데이터로써 $count$의 정보를 전송하기 위해 사용.
- S : 리더에서 생성한 랜덤수 R을 해쉬 연산 하여 회득하는 값 ($S=h(R)$)
- C : $flag=0$일때 $h(T_value \| R \| count)$과 $flag=1$일때 $h(T_ID \| R \| count)$의 데이터로써 전체 길이 C의 1/2의 좌측이 C_L이고, 나머지 1/2의 우측이 C_R
- D : 정당한 데이터베이스로부터 전송되었는지 확인하기 위한 데이터로 사용($D=C\_R \oplus SID_{i+1}$)

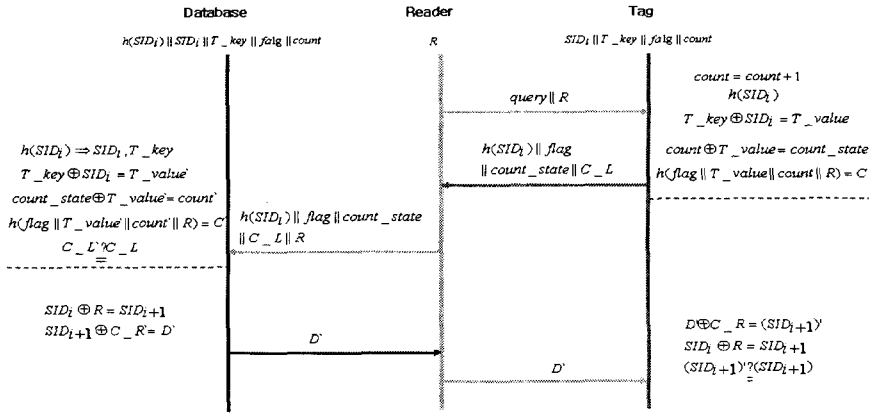

그림 5. 안전한 통신 채널에서의 flag=0

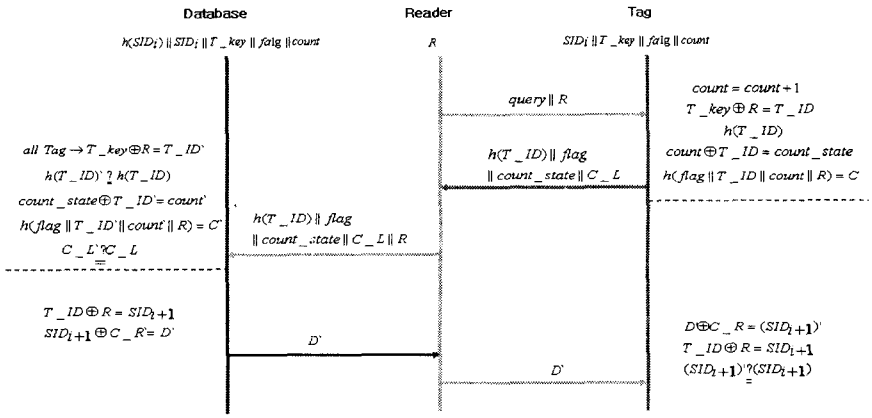

그림 6. 안전한 통신 채널에서의 flag=1

- $h()$: 안전한 일방향 해쉬 함수
- $\oplus$: XOR 연산
- $\|$: 연접

4.3 제안 프로토콜

본 제안 방식은 XOR 연산과 해쉬 연산으로 이루어져 있다. 인증 과정은 크게 데이터베이스와 리더간의 통신이 안전한 통신 채널을 이용할 때의 $flag=0$, $flag=1$과 안전하지 않은 통신 채널을 이용할 때의 $flag=0$인 경우와 $flag=1$인 경우로 총 4 가지로 분류된다.

4.3.1 제안 방식 1

- 안전한 통신 채널에서 전 세션이 정상적으로 종료($flag=0$) 되었을 경우 (그림 5)

Step 1. 리더기는 랜덤수 R을 생성 후, $query$와 연접하여 태그에게 전송한다.

$$query \| R$$

Step 2. 태그는 리더기로부터 $query$를 받으면, $count$에 1을 증가시키고 XOR 연산과 해쉬 연산을 이용하여 $h(SID_i)$, T_vaule, $count\_state$, C를 계산한다. 그리고 $h(SID_i)$, $flag$, C_L, count_state를 연접하여 리더에게 전송한다.

$$SID_i \oplus T\_key = T\_value$$
$$count \oplus T\_value = count\_state$$
$$h(flag \| T\_value \| count \| R) = C$$
$$h(SID_i) \| flag \| C\_L \| count\_state$$

Step 3. 리더는 태그로부터 전송받은 데이터에 R을 연접하여 데이터베이스에게 전송한다.

$$h(SID_i) \| flag \| C\_L \| count\_state \| R$$

Step 4. $h(SID_i)$, SID_i, T_key, $flag$, $count$를 사전에

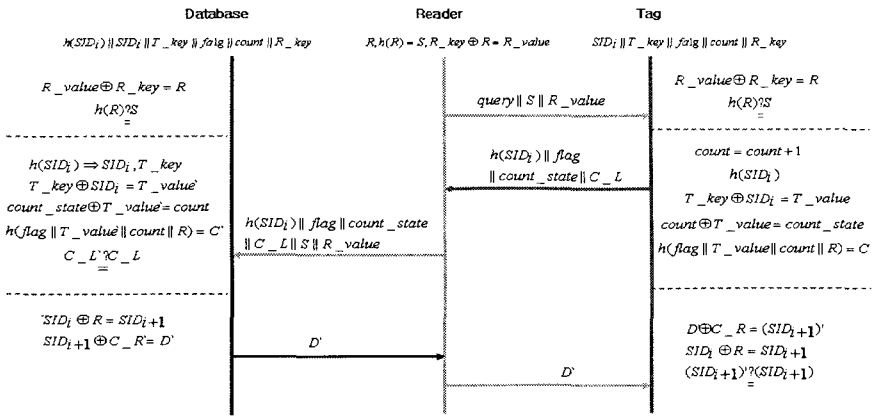

그림 7. 안전하지 않은 통신 채널에서 flag=0

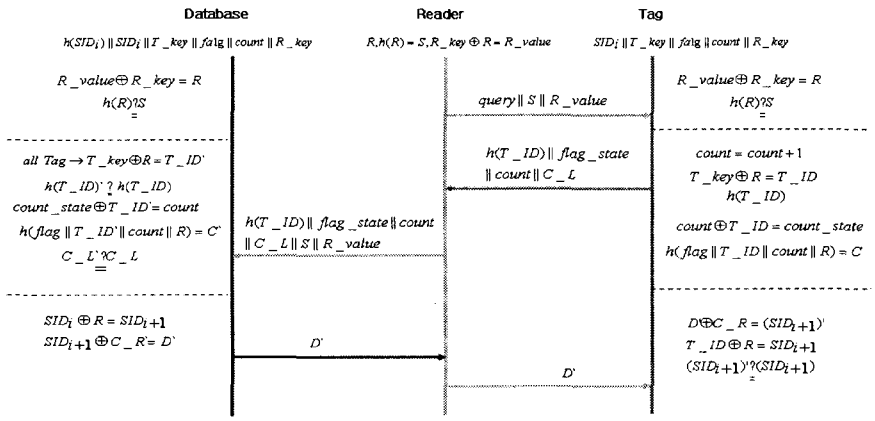

그림 8. 안전하지 않은 통신 채널에서 flag=1

갖고 있는 데이터베이스는 전송받은 데이터중 $h(SID_i)$를 이용하여 SID_i와 T_key를 데이터베이스에서 검색하고, 정당한 태그로부터 데이터가 전송되어 왔는지 확인하기 위하여 XOR 연산과 해쉬 연산을 통하여 T_value'를 계산한다. 그리고 $count_state$에 T_value'를 XOR 연산을 취해 $count$를 획득 하고, C'를 계산하다. C'의 좌측 $C_{_L}'$과 전송된 $C_{_L}$이 같다면 SID_i과 R를 XOR 연산하여 SID_{i+1}를 계산하고, SID_{i+1}에 $C_{_R}'$을 XOR 연산하여 D'를 계산한다. 그리고 리더에게 D'를 전송한다.

$$SID_i \oplus T\_key = T\_value'$$
$$count\_state \oplus T\_value' = count$$
$$h(flag \parallel T\_value' \parallel count \parallel R) = C'$$
$$C_{\_L}' \stackrel{?}{=} C_{\_L}$$
$$SID_i \oplus R = SID_{i+1}$$
$$C_{\_R}' \oplus SID_{i+1} = D'$$

Step 5. 리더는 데이터베이스로부터 전송받은 D'를 태그에게 전송한다.

Step 6. 태그는 전송받은 D'가 올바른 데이터인지 확인하기 위하여 D'에 $C_{_R}$을 XOR 연산하여 SID_{i+1}을 획득한다. 획득한 SID_{i+1}이 정확한 값인지 확인하기 위해서 태그는 자신의 SID_i에 랜덤수 R을 XOR 연산을 하여 $(SID_{i+1})'$을 획득하고 SID_{i+1}와 비교하여 같다면 정당한 데이터베이스로부터 전송되어졌다고 판단하고 ID를 SID_{i+1}로 갱신시킨다.

$$D' \oplus C_{\_R} = SID_{i+1}$$
$$SID_i \oplus R = (SID_{i+1})'$$
$$SID_{i+1} \stackrel{?}{=} (SID_{i+1})'$$

• 안전한 통신 채널에서 전 세션이 비정상적으로 종료($flag=1$) 되었을 경우 (그림 6)

Step 1. 안전한 통신 채널을 이용할 때 $flag=0$인 경우와 동일

Step 2. 태그는 리더기로부터 $query$를 받으면, $count$에 1을 증가시키고 XOR 연산과 해쉬 연산을 이용하여 $h(T\_ID)$, T_ID, $count\_state$, C를 계산한다. 그리고 $h(T\_ID)$, $flag$, C_L, $count_state$를 연접하여 리더에게 전송한다.

$$R \oplus T\_key = T\_ID$$
$$count \oplus T\_ID = count\_state$$
$$h(flag \| T\_ID \| count \| R) = C$$
$$h(T\_ID) \| flag \| C\_L \| count\_state$$

Step 3. 리더는 태그로부터 전송받은 데이터에 R을 연접하여 데이터베이스에게 전송한다.

$$h(T\_ID) \| flag \| C\_L \| count\_state \| R$$

Step 4. 데이터베이스는 각 태그의 T_key와 R을 XOR 연산을 하여 T_ID를 계산한다. 계산된 모든 태그의 T_ID를 해쉬 연산을 하여 전송받은 $h(T_ID)$와 같은 T_ID'를 찾아 $count_state$에 XOR 연산을 하여 $count$를 획득하고, C'를 계산한다. 계산된 C'의 좌측 C_L'과 전송된 C_L이 같다면 SID_{i+1}과 R를 XOR 연산하여 리더에게 D'를 전송한다.

$$\text{all tag의 } T\_key \oplus R = T\_ID'$$
$$h(T\_ID)' \stackrel{?}{=} h(T\_ID)$$
$$count\_state \oplus T\_ID' = count$$
$$h(flag \| T\_ID' \| count \| R) = C'$$
$$C\_L' = C\_L$$
$$T\_ID' \oplus R = SID_{i+1}$$
$$C\_R' \oplus SID_{i+1} = D'$$

Step 5. 안전한 통신 채널을 이용할 때 $flag=0$인 경우와 동일

Step 6. 태그는 전송받은 D'가 올바른 데이터인지 확인하기 위하여 D'에 C_R을 XOR 연산하여 SID_{i+1}을 획득한다. 획득한 SID_{i+1}이 정확한 값인지 확인하기 위해서 태그는 자신의 T_ID에 랜덤수 R을 XOR 연산을 하여 $(SID_{i+1})'$'을 획득하고 SID_{i+1}와 비교하여 같다면 정당한 데이터베이스로부터 전송되어졌다고 판단하고 ID를 SID_{i+1}로 갱신시킨다.

$$D' \oplus C\_R = SID_{i+1}$$
$$T\_ID \oplus R = (SID_{i+1})'$$
$$SID_{i+1} \stackrel{?}{=} (SID_{i+1})'$$

4.3.2 제안 방식 2

• 안전하지 않은 통신 채널에서 전 세션이 정상적으로 종료($flag=0$) 되었을 경우 (그림 7)

Step 1. 리더는 의사 난수 생성기를 이용하여 랜덤 수 R을 생성 한다. 그리고 R과 정당한 리더만이 가지고 있는 R_key를 XOR연산을 취해 R_value를 계산한다. 또한 R을 해쉬 함수를 통해 S를 획득하여 태그에게 전송한다.

$$R\_value = R\_key \oplus R$$
$$h(R) = S$$
$$query \| S \| R\_value$$

Step 2. 태그는 정당한 리더로부터 데이터가 왔는지 확인하기 위하여 다음과 같은 식을 계산한다. 나머지 태그의 연산 과정은 안전한 통신 채널을 이용할 때 $flag=0$인 경우와 동일

$$R = R\_value \oplus R\_key$$
$$h(R) \stackrel{?}{=} S$$

Step 3. 리더는 태그로부터 전송받은 데이터에 R와 R_value를 연접하여 데이터베이스에게 전송한다.

$$h(SID_i) \| flag \| C\_L \| count\_state \| S \| R\_value$$

Step 4. 데이터베이스는 정당한 리더로 전송이 되었는지 확인하기 위하여 데이터를 다음과 같이 확인한다. 나머지 데이터베이스의 연산 과정은 안전한 통신 채널을 이용할 때 $flag=0$인 경우와 동일

$$R = R\_value \oplus R\_key$$
$$h(R) \stackrel{?}{=} S$$

Step 5와 6. 안전한 통신 채널을 이용할 때 $flag=0$인 경우와 동일

• 안전하지 않은 통신 채널에서 전 세션이 비정상적으로 종료($flag=1$) 되었을 경우 (그림 8)

Step 1. 안전하지 않은 통신 채널을 이용할 때 $flag=0$인 경우와 동일

Step 2. 정당한 리더로부터 데이터가 왔는지 확인하는 과정은 안전한 통신 채널을 이용할 때 $flag=0$인 경우와 동일하며, 이후의 연산 과정은 안전한 통신

채널을 이용할 때 $flag=1$인 경우와 동일

Step 3. 리더는 태그로부터 전송받은 데이터에 R와 R_value를 연접하여 데이터베이스에게 전송한다.

$$h(T\_ID) \| flag \| C_{-L} \| count\_state \| S \| R\_value$$

Step 4. 정당한 리더인지 판단하는 과정은 안전하지 않은 통신 채널을 이용할 때 $flag=0$인 경우와 동일하며 이후의 연산 과정은 안전한 통신 채널을 이용할 때 $flag=1$인 경우와 동일

Step 5. 6. 안전한 통신 채널을 이용할 때 $flag=1$인 경우와 동일

4.4 제안 프로토콜 분석

본 제안 방식은 데이터베이스와 리더사이의 통신은 안전한 채널을 이용할 때와, 안전하지 않은 채널을 이용할 때로 분류하여 프로토콜을 설계하였다.

ID 동기화를 가지는 인증 프로토콜은 XOR 연산과 해쉬 연산으로 구성되어진다. 안전한 채널을 이용할 때에는 2번의 해쉬 연산을 수행하고 안전하지 않은 채널을 이용할 때에는 3번의 해쉬 연산을 수행한다.

- 도청에 대한 안전성 : 제안 방식 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 통신내용분석에 안전하다.
- 재전송공격에 대한 안전성 : 태그의 출력이 $count$, R 그리고 갱신되는 SID로 인해 항상 가변적이기 때문에 재전송 공격에도 안전하다.
- 위치확인에 대한 안전성 : 식별 데이터로 사용되는 SID_i와 T_ID가 항상 변하기 때문에 사용자의 위치 확인이 불가능하다.
- ID 동기화 제공 : 갱신되는 ID값으로 인증하고, T_ID를 이용하여 SID를 갱신시키기 때문에 ID 동기화 문제도 해결된다.
- 익명성 제공 : 갱신되는 ID 또는 T_ID 를 사용하여 태그를 식별하기 때문에 악의적인 제 3자는 어떠한 태그로부터 전송되었는지 확인할 수 가 없다.
- 효율성 제공 : 정상적으로 세션이 종료되었을 경우에는 정당한 태그인지 식별하기 위한 데이터베이스 연산이 효율적으로 이뤄지는 반면 비정상적으로 세션이 종료 되었을 때의 데이터베이스 연산은 연산량이 많아진다.

표 1. 인증 프로토콜 분석

		도청	통신내용분석	재전송공격	위치확인	ID 동기화	효율성	익명성
Hash-based ID Variation 프로토콜[2]		○	○	○	X	X	△	X
Low-Cost 프로토콜[12]		○	○	○	X	X	○	X
상태기반 프로토콜[8]		○	○	○	○	X	△	○
제안방식	제안방식1	○	○	○	○	○	○	○
	제안방식2	○	○	○	○	○	△	○

[○ : 안전, 제공 △ : 보통의 효율성 제공 X : 취약, 제공 못함]

표 2. 해쉬 연산의 횟수

		태그 해쉬 연산 횟수	리더 해쉬 연산 횟수	데이터베이스 해쉬 연산 횟수
Hash-based ID Variation 프로토콜[2]		3	0	3
Low-Cost 프로토콜[12]		2	0	3
상태기반 프로토콜[8]		3	0	4
제안방식	제안방식1	2	0	3
	제안방식2	3	1	4

본 방식의 단점으로는 위에서 언급하였듯이 세션이 비정상적으로 종료되었을 때, 식별 데이터로 쓰이는 T_ID를 데이터베이스에서의 모든 ID와 비교하는 것이다. 그러나 기존의 데이터베이스들은 데이터의 검색 능력이 향상되어 있으므로 이는 크게 문제가 되지 않을 것으로 사료된다.

5. 결 론

향후 다가오는 유비쿼터스 환경에서 주목받고 있으며, 현재 많은 연구가 진행 중에 있는 무선 통신 기술인 RFID는 비접촉식이라는 장점으로 바코드를 대체하여 사용될 수 있지만 사물 인식 과정에서 무선

통신으로 데이터를 주고받을 수 있다는 점에서 사용자의 프라이버시 침해의 가능성을 갖는다. 더욱이 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.

따라서 본 논문에서는 2장에서의 언급한 위협사항 및 고려사항을 최대한 만족하는 RFID시스템에서의 ID 동기화를 가지는 인증 프로토콜을 제안하였다. 그러나 제안된 방식의 경우 여전히 프로토콜 물리적 공격에는 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] A. Juels and R. Pappu, "Squealing euros: Privacy Protection in RFID-enabled banknotes," *In Proceedings of Financial Cryptography*, Vol. 2742 LNCS, pp. 103-121, 2003.

[2] D. Henrici and P. Müller, "Hash-based enhancement of location privacy for radio-frequency identification de-vices using varying identifiers," *PerSec'04 at IEEE PerCom*, pp. 219-224, 2004.

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

[4] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems using the AES Algorithm," *In Conference of Cryptographic Hardware and Embedded Systems*, Vol. 3156 LNCS, pp. 357-370, 2004.

[5] P. Golle, M, Jakobsson, A Juels, and P. Syverson, "Universal re-encryption for mixnets," *RSA Conference Cryptographers' Track '04*, Vol.2964 LNCS, pp. 163-178, 2004.

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

[7] 박장수, 이임영, "RFID에 기반한 안전한 디바이스 인증 프로토콜에 관한 연구," 한국정보처리학회 춘계학술발표대회, 제12권, 제1호, pp. 1151-1154, 2005.

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

[9] 이상진, 김진, 김광조, "저가형 RFID를 위한 효율적인 프라이버시 보호 기법," 한국정보보호학회 하계학술대회, 제15권, 제1호, pp. 569-573, 2005.

[10] 정병호, 강유성, 김신효, 정교일, 양대헌, "RFID/USN 환경에서의 정보보호 소고," 한국통신학회지, 제21권, 제5호, pp. 728-741, 2004.

[11] 한승우, 최재귀, 박지환, "효율적인 식별기능을 갖는 RFID 가변 정보화 방식," 한국멀티미디어학회 춘계학술발표대회, 제7권, 제1호, pp. 61-64, 2004.

[12] 황영주, 이수미, 이동훈, 임종인, "유비쿼터스 환경의 Low-Cost RFID 인증프로토콜," 한국정보보호학회 하계학술대회, 제14권, 제1호, pp. 109-114, 2004.

박 장 수

2004년 2월 순천향대학교 정보기술공학부 컴퓨터전공 학사

2004년 3월~현재 순천향대학교 전산학과 석사 과정

관심분야 : RFID 보안, 키 관리

이 임 영

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