익명성을 제공하는 RFID 상호 인증 프로토콜에 관한 연구

강수영*, 이임영

순천향대학교, 컴퓨터학부

A Study on RFID Mutual Authentication Protocol with Anonymity

Soo-Young Kang*, Im-Yeong Lee

Department of Computer SoonChunHyang Univ.

요 약

최근 인터넷의 급성장에 따라 새로운 유비쿼터스 환경을 기반으로 다양한 연구들이 수행되고 있다. 특히 유비쿼터스의 핵심기술로써 RFID는 큰 비중을 차지하고 있으며 국내뿐만 아니라 국외에서도 활발한 연구가 진행되고 있다. 그러나 RFID는 불법적인 공격자로부터 공격을 당할 경우 정보가 노출되어 사용자의 프라이버시 침해의 문제점을 가지고 있다. 따라서 본 논문에서는 태그의 가상 ID를 간단한 연산을 취하여 매번 다른 값을 출력함으로써 사용자의 익명성을 제공하며, 가변적인 값이 노출되므로 위치 추적에 안전한 방식이다. 또한 ID를 갱신하지 않고 가변적인 값을 생성하므로 동기화에 대한 문제점을 해결하여 안전하고 효율적으로 상호 인증을 제공하는 방식을 제안한다.

I. 서론

유비쿼터스(Ubiquitous) 환경이란 '언제, 어디서나'라는 뜻의 라틴어에서 유래된 말로 핸드핼드형 디바이스를 사용하여 시간과 장소에 구애 받지 않고 서비스를 제공받을 수 있는 환경을 의미한다. 이러한 유비쿼터스 환경에서 많은 기술들의 연구가 진행되고 있으며 가장 주목을 받는 기술로 RFID(Radio Frequency IDentification) 기술을 꼽을 수 있다.

RFID 기술은 유비쿼터스 센서 구성을 위한 핵심기술로 무선 주파수 인식 기술이다. 저전력이며 소형화된 디바이스 기술로 금융, 의료, 교통, 문화 등 다양한 분야에 응용되고 있는 차세대 인식 기술이라고 할 수 있다.

RFID 기술은 신속성 및 정확성으로 사용자에게 편리성을 제공할 수 있지만 무선 주파수 통신으로 인하여 도청에 취약하다는 단점을 가지고 있다. 따라서 통신 채널을 안전하게 하여 프라이버시를 보호해야 한다.

본 논문에서는 태그의 식별 값을 매번 변화 시켜 태그의 익명성을 제공하며 태그와 데이터베이스 간에 상호 인증을 제공하고자 한다. 2장에서는 RFID의 위협요소 및 요구사항에 대하여 기술하고 3장에서는 기존 방식 분석, 4장에서는 제안 방식에 대하여 분석 및 비교한 후 5장에서 결론과 향후 연구 방향에 대하여 논의한다.

II. 위협요소 및 요구사항

RFID 시스템에서 태그와 리더는 무선 기술을 사용하기 때문에 많은 공격을 당할 가능성을 가지고 있다. 무선 주파수 통신 채널에서의 도청으로 인한 데이터 위조 및 변조를 방지하고 다양한 공격에 대응할 수 있는 방안에 대한 연구가 반드시 필요하다. 따라서 RFID 시스템에서 발생할 수 있는 위협요소에 대하여 알아보고 이에 대응하기 위하여 만족해야 할 보안 요구사항에 대하여 정의하겠다.

1. RFID 시스템의 위협요소

RFID 시스템은 무선 주파수 통신으로 다음과 같은 위협요소를 가지고 있다.

- 도청(Eavesdropping) : 태그와 리더 간의 무선 통신으로 불안전한 채널에서 전송되는 데이터에 대하여 악의적인 제 3자가 데이터를 획득하는 공격 유형이다.

- 트래픽분석(Traffic Analysis) : 태그의 정보를 직접 노출시키지 않더라도 도청된 태그의 응답 값들을 종합하고 분석하여 정보를 획득하는 공격 유형이다.
- 재전송공격(Replay Attack) : 도청한 값을 다시 전송함으로써 얻고자하는 값을 획득하는 공격 유형이다.
- 트래킹공격(Tracking Attack) : 태그의 응답 값이 고정되어 있을 경우 이를 기반으로 태그의 위치를 추적할 수 있는 공격 유형이다.

2. RFID 시스템의 요구 사항

RFID 시스템은 다음과 같은 보안 요구 사항을 만족하여야 한다.

- 인증(Authentication) : 어떠한 객체가 정당한 객체인지 모르는 상황에서 정당한 객체만이 획득하거나 생성할 수 있는 값을 전송함으로써 정당하다는 것을 인증 받아야 한다.
- 익명성(Anonymity) : 전송되는 정보가 노출되어도 어떠한 태그로부터 전송된 정보인지 알 수 없어야 한다.
- 무결성(Integrity) : 전송되는 태그의 정보에 대해서 전송되는 도중에 위조 및 변조되지 않았다는 것을 증명해야 한다.
- 효율성(Efficiency) : 저가의 수동형 태그에서의 연산 가능해야 한다.
- 동기화(Synchronization) : 각 객체들이 통신을 시작하는 시간이 동일해야 하며 갱신되는 값들의 변화가 동일해야 한다.

III. 기존방식 분석

RFID 보안에 관련된 연구는 유비쿼터스 환경과 더불어 많은 주목을 받고 있으며 이와 관련된 많은 연구가 진행되고 있다. 그 중 기존 연구인 Low-Cost 인증 방식과 Mutual 인증 방식에 대해서 기술하고 각 방식들의 동작 과정 및 특징에 대해서 분석하겠다.

1. Low-Cost 인증 방식

본 방식은 MIT에서 제안한 Hash-Lock 방식에서 사용된 3번의 해쉬 연산을 2번으로 줄여 저가의 태그에서 구현 가능하고 태그에 보안을 제공하는 방식이다[4].

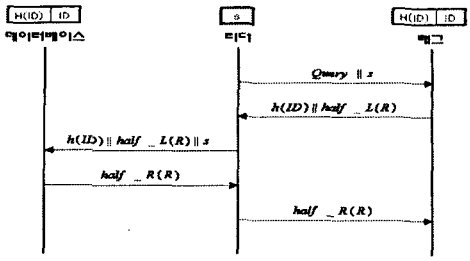

그림 1: Low-Cost 인증방식

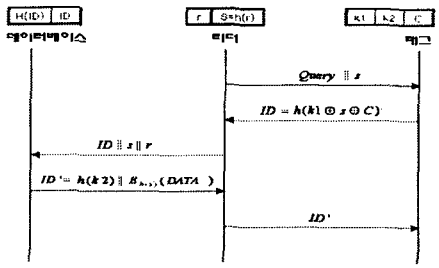

그림 2: Mutual 인증 방식

태그는 리더가 전송한 랜덤수와 ID를 해쉬하고 왼쪽 반값을 데이터베이스로 전송하여 태그를 인증하고 응답 값으로 오른쪽 반값을 태그에게 전송하여 인증 과정을 수행한다. 해쉬 연산을 1회 줄여 효율성 및 안전성을 제공하지만 비정상적 종료시 익명성을 제공하지 못하며 ID 갱신에 있어서 동기화 문제가 발생한다.

2. Mutual 인증 방식

본 방식은 태그와 리더 간의 통신 채널과 리더와 데이터베이스 간의 통신 채널 모두 불안전하다는 가정 하에 제안된 방식이다[3].

정당한 객체가 사전에 공유한 두 개의 비밀키와 리더가 생성한 랜덤수를 사용하여 태그와 데이터베이스 간의 상호 인증을 제공한다. 가변적인 값과 비밀키에 기반하여 태그의 안전성이 제공되지만 비정상적 종료시 갱신되지 않은 식별 값의 사용으로 익명성을 제공할 수 없으며 키의 갱신에 있어서 앞의 방식과 마찬가지의 동기화 문제가 발생한다.

IV. 제안 방식

본 장에서는 앞서 기술된 방식들의 취약점을 보완하여 태그의 익명성을 제공하며 태그와 데이터베이스 간의 상호 인증 방식을 제안한다.

1. 가정사항

본 프로토콜은 다음과 같은 가정사항을 기반으로 이루어진다.

- 사전단계에 정당한 객체(태그, 리더, 데이터베이스)만이 그룹키를 안전하게 공유한다.
- 태그와 데이터베이스는 해쉬 함수를 가지고 있으며 XOR 연산이 가능하다.
- 리더는 타이머를 탑재하여 태그에게 신호를 보내는 시간을 생성할 수 있다.
- 랜덤수와 타이머가 생성한 타임스탬프는 같은 형식으로 차 연산이 가능하다.
- 태그와 리더 간의 통신 채널은 무선 채널로써 불안전하다.

2. 시스템계수

- GK : 정당한 객체가 사전에 공유한 그룹키
- TS : 리더의 타이머에서 생성된 타임스탬프
- r : 리더에서 생성한 랜덤수
- $\triangle r$: SID를 생성하기 위한 가변적인 값
- ID : 각각의 태그마다 고유한 식별 값
- $metaID$: ID를 안전하게 해쉬한 값
- SID : $Secret\ ID$로 가변적인 식별 값
- R_Value1 : 리더가 생성한 값으로 랜덤수를 안전하게 전송하기 위한 값
- R_Value2 : 리더가 생성한 값으로 타임스탬프를 안전하게 전송하기 위한 값
- T_Value : 태그가 생성한 값으로 데이터베이스에서 태그를 인증할 때 사용되는 값
- DB_Value : 데이터베이스가 생성한 값으로 태그에서 데이터베이스 인증 시 사용되는 값

3. 제안 프로토콜

본 방식은 랜덤수 r과 타임스탬프 TS를 이용하여 태그의 ID를 매 세션 변형시킴으로써 태그의 익명성을 제공하며 동기화 문제가 발생하지 않는 상호 인증 프로토콜을 제안한다.

① 리더는 그룹키 GK와 랜덤수 r를 XOR 연산하여 R_Value1을 생성하고 GK와 타임스탬프 TS를 XOR 연산하여 R_Value2를 생성한다. 또한 r과 TS의 무결성을 제공하기 위하여 두 값을 연접하여 해쉬한 값을 태그에게 전송한다.

$$R\_Value1 = GK \oplus r$$

$$R\_Value2 = GK \oplus TS$$

$$R\_Value1 \| R\_Value2 \| H(r \| TS)$$

② 태그는 R_Value1과 R_Value2에 GK를 XOR 연산하여 r과 TS를 획득하고 해쉬된 값으로 r과 TS를 검증한다. 그 후 r과 $metaID$를 연접하여 해쉬한 T_Value를 생성하고 매 세션 변화하는 SID를 생성하여 리더에게 전송한다.

$$R\_Value1 \oplus GK = r$$

$$R\_Value2 \oplus GK = TS$$

$$T\_Value = H(r \| metaID)$$

$$SID = \triangle r \oplus metaID$$

$$T\_Value \| SID$$

③ 태그리더는 태그로부터 온 값과 태그에게 전송한 r과 TS를 연접하여 데이터베이스에 전송한다.

$$T\_Value \| SID \| r \| TS$$

④ 데이터베이스는 리더로부터 전송되어 온 r과 TS의 차를 구하여 가변적인 $\triangle r$을 획득하고 T_Value를 검증한다. 값이 일치할 경우 태그를 인증하고 $metaID$에 매칭되는 ID와 GK, TS를 연접하여 해쉬한 DB_Value를 생성하여 리더에게 전송한다.

$$SID \oplus \triangle r = metaID$$

$$DB\_Value = H(ID \| GK \| TS)$$

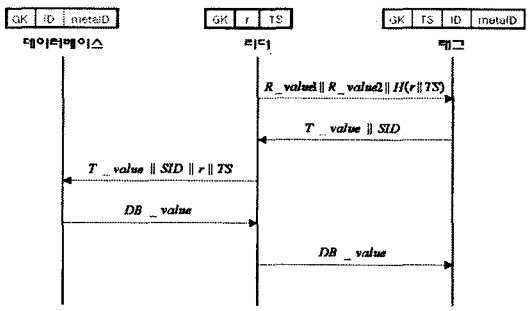

그림 3: 제안 방식

⑤ 리더는 데이터베이스로부터 온 값을 태그에게 전송한다.

$$DB\_Value$$

⑥ 태그는 리더로부터 전송된 DB_Value와 자신의 ID, GK, TS를 해쉬한 값을 비교하고 일치할 경우 데이터베이스를 인증한다.

$$DB\_Value \stackrel{?}{=} H(ID||GK||TS)$$

4. 제안 프로토콜 분석

앞서 기술한 기존의 연구들과 제안 방식을 비교하고 그 분석 결과는 표 1과 같다.

- 인증 : 데이터베이스는 SID와 T_Value를 전송받고 SID를 이용하여 T_Value를 검증하고 태그는 ID와 GK, TS를 이용하여 DB_Value를 검증한다. 따라서 태그와 데이터베이스는 상호 인증을 제공한다.
- 익명성 : $\triangle r$을 이용하여 매 세션 태그의 식별 값인 SID를 변형시킴으로써 태그의 익명성을 제공한다.
- 무결성 : 해쉬 함수를 사용하여 전송되는 데이터의 위조 및 변조에 대한 무결성을 제공한다.
- 효율성 : 해쉬 함수와 XOR 연산을 이용하므로 태그에서 구현 가능하며 데이터베이스에서 태그의 식별 값을 한 번의 검색으로 획득하므로 데이터베이스의 효율성도 제공한다.
- 동기화 : 리더에서 태그와 통신을 시작하는 시간인 TS를 생성하여 사용하고 식별 값의 갱신이 없으므로 동기화를 제공한다.

표 1: 각 방식별 비교 분석

	Low-Cost 인증 방식	Mutual 인증 방식	제안 방식
도청	불가능	불가능	불가능
트래픽분석	가능	가능	불가능
재전송공격	불가능	가능	불가능
트래킹공격	가능	가능	불가능
인증	제공	제공	제공
익명성	부분 제공 못함	부분 제공 못함	제공
무결성	제공 못함	제공 못함	제공
효율성	제공	제공 못함	제공
동기화	제공 못함	제공 못함	제공

V. 결론 및 향후 연구 방향

본 논문에서는 차세대 IT 기반의 유비쿼터스 환경에서의 RFID 기술을 적용하는데 있어서 프라이버시의 문제점을 해결하고자 연구를 수행하였다. 특히 유비쿼터스 환경과 같은 사용자 중심의 네트워크를 형성하기 위해서는 소형 디바이스 기술이 요구되고 있으며 이와 더불어 사용자 프라이버시 보호를 만족할 수 있는 보안 기술이 반드시 필요하다. 따라서 본 방식은 매 세션 가변적인 값을 사용하여 사용자의 익명성을 제공하며 일반화된 해쉬 함수와 XOR 연산을 사용하여 저가의 태그에서 구현 가능하도록 제안하였다. 기존 방식들에 비하여 전방향 채널에서도 안전하게 데이터를 전송하며 식별 값의 갱신을 사용하지 않으므로 동기화에 대한 문제가 발생하지 않는다는 장점을 가지고 있는 반면, 저가의 태그에서 타임스탬프를 비교하기 위한 메모리 공간이 필요하다는 취약점을 가지고 있다. 하지만 향후 RFID 태그의 발달로 공개키 암호 알고리즘의 탑재가 가능하기 때문에 메모리 공간에 대한 문제는 수년 내에 해결 가능할 것이다.

향후 RFID 기술은 지금보다 훨씬 더 많은 분야에서 응용될 핵심기술로, 많은 분야에서 응용되기 위해서는 프라이버시 보호가 가장 큰 과제라고 할 수 있다. 따라서 경량화 된 프로토콜로 보안을 제공할 수 있는 방안에 대한 연구가 지속적으로 진행되어야 할 것이다.

참고문헌

[1] D.Henrici , P.Muller, "Hash-based Enhancement of Locatoin Privacy for Radio-Fre-quency Identification Devices using Varying Identification", *PerSec'04 IEEE PerCom*, pp.149-153, Mar. 2004

[2] Istvan Vajda, Levente Buttyan, "Lightweight Authentication Protocols for Low-Cost RFID Tags", *Proceedings of the Second Workshop on Security in Ubiquitous Computing , Conjunction with Ubicomp 2003*, Oct. 2003

[3] JeongKyn Yang, Jaemin Park, Hyunrok Lee, Kui Ren, Kwangjo Kim, "Mutual Authentication Protocol for Low-cost RFID", *Ecrypt Workshop*, 2004

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