저가에서의 효율적인 RFID 인증 프로토콜

박장수*, 이임영

순천향대학교 컴퓨터학부

A Study on Authentication Protocol in RFID System

Jang-Su Park*, Im-Yeong Lee

Division of Computer, SoonChunHyang University

요 약

RFID 기술은 유비쿼터스(Ubiquitous)환경에서의 핵심적인 기술로 인정받아 중요한 위치를 차지하고 있지만 RFID 태그의 정보가 쉽게 노출된다는 기본적인 특징으로 인해 사용자의 프라이버시 침해 위협이 발생할 수 있다. 따라서 현재 사용자의 프라이버시 보호에 관한 연구가 활발히 진행중에 있다. 하지만 저가의 태그에서는 연산량과 저장 공간이 제한적이기 때문에 기존방식들을 이용하기에는 많은 어려움이 있다. 본 논문에서는 저가의 태그에서 효율적으로 이용될 수 있는 RFID 인증 프로토콜을 제안하고자 한다. 우리가 제안하는 방식은 저가의 태그에서 연산량을 고려하여 XOR 연산으로만 구성되어 있다.

I. 서론

최근 언제, 어디서나 컴퓨팅 능력이 편재되어 사용자에게 편리성을 제공하는 유비쿼터스 환경에 대해 많은 관심을 갖고 활발히 연구 중에 있다. 이러한 유비쿼터스 환경에서 가장 주목을 받고 있는 기술은 RFID (Radio Frequency Identification)기술이다. RFID는 초소형 반도체에 식별정보를 넣고 무선주파수를 이용해 이 칩을 지닌 객체를 판독·추적·관리할 수 있는 기술을 말한다. RFID는 저전력이고, 작은 크기에, 어디서나 통신이 가능하다. 또한 데이터 저장 및 읽기/쓰기가 가능하고, 한 번에 여러 개의 데이터를 식별할 수 있다는 장점을 가지고 있어 물류, 금융, 의료, 교통, 제조 등 다양한 분야에서 사용되어질 것으로 예측되어진다[6,7].

그러나 IT 기술이 편리함을 가져다 준 반면 이에 대한 역기능이 발생하였듯이 RFID 기술에서도 보안에 관하여 고려하지 않고 서비스를 제공한다면 사용자에게 편리성을 제공하겠지만, 디바이스들 간의 오작동, 도청, 프라이버시 위협 등 다양한 문제점이 발생하여 RFID 기술의 활성화를 방해하는 장애물로 대두될 것이라 생각되어지므로, 이에 대한 대응책 마련이 시급하다.

따라서 본 논문에서는 RFID 인증 프로토콜을 제안하여 사용자의 프라이버시를 보호하고자 한다. 저가의 태그는 저장 공간과 연산량이 매우 한정적이기 때문에 기존에 사용되고 있는 암호화 기법들을 적용하지는 못한다. 이에 따라서 제안방식은 저가의 태그에서 효율적인 RFID 인증 프로토콜로써 XOR 연산으로만 이루어진다.

본 논문의 구성은 다음과 같다. 2장에서는 RFID 시스템의 위협요소 및 고려사항에 대하여 알아본다. 3장에서는 기존 방식을 분석하고, 4장에서는 RFID 인증 프로토콜을 제안한다. 마지막으로 5장에서는 결론을 맺는다.

II. RFID의 위협요소 및 고려사항

본 장에서는 RFID 시스템의 위협요소 및 고려사항에 대하여 알아본다. 일반적인 RFID 시스템은 식별정보를 가지고 있으며 리더의 요청에 응답하는 태그(Tag), 태그에 정보를 요청하며 태그의 데이터의 읽기/쓰기를 진행하는 리더(Reader), 태그의 관련 정보를 저장하고 가공하는 데이터베이스(Database)로 구성되어있으며, 다음과 같은 위협요소 및 고려사항을 가질 수 있다[3,4,5,8].

- 도청(Eavesdropping) : 태그와 리더간의 통

신방식은 무선으로 이루어져있어 공격자는 쉽게 통신내용을 엿들을 수 있다.

- 통신내용분석(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.
- 동기화(Synchronization) : 식별데이터를 매 세션마다 갱신을 하는데, 태그와 데이터베이스간의 갱신되는 값의 서로 동기 되어야 한다. 그 이유는 다음 세션에서 인증을 정확하게 수행할 수 있기 때문이다.
- 효율성(Efficiency) : 저가의 태그에서 연산능력 및 저장 공간이 제한적인 것을 고려하여, 인증 프로토콜을 설계해야한다. 또한 데이터베이스나 리더에서의 연산이 효율적으로 이뤄져야한다.

Ⅲ. RFID 인증의 기존 연구

본 장에서는 기존에 연구되었던 방식을 2장에서의 언급한 위협사항 및 고려사항을 토대로 분석한다.

3.1 Hash-Lock 프로토콜

Hash-Lcok 프로토콜은 낮은 태그 가격을 고려하여 MIT에 의해 제시된 방식으로 Key, MetaID를 태그와 데이터베이스와 사전에 안전하게 공유되어 있다고 가정한다[5].

이 방법은 일방향 해쉬 함수에 기반하여, 효율성을 고려하였고, 익명성을 제공하기 위해 MetaID를 사용하였다. 하지만 태그의 식별값인 MetaID가 고정되어 있어, 출력되는 데이터가 같아 해당 태그로부터 데이터가 전송되었는지를 확인할 수가 있다. 또한 리더와 태그사이의 통신채널은 도청이 가능하기 때문에 악의적인 공격자는 Key를 획득한 후, 해쉬 연산하여 MetaID를 산출하여 인증 받을 수 있다. 마지막으로 악의적인 제 3자는 고정된 MetaID를 재전송함으로써 인증 받을 수 있다.

3.2 Low-Cost 프로토콜

유비쿼터스 환경의 Low-Cost 프로토콜은 태그는 해쉬함수와 XOR 연산을 수행할 수 있고, 리더는 랜덤수를 생성할 수 있다고 가정한다[8].

이 방법은 일방향 해쉬 함수 안전성에 기반하여 도청을 하는 공격자로부터 프라이버시 보호를 제공하고, 랜덤수 s를 사용하여 재전송 공격에도 강하다. 하지만 전 세션이 비정상적으로 종료되었다면 태그에서 출력되는 데이터는 h(ID)로 같은 데이터가 출력되므로 사용자의 위치 확인이 가능하게 된다. 또한 마지막 세션에서 데이터가 전송이 안 될 경우 데이터베이스는 ID를 갱신하고, 태그에서는 ID를 갱신하지 못하게 되므로 식별데이터의 동기화 문제점이 발생한다.

Ⅳ. 인증 프로토콜 제안

본 장에서는 기존 인증 프로토콜의 분석을 기반으로 하여 저가의 태그에서 조금 더 현실적으로 이용 가능한 프로토콜을 제안하고자 한다. 본 제안 방식은 기존 방식에서 설명한 프로토콜과는 달리 XOR 연산으로만 이뤄지고 있다.

4.1 가정사항

저가의 태그에서 효율적인 인증 프로토콜을 제안하기 위해 다음 사항을 가정한다.

- 태그와 리더사이의 통신은 Insecure 채널을 이용한다.
- 태그와 데이터베이스는 태그의 비밀 *ID* (TID_i)를 사전에 공유한다.
- 정당한 태그, 데이터베이스 그리고 리더는 그룹키(G_key)를 공유한다.
- 태그와 데이터베이스는 서로 값이 다른 비밀 값($K1, K2$)를 공유한다. 단 다른 태그와의 비밀 값 중 하나는 동일할 수 있다.
- 리더는 랜덤수(R_r)를 생성할 수 있다.

4.2 시스템 계수

다음은 본 프로토콜에서 사용되는 시스템 계수이다.

- TID_i : 태그의 ID로써 공개되지 않은 태그의 식별 값 ($i=(1,2,....,n)$, n:태그의 개수)
- $mataID_i$: 인증시 이용되는 태그의 가상 ID ($i=(1,2,....,n)$, n:태그의 개수)

- R_r : 리더에서 생성되는 랜덤 수
- G_key : 정당한 객체들이 소유하고 있는 그룹키
- $K1$: 태그와 데이터베이스와 서로 공유된 비밀 값으로 정당한 태그로부터 왔는지 확인하기 위해 데이터베이스에서 사용
- $K2$: 태그와 데이터베이스와 서로 공유된 비밀 값으로 정당한 데이터베이스로 부터 왔는지 확인하기 위해 태그에서 사용
- R_value : $G_key \oplus R_r$의 연산으로 획득하는 값으로 리더에서 출력되는 데이터
- T_value : $K1 \oplus R_r$의 연산으로 획득하는 값으로 태그에서 출력되는 데이터
- DB_value: $K2 \oplus R_r$의 연산으로 획득하는 값으로 데이터베이스에서 출력되는 데이터
- $Count$: query를 받을 시 마다 1씩 증가하는 데이터
- C : $Count$와 R_r이 XOR 연산을 통해 생성한 데이터 좌측 $L(C)$와 우측 $R(C)$로 나누어 짐
- $\oplus$: XOR 연산
- $\|$: 문자열 연접

4.3 제안 방식 프로토콜

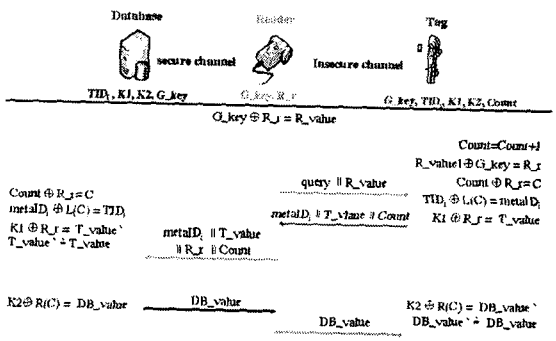
본 제안방식은 저가의 태그에서 실용 가능성 있게 XOR 연산만을 이용하여 인증 프로토콜 설계되었다. 인증과정은 다음과 같다.

Step1. 리더는 랜덤 수 R_r 을 생성하여 그룹키 (G_key)와 XOR연산을 취해 R_value를 계산한다. 그리고 $query$와 연접하여 태그에게 전송한다.

$$G\_key \oplus R\_r = R\_value$$

$$query \| R\_value$$

Step2. 태그는 $query$를 받을 때 마다 $Count$를 1씩 증가 시키고, 리더로부터 전송받은 R_value에 그룹키(G_key)를 XOR 연산을 취해 랜덤수(R_r)을 획득한 후, 획득한 랜덤수를 이용하여 $Count$와 XOR 연산을 취



(그림 1) 제안방식 프로토콜

하여 C를 생성한다. 생성한 C의 좌측$L(C)$와 태그 ID(TID_i)를 XOR연산을 취해 $metaID_i$를 계산하고 비밀값($K1$)과 랜덤수와 XOR연산을 취해 T_value를 계산한다. 그리고 리더에게 $metaID_i$와 T_value 그리고 $Count$를 연접하여 리더에게 전송한다.

$$Count = Count + 1$$

$$R\_value \oplus G\_key = R\_r$$

$$Count \oplus R\_r = C$$

$$TID_i \oplus L(C) = metaID_i$$

$$K1 \oplus R\_r = T\_value$$

$$metaID_i \| T\_value \| Count$$

Step3. 리더는 태그로부터 전송받은 데이터에 자신의 생성한 랜덤수(R_r)을 연접하여 데이터베이스에게 전송한다.

$$metaID_i \| T\_value \| Count \| R\_r$$

Step4. 데이터베이스는 리더로부터 전송받은 $Count$와 랜덤수를 XOR 연산을 취해 C를 생성한다. 생성한 C의 좌측$L(C)$와 $metaID_i$를 XOR연산을 취해 태그 ID(TID_i)를 획득하여 데이터베이스에 ID에 매칭 되는 $K1$, $K2$를 검색한다. 그리고 $K1$에 랜덤수(R_r)을 XOR 연산을 취해 T_value`를 계산하여 전송받은 T_value와 같은지 비교하여 같다면 정당한 태그로부터 전송되어졌다고 확인되어 $K2$에 C의 우측$R(C)$을 XOR 연산을 취해 DB_value를 계산하여 리더에게 전송한다.

$$Count \oplus R\_r = C$$

$$metaID_i \oplus L(R) = TID_i$$

$$K1 \oplus R\_r = T\_value`$$

$$T\_value` \stackrel{?}{=} T\_value$$

$$K2 \oplus R(C) = DB\_value$$

$$DB\_vlaue$$

Step5. 리더는 데이터베이스로부터 전송받은 데이터를 태그에게 전송한다.

$$DB\_vlaue$$

Step6. 태그는 $K2$에 랜덤수(R_r)을 XOR 연산을 취해 $DB_value`$를 계산하여 리더로부터 전송받은 DB_value와 서로 같은지 비교하고 서로 같다면 정당한 데이터베이스로부터 전송되어졌다고 확인되며, 이로써 인증과정이 종료된다.

$$K2 \oplus R(C) = DB\_value`$$

$$DB\_value` \stackrel{?}{=} DB\_value$$

4.4 제안 방식 분석

본 제안 방식은 저가의 태그에서 효율적으로 이용될 수 있도록 설계되었다. 가상 ID인 *metaID*를 이용하여 어떠한 태그로부터 데이터가 전송되어졌는지 알 수 없도록 익명성을 제공한다. 그리고 랜덤수와 *Count*로 인해 매 세션 이용되는 *metaID*가 매번 변경되어 재전송 공격에 안전하다. 또한 악의적인 제 3자는 데이터를 도청하여 정보를 획득하려고 노력하여도 사전에 안전하게 공유되었던 G_key, $K1$ 그리고 $K2$를 모르기 때문에 태그의 식별 정보를 취득할 수 없어 도청에 안전하며, 데이터의 갱신이 없어 데이터의 동기화에 대한 고려를 하지 않아도 된다. 마지막으로 $K1$, $K2$ 서로 값이 틀릴 뿐, 태그마다 동일한 데이터를 가질 수 있기 때문에 태그의 연결성을 찾기 힘들다. 따라서 위치 확인에 안전하다.

<표 1> 방식별 분석

	Hash-Lcok	Low-Cost	제안 방식
통신횟수	6	5	5
도청	취약	안전	안전
통신내용분석	취약	취약	안전
재전송 공격	취약	안전	안전
위치확인	가능	가능	안전
동기화	·	문제발생	·
효율성	비효율	비효율	효율

<표 2> 해쉬 연산량 분석

		Hash-Lcok	Low-Cost	제안 방식
해쉬 연산량	태그	1	2	0
	데이터베이스	1	2	0
	리더	0	0	0

V. 결론

현재 저가의 RFID 태그에서 기존의 해쉬 연산을 이용하는 방식들은 아직까지 많은 연산량을 필요로 하기 때문에 적용하기가 힘들다. 하지만 본 논문에서는 비교적 적은 자원으로도 가능한 XOR 연산만을 이용하여 RFID 인증 프로토콜을 제안하였기 때문에 저가의 태그에서 이용이 가능하다. 또한 제안 프로토콜은 태그의 계산량과 데이터베이스에서 부가되는 계산량이 현저하게 줄어든다. 하지만 태그의 저장이 데이터가 다른 방식들에 비해 많다. 따라서 향후 연구 방향으로는 저가의 연산능력 및 적은 데이터의 저장을 고려하여 연구가 지속적으로 진행되어야 한다.

[참고문헌]

[1] A. Juels, R. Pappu, "Squealing euros: Privacy Protection in RFID-enabled banknotes", In Proceedings of Finaancial Cryptography-FC'03, 2003.

[2] A. juels, R. L. Rivest and M. Szydlo, "The Blocker Tag: Selective Bloking of RFID Tags for Consumer Privacy", In Proceedings of 10th ACM Conference on Computer

[3] Ari, Juels, "Privacy and Authentication in Low-Cost RFID Tags", submission., 2003

[4] Henrici D, Muller P,."Hash-based Enhancement of :Location Privacy for Radio-Frequency Identification Devices using Varung Identifiers", PerSec'04 at IEEE PerCom, 2004

[5] S. A. Weis, "Security and Privacy in Radio -Frequency Identification Devices", Mastters Thesis. MIT. May, 2003

[6] 이상진, 김진, 김광조, "저가형 RFID를 위한 효율적인 프라이버시 보호 기법", 한국정보보호학회 하계 학술대회, 2005

[7] 이승구, 여상수, 조정식, 김성권, "RFID 프라이버시 보호를 위한 향상된 기법", 한국정보보호학회 하계학술대회, 2005

[8] 황영주, 이수미, 이동훈, 임종인, " 유비쿼터스 환경의 Low-Cost RFID 인증 프로토콜", 한국정보보호학회 하계 학술대회, 2004