RFID에 기반한 안전한 디바이스 인증 프로토콜에 관한 연구

박장수, 이임영
순천향대학교 정보기술공학부
e-mail:pjswise@sch.ac.kr

A Study on RFID-based Secure Deivces Authentication Protocol

Jang-Su Park, Im-Yeong Lee
Dept of Information Technology Engineering, SoonChunHyang University

요 약

최근 유비쿼터스(Ubiquitous)환경에서의 핵심 요소 기술로 RFID는 중요한 위치를 차지하고 있다. 이로 인해 RFID에 대해서 많은 연구가 진행되고 있으며, 다양한 분야에서 새로운 시장을 형성해 나갈 것으로 예측된다. 그러나 RFID 태그는 식별 정보가 쉽게 식별되는 기본적인 특징으로 인해 사용자의 프라이버시 침해 위협이 발생할 수 있다. 따라서 본 논문에서는 이러한 취약점을 해결하기 위해 RFID 시스템에서 사용자의 프라이버시를 보장하며, 안전하게 인증할 수 있는 방안에 대하여 연구를 수행하고자 한다. 제안방식은 저가의 RFID 태그에 기반한 디바이스들 사이에서 인증 프로토콜로써 안전하고 효율적인 장점을 갖는다.

1. 서론

현대 사회에서 디지털화의 가속 및 통신 인프라의 확충 등으로 전자, 정보통신, 가전 디바이스들이 디지털화 되어 단일 네트워크로 연결되어 영상 및 음향 정보를 서로 공유할 수 있는 환경이 구성되고 있다. 이와 같은 구성으로 디바이스들에 컴퓨팅 능력이 산재되는 환경을 유비쿼터스(Ubiquitous)환경이라고 한다. 유비쿼터스 환경에서는 사용자들에게 언제 어디서나 다양한 서비스를 제공하게 된다. 이러한 환경에는 저 전력이고, 작은 크기에, 어디서나 통신이 가능하여 데이터를 주고 받을 수 있고, 사용자들이 쉽게 이용할 수 있는 디바이스들이 필요하다. 이러한 기술로 현재 주목 받고 있는 기술이 RFID(Radio Frequency IDentification)이다. RFID는 앞에서 언급한 저 전력의 작은 크기에 무선통신 및 데이터를 저장할 수 있는 장점을 가지고 있어, 앞으로의 활용 분야는 금융, 의료, 교통, 제조, 문화 등 다양한 분야에서의 사용으로 산업전반에서 혁신적인 발전을 이룩할 것으로 기대되고 있다. 이는 사용자가 RFID 기반의 디바이스들을 이용하여 다양한 서비스를 제공받을 수 있을 것이다.

그러나 RFID 기반의 디바이스환경에서 보안에 대한 준비를 고려하지 않고 서비스를 제공한다면 디바이스들 간의 오작동, 해킹, 바이러스, 프라이버시 침해 등 많은 문제점이 발생 한다. 왜냐하면 RFID 기반의 디바이스들은 공개된 무선 네트워크에 연결되어 누구나 쉽게 접근이 가능하기 때문이다. 따라서 안전한 서비스를 제공하기 위해선 사용되는 각각의 디바이스들이 정당한 디바이스들인지를 판별 할 수 있어야 한다.

본 논문에서는 인증을 제공함으로써, 저가의 RFID 태그에서 정당한 디바이스들만 서비스를 이용할 수 있도록 2장에서는 RFID 보안 요구사항에 대해 알아보며, 3장에서는 기존의 RFID 인증 프로토콜을 분석하고, 4장에서는 제안 방식을 기술하며, 5장에서 결론을 맺는다.

2. RFID 시스템의 보안 요구 사항

일반적인 RFID 시스템은 일반적으로 다음의 세 가지 요소로 구성된다.

- 태그(Tag) : 식별정보를 가지고 다니며 리더기의 요청에 응답하여 정보를 준다.
- 리더기(Reader) : 태그에 정보를 요청하며 태그에 데이터의 읽기/쓰기를 진행한다.
- 데이터베이스(Database) : 태그의 관련 정보를 저장하고 가공한다.

일반적인 RFID시스템의 통신에서 리더기와 데이

터베이스 사이의 통신은 안전한 통신 채널을 이용하여 이루어지는 반면에, 태그와 리더기 사이의 무선 통신은 안전하지 않은 라디오통신을 사용하기 때문에 공격자에 의한 도청 가능성이 존재하게 된다. 그러므로 다음과 같은 보안 요구 사항이 필요하다.

- 도청공격 : 리더기와 태그간의 통신은 라디오주파수의 무선 통신으로 도청 가능하다.
- 트래픽분석공격 : 도청된 내용을 가지고 임의의 정보를 분석해 낼 수 있다.
- 재전송공격 : 도청된 내용을 정당한 리더기에게 재전송 할 수 있다.

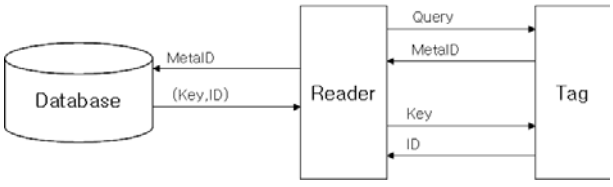
또한 저가의 태그에 안전한 보안기술이 적용 가능한지의 여부에 초점을 맞춰야 한다. 즉, 효율성인 측면도 고려해야 한다.

3. RFID 기존 인증 프로토콜 분석

본 장에서는 현재 진행되어왔던 연구 결과들을 분석하여 본다. 기존 인증 프로토콜로는 다음과 같은 방식들이 있다.

3.1 해쉬-락 프로토콜

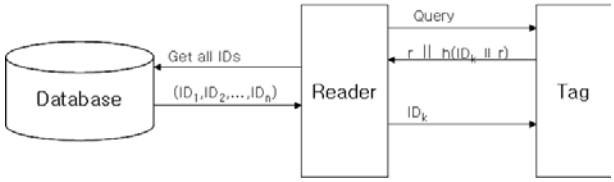
해쉬-락 프로토콜은 저가의 태그에서 리소스 제한 문제를 해결하면서 인가 받은 리더에게만 태그 정보를 전송하기 위한 방법으로, 해쉬 함수만을 가정하고 있다[6]. (그림 1)에서처럼 태그가 리더기로부터 Query를 전송 받으면 태그는 인증시 이용할 일시적인 MetaID=H(Key) 값을 리더기로 전송한다. 리더기는 태그로부터 받은 MetaID를 데이터베이스에 전송한다. 데이터베이스는 리더기로 받은 MetaID 값에 해당되는 Key와 ID를 리더기에 전송하고, 리더기는 태그에게 Key를 보내면 태그는 리더기가 보내온 Key를 받아 이를 해쉬해 보고 그것이 자신이 가지고 있는 MetaID와 같다면 옳은 정보라 판단하여 ID를 전송한다. 이 방법의 안전성은 일방향 해수 함수에 기반 한다. 해쉬 함수의 특정상 Key를 모르는 사람이 MetaID로부터 Key를 알아내는 것은 어렵기 때문이다. 그러나, 리더기와 태그간의 통신은 도청이 가능하므로 특정 태그와 정당한 리더기간의 통신을 도청한 공격자는 Key획득할 수 있다. 획득한 Key를 전송함으로써, 태그의 ID를 얻을 수 있다. 또한 식별자로 사용되는MetaID값이 고정되어 있어, 도청하는 자들에게 트래킹이 가능하고 재전송 공격이 가능하다. 즉, 저가로 구현 될 수 있는 장점은 가지고 있지만, 앞에서 언급한 보안상의 취약점을 내포하고 있다[8].



(그림 1) 해쉬-락 프로토콜

3.2 확장된 해쉬-락 프로토콜

확장된 핵쉬-락 프로토콜은 앞에서 설명한 해쉬-락 프로토콜의 변형이며, 태그는 해쉬 함수와 의사난수 생성기를 갖는다[6]. (그림 2)에서처럼 리더기가 태그에게 Query를 전송하면, 태그는 랜덤수 r을 생성하여 자신의 ID를 입력 값으로 하여 $h(ID_k \| r)$을 연산한다. 태그는 $h(ID_k \| r)$과 r을 리더기에게 전송한다. 리더기는 태그로부터 받은 정보를 데이터베이스에게 전송한다. 데이터베이스는 자신의 저장하고 있는 모든 태그의 식별정보 ID_k와 r로부터 $h(ID_k \| r)$에 대응하는 유일한 식별정보를 찾은 후, 그 값을 리더기에게 전송한다. 이 기법에서는 특정 태그의 아이디 ID_k를 도청하여 획득 후 부정 태그가 임의의 r'를 생성하여 $r' \| h(ID_k \| r')$을 전송하면 인증받을 수 있다. 그리고 $r \| h(ID_k \| r)$을 재전송하였을 경우 마찬가지로 인증 받을 수 있다. 이는 랜덤수를 태그가 선택하기 때문이다. 또한 저가의 태그에서 해쉬 함수와 동시에 R.N.G의 구현이 어렵다. 마지막으로 데이터베이스는 특정태그의 식별 정보를 찾기 위하여 매번 모든 태그의 식별정보와 랜덤수에 대한 해쉬 값을 계산해야 하는 취약점을 내포하고 있다[8].



(그림 2) 확장된 해쉬-락 프로토콜

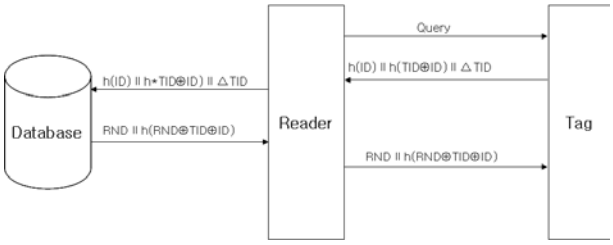
3.3 해쉬 기반의 ID 변형 프로토콜

해쉬 기반의 ID 변형 프로토콜은 ID값을 다양하게 함으로써 프라이버시를 보장한다. 태그에 대한 실제 정보는 데이터베이스에 저장되어 있으며, 리더기에게 전송할 필요가 있을 시, 데이터베이스가 직접 전달한다. 데이터베이스와 리더기사이의 통신은 안전하다고 가정하므로, 이를 통해 개인 정보 프라이버시가 보장된다[4,10].

이 기법은 (그림 3)에서처럼 리더기가 태그에게 Query를 전송하면, 태그는 두 번의 해쉬 연산을 하여, $h(ID) \| h(TID \oplus ID) \| \triangle TID$를 리더기에게 전송하고 리더기는 데이터베이스에게 전송한다. 이러한 정보를 받은 데이터베이스는 태그를 인증하고 임의의 랜덤 값 RND을 생성하여 태그에게 전송되도록 한다. RND는 ID를 갱신하는데 쓰인다. 그리고 $h(RND \oplus TID \oplus ID)$는 데이터베이스로부터 정보가 제대로 왔는지 확인하기 위해 쓰인다. 마지막 과정이 제대로 수행되면 태그는 $h(RND \oplus TID \oplus ID)$를 생성해 전송 받은 값과 비교해본 후, 값이 같으면 기존의 ID를 $(ID \oplus RND)$값으로 갱신한다.

이 기법은 ID를 각 인증세션마다 갱신을 시키므로, 도청을 하는 공격자로부터 프라이버시를 보장받게 되며 재전송 공격에도 강하다. 그러나 공격자는 태그에 Query를 전송함으로써, $h(ID) \| h(TID \oplus$

ID)‖△TID의 정보를 받을 수 있고, 그 정보를 가지고 태그가 다음 인증 세션을 열지 않은 사이에 정당한 리더기에게 인증을 받을 수 있다. 이후 데이터베이스의 ID는 갱신되고 정당한 태그는 갱신되지 못함으로 인증을 받지 못한다. 또한 해쉬 연산을 세 번 수행하므로 태그의 가격이 증가되는 것을 고려해야 한다는 취약성이 있다[10].

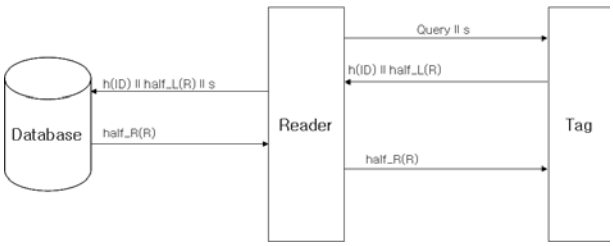


(그림 3) 해쉬 기반의 ID 변형 프로토콜

3.4 Low-Cost 인증 프로토콜

Low-Cost 인증 프로토콜은 앞에서 언급한 해쉬 기반의 ID 변형 프로토콜을 기반하여 해쉬 연산량을 3번에서 2번으로 줄여 제안한 인증 프로토콜로써 태그는 해쉬함수, 리더기는 R.N.G를 가지고 있다고 가정한다[10].

이 기법에서의 인증과정은 (그림 5)에서 처럼 리더기는 태그에게 Query를 전송하기 이전에, 의사 난수 생성기를 이용하여 랜덤값인 s를 생성해서 같이 전송한다. s를 전송 받은 태그는 h(ID‖s)=R을 생성하고 h(ID)를 생성한다. R은 나중에 세션이 다 끝난 후, ID 값을 갱신하기 위해 쓰이고, 데이터베이스와 태그가 서로 같은 R을 생성했는지 확인하기 위해 사용 되어진다. R은 half_L(R)과 half_R(R)로 나눠지며, 태그는h(ID)와 half_L(R)을 리더기에게 전송한다. 리더기는 태그로부터 받은 정보에 s를 같이 데이터베이스에 전송한다. 데이터베이스에서는 h(ID)를 통해 태그의 정보를 확인하고, ID와 s를 이용하여 R을 생성한다. 생성된 R과 리더기로부터 전송받은 half_L(R)이 같다면 태그를 정당하다고 판단하고 자신의 인증을 위해 half_R(R)을 전송한다. 이와 함께 데이터베이스는 R을 통해 ID를 갱신하고 저장한다. 리더기는 데이터베이스로 받은 정보를 태그에게 전송하며 태그는 리더기로 받은 half_R(R)을 비교한 후 같다면 태그도 ID를 ID⊕ (R‖R)로 갱신한다. 즉 ID를 변형시켜 프라이버시를 보장하고 재전송공격을 막으며, 해쉬 기반의 ID 변형 프로토콜의 단점을 극복하였다.



(그림 4) Low-Cost 인증프로토콜

4. 안전한 디바이스 인증프로토콜 제안

본 4장에서는 기존 인증 프로토콜의 분석을 기반으로, 보다 안전하고 효율적인 인증 프로토콜을 제안하고자 한다.

4.1 가정 사항

안전한 디바이스 인증 프로토콜을 제안하기 위해 다음 사항을 가정한다.

- 태그는 해쉬 함수와 XOR 연산을 수행할 수 있다.
- 태그와 데이터베이스는 사전에 SID_0를 공유한다.
- 리더기와 데이터베이스는 R.N.G를 가져 랜덤수를 생성할 수 있다.
- A는 $SID_i \oplus R$로 연산되어 얻는 값으로 전체 길이 A의 1/2의 좌측이 A_L이고, 나머지 1/2의 우측이 A_R이다.

4.2 시스템 계수

안전한 디바이스 인증 프로토콜에서는 다음과 같은 시스템 계수가 사용된다.

- SID : 인증을 위한 Security ID로서 공개 되지 않는 태그의 식별 값
- SID_i : 현재 세션에 사용되고 있는 SID값 (SID_0초기 공유한 SID값으로 i = 0~n)
- h() : 해쉬 함수
- ⊕ : XOR연산
- R, r : 리더기와 데이터베이스에서 각각 생성하는 랜덤수

4.3 제안 방식 인증과정

XOR연산과 한번의 해쉬 연산을 통해 RFID 기반의 디바이스 인증 프로토콜을 제안하였다. 인증과정은 다음과 같다.

1단계 : 리더기는 태그에게 Query를 전송하기 전, R.N.G를 이용해 R을 생성하여 같이 전송한다.

$$R \| Query$$

2단계 : 태그는 리더기에서 전송 받은 R을 이용하여 $SID_i \oplus R$를 연산하여 A를 생성한다. 생성된 A는 A_L과 A_R으로 구성 되어진다. A_L은 데이터베이스와 태그가 같은 값을 생성하였는지 확인하기 위해 사용되고, A_R은 정당한 데이터베이스로부터 전송되었는지 확인하기 위해 사용된다. 또한 해쉬 함수를 이용하여 태그의 정보를 찾는데 이용되는 $h(SID_i)$값을 생성한다. 태그는 생성된 값 $h(SID_i)$과 A_L을 리더기에 전송한다.

$$h(SID_i) \| A_L$$

3단계 : 리더기는 태그로 받은 정보와 함께 R을 같이 데이터베이스에 전송한다.

$$h(SID_i) \| A_L \| R$$

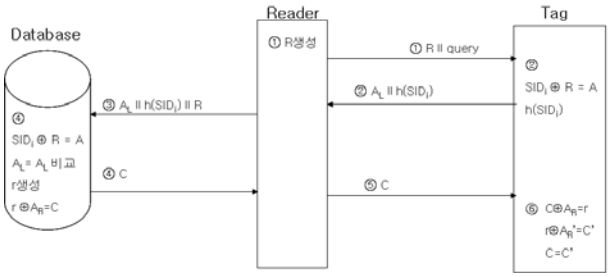
4단계 : 데이터베이스는 리더기로 전송받은 $h(SID_i)$를 통해 태그의 정보를 확인하고, SID_i와 R을 XOR연산하여 A를 생성하고 생성된 A_L의 값과 리더기로 부터 받은 A_L의 값을 비

교하여 값이 같다면 태그를 정당하다고 판단하고, R.N.G를 이용하여 SID갱신을 위한 랜덤수 r을 생성한다. 생성된 r을 이용하여 $C=r\oplus A_R$ 라는 값을 생성 후 전송한다.

5단계 : 리더기는 데이터베이스로 받은 C값을 태그에게 전송한다.

6단계 : 태그는 리더기로부터 전송 받은 C값을 이용하여 다음과 같은 검증과정을 수행한다. $C\oplus A_R$의 연산으로여 r을 획득하고 $r\oplus A_R'$의 연산으로 C'를 생성한다. $C'=C$면, 정당한 데이터베이스에서 전송되어진 것이 확인 가능하다.

세션이 안전하게 끝나는 경우, 태그와 데이터베이스는 $SID_{i+1}\leftarrow SID_i\oplus r$로 갱신한다.



(그림 5) 제안방식

4.2 안전성 및 장·단점

제안 방식인 안전한 디바이스 인증 프로토콜은 올바른 인증 세션마다 태그에 저장된 SID값이 매번 갱신되므로 추적이 불가능하여 프라이버시를 제공한다. 또한 해쉬 함수와 XOR연산으로만 하였어도 공격자가 얻을 수 있는 인자 값이 부족하므로 SID_i값을 유추할 수 없다. 그리고 공격자가 도청을 통해 $h(SID_i)$를 재전송하는 경우, 정당한 리더기와 데이터베이스는 R과 r을 매번 랜덤 한 수로 전송하여 SID가 갱신되므로 공격자는 정보를 획득할 수 없다. 따라서 재전송 공격에도 강하다. 마지막으로 [표 1]은 방식별 연산량 비교해 표로 작성한 것이다. 여기에서 볼 수 있듯이 저가의 태그에서의 해쉬 연산량을 다른 방식보다 줄여, 태그의 부담감을 줄였다.

[표 1] 방식별 연산량 비교

		해쉬-락	확장된 해쉬-락	ID 변형	Low-Cost	제안 방식
연산도구	태그	해쉬 함수	해쉬 함수 R.N.G	해쉬 함수	해쉬 함수	해쉬 함수
	리더기	.	.	.	R.N.G	R.N.G
	DB	해쉬 함수	해쉬 함수	해쉬 함수 R.N.G	해쉬 함수	해쉬 함수 R.N.G
해쉬함수량	태그	1	1	3	2	1
	DB	1	n	3	2	1

5. 결론

다가오는 유비쿼터스 환경에서는 프라이버시 보호 및 보안에 관한 연구가 반드시 뒤따라야 한다. 사용자에게 다양한 서비스를 제공하기 위해서는 어쩔 수 없이 개인정보를 이용해야 하기 때문에 프라이버시의 침해 소지가 크다. 이러한 프라이버시의 침해를 막기 위해 본 논문에서는 기존의 다른 방식에 비해 해쉬 연산을 한번으로 줄여 RFID에 기반한 안전한 디바이스 인증 프로토콜 제안하였다. 몇년 이내 저가의 태그에 해쉬 함수는 이용 가능하므로 여러 가지 유비쿼터스 환경에 유용할 것이다.

RFID 관련 프라이버시 보호에 대한 핵심 연구 주제 중 하나는 낮은 비용으로 암호화 프로세스가 가능한 RFID를 개발하고 구현하는 것이다[7]. 여기에는 해쉬 함수, 난수 생성기 그리고 대칭키 암호, 공개키 암호 등의 경량화 연구가 포함되며 지속적으로 연구가 진행 되어져야 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] P. Golle, M, Jakobsson, A Juels and P. Syverson, "Universal re-encryption for mixnets", 2002

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

[7] 정병호, 강유성, 김신효, 정교일, 양대헌, "RFID/USN 환경에서의 정보보호 소고" , 2003

[8] 주학수, "RFID 시스테의 보안 및 프라이버시 보호를 위한 기술 분석" , IT리포트, 2004

[9] 한승우, 최재귀, 박지환, "효율적인 식별기능을 갖는 RFID 가변 정보화 방식", 한국멀티미디어학회 춘계학술발표대회, 2004

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