스푸핑 공격에 안전한 랜덤 해쉬기반 양방향 RFID 인증 프로토콜

이종하° 남길현
국방대학교
jhlee6452@hanmail.net khnam@kndu.ac.kr

A Randomized Hash-Based Interactive RFID Authentication Protocol against Spoofing Attack

Jong-Ha Lee° Kil-Hyun Nam
Korea National Defense University

요 약

기존의 RFID 인증 프로토콜은 트래킹 공격이나 스푸핑 공격에 취약하다는 단점을 가지고 있다. 특히 해쉬기반이나 랜덤 해쉬기반 RFID 인증 프로토콜은 스푸핑 공격으로 인하여 태그와 리더간의 인증이 안전하지 못한 프로토콜이며, 해쉬체인 RFID 인증 프로토콜은 리더인증이 곤란한 일방향 인증 프로토콜이다. 본 논문에서 제안하는 프로토콜은 해쉬함수와 RNG(난수생성기)만을 사용하기 때문에 저가의 수동형 RFID 시스템에서 구현이 가능할 뿐만 아니라, 트래킹 공격과 스푸핑 공격에 안전하고, 태그와 리더간의 양방향 인증이 가능한 RFID 인증 프로토콜이다.

1. 서 론

21세기의 새로운 IT 혁명은 유비쿼터스 컴퓨팅(Ubiquitous Computing)이라 할 수 있는데, 이는 모든 사물이 지능화되고 네트워크화 됨으로써, 사람과 사람, 사람과 사물, 사물과 사물 간의 의사소통이 가능한 유비쿼터스 사회를 실현하는 기반 기술이라고 할 수 있다.

RFID(Radio Frequency IDentification)란 유비쿼터스 컴퓨팅의 실현을 위한 가장 핵심적인 기술로써, 모든 사물에 마이크로 칩을 내장한 전자태그를 부착한 후, 무선통신기술을 이용하여 사물의 정보 및 주변상황의 정보를 리더에서 자동으로 인식 및 감지하는 센서 기술이다. 현재는 전 세계적으로 무선 자동 인식 기술의 중요성이 부각되어 전자화폐, 물류관리, 보안 시스템 등의 핵심 기술로 급속히 확장 및 발전하고 있는 추세이다.

그러나 이러한 RFID 기술은 도청, 트래픽 분석, 서비스 거부 공격, 메시지 유실, 트래킹 공격, 스푸핑 공격 등 많은 취약점들을 지니고 있어서 개인이나 조직의 보안과 프라이버시 보호에 심각한 문제를 야기할 수 있다. 이 때문에 태그와 리더간의 양방향 채널에 대한 상호인증기술이 반드시 필요하다고 할 수 있다.

이를 위하여 본 논문에서는 저가(Low-Cost)인 수동형 RFID 시스템에서 구현이 가능하며, 트래킹 공격과 스푸핑 공격에 안전한 랜덤 해쉬기반 양방향 RFID 인증 프로토콜을 제안한다.

2. RFID 시스템

2.1 RFID 시스템 구성

RFID 시스템은 태그와 리더, 그리고 서버 등으로 구성되어 있다.

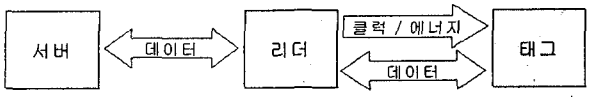

그림 1 RFID 시스템 구성

태그는 칩과 안테나로 구성되어 있으며, 유일한 식별코드와 정보가 저장되어 있어서 리더의 요청에 의해 또는 상황에 따라 태그 스스로 리더에게 자신의 정보를 송·수신하는 장치이다. 리더는 태그에게 신호를 보내거나 태그로부터 받은 데이터를 판독하여 서버에게 전송하는 장치로써, 태그의 활성화 및 비활성화, 통신주체간 연결, 데이터 충돌방지, 상호인증 등의 주요한 기능을 가지고 있다. 마지막으로 서버는 리더로부터 전송되는 태그의 다양한 데이터를 수집, 제어 및 관리하는 장치로써, 로컬서버, 객체검색시스템, 정보서버 등으로 구분된다.

2.2 RFID 인증 프로토콜

RFID 시스템에서 인증이란 태그와 리더의 정당성을 상호 입증해주는 절차를 의미하며, 태그와 리더는 서로를 인증하여 서로를 신뢰하는 경우에만 올바른 동작을 보장해야 하는데, 이는 접근제어(Access Control)와도 동일한 개념이다[1].

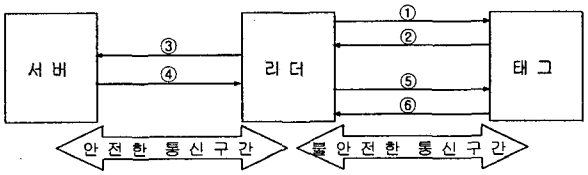

그림 2 RFID 인증 프로토콜 모델

통상적으로 태그-리더 구간은 안전성이 보장되지 않아 도청이 가능한 구간이라 볼 수 있으며, 리더-서버 구간은 보안이 유지되는 안전한 구간이라 볼 수 있다.

①에서 리더가 태그에게 정보를 요청하면 ②에서 태그는 자신을 인증시키기 위한 최소한의 정보와 함께 질의한 리더가 정당하다는 것을 태그가 알 수 있도록 하는 정보를 요구한다. 이후, ③과 ④에서 리더와 서버는 태그가 정당하다는 것을 확인하고, ⑤에서 리더는 자신이 정당한 리더임을 태그가 알 수 있도록 태그에게 태그가 원하는 정보를 보낸다. 마지막으로 태그 역시도 ⑤의 값을

확인하여 태그의 정보를 요구한 리더가 정당한 리더임을 확인하고 난 후, ⑥에서 자신의 정보를 리더에게 보낸다.

2.3 RFID 시스템에서의 보안 고려사항

태그-리더 구간은 무선 통신 구간으로 가정하므로, 다음과 같은 보안 취약점을 고려하여야 한다[2].

- 도청(Eavesdropping) : 태그와 리더간의 통신은 무선 통신으로 가정하므로, 공격자는 언제든지 태그와 리더간에 전송되는 데이터를 도청할 수 있다.
- 트래픽 분석(Traffic Analysis) : 공격자는 도청한 데이터를 가지고 필요한 정보를 분석해 낼 수 있다.
- 서비스 거부 공격(Denial of Service Attack) : 공격자는 RFID 시스템이 정상적으로 동작하지 못하도록 무선 구간에 잡음을 넣거나 통신 내용을 왜곡시킬 수 있다.
- 메시지 유실(Message Loss) : 공격자의 고의 또는 시스템상의 문제로 인하여 태그와 리더간에 전송되는 데이터가 유실될 수 있다.
- 트래킹 공격(Tracking Attack) : 공격자는 도청한 정보를 이용하여 임의 태그의 위치정보를 알아낼 수 있다.
- 스푸핑 공격(Spoofing Attack) : 공격자는 도청한 정보를 이용하여 임의의 태그에게 자신이 정당한 리더인 것처럼 가장하여 태그 정보를 얻어 내거나, 임의의 리더에게 자신이 정당한 태그인 것처럼 가장하여, 리더에게 거짓 정보를 보낼 수 있다.

위에서 언급한 보안 취약점 중에서 통상적으로 도청이나 트래픽 분석 및 서비스 거부 공격은 인증 프로토콜 설계시 고려되지 않으므로, 본 논문에서도 언급하지 않는다.

3. 기존 RFID 인증 프로토콜

기존에 제안된 RFID 인증 프로토콜로는 도청이나 트래픽 분석에 의한 개인 정보 유출을 방지하기 위해 제안된 해쉬기반 프로토콜과 위치 트래킹 공격을 방지하기 위해 제안된 랜덤 해쉬기반 프로토콜, 그리고 최근에 전방향 안전성(forward security) 확보를 목적으로 제안된 해쉬체인 프로토콜 등이 있다.

3.1 해쉬기반 RFID 인증 프로토콜[1][2]

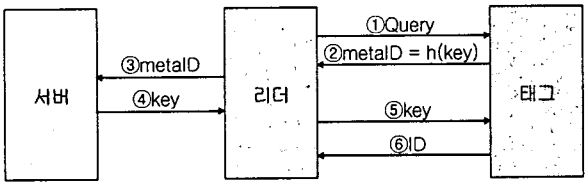

그림 3 해쉬기반 RFID 인증 프로토콜

해쉬기반 RFID 인증 프로토콜은 2003년에 Weis 등이 제안하였으며, ②metaID=h(key)를 사용하기 때문에 key 값의 유출을 방지할 수 있을 뿐만 아니라, 한번의 해쉬함수를 사용하기 때문에 저가로 구현할 수 있다.

그러나 리더의 질의시마다 태그는 항상 동일한 ② metaID값으로 응답하므로 이를 이용한 트래킹 공격이 가능할 뿐만 아니라, ②metaID 또는 ⑤key값이 공개되어 스푸핑 공격이 가능하다는 문제점이 있다.

3.2 랜덤 해쉬기반 RFID 인증 프로토콜[1][2]

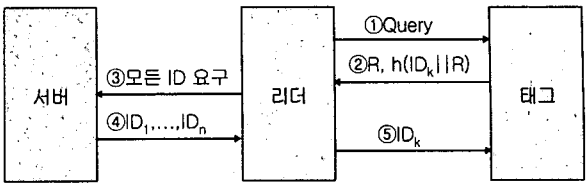

그림 4 랜덤 해쉬기반 RFID 인증 프로토콜

랜덤 해쉬기반 RFID 인증 프로토콜 역시도 2003년에 Weis 등이 제안하였으며, 해쉬기반 RFID 인증 프로토콜의 확장된 형태이다. 리더의 질의에 대한 태그의 응답값 ②R, $h(ID_k||R)$이 매번 바뀌기 때문에 트래킹 공격에도 안전하며, 한번의 해쉬함수와 한번의 RNG(Random Number Generator, 난수생성기)를 사용하기 때문에 저가로 구현할 수 있다.

그러나 해당 태그의 ID_k값을 알아내기 위해 리더는 매번 모든 태그의 식별정보와 난수에 대한 해쉬값을 계산해야하므로, 최악의 경우, 계산시간이 해쉬함수 n번 수행으로 증가하게 될 뿐만 아니라, ②R, $h(ID_k||R)$ 및 ⑤ ID_k값이 공개되어 스푸핑 공격이 가능하다는 문제점이 있다.

3.3 해쉬체인 RFID 인증 프로토콜[3]

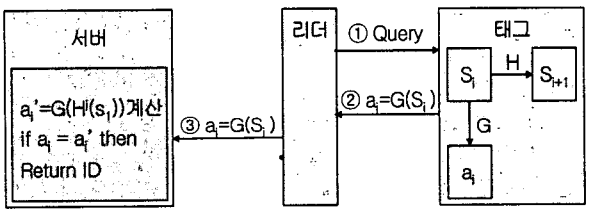

그림 5 해쉬체인 RFID 인증 프로토콜

해쉬체인 RFID 인증 프로토콜은 2003년에 Ohkubo 등이 제안하였으며, 리더의 질의에 대한 태그의 응답값 ② $G(s_i)$이 매번 바뀌기 때문에 트래킹 공격에 안전하고, 두 개의 해쉬함수 G, H를 사용하기 때문에 저가로 구현할 수 있다.

그러나 해당 태그의 ID값을 알아내기 위해 서버는 매번 모든 태그의 초기 비밀값을 가지고 해쉬값을 계산해야 하므로, 최악의 경우, 서버의 계산시간이 해쉬함수 n(1+i)번 수행으로 증가하게 될 뿐만 아니라, 리더인증을 실시하지 않는 일방향 인증이어서 정당한 리더라도 태그를 제어하기 곤란하다는 문제점이 있다.

4. 스푸핑 공격에 안전한 RFID 인증 프로토콜 제안

4.1 기존 RFID 인증 프로토콜 분석

해쉬기반 RFID 인증 프로토콜은 트래킹 공격이 가능할 뿐만 아니라, 스푸핑 공격이 가능하다.

랜덤 해쉬기반 RFID 인증 프로토콜은 계산시간이 증가할 뿐만 아니라, 스푸핑 공격이 가능하다.

해쉬체인 RFID 인증 프로토콜은 계산시간이 증가할 뿐만 아니라, 리더인증을 실시하지 않는 일방향 인증이다.

4.2 스푸핑 공격에 안전한 랜덤 해쉬기반 양방향 RFID 인증 프로토콜

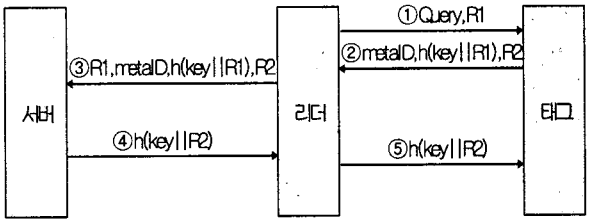

그림 6 스푸핑 공격에 안전한 랜덤 해쉬기반 양방향 RFID 인증 프로토콜

스푸핑 공격에 안전한 랜덤 해쉬기반 RFID 인증 프로토콜은 리더에서는 한번의 RNG를 사용하며, 태그에서는 두번의 해쉬함수(송수신시 각 한번)와 한번의 RNG를 사용하기 때문에 수동형에서 구현할 수 있다. 또한, key값이 공개되지 않을 뿐만 아니라, 공격자는 ①R1에 대한 태그의 응답값 ②h(key||R1)과 ②R2에 대한 리더의 응답값 ⑤h(key||R2)를 찾을 수 없기 때문에 스푸핑 공격에 안전하다.

그러나 metaID값이 노출되기 때문에, 해쉬기반 프로토콜과 마찬가지로 트래킹 공격에는 안전하지 못하다.

4.3 트래킹 공격과 스푸핑 공격에 안전한 랜덤 해쉬기반 양방향 RFID 인증 프로토콜

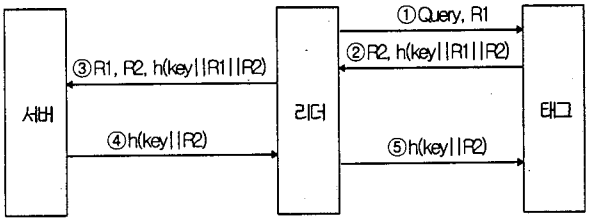

그림 7 트래킹 공격과 스푸핑 공격에 안전한 랜덤 해쉬기반 양방향 RFID 인증 프로토콜

트래킹과 스푸핑 공격에 안전한 랜덤 해쉬기반 RFID 인증 프로토콜은 리더에서는 한번의 RNG를 사용하고 태그에서는 두번의 해쉬함수(송수신시 각 한번)와 한번의 RNG를 사용하기 때문에 수동형에서 구현할 수 있다. 또한, key값이 공개되지 않을 뿐 아니라, 태그의 응답값 ②R2,h(key||R1||R2)이 매번 바뀌기 때문에 트래킹 공격에 안전하고, 공격자는 ①R1에 대한 태그의 응답값 ②h(key||R1||R2)과 ②R2에 대한 리더의 응답값 ⑤h(key||R2)를 찾을 수 없기 때문에 스푸핑 공격에 안전하다.

4.4 보안 특성 분석

해쉬기반 RFID 인증 프로토콜은 양방향 인증이 가능하고, 메시지 유실에도 안전하지만, 트래킹 공격이나 스푸핑 공격에는 안전하지 못하다.

랜덤 해쉬기반 RFID 인증 프로토콜은 양방향 인증이 가능하고, 메시지 유실이나 트래킹 공격에도 안전하지만, 리더의 계산시간이 증가하고, 스푸핑 공격에도 안전하지 못하다.

표 1 보안 특성 분석

	해쉬기반	랜덤 해쉬기반	해쉬체인	스푸핑공격에 안전한 랜덤해쉬기반	트래킹공격과 스푸핑공격에 안전한 랜덤해쉬기반
인증	양방향	양방향	일방향	양방향	양방향
메시지 유실	안전	안전	안전	안전	안전
트래킹 공격	취약	안전	안전	취약	안전
스푸핑 공격	취약	취약	보통	안전	안전
태그 계산량	해쉬1회 (수신)	해쉬1회 (송신) RNG 1회	해쉬2회 (송신)	해쉬2회 (송수신 각 1회) RNG1회	해쉬2회 (송수신 각1회) RNG1회
리더/서버 해쉬계산량	1 회	n 회	n(1+i) 회	1 회	n 회

해쉬체인 RFID 인증 프로토콜은 메시지 유실이나 트래킹 공격에는 안전하지만, 양방향 인증이 곤란하고, 서버의 계산시간이 증가한다.

스푸핑 공격에 안전한 랜덤 해쉬기반 양방향 RFID 인증 프로토콜은 트래킹 공격에 안전하지 못하지만, 양방향 인증이 가능하고, 메시지 유실과 스푸핑 공격에도 안전하다.

트래킹 공격과 스푸핑 공격에 안전한 랜덤 해쉬기반 양방향 RFID 인증 프로토콜은 서버의 계산시간이 증가하지만, 양방향 인증이 가능하고, 메시지 유실이나 트래킹 공격 및 스푸핑 공격도 안전하다.

5. 결 론

기존의 RFID 인증 프로토콜인 해쉬기반 RFID 인증 프로토콜은 트래킹 공격과 스푸핑 공격에 취약하고, 랜덤 해쉬기반 RFID 인증 프로토콜은 스푸핑 공격에 취약하다. 또한, 해쉬체인 RFID 인증 프로토콜은 양방향 인증이 곤란하다.

그러나 본 논문에서 제안하는 스푸핑 공격에 안전한 랜덤 해쉬기반 양방향 RFID 인증 프로토콜과 트래킹 공격과 스푸핑 공격에 안전한 랜덤 해쉬기반 양방향 RFID 인증 프로토콜은 양방향 인증이 가능하며, 스푸핑 공격에 안전하거나 트래킹 공격과 스푸핑 공격 모두에 안전한 프로토콜이다. 따라서 제안된 프로토콜은 RFID 시스템에서 요구되는 보안 특성과 서버의 능력에 따라 선택의 폭을 넓혀줄 수 있을 것이다.

참 고 문 헌

[1] 정병호, RFID/USN 환경에서의 정보보호, 제9회 정보보호심포지움 SIS2004, 456~457쪽, 2004년 7월

[2] S. A. Weis, S. E. Sarma, R. L. Rivest and D. W. Engels, Security and Privacy Aspects of Low-Cost Radio Frequency IDentification Systems, First International Conference on Security in Pervasive Computing 2003, 201~212쪽, 2004년

[3] M. Ohkubo, K. Suzuki and S. Kinoshita, Cryptographic Approach to "Privacy-Friendly" Tags, RFID Privacy Workshop, 1~9쪽, 2003년 11월