RFID Tag 보안을 위한 인증 프로토콜에 관한 연구

김정재*, 안재명*
*(주)리테일테크
e-mail:argniss@yahoo.co.kr

A Study on Authentication Protocol for Secure RFID Tag

Jeong-Jai Kim*, Jae-Myung Ahn*
*RetailTech Inc.

요 약

본 논문에서 제안하는 시스템은 기존의 RFID 시스템의 보안성을 높이기 위하여 2차원 배열 기법을 이용하여 안전성을 확보할 수 있게 되었다. 제안하는 시스템은 RFID Tag의 고유 ID 값인 UID값과 2차원 배열을 이용하여 태그와 리더간 인증을 하게 된다. 제안하는 시스템에서 암·복호화를 하기 위해서는 태그의 고유 ID값인 UID값과 관리자가 정의한 키셋을 이용한 암·복호화 과정에서의 안전성을 기존의 다른 시스템과의 비교를 통해 우수함을 입증한다.

1. 서론

RFID 시스템은 무선 주파수를 이용한 자동 인식 기술로서 물리적 접촉 없이 태그가 부착된 개체의 정보를 읽거나 기록할 수 있는 시스템으로서 제품 및 자산 관리, 운송 환경 관리, 화물 및 컨테이너 추적, 차량 접근 및 제어, 전자 문서 관리, 신원 확인, 관광, 교통, 위치 정보는 물론 사람과 동물의 이동 경로 추적 등에까지 폭 넓게 사용되어지고 있다.

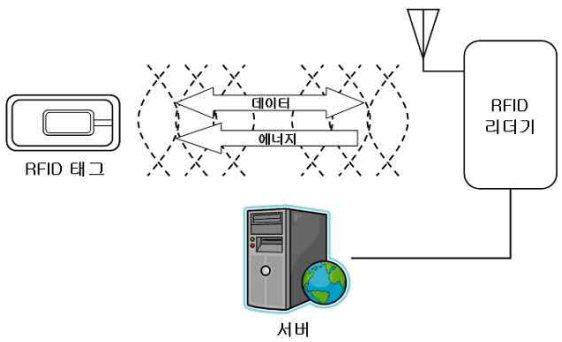
RFID 태그와 리더는 무선으로 통신하기 때문에 리더는 노출 되지 않은 형태로 숨겨져 있을 수 있으며, 리더가 설치된 곳을 통과할 때 그 물체의 위치 정보 확인, 저장, 축적될 수 있기 때문에 보안 위협과 개인 정보 침해라는 역기능도 동시에 가지고 있다[3].

기존의 RFID 시스템에서 이러한 문제를 해결하기 위해 본 논문에서는 태그(Tag)와 리더(Reader)간 상호 인증을 위하여 2차원 배열(Array)과 XOR방법[1]을 이용하여 불법적인 접근을 차단하는 RFID 시스템을 제안한다.

2. 관련 연구

2.1 RFID 시스템

RFID는 마이크로칩을 내장한 태그(tag), 레이블, 카드 등에 저장된 데이터를 무선 주파수를 이용한 리더에서 자동 인식하는 기술이다. 이러한 RFID 시스템은 태그(Tag), 리더(Reader), 백엔드 서버(Back-end-Server) 3가지 구성 요소로 이루어진다[2].



[그림 1] RFID 시스템

2.2 RFID 인증 프로토콜

2.2.1 물리적 인증 프로토콜

기존에 제안된 RFID 시스템의 물리적 인증 기법은 다음과 같이 킬 명령어 기법(Kill command), 패러데이 케이지(Faraday cage) 기법, 액티브 재밍(Active Jamming) 기법, 블로커 태그(Broker-Tag) 기법 등이 있으며 여러 가지 문제점이 있다[5].

- 킬 명령어(Kill command) 기법 : Auto-ID 센터가 제안한 방법으로 8 비트의 패스워드를 포함한 킬 명령어를 전송해 사용자에게 태그가 주어지기 전에 태그의 기능을 정지시키는 기법이다. 그러나 킬 명령어가 적용된 뒤에는 태그를 재사용할 수 없기 때문에 넓은 응용 환경을 지원하지 못하는 단점을 가지고 있다[4].

- 패러데이 케이지(Faraday cage) 기법 : 라디오 신호가 투과되지 않도록 하는 금속 혹은 망으로 만들어진 컨테이너(Faraday cage)를 이용하는 방법으로 사용자의 프라이버시를 보호해주는 부분적인 해결책이라 할 수 있다[5].

- 액티브 재밍(Active Jamming) : 근처에 있는 RFID 리더의 기능을 막거나 혹은 방해할 수 있는 라디오 신호를 브로드캐스트 하는 디바이스를 이용하는 것이다. 이 디바이스가 라디오 신호에 대한 전파 방해를 수행함으로써 태그가 노출되는 정보를 보호할 수 있으나, 이러한 접근법은 근처에 있는 모든 RFID 리더가 작동되지 않도록 방해할 수 있기 때문에 매우 강력한 해결책이라 할 수 있다[5].

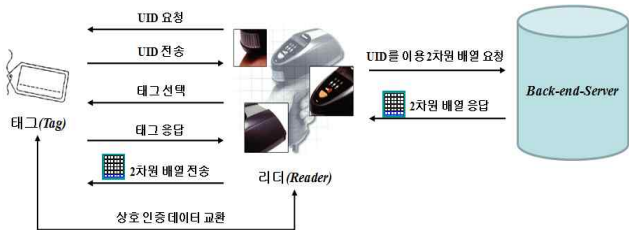
2.2.2 암호학적 인증 프로토콜

현재 RFID 시스템에서는 암호학적인 방법을 이용한 인증기법을 주로 연구하고 있으며, 현재까지 해쉬-락 기법, 확장된 해쉬-락 기법, 해쉬-체인 기법, 해쉬 기반 ID 변형 기법, 개선된 해쉬 기반 ID 변형 기법, 외부 재암호화 기법, Challenge-Response 기반 안전한 RFID 인증 기법 등이 제안되었다.

3. 제안 시스템 구조

3.1 2차원 배열을 이용한 인증 기법

본 논문에서 제안하는 RFID Tag 인증 기법은 기존에 제안된 RFID 시스템의 인증에 이용되었던 물리적 인증 기법과 암호학적 인증 프로토콜 방법을 사용해 정보 보호를 하는 방법 대신, 2차원 배열(Array)과 XOR 기법을 이용하여 복잡한 암호화 방법이 없는 인증 기법으로 제안하는 시스템의 전체 구조는 [그림 2]와 같다.



[그림 2] 전체 시스템 구조

리더가 태그에게 UID 값을 요청하면 태그는 리더에게 UID 값을 전송한다. 리더는 태그로부터 전송받은 UID 값을 백엔드 서버(back-end-server)로 전송하고 2차원 배열 생성을 요청한다. 백엔드 서버는 태그의 UID 값에 해당하는 키셋을 이용하여 2차원 배열을 생성하여 리더에게 전송한다. 리더는 서버로부터 전송받은 2차원 배열을 태그에게 전송하고, 태그는 리더로부터 전송받은 2차원 배열을 복호화 하고 자신이 보낸 태그 아이디(TagID)값과 동일한지 검사한다. 만일 동일할 경우 태그는 2차원 배열을 생성하여 리더로 전송하고 리더는 백엔드 서버로 전송한다. 이렇게 전송된 2차원 배열은 서버에서 복호화 하여 태그 아이디 값과 동일한지 비교하고 동일한 경우 상호 인증이 이루어진다.

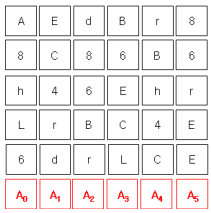
3.2 2차원 배열 기법 설계

RFID 시스템에서 태그에 대한 키셋(Keyset)은 태그와 서버 모두가 가지고 있다. 여기서 키셋이란 아스키코드와 같이 일련의 문자를 비트로 환산하기 위해 미리 정의해 놓은 코드표이며, 대문자 A~Z, 소문자 a~z, 숫자 0~9, +, - 해서 총 64개의 문자로 구성되어 있다. 각각의 리더, RFID Tag마다 서로 다른 키셋이 정의되어 있으며, 이 값은 나중에 중간 공격자로부터 공격이 들어오더라도 키셋값을 알지 못하기 때문에 안전히 통신을 할 수 있게 하는 값이다.

3.2.1 2차원 배열 생성

백엔드 서버는 2차원 배열을 생성하며 배열에 사용되는 키는 64바이트(Byte)로 총 64 가지의 문자를 이용하여 생성한다.

2차원 배열 생성 방법은 마지막 행을 제외한 나머지는 A~Z, a~z, 0~9 "+", "-" 총 64 가지의 문자를 이용하여 랜덤하게 패딩(padding) 된다. 마지막 행에 입력되는 값은 각각의 열을 XOR 연산한 결과 값으로 패딩 된다.



[그림 3] 난수값으로 패딩된 2차원 배열

[그림 3]은 난수값을 이용하여 마지막 행을 제외한 나머지를 64가지의 문자를 이용하여 패딩한 결과이다. 이렇게 패딩된 값을 XOR 하여 마지막 행에 들어갈 값을 구한다.

마지막 행에 패딩되는 값은 각 열을 XOR한 값과 각각의 마지막 행에 해당하는 A0값을 XOR한 값이 태그 아이디(tagID) 값이 된다. 1열의 태그 아이디(tagID)값을 "A8hL6"라 가정하고 마지막 행의 자세한 생성 방법은 A_0 이전의 값과 A_0값을 XOR하면 d(keyID)값이 나오고, A_0의 값을 구한다. 태그 아이 값을 얻는 방법은 [식 1]과 같다.

$$A \oplus 8 \oplus h \oplus L \oplus 6 \oplus A_0 = d(keyID) \quad \text{.....[식 1]}$$

각 열의 값을 XOR 하여 태그 아이디 값을 구하기 위해서는 키셋(keyset)을 필요로 하며, 키셋은 [그림 4]와 같다. 태그와 백엔드 서버에서는 동일한 키셋을 가지고 있다.

000001	B	111000	x
000010	C	111001	Z
000011	d	111010	s
000100	E	111101	h
000101	8	111110	L
...	...	...	...

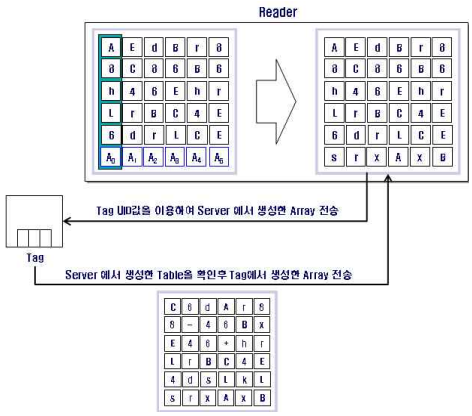
[그림 4] 키셋(keyset)

키셋의 값은 A~Z, a~z, 0~9 "+", "-" 총 64가지의 문자를 이용하여 랜덤하게 생성된다. 예를 들어 "A" 의 값은 "000000" 이 되지만 "000000" 값은 64가지 중 어떠한 문자가 될 수도 있다.

A	E	d	B	r	8
8	C	8	6	B	6
h	4	6	E	h	r
L	r	B	C	4	E
6	d	r	L	C	E
s	r	x	A	x	B

[그림 5] 완성된 2차원 배열

완성된 2차원 배열은 태그와 서버가 요청시 마다 새롭게 생성되어 전송된다.



[그림 6] 전체 시스템 흐름도

4. 구현 및 성능평가

4.1 안전성에 대한 평가

4.1.1. 스푸핑 공격에 대한 안전성

기존 시스템 해쉬-락 기법과 해쉬 기반 ID 변형 기법은 스푸핑 공격에 취약하지만 제안하는 시스템은 스푸핑 공격에 안전하다.

제안하는 시스템에서는 공격자가 정당한 리더로 위장해도 태그의 UID값에 해당하는 키셋과 태그 아이디를 모르고 있으므로 2차원 배열을 태그에서 복호화 한다 하더라도 인증 거부를 한다. 또한 위장된 태그에는 올바른 UID값을 알 수 있지만, UID값에 해당하는 키셋을 알 수 없으므로 획득한 2차원 배열로는 스푸핑 공격이 불가능하다.

4.1.2. 재전송 공격에 대한 안전성

기존 시스템 해쉬-락 기법은 재전송 공격에 취약

하지만, 해쉬 기반 ID 변형 기법은 재전송 공격에 안전하다.

제안하는 시스템에서는 정당한 리더가 쿼리와 함께 전송하는 2차원 배열에 대하여 태그가 리더에 응답으로 2차원 배열을 재생성하여 전송한다. 정당한 리더는 키셋을 이용하여 2차원 배열을 복화화 하지만 자신이 보낸 태그 아이디와 다른 값이 나오므로 정당한 리더는 태그에 대한 인증을 거부한다.

4.2 제안하는 RFID 인증 프로토콜

제안하는 RFID 인증 프로토콜 기법은 공격에 대한 안전성은 태그가 리더로부터 수신한 2차원 배열을 이용하여 요청마다 다른 2차원 배열로 응답을 하기 때문에 스푸핑 공격, 재전송 공격, 트래픽 분석 공격과 위치 트래킹 공격에 안전하게 나타났다. [표 4-1]은 공격에 대한 안전성을 비교분석한 결과이다.

[표 4-1] 공격에 대한 안전성 비교

프로토콜 / 공격형태	해쉬-락 기법	해쉬 기반 ID 변형 기법	개선된 해쉬기반 ID 변형 기법	제안하는 RFID 인증 프로토콜
스푸핑 공격	취약	취약	취약	안전
재전송 공격	취약	안전	안전	안전
트래픽 분석 공격	취약	안전	안전	안전
위치 트래킹 공격	취약	취약	보통	안전

5. 결 론

본 논문에서는 제안하는 RFID 시스템에서 제안하는 RFID 인증 프로토콜은 백엔드 서버에 등록된 태그의 UID, 태그 아이디(TagID), 키셋(KeySet)의 정보를 가지고 있다. 이러한 정보를 이용하여 상호 인증을 수행함으로써 인증되지 않은 태그 또는 리더에게 개인정보가 유출되지 않도록 보안성을 강화 하였다.

제안하는 RFID 인증 프로토콜은 리더와 태그가 2차원 배열을 요청할 때마다 새롭게 생성하여 전송하기 때문에 기존 시스템보다 공격에 강한 특징을 가지고 있으며, 2차원 배열은 별다른 암호화를 사용하지 않기 때문에 키셋만 가지고 있다면 복호화 과정까지 전부 자동으로 진행되기 때문에 속도가 빠르다는 장점을 가진다. 또한 키셋을 가지고 있지 않다면 2차원 배열을 복호화할 수 없으며 키셋을 이루고 있는 값들은 랜덤하게 바뀌므로 태그 아이디를 유추할 수 없다.

참고문헌

[1] 정용훈, “멀티미디어 콘텐츠 보호를 위한 인증 프로토콜에 관한 연구”, 숭실대학교 석사학위논문, 2006.

[2] 이근우, 오동규, 곽 진, 오수현, 김승주, 원동호, “분산 데이터베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜”, 한국정보처리학회 논문지 C, 제12권-C권, 제3호, pp.309-316, 2006. 6

[3] 강전일, 박주성, 양대헌, “RFID 시스템에서의 프라이버시 보호기술”, 한국정보처리학회지, 제12권, 제6호, pp.28-36, 2004. 12.

[4] Auto-ID Center, "860MHz-960MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical communication Interface Specification Proposed Recommendation Version 1.0.0", Technical Report MIT-AUTOID-TR-007, NOV, 2002

[5] Henrich, D. and Műller, P., “Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers”, Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshop (PERCOMW'04), pp. 149-153, IEEE, 2004.