저가형 RFID를 위한 개선된 인증 프로토콜 설계

양진희*, 양성훈*, 김진보*, 김미선**, 정석원*, 서재현*
목포대학교 정보보호전공*, 컴퓨터공학전공**

Design of Improvement Authentication Protocol for Low-Cost RFID

JinHee Yang*, SungHoon Yang*, JinBo Kim*, MiSun Kim**, Seokwon Jung*, JaeHyun Seo*
Information Security*, Computer Engineering**, Mokpo University

요 약

RFID(Radio Frequency Identification)는 무선 주파수를 이용하여 물리적인 접촉 없이 개체에 대한 정보를 읽거나 기록하는 자동인식 기술이다. 그러나 RFID의 특성으로 인하여 사용자의 프라이버시 침해가 발생하면서 이를 해결하기 위한 많은 프로토콜들이 제안되었으나 공격자의 여러 공격 형태로 인하여 많은 취약점이 발생하였다. 최근 저가형 RFID를 위한 효율적인 인증 프로토콜이 제안되었으나 공격자의 불법적인 태그에 대해 인증이 가능한 문제점을 해결하는 연구가 요구된다. 본 논문에서 제안된 프로토콜은 기존의 인증 프로토콜에서 리더에게 역할을 부여함으로써 처음 생산된 태그에 대해서도 위조된 태그의 인증이 불가능하다. 또한 연산량이 적은 장점과 더욱 강화된 보안성으로 인하여 안전하고 효율적인 저가의 RFID 태그에 적용이 가능할 것이다.

I. 서론

RFID(Radio Frequency Identification)란 무선 주파수를 이용하여 물리적인 접촉 없이 개체에 대한 정보를 읽거나 기록하는 자동인식 기술이다. 기존에 사용되고 있는 바코드를 대체할 RFID은 물류 및 유통, 의류, 축산관리, 교통요금 지불 시스템, 의료부문 등에서 사용되고 있다[1]. 그러나 RFID에서 무선 주파수 인식 기술의 특징은 RFID의 안전성과 개인의 프라이버시 측면에서 여러 가지 취약점이 존재한다. RFID에서 리더와 태그 사이의 통신은 무선 주파수를 사용하므로 제 삼자에 의해 도청이 가능하며 도청된 내용을 이용한 태그의 위조 및 변조, 위치 추적등은 개인의 프라이버시를 침해하는 문제와 직결된다. 이러한 RFID의 취약점을 해결하기위해 물리적인 기법을 이용하거나 암호학적 이론 및 단순 XOR연산 등의 기법들이 제안되었다.

본 논문에서는 기존 인증 프로토콜들과 달리 해쉬 연산을 없애고 단순 XOR과 + 연산만을 이용하는 기법의 저가형 RFID을 위한 효율적인 인증 프로토콜의 문제점을 분석하고 이러한 문제점을 개선하여 안전성을 지원하는 인증 프로토콜을 제안한다.

본 논문의 구성은 2장에서 기존에 제안된 프로토콜들의 안전성과 효율성을 기술한다. 3장에서는 기존의 인증 프로토콜의 문제점을 분석하고, 새로운 프로토콜을 제안하며 4장에서는 결론을 맺는다.

II. 관련 연구

RFID에서 취약점을 보안하기 위한 기법으로 물리적인 기법과 암호 알고리즘기법 그리고 XOR등의 연산을 이용하는 기법들이 있다. 본 장에서는 암호 알고리즘을 기반으로 하는 기존 인증 프로토콜들에 대해 표를 이용하여 안정성 및 효율성을 간단하게 분석한다.

암호 알고리즘을 기반으로 하는 인증 프로토

콜에는 해쉬 연산을 이용하는 해쉬 체인, 해쉬 락, 확장된 해쉬 락 기법이 있으며, 해쉬 연산 및 태그의 ID를 변형시켜 이용하는 기법으로

[표 1] 인증 프로토콜들의 연산량

기법	연산량(회수)		
	태그	리더	DB
해쉬 기반 ID 변형[3]	해쉬 함수 : 3	-	난수 생성 : 1 해쉬 함수 : 3
향상된 해쉬 기반 ID 변형[3]	해쉬 함수 : 2	난수 생성 : 1	해쉬 함수 : 2
해쉬 체인[4]	해쉬 함수 : 2	-	해쉬 함수 : (태그의 수/2)*i
해쉬 락[4]	해쉬 함수 : 1	-	-
확장된 해쉬 락[5]	난수 생성 : 1 해쉬 함수 : 1	해쉬 함수 : 태그의 수/2	-
Challenge -Response[7]	해쉬 함수 :3(4)	난수 생성 : 1	해쉬 함수 : (태그의수/2)+1

해쉬 기반 ID 변형, 확장된 해쉬 기반 ID변형 등이 있다. 그리고, 공개키 방식을 이용한 외부 재 암호화 기법등이 있으며 [표 1]은 기존에 설계된 인증 프로토콜의 연산량을 나타낸 것이다. 다음 [표 2]는 기존 인증 프로토콜들의 안전성을 나타낸 것이다.

[표 2] 인증 프로토콜들의 안전성

기법 / 종류	해쉬 락	확장 해쉬 락	해쉬 체인	해쉬 기반 ID변형	개선된 해쉬기반 ID 변형	Challenge - Response
스푸핑	×	×	×	×	O	O
재전송	×	×	×	O	O	O
내용분석	×	×	O	O	O	O
위치추적	×	×	O	△	△	O
메시지차단	×	×	×	×	×	×

O : 강, △ : 중, x : 약

[표 1]과 [표 2]에서 본 것과 같이 해쉬 기반 인증 프로토콜은 태그에서의 해쉬 연산과 DB에서 태그의 ID를 탐색하기 위한 해쉬 연산을 필요로 하는데 현재 태그의 제한된 자원으로 해쉬 연산을 적용하기가 어렵다. 또한 안전성 측면에서도 메시지 차단에 대한 공격은 모두 취약한 것으로 나타났다[3, 4, 5, 6, 7].

III. 제안하는 인증 프로토콜

본 장에서는 저가의 태그에 적합한 효율적이고 안전한 인증 프로토콜을 제안한다. 제안된 프로토콜은 리더가 매 세션마다 난수를 발생시켜 사용함으로써 기존의 논문 [2]에서 제안된 프로토콜보다 더 효율적인 안전성을 갖는다.

논문 [2]에서 제안된 인증 프로토콜은 단순한 비트 연산만을 사용하기 때문에 효율적이며, 공격자가 리더와 태그 사이의 통신을 모두 도청 가능하다는 가정에서도 안전하다. 그러나 태그가 생산된 후 인증 세션이 한 번도 이루어지지 않은 상태에서 다음과 같은 과정을 통해 공격자에 의한 불법적인 태그의 인증이 가능하다. 다음은 공격자가 리더와 태그 사이에 송·수신되는 정보들을 취득 하는 과정이다. 단, 태그가 생산된 후 인증 세션이 한 번도 이루어지지 않은 상태라 가정한다.

먼저, 본 논문에서 고려하는 위장된 Tag를 이용한 공격 시나리오는 다음과 같다.

① 공격자가 리더로 가장하여 정당한 태그에게 Query를 브로드 캐스팅하여 정당한 태그로부터 질의에 대한 응답 A_1을 획득하고 세션을 종료 시킨다. DB 및 Tag의 비밀 값, 랜덤 값은 변화가 없다.

② 공격자는 A_1의 값을 다음 세션의 정당한 리더의 질의응답으로 사용하여 B^1_1, B^2_1 를 획득하고 세션을 종료 시킨다. DB 및 Tag의 비밀 값, 랜덤 값은 변화가 없다.

③ 정상적인 세션이 시작되고 공격자는 도청을 통해 C_1, D_1을 획득 후 차단시킴으로 정상적인 세션은 종료된다. DB의 A_2 인덱스 필드가 생성되고 다음 세션에서 사용될 Tag의 랜덤 값이 저장되지만 Tag의 비밀 값, 랜덤 값은 변화가 없다.

공격자는 위 과정을 통해 획득한 값들을 다음 세션에서 이용하여 공격자 태그에 대해 인증이 가능하다. 다음은 위에서 취득한 값을 이용하여 공격자의 태그를 인증하는 과정이다.

(1) 리더의 질의에 대한 응답으로 ①에서 획득한 A_1을 전송한다.

(2) 데이터베이스는 이전 세션에서 메시지가 유실된 태그의 ID로 판별하고 수신된 A_1을 이용하여 이전 세션에 사용된 A_1의 인덱스 필드를 찾는다.

Index	SV				RN				AE	Data
A_1	α	β	γ	λ	r_1	s_1	k_1	t_1	N	···

(3) 데이터베이스는 A_1 인덱스 필드의 비밀 값, 랜덤 값을 이용하여 B^1_1, B^2_1 을 생성하여 공격자 태그에게 송신한다.

(4) 공격자 태그는 ③에서 획득한 C_1을 데이터베이스에 전송하고 데이터베이스는 C_1의 값이 A_1의 인덱스 필드에 있는 값들로 계산되어 졌는지 확인한다.

(5) 데이터베이스는 D_1의 값을 생성하여 공격자 태그에 전송하고 세션은 종료된다.

기존 인증 프로토콜은 태그가 처음 생산되고 인증 세션이 한 번도 이루어지지 않은 상태에서 공격자의 공격에 의해 위조된 태그가 인증되는 문제점 있다. 이러한 문제점은 리더에게 특정한 역할을 부여하여 아주 쉽게 해결이 가능하다. [그림 1]는 본 논문에서 제안하는 프로토콜의 구성도이며 리더에서 생성된 난수를 이용하여 처음 생산된 태그에 대해서도 공격자의 위조된 태그 인증이 불가능한 안전성이 강화된 인증 프로토콜이다.

본 논문에서 사용된 파라미터는 다음과 같다.

- A_n : 인덱스 어드레스
- SV : 비밀 값 $\{\alpha_i, \beta_i, \gamma_i, \lambda_i,\}$
- R_N : 랜덤 값 $\{r_i, s_i, k_i, t_i\}$
- AE : 메시지 유실시 이전 데이터를 찾기 위한 인덱스 어드레스
- R_i : 리더의 난수

SV	α	β	γ	λ
RN	r_1	s_1	k_1	t_1

- || : 연접
- function : $\oplus$, +

본 논문에서 제안하는 개선된 인증 프로토콜의 인증단계는 다음과 같다.

1. 리더는 자신이 생성한 난수 R_1과 함께 태그에게 질의 요청 한다.

2. 태그는 $A_1=(\alpha+r_1)\oplus(\lambda+r_1)$을 생성하여 리더로부터 수신한 R_1을 XOR하여 질의응답으로 전송하고 리더는 DB에게 A_1과 R_1을 전송한다.

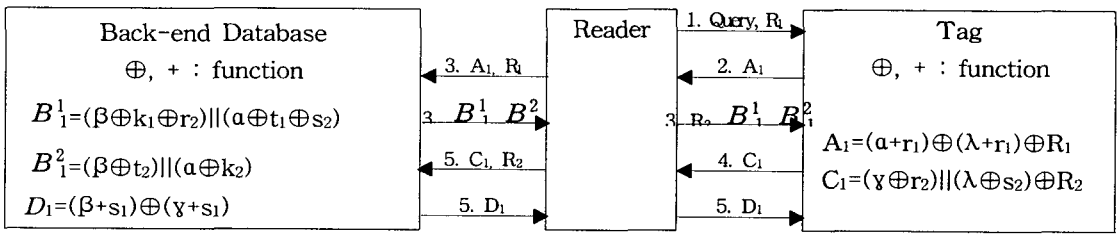
3. DB는 리더로부터 수신 받은 R_1을 이용하여 인덱스 넘버 A_1을 추출하여 태그를 인증하고 랜덤 값 r_2, s_2, k_2, t_2를 생성하고 B^1_1, B^2_1을 생성 후 리더에게 전송한다.

4. 리더는 다시 난수 R_2를 생성하여 B^1_1, B^2_1과 R_2를 태그에게 전송한다.

5. 태그는 수신 받은 B^1_1, B^2_1에서 r_2, s_2, k_2, t_2를 추출하고 리더로부터 수신 받은 R_2와 추출된 값 r_2, s_2와 자신의 비밀 값을 이용하여 C_1을 생성한 뒤 리더에게 전송한다.

6. 리더는 C_1을 수신 받아 자신의 난수 R_2와 함께 DB에게 전송한다.

7. DB는 수신 받은 R_2를 이용하여 C_1값을 추출하고 C_1 값이 DB에서 계산된 값과 같은지 비교하여 D_1을 생성하여 다시 리더를 통하여 태그에게 전송한다.



Index	SV				RN				AE	Data
A_1	α	β	γ	λ	r_1	s_1	k_1	t_1	A_2	···
A_2	α	β	γ	λ	r_2	s_2	k_2	t_2	A_1	···

SV	α	β	γ	λ
RN	r_2	s_2	k_2	t_2

[그림 1] 제안하는 저가형 RFID을 위한 개선된 인증 프로토콜

8. 태그는 수신 받은 D_1이 자신이 생성한 값과 같은지 확인하여 DB를 인증하고 태그에 저장된 랜덤 값 r_1, s_1, k_1, t_1을 r_2, s_2, k_2, t_2로 갱신한다.

제안된 기법은 연산의 효율성 측면에서 기존의 논문에서 기술한 바와 같이 단순한 XOR, + 연산만을 이용하므로 제한적인 기능을 갖는 태그에서도 쉽게 구현이 가능하다. [표 3]은 기존의 프로토콜과 제안하는 프로토콜의 안전성을 비교한 것이다.

[표 3] 제안 프로토콜의 안전성

	기존 프로토콜	제안 프로토콜
위치 추적	O	O
스푸핑	△	O
재전송	△	O
메시지차단	O	O

O : 강, △ : 중, X : 약

위와 같이, 안전성 측면에서는 기존의 프로토콜이 갖는 문제점을 보완하여 공격자의 태그가 인증되는 것을 막을 수가 있으므로 우수한 것으로 사료된다.

제안하는 프로토콜에서 공격자가 태그와 DB의 비밀 값, 랜덤 값을 알기 위해서는 여러 번의 세션을 거쳐야 한다. 그러나 매 세션마다 리더에서 생성시킨 난수를 이용하기 때문에 공격자는 세션마다 달라지는 각 Step 들의 값으로 비밀 값, 랜덤 값을 추출하기 어려우며 태그의 위치 추적도 불가능 하다. 또한, 태그에 저장된 랜덤 값이 DB에서 생성한 랜덤 값으로 갱신되므로 공격자에 의한 스푸핑 공격과 재전송 공격에 완벽하게 안전하며 공격자에 의해 D_1값의 메시지가 유실 되더라도 DB의 인덱스 필드에 의한 데이터 참조가 가능 하므로 태그와 관련된 정보를 쉽게 찾을 수 있다.

IV. 결 론

RFID은 무선 인식 기술로 여러 분야에서 활용되고 있으나 무선 인식 기술의 특성상 공격자에 의한 도청, 스푸핑 공격, 재전송 공격, 메시지 유실, 위치 추적등의 여러 취약점이 존재하였다. 이러한 취약점을 보완하기 위해 암호학적 함수를 이용한 기법등 여러 인증 프로토콜이 개발 되었으나 공격자에 의한 다양한 공격에 취약하거나 현재의 제한적인 태그에 적용하기 힘든 기법들이었다.

본 논문에서 제안된 프로토콜은 기존의 인증 프로토콜에서 리더에게 역할을 부여함으로써 처음 생산된 태그에 대해서도 위조된 태그의 인증이 불가능하다. 또한 연산량이 적은 장점과 더욱 강화된 보안성으로 인하여 안전하고 효율적인 저가의 RFID 태그에 적용이 가능할 것이다.

[참고문헌]

[1] 유승화, "유비쿼터스 사회의 RFID", 2004, 전자 신문사

[2] 최은영, 최동희, 임종인, 이동훈, "저가형 RFID을 위한 효율적인 인증 프로토콜", 정보보호학회 VOL. 15, NO5, 2005. 10.

[3] 황영주, 이수미, 이동훈, 임종민, "유비쿼터스 환경의 Low Cost RFID 인증 프로토콜", 한국정보보호학회 하계정보보호학술대회 논문집 Vol.14, No.1, pp.109-114, 2004.

[4] M. Ohkubo, K. suzuki, and s. Kinoshita, "Hash-Chain Based Forward Secure Privacy Protection scheme for Low Cost RFID", proceedings of the SCIS 2004, pp.719-724, 2004.

[5] S. E. Sarma, S. A. Weis, D. W. Engels, "RFID systems, Security & Privacy Implications", White Paper MIT AUTOID WH 014, MIT AUTO-ID Center, 2002.

[6] S. A. Weis, "Security an privacy in Radio frequency Identification Devices" MS Thesis, MIT. May, 2003.

[7] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, 분산 데이터베이스 환경에 적합한 Challenge response 기반의 안전한 RFID 인증 프로토콜, 이근우 외, KRF, 2004.