저가격 RFID를 위한 안전하고 효율적인 새로운 인증 방식에 관한 연구

서대희, 이임영
순천향대학교 정보기술공학부
e-mail:patima@sch.ac.kr

A Study on Secure and Efficient New Authentication for Low Cost RFID

Dae-Hee Seo, Im-Yeong Lee
Division of Information Technology Engineering
SoonChunHyang University

요약

최근 인터넷의 급성장에 따라 새로운 컴퓨팅 환경인 유비쿼터스 기반의 다양한 연구들이 수행되고 있다. 특히 RFID는 유비쿼터스 구현을 위한 핵심 요소 기술로 자리잡고 있으며, 이에 대한 연구는 국내외적으로 매우 활발히 진행되고 있다. 그러나 RFID의 특성상 소형화되고 제한된 물리적 특성 때문에 보안 서비스를 제공하는데 한계성이 있다.

따라서 본 논문에서는 저가격의 RFID에서 안전한 인증 방식을 제안하고자 한다. 제안된 방식은 기존의 연구보다 계산에 대한 효율성과 일반화된 적용을 위한 특징을 갖는다.

또한 암호화 알고리즘과 해쉬 함수로 대표되는 함수의 사용을 일반화된 함수로 표현하여 다양한 적용성을 가질 수 있어 응용 서비스로의 확장이 용이하다.

1. 서 론

유비쿼터스 네트워크 환경의 특징은 사용자 중심으로한 주변 상황이나 환경을 네트워크가 지능적으로 파악하여 사용자 네트워크 환경을 최적화시켜 네트워크에 편리하게 연결하는 것이다.

특히, 유비쿼터스 센서 구성을 위한 핵심 기술로 자리잡고 있는 RFID 태그는 무선 통신을 이용해 원격으로 감지 및 정보를 인식하여 정보의 교환을 가능케 하는 기술로써 기존의 오프라인에서 대표적으로 활용되고 있는 바코드 체계를 대체할 수 있어 개인생활은 물론 산업 전반에 많은 응용 서비스가 가능하여 최근 많은 연구 개발이 이루어지고 있다.

따라서 본 논문에서는 저가형 RFID 기반의 안전한 인증 방식을 제안하기 위해 본 논문의 2장에서는 RFID에 대한 일반적인 개요를 기술하고, 보안 요구사항을 제시한 뒤 3장에서 기존의 연구 방식을 분석하고자 한다. 4장에서는 2장에서의 보안 요구사항을 만족할 수 있는 저가형 RFID 기반의 안전한 인증 방식을 제안하고 5장에서 제안된 방식을 기존 방식과 비교 분석한 뒤 6장에서 결론을 맺고자 한다[1].

2. RFID의 개요와 보안요구사항

본 장에서는 RFID에 대한 일반적인 개요와 보안 요구사항을 제안하고자 한다.

2.1 RFID 개요

RFID 시스템은 판독 및 해독 기능을 하는 RF 리더기와 정보를 제공하는 RFID 태그로 구성된 무선통신 시스템이다. RFID 태그는 사람, 자동차, 화물등에 개체를 식별하는 정보를 부가하는 시스템으로 그 부가 정보를 무선 통신 매체를 이용함으로써 기존에 오프라인으로 이루어지는 다양한 어플리케이션을 자동화 할 수 있다. 따라서 연간 수십억개 이상의 보다 효율적인 RFID 태그 및 무선 네트워크가 필요할 것이며 새로운 소프트웨어와 많은 아이템을 다룰 수 있는 바코드 혹은 이와 비슷한 시스템이 요구될 수 있어 보다 다양한 형태의 어플리케이션을 지원할 수

1) 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음

있다[1][8].

2.2 보안 요구사항

안전성과 효율성을 고루 갖춘 시스템인 RFID 시스템의 경우 다양한 환경의 적용성을 가질 수 있다. 그러나 안전성 측면에서 ACIN (Authentication, Confidentiality, Integrity, Non-repudiation)과 관련된 공격 방법 뿐만 아니라 다양한 취약성이 태그 기반의 RFID 시스템에서 실제적으로 발생할 수 있으며, 이는 다음과 같다[3,4]. 따라서 저가형 RFID에서는 ACIN 뿐만 아니라 다음과 같은 추가적인 보안 요구사항을 만족해야 한다.

- 채널 보안 : RFID 시스템에서 신뢰된 DB와 리더기를 기반으로 리더기와 태그의 통신에 대한 안전성이 보장되어야 한다. 특히, 채널 보안 서비스 제공을 위한 태그의 연산량은 최소화 되어야 한다.
- 태그 비밀값의 안전성 : 태그의 비밀값이 인증 과정에서 노출되지 않아야 하며, 기밀 연산을 통해서 상호 인증 과정을 수행해야 한다.
- 효율성 : RFID 시스템에서 태그의 인증 과정시 수행되는 태그의 계산량은 최소화해야 한다.

3. 기존 연구 분석

RFID 태그와 관련된 연구는 최근 유비쿼터스 컴퓨팅과 관련하여 많은 주목을 받고 있으며, 이와 관련된 기존 연구로 대표적인 방식이 MIT Auto-ID 센터에서 제시된 방식이다. 현재 MIT Auto-ID 센터에서는 해쉬함수를 이용한 보안 서비스를 제공하기 위한 프로토콜이 제안하고 이를 적용시키기 위한 연구가 지속적으로 진행중에 있다.

(가) Hash Lock Scheme : MIT에 의해 제시된 방식으로 낮은 가격을 고려한 방식이다. 각각의 개체는 해쉬 함수를 가지고 있으며, 다음과 같은 방식으로 진행된다. 먼저 RF 리더기는 키 K를 각각의 RFID 태그에 전송하며, RFID 태그는 Meta ID를 계산한다. (Meta ID = Hash(K)) 태그는 ID 엑세스를 위해 Meta ID를 RF 리더기에 전송한다. RF 리더기는 사전 분배한 키와 Meta ID의 연계성을 고려하여 이를 검증한 뒤 검증 결과가 올바른 경우 그에 대한 응답 메시지를 RFID 태그에 전송한다. 이 방식의 경우 단지 전송 데이터에 대한 동의와 리더기가 가지고 있는 ID의 전송을 통해 인증 과정을 수행한다[2].

따라서 본 방식에서는 낮은 가격과 고정된 Meta ID를 통해 낮은 가격에 적용 가능한 방식을 제한하였지만 공격자는 공개된 Meta ID를 통해 태그에 대한 공격이 가능하다. 이외에도 Meta ID는 고정되어서는 안되지만 운영 시스템과 요구사항에 따라 약간의 차이가 존재하기도 한다.

(나) Randomized Hash Lock Scheme : MIT에서 제시된 방식으로 해쉬 Lock 방식의 확장된 형태이다. 이 방식의 경우 기존 방식과는 달리 RFID 태그가 안전한 해쉬 함수와 랜덤 생성기까지 가지고 있다고 가정한다. 각각의 RFID 태그는 랜덤 수를 생성하여 이를 입력 값으로 안전한 해쉬 값을 생성한다. (r와 ID. C=H(ID||r)), 태그는 C와 r을 리더기에 전송한다. RF 리더기는 전송된 데이터를 후방향 데이터 베이스에 전송한다. 데이터 베이스는 해쉬 함수를 이용해 전송된 r과 각각의 ID를 대응하여 저장한다. 데이터 베이스에서는 ID와의 연관성을 통해 C와 ID를 검증한다[5].

본 방식은 RFID 태그의 출력 정보가 엑세스 마다 매번 바뀌어 트래킹이 어려운 방식이다. 그러나 이와 같은 방식의 경우 RFID 태그의 위치 정보에 대해 추적 정보를 제공한다. 특히, RFID 태그의 비밀정보와 관계된다면, 전방향성 보안 사항에 만족할 수 없다. 추가적으로 해쉬 함수를 낮은 가격의 태그에 적용될 수 있으나 의사난수 생성기와 같은 경우에는 사실적으로 불가능하다.

(다) Hash-Chain Scheme : 일본의 NTT에서 제안된 방식으로써 안전한 해쉬 함수를 이용하여 해쉬 체인을 생성한다. 해쉬 체인값을 생성하기 위한 초기 값은 RFID 태그와는 무관한 값이며, 이를 기반으로 안전한 해쉬 체인 값을 생성하여 상호 인증을 수행하는 방식이다. 본 방식의 경우 기존의 EPC(Electronic Product Code)에 확장된 방식의 EPC 코드를 제안하였으며, PFS(Perfect Forward Secrecy)와 구분 불가능성을 만족하는 방식이다[6].

그러나 본 방식의 경우 데이터 베이스 서버에 대한 정보의 분할과 더불어 기밀성 측면에서의 안전성은 고려되지 않았다. 이는 초기 데이터 전송 이후의 전

송 데이터에 대한 PFS를 제공할 뿐이다. 따라서 NTT 방식의 경우 해쉬 체인을 생성하기 위한 초기값 전송시 기밀성 서비스와 확장성 부분에서 문제성 및 고유한 ID와 비밀정보 초기값에 대한 대응 저장으로 인해 발생할 수 있는 후방향성 서버의 안전성에 문제점을 지적할 수 있다.

4. 저가형 RFID 기반의 안전한 인증 방식 제안

본 장에서는 저가형 RFID 기반의 안전한 인증 방식을 다음과 같은 가정을 기반으로 제안하고자 한다.

- 제안 방식에서 사용되는 RFID 태그는 수동형 태그 기반의 매뉴얼 태그이다.
- 후방향성 DB와 리더기는 유선 채널로 신뢰된 개체이다.
- 초기 RFID 태그는 비밀값 x를 후방향성 DB에 안전하게 저장한다.
- 후방향성 DB는 RFID 태그의 비밀값 x에 해당되는 랜덤 스트링 L을 생성하여 이를 대응 테이블로 저장한다.
- 후방향성 DB는 RFID 태그의 비밀값 x와 이에 대응되는 랜덤 스트링 L을 이용하여 s를 계산한 뒤 이를 RFID 태그에 사전 등록한다. ($s = f_1(L) \oplus h_1(x)$)
- 각 구성 개체는 다음과 같은 함수를 사전에 내장하고 있다. (후방향성 DB(D), RF 리더기(R) : $f_1()$와 $h_1()$, RFID 태그(T) : $h_1()$)

4.1 각 개체 및 시스템 계수

다음은 저가형 RFID 인증 방식을 제안하기 위한 시스템 계수를 기술하고자 한다.

$f_1()$, $h_1()$: 일반화 함수

x : RFID 태그의 비밀 정보

L : 사전 등록된 RFID 태그의 비밀정보 x에 대응되는 값으로 후방향성 DB에서 생성한 랜덤 스트링

$\oplus$: Exclusive or

4.2 세부 프로토콜

① RF 리더기는 초기 Query 메시지를 RFID 태그에 전송한다.

② 초기 Query 메시지를 전송 받은 RFID 태그는 사전에 후방향성 DB로부터 분배받은 s를 RF 리더기에 전송한다.

③ RF 리더기는 내장된 $f_1()$ 함수를 이용해 v를 계산하여 v와 s를 후방향 DB에 전송한다.

$$v = f_1(s)$$

④ 후방향성 DB는 전송된 v를 다음의 과정을 거쳐 검증한다.

검증과정 : $s' = f_1(L) \oplus h_1(x)$을 계산한 뒤 전송된 s과 비교하여 올바른 경우 $f_1(s')$를 계산한 v'과 전송된 v를 비교하여 전송된 값을 검증한다.

검증이 올바른 경우 s와 대응되는 L을 이용해 z를 계산한 뒤 s와 z를 연접하여 RF 리더기에 전송한다.

$$z = f_1(L)$$

⑤ RF 리더기는 전송된 값 s가 ②에서 RFID 태그가 전송한 s와 동일한 것인지를 비교한 뒤 올바른 경우 z를 RFID 태그에 전송한다.

⑥ RFID 태그는 RF 리더기로부터 전송된 z를 기반으로 사전에 후방향성 DB로부터 전송된 s와의 비교를 통해 z의 정당성을 검증한다.

검증과정 : $z \oplus h_1(x) = s'$이고 $s' \equiv s$인지 검증한다.

검증 과정이 올바른 경우 RFID 태그는 w를 다음과 같이 계산한 뒤 이를 RF 리더기에 전송한다.

$$w = TID \oplus h_1(s)$$

⑦ RF 리더기는 ②에서 RFID 태그로부터 전송된 s와 ④에서 후방향 DB로부터 전송된 s로 $h_1(s)$를 생성한 뒤 RFID 태그로부터 전송된 w를 검증하고 올바른 경우 TID를 인증한다.

5. 제안방식 비교 분석

본 제안 방식은 2장에서 제시한 보안 요구사항을 다음과 같이 만족한다.

- ACIN : 제안방식은 저가형 RFID를 기준으로 제안된 인증 방식으로 일반화 함수 $f_1()$, $h_1()$를 통한 기밀성 제공과 무결성 서비스가 가능하며, 후방향 DB에서 사전에 RFID 태그에 분배된 s를 통해 태그에

대한 부인봉쇄 서비스가 가능하다.

- 채널 보안 : RF 리더기와 태그 사이의 전방향성 채널 보안은 $f_1()$ 함수의 안전성에 의존한다. 따라서 $f_1()$함수가 안전할 경우 제안 방식의 전방향성 채널 보안은 제공될 수 있다.

- 태그 비밀값의 안전성 : 제안방식은 RFID 태그의 비밀값 x가 공개되지 않고 이를 기반으로 생성된 s를 통해 인증 과정이 수행된다. 따라서 태그 비밀값의 안전성을 유지할 수 있는 보안적 특징을 제공한다.

- 효율성 : 제안된 방식은 기존의 방식들과 비교해볼 때 RFID 태그의 계산량이 검증과정과 TID 전송과정에서만 수행된다. 따라서 기존의 Hash Lock 방식과 비교해 볼때 같은 동등한 계산량을 제공한다. 또한 향상된 Hash Lock과 Hash Chain 방식과 비교 해볼 때 보다 경량화된 저가형 태그에 적용이 가능하다.

이상의 결과를 기존방식과 비교할 경우 표 1과 같이 정리할 수 있다.

[표 1] 기존 방식 분석

방식	ACIN	채널보안	태그 비밀값의 안전성	효율성
Hash Lock방식	AI만 만족	전방향 채널	비제공	구현 가능 (저가형 태그)
향상된 Hash Lock 방식	ACI 만족	전방향 채널	제공	구현 불가능 (고가형 태그)
Hash Chain 방식	AIN 만족	전방향 채널	제공	구현가능 (저가형 태그)
제안 방식	ACIN 만족	전방향 채널	제공	구현가능 (저가형 태그)

6. 결론

본 논문에서는 차세대 IT 기반 환경인 유비쿼터스 컴퓨팅 기술의 적용을 위해 다양한 연구가 추진중에 있는 RF 태그의 인증에 대한 연구를 수행하였다. 특히, 유비컴퓨팅 환경과 같은 사용자 중심의 네트워크 형성을 위해서는 소형 개체 기술이 반드시 요구되고 이와 더불어 사용자의 프라이버시를 보호할 수 있는 보안 기술이 반드시 요구되는 시점에서 매우 의미 있는 연구를 수행하였다. 제안된 방식은 2개의 일반화된 함수를 사용하면서도 RF 태그에서 사용되는 함수는 최소화 시켜 인증 과정을 수행하였다. 따라서 기존의 방식보다 효율적이면서 보안적인 안전성도 보장 받을 수 있는 장점이 있다. 그러나 능동적인 공격자에 대한 보안적 취약성은 여전히 존재하며 이를 보완하기 위한 연구는 지속적으로 추진해야 될 것이다. 따라서 향후 연구 방향으로는 보다 다양한 보안 위협에 대한 보완사항과 더불어 보다 현실적인 RFID 태그에 대한 보안 서비스를 위한 프로토콜이 연구되어야 할 것으로 사료된다.

7. 참고문헌

[1]. Stephen A. Weis, “Security and Privacy in Radio-Frequency Identification Devices”, Masters Thesis. MIT. May, 2003

[2]. Stephen A. Weis, Sanjay E.Sarma, Ronald L. Rivest and Daiel W. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, First International Conference on Security in Pervasive Computing, 2003. http://theory.lcs.mit.edu/ sweis/spc-rfid.pdf

[3]. Sanjay E.Sarma, “Towards the five-cent Tag”, Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org

[4]. Sanjay E.Sarma, Stephen A. Weis and Daiel W. Engels, “Radio-Frequency Identification : Secure Risks and Challenges”, RSA Laboratories Cryptobytes, vol. 6, no.1, pp.2-9. Spring 2003

[5] Sanjay E.Sarma, Stephen A. Weis and Daiel W. Engels, “Radio-frequency identification systems”, In Proceeding of CHES ’02, pp454-469. Springer-Verlag, 2002. LNCS no. 2523.

[6] Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, "Cryptographic Approach to "Privacy-Friendly" Tag" RFID Privacy Workshop@MIT, Nov, 2003

[7] MIT Auto-ID Center. http://www.autoidcenter.org

[8] RFID Journal. Gillette to Phurchase 500 Millin EPC Tags, http://www.rfidjournal.com