Multi-Purpose 구조에서 공개키 암호화를 이용한 RFID 인증 프로토콜에 관한 연구

신주석*, 윤태진**, 박용수*, 정경호*, 안광선*
*경북대학교 전자전기컴퓨터학부
**경운대학교 모바일공학과
e-mail:gome81@knu.ac.kr

A Study On A RFID Authentication Protocol Using Public Key Cryptography In Multi-Purpose Infrastructure

Ju-Seok Shin*, Tae-Jin Yun*, Yong-Soo Park*,
Kyung-Ho Chung*, Gwang-Sun Ahn**
*School of Electrical Engineering and Computer Science, Kyung-Pook University
**Dept of Mobile Engineering, Kyung-woon University

요 약

RFID 시스템에서 태그는 객체를 유일하게 식별하기 위한 정보를 가지고 있기 때문에 개인정보의 노출, 위치 추적 등의 프라이버시 침해를 유발할 수 있는 문제점이 있다. 태그가 다양한 목적을 위해 사용되어지는 경우 키 분배, 키 관리 등의 문제로 인해 공개키 암호화 기법이 적용될 수 있다. 공개키 암호화 기법을 이용한 기존 RFID 인증 프로토콜에서는 서버와 태그 사이에 공개키를 사전에 공유하고 있다고 가정을 하여 설계를 하였다. 하지만 하나의 태그가 다양한 목적으로 사용되는 다목적 구조에서 수동형 RFID 태그가 서로 다른 서버의 공개키를 모두 공유한다는 것은 현실적으로 불가능하다. 본 논문에서는 다목적 구조에서 XOR 연산과 리더와 태그가 사전에 공유한 마스터 키(K_m)를 사용하여 태그에게 공개키를 안전하게 전달하며 이를 이용한 공개키 암호화 기반의 RFID 인증 프로토콜을 제안한다. 또한 제안한 인증 프로토콜은 프라이버시 침해를 유발할 수 있는 도청, 재전송 공격, 위치 추적과 같은 공격에도 안전성을 보장한다.

1. 서론

RFID(Radio Frequency Identification) 시스템은 태그(Tag)와 리더(Reader)가 무선주파수(Radio Frequency)를 이용하여 물리적 접촉 없이 데이터 통신이 가능한 자동 인식 시스템이다. 하지만 기존의 바코드에 비해 비용이 높고, 스마트카드에 비해서는 메모리 용량이 작은 단점이 있다. 그러나 개개인 식별과 관련해서 서비스 제공을 위한 유비쿼터스 환경에 적합한 핵심기술로서 물류 및 재고관리, 교통카드, 가축관리, 의료관리 분야 등 다양한 분야에 활용이 가능하다.

RFID 태그는 객체를 유일하게 식별하기 위한 정보를 가지고 있기 때문에 개인정보의 노출, 위치 추적 등의 프라이버시 침해를 유발할 수 있는 문제점이 있다. 따라서 RFID 보안 기법에는 태그와 리더 간의 암호화된 데이터의 전송, 태그와 리더간의 효율적인 인증 등이 요구된다. 태그와 리더 간의 데이터 전송을 위한 암호학적 기술은 공개키 알고리즘이나 대칭키 알고리즘, 혹은 ID와 연관된 난수 값을 사용한다. RFID 시스템에서는 주로 대칭키 알고리즘을 이용하여 태그의 정보를 암호화하는 기법과 이를 바탕으로 한 인증 프로토콜이 많이 연구되었다[1].

RFID 시스템에서 태그가 하나의 목적을 위해 사용되어지는 경우에는 대칭키 기반의 암호화 기법이 적합하지만 태그가 다양한 목적을 위해 사용되어지는 경우에는 키 분배, 키 관리 등의 문제로 인해 공개키 암호화 기법이 적합하다[2]. 하지만 공개키 암호화 알고리즘의 경우 하드웨어 자원의 제약이 있는 저가의 태그에는 현실적으로 적용하기 어렵다. 그러나 최근에는 태그가 다양한 목적으로 사용되어지는 구조 또는 이와 유사한 구조에서 공개키를 이용한 연구가 많이 진행 중이며 실제 적용한 사례도 있다[2][3][4][5].

본 논문에서는 하나의 태그가 다양한 목적으로 사용되어지는 다목적 구조(Multi-Purpose infrastructure)에서 공개키 암호화를 이용한 RFID 인증 프로토콜을 제안한다. 또한 제안한 인증 프로토콜은 도청, 재전송 공격, 위치 추적과 같은 다양한 공격에도 안전하다.

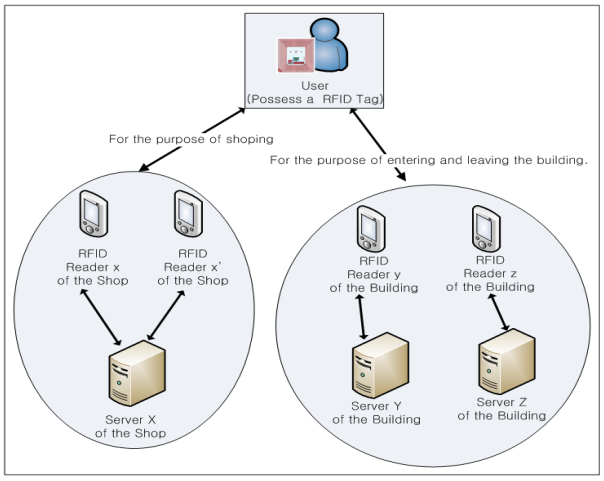
2. 관련연구

2.1 다목적 구조

본 논문에서 다목적 구조는 하나의 태그가 다양한 목적으로 사용될 수 있는 구조이다. 하나의 태그가 서로 다른

목적을 가지고 각각의 리더에게 자신의 고유정보를 전송함으로써, 리더는 태그에 대한 정보를 서버로부터 얻을 수 있다.

(그림 1)은 다목적 구조를 보여주고 있다.



(그림 1) 다목적 구조

다목적 구조에서 프라이버시 침해와 관련된 문제를 해결하기 위해 대칭키 암호화 방법을 사용할 경우에는 각각의 태그마다 서로 다른 서버의 대칭키를 가지고 있거나 모든 태그와 서버가 같은 대칭키를 공유하고 있어야 한다. 따라서 공격자에게 키 값을 알아낼 수 있는 더 많은 기회를 제공한다. 이를 보완하기 위해 많은 연구가 있었지만 여전히 키 분배 문제가 있으므로 위와 같은 다목적 구조에서는 공개키 암호화를 사용하는 것이 효율적이다. 이와 유사한 구조에서 공개키 암호화 방법을 사용하여 보안을 해결하기 위해 제안된 기법들이 많이 있으며 적용된 사례도 있다.

혈액을 관리하기 위해 센서와 태그, 태그와 리더 간에 공개키 암호화를 이용하여 상호 인증을 함으로써 안전하게 혈액을 관리하는 기법이 제안되었고[3], 태그가 다수의 도메인에 접근할 때 태그의 고유정보가 부정당한 리더에게 읽혀지지 않게 하기 위하여 공개키 암호화 방식에서 전자서명 방식을 이용한 인증 프로토콜도 제안되었다[4]. 또한 약을 제조한 후 최종 목적지까지 안전하게 전달하고 진품확인을 위하여 전자서명 방식을 이용한 사례도 있다[5]. 이와 같이 공개키 암호화체계를 이용한 연구가 활발히 진행 중이다.

2.2 공개키 기반의 암호화 기법

공개키 암호체계에서는 서버가 공개키와 비밀키 쌍을 생성한 후 공개키는 암호화에 사용하고 비밀키는 복호화에 사용하는 암호체계이다. 그리고 공개키는 공개가 되므로 누구나 공개키를 사용할 수 있기 때문에 키 분배문제를 해결 할 수 있다. 따라서 최근에는 공개키 암호화 알고리즘인 ECC(Elliptic Curve Cryptography) 또는 NTRU를 수동형 RFID 태그에 구현하고 이를 이용한 인증 프로토콜에 관한 연구들이 활발히 진행 중이다[2][6]. 수동형 RFID 태그에 ECC 암호화 알고리즘을 구현할 경우 18,121 게이트가 필요하고, NTRU 암호화 알고리즘을 구현할 경우는 10,500 게이트가 필요하다. 특히 NTRU 암호화 알고리즘은 태그에서 암호화만 수행할 경우에 3,000 게이트만 필요하므로 수동형 RFID 태그에 적합하다[2]. 따라서 본 논문은 수동형 RFID 태그에서 NTRU암호화 알고리즘의 암호화만 이용한 인증 프로토콜을 제안한다.

2.3 NTRU 암호화 알고리즘

NTRU 알고리즘은 링 R =Z[X]/(X^{N-1}) 상에서 다항식의 덧셈과 곱셈을 기반으로 하며, 세 개의 정수(N, p, q)를 사용한다. N, p, q에 대한 조건은 (그림 2)와 같다.

- N은 소수(prime)
- gcd(p,q)=1.(p와 q는 서로소)
- q는 p보다 훨씬 큰 수

(그림 2) 세 개의 정수(N, p, q)에 대한 조건

NTRU 알고리즘의 키 생성, 암호화, 복호화 과정은 (그림 3)과 같다[7][8].

(1) Key Generation
- Choose two random polynomial : f,g ∈ R
- Must exist $f_q \equiv f^{-1} \pmod q$, $f_p \equiv f^{-1} \pmod p$
- Compute $h \equiv f_q * g \pmod q$
- Public key is h
- Secret keys are f and f_q

(2) Encryption

Encrypted text is evaluated as,
- $e \equiv pr * h + m \pmod q$

(3) Decryption

In order to decrypt the encrypted text e as,
- First compute $a \equiv f*e \equiv pr * g + f * m \pmod q$
- Second compute $b \equiv a \pmod p = f * m$
- Final compute $c \equiv fp*b \pmod p = m$

(그림 3) NTRU 알고리즘의 키 생성, 암호화, 복호화 과정

3. 다목적 구조에서 RFID 인증 프로토콜

3.1 제안 인증 프로토콜 가정 사항

서버와 리더사이에는 안전한 채널이며, 리더와 태그 사이는 안전하지 못한 채널이다. RFID 시스템에서 발생할 수 있는 다양한 공격들은 안전한 채널에서는 발생하지 않으며 안전하지 못한 채널에서만 발생한다고 가정한다. 인증 프로토콜에서 사용되는 태그는 수동형 RFID 태그이다.

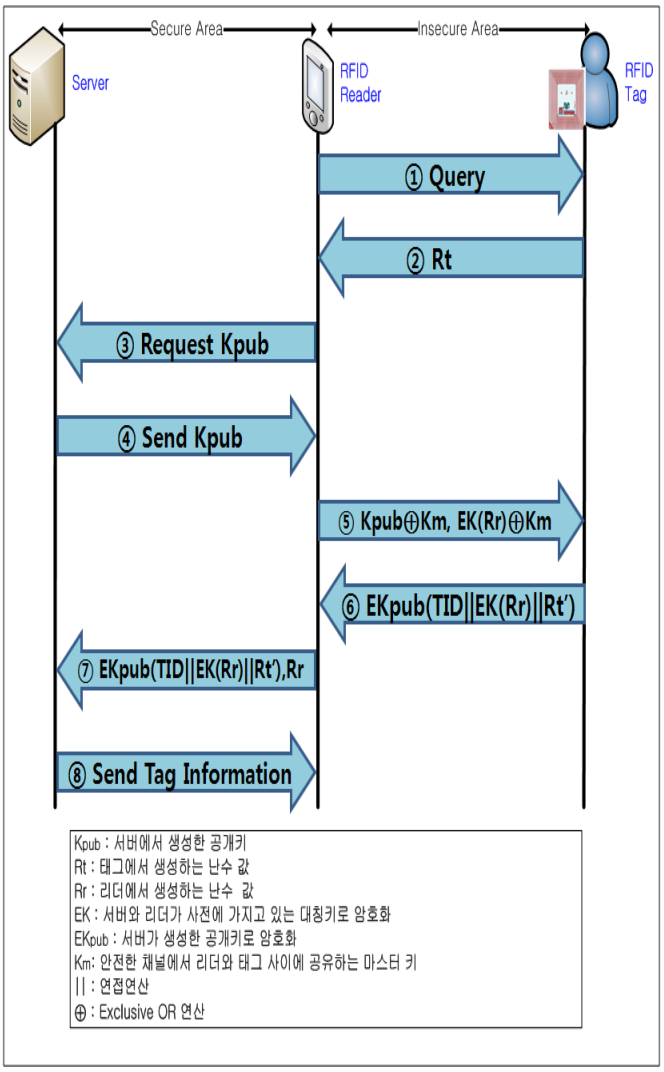
공개키 암호체계는 중간자 공격에 취약하기 때문에 믿을 수 있는 인증기관을 두어 공개키를 관리하는 방식으로 사용된다. 송신자가 메시지를 보낼 때 수신자의 공개키를 인증기관에서 발급하는 인증서에서 확인한 후 메시지를 공개키로 암호화 하여 수신자에게 보내준다. 하지만 수동형 RFID 태그에서는 위와 같은 기능을 할 수 없기 때문

에 중간자 공격을 방지하기 위하여 서버와 리더는 사전에 동일한 대칭키를 가지고 있으며 리더와 태그는 사전에 안전한 채널을 통하여 마스터키(K_m)를 서로 가지고 있다.

3.2 제안 인증 프로토콜

기존에 공개키 암호화 기법을 이용한 인증 프로토콜에서는 사전에 서버와 태그 사이에 공개키를 공유하는 것을 가정으로 하여 설계를 하였다[2]. 하지만 다목적 구조에서 서버와 태그 사이에 공개키를 공유하는 것을 가정으로 하면 수동형 RFID 태그가 사전에 서로 다른 서버의 공개키를 모두 공유하고 있어야 하므로 현실적으로 불가능하다. 따라서 본 논문에서는 서버에서 생성한 공개키를 리더가 XOR 연산과 마스터 키(K_m)를 이용하여 태그에게 안전하게 전달하는 방법을 사용한다.

(그림 4)는 제안한 인증 프로토콜을 보여주고 있다.



(그림 4) 제안 인증 프로토콜

다음은 제안한 인증 프로토콜에 대한 설명이다. 제안한 인증 프로토콜은 여덟 단계를 가지며 각 단계는 다음과 같다.

① 수동형 RFID 태그는 자체전원 없이 리더로부터 수신한 전자기파에 의해 유도된 전류를 전원으로 사용하고, 리더의 Query가 있어야 이에 반응하여 통신할 수 있다. 리더는 태그가 전송하는 데이터를 수신하여 태그를 인식하기 위해 주기적으로 Query를 보낸다.

② 리더가 전송하는 RF 신호에 의해 태그는 전원을 공급받고 리더에게 태그 내에 있는 난수 생성기를 통하여 생성된 랜덤 값 R_t를 보낸다.

③ 리더는 서버에 공개키 K_{pub}를 요청하고 서버는 NTRU 암호화 기법의 키 생성 알고리즘에 의해 공개키와 비밀키 쌍을 생성한다. 서버에서 생성한 비밀키를 알 수 없으면 공개키를 알더라도 공개키로 암호화한 값을 복호화 하기는 어렵다. 하지만 보안에 안전하도록 하기위해서 리더가 공개키를 요청할 때 일정 주기마다 공개키와 비밀키 쌍을 다시 생성 한다.

④ 생성된 키 쌍 중에서 공개키 K_{pub}를 리더에게 보낸다.

⑤ 리더는 태그와 안전한 채널에서 이미 저장되어있는 마스터 키 K_m과 서버에서 받은 공개키 K_{pub}를 XOR 연산을 한다. 그리고 리더는 서버와 사전에 가지고 있는 대칭키로 자신의 난수 생성기를 통해 생성한 랜덤 값 R_r을 암호화한 값과 XOR 연산을 하여 태그에 $K_{pub}⊕K_m$과 $EK(R_r)⊕K_m$을 보낸다.

⑥ 태그는 리더에서 받은 정보에서 K_{pub}, $EK(R_r)$ 값을 마스터 키 K_m과 XOR 연산을 통하여 얻을 수 있다. 두 값을 얻은 후 자신의 고유정보인 T_{ID}와 $EK(R_r)$값과 태그에서 생성한 랜덤 값 R_t'를 모두 연접한 값을 공개키 K_{pub}로 암호화하여 리더에게 $EK_{pub}(T_{ID}||EK(R_r)||R_t')$을 보낸다. 여기서 R_t' 값은 ②번 과정에서 태그가 생성한 랜덤 값이 아니라 태그에서 새로 생성한 랜덤 값이다.

⑦ 리더는 $EK_{pub}(T_{ID}||EK(R_r)||R_t')$과 ⑤에서 리더가 생성한 랜덤 값 R_r을 서버에게 전송한다. 리더와 서버 사이에는 안전한 채널이므로 R_r 값을 그냥 전송하더라도 다양한 공격에 안전하다.

⑧ 서버는 자신의 비밀키를 이용하여 태그의 고유정보인 T_{ID}, 리더에서 대칭키로 암호화한 값 $EK(R_r)$, 태그에서 생성한 랜덤 값 R_t', ⑤에서 리더가 생성한 랜덤 값 R_r을 모두 얻을 수 있다. 이 후 서버는 리더와 사전에 알고있는 대칭키를 이용하여 $EK(R_r)$값을 복호화 하여 R_r값을 얻는다. 만약 두 개의 값이 다르다면 리더는 정당한 리더가 아니므로 리더에게 T_{ID}에 해당하는 태그의 정보를 보내 주지 않는다. 두 개의 값이 같다면 서버는 리더에게 T_{ID}에 해당하는 정보를 보낸다.

제안한 인증프로토콜은 공개키를 태그에게 안전하게 전달하기 위해서 XOR연산과 마스터 키(K_m)를 사용하였다. 또한 태그가 보내는 고유한 정보를 암호화하고 리더와 태그를 인증하기 위하여 공개키 암호화 기법과 대칭키 암호화 기법 및 랜덤 값을 사용하였다.

4. 보안 분석

(1) 도청

안전하지 못한 채널인 ①,②,⑤,⑥에서는 도청이 가능하다. 공격자가 태그의 응답 ②를 도청하더라도 랜덤 값 R_t 뿐이므로 아무런 의미가 없다. ⑤의 경우는 공격자는 마스터 키 K_m값을 모르므로 공개키 K_{pub}값과 $EK(R_r)$값을 알지 못한다. ⑥의 경우는 서버의 비밀키를 공격자가 알 수 없으므로 태그가 보내는 값을 복호화 하지 못한다. 따라서 도청을 하여 얻은 정보만으로는 도청한 값이 항상 변하므로 값을 유추할 수 없으며 다른 공격에 활용될 수 없다.

(2) 재전송 공격(Replay Attack)

공격자가 ②과정을 도청하였다가 정당한 리더의 요청에 대해 정당한 태그인 척 위장하여 리더에게 전송하는 경우에 공격자는 ⑤값을 얻을 수 있다. 하지만 공격자가 마스터 키 K_m을 알지 못하기 때문에 공개키 K_{pub}값과 $EK(R_r)$값을 얻을 수 없으며, ⑥을 생성할 수 없거나 틀린 정보를 리더에게 보내게 되어 ⑦,⑧과정에 의해 서버에서 감지할 수 있다. 또한 공격자가 ⑤과정을 도청하여 정당한 리더인 척 위장하여 태그가 보내는 ⑥값을 얻을 수 있다. 그러나 서버만 가지고 있는 비밀키를 알 수 없기 때문에 T_{ID}, $EK(R_r)$, R_t' 값을 얻을 수 없으며 ⑥과정에서 태그는 항상 랜덤 값을 연접하여 보내기 때문에 서버의 비밀키 값을 유추할 수 없다.

(3) 위치 추적(Location Traceability)

태그가 리더에게 보내는 값이 고정되어 있는 경우 태그를 소지하고 있는 사용자나 태그가 부착된 물품의 위치 추적이 가능하다. 제안한 프로토콜에서는 ②,⑥과정에서 태그는 항상 다른 값을 리더에게 보내기 때문에 위치 추적의 문제를 해결한다.

5. 결론

단일 태그가 여러 목적으로 사용될 수 있는 다목적 구조에서는 키 분배, 키 관리 문제로 인하여 공개키 암호화 알고리즘을 사용하는 것이 적합하다. 하지만 기존에 공개키 암호화 기법을 이용한 인증 프로토콜에서는 서버와 태그 사이에 공개키를 서로 공유하는 방법을 사용하여 인증 프로토콜을 설계하였다. 따라서 서로 다른 서버의 공개키를 수동형 RFID 태그가 사전에 모두 공유해야 하므로 현실적으로 불가능하다.

본 논문에서는 서버에서 생성한 공개키를 XOR 연산과 리더와 태그가 사전에 공유한 마스터 키(K_m)를 사용하여 태그에게 안전하게 전달하며 이를 이용한 공개키 암호화 기반의 RFID 인증 프로토콜을 제안했다. 또한 제안된 인증 프로토콜은 수동형 RFID 태그에 적합한 공개키 암호화 알고리즘인 NTRU를 이용하였으며 보안 분석을 통하여 도청, 재전송 공격, 위치 추적과 같은 다양한 공격에도 안전함을 확인하였다.

참고문헌

[1] M. Feldhofer, S. Dominikus and J. Wolkerstorfer “Strong authentication for RFID systems using the AES algorithm,” In Conference of Cryptographic Hardware and Embedded Systems, 2004. Proceedings, pp.357 - 370. Springer 2004.

[2] S. V. Kaya, E. Savas, A. Levi and O. Ercertin “Public key cryptography based privacy preserving multi-context RFID infrastructure,” Ad Hoc Networks, online available, February 2008.

[3] M. Li, C. Fung, K. Sampigethaya, R. Robinson, R.Poovendran, R. Falk and A. Koepf “Public-key based authentication for secure integration of RFID and sensor data,” In Proceedings of 1st ACM workshop on heterogonous sensor and actor networks, Hong Kong, China, May, 2008.

[4] M. Li, R. Poovendran, R. Falk, A. Koepf, K. Sampigethaya, R. Robinson and S. Lintelman “Multi-Domain RFID Access Control Using Asymmetric Key Based Tag-Reader Mutual Authentication,” 26th International Congress of the Aeronautical Sciences, ICIS 2008.

[5] Texas Instruments and VeriSign Inc “Securing the pharmaceutical supply chain with RFID and public-key infrastructure technologies,” Whitepaper, http://www.ti.com/rfid/docs/manuals/whtPapers/wp-Securing_Pharma_Supply_Chain_w_RFID_and_PKI_final.pdf(1.4.2006).

[6] M. Braun, E. Hess and B. Meyer “Using Elliptic Curves on RFID Tags,” IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008.

[7] J. Hoffstein, J. Pipher, and J. H. Silverman “NTRU: A Ring-Base Public Key Cryptosystem,” In J. P. Buhler, editor, Algorithmic Number Theory (ANTS III), Lecture Notes in Computer Science, volume 1423, pp.267 - 88, Berlin, 1998.

[8] “The NTRU Public Key Cryptosystem A-Tutorial.”

[9] J. H. Silverman “Almost Inverses and Fast NTRU Key Creation,” Technical report, NTRU Cryptosystems, 1999.