AES 와 난수사용을 기반으로 하는 개선된 RFID 인증 프로토콜

강현우*, 김영백*, 윤태진**, 박용수*, 안광선*
*경북대학교 전자전기컴퓨터학부
**경운대학교 모바일공학과
e-mail : hsdevils@knu.ac.kr

An Enhanced RFID Authentication Protocol Based on Using of AES and Random Numbers

Hyun-Woo Kang*, Young-Back Kim*, Tae-Jin Yun**, Yong-Soo Park*, Kwang-Seon Ahn*
* School of Electrical Engineering and Computer Science, Kyung-Pook University
**Dept. of Mobile Engineering, Kyung-Woon University

요 약

수동형 RFID(Radio Frequency Identification)는 제한된 자원을 가지고 있으며, 무선채널을 사용하는 기술이다. 하지만 도청과 같은 악의적인 공격과 프라이버시 침해와 같은 문제점이 있으며, 이를 해결하기 위한 각종 암호화 기법 및 알고리즘과 인증 프로토콜이 있다. AES(Advanced Encryption Standard)는 RFID 에 적용 가능한 대표적인 대칭키 암호화 알고리즘으로써 그 안정성이 검증되었지만, RFID 태그에서 사용하기 위해서는 키 분배와 같은 문제점을 해결하여야 한다. 본 논문에서는 AES 와 난수사용을 기반으로 하는 개선된 RFID 인증 프로토콜을 제안한다. 리더에서 발생된 난수는 새로운 키를 생성하고, 태그와 리더를 인증하는 용도로 사용하며, 난수를 통해 생성된 키는 메시지를 암호화 하는데 이용한다. 따라서, 본 논문의 난수사용은 대칭키의 노출을 막아 키 분배 문제를 해결하며, 인증 단계를 줄일 수 있다. 또한, 태그에서 한번의 암호화만 수행되므로 태그에 발생하는 오버헤드를 최소화하며 도청, 재전송, 스푸핑 및 위치 추적과 같은 공격에도 안전하다.

1. 서론

RFID(Radio Frequency Identification) 시스템은 ISO 18000-2~7 에서 규정한 무선 주파수를 이용한 비 접촉 방식의 자동인식 기술이다. 특히 수동형 RFID 태그의 경우 인식 거리가 비교적 길고 기존의 바코드에 비해서 저장 할 수 있는 데이터의 양이 많다. 따라서 물류 시스템뿐만 아니라 가축 관리, 산업 자동화, 교통요금지불 시스템 등 많은 분야에서 널리 활용되고 있다. 하지만 수동형 RFID 는 제한된 자원을 가지며, 무선채널을 사용하므로 도청과 같은 악의적인 공격과 개인 위치 추적, 정보 노출 등 프라이버시 침해와 같은 문제점이 있다. 이를 해결하기 위해서 Hash-Chain[1], Cellular Automata[2]등과 같은 각종 암호화 기법과 AES(Advanced Encryption Standard)와 같은 암호화 알고리즘이 있다. 그리고 이것을 이용한 인증 프로토콜이 많이 연구 되고 있다.

AES 는 이미 안전성이 검증되고, Martin Feldhofer 에 의해 RFID 태그에 적용한 사례가 있다. 하지만 RFID 태그에 적용하기 위해서는 키 분배와 같은 문제점을 해결하여야 한다. 키 분배 문제는 공개키를 이용한 방식으로 해결할 수 있지만, 수동형 RFID 태그와 같은 제한된 환경에서는 하드웨어 자원이 많이 필요한 공개키는 적용 하기가 어렵다.

본 논문에서는 AES 와 난수사용을 기반으로 하는 개선된 RFID 인증 프로토콜을 제안한다. 리더에서 발생된 난수는 태그로 전달되어 태그의 키와 XOR 연산을 통해서 새로운 키를 생성한다. 태그에서 생성된 키는 구성된 메시지를 암호화 하여 리더로 전달한다. 이것은 서버를 통해서 리더와 태그를 인증하며, 상호인증 효과를 가진다. 따라서, 본 논문의 난수사용은 대칭키의 노출을 막아 키 분배 문제를 해결하며, 인증 단계를 효율적으로 줄인다. 또한, 태그에서 한번의 암호화만 수행되므로 태그에 발생하는 오버헤드를 최소화할 수 있다. 도청, 재전송 및 스푸핑의 경우 메시지가 암호화되어 전달되고, 인증 과정을 거쳐야 하므로 공격이 어렵다. 위치 추적의 경우 메시지에 포함되는 Nonce 값이 항상 바뀌므로 정상적인 리더가 아니라면 위치 추적이 어렵다.

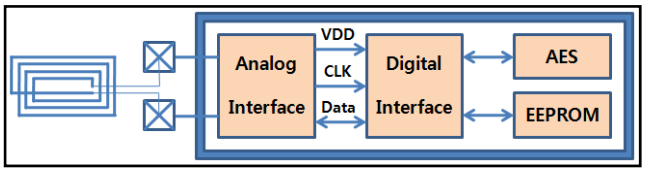
본 논문의 구성은 다음과 같다. 2 장에서는 RFID 에 적용 가능한 AES 대칭키 알고리즘과 기존 RFID 인증 프로토콜의 문제점에 대해 살펴보고 3 장에서는 기존 RFID 인증 프로토콜을 토대로 본 논문에서 제안한 개선된 프로토콜에 대해서 서술한다. 4 장에서는 제안된 인증 프로토콜의 보안에 대해 분석하며 마지막으로 결론을 맺는다.

2. 관련 연구

본 장에서는 RFID 에 적용 가능한 AES 알고리즘과 기존 RFID 인증 프로토콜의 문제점에 대한 관련 연구를 기술한다.

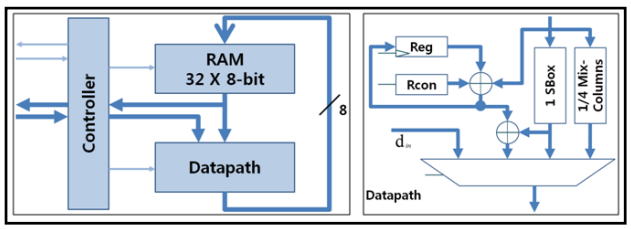
2.1. AES 알고리즘

AES 는 1987 년 NIST 에서 DES 를 대신할 새로운 암호화 알고리즘으로 채택된 것으로, V.Rindael 에 의해 제안한 알고리즘이다. 초기에는 키 값과 메시지 블록 사이즈를 128bit 로 하고 ARS 내부를 8 비트씩 암호화 하도록 설계 하였다가 이후 키와 블록사이즈를 128, 192, 256bit 에서 쓸 수 있도록 하였다. AES 는 블록의 크기에 따라서 10~14 라운드를 거쳐 암호화 하는데 각각의 라운드는 AddRoundKey, (Inv)SubBytes, (Inv) ShiftRows, (Inv)MixColumns 의 4 가지 연산으로 이루어진다.



(그림 1) M. Feldhofer 의 RFID 태그 구조

M. Feldhofer 가 제안한 RFID 태그의 구조는 (그림 1)과 같다. 안테나를 통해 전원과 클럭을 공급받고 데이터 모듈화를 하는 Analog Interface, Anti Collision 과 모든 명령을 수행하는 Digital Interface, ID 와 키를 저장하는 EEPROM 과 AES 암호화 연산 부분으로 구성되어 있다. 일반적으로 AES 알고리즘의 내부연산은 32bit 로 연산되지만 M. Feldhofer 의 경우 이것을 8bit 로 연산하여 S-box 의 갯수를 감소시키는 방법으로 하드웨어 자원을 절약하였다.



(그림 2) M.Feldhofer 의 AES 구조

(그림 1)의 AES 부분은 (그림 2)에서와 같이 총 3 부분으로 나누어진다. ShiftRows 연산을 수행하는 Controller, 저장과 SubBytes 연산을 돕는 RAM, 그리고 AddRoundKey, SubBytes, MixColumns 의 연산을 담당하는 Datapath 로 나누어 진다.[3]

2.2. 기존 RFID 인증프로토콜의 문제점

M. Feldhofer 가 제안한 인증 프로토콜[3][4]의 경우 난수를 이용한 단순 인증이었기 때문에 위치추적 공격과 도청공격에 취약하였다. Ohkubo 의 프로토콜[6]의 경우 프라이버시 관련 공격들을 방지하고, 전방위 보안성까지 보장하는 기법으로 가장 진보된 프로토콜이라 할 수 있다. 하지만 M. Feldhofer 의 연구[3]에 의하면 RFID 태그에 적용 가능한 크기를 약 5000Gate 카운트 미만으로 예측하고 있다. 따라서 해시함수를 태그 안에 구현하는 것은 현재로써 불가능하다. Toiruul[7]가 제안한 AES 를 활용한 인증 프로토콜의 경우 세션 키를 지속적으로 업데이트 하여 안전한 상호 인증 프로토콜을 제안했지만, 메시지 유실이 발생했을 경우 태그를 더 이상 사용할 수 없는 문제가 발생될 수 있다.

3. 제안 프로토콜

본 장에서는 AES 와 난수사용을 기반으로 하는 개선된 RFID 인증 프로토콜을 제안한다. 본문에서 사용하는 난수는 리더에서 발생되고 메시지를 암호화 하기 위한 새로운 키를 생성한다. 그리고 태그와 리더를 인증하는 용도로도 사용한다. (그림 3)은 제안한 RFID 인증 프로토콜을 나타낸다.

3.1. 초기 가정 및 용어

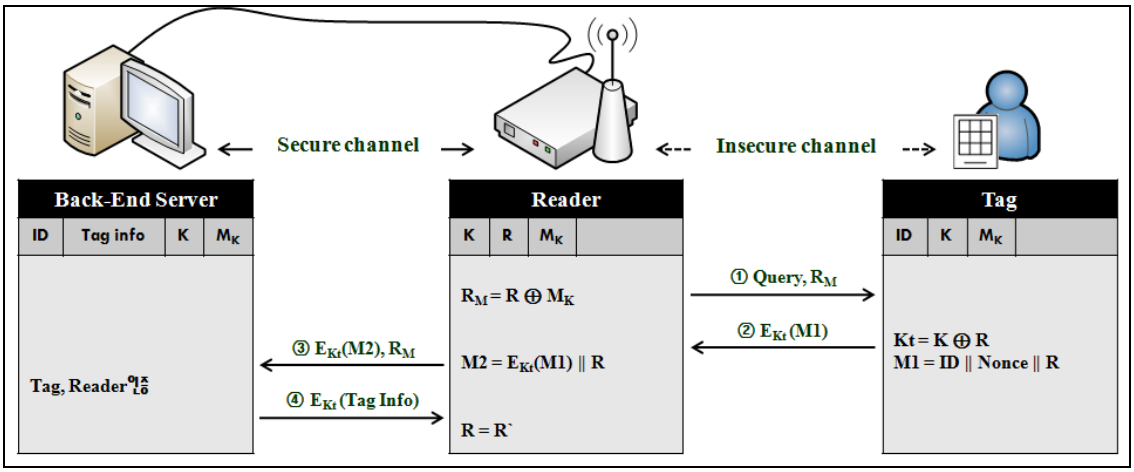
제안한 RFID 인증 프로토콜은 수동형 RFID 태그에 대한 다음의 4 가지 초기 가정하에 인증 프로토콜을 설계한다.

첫째 백 엔드 서버, 리더 및 태그에는 동일한 대칭키 K 와 리더에서 생성된 난수 R 을 숨기기 위한 비밀키 M_k 가 안전하게 초기화되고 보관되어 있다. 둘째 백 엔드 서버와 리더간에는 안전한 유선으로 통신이 이루어지고 있으며, 리더와 태그 사이는 불안전한 무선 구간이다. 셋째 태그는 AES 암호화 알고리즘을 통해 암호화가 가능하며 백 엔드 서버와 리더는 AES 를 통해 암·복호화가 가능하다고 가정한다. 마지막으로 리더와 태그는 난수를 생성할 수 있는 능력과 기능이 있다고 가정한다.

본 논문의 인증 프로토콜에 사용된 용어는 리더에서 생성된 난수를 비롯하여 서버, 리더 및 태그에서 동일하게 가지고 있는 대칭키, 난수를 숨기기 위한 비밀키 그리고 연산자 들이 존재한다. 리더난수의 경우 매 Query 마다 다른 난수를 생성한다. <표 1>은 인증 절차에 사용되는 용어를 나타낸 것이다.

<표 1> 용어 정리

표기법	설명
R	리더 난수
ID	태그의 ID
Tag Info	태그 정보
K	대칭키
M_K	비밀키
⊕	XOR 연산자
||	문자열 연접연산자



(그림 3) 제안 프로토콜

3.2. 상세 프로토콜

RFID 에 적용 가능한 AES 는 대칭키 방식의 암호화 알고리즘으로서 키 분배와 같은 문제점이 존재한다. 키 분배 문제는 공개키를 이용한 방식으로 해결할 수 있지만, 수동형 RFID 태그와 같은 제한된 환경에서는 공개키를 적용 하기가 어렵다. 따라서 본 절에서는 키 분배 문제를 해결하기 위하여 난수사용을 바탕으로 한 상세 프로토콜에 대해서 기술한다. 프로토콜의 절차는 총 4 가지로 설명될 수 있으며 각각의 단계는 다음과 같다.

① 단계

리더는 리더에서 생성된 난수 R 과 비밀키 M_K 를 XOR 연산하여 R_M 을 생성한 다음 Query 와 함께 태그에게 보낸다. 이때 R_M 을 생성하여 보내는 이유는 다음 단계의 암호화 과정에서 원문 메시지의 노출을 방지 하기 위함이다.

$$Reader : R_M = R \oplus M_K$$
$$Reader \rightarrow Tag : Query, R_M$$

② 단계

태그는 리더로부터 받은 R_M 에서 비밀키 M_K 를 이용해 난수 R 을 추출한 뒤 R 과 태그내 저장된 대칭키 K 를 이용하여 암호화에 사용할 새로운 대칭키 K_t 를 만든다. 이때 K_t 를 만드는 이유는 매 세션 암호화에 사용하는 대칭키를 바꿈으로써 대칭키 노출을 방지하고 도청이나 트래픽 분석과 같은 공격에 대비하기 위함이다. 더불어 리더로 전송되는 메시지 M1 은 위치 추적을 방지하기 위한 Nonce, 인증에 사용할 난수 R 그리고 ID 를 연접하여 대칭키 K_t 로 암호화 하여 보낸다.

$$Tag : K_t = K \oplus R$$
$$M1 = ID \,||\, Nonce \,||\, R$$
$$Tag \rightarrow Reader : E_{Kt}(M1)$$

③ 단계

리더는 태그로부터 받은 암호문 E_{Kt}(M1)에 난수 R 을 추가로 연접하여 새로운 메시지 M2 를 생성한다. 이후 M2 는 K_t 로 다시 한번 더 암호화 하여 백 엔드 서버에 R_M 과 함께 보낸다. 이때 암호화를 한번 더 하여 보내는 이유는 R_M 을 이용해 정당한 리더인지를 확인하기 위함이다.

$$Reader : M2 = E_{Kt}(M1) \,||\, R$$
$$Reader \rightarrow Back\text{-}End\ Server : E_{Kt}(M2), R_M$$

④ 단계

백 엔드 서버는 리더로부터 받은 암호문 E_{Kt}(M2)를 복호화 하여 메시지 M2 를 얻으며 R_M 역시 1 단계와 같은 방법으로 난수 R 을 추출하여 M2 에 연접 되어 있는 난수 R 과 비교한다. 이때 두 개의 난수값이 같을 경우 정당한 Reader 로부터 온 메시지라는 것을 백 엔드 서버가 알 수 있다. 또한 메시지 M2 로부터 연접된 암호문 E_{Kt}(M1)를 복호화하여 M1 에 연접된 난수 R 과 비교하여 같을 경우 정당한 태그로부터 오는 메시지인지 여부를 확인 알 수 있다.

따라서 두 가지 모두 정상적인 개체로 판단이 될 경우 백 엔드 서버는 태그 ID 정보를 대칭키 Kt 로 암호화 하여 리더로 보낸다. 만약 리더와 태그 중 하나라도 정당한 개체가 아니라면 백 엔드 서버는 즉시 통신을 중단한다. 마지막으로 리더는 태그 정보를 정상적으로 받은 후에 난수 R 을 새로운 값으로 갱신하고 통신을 끝낸다

$$Back\text{-}End\ Server \rightarrow Reader : E_{Kt}(Tag\ Info)$$

4. 제안한 프로토콜의 보안 분석

본 장에서는 기존 프로토콜과 제안 프로토콜을 비교 분석하고 RFID 시스템에 대해 공격자자 취할 수 있는 공격 유형을 토대로 제안한 인증 프로토콜의 보안과 안전성에 대해서 기술한다.

<표 2> 기존 프로토콜과 제안 프로토콜의 비교

	도청	재전송 공격	스푸핑	트래픽 분석	위치 추적	효율성	오버헤드
Kill 명령어	취약	취약	취약	취약	안전	낮음	낮음
Blocker 태그[5]	취약	취약	취약	취약	안전	보통	낮음
M. Feldhofer 의 프로토콜[3]	취약	취약	안전	안전	취약	높음	보통
Ohkubo 의 프로토콜[6]	안전	안전	안전	안전	안전	높음	높음
제안하는 프로토콜	안전	안전	안전	안전	안전	높음	보통

4.1. 제안한 프로토콜의 비교 분석

<표 2>는 본 논문에서 제안한 프로토콜과 기존의 연구된 프로토콜을 비교 분석한 자료이다.

'Kill'명령어나 Blocker 태그는 위치 추적을 피할 수 있지만, 다른 공격에 취약하다. M. Feldhofer 의 프로토콜에 경우 효율성은 향상시켰지만, 위치추적 및 도청 공격에 취약하다. Ohkubo 의 프로토콜에 경우 대부분의 공격에 안전하지만 오버헤드가 높아 실제로 태그에 적용하는데 무리가 있다. 하지만 제안하는 프로토콜의 경우 AES 를 사용해 대부분의 공격에 안전할 뿐만 아니라 오버헤드 역시 높지 않다.

4.2. 공격유형에 따른 안전성

(1) 도청, 트래픽 분석 및 재전송 공격(Replay Attack)
도청은 무선 통신에서 취약한 공격 방식으로 RFID 시스템에서 도청공격은 불가피하다. 트래픽 분석 역시 도청을 통해 얻은 트래픽을 분석하여 리더의 질의에 대한 태그의 응답을 예측할 수 있다. 재전송 공격은 공격자가 도청을 통하여 태그에서 전송되는 고유 정보를 얻어 리더의 요청에 정상 태그를 대신하여 응답하는 공격이다. ②단계에서 메세지 M1 은 Nonce 와 난수 R 이 암호화 되어 전송되므로 항상 다른 값을 가지게 되며 이것은 도청, 트래픽 분석, 재전송 공격을 무력하게 만든다.

(2) 스푸핑(Spoofing)
정당하지 않은 리더나 태그가 정당한 것처럼 속여 인증을 통과하는 공격법이다. 상호인증을 하지 않는 프로토콜의 경우 스푸핑 공격에 취약할 수 있다. ①단계에서 리더에서 발생한 난수를 태그와 서버로 전달하는 과정에서 대칭키로 암호화된 R 과 R_M 의 비교를 통해 상호인증 과정을 거치므로 스푸핑 공격에 안전하다.

(3) 위치 추적(Location Tracking)
공격자가 태그의 위치변화를 감지함으로써 태그의 소유자가 움직이는 위치를 추적해 프라이버시를 침해하는 것을 말한다. ②단계에서 메세지 M1 에 포함되는 Nonce 로 인해 M1 의 값이 항상 바뀌기 때문에 정상적인 리더가 아니라면 위치 추적을 할 수 없다

5. 결론

수동형 RFID 는 제한된 자원을 가지며, 무선채널을 사용하는 기술이지만 도청과 같은 악의적인 공격과 프라이버시 침해와 같은 문제점이 있다. 이를 해결하기 위하여 RFID 에 적용 가능한 대표적인 대칭키 암호화 알고리즘인 AES 는 키 분배와 같은 문제점을 해결하여야 한다.

본 논문에서는 AES 와 난수사용을 기반으로 하는 개선된 RFID 인증 프로토콜을 제안하였다. 리더에서 발생된 난수는 대칭키의 노출을 막아 키 분배 문제를 해결하며, 인증 단계를 줄이면서 상호인증의 효과를 가진다. 또한, 태그에서 한번의 암호화만 수행되므로 태그에 발생하는 오버헤드를 최소화할 수 있다. 제안한 인증 프로토콜의 분석을 통해 여러 공격유형에 따른 안전성도 확인하였다.

참고문헌

[1] M. Ohkubo, K. Suzuki and S. Kinoshita. "Efficient Hash-Chain Based RFID Privacy Protection Scheme," Ubcomp2004 workshop, 2004.

[2] Kang-Joong Seo, Jun-Cheol Jeon, Sang-Ho Shin, and Kee-Young Yoo, "CA based RFID Authentication Protocol for Privacy and An45020onymity," ICWMC 2008, IEEE Computer Society, pp.278-281, 2008.

[3] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," CHES'04, LNCS 3156, pp. 357-370, Springer-Verlag, 2004.

[4] Manfred Aigner and Martin Feldhofer, "Secure Symmetric Authentication for RFID Tags," Telecommunication and Mobile computing - TCMC 2005, March 2005.

[5] A. Juels and Rivest and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," Proceeding of the Conference on Computer and Communications Security – ACM CCS 2003, ACM, pp.103-111, October 2003.

[6] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, "Cryptographoc Approach to "Privacy-Friendly"Tags, " In RFID Privacy Workshop, MIT, November 2003.

[7] Toiruul, B., Lee, K. "An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems, "IJCSNS, Sepember 2006.