새로운 키 생성 방법을 통한 RFID시스템의 전방위보안성 보호 프로토콜*

조정환° 조정식 여상수 김성권
중앙대학교 컴퓨터 공학부
{jhcho°, mfg, ssyeo}@alg.cse.cau.ac.kr, skkim@cau.ac.kr

Forward Security Protection Protocol of RFID System using New Key Generation Method

Jung-Hwan Cho° Jung-Sik Cho Sang-Soo Yeo Sung kwon Kim
School of Computer Science and Engineering, Chung-Ang University

요 약

현대의 산업화 사회에서는 자동인식을 통해서 사람과 사물을 식별하고자 하는 연구들이 진행되고 있다. 그 대표적인 예로 바코드를 이용한 접촉식 판별기술이 있고, 라디오 주파수를 이용한 RFID(Radio Frequency Identification) 기술을 들 수 있다. RFID의 경우는 무선 주파수를 이용하기 때문에 대량의 사물을 동시에 인식 할 수 있다는 장점이 있다. 하지만, 어떠한 상황에서 리더의 요청에 응답을 하는 리더-태그 시스템이기 때문에 사용자의 프라이버시 침해 문제를 야기 할 수 있다. 사용자의 프라이버시 침해문제를 막기 위해서 많은 연구들이 진행되고 있다. 그 중에서, Miyako Ohkubo의 Hash체인을 이용한 프라이버시 보호 기법은 정보유출, 위치추적공격(Location Tracking Attack), 전방위보안성(Forward Security)과 같은 프라이버시 침해문제들로부터 사용자의 프라이버시를 보호 할 수 있는 프로토콜이다. 그러나, Hash함수를 태그에 구현하는 것은 현재까지는 불가능한 상황이다. 또, Martin Feldhofer의 AES(Advanced Encryption Standard)를 사용한 프로토콜은 실제로 태그에 구현 가능하면서 내부구조가 8bit인 AES를 사용함으로써 암호학적인 강도를 높였으나, 프라이버시 침해 문제에서 단점을 드러냈다. 이러한 단점을 보완한 AES기반에서의 개선된 RFID 프라이버시 보호 프로토콜은 실제적으로 태그에 구현 가능한 AES를 이용한 암호화 체인을 통해서 프라이버시 보호에 우수하면서 실제 사용이 가능한 프로토콜을 제안하였다[1]. 그러나, 이 프로토콜은 생성되는 키 값들이 물리적 공격을 통해서 노출이 되었을 때, 이전의 seed값과 키 값들이 노출 되는 단점이 있다. 본 논문에서는 이러한 문제들을 해결하고자 프라이버시 보호에 새로운 키 생성 방법을 통한 강력한 프로토콜을 제안 한다.

1. 서 론

현대 산업사회는 자동화 시스템을 통해서 사람이나 사물을 식별하는 자동인식에 대해서 많은 부분을 필요로 하고 있다. 자동인식은 크게 두 가지 부분으로 나눌 수가 있다. 그 중에 첫 번째는 유전적, 생물학적 정보를 이용해서 사람의 고유정보를 알아내는 얼굴인식, 지문인식, 홍채인식, 음성인식이 대표적이라고 할 수 있고, 두 번째는 광학문자나 OMR을 이용해서 대량의 물품들을 개별적으로 구분하는 바코드 시스템과 라디오 주파수를 이용하는 RFID 시스템(Radio Frequency Identification System)이 대표적이라고 할 수 있다[2,3].

바코드 시스템의 경우는 접촉식으로 바코드 리더기를 통해서 사물에 부착된 바코드 정보를 읽어서 사물을 판별 하는 기술이고, RFID 시스템은 비 접촉식으로 라디오 주파수(Radio Frequency)를 이용하는 기술이다. 전자의 경우는 대량의 사물을 판별할 때 각각의 바코드를 하나씩 하나씩 리더기에 읽혀서 정보를 파악해야 한다. 하지만, 후자의 경우는 라디오 주파수를 이용한 비 접촉식이기 때문에 동시에 다수의 사물을 인식할 수 있다는 장점이 있다. 이러한 장점 때문에 자동인식에서의 시간과 비용을 줄여서 이득을 얻어야 하는 산업 부분에서 RFID 시스템이 사용되게 된다.

대량의 사물을 동시에 인식할 수 있다는 장점이 있긴 하지만, 어떤 리더의 요청에도 자신의 ID를 응답하는 리더-태그 시스템은 원하지 않는 상황에서도 리더의 요청에 의해 태그정보를 리더에게 넘기기 때문에 정보 유출 및 프라이버시 침해 문제를 야기 할 수 있다. 이러한 문제들을 해결하기 위해서는 보안기술이 필수적인 요소이다. 현재 여러 논문들을 통해서 RFID 프라이버시 보호 프로토콜들이 연구되고 발표되고 있다[1,3,4.5,6]

본 논문에서는 기존의 제시되었던 RFID 프라이버시 보호 프로토콜들에 대한 동작과정과 문제가 되었던 점들을 살펴보고, 문제가 되는 점들을 개선하여 향상된 프라이버시 보호기술과 전방위보안성(Forward Security)을 보장하는 새로운 프로토콜을 제시하고자 한다.

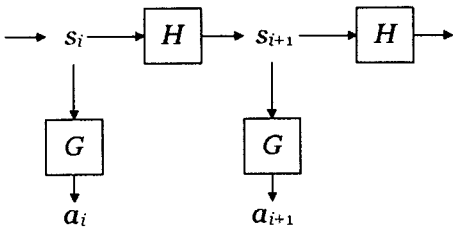
2. 관련연구

*본 연구는 한국과학재단 특정기초연구(R01-2005-000-10568-0) 지원으로 수행되었음

기존의 여러 논문들 가운데서 사용자의 프라이버시를 보호하기 위해 적합하고 실제 구현 가능한 프로토콜들을 소개하고, 그 프로토콜들의 문제점들을 소개한다.

2.1 Hash기반 프로토콜[4]과 AES기반 프로토콜[5,6]

Miyako Ohkubo는 Hash함수를 이용한 프라이버시 보호 프로토콜을 제시하였다[4]. Miyako Ohkubo의 이론이 가지는 장점은 기존에 제안된 여러 프로토콜들이 해결하지 못했던 전방위보안성을 보장 할 수 있다는 것이다. 이 프로토콜은 Hash체인을 이용해서 새로운 정보들을 태그에 저장하고, 리더에게 보내는 출력 값을 일정하지 않게 보내서 불구분성을 보장하게 했다. [그림 1]은 Miyako Ohkubo의 Hash체인을 이용한 태그 연산이다.



[그림 1] Miyako Ohkubo의 태그 연산

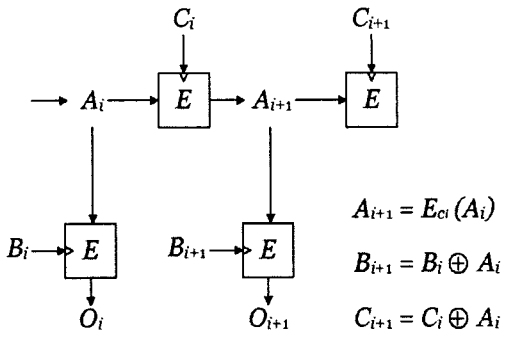
H와 G라는 Hash 함수를 통해서 $a_i=G(s_i)$라는 출력 값을 리더에게 보내게 된다. Hash함수의 특성상 역으로의 계산이 어렵기 때문에 이 프로토콜은 전방위보안성을 보장하기에 적합한 프로토콜이다.

Martin Feldhofer는 내부구조를 8bit로 하여 연산을 수행할 수 있는 저 전력, 소형의 AES(Advanced Encryption Standard)를 구현하였다[5,6]. NIST에서 공모하고 Rijndael이 제안한 AES 프로토콜의 구조적 변경성을 이용해서, 내부 연산이 128bit로 진행될 경우에 약 25000-30000 gate의 회로를 사용했던 것을 대략 3500 gate로 줄임으로써 하드웨어적 기반이 약한 태그에 실제적으로 사용 할 수 있도록 하였다. AES암호화를 통해서 Challenge-Response 인증 방식을 사용함으로 정보유출, 비 권한자 접근공격, 태그 위조와 같은 프라이버시 침해 문제들로부터 사용자의 프라이버시를 보호 받을 수 있도록 하였다.

2.2 AES기반의 개선된 RFID프라이버시 보호 프로토콜[1]

이전에 제시했던 Miyako Ohkubo의 프로토콜은 전방위보안성 및 위치추적공격을 확실히 보장하지만, 현실적으로는 20000-25000 gate 회로 이상의 하드웨어 기반이 필요하기 때문에 실제로 구현은 불가능한 상태이다. 또, Martin Feldhofer의 프로토콜은 정보유출, 비 권한자 접근공격, 태그 위조에 보안은 우수하지만 위치추적공격과 물리적 공격에는 많은 단점을 가지고 있다.

이 두 프로토콜의 문제점을 보완하기 위해서 AES암호화 체인을 이용한 보안 프로토콜을 제시하였다[1]. [그림2]는 개선되어진 RFID프라이버시 보호 프로토콜의 태그 연산이다.



[그림 2] AES기반의 개선된 RFID 프라이버시 보호 프로토콜에서의 태그 연산

E는 AES 암호화 알고리즘이다. A_1은 초기 Seed값이고 B_1, C_1은 암호화를 하기 위한 키 값이다. 그리고 다음번의 키 값은 $B_{i+1}=B_i\oplus A_i$, $C_{i+1}=C_i\oplus A_i$로 키를 갱신한다. 먼저 DB는 A_1, B_1, C_1의 초기 값을 저장하고, (ID, A_1)의 값을 따로 저장을 한다. 그리고, 리더가 태그의 $O_i=E_{b_i}(A_i)$ 값을 읽었을 때, DB에서 미리 계산해둔 O_i의 값과 O_i이 일치하는 값을 찾아 그 값과 함께 있는 ID를 리더에게 돌려주게 된다. 이 프로토콜은 각 리더의 요청 시에 내보내는 O_i값이 다르기 때문에, 위치추적공격으로부터 보호 받을 수 있고, 물리적 공격을 당했다고 하여도 트랜잭션이 변화 하면서 이전의 키 값을 추적 할 수가 없기 때문에 전방위보안성에도 우수함을 나타낸다. 또한, Martin Feldhofer의 내부구조가 8bit인 AES를 사용을 함으로써 저전력 소형의 태그를 실제적으로 구현하도록 하였다.

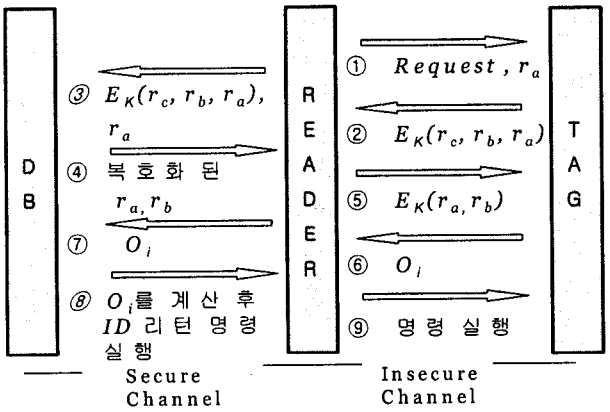
2.3 기존 연구의 문제점

이전에 보았던 AES를 사용하는 개선된 RFID프로토콜은 Miyako Ohkubo의 실제 구현이 어렵다는 단점과 Martin Feldhofer의 프라이버시 보호의 약점을 극복해서 실제로 구현가능하면서 프라이버시보호에 우수한 프로토콜을 제안하였다. 그러나, 이 프로토콜은 전방위보안성이 깨질 수 있다는 단점을 가지고 있다.

위의 [그림 2]에 $i+1$번째 트랜잭션에서 $B_{i+1}=B_i\oplus A_i$, $C_{i+1}=C_i\oplus A_i$, $O_{i+1}=E_{b_{i+1}}(A_{i+1})$, $A_{i+1}=E_{c_i}(A_i)$ 이 값들이 물리적 공격을 당하게 노출이 되었을 때 문제가 발생한다. $B_{i+1}\oplus C_{i+1} = B_i\oplus C_i = B_{i-1}\oplus C_{i-1} = \cdots = B_1\oplus C_1$ 식으로부터 $B_1\oplus C_1$ 이 노출이 되게 된다. 이 값을 가지고 위의 식들에 대입해 가면서 Brute force attack을 하게 되면 결국 A_1의 값을 찾아 낼 수가 있게 된다. 결국 전방위보안성은 깨지게 된다.

3. 제안 프로토콜

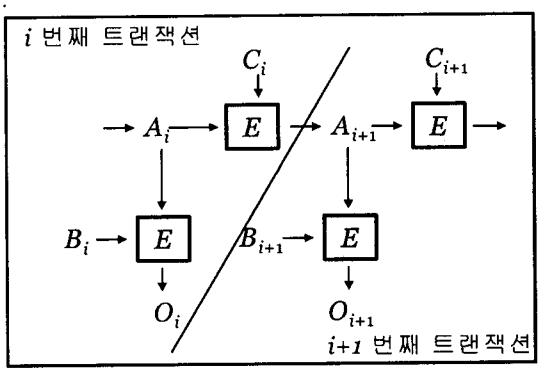
이전에 제안한 논문은 키 생성에 있어서 $B_{i+1}=B_i \oplus A_i$, $C_{i+1}=C_i \oplus A_i$로 키 생성을 하였는데, XOR 연산의 특성상 이 두 값을 가지고 이전의 키 값을 찾아 낼 수 있기 때문에 전방위보안성에 취약점을 드러냈다. [그림 3]은 본 논문이 제안하는 프로토콜이다.



[그림 3] 제안 프로토콜

위 [그림 3]에서 1-5번사이는 Challenge-Response방식을 사용을 해서 태그와 리더를 서로 인증을 하는 과정이다. 이 과정에서 태그는 r_b r_c를 리더는 r_a라는 난수를 생성을 하게 되는데, 생성된 난수를 가지고 다음번 트랜잭션의 키 값을 만들어 내게 된다.

$C_{i+1}=C_i \oplus r_c$ 와 $B_{i+1}=B_i \oplus r_b$로 키를 갱신한다. 키를 갱신한 후에 그 트랜잭션에서 r_b r_c를 삭제한다. 다음번 트랜잭션에서 물리적 공격으로 값들이 노출이 되어도 이전의 난수를 알 수가 없기 때문에 전방위보안성을 보장 할 수 있게 된다. [그림 4]는 제안 프로토콜에서의 태그 연산이다.



[그림 4] 제안하는 프로토콜의 태그 연산

DB는 A_1, B_1, C_1 의 초기 값을 저장하고 (ID, A_1)의 값을 따로 저장한 후에, 인증과정에서 얻어진 난수를 가지고 $O_i=E_{b_i}(A_i)$의 값을 계산하여 $O_i=O_i$이면 ID를 리턴하고, 다음 명령을 수행하도록 명령 메세지를 보낸다. 다음 트랜잭션의 키를 생성하는 과정에서 인증이 이루어 지지 않을 경우에는 키를 갱신하지 않음으로써 불법 리더에 의한 태그와 DB간의 비동기화 현상을 방지 할 수 있다.

4. 결론 및 향후 연구 과제

Miyako Ohkubo와 Martin Feldhofer가 제안 했던 프로토콜의 단점을 보완했던 AES기반의 개선된 RFID프라이버시 보호 프로토콜은 실제적으로 구현 가능한 AES를 사용하면서 전방위보안성과 위치추적공격, 정보유출과 태그 위조등의 프라이버시 보호 측면에서 우수함을 가졌었다. 하지만, 물리적인 공격을 통해서 내부의 정보들이 노출 되었을 때, 그 값들의 연산을 통해서 이전의 정보들이 유출이 되고 초기의 seed값 까지 알아낼 수 있게 되는 단점이 있었다.

본 논문에서는 그러한 단점들을 보완을 해서 새로운 키 생성방법을 통한 새로운 프로토콜을 제안 하였다. 본 논문에서 제안한 프로토콜은 AES기반의 Challenge-Response방식을 사용하고 있다. 이는 태그와 리더간에 상호 인증을 해서 정보유출, 비 권한자 접근공격과 도청공격을 막고, 또, AES암호화 체인을 통해서 출력 값을 다르게 하여 위치추적공격을 막을 수 있도록 하였다. 그리고, 난수를 사용한 새로운 키 생성방법을 통해 물리적 공격으로부터 발생할 수 있는 전방위보안성을 보장 하도록 하였다.

제안하는 기법은 태그에서 수행되는 연산의 양이 많아지고, DB에서 행해지는 연산의 양이 많으므로 이에 대한 향후 개선이 필요 할 것으로 보인다.

5. 참고문헌

[1] 조정환, 여상수, 김성권, "AES를 기반으로 하는 개선된 RFID 프라이버시 보호 프로토콜", 한국 정보과학회 한국컴퓨터종합학술대회 2005논문집 Vol.32 NO.1(A), pp. 100-102, 2005년 7월.

[2] Heiko Knospe and Hartmut Pobl, "RFID Security" Information Security Technical Report, pp. 39-50, November-December 2004.

[3] 강전일, 박주성, 양대현, "RFID 시스템에서의 프라이버시 보호 기술", 정보보호학회지, 제14권 제6호, 2004년 12월.

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

[5] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm", In Conference of cryptographic Hardware and Embedded systems, pp. 357-370, Springer, 2004.

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