AES를 기반으로 하는 개선된 RFID 프라이버시 보호 프로토콜*

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

Enhanced Protocol for RFID Privacy Protection Based on AES

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

요 약

유비쿼터스는 현재의 제한된 컴퓨팅 환경을 떠나서 시간과 장소에 구애받지 않는 자유로운 컴퓨팅 환경을 제공함으로서 각광받고 있다. 그 중 언제어디서나 정보를 주고받을 수 있으며 가격과 성능 면에서 단연 뛰어난 RFID(Radio Frequency Identification)의 중요성은 점점 증가되고 있는 추세이다. 그러나, 이와 같은 우수성에도 불구하고, 정보 유출의 위험성을 내포하고 있으며, 개인의 위치 추적이나, 비 접근 권한자의 위장행세 등의 사용자 프라이버시 보호에 대한 많은 문제점들을 수반한다. 현재까지 이와 관련된 연구들이 활발히 진행되고 있다. 특히 그 중, Ohkubo의 해시함수를 이용한 프로토콜은 프라이버시 보호 측면에서 위치추적 공격(location tracking), 전방위보안성(forward security)과 같은 문제들에 대한 해결책을 제시하고 있으나, 해시함수를 태그에 직접 구현하는 것은 현재까지는 불가능한 상태이다. 또한, Martin Feldhofer는 대칭키 암호 알고리즘인 AES(Advanced Encryption Standard)를 태그에 구현을 함으로서 암호학적인 강도를 높였으나. 위치추적 공격에 대한 문제점과 물리적 공격에 대한 가정을 하지 않은 단점을 가지고 있다. 본 논문에서는 기존연구에서의 문제점들을 보완하고자 현실적으로 구현 가능한 AES를 사용하고, 위치추적 공격, 비권한자 접근(unauthorized access) 공격과 물리적 공격으로부터 안전하며 전방위보안성을 제공하는 기법을 제안한다.

1. 서 론

앞으로 다가올 미래는 시간과 장소에 구애 받지 않고 자유롭게 컴퓨터 네트워크를 이용할 수 있는 유비쿼터스 세상으로 발전해 나갈 것이다. 유비쿼터스라는 말은 라틴어로 '언제 어디서나' 있다는 말로 제한된 사이버상의 네트워크 통신이 아니라 현실 세계에서의 인간을 위한 컴퓨터 환경을 이야기 한다. RFID(Radio Frequency Identification)시스템은 앞으로 유비쿼터스를 이끌어갈 중요한 기술중의 하나이다. RFID는 라디오 주파수를 통해서 자신의 고유한 ID를 가진 태그(Tag)와 고유한 ID를 읽어들이기 위한 리더(Reader), 그리고 읽어들인 ID를 인증하고 검색하는 데이터베이스(DB)로 구성이 된다. 태그는 일반적으로 자체 전력을 가지고 있는 능동형(Active) 태그와 자체 전력을 가지고 있지 않은 수동형(Passive) 태그로 구성이 된다.

우리가 제안하는 프로토콜에서는 수동형 태그를 가정한다. 현재의 수동형 태그는 리더의 전파를 통해서 전력과 데이터를 공급받게 되고, 데이터와 전력을 공급받으면 리더에게 자신의 고유 ID를 무조건 보내게 된다. 어떤 리더의 질의에 대해서도 태그는 항상 대답을 하기 때문에 프라이버시에 관한 문제점이 발생하게 된다.

또한, 전파를 통한 통신이기 때문에 언제 어디서든지 정보가 읽혀질 가능성이 있다. 프라이버시 보호[1,2]에 대한 관심이 높아지면서 여러 가지 기법들이 연구되고 있다.

이 논문에서는 기존에 있는 프라이버시 보호 알고리즘을 확장하여 Advanced Encryption Standard(AES)를 기반으로 한 개선된 프라이버시 프로토콜을 제안한다. AES만을 이용하여 태그를 구성하였을 때 보장 되지 못했던, 위치추적공격(location tracking)과 물리적 공격에 대한 문제점[3]을 보완하고, 현실적으로 태그에 구현할 수 있는 프로토콜을 제시한다.

2. 관련연구

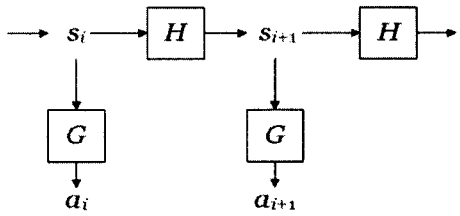
여러 논문들을 통해서 사용자의 프라이버시 보호에 대한 연구들이 진행되어 왔다. 그 중에서 프라이버시 보호에 적합한 연구들을 소개한다.

2.1 Ohkubo의 RFID 프라이버시 보호 프로토콜

Ohkubo의 이론[4]은 해시 체인을 이용하여 기존의 이론들이 가지지 못했던 전방위보안성(forward security)을 보장한다.

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

해시 체인을 이용하여 새로운 정보를 태그에 새롭게 쓰게 되므로, 밖으로 나오는 결과 값이 일정하지 않게 된다. 따라서 불구분성(Indistinguishability)을 보장하게 된다. [그림 1]은 Ohkubo가 제안한 태그 연산이다.



[그림 1] Ohkubo가 제안한 태그의 연산

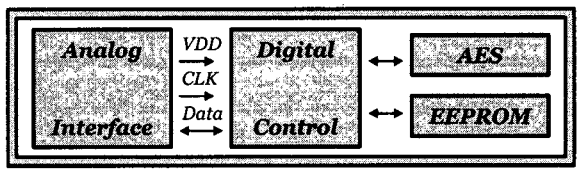
$a_i = G(s_i)$는 리더에게 보내는 태그의 응답
$a_{i+1} = G(s_{i+1})$ 다음번에 리더에게 보내는 응답

H와 G는 해시 함수이다. 리더는 태그로부터 받은 a_i값을 백엔드 서버(Back-End Server)에 보낸다. 백엔드 서버는 (ID, S_1)의 쌍의 값을 리스트로 가지고 있는다. 그리고, $a'_i = G(H^i(s_1))$의 값을 계산해 놓는다. $a'_i = a_i$인지 체크를 하고 두 값이 동일하다면 a'_i의 쌍인 ID를 리턴하게 된다.

위에서 제시된 Ohkubo의 프로토콜에서 쓰인 G와 H 함수는 일방향성 해시함수 이기 때문에 불구분성을 보장하고, 전방위보안성을 보장한다. 공격자가 물리적 공격에 의해서 s_{i+1} 값을 알았다고 하더라고, 해시함수의 특성상 역으로의 계산(s_i를 알아내는 것)은 어렵기 때문이다. 또한 이 프로토콜은 태그에 해시 함수가 구현가능하다는 가정을 하고 있다. 물론, 공개키 암호 알고리즘에 비해서는 해시 함수가 태그 내부에 구현될 가능성이 높지만, 현재로서는 AES만이 구현된 상태이다[5,6].

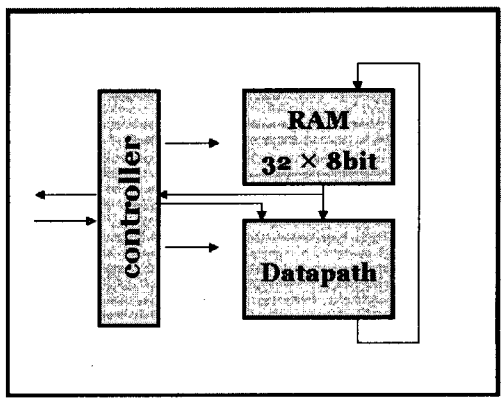
2.2 Martin Feldhofer의 AES를 이용한 RFID 태그

Feldhofer는 AES를 이용하여 저전력, 작은 크기의 RFID 태그를 제안 한다[5,6]. AES는 1987년에 NIST에서 공모한 기존 DES를 대신할 새로운 암호 알고리즘으로 채택된 V.Rindael이 제안한 암호화 알고리즘이다. 초기에는 키 값과 메시지블록 사이즈를 128bit로하고 AES내부를 8비트씩 암호화 하도록 설계 하였다가 이후에 키와 블록사이즈를 128, 192, 256비트에서 쓸 수 있도록 확대 수정 하였다. AES는 블록의 크기에 따라서 10-14라운드를 거쳐서 암호화 된다. 각 라운드 마다 4단계를 거치게 되는데, 첫 번째로 BS(Byte Sub)단계, 두 번째 SR(Shift Row)단계, 세 번째 MC(Mix Column)단계, 마지막 단계인 ARK(Add Round Key)단계로 구성되어 있다. 각 단계에 대해서 간략하게 살펴보면 BS단계에서는 각 블록의 바이트를 마치 DES(Data Encryption Standard)의 S-Box처럼 치환하는 기능을 한다. SR단계에서는 각 열의 변환을 수행을 하고, MC단계에서는 각행의 변환에 대한 연산을 수행한다. ARK 단계에세는 이미 만들어 놓은 보조키 수열과 각 라운드에서 생성된 라운드 보조키를 XOR 연산을 수행한다. AES의 복호화는 모든 연산의 역순으로 진행이 된다. 행렬곱연산은 역행렬곱연산으로 치환은 역 치환으로 연산을 수행한다.



[그림 2] Feldhofer 의 RFID 태그 구조

Feldhofer가 제안한 RFID 태그는 [그림 2]와 같다. 태그는 4 부분으로 나뉘는데, 첫 번째는 Analog Interface 이다. Analog Interface는 전원공급과, 데이터 모듈화, 주파수로부터 온 클럭 회복등을 담당한다. 두 번째 DIgital Control은 리더와의 통신을 담당하고, 충돌방지 알고리즘을 수행하고, 모든 명령을 수행한다. EEPROM은 메모리로서 Unique ID와 암호화 키를 저장한다. AES는 암호화 연산을 하는 부분이다. 위에서 보았던 AES알고리즘의 각 라운드 내부연산은 일반적으로 32bit로 진행이 되는데, 32bit연산을 태그에 적용하기에는 많은 제약이 따른다. 하드웨어적인 구현에 있어서 어려움이 있다. 그래서 Feldhofer는 AES의 원래 구조적 변경성을 이용해서 내부적으로 8bit로 계산하는 AES알고리즘을 태그에 구현한다. 이 AES 알고리즘은 S-Box의 개수를 감소 시킴으로 자원을 절약하는 장점이 있고, 32bit보다 저전력을 사용하고, 다른 버스 사이즈를 쓰기 때문에 하드웨어 구현이 용이하다.



[그림 3] Feldhofer의 AES 구조

이 AES의 구성요소는 총 3부분으로 나뉘는데, 첫 번째 Controller 부분은 AES의 연산에서 ShiftRow 연산을 수행한다. 두 번째 부분은 RAM부분으로 치환순열의 저장등의 임무를 맡는다. 세 번째 부분은 Datapath부분으로 Byte sub 연산과 Mixcolumns 연산, 그리고 Addroundkey 연산을 수행한다[그림 3].

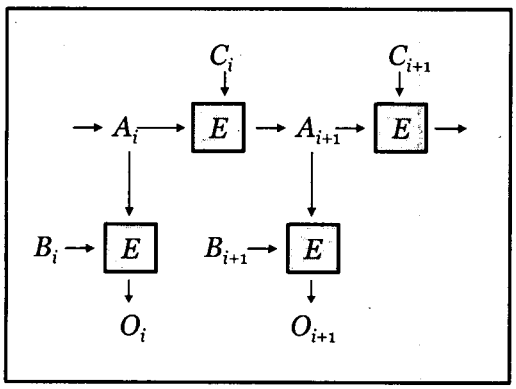
Feldhofer는 AES를 내장한 태그를 이용하는 인증프로토

콜을 제안하였다[5,6]. 이 프로토콜은 인증에 있어서는 AES의 안전성으로 인해 보안이 보장되지만, 위치추적 공격의 문제가 존재한다. 또한, 물리적인 공격에 대한 고려는 배제하고 있기 때문에 안전하다고 할 수 없다.

3. 제안하는 프로토콜

이전에 살펴 본 Ohukbo의 논문은 프라이버시 보호 측면에 있어서 매우 뛰어나다. 위치추적 공격뿐 아니라 불구분성을 통해서 전방위 보안성까지 보안을 할 수 있다. 그러나 Ohkubo가 제안한 해시함수 기반 프로토콜은 아직까지는 구현이 어려운 상황이다.

우리가 제안하는 알고리즘은 Ohkubo의 프로토콜을 보완해서 태그에 구현이 어려운 해시함수 대신에 태그에 현실적으로 구현 가능한 Feldhofer AES 암호화 알고리즘을 사용하는 것이다. [그림 4]는 우리의 제안 프로토콜이다.



[그림 4] 제안하는 프로토콜의 태그 연산

$O_i=E_{b_i}(A_i)$: 리더에게 보내는 태그의 응답
B_i: O_i출력을 위한 암호화 키 값
C_i: A_{i+1}를 구하기 위한 암호화 키 값
$B_{i+1}=B_i \oplus A_i$
$C_{i+1}=C_i \oplus A_i$
$A_{i+1}=E_{c_i}(A_i)$

E는 AES 암호화 알고리즘이다. Database는 A_1, B_1, C_1의 초기 값을 알고 있고, $O_i=E_{b_i}(A_i)$ 값을 계산해서 (ID, A_1)의 값을 리스트로 가지고 있는다. 그리고 $O_i=O_i$값이 같은지 체크를 해서 두 개의 값이 일치하면 O_i 의 쌍인 ID를 리턴하게 된다. 이 과정에서 만약에 공격자에 의해서 C_{i+1}, A_{i+1}, B_{i+1}, O_{i+1}의 값과 O_i의 값이 공격자에게 해킹을 당하게 되어도 C_i의 값을 모르기 때문에 A_i의 값을 찾아 낼 수가 없고 나머지 값들도 계산해 낼 수 없다 . 이 알고리즘을 사용하면 각 리더의 요청시에 내놓는 결과 값(O_i)의 값이 다르기 때문에 위치추적 공격으로부터 보호 받을 수 있고, 물리적 공격을 당했다고 하여도 이전의 값을 알아 낼 수가 없기 때문에 전방위보안성이 보장 된다.

또한, AES 암호화 알고리즘을 사용함으로써(100KHz에서 8.15㎂의 전력사용, 3,595개의 게이트를 사용), 저전력의 소형의 태그를 구현할 수 있게 됨으로 저가의 태그 생산이 가능해 지게 된다.

4. 결론 및 향후 연구 과제

Ohkubo의 프로토콜은 프라이버시를 침해하는 공격들에 대해서 방지하고, 전방위 보안성까지 보장하는 기법으로 가장 진보된 이론이라고 할 수 있다. 하지만, 해시함수를 태그안에 구현하는 것은 현재까지 불가능하다. 또한, Feldhofer의 기법은 암호학적으로 뛰어난 AES를 태그에 구현함으로써 태그의 암호학적인 강도를 매우 높였으나, 위치추적 공격, 그리고 도청등의 공격에는 매우 취약함을 드러냈다.

본 논문은 이런 문제점들을 보완하고자, AES기반의 프라이버시 보호 알고리즘을 제시 하였다. 우리가 제안한 프로토콜은 기존의 프라이버시 침해 공격들로부터 사용자의프라이버시를 보호하고, 강력한 암호알고리즘인 AES를 태그안에 직접 구현함으로써 암호학적인 안전성을 높임과 동시에 전방위보안성도 보장하도록 하였다.

제안하는 기법은 Ohkubo의 프로토콜과 마찬가지로 서버에서의 계산량이 매우 많으므로 이에 대한 개선이 필요할 것으로 보인다.

5. 참고문헌

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

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

[3] Dirk Henrici and Paul Müller, "Hash-Based Enhancement of Location Privacy For Radio-Frequency Identification Devices Using Varying Identifiers", Workshop on Pervasive Computing and Communications Security - Persec 2004, pp. 149-153, March 2004.

[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.