고가 물품에 적합한 강력한 RFID 프라이버시 보호 기법*

조정환° 여상수 김성권
중앙대학교 컴퓨터공학부, 단국대학교 정보컴퓨터학부, 중앙대학교 컴퓨터공학부
jhcho°@alg.cse.cau.ac.kr, ssyeo@dankook.ac.kr skkim@cau.ac.kr

Strong RFID Privacy Protection Scheme for High-price Products

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

요 약

RFID(Radio Frequency Identification)는 라디오 우선 주파수를 가지고 대량의 사물을 동식에 인식을 할 수 있는 장점이 있지만, 무선 주파수를 사용하기 때문에 정보유출의 문제와 위치 추적과 같은 프라이버시 침해 문제를 야기 할 수 있다. 프라이버시 침해 문제에 대한 관심이 높아지면서 Ohkubo는 해시 체인을 이용한 프라이버시 보호 기법을 제시 했고, Feldhofer는 AES를 이용한 프라이버시 보호 기법을 제시 하였다. 그러나, Ohkubo논문의 경우 프라이버시 보호에 있어서는 우수하지만, 데이터베이스에서의 연산량이 많다는 단점을 가지고 있고, Feldhofer의 경우에는 전방위보안성과 같은 물리적 공격에 취약하다는 단점을 가지고 있다. 본 논문에서는 해시체인과 공개키를 이용해서 고가 물품에 부착하기에 적합한 고기능의 태그 하드웨어를 제안하고, 이를 이용하는 프라이버시 보호 기법을 제시한다.

1. 서 론

RFID(Radio Frequency Identification)란 무선 주파수를 가지고 대량의 사물을 동시에 인식 할 수 있는 자동인식 기술 중의 하나이다. 최근에 RFID에 대한 사용량이 많아지면서 RFID의 중요성이 증가하고 있는 추세이다. RFID는 무선주파수를 사용해서 대량의 사물을 동시에 인식을 할 수 있는 장점이 있지만, 무선주파수를 사용하기 때문에 도청을 통한 정보유출의 문제와 위치 추적과 같은 프라이버시 침해 문제를 야기 할 수 있다. 프라이버시 침해문제를 해결하기 위해서 많은 연구 들이 진행되고 있다[1,2]. 그 중에서 공개키 암호화를 이용하는 방법은 현재까지 알려진 기법들 중에서 가장 강력한 보호 기법이라고 할 수 있다. 그러나, 저가의 태그에는 공개키를 사용 할 수 없다. 저가 태그의 하드웨어는 저장 공간이나 연산능력의 제한이 있기 때문이다.

RFID의 기능을 사용하는 물품 중에 높은 수준의 프라이버시 보호 기법이 필요한 고가의 물품들이 있는데, 저가의 태그를 사용하면 프라이버시 보호에 문제가 있게 된다. 따라서, 고가 물품에 들어가는 고기능 태그를 따로 만들어서 높은 수준의 암호서비스를 제공하는 것이 필요하다. 본 논문은 고가 물품에 들어가는 고기능 태그를 가정한다.

2. 관련 연구

Martin Feldhofer는 내부구조가 8bit로 진행되는 저 전력 소형의 AES(Advanced Encryption Standard)기법을 제시 하였다[3,4]. 이 기법은 기존의 128bit AES를 개선해서 저가의 태그에 적합한 태그를 제시하였다.

기존의 AES의 S-Box의 개수를 감소 시켜서 각 라운드마다 진행되는 bit수를 줄여서 기존 32bit 연산으로 진행되던 것을 8bit만으로 가능하도록 만들었다. 그래서, 기존의 AES보다 저 전력, 소형의 태그를 구현 할 수 있도록 하였다. 그러나, 물리적 공격을 통해서 태그내의 값들과 AES의 *key*값을 알아 낼 수 있기 때문에, 여러 가지 프라이버시 침해 문제가 발생하게 된다.

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

Miyako Ohkubo는 해시체인을 이용한 프라이버시 보호 프로토콜을 제시하였다[5]. 이 프로토콜은 해시함수를 사용해서 내부의 값을 변화시키기 때문에 전방위보안성에 우수함을 가지고 있다. 또한, 태그내부의 정보를 변화시키면서 출력 값을 다르게 하는 불구분성을 가지고 있어서 위치추적과 같은 프라이버시 침해문제에 있어서 장점을 가지고 있다. 그러나, 이 프로토콜은 데이터베이스에서의 연산량이 많다는 단점이 있다.

3. 제안 프로토콜

위 2장에서 언급했던 RFID 보호 프로토콜들은 다양한 문제들을 가지고 있었다. Martin Feldhofer가 제안했던 내부구조가 8bit인 AES를 사용하는 태그는 저 전력, 소형의 태그를 구현할 수 있다는 장점이 있지만, 물리적 공격과 같은 프라이버시 침해 문제에 있어서는 고려를 하지 않고 있다. Miyako Ohkubo의 해시 체인 기반 프로토콜의 경우에 정보유출, 위치추적 공격, 전방위보안성과 같은 프라이버시 침해문제를 해결하는데 가장 우수하지만 데이터베이스에서의 연산양이 많아서 태그를 식별하는데 많은 시간이 소요되는 단점을 가지고 있었다. 본 논문에서는 해시 체인 기반 방식을 토대로 데이터베이스에서의 태그 식별 시간을 줄이고, 보다 많은 프라이버시 보호가 필요한 고가의 물품에 적합한 강력한 프라이버시 보호 프로토콜을 제안한다.

3.1 제안 프로토콜 가정 사항

- 본 논문에 쓰는 태그는 수동형과 능동형 모두 사용가능하다.
- 태그는 공개키 기반의 암호화 연산을 수행 할 수 있다.
- 태그는 해시 연산을 수행 할 수 있다.
- 해시함수를 역으로 계산하는 것은 불가능하다.
- 태그와 데이터베이스는 태그의 식별 값을 사전에 알고 있다.
- 공개키센터를 통해서 태그와 데이터베이스는 키를 공유 한다.
- 리더와 데이터베이스사이의 유선 통신은 안전한 채널이다.
- 리더와 태그사이의 무선 통신은 불안전한 채널이다.
- 데이터베이스와 공개키 센터의 통신은 안전한 채널이다.
- 태그는 안전한 채널을 사용해서 공개키를 받는다.

3.2 시스템 계수

H : 해시 함수	D : 복호화
E : 암호화	S : 초기 seed 값

$S_{t,i}$: i번째 seed 값	O_i : i번째 태그 출력 값
$keyU$: 암호화 공개키	l : 마지막 seed 값
$keyR$: 복호화 개인키	

3.3 프로토콜 동작

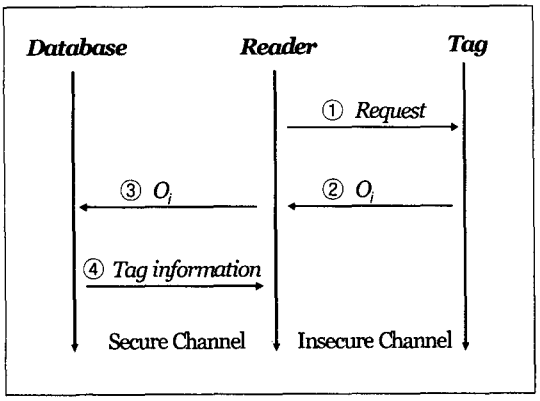
3.3.1. 키 분배 및 선행 계산 단계

프로토콜 과정을 수행하기 전에 태그와 데이터베이스는 암호화를 위한 공개키를 가지고 있어야 한다. 이 작업은 안전한 공개키 분배 센터를 통해서 데이터베이스와 태그에게 분배가 된다. 키 분배를 하는 과정은 안전한 채널을 이용한다고 가정한다. 제작단계는 어떠한 외부의 공격도 막을 수 있는 안전한 상태라고 가정을 한다. 그래서, 태그의 고유 ID와 공개키($keyU$), 개인키($keyR$)가 쌍을 이루어서 데이터베이스에 저장 되고, 태그에는 고유 ID와 공개키가 들어가게 된다. 태그에 공개키만을 넣는 것은 태그는 암호화 과정만 수행을 하기 때문이다. 데이터베이스에서는 태그의 초기 값을 가지고 해시연산을 해서 마지막 값을 계산하는 작업을 선행하게 된다. 마지막 값(l)과 초기 값(S)을 쌍으로 저장해서 가지고 있게 된다.

3.3.2. 프로토콜 수행 단계 (태그의 출력 값을 받음)

키 분배 단계가 끝난 후에 각각의 태그들은 물체에 부착이 되게 되고, 사용가능한 상태로 바뀌게 된다. 사용가능한 상태라는 것은 태그의 정보를 읽을 수 있게 되고, 다음에 설명 하게 될 태그와 데이터베이스에서의 연산이 가능하게 되는 것을 말한다. 모든 프로토콜은 리더로부터 시작된다. 리더는 필요한 정보를 얻기 위해서 $request$를 보내게 된다. $request$를 받은 태그들은 태그의 정보를 리더에게 보내게 되고, 리더는 태그의 정보를 데이터베이스로 보내서 태그의 정보를 확인하게 된다. 데이터베이스는 태그의 원래 정보를 계산해서 다시 리더에게 반환하게 된다. [그림-1]에서 1번 과정은 리더가 태그에게 정보를 요청하는 과정이다. 리더는 무선 주파수로 $request$를 보내게 된다. $request$를 보내면 무선 주파수의 범위 안에 있는 태그들이 주파수에 있는 클럭과 에너지를 받아서 동작을 하게 되고, 2번 과정에서 태그내부에서 $keyU$를 가지고 생성된 O_i값을 리더에게 전송하게 된다. 3번 과정에서 리더는 태그로부터 받은 O_i값을 다시 데이터베이스로 전송을 하게 된다. 데이터베이스는 리더로부터 받은 O_i값을 계산해서 태그의 원래 seed값을 알아내고, 그 seed값을 가진 태그의 정보를 리더에게 전송을 하게 된다. 4번 과정에서 리더는 태그의 정보를 받아서 태그를 식별하게 되

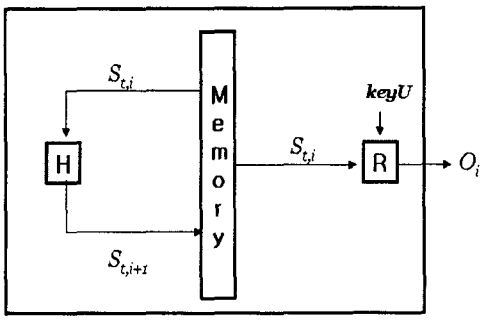
고 사용목적에 따라서 태그에 대한 작업을 진행 하게 된다.



[그림 1] 프로토콜 동작

3.3.3 태그 연산

태그는 리더로부터 에너지를 얻게 되면 태그내부 연산을 진행을 한다. 태그 내부연산을 하는 것은 초기의 시드 값을 그대로 내보내는 것이 아니라 연산을 통해서 생성된 다른 값을 리더에게 내보내고 원래의 시드 값을 태그 내부에서 변화시켜서 이전의 값을 알 수 없도록 해서 전방위보안성을유지하기 위함이다. 태그는 리더의 요청이 있을 때마다 암호화 체인을 통해서 태그 내부의 값을 변화 시킨다. 현재 트랜잭션인 i번째 $S_{t,i}$를 해시함수를 통해서 $S_{t,i+1}$로 바꾸고 memory에 저장한다. 다음 $i+1$번째 트랜잭션에서는 $S_{t,i+1}$을 $S_{t,i+2}$로 바꾸는 과정을 반복하게 된다. [그림-2]는 태그에서의 연산 과정이다.



[그림 2] 태그 내부 구조와 연산 과정

3.3.4 데이터베이스에서의 연산

DB는 O_i 값을 받으면 받은 값을 자신의 비밀키($keyR$)로 복호화하고 복호된 값을 해시체인에 넣어서 마지막 값(i)을 찾아내게 된다. 마지막 값과 쌍으로 저장되어 있는 초기 값(S)을 찾아서 태그를 식별하고 식별된 태그 정보를 리더에게 보낸다. 이때 최대 태그의 수명만큼의 해시연산만으로 태그의 정보를 알 수 있게 되기 때문에 데이터베이스에서의 연산량을 크게 줄일 수 있게 된다.

4. 프로토콜의 안전성

이 프로토콜은 리더의 요청시마다 보내는 태그의 출력 값이 태그내부의 해시연산을 통해서 달라지고 공개키를 통해서 암호화를 해서 보내기 때문에 위치추적공격과 도청 공격에 매우 강하다. 또한, 물리적 공격으로 태그 내부의 값이 드러나더라도 일방향 해시함수의 특성상 이전 트랜잭션의 값을 계산해 낼 수가 없기 때문에, 전방위보안성 측면에서도 우수하다는 장점을 가지고 있다.

5. 결론 및 향후 연구과제

지금까지 발표된 여러 가지 기법들은 프라이버시 보호 측면과 계산량 측면에서의 단점을 가지고 있다. 고가의 물품에 RFID를 사용하기 위해서는 좀 더 확실한 프라이버시 보호 기법이 필요하다. 본 논문에서는 공개키와 해시체인을 통한 RFID 프라이버시 보호 기법을 제안하였다. 이 기법은 강력한 프라이버시 보호와 데이터베이스에서의 연산량 단축을 가져 올 수 있음을 보였다. 앞으로는 저가의 태그에서도 사용 될 수 있는 공개키 모듈의 개발과 프라이버시 보호 기법에 대한 연구가 필요하다.

6. 참고문헌

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

[2] 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.

[3] 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.

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

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