강력한 프라이버시 보호를 필요로 하는 고가 물품을 위한 개선된 RFID 프라이버시 보호 프로토콜†

조정환*, 여상수**, 김성권*
*중앙대학교 컴퓨터 공학부, **단국대학교 정보컴퓨터학부

Enhanced RFID Privacy Protection Scheme for High Price Products which need Strong Privacy Protection

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

요 약

무선 주파수를 가지고 대량의 사물을 동시에 인식 할 수 있는 RFID(Radio Frequency Identification)는 현대 산업사회에서 중요성이 점점 증가하고 있는 자동 인식 기술중에 하나이다. RFID는 무선 주파수를 사용하기 때문에, 대량의 사물을 동시에 인식 한다는 장점 이외에 프라이버시 침해문제를 야기하는 단점을 가지고 있다. 이러한 문제들을 해결하기 위해서 많은 관련 연구들이 진행되고 있다. 그러나, 지금까지 연구된 기법들 중에서 강력한 프라이버시 보호를 필요로 하는 고가 물품을 위한 RFID보호 프로토콜은 없는 상태이다. 본 논문에서는 고가 물품에 부착하기 적합한 해시체인과 공개키를 이용한 향상된 RFID 프라이버시 보호 기법을 제안한다.

I. 서론

RFID(Radio Frequency Identification)는 최근에 사용이 급속도로 증가 하면서 여러 가지 산업분야에서 관심이 높아지고 있다. RFID는 무선 주파수를 이용해서 대량의 사물을 동시에 인식 할 수 있는 자동 인식 기술 중의 하나이다. 무선 주파수를 사용하기 때문에, 그에 따르는 프라이버시 침해 문제가 많이 발생하게 된다. 예를 들어서, 주파수 도청을 통한 정보 유출의 문제라든지, 주파수 발신지에 있는 사용자의 위치가 파악되어서 위치추적 문제를 야기 할 수 있다. 또한, 물리적 공격을 통한 태그의 이전 정보를 얻음으로써 전방위보안성에 대한 문제도 발생하게 된다. 이러한 문제들이 발생하게 되면서 여러 가지 관련 연구들이 진행되고 있다[1]. 현재 연구되고 있는 분야들은 주로 저가의 태그에 사용하는 기법들이다. 그러나, 저가의 태그에는 현재까지 알려진 가장 안전한 기법인 공개키 암호화를 이용하는 방식을 사용 할 수 없다. 저가 태그는 메모리나 연산 능력의 하드웨어적인 제한이 있기 때문이다.

RFID를 사용하는 여러 물품 중에서 강력한 수준의 프라이버시 보호 기법을 필요로 하는 고가의 물품들이 있다. 이러한 고가 물품에 저가의 태그를 사용하게 되면 프라이버시 침해문제를 통

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

한 큰 피해를 가져 올 수도 있다. 따라서, 고가 물품에는 강력한 프라이버시 보호를 할 수 있는 향상된 암호화 서비스 기법이 필요하다. 본 논문에서는 고가 물품에 사용되는 고기능의 태그와 이에 따른 프로토콜을 제시한다.

II. 관련연구

Miyako Ohkubo는 해시체인을 이용한 프라이버시 보호 프로토콜을 제안하였다[2]. 이 프로토콜의 장점은 해시 함수를 통해서 태그 내부 값을 변화시키기 때문에, 출력 값의 불구분성을 통해서 도청이나 위치추적 공격에 우수하다는 장점과 해시 암호화를 이용하기 때문에, 역으로의 계산이 되지 않아서 전방위보안성에 우수하다는 장점을 가지고 있다. 그러나, 데이터베이스에서의 연산량이 매우 많다는 단점을 가지고 있다.

Martin Feldhofer가 제안한 저 전력, 소형의 AES(Advanced Encryption Standard)는 저가에 적합한 태그를 구현 하였다[3,4]. 기존에 사용되는 AES의 내부 구조를 변화 시켜서 암호화의 강도를 조금 낮춰서 태그에서 사용 가능하도록 구현 하였다. 하지만, 프라이버시 침해문제에 있어서는 취약하다는 단점을 가지고 있다. 물리적 공격을 통해서 내부의 키 값이 드러나면 전방위 보안성이 깨진다는 단점과 불구분성이 없는 출력 값을 사용하기 때문에 위치 추적 공격에 단점을 가지고 있다.

III. 제안 프로토콜

앞장의 관련 연구에서 언급을 했던 RFID 프라이버시 보호 기법들은 여러 가지 문제들을 내포하고 있다. 해시 체인을 사용해서 정보 유출이나 위치추적 공격, 전방위보안성과 같은 프라이버시 침해 문제를 해결하는 Miyako Ohkubo의 기법은 프라이버시 보호 측면에서 굉장히 우수하지만, 하나의 태그를 식별하는데 따르는 데이터베이스에서의 연산량이 많기 때문에 많은 시간이 소비되는 단점을 가지고 있다. 또한, AES를 사용하는 Martin Feldhofer의 기법은 저 전력, 작은 사이즈의 태그를 실제로 구현 할 수 있다는 장점이 있지만, 물리적 공격에 대한 대비책이 없어서, 프라이버시 침해 문제가 드러났다. 본 논문에서는 위 기법들에서 드러난 단점들을 줄이기 위한 기법을 제시한다. 해시 체인 기반 방식을 토대로 데이터베이스에서의 연산량을 줄여서 태그의 식별시간을 단축하고, 강력한 프라이버시 보호가 필요한 고가물품에 사용하기 적합한 프라이버시 보호 프로토콜을 제안한다.

1. 가정 사항

-태그는 공개키 기반의 암호화 연산을 수행할 수 있다.
-태그는 해시 연산을 수행 할 수 있다.
-태그는 수동형과 능동형 모두 사용 가능하다.
-해시 함수를 역으로 계산하는 것은 불가능하다.
-태그와 데이터베이스는 태그의 식별 값을 사전에 알고 있다.
-태그가 생산되는 단계에서 공개키 센터를 통해 태그와 데이터베이스는 키를 공유한다.
-리더와 데이터베이스 사이의 통신은 안전하다.
-리더와 태그 사이의 통신은 불안전하다.

2. 용어 정의

H : 해시 함수
E : 암호화
D : 복호화
A : 초기 seed 값
$A_{t,i}$: i번째 seed 값
$keyU$: 암호화 공개키
$keyR$: 복호화 개인키
O_i : i번째 태그 출력 값
l : 마지막 seed 값

3. 선행 단계

태그와 데이터베이스는 프로토콜이 수행되기 전에 키 분배 작업을 통해서 공개키를 소유하고 있어야 한다. 일련의 작업들은 공개키 분배 센터를 통해서 데이터베이스와 태그에게 분배가 된다. 키 분배를 하는 과정은 안전한 상태에서 이루어진다고 가정을 한다. 어떠한 외부의 공격도 들어 올 수 없는 안전한 상태에서

태그는 제작되어진다. 그리고, 안전한 채널을 이용해서 키가 분배 된다. 이러한 작업이 끝나면 태그와 데이터베이스는 공개키($keyU$)와 태그의 고유 ID를 저장하게 되고, 데이터베이스는 추가로 복호화키($keyR$)을 저장을 하게 된다. 복호화키를 태그에 넣지 않는 것은 태그는 암호화 작업만을 하기 때문이다. 키 분배 작업이 끝나면 데이터베이스는 선행 계산 작업을 하게 된다. 태그의 초기 값(A)을 가지고 데이터베이스 안에 있는 태그와 동일한 해시 연산을 통해서 마지막 값(l)을 계산하는 작업을 하게 된다. 마지막 값과 태그의 초기 값을 쌍으로 저장해서 가지고 있게 된다.

4. 프로토콜 수행

위의 사전 작업 단계가 끝나고 난 후에 태그들은 각각의 물체에 부착이 되게 되고, 태그의 상태가 읽을 수 있는 상태가 되어서 리더를 통해서 태그를 읽는 것이 가능하게 된다. 이 상태가 되면 데이터베이스와 태그는 리더를 통해서 연산을 하게 된다. 이것은 다음에 자세히 설명한다. 본 논문에서 제안하는 프로토콜은 리더로부터 모든 연산이 시작되게 된다. 어떤 필요에 의해서 리더는 *request*를 발생을 하게 되고, 그 *request*는 리더 주위의 태그들에게 전달이 된다. *request*를 받게 된 태그들은 태그의 식별 정보를 *request*를 보낸 리더에게 보내게 된다. 이 후에 태그 식별 정보를 받은 리더는 이 식별 정보가 무엇인지 확인하기 위해서 데이터베이스로 받은 식별 정보를 보내게 된다. 데이터베이스는 이 받은 정보를 토대로 연산을 수행해서 태그의 정보를 확인하게 되고, 확인된 정보를 리더에게 돌려주게 된다.

그림-1은 제안하는 프로토콜의 동작이다. 가의 단계는 리더가 태그에게 정보를 요청하고 에너지와 클럭을 공급하는 단계이다. 리더는 *request*를 생성하고 태그에게 보낸다. 리더가 *request*를 발생시키면 무선 주파수 범위 안에 있는 태그들이 에너지와 클럭을 받고 동작을 하게 되고,*request*를 받아서 태그 내부 연산을 진행하게 된다. 나 단계는 태그 내부 연산을 진행한 후에 출력 값(O_i)과 공개키 값($keyU$)을 리더에게 보내는 단계이다.

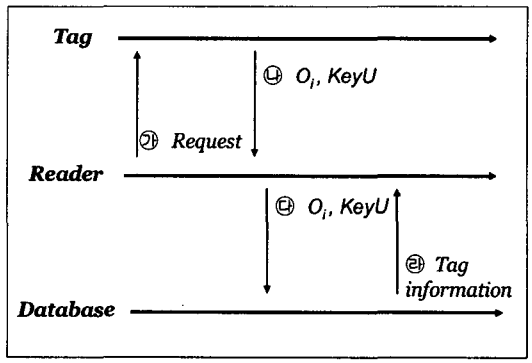

그림 1. 제안 프로토콜 동작 과정

태그내부 연산은 다음 절에서 자세히 설명한다. 다 단계에서 리더는 태그로부터 받은 출력 값을 데이터베이스로 전송하는 단계이다. 다 단계 이후에 데이터베이스는 리더로부터 받은 출력 값을 연산을 하고, 태그의 원래 초기 값을 찾아내고, 그에 따르는 태그의 정보를 리더에게 전송을 하게 된다. 라 단계에서 리더는 태그 정보를 받고 여러 가지 사용목적에 따라서 태그에 대한 작업을 수행 하게 된다.

5. 태그 내부 연산

전방위보안성을 유지하기 위해서 태그는 태그 내부의 해시 연산을 수행하게 된다. 태그는 리더로부터의 *request*와 에너지 클럭을 받고 난 후에 태그 내부 연산을 진행하게 된다. 이 과정을 수행하는 이유는 이 과정을 하지 않고 태그의 초기 값을 그냥 내보내면 도청을 통한 공격이 가능하기 때문에 프라이버시 침해 문제가 발생하기 때문이다. 태그는 각 리더의 *request*를 받을 때 마다 해시 체인을 통해서 태그 내부 식별 값을 변화 시킨다. 현재 수행되는 트랜잭션인 i 번째 $A_{t,i}$ 를 해시함수를 통해서 $A_{t,i+1}$ 로 변화시키고 메모리에 저장 한다. 다음 *request*가 오면 $i+1$번째 트랜잭션이 시작되고 그 때 저장되어 있던 $A_{t,i+1}$ 값을 다시 해시함수를 통해서 $A_{t,i+2}$로 변환한다. 리더의 *request* 마다 위와 같은 동작을 반복하게 된다. 다음 그림-2는 태그 내부 연산 과정이다.

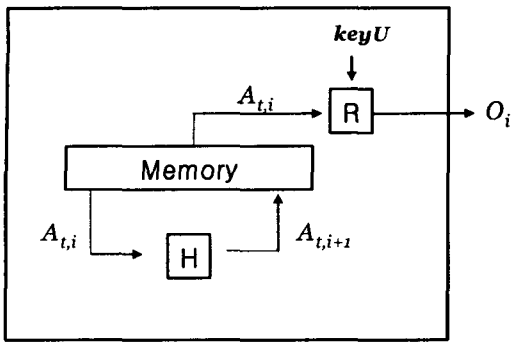

그림 2. 태그 내부 연산 과정

6. 데이터베이스 내부 연산

데이터베이스는 리더로부터 태그 출력 값에 대한 정보를 받게 되면 데이터베이스 연산을 수행하게 된다. 출력 값과 공개키 값을 받으면 선행 단계에서 저장해 두었던 복호화키로 받은 출력 값을 복호화하고, 복호화된 값을 태그와 같은 해시 체인에 넣어서 마지막 값을 찾아내게 된다. 그 후에 마지막 값과 쌍을 이루고 있는 태그의 초기 값을 찾아서 태그를 식별하고, 식별된 태그 정보를 리더에게 보낸다.

이런 과정을 함으로써 최대 태그의 수명만큼의 해시 연산을 통해서 태그의 정보를 알 수 있기 때문에, 데이터베이스에서의 연산량을 크게 감소시킬 수 있게 된다.

7. 프로토콜 안전성

제안하는 프로토콜은 해시 연산과 공개키를 통한 암호화를 하기 때문에 도청을 통한 위치 추적 공격 및 정보 유출 공격에 강하고, 물리적 공격을 통한 전방위보안성에도 우수함을 가진다. 공개키를 통한 암호화이기 때문에, 복호화키를 알지 못하면 도청을 통해서 정보를 얻었다고 하더라도 그 내부 정보를 알 수가 없게 된다. 또, 태그 내부 연산을 *request*마다 진행해서 내보내는 출력 값이 다르게 되기 때문에 불구분성을 보장해서 위치 추적에 대한 공격을 방지 할 수 있다. 물리적 공격을 통해서 태그의 정보가 드러나더라도 해시함수의 특성상 이전 값을 찾아내기가 어렵기 때문에 전방위보안성을 보장 할 수가 있게 된다.

IV.결론 및 향후 연구 과제

여러 가지 분야에서 RFID에 대한 관심이 높아지고 사용이 많아지면서 야기되는 많은 프라이버시 침해문제에 대한 관련 연구들은 프라이버시 보호와 데이터베이스에서의 연산량 측면에서 여러 단점을 가지고 있다. 또한, 고가의 물품에 사용하기에는 적합하지 못하다. 본 논문에서는 공개키 암호화와 해시 체인 연산을 통한 개선된 RFID 프라이버시 보호 기법을 제안하였다. 제안한 기법은 데이터베이스에서의 연산량 단축과 강력한 프라이버시 보호를 할 수 있음을 보였다. 향후에는 저가의 태그에서도 사용 가능한 공개키 모듈에 대한 개발과 이에 따르는 프라이버시 보호 기법에 대한 연구가 필요하다.

[참고문헌]

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

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

[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.