RFID 사용자를 위한 개인 프라이버시 보호 에이전트*

김수철° 여상수 김성권
중앙대학교 컴퓨터공학부
{sckim°, ssyeo}@alg.cse.cau.ac.kr , skkim@cau.ac.kr

Personal Privacy Protection Agent for RFID Users

Soo-Cheol Kim° Sang-Soo Yeo Sung Kwon Kim
School of Computer Science and Engineering, Chung-Ang University

요 약

본 논문에서는 RFID 프라이버시 보호를 위한 개인 모바일 장치에 대해 제안한다. 현재까지 제안되었던 보안 기법들은 태그와 리더 사이의 암호학적 기법에 중점을 두었다. 제안하는 프라이버시 보호 에이전트는 다른 논문과는 달리 특별한 모바일 기기를 사용하여 높은 수준의 보안을 제공한다. 에이전트에 등록된 태그가 자신의 정보를 보안 에이전트에 위임하여 태그의 역할을 대신하게 하는 방식을 사용한다. 에이전트는 접근하는 리더를 인증하고 자신이 관리하는 태그 정보들을 선별하여 높은 수준의 암호화 처리 후 안전하게 통신한다. 태그는 해쉬만 가능하면 위변조문제까지 막을 수 있으므로 현재 RFID 시스템의 큰 변경 없이 에이전트가 도입 가능하며 RFID 프라이버시 보호 문제를 해결 할 수 있을 것이라 기대된다.

1. 서 론

RFID(Radio Frequence Identification)는 무선 주파수를 이용하여 대상(물건, 사람 등)을 식별할 수 있는 기술로서, 안테나와 칩으로 구성된 RF 태그에 사용 목적에 알맞은 정보를 저장하여 적용 대상에 부착한 후 판독기에 해당하는 RFID 리더를 통하여 정보를 인식하는 방법이다. 이 RFID 시스템은 바코드를 대신하여 유통, 물류 산업에 큰 발전을 줄 것이라고 기대된다.

그러나 이와 같이 편리한 RFID 시스템에도 문제점이 존재한다. RFID는 바코드와는 달리 멀리서도 인식이 가능하다는 장점 때문에 오히려 사용자 프라이버시에 문제가 생긴다. 사용자도 알지 못하는 사이에 모든 리더에게 응답하여 식별가능하다는 점 때문에 정보유출 문제와 위치추적 문제가 생긴다. RFID의 대중화에 앞서 이와 같은 프라이버시 문제의 해결이 우선시 되고 있다.

프라이버시 보호를 위해 여러 가지 방법이 제시되었는데 가장 단순하면서도 확실한 방법은 kill 태그[1]를 사용하는 것이다. 그 외에도 sleep&wake 모드[2]를 이용해서 프라이버시를 보호하는 방법과 Blocker 태그[3,4]를 사용하여 사용자 프라이버시를 보호하는 방법들이 있다. 또한 모바일 프라이버시 보호 장치를 사용한 논문들도 발표되었다.[5,6]

본 논문에서는 기존에 제안된 여러 가지 프라이버시 보호 방법들 중 통신 계층을 이용한 기법들에 대하여 간략히 설명하고 그 기법들의 문제점에 대해 이야기한다. 그리고 저가형 태그에도 적용될 수 있는 효율적이고 실용적인 개인 프라이버시 보호 에이전트 기법을 제안한다.

2. 관련 연구

RFID 프라이버시 보호를 위한 가장 극단적인 방법은 사용자가 가게에서 물건을 사고 나면 출구에서 RFID 태그를 파괴하거나 kill 명령어를 사용해 사용 중지해 버리는 것이다[1]. 태그는 내부에 단락회로가 있기 때문에 이를 끊음으로서 'kill 명령'을 실행하게 되는데 한 번 죽은 태그는 다시 살릴 수 있는 방법이 없게 된다. 그러면 위치트래킹 같은 공격을 원천적으로 막을 수 있지만 RFID의 다양한 서비스를 포기하게 된다. 그래서 단순히 태그를 무력화 시키는 방법은 너무 극단적인 방법이다.

극단적인 kill 태그 대신 나온 방법이 sleep/wake 모드이다[2]. 이 방법은 태그의 상태를 sleep/wake 2가지로 나누어 sleep 모드일 경우 아무런 작동을 하지 않고 wake 모드일 경우에는 정상적인 태그로 동작하게 하는 방법이다. 하지만 이 방법도 사용자 프라이버시 문제에 근본적인 해결책이 되지 못한다.

다음은 Juels가 제안한 Blocker 태그 기법이다[3,4]. 이 기법의 요점은 상품 태그 이외에 사용자가 "Blocker 태그"를 가지고 있는 방식이다. Blocker 태그는 리더의 질의에 응답 할 때 항상 0과 1을 모두 대답함으로써, 특정 태그의 존재 여부를 숨기고, 리더가 중도에 태그인식을 포기하게 만든다. 일종의 전파방해로서 리더가 태그들의 ID를 알아내는 것을 방해한다. 하지만 Blocker 태그는 악용 가능성이 존재하고, 선별적인 blocking 이 불가능한 단점이 있다.

그 외 모바일 기기를 사용하여 태그와 리더 사이의 통신을 중재하는 기법도 있다[5,6]. 이 모바일 기기는 배터리가 있고 많은 메모리양과 높은 계산능력을 가지고 태그와 리더 사이에서 개인 프라이버시 보호를 한다. 이 기기의 기능은 크게 4가지로 나뉘는데 첫 번째로 리더가 태그를 스캔할 때, 작용범위 안에 등록되지 않은 태그가 들어올 때를 감시하는 역할을 한다. 두 번째로 태그를 대신하여 키를 관리해주거나 난수를 생성해주는 역할을

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

한다. 세 번째는 태그나 리더의 접근을 제어해주는 역할을 한다. 마지막으로 태그를 대신하여 리더가 정당한 리더인지 인증해주는 역할을 한다.

3. 제안하는 기법

본 논문에서 제안하는 개인 프라이버시 보호 에이전트(Personal Privacy Protection Agent : PPPA)는 앞서 보여준 관련 연구 중 모바일 기기를 사용하여 태그와 리더 사이를 중재하는 기법의 일종이다. 제안하는 기법의 핵심은 태그내의 비밀 정보를 PPPA 가 획득하여 태그 대신 높은 수준의 보안을 수행하여 리더와 통신하는 것이다.

태그는 자신이 가진 비밀정보를 모두 PPPA 에게 넘겨주고 Sleep 상태에 들어가게 된다. PPPA 는 사용자가 가지고 있는 모든 태그의 정보를 획득한 후 대표 태그의 역할을 하게 되는 것이다. 리더는 PPPA 와 인증한 후 통신하여 자기가 원하는 태그 정보를 얻게 되는 것이다. 이와 같은 개념을 그림으로 나타내면 (그림 1)과 같다.

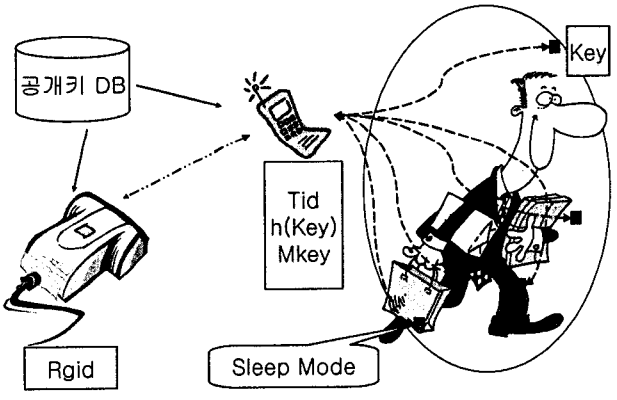

그림 1. Personal Privacy Protection Agent

3.1 Personal Privacy Protection Agent 준비 상태

PPPA 기법을 시행하려면 몇 가지 준비 사항이 필요하다. 일단 각 태그는 태그아이디와 비밀키 외 태그상태를 바꿀 수 있는 모드키가 필요로 한다. 그 키를 가진 PPPA만이 태그를 등록시킬 수 있는 것이다. 상점에서 물건을 팔 경우 계산이 끝난 후 상점에서 개인의 PPPA 에게 모드키를 넘겨주면 태그가 등록 가능해지는 형태로 진행되면 된다.

리더는 특별한 그룹 아이디를 가지게 된다[7]. 그룹 아이디로 태그를 읽을 수 있는 권한을 제한하게 되는 것이다. 일종의 클래스화 라고 볼 수 있다. 이 그룹 아이디와 그룹키(공개키 사용가능)를 가지고 합법적인 리더인지 인증하는 절차를 수행할 수 있다.

PPPA도 각자의 아이디와 공개키를 가지고 있다. 그리고 가지고 있는 데이터는 각 태그의 아이디와 모드키 그리고 해쉬된 비밀키를 가지고 있다. 그 외 태그를 읽을 수 있는 리더그룹과 그 공개키를 저장해두고 있다.

준비 상태에 대한 개념을 그림으로 나타내면 (그림 2)와 같다.

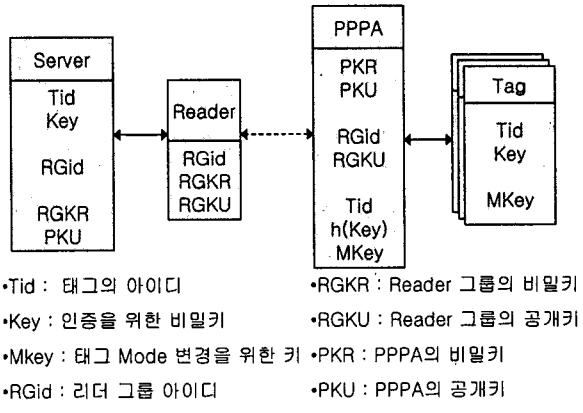

그림 2. PPPA 기법 Data 준비 상태

3.2 태그의 Sleep 상태 (Privacy 보호)

태그는 Sleep 모드로 들어가고 자신의 정보를 PPPA에게 위임한 상태가 제안하는 PPPA 기법의 가장 일반적인 상태이다. 이 상태에서는 리더와 PPPA와의 통신만 존재한다. 태그의 Sleep 상태에서의 프로토콜은 5단계로 이루어져 있으며, 각 단계별 프로토콜의 전송 내용과 처리 방법은 다음과 같다.

(1) 리더는 PPPA에게 요청과 함께 그룹 아이디와 난수를 리더그룹 개인키로 전자서명 하여 보낸다.

$$Reader \rightarrow PPPA: Query \| E_{RGKR}(RGid \| R_r)$$

(2) PPPA는 인증된 리더그룹의 공개키로 복호화 한 후 리더그룹의 아이디를 알게 된다. 그 후 받은 난수와 자신이 생성한 새로운 난수를 자신의 개인키로 서명하고 리더그룹의 공개키로 암호화 하여 안전하게 리더에게 전송한다.

$$PPPA \rightarrow Server: a_1 = E_{RGKU}(E_{PKR}(R_r \| R_d))$$

(3) 리더는 받은 정보를 서버에 보내고 서버는 저장된 PPPA의 공개키로 복호화 하여 PPPA의 아이디를 획득한다. 그 후 서버는 PPPA가 보낸 난수를 자신의 개인키로 서명하고 PPPA의 공개키로 암호화 하여 PPPA 에게로 보낸다.

$$Server \rightarrow PPPA: a_r = E_{PKU}(E_{RGKR}(R_d))$$

(4) PPPA가 리더로부터 정보를 받아 확인을 거치면 상호 인증이 완료된 것이다. 그 후 서로 가지고 있는 키들을 이용하여 PPPA가 가지고 있는 태그의 아이디 정보를 넘겨주게 된다.

$$PPPA \rightarrow Server: a_2 = E_{RGKU}(E_{PKR}(E_{h(key)}(Tid))$$

(5) 서버는 받은 정보를 복호화 하여 관련된 정보를 리더에게 넘겨주게 된다.

$$Server \rightarrow Reader: Tid \| Data$$

이와 같은 인증 절차는 (그림 3)에 자세히 나와 있다.

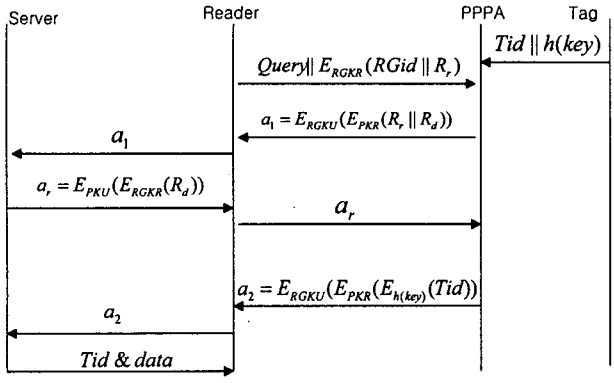

그림 3. 태그 Sleep 상태의 PPPA 기법

3.3 태그의 Wake 상태 (위변조 방지)

특별한 경우 태그의 위변조 가능성을 검사해야 할 경우가 있다. 그와 같은 경우에 사용되는 상태이다. 만약 태그가 비밀키 자체를 PPPA에 넘겨주었으면 태그의 위변조가 너무나 쉽게 된다. 따라서 해쉬된 비밀키를 넘겨주고 만약의 경우 태그의 위변조를 검사하고자 할 경우 비밀키를 이용하여 인증을 한다.

위변조 검사 프로토콜은 간단하게 3단계로 진행된다.

(1) 우선 서버에서 난수를 생성하여 PPPA에 보내게 된다. 그 후 PPPA는 모드키를 사용하여 태그를 Wake 상태로 만들어서 난수를 전송한다.

$$Server \rightarrow Tag: R$$

(2) Wake 상태의 태그에서는 받은 난수와 자신이 가지고 있는 비밀키를 XOR한 후 해쉬하여 다시 PPPA에게 보낸 후 다시 서버로 전송한다.

$$Tag \rightarrow Server: a_t = h(R \oplus Key)$$

(3) 서버는 태그에서 보내온 정보와 자신이 가지고 있는 정보를 계산하여 나온 값을 비교하여 서로 동일하면 태그는 인증 받게 된다.

$$Server: compare(a_t = T)$$

위변조 감시를 위한 Wake 모드에서의 인증 절차는 (그림 4)에 자세히 나와 있다.

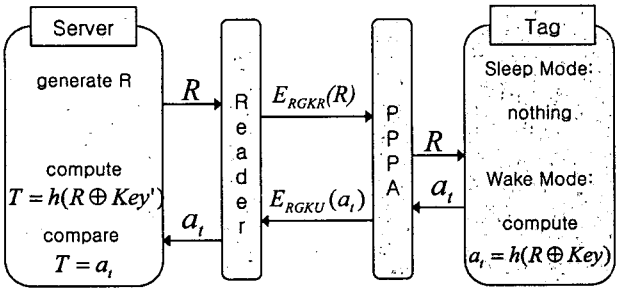

그림 4. 태그 Wake 상태의 PPPA 기법

4. 결 론

본 논문에서 제안한 개인 프라이버시 보호 에이전트는 등록된 태그를 대신하여 리더와 통신하는 기기이다. 이 에이전트는 태그의 근본적인 한계였던 메모리양과 계산 능력을 간단하게 해결하여 높은 수준의 보안을 제공한다. 또한 태그 자체의 특별한 변경 없이 RFID 시스템의 추가적인 구성요소이므로 저렴하게 효율적인 시스템 구축이 가능하다. 그리고 모바일 기기를 사용한 기법들의 기본적인 능력인 감시, 키 관리, 접근 제어, 인증을 수행할 수 있으면서 위변조 방지가 첨가된 향상된 기법이라 볼 수 있다.

향후에는 프라이버시 보호 에이전트 자체의 보안과 태그의 주요 비밀들을 저장, 삭제할 때의 보안에 대하여 연구할 필요가 있다.

5. 참고문헌

[1] S. Sarma, S. Weis, and D. Engels, "RFID Systems and Security and Privacy Implications", In CHES 2002, vol. 2523 of LNCS, pp. 454-469, August 2002.

[2] Guenter Karjoth, Paul Moskowitz. "Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced", WPES 2005 , November 2005.

[3] A. Juels, R. Rivest, and M Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy" , In Proceedings of 10th ACM Conference on Computer and Communications Security(CCS 2003), pp. 27-30, October 2003.

[4] A. Juels and J. Brainard , "Soft Blocking : Flexible Blocker Tags on the Cheap" , WPES '04 (one of worksEhop of ACM CCS 2004), October 2004.

[5] Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. "RFID guardian: A battery-powered mobile device for RFID privacy management.", ACISP 2005 , July 2005.

[6] Shinichi Konomi. "Personal Privacy Assistants for RFID Users", International Workshop Series on RFID 2004, November 2004.

[7] Xingxin (Grace) Gao, Zhe (Alex) Xiang, Hao Wang, Jun Shen, Jian Huang, and Song Song. "An approach to security and privacy of RFID system for supply chain.", In CEC-East'04, pages 164-168, September 2005.