모바일 RFID 환경에 적합한 프라이버시 보호 기법+

김일중, 최은영, 이동훈*
*고려대학교, 정보보호 대학원

Privacy protection scheme for RFID mobile environment

Il-jung Kim, Eun-young Choi, Dong-hoon Lee*
*Graduate School Information Security, Korea University.

요 약

무선 주파수 인식 (RFID : Radio Frequency Identification) 시스템은 유비쿼터스 시스템 환경에서 중요한 기술로 주목 받게 될 것이다. 최근에는 이런 RFID 시스템과 모바일 시스템이 결합하여 새로운 모바일 RFID 시스템이 소개되었다. 모바일 RFID (Mobile Radio Frequency Identification) 시스템은 모바일 기기에 RFID 시스템이 접목된 것으로 RFID 리더가 모바일 기기 안에 내장된 것으로 모바일 기기를 가진 사람이라면 누구든지 손쉽게 태그가 내장된 상품의 정보를 읽을 수 있다. 이러한 모바일 RFID 리더의 특성으로 인해 태그가 내장된 물품을 소유하고 있는 개인의 프라이버시 침해가 발생한다. 본 논문에서는 간단한 연산과 해쉬함수를 사용하여 모바일 RFID 시스템 환경에 적합한 프라이버시 보호 기법을 제안한다.

I. 서론

최근 다양한 정보 서비스와 유비쿼터스 환경을 지원하는 휴대 단말 이동통신과 인터넷이 결합한 무선 인터넷 인프라에 RFID 융합을 통해 새로운 서비스를 제공하는 모바일 RFID 시스템이 출현하였다. 모바일 RFID 시스템에서는 RFID 태그 칩과 RFID 리더를 휴대폰에 장착하여 다양한 RFID 서비스로 확대되고 있다. 모바일 기기의 휴대성과 RFID의 비접촉식 통신 특성으로 인하여 개인의 프라이버시 침해와 태그와 리더사이의 통신상의 정보누출이 예상되고 있다. 본 논문에서는 구매자의 mRFID 리더만이 상품의 내장된 태그로부터 정보를 읽을 수 있게 하여 개인 프라이버시 침해 문제를 예방하는 기법을 제안한다. 제안 기법은 해쉬함수와 XOR을 이용한 간단한 연산만을 사용하여 제삼자가 정보를 읽을 수 없게 한다[1].

+ 본 연구는 서울시 산학연 협력사업(10665) 지원으로 수행되었음

II. 모바일 RFID 시스템의 문제점

1. 모바일 RFID 시스템의 구성

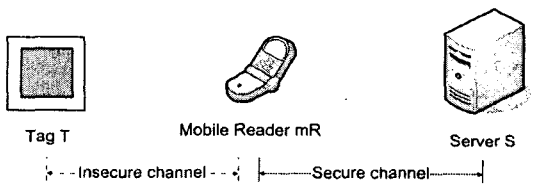

그림 1. 모바일 RFID 시스템의 구성

모바일 RFID 시스템은 세 가지 구성 요소, 태그, 모바일 리더, 서버로 구성되며 각각의 기능은 다음과 같다. 그림 1은 모바일 RFID 시스템의 구성을 나타낸 것이다.

- 태그 (Tag) : mRFID 리더로부터 질의를 받아 사물에 대한 고유정보를 무선 통신을 통하여 전송한다. 태그는 무선 통신을 위한 안테

나와 연산과 고유정보를 저장하는 마이크로 칩으로 구성 되어있다. 태그는 전력공급에 따라 능동형 태그 (active tag)와 수동형 태그 (passive tag)로 구분된다.

- 능동형 태그 (active tag) : 능동형 태그는 태그 자체에 내장되어 있는 배터리를 통하여 전력을 공급 받는다. 리더와 원거리 통신이 가능하지만 배터리가 내장되어 있어 가격이 비싸고 배터리가 모두 소모되면 태그의 사용이 불가능하다.

- 수동형 태그 (passive tag) : 수동형 태그는 리더로부터 받은 RF 신호(signal)로 부터 전력을 공급받는다. 근거리 통신이 가능하며 복잡한 연산을 어렵다. 수동형 태그는 배터리를 내장하고 있지 않아 수명이 반영구적이며 능동형 태그에 비해 가격이 싸다.

• 모바일 RFID 리더 (mRFID reader) : mRFID 리더는 기존의 RFID 시스템의 리더를 모바일 기기에 내장한 것이다. 태그에게 질의를 전송하며 태그로부터 전송된 데이터를 인식하거나 태그에 새로운 정보를 다시 쓰는 역할을 한다. 기존의 RFID 시스템의 리더에 비해 연산 능력이 뛰어나며 저장 공간 또한 더 크다.

• 서버 (Server) : 서버는 태그에 대한 정보를 전장하고 관리하는 역할을 한다. 리더로부터 전달받은 태그의 고유정보에 해당하는 정보를 리더에게 전송한다.

본 논문에서 다루는 모바일 RFID 시스템은 다음의 가정 하에서 동작한다.

• mRFID 리더로부터 전원을 공급받는 수동형 태그를 사용한다.

• 태그와 mRFID 리더 사이의 통신 채널은 안전하지 않다고 가정한다. 이 영역에서는 공격자가 시스템을 공격할 수 있다.

• mRFID 리더와 데이터베이스 사이의 통신 채널은 모바일 무선 보안기술을 사용하여 공격자의 공격으로부터 안전하다고 가정한다.

2. 모바일 RFID 시스템의 문제점

모바일 RFID 시스템의 특성상 mRFID 리더와 태그는 직접적인 접촉이 없이 무선 통신을 이용하여 데이터를 주고받는다. 태그는 mRFID 리더의 신호에 반응하여 자신의 고유정보를 mRFID 리더에 전송한다. 즉, mRFID 리더가 정당한지 아닌지에 상관없이 자신의 고유정보를 전송한다. 이러한 태그와 mRFID 리더의 통신방법은 태그 주변의 제 삼자가 손쉽게 사용자가 소유하고 있는 상품의 정보와 위치정보를 알아 낼 수 있어 사용자의 프라이버시 침해 문제가 발생하게 된다. 모바일 RFID 시스템에서 프라이버시 침해에 대한 문제점을 다음과 같이 두 가지로 나타낸다[2].

• 개인정보 노출(Information leakage) : 실생활에서 사람들이 모바일 RFID 시스템을 사용함에 따라 태그가 내장된 물건들과 각자의 mRFID 리더를 소유하게 될 것이다. 이것은 자신의 개인정보가 자신의 동의 없이 쉽게 누출될 수 있다는 것을 의미한다.

• 위치 추적(Traceability) :태그가 내장된 물건을 구매할 때, 공격자는 구매자와 태그의 고유정보에 대한 연관성을 가지고 구매자가 태그가 내장된 상품을 지니고 이동하면 태그의 고유정보를 이용하여 구매자의 이동경로를 추적할 수 있다.

3. 제안 프로토콜

본 논문에서는 모바일 RFID 시스템 환경에서 사용자의 프라이버시를 보호할 수 있는 기법을 제안한다. 제안 기법은 상품의 구매 전과 구매 후로 구성된다. 제안 기법에서는 mRFID 리더와 태그사이의 통신을 한 번의 세션으로 하고 i는 i번째 세션을 뜻한다.

1) 구매 전

매장에서 상품을 구매하기 전에 mRFID 리더를 사용하여 태그로부터 정보를 받아오는 것은 기존의 RFID 시스템과 유사하다. mRFID 리더로 태그에 신호(*Request*)를 보내면 태그는 자신의 ID를 mRFID 리더로 보내주고 mRFID 리더는 서버로 ID를 보낸다. 서버는 mRFID 리더로부터 받은 ID에 해당하는 데이터($Data_T$)를

mRFID 리더에게 보낸다. 그림 2는 상품을 구매하기 전의 태그, mRFID 리더, 서버의 동작을 나타내고 있다.

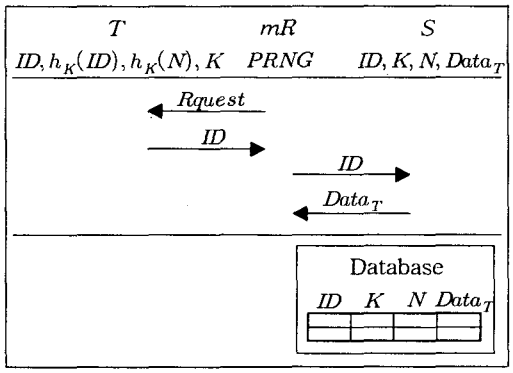

그림 2. 상품 구매 전.

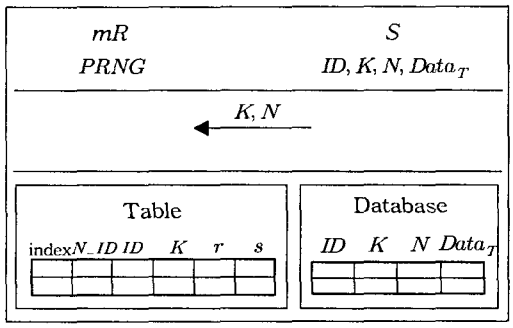

그림 3. 상품을 구매 후 태그ID 갱신.

2) 구매 후

가. 태그ID 갱신

상품을 구매 후에 (그림 3) mRFID 리더는 서버로부터 안전한 통신 채널을 통해 상품에 내장된 태그에 해당하는 키(K)와 정해진 난수(N)를 받는다. mRFID 리더는 주어진 K, N을 이용하여 $h_K(N)$를 생성하고 의사 난수 생성기 (PRNG : pseudo-random number gene- rator)를 이용하여 2개의 난수 r_i, s를 만든다. mRFID 리더는 ID 갱신 신호($Request1$)와 함께 $h_K(N)$, r_i, s를 보낸다. 태그는 가지고 있는 $h_K(N)$와 mRFID 리더가 보낸 $h_K(N)$을 비교하여 같으면 새로운 ID인 $N_ID_i = h_K(ID) \oplus h_K(s)$와 다음 통신에서 인증 과정에 사용 할 $h_K(r_i)$를 생성한다. 태그는 mRFID 리더에게 N_ID_i 보낸다. mRFID 리더는 태그로부터 받은 N_ID_i와 자신이 만든 $N_ID_i(h_K(ID) \oplus h_K(s))$가 같으면 mRFID 리더에 N_ID_i를 등록한다(그림 4).

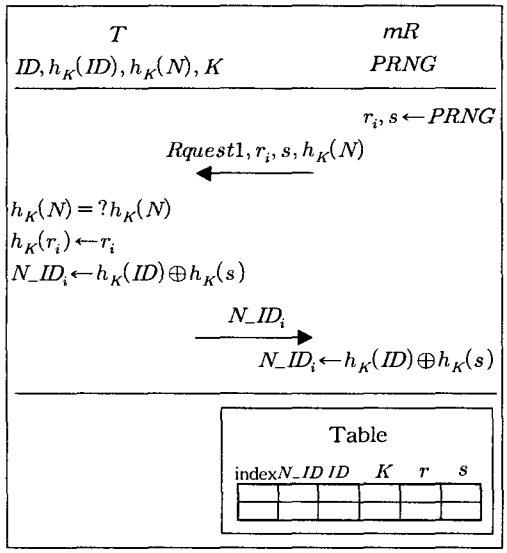

그림 4. 상품을 구매 후 태그ID 갱신.

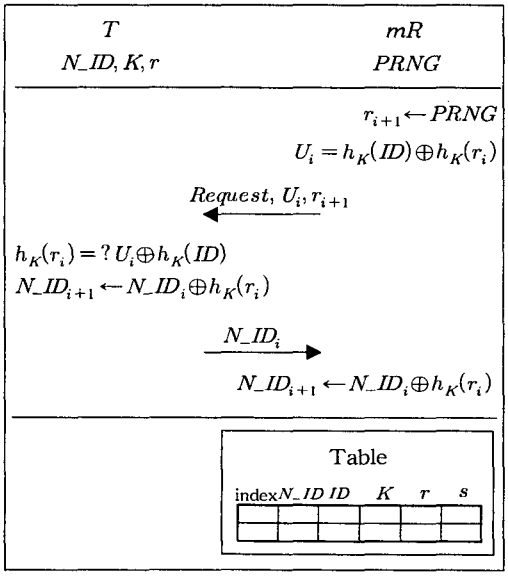

그림 5. 태그ID를 갱신 후 태그로부터 ID를 받는 과정1.

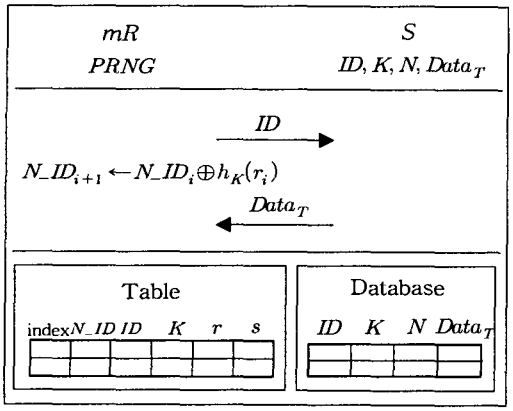

그림 6. 태그ID를 갱신 후 태그로부터 ID를 받는 과정2.

나. 태그ID 갱신 후 통신

태그ID를 갱신한 후 mRFID 리더가 태그로부터 정보를 읽어오기 위해 태그에게 신호(*Request*)와 함께 의사 난수 생성기로 생성한 r_{i+1}과 $h_K(r_i)$, $U_i(h_K(ID)\oplus h_K(r_i))$를 같이 보낸다. 태그는 mRFID 리더로부터 받은 정보를 가지고 ID를 갱신하기 전에 인증을 한다. 인증 과정은 mRFID 리더로부터 받은 U_i에 $h_K(ID)$를 XOR($U_i \oplus h_k(ID)$)하여 자신이 가진 $h_K(r_i)$와 같은 지 비교 하는 것이다. 비교하였을 때 틀리면 태그ID를 갱신하지 않고 같을 경우에만 태그 ID를 $N_ID_{i+1}(N_ID_i \oplus h_K(r))$로 갱신하고 mRFID 리더에게 N_ID_i를 보낸다. mRFID 리더는 N_ID_i를 태그로부터 받고 태그ID를 $N_ID_{i+1}(N_ID_i \oplus h_K(r))$로 갱신한다(그림 5). mRFID 리더는 가지고 있는 Table을 이용하여 N_ID_i에 해당하는 ID를 안전한 통신 채널을 통해 서버에게 전송한다. ID를 전달받은 서버는 mRFID에게 $Data_T$를 전송한다(그림 6).

III. 제안 기법의 안전성

본 절에서는 제안하는 모바일 RFID 시스템의 안전성에 대해서 논하고자 한다. 제안 기법에서는 구매자가 상품을 구매하여 태그ID를 갱신한 후에는 mRFID 리더가 태그와 통신을 할 때마다 태그를 읽을 권한을 가지는 mRFID 리더만이 태그의 정보에 접근 가능하다. 그러므로 제삼자는 태그의 정보에 대해서 알 수 없다. 또한 통신할 때마다 ID 값이 바뀌기 때문에 구매자의 mRFID와 태그사이의 통신을 제 삼자가 도청하더라도 매번 다른 난수만을 얻어낼 수 있어 위치 추적이 불가능하다.

IV. 결론

모바일 RFID 시스템은 무선 통신을 이용하여 상품을 인식하여 정보를 알아내기 때문에 물류, 유통, 재고 관리 등 넓은 분야에서 유용하게 쓰인다. 그러나 모바일 RFID 시스템의 환경 특성상 리더와 태그사이의 통신을 제 삼자가 도청 가능하며 이로 인해 개인 프라이버시 침해라는 문제점이 발생하게 된다. 본 논문에서는 이런 문제점을 해결하기 위한 기법을 제안하였다. 상품의 구매자만이 태그로부터 태그의 정보를 읽어 올 수 있으며 제 삼자에 의해 도청이 이루어지더라도 매번 다른 난수를 얻어 낼 수만 있어서 개인적인 정보가 누출되지 않으며 구매자의 위치추적 또한 불가능 하다.

[참고문헌]

[1] 박남제, "모바일 RFID 정보보호 표준화 동향 및 전망", TTA IT Standard Weekly, 2005.03

[2] Damith Ranasinghe, Daniel Engels, and Peter Cole, "Low-Cost RFID Systems: Confronting Security and Privacy" Auto-ID Labs Research Workshop, September 2004