대량의 RFID 태그에 적용할 수 있는 확장성 있는 랜덤 해쉬락 접근제어 프로토콜

오경희[O] 김호원
한국전자통신연구원
{khoh[O], khw}@etri.re.kr

Randomized Hash Lock Access Control Protocol for Mass RFID Tags

Kyunghee Oh[O] Howon Kim
Electronics and Telecommunications Research Institute

요 약

RFID는 기존의 바코드나 자기 인식 장치의 단점을 보완하고 사용의 편리성 향상으로 물류관리, 재고관리 등의 분야에서 활용 가능성이 비약적으로 증가되고 있는 차세대 핵심기술로 주목 받고 있다. 그러나 RFID 시스템이 활성화되기 위해서는 프라이버시 문제에 대한 해결책이 선행되어야만 한다. 해쉬락 기법은 리더가 태그를 인식하는 권한을 제어하여 임의의 리더가 태그 정보를 읽지 못하게 함으로써 프라이버시를 보호하는 기법이다. 본 논문은 기존의 해쉬락 기법에 의한 RFID 접근제어 프로토콜을 분석하고 취약점을 보완하여 대량의 태그를 사용하는 환경에서 도청자가 태그를 추적하지 못하도록 하는 접근제어 프로토콜을 제안한다.

1. 서 론

RFID(Radio Frequency Identification) 기술은, 사물의 식별정보 등을 극소형 태그에 장착하여 사물에 부착하고, 무선통신을 통해 리더 및 네트워크로 인식정보를 전달하는 무선인식기술로서, 기존의 바코드 시스템을 대체할 뿐만 아니라 센서 기술과의 융합을 통하여 차세대 정보통신 기술로 통칭되는 유비쿼터스 기술의 핵심요소로 부각되고 있다. 그런데 RFID 태그가 무선통신을 통하여 ID가 쉽게 식별된다는 점과 네트워크를 통하여 대량의 식별정보를 취급한다는 점에서 개인정보 유출 등의 심각한 프라이버시 침해가 일어날 수 있다. 이러한 문제점을 해결하기 위하여, RFID 보안 기술의 개발은 물론 관련법규를 마련해 강제적 규제방식을 취하거나 가이드라인을 제정하여 따르도록 하고 있다[1].

보안이 적용되지 않은 RFID/USN 기술은 개인 프라이버시 위협을 비롯한 다양한 문제점에 노출될 수 있다. 예를 들어, 태그가 부착된 소비자의 물건에 대한 추적을 통해 소비자의 위치 추적이 가능하며, 개개인이 가지고 다니는 물건들을 소비자 모르게 비밀리에 목록화하여 악용할 수 있다. 또한 태그가 출입 통제 시스템에 사용될 경우 악의적인 리더가 태그의 정보를 쉽게 읽어 들이고, 여기서 얻은 정보를 이용하여 태그를 위조하는 것이 가능하다. 이것은 태그의 정보에 대한 인증되지 않은 접근에서 비롯된다. 만약 태그의 메모리에 민감한 데이터가 저장되어 있다면, 이것은 심각한 보안 문제를 야기시킬 수 있다.

RFID 환경에서 발생하는 보안 문제는 도청, 트래픽 분석, 위조, 서비스 거부 공격 등이 있다. 이러한 보안 문제들을 해결하기 위하여 태그와 리더 사이에서 상호 신뢰할 수 있어야 하며, 인증되지 않은 리더로 정보가 유출되어서는 안되며, 재생공격(replay attack), 중간자 공격(man-in-the-middle attack) 등에 저항력이 있어야 한다[2]. 이러한 보안 문제를 해결하기 위한 다양한 연구가 진행되고 있다. 그 일환으로 RFID 시스템에서 사용자 프라이버시를 보호를 위해 kill tag, faraday cage, 방해 전파(active jamming), 블로커 태그 등과 같은 물리적 레벨의 대응 기법과 해쉬락, 재암호화 등과 같이 암호 기술을 이용한 보호 기법이 제안되고 있다. 본 논문에서는 기존의 해쉬락 보안 프로토콜을 분석하고 대량의 RFID 태그에 적용할 수 있는 랜덤 해쉬락 접근제어 프로토콜을 제안한다.

2. 해쉬락 RFID 접근제어 기술

AutoID센터가 제안한 킬 명령(Kill command) 기법, Faraday Cage 기술, 능동적 전파방해 기술, 블로커 태그 기술[3] 등의 방법들은 사용자가 직접 태그의 작동여부를 제어하는 방식이며 허가된 리더와 허가되지 않은 리더에 대한 접근 제어를 동시에 수행할 수가 없다. 그러나 암호학적 방법을 사용한다면 사용자가 직접 물리적으로 제어할 필요가 없으며, 리더에 대한 접근제어도 수행할 수 있다.

전통적인 공개키를 이용하는 방법은 태그의 제한된 컴퓨팅 파워라는 한계로 인하여 비현실적으로 판단된다. 그리고 네트워크 전체가 하나의 키를 공유하는 단순한 방법은 단지 하나의 태그가 훼손됨으로써 공유된 비밀키가 드러날 수 있고, 이에 따라 모든 태그의 정보가 유출될 수 있다[4]. 상대적으로 적은 컴퓨팅 파워를 사용하는 해쉬

함수를 이용하여 접근제어를 하는 방법은 다음과 같다.

2.1 해쉬락[5]

● 해쉬락의 잠금 과정

① 리더 R은 랜덤한 키 key를 선택하고, meta ID 값으로 hash(key)를 계산한다.
② R은 metaID를 태그 T에 기록한다.
③ T는 잠긴 상태(locked state)에 들어간다.
④ R은 (metaID, key)를 저장한다.

● 해쉬의 풀기 과정(그림 1 참조)

① 리더 R은 태그 T에게 T의 metaID를 질의한다.
② R은 데이터베이스에서 (metaID, key)를 조사한다.
③ R은 T에게 key를 전송한다.
④ 만약 hash(key)와 metaID가 일치하면, T는 잠긴 상태에서 빠져 나온다(unlock).

일방향 해시 함수의 역함수 계산 어려움에 기반한 해쉬락 스킴은 인가 받지 않은 리더가 태그 정보를 읽는 것을 방지한다. 위장(spoofing)은 방지하지 못하지만 탐지는 가능하다. 공격자는 태그에게 metaID를 요구한 후에 재전송 공격(replay attack)에서 합법적 리더에게 태그를 위장하는 것이 가능하다. 그러면 합법적 리더는 위장된 태그에게 키를 주게 된다. 그러나 리더는 태그의 콘텐츠(일반적으로 태그의 ID)를 체크하여 백엔드 데이터베이스로부터 적절한 metaID인지를 검증할 수 있다. metaID가 부적절한 경우, 리더는 적어도 위장이 발생했음을 경고할 수 있다.

해쉬락은 태그에 해쉬 함수의 구현만을 요구하고, 백앤드에 키관리를 요구한다. 이러한 요구 조건은 가까운 장래에 경제적인 것이 될 수 있다. 그러나, 위 방식에서는 metaID가 식별자처럼 사용되기 때문에 사용자 추적(tracking of individuals)이 가능하다.

2.2 랜덤 해쉬락[5]

해쉬락 기법에서 가능한 사용자 추적을 방지하기 위한 방식이다. 태그는 인가되지 않은 사용자에 의한 질의에 대하여 예상 가능한 응답을 하지 않지만, 합법적인 리더에 의해서는 여전히 식별 가능해야 하는 방식이다. 이 기법에서는 태그에 일방향 해시 함수와 난수발생기(PRNG)가 구축되어 있어야 한다. 합법적인 리더는 태그를 스캔하기 전에 " knows what she owns" 를 가정한다. 태그를 잠금 상태로 만드는 것은 프로토콜이 필요 없는 간단한 과정이나, 태그를 풀림 상태로 하는 프로토콜은 필요하다. 태그를 풀림 상태로 하는 프로토콜은 다음과 같다.

● 랜덤 해쉬락의 풀기 과정(그림 2 참조)

① 리더 R은 태그 T에게 질의를 보낸다.
② T는 랜덤한 난스(nonce) R을 생성하고, hash(ID_T ‖ R) 값을 계산한다.
③ T는 R에게 (R, hash(ID_T ‖ R))을 전송한다.
④ R은 모든 알려진 ID_i 값에 대해 hash(ID_i ‖ R)을 계산한다.
⑤ 만약 hash(ID_i ‖ R) == hash(ID_T ‖ R)을 만족하는 ID_i를 찾는다면, R은 T에게 ID_i를 전송한다.
⑥ 만약 ID_i와 ID_T가 일치한다면, T는 잠긴 상태에서 빠져 나온다.

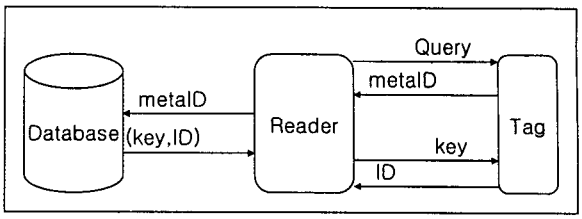

그림 1. 해쉬 기반 접근 제어 풀기 과정

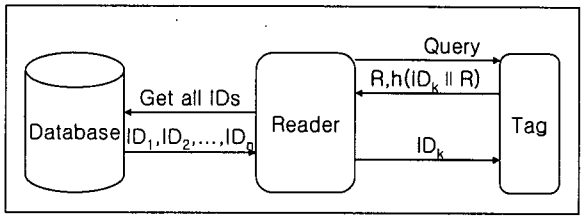

그림 2. 랜덤 접근 제어 풀기 과정

이 방식은 초당 100~200개의 태그를 읽어야 하는 많은 개수의 태그를 소유한 환경에서는 비현실적이다. 그러나 상대적으로 적은 수의 태그 사용자를 갖는 환경에서는 가능한 방식이다. 소매 상점은 일반 사용자에 비해서 위치 프라이버시와 연관성이 적기 때문에 소매 상인들은 해쉬락 기법을 적용하고, 구매하는 소비자에게는 랜덤 해쉬락 기법을 적용한다.

위 방식이 충분히 현실적이지만 이론적으로 완벽하지는 않다. 이는 일방향 함수의 정의가 역함수 계산의 어려움만을 의미하기 때문이다. ID 비트가 노출되지 않는 방법이 제공되어야 한다.

3. 확장성 있는 랜덤 해쉬락 접근제어

해쉬락 기법은 metaID에 의한 사용자 추적이 가능하다는 문제가 있다. 그리고 랜덤 해쉬락 기법은 사용자 추적이 불가능 하지만, 사용하는 태그의 수에 제한이 있다는 단점이 있다. 제안하는 해쉬락 기법은 이 두 가지 기법의 절충으로서, 사용하는 태그의 수에 제한을 없애면서도 사용자 추적이 어렵게 하는데 목적이 있다.

리더는 데이터베이스에 N개의 키를 가지고 있다. 각 태그는 N개의 키 중 임의의 하나의 키를 자신의 키로 설정한다. 제안하는 프로토콜에서 리더가 태그의 인식하는 과정에서 N개의 키에 대하여 모두 해쉬 계산을 수행하므로, N의 크기는 리더가 신속히 처리할 수 있을 정도로 충분히 작은 값이어야 한다. 그러나 N 값이 너무 작으면 임의의 두 태그가 같은 키를 공유할 가능성이 커진다.

제안하는 해쉬락 기법의 풀기 과정은 다음과 같다. 이때 난수 값들과 해쉬 값, 태그의 ID 및 키들의 비트 크기가 모두 동일하다고 가정한다.

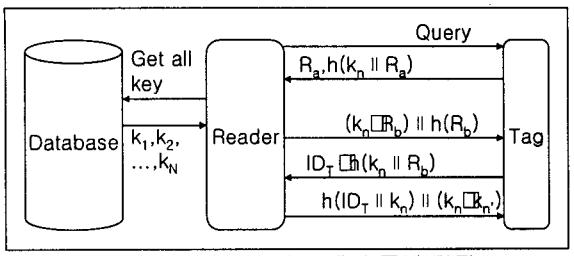

그림 3. 제안된 접근 제어 풀기 과정

● 제안하는 해쉬락의 풀기 과정(그림 3 참조)

① 리더 R은 태그 T에게 질의를 보낸다.

② T는 난수 R_a을 생성하고, 자신의 키 k_n을 사용하여 $hash(k_n \| R_a)$ 값을 계산한다.

③ T는 R에게 $R_a \| hash(k_n \| R_a)$을 전송한다.

④ R은 모든 알려진 k_i 값에 대해 $hash(k_i \| R_a)$을 계산한다.

⑤ 만약 $hash(k_i \| R_a) == hash(k_n \| R_a)$을 만족하는 k_i를 찾는다면, R은 난수 R_b 를 생성하고T에게 $(k_n \square R_b) \| hash(R_b)$를 전송한다.

⑥ 만약 T가 전송 받은 $(k_n \square R_b)$에 대하여 $hash((k_n \square R_b) \square k_n)$을 계산한 값과 전송 받은 $hash(R_b)$ 값과 같으면 T는 R에게 자신의 ID_T를 사용하여 $(ID_T \square hash(k_n \| R_b))$을 전송한다.

⑦ R은 저장중인 키들 중 임의의 키 $k_{n'}$을 선택하고 $hash(ID_T \| k_n) \| (k_n \square k_{n'})$을 T에 전송한다.

⑧ 만약 T가 전송 받은 $hash(ID_T \| k_n)$ 값과 T가 직접 $(ID_T \| k_n)$을 해쉬 계산한 값이 같으면, T는 잠긴 상태에서 빠져 나온다. 그리고, 전송 받은 $(k_n \square k_{n'})$ 값에 대하여 $(k_n \square k_{n'}) \square k_n$ 값, 즉 $k_{n'}$ 값으로 키를 갱신한다.

이 과정을 좀더 구체적으로 설명하면, ③~⑤ 과정에서 키를 외부에 유출하지 않고 R은 T의 키를 찾아낼 수 있다. 또한 ⑤ 과정은 T가 N개의 키 중 적어도 하나를 알고 있음을 의미하며, 이는 T에 대한 인증이 된다. ⑥ 과정에서 T는 R이 키 k_n을 알고 있음을 검증하여 접근 권한을 판단한다. ⑦ 과정에서 R은 T의 ID를 읽어오게 된다. ID_T 값은 키와 난수의 해쉬값과 XOR 연산으로 암호화 되므로 도청을 막는다. 이때 도청자가 ID_T 값을 알고 있다 하더라도 k_n이 유출되지 않는다. ⑧ 과정은 태그의 잠금을 해제하고 키를 갱신하는 과정이다. $(ID_T \| k_n)$의 해쉬는 R이 k_n을 알고 있음을 보장하며 갱신될 키 값 며, $k_{n'}$ 은 $(k_n \square k_{n'})$으로 암호화 되어 전송된다. 여기서 키의 갱신이 불필요하다면 $(k_n \square k_{n'})$은 생략될 수 있다. 이러한 과정을 통하여 R은 T의 ID와 키를 유출하지 않으면서, 잠금을 해제할 수 있다.

4. 결론

RFID 시스템이 유통물류 분야에서 널리 사용될 것으로 예상되고 있지만, 그 응용이 소비자에 대한 서비스로 이어지기에는 개인정보 유출과 같은 보안의 문제가 남아있다. 만약 도청 등의 방법으로 태그에 담겨있는 정보가 유출되는 것을 막을 수 있다면, RFID가 보다 다양한 응용 환경에서 사용되어질 수 있을 것이다.

RFID 태그라는 제한된 컴퓨팅 파워를 가진 환경에 기존의 암호알고리즘을 적용한 보안 프로토콜을 적용하는 것은 어려운 일이다. 이러한 문제를 해결하기 위하여 암복호 알고리즘을 전혀 사용하지 않고, 일방향 해쉬 함수와 난수 발생기만을 사용하여 태그에 대한 접근을 제어하는 해쉬락 기법이 MIT 연구진에 의해 제안되었다. 그러나, ID에 의한 추적이 가능하다던가, 혹은 사용할 수 있는 태그 수의 제한과 같은 한계가 있다.

본 논문에서 제안하는 방법은 이러한 추적이나 확장성의 문제를 해결하기 위한 프로토콜이다. 키와 난수, 그리고 해쉬를 사용하여 태그의 ID와 키를 암호화하며, 여러 태그에 중복된 키를 사용함으로써 제한된 수의 키만으로도 태그의 수에 상관 없는 키관리가 가능하게 된다. 또한 도청에 의한 ID의 유출을 막고, 도청자가 사전에 태그의 ID 값을 알고 있다 하더라도 키를 역산출할 수 없게 하며, 키의 갱신도 가능한 방법을 제공한다. 단점이 있다면, 어느 하나의 키가 유출이 되었을 때 동일한 키를 사용하는 다른 태그들에 대한 위협이 된다는 점과, 키 갱신과정에서 또 다른 키가 도청에 의해 유출될 수 있다는 점이다. 따라서 제안된 해쉬락 방법을 사용하는 환경에서는 키들이 유출되지 않도록 하는 보완책이 강화 되어야 한다. 특히 다수의 키가 한꺼번에 유출될 가능성이 낮은 환경에서 사용하여야 한다.

참고문헌

[1] 오길영, " 개인정보보호를 위한 RFID 규제에 관한 연구" , 정보화정책, 제12권 제2호, p.47-69, 2005.

[2] 김광조, " RFID/USN 정보보호" , TTA저널, 제95호, 2004. 10.

[3] 주학수, " RFID 시스템의 보안 및 프라이버시 보호를 위한 기술 분석" , 전자정보센터, 2004. 6.

[4] 홍도원, 장구영, 박태준, 정교일, " 유비쿼터스 환경을위한 암호 기술 동향" , 전자통신동향분석, 제20권 제1호, 2005. 2.

[5] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, " Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, " First International Conference on Security in Pervasive Computing, 2003.