한국산학기술학회논문지
Vol. 8, No. 1, pp. 33-40, 2007

사용자 프라이버시 보호를 위한 해쉬 기반의 안전한 RFID 인증 프로토콜

이한권[1*], 조태경[1], 유현중[1], 박병수[2]

Hash based Secure RFID Authentication Protocol for User Privacy Protection

Han-Kwon Lee[1*], Tae-Kyung Cho[1], Hyun-Joong Yoo[1] and Byoung-Soo Park[2]

요 약 RFID는 비접촉식 무선 인식 기술로서 유통, 물류 분야 및 산업전반에서 바코드를 대체할 기술로 주목을 받고 있다. RFID의 많은 장점에도 불구하고 본격적으로 실용화되기까지는 극복해야할 문제들이 있다. 그 중에서 가장 중요한 것은 사용자 정보 보호 문제 해결이다. 보안 기능이 없는 RFID 시스템은 개인의 신상정보가 노출이 되는 등 사용자의 프라이버시가 유출되는 위험을 갖게 된다. 본 논문에서는 보안 문제를 해결하기 위한 RFID 시스템 상호 인증 프로토콜을 제안한다. 안전한 인증 프로토콜을 통하여 태그에게 동적 ID를 제공함으로써 사용자의 프라이버시를 보호하는 것을 목적으로 한다. 백엔드, 리더, 태그 사이의 전송되는 정보는 태그의 ID와 직접적인 연관성이 없고, 일방향 해쉬함수를 이용하여 인증을 수행함으로써 송수신되는 정보를 이용하여 공격자가 태그의 정보를 획득할 수 없도록 한다.

Abstract RFID, a non-contact wireless identification technology is being noticed as a technology to alternate barcode system in distribution industry and general industry. Despite of merit of RFID, there are issues to be solved for practical use. One of them, which are most important, is resolution of user's information protection. RFID system without security function bears risk exposing personal data and user's privacy. In this paper, we propose mutual authentication protocol for RFID system in order to solve this security issue. This study aimed to protect user's privacy by providing dynamic ID for tag through authentication protocol safe from security threats. Information being transmitted between backend, reader and tag has no direct connection with ID of tag, and it conducts authentication process using one-way hash function, which prevents attacker's obtaining of tag information using information being transmitted.

Key Words : RFID, Security, Hash, 인증 프로토콜, 프라이버시

1. 서론

국내외에서 많은 관심의 대상이 되는 RFID 기술은 USN 기술과 더불어 유비쿼터스 환경을 현실화하는 기술로서, 유통 및 물류, 자동차, 의료 등 산업체 전 분야에 걸쳐 다양하게 응용 될 수 있다. 일반적으로 RFID 시스템은 크게 RFID 태그와 리더, 그리고 백엔드 데이터베이스로 구성되며, 수 미터의 거리에서도 초당 수백 개 이상의 태그를 한꺼번에 읽을 수 있다. RFID 기술은 기존의 바코드 시스템을 대체할 수 있는 기술로 응용 범위가 매우 넓다[7]. 하지만, 보호되지 않은 태그가 부착된 상품은 쉽게 모니터링 되고 사용자의 위치를 추적할 수 있기 때문에 RFID 기술에 대한 프라이버시 및 정보보호 문제가 발생하게 되며, 이에 적합한 새로운 정보보호 기술 개발도 필요하게 된다. 하지만 RFID 태그의 하드웨어 제약으로 인해 기존의 암호 알고리즘을 기반으로 하는 정보보호 기술을 RFID에 쉽게 적용하기는 어렵다[11].

본 연구보고서는 정보통신부의 IT SoC 핵심설계인력양성 사업을 통한 연구비 지원으로 수행한 정보통신연구개발사업의 연구결과입니다.
[1]상명대학교 정보통신공학과
[2]상명대학교 컴퓨터시스템공학과
*교신저자: 이한권(Leehk0131@smu.ac.kr)

적절한 정보보호 기술을 사용하지 않은 RFID 태그는 기존의 보안 공격 기법인 도청, 스푸핑, 서비스거부 등의 공격에 취약하며 이러한 공격으로 사용자의 개인 정보와 관련 있는 민감함 정보들이 누출될 수 있다. 또한, 위치 프라이버시 및 운송 데이터에 대한 위협도 가능하기 때문에, 적절한 접근 제어와 인증 과정을 통해 허용된 자만 태그 데이터를 읽을 수 있도록 해야 한다. 그리고 태그 내용이 보호되더라도 태그를 소유한 사람을 추적할 수 있고 여러 개의 리더로부터 정보를 가공하여 위치와 거래 정보를 추적할 수 있으므로 이에 대한 적절한 정보보호 기술도 함께 개발 되어야 한다[9].

본 논문에서는 위에서 언급한 보안 위협으로부터 사용자의 프라이버시를 보호할 수 있는 인증 프로토콜을 설계한다. 백엔드 서버로부터 리더와 태그를 인증하고, 태그에게 동적 ID를 생성함으로써 위치추적 등과 같은 보안 문제를 해결한다. 제안하는 프로토콜 동작 과정에서는 난수 및 키 인덱스와 같이 태그 ID와 직접적인 관련이 없는 정보들을 송수신하며, 데이터들을 일방향 해쉬함수를 이용하여 해쉬된 값들만을 전송하기 때문에 공격으로부터 안전할 수 있다.

2. RFID 시스템 보안 위협

RFID 태그가 모든 사물에 부착되어 일상화될 경우, 개인정보(Privacy) 침해 및 정보 유출에 따른 보안 문제가 중요한 사회적 이슈로 대두될 것이 확실시된다. RFID 기술은 리더와 태그사이에 물리적인 접촉 없이 인식 가능하고 태그의 정보가 전송과정에 무선특성에 따른 과도한 정보 노출과 사용자의 위치정보 추적과 같은 심각한 프라이버시 침해를 유발시킨다. 이러한 우려들이 RFID의 상용화에 걸림돌이 되며, 성공적인 산업화를 위해서는 제반 프라이버시 문제를 해결해야 하는 것이 선결 과제로 되고 있다.

다음은 RFID 시스템에서 문제가 되고 있는 보안 위협들이다[1].

■ 도청 (Eavesdropping)

RFID 시스템은 바코드 시스템과 달리, 효율성을 높이기 위해 수 미터의 범위 내에서도 리더와 태그간에 통신이 가능하도록 되어 있다. 이러한 특징은 악의적인 사용에 의해 보안 문제점을 노출시킨다. 공격자로부터 위협요소들은 다음과 같은 방법들이 있다.

■ 서비스 거부 (DoS, Denial of Service)

리더와 태그간에 질의와 반응의 메커니즘이 존재한다. 이러한 특징을 이용하여 공격자가 리더를 가지고 수많은 질의를 리더 및 태그에게 보낸다면 리더와 태그는 많은 질의에 대해서 일일이 반응해야 된다. 이는 너무 많은 계산이 요구되고, 리더와 태그가 정상적인 기능을 못하게 만드는 결과를 초래한다. 서비스 거부 공격은 RFID 시스템이 작동을 못하도록 하는 위협이다.

■ 스푸핑 (Spoofing)

스푸핑은 외부의 악의적 침입자가 자신이 사전에 지정한 코드가 작동되도록 함으로써 사용자의 권한을 획득하는 해킹 기법이다. 일반 사용자의 태그를 스푸핑한 공격자는 자동화된 체크아웃 혹은 보안 시스템을 속일 수 있으며, 스푸핑된 데이터로 값싼 물품과 비싼 물품을 교체할 수 있다.

■ 위치추적

태그가 고정된 ID를 가지고 있고, 공격자가 다수의 리더기를 이용하여 그 ID의 위치 변화를 감시하는 경우 태그 소유자의 이동경로를 파악할 수 있다[2].

■ 세션 가로채기(Hijacking), 재생(Replay) 공격, 중간자 공격 (Man In the Middle Attack)

RFID 리더와 태그사이의 상호인증을 위한 인증 프로토콜 수행 시 발생할 수 있는 공격들로, 인증된 세션을 가로채는 세션 가로채기 공격, 공격자가 검증자에게 이전에 수행되었던 프로토콜 부분 중 일부분을 다시 실행시키는 재생 공격, 공격자가 인증 프로토콜 수행 중간에 자신의 정보를 삽입하는 중간자 공격 등이 있다.

3. RFID 시스템에서 정보 보호를 위한 기존 연구

3.1 인증 및 추적 방지

태그가 리더를 인증하는 방법이 제공되면, 도청자에 의하여 태그 정보가 유출되는 것을 방지할 수 있다. 그리고 RFID의 추적을 방지하기 위해선 태그에서 리더로 전송되는 데이터를 난수화하거나 익명성 기술의 사용, 혹은 리더를 인증함으로써 합법적인 리더만 읽을 수 있도록 제어하면 된다.

가. 랜덤화된 해쉬 락 (Randomized Hash Lock) 기법

RFID 추적 방지 기술로 볼 수 있는 랜덤화된 해쉬 락 기술은 리더가 태그를 읽을 때 마다 태그에서 발생한 난수값에 의해, 태그는 다른 값을 리턴하게 된다. 이후, 리더는 DB로부터 모든 ID 값을 가지고 와서, 리더에서 해쉬를 수행하여 태그로부터 수신한 값과 비교하여 해당 ID 값을 찾는다. 이 기법은 리더에서 해쉬 함수를 반복적으로 수행할 필요가 있으며 ID에 대한 brute force look up의 필요성, 태그에는 해쉬 함수 외에 난수 생성기를 저가 및 저전력으로 설계해야 한다는 부담이 있다.

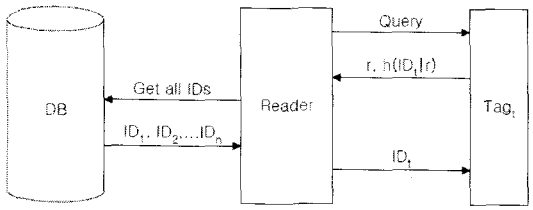


그림 1. 랜덤화된 해쉬 락 기법

나. 해쉬 체인(Hash Chain) 기법

해쉬 체인 기법은 태그에서 난수를 사용하지 않고도 태그 소유자의 프라이버시를 보호할 수 있다. 출력되는 값은 해쉬된 값이고 동작시 그 출력값이 계속 바뀌므로 역추적을 방지할 수 있게 된다. 리더와 태그는 초기에 ID 값과 초기 비밀값 S를 가지고 리더에는 G 함수로 해쉬처리된 값을 출력하며 비밀값은 H 해쉬로 갱신된다. 이 때 서버는 저장된 모든 태그의 S 값을 해쉬함으로서 해당 ID를 검출한다. 이는 서버에 해당 ID 값을 찾기 위해선 해쉬 함수를 반복적으로 수행해야 한다는 것을 의미한다[6].

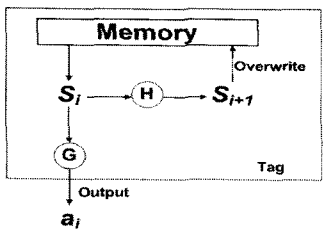


그림 2. 해쉬 체인 기법

3.2 도청 방지

가. Universal Re-encryption 방식을 사용한 Variable ID

이 기법은 Universal re-encryption 방식과 one-time pad에 기반하는 것으로 태그값이 매 출력때마다 달라지며, Elgamal에 기반한 Universal re-encryption을 적용한 공개키 암호 시스템을 사용한다. Universal re-encryption 기법은 공개키를 모르는 상황에서도 암호화가 가능하므로 이 때문에 키의 발생 및 분배, 관리가 필요 없다. 동작방식을 보면 각 태그는 비밀키 xt와 공개키 yt 값을 생성하고 DB에 각 태그의 (xt, IDt)를 저장한다. 리더는 각 태그의 암호문 C와 난수 값을 사용해서 one-time pad를 생성하고 초기에 one-time pad 값과 암호문 값은 태그에 저장되고 그 다음부터 이 값을 갱신한다. 리더(서버)가 태그로부터 암호문을 받으면 서버는 해당 ID가 식별 될 때까지 DB에 저장된 모든 태그의 비밀키를 이용하여 복호화를 수행한다. 태그가 리더로 다시 신호를 보낼 때 one-time pad에서 2개의 값을 선택해서 암호화를 수행한다. 이 때 공개키 값을 사용하지 않는다.

나. Silent Tree-Walking

기존의 tree-walking 프로토콜에서는 리더에서 broadcast되는 신호만으로 태그의 ID 추론이 가능하다. [그림 3]과 같이 backward range 밖 그리고 forward range 안에 도청자가 있다고 가정할 때, 도청자는 리더가 태그에게 보내는 매시지를 엿들을 수 있으나 태그에서 리더로 전송되는 신호는 들을 수 없게 된다. Silent tree-walking은 리더에서 태그로 가는 전방향 신호가 도청되더라도 태그에서 리더로 전송되는 신호만 도청되지 않는다면, 도청자가 태그의 ID를 추론하지 못하게 하며, 실행 시간에 있어서도 일반 binary tree-walking과 동일한 알고리즘을 갖는다.

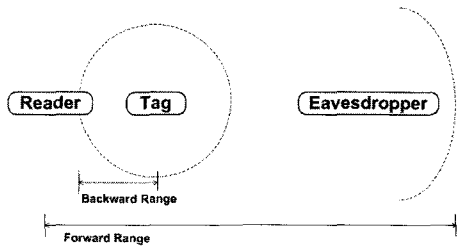


그림 3. Forward Range와 Backward Range

다. Randomized Tree-Walking

랜덤 트리워킹은 태그가 랜덤한 수를 생성하여 이를 리더에 보내고 이를 기초(Portion)로 하여 트리워킹을 시도하는 방식이다. 태그는 반드시 자신이 생성했던 랜덤한 수를 기억하고 있어야 하며, 난수 발생기를 가지고 있고 전원이 끊어지지 않도록 해야 한다는 제약사항이 있다.

4. 프라이버시 보호를 위한 RFID 보안 프로토콜

본 논문에서 제안하는 프로토콜은 태그, 리더와 백엔드간에 인증 과정에서 해쉬함수를 사용하였다. 현재 많은 논문들에서는 리더와 백엔드간을 안전한 채널로 간주하여 상호간에 인증절차를 생략하기도 한다[10]. 하지만, 핸드헬드(handheld) 리더와 같이 무선으로 백엔드와 통신하는 리더들은 도청과 같은 위협으로부터 노출되어 있다. 따라서 본 논문에서는 각 구성요소들 사이를 안전하지 않은 채널로 간주하고 서로간에 인증을 하는 과정을 제안한다.

본 논문에서는 해쉬함수를 이용하여 강력한 보안 성능을 제공하면서 태그에게 새로운 ID를 부여한다. 제안한 RFID 보안 프로토콜에서 태그와 리더, 백엔드간에 전송되는 정보들은 난수와 키 인덱스, 암호화된 데이터들이기 때문에 도청이나 위치 추적 등의 공격으로부터 안전하다. 또한, 본 프로토콜에서는 상호 인증을 기반으로 하고 있기 때문에 상대방과 동일한 키를 가지고 있지 않고서는 상대방을 속일 수 없으므로, 스푸핑 공격이나 재생 공격으로부터 안전하다.

4.1 사전 준비단계

백엔드와 리더, 태그 모두 기본적으로 해쉬함수를 내장하고 있다. 다만, 차이점은 태그에서는 일반 해쉬함수를, 리더에서는 키 값을 가지는 해쉬함수, 백엔드에서는 두 가지 모두를 갖는다. 또한, 각 구성요소들은 XOR 연산기를 가지고 있어야 하며, 리더는 난수 발생기(RNG, Random Number Generator)를 내장하고 있다.

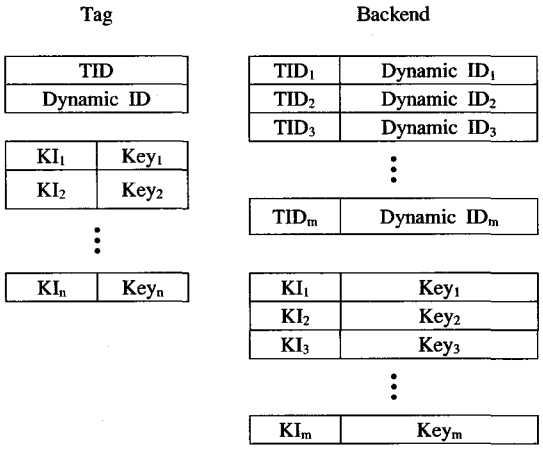


그림 4. 태그 및 백엔드 저장 정보

인증단계에 앞서 태그와 리더 및 백엔드는 인증에 필요한 여러 가지 정보들을 저장해 둔다. [그림 4]에서와 같이 태그는 인증 과정과 새로운 ID 생성에 필요한 키들과 그 키들을 가리키는 키 인덱스를 미리 저장하고 있다. 백엔드 역시 모든 태그들이 가지고 있는 키 값들과 키 인덱스들을 데이터베이스에 저장하고 있어야 한다. 또한 태그는 자신의 고유 ID(TID)와 동적 ID(Dynamic ID)를 저장하고 있으며, 동적 ID는 인증 과정 종료 후에 태그가 새로 생성하는 ID이다. 백엔드는 태그의 고유 ID와 동적 ID 쌍을 저장하고 있어야 한다.

4.2 제안 프로토콜 인증 과정

사전 준비단계에서 부여된 비밀키와 난수 발생기, 해쉬함수 등을 이용하여 태그와 리더에 대한 백엔드의 인증과정을 거치며 데이터 전송에 사용될 동적 ID를 할당받는다. [그림 5]는 프로토콜의 동작 흐름을 나타내고 있다. 본 프로토콜은 태그 인식 과정에서 선택된 하나의 태그와 리더, 백엔드 간에 동작한다. 동작과정은 다음과 같다.

① 리더는 난수 발생기로부터 랜덤한 값 R을 생성한다. 생성된 난수 R을 해쉬하여 Q를 도출한다. 이때 사용되는 해쉬함수는 백엔드와 리더간의 비밀키 k를 이용하는 키 값을 가지는 해쉬함수이다. 여기서 키 값을 가지는 해쉬함수를 이용하는 것은 백엔드로부터 리더를 인증하기 위한 것이며, 이는 허락되지 않은 리더로부터의 불법적인 침입을 방지하기 위함이다. 리더는 태그 인식 과정을 통하여 선택된 태그에게 Q를 전송한다.

$$Q = h_k(R)$$

② 태그는 리더로부터 받은 Q와 태그가 가지고 있는 키들 중에 하나를 임의로 선택하여 RES를 계산한다. RES를 생성하는데 있어 Q와 임의의 키 값 K_i를 XOR 연산을 하는 이유는, 재생공격을 막기 위해서이다. RES가 정상적으로 생성되면 태그는 K_i에 해당하는 키 인덱스 KI와 함께 RES를 리더에게 전송한다.

$$RES = h(Q \oplus K_i)$$

③ 리더는 태그로부터 받은 RES, KI와 함께 난수 R과 R을 해쉬 한 Q를 백엔드에게 전송한다. 백엔드는 리더가 가지고 있는 키를 이용하여 전달받은 R을 해쉬하고 그 결과가 Q와 동일한지 확인한다. 만약,

동일하지 않다면 불법적인 리더로 간주하고 통신을 중단한다. 결과가 동일하다면 정당한 리더로 판단하고 리더에 대한 인증을 완료한다. 백엔드는 다시 전달받은 KI_i에 해당하는 키 K_i와 Q를 XOR한 값을 태그와 동일한 해쉬함수로 해쉬한 값과 전달받은 RES가 동일한지 판단한다. 동일하다면 정당한 태그로 인정하고, 그렇지 않다면 불법적인 태그로 간주하여 통신을 종료한다.

④ 위 단계에서 리더와 태그에 대한 인증 절차를 마치고 백엔드는 앞으로 태그와 정보전송시 사용하게 될 $DynamicID$를 생성한다. $DynamicID$는 태그가 가지고 있는 임의의 비밀키 2개와 태그의 고유 ID인 TID를 XOR 연산하여 계산한다. 백엔드는 $DynamicID$ 연산에 사용된 키 중 하나를 해쉬하여 M_1을 생성하고, $DynamicID$ 연산에 사용된 키에 해당하는 두 개의 키 인덱스 KI_j, KI과 함께 리더로 전송한다.

$$DynamicID = TID \oplus K_j \oplus K_l$$
$$M1 = h(K_j)$$

⑤ 리더는 백엔드로부터 전달받은 M_1, KI_j, KI_l를 태그에게 전달하고, 태그는 KI_j에 해당하는 키 K_j를 해쉬하여 리더로부터 전달받은 M_1과 비교하여 동일한지 확인한다. 그 후에 두 개의 키 K_j, K_l와 태그 고유의 ID인 TID를 XOR 연산하여 앞으로 백엔드 및 리더와 통신시 사용하게 될 새로운 ID($DynamicID$)를 생성한다.

⑥ 성공적으로 $DynamicID$가 저장이 완료되면 태그는 K_l을 해쉬하여 M_2를 생성하고 백엔드로 전송한다.

$$M_2 = h(K_l)$$

⑦ M_2를 전송받은 백엔드는 자신이 K_l을 해쉬한 값과 비교하여 동일할 경우 태그의 ID 갱신이 성공적으로 완료되었음을 인식하고 인증 프로토콜을 종료한다. 이후에 태그와 백엔드간에는 $DynamicID$를 이용하여 데이터를 송수신한다.

4.3 프로토콜 안전성 및 성능 분석

본 절에서는 앞에서 설명한 RFID 인증 프로토콜의 안정성을 분석한다. 앞에서 설명했던 RFID 시스템의 보안 위협으로부터 제안하는 프로토콜의 안전성 여부를 판단한다.

■ 도청으로부터 안전성 분석

백엔드와 리더, 태그 사이에 전송하는 정보들은 난수 R과 키 인덱스(KIi, KIj, KIl), 해쉬된 정보(M_1, M_2, RES)들이다. 이러한 정보들은 태그에 새롭게 부여되는 ID와 직

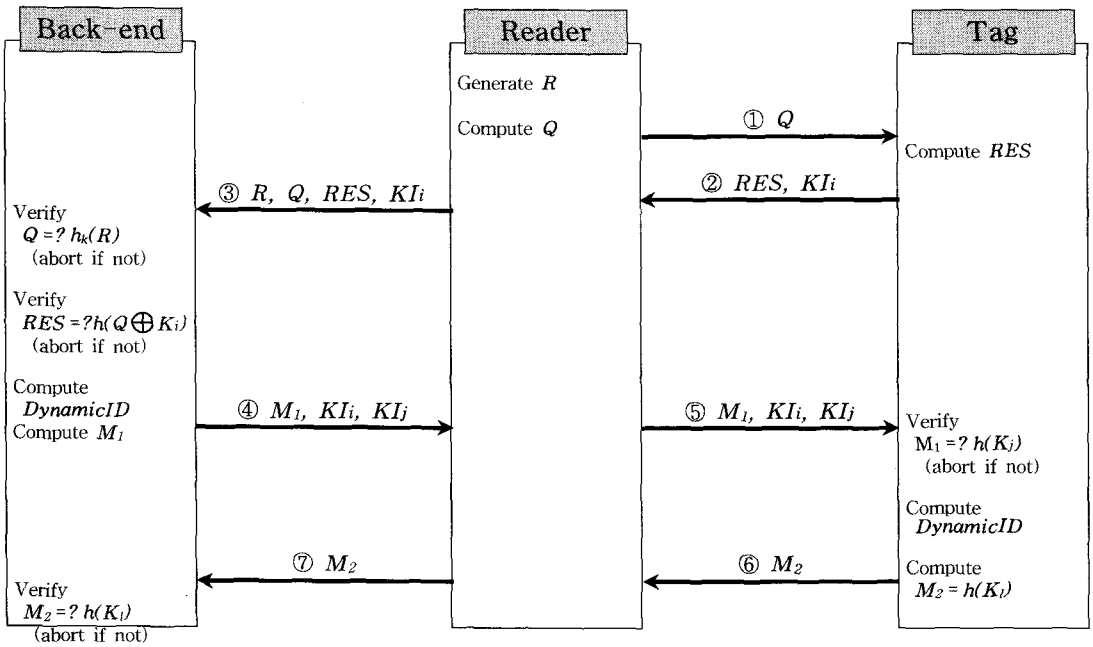


그림 5. 인증 프로토콜

접적인 상관관계가 없다. 키 인덱스에 해당하는 키 값들은 태그와 백엔드만이 알고 있기 때문에 키 인덱스만을 이용하여 키 값을 알아내는 것은 불가능하다. 뿐만 아니라, 새로운 ID를 생성하는데 사용하는 키는 매번 바뀌기 때문에 장시간에 걸친 도청이라 하더라도 ID를 알아내기는 정보가 불충분하다. 그리고, 해쉬함수의 특성상 해쉬된 정보들을 해독하여 원래 정보를 획득하는 것은 불가능하다.

■ 스푸핑으로부터 안전성 분석

본 논문에서 제안한 프로토콜은 백엔드, 리더, 태그 모두 상호간에 인증을 기반으로 하고 있다. 상대방과 동일한 키를 가지고 있지 않고서는 상대방을 속일 수 없다. 공격자가 리더로 가장하였을 경우, 난수 R은 발생시킬 수 있지만 리더와 백엔드가 가지고 있는 동일한 키 값을 알 수 없기 때문에 해쉬함수로 R을 암호화할 수 없다. 임의의 키로 R을 해쉬하여 전송했을 경우에는 단계 ③에서 백엔드가 계산한 결과와 다르기 때문에 이후에 인증절차는 종료된다. 공격자가 정당한 태그로 가장하였을 경우에도 마찬가지로 키 인덱스 *KI*와 *KI*을 이용하여 새로운 ID를 생성해야 하는데 키 인덱스만으로 키 값을 알아내는 것은 불가능하다.

■ 위치추적으로부터 안전성 분석

본 프로토콜에서는 상호 인증 과정과 새로운 ID를 생성하는 과정에서 EPC code와 같이 태그의 정보를 직접적으로 제공하는 데이터의 송수신을 원칙적으로 제한한다. 태그 고유의 정보인 TID와 새로 생성된 *DynamicID*와의 상관관계는 오직 태그 자신과 백엔드만이 알 수 있다. 뿐만 아니라, 기존의 존재하던 *DynamicID*와 새로 부여된 *DynamicID*간의 상관관계가 전혀 없기 때문에 위치 추적은 불가능하다. ISO 18000-6 Type C에서는 태그 충돌 중재 및 인식 과정에서 각각의 태그들은 난수를 생성하여 경쟁하게 되고 하나의 태그가 선택되면 EPC를 전송하게 된다[5]. 이럴 경우, 정보가 노출되어 위치 추적을 당할 수가 있다. 여기서, EPC와 같은 태그의 고유 ID 대신에 *DynamicID*를 이용하면 위치 추적을 피할 수 있다. *DynamicID*를 전송한 후에 바로 제안한 프로토콜이 동작하게 되고, 그러면 태그는 곧바로 새로운 *DynamicID*를 생성하고 백엔드와 통신할 때 이 정보를 이용한다.

■ 재생 공격, 중간자 공격으로부터 안전성 분석

인증 프로토콜 동작 과정 중에 단계 ③에서 중간자 공격으로부터 안전하기 위하여 난수 *R*과 *Q*를 백엔드에게 전송한다. 백엔드는 전달받은 *R*을 키 값을 가지는 해쉬함수를 거쳐 나온 결과로 *Q*를 확인한다. 불법적인 리더의 도청으로 *R*은 획득할 수 있지만 키 값 *k*를 알지 못하기 때문에 *Q*를 계산할 수 없다. ④, ⑤번 단계에서도 키 인덱스로 키 값을 알아낼 수 없기 때문에 중간자 공격으로부터 안전할 수 있다. 마찬가지로, 전송되는 키 인덱스에 해당하는 키 값과, 리더에서 해쉬를 계산할 때 사용하는 키를 알 수 없기 때문에 재생 공격을 할지라도 백엔드에서 드러나게 되어 재생 공격으로부터 안전하다.

[표 1]은 기존 보안 방식과 제안한 프로토콜의 비교를 나타내고 있다[3, 4]. 기존의 해쉬 기반 프로토콜과 본 논문에서 제안한 프로토콜을 비교해 볼 때, 제안한 프로토콜은 각종 보안 위협으로부터 안전하며, ID를 동적으로 할당하는 특징이 있다. 위에서 안전성을 분석한 것처럼 제안 방식은 각종 보안 위협으로부터 안전함을 입증하여 기존의 해쉬방식들보다 우수함을 입증하였다. 그러면서도 태그의 연산량은 줄었다. 제안 프로토콜에서 인증 과정중에 태그는 3번의 해쉬 연산을 하지만, 실제로는 ②번 단계에서 한번만 수행하면 된다. ⑤, ⑥번 단계에서는 태그가 가지고 있는 키 값들 중에서 백엔드가 선택한 두 개의 키 값만을 해쉬 연산한다. 하지만, 태그는 많은 키 값들을 가질 필요가 없기 때문에 태그가 가진 모든 키에 대해 해쉬 연산을 하여 저장을 해두고 해당되는 해쉬 값을 전송하는 편이 효율적이다. 결과적으로 제안 프로토콜에서는 하드웨어 제약의 가장 큰 비중을 차지하는 해쉬 연산을 단 한번으로 끝냄으로써 기존 방식들보다 낮은 하드웨어 제조 가격과 높은 안전성을 보장하고 있다.

표 1. 기존 방식과 제안 프로토콜 비교

구 분	해쉬기반 ID변형	확장된 해쉬-락	해쉬제안	제안 프로토콜
기밀성	O	O	O	O
불구분성	X	O	O	O
전방보안성	X	X	O	O
위치추적	취약	안전	안전	안전
스푸핑	취약	취약	안전	안전
재생공격	안전	안전	안전	안전
상호인증	X	X	X	O
태그 연산	3	2	2	1

5. 결론

본 논문에서는 해쉬 기반의 사용자 프라이버시 보호를 위한 RFID 인증 프로토콜을 제안하였다. RFID 리더와 태그간의 충돌 중재 과정을 거쳐 선택된 태그는 보안 프로토콜을 통하여 새로운 ID를 생성하게 된다. 프로토콜 진행 과정 중에는 태그의 고유 ID와 직접적으로 관련된 어떠한 정보도 전송하지 않는다. 또한, 인증 프로토콜 이후에 매번 갱신되는 DynamicID는 이전의 DynamicID와 어떠한 상관관계도 없기 때문에 위치추적과 같은 보안 위협으로부터 안전하다. 백엔드로부터 리더와 태그의 인증 절차 시에는 태그와 리더 각각 가지고 있는 일방향 해쉬 함수를 이용하여 해쉬된 정보만을 전송한다. 이 해쉬된 정보들은 각각의 해쉬 함수와 리더의 비밀키를 모두 가지고 있는 백엔드에서만 확인이 가능하다. 따라서, 불법적인 리더나 태그로부터의 스푸핑이나 재생공격 등의 보안 위협을 막을 수 있다. 제안한 프로토콜은 RFID 시스템의 보안 위협으로부터 안전성에 대한 분석을 통하여 우수성을 입증하였다. 뿐만 아니라, 기존의 해쉬 기반 프로토콜과 비교할 때, 태그의 연산량을 줄일 수 있었다.

본 논문에서 제안한 RFID 보안 프로토콜은 기존 기법들에 비해 정보 보호 기능이 강화되고, 태그의 연산량은 줄인 효율적인 방법이라 할 수 있다. 현재 RFID 시스템에 대한 많은 사회적 관심에도 불구하고 보안문제로 인하여 제한적으로 일부 부분에서 적용이 되고 있다. 해쉬 기반 보안 프로토콜은 현재까지 가장 안전한 프로토콜로 인식되고 있다. 하드웨어 제약으로 인해서 RFID 태그에는 현재 적용하기 어려우나 경량의 해쉬 함수 개발에 대한 연구가 활발히 진행되고 있기 때문에 머지않아 실현될 것이다. 향후 경량의 해쉬 함수 개발과 함께 비밀키 방식의 인증 프로토콜 개발을 병행하면서 RFID 시스템에 가장 적합한 보안 기술 개발에 대한 계속적은 연구를 할 것이다.

참고문헌

[1] 김광조, "RFID/USN 정보보호 기술", TTA 저널 제95호 pp.70-77, 2004.

[2] S. A. Weis, "Security and Privacy in Radio-Frequency Identification Devices", MIT, Masters thesis, 2003.

[3] D.Henrici and P.Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", PerSec'04 at IEEE PerCom, pp.140-153, Mar. 2004.

[4] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification System", Proc. of the 1st Security in Pervasive Computing, LNCS, vol.2802, pp.201-212, 2004.

[5] ISO/IEC 18000-6, Part 6 : Parameters for air interface communications at 860 MHz to 960 MHz, AMENDMENT 1 : Extension with Type C and update of Types A and B.

[6] M. Ohkubo, K. Suzuki, and S. Kinoshita, "A Cryptographic Approachto "Privacy-Frendly" Tag", RFID Privacy Workshop, 2003.

[7] K. Finkenzeller, "RFID Handbook, Second edition", John Wiley & Son, Ltd, 1999.

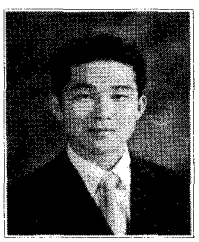
[8] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren and Kwangjo Kim, "Mutual Authentication Protocol for Low-cost RFID", Proc. of Workshop on RFID and Lightweight Crypto, pp.17-24, Jul. 14~15, 2005, Graz, Austria.

[9] 오경희, 김호원, "RFID 환경에서의 프라이버시 보호 기술", 한국통신학회지 제23권 제9호 pp.103~112, 2006.

[10] 박진성, 최명렬, "고기능 RFID 태그를 위한 보안 프로토콜", 대한전기학회논문지 54P권 4호, pp.217-223, 2005.

[11] 김광조, 양정규, "RFID의 프라이버시 보호기법", 한국전자파학회지 제5권 제2호 pp.96-104, 2004.

이 한 권 (Han-Kwon Lee) [준회원]



- 2005년 2월 : 상명대학교 정보통신공학과 (공학사)
- 2005년 3월 ~ 현재 : 상명대학교 대학원 정보통신공학과 석사과정

<관심분야>
RFID, 정보보안, 센서 네트워크, Ad-hoc 네트워크

조 태 경 (Tae-Kyung Cho) **[종신회원]**

- 1984년 2월 : 한양대학교 전자통신공학과 (공학사)
- 1986년 2월 : 한양대학교 대학원 전자통신공학과 (공학석사)
- 2001년 2월 : 한양대학교 대학원 전자통신공학과 (공학박사)
- 2003년 9월 ~ 현재 : 상명대학교 정보통신공학과 교수

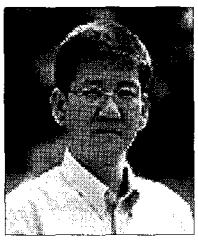
<관심분야>
초고속통신망, e-Learning

유 현 중 (Hyun-Joong Yoo) **[정회원]**

- 1982년 2월 : 서강대학교 전자공학과 (공학사)
- 1991년 2월 : Missouri University 전기 및 컴퓨터 공학과 (공학석사)
- 1996년 2월 : Missouri University 전기 및 컴퓨터 공학과 (공학박사)
- 1996년 ~ 현재 : 상명대학교 정보통신공학과 교수

<관심분야>
인공신경망응용, 패턴인식, 영상/동영상 처리

박 병 수 (Byoung-Soo Park) **[종신회원]**



- 1986년 2월 : 한양대학교 전자공학과 (공학사)
- 1989년 8월 : 한양대학교 대학원 전자공학과 (공학석사)
- 1994년 5월 : 텍사스 A&M (공학박사)
- 1995년 3월 ~ 현재 : 상명대학교 컴퓨터시스템공학과 교수

<관심분야>
임베디드 시스템, 병렬 알고리즘