한국산학기술학회논문지
Vol. 7, No. 4, pp. 635-641, 2006

해쉬락을 이용한 개선된 RFID 인증 프로토콜

배우식[1*], 장건오[2], 한군희[3]

Improved RFID Authentication Protocol using Hash Lock

Woo-Sik Bae[1*], Gun-Oh Jang[2] and Kun-Hee Han[3]

요 약 RFID 시스템의 전자 태그, 리더 간의 무선 통신에서, 기존의 해쉬-락 관련 알고리즘은 스푸핑, 재전송, 트래픽 분석 및 위치 추적 등 보안상의 취약점이 존재한다.
본 논문에서는 개인정보 보호를 위한 기존의 해쉬-락 관련 알고리즘을 비교, 분석하였으며 이를 보완하기 위하여 실시간과 매 세션마다 리더로부터 수신한 난수를 이용하여 해쉬 함수를 생성하고 인증 프로토콜을 가지는 새로운 해쉬 기반 보안 인증 알고리즘을 제안하였다.
제안한 알고리즘은 RFID 무선 인증 시스템에서 다양한 유용성을 제공할 수 있으며, 기존의 알고리즘에 비해 계산량을 절감할 수 있는 장점이 있다. 또한 추후 예상되는 주변의 수많은 태그중 필요한 태그만 선별하여 사용하며, 시간 기반으로 불필요 태그의 동작을 종료시켜 서버부담을 줄이는 방법이 될 것으로 기대된다.

Abstract On the wireless-communication between Electronic Tag of RFID system and Reader, there are some existing problems with weaknesses of security such as spoofing, replay, traffic analysis, position tracking, etc., in the established hash-lock related algorithm.
This paper has presented the comparison and analysis of the established hash-lock related algorithm for privacy and in order to make up for this, also suggested a new security authentication algorithm based on hash which has an authentication protocol and creates hash function by using random numbers received from the reader on real-time and every session.
The algorithm suggested is able to make RFID wireless authentication system offer a several of usefulness and it has an advantage to reduce the amount of calculations compared to established algorithm. It also uses just the tags needed among a lot of tags around which are expected later and it is expected to reduce a responsibility of the server by ending unnecessary tags' action with time based.

Key Words : RFID, 유비쿼터스, 해쉬락, 보안, 인증

1. 서론

RFID(Radio Frequency Identification)는 전자 태그(Tag)를 사물에 부착하여, 사물이 주위 상황을 인지하고 기존 IT 시스템과 실시간으로 정보를 교환, 처리할 수 있는 기술로써 앞으로 사용의 편리성 향상으로 개인 및 산업 전반에 활용이 예상 되며 국내 · 외적으로 많은 연구가 진행 되고 있다. 그러나 마이크로칩에 내장된 정보를 무선주파수를 이용하여 읽어내기 때문에 RFID 기술은 도청, 트래픽 분석, 서비스거부 공격, 메시지유실, 트래킹 공격, 스푸핑 공격 등 무선 네트워크상의 많은 취약점 들을 지니고 있어서 보안이나 프라이버시 보호문제에 심각한 문제를 야기할 수 있다. 따라서 RFID 시스템이 활성화되기 위해서는 리더(Reader)와 태그 사이의 안전한 상호인증이 매우 중요하다.

본 논문에서는 RFID의 프라이버시 문제를 해결하기 위한 기존 제안된 해쉬-락 기법[1,2,3], 확장된 해쉬-락 기법[4,5], 해쉬 체인기법[6,7] 및 해쉬 기반 ID 변형기법[8,9] 등이 해결하지 못한 문제점 분석을 통해 보다 안전하고 효율적으로 사용자의 프라이버시를 보호할 수 있는

[1]백석대학교 정보기술대학원
[2]광운대학교 경영학과
[3]백석대학교 정보통신학부
*교신저자: 배우식(future010@paran.com)

인증 프로토콜을 제안 한다. 제안하는 프로토콜은 해쉬 함수 와 난수 및 실시간을 이용하여 공격자의 각종 공격에 안전하고 실시간을 이용함으로써 추후 예상되는 불필요 태그의 산재된 공해로 시스템에 누적되는 부하문제를 줄여줄 수 있는 방식을 제안 하며, 분산된 데이터베이스에서도 적용이 가능하고 다양한 보안성 및 적용성을 제공하는 메커니즘을 제안 하고자 한다.

2. RFID 시스템

RFID 시스템은 일반적으로 태그, 리더, 백-엔드 데이터베이스로 구성되어 있다.

2.1 태그

태그는 마이크로 칩과 안테나로 구성되어 있으며, 유일한 식별코드와 정보가 저장되어 있어서 리더의 요청에 의해 또는 상황에 따라 태그 스스로 리더에게 자신의 정보를 송 · 수신 하는 장치이며 현재 두 가지 타입이 있다.

- 능동형 태그 : 태그에 내장된 배터리를 이용하여 데이터를 송 · 수신 한다. 원거리 데이터 송 · 수신이 가능하지만 수동형 태그에 비해 가격이 비싸고, 부피가 크며 배터리의 수명이 다하면 작동이 멈춘다는 단점이 있다.

- 수동형 태그 : 리더로부터 수신한 전자기파에 의한 유도 전류를 사용하여 전력을 공급 받는다. 능동형 태그에 비해 근거리 에서만 사용이 가능하다는 단점이 있지만, 가격이 저렴하고 크기가 작으며 수명에 제한이 없다.

2.2 리더

리더는 태그에게 신호를 보내거나 태그로부터 받은 데이터를 서버에게 전송하는 장치로써 태그의 활성화 및 비활성화, 수동형 태그에 전력공급, 태그로 보내는 데이터 신호를 인코딩 및 태그로부터 받는 데이터를 디코딩 등 주요한 기능을 가지고 있다.

2.3 백-엔드 데이터베이스

일반적으로 호스트 컴퓨터라고도 불리며 리더가 수집한 정보를 저장 및 연산능력이 낮은 리더 또는 태그를 대신하여 복잡한 연산을 수행한다. [그림 1]은 일반적인 RFID 인증 프로토콜 모델을 나타내었다.

3. 관련연구

3.1 해-쉬락 기법

해쉬-락[1] 프로토콜은 낮은 태그 가격을 고려하여 MIT에 의해 제시된 방식으로 Key를 태그, 데이터베이스와 사전에 안전하게 공유되어 있다고 가정하며 인증과정은 다음과 같다.

1) 해쉬-락의 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.

2) 해쉬-락의 풀림 과정[그림 2]

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 metaID 가 일치하면, T는 잠긴 상태 에서 빠져 나온다.

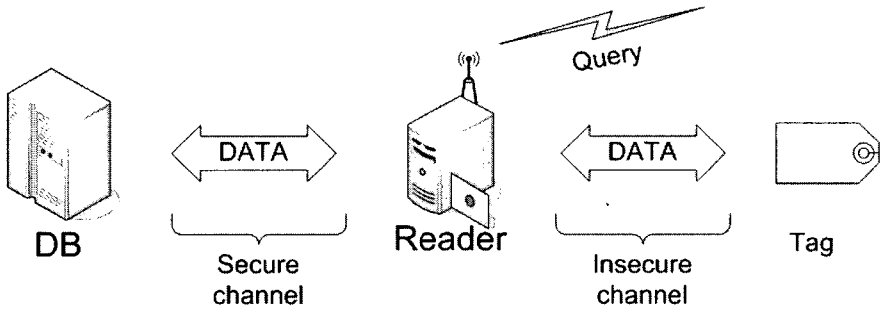


그림 1. RFID 인증 프로토콜 모델

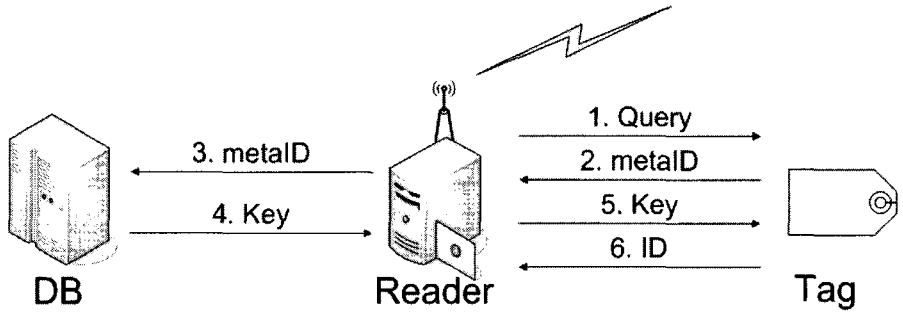


그림 2. 해쉬-락 기법

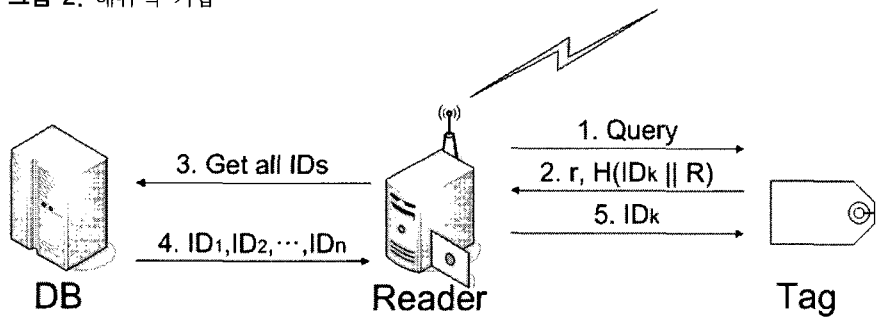


그림 3. 확장된 해쉬-락 기법

이 방법은 태그의 식별 값인 metaID가 고정되어 있어, 출력되는 데이터가 같아 해당 태그로부터 데이터가 전송되었는지 확인할 수 있게 된다. 그리고 리더기와 태그사이의 통신채널은 도청이 가능하기 때문에 악의적인 공격자는 Key를 획득한 후, 해쉬 연산 하여 metaID를 산출하여 인증을 받을 수 있다. 또한 제 3자가 고정된 metaID를 재전송함으로써 인증 받을 수 있으며, metaID가 식별자처럼 사용되기 때문에 스푸핑 공격 및 사용자 추적이 가능하다.

3.2 확장된 해쉬-락 기법

Hash Lock 기법에서 가능한 사용자 추적을 방지하기 위한 방식이다. 태그는 인가되지 않은 사용자에 의한 질의에 대하여 예상 가능한 응답을 하지 않지만, 합법적인 리더기에 의해서는 여전히 식별 가능해야 하는 방식이다. 이 기법에서는 태그에 일방향 해시 함수와 난수발생기가 구축되어 있어야 한다. 태그를 풀림 상태로 하는 프로토콜은 [그림 3]과 같다.

① 리더 R은 태그 T에게 질의를 보낸다.
② T는 랜덤 한 난수를 생성하고, hash(ID || R)값을 계산한다.
③ T는 R에게 (R, hash(ID || R))을 전송한다.
④ R은 모든 알려진 IDi값에 대해 hash(IDi || R)을 계산한다.
⑤ 만약 hash(IDi || R) == hash(ID || R)을 만족하는 IDi 를 찾는다면, R은T에게 IDi를 전송한다.
⑥ 만약 IDi와 ID가 일치한다면, T는 잠긴 상태에서 빠져 나온다.

이 방식은 난수를 이용하여 태그에서 리더로 가는 정보가 매 세션마다 바뀌므로 스푸핑 공격에는 강하지만 IDk 값이 노출되어 위치 추적이 가능하며 리더의 공격자가 r,H(IDk || r)을 도청하여 재전송 할 경우 정당한 태그로 가장하여 재전송 공격에도 취약하다.

3.3 해쉬 체인 기법

서로 다른 두개의 해쉬 함수를 사용하는 해쉬 체인 기법[6]은 세션마다 다른 Ai 값을 전송하므로 위치트래킹 공격에 안전하다. 하지만 최악의 경우 데이터베이스에서는 모든 Si에 대하여 H와 G를 i번 수행해야 한다. 또한 잘못된 응답이 수신 되었을 경우, 데이터베이스는 고유한 모든 ID에 대해 ∞번의 해쉬를 수행할 가능성이 있으며 [그림 4]는 해쉬 체인 기법의 동작 과정 이다.

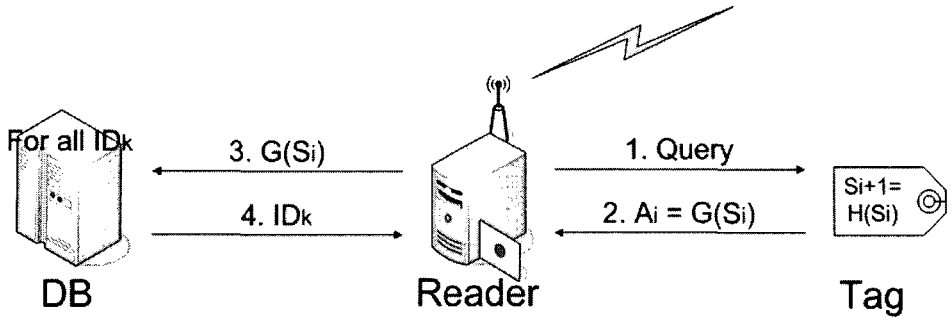


그림 4. 해쉬 체인 기법

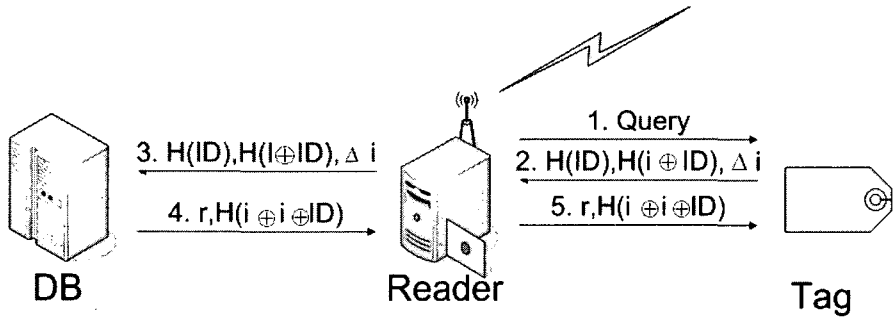


그림 5. 해쉬 기반 ID 변형 기법

3.3 해쉬 기반 ID변형기법

해쉬 기반 ID 변형기법[7,8]은 해쉬 체인 기법과 유사하게 태그의 인증정보인 ID를 매 세션마다 바꾸는 기법이다. [그림 5] 와 같이 매 세션마다 태그의 ID가 난수 R에 의해 갱신되므로 재전송 공격으로부터 안전하다. 그러나 공격자가 정당한 리더로 가장해 태그로부터 H(ID), H(i⊕D), Δi를 획득하고, 정당한 태그가 다음 인증세션을 수행하기 전에 이 정보들을 리더의 질의에 대한 응답으로 이용하면 공격자는 정당한 태그로 인정받을 수 있다.

4. 제안 프로토콜

4.1 구조

본 제안 프로토콜은 리더는 난수 생성기 RNG(Random Number Generator)를 갖고 있으며, 리더가 처음 태그에게 질의를 할 때 난수와 실시간을 함께 전송하고, 태그는 리더로부터 수신한 난수와 실시간을 자신이 가지고 있는 ID 및 저장 시간으로 해쉬한 값을 이용하여 매 세션마다 다르게 응답함으로써 기존 프로토콜들 에서 문제점으로 지적 되었던 재전송 공격과 스푸핑 공격에 대하여 안전하다. 제안프로토콜에서 백-엔드 데이터베이스는 태그의 ID와 관련 데이터를 저장하고 있으며, 해쉬 함수 2회의 연산만을 이용하여 태그를 인증한다.

리더는 난수 및 실시간 데이터를 송신해 주는 것 외에는 연산이 필요하지 않으며, 태그와 백-엔드 데이터베이스 사이에서 전송되는 정보를 저장하기 위한 임시메모리만이 요구 된다.

제안 프로토콜에서 사용되는 파라미터는 다음과 같으며, [그림 6]은 제안하는 프로토콜의 기본 구조를 나타낸 것이다.

4.1.1 가정 사항

본 제안 프로토콜을 제안하기 위하여 다음 사항을 가정한다.

- 태그는 능동형으로 내장된 배터리로 동작한다.
- 태그와 데이터베이스는 해쉬 함수 연산을 수행한다.
- 태그와 데이터베이스는 태그의 ID를 사전에 공유한다.
- 리더기는 난수 생성기능을 갖고 있다.
- 백-엔드 데이터베이스와 리더는 안전한 통신채널로 통신을 하고 있다.

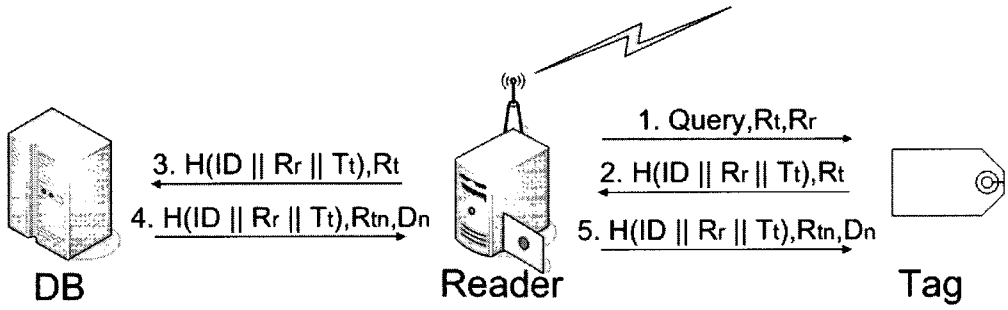


그림 6. 제안 프로토콜의 구조

[파라미터]
- Query : 질의, 태그의 응답을 요청
- ID : 태그 고유의 비밀 인증 정보
- H( ) : 일 방향 해쉬 함수
- R_t : 리더가 태그에게 전송하는 DB시간(μs)
- R_r : 리더가 생성하여 태그에게 전송하는 난수
- T_t : 태그에 저장되어 있는 시간(μs)
- R_{tn} : 태그에 기록될 시간(μs)
- D_n : 데이터베이스에서 태그에게 전송되는 명령
- || : 연접(Concatenate function)

4.2 인증과정

◎ 1단계 : 리더는 태그들에게 Query와 R_t,R_r 를 함께 브로드캐스팅 한다.

리더 → 태그 : Query, R_t,R_r

◎ 2단계 : 태그는 ID와 자신이 가지고 있던 T_t 를 R_r 와 연접한 후 해쉬 하여, R_t와 함께 Query에 대한 응답으로 리더에게 전송한다.

태그 → 리더 : H(ID || R_r || T_t), R_t

◎ 3단계 : 리더는 R_r과 태그로부터 수신한 H(ID || R_r || T_t), R_t를 백-엔드 데이터베이스로 전송한다.

리더 → 백-엔드 데이터베이스 : H(ID || R_r || T_t), R_t

◎ 4단계 : 백-엔드 데이터베이스에 저장된 ID를 R_t, R_r과 연접 하여 해쉬한 값과 리더로부터 수신한 H(ID || R_r || T_t), R_t를 비교하여 태그를 인증한다.

백-엔드 데이터베이스 → 리더 : 계산된 H(ID || R_r || T_t), R_t = 수신한 H(ID || R_r || T_t), R_t인증이 성공하면 H(ID || R_r || T_t), R_{tn}, D_n를 리더 에게 전송한다. 필요에 따라 데이터베이스에 입력되어진 기간 제한 태그 및 불필요 태그는 Kill 명령 등을 전송하여 동작을 완전히 종료시킨다.

◎ 5단계 : 리더는 백-엔드 데이터베이스로 부터 수신한 H(ID || R_r || T_t), R_{tn}, D_n를 태그에게 전송한다.

리더 → 태그 : H(ID || R_r || T_t), R_{tn}, D_n

태그는 자신의 ID와 인증 세션에서 생성한 R_t, T_t를 연접하여 해쉬한 값과 리더로부터 수신된 H(ID || R_r || T_t), R_{tn}, D_n를 비교하여 백-엔드 데이터베이스를 인증하고 R_{tn}을 기록하며 필요에 따라 D_n명령을 수행하여 태그동작을 종료하며, 인증세션을 성공적으로 종료 한다.

4.3 제안 프로토콜의 안전성

4.3.1 스푸핑 공격에 대한 안전성

공격자가 정당한 리더로 가장하여 Query와 함께 태그에게 난수 R_r및 실시간 R_t를 전송한다면, 태그로 부터 H(ID || R_r || T_t), R_t를 획득할 수 있으나 이 정보를 악의적인 태그에 넣어 리더에 대한 응답으로 보내지게 되면 이미 시간이 지나간 상태의 정보를 백-엔드 데이터베이스에 H(ID || R_r || T_t), R_t 를 전송해야 하기 때문에 인증을 할 수가 없어 스푸핑 공격이 불가능 하게 된다.

4.3.2 재전송 공격에 대한 안전성

정당한 리더가 Query와 함께 전송하는 R_t, R_r는 매 세션마다 변하기 때문에 태그의 응답 H(ID || R_r || T_t), R_t도 매 세션마다 바뀌게 된다. 그러므로 공격자는 도청으로 획득한 H(ID || R_r || T_t), R_t를 다음 세션에서는 응답으로 사용할 수 없으므로 재전송 공격에 안전하다. 또한 프로

토콜에서 공격자는 태그의 ID를 난수 및 실시간과 해쉬하기 때문에 알 수 없으므로 매 세션마다 변하는 R_t, R_r에 대하여 정당한 응답 $H(ID \parallel R_r \parallel T_t)$, R_t을 생성하는 것은 원천적으로 불가능 하다.

4.3.3 트래픽 분석과 위치 추적에 대한 안전성

공격자가 정당한 리더로 가장하여 지속적으로 고정된 R_t, R_r를 태그에게 전송하여도 다음 세션에서는 실시간이 바뀌고 태그는 난수, T_t를 공격자는 알 수 없는 해쉬된 ID를 이용하여 매 세션마다 변하는 응답 $H(ID \parallel R_r \parallel T_t)$, R_t를 전송하므로 공격자는 서로 다른 응답이 동일한 태그에 의한 것인지를 판별할 수 없다. 그러므로 정당한 리더로 가장한 공격자는 트래픽 분석이 불가능 하고 태그의 위치도 추적할 방법이 없게 된다.

4.3.4 정보전송 방해에 대한 안전성

제안 프로토콜은 상호 인증을 제공하므로 정보전송 방해 공격을 탐지할 수 있으며, 태그의 인증 정보 ID는 변하지 않기 때문에 세션마다 ID가 변하는 해쉬 기반 ID 변형 프로토콜에서 발생 가능한 데이터베이스의 정보유실은 일어나지 않으며 [표 1] 은 기존 프로토콜과의 안전성 비교표 이다.

4.4 제안 프로토콜의 효율성

본 논문 제안 프로토콜에서 태그는 해쉬 함수 연산 및 실시간 데이터 저장만 하므로 앞으로의 기술 발전으로 저가 태그 및 모든 태그에서 구현 가능할 것이며, 또한 [표 2]와 같이 인증 세션 동안 2회의 해쉬 함수 연산만을 수행 하므로 연산 부담도 크지 않으며 분산된 데이터베이스가 존재하는 유비쿼터스 환경에도 적용이 가능하다.

본 프로토콜은 난수 및 실시간만 적용 하고 다른 복잡한 연산은 하지 않으며 또한 데이터베이스의 연산이 적어 주변에 수많은 태그가 있어도 저가의 데이터베이스로도 구성이 가능하기 때문에 효율성 면에서도 우수하다고 할 수 있다.

5. 결론

RFID기술은 매우 편리하며 미래에 발전되어 사용 되어질 기술 이지만 문제점으로 지적 되어온 보안취약점을 제거하지 않는다면 크나큰 문제점을 발생시킬 수가 있다.

제안한 프로토콜은 태그가 리더로부터 수신한 난수 및 실시간으로 부터 새로운 해쉬 함수를 생성하여 매 세션마다 다른 응답을 전송할 수 있도록 함으로써 공격자의 재전송 공격, 스푸핑 공격, 위치추적 등에 안전한 프로토콜로써 안전성과 효율성이 뛰어나다고 할 수 있다. 그리고 앞으로 신기술이 적용될 태그에도 실시간 데이터를 지속적으로 태그에 기록함으로 도처에 산재되어 있는 수많은 태그 중 필요한 태그만 사용하고 오래되고 불필요한 태그들은 Kill 명령 등으로 동작을 종료해 줌으로써 서버부담을 줄이고 추후 생길 불필요 태그 쓰레기를 처리할 수 있는 방법이 될 것으로 기대된다.

표 1. 제안프로토콜의 안전성

	해쉬-락 기법	확장된 해쉬-락 기법	해쉬-체인 기법	해쉬 기반 ID변형 기법	제안 프로토콜
스푸핑 공격	취약	취약	취약	취약	안전
재전송 공격	취약	취약	취약	안전	안전
트래픽 분석 공격	취약	취약	안전	안전	안전
위치정보노출	취약	취약	안전	안전	안전
정보전송방해공격	안전	안전	안전	안전	안전

표 2. 제안프로토콜의 효율성

	해쉬-락 기법	확장된 해쉬-락 기법	해쉬-체인 기법	해쉬 기반 ID변형 기법	제안 프로토콜
인증	양방향	양방향	단방향	양방향	양방향
태그 연산량	해쉬1회	해쉬1회 난수 1회	해쉬2회	해쉬3회	해쉬1회 (시간쓰기)
리더 연산량	-	n회	-	-	난수1회
데이터베이스 연산량	-	-	n(1+i)회	해쉬3회 난수1회	해쉬1회

참고문헌

[1] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. w. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems," Security in Pervasive Computing 2003, LNCS 2802, pp. 201-202, Springer-Verlag Heidelderg, 2004.

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

[3] S. E. Sarma, S. A. Weis, D. W. Engels. "RFID systems, Security & Privacy Implications", White Paper MIT-AUTOID-WH-014, MIT AUTO-ID CENTER, 2002.

[4] Sanjay E.Sarma, Stephen A. Weis and Daiel W.Engels, "Radio-Frequency Identification Systems", In Proceeding of CHES '02, pp. 454-469. Springer-Verlag, 2002. LNCS NO.2523.

[5] Weis, S. et al. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, First International Conference on Security in Pervasive Computing (SPC), 2003.

[6] M. Ohkubo, K.Suzuki and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID, "Proceedings of the SCIS 2004, pp. 719-724, 2004.

[7] 이근우, 오동규, 곽진, 김승주, 원동호 "Low Cast RFID 시스템을 위한 Improved Hash Chain 프로토콜 " CISC'S04, 2004.

[8] Gildas Avoine and Philippe Oechslin "RFID Traceability : A Multilayer Problem", Financial Cryptography, March 2005.

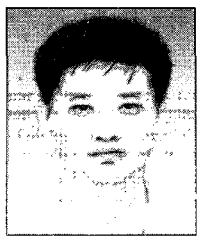
[9] D. Henrici, and P. Muller. "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", Procedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops(PERCOMW'04), pp.149-153, IEEE, 2004.

배 우 식(Woo-Sik Bae) [정회원]

- 2003년 8월 : 한국방송통신대학교 컴퓨터과학과 (이학사)
- 2004년 3월 ~ 2006. 8월 : 백석대학교 정보기술대학원 (공학석사)
- 1997년 3월 ~ 현재 : 아주자동차대학 전산소

<관심분야>
유비쿼터스 보안, 컴퓨터 네트워크,
암호 프로토콜/알고리즘

장 건 오(Gun-Oh Jang) [정회원]



- 1999년 2월 : 성균관대학교 경영학과(경영학석사)
- 1993년 1월 ~ 2001년 2월 : 한국전산원
- 2001년 3월 ~ 현재 : 중소기업기술정보진흥원 정보화사업2팀장
- 2003년 3월 ~ 현재 : 광운대학교 경영학과 박사 수료

<관심분야>
중소기업 정보화, 정보보호, 정보화경영체제(IMS),
마케팅정보화 등

한 군 희(Kun-Hee Han) [종신회원]

- 2000년 8월 : 충북대학교 컴퓨터공학과(공학박사)
- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
콘텐츠 보호, 웹시스템 개발, 암호 프로토콜/알고리즘