개선한 일회성 난수를 이용한 RFID 상호인증 프로토콜

(Improving an RFID Mutual Authentication Protocol using One-time Random Number)

윤 은 준 † 유 기 영 ††
(Eun-Jun Yoon) (Kee-Young Yoo)

요 약 2008년에 Kim-Jun은 의도하지 않은 정보의 누출로 인한 악의적인 공격들 및 범죄 악용 문제점들을 해결하기 위해 일회성 난수를 이용한 RFID 상호인증 프로토콜을 제안하였다. 보안성 분석을 통하여 Kim-Jun은 제안한 프로토콜이 재전송 공격을 포함한 다양한 공격들에 안전함을 증명하였다. 하지만 본 논문에서는 그들의 주장과는 달리 그들이 제안한 프로토콜이 여전히 재전송 공격에 취약함을 증명하며, 더 나아가 동일한 연산 효율성을 보장하며 재전송 공격을 막을 수 있는 간단히 개선된 일회성 난수 기반의 RFID 상호인증 프로토콜을 제안한다.

키워드 : RFID, 일회성 난수, 상호인증, RFID 시스템, 재전송 공격

Abstract In 2008, Kim-Jun proposed a RFID mutual authentication protocol using one-time random number that can withstand malicious attacks by the leakage of important information and resolve the criminal abuse problems. Through the security analysis, they claimed that the proposed protocol can withstand various security attacks including the replay attack. However, this paper demonstrates that Kim-Jun's RFID authentication protocol still insecure to the replay attack. In addition, this paper also proposes a simply improved RFID mutual authentication protocol using one-time random number which not only provides same computational efficiency, but also withstands the replay attack.

Key words : RFID, One-time random number, Mutual Authentication, RFID system, Replay attack

1. 서 론

유비쿼터스 컴퓨팅 환경에서 필수적인 차세대 핵심기술로 사용되어지고 있는 RFID(Radio Frequency Identification) 시스템은 다양한 목적으로 사용되어 지고 있는 Tag 내에 정보를 읽거나 필요한 내용을 갱신 또는 쓰기 위해서 Reader와의 직접적인 접촉이 요구되지 않는 무선 네트워크 통신 기반의 인식 시스템이다[1]. 일반적으로 RFID 시스템은 Tag, Reader, 그리고 Back-end Database의 3가지 구성요소로 구성된다[1]. 이러한 RFID 시스템은 현재 다양한 분야에서 사용되어 지고 있는 바코드 인식 시스템이나 자기 인식 장치들이 근본적으로 내재하고 있는 실용성 및 보안성 문제점들을 보완할 수 있는 대체 시스템을 각광받고 있다. 특히 교통카드, 출입구 보안 및 출결 카드 분야를 포함한 상거래와 직접적인 관련이 있는 물류관리, 재고관리, 항만관리, 동물관리 등 물류 및 유통 분야에서도 빠르게 응용 및 확산되어 사용되어지고 있다[2,3].

하지만 RFID 시스템이 가져다주는 실용성과 편리함 이면에는 개인 정보 노출 및 위치 정보 누출 등으로 인한 개인의 프라이버시 침해 문제가 발생할 수 있다[4,5]. 이러한 프라이버시 침해 문제를 해결하기 위한 많은 연

· 본 연구는 2단계 두뇌한국 21 프로젝트(2009)의 연구결과로 수행하였습니다.

† 정 회 원 : 경북대학교 전자전기컴퓨터학부 교수
ejyoon@tpic.ac.kr
†† 종신회원 : 경북대학교 컴퓨터공학과 교수
yook@knu.ac.kr
(Corresponding author임)

논문접수 : 2008년 10월 6일
심사완료 : 2009년 2월 2일

구자들에 의해 해쉬-락 기법, 확장된 해쉬-락, 해쉬기반 ID 변형기법, 개선된 해쉬기반 ID 변형기법 등 다양한 RFID 인증 프로토콜(Authentication Protocol)들이 최근까지 개발되어져 오고 있다[4-10]. 하지만 현재까지 제안되어져 오고 있는 대부분의 RFID 인증 프로토콜들은 태그의 재사용이 불가능하거나, 위치추적이 쉬우며, 재전송 공격이나 스푸핑 공격에 취약하는 등 여러가지 보안 취약점들을 가짐을 많은 연구자들에 의해 발견되어 지고 있다[7-14].

특히 2008년에 Kim-Jun은 의도하지 않은 정보의 누출로 인한 악의적인 공격들 및 범죄 악용 문제점들을 해결할 수 있는 일회성 난수를 이용한 RFID 상호인증 프로토콜을 제안하였다[14]. Kim-Jun이 제안한 프로토콜은 기존의 연구와는 달리 DB 서버가 난수를 생성하여 상호인증에 이용된다. 이러한 이유로 그들은 보안성 분석을 통하여 그들이 제안한 인증 프로토콜이 기존에 연구된 RFID 인증 기법들의 가장 큰 문제점인 재전송 공격(Replay Attack), 스푸핑 공격(Spoofing Attack), 위치 트래킹 공격(Location Tracking Attack) 등을 포함한 다양한 암호학적 공격들에 안전함을 증명하였다. 특히 안전하지 않은 채널(Insecure Channel)인 Reader와 Tag 사이의 모든 정보를 탈취하여 공격자가 재전송 공격에 수행하더라도 DB가 가지고 있는 난수 값이 매 인증 시도시마다 갱신되어 지기 때문에 과거의 송수신 정보는 쓸모없는 정보가 되어 인증을 통과할 수 없음을 주장하였다. 하지만 본 논문에서는 Kim-Jun의 주장과는 달리 그들이 제안한 프로토콜이 여전히 Reader로 위장한 공격자의 재전송 공격에 취약함을 증명한다. 더 나아가 동일한 연산 효율성을 보장하며 위와 같은 재전송 공격을 막을 수 있는 Tag의 난수를 이용한 간단히 개선된 일회성 난수 기반의 RFID 상호인증 프로토콜을 제안한다. 한 결론으로 제안한 RFID 상호 인증 프로토콜은 Kim-Jun의 프로토콜과 비교하여 더욱 더 강한 보안성을 제공하며 안전성을 저해하지 않는 불필요한 XOR 연산을 줄여 줌으로써 효율성 측면에서도 우수하다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 관련 연구로써 기존에 제안된 RFID 시스템 기반의 보안 인증 기법들과 Kim-Jun이 제안한 RFID 상호 인증 프로토콜에 대해 설명하며, 3장에서는 Kim-Jun이 제안한 프로토콜이 재전송 공격에 취약함을 보인다. 4장에서는 제안하고자하는 RFID 상호 인증 프로토콜에 대해 구체적으로 설명하고, 5장에서는 제안된 인증 프로토콜과 기존의 인증 프로토콜들을 안정성과 효율성 측면에서 비교 및 분석한다. 마지막으로 6장에서는 본 논문의 결론을 맺는다.

2. Kim-Jun의 일회성 난수를 이용한 RFID 상호 인증 프로토콜

본 장에서는 기존에 제안된 RFID 시스템 기반의 보안 인증 기법들에 관해 보안성 측면에서의 간략한 분석 내용을 설명하며 Kim-Jun이 제안한 일회성 난수를 이용한 RFID 상호인증 프로토콜을 살펴본다[14].

2.1 기존 연구내용 분석

일반적으로 대표적인 RFID 시스템의 소프트웨어적 보안 인증기법은 해쉬-락 기법, 확장된 해쉬-락, 해쉬기반 ID 변형 기법, 개선된 해쉬기반 ID 변형기법 등이 있다[4-10]. 해쉬-락 기법은 MIT에서 Weis가 연구한 기법으로 저가의 Tag를 이용하여 자원 제한 문제를 해결할 뿐만 아니라 정당하게 인가받은 Reader에게만 Tag 정보를 전송하도록 설계되었다. 저비용의 Tag의 자원 제한 문제를 해결하기 위해 Tag에 하드웨어적으로 구현된 안전한 해쉬 함수를 구현한 후 이를 이용하여 사용자 자신의 실질적인 데이타 ID 및 인증과정에 필요한 일시적인 metaID 값을 Tag 내에 안전하게 저장한다. 특히 MIT 해쉬-락 기법은 ID 대신 metaID를 사용함으로 인해 ID의 직접적인 노출을 방지한다는 장점을 가진다. 하지만 Reader와 Tag 사이는 안전하지 않은 통신 채널임으로 암호화나 복잡성을 부여하는 과정 없이 데이터를 송수신 하는 MIT 해쉬-락 기법은 위치 추적 공격, 재전송 공격, 그리고 스푸핑 공격 등에 취약하다[11-14]. 확장된 해쉬-락 기법은 해쉬-락 기법을 보안성 측면에서 확장한 기법으로 Tag는 일회성 난수를 이용하여 Reader의 요청 *query*에 매번 다른 응답을 송신하기 때문에 Tag의 위치추적은 어렵다는 장점이 있다. 즉, 악의적인 공격자가 Reader의 요청에 대한 응답 값들을 획득하였다 하더라도 다음 세션에는 또 다른 응답 값이 생성되기 때문에 어느 Tag에서 고정적인 데이터 값이 송신되는지를 관찰하기 어렵게 함으로써 위치추적을 어렵게 한다. 하지만 확장된 해쉬-락 기법 역시 많은 연구자들에 의해 여전히 재전송 공격과 스푸핑 공격 등에 취약함이 증명되었다[11-14]. 해쉬기반 ID 변형 기법은 위치트래킹 공격을 방지하기 위해 Henrici와 Muller가 제안한 해쉬 함수에 기반하여 ID를 매번 갱신하여 사용하는 기법이다. 이 기법은 ID 갱신 기법을 적용하여 위치추적을 막는다는 장점은 있다고 주장하였지만, 여전히 위치트래킹 공격과 스푸핑 공격 등에 취약함이 증명되었다[11-14]. 개선된 해쉬기반 ID 변형 기법은 해쉬기반 ID 변형 기법의 문제점인 스푸핑에 대한 취약점을 보완하고, 연산 효율성을 높이기 위해 Tag 측의 해쉬 수행 횟수를 줄여준 기법이다. 특히 개선된 해쉬기반 ID 변형 기법에서는 기존의 기법들과 다르게

Tag 측과 DB 측에서 문자열 나눔 연산을 요구한다. 하지만 이 기법도 많은 연구자들에 의해 위치추적 공격 및 스푸핑 공격 등에 취약함이 증명되었다[11-14].

2.2 Kim-Jun의 일회성 난수를 이용한 RFID 상호인증 프로토콜

위 2.1절과 같은 이유로 2008년에 Kim-Jun은 의도하지 않은 정보의 누출로 인한 악의적인 공격들 및 범죄 악용 문제점들을 해결할 수 있는 일회성 난수를 이용한 RFID 상호인증 프로토콜을 제안하였다[14]. Kim-Jun이 제안한 프로토콜은 기존의 연구와는 달리 DB 서버가 난수를 생성하여 상호인증을 제공케 하여 재전송 공격, 스푸핑 공격, 위치 트래킹 공격 등을 포함한 다양한 암호학적 공격들에 안전하도록 설계하였다. 그림 1은 Kim-Jun이 제안한 프로토콜의 세부 동작과정을 보여주며 다음과 같이 총 8단계로 수행되어 진다. 여기에서 DB와 Reader 사이의 채널은 안전한 채널(Secure Channel)이며 Reader와 Tag 사이의 채널은 공개된 채널(Open Channel)이라 가정한다.

① Reader → Tag : $query$, R_r

Reader → DB : $query$

Reader는 감응 인식 범위 내에 Tag가 존재하면 난수 R_r을 생성하여 $query$와 함께 Tag에게 전송한다. 동시에 Reader는 DB에게도 $query$를 전송한다.

② DB → Reader : R_{db}

Tag는 $query$와 R_r을 수신 후, 임시저장장소에 R_r을 저장한다.

DB는 $query$을 수신 후, 난수 R_{db}을 생성하여 Reader에게 전송한다.

③ Reader → Tag : R_{db}

Reader는 DB로부터 수신한 R_{db}을 Tag에게 전송한다.

④ Tag → Reader : $H(ID_t \| R_r) \oplus R_r$

Tag는 R_{db}을 수신 후, 임시저장소에 R_{db}을 저장한다. Tag는 자신의 ID_t와 기 저장된 R_r을 이용하여 $H(ID_t \| R_r) \oplus R_r$을 계산하여 Reader에게 전송한다. 여기에서 $H()$는 안전한 일방향 해쉬함수(Secure One-way Hash Function)을 의미하며, $\oplus$는 비트단위 배타적 논리합(Bit-wise Exclusive-or) 연산을 의미한다.

⑤ Reader → DB : $H(ID_t \| R_r) \oplus R_r$, R_r

Reader는 Tag로부터 수신 한 $H(ID_t \| R_r) \oplus R_r$과 R_r을 DB에게 전송한다.

⑥ DB → Reader : ID_{db}, $H(ID_{db} \oplus R_{db})$

DB는 ID 테이블에 저장된 Tag의 ID_{db}와 수신한 R_r을 이용하여 $H(ID_{db} \| R_r) \oplus R_r$을 계산한 후, Tag로부터 수신 한 $H(ID_t \| R_r) \oplus R_r$와 일치 여부를 비교한다. 만약 두 값이 일치한다면, DB는 Tag를 인증하게 되고 상호인증을 위해 ID_{db}와 $H(ID_{db} \oplus R_{db})$을 Reader에게 전송한다. 그렇지 않다면 인증과정을 중지한다.

⑦ Reader → Tag : $H(ID_{db} \oplus R_{db})$

Reader는 DB로부터 수신한 $H(ID_{db} \oplus R_{db})$을 Tag에게 전송한다.

⑧ Tag는 $H(ID_{db} \oplus R_{db})$을 수신 후, 자신의 ID_t와 기 저장된 R_{db}을 이용하여 $H(ID_t \oplus R_{db})$을 계산한 후, Reader로부터 수신 한 $H(ID_{db} \oplus R_{db})$와 일치 여부를 비교한다. 만약 두 값이 일치한다면, Tag는 Reader를 인증하게 되고 계속되는 과정을 수행한다. 그렇

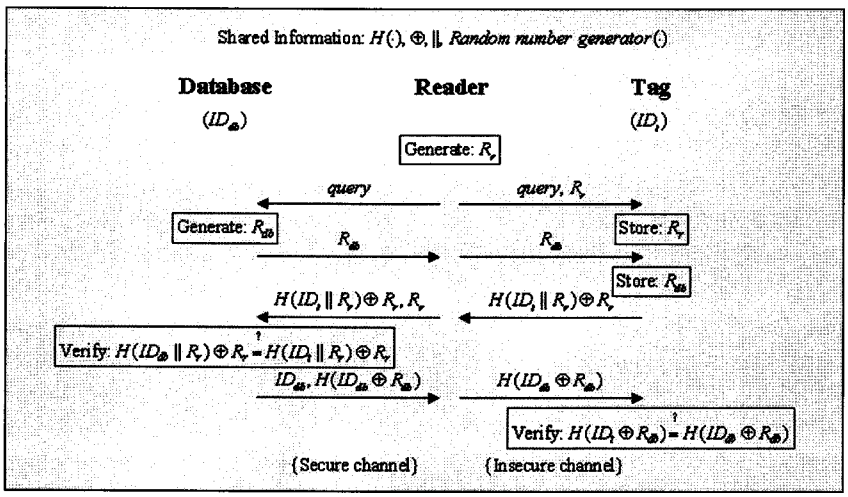

그림 1 Kim-Jun의 일회성 난수를 이용한 RFID 상호인증 프로토콜

지 않다면 인증과정을 중지한다.

3. Kim-Jun 프로토콜에 대한 재전송 공격

본 장에서는 Kim-Jun이 제안한 프로토콜이 재전송 공격(Replay Attack)에 취약함을 증명한다. 그림 2는 Kim-Jun의 프로토콜에 대한 재전송 공격 과정을 보여준다. 임의의 공격자(Attacker)는 과거의 성공적인 인증 세션에서 수행된 위 인증 단계들 ①, ②, ⑦에서 각각 전송되어 지는 정보들을 도청하여 아래의 과정을 통해 합법적인 Reader로 위장하여 Tag에게 인증을 받을 수 있는 재전송 공격을 수행할 수 있다.

① 공격자(Attacker)는 과거의 성공적인 인증 세션에서 전송된 단계 ①의 전송메시지 *query*와 R_t^{old}, 단계 ②의 전송 메시지 R_{db}^{old}, 그리고 단계 ⑦의 전송 메시지 $H(ID_{db} \oplus R_{db}^{old})$을 각각 도청한다. 여기에서 *old* 기호는 과거에 전송된 메시지를 의미한다.

② Attacker → Tag : *query*, R_t^{old}

공격자는 Reader로 위장하여 임의의 새로운 세션을 수행하기 위해 과거에 도청한 *query*와 난수 R_t^{old}을 Tag에게 전송한다.

③ Tag는 *query*와 R_t^{old}을 수신 후, 임시저장장소에 R_t^{old}을 저장하게 된다.

④ Attacker → Tag : R_{db}^{old}

공격자는 과거에 도청한 R_{db}^{old}을 Tag에게 전송한다.

⑤ Tag → Attacker : $H(ID_t \| R_t^{old}) \oplus R_t^{old}$

Tag는 R_{db}^{old}을 수신 후, 임시저장소에 R_{db}^{old}을 저장하게 된다. Tag는 자신의 ID_t와 기 저장된 R_t^{old}을 이용하여 $H(ID_t \| R_t^{old}) \oplus R_t^{old}$을 계산하여 Attacker에게 전송하게 된다.

⑥ Attacker → Tag : $H(ID_{db} \oplus R_{db}^{old})$

공격자는 Tag로부터 수신 한 $H(ID_t \| R_t^{old}) \oplus R_t^{old}$을 버리고, Tag를 인증한 것처럼 위장하여 상호인증을 수행하기 위해 과거에 도청한 $H(ID_{db} \oplus R_{db}^{old})$을 Tag에게 전송한다.

⑦ Tag는 $H(ID_{db} \oplus R_{db}^{old})$을 수신 후, 자신의 ID_t와 기 저장된 R_{db}^{old}을 이용하여 $H(ID_t \oplus R_{db}^{old})$을 계산한 후, 공격자로부터 수신 한 $H(ID_{db} \oplus R_{db}^{old})$와 일치 여부를 비교하게 된다. $H(ID_t \oplus R_{db}^{old})$와 $H(ID_{db} \oplus R_{db}^{old})$는 항상 동일한 값이 됨을 쉽게 알 수 있다. 결론적으로 두 값은 항상 일치함으로, Tag는 공격자를 인증하게 되어 공격자가 수행한 재전송 공격은 성공하게 된다.

위 재전송 공격을 통하여 공격자는 합법적인 Reader로 위장하여 Tag에게 인증을 받음으로써 이후에 송수신하게 되는 중요한 정보들을 쉽게 획득할 수 있다.

4. 제안하는 일회성 난수를 이용한 RFID 상호인증 프로토콜

본 장에서는 Kim-Jun이 제안한 RFID 상호인증 프로토콜이 가지는 재전송 공격에 대한 보안 취약점을 간단히 해결할 수 있는 개선된 일회성 난수를 이용한 RFID 상호인증 프로토콜 소개한다. 제안한 프로토콜에서는 기존에 제안된 해쉬-락 기법, 확장된 해쉬-락, 해쉬기반 ID 변형기법, 개선된 해쉬기반 ID 변형기법에서와 마찬가지로 Tag도 임의의 난수를 생성하여 상호인

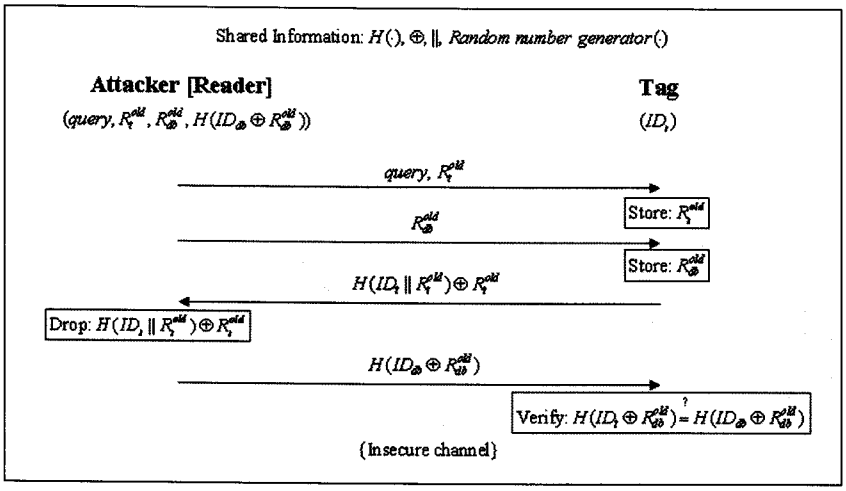

그림 2 Kim-Jun 프로토콜에 대한 재전송 공격

증을 수행케 함으로써 재전송 공격을 막도록 설계하였다. 그림 3은 제안한 프로토콜의 세부 동작과정을 보여주며 다음과 같이 총 8단계로 수행되어 진다. Kim-Jun의 프로토콜과 마찬가지로 DB와 Reader 사이의 채널은 안전한 채널(Secure Channel)이며 Reader와 Tag 사이의 채널은 공개된 채널(Open Channel)이라 가정한다.

① Reader → Tag : *query*, R_r

Reader → DB : *query*

Reader는 감응 인식 범위 내에 Tag가 존재하면 난수 R_r을 생성하여 *query*와 함께 Tag에게 전송한다. 동시에 Reader는 DB에게도 *query*를 전송한다.

② DB → Reader : R_{db}

Tag는 *query*와 R_r을 수신 후, 임시저장장소에 R_r을 저장한다.

DB는 *query*을 수신 후, 난수 R_{db}을 생성하여 Reader에게 전송한다.

③ Reader → Tag : R_{db}

Reader는 DB로부터 수신한 R_{db}을 Tag에게 전송한다.

④ Tag → Reader : $H(ID_t\|R_t\|R_r)$, R_t

Tag는 R_{db}을 수신 후, 임시저장소에 R_{db}을 저장한다. Tag는 난수 R_t을 생성하여 자신의 ID_t와 기 저장된 R_r을 이용하여 $H(ID_t\|R_t\|R_r)$을 계산하여 R_t와 함께 Reader에게 전송한다.

⑤ Reader → DB : $H(ID_t\|R_t\|R_r)$, R_t, R_r

Reader는 자신이 생성한 난수 R_r과 Tag로부터 수신한 $H(ID_t\|R_t\|R_r)$와 R_t을 DB에게 전송한다.

⑥ DB → Reader : ID_{db}, $H(ID_{db}\|R_r\|R_{db}\|R_t)$

DB는 ID 테이블에 저장된 Tag의 ID_{db}와 수신한 R_t와 R_r을 이용하여 $H(ID_{db}\|R_t\|R_r)$을 계산한 후, Tag로부터 수신 한 $H(ID_t\|R_t\|R_r)$와 일치 여부를 비교한다. 만약 두 값이 일치한다면, DB는 Tag를 인증하게 되고 상호인증을 위해 ID_{db}와 $H(ID_{db}\|R_r\|R_{db}\|R_t)$을 Reader에게 전송한다. 그렇지 않다면 인증과정을 중지한다.

⑦ Reader → Tag : $H(ID_{db}\|R_r\|R_{db}\|R_t)$

Reader는 DB로부터 수신 한 $H(ID_{db}\|R_r\|R_{db}\|R_t)$을 Tag에게 전송한다.

⑧ Tag는 $H(ID_{db}\|R_r\|R_{db}\|R_t)$을 수신 후, 자신의 ID_t와 기 저장된 R_{db}와 R_r 그리고 자신이 생성한 난수 R_t을 이용하여 $H(ID_t\|R_r\|R_{db}\|R_t)$을 계산한 후, Reader로부터 수신 한$H(ID_{db}\|R_r\|R_{db}\|R_t)$와 일치 여부를 비교한다. 만약 두 값이 일치한다면, Tag는 Reader를 인증하게 되고 계속되는 과정을 수행한다. 그렇지 않다면 인증과정을 중지한다.

5. 안전성과 효율성 분석

본 장에서는 제안한 RFID 상호인증 프로토콜에 대한 안전성(Security)과 효율성(Efficiency)을 분석한다.

5.1 안전성 분석

일반적으로 RFID 시스템에서는 상호인증(Mutual Authentication), 도청 공격(Eavesdropping Attack), 재전송 공격(Replay Attack), 스푸핑 공격(Spoofing Attack), 트래픽 분석 공격(Traffic Analysis Attack), 위치 트래

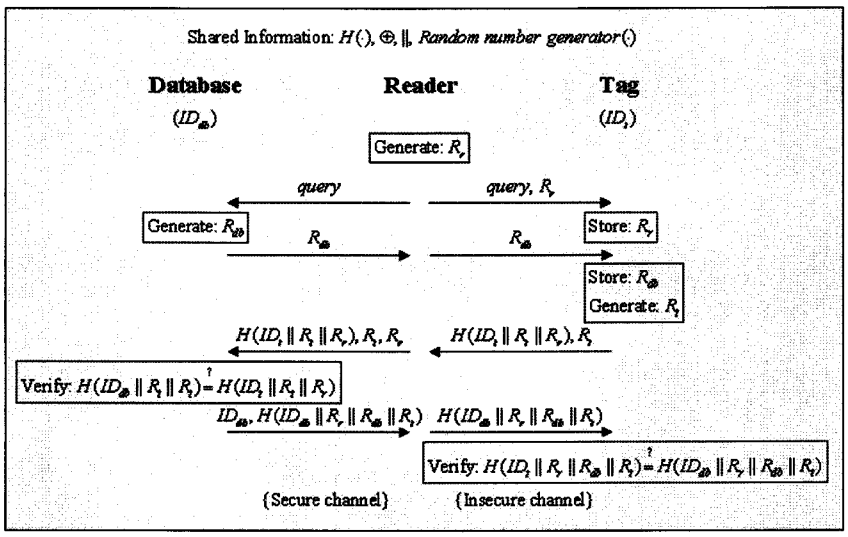

그림 3 제안한 일회성 난수를 이용한 RFID 상호인증 프로토콜

킹 공격(Location Tracking Attack), 서비스 거부 공격(Denial of Service Attack) 등과 같은 보안 문제들을 고려하여 설계되어져야 한다[7-14]. 제안한 프로토콜은 다음과 같이 상호인증을 명시적으로 제공함으로 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 안전하다.

1) 상호인증(Mutual Authentication): 상호인증은 태그와 리더 모두 상대 통신 당사자가 합법적인지를 명시적인 인증을 통해 확인하는 것이다. 제안한 프로토콜의 단계 ⑥에서 DB는 Tag로부터 수신한 $H(ID_t \| R_t \| R_r)$가 DB 자신이 계산한 $H(ID_{db} \| R_t \| R_r)$과 동일한지를 검증하며, 단계 ⑧에서 Tag는 Reader로부터 수신한 $H(ID_{db} \| R_r \| R_{db} \| R_t)$가 Tag 자신이 계산한 $H(ID_t \| R_r \| R_{db} \| R_t)$와 동일한지를 검증한다. Tag와 DB 사이에 공유된 비밀키 역할을 하는 식별자인 ID_t 또는 ID_{db}을 모르는 공격자는 Tag 또는 Reader로 위장하여 위장 공격 등을 수행할 수 없게 된다. 따라서 제안한 프로토콜은 상호인증을 제공한다.

2) 도청 공격(Eavesdropping Attack): 도청공격은 공격자가 Tag와 Reader간에 송수신되는 모든 통신 내용을 엿들은 후 Tag에 저장된 비밀 정보를 알아내고자 하는 공격이다. 제안한 프로토콜에서 공격자는 공개된 통신 채널 상으로 송수신되는 통신 메시지 *query*, R_{db}, R_r, R_t, $H(ID_t \| R_t \| R_r)$, $H(ID_{db} \| R_r \| R_{db} \| R_t)$ 등을 도청할 수 있다. 하지만 도청한 내용으로부터 공격자는 Tag와 Reader의 DB 간에 공유된 비밀키 역할을 하는 식별자인 ID_t 또는 ID_{db}를 구할 수 없다. 즉, ID_t 또는 ID_{db}을 얻기 위해서는 공격자가 $H(ID_t \| R_t \| R_r)$ 또는 $H(ID_{db} \| R_r \| R_{db} \| R_t)$로부터 ID_t 또는 ID_{db}을 얻을 수 있어야 한다. 하지만 안전한 일방향 해쉬 함수의 성질에 의해 공격자는 $H(ID_t \| R_t \| R_r)$ 또는 $H(ID_{db} \| R_r \| R_{db} \| R_t)$로부터 ID_t 또는 ID_{db}을 얻는 것은 불가능하다. 또한 비밀 값인 ID_t 또는 ID_{db}는 Tag와 DB측에서 내부적으로 활용되어 지며 공개된 통신 채널로 평문(Plantext) 형태로는 전송되어 지지 않기에 공격자는 ID_t 또는 ID_{db}를 구할 수 없다. 따라서 제안한 프로토콜은 도청 공격에 안전하다.

3) 재전송 공격(Replay Attack): 재전송 공격은 수동적 공격자가 과거에 Reader와 Tag 사이에 통신한 내용들을 도청한 후 이를 재전송하여 합법적인 Tag로 인증받으려는 공격이다. 제안한 프로토콜에서는 매 인증 세션마다 DB와 Reader 그리고 Tag가 각각 새로운 난수들(R_{db}, R_r, R_t)을 생성하여 상호인증을 수행하기 때문에 과거에 공격자에 의해 재전송된 난수 값들은 Tag와 Reader의 DB간의 상호인증 과정 중에 쉽게 검출된다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

4) 스푸핑 공격(Spoofing Attack): 스푸핑 공격은 공격자가 정당한 Tag로 위장하여 Reader로부터 인증에 필요한 정보를 획득하거나 또는 정당한 Reader로 위장하여 Tag로부터 인증에 필요한 정보를 획득하고 이를 이용하여 정당한 Tag 또는 Reader로 인증 받는 공격이다. 제안한 프로토콜에서 공격자가 DB와 Tag간에 공유된 비밀 ID_t 또는 ID_{db}을 얻을 수 있으면, 스푸핑 공격을 성공할 수 있다. 하지만 공격자는 DB와 Tag내에 각각 안전하게 저장하고 있는 비밀 ID_t 또는 ID_{db}을 직접적으로 얻을 수 있는 방법이 없다. 또한 공개된 통신 채널 상으로 송수신되는 통신 메시지 $H(ID_t \| R_t \| R_r)$ 또는 $H(ID_{db} \| R_r \| R_{db} \| R_t)$ 내의 비밀 ID_t 또는 ID_{db}는 매 세션마다 새로 생성되어 사용되어지는 난수들(R_{db}, R_r, R_t)과 안전한 일방향 해쉬 함수 $H()$에 의해 보호되어져 있다. 따라서 제안한 프로토콜은 일반적인 스푸핑 공격에 안전하다.

5) 트래픽 분석 공격(Traffic Analysis Attack): 트래픽 분석 공격은 공격자가 도청을 통해서 얻은 내용을 분석하여 Reader의 질의에 대한 Tag의 응답을 예측하여 Tag의 이동경로를 트래킹 할 수 있는 공격이다. 제안한 프로토콜에서는 난수들(R_{db}, R_r, R_t)에 의해 계산된 $H(ID_t \| R_t \| R_r)$ 또는 $H(ID_{db} \| R_r \| R_{db} \| R_t)$는 매 세션마다 변경되기에 공격자는 현재 세션에서 Tag의 응답들이 과거 세션에 도청한 응답들과 동일한지를 비교할 수 없다. 즉, 매 세션마다 서로 다른 난수들(R_{db}, R_r, R_t)을 생성함으로, 매 세션마다 서로 다른 두 개의 응답들이 과거의 응답들과의 비교를 통하여 동일한 Tag로부터 송신된 것인지 여부를 쉽게 구별할 수 없음으로 Tag의 이동경로를 쉽게 트래킹 할 수 없다. 따라서 제안한 프로토콜은 트래픽 분석 공격에 안전하다.

6) 위치 트래킹 공격(Location Tracking Attack): 위치 트래킹 공격은 공격자가 Tag의 위치변화를 감지함으로 인해 Tag 소유자의 이동 경로를 파악하여 사용자의 프라이버시를 침해하는 공격이다. 제안한 프로토콜에서는 위 트래픽 분석 공격과 마찬가지로 난수들(R_{db}, R_r, R_t)에 의해 계산된 $H(ID_t \| R_t \| R_r)$ 또는 $H(ID_{db} \| R_r \| R_{db} \| R_t)$는 매 세션마다 변경되기 때문에 공격자가 특정한 Tag를 식별할 수 없어 위치 트래킹을 할 수 없기에 사용자의 프라이버시 보호할 수 있다. 따라서 제안한 프로토콜은 위치 트래킹 공격에 안전하다.

7) 서비스 거부 공격(Denial of Service Attack): 서비스 거부 공격은 Reader 또는 Tag가 정당한 통신 상대방의 인증 요청임에도 불구하고 공격자에 의한 많은 계산이 요구되는 데이터 송신, 이전 세션에서 갱신되는

값들을 올바른 값으로 갱신되지 못하도록 방해하는 등 Reader와 Tag가 정상적인 서비스와 기능을 수행 하지 못하도록 하는 공격이다. 제안한 프로토콜에서는 Reader와 Tag간에 일방향 해쉬 함수 기반의 연산만을 이용하여 상호인증을 수행함으로, Tag 측에 서비스 거부 공격을 수행할 만큼의 많은 연산량을 요구하지 않는다. 또한 매 세션마다 DB와 Tag 간에 상호인증 완료 후 갱신되는 값이 전혀 없다. 따라서 제안한 프로토콜은 서비스 거부 공격에 안전하다.

표 1은 제안한 프로토콜과 해쉬 연산 기반의 프로토콜들인 해쉬-락 기법, 확장된 해쉬-락, 해쉬기반 ID 변형기법, 개선된 해쉬기반 ID 변형기법 그리고 Kim-Jun의 프로토콜과의 안전성을 비교 및 분석한 표이다. 표 1에서 보여주는 것과 같이 MIT 해쉬-락 기법과 확장된 해쉬-락 기법은 많은 보안 취약점들을 가진다. 해쉬기반 ID 변형 기법과 개선된 해쉬기반 ID 변형 기법은 상호인증 제공 및 재전송 공격 등에 안전하나 여전히 도청 공격, 스푸핑 공격, 위치 트래킹 공격 등에 취약하다. Kim-Jun은 기존의 기법들이 많은 보안 취약점들을 가지는 문제점들을 해결하기 위해 이들 공격에 안전한 새로운 RFID 인증 프로토콜을 제안하였으며 보안성 분석을 통해 강력한 보안성을 제공함을 증명하였다. 하지만 본 논문에서는 그들의 주장과는 달리 그들이 제안한 프로토콜이 여전히 재전송 공격에 취약함을 증명하였으며 이를 해결한 개선된 상호인증 프로토콜을 제안하였다. 결론적으로 표 1과 같이 제안한 프로토콜은 기존의 프로토콜들과 비교하여 상호인증을 명시적으로 제공함으로 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 안전함을 알 수 있다.

5.2 효율성 분석

표 2는 제안한 프로토콜과 Kim-Jun의 프로토콜과의 효율성을 비교 및 분석한 표이다. 표 2와 같이 Kim-Jun이 제안한 프로토콜과 비교하여 제안한 프로토콜은 해쉬 연산량 측면에서 동일한 성능을 보이며 특히 Tag와 DB 어디에서도 XOR 연산을 필요로 하지 않는다. 전체적으로 DB에 저장된 태그수(n)+3번의 XOR 연산량을 줄여 줄 수 있어 연산 성능 향상을 가져올 수 있다. Kim-Jun 프로토콜과 달리 Tag 측에서 추가적으로 생성되는 난수는 재전송 공격을 막기 위한 방법으로 사용되어 진다. Tag 측에서의 난수 생성 기능은 기존에 제안된 확장된 해쉬-락 기법 및 해쉬기반 ID 변형기법 등에서 사용되어 지는 방법으로 저비용 Tag 상에서도 빠른 시간 내에 충분히 수행되어 질 수 있다. Tag와 DB 간의 상호 인증을 수행하기 위해 수행되는 Step 수는 Kim-Jun이 제안한 프로토콜과 동일함을 알 수 있다. 결론적으로 제안한 프로토콜은 표 1에서 보여주는 것처럼 명시적인 상호인증을 제공함으로 인해 다양한 암호학적 공격들에 안전할 뿐만 아니라 표 2에서 보여주는 것처럼 Kim-Jun의 프로토콜과 비교하여 연산 오버헤드 차이가 많아 나지 않음으로 안전성과 효율성 모두를 보장해 줄 수 있다.

6. 결 론

본 논문에서는 2008년에 Kim-Jun이 제안한 일회용 난수 기반의 RFID 상호 인증 프로토콜이 그들의 주장

표 1 관련 프로토콜들과의 안전성 비교·분석

프로토콜 / 공격유형	MIT 해쉬-락 기법	확장된 해쉬-락 기법	해쉬기반 ID변형기법	개선된 해쉬기반 ID변형기법	Kim-Jun 프로토콜	제안한 프로토콜
상호인증	×	×	○	○	○	○
도청공격	×	×	×	×	○	○
재전송공격	×	×	○	○	×	○
스푸핑 공격	×	×	×	×	○	○
트래픽 분석 공격	×	○	○	○	○	○
위치 트래킹 공격	×	○	×	○	○	○
서비스 거부 공격	○	○	○	○	○	○

○ : 제공/안전, × : 제공안함/안전안함

표 2 관련 프로토콜들과의 효율성 비교·분석

프로토콜 / 연산종류	Kim-Jun 프로토콜			제안한 프로토콜		
	Tag	Reader	DB	Tag	Reader	DB
해쉬 연산량	2	0	n+1	2	0	n+1
XOR 연산량	2	0	n+1	0	0	0
난수 생성수	0	1	1	1	1	1
인증과정의 Step 수	7			7		

n : DB에 저장된 최대 태그수

과는 달리 여전히 RFID Reader로 위장하여 공격자가 과거의 세션에서 사용된 인증 메시지들을 이용한 재전송 공격을 수행할 수 있음을 증명하였다. 또한 동일한 연산 오버헤드를 보장하며 재전송 공격에 대한 보안 취약점을 해결한 개선된 RFID 상호 인증 프로토콜을 제안하였다. 결론적으로 제안한 RFID 상호 인증 프로토콜은 Kim-Jun의 프로토콜과 비교하여 더욱더 강한 보안성을 제공하며 안전성을 저해하지 않는 불필요한 XOR 연산을 줄여 줌으로써 효율성 측면에서도 우수하다. 따라서 제안한 RFID 상호 인증 프로토콜은 유비쿼터스 컴퓨팅 환경에서 필요한 다양한 RFID 시스템 응용 환경에 안전성 보장을 위한 프로토콜로 사용이 가능할 것으로 기대된다.

참 고 문 헌

[1] F. Klaus, "RFID handbook," Second Edition, Jone Willey & Sons, 2003.

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

[3] 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. 201-212, Springer-Verlag Heidelberg, 2004.

[4] 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.

[5] A. Juels and R. Pappu, "Squealing euros: privacy protection in RFID-enabled banknotes," In proceedings of Financial Cryptography-FC'03, Vol.2742 LNCS, pp. 103-121, Springer-Verlag, 2003.

[6] A. Juels, R. L. Rivest, 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. 103-111, 2003.

[7] S. Junichiro, H. Jae-Cheol and S. Kouichi, "Enhancing privacy of universal re-encryption scheme for RFID tags," EUC 2004, Vol.3207 LNCS, pp. 879-890, Springer-Verlag, 2004.

[8] S. A. Weis, S. Sarma, R. Rivest, D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212, Springer-Verlag, 2004.

[9] 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.

[10] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, "분산 데이타베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜," 한국정보처리학회 논문지C, 제12-C권, 제03호, pp. 309-316, 2005.

[11] 이영진, 정윤수, 서동일, 이상호, "부분ID를 이용한 읽기전용 RFID태그 인증프로토콜", 한국정보처리학회 논문지 C, 제13-C권, 제05호, pp. 595-600, 2006.10.

[12] 양형규, 안영화, "유비쿼터스 컴퓨팅 환경에 적합한 RFID 인증 프로토콜에 관한 연구", 전자공학회논문지, 제42권, 제CI-1호, pp. 45-50, 2005.

[13] 최은영, 최동희, 임종인, 이동훈, "저가형 RFID 시스템을 위한 효율적인 인증 프로토콜", 정보보호학회논문지, 제15권, 제5호, pp. 59-71, 2005.

[14] 김대중, 전문석, "일회성 난수를 이용한 안전한 RFID 상호인증 프로토콜 설계", 정보과학회논문지, 정보통신, 제35권, 제03호, pp. 243-250, 2008.

윤 은 준

1995년 2월 경일대학교 섬유패션학과(공학사). 2003년 2월 경일대학교 컴퓨터공학과(공학석사). 2007년 2월 경북대학교 컴퓨터공학과(공학박사). 2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사. 2009년~현재 경북대학교 전자전기컴퓨터학부 연구교수. 관심분야는 암호학, 정보보호, 유비쿼터스보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜 개발 등

유 기 영

1976년 경북대학교 수학교육학과(이학사). 1978년 한국과학기술원 컴퓨터공학과(공학석사). 1992년 Rensselaer Polytechnic Institute. Computer Science(공학박사). 1987년~1992년 Rensselaer Polytechnic Institute. Dept. of computer TA. 1978년 2월~현재 경북대학교 공과대학 컴퓨터공학과 정교수. 관심분야는 암호학, 정보보호, 스테가노그라피, 메쉬 네트워크 보안, RFID 보안 등