3K-RFID 인증 프로토콜에 대한 공격과 해결책

정회원 윤 은 준*, 부 기 동**, 하 경 주***, 유 기 영****°

Attack and Solution on 3K-RFID Authentication Protocol

Eun-Jun Yoon*, Ki-Dong Bu**, Kyeoung-Ju Ha***, Kee-Young Yoo****° *Regular Members*

요 약

최근 Ko-Kim-Kwon은 기존에 제안된 Henrici-Muller의 해쉬기반 RFID 인증 프로토콜이 위치트래킹 공격, 스푸핑 공격, 서비스 거부 공격 등에 안전하지 않음을 보였으며, 이러한 문제점을 해결한 새로운 RFID 인증 프로토콜(3K-RFID)을 제안하였다. 하지만, 본 논문에서는 3K-RFID 인증 프로토콜이 여전히 스푸핑 공격과 서비스 거부 공격에 취약할 뿐만 아니라 전방향 보안성을 제공하지 않음을 증명하며, 이들 문제점들을 해결한 개선된 안전한 I3K-RFID 인증 프로토콜을 제안한다.

Key Words : RFID System; Mutual Authentication; Ubiquitous; Security Analysis; Protocol

ABSTRACT

In 2005, Ko-Kim-Kwon pointed out Henrici-Muller's hash based RFID authentication protocol is insecure to location tracking attack, spoofing attack and Denial of Service attack. Then, they proposed a new RFID authentication protocol(3K-RFID) that can withstand these security problems. However, this paper shows that 3K-RFID authentication protocol is still not only vulnerable to spoofing attack and Denial of Service attack but also does not provide forward secrecy, and then proposes an improved secure I3K-RFID authentication protocol in order to resolve such problems.

Ⅰ. 서 론

오늘날 RFID(Radio Frequency Identification Device) 시스템은 유비쿼터스 컴퓨팅 환경에서 가장 중요하고 필수적인 핵심응용기술로 사용되어 지고 있다[1]. RFID 시스템은 RF Tag, Reader 그리고 백엔드 데이터베이스(DB)로 구성되어 진다. RFID 시스템에서 DB가 임의의 Tag를 식별하기 원할 때, Reader는 RF 신호를 방송 브로드캐스트하게 된다. 신호 반경 내에 존재하는 Tag는 신호에 반응(Triggered)을 하여 자신의 메모리 내에 저장된 데이터로 응답을 하게 된다. Reader는 Tag로부터 응답 메시지를 수신한 후에 자신의 백엔드 데이터베이스의 도움으로 해당 Tag가 합법적인지 아닌지를 식별하게 된다. 간단한 RFID 시스템의 응용으로써, RF Tag는 수 미터 반경 내에서 초당 100~200개의 Tag들을 읽을 수 있는 장점을 가지고 있기에 머천다이저 상에 인쇄된 UPC(Universal Product Code)인 바코드를 대신하여 사용되어 지고 있다. 특히, 스마트 라벨(Smart Label)로 사용되는 RF Tag는 자신의 메모리와 컴퓨팅 장치를 가지고 있다. 이러한 Tag는 더 나아가 접근 제어(Access Control) 또는 암호학적 기능(Cryptographic Functions) 등을 지원할 수 있어서 공급망 관리(Supply Chain Management), 재고 관리(Inventory Control), 위조 방지(Counterfeiting Prevention) 등 다양한 응용 분야에 적합한 RF Tag

* 경북대학교 전자전기컴퓨터학부(ejyoon@knu.ac.kr), ** 경일대학교 컴퓨터공학부(kdbu@kiu.ac.kr)
*** 대구한의대학교 모바일콘텐츠학부(kjha@dhu.ac.kr),
**** 경북대학교 컴퓨터공학과 정보보호연구실(yook@knu.ac.kr) (° : 교신저자)
논문번호 : KICS2008-10-482, 접수일자 : 2008년 10월 4일, 최종논문접수일자 : 2009년 5월 13일

들로 사용되어 질 수 있다[2].

하지만 RFID 시스템이 가져다주는 실용성과 편리함 이면에는 개인 정보 노출 및 위치 정보 누출 등으로 인한 개인의 프라이버시 침해 문제가 발생할 수 있다. 특히 RFID 시스템에서 발생할 수 있는 다음과 같은 여러가지 보안 취약점들은 반드시 해결하여야 할 중요한 과제이다[3]. (1) 보안성(Secrecy): 가짜 Reader가 합법적인 Tag를 속여 Tag 내의 중요한 비밀 정보를 획득할 수 있다. (2) 위치 프라이버시(Location Privacy): 악의적인 공격자가 제품 내에 포함된 임의의 Tag에 대한 추적을 통하여 사용자의 위치를 노출할 수 있다. (3) 전방향 보안성(Forward Secrecy): 공격자는 탈취한 Tag 내에 저장된 데이터를 이용하여, 해당 Tag가 참여한 과거의 모든 통신 내용을 추적하여 해당 제품의 이전 배송 위치 등이 노출되어 질 수 있다. (4) 재전송 공격(Replay Attack)과 서비스 거부 공격(DOS attack): 안전하지 않는 RFID 인증 프로토콜 설계로 인해 재전송 공격과 서비스 거부 공격 등에 취약할 수 있다.

위와 같은 프라이버시 침해 문제 등 보안 문제점들을 해결하기 위해, 많은 연구자들에 의해 해쉬-락 기법, 확장된 해쉬-락, 해쉬기반 ID 변형기법, 개선된 해쉬기반 ID 변형기법 등 다양한 RFID 인증 프로토콜(Authentication Protocol)들이 최근까지 제안되어져 오고 있다[4-24]. 또한 현재까지 제안되어져 오고 있는 많은 RFID 인증 프로토콜들이 태그의 재사용이 불가능하거나, 위치추적이 쉬우며, 재전송 공격이나 스푸핑 공격에 취약하는 등 다양한 보안 취약점들을 가짐을 많은 연구자들에 의해 계속 발견되어 지고 있다[6-24].

특히 최근 Ko-Kim-Kwon[17]은 기존에 제안된 Henrici-Muller[12]의 해쉬기반 RFID 인증 프로토콜이 위치트래킹 공격, 스푸핑 공격, 서비스거부 공격 등에 안전하지 않음을 보였으며, 이러한 문제점을 해결한 새로운 RFID 인증 프로토콜(3K-RFID)을 제안하였다. 하지만, 본 논문에서는 3K-RFID 인증 프로토콜이 여전히 Reader로의 스푸핑 공격과 서비스 거부 공격에 대해 취약할 뿐만 아니라 전방향 보안성을 제공하지 않음을 증명하며, 이러한 공격과 문제점들을 해결한 개선된 RFID 상호인증 프로토콜(I3K-RFID)을 제안한다. 결론적으로 제안한 I3K-RIFD 인증 프로토콜은 RFID 시스템에서 요구되는 보안 요구사항들을 모두 만족하며 경량의 해쉬 함수를 기반으로 인증을 수행하기 때문에 효율성을 보장할 수 있다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 관련연구로써 RFID 시스템 환경과 요구되는 보안 요구사항들에 대하여 정의한다. 3장에서는 Ko-Kim-Kwon이 제안한 3K-RFID 인증 프로토콜에 대해 설명하며, 4장에서는 3K-RFID 프로토콜이 스푸핑 공격 및 서비스 거부 공격에 취약하며 전방향 보안성을 제공하지 않음을 증명한다. 5장에서는 제안하고자하는 I3K-RFID 상호 인증 프로토콜에 대해 구체적으로 설명하고, 6장에서는 제안된 인증 프로토콜과 기존의 인증 프로토콜들을 안정성과 효율성 측면에서 비교 및 분석한다. 마지막으로 7장에서는 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 RFID 시스템 환경 및 필요한 보안 요구사항들을 기술한다[3].

2.1 RFID 시스템 환경

본 절에서는 RFID 시스템 환경에 관해 기술한다. 일반적으로 RFID 시스템은 다음과 같은 가정들 하에 운영된다.

(1) RFID 시스템은 그림 1과 같이 백엔드 데이터베이스 서버, RFID Reader, RFID Tag들의 3종류의 컴포넌트들로 구성되어 진다.
(2) 백엔드 데이터베이스 서버는 각 Tag를 위한 ID와 제품 정보 등 필요한 정보 집합을 관리하고 있다.
(3) 각 Tag는 읽고 쓰기가 가능한 메모리를 내장하고 있다.

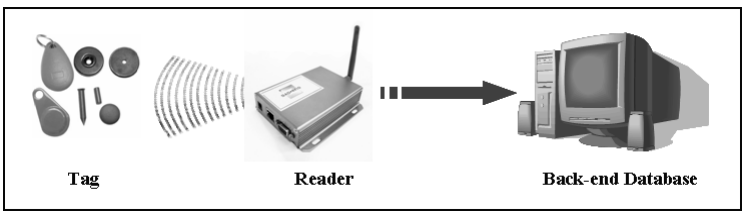


그림 1. RFID 시스템

(4) Reader와 Tag 사이의 채널은 안전하지 않으며 모든 통신 메시지들은 공격자에 의해 엿보기나 수정이 가능하다.
(5) RFID 인증 프로토콜은 3가지 흐름(Flow)으로 구성되어 진다. 통상적으로 첫 번째 흐름에서 Reader는 Tag에게 쿼리(Query) 메시지를 보내며, 두 번째 흐름에서 Tag가 자신을 인증받기 위해 Reader에게 답장(Replay) 메시지를 보내며, 세 번째 흐름에서 Reader가 자신을 인증받기 위해 Tag에게 응답(Response) 메시지를 보내게 된다.
(6) DB와 Tag는 상호 인증을 위해 비밀 값들을 공유하고 있다. 만약 성공적으로 상호 인증 세션을 수행하게 되면 그들은 동시에 공유된 비밀 값들을 갱신한다. 즉, DB는 두 번째 흐름에서 Tag를 인증하게 되면 저장된 Tag의 비밀 값을 갱신하게 되며, Tag는 세 번째 흐름에서 DB를 인증하게 되면 저장된 자신의 비밀 값을 갱신하게 된다.

2.2 보안 요구사항들

본 절에서는 RFID 시스템 환경에서의 보안 요구사항들을 기술한다. 일반적으로 RFID 시스템에서 다음의 세가지 속성에 의해 프라이버시(Privacy)를 정의하고 있다.

(1) Tag ID 익명성(Tag ID Anonymity): Tag의 ID는 평문 형태로 전송 되지 않아야 하며, 또한 Tag와 Reader 사이의 통신 채널 상으로부터 쉽게 계산되어지지 않아야만 된다.
(2) 개개의 위치 프라이버시(Individual Location Privacy): Tag와 Reader 사이의 통신 메시지 내용으로부터 Tag의 ID를 추적(Trace)할 수 없어야 한다. 만약 공격자(Adversary)가 임의의 통신 메시지 내용이 특정한 Tag로부터 송신되어 졌음을 구분할 수 있다면 해당 공격자는 Tag의 위치를 추적할 수 있게 된다.
(3) 전방향 보안성(Forward Secrecy): 비록 공격자가 임의의 Tag를 탈취하여 Tag내의 메모리에 저장된 중요한 정보들을 얻었더라도, 공격자는 이러한 정보와 함께 과거에 해당 Tag가 참여한 모든 통신 메시지를 이용하더라도 Tag를 추적할 수 없어야 한다.

또한, 다양한 보안 위협들로부터 안전하기 위해 RFID 시스템에서는 다음과 같은 공격들에 대해 견고하여야 한다.

(4) 재전송 공격(Replay Attack): 공격자는 Tag와 Reader 사이의 모든 통신 메시지들을 도청할 수 있으며 더 나아가 해당 공격자가 도청한 메시지들의 재전송을 통하여 합법적인 Tag 또는 Reader로 위장하여 인증을 받을 수 있다.
(5) 스푸핑 공격(Spoofing Attack): 일반적으로 Tag와 Reader 사이의 통신 채널은 안전하지 않은 공개 무선 채널이기 때문에, 공격자는 쉽게 송수신되는 모든 통신 메시지들을 엿볼 수 있다. 이에 공격자는 정당한 통신 당사자로 위장하여 Tag와 Reader간의 인증과정을 통과할 수 있다.
(6) 서비스 거부 공격(Denial Of Service Attack): 공격자는 간단한 메시지 위조 또는 가로채기 등을 통하여 Tag와 Reader 사이에 공유된 비밀 데이터를 비동기화(Desynchronize) 시킬 수 있다. 이로 인해 더 이상 Tag는 합법적인 Reader의 DB로부터 인증을 받을 수 없게 된다.

Ⅲ. 3K-RFID 인증 프로토콜

본 장에서는 Ko-Kim-Kwon[17]이 제안한 3K-RFID 인증 프로토콜에 대해 소개한다.

3.1 시스템 파라미터

3K-RFID 인증 프로토콜과 제안한 개선된 인증 프로토콜에서 사용되는 시스템 파라미터는 다음 표 1과 같다.

3.2 3K-RFID 인증 프로토콜

그림 2는 3K-RFID 인증 프로토콜의 세부 동작 과정을 보여주며 다음과 같이 총 5단계로 수행되어 진다. 여기에서 일반적인 RFID 시스템에서와 같이

표 1. 시스템 파라미터

기호	의미
Query	태그의 응답을 요청하는 리더의 요청
ID	태그에게 할당된 고유 식별자
h()	안전한 일방향 해쉬 함수
PRNG()	의사 난수 생성기(Pseudo Random Number Generator)
T	태그가 매 세션마다 생성하여 리더에게 전송하는 난수
Info	제품의 자세한 정보
$\oplus$	비트 단위 배타적 논리합(XOR) 연산
$\|$	연접(Concatenation) 연산

DB와 Reader 사이의 채널은 안전한 채널(Secure Channel)이며 Reader와 Tag 사이의 채널은 안전하지 않은 채널(Insecure Channel)이라 가정한다.

Step 1 : Reader → Tag : Query
Reader는 감응 인식 범위 내에 Tag가 존재하면 Query를 Tag에게 전송한다.

Step 2 : Tag → Reader : A, T
Tag는 Query를 수신 후, 난수 T를 생성한다. 생성한 난수 T와 Tag 내에 저장된 ID를 이용하여 A=h(ID||T)를 계산한다. Tag는 A와 T를 Reader에게 전송한다.

Step 3 : Reader → DB : A, T
Reader는 Tag로부터 수신한 A와 T를 DB에게 전송한다.

Step 4 : DB → Reader : A'
DB는 Reader로부터 A와 T를 수신 후, DB는 자신의 데이터베이스 내의 Tag 레코드를 찾기 위해, 데이터베이스 내의 ID 테이블에 저장된 Tag의 ID와 수신한 T를 이용하여 검색키 A'=h(ID||T)을 계산한다. DB는 검색키 A'이 수신한 A와 동일한지 검증한다. 만약 임의의 ID로부터 계산된 A'이 Tag로부터 수신 한 A와 동일한 결과를 가지게 되면, DB는 Tag를 인증하게 되고 상호인증을 위해 A'을 Reader에게 전송하고, 동시에 DB는 새로운 IDnew=ID⊕A를 계산하여 과거의 ID를 IDnew로 갱신한다. 그렇지 않다면 인증과정을 중지한다.

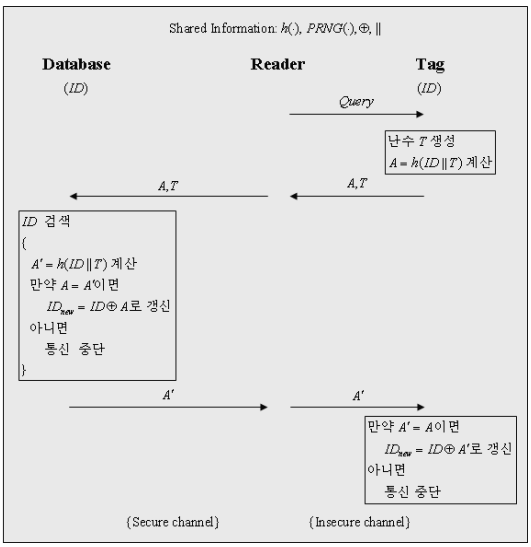


그림 2. 3K-RFID 인증 프로토콜

Step 5 : Reader → Tag : A'
Reader는 DB로부터 수신 한 A'을 Tag에게 전송한다.

Step 6 : Tag는 A'을 수신 후, 자신이 계산한 A와 동일한지를 검증한다. 만약 두 값이 일치한다면, Tag는 Reader를 인증하게 되고 새로운 IDnew=ID⊕A'을 계산하여 과거의 ID를 IDnew로 갱신한다. 그렇지 않다면 인증과정을 중지한다.

Ⅳ. 3K-RFID 인증 프로토콜에 대한 취약점 분석

본 장에서는 3K-RFID 인증 프로토콜이 반사 공격(Reflection Attack)을 이용한 스푸핑 공격과 서비스 거부 공격에 취약함을 증명하며, 더 나아가 중요한 전방향 보안성(Forward Secrecy)을 제공하지 않음을 증명한다.

4.1 반사 공격을 이용한 스푸핑 공격과 서비스 거부 공격 문제

본 절에서는 3K-RFID 인증 프로토콜이 반사 공격(Reflection Attack)을 이용한 스푸핑 공격과 서비스 거부 공격에 취약함을 증명한다. 반사 공격은 임의의 통신에서 통신에 참가하고 있는 합법적인 당사자들의 값을 공격자가 도청하여 아무런 메시지 변조를 수행하지 않고 그대로 송신자에게 반사(Reflection)를 시켜 합법적인 통신 당사자로 위장하여 수신자로부터 인증을 받을 수 있는 간단한 수동적인 공격유형이다. 이에, 3K-RFID 인증 프로토콜에서 공격자(Attacker)는 다음과 같은 간단한 반사 공격을 수행하여 합법적인 Reader로 쉽게 위장하여 Tag에게 인증을 받을 수 있다. 그림 3은 3K-RFID 인증 프로토콜에 대한 반사 공격 과정을 보여 준다.

Step 1* : Attacker → Tag : Query
Attacker는 감응 인식 범위 내에 Tag가 존재하면 Query를 Tag에게 전송한다.

Step 2* : Tag → Attacker : A, T
Tag는 Query를 수신 후, 난수 T를 생성하게 된다. 생성한 난수 T와 자신의 메모리에 저장된 ID를 이용하여 A=h(ID||T)를 계산한 후, A와 T를 Attacker에게 전송하게 된다.

Step 3* : Attacker → Tag : A*

Attacker는 Tag로부터 A와 T를 수신 후, A*=A로 두어 Tag에게 전송하여 반사 공격을 수행한다.

Step 4* : Tag는 A*을 수신 후, 자신이 계산한 A와 동일한지를 검증하게 된다. 위 step 2에서 계산한 A=h(ID||T)는 Attacker가 반사한 A*와 항상 두 값이 일치함으로, Tag는 Attacker를 쉽게 인증하게 되고 새로운 ID_{new}=ID⊕A*을 계산하여 과거의 ID를 ID_{new}로 갱신하게 된다.

결론적으로 3K-RFID 인증 프로토콜은 반사 공격에 취약함을 알 수 있다. 더 나아가 반사 공격으로 인해 공격자는 Tag로부터 합법적인 Reader로 인증을 받게 되어 스푸핑 공격을 성공하게 된다. 이로 인해 이후에 송수신되는 모든 기밀 메시지를 엿볼 수 있게 된다. 또한 이후의 모든 통신 세션에서 Reader의 백엔드 DB는 자신의 DB 테이블 내에 저장하고 있는 Tag의 ID값을 이용하여 계산 한 A'=h(ID||T) 값이 Tag가 송신한 A와 같지 않음을 판단하게 되어, 메시지에 대한 인증 또한 올바르게 수행 할 수 없는 서비스 거부 공격에 취약하게 된다.

4.2 전방향 보안성 문제

RFID 인증 프로토콜이 전방향 보안성(Forward Secrecy)을 제공하기 위해서는 다음과 같은 조건을 만족하여야 한다. 즉, 비록 공격자가 임의의 Tag를 탈취하여 Tag내의 메모리에 저장된 중요한 정보들을 얻었더라도, 공격자는 이러한 정보와 함께 과거에 해당 Tag가 참여한 모든 통신 메시지를 이용하더라도 Tag를 추적할 수 없어야 한다. 하지만 3K-RFID 인증 프로토콜은 다음과 같이 전방향 보안성을 제공하지 않는다.

Step 1* : 공격자가 임의의 Tag를 탈취하여 Tag내의 메모리에 저장된 중요한 정보인 ID_{new}를 얻었다고 가정하자. 여기에서 IDnew는 ID⊕A 임을 3K-RFID 인증 프로토콜의 단계 4로부터 쉽게 알 수 있다.

Step 2* : 공격자는 탈취한 ID_{new}와 함께 이전 세션에서 해당 Tag가 참여한 통신 메시지 A 또는 A'을 이용하여 ID_{new}⊕A 연산을 수행하여 이전의 비밀 ID를 쉽게 얻을 수 없다. 즉, ID_{new}⊕A=ID⊕A⊕A=ID가 됨으로 ID를 쉽게 얻을 수 있다.

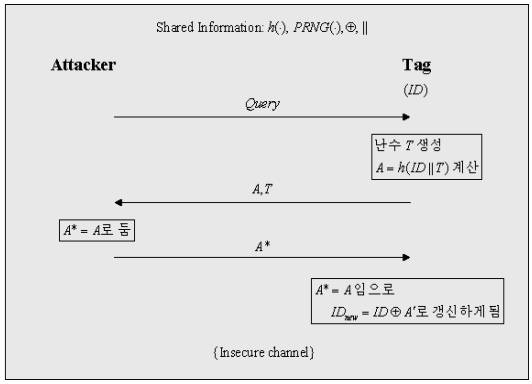


그림 3. 3K-RFID 인증 프로토콜에 대한 반사 공격

Step 3* : 공격자는 더 나아가 획득한 ID와 이전 이전 세션에서 도청한 A_{old} 또는 A'_{old}를 이용하여 ID⊕A_{old} 연산을 수행하여 이전 이전의 비밀 ID_{old}도 쉽게 얻을 수 없다.

결론적으로 위와 같은 방법을 수행하여 공격자는 과거의 모든 ID를 얻을 수 있기에 공격자는 임의의 Tag를 쉽게 추적할 수 있다. 따라서 3K-RFID 인증 프로토콜은 전방향 보안성을 제공하지 않음을 알 수 있다.

Ⅴ. 제안하는 I3K-RFID 인증 프로토콜

그림 4는 위 3K-RFID 인증 프로토콜에서의 반사 공격을 간단히 막을 수 있는 개선된 3K-RFID (I3K-RFID) 인증 프로토콜의 세부 동작과정을 보여주며 다음과 같이 총 5단계로 수행되어 진다. 여기에서 일반적인 RFID 시스템에서와 같이 DB와 Reader 사이의 채널은 안전한 채널(Secure Channel)이며 Reader와 Tag 사이의 채널은 안전하지 않은 채널(Insecure Channel)이라 가정한다.

Step 1 : Reader → Tag : Query

Reader는 감응 인식 범위 내에 Tag가 존재하면 Query를 Tag에게 전송한다.

Step 2 : Tag → Reader : A, T

Tag는 Query를 수신 후, 난수 T를 생성한다. 생성한 난수 T와 Tag 내에 저장된 ID를 이용하여 A=h(ID||T)를 계산한다. Tag는 A와 T를 Reader에게 전송한다.

Step 3 : Reader → DB : A, T

Reader는 Tag로부터 수신한 A와 T를 DB에게 전송한다.

Step 4 : DB → Reader : B, Info

DB는 Reader로부터 A와 T를 수신 후, DB는 자신의 데이터베이스 내의 Tag 레코드를 찾기 위해, 데이터베이스 내의 ID 테이블에 저장된 Tag의 ID와 수신한 T를 이용하여 검색키 A'=h(ID||T)을 계산한다. DB는 검색키 A'이 수신한 A와 동일한지 검증한다. 만약 임의의 ID로부터 계산된 A'이 Tag로부터 수신 한 A와 동일한 결과를 가지게 되면, DB는 Tag를 인증하게 되고, 다음 세션을 위해 새로운 ID_{new}=h(ID||A)를 계산하여 과거의 ID를 ID_{new}로 갱신하고, 동시에 상호인증을 위해 B=h(ID_{new})를 계산하여 제품에 대한 자세한 정보를 담고 있는 Info와 함께 Reader에게 전송한다. 그렇지 않다면 인증과정을 중지한다.

Step 5 : Reader → Tag : B

Reader는 DB로부터 수신 한 Info를 이용하여 필요한 정보를 획득하고, B를 Tag에게 전송한다.

Step 6 : Tag는 B를 수신 후, 새로운 ID_{new}=h(ID||A)를 먼저 계산한 후 검증 값 B'=h(ID_{new})을 계산한다. Tag는 자신이 계산한 B'이 수신한 B와 동일한지를 검증한다. 만약 두 값이 일치한다면, Tag는 Reader를 인증하게 되고 다음 세션을 위해 과거의 ID를 ID_{new}로 갱신한다. 그렇지 않다면 인증과정을 중지한다.

Ⅵ. 보안성과 효율성 분석

본 장에서는 제안한 I3K-RFID 상호인증 프로토콜에 대한 안전성과 효율성에 대해 증명한다.

6.1 보안성 분석

본 절에서는 제안한 I3K-RFID 인증 프로토콜이 2장에서 설명한 보안 요구사항들인 프라이버시 제공과 다양한 공격들에 안전함을 증명한다. 먼저, 제안한 I3K-RFID 인증 프로토콜의 안전성 분석을 위해 필요한 중요한 보안 항목을 다음과 같이 정의한다[25].

정의 1. 강력한 비밀 키(I3K-RFID 인증 프로토콜에서 ID)는 높은 엔트로피(entropy)를 가지는 값으로써 다항식시간(Polynomial time) 내에 추측되어 질 수 없다.

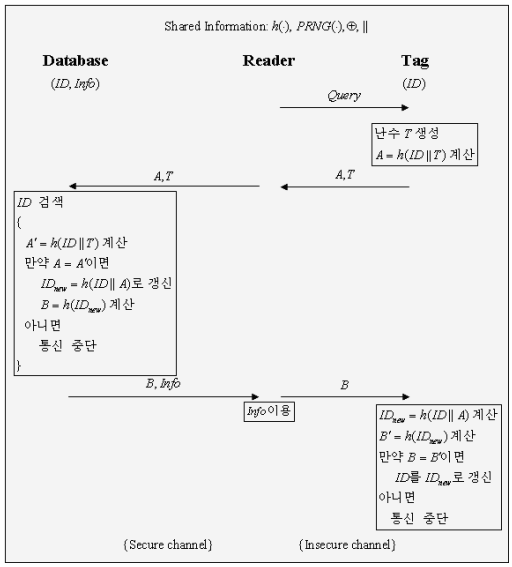


그림 4. 제안한 I3K-RFID 인증 프로토콜

정의 2. 안전한 일방향 해쉬 함수(Secure one-way hash function) y = h(x)에서, 주어진 x를 이용하여 y를 계산하는 것은 쉽지만, 주어진 y를 이용하여 x를 계산하는 것은 어렵다.

위의 정의 1과 2를 기반으로 제안한 I3K-RFID 인증 프로토콜은 다음의 Tag ID 익명성(Tag ID Anonymity), 개개의 위치 프라이버시(Individual Location Privacy), 전방향 보안성(Forward Secrecy), 재전송 공격(Replay Attack), 스푸핑 공격(Spoofing Attack), 서비스 거부 공격(Denial Of Service Attack)과 같은 6가지 보안 속성들을 만족한다.

(1) Tag ID 익명성(Tag ID Anonymity): 제안한 I3K-RFID 인증 프로토콜에서 Tag의 ID는 평문 형태로 전송 되지 않는다. 또한 제안한 I3K-RFID 인증 프로토콜의 Step 2와 4에서 각각 전송되어 지는 A=h(ID||T)와 B=h(IDnew) 값으로부터 공격자는 현재 세션에 사용되어 지는 비밀 ID와 다음 세션을 위해 사용되어 지는 비밀 IDnew를 얻을 수 없다. 즉, 위 정의 2의 안전한 일방향 해쉬 함수(Secure one-way hash function)의 성질에 의해 공격자는 A=h(ID||T)와 B=h(IDnew) 값으로부터 ID와

표 2. 관련 프로토콜들과의 안전성 비교·분석

프로토콜 / 공격유형	MIT 해쉬-락	확장된 해쉬-락	해쉬기반 ID변형	개선된 해쉬기반 ID변형	3K-RFID	I3K-RFID
상호인증	×	×	○	○	○	○
Tag ID 익명성	×	○	○	○	○	○
위치 프라이버시	×	○	×	○	○	○
전방향 보안성	×	×	×	×	×	○
재전송공격	×	×	○	○	○	○
스푸핑 공격	×	×	×	×	×	○
서비스 거부 공격	○	○	○	○	×	○

○ : 제공함/안전함, × : 제공안함/안전안함

IDnew를 얻을 수 없다. 따라서 제안한 I3K-RFID 인증 프로토콜은 Tag와 Reader 사이의 통신 채널 상으로부터 쉽게 Tag의 ID를 계산할 수 없기에 Tag ID 익명성을 제공한다.

(2) 개개의 위치 프라이버시(Individual Location Privacy): 제안한 I3K-RFID 인증 프로토콜에서 공격자는 Tag와 Reader 사이의 통신 메시지 내용으로부터 Tag의 ID를 추적(Trace)할 수 없다. 제안한 프로토콜에서는 난수 T에 의해 계산된 A와 B는 매 세션마다 변경되기 때문에 공격자가 특정한 Tag를 식별할 수 없어 위치 트래킹을 할 수 없기에 사용자의 프라이버시 보호할 수 있다. 또한 공격자는 현재 세션에서 Tag의 응답들이 과거 세션에 도청한 응답들과 동일한지를 비교할 수 없다. 즉, 매 세션마다 서로 다른 난수 T를 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 개개의 위치 프라이버시(Individual Location Privacy)를 보장한다.

(3) 전방향 보안성(Forward Secrecy): 제안한 프로토콜에서 공격자가 임의의 Tag를 탈취하여 Tag내의 메모리에 저장된 중요한 정보인 ID를 얻었다고 가정하자. 하지만 공격자는 탈취한 ID와 함께 과거에 해당 Tag가 참여한 모든 통신 메시지를 이용하더라도 이전의 비밀 ID를 얻을 수 없다. 즉, IDnew=h(ID||A)로부터 과거의 ID를 얻기 위해서 공격자는 일방향 해쉬 함수를 깰 수 있어야 한다. 하지만 정의 2에 의해 h(ID||A)로부터 ID를 얻는 것은 불가능하기 때문에 제안한 I3K-RFID 인증 프로토콜은 전방향 보안성을 제공하여 공격자가 임의의 Tag를 쉽게 추적할 수 없다.

(4) 재전송 공격(Replay Attack): 제안한 프로토콜에서는 매 인증 세션마다 Tag가 새로운 난수 T를 생성하여 상호인증을 수행하기 때문에 과거에 공격자에 의해 재전송된 난수 값들은 Tag와 Reader의 DB간의 상호인증 과정 중에 쉽게 검출된다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

(5) 스푸핑 공격(Spoofing Attack): 제안한 프로토콜에서 공격자가 DB와 Tag간에 공유된 비밀 ID를 얻을 수 있으면, 스푸핑 공격을 성공할 수 있다. 하지만 공격자는 DB와 Tag내에 각각 안전하게 저장하고 있는 비밀 ID를 직접적으로 얻을 수 있는 방법이 없다. 또한 공개된 통신 채널 상으로 송수신되는 통신 메시지 A=h(ID||T) 또는B=h(IDnew) 내의 비밀 ID는 매 세션마다 새로 생성되어 사용되어지는 난수 T와 안전한 일방향 해쉬함수 h()에 의해 보호되어져 있다. 따라서 제안한 프로토콜은 일반적인 스푸핑 공격에 안전하다.

(6) 서비스 거부 공격(Denial Of Service Attack): 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 Tag는 DB가 송신한 해쉬 값 B=h(IDnew)가 올바른 값인지 여부를 검증한 후에 과거의 ID를 새로운 IDnew로 갱신하기 때문에 공격자는 서비스 거부 공격을 성공할 수 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 3K-RFID 프로토콜과의 안전성을 비교 및 분석한 표이다. 표 1과 같이 제안한 I3K-RFID 프로토콜은 기존의 프로토콜과 비교하여 상호인증을 명시적으로 제공함으로 Tag ID 익명성 제공, 위치 프라이버시 제공, 전방향 보안성 제공 및 재전송 공격, 스푸핑 공격, 서비스 거부 공격 등에 안전함을 알 수 있다.

6.2 효율성 분석

본 절에서는 제안한 I3K-RFID 상호인증 프로토콜에 대한 효율성을 분석한다. 표 2는 제안한 I3K-RFID 인증 프로토콜과 3K-RFID 인증 프로토콜과의 효율성을 비교 및 분석한 표이다. 표 2에서 3K-RFID 인증 프로토콜과 비교하여 Tag와 DB 측에서 각각 계산되는 2번의 추가적인 해쉬 연산들은 3K-RFID 인증 프로토콜이 가지는 스푸핑 공격과 서비스 거부 공격에 취약한 문제점 해결과 전방향 보안성을 제공하기 위한 방법으로 사용되어 진다. 또한 3K-RFID 인증 프로토콜과 비교하여 제안한 I3K-RFID 인증 프로토콜은 Tag와 DB 어디에서도 XOR 연산을 필요로 하지 않으며, 인증 과정의 라운드 수는 동일함을 알 수 있다. 결론적으로 제안한 I3K-RFID 인증 프로토콜은 표 1에서 보여주는 것처럼 명시적인 상호인증을 제공함으로 인해 다양한 암호학적 공격들에 안전할 뿐만 아니라 표 2에서 보여주는 것처럼 3K-RFID 인증 프로토콜과 비교하여 연산 오버헤드 차이가 많아 나지 않음으로 안전성과 효율성 모두를 보장해 줄 수 있다.

Ⅶ. 결 론

현재 유비쿼터스 환경에 적합한 RFID 인증 프로토콜에 관하여 많은 연구가 진행 중에 있다. 본 논문에서는 2005년에 Ko-Kim-Kwon에 제안한 3K-RFID 인증 프로토콜이 여전히 스푸핑 공격과 서비스 거부 공격에 취약할 뿐만 아니라 전방향 보안성을 제공하지 않음을 증명하였으며, 이들 문제점들을 해결한 개선된 안전한 I3K-RFID 인증 프로토콜을 제안하였다.

보안성 분석과 효율성 분석을 통하여 제안한 I3K-RFID 인증 프로토콜은 기존에 제안된 많은 해쉬 기반의 RFID 인증 프로토콜들과 비교하여 보다 많은 보안성을 제공하며 효율성 또한 보장됨을 증명하였다. 결론적으로 제안한 I3K-RFID 인증 프로토콜은 유비쿼터스 컴퓨팅을 구축하기 위해 RFID 시스템 요소 기술로 안전하고 효율적인 유비쿼터스 인증을 실현할 수 있을 것으로 기대한다.

표 3. 관련 프로토콜들과의 효율성 비교·분석

프로토콜 / 연산종류	3K-RFID			I3K-RFID		
	Tag	Reader	DB	Tag	Reader	DB
해쉬 연산량	1	0	n	3	0	n+2
XOR 연산량	1	0	1	0	0	0
난수 생성수	1	0	0	1	0	0
인증 라운드 수	5			5		

n : DB에 저장된 최대 태그수

참 고 문 헌

〔1〕 F. Klaus, “RFID handbook,” *Second Edition, Jone Willey & Sons,* 2003.

〔2〕 EPCglobal web site, <http://www.epcglobalinc.org/>.

〔3〕 Y. Chen, J. S. Chou, and H. M. Sun, “A novel mutual authentication scheme based on quadratic residues for RFID systems”, *Computer Networks*, Vol. 52, pp. 2373-2380, 2008.

〔4〕 S. A. Weis, “Security an privacy in radio-frequency identification devices,” *MS Thesis. MIT*. May, 2003.

〔5〕 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.

〔6〕 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.

〔7〕 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.

〔8〕 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.

〔9〕 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.

〔10〕 S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography," *in: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 63-67, 2005.

〔11〕 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.

〔12〕 D. Henrici and P. Muller, "Hash based enhancement of location privacy for radio frequency identification devices using varying identifiers," *IEEE PerSec'04*, pp. 149-153, March 2004.

〔13〕 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.

〔14〕 이영진, 정윤수, 서동일, 이상호, "부분ID를 이용한 읽기전용 RFID태그 인증프로토콜", *한국정보처리학회 논문지* C, 제13-C권, 제05호, pp. 595-600, 2006.10.

〔15〕 양형규, 안영화, "유비쿼터스 컴퓨팅 환경에 적합한 RFID 인증 프로토콜에 관한 연구," *전자공학회논문지*, 제42권, 제CI-1호, pp. 45-50, 2005.

〔16〕 최은영, 최동희, 임종인, 이동훈, "저가형 RFID 시스템을 위한 효율적인 인증 프로토콜," *정보보호학회논문지*, 제15권, 제5호, pp. 59-71, 2005.

〔17〕 고 훈, 김배현, 권문택, "RFID 환경에서 보안 통신을 위한 안전한 인증 방안에 관한 연구", *정보보증논문지*, 제5권, 제3호, pp. 59-65, 2005.

〔18〕 오수현, 곽진, "유비쿼터스 환경에 적합한 사용자 프라이버시 보호 기능을 제공하는 RFID 시스템," *한국통신학회논문지*, 제29권, 제12C호, pp. 1729-1738, 2004.

〔19〕 오수현, 곽진, "전자 태그의 보안 레벨을 기반으로 하는 RFID 인증 프로토콜," *한국통신학회논문지*, 제30권, 제6C호, pp. 593-600, 2005.

〔20〕 이영진, 문형진, 정윤수, 이상호, "랜덤 부분 ID를 이용한 저비용 RFID 상호인증 프로토콜," *한국통신학회논문지*, 제31권, 제7C호, pp. 755-760, 2006.

〔21〕 김배현, 유인태, "반사공격에 안전한 RFID 인증 프로토콜," *한국통신학회논문지*, 제32권, 제3호 (통신이론 및 시스템), pp. 348-354, 2007.

〔22〕 김석매, 이영진, 이상호, 이충세, "RFID 프라이버시를 위한 ECC기반의 익명인증기법," *한국통신학회논문지*, 제33권, 제3호(통신이론 및 시스템), pp. 293-298, 2008.

〔23〕 김수철, 여상수, 김성권, "RFID 프라이버시 보호를 위한 향상된 모바일 에이전트 기법," *한국통신학회논문지*, 제33권, 제2호(통신이론 및 시스템), pp. 208-218, 2008.

〔24〕 김대중, 전문석, "일회성 난수를 이용한 안전한 RFID 상호인증 프로토콜 설계", *정보과학회논문지*, 정보통신, 제35권, 제03호, pp. 243-250, 2008.

〔25〕 A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," *CRC Press*, New York, 1997.

윤 은 준 (Eun-Jun Yoon) 정회원

1995년 2월 경일대학교 공학사 졸업
2003년 2월 경일대학교 컴퓨터공학과 공학석사
2007년 2월 경북대학교 컴퓨터공학과 공학박사
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2009년 3월~현재 경북대학교 전자전기컴퓨터학부 계약교수
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

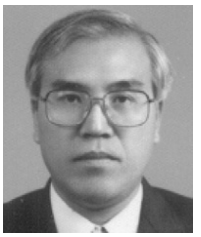
부 기 동 (Ki-Dong Bu) 정회원

1984년 2월 경북대학교 전자공학과 공학사
1988년 2월 경북대학교 전자공학과 공학석사
1996년 2월 경북대학교 전자공학과 공학박사
1983년~1985년 포항종합제철 시스템 개발실
2001년~2001년 일본 게이오대학 방문교수
1988년 3월~현재 경일대학교 컴퓨터공학과 교수
<관심분야> 데이터베이스, GIS, 시멘틱 웹, 데이터베이스 보안, RFID 보안

하 경 주(Kyeoung-Ju Ha) 정회원

1991년 2월 경북대학교 컴퓨터공학과 공학사
1993년 2월 경북대학교 컴퓨터공학과 공학석사
1996년 2월 경북대학교 컴퓨터공학과 공학박사
1996년~1999년 ETRI 부호기술연구부 선임연구원
1999년 3월~현재 대구한의대학교 모바일콘텐츠학부 부교수
<관심분야> 정보보호, 시각암호, 스테가노그라피

유 기 영 (Kee-Young Yoo) 정회원



1976년 2월 경북대학교 수학과 이학사
1978년 2월 한국 과학 기술원 컴퓨터 공학과 공학석사
1992년 2월 미국 뉴욕 Rensselaer Polytechnic Institute 컴퓨터 과학과 이학박사
1978년 3월~현재 경북대학교 컴퓨터공학과 교수
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜