情報保護學會論文誌
第 21 卷 第 5 號, 2011. 10

JK-RFID 인증 프로토콜에 대한 개선된 전방향 안전성

전 동 호,[1†] 최 성 운,[2] 김 순 자[3‡]
[1]영남대학교, [2]영남이공대학, [3]경북대학교

An Enhanced Forward Security on JK-RFID Authentication Protocol

Dong-ho Jeon,[1†] Seoung-un Choi,[2] Soon-ja Kim[3‡]
[1]Yeungnam University, [2]Yeungnam College of Science &Technology,
[3]Kyungpook National University

요 약

2009년에 전동호 등에 의해 경량의 강한 인증과 프라이버시를 제공하는 프로토콜이 제안되었다. 태그는 단지 간단한 비트연산들과 난수생성기를 필요로 한다. JK-RFID 인증 프로토콜은 도청, 재전송, 스푸핑, 위치추적, 서비스거부 공격, 전방향 안전성에 대한 강한 보안성을 제공한다. 하지만, 본 논문에서는 전방향 안전성에 대한 취약성을 지적하고 키 업데이트 과정에 대한 연산을 개선하였다. 본 논문은 전방향 안전성을 보장하는 개선된 JK- RFID 인증 프로토콜을 제안하고 전방향 안전성을 만족함을 검증하였다. 또한, 제안된 프로토콜의 안전성과 효율성을 분석하였다. 제안 프로토콜은 JK-RFID 인증 프로토콜에서 키 업데이트 부분의 연산을 수정하여 전방향 안전성을 개선하였다.

ABSTRACT

In 2009, Jeon et al proposed the lightweight strong authentication and strong privacy protocol, where the tag requrires only simple bitwise operations and random number generator. JK-RFID authentication protocol provides strong security: eavesdropping, replay, spoofing, Location tracking, DoS attack and forward security. Nevertheless, this paper points out the vulnerability of the forward security and improve the process of key updating. As a result, proposes an enhanced JK-RFID authentication protocol providing forward security and verify its satisfaction. In addition , a security and an efficiency of the proposed scheme analyze. Since partial adjustments of the key updating operation in JK-RFID authentication protocol, our protocol improve the forward security.

Keywords: RFID, Foreward Security, Authentication Protocol

I. 서 론

현재까지 제안된 RFID 인증기법을 태그에서의 연산능력과 저장능력에 따라 크게 네 가지 형태로 분류하면 첫째, 중량 인증방식은 해시함수, 암호화, 공개키 알고리즘 등 전통적 암호기법을 사용하는 프로토콜이다. 둘째, 단순인증 방식은 난수생성기와 일방향 해시함수를 사용하는 프로토콜이다. 셋째, 경량인증방식은 EPC class-1 Gen-2 가 PRNG와 CRC만 지원하기 때문에 해시함수를 사용하지 않고 난수생성과 CRC만 사용하는 프로토콜이다. 넷째, 초경량 인증방식은 xor, and, or같은 간단한 비트연산만을 사용하는 프로토콜이다[2-10]. 저가의 태그는 제한적인 연산능력과 저장 공간의 한계로 인해 대칭키, 공개키, 해시 같은 전통적인 암호기법의 사용이 힘들다. 이러한 저가형 태그를 위한 저비용의 안전한 인증기법과 암호기법의 연구를 필요로 하고 있다[11,12]. 전동호

접수일(2011년 7월 26일), 게재확정일(2011년 9월 22일)
† 주저자, jdh0692@korea.com
‡ 교신저자, snjkim@ee.knu.ac.kr

등에 의해 제안된 프로토콜은 태그에서 난수생성기와 비트연산만을 사용하였다. 보안성 분석에서 도청과 물리적 공격을 통하여 완벽한 전방향 안전성이 보장되지 않았다. 본 논문에서는 전동호 등에 의해 제안되었던 프로토콜의 전방향 안전성의 문제점을 분석하고 개선된 방법을 제안한다. 본 논문은 2장에서 전동호 등의 인증 프로토콜을 소개하고 공격 모델을 통해 전방향 안전성에 대해 분석한다. 3장에서는 개선된 인증 프로토콜의 전방향 안전성을 공격 모델을 통해 검증하고 4장에서는 안전성과 효율성을 분석한다. 마지막으로 5장에서 본 논문의 결론을 맺는다.

II. 관련연구

본 장에서는 전동호 등이 제안한 RFID 인증 프로토콜을 간략히 설명한다. 데이터베이스(DB)와 리더(Reader)는 안전한 채널 상에서, 리더와 태그(Tag)는 안전하지 않은 무선 채널 상에서 통신한다고 가정한다. 또한 리더와 태그는 난수생성이 가능하여야 하며, 데이터베이스와 태그는 비밀키 K를 공유하고 있다. 전동호 등이 제안한 프로토콜은 고정된 ID를 가짐으로서 데이터베이스에서 검색을 빠르도록 하고 데이터베이스와 태그에서 저연산(xor, rot, $+$)을 이용하여 연산속도를 빠르게 한다. 블로킹으로 인해 태그의 비밀키 K값이 업데이트 되지 않았을 경우, 데이터베이스에서 비밀키 K_{old}를 검색하여 비동기 문제를 해결한다. 매 세션마다 태그와 데이터베이스에서 연산되는 r_T, r_R, K 값이 바뀌게 되므로 도청, 재전송, 스푸핑, 위치추적 공격에 안전하다. 태그의 ID, K 값이 노출되더라도 이전의 K값이 갱신되었으므로 전방향 안전성을 어느 정도 만족한다.

2.1 전동호 등이 제안한 프로토콜

[그림 1]은 전동호 등이 제안한 경량 RFID 인증 프로토콜의 인증 과정을 보여주며, 아래와 같은 단계로 진행된다.

Step 1. Reader --〉 Tag : r_R

리더는 태그를 인식하여 랜덤값 r_R을 생성하여, Query와 함께 태그에게 전송한다.

Step 2. Tag --〉 Reader : S'

태그는 리더로부터 Query와 r_R를 수신한 후, 랜덤값 r_T를 생성하고, 데이터베이스와 공유 비밀값 $K(K_1,K_2)$를 절반으로 나누어 K_1,K_2를 다음 연산에 사용한다. 태그는 $S_1=(rot_L ID,r_R)+(K_1\oplus r_T)$과 $S_2=(rot_R ID,r_T)+K_2$를 연산한 결과인 S_1과 S_2를 XOR 연산하여 S'를 r_T와 함께 리더에게 전송한다.

Step 3. Reader --〉 DB : S', r_T, r_R

리더는 태그로부터 받은 S' 와 r_T 자신의 랜덤값 r_R 과 함께 데이터베이스에게 전송한다.

Step 4. DB --〉 Reader : S''

데이터베이스는 리더로부터 S', r_T, r_R을 받아서 태그에 대한 검증과정을 거친다. 데이터베이스는 $S_1=(rot_L ID,r_R)+(K_1\oplus r_T)$ 연산과 $S_2=(rot_R ID,r_T)+K_2$를 연산한다. S_1과 S_2를 XOR 연산하여 S'를 만족하는 $K_{new}(K_1,K_2)$를 가진 ID를 찾는다. S'값과 일치하는 ID를 찾지 못한다면 $K_{old}(K_1,K_2)$를 적용하여 S'값을 만족하는 ID를 찾는다. 일치하는 결과가 없다면 데이터베이스는 가짜 태그 또는 공격을 하는 태그로 인식하여 통신을 종료한다. 태그를 검증한 후 데이터베이스는 $K_{new}(K_1,K_2)$또는 $K_{old}(K_1,K_2)$를 이용하여 태그가 데이터베이스를 인증하기 위한 S''를 생성하는 과정과 업데이트 과정을 진행한다. 데이터베이스는 r_T,r_R,K_1,K_2를 이용하여 $S_3=(rot_L ID,r_R+r_T)+(K_1\oplus r_T)$ 와 $S_4=(rot_R ID,r_R-r_T)+K_2$ 를 연산한다. 연산한 결과인 S_3,S_4를 XOR 연산하여 S''를 생성하고 $K_{new}(K_1,K_2)$를 업데이트 한다. 데이터베이스는 리더에게 S''를 전송한다.

Step 5. Reader --〉 Tag : S''

리더는 데이터베이스에서 수신한 S''를 태그에게 전송하고 태그는 데이터베이스를 검증하기 위한 과정과 검증이 완료된 후 $K(K_1,K_2)$를 업데이트 한다. 태그에서 $S_3=(rot_L ID,r_R+r_T)+(K_1\oplus r_T)$와 $S_4=(rot_R ID,r_R-r_T)+K_2$를 연산하여 결과인 S_3,S_4를 XOR 연산하여 S''를 생성한 후 태그는 $K(K_1,K_2)$를 업데이트 한다.

2.2 전방향 안전성에 대한 취약성 분석

전방향 안전성이란 공격자가 어떠한 공격의 성공으로 그 태그의 현재정보를 알게 되었을 때 태그 소지자의 과거경로를 추측하지 못하는 것을 말한다. 공격자

는 이전 세션에서 도청을 통하여 리더의 난수값과 태그의 난수값을 알고 있으며 물리적 공격을 통하여 현재 태그의 ID, K_{new}값을 획득한다고 가정한다. 공격 모델의 절차는 아래와 같다.

Step 1. Attacker (이전 세션 도청) :

r_{R1}, r_{T1}, S', S''

공격자는 이전 세션에서 도청을 통하여 리더의 난수값 r_{R1}과 태그의 난수값 r_{T1}을 얻고 태그에서 리더로 전송된 값 S'과 리더에서 태그로 전송된 값 S''을 얻는다.

Step 2. Attacker (현재 세션 물리공격) :

ID, K_{new}

공격자는 물리적 공격을 통하여 태그의 정보 ID, K_{new}를 얻는다.

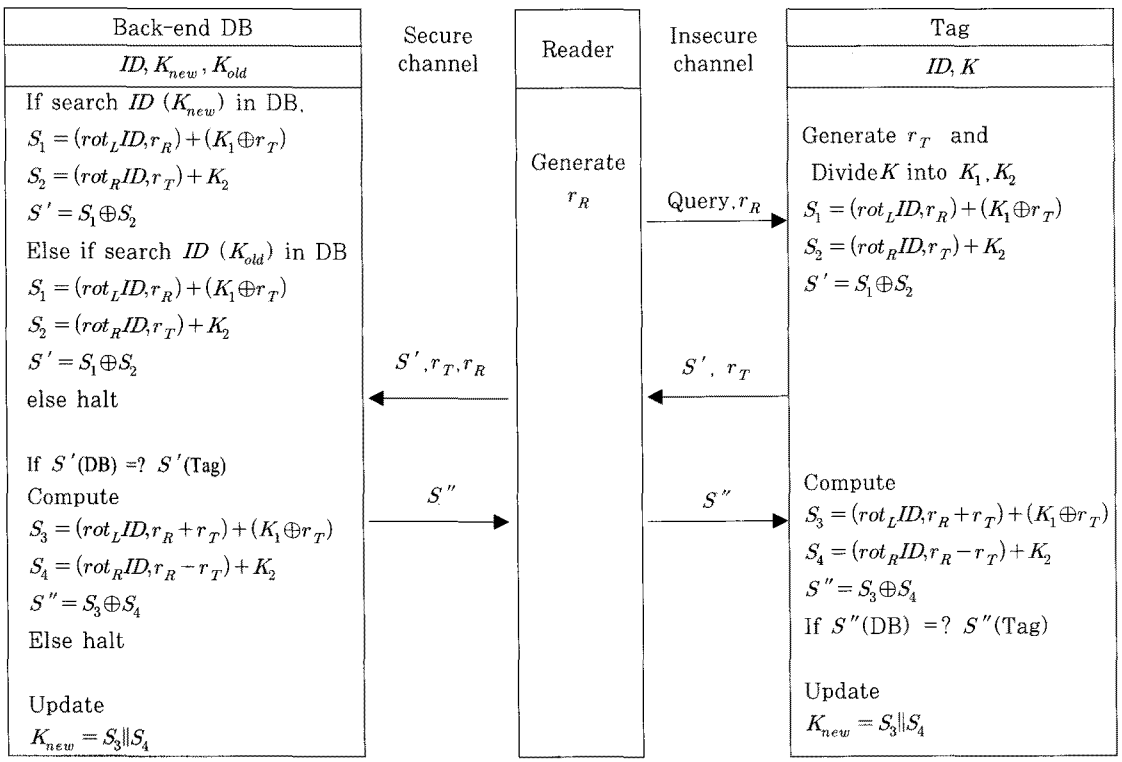
Step 3. Attacker (이전 세션의 키 복구)

공격자는 물리적 공격을 통하여 얻어진 ID, K_{new} 정보를 이용하여 이전의 키 값을 역으로 연산을 시도한다. 물리적 공격으로 획득한 K_{new}는 S_3 와S_4를 연접한 값이므로 K_{new}를 절반으로 나누면 S_3 ,S_4를 획득할 수 있다. 이전에 도청으로 획득한 r_{R1}, r_{T1}, S', S''값과 ID를 이용하여 $K_1=\{S_3-(rot_L ID, r_{R1}+r_{T1})\}\oplus r_{T1}$ 값과 $K_2=S_4-(rot_R ID, r_{R1}-r_{T1})$값을 역으로 연산한다. 이 두 값을 연접하면 이전의 키 K_{old}값이 된다.

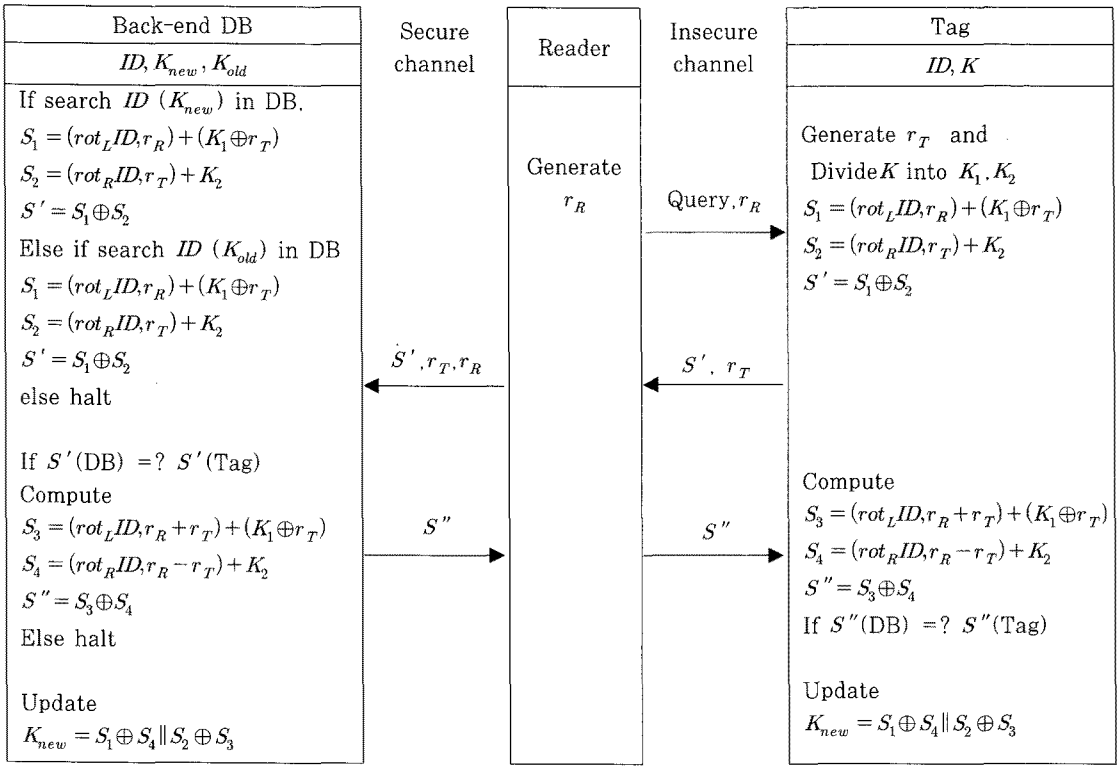
Step 4. Attacker (이전 세션의 위치추적)

공격자는 복구된 이전의 키값과 ID를 알고 있으며 이전에도 계속해서 도청을 하였다면 태그의 이전 위치 추적이 가능하다. 이전의 도청정보가 한 순간이라도 끊어지면 태그의 위치추적이 불가능하다.

위와 같은 전방향 안전성에 대한 취약성은 상호인증 후 새로운 키 값을 업데이트 하는 과정에서 연접 때문에 발생한다. 물리적 공격으로 알아낸 키값을 절반으로 나누면 S_3 ,S_4값이 된다. S_3 ,S_4값과 도청으로 획득한 정보와 ID를 이용하여 태그의 이전 키 값을 획득하게 된다. 공격자가 계속된 도청정보만 가지고 있으면 이전의 태그에 대한 위치추적이 가능하므로 전방향 안전성을 완전히 만족하지 않는다.



〔그림 1〕 전동호 등의 제안 프로토콜



〔그림 2〕 제안하는 프로토콜

III. 제안하는 프로토콜의 전방향 안전성 검증

본 장에서는 II장에서 보여준 전방향 안전성을 완전히 만족하기 위한 개선된 방법을 제안하고 공격 모델의 절차에 따라 검증한다. 전방향 안전성에 대한 취약성 분석에서 문제점은 연접으로 새로운 키값을 생성함으로 발생하였다. 물리적 공격으로 키값이 노출되었을 때 공격자는 절반으로 나누어 역으로 연산하여 이전의 키값을 획득하였다. 전방향 안전성 개선하기 위한 방법으로 상호인증 후 키 값을 업데이트 하는 과정에 S_3 와S_4를 연접하는 것이 아니라 S_1 ,S_4 와 S_2 ,S_3를 각각 xor 연산한 값을 연접한다. 업데이트 되는 새로운 키값으로 K_{new}= $S_1 \oplus S_4$ || $S_2 \oplus S_3$값을 사용한다. 공격자는 이전 세션에서 도청을 통하여 리더의 난수값과 태그 의 난수값을 알고 있으며 물리적 공격을 통하여 현재 태그의 ID, K_{new}값을 획득한다고 가정한다. 공격 모델의 절차는 다음과 같다.

Step 1. Attacker (이전 세션 도청) :

r_{R1}, r_{T1}, S', S''

공격자는 이전 세션에서 도청을 통하여 리더의 난수값 r_{R1}과 태그의 난수값 r_{T1}을 얻고 태그에서 리더로 전송된 값 S'과 리더에서 태그로 전송된 값 S''을 얻는다.

Step 2. Attacker (현재 세션 물리공격) :

ID, K_{new}

공격자는 물리적 공격을 통하여 태그의 정보 ID, K_{new}를 얻는다.

Step 3. Attacker (이전 세션의 키 복구 시도)

공격자는 물리적 공격을 통하여 얻어진 ID, K_{new} 정보를 이용하여 이전의 키 값을 역으로 연산을 시도한다. 물리적 공격으로 획득한 K_{new}는 S_1 ,S_4를 xor 연산한 값과 S_2 ,S_3를 xor 연산한 값을 연접한 값이다. 이전의 키를 복구하려고 하면 S_1 , S_2 , S_3, S_4의 값을 각각 알아야하므로 이에 대한 계산은 각각의 비트에 대한 확률적 추측을 하여야 한다. 따라서 공격자는 이전 세션의 키 값 K_{old}을 복구하지 못하므로 전방향 안전성을 완전히 만족한다.

공격자는 이전세션의 도청으로 r_{R1}, r_{T1}, S', S''를 획득하였다고 가정하면 S'= $S_1 \oplus S_2$, S''= $S_3 \oplus S_4$는

각 비트별로 1/2의 확률로 추측할 수 있다. 이후 공격자는 물리적 공격으로 ID, K_{new}를 획득하고 K_{new}를 절반으로 나누면 $S_1 \oplus S_4$과 $S_2 \oplus S_3$로 나누어진다. 이전의 키 값을 찾기 위해 다음과 같은 연산을 수행하여야 한다.

$$K_1 = \{S_1 - (rot_L ID, r_{R1})\} \oplus r_{T1}$$
$$K_2 = S_2 - (rot_R ID, r_{T1})$$
$$K_1 = \{S_3 - (rot_L ID, r_{R1} + r_{T1})\} \oplus r_{T1}$$
$$K_2 = S_4 - (rot_R ID, r_{R1} - r_{T1})$$

K_1, K_2의 값을 연접하면 이전의 키 K_{old}값이 되고 태그의 위치 추적이 가능해진다. K_1, K_2의 값을 알기 위해서는 위의 연산을 수행하여야 하지만 S_1, S_2, S_3, S_4의 값을 알 수 없다. 따라서 도청과 물리적 공격으로 획득한 정보로 이전의 키 K_{old}값을 연산할 수 없다. 개선된 JK-RFID 인증 프로토콜은 키 업데이트 과정에 새로운 키를 생성하는데 있어서 xor연산 후 연접을 하였다. 이것은 공격자가 물리적 공격과 이전의 도청정보를 이용하여 이전의 키 값을 알아낼 수 없다. 전방향 안전성을 완전히 보장하기 위해 태그와 데이터베이스에 키 업데이트 과정에 xor 연산이 한 번 더 필요하다.

IV. 제안 프로토콜의 안전성과 효율성 분석

본 장에서는 개선된 JK-RFID 인증 프로토콜에 대한 안전성과 효율성을 분석한다.

4.1 안전성 분석

제안한 프로토콜은 다음과 같이 상호인증과 안전한 키 업데이트 과정을 제공함으로 도청공격, 재전송 공격, 스푸핑 공격, 위치 추적 공격, 서비스거부 공격에 안전하고 전방향 안전성을 보장한다.

1) 상호인증 (Mutual Authentication)

상호인증은 태그와 리더에 연결된 데이터베이스 모두 인증을 통하여 합법적인지 확인하는 과정이다. 제안한 프로토콜은 통신과정에서 ID를 직접 노출 시키지 않고, 데이터베이스와 공유 비밀 값 K와 랜덤 넘버 r_T, r_R를 사용하여 인가된 사용자만이 해당 태그의 ID를 알아 낼 수 있도록 하였다. 데이터베이스에서 매 세션마다 $S' = S_1 \oplus S_2 = \{(rot_L ID, r_R) + (K_1 \oplus r_T)\} \oplus \{(rot_R ID, r_T) + K_2\}$값과 일치하는 ID를 찾아서 태그를 인증하게 된다. 태그 자신이 연산한 결과가 $S'' = S_3 \oplus S_4 = \{(rot_L ID, r_R + r_T) + (K_1 \oplus r_T)\} \oplus (rot_R ID, r_R - r_T) + K_2\}$를 만족하는 값이면 데이터베이스를 인증한다. 따라서 제안한 프로토콜은 안전한 상호인증을 제공한다.

2) 도청공격 (Eavesdropping Attack)

도청공격은 무선통신구간인 태그와 리더사이에 송수신되는 내용을 도청하여 태그에 대한 정보를 알아내는 공격이다. 제안한 프로토콜에서 공격자는 r_T, r_R, S', S''를 도청할 수 있다. 하지만 공격자는 도청한 내용으로 역으로 연산을 하지 못하므로 태그의 비밀 값 K,ID에 대한 정보를 얻어낼 수 없다. 따라서 제안한 프로토콜은 도청공격에 안전하다.

3) 재전송 공격 (Replay Attack)

재전송 공격은 공격자가 과거에 태그와 리더의 무선통신 구간에서 내용을 도청한 후 이를 재전송하여

〔표 1〕 안전성 비교 (O : 만족, △ : 부분만족, X : 불만족)

	LMAP[12]	M2AP[3]	EMAP[4]	SASI[5]	JK[12]	제안 프로토콜
상호인증	O	O	O	O	O	O
도청	X	X	X	O	O	O
재전송	X	X	X	X	O	O
스푸핑	X	X	X	X	O	O
Dos(비동기화유도)	X	X	X	X	O	O
위치추적	X	X	X	X	△	O
전방향안전성	X	X	X	X	△	O

합법적인 태그나 리더로 인증 받으려는 공격이다. 제안 프로토콜에 정당한 리더로 가장한 공격방법을 적용하면 공격자는 이전 세션에서 도청을 통하여 r_T, r_R, S', S''를 얻을 수 있지만 이전 세션에서 태그에서 K값이 갱신되어 있고 태그에서 생성된 난수 r_T가 다르므로 이전의 S''와 다르므로 정당한 리더로 인증되지 않는다. 공격자가 정당한 태그로 가장한 경우 세션마다 리더로부터 전송된 r_R값과 태그에서 생성된 r_T값을 $S_1 = (rot_L ID, r_R) + (K_1 \oplus r_T)$연산에 사용되어져 $S' = S_1 \oplus S_2$값이 데이터베이스에서 일치하지 않으므로 가짜 태그 또는 공격 태그로 쉽게 검출된다. 따라서 제안한 프로토콜은 재 전송공격에 안전하다.

4) 스푸핑 공격 (Spoofing Attack)

스푸핑 공격은 공격자가 정당한 태그로 위장하여 리더로부터 인증에 필요한 정보를 획득하거나 정당한 리더로 위장하여 태그로부터 인증에 필요한 정보를 획득하여 공격하는 방법이다. 제안 프로토콜에서는 공격자가 정당한 리더로 가장하여 태그를 속이기 위해서는 재전송 공격의 방법과 동일하게 올바른 $S'' = S_3 \oplus S_4 = \{(rot_L ID, r_R + r_T) + (K_1 \oplus r_T)\} \oplus \{(rot_R ID, r_R - r_T) + K_2\}$ 값을 계산해야 하지만 ID나 비밀키 K값을 알지 못하면 정당한 리더로 인증 받을 수 없어 공격에 안전하다. 정당한 태그로 위장하는 경우에 이전 세션에서 도청으로 얻은 정보 S'를 데이터베이스로 전송하면 데이터베이스에서 $S' = S_1 \oplus S_2 = \{(rot_L ID, r_R) + (K_1 \oplus r_T)\} \oplus \{(rot_R ID, r_T) + K_2\}$를 계산하는 과정에서 위장한 태그를 식별해 낼 수 있어서 스푸핑 공격에 안전하다.

5) 위치추적 공격 (Location Tracking Attack)

위치 트래킹 공격은 공격자가 태그의 위치변화를 감지하여 태그 소유자의 이동경로를 파악하여 사용자의 프라이버시를 침해하는 공격이다. 태그로부터 매 세션마다 동일한 정보가 나오는 RFID 시스템은 위치추적이 가능하다. RFID 시스템에서 랜덤한 두 개의 태그를 두고 이들을 구별해 낼 수 없으면 불구분성(indistinguishability)을 만족하며 태그의 위치 프라이버시를 보장받을 수 있다. 제안 프로토콜에서는 매 세션마다 r_T, r_R, K 값에 의해 계산된 S' 값이 계속해서 바뀌게 되어 이전 세션과 항상 다른 값을 전송하므로 공격자는 특정한 태그를 식별할 수 없으므로 위치추적에 안전하다.

6) 서비스 거부 공격 (DoS Attack ; 비동기화 유도 공격(Desynchronization attack))

서비스 거부공격은 RFID시스템의 정상적인 작동을 방해하여 비동기화 문제를 일으키는 방법이다. 또한 악의적으로 리더와 태그사이의 통신을 차단하여 정보 불일치를 유도하는 것이 비동기화 유도공격이다. 제안 프로토콜에서 비동기화 유도공격을 시도하려면 안전하지 못한 태그와 리더 사이에서 S'값이 전송된 후 데이터베이스는 일치하는 태그 인증과정을 거친 후 K_{new}값이 갱신되고 기존 K_{new}의 값은 K_{old} 값으로 바뀌게 된다. 데이터베이스에서 태그로 전송되는 S''를

〔표 2〕 효율성 비교

(L : 저장 공간, - : 불필요)

		LMAP[12]	M2AP[3]	EMAP[4]	SASI[5]	JK[12]	제안 프로토콜
Total message		4L	5L	5L	4L	3L	3L
Tag memory		6L	6L	6L	7L	2L	2L
DB memory		6L	6L	6L	4L	3L	3L
DB (Reader) operation	xor	14	13	21	10	5	6
	∧, ∨	1	4	4	2	-	-
	+, -	9	8	1	4	6	6
	rotate	-	-	-	2	4	4
	PRNG	2	2	2	2	1	1
Tag operation	xor	14	13	20	10	5	6
	∧, ∨	-	2	3	2	-	-
	+, -	7	8	-	3	6	6
	rotate	-	-	-	2	4	4
	PRNG	-	-	-	-	1	1

가로채면 태그에서 K값은 갱신되지 않는다. 데이터베이스는 K_{new}, K_{old}값이 업데이트 되고 태그는 K값이 업데이트 되지 않은 비동기 상태가 된다. 그러나 공격받은 태그는 다음 세션에서 K값을 이용하여 연산한 결과인 S'값을 리더에게 전송하면 데이터베이스에서 K_{new}값이 없을 경우 K_{old}값을 검색하여 통해 인증과정을 통하여 정상적인 K값을 갱신하는 과정이 진행된다. 따라서 S''의 정보가 차단되더라도 다음 통신 세션에서 데이터베이스에 K_{old}값을 통하여 상호인증을 진행할 수 있어 비동기화 유도공격에 안전하다.

7) 전방향 안전성 (Forward untraceability)

전방향 안전성은 공격자가 물리적인 공격을 통하여 어떤 태그의 ID, K값을 알아내더라도 이로부터 이전 세션의 정보를 획득할 수 없어야 한다. 3장의 전방향 안전성에 대한 분석에서 제안하는 프로토콜은 전방향 안전성을 완전히 보장함을 검증하였다. 공격자는 물리적 공격을 통하여 얻어진 ID, K_{new} 정보를 이용하여 이전의 키 값을 역으로 연산을 시도한다. 물리적 공격으로 획득한 K_{new}는 S_1 ,S_4를 xor 연산한 값과 S_2 ,S_3를 xor 연산한 값을 연접한 값이다. 이전의 키를 복구하려고 하면 S_1 , S_2 , S_3, S_4의 값을 각각 알아야하므로 이에 대한 계산은 각각의 비트에 대한 확률적 추측을 하여야 한다. 따라서 공격자는 이전 세션의 키 값 K_{old}을 복구하지 못하므로 전방향 안전성을 보장한다.

〔표 1〕은 제안 프로토콜과 기존에 제안된 JK, SASI, LMAP, M2AP, EMAP 프로토콜과의 안전성을 비교 분석한 표이다. 제안 프로토콜은 JK 프로토콜에서 키 업데이트 부분의 연산을 수정하여 전방향 안전성을 개선하였다.

4.2 효율성 분석

〔표 2〕는 제안 프로토콜과 기존에 제안된 JK, SASI, LMAP, M2AP, EMAP 프로토콜과의 효율성을 비교 분석한 표이다. 제안 프로토콜은 SASI 프로토콜과 비교하여 JK 프로토콜과 동일하게 태그와 데이터베이스에서 각각 난수생성기를 가져야 한다. JK 프로토콜과 비교하여 키 업데이트 과정에서 XOR 연산이 2번 수행된다. 태그와 데이터베이스에서 각각 XOR 연산이 추가적으로 수행되어야 한다. JK 프로토콜이 가지는 전방향 안전성에 대한 취약성을 개선하기 위해 필요한 연산이다. JK 프로토콜과 비교하여 XOR 연산이 한 번 추가되어 효율성이 조금 감소하였으나 전체적인 연산량과 비교하였을 때 구현하는데 있어서 큰 문제를 가지지 않는다.

V. 결 론

본 논문에서는 최근에 제안된 태그에서 난수생성기만을 필요로 하는 JK-RFID 인증 프로토콜에서 전방향 안전성에 대한 취약성을 분석하였다. 본 논문에서 전방향 안전성에 대한 취약성을 개선하기 위해 키 업데이트 부분의 연산을 수정한 프로토콜을 제안하였으며 공격자가 물리적 공격과 이전의 도청정보를 획득하여 이전의 키를 알아내지 못함을 검증하였다. 제안 프로토콜은 전방향 안전성을 완전히 보장하지만 이전의 JK-RFID 인증 프로토콜의 연산에 비해 데이터베이스와 태그에 추가적으로 xor연산이 한 번 필요하다.

참고문헌

〔1〕 K. Finkenzeller, *RFID Handbook*, John Wiley & Sons, 1999.

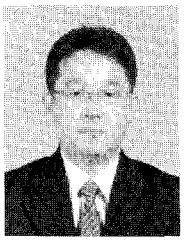
〔2〕 P. Peris-Lopez, J.C. Hernandez - Castro, J.M. Estevez - Tapiador, and A. Ribagorda, "LMAP: A Real Lightweight Low-Cost RFID Tags," Proc. Second Workshop RFID Security(RFIDSec 06), http://events.iaik.tugraz.at/RFIDSec06/Program/papers/013%20-%20Lightweight%20Mutual%20Authentication.pdf , Jul. 2006.

〔3〕 P. Peris - Lopez, J.C. Hernandez - Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "M2AP: A Minimalist mutual-Authentication Protocol for Low-Cost RFID Tags," Proc. Int' Conf Ubiquitous Intelligence and Computing(UIC ,06), LNCS 4159, pp. 912-923, 2006.

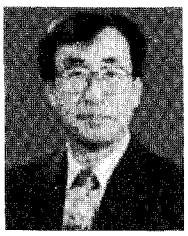
〔4〕 P. Peris - Lopez, J.C. Hernandez - Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags," Proc. OTM Federated Conf and Workshop: IS Workshop, LNCS 4277, pp. 352-361, 2006.

[5] H.Y. Chien. "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity," IEEE Transactions on Dependable and Secure Computing vol. 4, no. 4, pp. 337-340. Oct-Dec, 2007.
[6] T. Li and R.H. Deng, "Vulnerability Analysis of EMAP-an Effcinet RFID Mutual Authentication Protocol," in Proc. Second International Conference, Availability, Reliability, and Security (AReS'07), pp. 238-245 , Apr. 2007.
[7] T. Li and G. Wang, "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols," in Proc. 22nd IFIP TC-11 International Information Security Conference, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.8867&rep=rep1&type=pdf, May. 2007.
[8] H.Y. Chien and C.W. Hung, "Security of Ultra-Lightweight RFID Authentication Protocols and Its Improvements," ACM Operating System Rev., vol. 41, no. 2, pp. 83-86, Jul. 2007.
[9] T. Cao, E. Bertino, and H. Lei, "Security Analysis of the SASI Protocol," IEEE Transactions on Dependable and Secure Computing vol. 6, no. 1, pp. 73-77. Jan-Mar, 2009.
[10] 곽민혜, 김광조, "취약성 분석을 통한 경량 RFID 인증 프로토콜 고찰," CISC-W'08 Proceedings, pp.201-208, 2008년 12월.
[11] 하재철, 백이루, 김환구, 박제훈, 문상재, "해쉬함수에 기반한 경량화된 RFID 인증 프로토콜," 정보보호학회논문지, 19(3), pp. 61-72, 2009년 6월.
[12] 전동호, 김영재, 권혜진, 정선영, 김순자, "강한 인증과 프라이버시를 보장하는 개선된 초경량 RFID 인증 프로토콜," 정보보호학회논문지, 19(5), pp. 81-91, 2009년 10월.

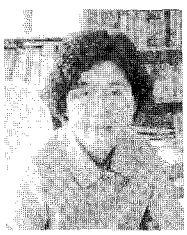
〈著者紹介〉



전 동 호 (Gil-dong Hong) 정회원
2000년 2월: 밀양대학교 컴퓨터공학과 졸업
2002년 2월: 경북대학교 정보통신학과 석사
2010년 2월: 경북대학교 정보보호학과 박사
2010년 3월~현재: 영남대학교 의료공학연구소 연구원
〈관심분야〉 정보보호, 생체인증, RFID



최 성 운 (Seong-un Choi) 정회원
1974년 2월: 영남대학교 전자공학과 졸업
1978년 2월: 한국대학교 전자공학과 석사
1988년 8월: 영남대학교 전자통신공학과 박사
1978년 3월~현재: 영남이공대학 전자정보계열 교수
〈관심분야〉 생체인증, 정보보호 및 보안기술



김 순 자 (Soon-ja Kim) 종신회원
1975년 2월: 경북대학교 수학과 졸업
1977년 2월: 경북대학교 수학과 석사
1988년 3월: 계명대학교 수학과 박사
1993년 3월~현재: 경북대학교 IT대학 전자전기공학부 교수
〈관심분야〉 정보보호 및 보안기술, 정보보호 응용기술