개선된 해시기반의 RFID 상호인증 프로토콜

준회원 신 주 석*, 오 세 진**, 정회원 정 철 호***, 정 경 호****, 안 광 선**°

Improved An RFID Mutual Authentication Protocol Based on Hash Function

Juseok Shin*, Sejin Oh** *Associate Members*, Cheolho Jeong***, Kyungho Chung****, Kwangseon Ahn**° *Regular Members*

요 약

2010년 Jeon-Kim은 상호인증 기법, 해시함수 및 비밀 키 업데이트를 이용하여 RFID 시스템에서의 다양한 보안상 문제점을 해결한 HMAP(Hash-based Mutual Authentication Protocol for RFID Environment)를 제안하였다. 안전성 분석을 통하여 Jeon-Kim은 HMAP가 도청공격을 포함한 다양한 공격들에 안전함을 증명하였다. 하지만 그들이 주장한 바와는 달리 HMAP 프로토콜은 도청공격으로 인해 다음 세션에서 사용하게 될 비밀 키가 노출되는 문제점이 있다. 본 논문에서는 보안성 분석을 통하여 HMAP의 문제점을 분석 및 증명하고 이를 해결하기 위해 개선된 해시기반의 RFID 상호인증 프로토콜을 제안한다.

Key Words : RFID, Authentication, Protocol, Hash Function, Security

ABSTRACT

In 2010, Jeon-Kim proposed HMAP(Hash-based Mutual Authentication Protocol for RFID Environment) to resolve a variety of problem related to security using Mutual authentication scheme, the hash function and secret key is used to update in RFID system. Jeon-Kim proved RMAP was safe for a variety of attacks including eavesdropping attacks through safety analysis. However, unlike the claims of the proposed protocol is vulnerable to next session of the secret key exposure due to eavesdropping. In this paper, we analyze the problem of RMAP and proves it through security analysis. And we also propose improved an RFID Mutual Authentication Protocol based on Hash Function to solve problems of HMAP.

Ⅰ. 서 론

RFID(Radio Frequency Identification) 시스템은 무선 주파수 인식을 통한 자동 인식 기술로 태그와 리더 그리고 백-엔드-서버(데이터베이스)로 구성이 된다. 이러한 RFID 시스템은 원거리에서도 물리적인 접촉 없이 인식이 가능하고, 여러 개의 정보를 동시에 판독 및 수정이 가능하다는 장점 때문에 바코드를 대체하는 신기술로서 현재 유통분야, 물류, 교통 보안 등의 분야로 적용이 나날이 확대되고 있다[1,2]. 하지만 태그와 리더간의 통신은 무선 채널을 통하여 데이터를 송·수신하므로 공격자에 의해 태그 정보가 노출되거나 위치추적으로 인한 사생활 침해 및 다양한 보안상의 취약점이 드러나게 되었다[3,4].

* 한국전자통신연구원 자동차IT플랫폼 연구팀(jsshin@etri.re.kr),
** 경북대학교 전자전기컴퓨터학부 임베디드 시스템 연구실({170m3, gsahn}@knu.ac.kr), (° : 교신저자)
*** 경남대학교 전자공학과(jch21@kyungnam.ac.kr), **** 경운대학교 컴퓨터공학과(mccart@ikw.ac.kr)
논문번호 : KICS2011-10-460, 접수일자 : 2011년 10월 12일, 최종논문접수일자 : 2012년 2월 22일

이를 해결하기 위하여 EPC-Global Class 1 Gen 2-UHF 프로토콜 SPEC에서는 Kill password 및 Access password를 제공하고 있다[5]. Kill password의 경우, 안전성이 뛰어난 반면 태그를 재사용하지 못하는 단점이 있으며, 이와 비슷한 접근 방법으로 Faraday Cage 기술, Blocker Tag 및 Active Jamming 기술 등이 있다. 또한 태그에 접근 및 통신을 하기 위해 Access password와 간단한 프로토콜을 제공하고 있으나, 보안상 취약점이 있다.

EPC-Global Class 1 Gen 2에서 제공하는 프로토콜에서는 EPC(Electronic Product Code)를 암호화 하지 않고 전송하고 있으며, 태그와 리더 간 상호인증을 제공하지 않기 때문에 보안에 취약하고 다양한 공격에 노출되기 쉽다. 따라서 태그를 재사용하고, RFID 시스템의 보안상 문제점을 해결하기 위해서는 암호학적인 보안기법과 상호인증 과정을 통하여 해결하여야 한다. 암호학적 접근 방법으로는 해시 함수, 공개키 암호화, 대칭키 암호화 등이 있으며, 이런 암호화 기법을 RFID시스템에 적용하기 위한 연구가 꾸준히 이루어지고 있다. 또한 암호화 기법들을 이용하여 다양한 RFID 인증 프로토콜을 제안하고 있으며, 제안한 프로토콜의 안전성을 증명하고 있다.

Jeon-Kim은 2010년에 HMAP(Hash-based Mutual Authentication Protocol for RFID Environment)를 제안하였다. HMAP에서는 서버를 통하여 리더와 태그가 정당하다는 것을 상호인증하고, 매 세션마다 비밀 키를 업데이트하는 방식으로 전방향 안전성을 제공한다. 또한 안전성 분석에서 도청 공격, 재전송 공격 등 다양한 공격에 안전한 프로토콜을 제안하였다[6]. 하지만 HMAP에서 분석한 내용과는 달리 도청공격으로 인해 다음 세션에서 사용하게 될 비밀 키가 노출 되는 문제점이 있다.

본 논문에서는 HMAP의 문제점을 개선한 해시기반의 상호인증 프로토콜을 제안하고, 다양한 공격에 대한 안전성과 효율성을 HMAP 프로토콜과 비교 분석한다.

본 논문의 구성은 다음과 같다. 2장 관련 연구에서는 기존에 제안된 RFID 인증 프로토콜들과 제안된 프로토콜들에서의 문제점 및 HMAP에서 제안한 인증 프로토콜에 대해 기술하고, 3장에서는 HMAP에서 제안한 프로토콜의 취약점을 분석 및 증명한다. 4장에서는 본 논문에서 제안한 개선된 해시기반의 상호인증 프로토콜을 설명한다. 5장에서는 제안한 프로토콜의 안전성을 분석하고, HMAP와 본 논문에서 제안한 프로토콜의 보안성 및 효율성을 비교 분석한다. 마지막으로 6장에서는 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 RFID 시스템 상에서 발생할 수 있는 다양한 보안상 문제점들을 해결하기 위해 제안된 해시기반의 RFID 인증 프로토콜들과 기존에 제안된 프로토콜들에서의 문제점 및 Jeon-Kim이 제안한 HMAP 프로토콜에 대해 기술한다.

2.1. HLP(Hash-Lock Protocol)

S. A. Weis 등은 전방향성을 특징으로 하는 해시 함수를 기반으로 HLP(Hash-Lock Protocol)을 제안하였다[2]. 하지만 공격자가 metaID를 도청하여 정당한 리더로 전송하게 되면, 상호인증 단계가 없기 때문에 리더는 공격자에게 정당한 키를 전달하는 문제점이 있다. 또한 HLP에서는 metaID, Key, 태그의 ID를 아무런 제약 없이 전송하고, 리더의 질의에 대한 응답으로 항상 같은 metaID 값을 전송하기 때문에 도청, 스푸핑 공격, 재전송 공격 및 위치 추적에 취약하다[16,17].

2.2. RHLP(Randomized Hash-Lock Protocol)

HLP에서 동일한 metaID로 인한 위치추적 문제를 해결하기 위하여 RHLP(Randomized Hash-Lock Protocol)[2]은 태그의 난수 생성기를 통하여 리더의 질의에 대해 항상 응답을 다르게 프로토콜을 설계하였다. 하지만 RHLP에서도 공격자가 도청으로 획득한 데이터를 이용하여 재전송 공격, 스푸핑 공격을 할 경우 IDk의 값이 노출되는 문제점이 있다[16-18]. 또한 RHLP의 경우, m개의 태그가 있을 때 데이터베이스에서 정당한 태그를 인식하기 위해서는 평균 [m/2] 번의 해시 연산이 필요하므로 다수의 태그를 인식해야하는 시스템이라면 데이터베이스에 많은 부하가 걸리게 된다[18].

2.3. AMAP(A Mutual Authentication Protocol)

Wei 등은 기존에 제안된 RFID 인증 프로토콜과는 달리 데이터베이스와 리더, 리더와 태그 사이의 채널이 모두 안전하지 못한 무선 상의 채널이라 가정하고 해시기반의 상호인증 프로토콜을 제안하였다[19]. 또한 매 세션마다 갱신되는 비밀 값을 사용하여 위치 추적, 재전송 공격 등에 안전하며, 전 방향 안전성을 제공한다고 주장하였다.

하지만 그들의 주장과는 달리, 공격자가 매 세션

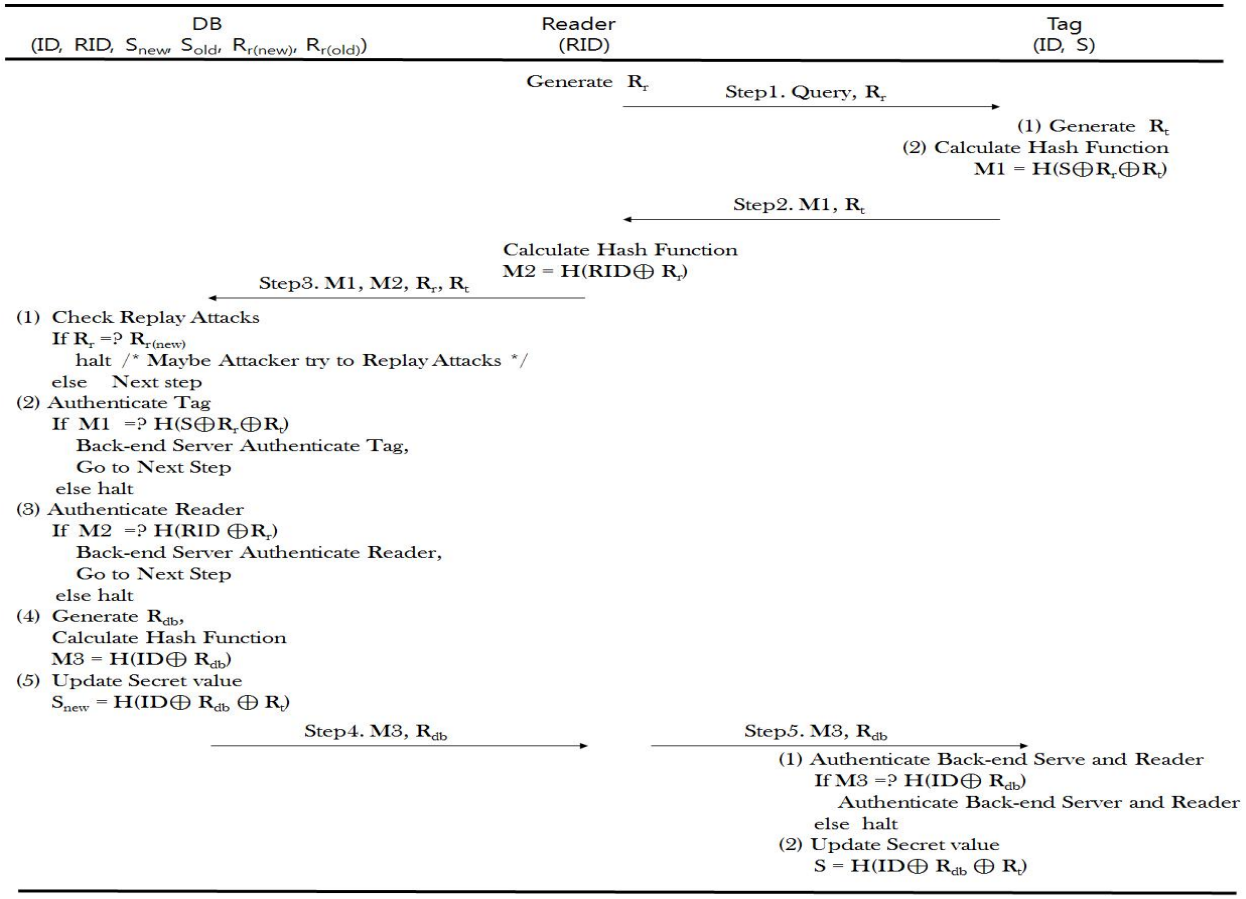


그림 1. AMAP에서 제안한 인증 프로토콜
Fig. 1. The Proposed Authentication Protocol in AMAP

전송되어지는 데이터들을 도청한 후, 이를 이용하여 RFID 시스템 상에 재전송공격을 가할 경우, 데이터베이스와 태그가 비동기적인 비밀 값을 가지게 되는 심각한 문제점이 있다. 그림 1은 AMAP(A Mutual Authentication Protocol)에 대해 나타낸 것이다. AMAP의 Step5에서 리더가 태그로 전송하는 모든 값들을 저장한 후, 이전에 전송된 $M3^{(n-i)}$, $R_{db}^{(n-i)}$를 이용하여 재전송 공격을 시도하게 되면, 태그는 리더와 데이터베이스가 정당하다고 판단하여 인증과정을 마치고 자신의 비밀 값을 갱신하므로, 데이터베이스와 태그가 가지는 비밀 값이 다르게 되는 문제가 있다. 따라서 AMAP는 도청, 재전송 공격에 취약하다.

2.4. HMAP(Hash-based Mutual Authentication Protocol)

본 장에서는 최근에 Jeon-Kim에 의해 제안된 HMAP를 간략히 설명한다. HMAP는 Ahn등이 제안한 인증 프로토콜[15]에 대하여 상호인증, 위치추적 및 전 방향 안전성에 대하여 문제점을 증명하고, 개선된 상호인증 프로토콜을 제안하였다. 표 1은 HMAP에서 사용되는 표기법이다. HMAP 프로토콜에서는 데이터베이스와 리더사이, 리더와 태그 사이 모두 채널이 안전하지 않다고 가정을 하였고 각 장치들은 다음과 같은 값들을 초기에 저장하고 있다.

표 1. HMAP의 표기법
Table 1. The Notation Used in AMAP

DB : 벡엔드 데이터베이스	K_{old} : DB에 저장된 태그의 이전 비밀키 값
	K_{new} : DB에 저장된 태그의 현재 비밀키 값
	$D_{SK}(x)$: x를 대칭키SK로 복호화 연산
	m_R : 해시연산 결과 값의 우측 절반
R : 리더	R_r : 리더에서 생성한 난수
	$E_{SK}(x)$: x를 대칭키SK로 암호화 연산
T : 태그	R_t : 태그에서 생성한 난수
	ID : 태그의 식별정보
	K : 태그에 저장된 키 값
	$H(x)$: x를 해시연산
	m_L : 해시연산 결과 값의 좌측 절반

- DB : ID, K_{new}, K_{old}, $info$, SK
- R : SK
- T : ID, K

그림 2는 HMAP에서 제안한 해시기반의 상호인증 프로토콜을 나타내고, HMAP에서 제안한 프로토콜의 세부 실행과정은 아래와 같다.

Step 1. $R \rightarrow T$: R_r

리더는 태그를 인식하기 위하여 $Query, R_r$을 태그로 전송한다.

Step 2. $T \rightarrow R$: m_L, R_r

태그는 리더로부터 $Query, R_r$을 수신한 후, R_t를 생성하고, 수신된 R_r값과 자신의 ID 및 DB와 공유한 비밀키 K를 이용하여 랜덤 해시 값 $m = H(ID \| K \| R_r \| R_t)$를 계산한 후, R_r과 m_L을 리더에게 전송한다.

Step 3. $R \rightarrow S$: $E_{SK}(m_L, R_r, R_t)$

리더는 DB와 설정된 대칭키 SK를 사용하여 태그로부터 수신한 m_L , R_t와 기존에 자신이 생성한 R_r을 암호화하여 DB로 전송한다.

Step 4. $DB \rightarrow R$: $E_{SK}(R_r, m_R, Info)$

DB는 리더로부터 수신한 값을 리더와 사전에 공유한 대칭키 SK로 복호화 한 후, 자신이 가지고 있는 ID, K_{new}, K_{old}값들을 이용하여 $m_L' = H(ID \| K_{new} \| R_r \| R_t)$ 를 계산하고 리더에서 수신한 m_L과 동일한 값이 있는지 확인한다. 동일한 값이 있다면 태그를 인증하고, 대칭키 SK를 사용하여 $E_{SK}(R_r, m_R, Info)$값을 리더로 전송한다. m_L'값과 m_L이 다르다면, 비밀키를 업데이트 하지 않은 태그라고 간주하고 $m_L'' = H(ID \| K_{old} \| R_r \| R_t)$ 를 계산하여 m_L''값과 리더에서 수신한 m_L과 동일한 값이 있는지 확인한다. 동일한 값이 존재한다면 태그를 인증하고, $E_{SK}(R_r, m_R, Info)$를 리더로 전송한다. m_L' , m_L'' 값 모두가 m_L값과 동일하지 않다면 오류 메시지를 리더에게 전송하고, 세션을 종료한다. 그 반대의 경우에는 서버와 태그가 공유한 비밀키 K를 업데이트 한다.

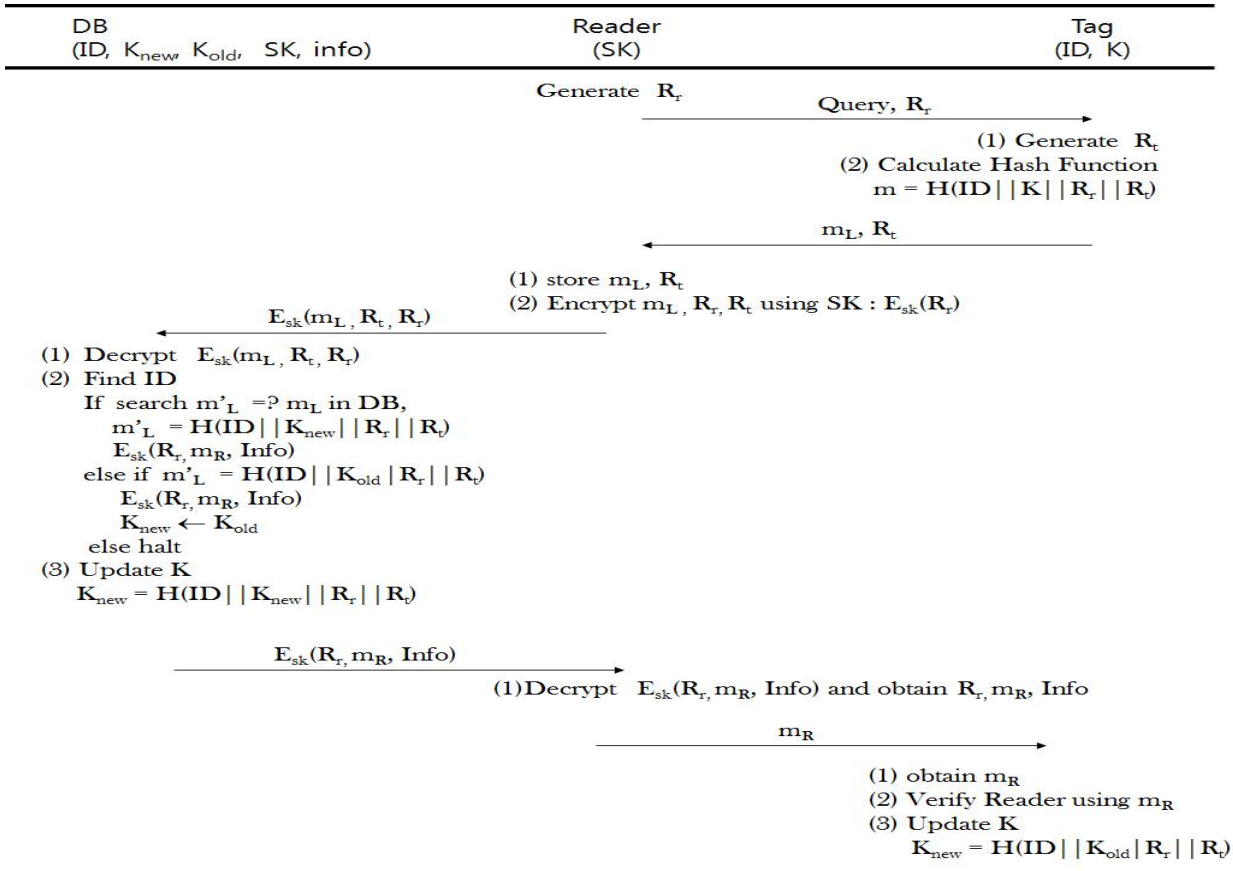


그림 2. HMAP에서 제안한 인증 프로토콜
Fig. 2. The Proposed Authentication Protocol in HMAP

Step 5. $R \rightarrow T$: m_R

리더는 DB에서 수신한 값이 오류 메시지일 경우 세션을 종료한다. 그렇지 않고 DB가 태그를 정상적으로 인증하였을 경우, 수신 받은 값을 SK로 복호화 하여 자신이 생성한 R_r값과 리더에서 전송받은 R_r값이 같은지를 확인하여 DB를 인증한다. 정상적인 DB일 경우, 리더는 태그에게 m_R값을 태그로 전송한다. 태그는 리더로부터 수신된 m_R값과 자신이 생성한 해시연산 결과 값의 우측 절반 값과 비교하여 같다면 리더와 DB를 인증하고, 일치하지 않으면 세션을 종료한다. 마지막으로 태그에서 리더와 데이터베이스에 대한 인증과정이 정상적으로 종료되면, 태그는 비밀키 K를 업데이트 한다.

Ⅲ. HMAP에서 제안한 프로토콜의 취약점

본 장에서는 HMAP에서 제안한 프로토콜이 도청공격으로 인하여 다음 세션에 사용하게 될 비밀 키가 노출되는 문제점이 있다는 것을 보여준다.

HMAP에서 제안한 프로토콜은 리더와 태그, 리더와 서버간의 통신 채널이 안전하지 못한 채널이라고 가정하고 있다. 따라서 공격자는 서버와 리더, 리더와 태그 사이에 통신하는 데이터들을 도청공격을 이용하여 획득할 수 있다. HMAP에서 제안한 프로토콜의 안전성 분석에서는 매 세션 마다 서버와 리더가 공유하고 있는 비밀키를 업데이트 하므로 전 방향 안전성에 안전하다고 주장하였지만, 아래의 시나리오와 같이 태그가 다음에 사용하게 되는 업데이트된 비밀 키를 공격자에게 노출되는 문제점을 가지고 있다. 그림 3은 도청공격으로 인한 비밀키 획득 시나리오를 나타낸다.

1) 공격자는 태그에서 리더로 전송하는 m_L값을 도청공격으로 획득한다.

2) 공격자는 리더에서 태그로 전송하는 m_R값을 도청공격으로 획득한다.

3) 비밀키의 업데이트는 m_L + m_R값이므로 1), 2)과정만으로도 태그가 다음에 사용하게 될 업데이트 되는 비밀키를 공격자가 알 수 있다.

Ⅳ. 제안한 프로토콜

본 장에서는 HMAP에서 제안한 프로토콜의 문제점을 개선한 프로토콜을 제안한다. 그림 4는 본 논문에서 제안한 프로토콜을 보여준다. 표 2는 본 논문에서 사용되는 용어들을 나타낸다.

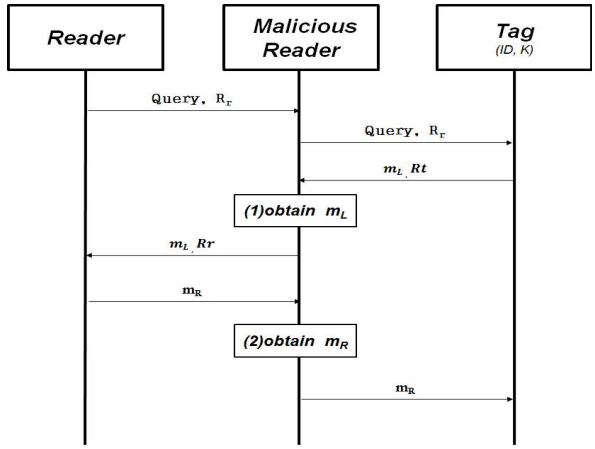


그림 3. 비밀키 획득 시나리오
Fig. 3. The Scenario of the Obtaining Secret Key

Step 1. $R \rightarrow T(Query, R_r)$

리더는 태그와 통신을 하기 위하여 주기적으로 $Query$를 태그로 보내고, 상호인증 및 보안 취약점을 해결하기 위해 난수 값 R_r을 생성하여 태그로 보낸다.

Step 2. $T \rightarrow R(m_L, R_t, H(K \parallel R_r \parallel R_t))$

리더로부터 질의를 받은 태그는 난수 R_t를 생성한다. 그리고 해시연산을 수행하여 $m = H(ID \| K \| R_r \| R_t)$ 과 리더와 서버를 인증하기 위해 $H(K \| R_r \| R_t)$를 생성한다. 마지막으로 해시연산 결과 값 m의 좌측 반값 m_L과, R_t, $H(K \| R_r \| R_t)$ 값을 리더로 전송한다.

표 2. 제안 인증 프로토콜에서의 표기법
Table 2. The Notations Used in the Proposed Protocol

DB : 백엔드 데이터베이스	K : DB에 저장된 비밀키 값
	$D_{SK}(x)$: x를 대칭키SK로 복호화 연산
	m_R : 해시연산 결과 값의 우측 절반
	$\oplus$: XOR 연산
	R_{db} : DB에서 생성한 난수
R : 리더	R_r : 리더에서 생성한 난수
	$E_{SK}(x)$: x를 대칭키SK로 암호화 연산
T : 태그	R_t : 태그에서 생성한 난수
	ID : 태그의 식별정보
	K : 태그에 저장된 비밀키 값
	$H(x)$: x를 해시연산
	m_L : 해시연산 결과 값의 좌측 절반

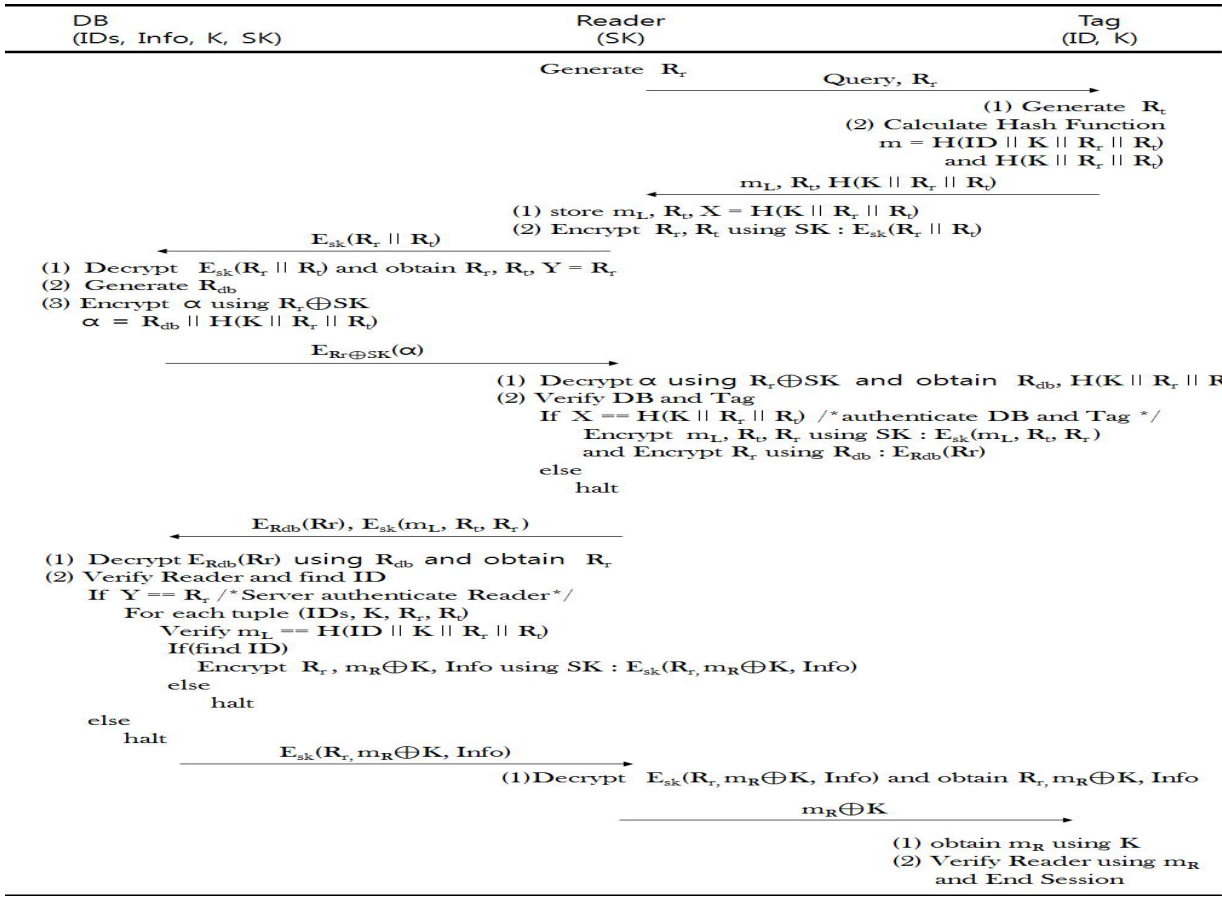


그림 4. 제안 프로토콜
Fig. 4. The Proposed Protocol

Step 3. $R \rightarrow DB(E_{SK}(R_r \| R_t))$

리더는 태그로부터 전송받은 값들을 서버로 바로 전송하지 않고, 서버와 상호인증을 시도하기 위하여 Step1에서 자신이 생성한 R_r와 R_t를 서버와 공유하고 있는 대칭키 SK로 암호화 하여 서버로 전송한다.

Step 4. $DB \rightarrow R(E_{R_r \oplus SK}(R_{db} \| H(K \| R_r \| R_t))$

서버는 리더로부터 전송받은 값을 자신의 대칭키로 복호화 하여 R_r값을 얻은 후 리더를 인증하기 위해 R_{db}를 생성하고 $R_{db} \| H(K \| R_r \| R_t)$값을 $R_r \oplus SK$로 암호화 하여 리더로 전송한다.

Step 5. $R \rightarrow DB(E_{R_{db}}(R_r), E_{SK}(m_L, R_t, R_r))$

리더는 서버로부터 받은 값을 Step1에서 자신이 생성한 R_r과 SK를 XOR 연산한 값으로 복호화 한다. 복호화 하여, $R_{db}, H(K \| R_r \| R_t)$ 두 개의 값을 얻을 수 있다. 여기서 Step1에서 태그가 생성한 $H(K \| R_r \| R_t)$값과 서버에서 전송한 $H(K \| R_r \| R_t)$값이 같은지 비교하여, 같다면 리더는 정당한 서버 및 태그로 인증한다. 같지 않다면 세션을 종료한다. 인증과정을 마친 후, 리더는 복호화 하여 획득한 R_{db}을 암호화키로 사용하여 R_r값을 대칭키 알고리즘으로 암호화 하고, Step 2에서 태그가 생성한 m_L, R_t, R_r을 리더와 서버가 공유한 대칭키 SK로 암호화하여 서버로 전송한다.

Step 6. $DB \rightarrow R(E_{SK}(R_r, m_R \oplus K, info))$

서버는 수신된 값을 Step 4에서 생성한 R_{db}값을 이용하여 복호화 연산을 수행한 후, Step 4에서 획득한 R_r값과 복호화 연산해서 얻은 R_r값이 동일한지를 비교하여, 같다면 정당한 리더로 인증한다. 만약 값이 동일하지 않다면 공격자가 전송한 데이터로 간주하고 세션을 종료한다. 리더의 인증과정을 마친 후, 서버는 리더와 공유한 대칭키 SK로 수신된 데이터를 복호화하여 m_L, R_t, R_r 값들을 획득한다. 그리고 이를 이용하여 ID 값에 대한 정보를 도

출한다. 마지막으로 서버는 $R_r, m_R \oplus K, info$ 값들을 대칭키 SK로 암호화 하여 리더로 전송한다.

Step 7. $R \rightarrow T(m_R \oplus K)$

리더는 서버에서 전송된 값을 복호화하여 태그에 대한 정보를 획득하고, 태그로 $m_R \oplus K$값을 전송한다. 태그는 자신이 가진 비밀키 K를 이용하여 m_R 값을 획득하고, 자신이 가지고 있는 값과 비교하여 같다면, 정당한 서버 및 리더로 인증함으로써 정상적으로 통신을 종료한다.

Ⅴ. 비교 분석

본 장에서는 RFID 시스템의 프로토콜이 지녀야 할 보안 요구사항을 기반으로 제안한 프로토콜이 다양한 공격에 안전함을 증명하고, HMAP에서 제안한 프로토콜과 보안성 및 효율성을 비교 분석한다. 표 3은 ABYN, HMAP와 제안한 프로토콜과의 안전성을 비교 분석한 것을 나타낸다.

5.1. 안전성 분석

RFID 시스템에서 프로토콜을 설계할 때, 상호인증(Mutual Authentication), 도청 공격(Eavesdropping Attack), 재전송 공격(Replay Attack), 중간자 공격(Man-in-the-middle attack), 위치 추적(Location Tracking) 등과 같은 보안 문제들을 고려하고 설계해야 한다. 제안한 프로토콜은 도청공격, 재전송 공격, 위치 추적 등에 안전하며 상호인증 및 전방향 안전성을 제공한다.

1) 상호인증(Mutual Authentication) : 상호인증은 태그와 리더가 상호간에 정당한지를 인증을 통해 확인하는 것이다. 제안한 프로토콜에서는 태그와 리더 뿐만 아니라 리더와 서버 사이도 안전하지 못한 채널이라고 가정하였으므로, 태그-리더 및 리더-서버 사이 모두 상호인증을 수행해야 한다. 제안한 프로토콜에서는 Step5~6번 과정을 거쳐 리더-서버 사이의 상호인증을 수행하고, Step5에서 리더는 서버를 통하여 태그를 인증한다. 그리고 Step7번 과정에 태그는 리더가 정당한지를 인증함으로써, 리더-태그간의 상호인증을 수행한다. 제안한 프로토콜에서는 각 객체 간에 상호 인증을 수행함으로써, 송·수신하는 객체가 정당한지를 확인할 수 있다.

2) 도청공격(Eavesdropping Attack) : 도청공격은 공격자가 안전하지 않은 채널사이에서 송·수신되는 모든 통신 내용을 엿듣고 저장하였다가 스푸핑 공격, 재전송 공격 등에 사용하거나 태그에 저장된 정보를 알아내고자 하는 공격이다. HMAP에서 제안한 프로토콜은 도청을 통하여 다음 세션에 사용할 태그의 비밀키 값을 유추할 수 있는 문제점이 있다.

제안 프로토콜에서도 도청 공격으로 리더와 태그 간, 리더와 서버 간 모든 데이터를 획득할 수 있지만, 공격자가 획득한 데이터에서 유효한 데이터를 알기 위해서는 $m_L = H(ID \| K \| R_r \| R_t)$ 에서 K, ID를 도출할 수 있어야 한다. 하지만 안전한 일 방향 해시 함수의 성질에 의해 공격자는 K, ID를 얻는 것은 불가능하다. 따라서 제안한 프로토콜은 도청공격에 안전하다.

3) 중간자 공격(Man-in-the-middle attack) : 통신하고 있는 리더-서버 또는 리더-태그 사이에 끼어들어 객체들이 교환하는 공개정보를 자기 것과 바꾸어버림으로써 들키지 않고 도청을 하거나 통신내용을 바꾸는 공격이다. 제안한 프로토콜에서는 리더와 서버 사이에서 비밀 키, 해시 값, 난수를 이용하여 상호인증하기 때문에 중간자 공격에 안전하다.

4) 재전송 공격(Replay Attack) : 공격자가 기존에 도청한 내용을 재전송하여 정당한 객체로 인증받으려는 공격이다. 제안한 프로토콜에서는 매 인증 세션마다 서버, 리더, 태그가 항상 새로운 난수들을 생성하여 상호인증을 수행하기 때문에 기존에 도청한 내용을 재전송하게 되면, 상호인증 과정에서 공격자임을 쉽게 알아낼 수 있다.

표 3. ABYN, HMAP와 제안 인증 프로토콜의 안전성 비교 분석
Table 3. The Security Analysis of the ABYN, HMAP and Proposed Authentication Protocol

공격유형 / 프로토콜	도청	위치추적	재전송 공격	중간자 공격	상호인증	전방향 안전성
ABYN	X	X	O	O	△	X
HMAP	X	O	O	O	O	△
제안한 프로토콜	O	O	O	O	O	O

O : 만족, △ : 부분만족, X : 불만족

표 4. 공격이 없을 경우의 효율성 비교 분석
Table 4. Efficiency of the HMAP and Proposed authentication protocol without attack

프로토콜 / 연산종류	HMAP				제안 인증 프로토콜			
	T	*R*	*DB*		*T*	*R*	*DB*	
해시연산량	2	0	Max	Avg	2	0	Max	Avg
			2n+1	n/2			n	n/2
대칭키 암복호화연산	0	2	2		0	5	5	
XOR 연산량	0	0	0		1	1	1	
난수 생성수	1	1	0		1	1	1	
인증과정 Step수	5				7			

n : *DB*에 저장된 최대 태그 수

표 5. 공격이 있을 경우의 효율성 비교 분석
Table 5. Efficiency of the HMAP and Proposed authentication protocol with attack

프로토콜 / 연산종류	HMAP				제안 인증 프로토콜				
	T	*R*	*DB*		*T*	*R*		*DB*	
해시연산량	2	0	Max	Avg	2	0		Max	Avg
			m*(2n+1)	m*(n/2)				n	n/2
대칭키 암복호화연산	0	2*m	2*m		0	Max	Min	Max	Min
						5*m	2*m	5*m	3*m

n : *DB*에 저장된 최대 태그 수, m : 중간자 공격 횟수

5) 위치 추적((Location Tracking)) : 리더의 요청에 대해 태그가 항상 동일한 값으로 응답하는 점을 이용하여 태그의 위치를 추적하는 공격이다. 그리고 위치 추적으로 인해 사용자의 프라이버시를 침해하는 문제점이 발생하게 된다. 제안한 프로토콜에서는 $m_L, R_t, H(K \| R_r \| R_t)$값들이 매 세션마다 변경되기 때문에 공격자가 특정한 태그를 식별할 수 없고, 사용자의 프라이버시를 보호 할 수 있다.

5.2. 효율성 분석

표 4는 제안한 프로토콜과 HMAP 프로토콜과의 효율성을 비교 및 분석한 표이다. 표 4와 같이 HMAP과 비교하여 제안한 프로토콜에서 리더와 서버의 대칭키 암·복호화 연산수가 증가하였고, 서버, 리더와 태그의 XOR연산의 수가 각각 1번 증가하였다. 암·복호화의 연산수와 인증과정의 스텝 수가 증가한 것은 서버와 리더간의 상호인증을 위해 늘어난 것이고, XOR의 연산의 경우 비밀키를 노출 시키지 않기 위해서이다. 하지만 해시 연산의 경우, HMAP에서는 최대 2n+1번 만큼 연산을 수행하는 것에 비해 제안한 프로토콜에서는 최대 n번만 해시 연산을 수행하면 된다. 표 5에서 보는 것과 같이 리더와 서버 사이에 중간자 공격이 가해질 경우, 제안한 프로토콜에서는 서버의 해시 연산량이 공격이 없을 경우와 동일하지만, HMAP은 서버의 해시 연산량이 공격횟수만큼 증가함을 볼 수 있다. 또한 본 논문에서 제안한 프로토콜은 리더와 서버의 대칭키 암·복호화 연산이 최소일 경우는 HMAP에서 제안한 프로토콜과 거의 동일하게 수행됨을 볼 수 있다.

Ⅵ. 결 론

본 논문에서는 최근 Jeon-Kim이 제안한 HMAP 프로토콜에서 도청공격으로 인해 다음 세션에 사용하게 되는 비밀 키가 노출되는 문제점을 분석하여 HMAP보다 개선된 해시기반의 상호 인증 프로토콜을 제안하였다. 또한 제안한 인증 프로토콜은 안전성 분석을 통하여 HMAP보다 도청공격을 이용한 보안 공격에 안전함을 증명하였다. 마지막으로 효율성 분석에서 제안 프로토콜이 HMAP에 비해 리더와 서버의 대칭키 암·복호화 연산수가 증가하였고, XOR연산의 수가 증가하였다. 그 이유는 HMAP과는 달리 제안한 프로토콜에서는 서버와 리더 사이에도 상호인증을 제공하기 때문이다. 하지만 공격자

가 중간자 공격을 할 경우, 제안한 프로토콜은 상호 인증을 제공하면서도 HMAP과 비슷한 효율을 보였고, 특히 서버의 해시 연산량의 경우 HMAP보다 적은 해시 연산을 수행하기 때문에 서버를 효율적으로 사용할 것으로 기대된다.

결론적으로 제안한 RFID 상호 인증 프로토콜은 HMAP에서 제안한 프로토콜과 비교하여 더욱 강한 보안성과 안전성을 제공하며, 공격이 있을 경우에는 효율성 측면에서도 우수하다. 따라서 본 논문에서 제안한 상호 인증 프로토콜은 다양한 RFID 시스템 응용 환경에서 안전성을 보장하기 위한 프로토콜로 사용 될 것으로 기대된다.

참 고 문 헌

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

[2] 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, 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] 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.

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

[6] Dong-ho Jeon, Hae-moon Kim, Hye-jin Kwon, Soon-ja Kim, "Hash-based Mutual Authentication Protocol for RFID Environment", *Journal of the Korea Information and Communications Society*, 35(1), pp. 42-52, Jan, 2010.

[7] Gene Tsudik, "YA-TRAP: Yet Another Trivial RFID Authentication Protocol", *Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops*, pp. 640-643, Mar. 2006.

[8] J. Aragones, A. Martinez-Balleste, and A. Solanas, "A brief survey on rfid privacy and security", *In World Congress on Engineering*, 2007.

[9] M. Ohkubo, K. Suzuki and S. Kinoshita, "Hash-chain based forward secure privacy protection sheme for low-cost RFID", *Proceedings of the 2004 Symposium on Cryptography and formation Security.Sendai*, pp. 719-724, 2004.

[10] D.W.Hong, K.Y.Chang, T.J.Park, K.I.Chung, "Trend of Cryptography for Ubiquitous Environment," *Electronics and Telecommunications Trends*, 20(1), pp. 63-72, Feb, 2005.

[11] Korea Information Security Agency, "RFID Privacy GuideLine", Sep, 2007.

[12] Tae Youn Won, Il Jung Kim, Eun Young Choi, Dong Hoon Lee, "Encryption scheme suitable to RFID Systems based on EPC Generation," *Journal of the Korea Institute of Information Security and Cryptology*, 18(1), pp. 67-75, Feb, 2008.

[13] Jung-Sik Cho, Sang-Soo Yeo, Sung-Kwon Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value", *Computer Communications*, Vol. 34, No. 3, pp.391-397, Mar. 2011.

[14] A. Juels, "RFID security and privacy: a research survey", IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp.381-394, Feb. 2006.

[15] Hae-Soon Ahn , Ki-Dong Bu , Eun-Jun Yoon , In-Gil Nam, "Improved Authentication Protocol for RFID/USN Environment," *Journal of the Institute of Electronics Enginners of Korea*, 46(1), pp.1-10. 2009.

[16] Kim-Dae Jung, Jun Moon Seog, "Design of RFID Mutual Authentication Protocol using One Time Random Number", *Journal of the Korea Information Science Society,* 35(3), pp.243-250, Jun, 2008.

[17] JangYoung Chung, YoungSik Hong, "RFID Authentication Protocol Verification in Serverless Environment", *Journal of the Korea Information Science Society,* 35(1A), pp.140-145, Jun, 2008.

[18] JaeCheol Ha , JeaHoon Park , JungHoon Ha,

HwanKoo Kim, SangJae Moon, "Low-cost Authentication Protocol Using Pre-synchronized Search Information in RFID System", *Journal of the Korea Institute of Information Security and Cryptology*, 18(1), pp.77-87, Feb. 2008.

[19] Chia-Hui Wei, Min-Shiang Hwang, Chin, A.Y, "A Mutual Authentication Protocol for RFID". *Computing & Processing*, vol.13, pp. 20-24. IEEE Computer Society (2011)

신 주 석 (Juseok Shin) 준회원

2006년 2월 경일대학교 컴퓨터 공학과 학사

2010년 2월 경북대학교 전자전기컴퓨터학부 석사

2010년 3월~현재 경북대학교 전자전기컴퓨터학부 박사과정, 한국전자통신연구원 연구원

<관심분야> RFID, 정보보호, 임베디드 시스템

오 세 진 (Sejin Oh) 준회원

2009년 2월 경운대학교 컴퓨터공학과 학사

2011년 2월 경북대학교 전자전기컴퓨터학부 석사

2011년 3월~현재 경북대학교 전자전기컴퓨터학부 박사과정

<관심분야> RFID, 충돌방지, 정보보호, 임베디드 리눅스 시스템

정 철 호 (Cheolho Jeong) 정회원

1984년 8월 경북대학교 전자공학 학사

1996년 8월 창원대학교 전자계산학과 석사

2010년 2월 경북대학교 컴퓨터공학과 박사

1999년 3월~현재 경남대학교 전자공학과 교수, 미래정보기술연구소 연구교수

<관심분야> 데이터베이스, RFID, 정보보호

정 경 호 (Kyungho Chung) 정회원

2000년 2월 대구대학교 컴퓨터 정보공학과 학사

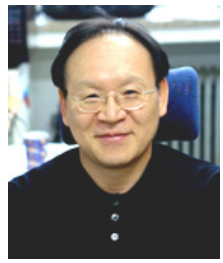
2002년 2월 경북대학교 컴퓨터공학과 석사

2011년 2월 경북대학교 컴퓨터공학과 박사

2005년 3월~현재 경운대학교 컴퓨터공학과 교수

<관심분야> 임베디드 리눅스 시스템, 시스템 프로그래밍, RFID, 정보보호

안 광 선 (Kwangseon Ahn) 정회원



1972년 2월 연세대학교 전기공학과 학사

1975년 2월 연세대학교 전자공학과 석사

1980년 2월 연세대학교 전자공학과 박사

1977년 3월~현재 경북대학교 컴퓨터공학과 교수

<관심분야> 임베디드 시스템 설계, RFID