인덱스를 사용한 초경량 RFID 인증 프로토콜

정회원 이 재 강*, 준회원 오 세 진*, 정회원 윤 태 진**, 정 경 호***, 안 광 선*

An Ultra-Lightweight RFID Authentication Protocol Using Index

Jaekang Lee* *Regular Member*, Sejin Oh* *Associate Member*,
Taejin Yun**, Kyungho Chung***, Kwang-seon Ahn* *Regular Members*

요 약

RFID 시스템은 바코드 대체 기술로 급부상 하지만 도청, 위치추적, 스푸핑 공격, 재전송 공격과 같은 다양한 공격에 취약하다. 이를 해결하고자 암호학적 기법이 연구되고 있지만 자원적 제약이 있는 수동형 태그에 적용하기 힘든 실정이다. 최근 초경량 RFID 인증 프로토콜은 RFID 태그에 적용 가능하지만 비동기화, T. Li가 제시한 능동 공격에 많은 문제가 있다. 본 논문에서는 초경량 RFID 인증 프로토콜의 문제를 해결하고, RFID 시스템에서 일어날 수 있는 일반적인 공격에 안전한 프로토콜을 설계하여 현실적으로 적용 가능한 프로토콜을 제안한다.

Key Words : RFID, Protocol, Ultra-Lightweight, Authentication, Index

ABSTRACT

Recently, the ultra-lightweight authentication RFID protocol that can actually implement on the RFID Tag is one among authentication protocols getting a concern, but recently many problems were clarified of the feature becase of the protocol which doesn't use the security algorithm. In this paper, we analyzed the problem of the ultra-lightweight authentication protocols and propose the design of ultra-lightweight RFID authentic ation protocols improving the index processing techniques. Because of improving the index processing technique in the method sending the Server authentication message to the authenticated tag, the proposed protocol is strong against the active attack which Li presents. Besides, the proposed protocol has the buffer storage of the keys and index and is strong against the asynchronous attack.

Ⅰ. 서 론

RFID(Radio Frequency Identification) 기술은 반도체 기술과 인터넷 기술의 발달로 교통, 물류, 국방, 의료, 축산 등 많은 분야에서 사용되고 있다. 이러한 RFID 기술은 라디오 주파수를 이용하여 사물의 정보를 주고받는데 기존의 바코드의 단점을 보완한 기술이다. RFID 시스템은 사물의 고유 정보를 저장하는 태그(Tag)와 태그의 정보를 읽어 들이는 리더(Reader), 리더가 태그로부터 읽어 들인 정보를 처리하는 서버로 구성된다[1]. 리더의 안테나 코일은 주변 지역에 자기장을 발생시키며, 이에 태그는 유도성 전압을 발생시켜 전원공급을 받아 태그의 고유 식별 정보(ID)를 리더에 전송하게 된다. 이와 같이 리더와 태그 사이는 무선 채널 상에서의 데이터 전송으로 인해 도청, 위치추적, 스푸핑 공격, 재전송 공격, 서비스 거부 공격과 같은 다양한 공격에 취약하다[2]. 이를 해결하고자 상호인증, 해시 함수, 공개키 암호화 기법, 대칭키 암호화 기법과 같은 다양한 프로토콜이 연구되고 있는 실정이다. 그

* 경북대학교 전자전기컴퓨터학부 임베디드 시스템 연구실({10004oke, 170m3, gsahn}@knu.ac.kr), (° : 교신저자)
** 경운대학교 모바일공학과(tjyun@ikw.ac.kr), *** 경운대학교 컴퓨터공학과(mccart@ikw.ac.kr)
논문번호 : KICS2011-08-369, 접수일자 : 2011년 8월 23일, 최종논문접수일자 : 2011년 12월 30일

러나 수동형 태그에 해시 함수, 공개키 암호화 기법, 대칭키 암호화 기법들은 현실적으로 적용이 불가능한 상황이다. 최근 초경량 인증 프로토콜은 현실적으로 적용 가능한 프로토콜로 인증 받아 활발히 연구가 이루어지고 있는 분야 중 하나이다. 새로운 프로토콜이 발표될 때 마다 그 안전성을 검토하는 논문이 연이어 발표되고 있어, 최근 지속적인 발전을 이루고 있다.

본 논문에서는 초경량 인증 기법으로 수동형 RFID 태그에 적용 가능하게 하며, RFID의 다양한 공격에 안전한 프로토콜을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 다양한 암호학적 인증 기법과 문제점에 대해서 기술한다. 3장에서는 다양한 공격에 안전하고 현실적으로 적용 가능한 프로토콜을 제안한다. 그리고 4장에서는 기존의 프로토콜과 제안 프로토콜과의 보안성 및 효율성을 비교 분석한다. 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

RFID 시스템은 태그(Tag)와 리더(Reader)간 무선 상에서 통신을 하기 때문에 도청, 위치 추적, 스푸핑 공격, 재전송 공격, 서비스 거부 공격과 같은 위험성을 가지고 있다. 이러한 문제를 해결하기 위해서 암호학적 연구의 필요성이 제기 되었고, 다양한 RFID 프로토콜이 제안되었다. 본 장에서는 다양한 암호학적 보안기법들과 문제점을 살펴본다.

2.1. 경량 인증 기법

인증 기법은 크게 중량, 경량, 초경량으로 분류할 수 있다. 중량 인증 기법은 기존의 유 무선망에서 사용하는 암호화 알고리즘을 적용하는 것으로서, 저가의 태그가 가지고 있는 제한된 자원 때문에 RFID 시스템에 적용하기 힘들다. 따라서 자원 소비를 최소로 하는 저가의 태그에 적용 가능한 기법으로 경량 및 초경량 인증 프로토콜 연구가 활발히 진행되고 있다. 경량 인증 기법은 난수 생성기와 간단한 함수를 사용하는 방식으로 Gen2 기반의 기법들이 이에 속한다. 초경량 인증 기법은 XOR, AND, OR과 같은 비트 연산만을 사용하며 대표적인 기법은 Peris-Lopez의 프로토콜[3-5]이다. 본 절에서는 경량, 초경량 인증 기법에 대해 알아본다.

2.1.1. Gen2 기반의 경량 인증 기법

EPC Class-1 Gen2는 PRNG(Pseudo Random Number Generator)와 같은 16비트 난수 생성기와 CRC(Cyclic Redundancy Code)를 지원하고 있다. Gen2 기반의 경량 인증 기법은 암호화 기법을 사용하지 않고 난수와 CRC만을 사용하여 안전하게 상호 인증을 수행한다. 8비트 패스워드를 지원하는 Gen1 반해, Gen2는 태그에 32비트의 Kill과 Access 패스워드가 추가되어있다. 이 패스워드는 태그 기능을 영구 정지시키거나 태그의 특정 메모리 영역의 쓰기 기능을 제한하여 프라이버시 보호와 향상된 안전성을 기대할 수 있다. 대표적으로 S. Karthikeyan은 XOR 연산과 행렬만을 이용하여 태그와 리더를 인증하는 기법을 제안하였으며[6], D.N. Duc은 Gen2에서 제공하는 PRNG 함수와 CRC만을 사용한 인증 기법을 제안하였다[7]. 그리고 M. Feldhofer는 난수를 이용한 상호 인증 기법을 제안하였다[8]. 그림 1은 EPC Class-1 Gen2 기반의 상호 인증 과정을 보여 주고 있다. Gen2 기반의 상호 인증 기법은 서버의 처리 동작 없이 리더와 태그가 상호 인증을 수행한다. 하지만 리더와 태그가 가진 $Apwd_R$을 비교하여 인증하는 과정은 공격자의 공격에 매우 취약하다. 공격자는 $Cpwd_1$과 $R1_{Tag}$를 도청 공격으로 획득하여 XOR연산을 수행하여 $Apwd_R$값을 획득할 수 있다. 그리고 공격자는 태그에게 $R1_{Tag}$를 보내게 되면 동일한 $Cpwd_1$값을 수신하기 때문에 위치 추적에 취약하다. 또한 재전송 공격으로 인증과정을 통과할 수 있다. 이 처럼 Gen2 기반의 경량 인증 기법은 단순 연산자만을 사용하기 때문에 높은 효율성은 보장하지만 RFID 시스템의 보안 및 프라이버시 문제를 완전히 해결하지 못한다.

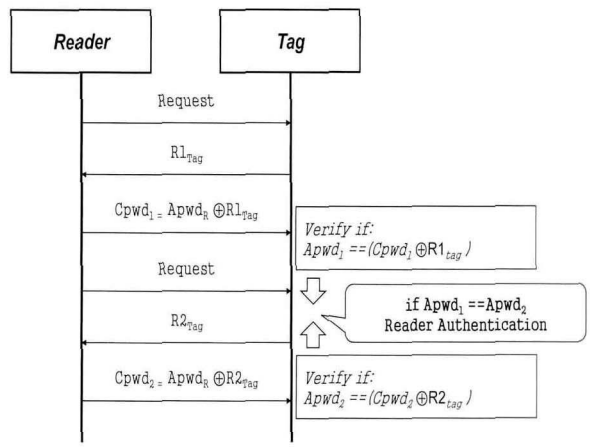


그림 1. EPC Classs-1 Gen2의 상호인증
Fig. 1. A Mutual Authentication of EPC Class-1 Gen2

2.1.2. Hash-Chain 프로토콜

Hash-Chain 프로토콜은 두 개의 해시 함수 H와 G를 사용하여 해시 체인을 구성하는 매우 안전한 프로토콜이다[9]. 태그는 리더의 i번째 요청에 자신의 $A_i=G(S_i)$를 보내고 자신은 $S_i+1=H(S_i)$로 갱신한다. 태그는 매번 다른 A_i를 전송하므로 위치 추적에 안전하나 서버의 연산량이 많고, 태그 역시 두 번의 해시 연산을 해야 하는 부담을 가지고 있다. 그림 2는 Hash-Chain의 프로토콜을 나타낸 것이다.

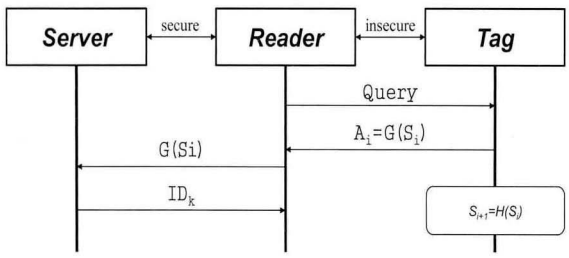


그림 2. Hash-Chain 프로토콜
Fig. 2. Hash-Chain Protocol

2.1.3. M. Feldhofer의 상호인증 프로토콜

M. Feldhofer는 AES(Advanced Encryption Standard)를 이용한 인증 프로토콜을 제안하였다[8].

AES 암호화 알고리즘을 사용하여 해시 함수와 공개키 기반의 암호화 알고리즘의 큰 문제였던 하드웨어 제약사항을 해결하였다. 리더와 태그의 난수를 암호화한 값을 전송하여 인증하여 도청, 스푸핑 공격, 재전송 공격에 안전하다. 그러나 암호화에 사용되는 리더와 태그의 난수가 노출된 값과 암호화된 값이 존재하여 전수 키 조사로 대칭키가 노출되는 문제점이 있다. 그림 3은 M. Feldhofer의 상호인증 프로토콜을 나타낸 것이다.

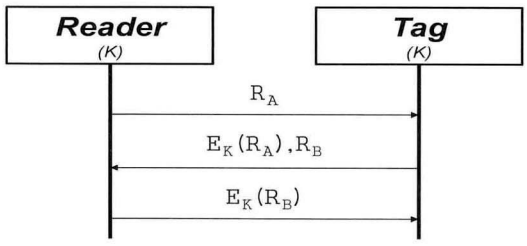


그림 3. M. Feldhofer의 상호인증 프로토콜
Fig. 3. M. Feldhofer's a Mutual Authentication Protocol

2.2. 초경량 인증 기법

초경량 인증 프로토콜은 논리 연산자(XOR, AND, OR)와 산술 연산자 (ADD, SUB)를 이용하여 자원 소비를 최소화 하는 인증 기법이다. 이러한 프로토콜은 300게이트 정도의 매우 효율적인 기법이다. 그러나 비동기화 공격 및 태그 완전 노출될 수 있는 문제점이 있다. 하지만 최소 하드웨어 요구조건과 EPC Global에서 요구하는 초당 100회 통신[10]등 모든 요구사항을 충족하는 유일한 기법이기 때문에 가장 연구가 활발한 분야 중 하나이다. 본 절에서는 최근 발표된 경량 인증 프로토콜을 살펴보고 이들이 가진 문제점을 알아보도록 한다.

2.2.1. Peris-Lopez의 프로토콜

Peris-Lopez는 초경량 인증 프로토콜인 LMAP(A Real Lightweight Mutual-Authentication Protocol)[3]을 시작으로 이를 보완한 M2AP(A Minmalist Mutual-Authentication Protocol)[4] 그리고 EMAP(An Efficient Mutual-Authentication Protocol)[5]를 연이어 발표하였다. 이 프로토콜의 특징은 우선 XOR, AND, OR, 그리고 ADD까지 총 4개의 논리·산술 연산자와 암호화를 위한 K1~K4의 키를 사용한다. 그리고 고정된 96비트의 ID를 사용하며 태그 식별을 위한 IDS(Index-pseudonym)를 사용한다. 인증을 위한 단계는 총 3단계로 이루어지며 과정은 다음과 같다.

단계 1: 초기 질의

(1) 리더→ 태그: hello

(2) 태그→ 리더: $IDS^{(n)}$

단계 2: 상호 인증

○ LMAP

(1) 리더→ 태그: $A||B||C$

(2) 태그→ 리더: D

- $A = IDS^{(n)} \oplus K1^{(n)} \oplus n1,$
- $B = (IDS^{(n)} \vee K2^{(n)}) + n1,$
- $C = IDS^{(n)} + K3^{(n)} + n2,$
- $D = (IDS^{(n)} + ID) \oplus n1 \oplus n2.$

○ M2AP

(1) 리더→ 태그: $A||B||C$

(2) 태그→ 리더: $D||E$

- $A = IDS^{(n)} \oplus K1^{(n)} \oplus n1,$
- $B = (IDS^{(n)} \wedge K2^{(n)}) \vee n1,$
- $C = IDS^{(n)} + K3^{(n)} + n2,$
- $D = (IDS^{(n)} \vee ID) \wedge n2,$
- $E = (IDS^{(n)} + ID) \oplus n1.$

○ EMAP

(1) 리더→ 태그: $A||B||C$

(2) 태그→ 리더: $D||E$

- $A = IDS^{(n)} \oplus K1^{(n)} \oplus n1,$
- $B = (IDS^{(n)} \vee K2^{(n)}) \oplus n1,$
- $C = IDS^{(n)} \oplus K3^{(n)} \oplus n2,$
- $D = (IDS^{(n)} \wedge K4^{(n)}) \oplus n2,$
- $E = (IDS^{(n)} \wedge n1 \vee n2) \oplus ID \oplus \bigoplus_{I=1}^{4} KT^{(n)}.$

단계 3: IDS와 비밀키 갱신

○ LMAP

- $IDS^{(n+1)} = (IDS^{(n)} + (n2 \oplus K4^{(n)})) \oplus ID,$
- $K1^{(n+1)} = K1^{(n)} \oplus n2 \oplus (K3^{(n)} + ID),$
- $K2^{(n+1)} = K2^{(n)} \oplus n2 \oplus (K4^{(n)} + ID),$
- $K3^{(n+1)} = (K3^{(n)} \oplus n1) + (K1^{(n)} \oplus ID),$
- $K4^{(n+1)} = (K4^{(n)} \oplus n1) + (K2^{(n)} \oplus ID)$

○ M2AP

- $IDS^{(n+1)} = (IDS^{(n)} + (n2 \oplus n1)) \oplus ID,$
- $K1^{(n+1)} = K1^{(n)} \oplus n2 \oplus (K3^{(n)} + ID),$
- $K2^{(n+1)} = K2^{(n)} \oplus n2 \oplus (K4^{(n)} + ID),$
- $K3^{(n+1)} = (K3^{(n)} \oplus n1) + (K1^{(n)} \oplus ID),$
- $K4^{(n+1)} = (K4^{(n)} \oplus n1) + (K2^{(n)} \oplus ID)$

○ EMAP

- $IDS^{(n+1)} = IDS^{(n)} \oplus n2 \oplus K1^{(n)},$
- $K1^{(n+1)} = K1^{(n)} \oplus n2 \oplus (IDS(95:48) || F_p(K4^{(n)}) || F_p(K3^{(n)})),$
- $K2^{(n+1)} = K2^{(n)} \oplus n2 \oplus (F_p(K1^{(n)}) || F_p(K4^{(n)}) || ID(47:0)),$
- $K3^{(n+1)} = K3^{(n)} \oplus n1 \oplus (IDS(95:48) || F_p(K4^{(n)}) || F_p(K2^{(n)})),$
- $K4^{(n+1)} = K4^{(n)} \oplus n1 \oplus (F_p(K3^{(n)}) || F_p(K1^{(n)}) || ID(47:0)).$

Peris-Lopez의 프로토콜의 가장 큰 문제점은 리더의 요청에 태그는 항상 같은 응답인 $IDS^{(n)}$으로 한다는 것이다. 이것은 T. Li[11,12]의 방법으로 ID까지 유출 되는 방법이 연구되었다. 뿐만 아니라 비정상적인 통신종료에 의해 비동기화 공격 또한 일어날 수 있다[13].

2.2.2. 경량 프로토콜에 대한 T. Li 능동 공격[11,12]

RFID 시스템의 공격 중에는 능동 공격과 수동 공격으로 나누어 볼 수 있다. 먼저 수동 공격은 리더와 태그 간에 송·수신되는 모든 통신 내용을 엿들은 후 태그에 저장된 비밀 정보를 알아내고자 하는 도청 공격이 있다. 능동 공격은 리더와 태그 간의 데이터를 도청 공격으로 획득한 데이터를 재전송하는 공격과 획득한 데이터를 위·변조하여 비동기화를 일으키는 비동기화 공격이 있다.

T. Li 능동 공격에서 LMAP, M2AP, EMAP 등에 적용된 분석 방법은 다음과 같다. 인증 과정에서 전송되는 메시지의 한 비트를 변형하고, 인증 여부를 확인한다. 그 후, 비밀키의 해당 비트 정보를 얻어내는 것이다. x, y, r이 미지수이고, A=x⊕r과 B=y+r이 주어졌을 때, A, B를 한 비트 씩 변형한 A'=x⊕y[I]i, B'=(y+r)⊕[I]i(는 i번째 비트만 1이고 나머지는 0인 비트열)가 유효한 응답 쌍이 될 확률(B'=y+(r⊕[I]i)이 될 확률)이 50%라는 점과, A, B, A', B''=y+(r⊕[I]i)가 주어지면 B'과 B''를 비교하여 [r]i의 정보를 얻을 수 있다는 성질을 이용한다[13].

2.2.3. 최은영의 프로토콜

최은영의 프로토콜은 저가의 RFID 태그를 위한 프라이버시를 보호하는 안전하고 효율적인 프로토콜을 제안하였다. 이 프로토콜은 해시함수, 암호화 알고리즘을 사용하지 않고, 앞서 소개한 Peris-Lopez의 프로토콜과 마찬가지로 인덱스와 비트 연산을 이용한 초경량 프로토콜의 하나이다. Peris-Lopez가 가지는 비동기화 공격 문제는 해결되었지만, 리더의 요청에 항상 같은 인덱스 값을 보내기 때문에 T. Li의 논문에서 제기된 비정상 종료에서 일어나는 비동기화 공격에 취약하며, 인덱스 값이 해킹되는 암호학적 문제점이 있다. 그림4는 최은영의 프로토콜[14]을 나타낸 것이다.

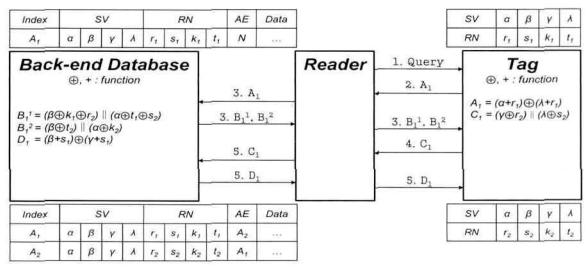


그림 4. 최은영의 프로토콜
Fig. 4. E. Choi's Protocol

2.3. OTP(One-Time-Pad)

OTP(One-Time-Pad)는 단순한 XOR 연산을 이용하여 암·복호화 하는 기법이다. 많은 암호화 기법 중 유일하게 완벽한 안전성을 지니고 있으며[15-16], 평문(m), 비밀키(k), 암호문(c)을 수식으로 나타내면 다음과 같다.

$$m = m1, m2, \cdots mn \in \{0,1\}n \quad (1)$$

$$k = k1, k2, \cdots kn \in \{0,1\}n \quad (2)$$

$$c = c1, c2, \cdots cn;\ ci = bi \oplus ki,\ 1 \le i \le n \quad (3)$$

OTP를 사용하기 위한 조건은 비밀키는 랜덤하게 생성하여야 한다. 그리고 한번 사용한 비밀키는 다

시 사용하지 않아야하며, 평문과 비밀키의 길이가 동일해야하는 특징을 지니고 있다[17].

Ⅲ. 제안 프로토콜

본 장에서는 RFID시스템에 알려진 일반적인 공격뿐만 아니라 초경량 RFID 상호인증 프로토콜에 대한 능동 공격에도 안전한 인덱스 처리기법을 개선한 초경량인증 프로토콜을 제안한다. 이 프로토콜은 실제 태그에 적용 할 수 있도록 OTP(One-Time-Pad)와 논리연산자(XOR, AND, OR)와 산술연산자(ADD, SUB)를 이용한 암호학적 기법을 적용하며 서버와 태그모두 인증을 거치는 상호인증을 수행한다. 제안 프로토콜은 가정 사항 및 표기법, 제안 프로토콜로 구성되며 초기화 단계, 상호인증 단계 IDS와 키 값 갱신 단계로 구성된다.

3.1. 가정 사항 및 표기법

제안 프로토콜의 가정 사항은 다음과 같고 표 1은 제안 프로토콜의 표기법을 나타낸 것이다.

표 1. 표기법
Table 1. Notations

표기법	내용
ID	태그의 고유 식별 값
IDS	Index-pseudonym
HRN	Hidden Random Number
Rr	리더에서 생성한 난수
Rt	태그에서 생성한 난수
Rs	서버에서 생성한 난수
R_{IDS}	IDS를 Rr로 XOR하여 숨긴 값
$K\eta$	η번째 키
X	new, old 임시 저장소
$\|$	연접 연산자
$\oplus$	eXclusive-OR (XOR) 연산
$\wedge$	OR 연산
$\vee$	AND 연산
+	더하기 연산
-	빼기 연산
PRNG()	난수 생성기

1) 서버와 리더 사이는 안전한 통신 채널을 이용함으로써 공격자의 공격에 안전하다.
2) 리더와 태그 사이는 무선 상의 통신 채널이므로 공격자의 공격에 취약하다.
3) 서버, 리더, 태그 모두 난수를 생성할 수 있다.
4) 서버는 ID, 초기화된 인덱스 값인 IDS, 키 값 K0~K6가 초기화 되어있다.
5) 태그는 ID, IDS, K0~K6 서버와 같은 동일한 값을 가지고 있다.
6) 리더와 태그는 사전에 난수를 숨기기 위한 동일한 키 값 K0를 안전하게 가지고 있다.
7) 리더와 태그가 생성한 난수는 처음 세션이 연결될 때 마다 새로이 생성된다.

3.2. 제안 프로토콜

본 논문에서는 OTP기법을 이용하여 R_{IDS}와 함께 인증 비교 값인 A, B, C를 함께 보내고 서버는 태그를 인증 후에 다음 진행을 함으로써 위치추적과 능동공격에 강하며 그리고, 임시 저장소 X를 이용하여 old값과 new값을 별도로 관리하여 어떤 비동기화 공격에도 안전하도록 설계 하였다. 제안 프로토콜의 전체 구성은 태그의 인증 단계, 서버의 인증 단계 그리고 키 갱신 단계까지 총 3단계로 이루어져 있다. 그림 5는 본 논문에서 제안한 프로토콜이다.

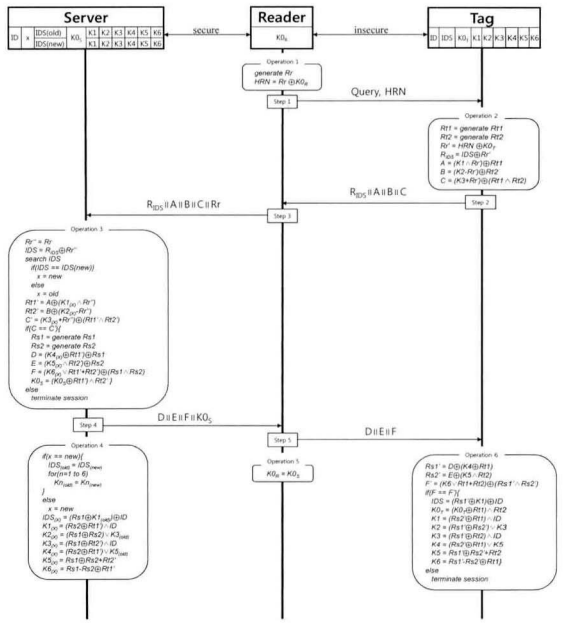


그림 5. 제안 프로토콜
Fig. 5. The Proposed Protocol

3.2.1. 태그 인증 단계

상호 인증 과정 중 태그 인증 단계는 리더가 태그에게 Query(질의)를 보내면서 시작된다. 그림 6는 본 논문에서 제안한 태그 인증 과정이다.

1) Operation 1.

초기 질의 단계에서 리더는 난수 Rr를 생성한다. 그리고 Rr를 $K0_R$와 OTP(One-Time Pad) 연산을 하여 HRN을 생성한다. 리더가 생성한 HRN을 Step 1과 같이 태그에게 Query와 함께 전송한다.

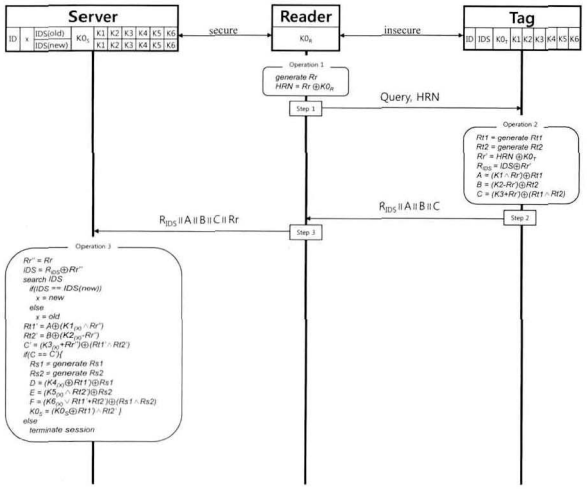


그림 6. 태그 인증
Fig. 6. Tag Authentication

2) Operation 2.

태그는 리더로 부터 받은 HRN과 $K0_T$를 OTP 복호화 연산을 통하여 Rr'을 획득한다. 그리고 태그가 가진 IDS와 Rr'을 이용하여 R_{IDS}를 생성하고, 태그 자신이 생성한 Rt1, Rt2를 K1~K3을 이용하여 A, B, C를 생성한다. 생성된 R_{IDS}와 A, B, C를 Step 2와 같이 리더에게 전송한다. 리더는 $R_{IDS} \| A \| B \| C$에 Rr을 연접하여 Step 3과 같이 서버로 보낸다.

3) Operation 3.

서버는 리더로 부터 받은 Rr''과 R_{IDS}를 통하여 IDS를 복호화 한다. 복호화 한 IDS를 DB에서 검색하여 K1~K6를 찾는다. 이때 IDS가 ID에서 old인지 new인지를 알아내고, 이 값을 X에 저장한다. 그리고 서버는 서버가 가지고 있는 K1, K2와 리더로 부터 받은 Rr''을 이용하여 Rt1', Rt2'를 생성한다. 생성된 Rt1', Rt2'을 이용하여 C'를 생성하여 태그로부터 받은 C와 서버에서 생성한 C'를 비교한다. 비교한 값이 같으면 정상적으로 태그가 인증 된 것이고 다르면 즉시 세션을 종료한다.

3.2.2 서버 인증 단계 및 키 갱신

그림 7은 서버를 인증하는 과정과 키를 갱신하는 과정을 세부적으로 나타낸 것이다.

1) Operation 3.

Operation 3에서 서버가 태그를 인증하였을 경우, 서버는 서버 난수 Rs1, Rs2와 리더 난수 Rt1', Rt2' 그리고 K4, K5, K6를 이용하여 D, E, F를 생성한다. 생성한 D, E, F와 갱신된 $K0_S$를 Step 4와 같이 연접하여 리더에게 전송하고, 리더는 태그에게 $D \| E \| F$를 전송한다.

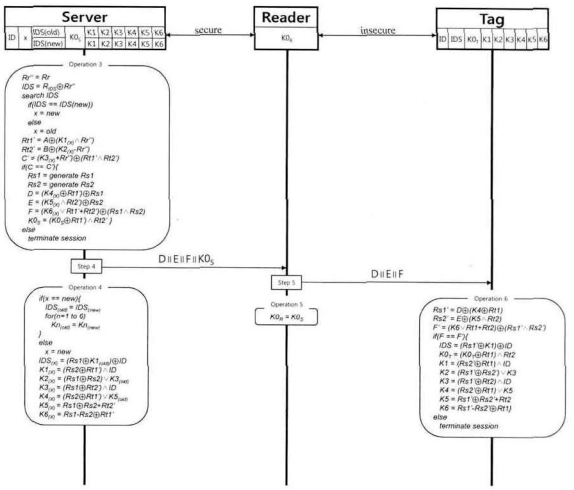


그림 7. 서버 인증 및 키 갱신
Fig. 7. Server Authentication and Key Change

2) Operation 6.

태그는 자신이 가지고 있는 K4, K5와 Rt1, Rt2를 이용하여 Rs1', Rs2'를 생성하여 F'를 생성한다. 태그는 F'과 서버로부터 받은 F를 비교하여 같으면 정상적으로 서버인증을 하고 다르면 즉시 세션을 종료한다.

3.2.3 키 갱신 단계

제안 프로토콜의 마지막 갱신 단계는 태그와 서버가 서로 인증이 되었을 때 다음 통신에 사용할 키를 갱신하는 단계이다. 키 갱신은 서버, 리더 그리고 태그까지 키 갱신이 이루어진다.

1) Operation 4.

서버는 정상적으로 태그 인증을 한 뒤, $D \| E \| F \| K0_S$를 전송하고 IDS, K1~K6값 갱신을 수행한다. 서버 측 키 갱신 작업은 old와 new값을 가진 X의 값을 비교하는 것부터 시작한다. X가 new값 즉 이전 세션이 정상인 경우 기존 IDS와 K1~K6를 old에 저장한다. 만약 X값이 old일 경우 그 값은 그냥 두고 new값 만 갱신한다.

2) Operation 5.

리더는 서버로부터 받은 키 값 $K0_S$를 $K0_R$로 갱신한다.

3) Operation 6.

태그가 정상적으로 서버를 인증한 경우 키 값 갱신이 이루어진다. 태그 측에서는 X값을 따로 저장하지 않으며 이를 판별하는 과정만 생략될 뿐 Operation 4의 갱신방법과 동일하다.

Ⅳ. 비교 분석

본 장에서는 기존 프로토콜과 제안 프로토콜의 보안성 및 효율성을 비교 분석한다.

4.1. 보안성 분석

본 절에서는 제안 프로토콜에 대한 도청 공격, 재전송 공격, 위치 추적, 서비스 거부공격, 비동기화 공격에 대한 보안성을 분석한다.

4.1.1. 도청 공격(Eavesdropping)

RFID 시스템에서 리더와 태그사이의 통신은 무선 채널로서, 불안전한 채널(Insecure Channel)이라고 가정하였다. 따라서 리더와 태그사이의 통신내용은 언제 듣지 도청될 수 있다. 그래서 통신의 내용이 도청 당하더라도 공격자에게 아무 의미 없는 값이 되어야 한다.

제안 프로토콜의 경우 Step 1, Setep 2, Step 5에서 무선 채널을 이용하여 통신을 한다. Step 1은 암호학 기법 중 완벽한 안전성을 가진 OTP 기법으로 암호화 하였기에 공격자의 공격에 안전하다. Step 2의 경우 두 개의 태그 난수를 생성한 뒤 이를 조합하여 항상 다른 값으로 Step 2를 진행한다. 따라서 공격자가 Step 2에서 도청하여 얻어진 데이터는 키 유추 및 재사용을 하지 못한다. Step 5역시 도청을 하더라도 두 개의 서버난수를 포함하여 암호화 되었으므로 특별한 정보를 알 수 없다. 더군다나 모든 메시지는 일회성 키에 의해 각각 암호화 되므로 첫 번째 통신에 무언가 알아내더라도 한번 세션이 종료되면 그 후에는 이미 모든 키와 IDS가 갱신되어 있으므로 쓸모없는 값이 된다.

4.1.2. 재전송 공격(Replay Attack)

도청으로 획득한 데이터를 특별한 가공 없이 리더에 재전송 하여 인증을 받거나, 획득하고자 하는 값을 유추하는 공격방법이다. 제안 프로토콜의 경우 IDS와 K0~K6가 갱신되기 때문에 재전송 공격은 인증 단계에서 실패하게 된다. 만약 이전 통신이 무언가의 문제에 의하여 중단되어 값이 갱신되지 않았다고 하더라도 리더에서 발생된 난수인 Rr값이 이미 바뀌어 있으므로 이전 통신에서 쓰인 값을 그대로 쓸 수는 없는 구조로 되어있다.

4.1.3. 위치 추적(Location Tracking)

위치 추적은 RFID 시스템의 초기 질의 단계에서 리더가 태그에게 통신을 요청하는 Query에 대한 항상 고정된 응답 값으로 태그의 위치를 추적하는 것이다. 본 논문에서는 Query에 대한 항상 가변적인 응답 값을 출력하고자 태그는 매 세션 마다 리더 난수 Rr'과 태그 난수 Rt1, Rt2를 사용하여 가변적인 $R_{IDS} \| A \| B \| C$ 이므로 위치 추적을 피할 수 있다.

4.1.4. 서비스 거부 공격(Denial of Service Attack)

여러 가지 형태로 서버에 부하를 주어 서비스를 방해하는 서비스 거부 공격도 최근 RFID 시스템에 일어날 수 있는 공격 형태의 하나로 많은 관심을 받고 있다. 해시와 AES 암호화 알고리즘을 사용하는 프로토콜은 서버, 리더, 태그에 많은 연산량과 연산 시간으로 부하가 크다. 부하가 큰 점은 공격자의 서비스 거부 공격의 대상이 될 수 있다. 본 논문에서는 연산량이 적은 논리·산술 연산만으로 상호 인증 과정과 태그 ID를 전달하므로 서비스 거부 공격에 안전하다. 상호 인증 과정을 통해서 인증 받지 못한 개체는 통신을 종료하는 과정 또한 서비스 거부 공격을 방어하는 역할을 한다.

4.1.5. 비동기화 공격(Desynchronization Attack)

초경량 인증 프로토콜의 경우 매 세션마다 키와 인덱스 값이 갱신되기 때문에 비동기화 공격에 상당히 약하다. 비동기화 공격이란 서버가 가지고 있는 IDS와 키 값이 태그가 가지고 있는 값과 달라서 태그를 더 이상 사용할 수 없는 상태가 되는 것을 말한다. 제안 프로토콜은 키 값을 old와 new로 나누어 서버에 저장한다. 따라서 시스템의 오류나 공격에 인한 통신 중단에도 서버는 바로 이전 정보까지 저장하고 있으므로 비동기화 공격에 안전하다.

4.1.6. T. Li 능동 공격

T. Li가 제안한 능동 공격이 이루어 질 수 있는 근본적인 원인은 리더의 요청(Query)이 있으면 태그는 IDS를 서버에 보내고 서버는 항상 응답을 하기 때문에 이러한 분석이 가능한 것이다. 본 논문에

서는 이러한 문제점을 해결하기 위하여 IDS와 함께 태그 인증 메시지인 A, B, C를 함께 보낸다. 서버는 정상적인 태그로 인증되어야 인증 메시지를 다시 태그로 돌려주므로 T. Li가 제시한 공격 방법에 안전하다.

표 2는 제안한 프로토콜과 해시기반 Hash-Chain 프로토콜, 대칭키 기반의 M. Feldhofer의 프로토콜, 그리고 초경량 프로토콜의 안전성을 도청, 재전송 공격, 위치추적, 서비스 거부공격, 비동기화 공격, T. Li의 능동 공격에 대하여 비교 및 분석한 결과이다.

표 2. 기존 프로토콜과 제안 프로토콜의 안정성 비교
Table 2. The Safety Analysis of RFID Protocols

	도 청	재전송 공격	위 치 추 적	DoS 공격	비동기화 공격	T. Li의 능동공격
Hash Chain[9]	safe	safe	partially safe	unsafe	unsafe	-
M. Feldhofer[8]	safe	safe	safe	unsafe	safe	-
Peris Lopez[5]	unsafe	safe	unsafe	Partially safe	unsafe	unsafe
최은영[14]	unsafe	safe	unsafe	Partially safe	safe	unsafe
제안 프로트콜	safe	safe	partially safe	Partially safe	safe	safe

4.2. 효율성 분석

표 3은 기존 프로토콜과 제안 프로토콜을 비교 분석 한 것이다. 효율성 분석에 주요 비교 요소인 게이트 수, 초당 100회 통신[10] 만족여부, 프로토콜 라운드, 그리고 서버 부하정도를 알아본다.

900MHz대 주파수를 이용하는 수동형 RFID 태그에서 사용할 수 있는 최대 전력량은 알려진 바와 같이 20μW이다. RFID 칩 제조에 사용하는 CMOS 공정을 이용하여 20μW 이내로 회로를 설계할 경우 우리가 사용할 수 있는 게이트 수는 5000게이트 내외로 알려져 있다. 따라서 기본적으로 회로를 설계함에 있어 5000게이트를 넘지 않게 설계하는 것은 매우 중요하다. 그리고 또 다른 제약사항은 초당 100회 통신의 만족여부이다. EPC Global에서는 원활한 통신을 위해 초당 100회 통신을 만족하는 프로토콜을 설계하여야 한다고 표준에서 명시하고 있다. 두 가지 주요 제약사항과 함께 프로토콜 라운드

표 3. 효율성 비교 분석
Table 3. The Efficiency Analysis of RFID Protocols

	Hash Chain[9]	M. Feldhofer[8]	Peris Lopez[5]	최은영[14]	제안 프로트콜
게이트 수	20,000 Gates 이상	5,000 Gates 미만	1,000 Gates 미만	1,000 Gates 미만	1,000 Gates 미만
100회 통신/Sec	만족	불만족	만족	만족	만족
프로토콜 라운드	4회	3회	4회	5회	3회
서버 부하	매우 큼	보통	보통	보통	보통

횟수, 그리고 서버 부하를 효율성 분석에서 알아본다.

먼저 Hash-Chain의 경우 알려진 바와 같이 표준 SHA에서 요구하는 게이트 수가 20,000~25,000게이트이다. 현재 이론적으로 가장 우수한 프로토콜 중 하나이지만 현실적으로 적용하기 힘든 프로토콜이다. 우수한 하드웨어 설계를 기반으로 하고 있어 초당 100회 통신을 만족하고 프로토콜 설계에 따라 프로토콜 라운드 횟수도 상당히 줄일 수 있다. 하지만 위치 추적, 재전송 공격 등을 피하기 위하여 모든 리더의 요청마다 새롭게 모든 ID를 해시 하여야 하기 때문에 태그의 숫자 증가와 함께 서버부하도 비례하여 늘어난다는 단점을 지니고 있다.

M. Feldhofer는 RFID 태그에서 AES의 사용 가능성을 제시하였다. 그 후 이를 이용한 많은 프로토콜이 제안되었다. 초기의 M. Feldhofer의 프로토콜에는 많은 문제점이 발견되어 최근에 연구된 프로토콜에서는 두 번 이상의 암·복호화를 태그에서 수행하여 알려진 대부분의 공격을 방어할 수 있다. 하드웨어적으로 5,000게이트는 만족하지만 32bit연산을 하던 AES를 8bit로 만들어 암·복호화 시간이 크게 늘어났고, 다른 문제점을 해결하기위해 암·복호화를 두 차례이상 수행하고 있어 AES를 이용하는 대부분의 프로토콜의 경우 초당 100회 통신을 만족하지 못한다.

Peris-Lopez, 최은영, 그리고 제안 프로토콜과 같은 초경량 프로토콜의 경우 AES나 해시와 같이 보안성이 검증된 암호화 알고리즘 보다는 보안성이 떨어지지만 1000게이트 미만으로 설계할 수 있고 초당 100회 통신만족하기 때문에 현실적으로 가장 적합한 인증 프로토콜 중 하나이다.

V. 결 론

RFID 시스템은 무선기술을 이용한 자동인식 기술로 최근 다양한 분야에서 그 사용이 증가되고 있다. RFID 시스템의 사용 증가와 함께 가장 큰 문제로 떠오르고 있는 것은 바로 보안문제이다. 최근 해시, 공개키, 그리고 대칭키 기반의 RFID 인증 프로토콜이 발표되고 있지만 현재 사용하기에는 하드웨어적으로 무리가 따른다. 따라서 최근 가장 관심받고 있는 RFID 인증 프로토콜은 산술연산자와 논리연산자를 이용하여 하드웨어적 부담을 낮추면서도 빠른 속도를 유지하는 초경량 인증 기법이다. 그러므로 보안 문제를 해결하기 위해서는 알고리즘을 경량화 하여야 한다. 하지만 최근 비동기화 공격과 능동 공격 등 여러 가지 방법으로 초경량 인증 기법의 문제점이 밝혀지고 있다.

본 논문에서는 인덱스 처리기법을 개선하여 능동 공격과 비동기화 공격문제를 해결한 초경량 RFID인증 프로토콜을 설계하였다. 서버 측에서 현재는 물론 이전에 사용하던 인덱스와 키를 모두 저장 해 두어 비정상적인 통신 종료와 비동기화 공격에 안전하도록 했다. 태그가 서버에게 인덱스를 보내면 항상 같은 서버 인증 메시지를 전송하던 기존의 문제점을 개선하였다. 그리고 T. Li의 능동공격에 약했던 초경량 프로토콜의 문제점도 해결하였고 일회성 난수를 활용하여 데이터의 값을 가변적으로 생성하여, 위치 추적, 재전송 공격, 스푸핑 공격과 같은 공격에 안전하며 현실적으로 사용 가능한 프로토콜을 제안하였다.

참 고 문 헌

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

[2] 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.

[3] P. Peris-Lopez, J. C. Hermandez-Castro, J. M. Estevez-Tapaidor, A. Ribagorda, "LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags," *Workshop on RFID security 2006(RFIDSec 06)*, pp.137-148, July 2006.

[4] P. Peris-Lopez, J. C. Hermandez-Castro, J. M. Estevez-Tapaidor, A. Ribagorda, "M2AP: A Minmalist Mutual-Authentication Protocol for Low-cost RFID tags," *Proceedings of UIC 2006*, pp.912-923, December 2006.

[5] P. Peris-Lopez, J. C. Hermandez-Castro, J. M. Estevez-Tapaidor, A. Ribagorda, "EMAP: An Efficient Mutual-Authentication Protocol for Low-cost RFID tags," *Proceedings of OTM Federated Conferences and Workshops*: IS Workshop 2006. pp.352-361, January 2006.

[6] S. Kathieyan 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.

[7] P. Golle, M. jakobsson, A. Juels and P. Syverson, "Universal Re-encryption for mixnets," *RSA Conference Cryptographers Track 04*, LNCS 2964, pp.163-178, 2003.

[8] M. Feldhofer, S. Dominikus and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," *Cryptographic Hardware and Embedded Systems*, LNCS 3156, pp.85-140, 2004.

[9] M. Ohkubo, K. Suzuki and S. Kinoshita "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID," *The Soft Computing and Intelligent Systems (SCIS 2004)*, pp.719-724, September 2004.

[10] EPCglobal, "EPCglobal Tag Data Translation (TDT) 1.0 Ratified Standard Specification," pp.1-107, 2006.

[11] T. Li, R. H. Deng. "Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol," *Proceeding of AReS 2007*, April 2007.

[12] T. Li, G. Wang. "Security Analysis of Two Ultra-Lightweight RFID Authentication *Protocols," Proceeding of IFIP SEC 2007*, May 2007.

[13] 권대성, 이주영, 구본욱, "경량 RFID 상호인증 프로토콜 LMAP, M2AP, EMAP에 대한 향상된 취약성 분석", *정보보호학회논문지*, 제17권, 제4호, pp.103-113, 2007

[14] 최은영, 최동희, 임종인, 이동훈, "저가형 RFID

시스템을 위한 효율적인 인증 프로토콜", *정보보호학회논문지*, 제15권, 제5호, 2005

[15] Shannon, C., "Communication Theory of Secrecy Systems." *Bell System Technical Journal*, Vol. 28, pp. 656-715, October 1949.

[16] Jiao-Hongqiang, Tian-Junfeng, Wang-Baomin, "A Study on the One-Time Pad Scheme Based Stern-Brocot Tree," ISCSCT 2008, pp.568-571, 2008.

[17] 오세진, 정경호, 윤태진, 안광선, "일회성 난수를 사용한 RFID 상호인증 프로토콜", *한국통신학회논문지*, 제36권, 제7호, pp.858-867, 20011

이 재 강 (Jaekang Lee) 정회원

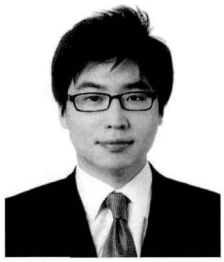
2002년 2월 가야대학교 컴퓨터 공학과 학사

2005년 8월 경북대학교 컴퓨터 공학과 석사

2009년 3월~현재 경북대학교 전자전기컴퓨터학부 박사과정

<관심분야> 임베디드 시스템, RFID, 리눅스 파일시스템

오 세 진 (Sejin Oh) 준회원



2009년 2월 경운대학교 컴퓨터공학과 학사

2011년 2월 경북대학교 전자전기컴퓨터학부 석사

2011년 3월~현재 경북대학교 전자전기컴퓨터학부 박사과정

<관심분야> RFID, 정보보호, 임베디드 시스템

윤 태 진 (Taejin Yun) 정회원

1994년 2월 경북대학교 컴퓨터공학과 학사

1996년 2월 경북대학교 컴퓨터공학과 석사

2012년 2월 경북대학교 컴퓨터공학과 박사

1999년 3월~현재 경운대학교 모바일공학과 교수

<관심분야> RFID, 센서네트워크, 임베디드 시스템, 정보보호

정 경 호 (Kyungho Chung) 정회원

2000년 2월 대구대학교 컴퓨터정보공학과 학사

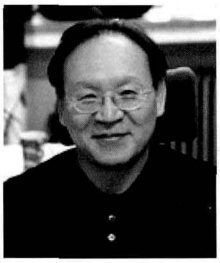
2002년 2월 경북대학교 컴퓨터공학과 석사

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