일회성 난수를 사용한 RFID 상호인증 프로토콜

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

An RFID Mutual Authentication Protocol Using One-Time Random Number

Sejin Oh* *Associate Member*,
Kyungho Chung**, Taejin Yun***, Kwangseon Ahn* *Regular Members*

요 약

RFID(Radio-Frequency IDentification) 시스템은 무선 주파수를 이용하여 메시지를 전송하기 때문에 다양한 보안 문제들을 가지고 있다. 이러한 문제는 도청, 재전송 공격, 위치 추적, 서비스 거부 공격 등이다. 그 중 서비스 거부 공격은 서버 또는 리더에서 ID를 검색하는데 많은 시간과 연산량의 문제점으로 보안에 취약하다. 이를 해결하기 위해서 상호 인증 후 태그의 ID를 검색해야한다. 본 논문에서는 매 세션 생성되는 일회성 난수를 암·복호화 키로 사용하며, 일회성 난수로 상호 인증을 한다. 또한 일회성 난수를 사용하여 RFID 시스템의 다양한 문제점들을 해결하며 특히, 서버에 대한 서비스 거부 공격에 매우 안전하다.

Key Words : RFID, Authentication, Symmetric Key, AES, Protocol

ABSTRACT

The RFID(Radio-Frequency IDentification) systems have many security problem such as eavesdropping, a replay attack, location tracking and DoS(Denial of Service) attacks. Because RFID systems use radio-frequency. So research are being made to solve the problem of RFID systems, one of which is AES algorithm. This paper presents an authentication protocol using AES and one-time random number to secure other attacks like eavesdropping, a replay attack, location tracking, In addtion, RSMAP uses OTP(One-Time Pad) in order to safely transmit.

I. 서 론

RFID(Radio Frequency IDentification) 기술은 유비쿼터스(Ubiquitous) 환경에 이용될 차세대 핵심 기술로 무선 주파수와 자기장 변화를 이용하여 물리적 접촉 없이 아이템을 인식하거나 식별하는 시스템이다. RFID 시스템의 구성 요소는 식별 장비인 태그(Tag)와 태그를 인식하여 저장된 정보를 읽을 수 있는 리더(Reader)로 구성된다. 바코드와 달리 RFID 시스템은 인식시 직접 접근할 필요가 없으며, 태그의 데이터 변경 및 추가가 자유롭고 일시에 다량의 태그 판독이 가능하며, 냉온, 습기, 먼지, 열 등의 열악한 판독 환경에서도 판독율이 높다.

국내에서는 현재, 상거래와 크게 관계가 없는 버스 카드, 출입구 보안 및 출결 카드 등 근접식 RFID 시스템만 주로 활용되고 있으나, 물류 유통 분야로 빠르게 확산되고 있다.

RFID 시스템의 리더는 무선채널을 통하여 태그와

* 경북대학교 전자전기컴퓨터학부 임베디드 시스템 연구실({170m3, gsahn}@knu.ac.kr),
** 경운대학교 컴퓨터공학과(mccart@korea.com), *** 경운대학교 모바일공학과(tjyun@ikw.ac.kr)
논문번호 : KICS2011-04-166, 접수일자 : 2011년 4월 5일, 최종논문접수일자 : 2011년 7월 12일

통신을 하는데, 태그는 리더가 보낸 신호를 듣게 되고 리더의 전송요구에 응답을 한다. 하지만 RFID 시스템에서 태그는 자신의 고유한 식별 정보를 무선 주파수를 통하여 리더에게 전송하기 때문에 도청, 위치 추적, 재전송 공격, 스푸핑 공격 등과 같은 여러 가지 문제점이 발생한다. 이러한 문제를 해결하기 위해서 많은 연구가 활발하게 진행되고 있으며, 물리적 접근 방법과 암호학적 접근 방법으로 분류할 수 있다. 물리적 접근 방법은 Kill 명령어, Faraday Cage 기술, Blocker Tag 및 Active Jamming과 같은 방법이 있으나 태그를 재사용할 수 없는 단점이 존재한다. 그래서 RFID 보안 및 프라이버시 보호 뿐 아니라 태그의 재사용까지 고려하기 위해서는 암호학적 보안 기법과 상호 인증과정으로 해결하여야한다.

암호학적 접근방법은 해시함수나, 공개키 암호, 대칭키 암호를 중심으로 RFID 시스템에 적용하기 위한 많은 연구가 이루어지고 있으며 안전성을 증명하고 있다. 하지만 하드웨어 제약으로 인해 현실적으로 적용하기 어렵다. 최근 M. Feldhofer 등에 의해 수동형 태그에서 구현 가능한 대칭키 기반의 저전력 AES (Advanced Encryption Standard)기법이 제안되어 RFID 시스템의 인증 및 암호 프로토콜로 사용가능함을 입증하였다[1]. 또한 저전력 AES를 이용한 많은 연구들은 고정된 키를 사용하여 암호화하기 때문에 리더와 태그의 값이 노출되는 문제점을 가지고 있다. 또한 인증을 수행하기위해 암·복호화 연산과 인증되지 않은 정보를 서버에서 검색하는 과정은 많은 시간과 연산량으로 서버에 부하를 가지게 된다. 서버의 부하를 가지는 점은 공격자가 서비스 거부 공격이 가능하게 하여 안전성에 큰 위협이 된다. 따라서 본 논문에서는 RFID 시스템에 적용 가능한 대칭키 방식의 안전한 상호 인증 프로토콜을 제안한다. 제안한 프로토콜은 일회성 난수와 AES, One-Time Pad 기법을 활용하여 리더와 태그를 안전하게 상호 인증하며 대칭키의 고정된 키를 사용하는 문제점을 일회성 난수로 해결하여, 도청, 위치 추적, 스푸핑 공격, 재전송 공격 등과 같은 다양한 공격에 대응할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 다양한 암호학적 인증 기법과 문제점에 대해서 기술하고, 3장에서는 본 논문에서 제안한 프로토콜을 기술한다. 4장에서는 기존의 프로토콜과 제안 프로토콜과의 보안성 및 효율성을 비교 분석한다. 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

RFID 기술은 다수의 태그를 동시에 인식 가능하다는 장점 때문에 바코드 시스템을 대체할 기술로 주목받고 있다. 하지만 리더와 태그는 안전하지 않은 무선상에서 통신을 하기 때문에 도청, 위치 추적, 스푸핑 공격, 재전송 공격, 서비스 거부 공격과 같은 위험성을 가지고 있다. 이를 해결하고자 암호학적 연구의 필요성이 제기 되었고 RFID 시스템에 적용하여 다양한 프로토콜이 제시되었다. 본 장에서는 다양한 암호학적 보안 기법에 대해 알아본다.

2.1 해시 기반의 프로토콜

해시 기반의 프로토콜은 Hash-Lock 기법에 의해 해시함수 기반 인증기법 연구가 활성화 되었다. 해시함수의 가장 큰 장점인 전방향 안전성이 우수하여 암호학적 기법의 하나로 많이 사용되고 있다. 또한 해시값이 중복될 수 있다는 근본적인 문제가 있지만 해시값을 충분히 늘려 그 가능성을 낮추는 방법으로 사용하고 있다. 하지만 수동형 RFID 태그에 탑재 가능한 20㎼, 5,000게이트 이내 설계에 적용하기에는 실용적인 문제를 많이 지니고 있는 실정이다. 본 절에서는 기존의 해시 기반의 프로토콜의 장단점을 살펴본다.

2.1.1 HLP

해시 기반의 기법은 가변 길이의 메시지로부터 고정된 길이의 해시 값을 계산하여 메시지가 전송되는 동안 의도되지 않은 변경이 발생하지 않도록 보장한다. 이러한 해시 함수의 전방향성 특징으로 해시 값을 계산하기는 쉬우나 해시 값으로부터 메시지를 찾는 것은 불가능하다. S. A. Weis 등은 HLP(Hash-Lock Protocol) 기법[2]을 제안하였으나 공격자가 metaID를 도청하여 정당한 리더에게 전송시 리더는 공격자에게 정당한 키를 전달하는 문제점이 발생하게 된다. HLP는 metaID, Key, ID값을 보호를 받지 못하여 도청,

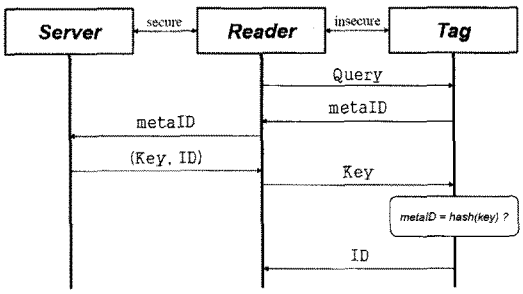


그림 1. HLP(Hash-Lock Protocol)

스푸핑 공격, 재전송 공격에 매우 취약하며, 리더의 Query에 대해 항상 같은 metaID값으로 위치 추적과 서비스 거부 공격에 취약하다[3,4]. 그림 1은 Hash-Lock 프로토콜을 나타낸다.

2.1.2 RHLP

Hash-Lock 기법의 동일한 metaID로 발생하는 문제점을 보안한 RHLP(Randomized Hash-Lock Protocol) 기법[2]은 태그의 난수를 사용하여 태그의 응답을 다르게 하였다. 하지만 재전송 공격, 스푸핑 공격을 할 경우 ID_k값이 노출된다. RHLP의 경우 데이터베이스에서 정당한 태그를 찾기 위해 m개의 태그가 있을 경우 평균 $\lceil m/2 \rceil$번의 해시 연산이 필요하다. 그리고 다수의 태그를 인식해야하는 시스템이라면 RFID 시스템에 많은 부하를 가지게 된다[5]. 그림 2는 RHLP기법이며 HLP에서 발생했던 문제점을 해결하고자 제안된 방식이다.

RHLP의 경우 태그의 난수 R, 리더가 태그에게 전송하는 ID_k가 노출되어 있어 도청 공격에 취약하다. 또한 태그가 리더에게 전송하는 $R,h(ID_k \| R)$를 도청하여 스푸핑 공격, 재전송 공격을 하면 정당한 ID_k를 획득하며 연속적인 전송으로 서비스 거부 공격이 가능하다[3,4,5].

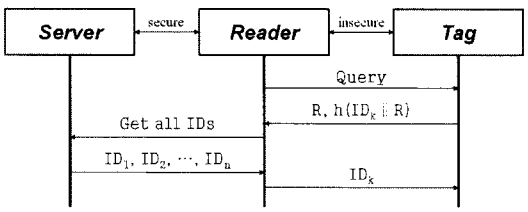


그림 2. RHLP(Randomized Hash-Lock Protocol)

2.1.3 CRAP

K. Rhee 등이 제안한 시도-응답형 인증 프로토콜인 CRAP(Challenge-Response 기반 인증 프로토콜)[6]는 메모리 사용과 태그의 계산량 측면에서는 효율적인 방법이다. 또한 해시 함수의 입력에 난수 r_R와 r_T를 각각 포함시키고 있기 때문에 가변적인 값으로 위치 추적에 안전하다. 그러나 서버에서는 태그의 인증을 위해 모든 태그 ID를 검색해야하므로 m개의 태그가 있다면 평균 $\lceil m/2 \rceil$+1번의 해시 연산이 필요하며 태그가 많은 환경에서는 서버에 부하가 많아지게 된다[5]. 그림 3은 K. Rhee 등이 제안한 CRAP이다.

CRAP는 해시함수의 큰 장점인 전방향 안전성을 이용하여 도청 공격을 방어하며, 리더의 난수 r_R, 태그

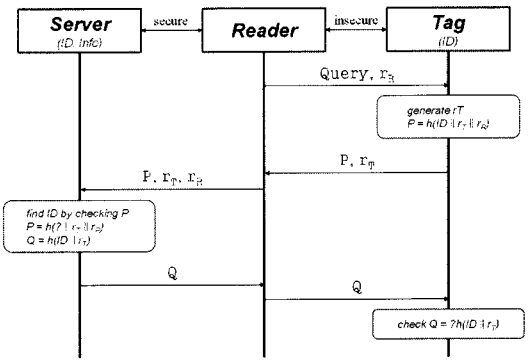


그림 3. CRAP(Challenge-Response 기반 인증 프로토콜)

의 난수 r_T를 이용하여 상호 인증 절차를 거치기 때문에 스푸핑 공격, 재전송 공격, 위치 추적에 안전하다. 하지만 태그가 리더에게 전송하는 P, r_T를 획득하여 리더에게 무차별 전송을 시도할 경우 서버에 많은 부하를 주어 서비스 거부 공격을 받을 수 있다[5,7].

2.1.4 HCP

Ohkubo 등은 위치 추적에 안전하며 전방향 안전성도 보장되는 HCP(Hash-Chain Protocol)[8]을 제안하였다. Hash-Chain 프로토콜은 두 개의 H와 G 해시함수를 바탕으로 구성되어 있다. 리더의 Query를 받은 태그는 $A_i=G(S_i)$를 수행하여 리더에게 전달하고 $S_{i+1}=H(S_i)$로 갱신한다. 리더에 대한 태그의 응답은 매번 다른 응답을 하므로 위치추적에 안전하다. 하지만 태그로부터 온 $A_i=G(S_i)$값에 해당하는 ID를 검색하기 위해서는 최악의 경우, 서버가 보유한 모든 S_i에 대해서 H와 G를 i번 수행해야 한다. 이는 서버에 많은 부하를 주게 되며, 공격자에 의해 서비스 거부 공격을 당할 수 있다.

그림 4.는 Ohkubo 등이 제안한 Hash-Chain 프로

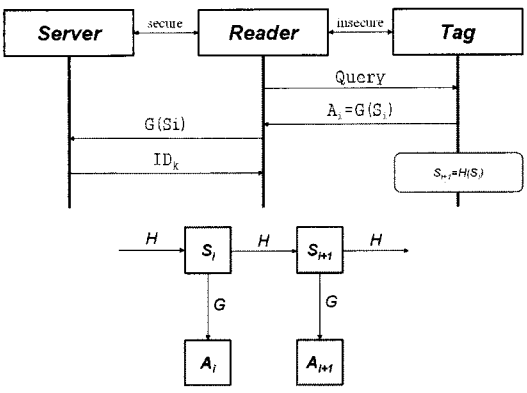


그림 4. HCP(Hash-Chain Protocol)

토콜이다.

HCP의 경우 CRAP와 같이 도청 공격에 안전하며, H와 G 두 개의 해시함수를 이용해서 위치추적과 재전송 공격에 안전하다. 하지만 태그가 리더에게 $A_i=G(S_i)$를 전송 후 S_i값이 $S_{i+1}=H(S_i)$로 변경되므로 부정당한 리더가 정당한 태그에게 Query를 보내게 되면 S_i값이 변경되어 비동기화 문제를 일으켜 서비스 거부 공격을 당하게 된다. 또한 하드웨어 자원 제약이 있는 태그에 두 개의 해시 함수를 사용해야하는 부담은 상당히 크다. SHA 계열의 해시함수를 하드웨어로 구현하면 20,000~25,000게이트 이상이 소요된다. 따라서 5,000게이트 미만으로 구현해야하는 수동형 태그에는 적합하지 않으며 태그의 5센트 이하 가격은 현실적으로 불가능하다.

2.2 대칭키 기반의 인증 프로토콜

벨기에의 수학자 존 데이먼과 빈센트 라이먼에 의해서 만들어진 Rijndael 알고리즘을 바탕으로 2000년 미국 정부 표준으로 AES(Advanced Encryption Standard)가 개발되었다[9,10]. 이를 바탕으로 M. Feldhofer 등은 RFID 태그에 적용이 가능한 크기를 5,000게이트 미만으로 예측하고 3,595게이트 크기의 8bit로 동작하도록 설계하였으며[11], Mark Jung, 구본석 등에 의해 4,000게이트 미만의 AES 연산기를 구현하여 AES가 수동형 RFID 태그에 적합함을 입증하였다[12].

2.2.1 MSAP

M. Feldhofer는 난수를 사용하여 태그를 인증하는 MSAP(M. Feldhofer의 AES를 이용한 인증 프로토콜)을 제안하였다[11]. 그러나 그림 5와 같이 Challenge-Response의 노출된 난수 값과 고정된 키를 사용하여 암호화하기 때문에 정보가 노출되는 점과 키가 노출될 수 있으며, R_A에 대한 $E_K(R_A)$는 항상 같으므로 위치 추적의 문제점이 있다. 또한 이를 이용하여 스푸핑 공격과 중간자 공격이 가능하다. 그림 5.는 M. Feldhofer의 AES를 이용한 RFID 인증 프로토콜이다.

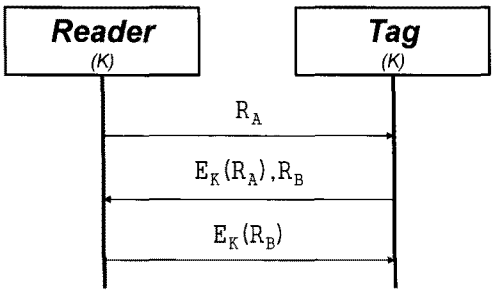


그림 5. MSAP

M. Feldhofer는 리더와 태그의 난수를 AES로 암호화하여 도청공격에 안전하며, 암호화 된 난수를 이용하여 상호 인증을 거치기 때문에 재전송 공격, 서비스 거부 공격에 안전하다. 하지만 정당한 리더로 가장하여 태그에게 난수를 연속적으로 보내게 되면, 난수를 암호화 한 고정된 값을 회신하기 때문에 위치추적과 스푸핑 공격이 가능하다.

2.2.2 TAMAP

Toiruul이 제안한 TAMAP(Toiruul의 프로토콜)[13]의 인증 과정은 그림 6과 같다.

서버는 태그와 비밀 공유키 K_1과 K_2를 XOR 연산하여 AES로 암호화한 $E_K(K_1 \oplus K_2)$값을 리더를 거쳐 태그에게 전송한다. 태그는 자신이 생성한 $E^*_K(K_1 \oplus K_2)$과 비교하여 인증과정을 거친다. 다를 경우 통신은 종료되고 같을 경우 태그는 서버를 인증하고 ID_K값을 포함한 $E_K(K_1 \oplus K_2 \oplus ID_K)$를 리더를 거쳐 서버에게 전송한다. 대칭키의 고정된 키를 사용하는 문제점을 해결하고자 태그의 ID_K를 전송한 후 일정한 방식으로 키를 업데이트한다. 하지만 일정한 방식으로 키 업데이트를 함으로써 위치 추적에 노출될 수 있고, 서버가 태그를 인증하는 과정은 완전하지 않기 때문에 보안에 취약하다.

TAMAP은 AES를 이용하여 데이터를 안전하게 보호하며 매 세션마다 변하는 K_1, K_2로 상호인증을 하며 위치 추적, 스푸핑 공격, 재전송 공격에 안전하다고 주장한다. 하지만 태그가 전송하는 $E_K(K_1 \oplus K_2 \oplus ID_K)$가 서버에게 정상적으로 전송되지 못하게 방해한다면 서비스 거부 공격을 일으킬 수 있다[14]. 또한 고정된 K를 사용하는 점은 시스템 전체에 공격을 받

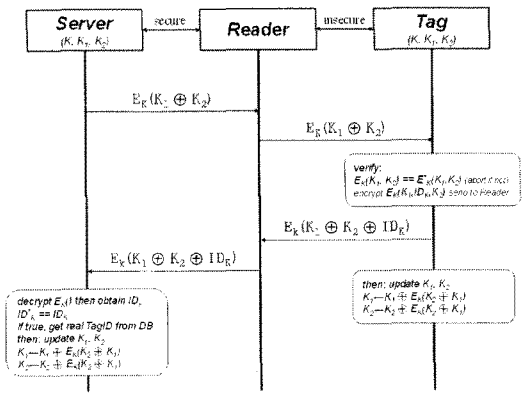


그림 6. TAMAP(Toiruul의 프로토콜)

을 수 있다.

2.2.3 LSAP

그림 7은 이남기 등의 AES 암호 프로세서를 이용한 강인한 RFID 인증 프로토콜인 LSAP(이남기의 Strong Authentication 프로토콜)이다[15].

RFID 시스템의 각 객체들은 난수를 활용하며 재전송 공격을 방지하기 위하여 서버와 태그의 CD (Change Data)를 변경하는 기법을 제안하였다. 태그는 리더가 전송한 RN을 받아 리더에게 E_k(ID, CD, $RN_{from\ Tag}$)을 전송한다. 리더는 E_k(ID, CD, $RN_{from\ Tag}$)을 자신이 가지고 있는 K를 이용하여 복호화하여 자신이 보낸 RN과 태그에게서 온 $RN_{from\ Tag}$를 비교하여 태그를 인증한다. 그러나 제안한 프로토콜 어디에도 태그가 리더를 인증하는 과정이 없다. 태그입장에서 리더에 대한 신뢰가 없는 CID, RN'을 받아 CD 값을 업데이트한다. 또한 고정된 키 사용과 리더와 태그사이의 노출된 정보는 태그의 고유정보 노출, 중간자 공격이 가능하다.

LSAP은 AES를 이용하여 도청 공격을 방어하고 상호 인증을 통하여 스푸핑 공격, 재전송 공격, 서비스 거부 공격을 방어한다. 그러나 리더가 Query와 함께 전송되는 리더의 난수 RN에 대한 태그의 응답 값은 고정된 값으로 위치 추적을 피할 수 없으며, 고정된 K를 사용하는 문제점을 지니고 있다.

이와 같이 저 전력 AES를 이용한 기존의 RFID 인증 프로토콜에서 항상 고정된 키를 이용하여 암호화하였고, 태그와 리더사이의 안전하지 않은 무선채널에서 공격자에 의해 키 값 노출, 재전송 공격, 위치 추적, 서비스 거부 공격과 같은 다양한 문제점을 가지고 있다.

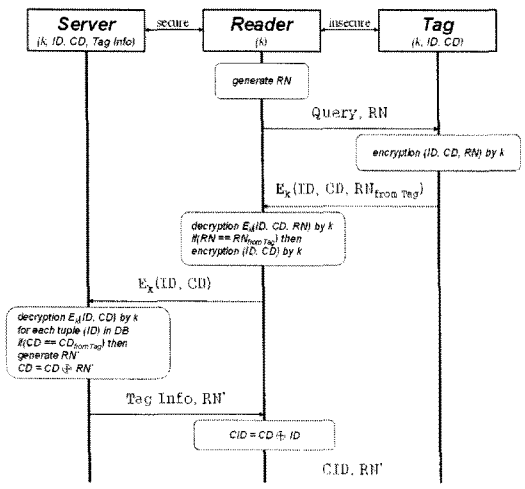


그림 7. LSAP(이남기의 Strong Authentication Protocol)

2.3 OTP(One-Time Pad)

OTP(One-Time Pad)는 1917년 미국 AT&T사의 Gilbert S. Vernam이 처음 제안했으며[16], Claude Shannon이 OTP가 완벽한 안전성을 가지고 있음을 검증하였다[17,18]. OTP의 평문(m), 비밀키(k), 암호문(c)을 수식으로 나타내면 다음과 같다.

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

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

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

OTP는 아주 쉬운 XOR 연산을 이용하여 암호화와 복호화를 간단하게 할 수 있다. OTP를 사용하기위한 조건은 비밀키는 랜덤하게 생성하여야 한다. 그리고 한번 사용한 비밀키는 다시 사용하지 않아야하며, 평문과 비밀키의 길이가 동일해야하는 특징을 지니고 있다.

Ⅲ. 제안 프로토콜

본 장에서는 RFID 시스템의 다양한 공격에 안전하고 수동형 RFID태그에 적합한 상호 인증 프로토콜 RSMAP을 제안한다. RSMAP(Randomized Symmetric Mutual Authentication Protocol)은 OTP(One-Time Pad)와 저전력 AES를 이용하여 무선 채널 상에 전송되는 데이터를 암호화하여 안전성을 높이고, 리더와 태그가 생성한 일회성 난수를 상호 인증에 사용되어진다. 제안 프로토콜은 가정사항 및 표기법, 제안프로토콜로 구성되며, RSMAP은 태그 인증 단계, 리더 인증 단계 및 태그의 정보 획득으로 구성된다.

3.1 가정 사항 및 표기법

본 논문의 RFID 시스템은 다음과 같은 가정 하에서 동작하며, 표 1은 표기법을 나타낸 것이다.

1) 서버와 리더 사이는 안전한 통신 채널을 이용함으로써 공격자의 공격에 안전하다.
2) 리더와 태그 사이는 무선 상의 통신 채널이므로 공격자의 공격에 취약하다.
3) 리더와 태그는 대칭키 기반의 AES, One-Time Pad 연산이 가능하며, 리더는 태그와 다르게 AES 복호화 연산이 가능하다.
4) 리더와 태그 모두 난수를 생성할 수 있다.

표 1. 표기법

용 어	내 용
ID	태그의 고유 식별 값
Mask	리더의 난수를 숨기기 위한 마스크 값
HRN	Hidden Random Number
Rr	리더가 매 세션 생성한 난수
Rt	태그가 매 세션 생성한 난수
‖	연접 연산자
⊕	eXclusive-OR (XOR) 연산
E( )	블록 암호문

5) 리더와 태그가 생성한 난수는 처음 세션이 연결될 때 마다 새로이 생성된다.
6) 리더와 태그는 사전에 난수를 숨기기 위한 동일한 마스크 값(Mask)를 안전하게 가지고 있다.
7) 리더와 태그의 난수 bit수는 마스크 값의 bit수와 동일하다.
8) 모든 태그에는 고유정보 ID를 가지고 있다.
9) 태그는 리더로부터 전원을 공급받는 수동형 태그로 가정한다.

3.2 RSMAP

본 논문에서 제안한 프로토콜은 OTP기법과 AES를 이용하여 리더와 태그가 생성한 일회성 난수를 안전하게 전달하여 리더와 태그간의 상호 인증을 수행한다. 서버를 활용한 기존의 인증 방법과 다르게 인증 과정에서 서버를 통하지 않고 수행하므로 서버의 부하가 적다. 기존의 여러 프로토콜에서 나타난 서버에 대한 부하로 서비스 거부 공격에 대한 취약점을 볼 수 있다. 또한 리더와 태그의 출력 값은 각각 내장된 난수 생성기를 이용하여 매 세션마다 항상 변하며 리더의 난수를 숨기기 위한 Mask값은 상호인증 후 다른 값으로 변하게 되어있다. 그리고 메시지 전달과정에서 OTP, AES 암호화 기법을 사용하므로 안전성을 보장한다. 그림 8은 제안 프로토콜 RSMAP의 전체 흐름을 보여주고 있다.

3.3 인증 과정

제안 프로토콜의 인증 과정은 3단계로, 태그 인증 단계, 리더 인증 단계, 태그의 정보 획득으로 구성되어 있다.

3.3.1 태그 인증 단계

그림 9는 본 논문의 제안 프로토콜인 RSMAP의 태그 인증 과정을 세부 과정으로 나타낸 것이다.

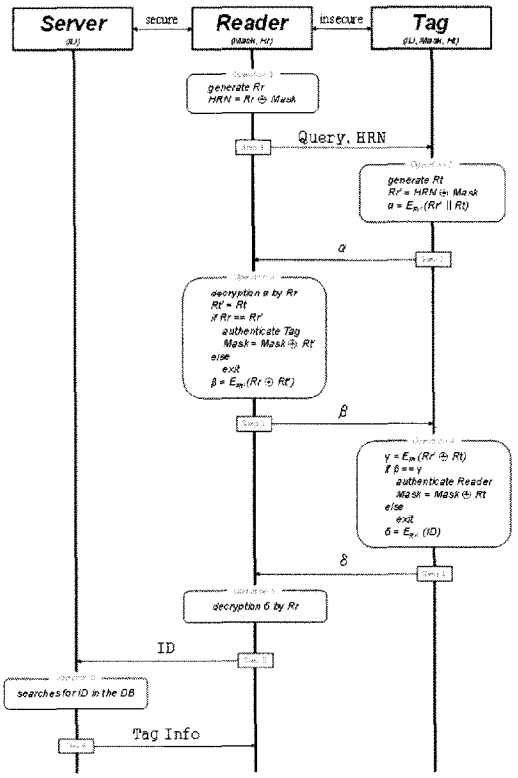


그림 8. RSMAP

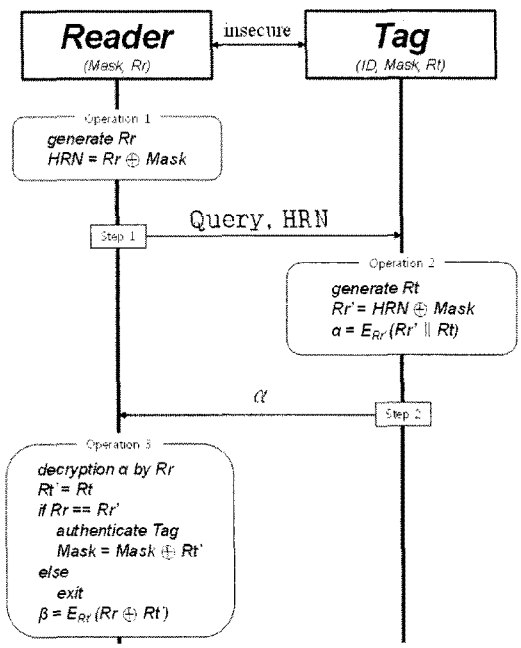


그림 9. 태그 인증

1) Operation 1.
초기 질의 단계에서 리더는 리더의 난수 Rr를 생성

한다. 그리고 Rr를 Mask와 OTP 암호화(XOR) 연산을 하여 HRN을 생성한다.

리더가 생성한 HRN을 Step 1과 같이 태그에게 Query와 함께 전송한다.

2) Operation 2.

태그는 리더로부터 받은 HRN과 Mask를 OTP 복호화(XOR) 연산을 통하여 Rr'을 획득한다. 그리고 태그는 Rr'과 태그 자신이 생성한 난수 Rt를 연접하여 Rr'을 키로 사용하여 AES로 암호화 한다. $E_{Rr'}$(Rr' ‖ Rt)한 α를 Step 2와 같이 리더에게 전송한다.

3) Operation 3.

α를 받은 리더는 Operation 1에서 생성한 Rr를 키로 사용하여 복호화한다. 이때 리더가 생성한 Rr과 복호화 하여 얻은 Rr'을 비교하여 같으면 태그를 인증한다. 그리고 리더의 Mask 값을 갱신한다. 만약 인증에 실패할 경우 세션은 종료된다.

3.3.2 리더 인증 단계

그림 10은 리더 인증 과정을 세부적으로 나타낸 것이다.

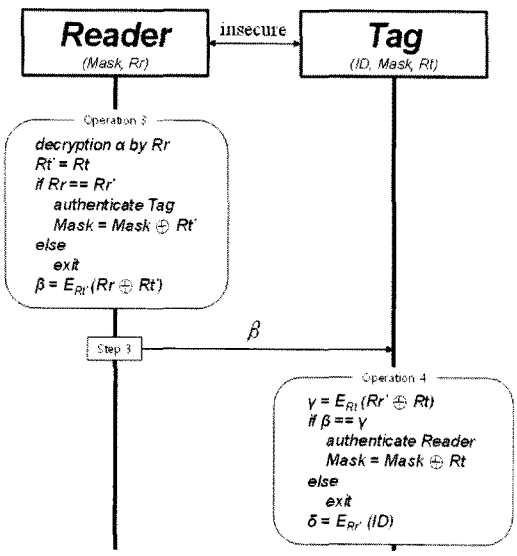


그림 10. 리더 인증

1) Operation 3.

Operation 3에서 리더가 태그를 인증하였을 경우, 리더는 Rr과 Rt'을 XOR 연산을 수행하고, Rt'을 키로 사용하여 AES로 $E_{Rt'}$(Rr⊕Rt')한 β를 Step 3와 같이 태그에게 전송한다.

2) Operation 4.

β를 받은 태그는 Operation 2에서 얻은 Rr'과 태그가 생성한 난수 Rt를 XOR 연산하여 Rt를 키로 사용하여 암호화한 γ를 생성한다. 이때 β와 γ를 비교하여 같으면 리더를 인증한다. 그리고 Mask 값을 갱신한다. 만약 β와 γ의 값이 다를 경우 리더 인증이 실패하며 세션은 종료된다.

3.3.3 태그의 정보 획득 단계

그림 11은 태그의 정보 획득 과정을 세부적으로 나타낸 것이다.

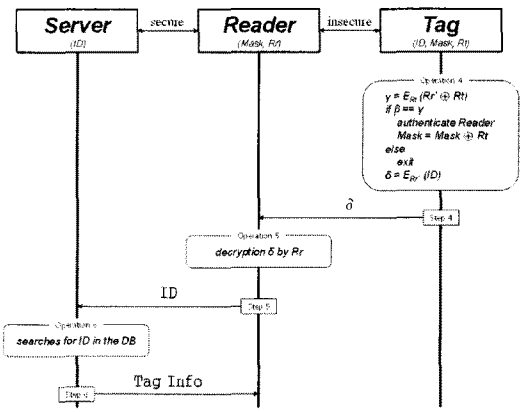


그림 11. 태그의 정보 획득

1) Operation 4.

Operation 4에서 태그가 리더를 인증하였으면 상호인증이 완료되어 리더와 태그 서로가 신뢰할 수 있는 상태가 된다. 정당한 상호 인증이 수행되면 태그는 Operation 1에서 획득한 Rr'을 키로 태그 ID를 암호화한 δ=$E_{Rr'}$(ID)를 Step 4와 같이 리더에게 전송한다.

2) Operation 5.

태그로부터 전송받은 δ를 리더의 난수 Rr를 키로 사용하여 복호하여 태그의 고유 식별 정보 ID를 Step 4와 같이 서버에게 전달한다.

3) Operation 6.

서버는 리더로부터 받은 태그의 고유 식별 정보 ID를 데이터베이스에서 검색하여 얻은 결과 값 Tag Info를 Step 6와 같이 리더에게 전송하므로써 완료된다.

Ⅳ. 비교 분석

본 장에서는 기존 프로토콜과 제안 프로토콜인 RSMAP의 보안성 및 효율성을 비교분석한다.

4.1 RSMAP의 보안성 분석

제안 프로토콜인 RSMAP이 RFID의 공격유형 중 도청 공격, 위치 추적, 스푸핑 공격, 재전송 공격, 서비스 거부 공격에 대한 보안성을 분석한다.

4.1.1 도청 공격(Eavesdropping)

리더와 태그간의 데이터 전송은 무선 채널 상에서의 데이터 전송으로 공격자에게 도청 공격을 받을 수 있다. 하지만 제안 프로토콜의 경우 OTP와 AES를 이용한 암호화 된 데이터이므로 도청 공격을 하여 데이터를 획득하더라도 알 수 없는 값이기 때문에 도청 공격에 안전하다. 설령 도청 공격으로 데이터를 획득하여 복호화 하더라도 의미 없는 난수이다.

4.1.2 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 태그의 난수 Rt를 매 세션 새로이 생성하여 α값을 리더에게 전송하므로 위치추적을 피할 수 있다.

4.1.3 스푸핑 공격(Spoofing Attack)

리더와 태그사이에 전송되는 데이터를 도청하여 승인받은 사용자 또는 승인받은 리더로 가장하더라도 매 세션 생성되는 리더의 난수 Rr과 태그의 난수 Rt를 사용한 상호 인증 절차에서 실패하게 되므로 스푸핑 공격에 안전하다.

4.1.4 재전송 공격(Replay Attack)

재전송 공격은 리더와 태그사이에서 도청 공격으로 데이터를 얻는다. 이후 정당한 리더의 요청에 도청한 데이터를 재전송하여 스푸핑 공격, 서비스 거부 공격으로 이어질 수 있으므로 매우 위험하다. 하지만 이와 같은 경우에도 리더와 태그가 매 세션 생성한 일회성 난수를 사용하는 상호 인증 과정을 통과할 수 없다.

4.1.5 서비스 거부 공격(DoS Attack)

최근 서비스 거부 공격(Denial of Service Attack)으로 인한 피해로 그 심각성은 매우 크게 인식되어 많은 보안이 요구되는 가운데, RFID 시스템의 많은 시간과 연산량이 요구되는 서버 또는 리더에 부하로 인하여 시스템 전체에 많은 영향을 끼친다. 본 논문은 리더와 태그의 상호 인증 단계를 거쳐야 서버에 접근하여 태그 ID를 데이터베이스에서 검색을 하기 때문에 리더와 태그뿐만 아니라 서버에 대한 서비스 거부 공격에 강한 안전성을 보장한다.

4.2 기존 프로토콜과의 비교 분석

비교 대상의 프로토콜은 해시 계열의 HLP, RHLP, CRAP, HCP과 AES 계열의 MSAP, TAMAP, LSAP을 대상으로 한다.

표 2는 기존 프로토콜과 제안 프로토콜인 RSMAP을 도청 공격, 위치추적, 스푸핑 공격, 재전송 공격, 서비스 거부 공격 5가지 측면에서 안전성을 비교한 내용이다.

해시 함수를 이용한 프로토콜의 경우 8,000~10,000게이트를 필요로하며 HCP의 경우 20,000~25,000게이트이다. HCP는 현재 우수한 프로토콜 중 하나이지만 수동형 태그에 적용하기는 현실적으로 불가능하며, 태그의 숫자 증가와 함께 서버 부하도 비례하여 늘어난다는 단점을 지니고 있다.

M. Feldhofer의 논문은 RFID 태그에서 AES를 사용 가능성을 제시하였다. AES를 적용시 3,500게이트로 태그를 구현 가능하여 현실적으로 적합함을 제안하였고, 이후 AES를 이용한 다양한 프로토콜이 연구되었다. TAMAP의 경우 상호 인증을 수행하여 다양한 공격에 안전하지만 키에 대한 비동기화 공격으로 서비스 거부 공격에 취약하다. 또한 LSAP의 경우 고정된 값으로 인하여 위치 추적에 안전하지 못하다.

본 논문에서 제안한 RSMAP의 경우 AES기반의 프로토콜에 비해 태그의 암호화 연산이 많은 단점이

표 2. 기존 프로토콜과 RSMAP의 비교 분석

	도청	위치 추적	스푸핑 공격	재전송 공격	DoS 공격	상호 인증	효율성	서버 연산량
HLP	×	×	×	×	×	×	×	m번
RHLP	×	○	×	×	×	×	×	m번
CRAP	○	○	○	○	×	○	×	m번
HCP	○	○	×	○	×	×	×	m번
MSAP	○	×	×	○	○	○	○	-
TAMAP	○	○	○	○	×	○	△	m번
LSAP	○	×	○	○	○	○	○	m-n번
RSMAP	○	○	○	○	○	○	△	m-n번

범례: m : 리더가 인식할 수 있는 범위의 태그 수
n : 불법태그 수
○ : 만족, × : 불만족, - : 해당사항 없음

있지만 일회성 난수를 AES 암·복호화 키와 상호 인증에 사용하므로써 대칭키 기반의 근본적인 키 문제점을 해결하였고 안전성에 초점을 두어 프로토콜을 설계하였다.

V. 결 론

RFID 시스템의 리더와 태그사이는 무선 주파수를 사용하기 때문에 다양한 위험성을 가지고 있다. RFID의 보안 연구와 관련하여 해시함수나 공개키 기반의 암호학적 접근방법의 경우 안전성을 해결하지만 현실적으로 적용하기 어려운 부분이 있다.

대칭키 기반의 AES 기법은 M. Feldhofer 등에 의해서 태그에 구현 가능한 저전력 AES 기법을 제안하여 자원 제약이 심한 수동형 태그에 적합함이 입증되었다. 그러나 대칭키 암호화의 근본적인 문제점인 항상 고정된 키를 이용하여 암호화함으로써 키 노출 시 모든 시스템이 공격되는 결정적인 단점이 있다.

본 논문에서는 RFID 시스템에 적용 가능한 저전력 AES를 이용하여 효율적인 상호 인증 프로토콜인 RSMAP(Randomized Symmetric Mutual Authentication Protocol)을 설계하였다. RSMAP은 리더와 태그간의 교환되는 메시지를 보호하기 위해 매 세션 생성되는 일회성 난수와 One-Time Pad기법을 적극 활용하였으며 대칭키 기반의 RFID 인증 프로토콜에서 항상 고정된 키를 사용하여 키 값이 노출되는 문제를 일회성 난수를 키로 사용하여 해결하였다. 또한 일회성 난수를 키와 메시지로 사용하여 가변적 응답 값으로 위치 추적과 같은 공격을 방어하였다. 만약 공격자에 의해 복호화 되더라도 의미 없는 난수 값이며 키 또한 일회성 키이므로 도청, 재전송 공격, 스푸핑 공격 등에 안전하다. 특히 리더와 태그 간의 상호 인증을 통해 서비스 거부 공격에 대응하며, 상호 인증 후 서버에 태그의 고유 식별 정보(ID)를 전달하는 과정은 서버에 부하를 최소화하고 서버에 대한 서비스 거부 공격에 매우 안전하다.

참 고 문 헌

[1] CHES2009, "Workshop on Cryptographic Hardware and Embedded systems", *http://www.ches workshop.org/*, 2009.

[2] S. Weis, S. Sarma, R. Rivest, "Security and Privacy Aspects of Low-cost Radio Frequency Identification System", *Security and Pervasive Computing 2003*, LNCS 2802, pp.201-212

[3] 김대중, 전문석, "일회성 난수를 이용한 안전한 RFID 상호인증 프로토콜 설계", *정보과학회논문지*, 제35권, 제3호, pp.243-250, 2008. 06.

[4] 정장영, 홍영식, "Serverless 환경에서 RFID 인증프로토콜 검증", *2008 한국컴퓨터종합학술대회 논문집*, Vol.35, No.1(A), pp.77-87, 2008. 06.

[5] 하재철, 박제훈, 하정훈, 김환구, 문상재, "검색 정보 사전 동기화를 이용한 저비용 RFID 인증 방식", *정보보호학회 논문지*, 제18권, 제1호, pp.77-87, 2008. 02.

[6] K. Rhee, J. Kwak, S. Kim and D. Won, "Challenge-Response Based on RFID Authentication Protocol for Distributed Database Environment", *SPC'05*, LNCS 3450, pp.70-84, springer-Verlag, 2005.

[7] 김진호, 서재우, 이필중, "저비용 RFID 시스템에 적합한 효율적인 인증 방법", *정보보호학회논문지*, 제18권, 제2호, pp.117-128, 2008. 04.

[8] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID", *Proceeding of the SCIS 2004*, pp.719-724, 2004.

[9] J. Daemen, V. Rijmen, "The Design of Rijndael," AES-The Advanced Encryption Standard, *Springer-Verlog*, Berlin, Heidelberg, New York, 2002.

[10] J. Daemen, V. Rijmen, "AES Proposal; Rijndael, Version2," *Submission to NIST*, March 1999.

[11] M. Feldhofer, S. Dominikus, Rijmen, J. Wolkerstorfer, "Strong Authentication for RFID Systems Using The AES Algorithm", *ICCHES*, pp.357-370, 2004.

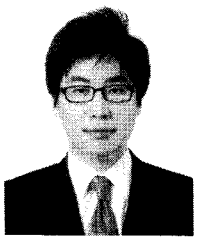
[12] 구본석, 유권호, 양상운, 장태주, 이상진, "RFID 태그를 위한 초소형 AES 연산기의 구현", *정보보호학회논문지*, 제16권, 제5호, pp.67-77, 2006. 10.

[13] B. Toiruul, K. Lee, "An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems," *IJCSNS*, Sep. 2006.

[14] S. Ji, "RFID-enabled Extensible Authentication Framework and Its Applications", A thesis for the Degree of Master, *ICU*, 2008.

[15] 이남기, 장태민, 전병찬, 전진오, 유수봉, 강민섭, "AES 암호 프로세서를 이용한 강인한 RFID 인증 프로토콜 설계", *한국정보처리학회 논문집*, 제15권, 제2호, pp.1473-1476, 2008. 11.
[16] Gilbert S. Vernam. U.S.Patent 1,310,719. Secret signaling system, 22 July 1919.
[17] Shannon, C., "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, Vol. 28, pp.656-715, Oct 1949.
[18] Jiao-Hongqiang, Tian-Junfeng, Wang-Baomin, "A Study on the One-Time Pad Scheme Based Stern-Brocot Tree", *ISCSCT 2008*, pp.568-571, 2008.

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 리눅스 시스템

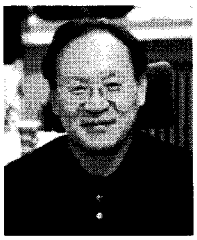
정 경 호 (Kyungho Chung) 정회원

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

윤 태 진 (Taejin Yun) 정회원

1994년 2월 경북대학교 컴퓨터공학과 학사
1996년 2월 경북대학교 컴퓨터공학과 석사
1998년 2월 경북대학교 컴퓨터공학과 박사수료
1999년 3월~현재 경운대학교 모바일공학과 교수
<관심분야> 정보보안, 센서네트워크, 임베디드시스템

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