개선된 해시함수와 CRC 코드 기반의 RFID 상호인증 프로토콜

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

Improved a Mutual Authentication Protocol in RFID based on Hash Function and CRC Code

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

요 약

2011년 배우식 등은 해시함수 기반의 새로운 저비용 RFID 상호인증 프로토콜(NLMAP)을 제안하였다. 그들은 난수 발생 등 연산량을 최소화하며, 상호인증으로 재전송 공격, 스푸핑 공격, 트래픽 공격, 도청 공격 등에 안전하기 때문에 RFID 시스템에 적용 시 제작비의 절감 및 보안성이 우수한 장점이 있다고 주장하였다. 그러나 그들의 주장과는 달리 도청 공격으로 해시된 태그의 고유 식별 정보 H(IDt)를 획득할 수 있다. 그리고 공격자가 획득한 H(IDt)를 이용하여 위치추적과 스푸핑 공격이 가능함을 본 논문에서 증명한다. 더 나아가 해시함수와 CRC코드를 이용한 상호인증 프로토콜을 제안한다. 그리고 제안 프로토콜이 NLMAP보다 다양한 공격에 안전하고 연산량 측면에서 효율적임을 증명한다.

Key Words : RFID, Authentication, Protocol, Hash, CRC

ABSTRACT

In 2011, Woosik Bae proposed a NLMAP(New Low-cost Mutual Authentication Protocol) in RFID based on hash function. They argued that minimize computation such as random number generation. In addition, NLMAP is safe against replay attack, spoofing attack, traffic analysis and eavesdropping attack due to using mutual authentication. So, when applied to RFID system has advantage such as providing a high level of security at a lower manufacturing cost. However, unlike their argue, attacker can obtain Tag's hash computed unique identification information. This paper proves possible the location tracking and spoofing attack using H(IDt) by attacker. In addition, we propose the improved a mutual authentication protocol in RFID based on hash function and CRC code. Also, our protocol is secure against various attacks and suitable for efficient RFID systems better than NLMAP.

Ⅰ. 서 론

RFID(Radio Frequency Identification)는 무선을 이용하여 다양한 개체의 정보를 관리하는 바코드 대체 기술로 교통, 물류, 국방, 축산 등 다양한 분야에 걸쳐 활용된다. RFID 시스템은 개체의 정보를

* 경북대학교 전자전기컴퓨터학부 임베디드 시스템 연구실({170m3, 10004oke, gsahn}@knu.ac.kr),
** 경운대학교 모바일공학과(tjyun@ikw.ac.kr), *** 계명문화대학 컴퓨터학부(chlee2k@live.co.kr),
**** 경운대학교 컴퓨터공학과(mccart@ikw.ac.kr)
논문번호 : KICS2011-10-459, 접수일자 : 2011년 10월 2일, 최종논문접수일자 : 2012년 2월 3일

담고 있는 태그(Tag)와 태그의 정보를 읽어 오는 리더(Reader), 태그 정보를 관리하는 서버(Server)로 구성되어 진다[1-3]. RFID는 바코드 대체 기술로 바코드에 비해 많은 데이터 처리, 빠른 인식 속도로 각광 받고 있지만, 무선 주파수를 이용하기 때문에 보안에 취약하다[4]. 이를 해결하고자 AES, 해시함수와 같은 암호학적 알고리즘과 상호인증 기법에 관한 연구가 활발히 진행되고 있다[5-7]. 2011년 배우식 등은 해시함수를 이용한 상호인증 프로토콜을 제안하였고, 태그의 정보를 해시한 값 H(Idt)와 리더의 난수 Rr, 서버의 난수 Rdbt를 이용하기 때문에 다양한 공격에 안전하다고 주장하였다[8]. 그러나 그들의 주장과는 다르게 위치추적, 스푸핑 공격에 취약하며, 도청 공격으로 인한 해시된 태그의 정보의 노출로 공격자가 상호인증과정을 통과하는 문제점이 발생하게 된다.

본 논문에서는 배우식 등이 제안한 프로토콜을 분석하고, 문제점을 기술한다. 그리고 이를 바탕으로 개선된 프로토콜을 제안하고 보안성, 효율성 측면에서 배우식 등의 NLMAP 프로토콜과 비교분석 한다.

Ⅱ. NLMAP

본 장에서는 2011년 배우식 등이 제안한 NLMAP(A New Low-Cost Mutual Authentication Protocol)를 알아본다. 그림 1은 배우식 등이 제안한 NLMAP을 나타낸 것이다.

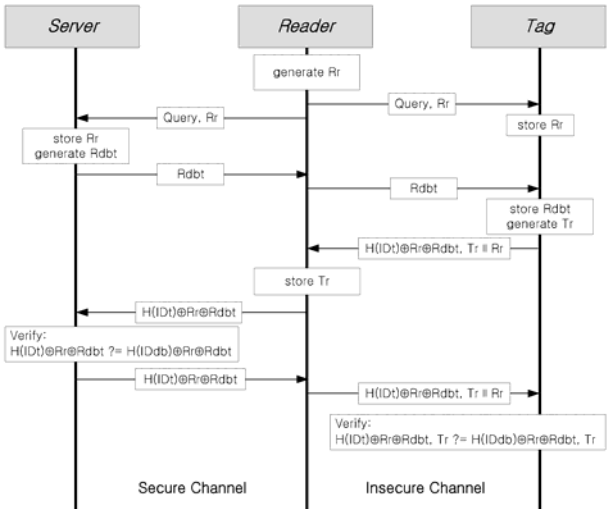

그림 1. 배우식 등이 제안한 NLMAP 프로토콜
Fig. 1. Woosik Bae's The NLMAP Protocol

2.1. NLMAP 프로토콜의 상호인증 과정

NLMAP 프로토콜은 그림 1과 같이 총 8단계로 이루어진다.

◎ 단계 ①, ② : 리더는 난수 Rr을 생성하여, Query와 함께 태그와 서버에게 전송한다.

◎ 단계 ③ : 리더난수 Rr을 받은 서버는 Rr을 저장한다. 그리고 서버의 난수 Rdbt를 생성하여, 리더에게 전송한다.

◎ 단계 ④ : 서버의 난수 Rdbt를 받은 리더는 태그에게 Rdbt를 전송한다.

◎ 단계 ⑤ : 리더로부터 서버의 난수 Rdbt를 받은 태그는 태그의 고유 식별 정보(IDt)를 해시 연산한다. 그리고 리더 난수, 서버 난수를 XOR연산한 H(IDt)⊕Rr⊕Rdbt와 태그의 난수 Tr을 생성하여 리더난수와 연접한 Tr ‖ Rr을 리더에게 전송한다.

◎ 단계 ⑥ : 태그로부터 H(IDt)⊕Rr⊕Rdbt, Tr ‖ Rr을 받은 리더는 태그의 난수 Tr을 저장하고 서버에게 H(IDt)⊕Rr⊕Rdbt을 전송한다.

◎ 단계 ⑦ : 서버는 서버에 저장된 태그의 값(IDdb)을 해시하여 H(IDdb)를 생성하고, ①②단계에서 저장되고 생성된 Rr와 Rdbt를 XOR 연산한 H(IDdb)⊕Rr⊕Rdbt를 생성한다. 그리고 리더로부터 전송받은 H(IDt)⊕Rr⊕Rdbt와 서버에서 생성된 H(IDdb)⊕Rr⊕Rdbt를 비교하여 같으면 태그를 인증한다. 만약 다를 경우 서버에 저장하여 추후 동일한 데이터가 전송될 시 공격자로 분류한다. 태그가 인증하였을 경우 H(IDt)⊕Rr⊕Rdbt를 리더에게 전송한다.

◎ 단계 ⑧ : 리더는 서버로부터 H(IDt)⊕Rr⊕Rdbt를 수신하고 Tr ‖ Rr를 포함하여 H(IDt)⊕Rr⊕Rdbt, Tr ‖ Rr을 태그에게 전송한다. 태그는 리더에게 H(IDt)⊕Rr⊕Rdbt, Tr ‖ Rr를 수신하고, 일치 여부를 확인한다. 만약 태그에 저장된 값과 같을 경우 리더를 인증하고, 다를 경우 인증 과정을 중지한다.

Ⅲ. 위치추적과 스푸핑 공격을 이용한 NLMAP의 취약점 분석

NLMAP는 태그와 리더, 서버의 난수와 태그ID의 해시 값을 이용하여 다양한 공격에 안전하다고 주장하였다. 그러나 SHA-1 해시함수 값 160비트와 리더, 서버의 난수 32비트를 각각 XOR 연산을 하는 것은 상위 128비트는 고정된 값이기 때문에 위치추적과 트래픽 분석이 가능함이 보여 진다. 또한,

리더와 태그의 무선 상에 노출된 난수로 공격자는 태그의 해시 연산된 ID값을 얻을 수 있다. 마지막 단계에서 태그의 난수와 리더의 난수가 연접되어진 값 Tr ‖ Rr은 5단계에서 태그가 리더에게 전송하는 값과 동일하기 때문에 이를 상호인증에 사용하는 것은 무의미한 과정이다. 그러므로 배우식 등이 제안한 프로토콜은 상호인증을 제공하지 않으며, 프로토콜 전체에 문제가 있음이 보여 지고 있다.

본 장에서는 무선 상의 노출된 난수로 위치추적과 스푸핑 공격이 가능함 알아본다.

3.1. NLMAP 프로토콜의 위치추적

NLMAP 프로토콜에서는 리더, 서버의 난수를 사용하여 가변적 값으로 위치추적을 피한다고 주장하지만 리더와 태그사이의 노출된 난수 값으로 이를 피할 수 없다. 그림 2은 NLMAP의 위치추적을 나타낸 것이다.

◎ 단계 ① : 공격자는 도청공격으로 획득한 Rr를 Query와 함께 태그에게 전송한다. Query, Rr를 받은 태그는 Rr을 저장한다.

◎ 단계 ② : 공격자는 도청공격으로 획득한 Rdbt를 태그에게 전송한다.

◎ 단계 ③ : 태그는 공격자로부터 받은 Rdbt를 저장하고 태그의 난수 Tr을 생성한다. 그리고 태그는 태그의 정보(IDt)를 해시한 값과 Rr, Rdbt를 XOR하여 Tr ‖ Rr과 같이 공격자에게 전송한다.

공격자는 이 같은 방법을 연속적으로 태그에 요청하여 고정된 응답 값 H(IDt)⊕Rr⊕Rdbt을 수신하게 되어 태그의 위치를 추적할 수 있게 된다. 뿐만 아니라 태그가 보낸 H(IDt)⊕Rr⊕Rdbt에서 공격자가 보낸 Rr와 Rdbt를 다시 XOR연산하면, H(IDt)를 획득할 수 있게 된다. 이는 공격자가 획득한 H(IDt)를 이용하여 인증과정을 통과할 수 있는 문제점을 지니게 된다. H(IDt)를 이용하여 공격자가 인증을 통과하는 과정을 3.2절에서 알아본다.

3.2. NLMAP 프로토콜의 스푸핑 공격

NLMAP의 경우 리더와 태그사이의 데이터를 도청공격으로 획득하여 스푸핑 공격이 가능하다. 그림 3은 NLMAP의 스푸핑 공격을 나타낸 것이다.

공격자는 정당한 리더와 태그사이에서 전송된 리더난수 Rr^{old}, 서버난수 $Rdbt^{old}$, 태그가 생성한 $H(IDt)\oplus Rr^{old}\oplus Rdbt^{old}$, $Tr^{old} \| Rr^{old}$를 도청 공격으로 획득하여 스푸핑 공격을 할 수 있다. 과정은 다음과 같다.

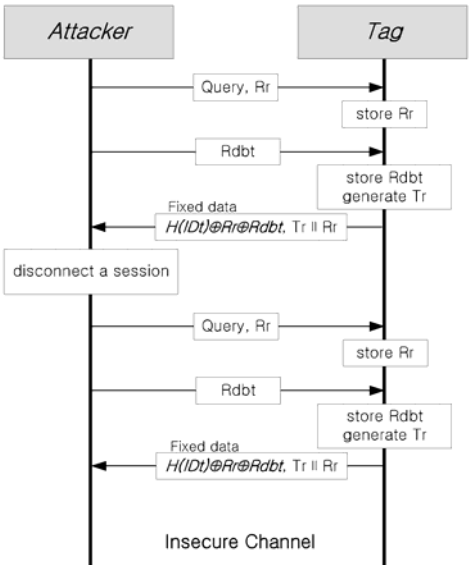

그림 2. NLMAP 프로토콜의 위치추적
Fig. 2. Location Tracking of The NLMAP

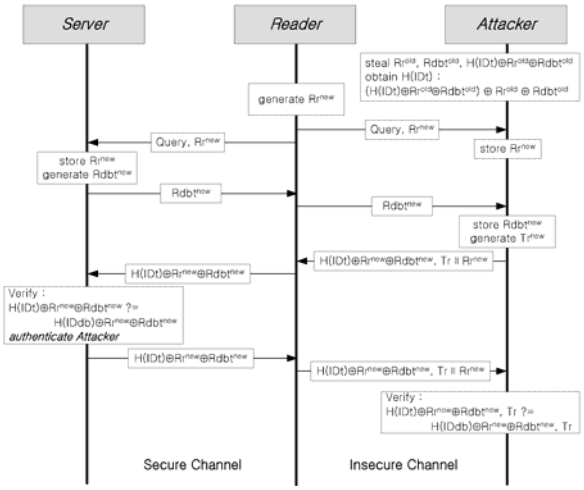

그림 3. NLMAP 프로토콜의 스푸핑 공격
Fig. 3. Spoofing Attack of The NLMAP

◎ 사전 단계 : 공격자는 도청 공격으로 획득한 $H(IDt)\oplus Rr^{old}\oplus Rdbt^{old}$에서 Rr^{old}와 $Rdbt^{old}$를 이용하여 H(IDt)를 획득한다. 그리고 정당한 태그인 척 위장하여 정당한 리더의 인식범위에 접근한다.

◎ 단계 ①, ② : 리더는 인식 범위에 있는 공격자에게 Query와 Rr^{new}를 전송한다. 그리고 서버에게도 동일한 데이터를 전송한다. 공격자는 리더에게 받은 Rr을 저장한다.

◎ 단계 ③ : 서버는 리더의 난수 Rr^{new}를 저장한다. 그리고 서버의 난수 $Rdbt^{new}$를 생성하여, 리더에게 전송한다.

◎ 단계 ④ : 리더는 공격자에게 서버에서 생성

한 $Rdbt^{new}$를 전송한다.

◎ 단계 ⑤ : 공격자는 리더에게 받은 $Rdbt^{new}$를 저장한다. 그리고 리더의 요청에 대한 응답을 위해 사전 단계에서 획득한 H(IDt)와 리더가 보낸 Rr^{new}, $Rdbt^{new}$를 XOR 연산하여 리더에게 전송한다.

◎ 단계 ⑥ : 리더는 공격자에게 받은 $H(IDt)\oplus Rr^{new}\oplus Rdbt^{new}$, $Tr^{old} \| Rr^{new}$에서 Tr^{old}를 저장하고, $H(IDt)\oplus Rr^{new}\oplus Rdbt^{new}$를 서버에게 전송한다.

◎ 단계 ⑦ : 서버는 서버에 저장된 태그의 정보 IDdb를 해시한 H(IDdb)와 리더난수 Rr^{new}, 서버난수 $Rdbt^{new}$를 XOR 연산한 $H(IDdb)\oplus Rr^{new}\oplus Rdbt^{new}$를 생성한다. 그리고 리더에게 받은 $H(IDt)\oplus Rr^{new}\oplus Rdbt^{new}$를 비교하여 같으면 태그를 인증한다. 여기서 정당한 태그에서 생성된 H(IDt)와 리더난수 Rr^{new}, 서버난수 $Rdbt^{new}$는 검증과정에서 문제가 없기 때문에 공격자를 인증하게 된다. 서버는 공격자를 인증하고 $H(IDt)\oplus Rr^{new}\oplus Rdbt^{new}$를 리더에게 전송한다.

NLMAP는 리더난수 Rr과 서버난수 Rdbt가 무선상에 노출되었기 때문에 공격자는 H(IDt)값을 획득할 수 있게 된다. 획득한 H(IDt)로 인해 위의 과정처럼 공격자임에도 불구하고 정당한 태그로 위장이 가능하고, 인증과정을 손쉽게 통과할 수 있게 된다.

Ⅳ. 제안 프로토콜

본 장에서는 NLMAP의 문제점을 개선한 상호인증 프로토콜을 제안한다. 그림 4는 해시함수와 CRC 코드 기반의 RFID 상호인증 프로토콜을 나타낸 것이다.

4.1. 가정 사항 및 표기법

본 논문에서 제안한 RFID 프로토콜은 다음과 같은 가정 하에서 동작하며, 표 1은 표기법을 나타낸 것이다. 첫째, 서버와 리더 사이는 안전한 통신 채널을 이용하며, 공격자의 공격에 안전하다. 둘째, 리더와 태그 사이는 공격자의 공격에 취약한 무선 채널을 사용한다. 셋째, 리더, 태그, 서버는 32비트 난수를 생성하며, 리더와 서버는 32비트의 안전한 난수 생성기를 사용한다. 넷째, 태그의 경우 EPC-Global C1 G2의 RN-16를 2번 사용하여 32비트를 생성한다. 다섯째, CRC 코드는 EPC-Global C1 G2에서 제공되는 CRC 함수를 사용한다. 마지막으로 태그는 고유 식별정보를 가지고 있으며, 리더로부터 전원을 공급받는 수동형 태그로 가정한다.

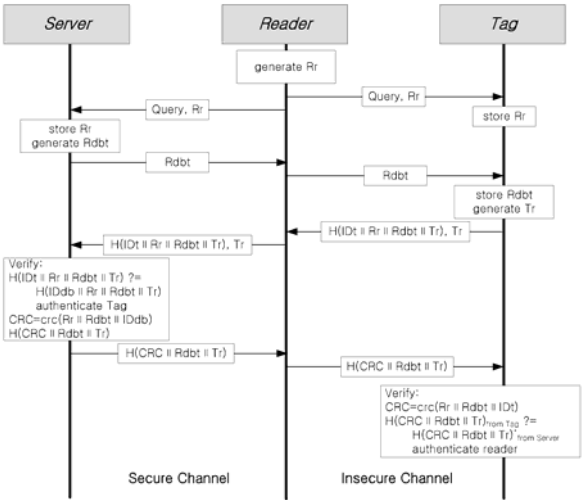

그림 4. 제안 프로토콜
Fig. 4. The Propose Protocol

표 1. 표기법
Table 1. The Notations

용 어	내 용
Rr	리더가 생성한 난수
Rdbt	서버가 생성한 난수
Tr	태그가 생성한 난수
IDt	태그에 저장된 태그의 고유 식별정보
IDdb	서버에 저장된 태그의 고유 식별정보
H( )	해시 연산(SHA-1)
crc( )	CRC 연산자
‖	연접 연산자

4.2. 제안 프로토콜의 인증 과정

제안 프로토콜은 해시함수와 CRC코드를 이용하여 다음과 같은 상호인증 과정을 거치게 된다.

◎ 단계 ①, ② : 리더는 난수 Rr을 생성하여, 태그와 서버에게 Query와 함께 전송한다. Rr을 받은 태그는 Rr을 저장한다.

◎ 단계 ③ : Rr을 받은 서버는 Rr을 저장하고, 서버의 난수 Rdbt를 생성하여 리더에게 전송한다.

◎ 단계 ④ : 서버로부터 Rdbt를 수신한 리더는 태그에게 Rdbt를 전송한다.

◎ 단계 ⑤ : 리더에게 Rdbt를 받은 태그는 Rdbt를 저장하고, 난수 Tr을 생성한다. 그리고 IDt와 Rr, Rdbt, Tr를 연접한 후 해시연산 한 $H(IDt \| Rr \| Rdbt$

‖Tr)를 생성하여 Tr과 함께 리더에게 전송한다.

◎ 단계 ⑥ : H(IDt ‖ Rr ‖ Rdbt ‖ Tr), Tr를 수신한 리더는 서버에게 전송한다.

◎ 단계 ⑦ : 서버는 리더에게 수신한 H(IDt ‖ Rr ‖ Rdbt ‖ Tr)를 검증한다. 검증 시 서버에 저장된 IDdb와 ②, ③단계의 Rr, Rdbt와 태그난수 Tr를 연접 연산하여 해시한다. 이 때 리더로부터 수신한 해시 값과 동일할 경우 태그를 인증한다. 만약 다르거나 없는 경우 공격자로 간주하여 통신을 종료한다.

서버에서 인증과정을 통과하면 CRC 코드를 생성한다. CRC코드는 Rr, Rdbt, IDdb를 연접하여 crc 함수를 통해 생성한다. 생성된 CRC 코드는 Rdbt와 Tr을 연접하여 해시연산 한 H(CRC ‖ Rdbt ‖ Tr)를 리더에게 전송한다.

◎ 단계 ⑧ : 리더는 서버로부터 받은 H(CRC ‖ Rdbt ‖ Tr)을 태그에게 전송한다.

◎ 단계 ⑨ : 태그는 ①, ④단계에서 저장한 Rr, Rdbt와 태그의 정보 IDt를 연접하여 CRC 코드를 생성한다. 생성한 CRC 코드는 Rdbt, Tr과 연접하여 태그에서 해시 연산한 $H(CRC \| Rdbt \| Tr)_{from\ Tag}$ 값과 리더로부터 수신된 서버에서 연산한 해시 값 $H(CRC \| Rdbt \| Tr)'_{from\ Server}$와 비교하여 인증과정을 수행한다. 같을 경우 리더를 인증하고 이 후 과정을 수행한다. 그러나 만약 다를 경우 공격자로 간주하여 통신을 종료한다.

Ⅴ. 비교 분석

본 장에서는 보안성 측면과 효율성 측면에서 NLMAP과 제안 프로토콜을 비교 분석한다.

5.1. 보안성 분석

RFID 시스템의 보안 프로토콜의 보안 요구사항은 기밀성, 익명성, 상호 인증, 전 방향 안전성, 불구분성 보장과 같은 측면에서 정형적으로 분석을 한다. 기밀성을 만족할 경우 도청공격에 안전하고, 익명성 및 불구분성을 보장할 경우 위치추적을 방어할 수 있다. 또한, 상호인증을 통해 스푸핑 공격과 재전송 공격을 방어할 수 있다. 이를 기반으로 배우식 등이 제안한 해시함수 기반의 NLMAP 프로토콜과 제안한 프로토콜의 보안성을 분석하여, NLMAP가 다양한 공격에 취약하며, 제안 프로토콜이 개선되었음을 증명한다. 표 2는 보안 분석을 표로 나타낸 것이다.

5.1.1. 도청 공격

NLMAP와 제안 프로토콜은 태그의 고유 식별정보를 해시 연산하였기 때문에 도청공격을 하여 획득하더라도 알 수 없는 값이다. 또한 해시함수는 일방향성 특성으로 인해 비밀성과 무결성을 보장하고, 복호화 할 수 없으므로 도청공격에 안전하다.

5.1.2. 위치 추적

위치 추적은 공격자가 연속적인 요청에 대한 태그의 고정된 응답으로 태그의 위치를 추적하는 방법이다. NLMAP의 경우 Rr과 Rdbt를 H(IDt)에 XOR연산하여 리더의 요청에 대해 가변적으로 응답하지만 노출된 Rr과 Rdbt의 재 XOR연산으로 고정된 H(IDt)을 획득할 수 있기 때문에 공격자는 위치추적을 할 수 있다. 또한 3장의 NLMAP의 위치추적과 같이 동일한 Rr과 Rdbt를 태그에게 전송 시 고정된 해시 값이 송신되기 때문에 위치추적에 취약하다.

본 논문에서 제안한 프로토콜은 Rr과 Rdbt를 해시연산에 포함하기 때문에 H(IDt)를 공격자가 획득할 수 없으며, 가변적으로 응답하고자 태그의 난수 Tr을 포함한 가변적 H(IDt ‖ Rr ‖ Rdbt ‖ Tr)이므로 위치추적에 안전하다.

5.1.3. 스푸핑 공격

스푸핑 공격은 정당한 개체인 척 위장하여 정당한 개체와 통신하고 이에 인증을 통과하는 공격이다. NLMAP의 경우 3.2절의 스푸핑 공격 시나리오처럼 노출된 Rr과 Rdbt로 인한 H(IDt)획득 이 후, 정당한 태그인 척 위장하여 리더로부터 전송된 리더난수 Rr과 서버난수 Rdbt를 이용하여 인증 과정을 통과할 수 있다.

제안 프로토콜의 경우 매 세션 생성되는 리더의 난수와 서버의 난수를 해시 값에 포함하여 IDt값을 획득할 수 없다. 이로 인해 정당한 H(IDt ‖ Rr ‖ Rdbt ‖ Tr)를 생성할 수 없다. 설령 과거에 획득한 값을 서버에 전송하더라도, 리더와 서버의 난수 값은 매 세션 새로이 생성되기 때문에 다른 해시 값으로 서버에 인증과정을 통과할 수 없다. 또한 공격자가 정당한 리더인 척 위장할 경우 공격자는 난수를 포함한 $H(CRC \| Rdbt \| Tr)'_{from\ Server}$을 생성할 수 없다. 그리고 CRC코드에는 ID값이 포함되어 있으므로 정당한 서버만이 생성할 수 있다. 그러므로 제안 프로토콜은 스푸핑 공격에 안전하다.

5.1.4. 재전송 공격

재전송 공격은 공격자가 리더와 태그 사이의 데이터를 도청공격으로 획득한 뒤, 재전송하여 인증과정을 통과하는 공격법이다. NLMAP은 데이터에 변형을 가하지 않고 있는 그대로 재전송 공격할 경우 인증과정에서 실패하기 때문에 재전송 공격에 안전하다. 제안 프로토콜 또한 난수와 CRC 코드가 포함된 해시 값으로 인증 절차를 수행하기 때문에 재전송 공격에 안전하다.

5.1.5. 불법 태그의 접근 차단

태그는 리더가 전송한 Query를 수신하고 1:1 통신을 위해 대기상태에서 슬롯 카운터를 사용한다. NLMAP는 리더에게 정당한 연속적인 인증과정을 공격자가 수행한다면, 정당한 개체들이 통신을 못하는 상황이 나타난다. 이는 서비스 거부 공격으로 이어질 수 있다. 제안 프로토콜은 안전한 상호인증과정을 통하여, 불법태그의 접근을 막아 정당한 태그만 통신이 가능하다.

5.1.6. 트래픽 분석 공격

트래픽 분석은 다수의 태그에 대한 응답 값을 분석하여 다양한 정보를 추측하는 공격법이다. NLMAP는 3.1절에서 언급한 위치추적 공격법으로 다수의 태그에 대한 응답 값을 관찰하여 태그의 개수와 같은 정보를 추측할 수 있다. 하지만 제안 프로토콜은 가변적인 해시 값으로 추측이 불가능 하므로 트래픽 분석 공격에 안전하다.

5.1.7. 상호 인증

상호 인증은 무선 상의 데이터 통신에 있어서 매우 중요한 기법이다. 안전하지 않은 채널을 이용하는 리더와 태그는 상호간에 인증과정을 거쳐 정당한 개체와 통신이 이루어 져야한다. NLMAP의 경우 공격자임에도 불구하고 스푸핑 공격으로 인증과정을 통과하는 것을 3.2절에서 언급하였다.

제안 프로토콜의 리더의 Query에 대한 응답 값 H(IDt ‖ Rr ‖ Rdbt ‖ Tr)은 정당한 태그만 생성할 수 있다. 그 이유는 정당한 태그만이 IDt를 가지고 있기 때문에, 서버에서 H(IDt ‖ Rr ‖ Rdbt ‖ Tr)와 H(IDdb ‖ Rr ‖ Rdbt ‖ Tr)를 비교하는 태그 인증 과정을 공격자는 통과할 수 없다. 그리고 태그에서 이루어지는 리더 인증과정은 정당한 서버만 무결성이 보장된 CRC코드를 생성할 수 있다. 이 또한 서버의 IDdb가 포함되어 있기 때문에 안전한 CRC코드와 서버, 태그의 난수의 값이 포함된 H(CRC ‖ Rdbt ‖ Tr)은 정당한 서버와 태그가 생성 가능하고, 리더를 인증함으로써 상호인증이 완료된다. 그러므로 제안 프로토콜은 난수와 태그의 고유 식별정보와 CRC코드를 이용하여 상호인증 과정을 수행하여 스푸핑 공격, 재전송 공격에 안전하다.

5.1.8. 보안 요구 사항

RFID 시스템은 무선 채널을 이용한 데이터 통신 방법 이기 때문에 상호인증, 익명성, 무결성, 기밀성과 같은 조건을 만족해야한다. NLMAP의 배우식 등은 해시된 데이터 값과 난수를 이용하여 상호인증을 제공한다고 주장한다. 그러나 무선 상의 노출된 데이터를 이용한 상호인증은 무의미한 과정이기 때문에 상호인증을 제공한다고 볼 수 없다. 뿐만 아니라 동일한 리더, 서버의 난수에 대한 태그의 응답 값은 항상 고정된 데이터이기 때문에 익명성, 불구분성 과 같은 조건을 만족하지 않는다. 무결성의 경우는 무선 상의 노출된 난수를 이용하여 제 복호화하여 태그ID의 해시된 값을 획득한 후, 공격자가 임의의 난수를 이용한 데이터 위·변조가 가능하다. 태그ID는 해시 화 되어 있어 태그ID에 대한 기밀성은 보장된다. 그러나 프로토콜에서 태그ID를 이용한 과정이 아닌 태그ID가 해시 연산된 자체를 이용한 과정이기 때문에 프로토콜 전체에 대한 기밀성은 보장하지 않고 있다.

제안 프로토콜은 태그와 리더, 서버의 난수와 태그 ID를 포함하여 해시연산 하기 때문에 익명성, 무결성, 기밀성을 모두 만족한다. 그리고 정당한 개체이여야만 CRC코드 생성과 해시 값을 생산할 수 있기 때문에 상호인증 또한 안전하다.

표 2. NLMAP와 제안 프로토콜의 보안 분석
Table 2. The Security Analysis of RFID Protocols

	NLMAP	제안 프로토콜
도청 공격	안전	안전
위치 추적	취약	안전
스푸핑 공격	취약	안전
재전송 공격	안전	안전
트래픽 분석 공격	취약	안전
상호 인증	미제공	제공
익명성	미제공	제공
무결성	미제공	제공
기밀성	미제공	제공
태그의 해시 연산된 데이터	고정	가변

5.2. 효율성 분석

NLMAP는 리더난수 Rr과 서버난수 Rdbt를 태그에서 H(IDt)와 XOR 연산하기 때문에 태그에서 XOR 연산을 2회 수행한다. 하지만 제안 프로토콜은 해시 연산에 리더, 서버 난수를 포함하기 때문에 XOR연산을 수행하지 않는다. NLMAP의 서버에서의 XOR연산은 서버에 저장된 IDdb에 대한 해시 값을 찾는데 평균 ⌈n/2⌉번(n: 서버에 저장된 태그의 수)의 해시 연산이 필요하다. 그러므로 XOR연산 또한, 평균 ⌈n/2⌉번의 XOR연산과 Rr과 Rdbt에 대한 XOR연산을 포함하여 ⌈n/2⌉+1번의 XOR연산을 수행하기 때문에 제안 프로토콜에 비해 연산량이 많음을 볼 수 있다.

태그의 해시 연산의 경우 제안 프로토콜은 2회에 비해 NLMAP는 1회이다. 하지만 NLMAP의 리더 인증과정인 H(IDt)⊕Rr⊕Rdbt와 H(IDdb)⊕Rr⊕Rdbt 비교는 그림 1의 5단계에서 태그가 전송하는 값과 동일하다. 이는 의미 없는 인증과정이므로 8단계가 5단계와 동일하여 해시연산 횟수에 포함하지 않고 기존 프로토콜에 비해 효율성 측면에서 우수하다는 것은 무의미하다. 표 3는 NLMAP와 제안 프로토콜의 효율성 분석을 나타낸 것이다.

표 3. NLMAP와 제안 프로토콜의 효율성 분석
Table 3. The Efficiency Analysis of RFID Protocols

	NLMAP	제안 프로토콜
태그 난수 생성	1	1
리더 난수 생성	1	1
서버 난수 생성	1	1
태그 XOR 연산	2	-
서버 XOR 연산	⌈n/2⌉+1	-
태그 해시 연산	1	2
서버 해시 연산	⌈n/2⌉	⌈n/2⌉+1
통신 라운드 수	8	8
리더와 태그간 총 송·수신량	512 bits	416 bits

n : 서버에 저장된 태그의 수

Ⅵ. 결 론

최근 유비쿼터스(Ubiquitous) 컴퓨팅의 핵심 기술로 각광 받는 RFID 시스템은 무선 주파수를 이용하여 데이터를 전송한다. 그러나 무선 주파수를 이용하기 때문에 도청, 위치추적, 스푸핑 공격, 재전송 공격 등 보안에 취약한 문제점이 있다. 이를 해결하고자 다양한 공격에 안전한 프로토콜이 연구되어지고 있는 실정이다. 2011년 배우식 등은 해시함수 기반의 새로운 저비용 RFID 상호인증 프로토콜(NLMAP)을 제안하였다. 배우식 등은 해시함수와 난수를 이용하여 연산량을 최소화하고, 상호인증과정으로 다양한 공격에 안전하다고 주장하였다. 그러나 그들의 주장과 달리 무선 채널 상의 노출된 리더와 서버의 난수로 위치추적과 스푸핑 공격이 가능함을 본 논문에서 증명하였다. 또한, 리더와 태그간 동일한 데이터로 리더를 인증하는 것은 무의미하며, 공격자도 인증과정을 통과하는 결과를 초래하게 된다. 배우식 등은 난수생성, XOR등의 연산을 최소화하고 복잡한 연산이 없어 저비용으로 구축할 수 있다고 주장한다. 그러나 5.2절에서 언급한바와 같이 ⌈n/2⌉+1번으로 서버에서의 XOR연산이 상당히 많음을 볼 수 있다. 뿐만 아니라 태그에서의 리더 인증과정인 H(IDt)⊕Rr⊕Rdbt와 H(IDdb)⊕Rr⊕Rdbt 비교는 무의미한 인증과정이므로 태그에서 해시연산 1회로 효율적임은 신뢰할 수 없게 된다.

본 논문에서는 NLMAP 프로토콜에서 도청 공격으로 리더와 태그간의 데이터를 획득하여 태그에 대한 위치추적이 가능하고, 스푸핑 공격으로 공격자가 인증과정을 통과함을 증명하였다. 또한 난수와 CRC코드를 이용한 상호인증으로 NLMAP 프로토콜을 개선하고, 다양한 공격에 안전한 프로토콜을 제안한다.

참 고 문 헌

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

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

[3] 홍도원, 장구영, 박태준, 정교일, "유비쿼터스 환경을 위한 암호 기술 동향," *전자통신동향분석,* 제20권, 제1호, pp. 63-72, 2005. 02.

[4] J. Cho, S. Yeo, S. 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.

[5] 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.

[6] S. Weis, S. Sarma, R. Rivest, D. Engels, Security and privacy aspects of low-cost radio frequency identification systems, in: *International Conference on Security in Pervasive Computing,* pp. 201-212, Mar. 2003.

[7] S. A. Sarma, S. E. Weis, D. W. Engels, "RFID systems and security and privacy implications", *cryptographic hardware and embedded systems – CHES 2002, LNCS,* Vol. 2523, pp. 454-469, Aug. 2002.

[8] 배우식, 이종연, 김상춘, "해시함수 기반의 새로운 저비용 RFID 상호인증 프로토콜", *컴퓨터교육학회논문지,* 제14권, 제1호, pp. 175-185, 2011. 01.

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

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> 정보보안, 센서 네트워크, 임베디드 시스템

이 창 희 (Changhee Lee) 정회원

1992년 2월 경북대학교 컴퓨터공학과 학사
1994년 2월 경북대학교 컴퓨터공학과 석사
1998년 8월 경북대학교 컴퓨터공학과 박사
1998년 9월~현재 계명문화대학 컴퓨터학부 교수
<관심분야> RFID, 임베디드 시스템, 시험구조

이 재 강 (Jaekang Lee) 정회원

2002년 2월 가야대학교 컴퓨터공학과 학사
2005년 8월 경북대학교 컴퓨터공학과 석사
2009년 3월~현재 경북대학교 전자전기컴퓨터학부 박사과정
<관심분야> RFID, 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, 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