저장 공간 및 연산 효율적인 RFID 경계 결정 프로토콜

정회원 안 해 순*, 종신회원 윤 은 준**, 정회원 부 기 동***, 남 인 길****°

A Storage and Computation Efficient RFID Distance Bounding Protocol

Hae-soon Ahn* *Regular Member*, Eun-jun Yoon** *Lifelong Member*,
Ki-dong Bu***, In-gil Nam****° *Regular Members*

요 약

최근에 근접 인증(proximity authentication)을 위해 사용하는 RFID 시스템이 경계 위조(distance fraud), 마피아 위조(mafia fraud), 테러리스트 위조(terrorist fraud) 공격들과 같은 다양한 위치 기반의 중계 공격(relay attack)들에 취약함이 증명되었다. 이러한 중계 공격들을 방지하기 위해 리더와 태그사이의 데이터 왕복 전송 시간을 측정하는 경계 결정(distance-bounding) 프로토콜이 한 해결책으로 연구되고 있다. 2008년에 Munilla와 Peinado는 Hancke-Kuhn이 제안한 프로토콜을 수정하여 보이드-시도(void-challenge) 기법을 적용한 RFID 경계 결정 프로토콜을 제안하였다. Hancke-Kuhn 프로토콜과 비교하여 Munilla-Peinado의 프로토콜은 공격자에게 n번의 왕복에서 (5/8)n의 성공 확률을 제공함으로써 공격 성공 확률을 감소시켜준다. 하지만 저장 공간 낭비와 많은 해쉬 함수 연산으로 인해 저비용 수동형 태그에는 비효율적이다. 이에 본 논문에서는 태그측의 해쉬 함수 연산량을 줄이고, 적은 저장 공간을 요구함으로써 저비용 수동형 태그에 적합한 새로운 RFID 경계 결정 프로토콜을 제안한다. 결론적으로 제안한 경계 결정 프로토콜은 Munilla-Peinado의 프로토콜과 비교하여 저장 공간 효율성과 연산 효율성을 높여줄 뿐만 아니라, $(5/8)^n$의 공격자 성공 확률을 보장함으로써 동일한 안전성을 제공할 수 있다.

Key Words : RFID, Authentication, Distance Bounding Protocol, Relay Attacks

ABSTRACT

Recently many researchers have been proved that general RFID system for proximity authentication is vulnerable to various location-based relay attacks such as distance fraud, mafia fraud and terrorist fraud attacks. The distance-bounding protocol is used to prevent the relay attacks by measuring the round trip time of single challenge-response bit. In 2008, Munilla and Peinado proposed an improved distance-bounding protocol applying void-challenge technique based on Hancke-Kuhn's protocol. Compare with Hancke-Kuhn's protocol, Munilla and Peinado's protocol is more secure because the success probability of an adversary has (5/8)n. However, Munilla and Peinado's protocol is inefficient for low-cost passive RFID tags because it requires large storage space and many hash function computations. Thus, this paper proposes a new RFID distance-bounding protocol for low-cost passive RFID tags that can be reduced the storage space and hash function computations. As a result, the proposed distance-bounding protocol not only can provide both storage space efficiency and computational efficiency, but also can provide strong security against the relay attacks because the adversary's success probability can be reduced by $(5/8)^n$.

* 대구대학교 기초교육원 컴퓨터과정(ahs221@hanmail.net), ** 경북대학교 전자전기컴퓨터학부(ejyoon@knu.ac.kr),
*** 경일대학교 컴퓨터공학과(kdbu@kiu.ac.kr), **** 대구대학교 컴퓨터·IT공학부(ignam@daegu.ac.kr) (° : 교신저자)
논문번호 : KICS2010-03-126, 접수일자 : 2010년 3월 29일, 최종논문접수일자 : 2010년 8월 10일

Ⅰ. 서 론

1.1 연구 배경

무선 주파수를 이용하여 통신하는 RFID(Radio Frequency IDentification) 시스템은 개체에 부착된 태그를 식별하여 정보를 처리하는 비접촉 방식이다. 이러한 RFID 기술은 최근 급속도로 발전하고 있는 분야로서 국가 주도의 신성장동력 산업으로 선정되었으며, 현재 125kHz에서 2.45GHz까지 다양한 주파수 대역에서 사용할 수 있는 RFID 인증 시스템들이 개발되고 있다. 일반적으로 RFID 시스템은 리더(reader)와 태그(tag), 그리고 리더에서 인식한 정보를 저장하고 처리하는 데이터베이스(database)로 구성된다. 하지만 물리적인 접촉 없이도 인식이 가능한 RFID 시스템의 특징 및 무선 통신환경으로 인해 개체를 유일하게 식별하기 위한 태그 식별자 정보의 노출, 시스템의 안전성 저해, 개인 정보 유출, 위치 추적 등의 다양한 프라이버시(privacy) 침해를 유발시킬 수 있는 문제점들을 가지고 있다[1-3]. 특히 RFID 장치나 비접촉식 스마트 카드는 근접 인증(proximity authentication)을 위해 사용자의 위치나 상황을 이용하여 통신하므로 위치 추적을 통해 합법적인 사용자로 위장한 공격자를 빨리 감지하여 인증 받지 못하도록 해야 한다[4]. 하지만 최근 근거리 RFID 인증 시스템상에서 근접 인증에 사용되는 RFID 태그들이 마피아 위조(mafia fraud) 공격, 테러리스트 위조(terrorist fraud) 공격과 같은 다양한 위치 기반 공격인 경계 위조(distance fraud)와 중계 공격(relay attack)들에 매우 취약함이 증명되었다[5-8].

일반적으로 중계 공격은 RFID 기반 시도-응답(challenge-response) 인증 프로토콜이 진행되는 동안 공격자가 리더와 태그사이에 교환되는 정보의 중계를 위해 두 개의 트랜스폰더를 사용한 물리적 공격이기 때문에 응용 계층에서 동작하는 RFID 인증 프로토콜들로는 예방하기 어렵다. 결론적으로 위와 같은 중계 공격들은 RFID 프로토콜 스택(stack)의 응용 계층(application layer)상에서 동작하는 암호학적 인증 프로토콜들(cryptographic authentication protocols)을 사용하여 방어할 수 있는 공격들이 아니다. 따라서 최근 위와 같은 중계 공격들에 대한 해결책으로 리더와 태그사이의 메시지 송수신 왕복 시간을 측정하는 RFID 경계 결정(distance-bounding) 프로토콜을 개발하여 기본 RFID 인증 메커니즘에 적용하는 연구가 활발히 진행되고 있다. RFID 경계 결정 프로토콜의 근본적인 목적은 공격자가 리더기인 검증자를 속이기 위한 다양한 중계 공격들을 수행할 때 이를 쉽게 방어할 수 있을 뿐만 아니라 합법적인 태그가 리더의 인식 반경 내에 실제 존재하는지 여부를 안전하게 감지할 수 있도록 하는 것이다.

1.2 연구 동기

응용 계층상에서의 송수신 메시지 도착 시간(arrival time)에 관한 정보는 하위 계층인 물리 계층에서 구현된 동기화(synchronization), 충돌 회피(collision-avoidance), 복조(demodulation), 심볼-감지(symbol-detection), 오류-감지(error-detection), 그리고 재전송 메커니즘들(re-transmission mechanisms)에 의해서 쉽게 훼손되어 질 수 있다. RFID 경계 결정 프로토콜은 인증(authentication) 기능과 경계 측정(distance measuring) 기능을 모두 포함하고 있기 때문에 위와 같은 문제점들을 해결할 수 있는 아주 효과적인 방어 대책이 될 수 있으며, 실제로 통신 프로토콜의 물리 계층(physical layer)에 적용하여 사용할 수 있는 경계 결정 프로토콜에 관한 연구가 최근에 아주 활발히 연구되고 있다.

경계 결정 개념을 최초로 소개한 Desmedt[5, 9-10]등은 송수신 메시지의 왕복 시간 측정을 기반으로 한 경계 결정 프로토콜이 마피아 위조 공격에 대한 정의와 공격 보안 대책으로 경계 결정이 활용될 수 있다는 점을 증명하였다. Desmedt의 아이디어를 기반으로 Brands와 Chaum[6]은 RFID 경계 결정 프로토콜을 처음으로 설계하여 시도-응답 기반 암호 프로토콜에서 단일 비트 왕복 중계 시간을 측정하는 실용적인 RFID 경계 결정 프로토콜을 개발하였다.

2005년에 Hancke-Kuhn[8]은 최초로 빠른 시도-응답 단계로 구성된 RFID 경계 결정 프로토콜을 발표하였다. Hancke-Kuhn 프로토콜은 태그와 리더간의 경계 측정은 각 라운드에서 리더에 의해 수행되도록 설계하였으며, 공격자에게 n번의 왕복에서 $(3/4)^n$의 공격성공 확률을 가지도록 설계되었다. 하지만 $(1/2)^n$과 비교하여 $(3/4)^n$의 높은 공격자 성공 확률은 마피아 위조 공격 또는 테러리스트 위조 공격과 같은 중계 공격들을 완벽히 방어할 수는 없었다. 이에 2007년에 Reid 등[13]은 위조 태그가 테러리스트 위조 공격과 같은 중계 공격을 수행할 수 없도록 비밀키 공유를 차단한 새로운 RFID 경계 결정 프로토콜을 제안하였다. 하지만 Reid 등이 제안한 프로토콜도 태그와 리더의 식별자(ID)가 평문으로 송수신되어 익명성을 보장할 수 없을 뿐만 아니라 위치 추적 공격에도 취약함이 증명되었다. 또한 Reid 등이 제안한 프로토콜은 공격자에게 n

번의 왕복에서 $(7/8)^n$의 성공 확률을 제공하여 Hancke-Kuhn 프로토콜의 $(3/4)^n$의 성공 확률과 비교하였을때 공격자의 성공 확률이 더 높아 심각한 보안성 문제점을 가지고 있다.

2007년에 Singelee와 Preneel[15]는 노이즈(noisy) 환경을 고려한 n번보다 적은 시도-응답 라운드를 요구하는 통신 시간 효율적인 새로운 RFID 경계 결정 프로토콜을 제안하였다. 하지만 Munilla와 Peinado[16]는 Singelee-Preneel 프로토콜이 여전히 중계 공격들에 취약함을 증명하였으며 더 나아가 Hancke-Kuhn 프로토콜의 $(3/4)^n$의 성공 확률보다 더 높은 확률로 공격자가 중계 공격을 성공할 수 있음을 증명하였다. 또 다른 연구로 2008년에 Munilla[11]등은 Hancke-Kuhn의 프로토콜을 기반으로 공격자의 성공 확률을 감소시키기 위해 보이드-시도(void-challenge) 기법을 적용한 공격자의 성공 확률은 $(5/8)^n$으로 감소시켜 주는 새로운 RFID 경계 결정 프로토콜을 제안하였다. 하지만 Munilla등이 제안한 프로토콜은 태그 측의 많은 저장 공간 낭비와 높은 해쉬 함수 연산량 요구로 인해 저비용 RFID 환경에서는 비효율적이다.

따라서 본 논문에서는 Munilla[11]등이 제안한 RFID 경계 결정 프로토콜(이하 MP-RFID 프로토콜)을 개선하여 안전성과 효율성을 보장하는 새로운 RFID 경계 결정 프로토콜을 제안한다. 제안하는 RFID 경계 결정 프로토콜은 두 번의 보이드-시도 기법 전송과 비밀키를 이용한 비트 단위의 XOR 연산을 기반으로 공격자의 공격 성공 확률을 MP-RFID 경계 결정 프로토콜과 마찬가지로 $(5/8)^n$ 상태로 높은 안전성을 유지할 수 있다. 더 나아가 태그의 저장 공간 효율성뿐만 아니라 해쉬 함수의 연산량을 줄여줌으로써 저비용 RFID 환경에서 실용적으로 사용될 수 있도록 설계되었다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 중계 공격의 유형과 MP-RFID 경계 결정 프로토콜에 대해 살펴보고, 3장에서는 제안하는 개선된 RFID 경계 결정 프로토콜에 대해 설명하고, 4장에서는 안전성을 분석하고, 5장에서는 효율성을 비교한다. 마지막으로, 6장에서는 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

2.1 중계 공격 유형

지불 및 접근 제어 애플리케이션에서 빈번하게 사용되고 있는 비접촉식 스마트 카드는 경계 위조 공격, 마피아 공격을 포함한 중계 공격, 테러리스트 공격과 같은 위치와 관련된 다양한 공격들에 취약하다.

중계 공격은 그림 1에서 보여지는 것처럼 중간자(man-in-the-middle) 공격과 유사하게 실제 리더가 공격자의 프록시 태그와 통신하고, 프록시 리더는 정당한 태그와 통신하여 합법적인 인증 정보를 획득하게 된다. 획득한 인증 정보를 담고 있는 프록시 태그는 실제 리더와 통신하게 됨으로써 프록시 태그로부터 수신된 인증 데이터를 실제 리더가 인증을 하게 된다. 따라서 리더는 사실상 멀리 떨어져있는 합법적인 태그 대신 프록시 태그의 존재를 검증하게 되는 것이다[7]. 이와 같이 RFID 시스템에서 리더와 태그는 데이터 교환을 위해서는 반드시 통신을 하기 때문에 이러한 중계 공격을 방지하기가 매우 어렵다.

일반적으로 중계 공격의 유형에는 다음과 같이 크게 두 가지로 분류 할 수 있다.

(1) 마피아 위조 공격(mafia fraud attack): 리더와 태그 둘 다 정당하지만, 공격자는 정당한 리더의 경계 내에 존재하여 리더와 태그 사이에서 프록시 리더와 프록시 태그를 사용하여 공격을 수행한다. 프록시 태그는 정당한 리더와 통신하고, 프록시 리더는 정당한 태그와 통신한다. 프록시 태그는 실제로 인증에 관련된 비밀 정보에 대한 어떠한 것을 알 필요도 없이 정당한 태그의 비밀 정보를 사용하여 리더와 인증하게 된다. 따라서 마피아 위조 공격은 공격자가 리더의 인증 범위 경계 내에 근접해 있으므로 리더와 태그 둘 다에게 어떠한 예고도 없이 공격을 가하는 매우 심각한 공격이며 이 공격을 방지하기 위해 많은 연구들이 진행되고 있다[6, 8].

(2) 테러리스트 위조 공격(terrorist fraud attack): 테러리스트 위조 공격은 정당한 태그가 공격자의 프록시 태그와 협력하여 인증을 하게 되는 마피아 위조 공격에서 확장된 공격이다. 이 공격에서 프록시 태그는 근접해 있는 리더와 인증하기 위해 정당한 태그와 공모하므로 정당한 태그의 비밀 키나 정보를 알지 못하더라도 인증에 성공하게 된다.

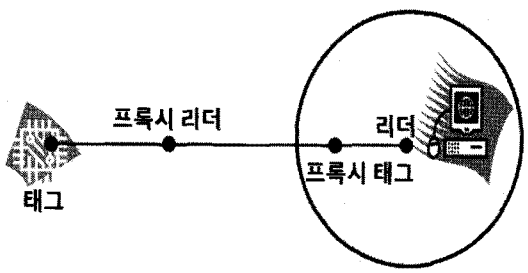


그림 1. 중계 공격 개요

2.2 MP RFID 경계 결정 프로토콜

본 절에서는 Munilla[11]등이 제안한 MP-RFID 경계 결정 프로토콜을 소개한다. 본 논문에서 사용되어지는 용어들의 표기법 및 정의는 표 1과 같다.

그림 2는 Munilla등이 제안한 MP-RFID 경계 결정 프로토콜의 전체적인 구성과 동작 과정을 보여주며, 아래와 같은 과정으로 수행된다. 준비 과정을 통해 리더와 태그는 사전에 비밀키 K를 공유하고 있다고 가정한다.

(1) 리더 → 태그: N_a

RFID 리더는 태그에게 자신이 생성한 난수 N_a를 전송한다.

표 1. 용어 정의

기호	의 미
C, N_a, N_b	난수들
K	비밀 값
$h()$	안전한 해쉬 함수(secure hash function)
$PRNG$	의사난수생성기(Pseudo Random Number Generator)
$\oplus$	배타적 논리합(XOR; eXclusive OR) 연산
$\|$	연접(concatenation) 연산
Ot_i	리더의 메시지 송신 시간
Rt_i	리더의 태그로부터 메시지 수신 시간
Δt_i	단일 비트 왕복 시간, $\Delta t_i = Rt_i - Ot_i$
$t_{\max}$	상위 경계 결정 값

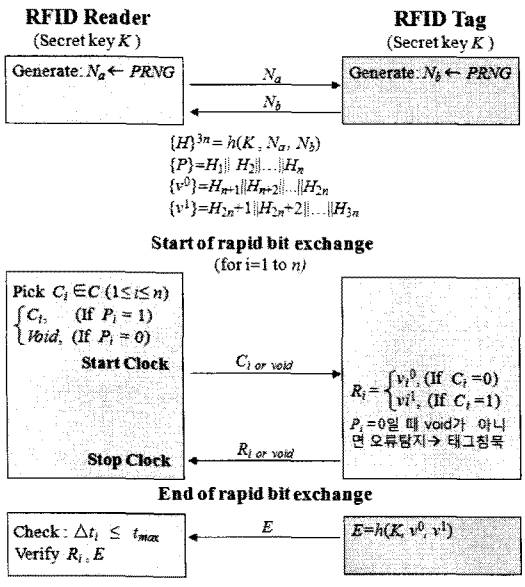


그림 2. MP-RFID 경계 결정 프로토콜

(2) 태그 → 리더: N_b

태그는 난수 N_a를 수신하고, 태그 자신이 생성한 난수 N_b를 리더에게 전송한다.

(3) 리더와 태그는 각각 비밀 키 K, 난수 N_a, N_b, 해쉬 함수 $h()$를 사용하여 $3n$ 비트 길이의 $h(K, N_a, N_b)$를 계산한 후 다음과 같이 n 비트 순서열 P, v^0, v^1 값으로 분리한다.

$$\{H\}^{3n} = h(K, N_a, N_b)$$
$$\{P\} = H_1 \| H_2 \| \ldots \| H_n$$
$$\{v^0\} = H_{n+1} \| H_{n+2} \| \ldots \| H_{2n}$$
$$\{v^1\} = H_{2n+1} \| H_{2n+2} \| \ldots \| H_{3n}$$

(4) 리더 → 태그: C_i or $void$

리더는 랜덤 비트열 C_n을 생성하고, 클럭사이클에서 정의된 비트열 값 n을 기반으로 단일 비트 시도-응답 교환을 순차적으로 시작한다. 만약 $P_i = 1$이면, 리더는 태그에게 $C_i (1 \le i \le n)$를 전송하고, $P_i = 0$이면 보이드-시도(void-challenge) 기법을 적용하여 비트 전송은 수행하지 않는다.

(5) 태그 → 리더: R_i or $void$

태그는 리더로부터 수신한 C_i 값에 의해 선택된 v_i^0 또는 v_i^1 둘 중 하나에 해당하는 R_i 의 왼쪽 1비트 값을 전송한다. 이때, $C_i = 0$ 이면 v^0의 1비트를 전송하고, $C_i = 1$ 이면 v^1의 1비트를 전송한다. 만약 $P_i = 0$이라면 태그 역시 보이드-시도 기법에 의해 응답 값으로 비트 전송을 수행하지 않는다. 이때, $P_i = 0$인데도 $void$ 상태가 아니라면 태그는 공격자에 의한 공격으로 탐지하거나 오류로 인식하고 침묵상태가 된다.

(6) 위 과정을 n번 동안 빠른 비트 교환을 모두 수행한 후에 태그는 해쉬 함수 연산을 수행한 값 $E = h(K, v^0, v^1)$을 리더에게 전송하여 마지막으로 검증을 요청한다. E를 수신한 리더는 태그와의 비트 왕복 전송 시간이 상위 경계 결정 값 이하로 측정되는지 검사하고, R_i와 E 값을 검증함으로써 인증하게 된다.

Ⅲ. 제안하는 RFID 경계 결정 프로토콜

본 장에서는 MP-RFID 경계 결정 프로토콜을 개선하여 태그측의 해쉬 함수 연산량을 줄여줄 뿐만 아니라 리더와 태그의 저장 공간 효율성을 제공하는 개선된 RFID 경계 결정 프로토콜을 제안한다.

3.1 제안 프로토콜 설명

그림 3은 제안하는 RFID 경계 결정 프로토콜의 전체적인 구성과 동작 과정을 보여주며, 다음과 같이 수행된다. 리더와 태그는 사전에 비밀키 K를 공유하고 있음을 가정한다.

(1) 리더 → 태그: N_a

RFID 리더는 태그에게 자신이 생성한 난수 N_a를 전송한다.

(2) 태그 → 리더: N_b

태그는 난수 N_a를 수신하고, 태그 자신이 생성한 난수 N_b를 리더에게 전송한다.

(3) 리더와 태그는 각각 비밀 키 K, 난수 N_a, N_b 그리고 해쉬 함수 $h()$를 사용하여 $h(K, N_a, N_b)$를 계산한 후 n 비트 순서열 P 값을 구한다.

(4) 리더 → 태그: C_i or *void*

리더는 랜덤 비트열 C_n를 생성하고, 클럭 사이클에서 정의된 비트열 값 n을 기반으로 단일 비트 시도-응답 교환을 순차적으로 시작한다. 만약 $P_i = 1$이면, 리더는 태그에게 $C_i (1 \le i \le n)$를 전송하고, $P_i = 0$이면 보이드-시도(void-challenge) 기법을 적용하여 비트 전송은 수행하지 않는다.

(5) 태그 → 리더: R_i or *void*

태그는 리더로부터 수신한 C_i 값에 대한 응답 값으로 R_i를 전송하게 되는데, 이때 $C_i = 1$이면 리더와 태그가 사전에 공유하고 있는 비밀키 값 K_i와 C_i를 XOR 연산을 수행한 $R_i = K_i \oplus C_i$ 값을 리더에게 전송한다. 만약 $C_i = 0$ 이면 보이드-시도 기법을 적용하여 응답 값을 전송하지 않게 되는 *void* 상태가 된다. 또한, $P_i = 0$일 경우에도 태그는 보이드 기법에 의해 응답 값으로 비트 전송을 수행하지 않게 된다. 이때, $P_i = 0$인데도 C_i 값이 수신된 경우에는 태그는 공격자의 공격이나 오류로 탐지하고 침묵상태가 된다.

(6) 리더는 태그로부터 단일 비트에 대한 응답 값 R_i를 수신하면, $\Delta t_i \le t_{max}$ 검증을 통하여 리더와 태그 사이의 빠른 비트 전송에 대한 왕복 시간이 상위 경계 값 이하로 측정되는지 검증하고, 태그로부터 수신한 값 R_i와 리더가 계산한 값 R_i'이 일치하는지를 검증한다. 이때, 리더 쪽에서의 연산도 태그와 동일하게 $C_i = 0$ 이면 $R_i' = void$로, $C_i = 1$이면 비밀키를 이용하여 XOR 연산을 수행한 $R_i' = K_i \oplus C_i$ 값을 계산하여 검증하게 된다.

3.2 검증 알고리즘 동작 원리 설명

앞 절에서 기술한 제안한 RFID 경계 결정 프로토콜의 단계 (6)에서의 단일 비트 왕복 전송 시간 추론 및 검증 알고리즘은 그림 4와 같다. 검증 루틴은 n비트만큼 수행하지만, 비트 왕복 전송 시간이 경계 결정 상위 값을 초과하게 되면 더 이상 루틴을 수행하지 않고 검증을 중단하게 된다. 그리고 $P_i = 0$일 경우 보이드-시도(void-challenge) 기법을 사용하여 리더는 비트 전송을 수행하지 않으며, 또한 한 번의 빠른 비트 왕복 수행이 끝나면 R_i'과 R_i의 동일여부 검증시 태

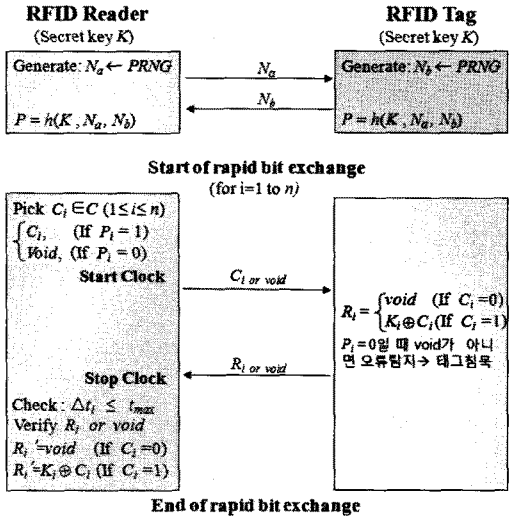


그림 3. 제안된 RFID 경계 결정 프로토콜

```
count_max = max threshold error value;
t_max = threshold time;
count = 0;
for (i = 1 to n)
{
  if (count == count_max) {중단;}
  else {
        if (P_i == 0) {
          if (void 기법 전송) {void 검증 성공;}
          else {검증 실패; count=count+1;}
        }
        else {
          Δt_i = Rt_i − Ct_i ;
          If((Δt_i ≤ t_max)&(R_i' == R_i)){검증 성공;}
          else {
              검증 실패;
              count = count + 1;}
        }
  }
}
```

그림 4. 검증 알고리즘

그가 리더로부터 수신한 값이 $C_i = 0$일 경우에 태그 측의 응답 값으로 보이드 기법인 *void* 전송을 적용함으로써 보이드-시도 검증 수행도 포함되어 있다.

위 그림 4의 검증 알고리즘에서 리더와 태그 간에 무선 통신을 수행하기 때문에 잡음 환경을 고려하여 상위 경계 결정 값을 초과하는 최대 허용 오류 값으로 $count_{max}$를 설정하였고, t_{max}는 단일 비트 왕복 전송 시간인 $\Delta t_i = Rt_i - Ct_i$의 임계 값(threshold value)으로 설정하였다. 단일 비트 왕복 전송 시간 ($\Delta t_i = Rt_i - Ct_i$)을 측정하여 경계 결정 상위 값이 t_{max} 이하이고($\Delta t_i \le t_{max}$), 리더가 계산한 값 R_i'과 태그로부터 수신한 값 R_i가 일치한다면 검증에 성공하며, 그렇지 않으면 검증에 실패할 뿐만 아니라 *count* 값을 1 증가 시킨다. 이러한 루틴은 n 비트까지인 n번 수행하게 된다. 그러나 비트 왕복 전송 시간이 경계 결정 상위 값 t_{max}를 초과하거나 R_i' 값과 R_i 값이 일치하지 않는다면 *count* 값은 계속 증가한다. 결국 증가한 *count* 값이 $count_{max}$값을 초과하게 되면 더 이상 검증 루틴은 수행되지 않고, 악의적인 공격자에 의한 통신으로 감지하여 검증을 중단한다.

3.3 제안 프로토콜 특징 및 차별성

일반적으로 RFID 태그는 무선 통신을 수행하기 위한 안테나 부분과 인증관련 연산을 수행하고 필요한 정보를 태그 내에 저장하는 마이크로 칩으로 구성되어 있다. 또한 태그는 특정 개체가 가지고 있는 고유의 정보인 식별자(ID; IDentifier)를 가지고 있고, 리더가 질의를 하면 태그는 자신에게 저장된 식별정보인 ID를 안전하지 않은 무선 통신 채널을 통해 리더에게 전송한다. 그러므로 공격자에 의한 태그의 정보 노출 가능성과 사용자의 위치 추적 등의 프라이버시 침해 문제를 유발시킨다. 특히 현재 교통카드, 신분증 등으로 많이 사용되는 수동형 RFID 태그는 저가의 하드웨어이기 때문에 물리적인 공격에 약할 뿐만 아니라, 저장 공간과 연산 능력은 리더와 백-엔드 데이터베이스의 연산 능력에 비해 훨씬 낮다. 이러한 이유로 태그의 정보 보호, 사용자 프라이버시 보호 및 다양한 공격들을 방지하기 위한 보안 및 인증 프로토콜의 필요성이 대두 되었다. 하지만 근접 인증에 사용되는 수동형 태그를 활용한 RFID 인증 프로토콜 기반의 시스템은 2장에 소개한 다양한 중계 공격들에 매우 취약함이 많은 연구를 통해 증명되고 있다. 대표적인 비접촉식 인터페이스들인 "proximity" (ISO 14443), "vicinity"(ISO 15693), "near field"(ISO 18092)와 같은 장치들은 대략 10센티미터에서 1미터 정도의 명목상의 작동 범위로 표준화 시켰다[17-19]. 교통카드나 건물 내 접근통제 등에 광범위하게 사용되는 ISO 14443과 ISO 18092 타입의 수동형 RFID 태그들과 비접촉식 스마트카드들은 근접 인증 과정에서 악의적인 프록시(proxy) 태그와 리더기를 사용한 다양한 중계 공격(relay attacks)들에 취약함이 최근에 증명되었다. 이러한 중계 공격 방지를 위해 리더와 태그간의 인증 부분에서 경계 결정 프로토콜은 아주 중요한 역할을 수행하고 있다. 따라서 본 논문에서는 저가의 수동형 태그의 특성에 맞도록 저장 공간 낭비와 연산량을 감소시킴으로써 중계 공격에도 안전할 뿐만 아니라 효율성을 보장하는 실용적인 RFID 경계 결정 프로토콜을 제안하였다. 제안한 프로토콜은 전통적인 응용 계층상에서의 RFID 인증 프로토콜에서 요구되는 다양한 보안 요구사항들을 만족할 뿐만 아니라 중계 공격이라는 물리적 공격에 대해서도 안전하여 높은 실용성을 보장 할 수 있다.

Ⅳ. 안전성 분석

본 장에서는 제안한 프로토콜에서 공격자의 공격 성공 확률이 MP-RFID 프로토콜과 마찬가지로 n번의 빠른 비트 왕복 전송에서 $(5/8)^n$을 유지함으로써 동일한 안전성을 보장함을 분석한다.

[정리 1] 제안한 프로토콜에서 공격자에 의한 중계 공격 성공 확률(Adv_A^{RFID})는 $\left(\frac{5}{8}\right)^n$ 이다.

[증명] 리더와 태그에서 각각 비밀 키 K, 난수 N_a, N_b 그리고 해쉬 함수 $h()$를 사용하여 $h(K, N_a, N_b)$를 계산한 n 비트 순서열 P에 대해 공격자가 P의 값을 정확하게 추측할 수 있는 확률은 0 또는 1중 하나이므로 1/2이라 할 수 있다. 또한, $P=0$일 경우에는 보이드 기법을 사용한 전송을 수행하므로 아무런 비트 전송이 수행되지 않은 채로 놔두게 되고, $P=1$일 경우에만 랜덤 비트열 C_i 값인 0 또는 1이 태그에게 전송되므로 역시 1/2이 된다. 따라서 공격자는 리더가 태그에게 전송하는 값에 대해 정확하게 추측할 수 있는 확률 P_f 값은 다음과 같이 계산된다.

$$P_f = \left(1 \times \frac{1}{2}\right) + \left(\frac{1}{2} \times \frac{1}{2}\right) = \frac{3}{4}$$

그리고 사전 요청이 없을 경우 공격자가 태그로부터 전송한 값에 대해 정확하게 응답 받을 수 있는 공

격 성공 확률의 수식과 확률 계산 과정은 다음과 같으며, 공격자의 성공 확률은 $(5/8)^n$이 된다.

$$Adv_A^{RFID} = \left(1 - \frac{P_f}{2}\right)^n = \left(1 - \frac{\frac{3}{4}}{2}\right)^n = \left(\frac{5}{8}\right)^n$$

[정리 2] 제안한 프로토콜은 태그 익명성(anonymity)을 보장하고, 안전한 태그 인증(authentication)을 제공한다.

[증명] 제안한 프로토콜의 리더와 태그의 비밀키는 해쉬 함수에 의해 보호되어 지며 절대로 외부로 공개되지 않으므로 익명성을 보장한다. 또한 합법적인 태그와 리더만이 난수를 생성하여 교환한 후에 비밀키를 가지고 해쉬 연산을 수행하여 $h(K, N_a, N_b)$ 값을 계산한다. 빠른 비트 교환 단계에서 리더는 태그에게 C_i or *void*를 전송하고, 태그는 리더에게 R_i or *void*를 응답한다. 이때 태그는 전송받은 비트 값이 공격자임을 인지하게 되면 전송을 중지한다. 빠른 비트 교환이 끝나면 태그가 계산한 $R_i = K_i \oplus C_i$와 리더가 계산한 $R_i' = K_i \oplus C_i$ 값을 검증하게 된다. 따라서 제안한 프로토콜은 인증을 제공한다.

[정리 3] 제안한 프로토콜은 재전송 공격에 안전하다.

[증명] 제안한 프로토콜에서는 매 세션마다 리더가 생성하는 새로운 난수, 태그가 생성하는 새로운 난수 그리고 비밀키를 이용하여 인증을 수행하기 때문에 과거에 공격자에 의해 재전송된 난수 값들은 태그와 리더의 인증 과정 중에 쉽게 검출된다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

[정리 4] 제안한 프로토콜은 위치 트래픽 공격에 안전하다.

[증명] 제안한 프로토콜에서는 난수에 의해 계산된 값이 매 세션마다 변경되기 때문에 공격자는 현재 세션에서 태그의 응답이 과거 세션에 도청한 응답과 동일한지를 비교할 수 없다. 즉, 매 세션마다 서로 다른 난수들을 생성하며, 매 세션마다 서로 다른 응답이 동일한 태그로부터 송신된 것인지 여부를 쉽게 구별할 수 없기 때문에 태그의 이동 경로를 쉽게 트래킹 할 수 없다. 따라서 제안한 프로토콜은 트래픽 분석 공격에 안전하다.

위에서 살펴본 바와 같이 제안하는 RFID 경계 결정 프로토콜도 MP-RFID 경계 결정 프로토콜[11]과 동일한 안전성을 제공함을 알 수 있다. 표 2는 MP-RFID 경계 결정 프로토콜과 제안한 RFID 경계 결정 프로토콜이 마피아 위조 공격 및 테러리스트 위조 공격인 중계 공격이 공격자에 의한 공격 성공 확률을 비교한 결과를 보여주고 있다.

표 2. 안전성 비교

프로토콜	Hancke-Kuhn 프로토콜	MP-RFID 프로토콜	제안한 프로토콜
마피아 위조 공격 성공 확률	$\left(\frac{3}{4}\right)^n$	$\left(\frac{5}{8}\right)^n$	$\left(\frac{5}{8}\right)^n$
테러리스트 위조 공격 성공 확률	$\left(\frac{3}{4}\right)^n$	$\left(\frac{5}{8}\right)^n$	$\left(\frac{5}{8}\right)^n$
Void 기법 적용 여부	미적용	적용	적용
보안강도	중간	높음	높음

V. 효율성 분석

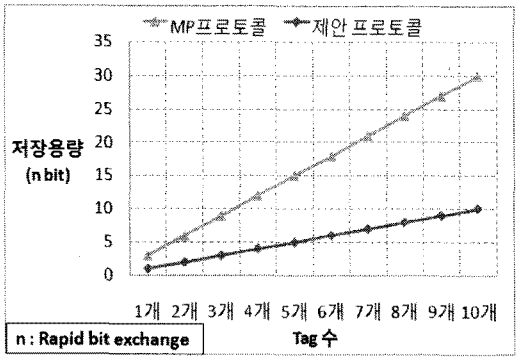
본 장에서는 MP-RFID 경계 결정 프로토콜과 제안한 RFID 경계 결정 프로토콜의 효율성에 대해 살펴본다. 표 3은 제안한 RFID 경계 결정 프로토콜과 MP-RFID 경계 결정 프로토콜[11]의 효율성을 비교한 결과를 보여주고 있다.

위에서 언급하였듯이 MP-RFID 경계 결정 프로토콜에서는 빠른 비트 교환 단계가 끝난 후에 마지막 검증을 위한 해쉬 함수 연산이 태그측에서 한 번 더 수행되었다. 그러나 저용량 태그에서 해쉬 함수 연산이 많아지면 비효율적이다. 제안한 RFID 경계 결정 프로

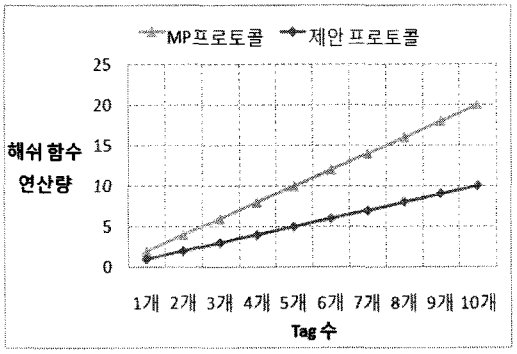
표 3. 효율성 비교

프로토콜 / 연산종류	MP-RFID 프로토콜		제안한 프로토콜	
	태그	리더	태그	리더
해쉬 연산량	2	1	1	1
저장공간 (bit수)	$3n$	$3n$	n	n
리더와 태그간 통신메시지량	$3h() + 6nbit$		$2h() + 2nbit$	
연산/통신 효율성	낮음		높음 저장 공간 : 67% 감소 해쉬 연산 : 34% 감소	

n : 비트열 개수, $h()$: 해쉬 연산 개수



(a) 저장 공간



(b) 해쉬 함수 연산량

그림 5. 효율성 분석

토콜은 리더와 태그측에서 각각 1번의 해쉬 함수 연산만을 수행하고, 태그가 리더로부터 수행한 값인 $C_i = 1$일 경우에만 XOR 연산을 수행한다. 이때의 XOR 연산량의 최대 값을 n번으로 하였지만, 그 이하로 연산량은 줄어든다는 점을 알 수 있다. 왜냐하면 $C_i = 0$일 경우에는 보이드 기법을 적용하여 $void$ 상태가 되기 때문이다. 또한, 리더는 수신한 R_i 또는 $void$를 이용하여 합법적인 태그인지 여부를 쉽게 판단할 수 있다. 무엇보다 본 논문에서는 리더와 태그의 저장 공간 효율성이 매우 우수하다는 점을 알 수 있다. MP 프로토콜에서는 리더와 태그에서 각각 비밀키 K, 난수 N_a, N_b 그리고 해쉬 함수 $h()$를 사용하여 $h(K, N_a, N_b)$를 계산한 후에 비트열을 $3n$으로 분리시키므로 리더와 태그 각각 $3n$비트의 저장 공간이 요구되어 총 $6n$비트의 저장 공간이 필요하다. 그러나 제안한 프로토콜에서는 비트열 분리 연산을 수행하지 않으므로 태그와 리더 각각 n비트의 공간만이 요구되어 $2n$비트만 있으면 된다. 따라서 본 논문에서 제안한 프로토콜에서는 RFID 리더와 태그측의 저장 공간을 약 67% 줄여주어 저장 공간의 효율성을 최적화하였으며, 태그의 해쉬 함수 연산량 또한 약 34% 줄여주어 더욱 효율적이다.

그림 5는 MP-RFID 프로토콜과 제안하는 프로토콜에 대한 저장 공간과 해쉬 함수 연산량을 분석한 그래프이다. 이 그래프에서는 제안한 프로토콜이 저장 공간뿐만 아니라 해쉬 함수 연산량 모두 효율적임을 알 수 있다. 위와 같은 이유로 본 논문에서 제안한 RFID 경계 결정 프로토콜이 MP RFID 경계 결정 프로토콜보다 효율성 면에서 매우 우수함을 보여주며, 저비용 및 저용량의 수동형 태그에 적합한 RFID 시스템에 적용되어 질 수 있다.

VI. 결 론

본 논문에서는 RFID 시스템에서 근접 인증에 사용되는 수동형 RFID 태그 환경에서 발생되는 중계 공격들을 방지하고, 기존의 연구와 비교하여 동일한 안전성을 보장함과 동시에 효율성 면에서 아주 우수한 개선된 RFID 경계 결정 프로토콜을 제안하였다. 제안한 프로토콜은 공격자에게 n번의 왕복에서 $(5/8)^n$의 성공 확률을 제공하는 MP-RFID 프로토콜을 개선하여 태그 측에서의 해쉬 함수 연산량을 줄여주고, 리더와 태그에서 각각 필요로 하는 저장 공간을 $3n$비트에서 n비트로 감소시켰다. 또한 응답 값으로 $C_i = 0$일 경우에는 비트 값을 전송하지 않는 보이드-시도 기법을 적용하였으며, $C_i = 1$일 경우에만 사전에 보유하고 있는 비밀키 K와 XOR 연산을 수행한 $R_i = K_i \oplus C_i$를 전송하게 하였다. 이러한 결과로 태그 측의 해쉬 연산량을 줄이고, 저장 공간의 효율성을 높여주어 수동형 저비용 태그에 적합한 RFID 시스템에 매우 효율적인 프로토콜로 개선하였다. 향후 연구로는 보이드-시도 기법과 XOR 연산을 기반으로 효율성과 안전성을 모두 고려하여 공격자에 의한 공격 성공 확률을 $(1/2)^n$으로 줄여줌으로써 더욱 강력한 안전성을 제공할 뿐만 아니라 높은 효율성을 제공하는 RFID 경계 결정 프로토콜을 제안하는 데 목표를 둔다.

참 고 문 헌

[1] 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.

[2] S. A. Weis, "Radio-frequency identification security and privacy," *Master's Thesis*, M.I.T. 2003.

[3] 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.

[4] I. Satoh. "Location-based services in ubiquitous computing environments", *Service-Oriented Computing -ICSOC 2003*, Springer-Verlag LNCS 2910, pp.527-42, November 2003.

[5] Y. Desmedt. Major security problems with the "Unforgeable" *(Feige)-Fiat-Shamir proofs of identiy and how to overcome them.* In SecuriCom ''88, pp.15-17, 1988.

[6] S. Brands and D. Chaum. Distance-bounding protocols. *Advances in Cryptology EUROCRYPT '3*, Springer-Verlag LNCS 765, pp.344-59, May 1993.

[7] G.P. Hancke. A practical relay attack on ISO 14443 proximity cards. http://www.cl.cam.ac.uk/ *'h275/relay.pdf*

[8] G. Hancke and M. Kuhn. An RFID distance bounding protocol. *In the 1st International Conference on Security and Privacy for Emergin Areas in Communications Networks (SECURECOMM''05)*, pp.67-73. IEEE Computer Society, 2005.

[9] Samy Bengio, Gilles Brassard, Yvo Desmedt, Claude Goutier, and Jean-Jacques Quisquater. Secure implementation of identification systems. *Journal of Cryptology*, 4(3):175-183, 1991.

[10] Thomas Beth and Yvo Desmedt. Identification tokens - or: Solving the chess grandmaster problem. *In CRYPTO*, pp.169-177. Springer Verlag, 1990.

[11] J. Munilla and A. Peinado. Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels. *Wireless communications and mobile computing*. Published online: Jan 17 2008.

[12] Y.-J. Tu and S. Piramuthu, RFID distance bounding protocols, In the 1st International EURASIP Workshop in RFID Technology. Vienna, Austria.

[13] J. Reid, J. Nieto, T. Tang, and B. Senadji, Detecting relay attacks with timing-based protocols, Proceedings of the 2nd ACM Symposium on Information, Computer, and Communications Security, pp.204-213, 2007.

[14] C. Meadows, R. Poovendran, D. Pavlovic, L.W. Chang, and P. Syverson. Distance bounding protocols: authentication logic analysis and collusion attacks. Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks, pp.279-298, Springer-Verlag, 2007.

[15] D. Singelee and B. Preneel, Distance bounding in noisy environments. In: F. Stajano et al., Editors, ESAS 2007, LNCS Vol.4572, Springer, Heidelberg (2007), pp.101-115.

[16] J. Munilla and A. Peinado, Attacks on a distance bounding protocol, Computer Communications, Vol.33, No.7, 2010, pp. 884-889.

[17] ISO 14443. Identification cards—contactless integrated circuit cards—proximity cards. International Organization for Standardization, Geneva.

[18] ISO 15693. Identification cards - contactless integrated circuit cards—vicinity cards. International Organization for Standardization, Geneva.

[19] ISO 18092 (ECMA-340). Information technology—telecommunications and information exchange between systems—near field communication—interface and protocol (NFCIP-1). Int. Organization for Standardization, Geneva, 2004.

안 해 순 (Hae-Soon Ahn) 정회원

1996년 2월 경일대학교 컴퓨터공학과(공학사)
2001년 경일대학교 컴퓨터공학과(공학석사)
2010년 대구대학교 컴퓨터정보공학과(공학박사)
2004년~2008년 경일대학교 컴퓨터공학부 전임강사
2008년~현재 대구대학교 기초교육원 컴퓨터과정 초빙교수
<관심분야> 데이터베이스, 정보보안, 정보검색, 데이터베이스 보안, RFID 보안

부 기 동 (Ki-Dong Bu) 정회원

1984년 경북대학교 전자공학과(공학사)
1988년 경북대학교 전자공학과(공학석사)
1996년 경북대학교 전자공학과(공학박사)
1983년~1985년 포항종합제철 시스템개발실
2001년~2002년 일본 게이오대학 방문교수
1988년~현재 경일대학교 컴퓨터공학과 교수
<관심분야> 데이터베이스, GIS, 시멘틱 웹, 데이터베이스 보안, RFID 보안

윤 은 준 (Eun-Jun Yoon) 종신회원

2003년 경일대학교 컴퓨터공학과(공학석사)
2007년 경북대학교 컴퓨터공학과(공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2008년~현재 경북대학교 전자전기컴퓨터학부 계약교수
2007년~현재 보안공학연구지원센터 보안공학논문지 편집위원
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

남 인 길 (In-Gil Nam) 정회원

1978년 경북대학교 전자공학과(공학사)
1981년 영남대학교 전자공학과(공학석사)
1992년 경북대학교 전자공학과(공학박사)
1978년~1981년 대구은행 전산부
1980년~1990년 경북산업대학 부교수
1990년~현재 대구대학교 컴퓨터·IT공학부 교수
<관심분야> 데이터베이스, 데이터베이스 보안, RFID 보안