DOI: 10.3745/KIPSTC.2010.17C.4.307

경량 RFID 경계 결정 프로토콜

안 해 순[†] · 부 기 동[††] · 윤 은 준[†††] · 남 인 길[††††]

요 약

최근 근접 인증에 사용되는 비접촉식 스마트카드와 같은 RFID 태그들이 경계 위조(distance fraud) 공격, 마피아 위조(mafia fraud) 공격, 테러리스트 위조(terrorist fraud) 공격과 같은 다양한 위치 기반 공격인 중계 공격(relay attack)들에 매우 취약함이 증명되었다. 더 나아가 이러한 중계 공격들을 방지하기 위해 리더와 태그사이의 메시지 송수신 왕복 시간을 측정하는 경계 결정(distance-bounding) 프로토콜이 한 해결책으로 연구되고 있다. 2005년에 Hancke과 Kuhn은 처음으로 해쉬 함수 기반의 RFID 경계 결정 프로토콜을 제안하였다. 하지만 Hancke-Kuhn 프로토콜은 공격자에게 n번의 왕복에서 $(3/4)^n$의 성공 확률을 제공하여 중계 공격을 완벽히 방어할 수 없다. 본 논문에서는 공격자에게 n번의 왕복에서 $(5/8)^n$의 성공 확률을 제공하는 새로운 경량 RFID 경계 결정 프로토콜을 제안한다. 연구 결론으로 제안한 프로토콜은 안전한 해쉬 함수와 XOR 연산을 기반으로 하여 높은 저장 공간 효율성을 제공할 뿐만 아니라, 공격자의 성공 확률을 $(5/8)^n$으로 최적화하여 중계 공격에 대해서도 더욱 더 안전하다.

키워드 : RFID, 인증, 경계 결정 프로토콜, 중계 공격, 마피아 위조 공격, 테러리스트 위조 공격

A Light-Weight RFID Distance Bounding Protocol

Hae-Soon Ahn[†] · Ki-Dong Bu[††] · Eun-Jun Yoon[†††] · In-Gil Nam[††††]

ABSTRACT

Recently, it is proved that contactless smart-card based RFID tags, which is used for proximity authentication, are vulnerable to relay attacks with various location-based attacks such as distance fraud, mafia fraud and terrorist fraud attacks. Moreover, distance bounding protocols have been researched to prevent these relay attacks that can measure the message transmitted round-trip time between the reader and the tag. In 2005, Hancke and Kuhn first proposed an RFID distance bounding protocol based on secure hash function. However, the Hancke-Kuhn protocol cannot completely prevent the relay attacks because an adversary has $(3/4)^n$ attack success probability. Thus, this paper proposes a new distance-bounding protocol for light-weight RFID systems that can reduce to $(5/8)^n$ for the adversary's attack success probability. As a result, the proposed protocol not only can provide high-space efficient based on a secure hash function and XOR operation, but also can provide strong security against the relay attacks because the adversary's attack success probability is optimized to $(5/8)^n$.

Keywords : RFID, Authentication, Distance Bounding Protocol, Relay Attacks, Mafia Fraud Attack, Terrorist Fraud Attack

1. 서 론

유비쿼터스 환경에서의 컴퓨팅 시스템은 사용자의 현재 상황이나 위치에 맞는 맞춤형 서비스를 제공하는 것이 목적이다. 특히 위치 추적을 통하여 합법적인 사용자로 위장한 공격자를 빨리 감지하여 권한이 부여되지 않은 서비스를 제공받을 수 없게 해야 한다[1].

일반적으로 RFID 장치나 비접촉식 스마트카드는 근접 인증(proximity authentication)을 위해 사용자의 위치나 상황을 이용하여 통신하게 된다[2-3]. 이러한 환경에 사용되는 수동형 RFID 태그(tag)는 자체 내장 배터리가 없으며, RFID 리더기(reader)에 의해 생성되는 전자기의 고주파로부터 필요한 전력을 수신 받아 동작한다. 대표적인 비접촉식 인터페이스들인 "proximity"(ISO 14443), "vicinity"(ISO 15693), "near field"(ISO 18092) 장치들은 대략 10센티미터에서 1미터 정도의 명목상의 작동 범위로 표준화 시켰다[4-6]. 오늘날 교통카드나 건물 내 접근통제 등에 광범위하게 사용되는 ISO 14443과 ISO 18092 타입의 수동형 RFID 태그들과 비접촉식 스마트카드들은 근접 인증 과정에서 악의적인 프록

† 정 회 원 : 대구대학교 기초교육원 컴퓨터과정 초빙교수
†† 종신회원 : 경일대학교 컴퓨터공학과 교수
††† 정 회 원 : 경북대학교 전자전기컴퓨터학부 연구교수
†††† 정 회 원 : 대구대학교 컴퓨터 · IT공학부 교수(교신저자)
논문접수 : 2010년 2월 24일
수 정 일 : 1차 2010년 4월 13일, 2차 2010년 5월 14일
심사완료 : 2010년 5월 18일

시(proxy) 태그와 리더기를 사용한 다양한 중계 공격(relay attacks)들에 취약함이 최근에 증명되었다. 이러한 중계 공격들은 RFID 프로토콜 스택(stack)의 응용 계층(application layer)에서 동작하는 암호학적 인증 프로토콜들(cryptographic authentication protocols)을 사용하여 방어할 수 있는 공격들이 아니다. 응용 계층에서 송수신 메시지들의 도착 시간들(arrival times)에 관한 정보는 응용 계층 이하의 하위 계층들에서 구현되어진 많은 동기화(synchronization), 충돌 회피(collision-avoidance), 복조(demodulation), 심볼-감지(symbol-detection), 오류-감지(error-detection), 그리고 재전송 메커니즘들(re-transmission mechanisms)에 의해서 이미 부분적으로 훼손이 되어질 수 있다. 따라서 이러한 문제들을 해결하기 위한 아주 효과적인 방어 대책으로 최근에 통신 프로토콜의 물리 계층(physical layer)에 적용하여 사용할 수 있는 경계 결정(distance-bounding) 프로토콜에 대한 연구가 활발히 연구되고 있다. 경계 결정 프로토콜의 목적은 공격자가 리더기인 검증자를 속이기 위한 다양한 중계 공격들을 방어할 수 있을 뿐만 아니라 합법적인 태그가 리더의 인식 반경 내에 실제 존재하는지 여부를 안전하게 감지할 수 있도록 하는 것이다.

이러한 근거리 RFID 시스템상에서 근접 인증에 사용되는 RFID 태그들은 경계 위조(distance fraud) 공격, 마피아 위조(mafia fraud) 공격, 테러리스트 위조(terrorist fraud) 공격과 같은 다양한 위치 기반 공격인 경계 위조(distance fraud)와 중계 공격에 취약하다. 중계 공격 시나리오는 다음과 같다. 먼저 공격자는 넓은 공간에서 RFID 기반 시도-응답 인증 프로토콜이 진행되는 동안 리더와 태그사이에 교환되는 정보의 중계를 위해 두 개의 트랜스폰더를 사용한다. 실제 리더와 공격자의 프록시 리더 장치에 인접해 있는 프록시 태그 장치는 실제 태그와 근접해 있으며, 실제 태그 소유자는 이 사실을 알지 못하게 된다. 이후 공격자의 프록시 리더는 정당한 태그와 통신하여 인증 정보를 획득하고, 획득한 인증 정보를 담고 있는 프록시 태그는 정당한 리더와 통신하게 된다. 결과로 프록시 태그로부터 수신된 인증 데이터를 실제 리더가 잘못 인증을 하게 되어 리더는 실제적으로는 멀리 떨어져있는 합법적인 태그 대신 프록시 태그의 존재를 검증하게 되는 것이다[7].

위와 같은 중계 공격들에 대한 해결책으로 2005년에 Hancke과 Kuhn은 해쉬 함수 기반의 효율적인 RFID 경계 결정 프로토콜을 제안하였다[8]. 하지만 Hancke-Kuhn 프로토콜은 공격자에게 n번의 왕복에서 $(3/4)^n$의 성공 확률을 제공하여 중계 공격을 완벽히 방어할 수는 없다. 따라서 본 논문에서는 공격자에게 n번의 왕복에서 $(5/8)^n$의 성공 확률을 제공하는 새로운 경량 RFID 경계 결정 프로토콜을 제안한다. 결론적으로 제안한 프로토콜은 안전한 해쉬 함수와 XOR 연산을 기반으로 하여 높은 저장 공간 효율성을 제공할 뿐만 아니라, 공격자의 성공 확률을 $(5/8)^n$으로 최적화하여 중계 공격에 대해서도 안전하다.

본 논문의 구성은 다음과 같다. 2장에서는 연구 배경으로 경계 결정 프로토콜의 시초인 Brands-Chaum 프로토콜과 중계 공격의 유형 및 현재까지 연구되어져 오고 있는 다양한 RFID 경계 결정 프로토콜들의 장단점에 대하여 기술하고, 3장에서는 Hancke-Kuhn의 RFID 경계 결정 프로토콜에 대하여 간단하게 재검토한다. 4장에서는 제안한 경계 결정 프로토콜에 대해 설명하고, 5장에서는 안전성과 효율성을 비교하고, 6장에서 본 논문의 결론을 맺는다.

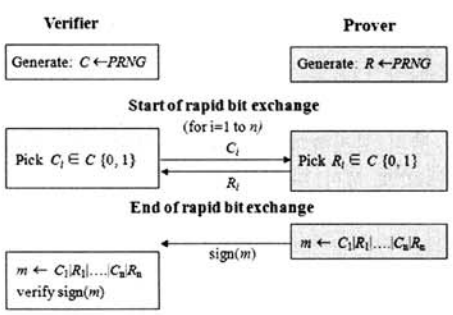
2. 연구 배경

2.1 Brands-Chaum의 경계 결정 프로토콜

Desmedt[9-11]등은 송수신 메시지의 왕복 시간 측정을 기반으로 경계 결정 개념을 최초로 소개하여 마피아 위조 공격에 대한 보안 대책으로 활용 가능함을 증명하였다. 그리고 1993년에 Brands와 Chaum[12]은 Desmedt의 아이디어를 기반으로 경계 프로토콜을 처음으로 설계하여 시도-응답 기반 암호 프로토콜에서 단일 비트 왕복 중계 시간을 측정하는 경계 결정 프로토콜에 대해서 소개하였다.

Brands-Chaum의 경계 결정 프로토콜에서, 검증자(verifier)가 1비트를 전송하는 시점에 타이머가 시작되며, 증명자(prover)가 검증자에게 응답 값으로 1비트를 전송하면 타이머는 중지한다. 이를 빠른 비트 교환 단계(rapid bit exchange phase)라고 한다. 검증자는 비트 전달 시간을 측정하기 위해 왕복 시간 측정 기법인 RTT(Round Trip Time)를 사용하여 실제 검증자 반경 내에 증명자가 존재하는 지를 검증하게 된다.

(그림 1)에서는 Brands와 Chaum[10]이 제안한 경계 결정 프로토콜 검증 수행과정을 보여준다. Brands -Chaum의 경계 결정 프로토콜에서는 검증자(verifier)와 증명자(prover)는 먼저 난수 비트 스트링인 $C = C_1 C_2 \ldots C_n$와 $R = R_1 R_2 \ldots R_n$을 각각 생성한다. 그러고 나서 검증자는 하나의 요청 비트인 $C_i (i = 1, \ldots, n)$를 한 번에 1비트씩 전송하고, 증명자는 R_i를 가지고 즉시 응답한다. 검증자는 각 비트 C_i의 전송과 그에 대응하는 응답 비트 R_i의 수신 사이의 시간을 왕복 중계 시간으로 기록한다. 모든 n비트가 교환된 후에 증명자는 두 개의 비트 스트링인 C와 R을 위해 메시지 인증 코드 또는 디지털 서명을 전송하여 검증함으로써 프로토콜을 종료한다.



(그림 1) Brands-Chaum의 경계 결정 프로토콜

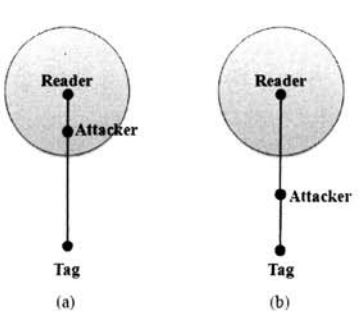
2.2 중계 공격 유형

RFID 시스템은 리더와 태그 사이에서 경계와 관련된 다양한 위치 기반 공격에 취약하다. 악의적인 태그는 정당한 태그보다 더 근접한 곳에서 리더에게 인증을 요구하게 되는데, 이를 경계 위조(distance fraud) 또는 중계(relay) 공격이라 한다. 이러한 중계 공격은 다시 마피아 위조(mafia fraud) 공격과 테러리스트 위조(terrorist fraud) 공격의 두 가지 형태의 중계 공격으로 나눌 수 있다. 그중에서 마피아 위조 공격은 리더와 태그에게 어떠한 예고도 없이 공격을 가할 수 있기 때문에 가장 심각한 공격으로서 중간자(man-in-the-middle) 공격과 같은 종류로 수행되는 공격이다. RFID 시스템에서 리더와 태그는 데이터 교환을 위해 반드시 통신해야 하므로 이러한 중계 공격은 예방하기가 매우 어렵다.

(그림 2)는 경계 결정 프로토콜에서 마피아 위조 공격과 테러리스트 위조 공격의 경계를 위한 시나리오를 보여준다. (a) 시나리오에서는 공격자가 리더의 경계 내에 존재하고, 리더는 공격자가 경계 내에 존재하는지 인식할 수 없으므로 공격자를 인증하게 된다. 따라서 이 공격의 유형은 마피아 위조 공격이라 한다. (b) 시나리오에서는 공격자가 리더의 경계 내에 존재하지 않지만 정당한 태그와 공모하여 리더에게 인증을 요청한다. 그러므로 이 공격의 유형은 테러리스트 위조 공격이라 한다. 두 가지의 중계 공격 유형에 대한 자세한 내용은 다음과 같다.

(1) 마피아 위조 공격(mafia fraud attack): 마피아 위조 공격은 Desmedt[9]에 의해 처음으로 기술되었다. 이 공격 시나리오에서는 리더와 태그 둘 다 정당하지만, 공격자는 정당한 리더의 경계 내에 존재하여 리더와 태그 사이에서 악의적인 리더와 태그를 사용하여 중간자 공격을 수행한다. 악의적인 태그는 정당한 리더와 통신하고, 악의적인 리더는 정당한 태그와 통신한다. 악의적인 태그와 리더는 서로 협력하며, 악의적인 태그는 실제로 비밀 정보에 대한 어떠한 것을 알 필요도 없이 정당한 태그의 비밀 정보에 관련된 진술서를 사용하여 리더와 인증하게 된다.

(2) 테러리스트 위조 공격(terrorist fraud attack): 테러리스트 위조 공격은 마피아 위조 공격에서 확장된 공격이다. 이 공격에서는 정당한 태그가 공격자의 악의적인 태그와 협력하여 인증을 한다. 악의적인 태그는 근접해 있는 리더와 인증하기 위해 정당한 태그와 공모하고, 악의적인 태그는 정당한 태그의 비밀 키나 프라이버시를 알지 못하더라도 상관없다.



(그림 2) 마피아와 테러리스트 위조 경계 시나리오

위 두 가지 공격 중에서 마피아 위조 공격은 공격자가 리더의 경계 내에 근접해 있으므로 리더와 태그 둘 다에게 어떠한 예고도 없이 공격한다. 따라서 마피아 위조 공격은 매우 심각한 공격이며 이 공격을 방지하기 위해 많은 연구들이 진행되고 있다[8, 12-19].

2.3 RFID 경계 결정 프로토콜에 관한 연구들

RFID 경계 결정 프로토콜은 인증(authentication) 기능과 경계 측정(distance measuring) 기능을 모두 포함하고 있다. 본 절에서는 현재까지 제안된 RFID 경계 결정 프로토콜들의 특징과 장단점을 간략히 살펴본다[8, 12-19].

현재까지 제안된 대표적인 RFID 경계 결정 프로토콜들 중 2005년에 Hancke-Kuhn[8]이 빠른 시도-응답 라운드로 구성된 RFID 경계 결정 프로토콜을 제안하였으며, 태그와 리더간의 거리 측정은 각 라운드에서 리더에 의해 수행하도록 설계하였다. 하지만 Hancke-Kuhn 프로토콜은 공격자에게 n번의 왕복에서 $(3/4)^n$의 성공 확률을 제공하여 위의 마파아 공격 또는 테러리스트 위조 공격과 같은 중계 공격들을 완벽히 방어할 수는 없는 문제점을 가진다.

2007년에 Reid 등[14]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 프로토콜은 태그와 리더의 식별자(ID)가 평문으로 송수신되어 익명성을 보장할 수 없을 뿐만 아니라 위치 추적 공격에도 취약함이 증명되었다[13]. 또한 Reid 등이 제안한 프로토콜은 공격자에게 n번의 왕복에서 $(7/8)^n$의 성공 확률을 제공하여 Hancke-Kuhn 프로토콜의 $(3/4)^n$의 성공 확률과 비교하였을 때 공격자의 성공 확률이 더 높아 안전하지 않은 문제점을 가진다.

2007년에 Meadows 등[15]은 중계 공격을 방어하기 위해 n번의 빠른 시도-응답 라운드를 요구하는 Hancke-Kuhn의 프로토콜과 Reid 등이 제안한 프로토콜과는 달리 단지 1-라운드 경계 결정 단계만을 수행하는 효율적인 RFID 경계 결정 프로토콜을 제안하였다. 하지만 Meadows 등이 제안한 프로토콜도 Reid 등의 프로토콜과 마찬가지로 태그와 리더의 식별자 정보가 평문상태로 송수신되어 공격자에 의해 태그 및 리더 추적에 쉽게 노출됨으로써 프라이버시(privacy) 보호를 제공하지 않는 취약점들이 존재한다는 것이 증명되었다[13]. 또한 경계 결정 단계에서 어떠한 비밀 키 정보도 포함되어 있지 않아 태그의 모든 기밀 정보들을 공격자가 공유하여 악의적인 태그에 의한 테러리스트 위조 공격이 가능함이 증명되었다[13].

2007년에 Singelee와 Preneel[16]는 노이즈(noisy) 환경을 고려한 n번보다 적은 시도-응답 라운드를 요구하는 통신 시간 효율적인 새로운 RFID 경계 결정 프로토콜을 제안하였다. 하지만 2010년에 Munilla와 Peinado[17]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.

2008년에 Nikov와 Vauclair[18]는 기존의 RFID 경계 결정 프로토콜이 가지는 익명성 및 보안성 문제를 개선한 새로운 RFID 경계 결정 프로토콜을 제안하였다. 하지만 Hancke-Kuhn 프로토콜과 비교하여 Nikov-Vauclair의 프로토콜은 n번보다 높은 시도-응답 라운드를 필요로 할 뿐만 아니라 태그가 HAMC이나 AES를 함수를 사용하여 2K 비밀키를 생성 및 저장해야하는 비효율적인 문제를 가진다[19].

위의 관련 연구를 기반으로 본 논문에서는 현재까지 제안되어져 오고 있는 많은 RFID 경계 결정 프로토콜들 가운데 Hancke-Kuhn의 RFID 경계 결정 프로토콜이 안전성 측면에서 가장 안전하다고 판단하여 Hancke-Kuhn의 RFID 경계 결정 프로토콜 분석 및 비교를 통하여 공격자의 중계 공격 성공 확률을 더욱더 줄여줄 뿐만 아니라 태그 측 연산 및 저장 공간 측면에서도 효율적인 새로운 RFID 경계 결정 프로토콜을 제안한다.

3. Hancke-Kuhn의 RFID 경계 결정 프로토콜

본 장에서는 Hancke-Kuhn[8]이 제안한 RFID 시스템 환경을 고려한 해쉬 함수 기반의 효율적인 RFID 경계 결정 프로토콜을 소개한다.

3.1 용어 정의

본 논문에서 사용할 용어들의 표기법 및 정의는 <표 1>과 같다.

〈표 1〉 용어 정의

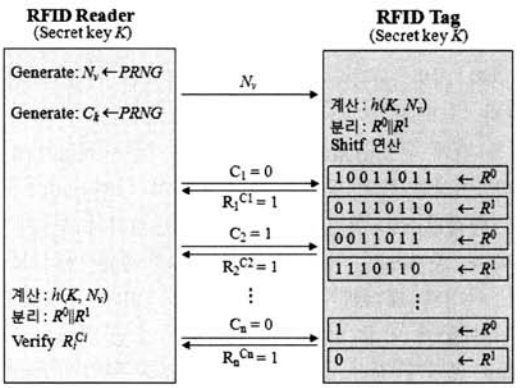
기호	의 미
C, N_V	난수
K	비밀 값
h	안전한 해쉬 함수(secure hash function)
$PRNG$	의사난수생성기(Pseudo Random Number Generator)
$\oplus$	배타적 논리합(XOR; eXclusive OR) 연산
$\|$	연접(concatenation) 연산
Δt	단일 비트 왕복 전송 시간
$t_{\max}$	상위 경계 결정 값

3.2 프로토콜 설명

(그림 3)은 Hancke-Kuhn가 제안한 RFID 경계 결정 프로토콜의 전체적인 구성과 동작 과정을 보여주며, 아래와 같은 과정으로 수행된다.

(1) 리더 → 태그: N_V

RFID 리더는 태그에게 난수 N_V를 전송한다.



(그림 3) Hancke-Kuhn의 RFID 경계 결정 프로토콜

(2) 태그는 수신한 난수 N_V, 비밀 키 K 그리고 함수 $h()$를 사용하여 $h(K, N_V)$를 계산한 후 다음과 같이 n 비트 순서열 R^0와 R^1 값으로 분리한다.

$$R_1^0 R_2^0 R_3^0 \ldots R_n^0 \| R_1^1 R_2^1 R_3^1 \ldots R_n^1 := h(K, N_V)$$

이때 리더도 태그와 동일하게 자신이 생성한 난수 N_V, 비밀 키 K 그리고 함수 $h()$를 사용하여 $h(K, N_V)$를 계산한 후 동일한 n 비트 순서열 R^0와 R^1 값으로 분리한다.

(3) 리더 → 태그: C_i

리더는 랜덤 비트열 C_k를 생성하고, 클럭 사이클에서 정의된 비트열 값 n을 기반으로 단일 비트 시도-응답 교환을 순차적으로 시작한다. 먼저 리더는 태그에게 $C_i (1 \le i \le n)$를 전송한다.

(4) 태그 → 리더: $R_i^{C_i}$

태그는 리더로부터 수신한 C_i 값에 의해 선택된 R_i^0 또는 R_i^1 둘 중 하나에 해당하는 $R_i^{C_i}$의 왼쪽 1비트 값을 리더에게 바로 전송한다. 이때, $C_i = 0$ 이면 R^0의 1비트를 전송하고, $C_i = 1$ 이면 R^1의 1비트를 전송한다. 이와 동시에 둘 중 전송되지 않은 값은 버리게 되고, R^0 와 R^1은 각각 1비트씩 왼쪽으로 이동 연산(shift register)을 수행한다.

(5) 리더는 태그로부터 수신한 $R_i^{C_i}$와 자신이 계산한 값이 일치하는지 검사한다. 이때 리더와 태그사이의 비트 왕복 전송 시간이 상위 경계 결정 값 이하로 측정된다면 리더와 태그가 인증된다.

4. 제안하는 경량 RFID 경계 결정 프로토콜

본 장에서는 공격자의 중계 공격 성공 확률을 $(5/8)^n$으로 최적화할 뿐만 아니라 리더와 태그의 저장 공간 효율성을 제공하는 경량 RFID 경계 결정 프로토콜을 제안한다.

4.1 프로토콜 설명

(그림 4)는 제안하는 경량 RFID 경계 결정 프로토콜의 전체적인 구성과 동작 과정을 보여주며, 다음과 같이 수행된다.

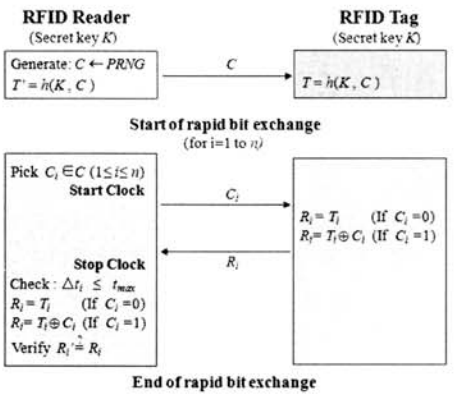
(1) 리더 → 태그: C
리더는 난수 C를 생성하여 태그에게 전송하고, 자신이 생성한 난수 C, 비밀 키 K 그리고 안전한 해쉬 함수 $h()$를 사용하여 $T' = h(K, C)$ 계산한 후 T' 값을 구한다.

(2) 태그는 리더로부터 수신한 난수 C, 비밀 키 K 그리고 안전한 해쉬 함수 $h()$를 사용하여 $T = h(K, C)$ 계산한 후 T값을 구한다.

(3) 리더 → 태그: C_i
리더는 자신이 생성한 난수 $C_i (1 \le i \le n)$를 태그에게 C_1부터 1비트씩 빠른 비트 전송을 시작한다.

(4) 태그 → 리더: R_i
태그는 리더로부터 수신한 C_i 값에 대한 응답 값으로 R_i를 전송하게 되는데, 이때 $C_i = 0$ 이면 $R_i = T_i$를, $C_i = 1$이면 T_i와 C_i를 XOR 연산을 수행한 R_i $(R_i = T_i \oplus C_i)$ 값을 리더에게 전송한다.

(5) 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 $R_i' = T_i'$로, $C_i = 1$이면 XOR 연산을 수행하여 $R_i' = T_i' \oplus C_i$ 값을 계산한다.



(그림 4) 제안한 경계 결정 프로토콜

4.2 검증 알고리즘 동작 원리 설명

앞 절에서 기술한 RFID 경계 결정 프로토콜의 단계 (5)에서의 단일 비트 왕복 전송 시간 추론 및 검증 알고리즘은 (그림 5)와 같다. 검증 루틴은 n비트만큼 수행하지만, 비트 왕복 전송 시간이 경계 결정 상위 값을 초과하게 되면 더 이상 루틴을 수행하지 않고 검증을 중단하게 된다.

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

(그림 5) 검증 알고리즘

또한, (그림 5)의 검증 알고리즘에서는 리더와 태그 간에 무선 통신을 수행하므로 잡음 환경을 고려하여 상위 경계 결정 값을 초과하는 최대 허용 오류 값으로 $count_{max}$를 설정하였고, t_{max}는 단일 비트 왕복 전송 시간인 $\Delta t_i = Rt_i - St_i$의 임계 값(threshold value)으로 설정하였다. 단일 비트 왕복 전송 시간($\Delta t_i = Rt_i - St_i$)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.

4.3 빠른 비트 교환 동작 과정 예시

(그림 6)은 본 논문에서 제안한 경계 결정 프로토콜의 단일 비트 왕복 시간 검증 및 인증을 위한 빠른 비트 교환(rapid bit exchange) 동작 과정 예시로서 수행 과정은 다음과 같다.

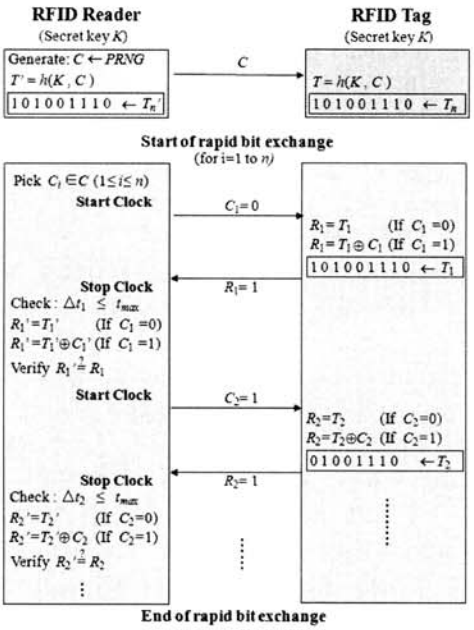
(1) 리더 → 태그: C
리더는 난수 C를 생성하여 태그에게 전송하고, 다음과 같은 $T' = h(K, C)$ 값을 계산한다.

$$\boxed{1\,0\,1\,0\,0\,1\,1\,1\,0 \leftarrow T_n'}$$

(2) 태그는 리더로부터 수신한 난수 C와 비밀키를 가지고 안전한 해쉬 함수 연산을 수행하여 아래와 같은 리더와 동일한 $T = h(K, C)$ 값을 계산한다.

$$\boxed{1\,0\,1\,0\,0\,1\,1\,1\,0 \leftarrow T_n}$$

(3) 리더 → 태그: $C_1 = 0$
리더는 난수 비트열 C 중에서 단일 비트인 $C_1 = 0$을 태그에게 전송함으로써 클럭(clock)이 시작된다.



(그림 6) 제안한 프로토콜에서의 빠른 비트 교환 예시

(4) 태그 → 리더: $R_1 = 1$

태그는 수신한 난수 C_1을 이용하여 응답 메시지 R_1을 아래 비교를 통해 구한다.

$$R_1 = T_1 \quad (\text{If } C_1 = 0)$$
$$R_1 = T_1 \oplus C_1 = 1 \oplus 1 = 0 \quad (\text{If } C_1 = 1)$$

위에서 태그가 리더로부터 수신한 난수는 $C_1 = 0$이므로 T_1의 값이 그대로 R_1 값이 되어 리더에게 응답한다. 만약 리더가 $C_1 = 1$을 태그에게 전송하면 태그는 $R_1 = T_1 \oplus C_1$인 XOR 연산을 수행하여 리더에게 $R_1 = 0$ 값을 전송하게 된다. 그러고 나서 T의 값은 1비트씩 왼쪽 이동 연산(shift register)을 한다.

(5) 리더는 태그로부터 응답 비트 값을 수신하면, $\Delta t_1 \leq t_{max}$와 같이 비트 왕복 전송 시간을 측정하여 상위 경계 결정 값을 초과하지 않았는지 검증한 후 리더로부터 수신한 값과 리더 자신이 계산한 값이 $R_i' = R_i$ 일치하는지 다음과 같이 검증한다.

$$\text{Check} : \Delta t_1 \leq t_{max}$$
$$R_1' = T_1' \quad (\text{If } C_1 = 0)$$
$$R_1' = T_1' \oplus C_1' = 1 \oplus 1 = 0 \quad (\text{If } C_1 = 1)$$
$$\text{Verify } R_1' \stackrel{?}{=} R_1$$

위와 같이 (1)~(5) 단계를 n 비트열까지 단일 비트 왕복 교환을 반복적으로 수행하고, 검증함으로써 리더와 태그가 인증하게 된다. 만약 비트 왕복 전송 시간 Δt가 상위 경계 결정 값 t_{max}보다 초과한 횟수가 $count_{max}$를 초과하게 되면 악의적인 리더나 태그의 공격으로 인식하고 더 이상 빠른 비트 교환을 수행하지 않고 검증을 중단한다.

5. 안전성과 효율성 분석

본 장에서는 제안한 경량 RFID 경계 결정 프로토콜에 대한 안전성과 효율성에 대해 분석한다.

5.1 안전성 분석

<표 2>는 Hancke-Kuhn의 RFID 경계 결정 프로토콜과 제안한 RFID 경계 결정 프로토콜이 마피아 위조 공격 및 테러리스트 위조 공격인 중계 공격에 대한 공격자가 공격에 성공할 확률을 비교한 표이다.

<표 2>에서 보여준 바와 같이 Hancke-Kuhn 경계 결정 프로토콜에서 안전한 해쉬 함수 $h()$는 난수 N_V와 키 K를 이용하여 시간 결정 시도-응답 단계 전에 태그에 의해서 연산한 후 두 개의 비트열로 분리한다. 그러므로 이렇게 획득한 모든 비트들에 대해 1/2의 비트만 리더에게 응답 값으로 전송하게 된다. Hancke-Kuhn 프로토콜의 n번의 고속 비트 교환 시도-응답 메시지 교환과정에서 공격자는 태그에게 제공된 클럭 신호의 속도를 약간 가속화시키고, 리더가 C_i를 전송하기 전에 공격자가 추측한 C_i'을 태그에게 전송할 수 있다. 이 상황에서 공격자가 $C_i' = C_i$인 요청 비트를 정확하게 추측할 수 있는 확률은 1/2이다. 또한, 공격자는 리더를 만족시키기 위해 필요로 하는 정확한 값 $R_i^{C_i}$를 획득하게 될 확률도 1/2이다. 이때 나머지 상황의 반인 즉 $C_i' \neq C_i$인 경우에서의 공격자가 정확한 응답 $R_i^{C_i}$를 다시 시도할 수 없도록 이동 연산을 사용하여 파괴시켜 버린다. 그런 경우 공격자는 모든 상황의 반에서 정확하게 추측한 비트를 가지고 응답할 수 있다. 그러므로 공격자는 요청한 C_i에 대해 정확하게 응답할 공격 성공 확률 계산은 다음과 같다.

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

따라서 Hancke-Kuhn 프로토콜에서 공격자가 모든 비트에 대한 n번의 요청에 대해 정확하게 응답할 확률은 $(3/4)^n$이다.

본 논문에서 제안한 경계 결정 프로토콜에서도 n번의 고속 비트 교환 시도-응답 과정동안 리더가 C_i를 전송하기 전에 공격자가 추측한 C_i'을 태그에게 전송할 수 있으며, 공격자가 $C_i' = C_i$인 요청 비트를 정확하게 추측할 수 있는

〈표 2〉 경계 결정 프로토콜의 안전성 비교

프로토콜 / 공격유형	Hancke-Kuhn 프로토콜	제안 프로토콜
마피아 위조 공격 성공 확률	$\left(\frac{3}{4}\right)^n$	$\left(\frac{5}{8}\right)^n$
테러리스트 위조 공격 성공 확률	$\left(\frac{3}{4}\right)^n$	$\left(\frac{5}{8}\right)^n$

확률은 1/2이다. 그러나 제안한 프로토콜의 고속 비트 교환의 (4)단계에서 태그는 리더로부터 수신한 C_i 값에 대한 응답 값으로 R_i를 전송하게 되는데, 만약 $C_i=0$ 이면 $R_i=T_i$를, $C_i=1$이면 T_i와 C_i를 XOR 연산을 수행한 랜덤한 $R_i(R_i=T_i\oplus C_i)$ 값을 리더에게 전송하게 된다. 여기에서 T_i 값은 태그가 리더로부터 수신한 난수 C, 비밀 키 K, 안전한 해쉬 함수 h를 사용하여 계산한 값이고, $C_i=1$일 경우에는 C_i와 T_i를 XOR 연산을 수행하게 되므로 공격자가 리더를 만족시키기 위해 필요로 하는 C_i에 대응하는 정확한 값 R_i를 획득하게 될 공격 성공 확률 계산은 다음과 같다.

$$(1\times\frac{1}{2})+(\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2})=\frac{5}{8}$$

결국 공격자는 모든 n 번의 요청에 대해 정확하게 응답할 확률은 단지 $(5/8)^n$이라는 점이다. 따라서 본 논문에서 제안한 경계 결정 프로토콜이 중계 공격에 더욱더 안전하다는 것을 증명한다.

5.2 효율성 분석

본 절에서는 제안한 경계 결정 프로토콜의 효율성에 대해 살펴본다. <표 3>은 제안한 경계 결정 프로토콜과 Hancke-uhn의 경계 결정 프로토콜의 효율성을 비교한 표이다.

Hancke-Kuhn 프로토콜은 리더측에서 2번의 난수를 생성하고, 제안한 프로토콜은 1번의 난수만을 생성한다. 해쉬 연산은 두 프로토콜 모두 태그와 리더 측에서 각각 1번씩의 연산을 요구하며, XOR 연산은 제안한 프로토콜에서만 C_i가 0일 경우에 XOR 연산을 수행하여 응답 값으로 전송되므로 리더와 태그에서 각각 최대 n번보다 적은 연산량이 요구된다. 비트열의 저장 공간은 Hancke-Kuhn 프로토콜에서 태그와 리더 모두 해쉬 연산 후에 비트열을 분리시키므로 각각 $2n$비트의 공간이 요구되지만, 제안한 프로토콜에서는 비트열 분리 연산이 수행되지 않으므로 태그와 리더 각각 n비트의 공간만이 요구된다. 또한 Hancke-Kuhn 프로토콜에서는 해쉬 값이 두 개의 n비트로 분리됨으로써 shift 연산도 제안한 프로토콜보다 2배나 많은 연산량이 요구된다. 따라서 XOR 연산량을 제외한 모든 연산량에서 제안한 프로토콜이 훨씬 우수함을 알 수 있다. 비록 제안한 프로토콜에서는 XOR 연산이 리더와 태그 측에서 수행되지만 빠른 속도로 XOR 비트 연산을 수행하기 때문에 경량 RFID 시스템에서 매우 적합하다. 무엇보다 본 논문에서 제안한 프로토콜에서는 RFID 태그측의 저장 공간을 반으로 줄여주어 높은 저장 공간 효율성을 제공할 수 있다. 결론적으로 제안한 프로토콜은 Hancke-Kuhn 프로토콜보다 훨씬 더 효율적이라는 것을 알 수 있으며 경량 RFID 시스템에 더욱 실용적으로 사용될 수 있다. 또한, 제안한 프로토콜은 Hancke-Kuhn 프로토콜과는 달리 리더와 태그 간에 더 적은 수의 통신 메시지량을 사용한다. 위와 같은 이유로 본 논문에서 제안한 RFID 경계 결정 프로토콜이 Hancke-Kuhn 프로토콜보다 효율성 면에서도 훨씬 더 우수함을 명백하게 보여준다.

〈표 3〉 경계 결정 프로토콜의 효율성 비교

프로토콜 / 연산종류	Hancke-Kuhn 프로토콜[8]		제안한 프로토콜	
	태그	리더	태그	리더
난수 생성수	0	2	0	1
해쉬 연산량	1	1	1	1
XOR 연산량	0	0	n	n
저장공간 (bit수)	$2n$	$2n$	n	n
Shift 연산수	$2n$	0	n	0
(‖) 연산량	1	1	0	0
리더와 태그간 통신메시지량	$2Rn+2h()+2(\|\|)$ $+4nbit+2nSR$		$2Rn+2h()+2nXOR$ $+2nbit+nSR$	

n : 비트열 개수
Rn : 일회성 난수 개수
$h()$: 해쉬 연산 개수
SR : Shift 연산 개수
(‖) : 분리 연산 개수

6. 결 론

본 논문에서는 근접 인증에 사용되는 수동형 RFID 태그 환경에서 발생되는 중계 공격들을 방어할 수 있으며 기존의 연구와 비교하여 안전성과 효율성을 보장하는 경량 RFID 시스템 인증을 위한 새로운 RFID 경계 결정 프로토콜을 제안하였다. 공격자에게 n번의 왕복에서 $(3/4)^n$의 성공 확률을 제공하는 Hancke-Kuhn 프로토콜과 비교하여 제안한 프로토콜은 공격자의 성공 확률을 $(5/8)^n$으로 최적화하였다. 또한 안전한 해쉬 함수와 XOR 연산을 기반으로 하여 저장 공간의 효율성을 높여주어 수동형 저비용 태그와 잡음 환경 그리고 고속 애플리케이션에서의 사용에 매우 적합하도록 설계하였다.

향후 연구로는 리더가 랜덤 비트열의 단일 비트 전송에서 전송할 비트가 0일 경우에는 void를 전송하고, 태그 역시 void를 수신하면 void로 리더에게 응답함으로써 공격자의 중계 공격 성공 확률을 절반 이하로 감소시키는 것을 목표로 둔다.

참 고 문 헌

[1] S. ˇCapkun and J. Hubaux. Secure positioning of wireless devices with application to sensor networks, IEEE INFOCOM 2005. http://lcawww.epfl.ch/capkun/secpos.pdf

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

[3] J.E. Bardram, R.E. Kjær and M.Ø. Pedersen. Context-aware user authentication-Supporting proximity-based login in pervasive computing, UbiComp 2003, LNCS 2864, pp.107-123, Spring-Verlag 2003.

[4] ISO 14443. Identification cards-contactless integrated circuit

cards-proximity cards. International Organization for Standardization, Geneva.
[5] ISO 15693. Identification cards-contactless integrated circuit cards-vicinity cards. International Organization for Standardization, Geneva.
[6] 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.
[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), pages 67-73. IEEE Computer Society, 2005.
[9] Y. Desmedt. Major security problems with the "Unforgeable" (Feige)-Fiat-Shamir proofs of identity and how to overcome them. In SecuriCom'88, pp.15-17, 1988.
[10] 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.
[11] Thomas Beth and Yvo Desmedt, Identification tokens-or: Solving the chess grandmaster problem. In CRYPTO, pages 169-177. Springer Verlag, 1990.
[12] S. Brands and D. Chaum, Distance-bounding protocols, Advances in Cryptology EUROCRYPT'03, Springer-Verlag LNCS 765, pp 344-59, May, 1993.
[13] Y.-J. Tu and S. Piramuthu, RFID distance bounding protocols, In the 1st International EURASIP Workshop in RFID Technology. Vienna, Austria.
[14] 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.
[15] 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.
[16] 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.
[17] J. Munilla and A. Peinado, Attacks on a distance bounding protocol, Computer Communications, Vol.33, No.7, 2010, pp.884-889.
[18] V. Nikov and M. Vauclair. Yet another secure distance-bounding protocol. Available at http://eprint.iacr.org/2008/319. An earlier version appears in SECRYPT 2008.
[19] C. Kim, G. Avoine, F. Koeune, F, Standaert, and O. Pereira, Pereira, The swiss-knife RFID distance bounding protocol, Information Security and Cryptology-ICISC 2009, pp.98-115, Springer-Verlag, 2009.

안 해 순

e-mail : ahs221@hanmail.net
1996년 경일대학교 컴퓨터공학과(공학사)
2001년 경일대학교 컴퓨터공학과(공학석사)
2010년 대구대학교 컴퓨터정보공학과(공학박사)
2004년~2008년 경일대학교 컴퓨터공학부 전임강사
2008년~현 재 대구대학교 기초교육원 컴퓨터과정 초빙교수
관심분야 : 데이터베이스, 정보보안, 정보검색, 데이터베이스 보안, RFID 보안

부 기 동

e-mail : kdbu@kiu.ac.kr
1984년 경북대학교 전자공학과(공학사)
1988년 경북대학교 전자공학과(공학석사)
1996년 경북대학교 전자공학과(공학박사)
1983년~1985년 포항종합제철 시스템개발실
2001년~2002년 일본 게이오대학 방문교수
1988년~현 재 경일대학교 컴퓨터공학과 교수
관심분야 : 데이터베이스, GIS, 시멘틱 웹, 데이터베이스 보안, RFID 보안

윤 은 준

e-mail : ejyoon@knu.ac.kr
2003년 경일대학교 컴퓨터공학과(공학석사)
2007년 경북대학교 컴퓨터공학과(공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2008년~현 재 경북대학교 전자전기컴퓨터학부 연구교수
2007년~현 재 보안공학연구지원센터 보안공학논문지 편집위원
관심분야 : 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

남 인 길

e-mail : ignam@daegu.ac.kr
1978년 경북대학교 전자공학과(공학사)
1981년 영남대학교 전자공학과(공학석사)
1992년 경북대학교 전자공학과(공학박사)
1978년~1981년 대구은행 전산부
1980년~1990년 경북산업대학 부교수
1990년~현 재 대구대학교 컴퓨터·IT공학부 교수
관심분야 : 데이터베이스, 데이터베이스 보안, RFID 보안