논문 14-39A-11-05 The Journal of Korean Institute of Communications and Information Sciences '14-11 Vol.39A No.11
http://dx.doi.org/10.7840/kics.2014.39A.11.660

테러리스트 공격과 마피아 공격에 안전한 RFID 거리 제한 프로토콜

권 혜 진•, 김 순 자°

RFID Distance Bounding Protocol Secure Against Mafia and Terrorist Fraud

Hye Jin Kwon•, Soon Ja Kim°

요 약

RFID 시스템은 무선 식별이라는 장점으로 인해 다양한 서비스에 사용되고 있다. 그러나 서비스에 무임승차하거나 자산, 개인정보 탈취를 위한 공격들이 알려지고 있어 그 해결책에 대한 연구도 활발하다. 그 중 중계 공격의 일종인 마피아 공격은 먼 거리에 있는 태그와 리더의 메시지를 중간에서 전달만 하여 인증에 성공할 수 있는 공격으로 일반적인 보안 프로토콜로는 방어할 수 없다. 이에 Hancke와 Kuhn은 거리 제한 프로토콜을 RFID 태그와 리더의 인증에 적용하였다. 그 이후 Munilla와 Peinado는 Hancke와 Kuhn의 프로토콜에 무요청를 추가하여 공격자의 마피아 공격 성공 확률을 낮춘 거리 제한 프로토콜을 제안하였다. Ahn et al.은 Munilla와 Peinado의 프로토콜보다 통신량과 해시 연산량을 줄인 프로토콜을 제안하였다. 본고에서는 Munilla와 Peinado의 프로토콜이 테러리스트 공격에 취약하고, 카운터를 사용하여 잡음을 고려하였음에도 불구하고 잡음이 생길 경우 비동기로 인해 더 이상의 인증이 불가함을 밝힌다. 또, Ahn et al.의 프로토콜이 마피아 공격과 키 노출에 취약함을 밝히고, 이 취약점들을 개선하여 테러리스트 공격과 마피아 공격에 안전하고 잡음을 고려한 프로토콜을 제안하며, 기존 프로토콜과 제안 프로토콜의 안전성, 효율성을 비교분석한다.

Key Words : RFID authentication protocol, distance bounding protocol, mafia fraud, terrorist fraud

ABSTRACT

RFID system has been used in a variety of services. So, a lot of attacks like a free ride on the service, leakage of property or personal information are known. Therefore, the solutions that address these attacks have been proposed. Among the attacks, mafia fraud, a kind of relay attack, can not be addressed by common authentication protocol. So, Hancke and Kuhn used distance bounding protocol for RFID authentication. After that, Munilla and Peinado modified HK protocol by adding void challenge. So the mafia fraud success probability of adversary is lower than probability of HK protocol. Ahn et al. proposed a protocol that reduces number of a hash computation and traffic than MP protocol. Here, we show that MP protocol can not defend the terrorist fraud and is vulnerable to noise. And we show that also AYBN protocol is vulnerable to mafia fraud and key leakage. Moreover, we propose a new protocol and our experimental results show that our protocol is secure to terrorist and mafia fraud.

※이 논문은 2012학년도 경북대학교 학술연구비에 의하여 연구되었음.
• First Author : College of IT Engineering, Kyungpook National University, heyjk90@gmail.com, 학생회원
° Corresponding Author : College of IT Engineering, Kyungpook National University, sjkim@ee.knu.ac.kr, 종신회원
논문번호 : KICS2014-10-431, Received October 24, 2014; Revised November 11, 2014; Accepted November 11, 2014

Ⅰ. 서 론

RFID(Radio Frequency Identification) 시스템은 무선 채널을 통해 RFID 태그(tag)의 정보를 인식하는 시스템이다. 무선 인식의 장점으로 인해 기존의 인식 시스템인 바코드보다 다양한 서비스에 활용되고 있다. 도서관이나 병원, 기업 등의 기관에 RFID 시스템을 도입할 경우 도난 방지, 자산의 위치 파악 등 자산 관리가 용이하고, 항공 수하물 관리에 사용될 경우 수하물의 관리 및 위치 추적이 가능하다. 또, 출입 통제, 출석 관리 등의 출입 관리와 교통카드 등의 전자 지불 서비스를 비접촉 방식으로 제공할 수 있다[1-4].

이런 응용의 대부분은 프로토콜이 사칭에 안전하고, 무선 환경에서의 제한된 통신 범위로 인해 통신이 가능한 기기는 물리적으로 근접하다는 가정에 기초하여 서비스를 제공한다. 실제로 RFID 리더(reader)의 인식 영역은 고주파(HF, High-frequency) 태그의 경우 10cm에서부터 10m인 극초단파(UHF, Ultrahigh-frequency) 태그까지 상대적으로 근거리로 볼 수 있다[5]. 도서 위치 파악 서비스를 예로 들면, 바코드 시스템에서는 도서가 지정된 곳에 배치되어 있지 않으면 해당 도서의 위치 파악이 어렵지만, RFID 시스템을 도입한 경우에는 도서가 지정된 곳에 없더라도 해당 도서에 부착된 RFID 태그의 정보를 수신한 리더 근방에 있는 것으로 파악할 수 있다. 또, RFID 기반 도난 방지 서비스에서는 리더가 고가의 물품에 부착된 RFID 태그에게 인증 메시지를 보내고 그 응답이 올바르게 온다면 해당 물품이 잘 보관되고 있는 것으로 파악할 수 있다. 만약 응답이 오지 않거나 올바르지 않을 경우, 물품이 해당 위치에 없어 도난당했거나 통신에 이상이 있는 등의 문제가 발생했다고 볼 수 있다.

그러나 이런 가정을 악용하는 마피아 공격이 [6]에서 처음 제안되었다. 마피아 공격은 메시지 내용에 대해 전혀 모르는 공격자가 먼 거리에 있는 정당한 리더와 태그 사이에서 오가는 메시지를 그대로 전달(relay)하여 인증 프로토콜에서 성공적으로 인증 받는 공격이다. [6]은 RFID 프로토콜을 공격한 것이 아니라 Fiat-Shamir 프로토콜을 공격한 것이지만 RFID의 지불 서비스에도 다음과 같이 적용하여 공격할 수 있다[7]. 이 공격은 RFID 리더와 태그를 가진 공격자 두 명으로 구성되며, 이 공격을 통해 타인의 RFID 카드(태그)를 통해 고가의 물건을 구입하고자 한다. RFID 태그를 가진 공격자 A_1은 상점에, 리더를 가진 또 다른 공격자 A_2는 RFID 카드 소유자 근방에 위치한다. 상점에서 공격자 A_1이 고가의 물품을 구입하려 할 때, 상점의 RFID 리더는 고객으로 보이는 공격자 A_1에게 챌린지(challenge)를 보낸다. 공격자 A_1은 리더의 챌린지를 받자마자 공격자 A_2에게 챌린지를 전달하고, A_2는 그 챌린지를 그대로 RFID 카드에게 보내면 태그는 반사적으로 챌린지에 응답한다. A_2는 즉시 이 응답을 A_1에게 보내고 A_1은 상점의 리더에게 그 응답을 전송한다. 이 응답이 정당한 태그가 보낸 값과 일치하기 때문에 리더는 공격자 A_1을 정당한 태그 소유자로 간주하고, 결제 과정을 진행한다. 이 시나리오는 비단 지불 서비스 뿐 아니라 출입 통제, 도난 방지 서비스 등에도 똑같이 적용할 수 있다.

위와 같은 공격이 발생한 이유는 리더가 인증하려는 상대방 A_1이 인증 메시지를 생성하지 않았는데도 불구하고, 리더는 메시지의 정당성만 확인할 뿐 메시지 생성자가 A_1인지를 확인하지 않았기 때문이다. Desmedt는 이런 마피아 공격을 방어할 방법으로 [6]에서 인증 받으려는 참가자(prover)가 검증자(verifier)에게 자신의 물리적인 위치를 포함한 메시지를 생성하고 그에 서명하는 방법을 제안하였다. 그러나 이는 인증 받으려는 참가자가 GPS 장치와 같은 물리적인 위치 판단 기능을 가지고 있어야 한다는 점으로 인해 RFID 태그에 적용하기는 어렵다. 그 이후, [8]에서는 통신을 할 때, 외부의 통신 간섭을 피하기 위해서 패러데이 상자(Faraday cage)와 같은 차폐막을 사용할 것을 제안했다. 그러나 이 또한 RFID 시스템의 장점인 비접촉 인식을 불가능케 하여 RFID 시스템에서 활용되기는 어렵다. 이에 Brands와 Chaum는 거리 제한 프로토콜(distance bounding protocol)을 제안하였다[9]. 거리 제한 프로토콜은 한 비트의 챌린지와 응답을 n라운드 동안 빠르게 진행하여 RFID 리더가 메시지 왕복 시간(RTT, Round Trip Time)을 통해 태그의 물리적인 위치의 상한선을 결정할 수 있도록 하였다. 만약 거리의 상한선이 기준보다 클 경우, 인증을 거부 하여 마피아 공격을 막을 수 있다.

2005년 Hancke와 Kuhn는 RFID 시스템을 위해 경량화한 거리 제한 프로토콜을 제안했다. 그 이후, 마피아 공격 성공 확률을 낮추고 보다 효율적이고 경량화한 거리 제한 프로토콜을 위한 연구가 많이 이루어지고 있다. 2장에서는 이런 연구 결과들과 RFID 시스템의 보안 요구 조건을 소개하고 분석한다. 3장에서는 2장에서 제시한 보안 요구 조건과 이전의 프로토콜의 문제점을 보완한 새로운 프로토콜을 제안한 후 비교 분석

하고 4장에서 결론을 맺는다.

Ⅱ. 연구 배경

RFID 시스템은 서버, RFID 리더, RFID 태그로 구성되고, RFID 태그는 특정한 물품이나 동물 등에 장착되어 해당 물품에 대한 식별 정보를 저장한다. 리더는 무선으로 태그를 인식하고 자체적으로 데이터베이스가 있어 정보를 파악하거나, 자체적인 데이터베이스가 없는 경우에는 서버에게 식별 정보를 보내 해당 태그의 정보를 얻는다. 이 시스템은 식별의 간편성으로 인해 다양한 분야에 활용되고 있는데 서비스마다 보안 요구 조건이 다르다. 2003년 SARS 확산 방지를 위해 싱가포르의 병원에서 도입한 RFID 시스템에서는 자산에만 태그를 부착하는 것이 아니라 환자와 방문객, 병원 직원이 RFID 태그를 소지하였다[10]. 이런 시스템에서는 환자나 직원의 프라이버시 보호를 위해 공격자에 의한 위치 추적에 안전한 프로토콜을 선택해야 한다. 그러나 재고 관리나 수화물 관리 등과 같이 사물에 태그를 부착할 경우 위치 프라이버시가 그다지 요구되지 않고 도난 방지 및 정확한 위치 파악을 위해 마피아 공격에 대한 안전성이 더욱 요구 된다. 이런 다양한 서비스 중에서 본고에서는 도난 방지, 자산 및 수화물 관리 등 물품에 태그를 부착하는 환경으로 제한하여 RFID 시스템의 보안 요구 조건과 기 제안된 프로토콜을 분석한다.

2.1 보안 요구 조건

RFID 시스템에서 보안 요구 조건은 크게 사칭에 대한 안전성과 개인 프라이버시 보장으로 나눌 수 있다. 이 중, 사칭은 공격자가 정당한 RFID 시스템 구성원으로 인증 받는데 성공하는 것으로, 공격자는 리더나 태그로 사칭 할 수 있다. 공격자가 태그로 사칭할 경우, 다양한 서비스에 무임승차할 수 있고, 물품 관리나 도난 방지 서비스에서는 물품을 탈취할 수 있어 문제가 생긴다. 리더로 사칭할 경우 공격자가 태그의 정보에 접근할 수 있는 문제가 생긴다.

개인 프라이버시는 크게 태그 정보에 대한 프라이버시와 위치 프라이버시로 나뉜다. RFID 태그는 크기에 제약을 받기 때문에 전력과 연산 등의 스펙이 리더보다 낮은 편이다. 따라서 RFID 리더가 챌린지를 보내면 리더가 정당한지 여부에 관계없이 태그는 반사적으로 응답을 보낸다. 만약 보안 프로토콜을 사용하지 않는다면 태그는 식별 번호를 그대로 노출 하는데, 이런 환경에서는 공격자는 단지 태그에게 챌린지를 보내는 것만으로도 태그가 부착된 물품의 정보를 알 수 있다. 즉, 공격자가 어떤 사람의 근처에서 RFID 리더를 통해 태그 정보를 획득한다면, 그 사람이 소지하고 있는 물품을 알 수 있어 개인의 프라이버시가 침해된다. 또 공격자가 도처에 설치한 여러 개의 리더를 통해 태그의 위치를 파악하고 이동 경로를 추적할 수 있다면 개인의 위치 프라이버시가 침해된다. 그러나 본고에서는 기업의 자산 관리, 도난 방지, 화물 추적 등의 위치 프라이버시가 중요하지 않은 서비스로 환경을 제한하였기 때문에 위치 프라이버시는 다루지 않으며, 프라이버시는 오직 태그 정보에 대한 것으로만 다룬다.

2.1.1 사칭(Impersonation)에 안전

공격자가 정당한 리더 또는 태그로 인증되는 것을 사칭이라 한다. 공격자는 정당한 리더와 태그의 통신을 도청(eavesdropping)한 후 재사용 공격(replay attack, Mafia fraud)하거나, 마피아 공격(mafia attack), 테러리스트 공격(terrorist attack)등의 수단을 통해 사칭을 할 수 있다.

(1)도청(Eavesdropping)과 재사용공격(Replay attack)

RFID 시스템은 무선으로 통신하기 때문에 유선 통신보다 도청하기가 더욱 용이하다. 공격자가 정당한 리더와 태그의 통신을 도청한 후, 그 내용을 그대로 사용하는 것을 재사용 공격이라 한다. RFID 인증 프로토콜이 단순할 경우 공격자는 단순히 재사용 공격만 실행하여 사칭에 성공할 수도 있다[11]. RFID 프로토콜이 재사용 공격에 안전하기 위해서는 난수 등을 사용하여 매 세션마다 송수신되는 메시지가 바뀌도록 해야 한다.

(2) 마피아 공격(Mafia fraud)

중계 공격은 공격자가 정당한 태그와 리더의 메시지를 중간에서 그대로 전달하는 공격이다. 마피아 공격은 중계 공격의 일종으로, 일반적으로 중계 공격에서는 리더와 태그의 거리에 제한을 두지 않는데 반해 마피아 공격은 태그와 리더 사이의 거리를 일반적인 RFID 시스템에서는 통신이 불가능한 먼 거리로 한정한다[12]. 이 공격은 정당한 태그의 응답을 그대로 사용하기 때문에, 일반적인 보안 프로토콜로는 방어할 수 없고 메시지 왕복 시간을 통해 거리를 추측하는 거리 제한 프로토콜과 같은 특수한 방법으로 방어할 수 있다. 거리 제한 프로토콜을 사용하더라도 공격자는 공격을 시도할 수 있는데, 공격자는 리더의 1 비트 챌린지가 도착하기 전에 태그에게 임의의 1 비트를 챌린지로 보내고 응답을 받아 놓고, 리더의 챌린지가 자신이 태그에

게 보낸 챌린지와 일치하면 태그의 챌린지를 사용하고, 일치 하지 않으면 임의의 비트로 응답하여 거리 제한 프로토콜을 공격할 수 있다. 이와 같은 전략을 사전 질의 전략이라 한다. 반대로 리더의 챌린지를 수신한 후에 그 챌린지를 태그에게 질의한 후 수신한 응답을 리더에게 보내는 전략을 사후 질의 전략이라 한다. 마피아 공격에서 태그와 리더는 먼 거리에 있기 때문에 사후 질의 전략을 사용할 경우 메시지 왕복 시간이 길어져 마피아 공격에 성공할 수 없다.

(3) 테러리스트 공격(Terrorist attack)

테러리스트 공격에서 공격자는 정당한 사용자에게 위협을 가하거나, 사용자와 공모를 하여 1회에 한하여 인증 프로토콜을 성공할 수 있는 정보를 얻은 상태에서 공격을 한다. 예를 들어 RFID 출입 시스템에서 사용자가 1회에 한하여 공격자에게 출입할 수 있는 정보를 주고, 공격자가 이 정보를 사용하여 단 1번 출입할 수 있다면 이 시스템은 테러리스트 공격에 취약한 것으로 파악된다. 단, 태그는 일회성으로 공격자를 도울 뿐, 공격자가 이후에도 계속 자신으로 사칭하는 것을 원치 않는다. 따라서 정당한 태그는 자신의 영구 키(long-term key)를 직·간접적으로 노출하지 않는다[13, 14].

2.1.2 프라이버시 보장 : 정보 노출(Information leakage)에 안전

RFID 시스템에서 리더와 태그 간의 통신은 무선으로 이루어지고, 또한 태그는 리더의 요청을 받으면 반사적으로 응답을 하게 된다. 따라서 공격자는 별 다른 노력 없이 쉽게 정당한 태그의 응답을 얻을 수 있다. 그러므로 안전한 RFID 시스템은 공격자가 정당한 태그의 메시지를 얻더라도 그로부터 어떠한 유용한 정보도 얻을 수 없게 설계되어야 한다.

2.2 용어

프로토콜과 그 분석에 필요한 용어는 다음과 같다.

K	: 정당한(legitimate) 리더(이하, 리더)와 정당한 태그(이하, 태그)가 공유한 영구(long-term) 비밀 키
N_x	: x가 생성한 난수(random number)
$h(x)$	: 해시(hash) 함수
$\|$	: 연접(concatenation)
$C_i(C_i^A)$	: i번째 라운드에서 리더(공격자)가 보내는 1비트 챌린지(challenge)
$R_i(R_i^A)$	: i번째 라운드에서 태그(공격자)가 보내는 1비트 응답(response)
C_i'	: i번째 라운드에서 태그가 수신한 실제 챌린지
R_i'	: i번째 라운드에서 리더가 수신한 실제 응답
RTT	: 메시지 왕복 시간(Round Trip Time)
$c_{\max}$	: 거리 제한 프로토콜에서 잡음을 고려할 때, 허용하는 최대 오류 수
$t_{\max}$	: 거리 제한 프로토콜에서 리더가 허용하는 최대 RTT
$A_i(B_i)$	: 공격자가 i 라운드에서 처음으로 리더(태그)에게 들키는 사건
$\overline{A_i}(\overline{B_i})$	: 공격자가 i 라운드까지 리더(태그)에게 들키지 않는 사건
$\overline{a_i}$	: 공격자가 i 라운드에서 리더에게 들키지 않는 사건
$void\ challenge$	: 챌린지를 보내지 않음
$void\ response$	: 응답을 보내지 않음
$NAND(x,y)$	: 부정 논리곱(Non-conjunction)

2.3 기존 거리 제한 프로토콜

거리 제한 프로토콜은 일반적으로 두 단계로 구성된다[15]. 첫 번째 단계는 비밀정보 공유를 위한 난수 생성 및 교환, 해시 연산 등 비교적 시간이 소요되는 연산을 수행하는 느린 단계(slow phase), 두 번째는 리더가 1비트 챌린지를 보내고 태그의 응답이 도착할 때까지 걸리는 왕복시간(RTT, round trip time)을 측정하여 거리의 상한선을 계산하기 위해 빠르게 진행되는 빠른 단계(fast phase)이다. 빠른 단계는 n번의 라운드로 구성이 되는데 각 라운드에서리더가 RTT를 통해 거리를 정확하게 계산하기 위해 느린 단계와는 달리 메시지 생성에는 시간이 거의 소요되지 않는 XOR과 같은 간단한 연산이 사용된다. 또한 리더는 각 라운드에서 태그의 1비트 응답을 토대로 거리 측정 뿐 아니라 인증도 진행 한다.

이런 형태의 거리 제한 프로토콜은 Hancke와 Kuhn[16]에 의해 제안되었는데, [16]에서 태그와 리더는 사전에 공유한 비밀 키 K와 느린 단계에서 교환한 리더가 생성한 난수 N_R를 토대로 $2n$비트의 해시 값 $h(K\|N_R)$을 계산한다. 이 때, $h(K\|N_R)$는 n비트로 나누어 $R^0\|R^1$로 나타낸다. 빠른 단계의 i $(1 \le i \le n)$번째 라운드에서 리더는 1비트 챌린지 $C_i \in_R \{0,1\}$를 임의로 생성하여 태그에게 보냄과 동시에 타이머를 작동시킨다. 태그는 C_i를 받는 즉시

RFID Reader(K)		RFID Tag(K)
Slow phase		
Pick $N_R \in \{0,1\}^k$	$\xrightarrow{N_R}$	
		Compute $R^0 \| R^1 = h(K \| N_R)$
Fast phase for $1 \le i \le n$ **and** $success = true$		
ith round		
If $success = true$, {		
$C_i \in_R \{0,1\}$, $R_i = \left(R^{C_i}\right)_i$		
Start Clock	$\xrightarrow{C_i}$	$R_i' = \left(R^{C_i}\right)_i$
	$\xleftarrow{R_i'}$	
Stop Clock : record Δt_i		
If $\left(R_i' \neq R_i\right) \vee \left(\Delta t > t_{\max}\right)$, $success = false$		
}		
Else, halt.		
If $i = n$, the tag is legitimate and close to the reader		

그림 1. HK 프로토콜[16]
Fig. 1. HK protocol[16]

R^{C_i}의 i번째 비트를 i번째 응답 R_i로 하여 리더에게 보내고, $R_i = \left(R^{C_i}\right)_i$를 받은 리더는 타이머를 정지하여 RTT을 통해 거리의 상한선을 계산한다. 리더가 수신한 태그의 응답을 R_i'라 할 때, 그 값과 느린 단계에서 자신이 계산한 R_i이 일치하는지 확인한다. 이때 모든 라운드에서 거리의 상한선이 일정 수준을 넘지 않고, 태그의 메시지가 정확할 경우, 리더는 태그가 정당하고 근거리에 있음을 확인할 수 있다.

2.3.1 Munila와 Peinado에 의해 제안된 거리 제한 프로토콜[14]

Hancke와 Kuhn의 프로토콜이 제안된 이후, 여러 RFID 거리 제한 프로토콜이 제안되었는데 그 중 Munila와 Peinado는 빠른 단계에서 리더의 1비트 챌린지 C_i를 $\{0,1\}$이 아니라, $\{0,1,void\}$에서 선택하도록 제안했다(이하 MP 프로토콜). 여기에서 $C_i = void$은 리더가 i번째 라운드에서 챌린지를 보내지 않음을 의미한다. 이는 느린 단계에서 생성한 비트열 P로부터 결정되는데, 이 값을 통해 공격자가 사전 질의 전략을 통해 마피아 공격을 시도할 경우 태그가 알아차릴 수 있도록 하여 마피아 공격의 성공 확률을 낮추었다. 또, 잡음으로 인해 메시지가 잘못 전송될 경우를 고려해 리더와 태그 모두 카운터를 사용하여 사전 정의한 상한 값 이내의 메시지 오류는 잡음으로 간주한다.

(1) MP 프로토콜

느린 단계에서 리더와 태그는 각각 난수 N_R, N_T를 생성하여 교환한 후, $3n+1$ 비트의 해시 값 $h(K \| N_R \| N_T)$을 생성한다. $h(K \| N_R \| N_T)$는 $P^{temp} \| v$로 나타내고, 이때 $P^{temp} = P_1^{temp} \| \cdots \| P_j^{temp} \| \cdots \| P_{2n}^{temp}$와 v는 각각 $2n$ 비트, $n+1$ 비트이다. 리더와 태그는 각각 P^{temp}를 통해 n 비트열 P의 i번째 비트 P_i를 $NAND\left(P_{2i-1}^{temp}, P_{2i}^{temp}\right)$와 같이 계산 한다($1 \le i \le n$). 예를 들어, $P^{temp} = 01001110100 \cdots$이라면 $P_1 = NAND(0,1) = 1$, $P_2 = NAND(0,0) = 1$, $P_3 = NAND(1,1) = 0$, …이 되어 $P = 11011 \cdots$가 된다.

빠른 단계의 i번째 라운드에서 리더는 $P_i = 0$일 경우 챌린지를 보내지 않는데, 이 경우 $C_i = void$라고 한다. $P_i = 1$인 경우에는 C_i를 $\{0,1\}$에서 임의로 선택하여 태그에게 보냄과 동시에 타이머를 작동시킨다. 태그는 C_i를 받자마자 P_i와 C_i를 참고하여 응답 R_i를 생성하는데, $(P_i = 0) \wedge (C_i = void)$이면 R_i도 $void$로, $(P_i = 1) \wedge (C_i = 0)$이면 R_i는 v의 최하위 비트(LSB)인 v_{LSB}가 되고 사용한 비트는 삭제한다. $(P_i = 1) \wedge (C_i = 1)$이면 R_i는 v의 최상위 비트(MSB)인 v_{MSB}가 되고 역시 사용한 비트는 삭제한다.

RFID Reader(K)		RFID Tag(K)
Slow phase		
Pick $N_R \in_R \{0,1\}^k$	$\xrightarrow{N_R}$	
	$\xleftarrow{N_T}$	Pick $N_T \in_R \{0,1\}^{k'}$
Compute $P' \| v = h(K \| N_R \| N_T)$, where $\|P'\| = 2n$, $\|v\| = n+1$.		
And compute P, where $P_i = NAND(P_{2i-1}', P_{2i}')$, $\|P\| = n$.		
Fast phase $(c=0)$		
ith round $(1 \le i \le n)$		$c_T = 0$
If $P_i = 0$, reader does not send challenge. (i.e., $C_i = void$) Else, reader sends random one bit challenge. (i.e., $C_i \in_R \{0,1\}$)		
Start Clock	$\xrightarrow{C_i}$	If $(P_i=0) \wedge (C_i = void)$, $R_i = void$. Else $(P_i=1) \wedge (C_i=0)$, $R_i = v_{LSB}$ and delete R_i from v. Else if $(P_i=1) \wedge (C_i=1)$, $R_i = v_{MSB}$ and delete R_i from v.
	$\xleftarrow{R_i}$	
Stop Clock : compute Δt_i		Otherwise, $c_T = c_T + 1$. If $c_T \ge c_{\max T}$, halt.
If $(R'_i \ne R_i) \vee (\Delta t \ge t_{\max})$, $c = c+1$. Else, $c = c$. If $c \ge c_{\max}$, halt.		

그림 2. MP 프로토콜[14]
Fig. 2. MP protocol[14]

나머지 경우는 $(P_i=0) \wedge (C_i \ne void)$인 경우인데, 원래 $P_i=0$ 이라면 챌린지가 오지 않아야 하는데 왔으므로 태그는 공격자가 마피아 공격을 시도한다고 간주하고 카운터 값을 증가시킨다. 이 카운터 값이 사전에 정의한 상한치를 넘어서게 되면 태그는 세션을 종료한다.

리더는 R_i를 받으면 타이머를 정지시키고, RTT가 $t_{\max}$이내이고, R_i가 정확한 경우 다음 라운드를 진행하고, 이 외의 경우 카운터 값을 증가시키고 카운터 값이 상한치 이상이 될 경우 세션을 종료한다. 성공적으로 n 라운드를 마친다면 해당 태그를 정당한 태그로 인증한다.

(2) MP 프로토콜의 안전성 분석

이 항에서는 MP 프로토콜이 테러리스트 공격에 취약하고, 잡음 환경을 고려하여 카운터를 사용하였음에도 불구하고 한 라운드에서 잡음이나 공격에 의한 통신 오류가 발생하면 리더와 태그가 가지고 있는 v값이 동기화가 되지 않아 그 이후의 라운드는 연속적으로 실패할 가능성이 있어 잡음 환경에 적절하지 않다는 것을 밝힌다.

- 테러리스트 공격 : 테러리스트 공격에서 태그는 일회성으로 공격자에게 정보를 주어 공격자가 리더에게 인증 받는 것을 도와준다. 그러나 태그는 공격자가 영구적으로 자신의 도움 없이 인증 받는 것은 원치 않는다. 즉, 태그가 자신의 영구적인 키(long-term key)를 노출시키지 않고 한 번의 인증만 도울 수 있을 때, 테러리스트 공격은 성공하게 된다. MP 프로토콜에서 테러리스트 공격은 다음과 같이 성공할 수 있다. 먼저 공격자 A는 리더의 인식 범위 안으로 들어가 리더와 난수 N_R, N_A를 교환하고 빠른 단계가 시작되기 전에 이를 태그에게 전달한다. 태그는 두 난수 N_R, N_A와 비밀 키 K를 통해 해당 세션에서 사용될 P와 v를 계산하고, 공격자를 돕기 위해 그 값을 공격자에게 보낸다. 공격

자는 태그에게서 받은 P와 v를 통해 빠른 단계를 진행하고 리더에게서 정당한 태그로 인증 받을 수 있게 된다. 이 공격에서 태그가 비밀 키 K를 노출시키지 않고, 한 세션에 한해 공격자가 인증 받을 수 있게 만들었으므로 테러리스트 공격은 성공한다.

- 잡음에 취약 : MP 프로토콜은 잡음 환경을 고려하여 카운터를 사용하였지만 잡음으로 인해 한 라운드에서 리더의 챌린지가 태그에게 다르게 전달 될 경우, 인증에 성공할 수 없게 된다. 이는 빠른 비트 교환단계에서 v의 LSB나 MSB를 사용한 뒤 사용한 비트를 제거하기 때문에, 한번 오류가 나면 리더와 태그가 가지고 있는 비트열 v가 서로 달라지기 때문이다. 예를 들어, 느린 단계에서 공유된 n비트열 $P=01010\cdots11$이고, $n+1$비트열 $v=110100\cdots010$일 때, 첫 번째 라운드는 $P_1=0$이기 때문에 리더는 챌린지를 보내지 않고, 태그도 응답을 하지 않는다. 두 번째 라운드는 $P_2=1$이기 때문에 리더는 임의로 $C_2=0$를 보낸다. 그런데 잡음이나 공격으로 인해 태그가 수신한 C_2'가 1인 경우, 태그는 v의 MSB인 1을 보내고 1을 삭제하여 태그의 v는 $10100\cdots010$이 되는 반면, 리더는 자신이 보낸 C_2가 0이기 때문에 v의 LSB인 0을 삭제하여 $v=110100\cdots01$이 된다. 이 후에는 리더와 태그가 저장하고 있는 v의 값이 다르므로 인증에 성공하기는 힘들다.

2.3.2 Ahn et al.에 의해 제안된 거리 제한 프로토콜[17]

(1) AYBN 프로토콜

Ahn et al.은 MP 프로토콜에서 저장 공간 및 통신 메시지 양을 효율적으로 개선한 프로토콜을 제안하였다(이하 AYBN 프로토콜). AYBN 프로토콜은 전체적으로 MP 프로토콜과 유사하지만, 잡음 환경을 리더에게만 허용하여 태그는 카운터를 사용하지 않았다. 또한, 해시 값을 n비트로 줄이기 위하여 P_i가 1인 경우에도 태그가 응답을 하지 않는 경우도 있다.

느린 단계에서 리더와 태그는 각각 난수 N_R, N_T를 생성하고 교환한 후, 그 난수와 사전에 공유한 비밀 키 K를 통해 n 비트 해시 값 $P=h(K\|N_R\|N_T)$ 를 계산한다. 빠른 단계는 n번의 라운드로 구성되는데 i번째 라운드에서 리더는 MP 프로토콜과 동일하게 $P_i=0$이면 요청하지 않고, P_i가 1일 경우 임의로 한 비트를 선택하여 태그에게 보내고 타이머를 실행한다. 태그는 $(P_i=0)\wedge(C_i=void)$인 경우와 $(P_i=1)\wedge(C_i=0)$인 경우에는 응답을 하지 않고, $(P_i=1)\wedge(C_i=1)$인 경우에는 $R_i=K_i\oplus C_i$로 응답한다. 그리고 P_i가 0임에도 챌린지를 수신한 경우, 공격자가 개입되어 있는 것으로 간주하고 세션을 종료한다. 태그의 응답을 받은 리더는 타이머를 정지 시키고, 메시지 왕복시간을 계산하여 그 값이 상한치를 넘거나 R_i를 검증하여 올바르지 않은 경우 카운터 값을 증가시킨다. 카운터 값이 최대치 미만인 경우 다음 라운드를 진행하고, 카운터 값이 최대치 이상이 될 경우 세션을 종료한다. n 라운드를 성공적으로 마치면, 리더는 태그를 정당한 태그로 간주하고, 근거리에 있음을 확신한다.

(2) AYBN 프로토콜의 안전성 분석

MP 프로토콜에서 $void$ 챌린지는 공격자가 태그에게 사전 질의를 할 때에는 태그가 공격을 눈치 채게 할 수 있어 마피아 공격 성공 확률을 낮추는 효과가 있다. 반면 공격자가 리더와 프로토콜을 진행 할 경우에는 리더가 $void$ 챌린지를 보내면 공격자도 응답하지 않으면 해당 라운드를 성공할 수 있기 때문에 한편으로는 마피아 공격 성공 확률을 높일 수도 있는 양면성이 있다. 따라서 $void$ 챌린지의 횟수는 적정 수준으로 조정해야 하는데, Munilla와 Peinado는 실험을 통해 $void$ 챌린지의 수가 전체 라운드의 1/5인 경우, 가장 안전하다는 결과를 얻었다[14]. $void$ 챌린지의 수를 전체의 1/5로 조정하려면 챌린지를 결정하는 비트열 P에서 0의 개수를 전체의 1/5로 조정해야 한다. 그러나 전체 비트열의 1/5을 0으로 만드는 것은 구현하기 어렵기 때문에 MP 프로토콜에서는 구현이 쉬운 $NAND$을 통해 비트열에서의 0의 비율을 1/5에 가까운 값인 1/4로 조정하였다. $2n$비트열 P^{temp}에서 $NAND$ 연산을 한 비트열인 P에서 0의 비율이 1/4이 되는 이유는 P^{temp}는 해시의 결과로 생성된 비트열이기 때문에 일반성을 잃지 않고 $\Pr(P_i^{temp}=0)=\Pr(P_i^{temp}=1)$으로 간주할 수 있고, $NAND(0,0)=1$, $NAND(0,1)=1$, $NAND(1,0)=1$, $NAND(1,1)=0$이기 때문이다. 따라서 MP 프로토콜은 $\Pr(P_i=0)=1/4$로, $\Pr(P_i=0)=1/5$인 경우와 유사한 높은 수준의 안전성을 $NAND$연산을 통해 얻을 수 있었다[14].

그러나 AYBN 프로토콜은 저장 공간의 효율성을 높이고 해시 연산량을 낮추기 위해, MP 프로토콜에서 $3n+1$비트이던 해시 값을 n비트로 낮추고 비트열에

RFID Reader(K)		RFID Tag(K)
Slow phase		
Pick $N_R \in \{0,1\}^k$	$\xrightarrow{N_R}$	
	$\xleftarrow{N_T}$	Pick $N_T \in \{0,1\}^{k'}$
Compute $P = h(K \| N_R \| N_T)$		
Fast phase $(c=0)$		
ith round $(1 \le i \le n)$		
If $P_i = 0$, reader does not send challenge.(i.e., $C_i = void$) Else, reader sends random one bit challenge. (i.e., $C_i \in_R \{0,1\}$)		
Start Clock	$\xrightarrow{C_i}$	If $(P_i=0) \wedge (C_i = void)$, $R_i = void$. Else if $(P_i=0) \wedge (C_i \neq void)$, halt. Else if $(P_i=1) \wedge (C_i=0)$, $R_i = void$ Else if $(P_i=1) \wedge (C_i=1)$,
	$\xleftarrow{R_i}$	$R_i = K_i \oplus C_i$.
Stop Clock : compute Δt_i		
If $(R'_i \neq R_i) \vee (\Delta t \ge t_{\max})$, $c = c+1$.		
Else, $c = c$.		
If $c \ge c_{\max}$, halt.		

그림 3. AYBN 프로토콜[17]
Fig. 3. AYBN protocol[17]

서 0의 확률을 조정하지 않아 $void$ 챌린지의 수가 전체 라운드의 1/2이 되어 MP 프로토콜에 비해 상대적으로 많아졌다. 이에, AYBN 프로토콜은 MP 프로토콜과 같은 수의 라운드를 진행할 때, MP 프로토콜에 비해 마피아 공격에 대한 안전성이 낮아졌다. 또, 영구 키 노출에 취약하고, 태그의 도움 없이 진행하는 사칭에 취약하다.

- 태그의 도움 없는 사칭 : 이 경우, 공격자는 성공 확률을 높이기 위해서 다음과 같은 전략을 취한다. AYBN 프로토콜의 빠른 단계에서 리더의 챌린지가 $void$이거나 0인 경우 공격자는 응답하지 않는다. 리더가 챌린지로 1을 보낸 경우에는 공격자는 비밀 키 K 값을 알 수 없어 정확한 값을 알 수 없기 때문에, $\{0,1\}$에서 임의로 하나를 선택하여 응답한다. 이런 전략으로 공격을 시도할 때, 공격자의 성공 확률은 다음과 같다. AYBN 프로토콜은 MP 프로토콜과 달리 해시 출력에 어떤 조작도 하지 않았기 때문에 $\Pr(P_i=0) = \Pr(P_i=1) = 1/2$이고, 리더가 생성하는 챌린지 C_i 역시 임으로 생성한 1비트 난수이기 때문에 $\Pr(C_i=0) = \Pr(C_i=1) = 1/2$를 만족한다. 따라서 $\Pr(((P_i=1) \wedge (C_i=1))^c) = 1 - 1/4 = 3/4$인 경우는 공격자의 성공 확률은 1, $\Pr((P_i=1) \wedge (C_i=1)) = 1/4$인 경우 공격자의 성공 확률은 $\frac{1}{2}$로, 총 n라운드에서 정당한 태그의 도움 없이 공격자가 사칭에 성공할 확률은 $\left(\frac{7}{8}\right)^n$이다. $c_{\max}$번의 잡음을 허용할 경우, 성공 확률은 $\sum_{c=0}^{c_{\max}} \binom{n}{c} \left(\frac{7}{8}\right)^{n-c} \left(\frac{1}{8}\right)^c$이 된다.

- 키 노출 : 이 프로토콜에서 K는 갱신과정을 거치지 않는 영구 키(long-term key)이다. 그런데, $(P_i=1) \wedge (C_i=1)$인 경우 태그의 응답 R_i가 $K_i \oplus C_i = K_{\ i} \oplus 1$로 K_i가 노출된다. P에 제약을 하지 않았기 때문에 $\Pr(P_i=0) = \Pr(P_i=1) = \Pr(C_i=0) = \Pr(C_i=1) = 1/2$로, 키 길이 전체의 $\Pr(\{K_i | i \in \{i | C_i=1\}\}) = 1/4$이 노출된다. 따라서 공격자가 합법한 리더와 태그의 통신 내용을 도청만 하더라도 $\{K_i | i \in \{i | C_i=1\}\}$를 알 수 있다.

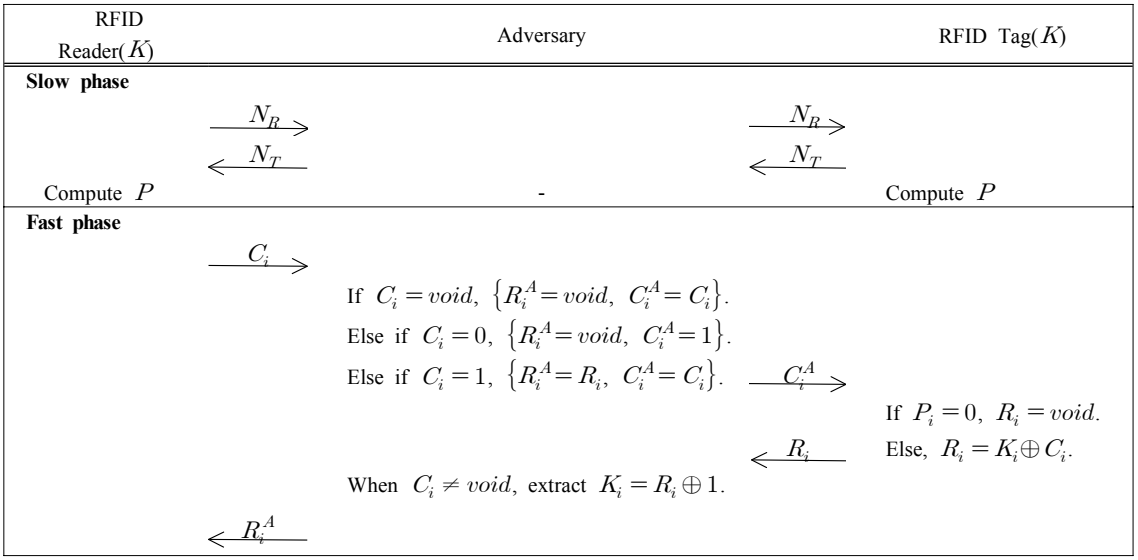


그림 4. AYBN 프로토콜에 대한 키 노출 공격
Fig. 4. Key leakage of AYBN protocol

그러나 만약 공격자가 도청에 그치지 않고 그림 4. 와 같이 근거리에서 통신하고 있는 리더와 태그 사이에서 메시지를 조작한다면 공격자가 획득할 수 있는 키 정보는 더욱 늘어난다. 공격자는 느린 단계에서는 리더와 태그의 메시지를 그대로 전달하고, 빠른 단계를 리더와 먼저 시작한다. 리더가 요청하지 않으면 공격자도 태그에게 요청하지 않는다. 리더의 요청이 오면, 공격자는 무조건 $C_i = 1$로 바꾸어 태그에게 보낸다. $C_i = 1$이라면, 태그는 $R_i = K_i \oplus 1$를 보내기 때문에 공격자는 K_i를 알 수 있게 된다. 이렇게 공격할 경우, $P_i = 1$인 경우 키가 노출되기 때문에 한 세션동안 $n/2$의 키가 노출되고, 공격횟수를 늘릴 경우 키 정보 노출이 늘어난다.

- 마피아 공격(Mafia fraud) : 공격자는 마피아 공격 성공 확률을 높이기 위해 다음과 같이 사전 질의 전략을 취한다. 먼저 느린 단계에서 공격자는 리더와 태그 사이의 메시지를 그대로 전달한다. 빠른 단계에서 공격자는 챌린지 $C^A{}_i \in_R \{void, 1\}$를 C_i를 수신하기 전에 태그에게 전송한 후, 그 응답을 보관한다. 공격자는 $C_i = void$, 또는 $C_i = 0$이라면 침묵하고($R_i^A = void$), 리더의 챌린지와 자신이 태그에게 보낸 챌린지가 모두 1이라면 태그의 응답을 그대로 보낸다. 만약 리더의 챌린지가 1인데 자신이 보낸 챌린지가 $void$이었다면 태그에게 들켜 태그의 응답을 받지 못하였기 때문에 $\{0, 1\}$에서 임의로 하나를 선택하여 보낸다.

리더가 챌린지를 $void$나 0으로 보낸다면 공격자는 태그의 도움 없이도 $void$로 응답하면 해당 라운드는 성공하고, 챌린지를 1로 보낸다면 태그의 도움이 필요하다. 따라서 공격자는 태그에게 사전 질의를 할 때, 가능한 챌린지 값 $void$, 0, 1에서 0은 제외하고 보낸다. 공격자가 보내는 챌린지 값이 $void$인 경우에도 태그의 응답을 알 수는 있지만, 실제 $P_i = 0$인 경우 태그에게 $C^A{}_i = 1$을 보내게 되면 태그가 정당한 리더가 아닌 공격자가 개입되어 있음을 알게 된다. 따라서 공격자가 정당한 리더로 가장하여 태그의 응답을 계속해서 수신하기 위해 챌린지 값에서 $C^A{}_i = void$는 허용하여, 태그에게 보내는 요청 값을 $void$, 1로 제한한다.

먼저 잡음을 고려하지 않는 환경에서 공격자가 n 라운드까지 리더를 상대로 마피아 공격에 성공할 확률은

$$\Pr(\overline{A_n}) = \Pr(\overline{A_n} \cap \overline{B_n}) + \sum_{i=1}^{n} P(\overline{A_n} \cap B_i)$$

$$= \Pr(\overline{A_n}|\overline{B_n})P(\overline{B_n}) + \sum_{i=1}^{n} \Pr(\overline{A_n}|B_i)P(B_i)$$

$$= 1 \cdot \left(\frac{1}{2}\right)^n + \sum_{i=1}^{n} \Pr(\overline{a_1}|B_i) \prod_{j=2}^{n} \Pr(\overline{a_j}|\overline{a_{j-1}}, .., \overline{a_1}, B_i) \Pr(B_i)$$

$$= 1 \cdot \left(\frac{1}{2}\right)^n + \sum_{i=1}^{n} \left(\frac{7}{8}\right)^{n+1} \left(\frac{4}{7}\right)^i = \frac{7}{6}\left(\frac{7}{8}\right)^n - \frac{1}{6}\left(\frac{1}{2}\right)^n$$

이다. AYBN 프로토콜에서 태그는 잡음을 고려하지 않고 리더의 요청이 잘못 올 경우 바로 세션을 종료하지만, 리더는 잡음을 고려하여 최대 $c_{\max}$의 오류를 허용

RFID Reader(K)		RFID Tag(K)
Slow phase		
Pick $N_R \in \{0,1\}^k$	$\xrightarrow{N_R}$	
	Compute $P' \| Q = h(K \| N_R)$, where $\|P'\| = 2n$, $\|Q\| = n$.	
	And calculate P, where $P_i = NAND(P_{2i-1}', P_{2i}')$, $\|P\| = n$.	
Fast phase $(c = 0)$		
ith round $(1 \le i \le n)$		
If $P_i = 0$, reader does not send challenge.(i.e., $C_i = void$) Else, reader sends random one bit challenge. (i.e., $C_i \in_R \{0,1\}$)		
Start Clock	$\xrightarrow{C_i}$	If $(P_i = 0) \wedge (C_i = void)$, $R_i = void$. Else if $\{((P_i = 0) \wedge (C_i \neq void)) \vee ((P_i = 1) \wedge (C_i = void))\}$, halt. $R_i = \begin{cases} Q_i, & if\ C_i = 0 \\ Q_i \oplus K_i, & if\ C_i = 1 \end{cases}$ Else,
	$\xleftarrow{R_i}$	
Stop Clock : record Δt_i		
If $(R'_i \neq R_i) \vee (\Delta t \ge t_{\max})$, $c = c+1$.		
Else, $c = c$.		
If $c \ge c_{\max}$, halt.		

그림 5. 제안하는 프로토콜
Fig. 5. Proposed protocol

한다. 이때 공격자의 성공 확률은 태그에게 $n - c_{\max}$번째까지 들키지 않은 경우나, 그 이전에 들킨 경우로 나누어 생각한다. $n - c_{\max}$번째까지 태그에게 들키지 않았다면 그 이후의 라운드는 태그에게 질의하지 않아도 남은 $c_{\max}$개의 라운드에서 리더에게 어떤 값을 주더라도 결과적으로 인증에 성공한다. 그러나 $n - c_{\max}$번째나 그 이전에 태그에게 들켰다면, 리더와 $n - c_{\max}$ 이상의 라운드에서 성공해야 한다. $n - c_{\max}$번째까지 태그와의 라운드에서 실패하지 않은 경우 성공 확률은 $\left(\frac{1}{2}\right)^{n-c_{\max}}$, 태그와의 $i(\le n - c_{\max})$번째 라운드에서 인증에 실패한 경우 리더와의 라운드에서 성공할 확률은 $\sum_{c=0}^{c_{\max}} \binom{n-i+1}{c} \left(\frac{1}{2}\right)^{i} \left(\frac{7}{8}\right)^{n-i+1-c} \left(\frac{1}{8}\right)^{c}$이다. 따라서 잡음 환경에서의 성공 확률은 $\left(\frac{1}{2}\right)^{n-c_{\max}} + \sum_{i=1}^{n-c_{\max}} \left\{ \sum_{c=0}^{c_{\max}} \binom{n-i+1}{c} \left(\frac{1}{2}\right)^{i} \left(\frac{7}{8}\right)^{n-i+1-c} \left(\frac{1}{8}\right)^{c} \right\}$이다.

Ⅲ. 제안하는 프로토콜

이번 장에서는 2장에서 제시한 보안 요구 조건을 만족하고, 기 제안된 프로토콜의 취약점을 보완한 새로운 프로토콜을 제안하고 그 안전성을 분석한다. 제안 프로토콜에서 리더와 태그는 비밀 키 K를 공유하고 해시와 NAND 연산이 가능하고, 리더는 추가적으로 난수를 생성할 수 있다.

3.1 제안 프로토콜 소개

제안하는 프로토콜의 느린 단계에서는 리더만 난수 N_R을 생성하여 태그에게 전송한다. 태그와 리더는 각각 공유키 K와 리더의 난수 N_R를 통해 $P' \| Q = h(K \| N_R) \in \{0,1\}^{3n}$를 생성한다. 이때, P'와 Q는 각각 $2n$, n비트이다. P'은 MP 프로토콜에서와 같이 $NAND$ 연산을 통해 n 비트열 P로 변환되고, P의 i번째 비트는 $P_i = NAND(P'_{2i-1}, P'_{2i})$이다. 해시의 결과로 생성된 P'를 $NAND$ 연산을 통해 P로 변환하는 이유는 AYBN의 분석 단계에서 언급한 바와 같이 비트열에서 0의 확률을 1/4로 만들기 위함이다.

표 1. 제안하는 프로토콜과 기존 프로토콜의 안전성 비교
Table 1. Security and privacy comparison of existing protocols with proposed protocol

			HK protocol[16]	MP protocol[14]	AYBN protocol[17]	Proposed protocol
Impersonation	Replay attack		Secure	Secure	Secure	Secure
	Mafia fraud success probability	Noise-free	$\left(\frac{3}{4}\right)^n$	$2\left(\frac{5}{8}\right)^n-\left(\frac{65}{128}\right)^n$	$\frac{7}{6}\left(\frac{7}{8}\right)^n-\frac{1}{6}\left(\frac{1}{2}\right)^n$	$2\left(\frac{5}{8}\right)^n-\left(\frac{65}{128}\right)^n$
		Noise	$\sum_{c=0}^{c_{\max}}\binom{n}{c}\left(\frac{3}{4}\right)^{n-c}\left(\frac{1}{4}\right)^c$	-	$\sum_{i=1}^{n-c_{\max}}\left\{\sum_{c=0}^{c_{\max}}\binom{n-i+1}{c}\left(\frac{7}{8}\right)^{n+1}\left(\frac{4}{7}\right)^i\left(\frac{1}{7}\right)^c\right\}+\left(\frac{1}{2}\right)^{n-c_{\max}}$	$\sum_{c=0}^{c_{\max}}\left\{\sum_{c_1=\max(0,\,c-n+i)}^{\min(c,\,i-1)}\binom{n-i+1}{c-c_1}\binom{i-1}{c_1}\left(\frac{6}{13}\right)\left(\frac{5}{8}\right)^n\left(\frac{13}{16}\right)^i\left(\frac{3}{5}\right)^c\left(\frac{5}{13}\right)^{c_1}\right\}$
	Terrorist attack		Insecure	Insecure	Secure	Secure
	Without any information		$\left(\frac{1}{2}\right)^n$	$\left(\frac{5}{8}\right)^n$	$\left(\frac{7}{8}\right)^n$	$\left(\frac{5}{8}\right)^n$
Key leakage			Secure	Secure	Eavesdropping : $1/4$ of key per each session Active attack : $1/2$ of key per each session	Secure

한 세션동안 사용될 비트열 P와 Q를 생성하는 느린 단계가 완료되면, n 라운드로 구성된 빠른 비트 교환 단계가 시작된다. 빠른 단계의 i라운드에서 리더는 P_i에 따라 요청을 달리 생성하는데, $P_i=0$일 경우 리더는 요청하지 않는다. 즉, $C_i=void$가 된다. $P_i=1$일 경우, 리더는 1비트 난수를 생성하여 $C_i\in_R\{0,1\}$를 보내고, 요청을 보내는 즉시 타이머를 작동시킨다.

태그는 C_i를 받자마자, 다음과 같이 응답을 생성한다. $P_i=0$일 때, 리더의 챌린지가 없다면 태그 역시 응답하지 않고 다음 라운드로 넘어간다. P_i가 1인 경우, $C_i=0$이면 태그는 $R_i=Q_i$로 응답하고, $C_i=1$이면 $R_i=Q_i\oplus K_i$로 응답하고 다음 라운드로 넘어간다. P_i가 0임에도 리더의 요청을 받거나, P_i가 1인데도 요청을 받지 못한다면, 태그는 이후의 모든 요청에 응답하지 않는다. 리더는 태그의 응답이 도착하면 RTT가 사전에 정의한 최대 시간 $t_{\max}$를 넘지 않고, 태그의 응답이 정확한 경우 다음 라운드를 진행하고 아닐 경우 카운터를 증가시킨다. 리더의 카운터가 사전에 정의한 최대치 $c_{\max}$ 이하일 경우 다음 라운드를 진행하고, 이상인 경우 해당 태그가 근거리에 존재 하지 않거나, 정당한 태그가 아니라고 추정하여 다음 라운드를 진행하지 않고 세션을 종료한다. n 라운드를 무사히 마치게 되면 해당 태그가 일정 거리 내에 있고, 정당한 태그임을 인증한다.

3.2 제안 프로토콜 안전성 분석

제안프로토콜은 NAND 연산으로 $void$ 챌린지의 횟수를 전체의 $1/4$로 조정하여 같은 횟수의 라운드를 실행 하였을 때 AYBN보다 사칭, 마피아 공격에 안전하게 설계하였다. 또, 태그가 응답을 생성할 때 비밀 키 K뿐만 아니라 한 세션에 한하여 사용하는 비밀 값 Q를 사용하여 영구 키 K의 노출에 안전하고 테러리스트 공격에 안전하다. 또 MP 프로토콜과 달리 n비트열 Q를 MSB부터 순차적으로 사용하여 리더와 태그의 비동기화를 막고, 카운터를 사용하여 잡음에 대한 탄력성이 있어 정당한 리더와 태그라면 인증에 성공하도록 설계 하였다.

- 태그의 도움 없는 사칭 : 비트열 P에서 1의 개수가 작을수록 공격자의 사칭 성공률이 높아지는데, 제안 프로토콜은 NAND 연산을 통해 1의 개수를 조정하였으므로 일반성을 잃지 않고 $\Pr(P_i=1)=3/4$로 가정

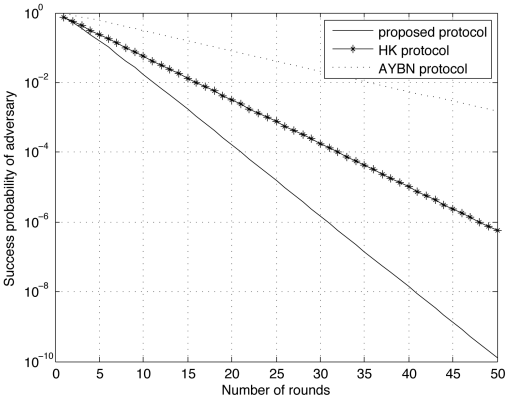
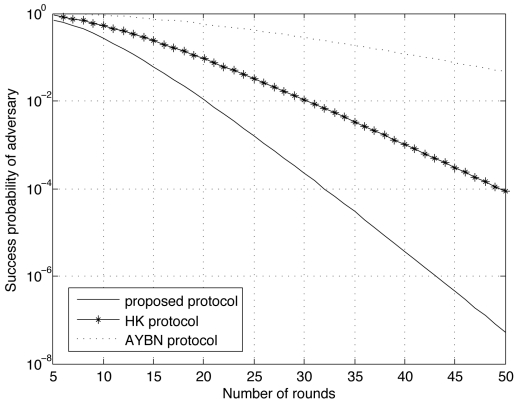
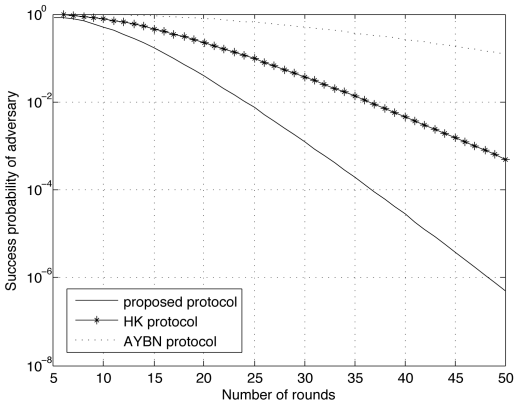


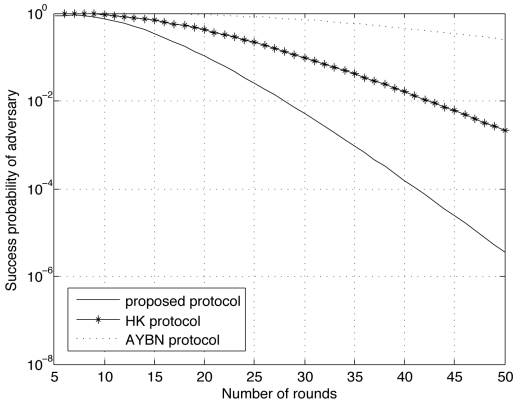
그림 6. 잡음을 고려하지 않는 환경에서 마피아 공격 성공 확률 비교
Fig. 6. Comparison of mafia fraud success probability in the noise-free case



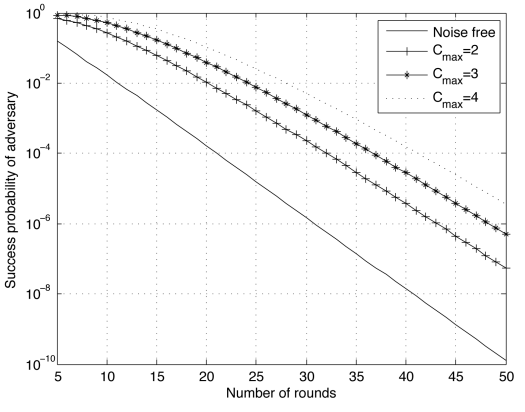
7.(a) $c_{\max}=2$



7.(b) $c_{\max}=3$



7.(c) $c_{\max}=4$



7.(d) 제안 프로토콜에 대한 카운터 별 공격 성공 확률

그림 7. 잡음을 고려한 환경에서 마피아 공격 성공 확률 비교
Fig. 7. Comparison of mafia fraud success probability in the noise case

한다. 공격자는 성공 확률을 높이기 위해서 *void* 챌린지가 올 경우는 응답을 하지 않고, 0이나 1의 챌린지가 올 경우 정확한 응답 값을 계산할 수 없기 때문에 임의의 한 비트로 응답하는 전략을 취한다. 이때 잡음을 고려하지 않는 환경에서 n라운드의 인증에 성공할 확률은 $\left(\frac{5}{8}\right)^n$이다. 최대 $c_{\max}$번의 잡음을 허용할 경우, 공격자의 성공 확률은 $\sum_{c=0}^{c_{\max}}\binom{n}{c}\left(\frac{5}{8}\right)^{n-c}\left(\frac{3}{8}\right)^c$이다.

- 마피아 공격(Mafia fraud) : 공격자는 마피아 공격 성공 확률을 높이기 위해 사전 질의 전략을 취하는데 $C_i = C_i^A$이라면 리더에게 R_i를 그대로 보내고, $\left(C_i \neq C_i^A\right) \wedge \left(C_i = void\right)$이라면 $R_i^A = void$, $\left(C_i \neq C_i^A\right) \wedge \left(C_i \neq void\right)$이라면 $R_i^A \in_R \{0,1\}$로 응답한다. 잡음을 고려하지 않는 환경에서의 성공 확률 $\Pr(\overline{A_n})$는 $\Pr(\overline{A_n} \cap \overline{B_n}) + \sum_{i=1}^{n}\Pr(\overline{A_n} \cap B_i) =$

$$= \left(\frac{13}{16}\right)^n\left(\frac{5}{8}\right)^n + \sum_{i=1}^{n}\left(\frac{5}{8}\right)^{i-1}\left(\frac{3}{8}\right)\left(\frac{13}{16}\right)^{i-1}\left(\frac{5}{8}\right)^{n-i+1}$$

$$= 2\left(\frac{5}{8}\right)^n - \left(\frac{65}{128}\right)^n$$

이다. 제안 프로토콜에서 태그는 잡음을 고려하지 않기 때문에 태그는 잘못된 챌린지가 오면 바로 세션을 종료하고 리더는 최대 $c_{\max}$번의 오류를 허용한다. i번째에 태그가 공격을 탐지한 경우 리더로부터 인증 받을 확률은

$$\sum_{c=0}^{c_{\max}}\left\{\sum_{c_1=\max(0,\,c-n+i)}^{\min(c,\,i-1)}\binom{n-i+1}{c-c_1}\binom{i-1}{c_1}\left(\frac{5}{8}\right)^{i-1}\left(\frac{13}{16}\right)^{i-1-c_1}\right.$$

표 2. 제안하는 프로토콜과 기존 프로토콜의 효율성 비교
Table 2. Perfomance comparison of existing protocols with proposed protocol

$k(k')$: length of random number of Reader(Tag), n : number of rounds of fast phase

		HK protocol[16]	MP protocol[14]	AYBN protocol[17]	Proposed protocol
Hash # of reader and tag		1 ($2n$ bit)	1 ($3n+1$ bit)	1 (n bit)	1 ($3n$ bit)
# of random number generation	Reader	1 (k bit) n (1 bit)	1 (k bit) $3n/4$ (1 bit)	1 (k bit) $n/2$ (1 bit)	1 (k bit) $3n/4$ (1 bit)
	Tag	-	1 (k' bit)	1 (k' bit)	-
Additional operation		-	n (NAND)	$n/4$ (XOR)	n (NAND) $3n/8$ (XOR)
Length of tag's message		n bit	$k'+3n/4$ bit	$k'+n/4$ bit	$3n/4$ bit
Storage of tag		$\|K\|+2n$ bit	$\|K\|+2n+1$ bit	$\|K\|+n$ bit	$\|K\|+2n$ bit

$\left(\frac{3}{16}\right)^{c_1}\left(\frac{3}{8}\right)\left(\frac{5}{8}\right)^{n-i+1-c+c_1}\left(\frac{3}{8}\right)^{c-c_1}\Big\}$이다.

- 키 노출 : 공격자는 비 갱신키 K를 알기 위해 도청을 하더라도 C_i가 1인 경우에 한하여 $Q_i \oplus K_i$를 알 수 있다. 그러나 공격자는 Q_i를 알 수 없기 때문에 결국 K_i를 알 수 없다.

- 테러리스트 공격 : 테러리스트 공격에 성공하기 위하여 공격자는 느린 단계에서 인증에 필요한 정보를 태그로부터 제공 받고, 그 정보를 통해 리더와 빠른 단계를 진행한다. 이때, 태그는 1회에 한하여 공격자에게 정보를 제공하는 것이므로 태그가 영구키를 노출하지 않는다. 제안 프로토콜을 공격하기 위해 공격자는 태그와 공모하고, 리더의 인식 영역으로 진입한다. 공격자는 느린 단계에서 리더로부터 난수 N_R을 받으면 태그에게 전달하고, 태그는 N_R과 비밀키 K를 통해 해당 세션 인증에 필요한 값을 전달해야 한다. 그런데, 인증에 필요한 값이 Q와 고정 키K이기 때문에 태그는 이 정보를 공격자에게 줄 수 없으므로 제안 프로토콜은 테러리스트 공격에 안전하다. 세션 리더에게서 정당한 태그로 인증 받을 수 있게 된다. 이 공격에서 태그가 비밀 키 K를 노출시키지 않고, 한 세션에 한해 공격자가 인증 받을 수 있게 만들었으므로 테러리스트 공격은 성공할 수 없다.

3.3 안전성 및 효율성 비교`

이번 절에서는 2장과 3장의 프로토콜 분석을 바탕으로 각 프로토콜을 비교한다. 공격자는 재전송, 마피아, 테러리스트 공격과 태그에 대한 사전 정보 없이 공격하는 방법을 통해서 태그로 사칭할 수 있다. 비교한 프로토콜 모두 난수를 사용하였기 때문에 재전송 공격에는 안전하다. 그림 6.과 그림 7.에서는 라운드 실행 횟수에 따른 마피아 공격 성공 확률을 나타낸 것이다. 그래프에서 가로 축은 라운드 수 n을 나타내고, 세로 축은 공격자의 성공 확률을 나타낸다. 마피아 공격은 카운터를 사용하지 않는 잡음을 무시하는 환경과 카운터를 사용하여 잡음을 고려한 환경에서의 성공 확률이 다르다. 잡음을 무시하는 환경에서는 올바르지 않은 응답이 올 경우 바로 세션을 종료하여 공격자의 성공 확률이 가장 낮은데, 오류 응답을 허용 횟수를 나타내는 $c_{\max}$가 커질수록 공격자의 성공 확률도 높아짐을 그림 7.에서 확인할 수 있다. 최대 허용 오류 횟수가 3 ($c_{\max}=4$)일 때, 총 50회의 라운드를 진행하는 경우와 최대 허용 오류 횟수가 1($c_{\max}=2$)일 때, 총 40회의 라운드를 진행하는 경우의 공격자의 성공 확률이 비슷하다. 이는 같은 수준의 안전성을 달성하기 위해서 $c_{\max}$가 커질수록 라운드 수를 늘려야 함을 의미한다. 잡음을 무시하는 환경에서 공격자의 성공 확률은 그림 6.에서와 같이 나타나며 제안 프로토콜과 MP 프로토콜에서의 성공 확률이 가장 낮다.

표 2.는 제안 프로토콜과 기존 프로토콜의 메시지 통신량, 연산량, 저장량을 비교한 결과이다. 리더는 태그에 비해 상대적으로 스펙이 높기 때문에 태그의 저장량과 통신량만을 비교한다. 해시 연산량은 제안 프로토콜과 비교하는 프로토콜 모두 1회 이지만, 해시 출력이 리더와 태그 모두 $3n$비트로 비교하는 프로토콜에 비해 긴 편이다. 다른 비교 프로토콜과는 달리 제안 프로토콜에서는 태그는 난수 생성하지 않는다. 그 대신 태그는 NAND와 XOR이 가능해야한다. 또, 태그 메시지의 길이는 난수를 생성하지 않고 void 챌린지를 사용하였기 때문에 비교 프로토콜에 상대적으로 낮은 편이다. 태그의 저장량은 다른 프로토콜과는 비슷하지만 AYBN 프로토콜보다는 높다.

Ⅳ. 결 론

본 논문에서는 RFID 시스템을 도난 방지, 자산 파악 등의 서비스에 한정시키고, 이런 종류의 서비스에서 필요한 보안 요구 조건을 제시 하였다. 특히 마피아 공격에 안전한 프로토콜 설계를 위해 기 제안된 프로토콜을 소개하고 분석하였다. 그 결과 Munilla와 Peinado의 프로토콜이 빠른 단계를 n라운드 실행할 때, 마피아 공격 성공률은 $2\left(\frac{5}{8}\right)^n-\left(\frac{65}{128}\right)^n$로 만족할 수준의 안전성을 제공하지만, 테러리스트 공격과 주변의 잡음에 취약하다는 것을 밝혔다. 또, 그 이어 태그의 저장 공간의 효율성을 높이기 위해 제안된 Ahn et al.의 프로토콜이 마피아 공격 성공 확률이 $\frac{7}{6}\left(\frac{7}{8}\right)^n-\frac{1}{6}\left(\frac{1}{2}\right)^n$로 높고, 적극적인 공격을 할 경우 한 세션을 진행 할 경우 영구키(long-term key)의 절반이 노출된다는 것을 밝혔다.

이에 본 연구에서는 잡음이 없는 경우에는 마피아 공격에 대한 안전성이 Munilla와 Peinado의 프로토콜과 동일한 프로토콜을 제안하였다. 그러나 Munilla와 Peinado의 프로토콜이 잡음이 있을 경우 인증이 진행되지 않는 것과 달리, 제안 프로토콜은 잡음을 $c_{\max}$번 고려하여 잡음이 있는 환경에서도 적용할 수 있으며 그 안전성을 분석하였다. 또한, 제안 프로토콜은 테러리스트 공격, 영구키 노출에 안전하다는 것을 보였다. 그러나 태그 저장 공간의 효율성은 Ahn et al.의 프로토콜보다 높아 Munilla와 Peinado의 프로토콜과 유사하거나 낮은 수준을 보이므로 향후 태그 저장 공간의 효율성을 높이는 연구가 필요하다.

References

[1] A. Gildas, Adversarial model for radio frequency identification(2005), Retrieved Aug., 12, 2007, from http://eprint.iacr.org.

[2] R. Angeles, “RFID technology: supply-chain applications and implementations issues,” *Inf. Syst. Management*, vol. 22, no. 1, pp. 51-65, 2005.

[3] M. Kärkkäinen, “Increasing efficiency in the supply chain for short shelf life goods using RFID tagging,” *Int. J. Retail & Distrib. Management*, vol. 31, no. 10, 2003.

[4] B. Srivastava, “Radio frequency ID technology: the next revolution in SCM,” *Business Horizons*, vol. 47, no. 6, pp. 60-68, 2004.

[5] K. Finkenzeller, *RFID Handbook: radio-frequency identification fundamentals and applications*, NY: John Wiley & Sons, 1999.

[6] Y. Desmedt, “Major securitv problems with the unforgeable (Feige)-Fiat-Shamir proofs of identity and how to overcome them,” in *Proc. SecuriCom ’88*, pp. 15-17, Paris, France, 1988.

[7] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, and B. Martin, “A framework for analyzing RFID distance bounding protocols,” *J. Computer Security*, vol. 19, no. 2, pp. 289-317, Mar. 2011.

[8] S. Bengio, G. Brassard, G. Desmedt, C. Goutier, and J. Quisquater, “Secure implementation of identification schemes,” *J. Cryptology*, vol. 4, no. 3, pp. 175-183, 1991.

[9] S. Brands and D. Chaum, “Distance-bounding protocols,” in *Advances in Cryptology — EUROCRYPT’93*, pp. 344-359, Berlin Heidelberg, Jan. 1994.

[10] S. W. Wang, W. H. Chen, C. S. Ong, L. Liu, and Y. W. Chuang, “RFID application in hospitals: a case study on a demonstration RFID project in a Taiwan hospital,” in *Proc. HICSS Int. Conf. 2006*, pp. 184a-184a, Jan. 2006.

[11] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, “Security and privacy aspects of low-cost radio frequency identification systems,” in *Security in pervasive computing*, pp. 201-212, Springer Berlin Heidelberg, 2004.

[12] A. Abu-Mahfouz and G. P. Hancke, “Distance bounding: a practical security solution for real-time location systems,” *IEEE Trans. Ind. Informatics*, vol. 9, no. 1, pp. 16-27. Feb. 2013.

[13] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, “Detecting relay attacks with timing-based protocols,” in *Proc. 2nd ACM*

symp. Inf., Comput. Commun. Security, pp. 204-213, Mar. 2007.

[14] J. Munilla and A. Peinado, "Distance bounding protocols for RFID enhanced by using void challenges and analysis in noisy channels," *Wirel. Commun. Mob. Comput.*, vol. 8, no. 9, pp. 1227-1232, 2008.

[15] R. Trujillo-Rasua, B. Martin, and G. Avoine, *Distance-bounding facing both mafia and distance frauds:* Technical report(2014), Retrieved Aug., 18, 2014, from http://arxiv.org/abs/1405.5704v1.

[16] G. P. Hancke and M. G. Kuhn, "An RFID distance bounding protocol," in *1st Int. Conf. Security and Privacy for Emerging Areas in Commun. Netw. (SecureComm 2005)*, pp. 67-73, Sept. 2005.

[17] H. S. Ahn, E. J. Yoon, K. D. Bu, and I. G. Nam, "A Storage and Computation Efficient RFID Distance Bounding Protocol," *J. KICS*, vol. 35, no. 9, pp. 1350-1359, 2010.

권 혜 진 (Hye Jin Kwon)

2007년 2월 : 경북대학교 수학과 학사 졸업

2009년 2월 : 경북대학교 정보보호학과 석사

2009년 3월~현재 : 경북대학교 전자공학과 박사과정

<관심분야> 정보보호, 암호이론, 네트워크 보안

김 순 자 (Soon Ja Kim)

1975년 2월 : 경북대학교 수학교육학과 학사

1977년 2월 : 경북대학교 수학과 석사

1988년 2월 : 계명대학교 수학과 박사

1993년 4월~현재 : 경북대학교 전자공학부 교수

<관심분야> 정보보호 및 보안기술, 정보보호 응용기술