RFID 환경에서 중계공격을 방지를 위한 2BP Distance Bounding 프로토콜 연구

정윤성*, 김형주*, 이아영**, 전문석*
*숭실대학교 컴퓨터공학과
**숭실대학교 정보과학대학원 정보보안학과
*숭실대학교 컴퓨터공학과
e-mail: edward.ysj@ssu.ac.kr, hyungjoo.kim@ssu.ac.kr, layinc@daum.net, mjun@ssu.ac.kr

Study on 2BP Distance Bounding Protocol to Prevent Relay Attack in RFID environment

Youn-Sung Jung*, A-Young Lee**, Moon-Seog Jun*
*Dept of Computer Science, Soongsil University
**Dept of Information Security, Soongsil University
Graduate School of Infromation Sciences

요 약

RIFD 시스템은 개체 인증, 전자결제 등 다양한 분야에서 사용되고 있다. 무선통신의 특성상 악의적인 공격자로부터 중계공격이 가능하여 공격자가 정당한 사용자로 가장할 수 있다. 이러한 중계공격을 예방하기 위하여 Distance Bounding이라는 개념의 프로토콜이 제안되어 왔다. 하지만, 기존 연구는 태그 ID 전달의 기밀성을 보장하지만 ID 검색의 비효율성 및 불필요한 두 번째 저속 단계가 존재하는 단점이 있다. 따라서 본 논문은 ID의 검색 없고, 시도 값과 응답 값을 2bits로 하여 마지막 저속 단계를 생략하며, 고속 단계에서 공격자의 공격 탐지 및 Terrorist 공격에 대하여 $(1/2)^n$의 공격 성공률을 갖는 2BP(2Bit 2Phase) Distance Bounding 프로토콜을 제안한다.

1. 서론

태그와 리더, 데이터베이스로 구성된 RFID(Radio Frequency IDentification) 시스템은 개체 인증, 전자결제, 유통관리 등 다양한 서비스를 제공하고 있다. 하지만 기존의 RFID와 관련된 연구는 태그의 기밀성 있는 인증 및 태그의 추적을 불가능하게 하는 방법 등 보안성을 제공하는데 국한되어 있다. 기존 연구는 공격자가 정당한 사용자로 가장하는 중계공격(Relay Attack)에는 취약하다. 따라서, 중계공격을 방지하고 태그의 기밀성 있는 인증 및 태그의 추적을 불가능하게 하는 방법이 필요하다.

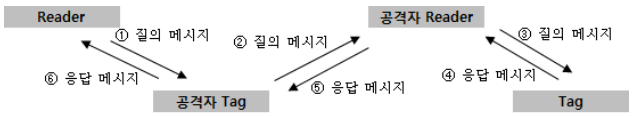
본 논문은 2장에서 중계 공격과 Distance Bounding 프로토콜과 중계공격 전략을 살펴보고, Distance Bounding 프로토콜의 적용 방법을 알아본다. 3장에서는 프로토콜을 제안하며, 4장에서는 제안하는 프로토콜과 기존 프로토콜의 효율성 및 보안성을 비교 분석하며 5장에서 결론을 맺는다.

2. 관련연구

2.1 중계공격

중계공격은 Chess Grand Master Problem[2]에 기반한 공격방법이다.

(그림 1)과 같이 인증 프로토콜 과정에서 리더와 태그 사이의 질의 메시지와 응답 메시지를 위조나 변조 과정 없이 전송하여 정당한 태그의 정보로 인증하거나 리더와 태그사이의 물리적인 거리를 속일 수 있다. 공격자의 리더와 태그사이는 Bluetooth나 3G, WiFi 등으로 통신하며 리더와 공격자 태그, 공격자 리더와 태그 사이는 RFID를 이용하여 통신한다.



(그림 1) 중계공격 예시

2.2 Distance Bounding 프로토콜

Distance Bounding 프로토콜은 Brands와 Chaum에 의해 제안되었으며 (저속 단계→고속 단계)나 (저속 단계→고속 단계→저속 단계)로 구성된다. 처음 저속 단계에서는 리더와 태그의 인증에 필요한 값을 공유하고 다음 단계에서 필요한 값들을 계산한다. 고속 단계에서는 리더와 태그 간의 거리 측정을 위해 빠른 속도의 데이터 교환이 수행되며 마지막 저속 단계는 상호인증을 위한 값을 전송한다. 프로토콜이 상호인증하지 않거나 기밀성 없는 ID 전달할 경우 마지막 저속 단계는 생략될 수 있다.

고속 단계는 Distance Bounding 프로토콜의 핵심 단계

로 연산 속도로 인한 거리 측정 지연을 막기 위해서 암호학적 연산을 수행하지 않고 비교연산, XOR 연산, 연접 연산 등의 매우 빠른 연산만을 수행한다. 고속 단계에서 리더(검증자)는 태그(증명자)에게 시도(challenge)값을 전송하며 태그는 시도 값에 대한 응답(response) 값을 리더에게 전송한다. 이러한 시도 값과 응답 값의 전송 및 수신은 매우 빠른 속도로 반복된다. 태그의 응답 값은 최대 라운드트립 시간 이내에 수신되어야 한다. 만약 모든 응답 값이 최대 라운드트립 시간 이내에 수신된다면 태그는 리더에게 물리적으로 근접해 있다는 것을 증명할 수 있다.

2.3 중계공격 전략

1) Mafia 공격

공격자는 태그와 주고받는 데이터를 위조 및 변조 할 수 없으며 단순히 정보를 중계만하는 공격이다. 공격자의 리더는 고속 단계의 시작 전 리더의 시도 값을 예측하여 태그에게 전송하여 응답 값을 얻는다. 리더가 고속 단계를 시작하면 공격자는 태그의 응답 값을 위조 및 변조 없이 리더에게 전송한다.

2) Terrorist 공격

공격자는 태그와 주고받는 데이터를 위조 및 변조 할 수 있다. 공격자는 리더와 태그 사이에서 저속 단계를 중계하고 리더가 고속 단계를 시작하기 전 공격자의 리더가 태그에게 시도 값을 전송하여 응답 값을 얻는다. 리더가 고속 단계를 시작하여 시도 값을 전송하면 공격자는 태그의 응답 값을 이용하여 새로운 응답 값을 생성하여 리더에게 전송한다.

2.4 The Swiss-Knife RFID Distance Bounding 프로토콜

Kim 등이 제안한 The Swiss-Knife RFID Distane Bounding[3] 프로토콜(이하 SDP)은 태그의 ID를 전달의 기밀성을 보장하는 상호인증 프로토콜이다.

2.4.1 용어 및 표기 설명

ID : n bits의 태그 ID

N_t : 태그가 생성하는 n bits의 의사난수 수열

N_r : 리더가 생성하는 n bits의 의사난수 수열

A_t : 태그가 미리 정해놓은 공개된 상수

k : 태그와 리더 둘 사이의 공유된 비밀 값

f_k : k를 키로 갖는 의사난수함수

2.4.2 프로토콜 구조

SDP는 (그림 2)와 같이 저속 단계→고속 단계→저속 단계로 구성된다.

1) 저속 단계

처음 저속 단계에서 리더와 태그는 의사난수 수열 N_r과 N_t를 교환하고 f_k를 이용하여 $S^0 = f_k(A_t, N_t)$를 계산하고 S^0와 k를 XOR 연산하여 S^1을 생성한다. 리더는 시도에 사용되는 의사난수 수열 c를 생성한다.

2) 고속 단계

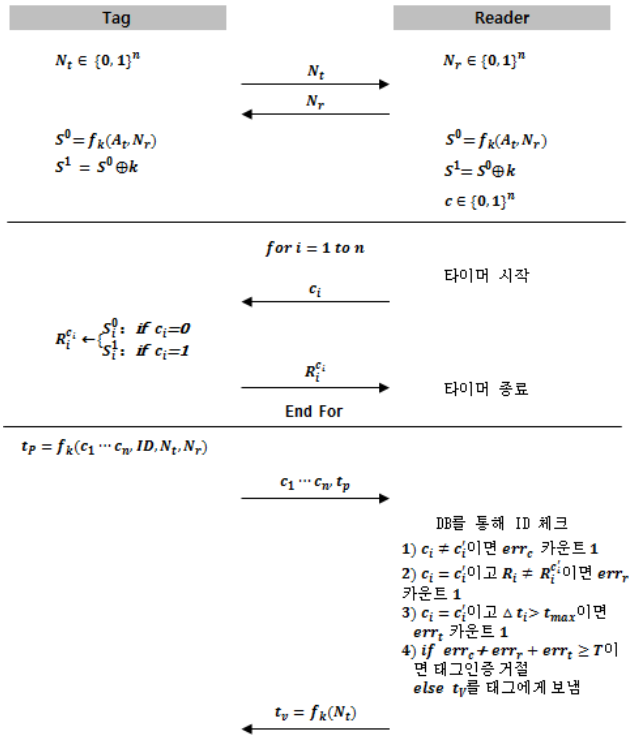
리더는 저속 단계에서 생성한 시도 값 c_i를 태그에게 전송하며 태그의 응답 값에 대한 라운드트립 시간을 측정한다.

태그는 리더가 보낸 c_i가 0일 경우 응답 값을 S_i^0으로 하며 c_i가 1일 경우 S_i^1로 하여 응답한다.

3) 저속 단계

태그는 $t_p = f_k(c_1 \cdots c_n, ID, N_t, N_r)$를 계산하여 $c_1 \cdots c_n$과 t_p를 리더에게 전송한다.

리더는 태그가 보내온 t_p를 생성하는 값 중 ID를 제외한 값과 t_p를 데이터베이스로 보낸다. 데이터베이스는 자신이 보유한 모든 ID와 이용하여 데이터베이스에 저장된 ID를 체크한다. 또한 태그가 전송한 c_i와 R_i를 체크하여 상한 값 이상의 에러일 경우 태그의 인증을 거절하며 상한 값 이하일 경우 $t_v = f_k(N_t)$를 생성하여 태그에게 전송하여 상호인증 한다.



(그림 2) The Swiss-Knife RFID Distance Bounding 프로토콜

2.4.3 프로토콜 특징

SDP는 상호인증과 무선 통신에서 발생할 수 변조와 전송 지연에 대한 저항성을 제공하는 프로토콜이다. 프로토콜에 대한 Mafia 공격 성공률은 리더의 시도 값이 0이나 1이기 때문에 $(1/2)^n$이며 Terrorist 공격의 경우 공격

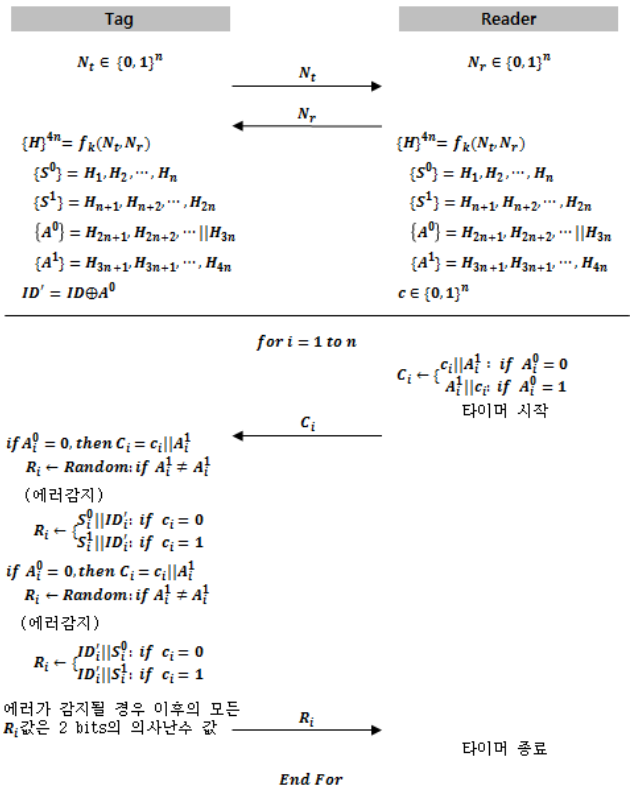
자의 리더가 정당한 태그에게 시도 값을 0으로만 보낸다면 정당한 리더의 시도 값의 절반을 알기 때문에 $(3/4)^n$의 성공률을 갖는다.

SDP는 태그의 ID의 기밀성을 보장하지만 데이터베이스에서 태그가 전송한 정보 및 비밀 값 k를 이용하여 전수조사 해야 하는 비효율적인 검색구조이다. 또한 고속 단계의 안전성은 전송 bits에 의존하는데 마지막 저속 단계의 연산은 프로토콜의 안전성에 무의미하기에 프로토콜의 수행시간을 증가시키는 비효율을 갖는다.

3. 제안하는 2BP Distance Bounding 프로토콜

제안하는 2BP(2bits 2Phase) Distance Bounding 프로토콜은 태그 ID 전송에 기밀성 및 전방향 안전성을 보장하며 위치추적 공격과 중계 공격으로부터 안전하며 태그 ID의 검색이 필요 없는 상호 인증 프로토콜이다.

2BP Distance Bounding 프로토콜은 고속 단계의 시도 값과 응답 값을 2bits로 구성하여 Post-ask 공격에 대한 안전성을 향상 시켰으며 저속 단계→고속 단계로 구성하여 프로토콜 수행시간을 단축시켰다.



(그림 3) 2BP Distance Bounding 프로토콜 구조

3.1 용어 및 표기 설명

ID : n bits의 태그 ID

N_t : 태그가 생성하는 n bits의 의사난수 수열

N_r : 리더가 생성하는 n bits의 의사난수 수열

k : 태그와 리더 둘 사이의 공유된 비밀 값

f_k : k를 키로 갖는 의사난수함수로 2n bits를 입력 값으로 받아서, 4n bits를 출력

H : f_k로 생성되는 4n bits의 난수 수열

$\|$: 연접연산

$\oplus$: Execlusive-OR(XOR) 연산

c : 리더가 생성하는 n bits의 의사난수 수열

3.2 프로토콜의 가정

1) 태그와 리더는 사전에 공유된 비밀 값 k를 알고 있다.
2) 공격자는 사전에 공유된 비밀 값 k를 알 수 없다.
3) 프로토콜은 Slow Phase, Fast Phase 의 2단 구성으로 이루어진다.

3.3 2BP Distance Bounding 프로토콜 구조

제안하는 2BP Distance Bounding 프로토콜은 (그림 3)과 같은 구조를 가지며 리더와 태그 간에 2간계의 통신을 수행한다.

1) 저속 단계

리더와 태그는 의사난수 수열 N_r과 N_t를 교환하고 f_k를 이용하여 $H^{4n} = f_k(N_t, N_r)$를 계산한다. H^{4n}은 n bits 블록 S^0, S^1, A^0, A^1으로 각각 나누어진다. 리더는 시도(challenge)에 사용되는 의사난수 수열 c를 생성하고 태그는 자신의 ID와 A^0를 XOR연산하여 ID'을 구한다.

2) 고속 단계

리더는 저속 단계에서 생성한 A_i^0과 c를 이용하여 시도 값 C_i를 생성한다. C_i는 A_i^0이 0일 경우 $C_i = c_i \| A_i^1$로 구성되고 A_i^0가 1일 경우 $C_i = A_i^1 \| c_i$로 구성된다. 리더는 C_i를 태그로 전송하여 태그의 응답 값에 대한 라운드트립 시간을 측정한다.

태그는 A^0을 알고 있으므로 리더가 전송한 C_i를 $C_i = A_i^1 \| c_i$와 $C_i = c_i \| A_i^1$로 구별할 수 있다. 태그는 A_i^0가 0일 경우 $R_i = ID_i' \| S_i^0$나 $R_i = ID_i' \| S_i^1$을 생성하며 A_i^0가 1일 경우 $R_i = S_i^0 \| ID_i'$나 $R_i = S_i^1 \| ID_i'$를 생성한다. 이때 S_i^0과 S_i^1는 리더가 보낸 c_i가 0일 경우 S_i^0를 전송하고 c_i가 1일 경우 S_i^1로 전송한다. 만약 리더가 전송한 A_i^1가 $A_i^1 \neq A_i^1$일 경우 이후의 태그는 응답 값 R_i를 의사난수 값으로 구성하며 공격자의 공격을 무력화 한다.[1]

4. 공격 가능성 및 보안성 분석

4.1 공격 가능성

Mafia 공격에서 공격자는 정당한 리더의 2bits 시도 값을 맞춰야 하기 때문에 $(1/4)^n$의 공격확률은 갖는다. 제

<표 1> SDP와 2BP Distance Bound 프로토콜 비교

	제안하는 프로토콜	RDP[4]	TDP[5]	SDP[3]
Mafia 공격 성공률	$(1/2)^n$	$(1/2)^n$	$(1/2)^n$	$(1/2)^n$
Terrorist 공격 성공률	$(1/2)^n$	$(3/4)^n$	$(3/4)^n$	$(3/4)^n$
고속 단계에서 공격감지	YES	NO	NO	NO
태그 ID 검색시간	검색이 불필요	-	-	최대 데이터베이스의 모든 ID 비교 검색
태그 ID 획득 위치	리더	-	-	데이터베이스
단계 구성	2단계	3단계	3단계	3단계
태그의 ID 익명성	YES	-	NO	YES
위치 추적 불가능성	YES	NO	NO	YES
전방향 안전성	YES	NO	NO	YES

안하는 논문의 시도 값이 2bits이기 때문에 SDP와 비교 시 $(1/4)^n$이 아닌 $(1/4)^{n/2}=(1/2)^n$으로 표기한다.

Terrorist 공격의 경우 공격자는 정당한 리더의 시도 값 중 A_i^0의 값과 그 위치를 정확히 맞추어야 한다. 만약 공격자의 리더가 전송한 A_i^0이 $A_i^0 \neq A_i^0$라면 태그는 프로토콜의 종료까지 모든 응답 값 R_i를 의사난수로만 전송한다. 따라서 공격자의 공격 성공률은 $(1/4)^n$이며 SDP와 비교 시 $(1/4)^{n/2}=(1/2)^n$이 된다.

4.2 태그의 익명성 및 위치 추적 가능성과 전방향 안전성

태그의 ID 익명성: 태그의 ID는 직접 전송되지 않고 $f_k(N_t,N_r)$의 결과 값 중 한 블록인 A^0과 XOR 연산되어 A^0의 값에 따라 첫 번째 bit나 두 번째 bit로 연접되기 때문에 태그의 ID는 노출되지 않고 리더로 전송된다.

태그의 위치 추적 불가능성: 리더와 태그 간의 통신 시에 태그는 항상 새로운 N_t로 응답한다. 리더의 질의에 항상 다른 값을 생성하여 응답하기 때문에 태그의 위치를 추적하는 것은 불가능하다.

전방향 안전성: 리더와 태그 간에 전송되는 데이터는 매 인증마다 새로운 의사난수 수열 N_r과 N_t, c를 사용하기 때문에 전방향 안전성을 만족한다.

4.3 2BP Distance Bounding 프로토콜의 효율성

<표 1>는 제안하는 2BP Distance Bounding 프로토콜과 기존에 제안되었던 SDP, RDP[4], TDP[5]를 비교하여 정리한 것이다. 2BP Distance Bounding 프로토콜 모두 태그의 ID 익명성, 태그의 위치 추적 불가능성, 전방향 안전성을 보장하며 고속 단계에서 태그는 ID와 A^0을 XOR 한 값을 리더에게 전송하여 ID 검색이 필요 없다. 프로토콜을 (저속 단계→고속 단계)의 2단계로 구성하여 불필요한 마지막 저속 단계를 생략하였으며 고속 단계에서 공격자의 공격이 감지가능하다. 또한 Terrorist 공격 성공률이 $(1/2)^n$이었던 기존 프로토콜과 비교 시 Terrorist 공격 성공률 $(3/4)^n$로, n이 10일 경우 기존 프로토콜은 약 5.631%의 성공률을 갖지만 2BP Distance Bounding 프로토콜 약 0.097%의 성공률로 현저히 낮은 성공률을 갖는다.

5. 결론

본 논문은 RFID 시스템에 대한 중계공격을 예방하며, 태그 ID의 안전한 전송을 보장한다. 고속 단계에서의 시도 값과 응답 값을 2bits로 구성하여 공격자의 공격을 감지 할 수 있으며 Terrorist 공격 성공률이 $(1/2)^n$로 기존에 제안된 SDP와 비교 시 현저히 낮은 확률을 갖는다. 또한 고속 단계 이후의 불필요한 저속 단계를 생략함으로써 프로토콜의 수행시간 효율을 증가시켰다.

일반적인 Distance Bounding 프로토콜은 1bit의 시도 값과 응답 값을 갖지만 본 논문은 2bits의 시도 값과 응답 값을 갖는다. 따라서 향후, 2bits로 구현 시 발생 가능한 문제점을 연구해 나갈 것이다.

참고문헌

[1] Chong Hee Kim, Gildas Avoine, "RFID Distance Bounding Protocols with Mixed Challenges" IEEE Transaction on Wireless Communications, 2011

[2] J. H. Conway. “On Numbers and Games” Number 6 in London Mathematical Society Monographs. Academic Press, London-New-San Francisco, 1976.

[3] Chong Hee Kim, Gildas Avoine, Francois Koeune, Francois-Xavier, Stadaert, Olivier Pereira, “The Swiss-Knife RFID Distane Bounding Protocol”, Springer Berlin, ICISC 2008, vol 5461, pp.98-115 , 2008

[4] Gerhard P. Hancke, Markus G. Kuhn, “An RFID Distance Bounding Protocol”, IEEE, SecureComm, [4] C.Meadows, pp.67-73, 2005

[5] Jason Reid, Juan M. Gonzalez Nieto, Tee Tang, Bouchra Senadji ,“Detecting Relay Attacks with Timing-Based Protocols”, ACM, ASIACCS, pp.204 - 213, March 2007