개선한 Munilla-Peinado RFID 경계 결정 프로토콜

안해순*, 윤은준**, 부기동***, 남인길****
*대구대학교 기초교육원 컴퓨터과정
**경북대학교 전자전기컴퓨터학부
***경일대학교 컴퓨터공학과
****대구대학교 컴퓨터·IT공학부
e-mail:ahs221@hanmail.net

Improved Munilla-Peinado's RFID Distance Bounding Protocol

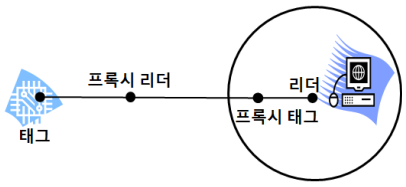
Hae-Soon Ahn*, Eun-Jun Yoon**, Ki-Dong Bu***, In-Gil Nam****
*Dept of Computer Information Engineering, Dae-gu University
**School of Electrical Engineering and Computer Science Kyungpook National University
***Dept of Computer Engineering, Kyung-il University
****School of Computer IT Engineering, Dae-gu University

요 약

최근 RFID 태그들이 근접 인증(proximity authentication)을 위해 사용자의 위치나 상황을 이용하여 통신하기 때문에 위치 기반 공격인 중계 공격(relay attack)에 매우 취약함이 증명되었다. 이러한 중계 공격들을 방지하기 위해 리더와 태그사이의 메시지 송수신 왕복 시간을 측정하는 경계 결정(distance-bounding) 프로토콜이 한 해결책으로 연구되고 있다. 2008년에 Munilla와 Peinado는 Hancke-Kuhn이 제안한 프로토콜을 수정하여 보이드(void) 기법을 적용한 RFID 경계 결정 프로토콜을 제안하였다. 공격자에게 n번의 왕복에서 $(5/8)^n$으로 성공 확률을 감소시켰지만, 저비용 수동형 태그에서 많은 통신량과 저장 공간을 요구하므로 비효율적이다. 따라서 본 논문에서는 태그측의 해쉬 함수 연산량을 줄이고, 적은 저장 공간을 요구함으로써 저비용 RFID 시스템에 적합한 효율적인 RFID 경계 결정 프로토콜을 제안한다.

1. 서론

RFID 기술은 최근 급속도로 발전하고 있는 분야로서 국가 주도로 신성장동력 산업으로 선정되었으며, 현재 125kHz에서 2.45GHz까지 다양한 주파수 대역에서 사용할 수 있는 시스템들이 개발되었다. RFID 장치나 비접촉식 스마트카드는 근접 인증(proximity authentication)을 위해 사용자의 위치나 상황을 이용하여 통신을 하기 때문에 위치 추적을 통해 합법적인 사용자로 위장한 공격자를 빨리 감지하여 서비스를 제공받을 수 없게 해야 한다[1]. 이러한 이유로 최근 근거리 RFID 인증 시스템상에서 근접 인증에 사용되는 수동형 RFID 태그들이 마피아 위조(mafia fraud) 공격, 테러리스트 위조(terrorist fraud) 공격과 같은 경계 위조(distance fraud)와 중계 공격(relay attack)들에 매우 취약함이 증명되었다[2-5]. RFID 시스템에서의 중계 공격은 그림 1에서 보여지는 것처럼 중간자(man-in-the-middle) 공격의 종류로서 실제 리더와 공격자의 프록시 태그와 통신하고, 프록시 리더는 정당한 태그와 통신하여 인증 정보를 획득한다. 획득한 인증 정보를 담고 있는 프록시 태그는 실제 리더와 통신하게 됨으로써 프록시 태그로부터 수신된 인증 데이터를 실제 리더가 인증을 하게 된다. 이러한 중계 공격을 방지하기 위해 많은 연구들이 진행되고 있다. Desmedt[2]등은 송수신 메시지의 왕복 시간을 측정하여 최초로 경계 결정 개념을 소개하였으며, Brands와 Chaum[3]은 Desmedt의 아이디어를 기반으로 경계 결정 프로토콜을 처음으로 설계하여 도전-응답(challenge-respond) 기반 암호 프로토콜에서 단일 비트 왕복 중계 시간을 측정하는 경계 결정 프로토콜을 최초로 제안하였다.

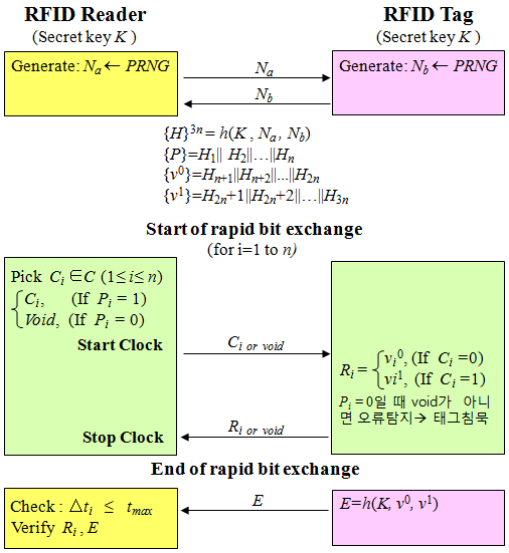


(그림 1) 중계 공격 개요

2005년에 Hancke과 Kuhn[4]은 RFID 환경에 적합한 경계 결정 프로토콜을 제안하였지만 공격자에게 n번의 왕복에서 $(3/4)^n$의 성공 확률을 제공하여 중계 공격을 완벽히 방어할 수는 없었다. 2008년에는 Munilla[5]등이 Hancke-Kuhn의 프로토콜을 수정하여 공격자의 성공 확률을 감소시키기 위해 보이드(void) 기법을 적용한 공격자의 성공 확률을 $(5/8)^n$으로 감소시켜주는 프로토콜을 제안하였다. 하지만 Munilla등이 제안한 프로토콜(MP 프로토콜)은 태그의 많은 저장 공간 낭비와 두 번의 해쉬 함수 연산을 수행하여 비효율적이다. 따라서 본 논문에서는 Munilla등이 제안한 MP RFID 경계 결정 프로토콜을 개선하여 태그의 높은 저장 공간 효율성을 제공할 뿐만 아니라 해쉬 함수의 연산량을 줄여줌으로써 태그의 부담을 줄여줄 수 있는 개선된 RFID 경계 결정 프로토콜을 제안한다.

2. MP RFID 경계 결정 프로토콜 소개

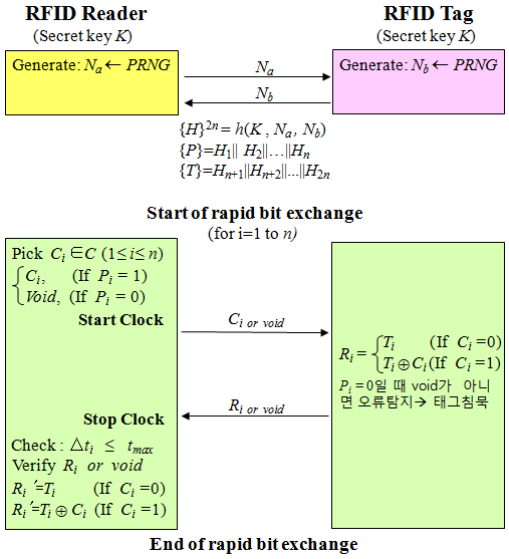
그림 2는 Munilla등[5]이 제안한 MP RFID 경계 결정 프로토콜의 전체적인 구성을 보여주며, 사전에 리더와 태그는 비밀키 K를 공유하고 있다.



(그림 2) MP RFID 경계 결정 프로토콜

3. 제안하는 RFID 경계 결정 프로토콜

그림 3은 Munilla등이 제안한 MP 프로토콜을 개선한 RFID 경계 결정 프로토콜의 전체적인 구성과 동작 과정을 보여준다.



(그림 3) 제안하는 RFID 경계 결정 프로토콜

4. 효율성 분석

제안한 프로토콜에 대한 단일 비트 왕복 전송 시간 추론 및 검증 알고리즘은 그림 4와 같이 수행된다. 검증 루틴은 n비트만큼 수행하지만, 비트 왕복 전송 시간이 경계 결정 상위 값을 초과하게 되면 더 이상 루틴을 수행하지 않고 검증을 중단하게 된다. 표 1은 제안한 RFID 경계 결정 프로토콜과 MP RFID 경계 결정 프로토콜의 효율성을 비교한 표이다. 본 논문에서 제안한 프로토콜에서는 RFID 리더와 태그측의 저장 공간을 34% 줄여주어 저장 공간의 효율성을 제공하고, 태그의 해쉬 함수 연산량 또한 34% 줄여주어 더욱 효율적임을 알 수 있다.

```
count_max = max error value;
t_max = threshold time;
count = 0;
for (i = 1 to n)
{
  if (count == count_max) {중단;}
  else {
        if (P_i == 0) void 검증
        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

<표 1> RFID 경계 결정 프로토콜의 효율성 비교

프로토콜 / 연산종류	MP 프로토콜[5]		제안한 프로토콜	
	태그	리더	태그	리더
해쉬 연산량	2	1	1	1
저장공간(bit)	$3n$	$3n$	$2n$	$2n$
리더와 태그간 통신메시지량	$3h()+6nbit$		$2h()+4nbit$	

n : 비트열 개수 / $h()$: 해쉬 연산 개수

6. 결론

본 논문에서는 근접 인증에 사용되는 수동형 RFID 태그 환경에서 발생되는 중계 공격들을 방어할 수 있는 개선된 RFID 경계 결정 프로토콜을 제안하였다. 제안한 프로토콜은 MP 프로토콜을 개선하여 XOR 연산을 기반으로 하고, 태그 측의 저장 공간의 효율성 및 해쉬 연산량을 줄여줌으로써 수동형 저비용 태그와 잡음 환경 그리고 고속 애플리케이션에서의 사용에 매우 적합하도록 설계하였다.

참고문헌

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

[2] Y. Desmedt. Major security problems with the “”Unforgeable”” (Feige)-Fiat-Shamir proofs of identiy and how to overcome them. In SecuriCom ‘’88, pages 15 - -17, 1988.

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

[4] 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.

[5] 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.