# 다중 비트 시도와 응답을 이용한 RFID 거리 한정 프로토콜†

# (RFID Distance Bounding Protocol Using Multiple Bits Challenge and Response)

**전 일 수*, 윤 은 준****
(Il-Soo Jeon and Eun-Jun Yoon)

**요 약** RFID 시스템에서 중계 공격에 저항하기 위해 리더와 태그 간의 시도와 응답에 소요된 1비트의 왕복 여행시간 측정을 이용한 거리 한정 프로토콜이 주로 사용된다. 이러한 프로토콜에서 1비트 시도와 응답에 대한 중계 공격의 성공확률을 줄일 수 있으면 효율적인 거리 한정 프로토콜을 만들 수 있다. 본 논문에서는 Hancke와 Khun이 제안한 1비트 시도와 응답 기반의 RFID 거리 한정 프로토콜을 2비트 시도와 응답 기반으로 수정한 효율적인 RFID 거리 한정 프로토콜을 제안한다. n번의 시도와 응답에 대한 중계 공격의 성공확률이 제안된 프로토콜에서는 (7/16)n으로 (3/4)n인 Hancke와 Khun의 프로토콜보다 훨씬 낮다.

**핵심주제어 :** RFID, 중계공격, 거리 한정 프로토콜

**Abstract** To resist the relay attacks in RFID system, it is commonly used RFID distance bounding protocols using the round trip time measurement for 1 bit challenge and response between a reader and a tag. If the success probability of relay attacks for the 1 bit challenge and response can be reduced in these protocols, it is possible to make an efficient distance bounding protocol. In this paper, we propose an efficient RFID distance bounding protocol based on 2 bit challenge and response which is modified the RFID distance bounding protocol proposed by Hancke and Khun based on 1 bit challenge and response. The success probability of relay attack for the proposed protocol is (7/16)n for the n times of challenge and response, which is much lower than (3/4)n given by Hancke and Khun's protocol.

**Key Words :** RFID, Relay Attack, Distance Bounding Protocol

## 1. 서 론

오늘날 RFID 시스템은 사람이나 사물을 식별하는 수단으로뿐만 아니라 지불시스템이나 접근제어 시스템 등과 같은 응용에 유용하게 사용되고 있다. RFID 시스템이 가져다주는 유용성과 편리함 때문에 이들을 사용하는 응용이 급속적으로 증가하고 있는 추세이지만, RFID 인증(authentication) 시스템은 위치(location)와 관련한 거리 속임 공격(distance fraud attack)과 중계 공격(relay attack)인 마피아 공격(mafia attack)과 테러리스트 공격(terrorist attack)에

† 본 연구는 금오공과대학교학술연구비에 의하여 연구된 논문
* 금오공과대학교 전자공학부, 제1저자
** 경일대학교 사이버보안학과, 교신저자

취약하다[9].

거리 속임 공격은 태그(tag)가 지정된 범위 밖에서 동작하여 공격하는 것이고, 마피아 공격은 진짜 리더(reader)와 진짜 태그 사이에서 가짜 리더와 가짜 태그를 사용하여 진짜 태그가 모르는 상태에서 공격을 행하는 일종의 중간자 공격이다. 그리고 테러리스트 공격은 공격자가 적법한 태그와 공모하여 그로부터 시스템에 접근하는데 필요한 정보를 받아서 자신을 위장하여 행하는 공격이다. 이러한 공격들은 통신 프로토콜 스택의 응용 계층에서 동작되는 암호 프로토콜로는 쉽게 방지하기가 어려우므로 이에 대응하는 수단으로 통신 프로토콜의 물리 계층에 밀접하게 통합되어 동작하는 거리 한정(distance bounding) 프로토콜을 일반적으로 사용한다. 거리 한정 프로토콜에서는 리더는 태그가 알고 있는 비밀정보뿐만 아니라 태그가 한정된 범위 내에 있는 지도 확인한다.

1993년에 Brands와 Chaum[1]이 처음으로 거리 한정 프로토콜을 제안하였고, 2005년에 Hancke와 Khun[2]이 RFID 거리 한정 프로토콜(향후 HKP로 표기함)을 제안하였다. HKP는 RFID 시스템에서 위치기반의 공격에 저항할 수 있도록 하기 위해 리더와 태그 사이에 1비트의 왕복 여행 시간을 측정하는 기법을 기반으로 하고 있다. 만약 거리 속임 공격이나 중계 공격이 존재하면 리더로부터 시도비트 전송 후 태그로부터 응답비트가 도착하기까지의 시간이 허용시간 한계치를 초과하게 되므로 이러한 공격을 탐지할 수 있다. HKP는 RFID 거리 한정 프로토콜 연구 분야에서 새로운 한 기준점이 되었으며, 그 후 HKP는 많은 연구[3-11]의 참고논문으로 활용되고 있다. 그런데 HKP에서는 마피아 공격으로 알려진 중계(relay) 공격에 대한 성공 확률이 (1/2)n이 아닌 (3/4)n이다. 여기서 n은 1비트의 시도와 응답(challenge and response) 회수를 말한다. HKP가 제안된 후 1비트의 시도와 응답 반복구조를 이용하면서 중계 공격의 성공확률을 줄이기 위한 연구[3-8]가 꾸준히 진행되었다.

본 논문에서는 HKP 기반 위에서 중계 공격 성공확률을 줄이기 위한 방법으로 HKP에서와 같이 1비트의 시도와 응답 기법이 아닌 2비트 시도와 응답 기법을 제안하고, 이를 이용한 RFID 거리 한정 프로토콜을 제안한다. 또한 제안한 프로토콜은 1비트 시도와 응답 기반의 프로토콜보다 훨씬 효율적임을 보인다.

본 논문의 구성은 다음과 같다. 2장에서는 HKP를 비롯한 관련연구와 프로토콜 기술에 필요한 기호 표기법을 소개하며, 3장에서는 본 연구에서 제안하는 거리 한정 프로토콜을 소개한다. 그리고 4장에서는 제안된 프로토콜에 대한 성능을 분석하고 5장에서는 결론을 맺는다.

## 2. 관련연구

본 장에서는 본 연구에 대한 선행연구의 근간이 되는 HKP를 소개하고, 중계공격에 대한 성공확률을 줄이기 위한 연구결과들을 간략히 소개한다. 그리고 본 논문에서 언급되는 모든 프로토콜 기술에 사용되는 기호의 표기법을 소개하며 표 1에서 그 표기법을 정의하였다.

<표 1> 기호 표기법

| 기호 | 정의 |
|---|---|
| $x$ | 리더와 태그가 공유하는 비밀값 |
| $N_r$, $N_t$ | 각각 리더 및 태그에 의해 생성된 난수 |
| $f_x()$ | 비밀값 x를 사용하는 의사난수 함수 |
| $R^i$ | 태그에서 생성되는 i번째 비트열 |
| $R^{i}{}'$ | 리더에서 생성되는 i번째 비트열 |
| $c_i$, $r_i$ | 각각 i번째 시도 및 응답 비트(들) |
| $\triangle t_i$ | i번째 시도비트 전송후 응답 비트 도착까지의 시간 |
| $\triangle t_{max}$ | 시도 후 응답까지의 허용 시간 한계치 |
| $\|$ | 연결(concatenation) 연산자 |
| $\rightarrow$ | 메시지 전송 |

HKP는 1비트의 시도와 응답 반복구조를 이용하며, 프로토콜은 준비단계와 빠른 비트교환 단계로 구성되어 있다. 그 세부적인 과정을 다음에 기술하였고, 이를 그림 1에 요약하였다.

**[준비 단계]**

Step 1. 리더는 난수 Nr을 생성하여 태그에게 전송한다.

Step 2. 태그는 난수 Nt를 생성하고 x, Nr, Nt를 입력으로 하는 의사난수함수를 적용하여 길이가 2n인 비트열을 생성하고 이를 분할하여

각각의 길이가 n인 비트열 R0와 R1을 생성한 다음 Nt를 리더에게 전송한다.

$R^0 \| R^1 = f_x(N_r, N_t)$

$R^i = R_1^i \| R_2^i \| \cdots R_n$, 여기서 $i$는 $0 \le i \le 1$

Step 3. 리더는 x, Nr, Nt를 입력으로 하는 의사난수함수를 적용하여 길이가 2n인 비트열을 생성하고 이를 분할하여 각각의 길이가 n인 비트열 R0'와 R1'를 생성한다.

$R^{0'} \| R^{1'} = f_x(N_r, N_t)$

$R^{i'} = R_1^{i'} \| R_2^{i'} \| \cdots R_n^{i'}$, 여기서 $i$는 $0 \le i \le 1$

**[빠른 비트교환 단계]**

이 단계는 아래 기술한 과정을 n번 빠르게 반복한다.

Step 1. 리더는 임의의 이진수 한 비트, ci를 태그에게 보내고 바로 타이머를 작동시킨다.

Step 2. 태그는 받은 $c_i'$가 0이면 R0의 i번째 비트, $R_i^0$를, $c_i'$가 1이면 R1의 i번째 비트, $R_i^1$를 값으로 하는 ri를 리더에게 전송한다.

$r_i = R_i^{c_i'}$

Step 3. 리더는 ri를 수신하는 즉시 타이머를 중지시킨다. 그리고 $r_i' = R_i^{c_i}$를 생성하여 $r_i = r_i'$이면서 시도와 응답에 걸린 시간(타이머시간), $\Delta t_i$가 한계시간, $\Delta t_{max}$보다 작은지를 체크한다.

HKP가 제안된 후로 RFID 거리 한정 프로토콜에서 중계공격의 성공확률을 줄이기 위해 서명(혹은 메시지 인증 코드)를 포함하는 프로토콜[3,4]이 제안되었다. 그러나 빠른 비트교환을 위한 통신 채널은 백그라운드 노이즈에 매우 민감하기 때문에 그 채널로 서명을 전송하기는 어렵고 일반통신 채널로 전송해야 한다. 이렇게 되면 통신 비용이 증가되어 프로토콜 수행이 매우 느려질 뿐만 아니라 서명을 위한 계산 오버헤드가 수반되기 때문에 태그의 제한된 계산 능력을 감안하면 실질적인 적용에는 무리가 있다. 한편 Munilla 등[5,6]은 중계공격의 성공확률을 줄이기 위해 서명을 사용하지 않고 공시도(void-challenge)를 사용한 프로토콜을 제안하였다. 하지만 그 기법은 리더와 태그 간

| *Reader* | | *Tag* |
|---|---|---|
| | *Setup phase* | |
| $N_r \in_R \{0\|1\}^n$ | | |
| | $\xrightarrow{N_r}$ | $N_t \in_R \{0\|1\}^n$ |
| | | $R^0 \| R^1 = f_x(N_r, N_t)$ |
| | | $R^i = R_1^i \| R_2^i \| \cdots R_n,\ 0 \le i \le 1$ |
| | $\xleftarrow{N_t}$ | |
| $R^{0'} \| R^{1'} = f_x(N_r, N_t)$ | | |
| $R^{i'} = R_1^{i'} \| R_2^{i'} \| \cdots \| R_n^{i'},\ 0 \le i \le 1$ | | |
| | *Rapid bit exchange phase* | |
| | *for i=1 to n* | |
| $c_i \in \{0\|1\}$ | | |
| *Start clock* | | |
| | $\xrightarrow{c_i}$ | |
| | | $r_i = R_i^{c_i'}$ |
| | $\xleftarrow{r_i}$ | |
| *Stop clock* | | |
| $r_i' = R_i^{c_i}$ | | |
| *Check* $r_i = r_i'$ & $\Delta t_i < \Delta t_{max}$ | | |

<그림 1> HKP 요약

에 3가지의 상태, 즉 0과 1 이외에 void 상태를 가지기 때문에 물리적으로 구현하기가 어려운 단점을 가지고 있다.

최근 Gürel 등[7]은 리더의 시도에 대해 태그에서 비균일 스텝 (Non-Uniform Step) 접근 기법의 프로토콜(향후 NUSP로 표기함)을 제안하였고, 그림 2에 그 프로토콜을 요약하였다. 그림 2에서 알 수 있듯이, 리더와 태그간에 난수 Nr과 Nt를 교환하고 나서 의사난수 함수를 이용하여 각각 길이가 2n인 비트열을 생성한다. 그리고 빠른 비트 교환 단계에서 태그는 공유하는 비밀값 x를 기반으로 하여 반복시마다 비균일 스텝으로 길이가 2n인 비트열을 접근하여 응답 비트를 생성하고 이를 리더에게 전송한다. 이렇게 해서 빠른 비트 교환 단계가 끝이 나면 태그는 리더로부터 받은 시도 비트들을 리더에게 전송하고 리더는 태그로부터 받은 응답 비트들과 시도 비트들을 이용하여 오류를 체크한다.

Gürel 등[7]은 그들의 논문에서 서명을 사용하지 않

| *Reader* | | *Tag* |
|---|---|---|
| | *Setup phase* | |
| $N_r \in_R \{0\|1\}^n$ | | |
| | $\xrightarrow{N_r}$ | $N_t \in_R \{0\|1\}^n$<br>$R = f_x(N_r, N_t), \|R\| = 2n$<br>$j1 = 1, j2 = n$<br>$k1 = 0, k2 = 2n+1$ |
| | $\xleftarrow{N_t}$ | |
| $R' = f_x(N_r, N_t), \|R'\| = 2n$ | | |
| | *Rapid bit exchange phase*<br>*for i=1 to n* | |
| $c_i \in \{0\|1\}$<br>*Start clock* | | |
| | $\xrightarrow{c_i}$ | *if* $c_i' = 0$<br>*if* $x_{j1} = 0$<br>$k1 = k1+1, r_i = R_{k1}$<br>*else*<br>$k2 = k2-2, r_i = R_{k2}$<br>$j1 = j1+1$<br>*else*<br>*if* $x_{j2} = 0$<br>$k2 = k2-1, r_i = R_{k2}$<br>*else*<br>$k1 = k1+2, r_i = R_{k1}$<br>$j2 = j2-1$ |
| | $\xleftarrow{r_i}$ | |
| *Stop clock, Compute* $\Delta t_i$ | | |
| | *End of rapid bit exchange* | |
| | | $m = \{c_1', \ldots, c_n'\}$ |
| | $\xleftarrow{m}$ | |
| *compute* $r_i' \, using \, c_i$<br>$err_c = \#\{i : c_i \neq c_i'\}$<br>$err_r = \#\{i : c_i = c_i', r^i \neq r_i'\}$<br>$err_t = \#\{i : c_i = c_i', \Delta t_i > t_{\max}\}$<br>*Check* $err_c + err_r + err_t \leq \tau$ | | |

<그림 2> NUSP 요약

는 기존의 거리 한정 프로토콜들 중에서 중계공격 성공확률이 (3/4)n 보다 작은 프로토콜은 없고, 자신들의 프로토콜인 NUSP는 서명을 사용하지 않는 프로토콜로서 중계공격의 성공확률이 (1/2)n 이라고 주장하였다. 그러나 Abyaneh[8]는 그들의 프로토콜에 대한 중계공격의 성공확률이 (1/2)n이 아니라 (3/4)n 임을 보였다.

## 3. 제안한 프로토콜

본 절에서는 HKP를 수정하여 시도와 응답에 대한 공격자의 성공확률을 줄여서 필요한 시도와 응답의 라운드 수를 줄임으로 말미암아 프로토콜 수행시간을 감소시킬 수 있는 방법을 제안한다. 제안한 기법은 HKP에서 1비트의 시도와 응답 구조 대신에 2비트의 시도와 응답 구조를 사용한다. 제안한 프로토콜은 HKP에서와 같이 준비단계와 빠른 비트교환 단계로 구성되어 있다.

준비단계에서 리더와 태그는 서로 난수를 주고받으며 이들과 공유비밀값, x를 입력으로한 해쉬함수를 적용하여 길이가 4n인 임의의 비트열을 만들고, 이를 이용하여 각각의 길이가 n인 4개의 비트열을 만든다. 그리고 빠른 비트교환 단계에서는 리더에서 보내는 임의의 2비트 시도에 대해 태그에서 만들어진 비트열들 중 2개의 비트열에서 각각 지정된 1비트를 추출하여 전체 2비트로 응답한다. 그러면 리더에서는 만들어진 비트열 중에서 태그와 동일한 비트열의 동일 위치 비트들을 추출하여 이들을 태그로부터 응답된 비트들과 비교함으로써 바른 응답인지를 체크한다.

본 논문에서 제안한 프로토콜의 세부적인 절차를 다음에 기술하였고, 이를 그림 2에 요약하였다.

**[준비 단계]**

Step 1. 리더는 난수 Nr을 생성하여 태그에게 전송한다.

Step 2. 태그는 난수 Nt를 생성한 후 x, Nr, Nt를 입력으로 하는 의사난수함수를 적용하여 길이가 4n인 비트열을 생성한다. 그리고 이를 분할하여 각각의 길이가 n인 비트열 R0,R1,R2,R3을 생성한 다음에 Nt를 리더에게 전송한다.

$R^0 \| R^1 \| R^2 \| R^3 = f_x(N_r, N_t)$

| *Reader* | | *Tag* |
|---|---|---|
| | *Setup phase* | |
| $N_r \in_R \{0\|1\}^n$ | | |
| | $\xrightarrow{N_r}$ | $N_t \in_R \{0\|1\}^n$ |
| | | $R^0 \| R^1 \| R^2 \| R^3 = f_x(N_r, N_t)$ |
| | | $R^i = R_1^i \| R_2^i \| \cdots R_n,\ 0 \le i \le 3$ |
| | $\xleftarrow{N_t}$ | |
| $R^{0'} \| R^{1'} \| R^{2'} \| R^{3'} = f_x(N_r, N_t)$ | | |
| $R^{i'} = R_1^{i'} \| R_2^{i'} \| \cdots \| R_n^{i'},\ 0 \le i \le 3$ | | |
| | *Rapid bit exchange phase* | |
| | *for i=1 to n* | |
| $c_{i1} \in \{0\|1\}, c_{i2} \in \{0\|1\}$ | | |
| $c_i = \{c_{i1} \| c_{i2}\}$ | | |
| *Start clock* | | |
| | $\xrightarrow{c_i}$ | |
| | | $r_i = \left\{R_i^{c_{i1}'} \| R_i^{c_{i2}'+2}\right\}$ |
| | $\xleftarrow{r_i}$ | |
| *Stop clock* | | |
| $r_i' = \left\{R_i^{c_{i1}} \| R_i^{c_{i2}+2}\right\}$ | | |
| *Check* $r_i = r_i'$ & $\Delta t_i < \Delta t_{\max}$ | | |

<그림 3> 제안한 프로토콜 요약

$R^i = R_1^i \parallel R_2^i \parallel \cdots \parallel R_n^i$, 여기서
$0 \le i \le 3$

Step 3. 리더는 x, Nr, Nt를 입력으로 하는 의사난수 함수를 적용하여 길이가 4n인 비트열을 생성하고 이를 분할하여 각각의 길이가 n인 비트열 R0',R1',R2',R3'를 생성한다.
$R^{0'} \parallel R^{1'} \parallel R^{2'} \parallel R^{3'} = f_x(N_r, N_t)$
$R^{i'} = R_1^{i'} \parallel R_2^{i'} \parallel \cdots \parallel R_n^{i'}$, 여기서
$0 \le i \le 3$

**[빠른 비트교환 단계]**

이 단계는 아래 기술한 과정을 빠르게 n번 반복한다.

Step 1. 리더는 임의의 이진수 두 비트, ci를 태그에게 보내고 바로 타이머를 작동시킨다.
$c_i = \{c_{i1} \parallel c_{i2}\}$

Step 2. 태그는 $R^{c_i'}$의 i번째 비트, $R_i^{c_{i1}}$과 $R^{c_{i2}'+2}$의 i번째 비트, $R_i^{c_{i2}+2}$를 연결하여 비트열 ri를 만들고, 이 ri를 리더에게 전송한다.
$r_i = \left\{R_i^{c_{i1}'} \parallel R_i^{c_{i2}'+2}\right\}$

Step 3. 리더는 ri를 수신하는 즉시 타이머를 중지시킨다. 그리고 $r_i' = \left\{R_i^{c_{i1}} \parallel R_i^{c_{i2}+2}\right\}$를 생성하여 $r_i = r_i'$이면서 시도와 응답에 걸린 시간(타이머시간), $\triangle t_i$가 한계시간, $\triangle t_{max}$보다 작은지를 체크한다.

## 4. 성능평가

HKP가 제안된 후로 중계공격에 대한 성공확률을 줄이기 위해 서명기법을 사용[3,4]하거나 공시도 기법을 사용[5,6]한 프로토콜이 제안되었다. 하지만 관련연구에서 언급하였듯이, 서명기법을 사용한 프로토콜은 서명을 빠른 비트교환 통신 채널에서 전송하기 어렵고, 또한 계산 오버헤드 때문에 컴퓨팅 능력이 떨어지는 태그에 실제 적용하기가 어렵다. 그리고 공시도 기법을 사용한 프로토콜은 3가지 상태를 물리적으로 구현하기가 쉽지 않은 문제점을 가지고 있다. 따라서 그러한 기법들은 본 연구 결과의 성능평가 비교대상에서 제외하고, HKP와 최근 연구결과인 NUSP를 본 연구의 성능평가 대상으로 삼았다. 본 연구에서 제안한 프로토콜에 서명기법을 추가하거나 공시도 기법을 추가하여 프로토콜을 수정한다면 그에 대한 중계공격의 성공확률은 본 연구에서 제안한 프로토콜보다 더 낮아질 것이다.

HKP 및 NUSP는 한 라운드, 즉 1비트의 시도와 응답에 있어서 중계공격의 성공확률이 1/2이 아닌 3/4이다. 그 이유는 공격자가 진짜 리더로부터 시도비트를 받기 전에 임의의 값으로 미리 진짜 태그에게 질의를 하여 그 값에 대한 바른 응답을 확보해 놓는다. 이 경우 공격자가 시도비트를 정확히 예측할 확률과 그렇지 못할 확률이 각각 1/2이다. 그러므로 진짜 리더가 시도비트를 전송할 때 그 시도비트가 공격자가 미리 질의한 값과 같으면 성공확률은 (1/2)*1, 즉 1/2이 되고, 그렇지 않으면 공격자는 임의의 값으로 응답하며 이 경우의 성공확률은 (1/2)*(1/2), 즉 1/4이 된다. 따라서 전체적으로 (1/2)+(1/4), 즉 3/4의 공격 성공확률을 가지며, n번의 시도와 응답에 대한 공격 성공확률은 (3/4)n이 된다.

제안한 프로토콜에서는 한 라운드의 시도와 응답에 대한 중계공격의 성공확률은 7/16이 된다. 그 이유는 제안한 프로토콜에서 한 라운드에 2비트로 시도하고 2비트로 응답하므로 공격자가 시도비트들을 예측할 확률은 1/4이 되고 그렇지 못할 확률이 3/4이 된다. 그러므로 진짜 리더가 시도비트들을 전송할 때 그 시도비트들이 공격자가 미리 질의한 값과 같으면 성공확률은 (1/4)*1, 즉 1/4이 되고, 그렇지 않으면 공격자는 임의의 2비트로 응답하며 이 경우의 성공확률은 (3/4)*(1/4), 즉 3/16이 된다. 따라서 전체적으로 (1/4)+(3/16), 즉 7/16의 공격 성공확률을 가지며, n번의 2비트 시도와 응답에 대한 공격 성공확률은 (7/16)n이 된다.

표 2에 HKP 및 NUSP와 제안한 프로토콜의 시도와 응답 반복회수에 따른 중계공격의 성공확률을 나타내었다. 표 2에서 알 수 있듯이, 같은 공격 성공확률에 대해서 제안한 프로토콜에서의 반복회수는 HKP 및 NUSP에서 반복회수의 1/2보다도 작으므로 매우 효율적인 프로토콜임을 알 수 있다. 그리고 HKP에서는 프로토콜 수행을 위한 비트열이 2개가 필요하고 NUSP에서는 1개 필요하나 그 크기가 2n이므로 필요한 비트열의 길이는 두 프로토콜에서 동일하다. 그런데 제안한 프로토콜에서는 비트열 4개가 필요하지만,

동일한 공격성공확률 가정 시 제안한 프로토콜은 HKP 및 NUSP 보다 반복회수가 1/2 이하여서 각 비트열의 길이는 HKP의 각 비트열 길이의 1/2 이하면 충분하다. 따라서HKP 및 NUSP에서 전체 비트열의 길이가 2n이고 제안한 프로토콜의 전체 비트열의 길이는 4n이 아니라 2n보다 작다. 그러므로 제안한 프로토콜은 HKP 및 NUSP보다 공간적으로도 효율적이다.

그러나 본 연구에서 제안한 프로토콜은 빠른 비트 교환 단계에서 2 비트의 시도와 응답 구조를 사용함으로써 기존 프로토콜들이 사용하는 1 비트의 시도와 응답 구조보다 통신 채널 상에서 노이즈 영향을 더 받을 수 있는 여지가 있다.

<표 2> 시도와 응답 반복회수(n)에 따른 중계공격 성공확률

| n | HKP 및 NUSP | 제안한 프로토콜 |
|---|---|---|
| 1 | $7.5*10^{-1}$ | $4.4*10^{-1}$ |
| 2 | $5.6*10^{-1}$ | $1.9*10^{-1}$ |
| 4 | $3.2*10^{-1}$ | $3.7*10^{-2}$ |
| 8 | $1.0*10^{-1}$ | $1.3*10^{-3}$ |
| 16 | $1.0*10^{-2}$ | $1.8*10^{-6}$ |
| 32 | $1.0*10^{-4}$ | $3.3*10^{-12}$ |
| 64 | $1.0*10^{-8}$ | $1.1*10^{-23}$ |

## 5. 결 론

RFID 시스템에 있어서 중계공격에 대항하기 위해서 비트들의 왕복 여행시간 측정에 기반을 둔 거리 한정 프로토콜을 주로 사용한다. 이러한 거리 한정 프로토콜 연구에서 널리 알려진 HKP는 1비트의 시도와 응답을 기반으로 하는 프로토콜인데 본 연구에서는 이를 수정하여 2비트 시도와 응답 구조를 가지는 프로토콜을 제안하였다. 제안한 프로토콜은 각 라운드에 대한 중계공격 성공확률을 현저히 줄임으로써 HKP와 HKP를 근간으로 하는 기존 프로토콜들 보다 효율적인 수행이 가능한 프로토콜이다. 본 논문에서 제안한 프로토콜은 다중 비트 시도와 응답 구조를 이용하는 거리 한정 프로토콜에 대한 연구의 참고자료로 활용될 수 있을 것이다.

## 참 고 문 헌


[1] S. Brands and D. Chaum, “Distance-Bounding Protocols", *Advances in Cryptology, EUROCRYPT'93”*, Vol. 765 of LNCS, pp. 344-359, 1993.

[2] G. Hancke and M. Kuhn, "An RFID Distance Bounding Protocol", *Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm'05)* pp. 67-73, 2005.

[3] D. Singel´ee and B. Preneel, "Distance Bounding in Noisy Environments", *European Workshop on Security in Ad-hoc and Sensor Networks (ESAS'07)*, Vol. 4572 of LNCS, pp. 101-115, 2007.

[4] Y.-J. Tu and S. Piramuthu, "RFID Distance Bounding Protocols", *First International EURASIP Workshop on RFID Technology*, 2007.

[5] J. Munilla, A. Ortiz, and A. Peinado, "Distance Bounding Protocols with Void-Challenges for RFID", Workshop on RFID Security(RFIDSec'06), 2006.

[6] 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*, Vol. 8, No. 9, pp. 1227-1232, 2008.

[7] A. Ö. Gürel, A. Arslan, and M. Akgün, “Non-uniform stepping approach to RFID distance bounding problem”, *5th International Workshop on Data Privacy Management(DPM'10)*, Vol. 6370 of LNCS, 2010.

[8] M. R. S. Abyaneh, “Security analysis of two distance-bounding protocols”, *RFIDSec'11 Proceedings of the 7th international conference on RFID Security and Privacy,* pp. 94-107, 2011.

[9] C. H. Kim and G. Avoine, "RFID distance bounding protocol with mixed challenges to prevent relay attacks", http://eprint.iacr.org/2009/310, 2009.

[10] P. Peris-Lopez, J. C. Hernandez- Castro, J. M. Estevez-Tapiador, and J. C. A. vander Lubbe. “Shedding Light on RFID Distance Bounding Protocols and Terrorist Attacks”, arXiv.org, Computer Science, Cryptography and Security, 2010.
[11] V. Nikov and M. Vauclair, "Yet another secure Distance-bounding Protocol", *http://eprint.iacr.org/2008/319*, 2008.

**전 일 수** (Il-Soo Jeon)

• 정회원
• 경북대학교 전자공학과 공학사
• 경북대학교 전자공학과학과 공학석사
• 경북대학교 전자공학과 공학박사
• 금오공과대학교 전자공학부 교수
• 관심분야 : 정보보호, 암호프로토콜

**윤 은 준** (Eun-Jun Yoon)

• 정회원
• 경일대학교 섬유공학과 공학사
• 경일대학교 컴퓨터공학과 공학석사
• 경북대학교 컴퓨터공학과 공학박사
• 경일대학교 사이버보안학과 조교수
• 관심분야 : 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 인증, 융합보안, 스테가노그라피

논 문 접 수 일 : 2012년 02월 27일
1차수정완료일 : 2012년 04월 23일
2차수정완료일 : 2012년 05월 07일
게 재 확 정 일 : 2012년 05월 18일