http://dx.doi.org/10.3745/KIPSTC.2012.19C.1.009

강한 프라이버시와 연산 효율성을 제공하는 암호 퍼즐 기반 RFID 경계 결정 프로토콜

안 해 순[†] · 윤 은 준[††] · 남 인 길[†††]

요 약

2010년에 Pedro등은 WSBC 암호 퍼즐 기반 RFID 경계 결정 프로토콜을 제안하였다. 본 논문에서는 Pedro등이 제안한 프로토콜이 공격자에 의한 비밀키인 *ID* 유출 공격으로 인해 태그의 프라이버시 침해와 위치 트래킹 공격에 취약할 뿐만 아니라, 제한적인 자원을 가지는 수동형 태그에서 대칭키 기반의 연산을 수행함으로써 연산 효율성 저하 및 리더와 태그 간에 많은 통신 라운드가 필요함을 지적한다. 더 나아가 위와 같은 보안 취약점과 연산 및 통신 효율성 문제를 해결하기 위해 본 논문에서는 보안성을 강화하고 높은 효율성을 제공하는 새로운 암호 퍼즐 기반의 RFID 경계 결정 프로토콜을 제안한다. 결론적으로 제안한 프로토콜은 수동형 태그의 특성을 고려하여 안전한 해쉬 함수 연산만을 수행함으로써 연산 효율성을 높여줄 뿐만 아니라 일방향 해쉬 함수의 성질을 기반으로 연산된 값을 리더와 태그 간에 안전하게 송수신하기 때문에 공격자에 의한 비밀키 *ID* 유출 공격이 발생되지 않는 강력한 안전성을 보장한다.

키워드 : RFID, 경계 결정 프로토콜, 암호 퍼즐, 중계 공격, 태그 프라이버시

An RFID Distance Bounding Protocol Based on Cryptographic Puzzles Providing Strong Privacy and Computational Efficiency

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

ABSTRACT

In 2010, Pedro et al. proposed RFID distance bounding protocol based on WSBC cryptographic puzzle. This paper points out that Pedro et al.'s protocol not only is vulnerable to tag privacy invasion attack and location tracking attack because an attacker can easily obtain the secret key(ID) of a legal tag from the intercepted messages between the reader and the tag, but also requires heavy computation by performing symmetric key operations of the resource limited passive tag and many communication rounds between the reader and the tag. Moreover, to resolve the security weakness and the computation/communication efficiency problems, this paper also present a new RFID distance bounding protocol based on WSBC cryptographic puzzle that can provide strong security and high efficiency. As a result, the proposed protocol not only provides computational and communicational efficiency because it requires secure one-way hash function for the passive tag and it reduces communication rounds, but also provides strong security because both tag and reader use secure one-way hash function to protect their exchanging messages.

Keywords : RFID, Distance Bounding Protocol, Cryptographic Puzzles, Relay Attack , Tag Privacy

1. 서 론

RFID(Radio Frequency IDentification) 기술은 RFID 태그를 사람, 동물 또는 제품과 같은 아이템에 부착하여 개체를 식별하기 위한 수단으로 최근에 많이 사용되고 있다. 일반적으로 RFID 시스템은 리더(reader), 태그(tag), 백-엔드 데이터베이스(back-end database)로 구성되어 있다. 리더는 태그내의 메모리에 저장된 정보를 얻기 위해 태그에게 질의한 후 인증과 관련된 정보를 태그로부터 수신한다. 이후 리더는 태그와 연관된 모든 정보들의 위치에 대한 검색 인덱스를 사용하여 백-엔드 데이터베이스에 태그의 정보들을 요청하여 해당 정보를 다양한 응용 목적에 맞게 활용한다[1-3]. 하지만 RFID 식별 기술은 프라이버시 침해와 같은 다양한 공격들에 대한 취약점들이 발견되어 광범위한 사용에 걸림돌이 되고 있다[4-6]. 이러한 RFID 식별 기술에서의

† 정 회 원 : 대구대학교 기초교육원 컴퓨터과정 초빙교수
†† 정 회 원 : 경일대학교 컴퓨터공학과 교수
††† 정 회 원 : 대구대학교 컴퓨터·IT공학부 교수(교신저자)
논문접수 : 2011년 8월 17일
수 정 일 : 1차 2011년 11월 24일
심사완료 : 2011년 11월 29일

보안 취약점 해결을 위해 최근까지 많은 연구가 진행되어져 오고 있다. 특히 2010년에 Pedro등은 WSBC 암호 퍼즐(cryptographic puzzles) 기반의 실용적인 RFID 경계 결정 프로토콜을 제안하였다[7]. Pedro등은 Syverson[8]에 의해 소개된 WSBC(Weakly Secret Bit Commitment) 함수를 사용하여 생성된 암호 퍼즐 기법과 Brands와 Chaum[9]에 의해 제안된 경계 결정 프로토콜의 아이디어를 융합한 안전성을 강화한 WSBC+CE 프로토콜과 효율성을 강화한 WSBC+Noent 프로토콜을 각각 제안하였다. 하지만 본 논문에서는 Pedro등[7]이 제안한 두 프로토콜 모두 태그의 고유 식별자이면서 비밀키 역할을 수행하는 *ID*의 유출 문제점을 가짐으로 인해 태그의 프라이버시 침해 및 위치 트래킹 공격에 취약할 뿐만 아니라 제한적인 자원을 가지는 수동형 태그에서 값비싼 대칭키 기반의 암호 연산을 수행함으로써 연산 효율성 저하 및 리더와 태그간의 많은 통신 라운드 수행으로 인해 통신 효율성이 떨어짐을 각각 지적한다. 또한 위와 같은 문제점들을 해결하기 위해 본 논문에서는 안전성과 효율성을 제공하는 새로운 WSBC 암호 퍼즐 기반의 RFID 경계 결정 프로토콜을 제안한다. 결론적으로 제안한 프로토콜은 수동형 태그의 특성을 고려하여 안전한 암호학적 해쉬 함수 연산만을 수행함으로써 연산 효율성을 높여줄 뿐만 아니라 일방향 해쉬 함수의 성질을 기반으로 연산된 값을 리더와 태그 간에 안전하게 송수신함으로써 공격자에 의한 비밀키 *ID* 유출 공격이 발생되지 않으므로 강력한 안전성을 보장한다. 또한, 고속 비트 교환(rapid bit exchange) 단계에서 리더와 태그간의 안전한 상호 인증을 제공하도록 하여 안전성과 통신 라운드 효율성을 동시에 제공할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 연구 배경으로 RFID 경계 결정 프로토콜 및 WSBC 기반 암호 퍼즐 스킴에 대해 간단히 살펴보며, 3장에서는 Pedro등이 제안한 WSBC+CE 프로토콜과 WSBC+Noent 프로토콜에 대하여 간단하게 검토하고, 4장에서는 취약점들을 분석한다. 5장에서는 제안하는 암호 퍼즐 기반의 RFID 경계 결정 프로토콜에 대해 설명하고, 6장에서는 안전성과 효율성을 비교하며, 7장에서 본 논문의 결론을 맺는다.

2. 연구 배경

2.1 RFID 경계 결정 프로토콜

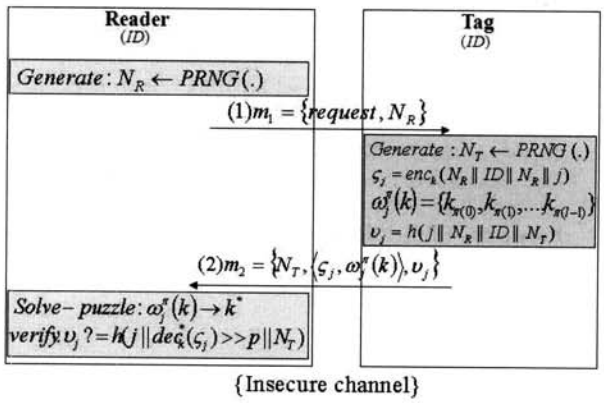
RFID 인증 기술은 응용 계층상에서 송수신되는 메시지에 대한 다양한 보안성을 제공하는 기술로 많이 활용된다[10-11]. 이로 인해 공격자가 악의적인 리더나 태그를 사용하여 다양한 물리적 공격을 수행하였을 때 RFID 인증 기술로는 방어하기 어렵다. 이러한 이유로 근접 인증에서 발생하는 물리적 보안 취약점을 해결하기 위한 대책으로 최근 경계 결정 프로토콜(distance bounding protocol)에 대한 연구가 활발히 진행되고 있다[12-16]. RFID 경계 결정 프로토콜은 도전 비트 전송과 그에 대응하는 응답 값으로 수신하는 리더와 태그 사이의 전송 지연 시간 측정에 의해 마피아 위조(mafia fraud) 공격 및 테러리스트 위조(terrorist fraud) 공격과 같은 중계 공격(relay attacks)과 관련된 보안성 문제를 해결할 수 있다.

마피아 위조 공격은 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.

테러리스트 위조 공격은 마피아 위조 공격에서 확장된 공격으로서 정당한 태그가 공격자의 악의적인 태그와 협력하여 인증을 한다. 악의적인 태그는 근접해 있는 리더와 인증하기 위해 정당한 태그와 공모하고, 악의적인 태그는 정당한 태그의 비밀키나 프라이버시를 알지 못하더라도 상관없다.

2.2 WSBC 기반 암호 퍼즐 스킴

(그림 1)은 Pedro등[7]이 제안한 RFID 경계 결정 프로토콜에서 사용되고 있는 WSBC 암호 퍼즐 기반 인증 스킴을 보여주고 있으며, 인증 과정은 다음과 같이 수행된다. 스킴에서 비밀키 *ID*는 안전하게 공유하고 있음을 가정하며, $enc_k(x)$와 $dec_k(x)$는 k를 사용하여 메시지 x를 AES[16]와 같은 대칭키 알고리즘으로 암호화 또는 복호화한 값을 의미하며, 함수 $w_j^{\pi}(k)$는 트랩도어 역할을 하는 WSBC 함수를 의미한다.



(그림 1) WSBC 인증 스킴

(1) 리더 → 태그: $m_1 = \{request, N_R\}$

리더는 난수 N_R을 생성한 후, 요청 메시지 $request$와 함께 $m_1 = \{request, N_R\}$을 태그에게 전송한다.

(2) 태그 → 리더: $m_2 = \{N_T, \langle \varsigma_j, \omega_j^{\pi}(k) \rangle, \upsilon_j\}$

태그 역시 새로운 난수 N_T를 생성한 후 비밀키 *ID*를 사

용하여 암호 퍼즐 $\langle \zeta_j, \omega_j^{\pi}(k) \rangle$와 해쉬 값 v_j를 계산한 후 메시지 $m_2 = \{N_T, \langle \zeta_j, \omega_j^{\pi}(k) \rangle, v_j\}$를 리더에게 전송한다.

(3) 리더

메시지 m_2를 수신한 리더는 태그에 의해 전송된 값들 중 WSBC 함수 $w_j^{\pi}(k)$의 암호 퍼즐을 풀어 k^*값을 얻어 ζ_j를 복호화 한다. 이때, k^* 값은 l비트 길이로 랜덤하게 선택되기 때문에 랜덤한 $w_j^{\pi}(k)$ 값들을 생성할 수 있다. 리더는 평균 $\binom{n}{l}2^{n-l-1}$의 키 값 만큼 전수조사(brute-force process)를 수행하여 풀게 된다. 또한, 리더는 태그와의 공유 비밀키인 ID를 알고 있으므로 암호 퍼즐을 풀어서 얻은 k^* 값과 ID를 이용하여 아래 수식(1)과 같이 v_j 값 검증을 수행하여 태그의 합법성을 인증한다. 수식(1)에서 $\gg$ 기호는 논리적 우측 비트 이동 연산자이며, p는 난수 N_R과 현재 세션 j에 대한 총 비트 크기를 의미한다.

$$v_j \,?= h(j \| dec_k^*(\zeta_j) \gg p \| N_T) \quad (1)$$

3. Pedro등이 제안한 WSBC 스킴 기반의 RFID 경계 결정 프로토콜

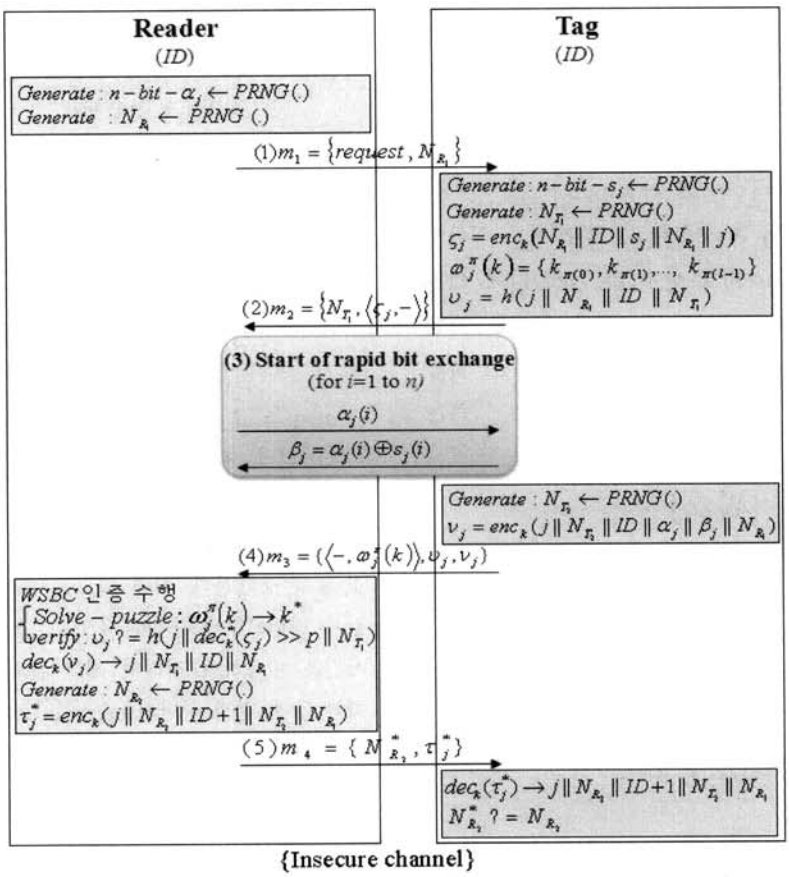
본 장에서는 Pedro등[7]이 제안한 WSBC 스킴 기반의 RFID 경계 결정 프로토콜들인 WSBC+CE 프로토콜과 WSBC+Noent 프로토콜을 각각 소개한다. 본 논문에서 사용할 용어들의 표기법 및 정의는 <표 1>과 같다.

〈표 1〉 용어 정의

기호	의 미
N_T, N_R	태그와 리더가 각각 생성한 난수
k	매 세션마다 서로 다른 랜덤한 비밀 값
$h(.)$	안전한 해쉬 함수(secure hash function); $h:\{\ \}^* \rightarrow \{\ \}^{2n}$
$PRNG()$	의사난수생성기(Pseudo Random Number Generator)
j	현재 세션 값
α_j, s_j	현재 세션에서 생성한 n-bit 난수
$\oplus$	배타적 논리합(XOR; eXclusive OR) 연산
$\|$	연접(concatenation) 연산
$enc_k(.)$	비밀키 k를 이용한 대칭키 암호화 알고리즘
$dec_k(.)$	비밀키 k를 이용한 대칭키 복호화 알고리즘

3.1 WSBC+CE 프로토콜

모든 RFID 경계 결정 프로토콜 연구에서와 같이 리더와



(그림 2) WSBC+CE 경계 결정 인증 프로토콜

태그는 일반적으로 검증기와 증명자의 역할을 수행한다. (그림 2)는 WSBC 스킴에 경계 결정 인증 프로토콜을 결합시켜 확장한 WSBC+CE 프로토콜의 전체적인 구성을 보여주고 있으며, 수행 과정은 다음과 같다.

(1) 리더 → 태그: $m_1 = \{request, N_{R_1}\}$

리더는 고속 비트 교환 단계에서 사용될 n 비트 난수 α_j를 생성한다. 또한, 리더는 난수 N_{R_1}을 생성하여 요청 메시지 $m_1 = \{request, N_{R_1}\}$을 태그에게 전송하여 프로토콜 수행을 시작한다.

(2) 태그 → 리더: $m_2 = \{N_{T_1}, \langle \zeta_j, - \rangle\}$

태그 역시 고속 비트 교환 단계에서 사용될 n 비트 난수 s_j와 난수 N_{T_1}을 각각 생성하고, $\zeta_j = enc_k(N_{R_1} \| ID \| s_j \| N_{R_1} \| j)$ 값과 WSBC 함수를 사용하여 암호 퍼즐 $\omega_j^{\pi}(k)$를 생성하고, 해쉬 값 $v_j = h(j \| N_{R_1} \| ID \| \alpha_j \| N_{T_1})$을 계산한 후 리더에게 메시지 $m_2 = \{N_{T_1}, \langle \zeta_j, - \rangle\}$를 전송한다.

(3) 고속 비트 교환 단계 수행

리더와 태그는 물리적 계층에서 다음의 2단계로 구성되는 n-라운드의 경계 결정 교환 과정을 수행한다.

[단계 1] 리더는 태그에게 n비트 난수 α_j의 i번째 라운드 비트 값인 $\alpha_j(i)$ 비트를 전송한다.

[단계 2] 태그는 리더로부터 $\alpha_j(i)$ 비트를 수신한 후 리더에게 n비트 난수 s_j의 i번째 라운드 비트 값인 $s_j(i)$와 XOR 연산을 수행한 결과 비트 값인 $\beta_j(i) = \alpha_j(i) \oplus s_j(i)$ 비트를 계산하여 전송한다.

위 고속 비트 교환 과정을 총 n-라운드 수행한다.

(4) 태그 → 리더: $m_3 = \{\langle -, \omega_j^{\pi}(k) \rangle, v_j, \nu_j\}$

태그는 새로운 난수 N_{T_2}를 생성하고, 고속 비트 교환이 수행되는 동안 송수신된 n 비트 난수 값 $\{\alpha_j \| \beta_j\}$에 대한 암호화된 메시지 $\nu_j = enc_k(j \| N_{T_2} \| ID \| \alpha_j \| \beta_j \| N_{R_1})$를 계산한다. 계속해서 태그는 단계 (2)에서 생성한 암호 퍼즐 $\omega_j^{\pi}(k)$와 해쉬 값 v_j와 ν_j를 메시지로 하는 $m_3 = \{\langle -, \omega_j^{\pi}(k) \rangle, v_j, \nu_j\}$를 리더에게 전송한다.

(5) 리더 → 태그: $m_4 = \{N_{R_2}^*, \tau_j^*\}$

리더는 수신한 m_3에서 WSBC 기반 암호 퍼즐 $\omega_j^{\pi}(k)$를 풀어 k^* 값을 얻은 후, 아래 수식 (2)와 같이 v_j 값 검증을 수행하여 태그의 합법성을 인증한다. 수식 (2)에서 p는 난수 s_j와 N_{R_1} 그리고 세션 j에 대한 총 비트 크기를 의미한다.

$$v_j ? = h(j \| dec_k^*(s_j) \gg p \| N_{R_1}) \quad (2)$$

해쉬 값 v_j에 대한 검증이 완료되면 리더는 태그를 인증하게 되며, 상호 인증을 위해 수신한 ν_j를 복호화하여 난수 N_{T_2}를 얻는다. 그런 다음 리더 자신도 새로운 난수 N_{R_2}를 생성하여 암호화된 메시지 $\tau_j^* = enc_k(j \| N_{R_2} \| ID+1 \| N_{T_2} \| N_{R_1})$를 계산한 후 태그에게 $m_4 = \{N_{R_2}^*, \tau_j^*\}$를 전송한다.

(6) m_4를 수신한 태그는 k를 이용하여 τ_j^*를 복호화한 후 $N_{R_2}^*$ 검증을 통해 상호 인증을 수행한다.

3.2 WSBC+Noent 프로토콜

Pedro등[7]이 제안한 WSBC+Noent 프로토콜에서는 WSBC+CE 프로토콜과는 달리 정확하고 효율적인 경계 결정을 수행할 수 있다. (그림 3)은 WSBC+Noent 프로토콜을 보여주며 인증 과정은 다음과 같이 수행된다.

(1) 리더 → 태그: $m_1 = \{request, N_{R_1}, \gamma_j\}$

리더는 고속 비트 교환 단계에서 사용될 n 비트 난수 s_j를 생성한다. 또한, 난수 N_{R_1}과 N_{R_2}를 각각 생성하여 해쉬 값 $\gamma_j = h(N_{R_1} \| N_{R_2} \| s_j)$를 계산한 후 요청 메시지 $m_1 = \{request, N_{R_1}, \gamma_j\}$를 태그에게 전송하여 프로토콜 수행을 시작한다. m_1을 수신한 태그는 고속 비트 교환 단계에서 사용될 n 비트 난수 α_j를 생성한다.

(2) 고속 비트 교환 단계 수행

리더와 태그는 물리적 계층에서 다음의 3 단계로 구성되는 n-라운드의 경계 결정 교환 과정을 수행한다.

[단계 1] 리더는 i번째 라운드 비트값인 $c(i)$를 생성한 후 태그에게 전송한다.

[단계 2] 태그는 리더로부터 $c(i)$ 비트를 수신한 후 리더에게 n 비트 난수 α_j의 i번째 라운드 비트 값인 $\alpha_j(i)$ 비트를 전송한다.

[단계 3] 리더는 $\alpha_j(i)$ 비트를 수신한 후 태그에게 n비트 난수 s_j의 i번째 라운드 비트 값인 $s_j(i)$와 XOR 연산을 수행한 결과 비트 값인 $\beta_j(i) = \alpha_j(i) \oplus s_j(i)$ 비트를 계산하여 전송한다.

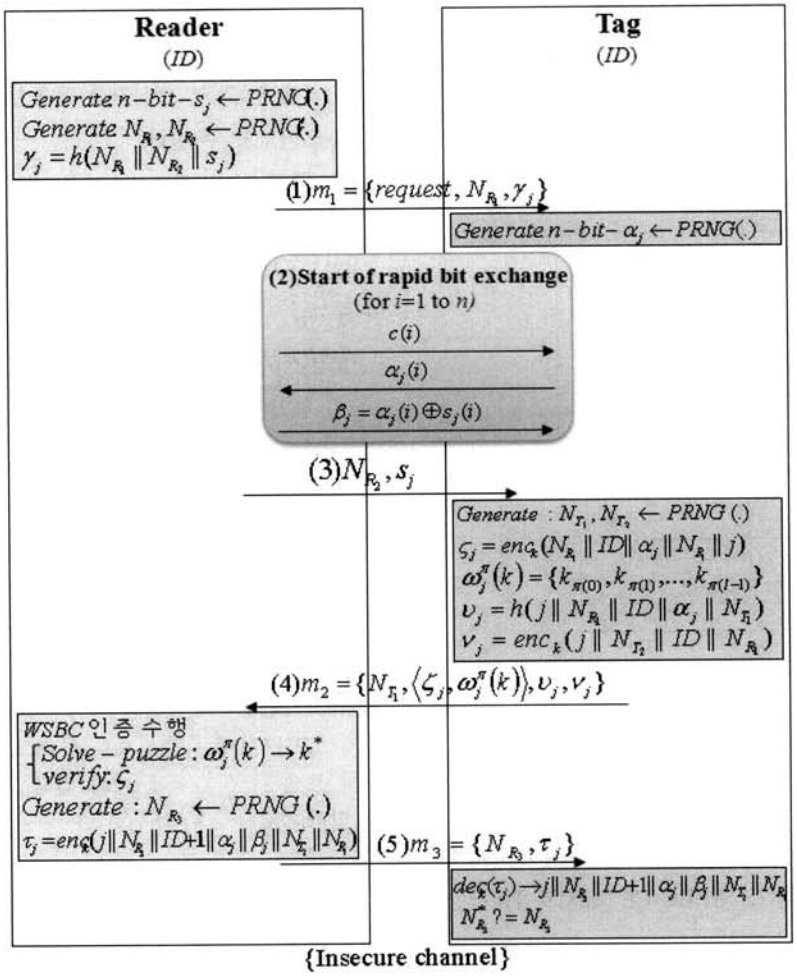
위 고속 비트 교환 과정을 총 n-라운드 수행한다.

(3) 리더 → 태그: $m_2 = \{N_{R_2}, s_j\}$

태그와 리더 사이에 고속 비트 교환이 완료된 후에 리더는 $m_2 = \{N_{R_2}, s_j\}$를 태그에게 전송함으로써 합의된 비밀 값 s_j를 공개한다. 이때 태그는 자신이 전송한 $\{\alpha_j(i)\}$ 비트 값과 리더로부터 수신한 $\{\beta_j(i)\}$ 비트 값 사이의 최대 지연 시간을 이용하여 리더와 태그 간의 거리 $\{d_{rn}\}$를 기반으로 하는 경계 결정 상한치(upper bound)를 결정할 수 있다.

(4) 태그 → 리더: $m_2 = \{N_{T_1}, \langle \zeta_j, \omega_j^{\pi}(k) \rangle, v_j, \nu_j\}$

태그는 새로운 난수 N_{T_1}과 N_{T_2}를 생성하고, WSBC 함수를 사용하여 $\zeta_j = enc_k(N_{R_1} \| ID \| \alpha_j \| N_{R_1} \| j)$와 암호 퍼즐 $\omega_j^{\pi}(k)$를 생성하고, 해쉬 값 $v_j = h(j \| N_{R_1} \| ID \| \alpha_j \| N_{T_1})$와 암



(그림 3) WSBC+Noent 경계 결정 인증 프로토콜

호화된 메시지 $\nu_j = enc_k(j \| N_{T_2} \| ID \| N_{R_1})$을 계산한다. 최종적으로 태그는 $m_2 = \{N_{T_1}, \langle \zeta_j, \omega_j^{\pi}(k) \rangle, \upsilon_j, \nu_j\}$를 리더에게 전송한다.

(5) 리더 → 태그: $m_3 = \{N_{R_3}, \tau_j\}$

리더는 수신한 m_2에서 $\omega_j^{\pi}(k)$를 이용하여 WSBC 기반 암호 퍼즐을 풀어 k^* 값을 얻은 후, 아래 수식 (3)과 같이 υ_j 값 검증을 수행하여 태그의 합법성을 인증한다. 수식 (3)에서 p는 난수 s_j와 N_{T_1} 그리고 세션 j에 대한 총 비트 크기를 의미한다.

$$\upsilon_j ? = h(j \| dec_k^*(s_j) \gg p \| N_{T_1}) \quad (3)$$

해쉬 값 υ_j에 대한 검증이 완료되면 리더는 태그를 인증하게 되며 상호 인증을 위해 수신한 ν_j를 복호화하여 난수 N_{T_2}를 얻은 후 자신도 새로운 난수 N_{R_3}를 생성하여, 암호화된 메시지 $\tau_j = enc_k(j \| N_{R_3} \| ID+1 \| \alpha_j \| \beta_j \| N_{T_2} \| N_{R_1})$을 계산한 후 태그에게 $m_3 = \{N_{R_3}, \tau_j\}$를 전송한다.

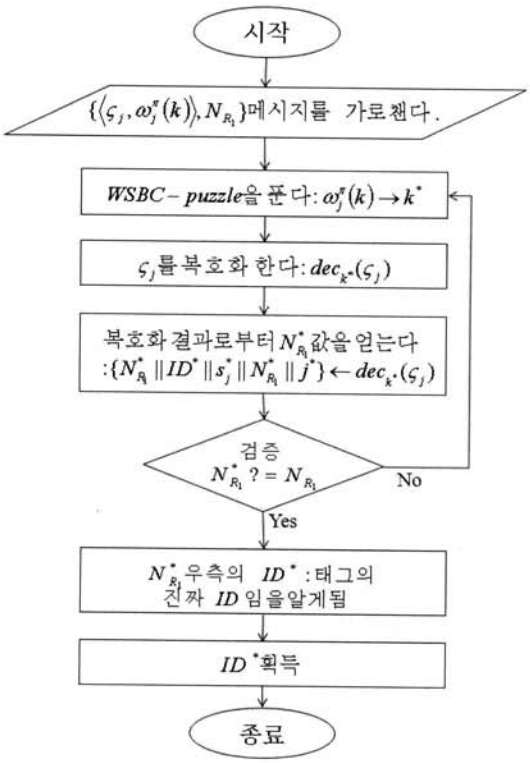
(6) m_4를 수신한 태그는 k를 이용하여 τ_j를 복호화한 후 N_{R_3} 검증을 통해 상호 인증을 수행한다.

4. Pedro등이 제안한 프로토콜의 취약점 분석

본 장에서는 Pedro등[7]이 제안한 WSBC+CE 프로토콜과 WSBC+Noent 프로토콜이 비밀키 유출 공격에 의한 태그 프라이버시 침해 공격 및 안전성에 대해 분석한다.

[정리] *Pedro등이 제안한 프로토콜은 비밀키인 ID 유출 공격에 취약하므로 안전성과 프라이버시를 제공하지 못한다.*

[증명] 태그와 리더 사이의 통신은 RFID 시스템의 특성상 안전하지 않은 채널을 사용하므로 메시지를 송수신하는 단계에서 공격자는 모든 송수신 메시지들을 가로챌 수 있다. 이를 이용하여 공격자는 (그림 4)와 같은 공격을 수행하여 WSBC 암호 퍼즐 조각을 풀어 *ID* 유출 공격을 수행할 수 있다.



(그림 4) ID 유출 공격 순서도

(1) 공격자는 리더와 태그 간에 전송되는 메시지 $\langle \zeta_j, \omega_j^{\pi}(k)\rangle, N_{R_1}$을 도청한다. WSBC+CE 프로토콜에서는 공격자가 단계 (1),(2),(4)를 통해 송수신되는 메시지를 도청하여 $\langle \zeta_j, \omega_j^{\pi}(k)\rangle, N_{R_1}$ 메시지를 가로챌 수 있으며, WSBC+Noent 프로토콜에서는 공격자가 단계 (1),(3),(4)를 통해서 송수신되는 메시지를 도청하여 $\langle \zeta_j, \omega_j^{\pi}(k)\rangle, N_{R_1}$ 메시지를 가로챌 수 있다.

(2) 공격자는 WSBC 스킴을 기반으로 $\omega_j^{\pi}(k)$ 퍼즐을 풀어 k로 추측되는 k^*를 얻는다.

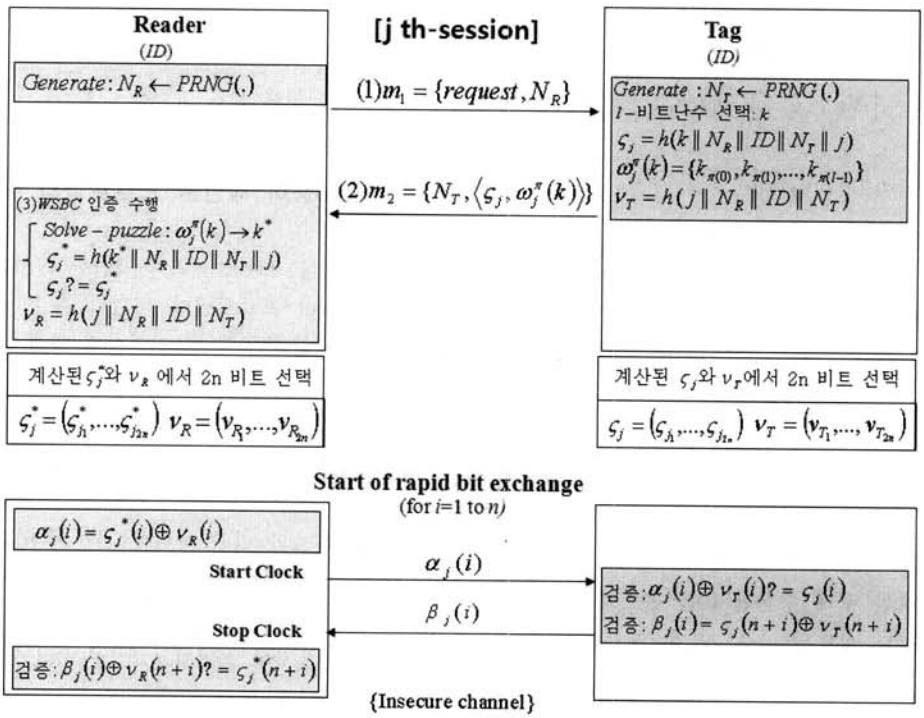
(3) 공격자는 퍼즐을 맞춘 결과 값인 k^*를 이용하여 $dec_{k^*}(\zeta_j)$ 과정을 수행한 후 ζ_j를 복호화하여 $(N_{R_1}^* \| ID^* \| s_j^* \| N_{R_1}^* \| j^*)$ 값을 얻게 된다.

(4) 공격자는 $N_{R_1}^* ? = N_{R_1}$인지 여부를 검증한다. 만약 두 값이 일치하면 공격자는 $N_{R_1}^*$의 우측 값인 ID^*가 태그의 진짜 ID임을 알게 되므로 리더와 태그 간에 공유하고 있는 비밀키인 ID를 획득하게 된다.

만약, N_{R_1}이 $N_{R_1}^*$과 일치하지 않으면 공격자는 일치할 때까지 위 (2)~(4)번 과정을 반복 수행한다.

결론적으로 Pedro등이 제안한 WSBC+CE 프로토콜과 WSBC+Noent 프로토콜은 모두 위와 같은 공격에 의해 비밀키 ID가 쉽게 유출됨으로써 태그의 프라이버시 침해 및 위치 트래킹 공격 등에 대해 안전성을 제공하지 못함을 알 수 있다.

5. 제안하는 암호 퍼즐 기반 RFID 경계 결정 프로토콜



(그림 5) 제안하는 암호 퍼즐 기반의 RFID 경계 결정 프로토콜

본 장에서는 Pedro등[7]이 제안한 프로토콜들의 문제점을 해결한 안전하고 효율적인 WSBC 암호 퍼즐 기반의 RFID 경계 결정 프로토콜을 제안한다. (그림 5)는 제안하는 WSBC 암호 퍼즐 기반의 RFID 경계 결정 프로토콜의 전체적인 수행 과정을 보여주고 있다. 인증 과정은 태그와 리더 간에 암호 퍼즐 인증 단계와 n 라운드 고속 비트 교환 및 인증 단계로 구성되며 다음과 같은 과정으로 수행된다.

5.1 암호 퍼즐 인증 단계

(1) 리더 → 태그: $m_1 = \{request, N_R\}$

리더는 난수 N_R을 생성한 후, 메시지 $m_1 = \{request, N_R\}$을 태그에게 전송함으로써 인증 프로토콜 수행을 시작한다.

(2) 태그 → 리더: $m_2 = \{N_T, \langle \zeta_j, \omega_j^{\pi}(k) \rangle\}$

태그 역시 난수 N_T를 생성하고, l 비트 길이의 난수를 선택하여 세션 비밀키인 k값으로 설정한다. 태그는 k값과 리더로부터 수신한 난수 N_R, 비밀키인 ID, 태그가 생성한 난수 N_T, 그리고 현재 세션 값 j를 연접한 후 안전한 일방향 해쉬 함수를 사용하여 계산한 해쉬 값 $\zeta_j = h(k \| N_R \| ID \| N_T \| j)$와 WSBC 암호 퍼즐 값 $\omega_j^{\pi}(k)$을 생성한 후 리더에게 $m_2 = \{N_T, \langle \zeta_j, \omega_j^{\pi}(k) \rangle\}$ 메시지를 전송한다. 이때, 태그는 경계 결정 프로토콜 인증 수행 단계의 n-라운드 고속 비트 교환 과정에서 태그와 리더 간에 상호 인증을 위해 사용할 해쉬 값 $\nu_T = h(j \| ID \| N_T)$을 계산한 후 ζ_j 값과 ν_T 값에서 각각 $2n$ 비트를 선택한다.

(3) m_2를 수신한 리더는 WSBC 퍼즐 인증 수행을 위해 태그로부터 수신한 암호 퍼즐을 풀어서 k^*를 얻은 후 해쉬 값 $\zeta_j^* = h(k^* \| N_R \| ID \| N_T \| j)$를 계산하여 $\zeta_j ? = \zeta_j^*$를 검증한다. 만약 두 값이 일치하면 리더는 태그를 인증하며, 리더 역시 RFID 경계 결정 프로토콜 인증 수행 단계의 n-라운드 고속 비트 교환 과정에서 태그와 리더 간에 상호 인증을 위해 사용될 $\nu_R = h(j \| N_R \| ID \| N_T)$ 해쉬 값을 계산한 후 ζ_j^* 값과 ν_R 값에서 각각 $2n$ 비트를 선택한다.

5.2 n-라운드 고속 비트 교환 및 인증 단계

리더와 태그는 경계 결정을 위해 다음의 $i = 1, ..., n$번까지 수행되는 n-라운드 고속 비트 교환 프로토콜을 수행한다.

[단계 1] 리더는 $2n$ 비트 난수 ζ_j^*의 i번째 라운드 비트 값인 $\zeta_j^*(i)$와 $2n$ 비트 난수 ν_R의 i번째 라운드 비트 값인 $\nu_R(i)$를 XOR 연산 수행한 결과 값인 $\alpha_j(i) = \zeta_j^*(i) \oplus \nu_R(i)$를 계산한 후 태그에게 $\alpha_j(i)$를 전송한다.

[단계 2] 태그는 리더로부터 $\alpha_j(i)$를 수신한 후 자신이 생성한 $2n$ 비트 난수 ν_T의 i번째 비트 값인 $\alpha_j(i) \oplus \nu_T(i)$를 계산하여 자신이 가지고 있는 $2n$ 비트 난수 ζ_j의 i번째 라운드 비트 값인 $\zeta_j(i)$와 동일한지 검증한다. 만약 두 값이 일치하면 태그는 $2n$ 비트 난수 ζ_j의 $(n+i)$ 번째 비트 값인 $\zeta_j(n+i)$와 $2n$ 비트 난수 ν_T의 $(n+i)$ 번째 비트 값인 $\nu_T(n+i)$을 XOR 연산을 수행한 결과값 $\beta_j(i) = \zeta_j(n+i) \oplus \nu_T(n+i)$를 계산한 후 리더에게 전송한다.

[단계 3] 리더 역시 태그로부터 수신한 비트를 검증하기 위해 자신의 $2n$ 비트 난수 ν_R의 $(n+i)$ 번째 비트 값인 $\nu_R(n+i)$와 수신한 $\beta_j(i)$를 XOR 연산을 수행한 결과값 $\zeta_j(n+i) = \beta_j(i) \oplus \nu_R(n+i)$를 계산하여 자신의 $\zeta_j^*(n+i)$와 동일한지 여부를 검증한다. 만약 두 값이 일치하면 리더는 태그를 인증하게 되어 태그와 리더 간에 상호 인증 과정이 수행됨을 알 수 있다.

6. 안전성과 효율성 분석

6.1 안전성 분석

본 절에서는 Pedro등[7]이 제안한 WSBC+CE 프로토콜과 WSBC+Noent 프로토콜 및 제안한 프로토콜의 안전성에 대하여 분석한다. 제안한 프로토콜은 위 2.2절에서 언급한 암호 퍼즐 스킴의 성질 외에 해쉬 함수의 성질을 기반으로 하고 있다. 일반적인 안전한 일방향 해쉬 함수의 정의는 다음과 같으며 제안한 프로토콜의 암호 퍼즐 인증 단계에서 안전성 보장을 위해 반드시 필요한 성질이다.

[정의] *안전한 일방향 해쉬 함수 $y = h(x)$에서 주어진 x로 y를 계산하는 것은 쉽고, 주어진 y로 x를 계산하는 것은 어렵다.*

제안한 프로토콜은 암호 퍼즐 스킴의 안전성과 일방향 해쉬 함수의 안전성을 기반으로 다음의 비밀키 유출 공격 및 중계 공격에 안전할 뿐만 아니라 안전한 상호 인증을 제공할 수 있다.

(1) 비밀키(ID) 유출 공격 : 제안한 프로토콜에서는 태그가 리더에게 전송할 메시지에서 $\zeta_j = h(k \| N_R \| ID \| N_T \| j)$ 값과 $\nu_T = h(j \| ID \| N_T)$ 값을 안전한 일방향 해쉬 함수를 이용하여 비밀키인 ID 를 보호하고 있다. 만약, 공격자가 이 메시지를 가로채더라도 안전한 일방향 해쉬 함수의 성질로 인해 비밀키인 ID가 유출 되지 않음으로 제안한 프로토콜은 비밀키 유출 공격에 안전하다. 만약, 공격자가 비밀키(ID)를 획득하게 된다면 태그 프라이버시 침해 공격 및 위치 트래킹 공격도 수행할 수 있다. 따라서 Pedro 등이 제안한 프로토콜과 비교하여 제안한 프로토콜은 태그와 리더 간에 비밀키 유출 공격에 안전하고, 태그 프라이버시 침해

문제를 발생시키지 않을 뿐만 아니라 위치 트래킹 공격에도 안전하므로 강력한 안전성을 제공함을 알 수 있다.

(2) 상호 인증 : 제안한 프로토콜의 (3)번 단계에서 리더는 태그로부터 수신한 암호 퍼즐을 풀어서 k^*를 얻은 후 $\zeta_j^* = h(k^* \| N_R \| ID \| N_T \| j)$를 계산하여 태그가 계산한 해쉬 값 $\zeta_j ? = \zeta_j^*$ 검증을 수행함으로써 상호 인증을 수행한다. 또한 (2)번과 (3)번 단계에서 태그와 리더는 RFID 경계 결정 프로토콜 인증 수행 단계의 n-라운드 고속 비트 교환 과정에서 태그와 리더 간에 상호 인증을 위해 사용될 $\nu_T = h(j \| ID \| N_T)$와 $\nu_R = h(j \| N_R \| ID \| N_T)$ 해쉬 값을 계산한 후 $2n$ 비트를 각각 선택한다. 그런 다음 n-라운드 고속 비트 교환 및 인증 단계에서 태그 $\alpha_j(i) \oplus \nu_T(i) ? = \zeta_j(i)$를 검증하고, 리더는 $\beta_j(i) \oplus \nu_R(n+i) ? = \zeta_j^*(n+i)$를 검증함으로써 n-라운드 고속 비트 교환 단계에서도 상호 인증을 수행한다.

(3) 중계 공격 : 제안한 프로토콜은 WSBC 스킴을 기반으로 태그와 리더 간에 암호 퍼즐을 사용하여 상호 인증을 제공하는 RFID 경계 결정 프로토콜이다. 암호 퍼즐 기반에서의 태그는 (2)번 단계에서 세션 비밀키인 k값을 설정하여 해쉬 값 $\zeta_j = h(k \| N_R \| ID \| N_T \| j)$와 WSBC 암호 퍼즐 값 $\omega_j^{\pi}(k)$를 계산한다. 또한 중계 공격 방지를 위해 n-라운드 고속 비트 교환 및 인증 단계에서 상호 인증을 위해 사용할 $\nu_T = h(j \| ID \| N_T)$ 값을 계산하고, 리더는 (3)번 단계에서 태그로부터 수신한 암호 퍼즐을 풀어 k^*를 얻은 후 해쉬 값 $\zeta_j^* = h(k^* \| N_R \| ID \| N_T \| j)$를 계산하여 $\zeta_j ? = \zeta_j^*$를 검증 한다. 만약 두 값이 일치하면 리더는 태그를 인증한 후 리더 역시 중계 공격 방지와 상호 인증을 위해 $\nu_R = h(j \| N_R \| ID \| N_T)$ 해쉬 값을 계산하여 n-라운드 고속 비트 교환 단계에서 인증 과정을 수행함으로써 중계 공격 성공 확률은 $(1/2)^n$을 제공함을 할 수 있다.

아래 <표 2>는 각 프로토콜들에 대한 안전성을 비교한 결과를 보여주고 있다. 표를 통해 알 수 있듯이 Pedro등이 제안한 두 프로토콜은 모두 비밀키 ID 유출 공격에 안전하지 않음으로 인해 태그 프라이버시 침해 공격과 위치 트래킹 공격에 매우 취약하다. 그러나 제안한 프로토콜은 다음과 같이 비밀키 ID 유출 공격에 안전할 뿐만 아니라 태그 프라이버시 침해 공격과 위치 트래킹 공격에도 안전함을 알 수 있다.

〈표 2〉 안전성 비교

프로토콜 / 공격유형	WSBC+CE 프로토콜	WSBC+Noent 프로토콜	제안 프로토콜
상호 인증	제공함	제공함	제공함
비밀키(ID) 유출 공격	안전하지 않음	안전하지 않음	안전함
태그 프라이버시 침해 공격	안전하지 않음	안전하지 않음	안전함
위치 트래킹 공격	안전하지 않음	안전하지 않음	안전함
중계 공격 성공 확률	$\left(\frac{1}{2}\right)^n$	$\left(\frac{1}{2}\right)^n$	$\left(\frac{1}{2}\right)^n$

6.2 효율성 분석

본 절에서는 Pedro 등이 제안한 프로토콜들과 제안한 프로토콜의 효율성에 대해 분석한다. <표 3>은 제안한 프로토콜과 Pedro 등이 제안한 두 프로토콜의 효율성을 비교한 표이다.

〈표 3〉 효율성 비교

프로토콜 / 연산종류	WSBC+CE 프로토콜		WSBC+Noent 프로토콜		제안 프로토콜	
	태그	리더	태그	리더	태그	리더
대칭키 암호/복호 연산	3	3	3	2	0	0
해쉬 연산	1	0	1	1	2	2
리더/태그간 통신라운드량	$4+2n$		$4+3n$		$2+2n$	
연산/통신 효율성	낮음		낮음		높음	

- n : 비트 단위 라운드 횟수

(1) WSBC+CE 프로토콜 : 태그와 리더 측에서 모두 각각 대칭키 암호 및 복호 연산을 3회씩 수행하고, 해쉬 연산은 태그에서만 1회 수행한다. 또한 리더와 태그 간의 통신 라운드 량은 $4+2n$으로써 통신 효율성 면에서도 매우 낮음을 알 수 있다.

(2) WSBC+Noent 프로토콜: 대칭키 암호 및 복호 연산은 태그에서는 3회, 리더에서는 2회 수행한다. 또한, 해쉬 연산은 태그와 리더 모두 각각 1회씩 수행하고, 리더와 태그 간의 통신 라운드 량은 $4+3n$으로써 통신 효율성이 낮다.

(3) 제안한 프로토콜 : 태그와 리더 측 모두 대칭키 암호 및 복호 연산을 전혀 수행하지 않으며, 해쉬 연산만을 태그와 리더 측에서 각각 2회씩 수행하므로 연산 효율성이 아주 높다. 또한 제안한 프로토콜의 통신 라운드 량은 $2+2n$이므로 통신 효율성도 매우 높다.

일반적으로 워크스테이션급 컴퓨터에서 대칭키 암호 연산은 초당 2,000번이 수행되는 반면 해쉬 함수 연산은 초당 20,000번을 수행할 수 있다[18]. 그러므로 대칭키 암호 연산은 RFID 시스템 환경에서의 한정된 자원을 가지고 있는 수동형 태그에는 상당히 에너지 소비가 많은 비효율적인 연산이다. 앞서 언급하였듯이 Pedro등이 제안한 프로토콜들에서 수동형 RFID 태그는 3회의 대칭키 암호 및 복호화 연산이 필요함으로 연산 및 통신 효율성 저하 문제를 가짐을 알 수 있다. 하지만 제안한 프로토콜은 수동형 RFID 태그 및 리더

에서 대칭키 암호 연산은 전혀 수행하지 않고, 오직 안전한 일방향 해쉬 함수 연산만을 수행하기 때문에 Pedro등이 제안한 프로토콜에 비해 훨씬 우수한 연산 효율성과 통신 효율성을 제공할 수 있다. 결론적으로 제안한 프로토콜에 Pedro 등이 제안한 프로토콜과 비교하여 수동형 저비용 RFID 시스템 환경에 더욱 적합하며 실용적임을 알 수 있다.

7. 결 론

본 논문에서는 Pedro 등이 제안한 WSBC 스킴 기반 RFID 경계 결정 프로토콜들이 가지는 안전성 및 효율성을 해결하여 강력한 보안성과 높은 연산 및 통신 효율성을 제공하는 새로운 WSBC 암호 퍼즐 기반의 RFID 경계 결정 프로토콜을 제안하였다. 결론적으로 제안한 프로토콜은 경계 결정 인증 단계에서도 공격자의 중계 공격 성공 확률을 $(1/2)^n$으로 줄여줄 뿐만 아니라 안전한 상호 인증을 제공한다. 또한, 비밀키인 ID 유출 공격에도 안전하므로 태그의 프라이버시 보호와 위치 트래킹 공격에도 안전하다. 더 나아가 리더와 태그 측에서 값 비싼 대칭키 연산을 전혀 수행하지 않으므로 한정된 자원을 가지는 수동형 태그에 적합하기 때문에 경계 결정이 필요한 저비용 RFID 시스템에 실용적으로 사용될 수 있다.

참 고 문 헌

[1] K.Finkenzeller, "RFID handbook: fundamentals and applications in Contactless smart cards and identification", (2nd ed.), Munich, Germany: Wiley, 2003.

[2] S. Garfinkel and B. Rosenberg, "RFID applications, security, and privacy", Boston, USA: Addison-Wesley, 2005.

[3] A Juels. "RFID security and privacy: A research survey", Manuscript, 2005.

[4] T. van Deursen and S. Radomirovic. "Attacks on rfid protocols", Cryptology ePrint Archive, Report 2008/310, 2008. http://eprint.iacr.org/.

[5] A Juels. "RFID security and privacy: A research survey", Manuscript, 2005.

[6] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum. "Classification of RFID Attacks", In Proceedings of the 2nd International Workshop on RFID Technology, 2008.

[7] Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. E. Tapiador, Esther Palomar, and Jan C.A. van der Lubbe, "Cryptographic Puzzles and Distance-bounding Protocols: Practical Tools for RFID Security" IEEE RFID 2010, pp.45-52, 2010.

[8] P. Syverson. "Weakly secret bit commitment: Applications to lotteries and fair exchange", In Proceedings of the 11th IEEE Computer Security Foundations Workshop, pp.2-13, 1998.

[9] S. Brands and D. Chaum, "Distance-bounding protocols", Advances in Cryptology EUROCRYPT'03, Springer-Verlag LNCS 765, pp.344-59, May, 1993.

[10] ISO 14443. Identification cards—contactless integrated circuit cards—proximity cards. International Organization for Standardization, Geneva.

[11] ISO 15693. Identification cards - contactless integrated circuit cards—vicinity cards. International Organization for Standardization, Geneva.

[12] 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), pp.67-73. IEEE Computer Society, 2005.

[13] C H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira. "The Swiss-Knife RFID Distance Bounding Protocol", In Proceedings of International Conference on Information Security and Cryptology-ICISC, LNCS. Springer-Verlag, 2008.

[14] 안해순, 부기동, 윤은준, 남인길. "경량 RFID 경계 결정 프로토콜," 정보처리학회논문지C, 제17-C권, 제4호, pp.307-314, 2010.

[15] 안해순, 윤은준, 부기동, 남인길. "저장 공간 및 연산 효율적인 RFID 경계 결정 프로토콜," 한국통신학회 논문지, 제35권, 제9호, pp.1350-1359, 2010.

[16] J. Munilla and A. Peinado, "Attacks on a distance bounding protoco"l, Computer Communications, Vol.33, No.7, 2010, pp.884-889.

[17] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen. "AES Implementation on a Grain of Sand", IEE Proceedings - Information Security, 152(1):13-20, 2005.

[18] M.S. Hwang, I.C. Lin, and L.H. Li. A Simple Micro-payment Scheme, The Journal of Systems and Software, Vol.55, pp.221-229, 2001.

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

윤 은 준

e-mail : ejyoon@tpic.ac.kr
2003년 경일대학교 컴퓨터공학과(공학석사)
2007년 경북대학교 컴퓨터공학과(공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2008년~2011년 경북대학교 전자전기컴퓨터학부 연구교수
2011년~현 재 경일대학교 컴퓨터공학과 교수
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