DOI: 10.3745/KIPSTC.2009.16-C.3.347

강화된 사용자 프라이버시를 보장하는 효율적인 RFID 검색 프로토콜

임 지 환[†] · 오 희 국[††] · 양 대 헌[†††] · 이 문 규[††††] · 김 상 진[†††††]

요 약

RFID 검색 프로토콜에서 리더는 특정한 태그만이 인식할 수 있는 질의를 전송하고 그 응답을 수신하여 해당 태그의 존재 유무를 판단한다. 리더의 질의에는 검색하고자 하는 태그의 식별자가 포함되어야한다는 검색 프로토콜의 구조적인 특징은 검색 프로토콜을 재전송 공격에 더욱 취약하게 만들며 일반적인 RFID 인증 프로토콜에서 사용하는 상호 인증 기법들을 그대로 적용하기 어렵게 만든다. 본 논문에서는 카운터를 사용하여 이러한 문제를 해결한 정적 아이디 기반의 RFID 검색 프로토콜과 동적 아이디 기반의 RFID 검색 프로토콜을 제안한다. 또한 본 논문에서는 전방향/후방향 위치추적, 비동기, 위장 공격의 개념을 포함하는 새로운 보안 모델을 제시하며 이에 근거해 기 제안된 프로토콜들과 제안하는 프로토콜의 안전성을 분석한다.

키워드 : RFID 검색 프로토콜, 사용자 프라이버시, 카운터

Efficient RFID Search Protocols Providing Enhanced User Privacy

Jihwan Lim[†] · Heekuck Oh[††] · Daehun Nyang[†††] · Munkyu Lee[††††] · Sangjin Kim[†††††]

ABSTRACT

In an RFID search protocol, a reader uses designated query to determine whether a specific tag is in the vicinity of the reader. This fundamental difference makes search protocol more vulnerable to replay attacks than authentication protocols. Due to this, techniques used in existing RFID authentication protocols may not be suitable for RFID search protocols. In this paper, we propose two RFID search protocols, one based on static ID and the other based on dynamic ID, which use counter to prevent replay attacks. Moreover, we propose a security model for RFID search protocols that includes forward/backward traceability, de-synchronization and forgery attack. Based on this model, we analyze security of our protocols and related works.

Keywords : RFID Search Protocol, User Privacy, Counter

1. 서 론

1.1 RFID 검색 프로토콜 개요

최근 Tan[1]등은 일반적인 RFID 인증 프로토콜과는 다른 RFID 검색 프로토콜을 소개하였다. RFID 검색 프로토콜은 리더의 이동성이 강조되는 모바일 RFID와 같은 환경에 적합한 응용이라 할 수 있어 더욱 관심을 끌고 있다. RFID 검색 프로토콜과 일반적인 인증 프로토콜의 차이점은 리더의 질의 메시지에 있다. 인증 프로토콜이 리더 주변에 존재하는 태그를 인식하기 위해 임의의 태그를 대상으로 하는 질의를 전송하고 질의를 수신한 모든 태그의 응답을 받아 각각의 태그를 인증하는 반면, 검색 프로토콜에서는 특정 태그를 대상으로 하는 검색 질의 메시지를 전송하고 해당 태그의 응답만을 수신하여 메시지를 검증한다. 즉 검색 대상 태그가 아닌 다른 태그들은 자신을 검색하는 질의가 아닐 경우 응답을 하지 않고 무시한다. 이처럼 리더의 질의 메시지에 검색을 원하는 특정 태그의 정보가 포함되어야 한다는 점과 검색 대상이 되는 태그만 리더의 질의에 응답한다는 점은 보안적 측면에서 여러 위협을 야기할 수 있는 인증 프로토콜과의 핵심적인 차이점이다.

1.2 정적 ID vs. 동적 ID

최근 제안되고 있는 해쉬 기반 RFID 프로토콜들은 리더

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성·지원사업의 연구결과로 수행되었음.
본 연구는 2008년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. R01-2006-000-10 957-0).
† 준 회 원 : 한양대학교 컴퓨터공학과 박사과정
†† 종신회원 : 한양대학교 컴퓨터공학과 교수
††† 정 회 원 : 인하대학교 정보통신대학원 부교수
†††† 정 회 원 : 인하대학교 컴퓨터공학부 조교수
††††† 종신회원 : 한국기술교육대학교 인터넷미디어공학부 부교수(교신저자)
논문접수 : 2009년 2월 24일
수 정 일 : 2009년 3월 16일
심사완료 : 2009년 3월 16일

와 태그간 인증을 위해 이용하는 정보가 태그에 고정된 상태로 저장되어 변하지 않는 값인지, 동적으로 갱신되며 저장되는 값인지에 따라 정적 아이디 기반[2-4]과 동적 아이디 기반[5-10]의 상호 인증 프로토콜로 분류할 수 있다[11, 12].

먼저 정적 아이디 기반 프로토콜에서 태그는 리더의 질의에 고정된 아이디(인증/식별 정보) 값을 사용하여 응답한다. 즉 매 세션마다 랜덤수를 사용하는 방법으로 응답하는 값을 변형하긴 하지만 태그에 저장되어 있는 고유 아이디 자체는 변경되지 않는다. 따라서 정적 아이디 기반 프로토콜은 태그가 고정된 아이디 값을 유지하기 때문에 태그-데이터베이스간 공유하고 있는 비밀정보에 대한 동기화가 필요 없다. 하지만 태그는 고정된 아이디 값을 매 응답마다 변형하여 응답하기 위해 자신의 랜덤수와 아이디를 해쉬하여 전송하게 되는데, 데이터베이스가 이 메시지로부터 태그를 구분하고 인증하기위해서는 매번 수신한 랜덤 수와 태그 ID를 저장하고 있는 태그의 수만큼 해쉬하여 비교해 보아야하는 단점이 있다. 또한 태그가 변형 억제(tamper resistant) 기능을 가지도록 만드는 것이 태그의 생산가격 측면에서 현실적이지 못 하다는 점을 감안할 때 태그 포획 능력이 있는 공격자는 태그를 포획하여 저장되어 있는 고유 아이디 정보를 획득할 수 있고 이를 이용하여 태그 사용자의 과거 행적을 추적할 수 있어 전방향 안전성(forward secrecy)을 만족시킬 수 없다는 단점이 있다.

반면 동적 아이디 기반 상호인증 프로토콜에서 태그는 매 세션마다 새로운 아이디로 이전 세션의 아이디를 갱신하여 리더의 질의에 응답하는 값을 변형한다. 동적 아이디 기반 상호인증 프로토콜은 정상적인 경우 동기화된 아이디 및 인증 정보를 이용하여 데이터베이스에서 저장하고 있는 아이디를 별도의 계산과정 없이 검색을 통해 태그를 인식할 수 있으며 아이디 갱신에 일방향 함수(one-way function)를 활용하여 전방향 안전성을 보장해 줄 수 있는 장점이 있다. 하지만 이를 위해서 데이터베이스와 태그는 갱신되는 아이디 및 인증 정보를 동기화하여 유지하여야 하고 동기화가 깨진 경우 재 동기화를 위한 알고리즘이 필요하다는 점과 분산된 데이터베이스 환경을 구축하기 힘들다는 단점이 있다.

1.3 카운터

지금 까지 제안된 대부분의 RFID 프로토콜은 메시지의 최신성(freshness)을 확보하기 위해 랜덤수를 사용하였다. 태그는 리더가 보내온 랜덤수를 자신의 응답을 생성할 때 포함시킴으로써 응답 값의 최신성을 보장한다. RFID 인증 프로토콜의 경우 태그의 응답에 대한 최신성만 확보하면 되지만 리더의 질의에 특정 태그에 대한 정보가 포함된 RFID 검색 프로토콜의 경우 리더의 질의 메시지에 대한 최신성도 보장해야한다. 만약 최신성이 보장되지 않은 리더의 질의에 태그가 반응하여 응답한다면 공격자는 쉽게 태그의 위치를 추적할 수 있게 된다. 이러한 측면에서 카운터는 기존의 랜덤수만 가지고는 해결하기 힘든, 리더의 질의 메시지에 최신성을 부여하는 효과적인 방법이라 할 수 있다.

하지만 카운터를 사용하게 되면 공개되는 카운터 값 자체로 프라이버시에 영향을 미칠 수 있다. 특정 태그의 카운터가 다른 카운터에 비해 구분될 만큼 커져 있다면 랜덤수와는 달리 일정하게 커지는 카운터의 특성상 공격자에게 쉽게 추적당할 수 있다. 기 제안된 Kim[12] 등의 프로토콜이 이에 해당하는 경우로 제안하는 프로토콜에서는 카운터 값을 노출시키지 않고 전달하여 카운터로 인한 프라이버시 노출을 방지하고자 한다.

또 한 가지 고려되어야 하는 사항은 계속 증가하게 되는 카운터 값의 리셋 문제이다. 하지만 현재 RFID 표준(EPC Gen2, ISO 18000-6C)에서처럼 32-bit 카운터를 사용한다고 할 때 카운터의 최댓값은 4,294,967,296 이고 이 경우 매 10초마다 태그를 검색한다고 했을 때 카운터가 최댓값에 도달하기 위해선 1,361년이 걸린다. 더욱이 카운터의 증가가 합법적인 리더에 의해서만 가능하다는 점을 고려하면 카운터가 최댓값에 도달하는 가능성을 현실적으로 무시할 수 있다.

카운터의 최댓값 문제는 카운터를 다시 초기화 방법으로 해결할 수도 있다. 카운터의 초기화는 동적 아이디 기반 프로토콜의 경우 태그의 아이디가 계속 갱신되기 때문에 재사용된 카운터의 사용으로 인한 메시지의 최신성문제가 발생하지 않는다. 하지만 정적 아이디 기반 프로토콜의 경우 초기화된 카운터는 고정된 아이디와 함께 계산되어 중복된 메시지가 생성될 수 있기 때문에 카운터가 초기화 될 때 태그의 정적 아이디를 함께 갱신 해주어야 한다. 이 경우 태그의 아이디가 갱신되기 때문에 완전한 정적 아이디 기반의 프로토콜로 분류할 수는 없지만 태그 아이디의 갱신 주기가 매우 길어 동적 아이디 기반 프로토콜보다는 정적 아이디 기반에 가깝다 할 수 있다.

2. 보안 모델

본 장에서는 RFID 검색 프로토콜을 위한 새로운 RFID 보안 모델을 정의하고 이를 이용해 기존 프로토콜 및 제안하는 프로토콜을 분석한다. 제안하는 보안 모델에서는 리더와 백엔드 시스템간의 통신 채널을 안전한 채널로 가정하며, 공격자는 Juels[8] 등의 모델에서처럼 리더와 태그 사이의 모든 구간, 즉 전방(forward) 채널과 후방(backward) 채널[13]을 모두 도청할 수 있다고 가정한다.

2.1 표기법

본 논문에서는 <표 1>과 같은 표기법을 사용한다.

2.2 공격의 목적

본 모델에서 공격자는 태그-리더 구간의 평문 메시지 또는 기밀성이 보장된 메시지에 대해 위치추적, 비동기, 위조 공격을 시도하며 무시할 수 없는 확률[3]로 다음과 같은 성과를 거두었을 때 공격자의 해당 공격이 성공하였다고 말한다.

• 위치 추적(Traceability): 공격자는 임의 태그 또는 태

〈표 1〉 표기법

T	RFID 시스템의 태그 집합 $T=\{t_1,t_2,...,t_n\}$	N_x	객체 x의 Nonce
R	RFID 리더	ID_r	리더의 아이디
I_m	프로토콜 세션 구간, 세션구간 $I_m=[I_{m_1},I_{m_s}]$은 총 s개의 프로토콜 세션으로 구성	H	일방향 해쉬함수
Challenger	공격자와 객관적 공격 게임을 수행할 제 3의 개체	ID_x, K_x, C_x EPC_x	각각 태그와 데이터베이스가 공유하고 있는 태그 x의 아이디와 키, 카운터, EPC
O	공격자가 사용할 수 있는 오라클의 집합 $O^{\bar{}}(X)$는 오라클 X를 제외한 모든 오라클의 부분집합	ID^{curr}, ID^{prev}	각각 현재 세션구간, 이전 세션구간에서 사용하는 태그의 아이디
$\Omega_{I_m}(T)$	태그 집합 T에 대해 구간 I_m에서 획득할 수 있는 실험 결과 집합, 실험 결과 v_i는 태그로의 질의와 그 응답, 그리고 기타 프로토콜 수행 결과와 관련된 여분 정보들로 구성 $\Omega_{I_m}(T)=\{v_1,v_2,...,v_s\}$		

그 집합을 다른 태그들로부터 구분해 이전에 있었던(forward) 또는 다음에 일어날(backward) 행적을 추적할 수 있다.

- 비동기(Desynchronization): 공격자는 임의 태그 또는 태그 집합을 RFID 시스템이 인식/인증 할 수 없게 할 수 있다.
- 위조(Forgery): 공격자는 특정 태그를 위장하여 해당 태그인 것처럼 인증 받을 수 있다.

공격자가 변형 억제 기능을 구현할 수 없는 태그를 물리적으로 포획하였다면 태그의 모든 기능을 획득하였다고 할 수 있으므로 위에 제시한 공격자의 목적 중 비동기와 위조 공격의 경우에는 태그 포획이 가능한 공격자는 고려하지 않는다. 다만 공격자의 태그 포획이 포획시점 이후의 태그 제어권을 의미하므로 위치추적의 경우 포획 시점 이전 행적에 대한 추적 불가능성을 제공할 수 있어야하며 이를 보장할 때 전방향 안전성을 만족한다고 정의한다.

본 보안 모델에서는 공격자가 어떤 프로토콜에 대해 위 3가지 공격 목적을 달성할 수 없을 때 해당 프로토콜이 *TDF-O-Secure*하다고 정의한다.

2.3 공격자의 능력

본 모델에서의 공격자는 정당한 리더-태그 구간의 모든 메시지를 도청할 수 있으며, 통신에 끼어들어 전송되는 메시지를 선택적으로 전달할 수 있고 태그를 포획하여 내부 정보를 읽어 들일 수 있다.

공격자는 다음과 같은 오라클을 사용할 수 있다.

- LISTEN(t_i,R,I_m): 공격자 A의 도청을 모델링한다. 구간 I_m에서 전송된 태그 t_i와 리더 R간의 통신 메시지를 리턴한다.
- SEARCH(t_i,m,I_m): 구간 I_m에서 공격자 A가 태그 t_i에게 검색을 위한 질의 메시지 m을 전송하는 것을 모델링한다. 합법적인 질의 메시지 m을 이용한 SEARCH 오라클 호출은 태그의 응답 $resp$을 리턴한다.
- RESPONSE(t_i,R,m_1,m_2,I_m): 구간 I_m에서 공격자 A가 리더 R의 태그 t_i에대한 검색 질의 메시지를 수신한 후 이에 대한 응답을 전송하는 것을 모델링한다. 검색 질의 메시지 m_1에 대한 합법적인 응답 메시지 m_2를 이용한 RESPONSE 오라클 호출은 1을 리턴하고 그렇지 않은 경우 0을 리턴한다.
- DESYNCH(t_i,R,m,I_m) : 공격자 A가 구간 I_m에서 합법적 질의 메시지에 대한 태그 t_i의 응답메시지를 막아 리더 R에게 전달되지 못하게 하는 것을 모델링한다. 공격자에 의한 DESYNCH 호출은 구간 I_m에서 하나의 프로토콜 세션을 진행 시키지만 질의 메시지 m에 대한 태그 t_i의 응답 메시지는 의도적으로 생성하지 않는다.
- CORRUPT(t_i,I_m): 구간 I_m에서 공격자 A가 태그 t_i를 포획하여 태그 내부 상태 정보를 획득한다.

2.4 공격 게임

제안하는 모델의 위치 추적, 비동기, 위조 공격은 공격자 A와 *Challenger* 간의 공격 게임으로 정의할 수 있다. O를 공격자가 호출할 수 있는 오라클의 집합 ($O\subset\{L,S,R,D,C\}$)이라고 할 때 *Oracle*은 태그 t_i 또는 태그 집합 $T=\{t_1,t_2,...,t_n\}$와 세션 구간 I_m을 입력으로 공격자 오라클 집합 O를 실험하여 결과 집합 $\Omega_{I_m}(T)$를 출력한다.

2.4.1 위치추적 게임

1. 구간 I_m에서 공격자 A는 $Oracle(T,I_m,O)$를 이용하여 모든 태그 T에 대한 실험 결과 집합 $\Omega_{I_m}(T)$를 획득한다.
2. *Challenger*는 공격 대상 태그 t_b를 랜덤하게 선택하여($b\in\{1,2,...,n\}$) 공격자 A에게 넘긴다.
3. 공격자 A는 구간 I_1에서 실험 결과 집합 $\Omega_{I_m}(T)$을 이용하여 태그 t_b에 대한 검색 질의 m을 생성한다.
4. 공격자 A는 SEARCH(t_b,m,I_1)를 호출하고 태그 t_b을 응

답을 기대한다.

5. 공격자가 태그 t_b의 응답 $resp$을 수신하면 게임에서 승리한다.

2.2 절에서 언급하였듯이 오라클 CORRUPT를 사용할 수 있는 공격자 $A-O(O \subset \{L,S,R,D,C\}$는 $m \leq l$인 구간에서 모든 태그에 대해 추적이 가능하므로 $m \leq l$인 구간에서의 공격자는 $A-O^c(C)$로 가정하며 이 공격자가 수행하는 위치추적에 안전한 프로토콜을 $BT\text{-}O^c(C)\text{-}Secure$하다고 정의한다. 다만 $l < m$인 구간에서 공격자 $A-O$에 대해 위치 추적에 안전한 프로토콜을 $FT\text{-}O\text{-}Secure$하다고 정의한다. $FT\text{-}O\text{-}Secure$한 프로토콜은 $FT\text{-}O^c(C)\text{-}Secure$ 역시 만족하기 때문에 본 모델에서 정의할 수 있는 가장 강한 위치 추적 안전성의 등급은 $BT\text{-}O^c(C)\text{-}Secure$하면서 $FT\text{-}O\text{-}Secure$한 경우 이며, 이를 만족하는 프로토콜을 $T\text{-}O\text{-}Secure$하다고 정의한다. 각각은 후방향, 전방향 위치추적에 안전하다고 표현할 수 있다.

2.4.2 비동기 게임

1. $Challenger$는 공격 대상 태그 t_b를 랜덤하게 선택하여($b \in \{1,2,...,n\}$) 공격자 A에게 넘긴다.
2. 공격자 A는 구간 I_m에서 LISTEN(t_b,R,I_m), SEARCH(t_b,m,I_m), RESPONSE(t_b,R,m_1,m_2,I_m), DESYNCH(t_b,R,m,I_m) 오라클을 전략적인 순서로 호출한다.
3. $Challenger$는 공격 대상 태그 t_b를 검색하는 합법적 질의 메시지 m_1과 그에 대한 응답 m_2를 이용해 RESPONSE(t_b,R,m_1,m_2,I_m) 호출한다. 만약 이 오라클의 결과 값이 1이 아니라면 공격자가 승리한다.

위 비동기 공격에 대해 안전한 프로토콜을 $D\text{-}O\text{-}Secure$하다고 정의한다.

2.4.3 위장 게임

1. 구간 I_m에서 공격자 A는 $Oracle(T,I_m,O)$를 이용하여 모든 태그 T에 대한 실험 결과 집합 $\Omega_{I_m}(T)$를 획득한다.
2. $Challenger$는 공격자 A에게 랜덤하게 선택한 공격 대상 태그 $t_b(b \in \{1,2,...,n\})$와 시스템으로부터 획득할 수 있는 t_b의 합법적 질의 메시지 m_1을 제시한다.
3. 구간 I_l에서 공격자 A는 $\Omega_{I_m}(T)$를 이용하여 $Challenger$에게 넘겨받은 검색 질의 메시지 m_1에 대한 응답 m_2을 만들어 내고 RESPONSE(t_b,R,m_1,m_2,I_l)를 호출하여 검색 성공 결과 값 1을 리턴 받으면 게임에서 승리한다.

위 위장 공격에 대해 안전한 프로토콜을 $F\text{-}O\text{-}Secure$하다고 정의한다.

공격자가 시도하는 비동기와 위장 공격은 $m \leq l$인 구간에서 수행되기 때문에 해당 공격을 시도하는 공격자는 기본적으로 $A-O^c(C)$로 가정할 수 있다. 따라서 이후 표기법의 단순화를 위해 $DF\text{-}O^c(C)\text{-}Secure$의 경우 $DF\text{-}O\text{-}Secure$로 표기하며 어떤 프로토콜이 $TDF\text{-}O\text{-}Secure$하다는 것은 $T\text{-}O\text{-}Secure$하고 동시에 $DF\text{-}O^c(C)\text{-}Secure$하다는 것을 의미한다. 반면 어떤 프로토콜이 $TDF\text{-}O^c(C)\text{-}Secure$하다는 것은 $BT\text{-}O^c(C)\text{-}Secure$하고 동시에 $DF\text{-}O^c(C)\text{-}Secure$하다는 것을 의미한다.

3. 관련 연구

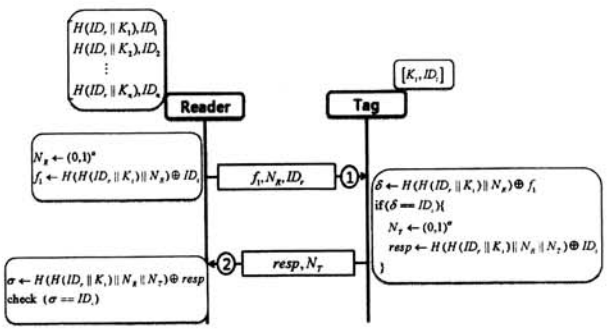
3.1 Tan 등의 검색 프로토콜

Tan[1] 등은 리더와 연결된 데이터베이스가 없는 환경을 가정하며 4가지 RFID 검색 프로토콜을 제안한다.

Tan 등이 가정하고 있는 데이터베이스가 없는 환경은 리더와 데이터베이스가 안전한 채널을 형성하고 있기 때문에 둘을 하나의 객체로 간주하는 기존 접근과는 달리 데이터베이스(시스템)에서 관리하는 태그 인증정보를 리더 쪽으로 위임(delegation)하였다는 부분에서 의미가 있다. (그림 1)은 Tan 등의 기본 검색 프로토콜을 본 논문의 표기법으로 표현한 그림이다.

하지만 Tan 등의 기본 프로토콜은 리더의 검색 질의 메시지를 재전송하는 공격자에 의해서 태그의 위치를 추적당할 수 있다. 태그 측면에서는 리더 질의 메시지의 최신성을 확인할 방법이 없기 때문에 재전송된 질의 메시지에 응답할 수밖에 없다. 또한 정적 아이디를 사용하고 있기 때문에 태그 포획이 가능한 공격자에 대해 전방향 안전성을 보장할 수 없다. 정적 아이디 기반의 프로토콜이기 때문에 비동기 공격에는 영향을 받지 않으며 태그 ID와 키 K_i를 알지 못하는 공격자 $A\text{-}O^c(C)$는 올바른 응답 값을 생성할 수 없기 때문에 위장 공격에도 안전하다. Tan 등의 기본 프로토콜은 제안하는 보안 모델의 $DF\text{-}O\text{-}Secure$ 프로토콜로 분류 할 수 있다.

Tan 등은 자신들의 기본 프로토콜을 위치추적의 강건한 형태로 개선하고자 3가지 검색 프로토콜을 추가로 제안하였다. 첫 번째 프로토콜은 태그가 이전 세션에서 수신한 리더의 랜덤수 N_R을 저장하여 재전송 공격에 대응하고자 했으



(그림 1) Tan 등의 기본 검색 프로토콜

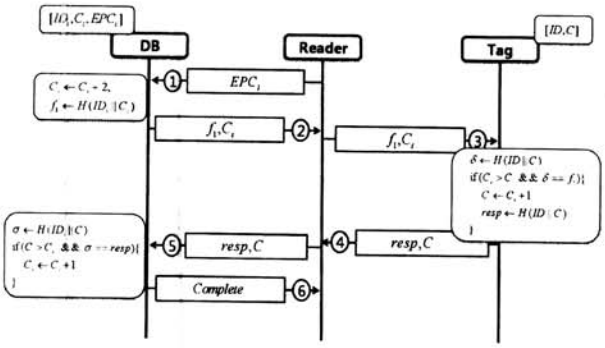
나 태그가 모든 리더의 랜덤수를 계속 저장하고 유지할 수 없기 때문에 완전한 해결책이 될 수 없다. 두 번째와 세 번째 프로토콜 역시 리더 검색 질의에 다수의 태그가 함께 응답하거나 인증 프로토콜에서처럼 리더 주변의 모든 태그가 응답하는 등 검색 프로토콜의 기본 구조를 벗어난 접근으로 근본적인 해결책으로 보기 힘들다.

3.2 Kim 등의 검색 프로토콜

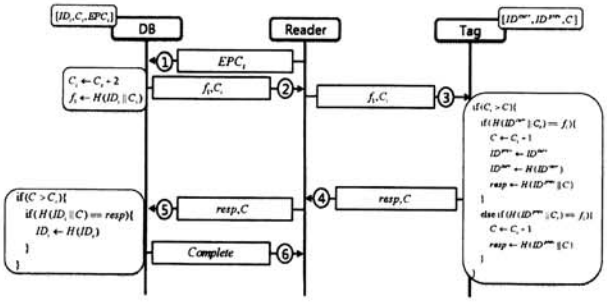
Kim[12] 등은 카운터를 사용하여 재전송 공격에 강건한 정적 아이디 기반 검색 프로토콜과 동적 아이디 기반 검색 프로토콜을 제안하였다. Kim 등의 프로토콜은 카운터의 특성을 이용하여 효과적으로 공격자의 재전송 공격에 대응할 수 있으며 비동기 및 위장 공격에도 안전하게 태그를 검색하고 인증할 수 있다.

하지만 Kim 등의 프로토콜에서 카운터는 공개된 채널에 평문으로 전송되기 때문에 1.3절에서 언급한 것처럼 특정 태그의 카운터가 다른 카운터에 비해 구분될 만큼 커져 있다면 태그의 위치 추적이 가능하게 된다. Kim 등은 자신들의 논문에서 태그의 수와 검색 질의의 빈도수에 따라 카운터가 사용자 프라이버시에 다른 영향을 끼칠 것이라고 분석하고 있으며 이에 대한 대안으로 시스템이 단일한 카운터를 사용하는 방법을 제시하고 있다. 하지만 시스템 전체가 단일한 카운터를 사용하게 되면 카운터 값이 매우 빠르게 증가할 것이고 1.3절에 언급한 카운터의 최대치 문제를 효과적으로 해결해야 하는 문제가 발생하게 된다. 또한 동적 아이디 기반의 프로토콜과는 달리 카운터 값의 빠른 증가로 인한 잦은 카운터 값 초기화는 정적 아이디 기반 프로토콜의 효율성에 심각한 영향을 끼치게 된다. 정적 아이디 프로토콜의 단점은 동적 아이디 기반 프로토콜과는 달리 고정된 아이디로 저장하고 있는 태그의 수만큼 수신한 인증값을 계산해 보아야 한다는 점인데 카운터의 초기화로 인한 고정 아이디의 갱신 여부를 알지 못하는 상황에서 데이터베이스는 수신한 인증값의 적법성을 계산하기 어렵게 되기 때문이다.

이처럼 카운터 값의 공개는 태그의 전방향, 후방향 위치 추적에 모두 영향을 미치게 되어 위치 추적이 가능할 수 있으므로 본 논문에서는 Kim 등의 프로토콜을 *DF-O-Secure* 프로토콜로 분류한다.



(그림 2) Kim 등의 정적 아이디 기반 검색 프로토콜



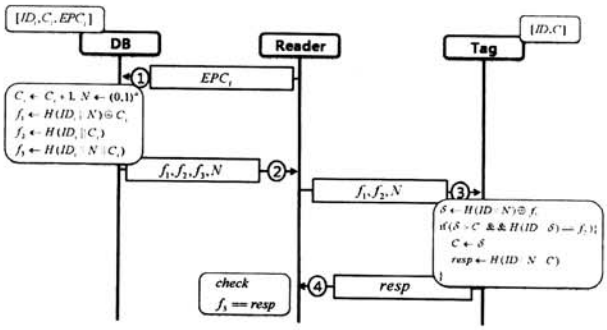
(그림 3) Kim 등의 동적 아이디 기반 검색 프로토콜

4. 제안하는 프로토콜

4.1 정적 아이디 기반 검색 프로토콜

제안하는 정적 아이디기반 검색 프로토콜에서 태그와 데이터베이스는 태그 고유 식별정보 EPC와 매핑되는 태그 ID와 카운터 값 C를 공유하고 있다. 즉 데이터베이스는 각 태그 마다 $[ID_i, C_i, EPC_i]$를 유지하고 있으며 프로토콜의 동작은 (그림 4)와 같다.

- Step 1. 리더는 검색하길 원하는 태그 t_i의 EPC를 데이터베이스에 전송한다.
- Step 2. 데이터베이스는 수신한 EPC로부터 태그 t_i의 카운터 C_i와 ID_i를 찾아 카운터를 1증가 시키고 랜덤수 N을 선택하여 ID_i와 함께 f_1, f_2, f_3를 계산한다. 데이터베이스는 이 값을 랜덤수와 함께 리더에게 전송한다.
- Step 3. f_1, f_2, f_3, N을 수신한 리더는 태그 t_i의 예상 응답 값인 f_3를 저장하고 f_1, f_2, N을 태그에게 전송한다.
- Step 4. 리더의 질의를 수신한 태그는 $H(ID\|N)\oplus f_1$을 계산하여 리더가 사용한 카운터 값을 추출하고 자신의 카운터 보다 큰 값일 때 $H(ID\|\delta)$값을 계산하여 수신한 f_2와 일치하는지 비교한다. 계산한 값과 f_2값이 같다면 태그는 수신한 리더의 카운터로 자신의 카운터를 갱신하고 응답 값 $H(ID\|N\|C)$를 생성하여 리더에게 응답 한다.
- Step 5. 태그의 응답 값을 수신한 리더는 데이터베이스에게서 수신한 f_3와 태그의 응답 값을 비교하여 정당한 태그의 응답인지를 확인한다.



(그림 4) 제안하는 정적 아이디기반 검색 프로토콜

제안하는 정적 아이디기반 검색 프로토콜의 핵심 기여는 다음에 있다.

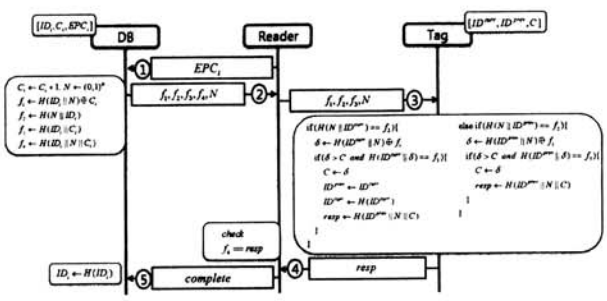
- 재전송 공격에 효과적으로 대응할 수 있도록 카운터를 사용하였다.
- 카운터가 노출 되었을 때 발생하였을 때 문제가 될 수 있는 사용자 프라이버시 문제를 해결하기 위해 랜덤수를 함께 사용해 카운터 정보를 숨겼다.
- 태그의 응답 값을 검증하기 위해 데이터베이스에 다시 질의 했던 기존 프로토콜과는 달리 태그의 응답 값을 미리 예측할 수 있기 때문에 데이터베이스로의 별도 질의가 필요 없다.

각 항목에 대한 추가적인 분석은 5장 분석 부분에서 자세히 다루도록 하겠다.

4.2 동적 아이디 기반 검색 프로토콜

제안하는 동적 아이디기반 검색 프로토콜에서 태그와 데이터베이스는 정적 아이디 기반 검색 프로토콜에서와 마찬가지로 태그 고유 식별정보 EPC와 매핑되는 태그 ID와 카운터 값 C를 공유하고 있다. 데이터베이스는 각 태그 마다 $[ID_i, C_i, EPC_i]$를 유지하고 있으며 태그는 자신의 현재 아이디 ID^{curr}와 이전 세션의 아이디ID^{prev}, 그리고 카운터 값 C를 유지하고 있다. 프로토콜의 동작은 아래 그림과 같다.

- Step 1. 리더는 검색하길 원하는 태그 t_i의 EPC를 데이터베이스에 전송한다.
- Step 2. 데이터베이스는 수신한 EPC로부터 태그 t_i의 카운터 C_i와 ID_i를 찾아 카운터를 1증가 시키고 랜덤수 N을 선택하여 ID_i와 함께 f_1, f_2, f_3, f_4를 계산한다. 데이터베이스는 이 값을 랜덤수와 함께 리더에게 전송한다.
- Step 3. f_1, f_2, f_3, N을 수신한 리더는 태그 t_i의 예상 응답 값인 f_4를 저장하고 f_1, f_2, f_3, N을 태그에게 전송한다.
- Step 4. 리더의 질의를 수신한 태그는 $H(N \| ID^{curr})$를 계산, 수신한 f_2와 비교하여 리더의 질의가 자신의 현재 아이디와 동기화 되어있는지 이전 아이디와 동기화 되어 있는지를 확인한다. 현재 아이디 ID^{curr}와 동기화 되어 있다면 $H(ID^{curr} \| N) \oplus f_1$을 계산하여 리더가 사용한 카운터 값을 추출하고 자신의 카운터 보다 큰 값일 때 $H(ID^{curr} \| \delta)$값을 계산하여 수신한 f_3와 일치하는지 비교하여 자신에게 온 합법적인 질의인지를 확인한다. 계산한 값과 f_3값이 같다면 태그는 수신한 리더의 카운터로 자신의 카운터를 갱신하고 현재 아이디를 이전 세션 아이디 필드에 저장하고 현재 아이디를 일방향 함수 H를 이용하여 갱신하여 저장한다. 아이디와 카운터의 갱신이 끝나면 태그는 응답 값 $H(ID \| N \| C)$를 생성하여 리더에게 응답 한다. 만약 리더의 질의가 자신의 이전 아이디와 동기화 되어있다면 태그는 자신의 카운터 값만 리더로부터 수신한 카운터 값으로 갱신하고 아이디의 갱신 없이 응답 값을 계산해 응답한다.
- Step 5. 태그의 응답 값을 수신한 리더는 데이터베이스에게서 수신한 f_4와 태그의 응답 값을 비교하여 정당한 태그의 응답인지를 확인하고 데이터베이스의 동적 아이디 갱신을 위해 확인 메시지를 전송한다. 리더의 확인 메시지를 수신한 데이터베이스는 태그 t_i의 아이디를 일방향 함수 H를 이용하여 갱신하여 저장한다.



(그림 5) 제안하는 동적 아이디기반 검색 프로토콜

제안하는 동적 아이디 기반 검색 프로토콜에서 태그는 데이터베이스와의 비동기문제를 해결하기 위해 현재 아이디 값과 이전 세션에서 사용한 아이디 값을 함께 유지하고 있다. 4.1절의 정적 아이디 기반 검색 프로토콜과의 차이점은 동적으로 갱신되는 아이디의 동기화 상태를 확인하기 위해 조건절을 한 번 더 거쳐야 하는 부분과 동기화 상태에 따라 아이디의 갱신 여부를 판단하는 부분, 그리고 리더가 태그의 응답 값의 검증 후에도 데이터베이스의 태그 아이디 갱신을 위해 확인 메시지를 전송해야 하는 부분이다.

5. 분석

본 절에서는 제안하는 정적 · 동적 아이디 기반 프로토콜이 각각 *TDF-O^c(C)-Secure, TDF-O-Secure* 프로토콜임을 보인다.

Lemma 1. 제안하는 정적 · 동적 아이디 기반 검색 프로토콜은 공격자 $A-O(O \subset \{L,S,R,D,C\})$에 대해 각각 *T-O^c(C)-Secure, T-O-Secure*하다.

증명. 1) $A-O^c(C)$에 대한 후방향 위치추적 불가능성

2.4.1절의 위치추적 게임을 수행하는 공격자 $A-O^c(C)$를 생각해보자. 공격자가 현재 구간 I_i에서 공격 대상 태그 t_b의 위치를 추적하기 위해서는

- 이전 구간에 수집한 질의 메시지를 재전송하거나,

- 수집한 메시지로부터 새로운 검색 질의 메시지를 생성하여 질의하고,

이후 해당 질의에 대한 태그 t_b의 응답을 수신하여야 한다.

하지만 (그림 4, 5)에서처럼 태그는 카운터 값을 통해 재전송 되는(현재 카운터보다 낮은 수의) 검색 질의 메시지에는 응답을 생성하지 않는다. 따라서 공격자는 새로운 검색 질의 메시지를 생성해야하고 이를 위해서는 공격 대상 태그 t_b의 현재구간 I_l에서의 아이디를 계산할 수 있어야한다. 공격자는 CORRUPT 오라클을 사용할 수 없으며 아이디 갱신에 사용되는 일방향 해쉬 함수 H는 랜덤 오라클 모델[14]을 기반으로 설계되었다고 가정하면 t_b의 아이디를 알아내기 위해 전수 공격을 시도할 수밖에 없다. 공격자가 전수 공격(brute force)을 통해 공격 대상 태그 t_b의 아이디를 계산할 수 있는 확률은 α-bit 아이디에 대해 $1/2^{\alpha}$이므로 이는 무시할 수 있다. 따라서 현재 구간 I_l에서 공격 대상 태그 t_b의 아이디를 모르는 공격자가 합법적인 검색 질의 메시지 m을 생성하는 확률 역시 무시할 수 있다. 그러므로 합법적 질의 메시지 m을 생성 할 수 없는 공격자 A의 SEARCH(t_b,m,I_l) 오라클 호출은 공격 대상 태그 t_b는 응답을 생성하지 못하기 때문에 후방향 위치추적에 안전하다.

2) $A-O(O\subset\{L,S,R,D,C\}$에 대한 전방향 위치추적 불가능성

다시 2.4.1절의 위치추적 게임을 수행하는 공격자 $A-O$를 생각해보자. 공격자 $A-O$는 구간 I_l에서 태그를 포획하여 태그의 현재 아이디와 카운터 값 등을 포함하는 태그 내부 정보와 이전 구간 I_m의 실험 결과 집합 $\Omega_{I_m}(T)$을 확보하고 있다. 공격자 A가 전방향 위치추적 공격에 성공하기 위해서는 이전 실험 결과 집합 $\Omega_{I_m}(T)$에 포함된 태그의 응답 값 집합으로부터 공격 대상 태그 t_b의 응답을 구분해 낼 수 있어야한다.

- 제안하는 정적 아이디 기반 프로토콜에서 태그 t_b는 데이터베이스와 공유하고 있는 아이디를 갱신하지 않은 채 고정된 값으로 사용하기 때문에 태그 t_b의 아이디를 확보한 공격자는 이전 세션 구간의 응답 값을 쉽게 계산할 수 있다. 따라서 공격자 $A-O$에 의한 전방향 위치추적을 막을 수 없다.
- 제안하는 동적 아이디 기반 프로토콜에서 태그 t_b의 응답 메시지는 해당 구간에서의 동적 아이디 값에 의해 계산된다. 하지만 태그 t_b는 데이터베이스와 공유하고 있는 아이디를 매 세션마다 일방향 함수 H를 이용하여 갱신하여 사용하기 때문에 공격자가 이전 세션 구간의 공격 대상 태그 t_b의 응답 값을 계산하려면 이전 세션 구간에서 사용한 태그 t_b의 동적 아이디를 계산할 수 있어야 한다. 이는 일방향 함수의 가정에 의해 계산적으로 어렵기 때문에 무시할 수 있다. 따라서 이전 실험 결과 집합 $\Omega_{I_m}(T)$에 포함된 태그의 응답 값 집합으로부터 공격 대상 태그 t_b의 응답을 구분해 낼 수 없는 공격자는 후방향 위치추적을 성공할 수 없다.

1), 2)와 2.4.1절의 정의에 의해서 제안하는 정적 아이디 기반 검색 프로토콜은 *T-O^c(C)-Secure*하고, 동적 아이디 기반 검색 프로토콜은 *T-O-Secure*하다.

Lemma 2. 제안하는 정적·동적 아이디 기반 검색 프로토콜은 공격자 A-O($O\subset\{L,S,R,D\}$)에 대해 *D-O-Secure*하다.

증명. 2.4.2절의 비동기 게임을 수행하는 공격자 $A-O^c(C)$를 생각해보자. *Challenger*에게 공격 대상 t_b를 넘겨받은 공격자는 구간 I_m에서 LISTEN, SEARCH, RESPONSE, DESYNCH 오라클을 전략적으로 호출하고자 한다. 하지만 공격자 $A-O^c(C)$는 태그의 내부 상태를 알 수 없기 때문에 공격 대상 태그 t_b의 아이디를 α-bit 아이디에 대해 $1/2^{\alpha}$ 확률로 계산할 수 있으며 이는 무시할 수 있다. 따라서 공격 대상 태그 t_b의 아이디를 모르는 공격자 $A-O^c(C)$가 합법적인 질의메시지 m_1이나 응답 메시지 m_2를 계산하는 확률 역시 무시할 수 있다. 즉 공격자 $A-O^c(C)$는 오라클 SEARCH(t_i,m_1,I_m) RESPONSE(t_i,R,m_1,m_2,I_m)는 사용할 수 없으며 LISTEN(t_i,R,I_m)과 DESYNCH(t_i,R,m,I_m)만 사용하여 게임을 진행한다. 다만 LISTEN 오라클의 경우 리더가 태그 검색에 성공한 경우와 실패한 경우로 나누어 LISTEN-S, LISTEN-F로 구분한다. <표 2>에는 공격자가 선택한 오라클이 프로토콜에서 어떤 결과를 가져오는지 나타나있다. 공격자가 오라클을 호출할 때 마다 태그와 데이터베이스의 내부 상태는 변경되게 되며 이에 따라 아이디와 카운터 값의 동기화 상태도 변하게 된다.

<표 3, 4>와 (그림 6, 7)은 데이터베이스와 태그의 동기화 상태 및 재동기가 되는 과정을 게임에서 공격자가 어떤 오라클을 호출하는가에 따라 보여주고 있다. 데이터베이스와 태그의 동기화 상태는 <표 3, 4>와 같이 분류할 수 있고 공격자의 O(L,D) 호출은 프로토콜에서 <표 2>와 같은 결과를 가져오게 된다.

공격자는 태그와 데이터베이스의 동기화 상태가 Broken-

〈표 2〉 공격자의 행동(Oracle)에 따른 세션의 진행 상태

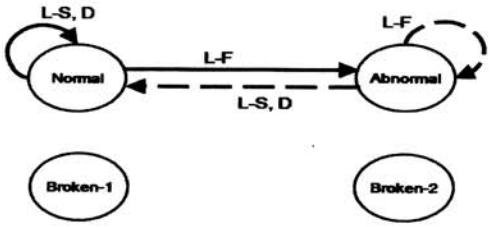
Oracle	프로토콜에서의 결과
LISTEN-S	검색 성공, 정상 세션
LISTEN-F	검색 실패, DB의 카운터만 증가
DESYNCH	단계 4의 메시지 전달 X, DB의 태그 아이디 갱신 X

〈표 3〉 태그와 데이터베이스의 동기화 - 정적 아이디

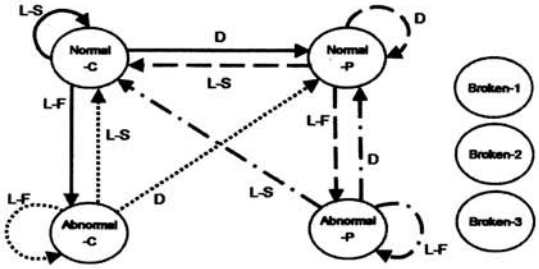
State	ID Synch.	Counter Synch.
Normal	O	$C_{DB} = = C_{Tag}$
Abnormal	O	$C_{DB} > C_{Tag}$
Broken-1	O	$C_{DB} < C_{Tag}$
Broken-2	X	

〈표 4〉 태그와 데이터베이스의 동기화 - 동적 아이디

State	ID Synch.	Counter Synch.
Normal-C	Synch. with IDcurr	$C_{DB} = = C_{Tag}$
Normal-P	Synch. with IDprev	$C_{DB} = = C_{Tag}$
Abnormal-C	Synch. with IDcurr	$C_{DB} > C_{Tag}$
Abnormal-P	Synch. with IDprev	$C_{DB} > C_{Tag}$
Broken-1	Synch. with IDcurr	$C_{DB} < C_{Tag}$
Broken-2	Synch. with IDprev	$C_{DB} < C_{Tag}$
Broken-3	X	



(그림 6) 태그와 DB의 동기화 상태 전이도 - 정적 아이디



(그림 7) 태그와 DB의 동기화 상태 전이도 - 동적 아이디

1, Broken-2, Broken-3 중 하나로 전이되는 것을 목표로 오라클 $O(L,D)$를 전략적으로 호출하지만 (그림 6, 7)의 동기화 상태 전이도에서 보이는 것처럼 어떠한 경우에도 Broken 상태로 전이되지 않는다. 따라서 제안하는 정적·동적 아이디기반 프로토콜은 *D-O-Secure* 프로토콜이다.

Lemma 3. 제안하는 프로토콜은 공격자 A-O ($O \subset \{L, S, F, D\}$)에 대해 *F-O-Secure*하다.

증명. 3.3절의 위장 공격 게임을 수행하는 공격자 A를 생각해보자. 공격자는 구간 I_m에서의 실험 집합 $\Omega_{I_m}(T)$을 획득한다. 이후 구간 I_l에서 공격자는 $\Omega_{I_m}(T)$을 이용하여 t_b인척 위장하여 리더의 검색 질의에 응답하고 시스템으로부터 인증을 시도한다. 공격자가 공격에 성공하기 위해 다음이 가능해야 한다.

- 이전 구간에서 수집된 메시지로부터 적법한 응답 메시지를 새롭게 생성하여 인증을 통과한다.
- 이전 구간에서 전송된 태그의 응답 메시지를 재전송하여 인증을 통과한다.

하지만 공격자가 공격 대상 태그 t_b를 검색하는 리더의 질의 메시지 m_1에 대한 응답 메시지 m_2를 생성해 내기 위해선 위치 추적게임에서처럼 태그 t_b의 아이디를 알고 있어야한다. CORRUPT 오라클을 사용할 수 없는 공격자가 전수공격을 통해 공격 대상 태그 t_b의 아이디를 계산할 수 있는 확률은 α-bit 아이디에 대해 $1/2^{\alpha}$이므로 이는 무시할 수 있다. 또한 재전송의 경우 공격자가 전송한 이전 세션의 응답 메시지는 리더가 가지고 있는 현재 세션의 응답 메시지와 일치하지 않아 리더의 인증을 통과할 수 없다.

따라서 본 프로토콜은 *F-O-Secure*하다.

Lemma 1, 2, 3로부터 제안한 정적 아이디 기반 검색 프로토콜은 *T-O^c(C)-Secure*하고 *D-O-Secure*하며 *F-O-Secure*하므로 *TDF-O^c(C)-Secure*하고, 동적 아이디 기반 검색 프로토콜은 *T-O-Secure*하고 *D-O-Secure*하며 *F-O-Secure*하므로 *TDF-O-Secure*하다.

〈표 5〉 관련 연구 및 제안하는 프로토콜의 안전성 비교.

	위치추적		비동기	위장	구분	비고
	후방	전방				
Tan 등	X	X		O	*DF-O-Secure*	비동기 공격 해당사항 없음
Kim 등의 정적 아이디	X	X	O	O	*DF-O^c(C)-Secure*	카운터에 의한 위치 프라이버시 노출
Kim 등의 동적 아이디	X	X	O	O	*DF-O-Secure*	카운터에 의한 위치 프라이버시 노출
제안하는 정적 아이디	O	X	O	O	*TDF-O^c(C)-Secure*	
제안하는 동적 아이디	O	O	O	O	*TDF-O-Secure*	

6. 결 론

본 논문에서는 카운터를 사용하는 2가지 RFID 검색 프로토콜을 제안하였다. 제안하는 정적 아이디 기반 검색 프로토콜과 동적 아이디 기반 검색프로토콜은 카운터를 사용하여 일반적인 랜덤수만 사용하는 검색 프로토콜에서 방어하기 힘든 재전송 공격에 쉽게 대응할 수 있으며 카운터 크기의 노출로 인한 태그의 위치 추적 가능성을 제거하였다. 제안하는 프로토콜은 카운터를 숨기기 위해 Kim[12] 등의 프로토콜보다 태그와 데이터베이스가 각각 정적 기반은 1회씩 동적 기반은 1회와 2회 씩의 해쉬 연산을 더 수행해야한다. 하지만 리더가 검색 대상 태그의 질의 메시지를 데이터베이스로부터 수신할 때 태그의 응답 값도 함께 수신할 수 있어 데이터베이스로의 통신량을 줄일 수 있다. 제안하는 정적/동적 아이디기반 검색 프로토콜은 각각 제안하는 보안 모델의 $TDF\text{-}O^{c}(C)\text{-}Secure$, $TDF\text{-}O\text{-}Secure$ 프로토콜로 분류되며 강화된 사용자 프라이버시를 제공할 수 있다.

참 고 문 헌

[1] C.C. Tan, B. Sheng, and Q. Li, "Secure and Serverless RFID Authentication and Search Protocols," *IEEE Transactions on Wireless Communications*, volume 7(3), pages 1400-1407, 2008.

[2] A. Juels and S. Weis, "Defining Strong Privacy for RFID," *Cryptology ePrint Archive*, Report 2006/137, 2006.

[3] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," *Proc. of the SPC 2005*, volume 3450 of LNCS, pages 70-84, Springer-Verlag, 2005.

[4] S.A. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," *Proc. of the SPC 2003*, volume 2802 of LNCS, pages 201-212, Springer-Verlag, 2004.

[5] C. Lim and T. Kwon, "Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer," *Proc. of the ICICS 2006*, volume 4307 of LNCS, pages 1-20, Springer-Verlag, 2006.

[6] S. Vaudenay, "On Privacy Models for RFID," *Proc. of the Asiacrypt 2007*, volume 4833 of LNCS, pages 68-87, Springer-Verlag, 2007.

[7] P.I. Paise and S. Vaudenay, "Mutual Authentication in RFID: Security and Privacy," *Proc. of the CCS 2008*, pages 292-299, ACM, 2008.

[8] T. Dimitriou, "A Lightweight RFID protocol to protect against traceability and cloning attack," *Proc. of the SecureComm 2005*, pages 59-66, 2005.

[9] S. Lee and Y. Hwang, "Efficient authentication for low-cost RFID systems," Proc. of the ICCSA 2005, volume 3480 of LNCS, pages 619-629, Springer-Verlag, 2005.

[10] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Efficient hash-chain based RFID privacy protection scheme," *Proc. of the Ubicomp*, 2004.

[11] J. Lim, S. Kim, and H. Oh, "A New Hash-base RFID Mutual Authentication Protocol Providing Enhanced User Privacy Protection," *Proc. of the ISPEC 2008*, volume 4991 of LNCS, pages 278-289, Springer-Verlag, 2008.

[12] S. Kim, J. Lim, J. Han, and H. Oh, "Efficient RFID Search Protocols Using Counters," *IEICE Transactions on Communications*, volume E91-B(11), pages 3552-3559, 2008.

[13] G. Avoine, "Adversarial Model for Radio Frequency Identification," Cryptology ePrint Archive, Report 2005/049, 2005.

[14] M. Bellare, P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," *Proc. of the CCS 1993*, pages 62-73, ACM, 1993.

임 지 환

e-mail : jhlim@cse.hanyang.ac.kr

2005년 한양대학교 전자컴퓨터공학부(학사)

2007년 한양대학교 컴퓨터공학과(석사)

2007년~현 재 한양대학교 컴퓨터공학과 박사과정

관심분야 : 네트워크 보안, 암호프로토콜

오 희 국

e-mail : hkoh@hanyang.ac.kr

1983년 한양대학교 전자공학과(학사)

1989년 아이오와주립대학 전자계산학과(석사)

1992년 아이오와주립대학 전자계산학과(박사)

1993년~1994년 한국전자통신연구원 선임연구원

1995년~현 재 한양대학교 컴퓨터공학과 교수

관심분야 : 암호프로토콜, 네트워크 보안

양 대 헌

e-mail : nyang@inha.ac.kr

1994년 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업(학사)

1996년 연세대학교 컴퓨터과학과(석사)

2000년 연세대학교 컴퓨터과학과(박사)

2000년~2003년 한국전자통신연구원 정보보호연구본부 선임연구원

2003년~현 재 인하대학교 정보통신대학원 부교수

관심분야 : 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안

이 문 규

e-mail : mklee@inha.ac.kr

1996년 서울대학교 컴퓨터공학과(공학사)

1998년 서울대학교 컴퓨터공학과(공학석사)

2003년 서울대학교 전기컴퓨터공학부(공학박사)

2003년~2005년 한국전자통신연구원 선임연구원

2005년~현 재 인하대학교 컴퓨터공학부 조교수

관심분야 : 정보보호, 암호알고리즘, 계산이론

김 상 진

e-mail : sangjin@kut.ac.kr

1995년 2월 한양대학교 전자계산학과(학사)

1997년 2월 한양대학교 전자계산학과(석사)

2002년 8월 한양대학교 전자계산학과(박사)

2003년 3월~현 재 한국기술교육대학교 인터넷미디어공학부 조교수

관심분야 : 암호기술 응용