



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0010604
(43) 공개일자 2012년02월06일

(51) Int. Cl.

H04L 9/32 (2006.01) H04L 12/22 (2006.01)

(21) 출원번호 10-2010-0070091

(22) 출원일자 2010년07월20일

심사청구일자 2010년07월20일

(71) 출원인

충남대학교산학협력단

대전 유성구 공동 220 충남대학교

(72) 발명자

여돈구

충청남도 아산시 신창면 읍내리 순천향대학교
M114

이상래

충청남도 아산시 신창면 읍내리 순천향대학교
M114

(뒷면에 계속)

(74) 대리인

특허법인정직과특허

전체 청구항 수 : 총 12 항

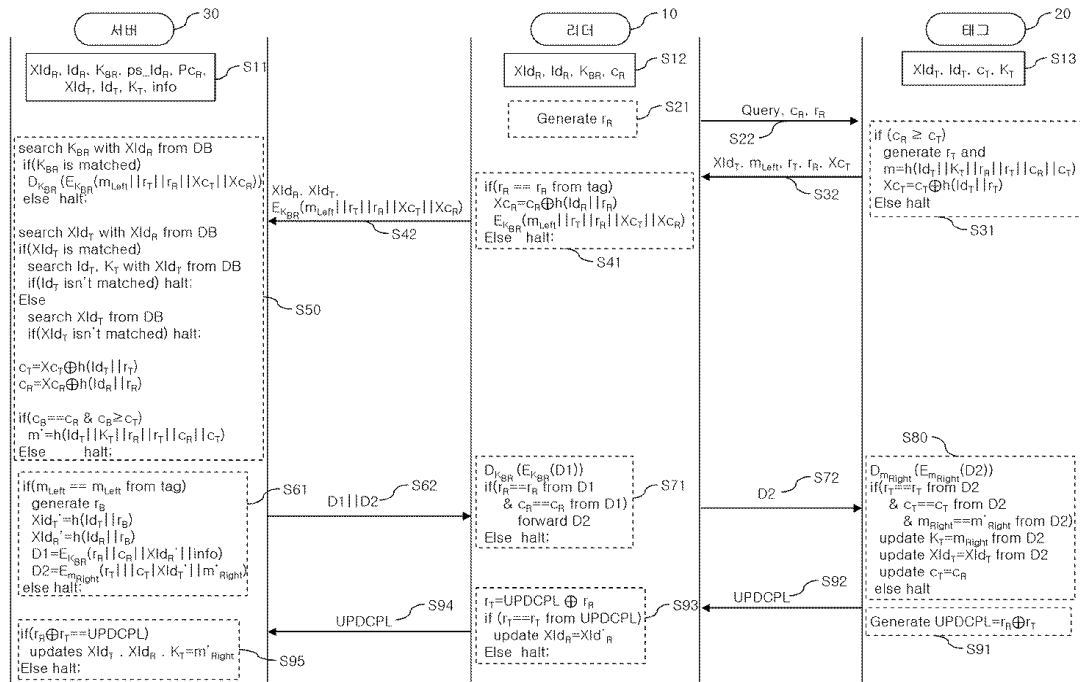
(54) 서버와 리더의 위장공격 탐지가 가능한 랜덤 아이디 기반 RFID 상호 인증 방법

(57) 요약

서버, 다수의 리더, 및 다수의 태그로 구성된 RFID 태그 시스템에서 동기화 카운터를 이용하여 동기화된 상대와 인증을 처리하는 랜덤 아이디 기반 RFID 상호 인증 방법에 관한 것으로서, (a) 각 리더 및 태그는 각자 카운터 및 동적 아이디를 저장하고, 서버는 서버의 카운터(이하 제3 카운터)를 저장하고, 서버와 태그는 비밀키를 공유하는 단계; (b) 제1 리더는 자신 카운터(이하 제1 카운터)를 제2 태그에 전송하는 단계; (c) 제2 태그는 자신 카운터(이하 제2 카운터)와 제1 카운터가 정당한 상태이면, 비밀키를 이용하여 제1 인증 메시지를 생성하여 제2 카운터 및 자신 동적 아이디(이하 제2 동적 아이디)와 함께 제1 리더로 전송하는 단계; (d) 제1 리더는 자신 동적 아이디(이하 제1 동적 아이디) 및 제2 동적 아이디를 제1 및 제2 카운터와 함께 서버로 전송하는 단계; (e) 서버는 제1 및 제2 카운터가 제3 카운터와 정당한 상태이면 공유된 비밀키를 이용하여 제2 인증 메시지를 생성하는 단계; (f) 서버는 제1 인증 메시지를 제2 인증 메시지를 비교하여 검증하고, 제1 및 제2 갱신 아이디를 생성하여 제2 인증 메시지와 함께 제1 리더를 전송하는 단계; (g) 제1 리더는 서버로부터 수신한 제2 갱신 아이디 및 제2 인증 메시지를 제2 태그로 전송하는 단계; (h) 제2 태그는 제2 인증 메시지를 제1 인증 메시지와 비교하여 검증하고, 제2 비밀키를 갱신하고, 제2 동적 아이디를 제2 갱신 아이디로 갱신하고, 제2 카운터를 제1 카운터로 갱신하는 단계; (i) 제2 태그는 응답 메시지를 생성하여 제1 리더로 전송하는 단계; (j) 제1 리더는 응답 메시지를 수신하면 제1 동적 아이디를 제1 갱신 아이디로 갱신하고, 응답 메시지를 서버로 전송하는 단계; (h) 서버는 응답 메시지를 수신하면 공유된 제1 및 제2 공유 아이디를 제1 및 제2 갱신 아이디로 갱신하고, 공유된 비밀키를 갱신하는 단계를 포함하는 구성을 마련한다.

상기와 같은 랜덤 아이디 기반 RFID 상호 인증 방법에 의하여, 서버, 리더, 태그 사이의 상호인증을 지원하고, 재전송 공격 및 태그와 리더의 위장공격, 태그 위치추적공격, 서비스 거부 공격에 안전하고, 서버의 태그 탐색에 대한 서버 검색률을 개선하여 상호인증의 효율성을 높일 수 있다.

대표도



(72) 발명자

장재훈

충청남도 아산시 신창면 읍내리 순천향대학교 M114

염홍열

충청남도 아산시 신창면 읍내리 순천향대학교 M114

류재철

대전광역시 유성구 어은로 57, 132동 801호 (어은동, 한빛아파트)

특허청구의 범위

청구항 1

서버, 다수의 리더, 및 다수의 태그로 구성된 RFID 태그 시스템에서 동기화 카운터를 이용하여 동기화된 상대와 인증을 처리하는 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서,

- (a) 각 리더는 상기 리더의 카운터 및 동적 아이디를 저장하고, 각 태그는 상기 태그의 카운터 및 동적 아이디, 비밀키를 저장하고, 상기 서버는 서버의 카운터(이하 제3 카운터) 및, 모든 태그의 동적 아이디와 비밀키를 저장하는 단계;
- (b) 하나의 리더(이하 제1 리더)는 제1 랜덤수를 발생하고, 상기 제1 리더의 카운터(이하 제1 카운터)와 상기 제1 랜덤수를 쿼리와 함께 태그(이하 제2 태그)에 전송하는 단계;
- (c) 상기 제2 태그는 상기 제2 태그의 카운터(이하 제2 카운터)가 상기 제1 카운터와 정당한 상태이면, 제2 랜덤수를 발생하고, 상기 제2 태그의 비밀키(이하 제2 비밀키)를 이용하여 제1 인증 메시지를 생성하고, 상기 제2 카운터 및 제2 태그의 동적 아이디(이하 제2 동적 아이디), 상기 제1 인증 메시지, 제1 및 제2 랜덤수를 상기 제1 리더로 전송하는 단계;
- (d) 상기 제1 리더는 수신한 제1 랜덤수를 검증하고, 검증되면 상기 제1 리더의 동적 아이디(이하 제1 동적 아이디), 상기 제2 동적 아이디, 제1 및 제2 카운터, 상기 제1 및 제2 랜덤수를 상기 서버로 전송하는 단계;
- (e) 상기 서버는 상기 제2 동적 아이디에 대응되는 공유된 비밀키를 검색하고, 상기 제1 및 제2 카운터가 제3 카운터와 정당한 상태이면 공유된 비밀키를 이용하여 제2 인증 메시지를 생성하는 단계;
- (f) 상기 서버는 상기 제1 인증 메시지를 상기 제2 인증 메시지를 비교하여 검증하고, 검증되면 제1 및 제2 갱신 아이디를 생성하고, 상기 제2 태그에 대한 부가정보(info)를 상기 제2 인증 메시지, 상기 제1 및 제2 갱신 아이디, 제1 및 제2 카운터, 제1 및 제2 랜덤수와 함께 상기 제1 리더로 전송하는 단계;
- (g) 상기 제1 리더는 수신한 제1 카운터 및 제1 랜덤수로 검증하고, 검증되면 상기 서버로부터 수신한 제2 갱신 아이디 및 제2 인증 메시지, 제2 랜덤수, 제2 카운터를 상기 제2 태그로 전송하는 단계;
- (h) 상기 제2 태그는 수신한 제2 카운터 및 제2 랜덤수로 검증하고, 검증되면 상기 제2 인증 메시지를 상기 제1 인증 메시지와 비교하여 검증하고, 검증되면 상기 제2 비밀키를 상기 제2 인증 메시지를 이용하여 갱신하고, 상기 제2 동적 아이디를 상기 제2 갱신 아이디로 갱신하고, 상기 제2 카운터를 상기 제1 카운터로 갱신하는 단계;
- (i) 상기 제2 태그는 응답 메시지를 생성하여 상기 제1 리더로 전송하는 단계;
- (j) 상기 제1 리더는 상기 응답 메시지를 수신하여 검증하고, 검증되면 상기 제1 동적 아이디를 상기 제1 갱신 아이디로 갱신하고, 상기 응답 메시지를 상기 서버로 전송하는 단계;
- (k) 상기 서버는 상기 응답 메시지를 수신하여 검증하고, 검증되면 공유된 제1 및 제2 공유 아이디를 상기 제1 및 제2 갱신 아이디로 갱신하고, 공유된 비밀키를 상기 제2 인증 메시지를 이용하여 갱신하는 단계를 포함하는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 2

제1항에 있어서,

상기 서버와 태그는 상기 태그의 고정 아이디를 공유하고,

상기 제1 및 제2 인증 메시지는 태그의 고정 아이디 및 비밀키를 해쉬하여 생성되는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 3

제2항에 있어서,

상기 제1 및 제2 인증 메시지는 제1 및 제2 카운터, 제1 및 제2 랜덤수를 더 포함하여 해쉬하는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 4

제1항에 있어서,

상기 리더 또는 태그는 수신한 카운터 또는 랜덤수를 상기 리더 또는 태그가 저장하고 있는 카운터 또는 랜덤수를 비교하여 동일여부로 검증하는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 5

제1항에 있어서,

상기 (c)단계에서, 상기 제2 태그는 상기 제1 인증 메시지의 제1 부분을 전송하고,

상기 (f)단계에서, 상기 서버는 상기 제2 인증 메시지의 제2 부분을 전송하되, 상기 제2 인증 메시지의 제2 부분은 상기 제1 인증 메시지의 제1 부분과는 메시지의 서로 다른 위치인 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 6

제1항에 있어서,

상기 제1 카운터의 값이 상기 제2 카운터 보다 같거나 클 때 동기화가 검증되거나, 상기 제3 카운터의 값이 상기 제2 카운터 보다 같거나 클 때 동기화가 검증되거나, 상기 제2 및 제3 카운터의 값이 동일할 때 동기화가 검증되는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 7

제2항에 있어서,

상기 서버와 리더는 상기 리더의 고정 아이디를 공유하고,

상기 카운터를 암호화하여 전송하되, 상기 카운터에 상기 고정 아이디 및 카운터를 해쉬한 값을 XOR연산하여 암호화하고,

암호화된 카운터를 복호화하여 처리하되, 상기 암호화된 카운터에 상기 고정 아이디 및 카운터를 해쉬한 값을 XOR연산하여 복호화하는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 8

제7항에 있어서,

상기 (f)단계에서, 상기 서버는 제3 랜덤수를 생성하고 공유된 제1 또는 제2 고정 아이디에 상기 제3 랜덤수를 연접하고 해쉬하여 상기 제1 또는 2 갱신 아이디를 생성하는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 9

제1항에 있어서,

상기 서버와 리더는 공유키를 공유하여, 상기 공유키로 데이터를 암호화하여 전송하고 수신한 데이터를 복호화하는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 10

제1항에 있어서,

상기 응답 메시지는 상기 제1 및 제2 랜덤수를 XOR 연산하여 생성되고,

상기 응답메시지에 제1 또는 제2 랜덤수를 XOR 연산하여 상기 제2 또는 제1 랜덤수를 추출하고, 추출된 제2 또는 제1 랜덤수를 저장된 제2 또는 제1 랜덤수와 비교하여 동일여부로 검증되는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 11

제1항에 있어서,

상기 (g)단계 또는 상기 (h)단계는, 상기 제1 리더 또는 제2 태그는 수신한 랜덤수 및 카운터로 검증하되, 수신한 랜덤수 및 카운터와 저장된 랜덤수 및 카운터와 동일여부로 검증하는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

청구항 12

제2항에 있어서,

상기 (a)단계에서, 상기 서버는 태그의 동적 아이디에 대응되는 태그의 고정 아이디 및 비밀키를 제1 테이블로 구성하고, 리더의 동적 아이디 및 태그의 동적 아이디에 대응되는 태그의 고정 아이디 및 비밀키를 제2 테이블로 구성하고,

상기 (e)단계는 상기 서버는 상기 제2 테이블을 검색하여 태그의 고정 아이디 및 비밀키를 검색하고, 상기 제2 테이블에서 검색결과가 없으면 상기 제1 테이블에서 검색하는 것을 특징으로 하는 랜덤 아이디 기반 RFID 상호 인증 방법.

명세서

기술 분야

- [0001] 본 발명은 서버, 다수의 리더, 및 다수의 태그로 구성된 RFID 태그 시스템에서 동기화 카운터를 이용하여 동기화된 상대와 인증을 처리하는 랜덤 아이디 기반 RFID 상호 인증 방법에 관한 것이다.
- [0002] 특히, 본 발명은 서버와 태그가 공유하는 비밀키로 인증 메시지를 생성하여 인증 메시지를 통해 상호 검증하는 랜덤 아이디 기반 RFID 상호 인증 방법에 관한 것이다.
- [0003] 또한, 본 발명은 서버, 리더, 태그는 상호 인증 후 동적 아이디를 갱신하되, 태그가 동적 아이디를 갱신 후 응답 메시지를 보내면 리더와 서버는 순차적으로 동적 아이디를 갱신하여 동적 아이디를 동기화시키는 랜덤 아이디 기반 RFID 상호 인증 방법에 관한 것이다.
- [0004]

배경 기술

- [0005] 일반적으로, 유비쿼터스 환경에서 RFID(Radio Frequency Identification) 태그를 사물에 부착하여 사물을 식별하고, 정보를 빠르고 편리하게 확인할 수 있어 군사, 물류, 에너지/환경, 융합신산업, 바이오산업 등에서 바코

드의 대체 수단으로 이용되고 있다.

- [0006] 하지만, 실생활에서 거의 모든 사물에 RFID 태그가 부착되었다고 본다면 태그의 식별정보 수집으로 인한 이동경로추적, 금전적 지출 및 사회적 지위 등의 개인 프라이버시와 관련된 정보가 노출될 수 있는 문제점이 있다. 즉, RFID 시스템에는 무선 구간이 존재함으로써 도청, 전파범위 제한에 따른 통신 두절, 간섭 등의 문제점이 발생할 수 있다.
- [0007] RFID 시스템의 안전성을 위협할 수 있는 공격으로 도청, 트래픽 분석 등의 수동적 공격과 위조, 서비스 거부 공격 등의 능동적 공격들이 있으며, 이런 공격들로부터 안전한 RFID 시스템 설계를 위해서는 전달되는 인증 정보의 기밀성 및 무결성, 태그 식별 정보의 익명성 등의 기본적인 보안 요구사항이 만족되어야 할 것이다. 하지만 RFID 태그의 경우, 연산능력과 저장 능력에 제한이 있으므로 기존의 공개키 방식이나 대칭키 방식의 암호화 알고리즘을 적용하는 것은 적절하지 않다.
- [0008] 초기 RFID 보안 대책으로 kill tag, faraday case, active jamming, blocker tag를 이용한 방식들이 알려졌으며, 이후 해쉬 연산을 이용한 해쉬락, 재암호화, 해쉬 체인 방식 등이 소개되었다. 최근에는 경량화된 대칭키 및 공개키 암호에 대한 연구가 활발히 연구되고 있다.
- [0009] 먼저, 종래의 XOR과 해쉬를 이용한 인증 방법(이하 제1 종래방법)을 설명한다.
- [0010] 상기 제1 종래방법에서는 백엔드 서버가 사전에 리더에게 공유키(K_{BR})를 제공함으로써 백엔드 서버와 리더 구간에 암호화를 지원하고 있다. 리더는 태그로부터 수신한 태그 아이디(Id_T)를 백엔드 서버로 전달하고, 아이디(Id_T)에 해당하는 비밀키(K_T)를 수신하게 된다. 이후 리더가 랜덤수(r_R)를 생성한 후 태그에게 전송하고, 태그로부터 인증 메시지 $m=h(r_R \oplus K_T)$ 를 수신한다. 리더는 백엔드 서버로부터 수신한 비밀키(K_T)를 이용하여 인증 메시지(m)를 계산하고, 태그로부터 수신한 인증 메시지(m)와 동일한 경우 태그를 인증하게 된다. 인증에 필요한 연산량은 리더에서 암호화 각 1회, 랜덤값 생성 1회, XOR 연산 1회, 해쉬 연산 1회를 수행하고, 태그에서, XOR 연산 1회, 해쉬 연산 1회가 수행된다. 총 메시지 전송 횟수는 6회이다.
- [0011] 하지만, 공격자는 태그가 리더를 인증하지 않은 상태에서 리더로 전달되는 아이디(Id_T)가 그대로 노출된다는 점을 이용하여 도청 공격 및 태그의 위치 추적 공격을 할 수 있다. 도청의 경우 리더와 태그 사이가 무선 구간이므로 전달되는 아이디(Id_T)를 수집할 수 있다. 설령, 무선 구간이 사용하지 않더라도 유선 근거리통신망 상에 존재하는 내부 공격자가 존재한다면 공격 가능성은 상존한다. 유선 네트워크를 태그의 위치 추적 공격은 태그에게 쿼리를 전달하면 동일한 아이디(Id_T)가 리턴되므로 가능하다. 또한, 공격자가 리더로 가장하여 사전에 관련 데이터(Id_T, r_R, m)를 수집하는 경우, 인증 정보 재전송을 통한 태그 위장 공격이 가능할 것이다.
- [0012] 다음으로, 랜덤수를 이용하여 개선한 인증 방법(이하 제2 종래방법)을 설명한다.
- [0013] 상기 제2 종래방법은 리더가 태그로 쿼리 전송시 제1 랜덤수(r_R)를 함께 전달함으로써 재전송 공격이 불가능하도록 개선하였다. 태그의 응답에서 제2 랜덤수(r_T)가 포함되므로 태그의 익명성과 위치 추적 공격에 대한 안전성을 제공한다.
- [0014] 태그는 인증 메시지(m)와 제2 랜덤수(r_T)만을 리더로 전송함으로 태그 아이디(Id_T)와 비밀키(K_T)에 대한 노출을 방지할 수 있다. 인증에 필요한 연산량은 리더의 경우 랜덤 값 생성 1회, 암호복호화 각 1회를 수행한다. 태그의 경우, 랜덤 값 생성 1회, 해쉬 연산 1회로 상기 제1 종래방법 보다 리더와 태그의 연산 모두 감소하였으며, 라운드 수를 4회로 감소시켰다.
- [0015] 하지만, 태그 아이디(Id_T)와 비밀키(K_T)가 갱신되지 않으므로 공격자가 태그의 그룹에 동일한 리더 랜덤수(r_R)를 쿼리와 함께 반복적으로 요청하는 경우 (r_R, m, r_T)쌍을 수집할 수 있어 태그의 위치 추적이 가능하다.
- [0016] 다음으로, 동적 아이디기반 RFID 상호 인증 방법(이하 제3 종래방법)을 설명한다.

- [0017] 상기 제3 종래방법은 동적 아이디를 지원하는 RFID 시스템에 적용한 방법으로서, 백엔드 서버와 리더 구간을 안전한 채널로 가정하여 백엔드 서버와 리더를 하나의 시스템으로 표현하고 있다.
- [0018] 태그는 자신의 아이디(Id_T)와 비밀키(K_T)를, 백엔드 서버는 아이디(Id_T), 현재키(CK_T), 이전키(PK_T), info정보를 저장한다. 리더가 제1 랜덤수(r_R)를 생성하여 쿼리와 함께 태그로 전송하고, 태그로부터 아이디(Id_T), (태그가 생성한) 제2 랜덤수(r_T), 인증정보 $m=h(K_T, r_R || r_T)$ 의 좌측 절반 값인 m_{Left} 를 응답 받는다. 리더는 이를 수신하여 제1 랜덤수(r_R)와 함께 백엔드 서버로 전달한다.
- [0019] 한편, 리더에 인증 정보 전달을 마친 태그는 아이디(Id_T)를 $h(K_T, Id_T)$ 로 갱신한다. 백엔드 서버는 태그로부터 수신한 아이디(Id_T)를 식별자로 DB를 검색하여 m_{Left} 를 확인하고, 인증 된 경우 비밀키(K_T)와 아이디(Id_T)를 각각 $h(K_T || r_R)$, $h(K_T, Id_T)$ 로 갱신한다.
- [0020] 아이디(Id_T)가 DB에서 색인되지 않을 경우, 전체 태그의 현재키(CK_T)와 이전키(PK_T)를 대상으로 m_{Left} 연산을 수행하여 일치하는 경우 현재키(CK_T), 이전키(PK_T), 아이디(Id_T)를 갱신한다. 태그의 키가 서버와 비동기화되고 아이디(ID)까지 비동기화되는 경우 전체 이전키(PK_T)를 대상으로 m_{Left} 연산을 수행하고, m_{Left} 이 일치하는 경우 아이디(Id_T)만을 갱신한다.
- [0021] 서버는 태그에게 m_{Right} 과 info정보를 전달하고, 태그는 m_{Right} 을 인증한 경우에만 비밀키(K_T)를 각각 $h(K_T || r_R)$ 로 갱신한다.
- [0022] 이와 같은 과정을 통해 위치추적 공격, 서비스 거부 공격 등에 안전하지만, 서버를 안전한 구간으로 정의함으로써 서버 위장 공격은 고려하지 않았다. 상기 제3 종래방법은 백엔드 서버와 리더 구간에서의 전송 과정을 고려한다면, 리더에서 서버로의 제1 랜덤수(r_R) 전송 1회를 포함하여 총 6회의 통신을 거치게 된다. 또한 인증을 위해 리더는 랜덤값 생성 1회만 수행하며, 태그는 1회의 랜덤값 생성과 3번의 해쉬 연산을 수행한다.
- [0023] 상기 제3 종래방법에서는 태그의 아이디 갱신을 위해 별도의 통신과정을 두지 않고, 쿼리 응답 후에 스스로 아이디를 갱신하도록 하고 있다. 공격자는 이점을 이용하여 태그에게 쿼리와 난수를 브로드캐스트함으로써 손쉽게 서버와 태그 사이에 아이디 비동기화를 발생시킬 수 있다. 아이디 비동기화가 발생하게 되면 서버는 DB에 있는 모든 태그를 대상으로 해쉬 연산을 수행해야만 하므로 동적 아이디를 이용한 태그 검색 효율성을 유지할 수 없게 된다. 다만, 아이디 비동기화는 1회에 한정되므로 시스템과의 통신이 정상적으로 완료되면 동기화가 맞춰진다.
- [0024] 다음으로, 동기화 카운터를 이용한 RFID 상호 인증 방법(이하 제4 종래방법)을 설명한다.
- [0025] 상기 제4 종래방법은 고정 아이디 기반 RFID 인증 방법으로 카운터를 이용하여 태그가 비동기화된 리더를 구분함으로써 태그의 인증 정보 노출을 방지하고 있다. 백엔드 서버와 리더 사이를 안전한 구간으로 가정하고 있으며, 백엔드 서버는 시스템에 대한 모든 공격을 탐지할 수 있다는 가정을 둔다.
- [0026] 백엔드 서버는 리더 아이디(Id_R), 태그 아이디(Id_T), 비밀키(K_T), 서버 카운터(c_B)를, 리더는 리더 아이디(Id_R), 태그 아이디(Id_T), 리더 카운터(c_B), 태그-리더간 공유키(K_{TR})를, 태그는 태그 아이디(Id_T), 비밀키(K_T), 태그 카운터(c_T)를 각각 저장하고 있다.
- [0027] 백엔드 서버는 $K_{TR}=E_{K_{TR}}(Id_R, c_R)$ 을 생성하고 리더에게 전달한다. 리더의 요청시 태그는 리더 아이디(Id_R), 리더 카운터(c_B), 제1 랜덤수(r_R)를 수신 받고, 암호화 통신을 위하여 $K_{TR}=E_{K_T}(Id_R, c_R)$ 을 생성하고 태그의 제1 랜덤수(r_T)을 암호화하여 $E_{K_T}(r_R, r_T)$ 전달한다. 이를 수신한 리더는 $E_{K_T}(r_R, r_T)$ 를 복호화 한 후 제1 랜덤수(r_R)를 확인함으로써 리더가 태그를 인증하고, 자신의 제1 랜덤수(r_R)를 태그로 재전송함으로써 태그가 리더를 인증한다.
- [0028] 공격 탐지시 백엔드 서버는 서버 카운터(c_B)를 증가시키고 정당한 리더들만 동기화시킨다. 태그는 평상시 사전에 백엔드 서버와 공유하고 있는 태그 카운터(c_T) 값을 유지하고 있다가 리더 요청시, 자신의 정보와 리더의 정보를 이용하여 해쉬 값을 생성하고, 생성된 해쉬 값이 백엔드 서버에서 인증되는 경우에만 정당한 리더로부터 전달받

은 카운터로 갱신하는 과정을 거친다. 이후 리더 아이디(Id_R)와 증가된 서버 카운터(c_B)를 태그의 키로 암호화함으로써 암호키를 갱신한다.

- [0029] 하지만, 각 태그와 리더 사이에 유일한 K_{TR} 을 소유하므로 통신에 대한 안전성을 높일 수 있는 반면, 리더가 모든 태그의 K_{TR} 을 저장해야 한다는 점과, 백엔드 서버가 모든 공격을 탐지할 수 있다는 강력한 가정을 만족해야만 프로토콜이 동작할 수 있다. 리더로 위장한 공격자가 충분히 높은 카운터를 생성하여 전송할 경우 태그 카운터 비동기화 공격이 가능하다. 이와 같은 공격에 의해 비동기화가 발생할 수 있지만 제안된 프로토콜은 재동기화 과정 및 카운터 초기화 방법을 제시하지 않고 있다.

발명의 내용

해결하려는 과제

- [0030] 본 발명의 목적은 상술한 바와 같은 문제점을 해결하기 위한 것으로, RFID 시스템의 모든 구간을 안전하지 않은 구간으로 고려하여 공격자가 백엔드 서버와 리더 그리고 태그로 위장 공격에 대처할 수 있는 랜덤 아이디 기반 RFID 상호 인증 방법을 제공하는 것이다.
- [0031] 즉, 본 발명의 목적은 RFID 시스템의 전 구간에서의 공격에 대처하고, 각 구간에서의 정보의 노출을 방지하고, 동적 아이디에 의한 비동기화 문제를 해결하고, 태그의 연산 능력을 고려하여 경량화되고, 서버에서 효율적인 태그 검색을 지원해야 하는 등의 요구사항을 만족하는 RFID 상호 인증 방법을 제공하는 것이다.
- [0032] 또한, 본 발명은 서버, 다수의 리더, 및 다수의 태그로 구성된 RFID 태그 시스템에서 동기화 카운터, 비밀키로 생성된 인증 메시지로 인증하고, 동적 아이디를 이용하되, 태그가 유동 아이디를 갱신 후 응답 메시지를 보내면 리더와 서버가 순차적으로 동적 아이디를 갱신하는 랜덤 아이디 기반 RFID 상호 인증 방법을 제공하는 것이다.

과제의 해결 수단

- [0033] 상기 목적을 달성하기 위해 본 발명은 서버, 다수의 리더, 및 다수의 태그로 구성된 RFID 태그 시스템에서 동기화 카운터를 이용하여 동기화된 상대와 인증을 처리하는 랜덤 아이디 기반 RFID 상호 인증 방법에 관한 것으로서, (a) 각 리더는 상기 리더의 카운터 및 동적 아이디를 저장하고, 각 태그는 상기 태그의 카운터 및 동적 아이디, 비밀키를 저장하고, 상기 서버는 서버의 카운터(이하 제3 카운터) 및, 모든 태그의 동적 아이디와 비밀키를 저장하는 단계; (b) 하나의 리더(이하 제1 리더)는 제1 랜덤수를 발생하고, 상기 제1 리더의 카운터(이하 제1 카운터)와 상기 제1 랜덤수를 쿼리와 함께 태그(이하 제2 태그)에 전송하는 단계; (c) 상기 제2 태그는 상기 제2 태그의 카운터(이하 제2 카운터)가 상기 제1 카운터와 정당한 상태이면, 제2 랜덤수를 발생하고, 상기 제2 태그의 비밀키(이하 제2 비밀키)를 이용하여 제1 인증 메시지를 생성하고, 상기 제2 카운터 및 제2 태그의 동적 아이디(이하 제2 동적 아이디), 상기 제1 인증 메시지, 제1 및 제2 랜덤수를 상기 제1 리더로 전송하는 단계; (d) 상기 제1 리더는 수신한 제1 랜덤수를 검증하고, 검증되면 상기 제1 리더의 동적 아이디(이하 제1 동적 아이디), 상기 제2 동적 아이디, 제1 및 제2 카운터, 상기 제1 및 제2 랜덤수를 상기 서버로 전송하는 단계; (e) 상기 서버는 상기 제2 동적 아이디에 대응되는 공유된 비밀키를 검색하고, 상기 제1 및 제2 카운터가 제3 카운터와 정당한 상태이면 공유된 비밀키를 이용하여 제2 인증 메시지를 생성하는 단계; (f) 상기 서버는 상기 제1 인증 메시지를 상기 제2 인증 메시지를 비교하여 검증하고, 검증되면 제1 및 제2 갱신 아이디를 생성하고, 상기 제2 태그에 대한 부가정보(info)를 상기 제2 인증 메시지, 상기 제1 및 제2 갱신 아이디, 제1 및 제2 카운터, 제1 및 제2 랜덤수와 함께 상기 제1 리더를 전송하는 단계; (g) 상기 제1 리더는 수신한 제1 카운터 및 제1 랜덤수로 검증하고, 검증되면 상기 서버로부터 수신한 제2 갱신 아이디 및 제2 인증 메시지, 제2 랜덤수, 제2 카운터를 상기 제2 태그로 전송하는 단계; (h) 상기 제2 태그는 수신한 제2 카운터 및 제2 랜덤수로 검증하고, 검증되면 상기 제2 인증 메시지를 상기 제1 인증 메시지와 비교하여 검증하고, 검증되면 상기 제2 비밀키를 상기 제2 인증 메시지를 이용하여 갱신하고, 상기 제2 동적 아이디를 상기 제2 갱신 아이디로 갱신하고, 상기 제2 카운터를 상기 제1 카운터로 갱신하는 단계; (i) 상기 제2 태그는 응답 메시지를 생성하여 상기 제1 리더로 전송하는 단계; (j) 상기 제1 리더는 상기 응답 메시지를 수신하여 검증하고, 검증되면 상기 제1 동적 아이디를 상기 제1 갱신 아이디로 갱신하고, 상기 응답 메시지를 상기 서버로 전송하는 단계; (k) 상기 서버는 상기 응답 메시지를 수신하여 검증하고, 검증되면 공유된 제1 및 제2 공유 아이디를 상기 제1 및 제2 갱신 아이디로 갱신

하고, 공유된 비밀키를 상기 제2 인증 메시지를 이용하여 갱신하는 단계를 포함하는 것을 특징으로 한다.

- [0034] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 서버와 태그는 상기 태그의 고정 아이디를 공유하고, 상기 제1 및 제2 인증 메시지는 태그의 고정 아이디 및 비밀키를 해쉬하여 생성되는 것을 특징으로 한다.
- [0035] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 제1 및 제2 인증 메시지는 제1 및 제2 카운터, 제1 및 제2 랜덤수를 더 포함하여 해쉬하는 것을 특징으로 한다.
- [0036] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 리더 또는 태그는 수신한 카운터 또는 랜덤수를 상기 리더 또는 태그가 저장하고 있는 카운터 또는 랜덤수를 비교하여 동일여부로 검증하는 것을 특징으로 한다.
- [0037] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 (c)단계에서, 상기 제2 태그는 상기 제1 인증 메시지의 제1 부분을 전송하고, 상기 (f)단계에서, 상기 서버는 상기 제2 인증 메시지의 제2 부분을 전송하되, 상기 제2 인증 메시지의 제2 부분은 상기 제1 인증 메시지의 제1 부분과는 메시지의 서로 다른 위치인 것을 특징으로 한다.
- [0038] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 제1 카운터의 값이 상기 제2 카운터 보다 같거나 클 때 동기화가 검증되거나, 상기 제3 카운터의 값이 상기 제2 카운터 보다 같거나 클 때 동기화가 검증되거나, 상기 제2 및 제3 카운터의 값이 동일할 때 동기화가 검증되는 것을 특징으로 한다.
- [0039] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 서버와 리더는 상기 리더의 고정 아이디를 공유하고, 상기 카운터를 암호화하여 전송하되, 상기 카운터에 상기 고정 아이디 및 카운터를 해쉬한 값을 XOR연산하여 암호화하고, 암호화된 카운터를 복호화하여 처리하되, 상기 암호화된 카운터에 상기 고정 아이디 및 카운터를 해쉬한 값을 XOR연산하여 복호화하는 것을 특징으로 한다.
- [0040] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 (f)단계에서, 상기 서버는 제3 랜덤수를 생성하고 공유된 제1 또는 제2 고정 아이디에 상기 제3 랜덤수를 연결하고 해쉬하여 상기 제1 또는 2 갱신 아이디를 생성하는 것을 특징으로 한다.
- [0041] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 서버와 리더는 공유키를 공유하여, 상기 공유키로 데이터를 암호화하여 전송하고 수신한 데이터를 복호화하는 것을 특징으로 한다.
- [0042] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 응답 메시지는 상기 제1 및 제2 랜덤수를 XOR 연산하여 생성되고, 상기 응답메시지에 제1 또는 제2 랜덤수를 XOR 연산하여 상기 제2 또는 제1 랜덤수를 추출하고, 추출된 제2 또는 제1 랜덤수를 저장된 제2 또는 제1 랜덤수와 비교하여 동일여부로 검증되는 것을 특징으로 한다.
- [0043] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 (g)단계 또는 상기 (h)단계는, 상기 제1 리더 또는 제2 태그는 수신한 랜덤수 및 카운터로 검증하되, 수신한 랜덤수 및 카운터와 저장된 랜덤수 및 카운터와 동일여부로 검증하는 것을 특징으로 한다.
- [0044] 또, 본 발명은 랜덤 아이디 기반 RFID 상호 인증 방법에 있어서, 상기 (a)단계에서, 상기 서버는 태그의 동적 아이디에 대응되는 태그의 고정 아이디 및 비밀키를 제1 테이블로 구성하고, 리더의 동적 아이디 및 태그의 동적 아이디에 대응되는 태그의 고정 아이디 및 비밀키를 제2 테이블로 구성하고, 상기 (e)단계는 상기 서버는 상기 제2 테이블을 검색하여 태그의 고정 아이디 및 비밀키를 검색하고, 상기 제2 테이블에서 검색결과가 없으면 상기 제1 테이블에서 검색하는 것을 특징으로 한다.

발명의 효과

- [0045] 상술한 바와 같이, 본 발명에 따른 랜덤 아이디 기반 RFID 상호 인증 방법에 의하면, 서버, 리더, 태그 사이의 상호인증을 지원하고, 재전송 공격 및 태그와 리더의 위장공격, 태그 위치추적공격, 서비스 거부 공격에 안전하고, 서버의 태그 탐색에 대한 서버 검색량을 개선하여 상호인증의 효율성을 높일 수 있는 효과가 얻어진다.

도면의 간단한 설명

- [0046] 도 1은 본 발명을 실시하기 위한 전체 RFID 시스템 구성의 일례를 도시한 도면이다.
 도 2는 본 발명의 일실시예에 따른 랜덤 아이디 기반 RFID 상호 인증 방법을 설명하는 흐름도이다.
 도 3은 본 발명의 일실시예에 따른 데이터베이스의 구조를 도시한 도면이다.
 도 4는 본 발명의 일실시예에 따른 공격 시나리오를 설명하는 흐름도이다.
 도 5는 본 발명의 일실시예에 따라 동기화 실패를 위한 재동기화 방법을 설명하는 흐름도이다.
 도 6은 본 발명과 종래 기술의 안정성 및 효율성을 대비한 표이다.

* 도면의 주요 부분에 대한 부호의 설명 *

- | | |
|-------------|-------------|
| 10 : 리더 | 20 : 태그 |
| 30 : 서버 | 40 : 데이터베이스 |
| 41 : 리더정보DB | 42 : 태그정보DB |
| 43 : 태그목록DB | |

발명을 실시하기 위한 구체적인 내용

- [0047] 이하, 본 발명의 실시를 위한 구체적인 내용을 도면에 따라서 설명한다.
- [0048] 또한, 본 발명을 설명하는데 있어서 동일 부분은 동일 부호를 붙이고, 그 반복 설명은 생략한다.
- [0049] 먼저, 본 발명을 실시하기 위한 전체 RFID 시스템 구성의 일례를 도 1을 참조하여 설명한다.
- [0050] 도 1에서 도시한 바와 같이, 본 발명을 실시하기 위한 RFID 시스템은 다수의 리더(10), 다수의 태그(20), 및 서버(30)로 구성된다. 또한, 추가적으로 데이터를 저장하기 위한 데이터베이스(40)를 추가적으로 구성한다.
- [0051] 태그(20)는 RFID태그 등 정보를 저장하는 소형 회로 장치로서 리더(10)로부터 무선신호(radio frequency)를 수신하면 저장된 데이터를 리더(10)로 송신하는 장치이다. 태그(20)는 회로에 의해 연산을 처리하거나 데이터를 저장하고 읽을 수 있다.
- [0052] 리더(10)는 무선신호를 브로드캐스팅하고 상기 무선신호에 반응하는 태그(20)로부터 신호를 수신한다. 이를 통해, 태그(20)에 저장된 데이터를 수신하거나 태그(20)가 일정한 작업(또는 연산)을 처리하게 하거나, 또 그 처리 결과를 수신한다. 리더(10)가 무선신호를 브로드캐스팅하면 무선신호를 받는 태그(20)들은 모두 상기 리더(10)의 무선신호에 반응한다.
- [0053] 서버(30)는 컴퓨팅 기능을 가진 통상의 서버로서, 상기 리더(10)와 데이터 통신을 하고, 상기 태그(20) 및 리더(10)에 관한 정보를 저장한다. 그래서 서버(30)는 리더(10)가 필요로 하는 태그(20)의 정보를 리더(10)에 전송한다.
- [0054] 즉, 리더(10)는 태그(20)에 관한 보다 상세한 정보를 얻기 위하여, 상기 태그(20)에 쿼리를 전송하여 태그(20)의 아이디(XId_T)를 수신하고, 수신한 태그(20)의 아이디(XId_T)를 서버(30)에 전송한다. 서버(30)는 수신한 아이디(XId_T)에 대한 태그 정보(info)를 검색하고 그 결과를 리더(10)에 전송한다. 최종적으로, 리더(10)는 서버(30)로부터 송신한 태그(20)에 관한 상세한 정보(info)를 수신할 수 있다.
- [0055] 한편, 서버(30)와 태그(20)는 상호 인증을 하기 위하여 비밀키(K_T)를 공유한다. 즉, 서버(30)는 진정한 태그(20)에 관한 태그 정보(info)를 원하는 것인지를 인증하고, 태그(20)는 진정한 서버(30)에 의한 태그 정보(info)인 것을 인증하기 위한 것이다. 구체적으로, 서버(30)와 태그(20)는 비밀키(K_T)를 이용하여 인증 메시지를 생성하여 서로 교환한다. 교환된 인증 메시지를 서로 비교하여 동일한지 여부로 상호 인증을 수행한다.
- [0056] 또한, 리더(10), 태그(20), 서버(30)는 모두 동기화 카운터(c_R, c_T, c_R)를 갖는다. 서버(30)는 공격이 탐지되면 자신의 카운터(c_R)를 증가시키고, 정당한 리더(10)들의 카운터(c_R)만 자신의 카운터(c_R)로 동기화시킨다. 이때,

태그의 카운터(c_T)는 동기화되지 않는다. 대신, 리더(10)에 의해 태그(10)에 관한 태그 정보(info)가 요청될 때, 태그의 카운터(c_T)를 동기화 시킨다.

[0057] 따라서 서버(30)와 리더(10)는 항상 서로의 카운터(c_R , c_R)가 동일한 값을 가지는 경우(즉, 동기화된 상태인 경우)에만 정당한 상태이다. 그러나 리더(10)와 태그(20), 또는 서버(30)와 태그(20)는 리더(10) 또는 서버(30)의 카운터(c_R , c_R)가 태그의 카운터(c_T) 보다 같거나 큰 경우에도 정당한 상태이다.

[0058] 또한, 리더(10) 및 태그(20)는 고정 아이디(Id_R , Id_T) 및 동적 아이디(XId_R , XId_T)를 모두 저장하여 갖는다. 그러나 상대방에게 전송되는 아이디는 동적 아이디(XId_R , XId_T)만이다. 즉, 태그(20)가 리더(10)의 쿼리 요청에 응답하여 태그의 동적 아이디(XId_T)를 전송하고, 그 태그의 동적 아이디(XId_T)가 서버(30)까지 전달된다. 또, 리더(10)가 서버(30)에 태그의 아이디를 전송하면서 자신의 식별정보로서 자신의 동적 아이디(XId_R)를 함께 전송한다.

[0059] 고정 아이디(Id_R , Id_T)는 전송되지 않고, 서버(30)에도 사전에 저장된다. 그리고 리더(10) 및 태그(20)는 자신들의 고정 아이디(Id_R , Id_T)로 자신들의 카운터(c_R , c_T)를 암호화하면, 서버(30)는 저장하고 있던 리더(10) 및 태그(20)의 고정 아이디(Id_R , Id_T)로 카운터(c_R , c_T)를 복호화한다. 유사한 방식으로 인증 메시지를 생성할 때도 이용된다. 또한, 고정 아이디(Id_R , Id_T)는 동적 아이디(XId_R , XId_T)를 갱신할 때도 이용된다.

[0060] 한편, 리더(10)와 서버(30) 사이에는 암호화 통신을 하는 것이 바람직하다. 이를 위해, 리더(10)와 서버(30)는 암호화 통신을 위한 공유키(K_{RR})를 서로 공유하고, 상기 공유키(K_{RR})로 전송하고자 하는 데이터를 암호화하여 전송한다.

[0061] 또한, 리더(10), 또는 태그(20), 서버(30)가 상대방에게 데이터를 송신하고 그 응답으로서 상대방으로부터 데이터를 수신하는 경우, 자신이 수신한 데이터가 "자신이 데이터를 보내고자 한 진정한 상대"로부터 오는 데이터인지를 검증한다. 이때, 이를 검증하기 위하여 랜덤수(r_B , r_R , r_T)를 사용한다. 따라서 랜덤수(r_B , r_R , r_T)는 상호 인증을 할 때마다 새로 생성하고, 랜덤한 방식으로 생성된 임의의 수를 이용한다. 서버(30)의 랜덤수(r_B)는 동적 아이디(XId_R , XId_T)를 갱신할 때 갱신 변수로 활용된다.

[0062] 데이터베이스(40)는 서버(30)가 필요로 하는 데이터를 저장하기 저장소로서, 리더(10)의 동적 아이디(XId_R), 고정 아이디(Id_R), 공유키(K_{RR}) 등을 저장하기 위한 리더정보DB(41), 태그(20)의 동적 아이디(XId_T), 고정 아이디(Id_T), 비밀키(K_T) 등을 저장하기 위한 태그정보DB(42), 리더(10)에 의해 태그(20)가 읽혀졌을 때 리더(10)와 태그(20)의 쌍을 기록한 태그목록DB(43) 등으로 이루어진다. 그러나 상기 데이터베이스(40)의 구성은 바람직한 일 실시예일 뿐이며, 구체적인 장치를 개발하는데 있어서, 접근 및 검색의 용이성 및 효율성 등을 감안하여 데이터베이스 구축이론에 의하여 다른 구조로 구성될 수 있다.

[0063] 다음으로, 본 발명의 일 실시예에 따른 랜덤 아이디 기반 RFID 상호 인증 방법을 도 2를 참조하여 설명한다. 도 2는 본 발명의 일 실시예에 따른 랜덤 아이디 기반 RFID 상호 인증 방법을 설명하는 흐름도이다.

[0064] 도 2에서 보는 바와 같이, 본 발명의 일 실시예에 따른 센서 네트워크 인증방법은 (a) 각 리더 및 태그는 각자 카운터 및 동적 아이디를 저장하고, 서버는 서버의 카운터(이하 제3 카운터)를 저장하고, 서버와 태그는 비밀키를 공유하는 단계(S10); (b) 제1 리더는 자신 카운터(이하 제1 카운터)를 제2 태그에 전송하는 단계(S20); (c) 제2 태그는 자신 카운터(이하 제2 카운터)와 제1 카운터가 정당한 상태이면, 비밀키를 이용하여 제1 인증 메시지를 생성하여 제2 카운터 및 자신 동적 아이디(이하 제2 동적 아이디)와 함께 제1 리더로 전송하는 단계(S30); (d) 제1 리더는 자신 동적 아이디(이하 제1 동적 아이디) 및 제2 동적 아이디를 제1 및 제2 카운터와 함께 서버로 전송하는 단계(S40); (e) 서버는 제1 및 제2 카운터가 제3 카운터와 정당한 상태이면 공유된 비밀키를 이용하여 제2 인증 메시지를 생성하는 단계(S50); (f) 서버는 제1 인증 메시지를 제2 인증 메시지를 비교하여 검증하고, 제1 및 제2 갱신 아이디를 생성하여 제2 인증 메시지와 함께 제1 리더를 전송하는 단계(S60); (g) 제1 리더는 서버로부터 수신한 제2 갱신 아이디 및 제2 인증 메시지를 제2 태그로 전송하는 단계(S70); (h) 제2 태그는 제2 인증 메시지를 제1 인증 메시지와 비교하여 검증하고, 제2 비밀키를 갱신하고, 제2 동적 아이디를 제2

갱신 아이디로 갱신하고, 제2 카운터를 제1 카운터로 갱신하는 단계(S80); (i) 제2 태그는 응답 메시지를 생성하여 제1 리더 및 서버로 전송하면, 제1 리더 및 서버는 아이디 등을 갱신하는 단계(S90)로 구성된다.

- [0065] 각 단계를 구체적으로 설명한다.
- [0066] 먼저, 서버(30) 및, 각 리더(10) 및 태그(20)는 필요한 데이터를 사전에 등록한다. 즉, 각 리더(10)는 상기 리더(10)의 카운터(c_R) 및 동적 아이디(XId_R)를 저장하고, 각 태그(20)는 상기 태그의 카운터(c_T) 및 동적 아이디(XId_T), 비밀키(K_T)를 저장하고, 상기 서버(30)는 서버의 카운터(이하 제3 카운터)(c_B) 및, 모든 태그의 동적 아이디(XId_T)와 비밀키(K_T)를 저장한다(S10). 또한, 리더(10) 및 태그(20)는 자신의 고정 아이디(Id_R , Id_T)를 저장하고, 서버(30)도 이들 고정 아이디(Id_R , Id_T)를 공유하여 저장하는 것이 바람직하다.
- [0067] 사전 등록 단계는 사용하지 않았던 리더(10)나 태그(20)를 제안하는 RFID 시스템에서 사용하기 위해 반드시 거쳐야하는 준비과정이며, 오프라인에서 별도의 인증 및 등록 과정을 거친다. 새로운 리더와 태그는 다음과 같은 정보를 백엔드 서버(30)로부터 전달받거나 서버(30)에 저장하게 된다.
- [0068] 사전 등록 단계에서 리더(10)는 백엔드 서버(30)로부터 동적 아이디(XId_R), 카운터(c_R), 공유키(K_{BR})를 오프라인을 통해서 발급받고, 백엔드 서버(30)에 리더의 동적 아이디(XId_R), 고정 아이디(Id_R), 패스워드(ps_Id_R), 공유키(K_{BR})를 저장한다. 패스워드는 비동기화시 복구를 위한 인증 수단으로 리더 동기화 단계에서 사용된다.
- [0069] 또, 사전 등록 단계에서 태그(20)는 백엔드 서버(30)로부터 동적 아이디(XId_T), 카운터(c_T), 비밀키(K_T)를 오프라인을 통해 발급받고, 백엔드 서버에 동적 아이디(XId_T), 고정 아이디(Id_T), 비밀키(K_T), 및 태그의 부가정보(info)를 저장한다.
- [0070] 다음으로, 하나의 리더(이하 제1 리더)(10)는 제1 랜덤수(r_R)를 발생하고(S21), 상기 제1 리더의 카운터(이하 제1 카운터)(c_R)와 상기 제1 랜덤수(r_R)를 쿼리(Query)와 함께 태그(이하 제2 태그)(20)에 전송한다(S22). 다수의 리더 및 다수의 태그 중에서 특정 리더 및 특정 태그를 지칭하기 위해, "제1 리더" 및 "제2 태그"라는 용어를 사용한다.
- [0071] 다음으로, 제2 태그(20)는 자신의 카운터(이하 제2 카운터)(c_T)가 제1 카운터(c_R)와 정당한 상태이면, 제2 랜덤수(r_T)를 발생하고, 제2 태그의 비밀키(이하 제2 비밀키)(K_T)를 이용하여 제1 인증 메시지(m)를 생성한다(S31).
- [0072] 즉, 제2 태그(20)는 자신이 가지고 있는 제2 카운터(c_T)와 제1 리더(10)로부터 수신한 제1 카운터(c_R)의 크기를 비교한다. 제1 카운터(c_R)가 제2 카운터(c_T) 보다 작은 경우 통신을 중단한다. 제1 카운터(c_R)가 제2 카운터(c_T)와 같거나 큰 경우에만 다음 과정을 거친다. 태그(20)는 제2 랜덤수(r_T)를 생성하고 리더(10)로부터 수신한 정보(c_R , r_R)와 자신의 정보(Id_T , K_T , r_T , c_T)를 이용해 인증 메시지(m)을 생성한다. 카운터 정보를 숨기기 위해 태그의 고정 아이디(또는 제2 고정 아이디)(Id_T)와 제2 랜덤수(r_T)를 해쉬하고 이 값을 제2 카운터(c_T)와 XOR 연산하여 암호화된 제2 카운터(Xc_T)를 생성한다.
- [0073] 그리고 제2 태그(20)는 제2 카운터(c_T) 및 제2 태그의 동적 아이디(이하 제2 동적 아이디)(XId_T), 제1 인증 메시지(m), 제1 및 제2 랜덤수(r_R , r_T)를 제1 리더(10)로 전송한다(S32). 이때 바람직하게는 제2 카운터(c_T)는 암호화된 제2 카운터(Xc_T)를 보낸다. 또한, 제1 인증 메시지(m)에서 왼쪽 반(m_{left})만 전송하는 것이 바람직하다.
- [0074] 다음으로, 제1 리더(10)는 수신한 제1 랜덤수(r_R)를 검증한다(S41). 즉, 제1 리더(10)는 제2 태그(20)로부터 수신한 인증 정보의 일치여부를 확인하기 위해서 제1 랜덤수(r_R) 값을 확인한다. 그리고 이 값이 동일한 경우에 검증된 것으로 판단된다.
- [0075] 제1 리더(10)는 검증되면 제1 태그의 동적 아이디(이하 제1 동적 아이디)(XId_R), 제2 동적 아이디(XId_T), 제1 및 제2 카운터(c_R , c_T), 제1 및 제2 랜덤수(r_R , r_T)를 서버(10)로 전송한다(S42). 바람직하게는, 제1 카운터(c

r_r)를 암호화하여 암호화된 제2 카운터(X_{c_T})를 생성한다.

- [0076] 그리고 제1 리더(10)는 인증정보 보호를 위해 자신의 정보와 태그의 정보를 공유키(K_{BR})로 암호화하고, 리더와 태그를 구분할 수 있는 제1 및 제2 동적 아이디(XID_R , XID_T)를 함께 전달한다.
- [0077] 다음으로, 서버(30)는 수신한 제2 동적 아이디(XID_T)에 대응되는 공유된 비밀키(K_T)를 검색하고, 제1 및 제2 카운터(c_R , c_T)가 제3 카운터(c_B)와 정당한 상태이면 공유된 비밀키(K_T)를 이용하여 제2 인증 메시지(m')를 생성한다(S50).
- [0078] 구체적으로, 백엔드 서버(30)는 복호화를 위해 제1 리더(10)로부터 수신한 제1 동적 아이디(XID_R)를 이용하여 공유키(K_{BR})를 서버(30)(또는 데이터베이스 40)에서 검색한다. 백엔드 서버(30)에 공유키(K_{BR})이 없는 경우 통신을 종료한다.
- [0079] 메시지를 복호화한 후 제1 동적 아이디(XID_R)를 가지고 있는 태그목록(또는 태그 리스트)(43)에서 제2 동적 아이디(XID_T)를 검색하고, 제2 동적 아이디(XID_T)를 식별자로 하여 태그의 정보를 참조한다. 색인된 데이터를 이용하여 암호화된 제1 및 제2 카운터(X_{c_R} , X_{c_T})로부터 복호화된 제1 및 제2 카운터(c_R , c_T)를 계산한다. 이 값은 백엔드 서버(30)가 동기화 검사를 하는데 이용한다.
- [0080] 동기화가 맞는 경우에만 인증 메시지(m_{Left})의 검증 과정을 거치게 된다.
- [0081] 즉, 서버(30)는 제1 인증 메시지(m_{Left})를 제2 인증 메시지(m'_{Left})를 비교하여 검증하고, 검증되면 제1 및 제2 갱신 아이디(XID_R' , XID_T')를 생성한다(S61).
- [0082] 동기화 및 해쉬 값 검증 과정에서 불일치하는 정보가 있다면 현재 통신을 종료하고 공격 시나리오를 따라 인증 정보 갱신 과정이 이루어지게 된다. 동기화 및 해쉬 값 검증이 완료된 경우, 백엔드 서버(30)는 제3 랜덤수(c_B)를 생성하고 제1 및 제2 동적 아이디(XID_R , XID_T)의 갱신 과정을 거친다.
- [0083] 서버(30)는 검증되면 제1 및 제2 갱신 아이디(XID_R' , XID_T')를 생성하고(S61), 제2 태그(20)에 대한 부가정보(info)를 제2 인증 메시지(m'_{Right}), 제1 및 제2 갱신 아이디(XID_R' , XID_T'), 제1 및 제2 카운터(c_R , c_T), 제1 및 제2 랜덤수(r_R , r_T)와 함께 제1 리더(10)에 전송한다(S62).
- [0084] 즉, 서버(30)는 제1 리더(20)가 자신을 인증할 수 있도록 공유키(K_{BR})를 이용하여 제1 랜덤수(r_R), 제1 카운터(c_R), 제1 동적 아이디(XID_R), 태그의 부가정보(info)로 구성된 제1 데이터(D1)를 암호화하여 전달하고, 태그가 자신을 인증할 수 있도록 제2 인증 메시지(m_{Right}')를 이용하여 제2 랜덤수(r_T), 제2 카운터(c_T), 제2 동적 아이디(XID_T), 제2 인증 메시지(m_{Right}')로 구성된 제2 데이터(D2)를 암호화하여 전달한다.
- [0085] 이때, 제1 인증 메시지(m)는 왼쪽 반(m_{Left})을 전송하는 반면, 제2 인증 메시지(m)는 오른쪽 반(m_{Right}')을 전송한다.
- [0086] 다음으로, 제1 리더(10)는 수신한 제1 카운터(c_T) 및 제1 랜덤수(r_R)로 검증하고(S71), 검증되면 서버(10)로부터 수신한 제2 갱신 아이디(XID_T') 및 제2 인증 메시지(m_{Right}'), 제2 랜덤수(r_R), 제2 카운터(c_T)를 제2 태그(20)로 전송한다(S72).
- [0087] 즉, 제1 리더(10)는 전달받은 메시지(D1)를 복호하고, 제1 카운터(c_T) 및 제1 랜덤수(r_R)가 검증된 경우에만 제2 데이터(D2)를 제2 태그(20)에게 전달한다.
- [0088] 제2 태그(20)는 수신한 제2 카운터(c_T) 및 제2 랜덤수(r_R)로 검증하고, 검증되면 제2 인증 메시지(m_{Right}')를 제1 인증 메시지(m_{Right})와 비교하여 검증하고, 검증되면 제2 비밀키(K_T)를 제2 인증 메시지(m_{Right})(또는 제1 인증 메시지의 오른쪽 부분)를 이용하여 갱신하고, 제2 동적 아이디(XID_T)를 상기 제2 갱신 아이디(XID_T')로 갱신하고, 제2 카운터(c_T)를 제1 카운터(c_R)로 갱신한다(S80).

- [0089] 즉, 제2 태그(20)는 제1 리더(10)로부터 전달받은 제2 데이터(D2)를 복호하고, 제2 카운터(c_T), 제2 랜덤수(r_R), 제2 인증 메시지(m_{Right})가 검증된 경우에만 비밀키(K_T), 제2 동적 아이디(XID_T), 제2 카운터(c_T)를 갱신한다. (단, 제2 데이터(D2)의 제2 카운터(c_T) 값이 0으로 전달된 경우 백엔드 서버가 카운터를 초기화한 것이므로, 제2 카운터(c_T)를 제1 카운터(c_R)로 갱신하지 않고 0으로 초기화한다.)
- [0090] 다음으로, 제2 태그(20)는 응답 메시지(UPDCPL)를 생성하여(S91) 제1 리더(10)로 전송한다(S92). 이때, 응답 메시지(UPDCPL)는 제1 및 제2 랜덤수(r_R , r_T)를 XOR 연산하여 얻는다.
- [0091] 제1 리더(10)는 응답 메시지(UPDCPL)를 수신하여 검증하고, 검증되면 상기 제1 동적 아이디(XID_R)를 제1 갱신 아이디(XID_R')로 갱신하고(S93), 응답 메시지(UPDCPL)를 서버(30)로 전송한다(S94).
- [0092] 즉, 제1 리더(10)는 수신한 응답 메시지(UPDCPL)와 자신의 랜덤수(r_R)의 XOR 연산 결과가 제2 랜덤수(r_T)가 되는지 검증한다. 검증된 경우에만, 수신한 응답 메시지(UPDCPL)를 서버(10)에 전달하고, 제1 동적 아이디(XID_R)를 갱신한다.
- [0093] 다음으로, 서버(30)는 응답 메시지(UPDCPL)를 수신하여 검증하고, 검증되면 공유된 제1 및 제2 공유 아이디(XID_R , XID_T)를 상기 제1 및 제2 갱신 아이디(XID_R' , XID_T')로 갱신하고, 공유된 비밀키(K_T)를 제2 인증 메시지(m_{Right})를 이용하여 갱신한다(S94).
- [0094] 즉, 백엔드 서버(30)는 암호화된 제1 및 제2 카운터(Xc_R , Xc_T)로부터 계산한 제1 및 제2 카운터(c_R , c_T)를 이용해 응답 메시지(UPDCPL)를 검증한다. 응답 메시지(UPDCPL)가 일정 기간 동안 도착하지 않을 경우, 사전에 설정된 횟수 동안 제1 및 제2 데이터(D1, D2)의 전달 과정을 반복한다.
- [0095] 다음으로, 본 발명의 일실시예에 따른 데이터베이스(40)의 구조를 도 3을 참조하여 설명한다.
- [0096] 도 3에서 보는 바와 같이, 본 발명의 일실시예에 따른 데이터베이스(40)는 리더(10)에 대한 정보를 저장하는 리더정보DB(41), 태그(20)에 대한 정보를 저장하는 태그정보DB(42), 리더(10)에 의해 태그(20)가 읽혀졌을 때 리더(10)와 태그(20)의 쌍을 기록한 태그목록DB(43)로 구성된다.
- [0097] 종래의 인증방법들은 태그로부터 전달된 해쉬 값을 인증하기 위해서 최악의 경우 태그의 수만큼 해쉬 연산을 거쳐야한다. 그러나 본 발명은 RFID 시스템에서 효율적인 태그 검색을 위해서 데이터베이스(40)의 구성을 이용한다.
- [0098] 일반적으로 일회용 태그의 경우라도 등록 후에 사용을 해야 하기 때문에, 최소 2번은 동일한 리더에 의해 읽혀질 가능성이 높다. 반복적으로 사용되는 태그가 동일한 리더에 의해 읽혀질 확률은 일회용 태그의 경우보다 더 높다고 볼 수 있다. 따라서 본 발명에 따른 데이터베이스(40)를 이용한 검색방법은 RFID 시스템의 리더와 태그에 랜덤한 식별자를 할당함으로써 태그 검색 효율을 높이하고자 한다.
- [0099] 백엔드 서버(30)는 리더의 동적 아이디(XID_R)를 식별자로 공유키(K_{RR})를 검색하고, 검색된 키를 이용하여 리더(10)로부터 수신한 메시지를 복호화 한다. 이후 동적 아이디(XID_R)를 식별자로 태그목록DB(43)(또는 태그 리스트 테이블)의 태그 리스트 테이블에서 태그의 동적 아이디(XID_T)를 검색하여 검색률을 높인다. 리더의 동적 아이디(XID_R)를 식별자로 태그의 동적 아이디(XID_T)를 찾지 못한 경우에만 태그정보DB(42)(또는 태그 정보 테이블)에서 다른 동적 아이디(XID_T)를 검색한다.
- [0100] 이와 같은 방식을 통해 해쉬 값을 알아내기 위해 전체 태그의 아이디(ID) 및 비밀키(K_T) 쌍을 이용하여 전체 태그를 대상으로 해쉬 연산을 수행하는 오버헤드를 줄일 수 있다.
- [0101] 정당한 리더(10)는 자신이 인증했던 정보를 저장하는 태그목록DB(43)만을 우선적으로 검색하여 태그(20)의 정보를 참조할 수 있다. 정당한 리더(10)는 랜덤 식별자인 리더의 동적 아이디(XID_R)와 자신이 가지고 있는 공유키(K_{RR})의 신선성을 보장할 수 있어야 한다. 신선성이 보장되지 않는 리더(10)의 경우는 백엔드 서버(30)로부터 인증을 받을 수가 없다. 만일, 백엔드 서버(30)가 인증 과정에서 리더의 인증 정보가 위조된 사실을 알아낼 경우,

리더정보DB(41)(또는 리더 정보 테이블)의 리더 비활성화 비트를 1로 설정한다. 만일 리더 비활성화 비트가 1로 설정된 리더가 인증 요청을 시도하는 경우, 리더 동기화 단계를 거쳐 인증 정보를 갱신해야만 현재 세션에서 통신이 가능해진다.

- [0102] 다음으로, 본 발명의 일실시예에 따른 공격 시나리오를 도 4를 참조하여 설명한다.
- [0103] 공격자가 암호화된 데이터를 습득하여 내부 데이터를 위변조할 수 있는 능력을 가졌다고 가정한다. 이런 가정은 공격을 더욱 수월하게 하며 공격자에게 유리한 환경을 제공할 수 있다. 도청공격, 위변조 공격, 서비스 거부 공격, 위치추적 공격 등의 위협에 대한 공격 시나리오를 살펴보고, 공격자가 각 개체로 위장하여 RFID 시스템의 인증을 우회하는 공격의 시나리오를 제시한다. 또한, 시나리오별 분석을 통하여 본 발명의 인증방법이 각 개체의 위장공격에 안전함을 증명한다.(단 위장 공격에서 물리적 공격은 고려하지 않는다.)
- [0104] 먼저, 시나리오 1에 의한 태그 위장 공격 시나리오를 도 4a를 참조하여 구체적으로 설명한다.
- [0105] 공격자는 자신이 가지고 있는 태그의 인증 정보를 인가된 태그의 인증 정보로 위변조하여 리더에게 전달하여 할 수 있다. 태그 위장 시나리오의 경우, 공격자는 노출되지 않는 Id_T 와 K_T , C_T 에 대한 정보를 알 수 없으며, 이전 세션에서 사용되었던 XId_T 와 Xc_T 는 도청을 통해서 수집할 수 있다.
- [0106] 태그 위장 시나리오의 경우, 공격자는 노출되지 않는 Id_T , K_T , C_T 에 대한 정보를 알 수 없으며, 이전 세션에서 사용되었던 XId_T 와 Xc_T 는 도청을 통해서 수집할 수 있다. 하지만, 현재 세션에서 이용될 XId_T 는 암호화되어 전송되므로 획득할 수 없다.
- [0107] 도 4a에서 보는 바와 같이, 태그 위장 공격 시나리오는 다음과 같다.
- [0108] 단계 ①?② : 정당한 리더가 태그로 정보를 요청한다.
- [0109] 단계 ③?④ : 태그는 리더의 응답에 $_XId_T$, $_m_{Left}$, $_r_R$, r_R , $_Xc_T$ 를 회신한다. 여기서 Id_T , K_T , C_T 값을 알 수 없으므로, 정확한 m_{Left} , Xc_T 및 XId_T 를 생성할 수 없다.
- [0110] 단계 ⑤?⑥ : 리더는 태그로부터 수신한 정보와 자신의 정보를 이용하여 백엔드 서버에 인증 정보를 전달한다.
- [0111] 단계 ⑦?⑨ : 리더로부터 인증 정보를 수신한 백엔드 서버는 암호화된 메시지를 복호한 후, c_T , c_R , m_{Left} 검증 단계를 진행한다. Id_T 와 K_T 를 모르는 태그는 올바른 c_T 와 m_{Left} 을 생성할 수 없으므로 태그 정보가 위조되었음을 확인할 수 있다. 이런 경우, 백엔드 서버는 통신을 종료한다.
- [0112] 다음으로, 시나리오 2에 의한 리더 위장 공격 시나리오를 도 4b를 참조하여 구체적으로 설명한다.
- [0113] 공격자는 인가된 태그의 정보를 수집하기 위하여 정상적인 리더로 위장 공격을 시도할 수 있다. 리더 위장 시나리오의 경우, 공격자는 노출되지 않은 Id_R 과 K_{RR} 에 대한 정보를 알 수 없으며, 이전 세션에 이용되었던 XId_R 과 c_R 은 도청을 통해서 수집할 수 있다. 하지만, 현재 세션에 이용될 XId_R 은 암호화되어 전송되므로 획득할 수 없다.(하지만, 본 시나리오에서는 공격자가 XId_R 과 K_{RR} 쌍을 알고 있다고 가정한다.)
- [0114] 리더 위장 시나리오의 경우, 공격자는 노출되지 않은 Id_R 과 K_{RR} 에 대한 정보를 알 수 없으며, 이전 세션에 이용되었던 XId_R 과 c_R 은 도청을 통해서 수집할 수 있다. 하지만, 현재 세션에 이용될 XId_R 은 암호화되어 전송되므로 획득할 수 없다. 하지만, 본 시나리오에서는 공격자가 XId_R 과 K_{RR} 쌍을 알고 있다고 가정함으로써 위조된 정보가 정상적으로 백엔드 서버로 전달되더라도 리더 공격을 탐지할 수 있음을 보인다.
- [0115] 도 4b에서 보는 바와 같이, 리더 위장 공격 시나리오는 다음과 같다.
- [0116] 단계 ①?② : 공격자는 태그에게 위조된 쿼리, $_c_R$, $_r_R$ 을 전달한다.

- [0117] 단계 ③?④ : 태그는 리더로부터 전달받은 정보를 이용하여 인증정보 m_{Left} , Xc_T 를 생성하고, XId_T , r_T , $_r_R$ 와 함께 리더에게 전달한다.
- [0118] 단계 ⑤?⑥ : 공격자는 태그로부터 수신한 정보와 자신이 위조한 정보를 조합하여 생성한 인증 정보를 백엔드 서버로 전달한다.
- [0119] 단계 ⑦?⑩ : 리더로부터 인증 정보를 수신한 백엔드 서버는 XId_R 을 이용하여 K_{BR} 을 검색한다. 정상적인 인증과정에서는 공격자가 K_{BR} 을 알고 있다 하더라도 대응되는 XId_R 을 알지 못하면 백엔드 서버 측의 인증절차를 수행할 수 없다. (본 시나리오에서는 공격자가 XId_R 과 K_{BR} 쌍을 알고 있다고 가정함으로 다음 단계를 수행한다.)
- [0120] 백엔드 서버는 XId_T 를 인덱스로 검색함으로써 Id_T 와 K_T 값을 알 수 있으며, 이 값을 기반으로 c_T , $_c_R$, $_m_{Left}$ 의 값을 검증한다. 공격자는 Id_T 를 알 수 없으므로 정상적인 c_R 과 m_{Left} 를 생성할 수 없고, 백엔드 서버에서는 정보의 위조 여부를 확인할 수 있다. 정보가 위조된 경우, $_XId_R$ 과의 통신을 종료하고 $_XId_R$ 의 비활성화 비트를 1로 설정한다. (만약, 공격자에 의해서 $_XId_R$ 값을 갖는 정당한 리더가 비활성화 되었다면 "리더 동기화 과정"을 통해서 다시 세션을 동기화할 수 있다.) 이와 동시에 백엔드 서버는 c_B 를 증가시키고, Id_R 을 제외한 모든 리더들의 XId_R 과 K_{BR} 을 갱신한다. 새로운 XId_R 은 각 리더의 Id_R 과 백엔드 서버에서 생성한 r_B 의 해쉬 연산에 의해 생성되고, K_{BR} 은 기존 K_{BR} 에 위에서 생성한 정당한 m_{Right} 의 해쉬 연산에 의해 생성된다. 정당한 리더들의 업데이트를 위해 전달되는 DATA는 메시지 구분을 위한 식별자 XId_R 과 암호화된 부분으로 구성된다.
- [0121] 단계 ⑫?⑬ : 자신의 식별자 XId_R 과 함께 전달된 메시지를 복호한 정당한 리더들은 메시지에서 XId_R 과 Pc_R 값이 자신의 XId_R 및 c_R 값과 동일한지 검증한다. 검증된 경우에만 c_R 과 K_{BR} 을 갱신한다. UPDCPL 메시지를 생성하기 위해 $C_B = C_B + 1$ 과 XId_R 값을 XOR 연산한 이후에, DATA전송시 노출되었던 XId_R 값을 새로이 갱신한다. 마지막으로 생성된 UPDCPL을 백엔드 서버로 전달한다.
- [0122] 단계 ⑭ : 리더의 업데이트를 확인하는 단계로, 백엔드 서버는 전송된 UPDCPL에 갱신된 카운터 c_B 를 XOR 연산함으로써 어떤 리더가 데이터 업데이트를 마쳤는지 확인할 수 있다. 확인된 리더가 다음 세션에 사용할 XId_R 을 갱신함으로써 리더와 랜덤 ID의 동기화를 맞춘다. UPDCPL이 일정 기간 동안 도착하지 않을 경우, 사전에 설정된 횟수 동안 DATA 전달 과정을 반복한다.
- [0123] 다음으로, 시나리오 3에 의한 서버 위장 공격 시나리오를 도 4c를 참조하여 구체적으로 설명한다.
- [0124] 공격자는 보다 많은 정보를 수집하거나, 서비스 거부 공격을 목적으로 합법적인 백엔드 서버로 위장 공격을 시도할 수 있다. 백엔드 서버 위장 시나리오의 경우, 공격자는 노출되지 않은 Id_R , K_{BR} , ps_Id_R , Id_T , K_T , $info$ 의 정보를 알 수 없으며, 이전 세션에서 사용되었던 XId_R , XId_T , Pc_R 은 도청을 통해 수집할 수 있다. 현재 세션에서 이용될 XId_R , XId_T 는 암호화되어 전송되므로 획득할 수 없다. (하지만, 본 시나리오에서는 공격자가 XId_R 과 K_{BR} 쌍을 알고 있다고 가정한다.)
- [0125] 백엔드 서버 위장 시나리오의 경우, 공격자는 노출되지 않은 Id_R , K_{BR} , ps_Id_R , Id_T , K_T , $info$ 의 정보를 알 수 없으며, 이전 세션에서 사용되었던 XId_R , XId_T , Pc_R 은 도청을 통해 수집할 수 있다. 현재 세션에서 이용될 XId_R , XId_T 는 암호화되어 전송되므로 획득할 수 없다. 하지만, 본 시나리오에서는 공격자가 XId_R 과 K_{BR} 쌍을 알고 있다고 가정함으로써 정당한 인증 정보가 백엔드 서버로 전달되더라도 백엔드 서버 위장 공격을 리더가 탐지할 수 있음을 보인다.
- [0126] 도 4c에서 보는 바와 같이, 서버 위장 공격 시나리오는 다음과 같다.
- [0127] 단계 ①~⑥ : 정당한 리더와 태그 사이의 메시지 전송 과정을 보여준다. 리더는 태그로부터 수신한 인증 정보를 이용하여 새로운 인증 정보를 생성하고 이를 백엔드 서버로 전달한다.
- [0128] 단계 ⑦~⑨ : 공격자는 자신이 정당한 백엔드 서버인 것처럼 데이터를 변조하고 이를 리더에게 전달한다. 이 과

정에서 Id_R , Id_T , K_T 를 모르는 공격자는 정확한 c_T , c_R , m_{Right} 을 생성할 수 없다. 하지만, 공격자는 자신이 알고 있는 K_{BR} 을 이용하여 거짓 정보를 리더에게 전달할 수 있다.

[0129] 단계 ⑩~⑪ : 리더는 수신한 데이터를 복호하고 r_R 과 c_R 을 검증한다. Id_R 을 모르는 공격자는 정확한 c_R 을 생성할 수 없다. 하지만, 도청을 통해 c_R 값을 습득할 수 있으므로, 태그로 DATA'를 송신할 가능성이 있다.

[0130] 단계 ⑫ : 태그는 수신한 데이터(DATA')를 복호하고, r_T , c_T , m_{Right} 을 검증한다. 공격자가 c_T 와 m_{Right} 을 생성할 수 없으므로 태그는 통신을 중단한다. 이와 같은 방법으로 거짓 정보를 전송하려는 백엔드 서버 위장 공격을 방지할 수 있다.

[0131] 다음으로, 본 발명의 일실시에 따라 동기화 실패를 위한 재동기화 방법을 도 5를 참조하여 설명한다.

[0132] 무선 리더의 경우 이동시 전파 송수신 상태가 원활하지 않거나, 리더가 오프라인 상태인 경우 백엔드 서버와 통신이 두절될 수 있다. 통신이 두절된 동안 공격이 발생하지 않아 c_B 값이 증가하지 않은 경우라면 K_{BR} 이 갱신되지 않으므로, 통신이 재개되거나 리더가 오프라인 상태가 되면 추가적인 정보의 갱신 없이 통신이 가능하다. 반면, 통신이 두절된 동안 공격이 발생하여 c_B 값이 갱신된 경우에는 c_R 보다 c_T 가 더 커지는 상황이 발생하므로 태그가 리더의 요청에 반응하지 않게 된다. 또는, 공격자에 의해 XId_R 이 도용된 경우 백엔드 서버에서 XId_R 을 이용하는 리더를 비활성화 시키는 경우가 발생할 수 있다. 이와 같이 정당한 리더가 통신이 불가능해진 경우, 리더 동기화 단계를 통해 백엔드 서버와 동기화를 맞출 수 있다.

[0133] 도 5에서 보는 바와 같이, 동기화 실패를 위한 재동기화 방법은 다음과 같다.

[0134] 단계 ① : 통신이 불가능해진 리더는 XId_R 을 식별자로 백엔드 서버로 동기화 요청 메시지를 전달한다.

[0135] 단계 ②~④ : 백엔드 서버는 XId_R 을 확인하고 존재하는 경우 r_B 와 함께 패스워드 요청 메시지를 전달한다.

[0136] 단계 ⑤~⑥ : 리더는 $sk=h(r_B||ps_Id_R)$ 를 생성하고, 이를 이용하여 Id_R 과 c_R 을 암호화해 회신한다.

[0137] 단계 ⑦~⑨ : 백엔드 서버는 세션키를 생성하고 수신한 메시지를 복호한다. 패스워드와 Id_R , Pc_R 이 동일한 경우에만 $sk(Id_R||c_R)$ 를 복호화 하고 c_R 이 Id_R 의 이전 세션 정보로 확인되면, XId'_R , K'_{BR} , c_B , 메시지를 세션키를 이용해 암호화한 후 리더에게 전달한다.

[0138] 단계 ⑩~⑫ : 리더는 c_R , K_{BR} 을 갱신하고, UPDCPL을 생성한 뒤, XId_R 을 갱신한다. 마지막으로 UPDCPL을 회신한다.

[0139] 단계 ⑬~⑭ : UPDCPL을 수신한 백엔드 서버는 c_B 를 이용하여 이를 검증하고 맞을 경우 다음 세션에서 이용할 XId_R 을 갱신한다.

[0140] 본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 컴퓨터 판독 가능 매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0141] 다음으로, 본 발명의 일실시에에 따른 발명의 효과를 도 6을 참조하여 보다 구체적으로 설명한다.

[0142] 먼저, 도청 공격에 안전성 보장에 대하여 구체적으로 설명한다.

- [0143] 도청 공격은 무선 구간에서 전달되는 정보를 수집하여 태그의 정보를 알아내는 공격이다. 도청 공격을 막기 위해서는 도청을 통해 알아낸 정보로부터 다음 세션에 이용되는 인증 정보를 생성하지 못하도록 설계해야 한다. 본 발명의 통신 과정에서는 XId_R , XId_T , m_{left} , r_T , r_R , Xc_T , Xc_R , c_R , UPDCPL 등이 암호화되지 않고 전달되므로 도청이 가능하다. XId_R 과 XId_T 는 리더와 태그의 식별자로 매 세션에서 갱신되는 값이며, 갱신된 값은 리더와 태그가 소유한 각각의 키로 암호화되어 전달된다. Xc_R 과 Xc_T 는 리더와 태그가 소유하고 있는 Id_R 과 Id_T 를 알고 있어야 생성할 수 있으며, 리더와 태그에 의해 매 세션 갱신된다. 즉, 본 발명에서 암호화되지 않고 전달되는 정보는 모두 다음 세션에 갱신되는 값들이며, 백엔드 서버가 갱신한 정보는 모두 암호화되어 전달되므로 도청 공격에 대하여 안전성을 보장한다고 볼 수 있다.
- [0144] 다음으로, 위장 공격 및 위조 공격에 안전성 보장에 구체적으로 설명한다.
- [0145] 위장 공격은 공격자가 정당한 개체로 인식되도록 하기위해서 전달되는 인증정보를 재전송하거나 위조하는 공격이다. 공격자는 도청을 통해 이전 세션들의 인증정보를 수집할 것이다. 공격자는 전달되는 정보를 위조해야만 정당한 개체로 위장이 가능하지만, 본 발명에서는 암호화되지 않고 전달된 인증정보는 다음 세션에서 사용되지 않는다. 앞서 각 개체에 대한 위장 공격 시나리오 분석을 통하여 백엔드 서버, 리더, 태그 각각의 위장 공격을 탐지하고 인증정보를 갱신하는 과정을 소개하였다. 따라서 본 발명은 위장 및 위조 공격에 대하여 안전성을 보장한다고 볼 수 있다.
- [0146] 다음으로, 위치추적 공격에 안전성 보장에 대해 설명한다.
- [0147] 위치추적 공격은 공격자가 도청 공격을 통하여 획득한 인증정보를 수집하여 태그의 위치 정보를 추적하는 공격이다. 위치추적 공격을 막으려면 노출되는 정보를 모두 갱신해야 한다. 본 발명에서는 다음 세션에 이용되는 인증정보가 모두 갱신되도록 설계하였고, 갱신된 정보 또한 암호화되어 전달되므로 이전 인증정보들을 모두 수집하더라도 상관관계를 알아낼 수 없으므로 위치추적이 불가능하다. 따라서 본 발명은 위치추적 공격에 대하여 안전성을 보장한다고 볼 수 있다.
- [0148] 다음으로, 서비스 거부 공격에 안전성 보장에 대해 설명한다.
- [0149] RFID 시스템에서의 서비스 거부 공격은 두 가지 형태로 나누어볼 수 있다. 첫째, 태그로의 서비스 거부 공격 - 공격자는 태그로 과도한 쿼리를 전송함으로써 태그의 전력을 소비하거나 다른 태그의 요청을 수신하지 못하도록 할 수 있다. 둘째, 거짓 인증정보 갱신을 통한 서비스 거부 공격 - 공격자는 고의로 변조하여 갱신되는 인증정보를 리더나 태그가 수신하지 못하도록 함으로써 각 개체 간의 비동기화를 유발할 수 있다.
- [0150] 본 발명에서는 첫 번째 타입의 공격을 방지하기 위해 카운터를 이용한 동기화 검증 방식을 이용하였다. 태그가 동기화되지 않은 리더를 확인하고 정당한 리더의 요청으로 판단될 경우에만 인증정보를 생성함으로써 무조건적인 인증정보 제공과 태그 전력 소모 공격을 막을 수 있다. 두 번째 타입의 공격의 경우, 백엔드 서버에서 정상적으로 인증이 이루어졌거나, 인증정보 갱신이 필요한 경우에 UPDCPL 메시지를 전송하도록 2번의 통신횟수를 추가하였으며, 메시지가 완전히 수신되기 전까지는 특정횟수 만큼 반복 전송하도록 하였다. UPDCPL 값은 인증된 백엔드 서버, 리더, 태그만이 현재 세션에서 유일하게 생성할 수 있는 값이다. 인증이 완료된 경우 태그가 생성한 UPDCPL을 백엔드 서버와 태그가 인증함으로써 동기화가 이루어졌음을 확인하고, 인증정보가 갱신된 경우에는 UPDCPL을 통해 동기화를 확인한 이후 백엔드 서버에서 XId_R 을 갱신한다.
- [0151] 본 발명에서는 공격이나 주변 환경에 의하여 비동기화가 발생한 경우, 리더의 동기화를 위해서 "리더 동기화 단계"를 수행할 수 있도록 하고 있다. 리더 동기화 단계에서 전달되는 정보는 XId_R 과 r_B 를 제외한 모든 정보는 백엔드 서버와 비동기된 리더 사이의 세션키에 의해 암호화되므로 갱신된 정보를 안전하게 수신하는 것을 보장한다. 따라서 본 발명은 서비스 거부 공격에 대하여 안전성을 보장한다고 볼 수 있다.
- [0152] 다음으로, 상호 인증 보장에 대해 설명한다.
- [0153] RFID 시스템에서 안전한 통신을 위해 각 개체는 서로의 신분 확인 과정을 거쳐야 한다. 본 발명에서는 백엔드 서버는 리더 및 태그와 상호인증을 제공하고, 리더는 백엔드 서버 및 태그와 상호인증을 제공하고, 태그의 경우 백엔드 서버와의 상호인증을 제공함으로써 리더와의 상호인증은 간접적으로 이루어지게 된다. 각 과정은 아래 도 6a와 같다.
- [0154] 다음으로, 부가정보 생성 공격에 대한 안전성 보장에 대하여 구체적으로 설명한다.

- [0155] 위에서 언급한 요구사항을 만족한다하더라도 노출된 정보들을 결합하여 갱신되는 정보에 대한 유추나, 부가적으로 개체 식별이 가능한 인증 정보를 생성할 수 없어야 한다. 즉, 암호화되지 않은 데이터의 취합하여 새로운 정보를 생성할 수 없어야 한다. 본 발명에서 XID_R 과 XID_T 는 각각의 ID_T 와 r_B 의 해쉬 연산에 의해 생성되고, 식별자는 개체 식별을 위해서만 사용되며 다른 인증정보에 포함되지 않는다. 이외에 노출되는 정보들은 랜덤하게 생성되는 값이기 때문에 개방된 환경에서 도청된 정보를 통해 각각의 리더와 태그를 구분할 수 없다.
- [0156] 다음으로, 전방향 안전성 보장에 대하여 설명한다.
- [0157] 전방향 안전성은 모든 세션의 정보가 공격자에게 노출되어도 메시지 분석을 통해 태그의 정보가 노출되거나 위치추적이 불가능해야 함을 보장해야 한다. 본 발명에서는 다음 세션에 이용되는 인증정보가 모두 갱신되도록 설계하였고, 갱신된 정보는 암호화되어 전달되므로 이전 세션의 식별자 XID_R , XID_T 와 다음 세션의 식별자 XID'_R , XID'_T 의 상관관계를 알아낼 수 없다. 또한, m_{Left} , X_{CT} , X_{CR} , $UPDCPL$ 에는 리더와 태그의 랜덤 값이 포함되어 연관성을 알아내기 어렵다. 따라서 본 발명은 전방향 안전성을 보장한다고 볼 수 있다.
- [0158] 한편, 본 발명의 안정성을 종래의 인증방법과 비교한 결과는 도 6b에서 나타내는 바와 같다.
- [0159] 다음으로, 본 발명의 효율성에 대해 분석해보고자 한다.
- [0160] 종래의 인증방법 중 안전성이 가장 뛰어난 제3 종래방법과 본 발명의 연산량 분석을 수행하도록 한다. 효율성 분석을 위한 지표로 태그 검색을, 난수 생성 횟수, 대칭키 연산 횟수, 해쉬 연산 횟수, XOR 연산 횟수, 타임스탬프 연산 횟수와 최종적인 통신 라운드 횟수 등을 정하였다. 먼저 LOK의 연산량에 대한 분석을 제시하고 이어서 제안하는 프로토콜의 연산량에 대한 분석을 기술한다.
- [0161] 제3 종래방법은 백엔드 서버와 리더를 하나의 시스템으로 설계하였으나 백엔드와 서버 구간을 고려할 경우 총 6의 통신이 이루어진다. 백엔드 서버의 경우 난수 연산은 수행하지 않으며, 시스템을 안전한 구간으로 가정하였으므로 시스템 내에서 백엔드 서버와 리더 구간에 전달되는 3회의 통신에 대한 암호복호화 3회가 필요할 것으로 보인다. 태그의 인증 메시지 연산을 위해서 사용되는 해쉬 연산은 동적 ID의 상태에 따라 2가지로 분류될 수 있다. 서버에 저장된 ID와 태그의 ID 간에 동기화가 맞는 경우, 인증값 검증에 1회, 인증될 경우 키 갱신에 1회, ID 갱신 1회가 수행되어 총 3회의 해쉬 연산이 수행된다. 서버에 저장된 ID와 태그의 ID 간에 동기화가 맞지 않을 경우, 모든 태그를 대상으로 다음 과정을 수행한다. 현재 키로 생성된 인증값 검증을 위해 1회, 인증될 경우 키 갱신에 1회, ID 갱신에 1회를 수행하므로 총 3회의 해쉬 연산이 수행된다. 만약, 현재 키로 검증되지 않을 경우 이전키로 생성된 인증값 검증을 위해 1회, ID 갱신에 1회가 수행되어 총 2회의 해쉬 연산이 추가로 수행된다. 즉, ID가 동기화된 경우 최소 1회에서 3회의 해쉬 연산이 수행되고, ID가 비동기화된 경우 현재키나 이전키로 인증 여부를 확인하게 되므로 3회의 해쉬 연산이 수행된다. 이는 백엔드 서버의 DB에 n 개의 태그가 존재한다고 가정하면 최악의 경우 $3n$ 회의 해쉬 연산이 수행될 수 있음을 의미한다. 제3 종래기술의 시스템 상에서 리더는 쿼리 전송시 난수 생성을 1회 수행하고, 이 값을 백엔드 서버로 전송해야 백엔드 서버와 태그 간의 난수 동기화가 필요하다. 또한, 백엔드 서버와 리더의 구간을 안전하다고 가정하였으므로 백엔드 서버와 동일하게 3회의 암호복호화가 필요할 것으로 보인다. 태그는 인증정보 생성 및 키 갱신에 1회의 난수 생성이 필요하다. 인증정보 생성, ID 갱신, 키 갱신에 각각 1회의 해쉬 연산이 수행되므로 총 3회의 해쉬 연산이 필요하다.
- [0162] 본 발명의 연산량을 살펴보면 다음과 같다. 먼저 백엔드 서버에서는 리더와 태그의 랜덤 ID 갱신을 위해서 1회의 난수를 생성한다. 백엔드 서버와 리더의 안전한 메시지 교환을 위해 2회, 백엔드 서버에서 태그로 전달되는 메시지의 안전성을 위해 1회의 암호복호화가 수행되므로 총 3회의 대칭키 연산이 수행된다. 해쉬 연산의 경우, 리더와 태그의 랜덤 카운터 연산에 각 1회, 인증 정보 검증에 1회, 리더와 태그의 랜덤 ID 갱신에 1회로 총 5회의 해쉬 연산이 수행된다. (단, 리더 공격이 탐지된 경우, 백엔드 서버와 리더 구간의 비밀키 갱신을 위해 $m-1$ 회의 해쉬 연산이 수행된다.) XOR 연산의 경우 리더와 태그의 랜덤 카운터 연산에 각 1회, $UPDCPL$ 인증을 위해 1회로 총 3회의 XOR 연산이 수행된다. 타임스탬프 연산의 경우, 백엔드 서버가 전송한 메시지의 응답시간을 측정하는데 1회 사용된다. 리더는 쿼리 전송시 난수 생성을 1회 수행하고, 태그로부터 수신 받은 메시지를 백엔드 서버로 전송하는데 1회, 백엔드 서버로부터 전달 받은 메시지를 복호화하는데 1회로 총 2회의 암호복호화 연산이 수행된다. 해쉬 연산의 경우 리더가 가지고 있는 카운터를 랜덤 카운터로 변경하는데 1회 수행된다. XOR 연산의 경우 리더의 카운터를 랜덤 카운터로 변경하는데 1회, $UPDCPL$ 값을 검증하는데 1회로 총 2회 연산이 수행된다. 타임스탬프 연산은 태그로 쿼리 전송 후 응답을 측정하는데 1회, 태그의 정보의 인증을 위해 백엔드 서버로 전

송하는 과정에서 1회, 인증 후 태그의 정보 갱신을 위해 태그로 전달하는 과정에서 1회로 총 3회의 타임스탬프 연산이 수행된다. 태그는 자신의 인증관련 정보를 생성하기 위해 1회의 난수 생성 과정을 수행하고, 리더가 태그의 정보를 확인하고 백엔드 서버로부터 갱신 정보를 수신하여 암호화된 메시지의 복호화 1회를 수행한다. 해쉬 연산의 경우 인증정보 m 을 생성하는데 1회 사용된다. XOR 연산의 경우 랜덤 카운터 생성시 1회, UPDCPL 생성시 1회로 총 2회의 XOR 연산을 수행한다. 타임스탬프 연산은 수행되지 않는다. 마지막으로 통신 횟수의 경우 백엔드 서버와 리더 구간에서 3회, 리더와 태그 구간에서 4회로 총 7회의 통신이 이루어진다.

[0163] 가장 자원제약적인 태그의 측면에서 살펴보면 해쉬 연산이 3회에서 1회로 줄었다. 반면, 갱신정보의 노출을 방지하기 위한 1회의 복호화 과정이 추가되었으며, 2회의 XOR 연산이 추가되었다. 경량화된 암호 알고리즘을 적용할 수 있다고 본다면, 2회의 해쉬 연산을 줄임으로써 연산량 부하를 줄이면서 안전성을 높였다고 볼 수 있다. 종래방법과의 연산량 비교는 도 6c와 같다.

[0164] 요약하면, 본 발명은 상호인증, 재전송 공격, 위장공격, 태그 위치 추적 공격, 서비스 거부 공격에 안전함은 물론, 고정 ID 방식에 랜덤 식별자와 카운터를 활용하여 공격자가 백엔드 서버, 리더, 태그로 가장하더라도 개체 간의 인증 과정에서 공격을 탐지할 수 있다. 한편, 제3 종래방법과 비교해볼 때, 효율성면에서 인증 과정에서 XOR 연산과 대칭키 암호 연산이 추가되고 통신횟수가 증가하는 단점은 Trade-off 로 작용한다.

[0165] 하지만 고정 ID 방식의 RFID 시스템에 해쉬 연산을 통해 랜덤 ID 만들어 사용함으로써 백엔드 서버가 갖는 동적 ID의 일반적인 효율적인 태그 검색을 지원하고, 프로토콜 자체 적으로 민감한 인증 정보를 암호화함으로써 별도의 보안 채널을 요구하지 않는다는 점에서 기존 논문들 보다 높은 보안성을 제공한다.

[0166] 이상, 본 발명자에 의해서 이루어진 발명을 실시 예에 따라 구체적으로 설명하였지만, 본 발명은 실시 예에 한정되는 것은 아니고, 그 요지를 이탈하지 않는 범위에서 여러 가지로 변경 가능한 것은 물론이다.

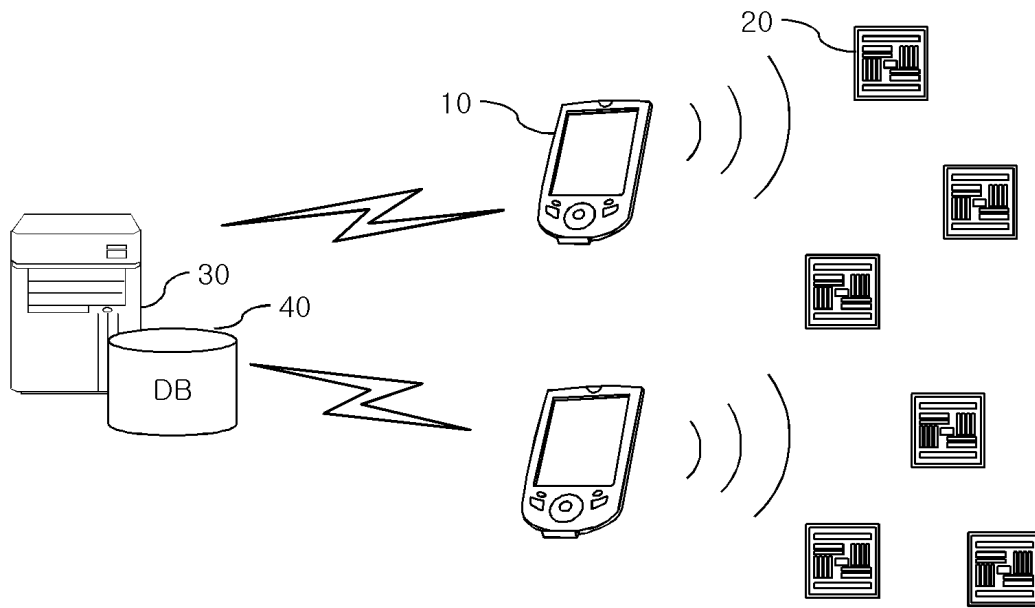
[0167]

산업상 이용가능성

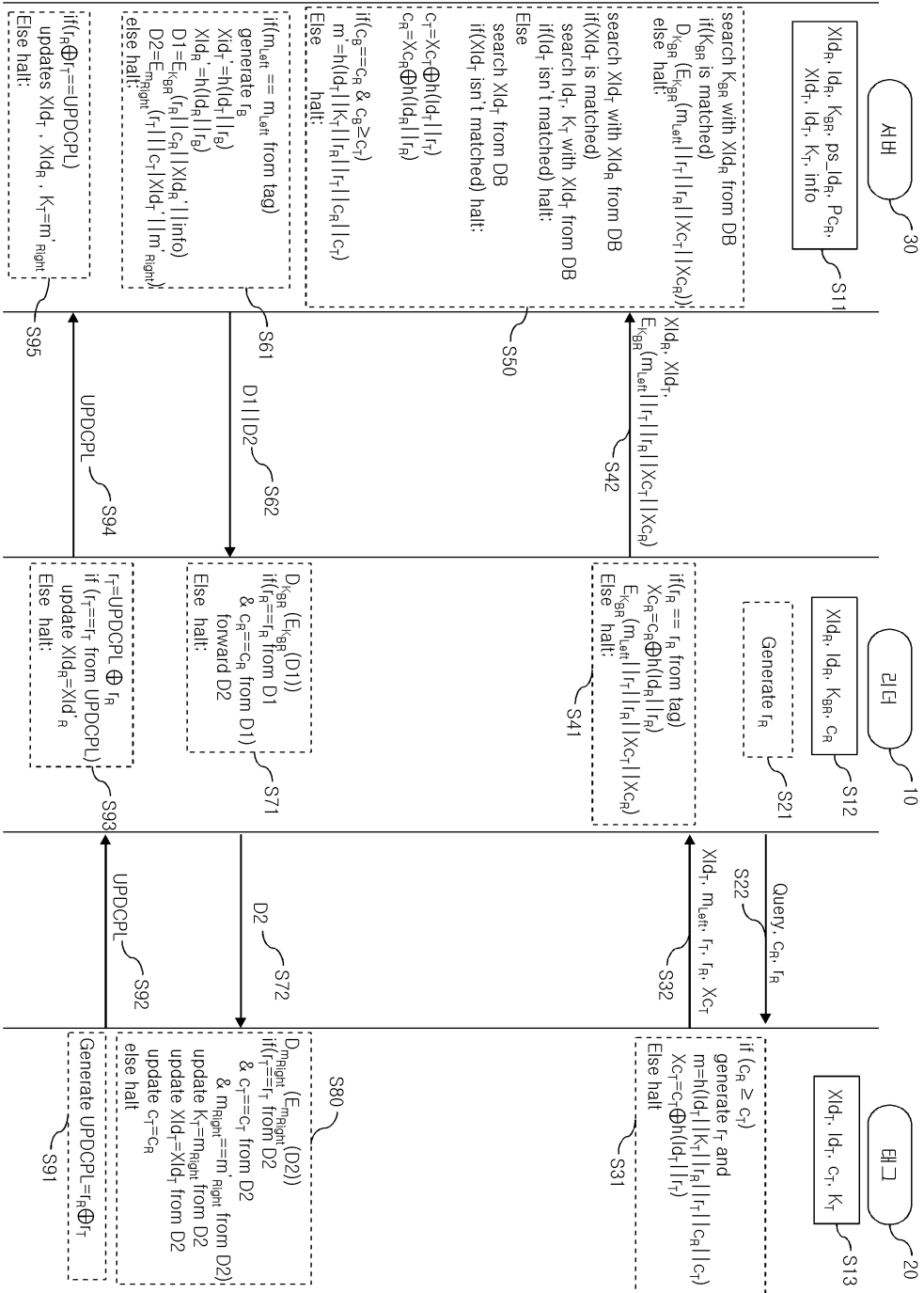
[0168] 본 발명은 서버, 다수의 리더, 및 다수의 태그로 구성된 RFID 태그 시스템에서 동기화 카운터를 이용하여 동기화된 상대와 인증을 처리하는 랜덤 아이디 기반 RFID 상호 인증 시스템을 개발하는 데 적용이 가능하다.

도면

도면1



도면2



도면3

41

테이블명	리더 정보 테이블					
필드명	랜덤 식별자	식별자	암호키	태그 패스워드	이전 세션 카운터	리더 비활성화
값	XId _R	Id _R	K _{BR}	ps_Id _R	Pc _R	0

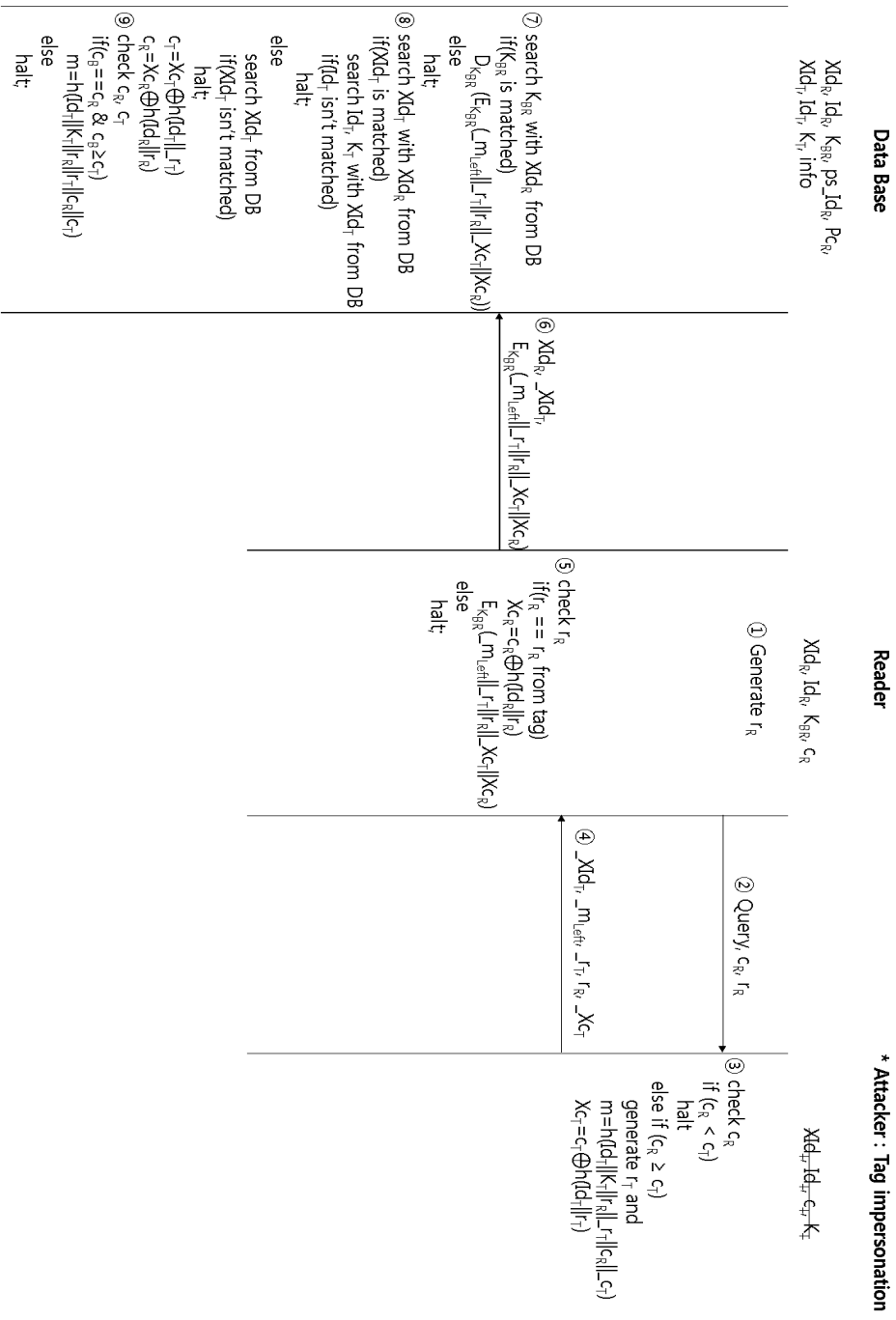
42

테이블명	태그 정보 테이블			
필드명	랜덤 식별자	식별자	키	상품정보
값	XId _T	Id _T	K _T	info

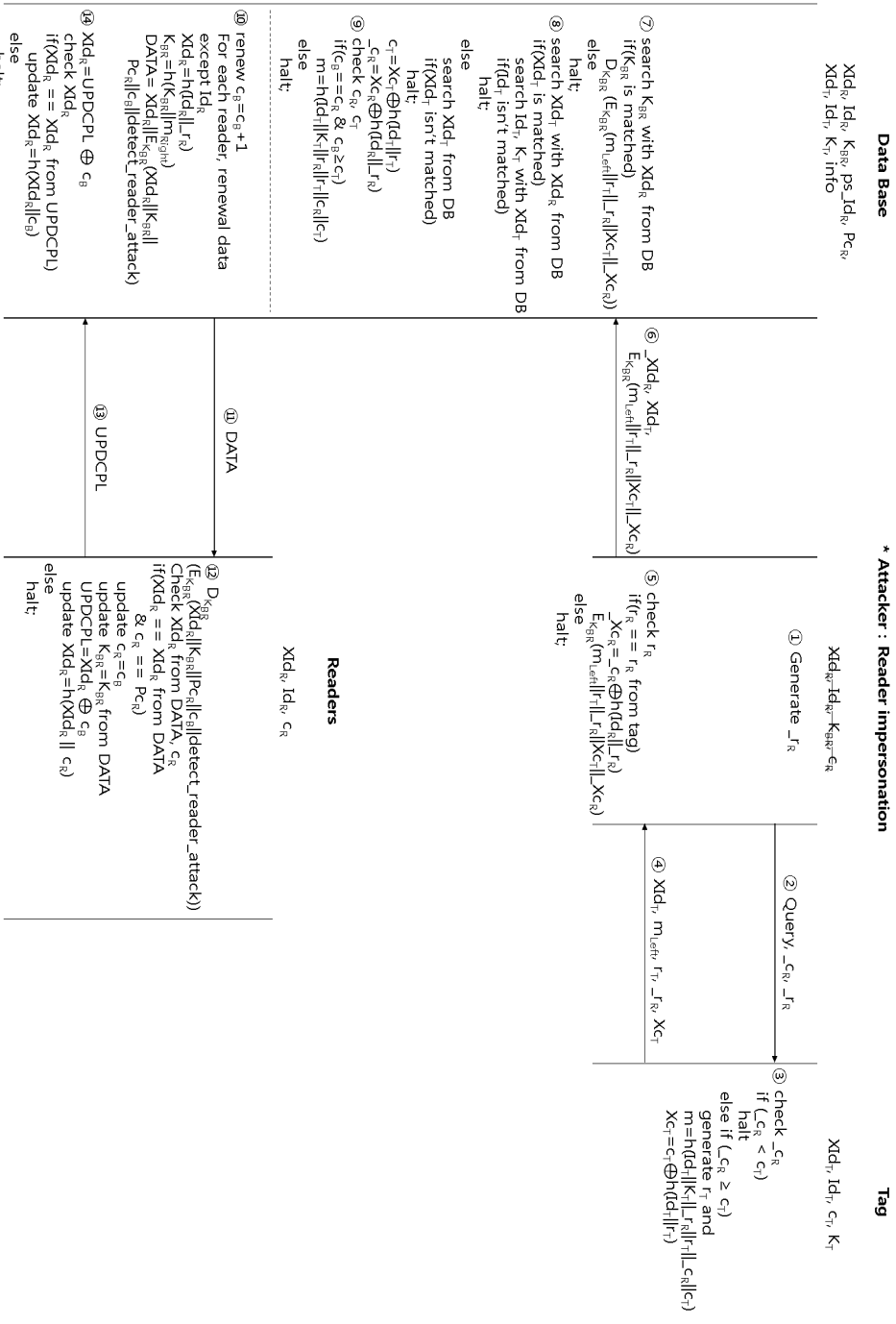
43

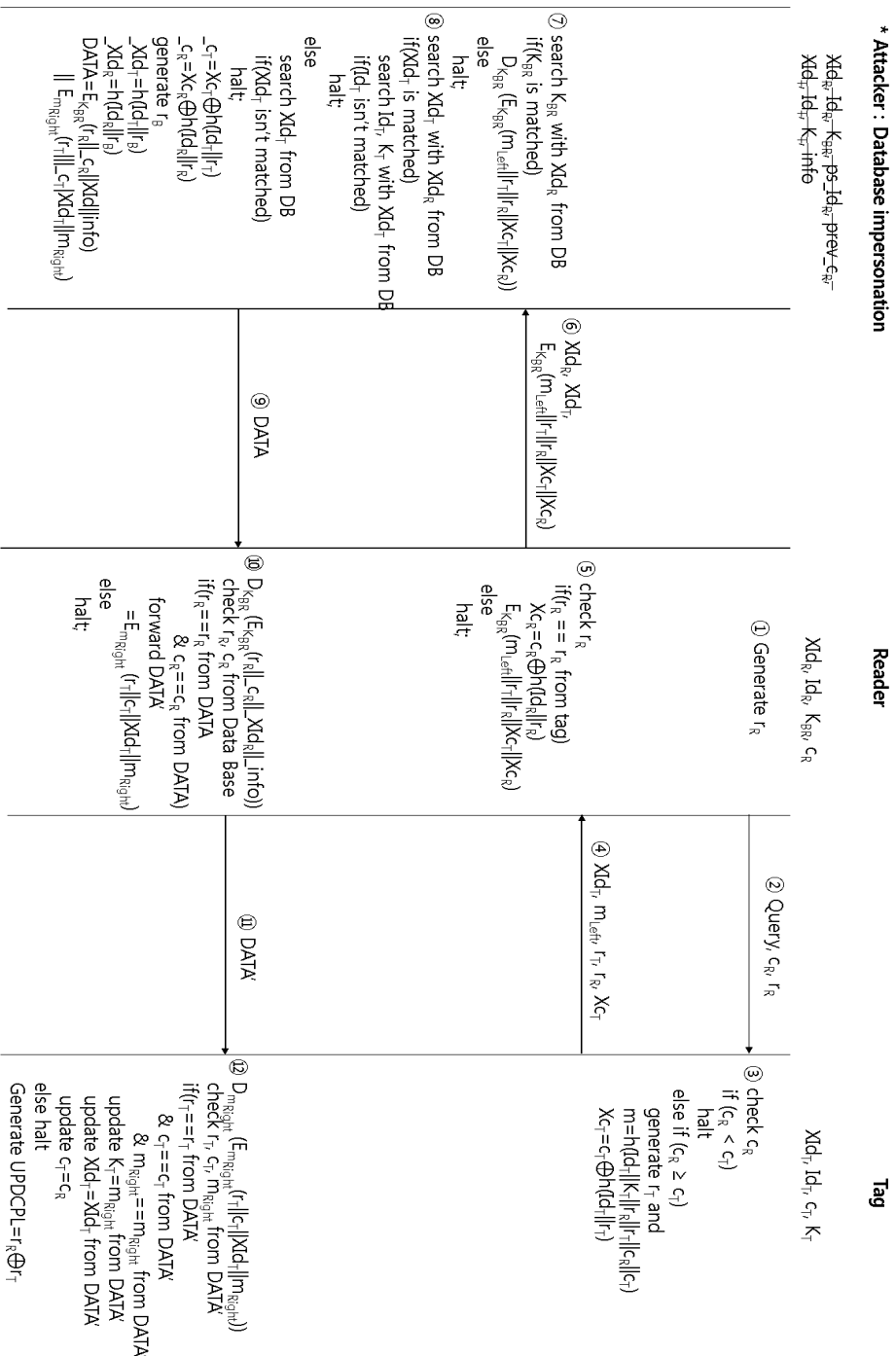
테이블명	태그 리스트 테이블	
필드명	랜덤 식별자	랜덤 식별자
값	XId _R	XId _T

도면4a

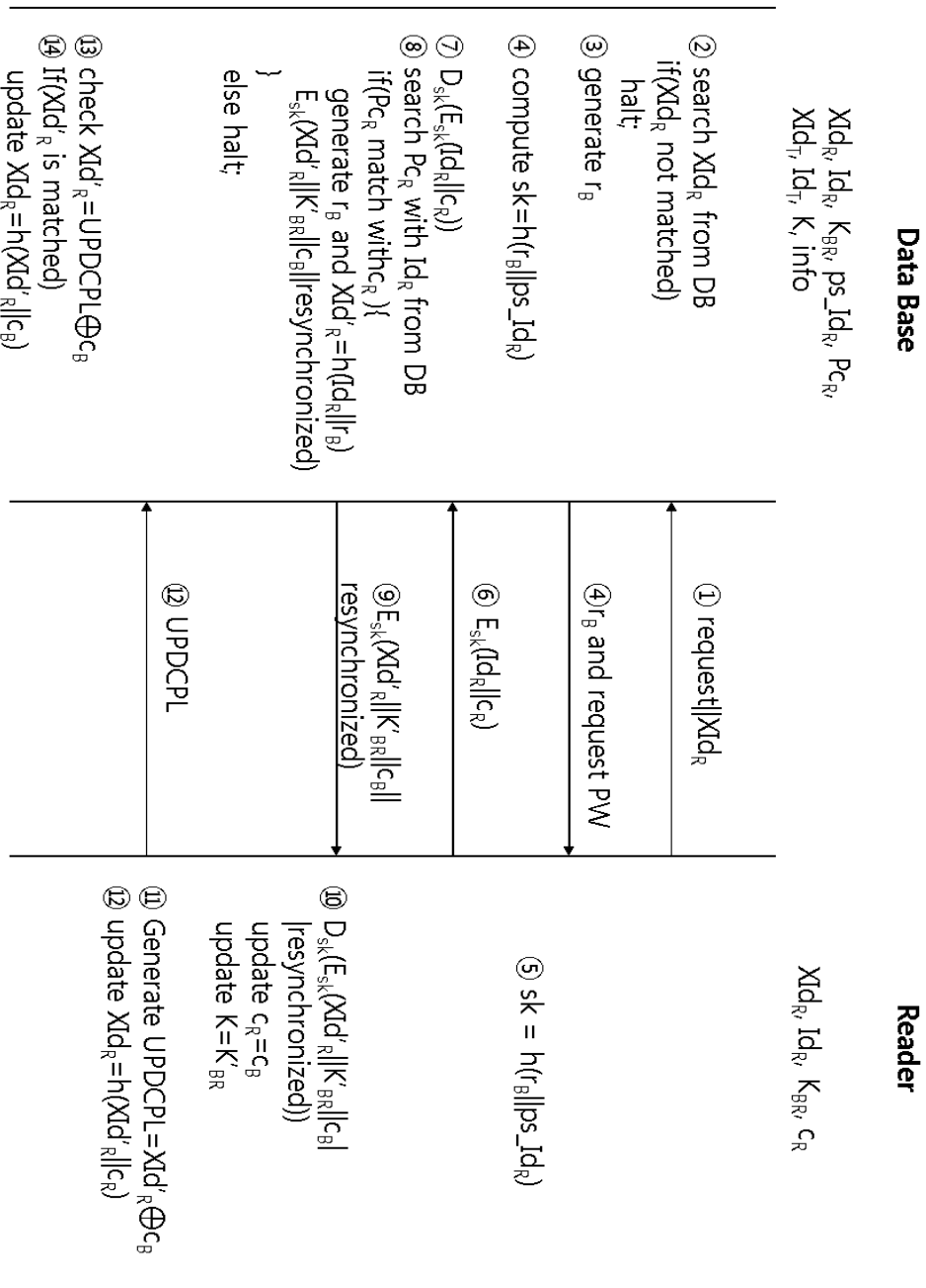


도면4b





도면4c



도면5

도면6a

B->R	R->B	T->R
XId _R 수신 후 K _{BR} 로 암호화 Xc _R 수신 후 c _R 을 이용한 m _{Left} 확인	r _T 전달 후 r _T 수신 Xc _T 전달 후 c _R 수신 XId _R , K _{BR} 쌍을 이용한 암호화	카운터 비교를 통한 동기화 검사 T->B을 인증시 T->R 간접인증
B->T	B->T	T->B
Xc _T 수신 후 c _T 를 이용한 m _{Left} 확인 m _{Left} 확인 후 m _{Right} 로 암호화	r _R 전달 후 r _R 수신 r _R , c _R 정보가 포함된 m _{Left} 을 B에서 인증될 경우에만 상품정보 수신	r _T 전달 후 r _T 수신 Xc _T 전달 후 c _T 수신 m _{Left} 전달 후 m _{Right} 수신 m _{Right} 로 암호화된 메시지 수신

*기호 설명 B : Backend-database, R : Reader, T : Tag
: B->R : Backend-database가 리더를 인증하는데 필요한 인증 요소

도면6b

	제1 종래방법	제2 종래방법	제3 종래방법	본 발명
상호인증	리더<->태그, 태그->DB 불가	태그->DB, 태그->리더 불가	모두 가능	모두 가능 + 비동기리더 탐지가능
DB-리더 구간	안전한 채널로 가정	안전한 채널로 가정	안전한 채널로 가정	공개 채널로 가정
재전송/위조 공격	X	0	0	0
위장 공격	X	Δ^1	Δ^1	0
태그 위치 추적 공격	X	X	0	0
서비스 거부 공격	X	X	Δ^2	0
전방향안전성 공격	X	X	0	0
부가정보 생성 공격	X	0	0	0

*부가설명 : Δ^1 : DB-리더 구간을 안전한 채널로 가정하여 백엔드 서버의 위조 공격을 고려하지 않음.
 Δ^2 : 태그-리더 구간의 프로토콜 취약성을 이용한 서비스 거부 공격만을 고려하였음.

도면6c

	제1 종래방법			제2 종래방법			제3 종래방법			본 발명		
태그 타입	정적 ID			정적 ID			동적 ID			동적 ID 특성을 만족하는 정적 ID		
태그 검색을	전사적 해쉬 연산			전사적 해쉬 연산			전사적 DB 검색 후 1회의 해쉬연산			리더 랜덤 ID 기반(m회) DB 검색 후 1회의 해쉬연산		
비동기화시 태그 검색을	-			-			전사적 DB 검색 후 2n회의 해쉬연산			(m+n)회 DB 검색 후 1회의 해쉬연산		
	DB	리더	태그	DB	리더	태그	DB	리더	태그	DB	리더	태그
난수생성	-	1	-	-	1	1	-	1	1	1	1	1
대칭키 연산	2	2	-	2	2	-	3	3	-	3	2	1
해쉬연산	-	1	1	n	1	1	$\frac{3}{3n^{1)}$	-	3	$\frac{5}{2m+2^{2)}$	1	1
XOR연산	-	1	1	-	-	-	-	-	-	3	2	2
타임스탬프	-	-	-	-	-	-	-	-	-	1	3	-
통신 횟수	6			4			6			7		

*기호설명 : n : 태그의 수, m : 리더의 수,

¹⁾ 태그 검색의 최악의 경우, 3n회만큼의 해쉬 연산이 필요함.

²⁾ 리더 공격이 탐지된 경우, ID와 암호키 갱신을 위해 2m+2회의 해쉬 연산이 필요함.