(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06K 17/00 (2006.01)

(45) 공고일자 2006년08월09일
(11) 등록번호 10-0610239
(24) 등록일자 2006년08월01일

(21) 출원번호 10-2005-0054645
(22) 출원일자 2005년06월23일

(65) 공개번호
(43) 공개일자

(73) 특허권자 인하대학교 산학협력단
인천 남구 용현동 253 인하대학교

(72) 발명자 양대헌
서울 서초구 서초동 신동아아파트 3동 210호

강전일
충남 공주시 옥룡동 284-1

(74) 대리인 이원희

(56) 선행기술조사문헌
KR1020000057711 A
KR1020020074494 A
KR1020050081777 A
KR102060028222 A
* 심사관에 의하여 인용된 문헌

심사관 : 김창주

(54) 위치 추적과 서비스 거부 공격에 강한 알에프아이디인증방법

요약

본 발명은 태그가 랜덤수를 생성하여 통신 과정에서 사용되는 메시지 인증의 예측 불가능성을 보장하여 보안성이 높아지도록 한 위치 추적과 거부 공격에 강한 RFID 인증방법을 제공한다.

이러한 본 발명은 인증을 위한 세션을 시작하기 위해 상기 리더가 상기 태그에게 리퀘스트 메시지를 요청하는 단계; 상기 요청 메시지를 받은 태그가 메시지의 예측불가능성을 위해 랜덤수를 이용하여 제 1 메시지를 계산하여 데이터베이스 서버에게 전송하는 단계; 상기 제 1 메시지를 받은 데이터베이스 서버가 제 2 메시지를 계산하여 전송하는 단계; 상기 제 2 메시지를 받은 태그가 또 다른 랜덤수를 생성하여 상기 서버를 확인하고 인증하는 단계; 상기 태그와 데이터베이스 서버가 다음 세션을 위해 초기화 하는 단계; 를 포함하는 것을 특징으로 한다.

대표도

도 2

색인어

스마트태그, RFID, 인증, 위치추적, 서비스 거부 공격.

명세서

도면의 간단한 설명

도 1은 종래의 RFID의 전체적인 구조도.

도 2는 본 발명에 따른 RFID의 전체적인 구조도.

도 3는 본 발명에 따른 태그에서 필요로 하는 메모리 필드를 나타낸 표.

도 4은 본 발명에 따른 RFID의 데이터베이스 구조의 실시예.

도 5는 본 발명에 따른 태그와 데이터베이스 서버 사이의 인증을 위한 인증과정을 나타낸 개략도.

도 6은 본 발명에 따른 태그와 데이터베이스 서버 사이의 인증 과정을 나타낸 흐름도.

도 7는 본 발명에 따른 태그와 데이터베이스 서버 사이의 인증을 위한 또 다른 인증 과정을 나타낸 개략도.

도 8은 본 발명에 따른 태그와 데이터베이스 서버 사이의 또 다른 인증과정을 나타낸 흐름도.

도 9은 본 발명에 의한 세션 도중 요청 메시지를 처리하는 과정을 나타낸 개략도.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 RFID에 관한 것으로, 특히 태그가 랜덤수를 생성하여 인증을 위한 메시지를 예측할 수 없도록 하여 보안을 강화한 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법에 관한 것이다.

RFID(Radio Frequency IDentification)는 물체나 동물 또는 사람 등을 식별하기 위해 전자기 스펙트럼 부분의 무선 주파수 내에 전자기 또는 정전기 커플링 사용을 통합시킨 기술이다. 1980년대부터 등장한 이 시스템은 전용 근거리 통신 또는 무선 식별 시스템이라고도 한다.

기능은 바코드와 비슷하지만 먼 거리에서도 인식이 가능하며, 동시에 여러 개를 인식할 수 있다는 장점이 있어 바코드보다 활용범위가 훨씬 넓으며, 향후 900MHZ 대역 제품이 현재의 13.56MHZ 대역을 대신하여 주력 제품이 될 것이다.

또한, 마그네틱 인식 또는 바코드 인식 시스템의 경우 특정한 외부적 표시가 필요하고 자기력 약화 및 훼손이나 파손 등으로 인해 시간이 지날수록 인식률이 점차 떨어지는데 반해 RFID 시스템은 그러한 단점을 줄일 수 있다.

RFID 시스템은 각종 자동화 사업, 유통업, 가축관리, 출입 통제, 근태관리, 물류 관리, 주차 관리 등에 사용되는 등 새로운 솔류션으로 급부상하고 있는데, 구체적으로 신용/직불 카드를 비롯하여 선불식/후불식 버스, 지하철 카드. 주차장 출입용 카드, 백화점 카드, 컨베이어 벨트 상의 제조공정품, 우편송달 시스템, 동물의 정보를 기록한 식별표 등에 사용할 수 있다.

예를 들어, 바코드의 경우에는 어느 회사의 어떤 상품 정도의 정보만 담고 있지만 RFID는 언제, 어느 공장에서 만들어졌고 어디에 출하됐는지 등의 방대한 정보를 수록할 수 있다. 즉 물류를 더욱 정확하고 세세하게 파악할 수 있을 뿐만 아니라, 한 장의 카드에 방대한 정보가 담기기 때문에 신원 및 정보확인이 용이하다.

도 1 종래의 RFID의 전체적인 구조도이며, 태그(10), RFID 안테나(20), 정보처리 시스템(40), 태그와 정보처리 시스템과 연결하는 리더(30)로 구성된다.

상기 RFID 안테나(20)는 태그(10)를 활성화시키기 위한 신호를 전달하기 위해 무선 주파수 전파를 사용한다. 생성된 전자기장을 통해 태그(10)를 활성화시켜 정보처리 시스템(40)과 태그(100) 사이의 소통을 가능하게 한다. 상기 RFID 안테나(20)는 판독기의 역할을 위해서 트랜시버나 디코더 등과 합쳐지는 경우가 많다.

상기 태그(10)는 송수신을 위한 송수신 안테나와 태그의 정보를 저장하고 있는 메모리로 구성되어 있으며, 수동식과 능동식이 있다. 수동식이 내부 전원 없이 판독기의 전파신호로부터 에너지를 공급받아 동작하는 데 비해 능동식에는 스스로 작동하기 위해 태그 전지가 내장되어 있다. 실리콘 반도체 칩을 사용하는 칩 태그와 LC 소자, 플라스틱 또는 폴리머(polymer:중합체) 소자로만 구성된 무선칩 태그로 구분하기도 한다.

상기 RFID 안테나(20)에 의해 태그(10)가 활성화되면, 상기 태그(10)는 가지고 있던 데이터를 RFID 안테나(20)로 전송한다. 이 데이터는 대개 리더(30)를 통해 데이터가 처리되는 정보처리 시스템(40)으로 넘겨지게 된다.

상기 리더(30)는 RFID 안테나(20)와 컴퓨터, 서버등과 같은 정보처리 시스템(40) 사이의 소통을 관리한다. 태그(10) 메모리 안의 데이터로부터 직접 프로세스 컨트롤을 수행하도록 할 수도 있다. 리더(30)는 태그(100)의 칩 안에 암호화되어 있는 데이터를 풀어내고 그 데이터는 정보처리 시스템(40)으로 보내져 실행된다.

상기와 같이 구성된 RFID의 동작 과정은 다음과 같다.

RFID 안테나(20)의 전파 영역 내에 정보가 저장되어 있는 상기 태그(10)가 진입하면, 상기 RFID 안테나(20)는 태그(10)의 메모리에 저장된 정보를 리더(30)에 전송하고, 상기 태그(10)의 정보를 전송받은 리더(30)는 정보처리 시스템(40)에 전달한다.

그러나, 이러한 RFID 시스템은 보안성이 높아질수록 가격이 높아져 보급의 한계가 있다는 단점이 있다.

또한, 상기 태그(10)의 내부는 프로세서가 없고 태그(10)를 제어하는 단순한 제어장치와 메모리 및 송수신 안테나만이 있으며, 표식체 또는 인식체로서의 메모리 역할을 하는 것에 불과하므로 보안 능력이 전혀 없다는 문제점이 있다.

이러한 RFID의 보안적인 문제점을 해결하기 위해 몇몇 설계자들은 태그가 보내는 메시지의 예측 불가능함을 보장하기 위한 방법으로 리더를 이용하여 랜덤수를 생성하게 하여 메시지를 포장하였다.

그러나 리더는 단지 태그와 데이터베이스 서버 사이의 중계자의 역할을 할 뿐이며, 리더는 통신을 수행하기 위해 세션을 여는 역할을 수행하므로, 세션을 선점하거나 또는 선점하지 못하는 경우에 있어서 보안 취약성이 존재하는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 이러한 문제점을 해결하기 위한 것으로, 본 발명의 목적은 태그의 인증을 위해 태그가 직접 랜덤수를 이용한 메시지를 생성하여 세션 사이에 메시지의 예측 불가능성을 보장하고, 메시지의 다중 수신을 허용함으로써 선점적이거나 비선점적이어야 하는 인증 과정을 탈피하여 위치 추적 문제와 각종 서비스 거부 공격을 해결할 수 있도록 한 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법을 제공함에 있다.

발명의 구성 및 작용

상기 본 발명의 목적을 달성하기 위한 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법은, RFID와 데이터베이스 서버 사이의 인증하는 방법에 있어서 리더가 태그에게 요청 메시지를 보내는 단계; 상기 메시지에 대한 응답으로 상기 태그가 데이터베이스 서버에게 응답메시지를 보내는 단계; 상기 응답 메시지에 대하여 데이터베이스 서버는 태그에게 확인 메시지를 보내는 단계; 및 상기 태그는 인증을 확인했음을 알리는 재확인 메시지를 보내는 단계를 포함한다.

이에 따른 상세한 RFID 인증방법은 인증을 위한 세션을 시작하기 위해 상기 리더가 상기 태그에게 리퀘스트 메시지를 요청하는 단계; 상기 태그가 메시지의 예측불가능성을 위해 랜덤수를 이용하여 제 1 메시지를 계산한 후, 상기 데이터베이스 서버에게 전송하는 단계; 상기 데이터베이스 서버가 태그를 인증하면, 랜덤수를 이용하여 제 2 메시지를 계산하여 전송하는 단계; 상기 제 2 메시지를 받은 태그가 상기 서버를 확인하고 성공 메시지를 송신하는 단계; 상기 태그와 데이터베이스 서버가 다음 세션을 위해 초기화 하는 단계; 를 포함하여 이루어지는 것을 특징으로 한다.

이러한 RFID 인증방법에서, 상기 태그는 인증을 위한 메시지의 예측 불가능성을 보장하기 위해 랜덤수를 생성하는 것을 특징으로 한다.

또한, 상기 태그는 내부 변수를 사용하여, 태그의 상태를 알아낸다. 내부 변수가 참이면, 메모리에 저장된 랜덤수를 사용하고, 거짓이면, 랜덤수를 생성하여 사용하고 이를 다시 메모리에 저장하는 것을 특징으로 한다.

상기 내부변수는 태그 내에 전원이 들어오면 거짓으로 초기화 되었다가, 메모리에 랜덤수를 저장하면 참으로 바뀌고, 세션이 끝나면 다시 거짓 상태로 바뀌는 것을 특징으로 한다.

뿐만 아니라, 확인 메시지를 처리하기 위해 타이머를 사용하지 않고 카운트를 사용하여, 메시지를 수신할 때마다 카운트를 증가시키며 다중의 메시지를 수신하고 처리한다. 만약 카운트가 설정된 최대 값에 도달하면 태그는 이를 공격으로 간주하고 세션을 닫는 것을 특징으로 한다.

또한, RFID 인증을 위한 세션을 여는 것은 리더이나 세션을 닫을 수 있는 권한이 태그에게만 존재하여 선점적이거나 비선점적인 문제를 해결하는 것을 특징으로 한다.

이하, 본 발명의 바람직한 실시예를 첨부된 도면을 첨부하여 보다 상세하게 설명한다. 단, 하기 실시예는 본 발명을 예시하는 것일 뿐 본 발명의 내용이 하기 실시예에 한정되는 것은 아니다.

도 2는 본 발명에 따른 RFID 의 전체적인 구조도이며, 태그(100)와 리더(200)와 데이터베이스(300)로 구성된다.

상기 태그(100)는 제어부(120)와 메모리(110)로 구성되어 있다. 상기 제어부(120)는 연산기능과 데이터 입출력 기능을 제공하며, 태그(100)의 인증을 받기 위해 랜덤수를 이용하여 메시지를 생성한다. 상기 메모리(110)는 태그(100)의 무선식별정보를 저장하고 있으며, 상기 제어부(120)에서 생성된 메시지가 저장된다.

상기 데이터베이스(300)는 상기 데이터베이스(300)의 데이터를 처리하는 서버(310)를 구비하고 있으며, 여러 태그의 정보를 조직적으로 통합하여, 저장하고 있다. 특정 태그(100)가 서버(310)에 인증을 요청하면 상기 서버(310)는 데이터베이스(300)를 검색하여 요청을 처리한다.

상기 리더(200)는 태그(100)와 데이터베이스(300) 사이의 소통을 관리한다. 상기 태그(100)에서 생성된 메시지는 상기 리더(200)를 통해 상기 데이터베이스(300)로 전송되며, 그 역도 가능하다.

도 3 본 발명에 따른 태그에서 필요로 하는 메모리 필드를 나타낸 표이다.

태그(100)가 인증 세션 중인지 아닌지를 나타내는 내부변수(이하, SFlag라 칭함)는 세션이 시작하면 참이 되며, 세션이 정상 또는 비정상으로 끝나게 되면 거짓이 된다. 상기 SFlag는 태그(100)가 전원이 들어온 즉시 false로 초기화된다.

ID는 IDentifier의 약자로, 인증 세션 동안 다른 태그들과 구별하기 위해 사용하며 0과 1로 구성된 n비트열이다.

CWD는 Confirm Word의 약자로, 서버(310)가 데이터베이스(300)에서 상기 태그(100)의 ID를 확인하는데 사용하며 0과 1로 구성된 n비트열이다.

태그(100)에서 매 세션마다 랜덤하게 바뀌어 생성되는 R1은 SFlag가 참이면 메모리(110)에 저장되었던 기존의 R1으로 대체되며, SFlag가 거짓이면 태그(100)에 의해 새롭게 생성된다. 0과 1로 구성된 n비트열이다. R2 역시 랜덤수이다.

C는 Count의 약자로, 매 세션마다 일정하게 증가하거나 무작위로 바뀐다. 상기 SFlag가 참이면 기존에 저장되었던 C로 대체되지만, 상기 SFlag가 거짓이면 태그(100)에 의해서 바뀐다. 0과 1로 구성된 m비트열이다.

한계값 변수(이하, THR_COUNT라 칭함)는 메시지 교환을 통해 서로를 인식한 이후부터 통신을 마칠 때까지의 기간인 하나의 세션동안 얼마나 많은 시도가 있었는지를 나타낸다. THR_COUNT가 최대값 변수(이하, THR_MAX라 칭함)에 다다르게 되면, 태그(100)는 현재의 세션을 종료하고 새로운 세션을 시작한다. 선택적으로 서비스 거부 공격을 보고할 수 있다.

UR은 User Reserved memory를 나타낸다.

상기와 같은 필드를 필요로 하는 태그(100)는 인증하기 위해 UR 필드를 제외한 나머지 필드를 반드시 가지고 있어야 하며, m과 n의 크기는 태그 보안상의 이유로 충분히 큰 것이 좋으나 m이 너무 클 경우 데이터베이스의 용량이 늘어나기 때문에 적당히 정해야한다.

도 4은 본 발명에 따른 RFID 의 데이터베이스 구조의 실시예이다.

데이터베이스(300)는 슬롯(slot)이라는 기본단위로 서로 링크된(linked) 형태로 구현된다. 상기 도면에서 흰색슬롯(301) 비어있는 슬롯이며, 회색슬롯(302)은 정보가 저장되어 있는 슬롯이고, 가장 진한 색으로 칠해진 슬롯(303)은 동일한 ID를 가지고 있는 슬롯이다.

하나의 슬롯은 H(ID||C), CWD를 구성요소로 갖고 있다. H는 해싱함수를 나타낸다. H(ID||C)는 ID와 C의 OR연산을 통해 나온 값을 해싱함수로 계산한 값이고, CWD는 태그의 ID를 확인하는데 사용된다.

동일한 ID를 가지고 있는 슬롯의 개수는 2^m(2의 m제곱)개로 태그(100)의 카운터인 C의 크기 m에 의해 결정되며, 상기 슬롯은 주소의 충돌을 막기 위해 동일한 주소를 가진 슬롯은 링크로 이어져있다.

상기 도 2, 3, 4와 같은 구성을 갖는 RFID 에서 태그(100)와 서버(310) 사이의 인증과정을 도 5의 개략도로 설명한다.

우선, 태그(100)가 RFID 안테나의 영역 안에 들어가면, 리더(200)는 상기 태그(100)의 정보를 얻기 위해 {REQUEST} 메시지를 보낸다(단계 S1).

상기 {REQUEST} 메시지를 받은 태그(100)는 자신의 상태를 체크하는 SFlag를 확인한 후, 랜덤수를 이용하여 제 1 메시지를 생성하고 리더(200)를 통해 데이터베이스(300)로 전송한다(단계 S2).

상기 제 1 메시지를 전송받은 서버(310)는 상기 태그(100)의 인증을 위해 ID를 데이터베이스(300)에서 검색한 후, 랜덤수를 이용하여 제 2 메시지를 생성하고 리더(200)를 통해 상기 태그(100)로 전송한다(단계 S3).

상기 제 2 메시지를 전송받은 태그(100)는 현재 세션의 시도 횟수를 저장하고 있는 THR_COUNT를 체크하여 세션이 종료되는 THR_MAX가 될 때까지 제 2 메시지를 전송받으며, 상기 전송받은 제 2 메시지와 비교하여 상기 데이터베이스(300)를 확인한다.

상기 단계에서 상기 태그(100)가 데이터베이스(300)를 확인하면, 상기 서버(310)에 {CWD} 메시지를 보내 인증이 완료되었음을 알린다(단계 S4).

이와 같은 과정으로 구현되는 태그(100)와 데이터베이스(300) 사이의 인증방법을 도 6의 흐름도와 함께 자세히 설명한다.

우선, 태그(100)가 RFID 안테나의 영역안에 들어가면, 리더(200)는 상기 태그(100)의 정보를 얻기 위해 {REQUEST} 메시지를 보낸다(단계 S101).

상기 리퀘스트 메시지를 태그가 받으면, 태그(100)는 SFlag를 체크한다. 상기 체크 결과 SFlag가 참이면, 태그(100)는 메모리(120)에 저장되어 있는 랜덤수 R1과 카운트 C를 사용하여 제 1 메시지를 만든다.

상기 체크 결과, SFlag가 거짓이면 새로운 랜덤수 R1과 C를 생성하여 SFlag를 참으로 만든 후, 다음과 같은 제 1 메시지를 만들어 리더(200)를 통해 서버(310)로 전송한다. 상기 서버(310)로 전송하는 제 1 메시지는 다음과 같다.

{HID<- H(ID||C), HCWD<- H(R1||CWD), XR1<- ID $\oplus$ R1}

상기 메시지에서 ||는 입력 비트의 OR연산으로, 두 입력 비트가 모두 0일 때 0을 출력한다. $\oplus$는 입력 비트의 XOR연산으로, 두 입력 비트가 다르면 1을 출력하고, 같으면 0을 출력한다.

따라서 HID는 ID와 C의 OR연산을 통해 나온 값을 해싱함수로 계산한 값이고, HCWD는 R1과 CWD의 OR연산을 통해 나온 값을 해싱함수로 계산한 값이다. XR1은 ID와 R1의 XOR연산을 통해 나온 값이다(단계 S102~106).

상기 제 1 메시지를 전송받은 데이터베이스 서버(310)는 상기 메시지의 HID를 사용하여 ID와 CWD의 후보를 추출해내고, XR1⊕(후보 ID)를 계산하여 후보 R1을 얻어낸 후, (후보 R1)⊕(후보 CWD)를 계산한다.

상기 계산된 값과 상기 태그(100)에서 전송받은 메시지의 HCWD의 값이 동일한지를 확인하여 상기 태그(100)의 실제 ID를 찾아낸다(단계 S107).

여기서 상기 서버(310)가 상기 태그(100)의 ID를 찾지 못하면, 상기 서버(310)는 제 1 메시지를 공격으로 간주하고 무시하며, 상기 서버(310)가 ID를 찾으면, 서버(310)는 0과 1의 n비트를 가지는 새로운 랜덤수 R2를 생성한 후, 다음과 같은 제 2 메시지를 계산하여 태그(100)에게 전송한다.

{HR<- H(R1||R2), XR2<- ID ⊕R2}

HR은 상기 태그(100)가 생성한 랜덤수인 R1과 R2의 OR연산을 통해 나온 값을 해싱함수로 계산한 값이고, XR2는 ID와 R2의 XOR연산을 통해 나온 값이다(단계 S108~S111).

태그(100)는 상기 제 2 메시지를 받으면 상기 태그(100)의 필드인 THR_COUNT를 증가시키고, ID와 상기 제 2 메시지의 XR2의 XOR 연산한 후, R1과 OR연산한 값을 해싱함수로 계산한 값인 H(R1||(ID ⊕XR2))이 상기 전송된 메시지의 HR과 일치하는지 체크한다.

상기 체크 결과 H(R1||(ID ⊕XR2))과 HR이 일치하면 상기 태그(100)는 {CWD} 메시지를 서버(310)에게 전송한다. 서버(310)는 CWD가 올바르다면 ID와 CWD를 새롭 게 갱신한다. 태그(100)는 메시지를 보낸 후, ID와 CWD를 새롭게 갱신한 후, 상기 태그(100)는 SFlag를 false로 만들고, 상기 서버(310)는 새로운 ID를 위한 슬롯을 다시 준비한다.

여기서, CWD는 이전 세션의 랜덤수인 R1과 R2로 구성된다. 이것은 i가 현재 세션을 나타내고, i-1이 이전 세션을 의미할 때 CWDi= R1i⊕R2i-1 와 같고 또한, IDi = IDi-1⊕R1i-1⊕R2i-1 을 나타낸다.

상기 체크 결과 H(R1||(ID ⊕XR2))과 HR이 일치하지 않거나, 태그(100)가 거절할 어떠한 이유가 있다면, 태그(100)는 THR_COUNT가 THR_MAX에 다다를 때까지 다른 메시지를 기다려야한다. THR_COUNT가 THR_MAX에 도달하면, 태그(100)는 SFlag를 거짓으로 만들고, 리더(200)에 의해 세션이 열리기 전까지 모든 메시지를 무시한다(단계 S112~S117).

도 7는 RFID에서 태그(100)와 서버(310) 사이의 또 다른 인증과정을 나타낸 개략도이다.

태그(100)의 데이터를 리더(200)가 필요로 하면, 상기 리더(200)는 {REQUEST} 메시지를 상기 태그(100)로 전송한다(단계 S10).

상기 {REQUEST} 메시지를 받은 태그(100)는 자신의 상태를 체크하는 SFlag를 확인한 후, 랜덤수를 이용하여 제 1 메시지를 생성하고 리더(200)를 통해 데이터베이스(300)로 전송한다(단계 S20).

상기 제 1 메시지를 전송받은 데이터베이스 서버(310)는 상기 태그(100)의 인증을 위해 ID를 데이터베이스(300)에서 검색한 후, 새로운 랜덤수를 이용하여 제 2 메시지를 생성하고 리더(200)를 통해 상기 태그(100)로 전송한다(단계 S30).

상기 제 2 메시지를 전송받은 태그(100)는 현재 세션의 시도 횟수를 저장하고 있는 THR_COUNT를 체크하여 세션이 종료되는 THR_MAX가 될 때까지 제 2 메시지를 전송받으며, 상기 전송받은 제 2 메시지와 비교하여 상기 데이터베이스(300)를 인증한다.

상기 단계에서 데이터베이스(300)를 인증하면, 상기 서버(310)에 {CWD} 메시지를 보내 인증이 완료되었음을 알리며, 인증이 되지 않으면 {false} 메시지를 보내어 단계 S30으로 되돌아간다(단계 S40).

이와 같은 과정으로 구현되는 태그와 데이터베이스 사이의 또 다른 인증방법을 도 8의 흐름도와 함께 자세히 설명한다.

태그(100)의 데이터를 리더(200)가 필요로 하면, 리더(200)는 {REQUEST} 메시지를 태그(100)로 전송한다(단계 S201).

상기 {REQUEST} 메시지를 태그(100)가 받으면, 상기 태그(100)는 SFlag를 체크한다. 상기 체크 결과 SFlag가 참이면, 태그(100)는 메모리(110)에 저장 되어있는 랜덤수인 R1과 카운트 C를 사용하여 제 1 메시지를 만들고, 상기 체크 결과, SFlag가 거짓이면 새로운 랜덤수 R1과 C를 생성하고 SFlag를 참으로 만든 후, 제 1 메시지를 만들어 리더(200)를 통해 데이터베이스 서버(310)로 전송한다. 데이터베이스 서버(310)로 전송하는 제 1 메시지는 다음과 같다.

{HID<- H(ID||C), XR1<- ID $\oplus$R1}

상기 제 1 메시지에서 HID는 ID와 C의 OR연산을 통해 나온 값을 해싱함수로 계산한 값이고, XR1은 ID와 R1의 XOR 연산을 통해 나온 값이다(단계 S202~S206)

상기 제 1 메시지를 전송받은 서버(310)는 상기 메시지의 HID를 사용하여 ID와 CWD의 후보를 추출해내고, XR1$\oplus$(후보 ID)를 계산하여 후보 R1을 얻어낸다. 여기서, 어떠한 후보도 추출해낼 수 없다면 서버(310)는 이를 공격으로 간주하고 무시한다(단계 S208, S209).

상기 서버(310)는 ID, CWD, R1의 후보들 중에 하나를 선택한 후, 새로운 랜덤수 R2를 생성하고, 다음과 같은 제 2 메시지를 계산하여 태그(100)에게 전송한다.

{HR<- H(R1||R2), XR2<- ID $\oplus$R2}

HR은 R1과 R2의 OR연산을 통해 나온 값을 해싱함수로 계산한 값이고, XR2는 ID와 R2의 XOR연산한 값이다(단계 S210~S212).

상기 제 2 메시지를 태그(100)가 받으면, THR_COUNT를 증가시키고, H(R1||ID $\oplus$XR2)가 상기 제 2 메시지의 HR과 일치하는지 체크한다. 상기 체크결과, 일치하면 태그(100)는 {CWD}를 서버(310)에게 전송한다.

상기 태그(100)와 서버(310)는 해당 ID와 CWD를 새롭게 갱신한 후, 태그(100)는 SFlag를 거짓으로 만들고, 서버(310)는 데이터베이스(300)의 구조인 슬롯의 기본값인 H(ID||C)를 위하여 해쉬 공간을 준비한다.

여기서, CWD는 이전 세션의 R1과 R2로 구성된다. 이것은 i가 현재 세션을 나타내고, i-1이 이전 세션을 의미할 때 $CWDi= R1i-1 \oplus 2i-1 (\mathrm{mod}\ 2^n)$와 같고 또한, IDi = IDi-1$\oplus$R1i-1$\oplus$R2i-1 을 나타낸다.

태그(100)가 상기 {HR<- H(R1||R2), XR2<- ID $\oplus$R2} 메시지가 올바르지 않거나, 상기 태그(100)가 거절할 어떠한 이유가 있다면, {false} 메시지를 데이터베이스 서버(310)에게 전송한다.

상기 태그(100)는 THR_COUNT가 만료되기까지 또 다른 제 2 메시지를 기다려야 하며 THR_COUNT가 THR_MAX에 도달하면, 태그(100)는 SFlag를 거짓으로 만들고, 다른 리더(200)에 의해서 세션이 열리기 전까지 모든 다음 메시지를 무시한다(단계 S213~S218).

도 9는 본 발명에 의한 세션 도중 요청 메시지를 처리하는 과정을 나타낸 개략도이다.

태그(100)는 이러한 요청 메시지에 대해서 이전에 전송하였던 메시지와 동일한 응답 메시지로 응답한다. 리더(200)에 의해 요청 메시지가 들어와 세션을 수행하는 도중에 또 다른 요청 메시지가 들어오면, 이전에 전송하였던 메시지와 동일한 응답 메시지로 응답한다.

이처럼 매 세션마다 랜덤수가 바뀌기 때문에 세션마다 메시지의 내용은 달라지나 동일한 세션에 대해서는 다른 요청 메시지가 들어와도 메시지가 바뀌지 않도록 하여 세션 도중 공격자의 요구에 따른 보안 취약성을 극복한다.

상술한 바와 같이, 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 또는 변형하여 실시할 수 있다.

발명의 효과

이상에서 설명한 바와 같이, 본 발명에 따른 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법은 매 세션마다 태그가 랜덤수를 생성함으로써 보안이 강화되었다.

또한, 특정 종류의 요구에 대해서 동일한 메시지를 반복적으로 전송하여 세션 도중의 공격자의 요구에 대한 처리를 명확히 하지 않는 부분과 이에 대한 구체적인 지원을 하지 않아 발생하는 보안적인 문제점을 극복하였다.

뿐만 아니라, 데이터베이스 서버의 해쉬값을 자르거나 하지 않아 보안성과 시스템의 안정성을 확보하였고, 공격자는 어떠한 경우라도 서버에게 해시 연산을 수행하게 할 수 없기 때문에 서버로의 서비스 거부 공격이 성공하기 힘들다.

따라서 본 발명과 같은 RFID 인증방법을 이용하여 보다 저렴하고 보안성이 우수한 RFID 시스템을 설계할 수 있어 RFID 시스템의 보편화에 도움이 되며, 보안이 필요한 인증 및 결제 시스템에 유용하게 사용될 수 있다.

(57) 청구의 범위

청구항 1.

메모리를 구비하고 있는 태그와 슬롯으로 구현된 데이터베이스와 상기 데이터베이스의 데이터를 처리하는 서버와 상기 태그와 상기 데이터베이스의 소통을 관리하는 리더로 구성되는 RFID의 인증방법에 있어서,

인증을 위한 세션을 시작하기 위해 상기 리더가 상기 태그에게 리퀘스트 메시지를 요청하는 단계;

상기 요청 메시지를 받은 태그가 랜덤수를 이용하여 예측불가능한 제 1 메시지를 계산한 후, 서버에게 전송하는 단계;

상기 제 1 메시지를 받은 서버가 또 다른 랜덤수를 이용하여 제 2 메시지를 계산하여 전송하는 단계; 및

상기 태그가 상기 제 2 메시지를 확인하고 상기 서버에 성공메시지를 보내면, 상기 태그와 서버가 다음 세션을 위해 초기화하는 단계;

를 포함하여 이루어지는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 2.

제 1 항에 있어서,

인증을 위한 메시지의 예측 불가능성을 보장하기 위해 태그가 랜덤수를 생성하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 3.

제 1 항에 있어서,

상기 태그는 자신의 상태를 알 수 있는 내부 변수를 사용하여 참 또는 거짓에 따라, 참인 경우 메모리에 저장된 랜덤수를 사용하고, 거짓인 경우 랜덤수를 생성하여 사용하고 이를 다시 메모리에 저장하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 4.

제 3 항에 있어서,

상기 내부변수는 태그 내에 전원이 들어오면 거짓으로 초기화 되었다가, 메모리에 랜덤수를 저장하면 참으로 바뀌고, 한 세션동안 시도된 횟수를 나타내는 한계값 변수가 최고값에 도달하였거나, 인증 세션이 올바르게 끝났을 경우 다시 거짓 상태로 바뀌는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 5.

제 4 항에 있어서,

확인 메시지를 처리하기 위해 타이머를 사용하지 않고 상기 한계값 변수를 사용하며, 상기 한계값 변수는 최고값에 도달하여 만료되면, 상기 태그는 이를 공격으로 간주하고 세션을 닫는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 6.

제 1 항에 있어서,

상기 태그가 {HID<- H(ID||C), HCWD<- H(R1||CWD), XR1<- ID ⊕R1} 메시지를 계산하여 전송하며, 상기 메시지에서 HID는 ID와 카운터인 C의 OR연산을 통해 나온 값을 해싱함수로 계산한 값이고, 여기서, HCWD는 랜덤수 R1과 CWD의 OR연산을 통해 나온 값을 해싱함수로 계산한 값이며, XR1은 ID와 랜덤수 R1을 XOR연산을 통해 나온 값임을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 7.

제 6 항에 있어서,

상기 서버는 상기 태그에 의해 생성된 메시지의 유효성을 판단하고 데이터베이스를 검색하며, 상기 태그의 ID를 확인하기 위해 상기 태그의 필드인 CWD를 사용하여 실제 ID와 CWD를 찾아내고, 상기 ID와 CWD를 찾지 못하면 공격으로 간주하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 8.

제 1 항에 있어서,

상기 서버는 상기 태그에게 인증받기 위해 {HR<- H(R1||R2), XR2<- ID ⊕R2} 제 2 메시지를 생성하여 전송하며, 여기서, HR은 랜덤수 R1과 랜덤수 R2의 OR연산한 값을 해싱함수로 계산한 값이고, XR2는 ID와 R2의 XOR연산한 값임을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 9.

제 8 항에 있어서,

상기 태그는 상기 서버로부터 제 2 메시지를 수신할 때, 상기 한계값 변수를 증가시키며, 상기 제 2 메시지가 ID와 XR2의 XOR연산한 값과 랜덤수인 R1과 OR연산한 값을 해싱함수로 계산한 값인 H(R1||(ID ⊕XR2))와 일치하면, {CWD} 메시지를 생성하여 전송하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 10.

제 6 항에 있어서,

상기 서버는 상기 태그가 생성하는 제 1 메시지를 처리하기 위해 모든 가능한 슬롯을 준비하며, 인증이 끝나면, 상기 서버가 슬롯을 파기하고 초기화하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 11.

제 6 항에 있어서,

상기 슬롯은 주소, ID, CWD 필드를 가지고 있으며, 주소의 충돌을 해결하기 위해 동일한 주소를 가진 슬롯을 링크로 이어놓는 단계를 포함하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 12.

제 6 항에 있어서,

상기 태그는 세션의 실행 도중 다른 리더의 요청 메시지가 들어오면, 이를 처리하기 위해 이전에 전송하였던 메시지와 동일한 응답 메시지를 전송하여 보안성을 높인 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 13.

제 1 항 내지 제 12 항 중 어느 한 항에 있어서,

인증을 위한 세션을 시작하는 것은 리더이나, 세션을 닫을 수 있는 권한은 오로지 태그에게 존재하여 선점적이거나 비선점적인 문제를 해결하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 14.

메모리를 구비하고 있는 태그와 슬롯으로 구현된 데이터베이스와 상기 데이터베이스의 데이터를 처리하는 서버와 상기 태그와 상기 데이터베이스의 소통을 관리하는 리더로 구성되는 RFID의 또 다른 인증방법에 있어서,

인증을 위한 세션을 시작하기 위해 상기 리더가 상기 태그에게 리퀘스트 메시지를 요청하는 단계;

상기 요청 메시지를 받은 태그가 메시지의 예측불가능성을 위해 랜덤수를 이용하여 제 1 메시지를 계산한 후, 서버에게 전송하는 단계;

상기 제 1 메시지를 받은 서버가 태그의 ID를 찾을 때까지 또 다른 랜덤수를 이용하여 제 2 메시지를 생성하고 전송하는 단계; 및

상기 태그가 상기 제 2 메시지를 확인하고 상기 서버에 확인 메시지를 보내면, 상기 태그와 서버가 다음 세션을 위해 초기화하는 단계;

를 포함하여 이루어지는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 또 다른 인증방법.

청구항 15.

제 14 항에 있어서,

인증을 위한 메시지의 예측 불가능성을 보장하기 위해 태그가 랜덤수를 생성하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 16.

제 14 항에 있어서,

상기 태그는 자신의 상태를 알 수 있는 내부 변수를 사용하여 참 또는 거짓에 따라, 참인 경우 메모리에 저장된 랜덤수를 사용하고, 거짓인 경우 랜덤수를 생성하여 사용하고 이를 다시 메모리에 저장하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 17.

제 16 항에 있어서,

상기 내부변수는 태그 내에 전원이 들어오면 거짓으로 초기화 되었다가, 메모리에 랜덤수를 저장하면 참으로 바뀌고, 한 세션동안 시도된 횟수를 나타내는 한계값 변수가 최고값에 도달하였거나, 인증 세션이 올바르게 끝났을 경우 다시 거짓 상태로 바뀌는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 18.

제 17 항에 있어서,

확인 메시지를 처리하기 위해 타이머를 사용하지 않고 상기 한계값 변수를 사용하며, 상기 한계값 변수는 최고값에 도달하여 만료되면, 상기 태그는 이를 공격으로 간주하고 세션을 닫는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 19.

제 14 항에 있어서,

상기 태그가 {HID<- H(ID||C), XR1<- ID $\oplus$R1} 제 1 메시지를 계산하여 전송하며, 여기서, HID는 ID와 카운터인 C의 OR연산한 값을 해싱함수로 계산한 값이고, XR1은 ID와 랜덤수 R1을 XOR 연산한 값임을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 20.

제 19 항에 있어서,

상기 서버는 상기 태그에 의해 생성된 제 1 메시지를 이용하여 ID, CWD, R1의 후보를 추출해내고, {HR<- H(R1||R2), XR2<- ID $\oplus$R2} 제 2메세지를 유효한 ID와 CWD를 찾을 때까지 반복적으로 계산하여 상기 태그에게 전송하며, 여기서, HR은 랜덤수 R1과 R2의 OR연산한 값을 해싱함수로 계산한 값이고, XR2는 ID와 랜덤수 R2의 XOR연산한 값임을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 21.

제 20 항에 있어서,

상기 태그가 상기 서버로부터 받은 제 2 메시지가 ID와 상기 제 2 메시지의 XR2의 XOR연산한 값과 랜덤수 R1을 OR연산한 값을 해싱함수로 계산한 값인 H(R1||(ID⊕XR2))와 일치하면, 상기 데이터베이스 서버에 {CWD}또는 {false}를 생성하여 전송하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 22.

제 21 항에 있어서,

상기 서버가 태그에 전송하는 {CWD} 메시지는 어떠한 방법으로 가공하지 않고 평문형태로 전송하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 23.

제 19 항에 있어서,

상기 서버는 상기 태그가 생성하는 제 1 메시지를 처리하기 위해 모든 가능한 슬롯을 준비하며, 인증이 끝나면, 상기 서버가 슬롯을 파기하고 초기화하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 24.

제 19 항에 있어서,

상기 슬롯은 주소, ID, CWD 필드를 가지고 있으며, 주소의 충돌을 해결하기 위해 동일한 주소를 가진 슬롯을 링크로 이어놓는 단계를 포함하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

청구항 25.

제 19 항에 있어서,

상기 태그는 세션의 실행 도중 다른 리더의 요청 메시지가 들어오면, 이를 처리하기 위해 이전에 전송하였던 메시지와 동일한 응답 메시지를 전송하여 보안성을 높인 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

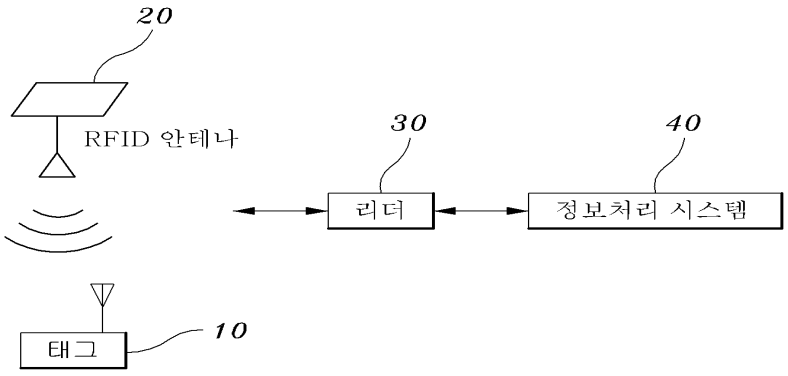
청구항 26.

제 14 항 내지 제 25 항 중 어느 한 항에 있어서,

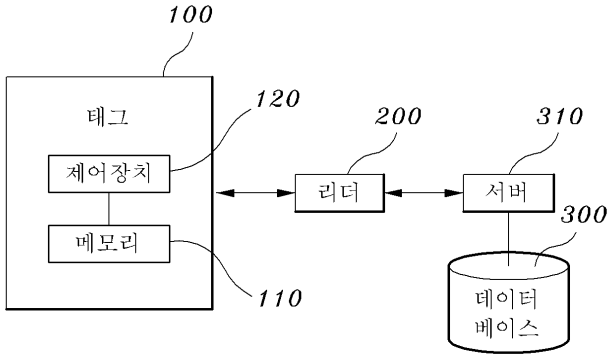
인증을 위한 세션을 시작하는 것은 리더이나, 세션을 닫을 수 있는 권한은 오로지 태그에게 존재하여 선점적이거나 비선점적인 문제를 해결하는 것을 특징으로 하는 위치 추적과 서비스 거부 공격에 강한 RFID 인증방법.

도면

도면1



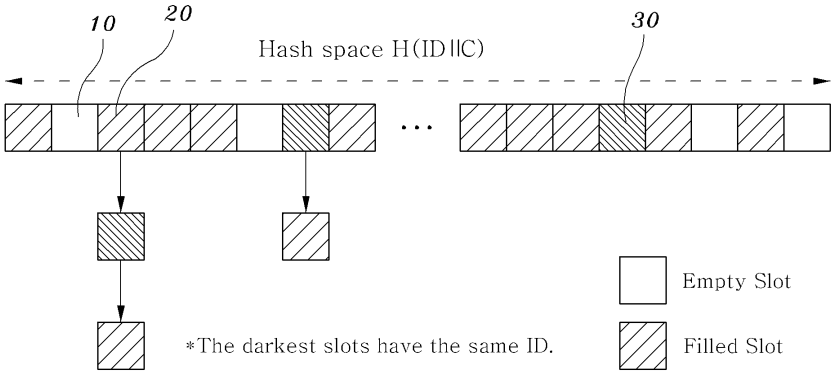
도면2



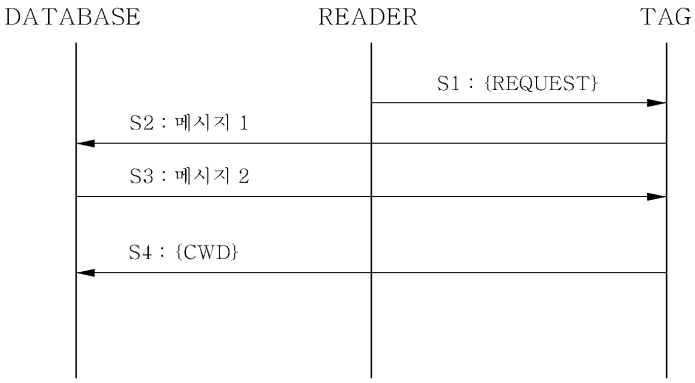
도면3

필드지시자	필드 영어의미
SFlag	Session Flag
IP	IDentifier
CWD	Confirn word
R1	Random nonce 1
R2	Random nonce 2
C	Counter
THR_COUNT	THReshold COUNTer
THR_MAX	THReshold MAXimum
UR	User Reserved memory

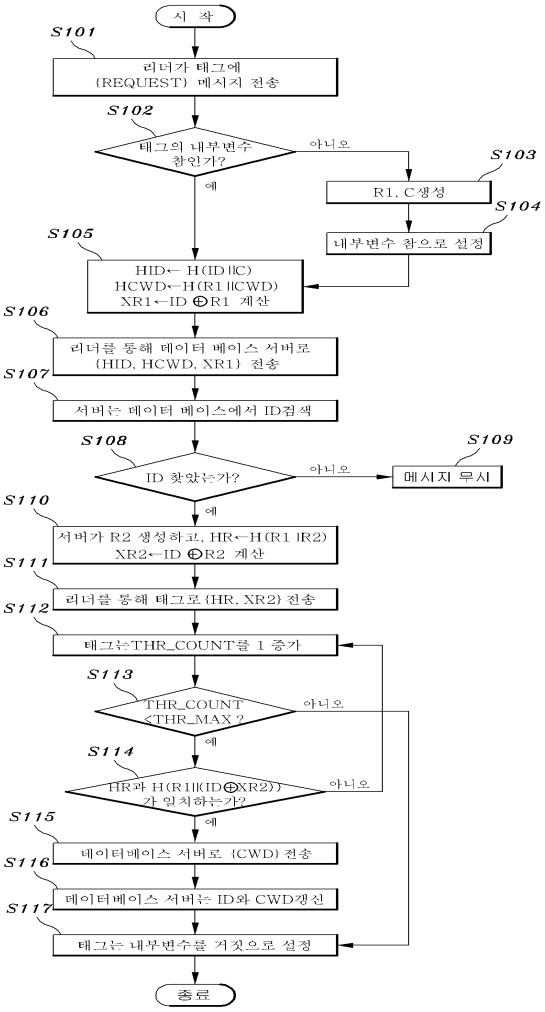
도면4


10
20
30
Hash space H(ID||C)
Empty Slot
*The darkest slots have the same ID.
Filled Slot

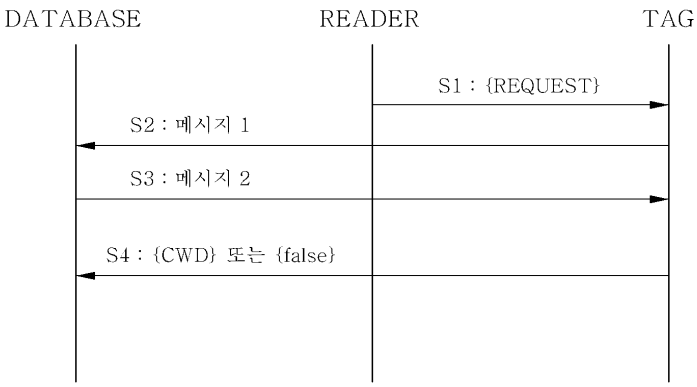
도면5


DATABASE
READER
TAG
S1 : {REQUEST}
S2 : 메시지 1
S3 : 메시지 2
S4 : {CWD}

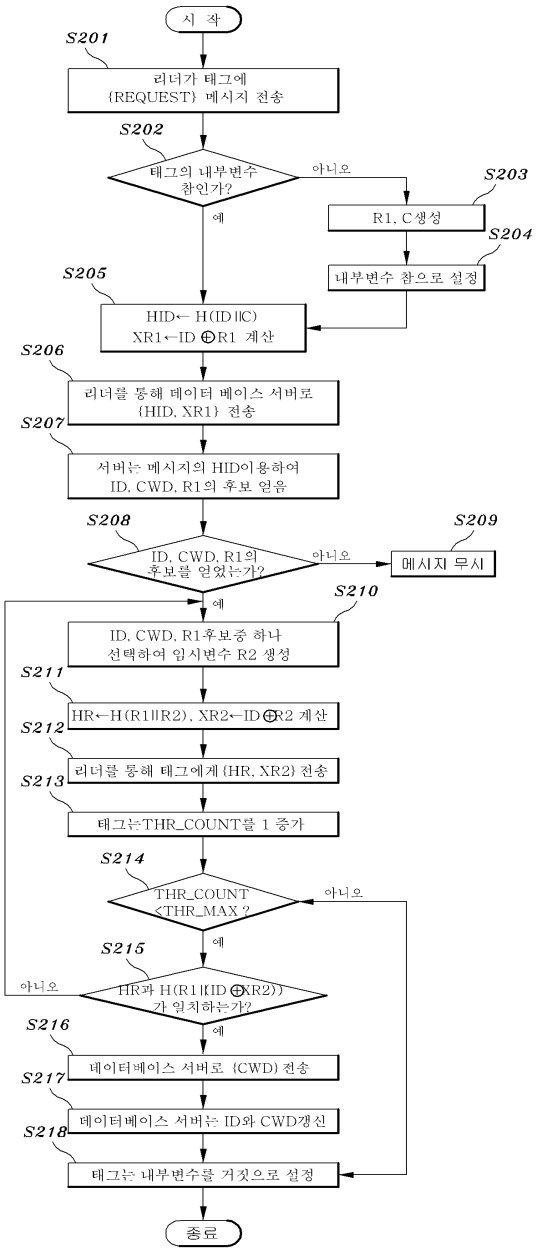
도면6


시 작
S101
리더가 태그에 {REQUEST} 메시지 전송
S102
태그의 내부변수 참인가?
아니오
예
S103
R1, C생성
S104
내부변수 참으로 설정
S105
HID←H(ID||C)
HCWD←H(R1||CWD)
XR1←ID ⊕R1 계산
S106
리더를 통해 데이터 베이스 서버로 {HID, HCWD, XR1} 전송
S107
서버는 데이터 베이스에서 ID검색
S108
ID 찾았는가?
아니오
S109
메시지 무시
예
S110
서버가 R2 생성하고, HR←H(R1 IR2)
XR2←ID ⊕R2 계산
S111
리더를 통해 태그로 {HR, XR2} 전송
S112
태그는THR_COUNT를 1 증가
S113
THR_COUNT <THR_MAX ?
아니오
예
S114
HR과 H(R1||(ID⊕XR2)) 가 일치하는가?
아니오
예
S115
데이터베이스 서버로 {CWD} 전송
S116
데이터베이스 서버는 ID와 CWD갱신
S117
태그는 내부변수를 거짓으로 설정
종료

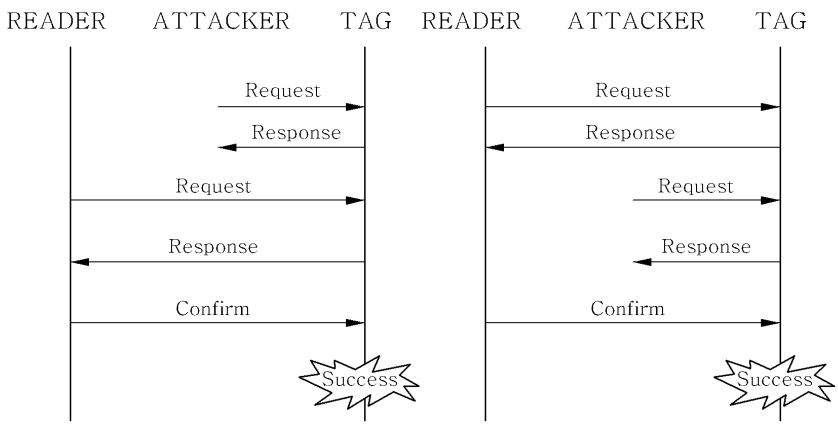
도면7


DATABASE
READER
TAG
S1 : {REQUEST}
S2 : 메시지 1
S3 : 메시지 2
S4 : {CWD} 또는 {false}

도면8


시 작
S201
리더가 태그에 {REQUEST} 메시지 전송
S202
태그의 내부변수 참인가?
아니오
예
S203
R1, C생성
S204
내부변수 참으로 설정
S205
HID← H(ID||C)
XR1←ID ⊕R1 계산
S206
리더를 통해 데이터 베이스 서버로 {HID, XR1} 전송
S207
서버는 메시지의 HID이용하여 ID, CWD, R1의 후보 얻음
S208
ID, CWD, R1의 후보를 얻었는가?
아니오
S209
메시지 무시
예
S210
ID, CWD, R1후보중 하나 선택하여 임시변수 R2 생성
S211
HR←H(R1||R2), XR2←ID⊕R2 계산
S212
리더를 통해 태그에게 {HR, XR2} 전송
S213
태그는THR_COUNT를 1 증가
S214
THR_COUNT <THR_MAX ?
아니오
예
S215
HR과 H(R1||(ID ⊕XR2)) 가 일치하는가?
아니오
예
S216
데이터베이스 서버로 {CWD} 전송
S217
데이터베이스 서버는 ID와 CWD갱신
S218
태그는 내부변수를 거짓으로 설정
종료

도면9


READER
ATTACKER
TAG
Request
Response
Request
Response
Confirm
Success
READER
ATTACKER
TAG
Request
Response
Request
Response
Confirm
Success