(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0101260
(43) 공개일자 2012년09월13일

(51) 국제특허분류(Int. Cl.)
G06K 17/00 (2006.01) *H04W 12/06* (2009.01)
H04B 5/02 (2006.01)
(21) 출원번호 10-2011-0019460
(22) 출원일자 2011년03월04일
심사청구일자 2011년03월04일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
염흥열
충청남도 아산시 신창면 읍내리 순천향대학교 M114
여돈구
충청남도 아산시 신창면 읍내리 순천향대학교 M114
이상래
충청남도 아산시 신창면 읍내리 순천향대학교 M114
(74) 대리인
특허법인 정안

전체 청구항 수 : 총 7 항

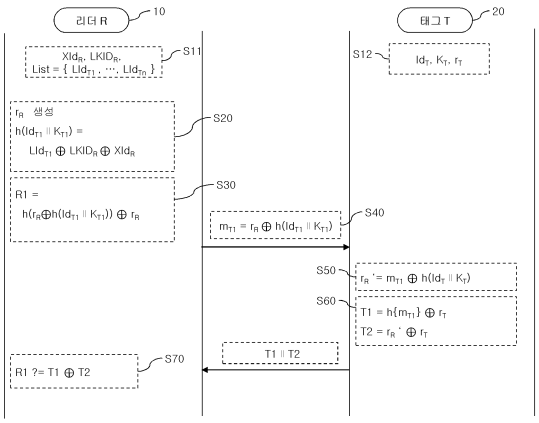
(54) 발명의 명칭 **모바일 리더의 태그 리스트 재사용을 방지하는 저비용 ＲＦＩＤ 태그 검색방법**

(57) 요 약

리더가 태그의 인증키로 다수의 태그 중에서 특정 태그를 인증하여 검색하되, 리더가 태그의 인증키 정보를 암호화된 상태로 보유하게 하는 RFID 태그 검색방법에 있어서, (a) 리더는 XOR연산으로 암호화된 태그의 인증키를 리스트로 저장하는 단계; (b) 리더는 검색하고자 하는 태그(이하 검색 태그)의 인증키(이하 제1 인증키)를 복호화하고, 랜덤값(이하 제1 랜덤값)을 생성하는 단계; (c) 리더는 제1 인증키에 제1 랜덤값을 XOR 연산하고 해쉬하고, 다시 제1 랜덤값으로 XOR연산하여 검증 메시지를 생성하는 단계; (d) 리더는 제1 랜덤값과 제1 인증키와의 XOR 연산으로 요청 메시지를 생성하여 전송하는 단계; (e) 태그는 요청 메시지를 수신하여, 자신의 인증키(이하 제2 인증키)로 XOR 연산하여 랜덤값(이하 제2 랜덤값)을 추출하는 단계; (f) 태그는 요청 메시지 및 제2 랜덤값을 각각 자신의 랜덤값(이하 제3 랜덤값)으로 XOR연산하여 제1 및 제2 응답 메시지를 생성하고, 제1 및 제2 응답 메시지를 리더로 전송하는 단계; 및, (g) 리더는 제1 및 제2 응답 메시지를 XOR연산하고, XOR 연산 결과와 검증 메시지와 대비하여 검색 태그를 인증하는 단계를 포함하는 구성을 마련한다.

상기와 같은 방법에 의하여, 리더가 태그의 인증키 정보를 암호화된 상태로 보유하게 함으로써, 태그 리스트의 재활용을 방지하고, 이를 통해 보안이 향상된 태그 리스트를 제공하고, 모바일 리더 기반의 RFID 환경에 적합한 동적 ID 기반의 효율적인 태그 검색 프로토콜을 제공할 수 있다.

대 표 도 - 도4



특허청구의 범위

청구항 1

리더가 다수의 태그 중에서 특정 태그를 검색하는 RFID 태그 검색방법에 있어서,

(a) 상기 리더는 XOR연산으로 암호화된 태그의 인증키를 리스트로 저장하는 단계;

(b) 상기 리더는 검색하고자 하는 태그(이하 검색 태그)의 인증키(이하 제1 인증키)를 복호화하고, 랜덤값(이하 제1 랜덤값)을 생성하는 단계;

(c) 상기 리더는 상기 제1 인증키에 상기 제1 랜덤값을 XOR 연산하고 해쉬하고, 다시 상기 제1 랜덤값으로 XOR 연산하여 검증 메시지를 생성하는 단계;

(d) 상기 리더는 상기 제1 랜덤값과 상기 제1 인증키와의 XOR 연산으로 요청 메시지를 생성하여 전송하는 단계;

(e) 상기 태그는 상기 요청 메시지를 수신하여, 자신의 인증키(이하 제2 인증키)로 XOR 연산하여 랜덤값(이하 제2 랜덤값)을 추출하는 단계;

(f) 상기 태그는 상기 요청 메시지를 해쉬한 값 및 상기 제2 랜덤값을 각각 자신의 랜덤값(이하 제3 랜덤값)으로 XOR연산하여 제1 및 제2 응답 메시지를 생성하고, 상기 제1 및 제2 응답 메시지를 상기 리더로 전송하는 단계; 및,

(g) 상기 리더는 상기 제1 및 제2 응답 메시지를 XOR연산하고, XOR 연산 결과와 상기 검증 메시지와 대비하여 상기 검색 태그를 인증하는 단계를 포함하는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 2

리더가 다수의 태그 중에서 특정 태그를 검색하는 RFID 태그 검색방법에 있어서,

(a) 상기 리더는 XOR연산으로 암호화된 태그의 인증키를 리스트로 저장하는 단계;

(b) 상기 리더는 검색하고자 하는 태그(이하 검색 태그)의 인증키(이하 제1 인증키)를 복호화하고, 랜덤값(이하 제1 랜덤값)을 생성하는 단계;

(c) 상기 리더는 상기 제1 인증키에 상기 제1 랜덤값을 XOR 연산하고 상기 제1 인증키를 연접한 후 해쉬하고, 다시 상기 제1 랜덤값으로 XOR연산하여 검증 메시지를 생성하는 단계;

(d) 상기 리더는 상기 제1 랜덤값과 상기 제1 인증키와의 XOR 연산으로 요청 메시지를 생성하여 전송하는 단계;

(e) 상기 태그는 상기 요청 메시지를 수신하여, 자신의 인증키(이하 제2 인증키)로 XOR 연산하여 랜덤값(이하 제2 랜덤값)을 추출하는 단계;

(f) 상기 태그는 상기 요청 메시지와 상기 제2 인증키와 연접한 값을 해쉬한 값, 및, 상기 제2 랜덤값을 각각 자신의 랜덤값(이하 제3 랜덤값)으로 XOR연산하여 제1 및 제2 응답 메시지를 생성하고, 상기 제1 및 제2 응답 메시지를 상기 리더로 전송하는 단계; 및,

(g) 상기 리더는 상기 제1 및 제2 응답 메시지를 XOR연산하고, XOR 연산 결과와 상기 검증 메시지와 대비하여 상기 검색 태그를 인증하는 단계를 포함하는 것을 RFID 태그 검색방법.

청구항 3

제1항 또는 제2항에 있어서,

상기 제1 또는 제2 인증키는 태그의 아이디 및 비밀키를 해쉬하여 생성되는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 4

제1항 또는 제2항에 있어서,

상기 제1 인증키는 리스트의 인증키와 XOR연산에 의해 암호화 또는 복호화되고, 상기 리스트의 인증키는 모든 태그의 인증키를 XOR연산하여 생성되는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 5

제3항에 있어서,

상기 제1 인증키는 추가적으로 상기 리더의 동적 아이디와 XOR 연산에 의해 암호화 또는 복호화되는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 6

제2항에 있어서,

상기 (c)단계에서, 마지막 제1 랜덤값으로 XOR연산시, 상기 제1 랜덤값을 중복하여 연접하여 XOR연산하고,

상기 (f)단계에서, 상기 제2 및 제3 랜덤값은 각각 중복하여 연접한 값으로 연산되는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 7

제1항 또는 제2항의 방법을 수행하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 리더가 태그의 인증키로 다수의 태그 중에서 특정 태그를 인증하여 검색하되, 리더가 태그의 인증키 정보를 암호화된 상태로 보유하게 하는 RFID 태그 검색방법에 관한 것이다.

[0002] 또한, 본 발명은 태그 리스트의 재활용을 방지함으로써 보안이 향상된 태그 리스트를 제공하고, 모바일 리더 기반의 RFID 환경에 적합한 동적 ID 기반의 효율적인 RFID 태그 검색방법에 관한 것이다.

배 경 기 술

[0003] 최근 일상에서 자유롭게 정보통신 기술을 이용하는 유비쿼터스 환경이 많이 구성되고 있다. 이러한 유비쿼터스 환경을 구성하는 기술 중 RFID/USN 기술이 많은 관심을 받고 있다. RFID/USN 시스템과 관련된 최근 연구들은 RFID와 관련된 다양한 취약성 및 프라이버시 문제를 제기하고 있으며, 리더와 태그 간의 안전한 통신 및 프라이버시의 보호를 위한 RFID 인증 프로토콜 및 태그 검색 프로토콜의 연구가 활발하게 진행되고 있다. RFID 태그 검색 프로토콜은 리더 소유자가 찾고자하는 특정 태그의 위치를 판별하는데 사용된다.

[0004] 초기 RFID 시스템은 백엔드 서버, 리더, 태그로 나누어지며, 백엔드 서버와 리더는 유선구간으로 구성된다. 즉, 백엔드 서버와 리더 사이의 구간을 안전한 채널로 가정함으로써 정당한 리더만이 백엔드 서버로 접속할 수 있다. 유선 RFID 기반 환경에서도 보안성 향상 및 태그 인증 연산의 효율성을 증가시키기 위해 동적 ID 기반 RFID 상호 인증 프로토콜에 대한 연구가 활발히 진행되고 있다.

[0005] 최근 스마트폰 및 모바일 기기의 보급이 일반화되면서 무선 환경에서의 이동형 리더에 대한 연구가 지속되고 있다. 즉, 모바일 환경에서 이동형 리더 기반의 태그 검색 프로토콜들에 대한 연구가 진행되고 있다. 사용자는

RFID 리더칩이 내장된 휴대용 단말을 이용하여 물품 또는 위치에 부착된 태그를 읽고, 태그의 정보를 검색할 수 있다. 이동형 리더의 검색 기능을 지원하기 위해서는 일반적으로 백엔드 서버가 없는 독립된 환경에서 리더 소지자가 이동하면서 태그를 검색할 수 있어야 한다. 리더 소지자는 태그 검색 이전에 백엔드 서버로부터 리더 소지자의 권한에 따라 할당된 태그 리스트를 할당 받아야 한다.

[0006] 모바일 환경에서는 백엔드 서버와 리더의 실시간 통신을 보장할 수 없으므로, 리더는 백엔드 서버와 독립된 상황에서 검색하고자 하는 태그를 정확히 검색할 수 있는 능력을 보장할 수 있어야 한다. 기존의 유선환경의 RFID 인증 시스템에서는 주로 태그의 프라이버시 문제가 거론되었지만, 모바일 환경의 RFID 검색 시스템에서는 태그의 프라이버시는 물론 모바일 리더에 대한 프라이버시 문제 또한 해결해야 한다.

[0007] 한편, 최근 연구되고 있는 이동형 리더 기반의 태그 검색 프로토콜에서는 태그 및 리더의 프라이버시 문제를 고려하고 있지만, 리더가 기존에 소유하던 태그 리스트의 재활용문제는 고려하지 않고 있다. 즉, 특정 태그에 대한 검색 권한이 삭제되었음에도 기존에 소유하던 태그 리스트를 재활용함으로써 권한이 삭제된 태그를 검색할 수 있는 문제가 발생할 수 있다.

[0008] 정리하면, 모바일 환경에서의 RFID 시스템의 태그 검색 프로토콜의 요구사항은 다음과 같다. 즉, 백엔드 서버와 독립된 모바일 환경의 RFID 태그 검색 프로토콜은 다음의 요구사항을 만족해야 한다.

[0009] (1) 요구사항1은 태그 위조에 대한 안전성에 관한 것이다. 즉, 이동형 리더가 특정 태그의 검색을 요청할 경우, 정당한 태그 외의 어떠한 개체도 유효한 응답을 만들 수 없어야 한다.

[0010] (2) 요구사항2는 리더 위조에 대한 안전성이다. 이동형 리더가 특정 태그의 검색을 요청할 경우, 정당한 태그 리스트와 인증키를 소유하지 않은 개체는 유효한 쿼리를 만들 수 없어야 한다.

[0011] (3) 요구사항3은 태그 및 리더 프라이버시 노출에 대한 안전성이다. 리더의 쿼리 및 태그의 메시지로부터 통신에 참여하였던 각 개체를 구분할 수 없어야 한다. 태그의 위치추적(요구사항3-1) 및 리더의 위치추적(요구사항3-2), 후방향 위치추적(요구사항3-3)과 전방향 위치추적(요구사항3-4)에 안전해야 한다.

[0012] (4) 요구사항4는 동적 ID(아이디) 방식의 경우, 비동기화 발생에 대한 안전성에 관한 것이다. 동기화 방식의 RFID 검색 프로토콜에서 키 갱신이 이루어지는 경우, 검색 프로토콜 상의 메시지가 차단되어도 키 갱신이 성공적으로 이루어져야 한다.

[0013] 상기와 같은 요구사항들을 만족하기 위하여, 다음과 같은 공격 시나리오에 대하여 방어할 수 있어야 한다.

[0014] 즉, 요구사항1에 대한 공격 시나리오로서, 공격자는 태그 위조 공격을 통하여 자신이 리더가 찾고자 하는 정당한 태그인 것처럼 응답 메시지를 조작할 수 있다. 또한, 요구사항2에 대한 공격 시나리오로서, 공격자는 리더 위조 공격을 통하여 자신이 원하는 특정 태그를 검색하기 위해 정당한 리더인 것처럼 요청 메시지를 조작할 수 있다.

[0015] 요구사항3에 대한 공격 시나리오로서, 공격자는 리더의 요청 메시지 및 태그의 응답 메시지를 지속적으로 도청하고, 그 결과를 분석하거나 습득한 메시지를 재사용할 경우, 상황에 따라 태그의 위치추적(요구사항3-1), 리더의 위치추적(요구사항3-2), 후방향 위치추적(요구사항3-3) 및 전방향 위치추적(요구사항3-4)이 가능하다. 요구사항4에 대한 공격자 시나리오로서, 동적 ID 기반의 RFID 검색 시스템에서 통신에 참여한 개체의 갱신정보가 전달 도중에 차단 혹은 공격자에 의해 고의적으로 변조된 경우, 통신에 참여한 개체간의 비동기화가 발생할 수 있다.

[0016] 다음으로, 종래 기술에 의한 모바일 기반 RFID 태그 검색 시스템들의 내용과 그 기술의 안전성을 상기 요구사항 기준으로 설명한다.

[0017] 도 1a에서 보는 바와 같이, 선행기술 1은 고정 ID 방식 기반의 RFID 태그 검색 프로토콜이다. 상기 선행기술 1에서는 백엔드 서버에서 리더의 Id_R와 태그의 K_T를 저장하고 있다가 안전한 채널을 통해 리더에게 전달한다. 권한에 맞는 리스트를 수신한 Id_R은 자신이 검색하고 싶은 태그 Id_T의 리스트 정보 $h(Id_R \| K_T)$와 리더의 랜덤값 r_R 정보를 이용해 요청 메시지 ②를 생성한다. 태그는 메시지 ②의 정보와 자신이 소유한 정보 Id_R, K_T를 이용하여 리더가 자신의 Id_T정보를 알고 있는지 확인한다. 태그는 리더가 소지한 Id_T정보가 자신의 Id_T와 일치할 경우에만 메시지 ③을 전송하고, 불일치할 경우, 특정 확률에 따라 랜덤값을 생성하여 전달한다.

[0018] 상기 선행기술 1은 리더의 태그 리스트가 노출되지 않고 해쉬 연산의 충돌이 없다고 가정한다면, 리더의 Id_R이 노출되므로 리더의 위치추적이 가능하다. 또한, 응답 메시지 ③가 매번 변경되지만 Id_T가 불일치할 경우 태그는 확률에 따라 반응하므로, 공격자가 메시지 ②를 재사용하는 하는 시점에 공격자 주변에 태그 수가 적을 경우 공격에 성공할 수도 있다. 그러므로 요구사항2 및 요구사항3-2을 만족하지 못하며, 리더의 Id_R을 수집하는 경우 요구사항3-3, 요구사항3-4를 만족하지 못한다.

[0019] 다음으로, 도 1b에서 보는 바와 같이, 선행기술 2는 동적 ID 방식 기반의 RFID 태그 검색 프로토콜이다. 상기 선행기술 2에서는 시드값을 의사난수 함수를 이용하여 갱신한다. 과정 ②~④에서 리더가 전달한 시드값을 태그가 확인하고, 동일할 경우에 시드값을 증가하여 리더에게 전달한다. 과정 ⑤에서 리더는 자신의 시드값을 1증가하여 태그가 전달한 시드값과 비교한 후, 시드값이 증가한 경우에 해당 태그를 찾은 것으로 간주한다.

[0020] 상기 선행기술 2는 리더의 태그 리스트가 노출되지 않고 의사난수 생성에 충돌이 없다고 가정한다면, 공격자는 시드값만 노출되므로 요구사항2와 요구사항3을 만족한다고 볼 수 있다. 하지만, 태그로 가장한 공격자가 리더의 전달 메시지 ②의 시드값을 고의로 증가시켜 전달할 수 있으므로 요구사항1을 만족하지 못한다. 또한, 태그 측에서 시드값을 갱신하여 전달하므로, 메시지 ④가 공격자에 의해 고의적인 갱신되거나 정당한 태그의 응답 메시지가 리더로 전달되지 못하는 경우 비동기화가 발생하게 되므로 요구사항4를 만족하지 못한다.

[0021] 다음으로, 도 1c에서 보는 바와 같이, 선행기술 3은 수동형 태그에 적합하게 개발된 AES-128 암호 알고리즘을 사용한다. 상기 선행기술 3의 태그 리스트 정보는 리더의 Id_R과 Id_T를 연접하여 태그의 비밀키 K_T로 암호화되어 생성된다. 과정 ①~②에서 리더는 검색하고자 하는 리더의 Id_R와 랜덤값 r_R정보를 태그의 Id_T로 암호화하여 전달한다. 과정 태그는 수신한 정보를 자신의 Id_T를 이용하여 복호화 한다. 이후 Id_R과 Id_T정보를 K_T로 암호화하여 메시지 ④에 사용할 암호화 키 SK를 생성한다. 이후 SK를 이용하여 Id_T와 r_R을 암호화하고 $r_R \| r_R$을 XOR 연산하여 전달한다.

[0022] 상기 선행기술 3에서 리더는 백엔드 서버로부터 Id_T에 해당하는 SK를 사전에 전달 받는다. 리더의 태그 리스트가 노출되지 않는다고 가정하면, 전달되는 메시지 ②와 ④의 위/변조가 불가능하므로 요구사항1, 요구사항2 및 요구사항3을 만족한다고 볼 수 있다. 반면, 메시지 ④의 값 생성시 메시지 ②의 정보와 고정된 태그의 값만 이용되므로 메시지 ④값은 메시지 ②에 의존하게 된다. 공격자는 도청을 통해 메시지 ②의 값을 재사용할 수 있지만, 모든 태그가 동일한 방식 ③~④을 통해 응답하므로 어떤 태그를 찾고자 하는지 알 수 없게 된다.

[0023] 도 1d에서 보는 바와 같이, 선행기술 4는 동적 ID 기반 태그 검색 프로토콜 또한 수동형 태그에 적합하게 개발된 AES-128 암호 알고리즘을 사용한다. 한 가지 특징은 메시지의 최신성을 확인하기 위해 타임스탬프 값(δ)를 사용한다는 점이다. 리더와 태그는 각각 타임스탬프 값을 추가로 저장해야 한다. 리더는 백엔드 서버로부터 K_R, $E_{KT}(K_R \| ID_T)$, ID_T 정보로 이루어진 태그 리스트를 수신 받는다. 과정 ①에서 검색하고자 하는 태그의 정보와, 현재 타임스탬프 값을 암호화하여 태그에게 전달한다. 과정 ②에서 태그는 수신한 태그 정보를 복호화하여 정보가 일치하는 경우에만, 타임스탬프 값을 비교하여 메시지의 재전송 여부를 확인한다. 메시지의 최신성이 확인되면 타임스탬프 값을 및 다음 번에 사용할 태그 정보를 갱신하고, 과정 ③에서 갱신된 정보를 암호화 하여 전달한다. 과정 ④에서 이를 수신한 리더는 메시지를 복호화하고 메시지의 신선성을 확인한 이후 다음 번에 사용될 리스트 정보를 갱신한다.

[0024] 상기 선행기술 4의 메시지 ①이 태그의 비밀키로 암호화되어 전송되므로, 태그 리스트 정보와 암호화 키가 노출되지 않는다고 가정한다면 요구사항2는 만족한다. 또한, 메시지 ①의 K_R이 세션 마다 갱신되며, 갱신된 값이 응답 메시지 생성에 사용되므로 요청 및 응답 메시지 분석을 통한 추적이 불가능하므로 요구사항3-1, 요구사항3-2, 요구사항3-3을 만족한다고 볼 수 있다. 하지만, 상기 선행기술 4에서는 하나의 태그만 반응하므로 리더가 전송한 메시지 ①을 도청한 공격자가 다른 지역에서 대상 리더를 찾아낸다면, 태그의 정보가 갱신되므로 정당한 사용자는 태그를 찾을 수 없다. 그러므로 요구사항3-4를 만족한다고 볼 수 없다. 또한, 과정 ②에서 태그가 다음 세션의 비밀정보를 갱신한 이후에 메시지 ③을 전달하므로, 메시지 ③이 공격자에 의해 고의적인 갱신되거나 정당한 태그의 응답 메시지가 리더로 전달되지 못하는 경우 비동기화가 발생하게 되므로 요구사항4를 만족하지 못한다.

[0025] 결론적으로, 앞서 본 바와 같은 선행기술의 RFID 태그 검색 방법들은 태그 및 리더의 프라이버시 문제를 다루고 있지만, 리더가 기존에 소유하던 태그 리스트의 재활용함으로써 발생할 수 있는 문제점은 고려하지 않고 있다.

다시 말해, 특정 태그에 대한 권한이 삭제된 리더가 기존에 소지하던 태그 리스트를 재활용함으로써 권한이 삭제된 태그를 검색할 수 있는 문제가 발생할 수 있다.

[0026] 즉, 상기 선행기술들에서 사용되는 태그 리스트 정보는 리더 및 태그의 비밀정보로 이루어진다. 정적 ID 기반의 경우, 리더 혹은 태그의 고정된 ID 정보와 키값으로 생성되거나 고정된 대칭키 기반의 암호화키를 이용한다. 이와 같이 고정된 값을 이용하는 경우에는 랜덤값을 생성하여 전달되는 메시지를 변경함으로써 위치 추적 공격을 방지할 수 있다.

[0027] 동적 ID 기반의 경우에는 리더 혹은 태그의 동적 ID 정보와 키값으로 생성되거나 갱신 가능한 대칭키 기반의 암호화 키를 이용한다. 이와 같이 변경되는 값을 이용하는 경우 세션마다 태그 리스트 정보가 변경되어 추적 공격을 방지하거나 태그 리스트 정보의 노출에 따른 문제를 방지할 수 있다. 하지만, 일반적으로 태그 검색 프로토콜이 요청 및 응답의 2-Way 이루어지므로 응답 메시지의 손실이나 공격자에 의해 메시지가 차단되는 경우 비동기화가 발생할 수 있다. 또한, 기존의 동적 ID 기반의 방식은 태그 측에 다음과 같은 연산부하를 가져온다. 첫째, 태그가 리더를 인증하기 위한 연산이 요구된다. 둘째, 인증된 경우 정보를 갱신하기 위한 연산이 요구된다. 셋째, 갱신된 정보를 노출되지 않고 전달하기 위한 연산이 요구된다.

발명의 내용

해결하려는 과제

[0028] 본 발명의 목적은 상술한 바와 같은 문제점을 해결하기 위한 것으로, 태그 리스트의 재활용을 방지함으로써 보안이 향상된 태그 리스트를 제공하고, 모바일 리더 기반의 RFID 환경에 적합한 동적 ID 기반의 효율적인 RFID 태그 검색방법을 제공하는 것이다.

[0029] 또한, 본 발명의 목적은 리더가 태그의 인증키로 다수의 태그 중에서 특정 태그를 인증하여 검색하되, 리더가 태그의 인증키 정보를 암호화된 상태로 보유하게 하는 RFID 태그 검색방법을 제공하는 것이다.

과제의 해결 수단

[0030] 상기 목적을 달성하기 위해 본 발명은 리더가 다수의 태그 중에서 특정 태그를 검색하는 RFID 태그 검색방법에 관한 것으로서, (a) 상기 리더는 XOR연산으로 암호화된 태그의 인증키를 리스트로 저장하는 단계; (b) 상기 리더는 검색하고자 하는 태그(이하 검색 태그)의 인증키(이하 제1 인증키)를 복호화하고, 랜덤값(이하 제1 랜덤값)을 생성하는 단계; (c) 상기 리더는 상기 제1 인증키에 상기 제1 랜덤값을 XOR 연산하고 해쉬하고, 다시 상기 제1 랜덤값으로 XOR연산하여 검증 메시지를 생성하는 단계; (d) 상기 리더는 상기 제1 랜덤값과 상기 제1 인증키와의 XOR 연산으로 요청 메시지를 생성하여 전송하는 단계; (e) 상기 태그는 상기 요청 메시지를 수신하여, 자신의 인증키(이하 제2 인증키)로 XOR 연산하여 랜덤값(이하 제2 랜덤값)을 추출하는 단계; (f) 상기 태그는 상기 요청 메시지를 해쉬한 값 및 상기 제2 랜덤값을 각각 자신의 랜덤값(이하 제3 랜덤값)으로 XOR연산하여 제1 및 제2 응답 메시지를 생성하고, 상기 제1 및 제2 응답 메시지를 상기 리더로 전송하는 단계; 및, (g) 상기 리더는 상기 제1 및 제2 응답 메시지를 XOR연산하고, XOR 연산 결과와 상기 검증 메시지와 대비하여 상기 검색 태그를 인증하는 단계를 포함하는 것을 특징으로 한다.

[0031] 또한, 본 발명은 리더가 다수의 태그 중에서 특정 태그를 검색하는 RFID 태그 검색방법에 관한 것으로서, (a) 상기 리더는 XOR연산으로 암호화된 태그의 인증키를 리스트로 저장하는 단계; (b) 상기 리더는 검색하고자 하는 태그(이하 검색 태그)의 인증키(이하 제1 인증키)를 복호화하고, 랜덤값(이하 제1 랜덤값)을 생성하는 단계; (c) 상기 리더는 상기 제1 인증키에 상기 제1 랜덤값을 XOR 연산하고 상기 제1 인증키를 연접한 후 해쉬하고, 다시 상기 제1 랜덤값으로 XOR연산하여 검증 메시지를 생성하는 단계; (d) 상기 리더는 상기 제1 랜덤값과 상기 제1 인증키와의 XOR 연산으로 요청 메시지를 생성하여 전송하는 단계; (e) 상기 태그는 상기 요청 메시지를 수신하여, 자신의 인증키(이하 제2 인증키)로 XOR 연산하여 랜덤값(이하 제2 랜덤값)을 추출하는 단계; (f) 상기 태그는 상기 요청 메시지와 상기 제2 인증키와 연접한 값을 해쉬한 값, 및, 상기 제2 랜덤값을 각각 자신의 랜덤값(이하 제3 랜덤값)으로 XOR연산하여 제1 및 제2 응답 메시지를 생성하고, 상기 제1 및 제2 응답 메시지를 상기 리더로 전송하는 단계; 및, (g) 상기 리더는 상기 제1 및 제2 응답 메시지를 XOR연산하고, XOR 연산 결과와 상기 검증 메시지와 대비하여 상기 검색 태그를 인증하는 단계를 포함하는 것을 특징으로 한다.

[0032] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 제1 또는 제2 인증키는 태그의 아이디 및 비밀키를 해쉬하여 생성되는 것을 특징으로 한다.

[0033] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 제1 인증키는 리스트의 인증키와 XOR연산에 의해 암호화 또는 복호화되고, 상기 리스트의 인증키는 모든 태그의 인증키를 XOR연산하여 생성되는 것을 특징으로 한다.

[0034] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 제1 인증키는 추가적으로 상기 리더의 동적 아이디와 XOR 연산에 의해 암호화 또는 복호화되는 것을 특징으로 한다.

[0035] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 (c)단계에서, 마지막 제1 랜덤값으로 XOR연산시, 상기 제1 랜덤값을 중복하여 연접하여 XOR연산하고, 상기 (f)단계에서, 상기 제2 및 제3 랜덤값은 각각 중복하여 연접한 값으로 연산되는 것을 특징으로 한다.

[0036] 또한, 본 발명은 상기 방법을 수행하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

[0037]

발명의 효과

[0038] 상술한 바와 같이, 본 발명에 따른 RFID 태그 검색방법에 의하면, 리더가 태그의 인증키 정보를 암호화된 상태로 보유하게 함으로써, 태그 리스트의 재활용을 방지하고, 이를 통해 보안이 향상된 태그 리스트를 제공하고, 모바일 리더 기반의 RFID 환경에 적합한 동적 ID 기반의 효율적인 태그 검색 프로토콜을 제공할 수 있는 효과가 얻어진다.

[0039] 즉, 본 발명은 기존 무선 리더가 소지하는 태그 리스트의 재사용을 방지함으로써, 보안성을 강화하고, 이동이 잦은 모바일 환경에서의 발생할 수 있는 리더 도난, 태그 상태 변경 및 리더의 권한 변경에 유연하게 대처할 수 있다. 또한, 본 발명은 해쉬 연산과 XOR 연산만을 이용하므로 암호화 기법을 사용하는 기존의 동적 ID기반 태그 검색 프로토콜보다 효율적으로 동작하며 태그 측에서 저장해야하는 정보 또한 최소화할 수 있다.

도면의 간단한 설명

[0040] 도 1은 종래의 RFID 태그 검색 방법을 설명하는 흐름도이다.

도 2는 본 발명을 실시하기 위한 전체 RFID 시스템 구성의 일례를 도시한 도면이다.

도 3은 본 발명의 일실시예에 따른 태그 리스트 구조의 일례를 도시한 것이다.

도 4는 본 발명의 제1 실시예에 따른 RFID 태그 검색방법을 설명하는 흐름도이다.

도 5는 본 발명의 제2 실시예에 따른 RFID 태그 검색방법을 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

발명을 실시하기 위한 구체적인 내용

[0041] 이하, 본 발명의 실시를 위한 구체적인 내용을 도면에 따라서 설명한다.

[0042] 또한, 본 발명을 설명하는데 있어서 동일 부분은 동일 부호를 붙이고, 그 반복 설명은 생략한다.

[0043] 먼저, 본 발명을 실시하기 위한 전체 RFID 시스템 구성의 일례를 도 2를 참조하여 설명한다.

[0044] 도 2에서 도시한 바와 같이, 본 발명을 실시하기 위한 RFID 시스템은 리더(10), 다수의 태그(20), 및 서버(30)

로 구성된다.

[0045] 태그(20)는 RFID태그 등 정보를 저장하는 소형 회로 장치로서 리더(10)로부터 무선신호(radio frequency)를 수신하면 수신된 데이터에 응답하여 그 결과를 리더(10)로 송신하는 장치이다. 태그(20)는 회로에 의해 연산을 처리하거나 데이터를 저장하고 읽을 수 있다.

[0046] 태그(20)는 이동형 리더(10)로부터 전달받은 쿼리 정보를 이용하여 응답 메시지를 생성하고, 그 결과를 이동형 리더(10)에게 전달한다.

[0047] 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 상기 리더(10)의 무선신호에 반응한다.

[0048] 즉, 리더(10)는 특히 이동형 리더로서, 태그 검색 이전에 백엔드 서버로부터 이동형 리더의 권한에 맞는 태그 리스트를 수신 받아야 한다. 정당한 이동형 리더(10)는 수신 받은 태그 리스트의 정보를 이용하여 검색하고자 하는 특정 태그를 찾기 위해 쿼리를 브로드캐스트한다.

[0049] 서버(30)는 신뢰기관의 서버(또는 백엔드 서버)로서, 컴퓨팅 기능을 가진 통상의 서버 또는 컴퓨터 단말이다. 서버(30)는 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 검색과 관련한 정보를 리더(10)에 전송한다.

[0050] 즉, 백엔드 서버(30)는 정당한 리더 및 태그의 정보를 저장하고 있으며, 이동형 리더(10)가 독립적으로 태그(20)를 검색할 수 있도록 리더 및 태그의 정보를 이용하여 태그 리스트를 생성한다. 백엔드 서버(30)는 정당한 이동형 리더(10)에게 태그 리스트 정보를 안전한 채널을 이용하여 전달한다. 백엔드 서버(30)의 데이터베이스의 정보는 유효한 것으로 가정하므로, 이동형 리더(10)에게 전달되는 태그 리스트 또한 유효한 정보로 가정한다.

[0051] 즉, 리더(10)는 태그를 검색하기 위한 태그 리스트 등을 사전에 신뢰기관 서버(30)로부터 수신하여 자신의 메모리에 저장한다. 태그 리스트는 리더(10)가 접근 가능한 모든 태그의 인증키로 만든 리스트의 인증키를 포함한다. 따라서 리더(10)는 태그 리스트에 포함된 태그(20)에 대해서만 안전한 태그 검색을 할 수 있다.

[0052] 다음으로, 리더(10)와 태그(20), 서버(30)가 저장하는 데이터들을 보다 구체적으로 설명한다.

[0053] 태그 집합은 $T = (ID_{T1}, K_{T1}), (ID_{T2}, K_{T2}), \ldots, (ID_{Tn}, K_{Tn})$ 이다. 이것은 백엔드 서버에 등록된 태그 집합으로, 각 태그는 (자신의) ID_T와 K_T를 저장한다.

[0054] 리더 집합은 $R = \{Id_{R1}, Id_{R2}, \ldots, Id_{Rm}\}$이다. 이것은 백엔드 서버에 등록된 이동형 리더 집합으로 각 리더는 리더의 동적ID XId_R, 리더의 태그 리스트 인증키 $LKId_R$, 리더의 태그리스트 LId_R를 저장한다.

[0055] 리더의 태그 리스트는 $LId_R = \{LId_{T1}, LId_{T2}, \ldots, LId_{Tn}\}$이다. 이것은 이동형 리더 Id_R의 권한에 해당하는 태그 리스트 LId_T로 이루어진 집합이다.

[0056] 리더의 태그 리스트 인증키는 다음 [수학식 1]과 같다. 이것은 리더 Id_R의 권한에 해당하는 태그의 정보로 계산된 128bit의 키 정보이다.

[0057] [수학식 1]

$$LKId_R = h(Id_{T1} \| K_{T1}) \oplus h(Id_{T2} \| K_{T2}) \oplus \ldots \oplus h(Id_{Th} \| K_{Th})$$

[0058]

[0059] 태그 리스트 정보는 다음 [수학식 2]와 같다. 이것은 리더 Id_R의 태그 리스트 인증키값 $LKId_R$, 검색하려는 태그의 정보 $h(Id_{Tn} \| K_{Tn})$, 리더의 현 세션의 아이디(ID) XId_R의 XOR 연산에 의해 계산된 128bit의 정보이다.

[0060] [수학식 2]

[0061] $$LId_{Tn} = LKId_R \oplus h(Id_{Tn} || K_{Tn}) \oplus XId_{Rn}$$

[0062] 이때, 태그의 정보 $h(Id_{Tn} \| K_{Tn})$를 태그의 인증키라고 부르기로 한다. 또한, 태그의 인증키에 리스트 인증키 $LKId_R$와 리더의 유동 아이디 XId_R를 XOR 연산함으로써, 태그의 인증키를 암호화한다. 따라서 LId_T(또는 LId_{Tn})를 암호화된 태그의 인증키라고도 부르기로 한다.

[0063] 백엔드 서버 B는 RFID 시스템 내의 정당한 리더 및 태그의 정보를 저장하고 있는 데이터베이스로서, 이동형 리더 Id_R의 권한에 해당하는 태그 리스트 LId_R을 발급한다.

[0064] 한편, 동적 ID 방식(또는 유동 아이디 방식)의 RFID 시스템에서 XId_R 정보 갱신시, 갱신 정보 메시지 손실로 인한 비동기화가 발생하지 않아야 한다. 본 발명에서는 인증 프로토콜이 정상 종료될 경우에 백엔드 서버(30)에 의해 리더의 ID(XId_R) 정보가 갱신된다고 가정한다. 즉, 백엔드 서버와 리더 간의 인증이 이루어지지 않은 경우에는 동일한 XId_R를 이용하게 된다.

[0065] 다음으로, 본 발명의 일실시예에 따른 태그 리스트 구조를 도 3을 참조하여 보다 구체적으로 설명한다.

[0066] 본 발명에서는 기존 태그 리스트에 대한 새로운 측면의 문제점을 제시하고자 한다. 기존 검색 프로토콜에서 수신 받은 태그 리스트를 업데이트 받는 상황으로 1)리더가 읽을 수 있는 태그가 추가된 경우, 2)기존 태그의 정보가 비동기화 된 경우, 3)리더의 권한이 변경된 경우가 있을 수 있다. 이 중 리더의 권한이 변경된 경우에는 기존에 리더가 가지고 있던 태그 리스트를 재활용한다면 변경 이전의 권한으로 태그를 검색할 수 있는 문제점이 발생할 수 있다.

[0067] 본 발명의 일실시예에 따른 태그 리스트 구조는 도 3과 같다.

[0068] $LKId_R$값은 리더의 권한을 의미하며, 리더의 권한에 따라 읽을 수 있는 태그들의 비밀정보들을 XOR 연산으로 연결한 체인 값이다. 백엔드 서버(30)는 리더 Id_R의 태그 리스트를 생성하는데 $LKId_R$, 읽으려는 태그의 비밀정보(또는 인증키) $h(Id_T \| K_T)$, 리더의 동적 ID XId_R를 XOR로 연산한 결과를 태그 Id_T의 리스트 LId_T로 표현한다. 태그 인증이 성공한 경우에 변경되는 유동 아이디 XId_R를 이용한다. 이렇게 생성된 태그 리스트는 다음과 같은 특징을 갖는다.

[0069] (1) 특징1 : LId_T가 노출되어도 $LKId_R$와 XId_R정보를 가지고 있지 않은 공격자는 태그의 비밀정보(또는 인증키) $h(Id_T \| K_T)$를 알아낼 수 없다.

[0070] (2) 특징2 : 태그 리스트 정보는 리더 Id_R가 인증에 참가하는 경우 갱신되므로 리더는 태그 검색이 필요한 시점 이전에 백엔드 서버(30)로부터 태그 리스트를 재전송 받아야 한다.

[0071] (3) 특징3 : 특징2에 따라, 태그 검색 리스트가 노출되어도 XId_R와 $LKId_R$를 모르는 공격자는 태그 검색 리스트 정보를 활용할 수 없다.

[0072] (4) 특징4 : 권한이 변경된 리더 Id_R는 $LKId_R$ 및 XId_R가 갱신되므로 기존 태그 리스트의 정보를 활용할 수 없다.

[0073] (5) 특징5 : 만약, 동적 ID 기반의 환경 적용하기 위해서는 태그의 비밀정보(또는 인증키) $h(Id_T \| K_T)$에서 변경되는 부분을 제외하면 된다.

[0074] 위와 같은 특징에 의해 태그 리스트의 보안성을 강화할 수 있다.

[0075] 다음으로, 본 발명의 제1 실시예에 따른 RFID 태그 검색방법을 도 4를 참조하여 구체적으로 설명한다.

[0076] 도 4에서 보는 바와 같이, 리더(10)는 태그 검색이전에 백엔드 서버(30)로부터 유동 아이디 XId_R, 리스트 인증

키 $LKId_R$, 태그 리스트 List를 전달 받는다(S11). 리더(10)는 XOR연산으로 암호화된 태그의 인증키를 리스트로 저장한다. 태그의 인증키(또는 비밀정보) $h(Id_T \| K_T)$는 상기 [수학식 2]와 같이 리더의 유동 아이디 XId_R 및 리스트 인증키 $LKId_R$로 XOR연산을 하여, 암호화된 형태 LId_T로 표시된다.

[0077] 태그(20)는 연산 능력이 적은 수동형 태그로 가정하며 아이디 Id_T, 비밀키 K_T을 갖는다(S12).

[0078] 다음으로, 리더(10)는 검색하고자 하는 태그(이하 검색 태그)의 정보를 추출하기 위해, 태그 리스트 List상의 해당 태그(또는 검색 태그)의 정보 LId_T, 리스트 인증키 $LKId_R$, 리더의 유동 아이디 XId_R를 XOR 연산한다. 이를 통해, 리더(10)는 검색 태그의 인증키(이하 제1 인증키)를 복호화한다(S20).

[0079] 또한, 리더(10)는 랜덤값(이하 제1 랜덤값) r_R을 생성한다.

[0080] 그리고 리더(10)는 제1 랜덤값 r_R을 추출한 태그 정보(또는 제1 인증키)와 XOR 연산하여 브로드캐스트한다(S40). 이때, 제1 인증키와 제1 랜덤값을 XOR 연산한 것을 요청 메시지 m_{T1} 이라고 한다. 즉, 리더(10)는 제1 랜덤값과 상기 제1 인증키와의 XOR 연산으로 요청 메시지를 생성하여 전송한다.

[0081] 요청 메시지를 수신한 태그(20)는 자신의 Id_T와 K_T를 해쉬 연산한 후 메시지 ②와 XOR 연산을 통해 리더가 전송한 랜덤값 r_R(이하 제2 랜덤값)을 추출한다(S50). 즉, 태그(20)는 자신의 아이디 Id_T와 비밀키 K_T를 해쉬 연산하여, 자신의 인증키(이하 제2 인증키)를 추출한다. 그리고 태그(20)는 제2 인증키로 요청 메시지를 XOR 연산하여 제2 랜덤값을 추출한다.

[0082] 그리고 태그(20)는 요청 메시지를 해쉬한 값 및 제2 랜덤값을 각각 자신의 랜덤값(이하 제3 랜덤값)으로 XOR연산하여 제1 및 제2 응답 메시지 T1, T2 를 생성한다(S60). 즉, 태그(20)는 요청 메시지를 해쉬하고, 해쉬한 요청 메시지를 숨기기 위하여, 제3 랜덤값 r_T를 XOR 연산한다. 그래서 제1 응답 메시지 T1을 생성한다.

[0083] 이때 제3 랜덤값 r_T은 태그(20) 자신이 생성한 랜덤값으로, 미리 생성하여 저장하거나, 리더(10)와 통신할 때마다 새로 생성할 수도 있다.

[0084] 또한, 태그(20)는 생성한 랜덤값(또는 제3 랜덤값 r_T)을 숨기기 위해 r_R과 XOR 연산하여 제2 응답 메시지 T2를 연산한다.

[0085] 그리고 태그(20)는 제1 및 제2 응답 메시지 T1, T2를 리더(10)에게 응답한다.

[0086] 각 태그(20)가 앞서 과정 S50 내지 S60을 연산하는 동안, 리더(10)는 요청 메시지를 해쉬 연산 후 제1 랜덤값 r_R과 XOR 하여 검증 메시지 R1값을 사전에 연산해둔다(S30).

[0087] 그리고 리더(10)가 태그(10)로부터 제1 및 제2 응답 메시지를 수신하면, 수신한 응답 메시지를 상기 검증 메시지로 검증한다(S70). 즉, 제1 및 제2 응답 메시지를 XOR연산하고, XOR 연산 결과와 상기 검증 메시지와 대비하여 상기 검색 태그를 인증한다. 각 태그들로부터 전달 받은 메시지(또는 응답 메시지)를 확인하는 과정으로 태그마다 T1, T2값을 XOR하여 확인할 수 있다. 응답 메시지와 검증 메시지가 동일한 경우, 검색하고자 하는 태그(또는 검색 태그)로 인증한다.

[0088]

[0089] 다음으로, 본 발명의 제2 실시예에 따른 RFID 태그 검색방법을 도 5를 참조하여 구체적으로 설명한다.

[0090] 도 5에서 보는 바와 같이, 제2 실시예에 따른 RFID 태그 검색방법은 앞서 설명한 제1 실시예와 거의 동일하다. 다만, 검증 메시지 또는 제1 응답 메시지를 생성할 때, 태그의 인증키를 더 연접하여 해쉬하는 것에 차이가 있다. 이하에서 차이 부분만 설명하기로 한다. 그 외 방법은 제1 실시예를 참고한다.

[0091] 즉, 도 5의 S60 단계에서, 태그(20)는 요청 메시지와 제2 인증키와 연접한 값을 해쉬한 값, 및, 제2 랜덤값을 각각 자신의 랜덤값(이하 제3 랜덤값)으로 XOR연산하여 제1 및 제2 응답 메시지를 생성하고, 상기 제1 및 제2 응답 메시지를 상기 리더로 전송한다(S60).

[0092] 즉, 태그(20)는 요청 메시지와 제2 인증키와 연접한 값을 해쉬하고, 해쉬한 값에 제3 랜덤값 R_T를 XOR연산하여 제1 응답 메시지 T1을 생성한다. 이때, 제2 인증키는 태그의 아이디 Id_T와 비밀키 K_T를 연접하여 해쉬한 값

$h(Id_T \| K_T)$이다. 한편, 제3 랜덤값을 중복하여 연접한 값으로 XOR 연산을 한다. 즉, $(r_T \| r_T)$로 XOR 연산한다. 이것은 bit의 자리수를 맞추기 위함이다.

[0093] 또한, 제2 응답 메시지도 제2 랜덤값과 제3 랜덤값을 XOR 연산하여 생성하되, 제2 랜덤값과 제3 랜덤값도 중복하여 연접한 값으로 XOR 연산을 한다.

[0094] 한편, 도 5의 S30 단계에서, 리더(10)는 요청 메시지와 $h(Id_T \| K_T)$를 연접하여 해쉬 연산 후 제1 랜덤값 r_R과 XOR 하여 검증 메시지 R1값을 사전에 연산해둔다(S30). 이때, 제1 랜덤값도 중복하여 연접한 값으로 XOR 연산을 한다.

[0095] 다음으로, 본 발명이 모바일 환경에서의 RFID 시스템의 태그 검색 프로토콜의 요구사항을 만족하는지를 보다 구체적으로 설명한다. 상기 요구사항들은 앞서 배경기술에서 설명된 것을 참조한다.

[0096] 결론부터 말하면, 본 발명에 따른 태그 검색 방법은 요구사항1, 요구사항2, 요구사항3, 요구사항4를 모두 만족한다.

[0097] 먼저, 요구사항1에 관하여, 태그 위조 공격을 위해서는 요청 메시지에서 랜덤값 r_R을 추출해낼 수 있어야 한다. 태그의 Id_R, K_R를 모르는 공격자는 r_R를 유추할 수 없으므로 요구사항1을 만족한다.

[0098] 다음으로, 요구사항2에 관하여, 요청 메시지에 포함된 태그 비밀정보는 $LKId_R$, XId_R, LId_T를 모두 소유한 정당한 리더만이 생성할 수 있는 값이다. 이 값은 매 세션 갱신되는 값이므로 이 정보를 소유하지 않은 리더는 유요한 쿼리를 만들 수 없어 요구사항2를 만족한다.

[0099] 다음으로, 요구사항3에 관하여, 요청 메시지는 리더의 랜덤값 r_R에 의해 세션 마다 변경되고 응답 메시지에는 태그의 랜덤값이 추가되므로, 요청 메시지가 공격자에 의해 재활용된다 하더라도 모든 태그가 반응하므로 찾고자 하는 태그를 검색할 수 없으며 태그의 랜덤값이 포함되므로 응답 메시지는 항상 변경되게 된다. 그러므로 요구사항3-1, 요구사항3-2, 요구사항3-3, 요구사항3-4를 모두 만족한다.

[0100] 다음으로, 요구사항3에 관하여, 본 발명에 의한 검색 방법에서는 동적 ID 동기화 방식을 이용하므로, 리더 XId_R의 변경시점은 리더가 태그 인증을 시도하는 시점, 즉, 백엔드 서버와 리더가 연결되는 시점이다. 그러므로 태그 검색 프로토콜 상에서는 비동기화가 발생할 수 없으며, 태그 리스트가 변경되는 시점은 기존 정적 ID기반의 태그 검색 프로토콜보다는 짧고, 동적 ID 방식의 태그 검색 프로토콜보다는 길지만, 비동기화로 인한 프로토콜 실패의 위험이 없다.

[0101] 다음으로, 본 발명에 따른 발명의 안전성 및 효율성을 종래 선행기술과의 비교를 도 6을 참조하여 보다 구체적으로 설명한다.

[0102] 비교대상은 배경기술에서 살펴본 4가지의 검색 방법, 즉, 선행기술 1 내지 4이며, 각 기술의 특징을 도 6과 같이 정리하였다.

[0103] 기존 프로토콜은 타입, 암호화여부 구분해볼 수 있다. RFID 타입을 기준으로 살펴보면 태그 리스트, 리더나 태그의 정보가 변경되지 않는 정적ID, 태그의 리스트 정보나, 리더나 태그의 정보가 변경되는 동적ID로 구분할 수 있다.

[0104] 정적ID에는 선행기술 1과 3이 해당하고, 동적ID에는 선행기술 2와 4가 해당한다. 암호화 지원여부로 살펴본다면 암호화를 지원하는 선행기술 3과 4와 해쉬 연산을 지원하는 선행기술 1과 2로 구분해볼 수 있다. 제안하는 기법은 태그 테이블 할당시 리더의 동적ID를 사용하므로 동적ID기반으로 분류할 수 있으며, 프로토콜 상에서 암호화 연산은 사용하지 않는다.

[0105] 종래 선행기술 1 내지 4 및 본 발명의 안전성 분석은 앞서 설명되었으므로, 연산량 측면의 비교만 언급하도록 한다. 일방향함수를 사용한 의사난수생성을 해쉬 연산과 동일한 연산량이 소모된다고 가정하면, 태그 측면의 연산량은 선행기술 4 > 선행기술 3 > 선행기술 1 > 선행기술 2 > 본 발명 순이다. 즉, 본 발명의 연산이 태그 측면에서 가장 적은 연산을 소비한다.

[0106] 리더 측면의 연산량은 선행기술 3 > 선행기술 2 > 선행기술 1 > 본 발명 순이다(선행기술 4 의 프로토콜은 하나의 태그만 반응하므로 비교에서 제외하도록 한다.). 즉, 본 발명의 연산이 N개의 태그로부터의 응답을 수신하는 경우에 연산량이 가장 적은 연산을 소비한다.

[0107]

[0108] 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.

[0109]

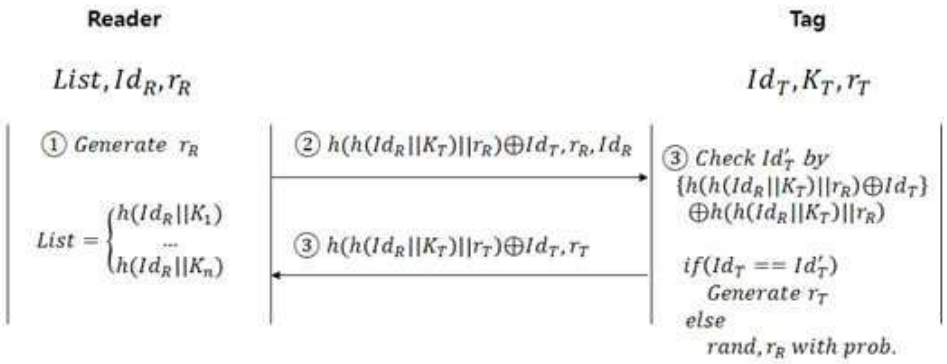
산업상 이용가능성

[0110] 본 발명은 태그 리스트의 재활용을 방지함으로써 보안이 향상된 태그 리스트를 제공하고, 모바일 리더 기반의 RFID 환경에 적합한 동적 ID 기반의 효율적인 RFID 리더 및 태그 장치를 개발하는 데 적용이 가능하다.

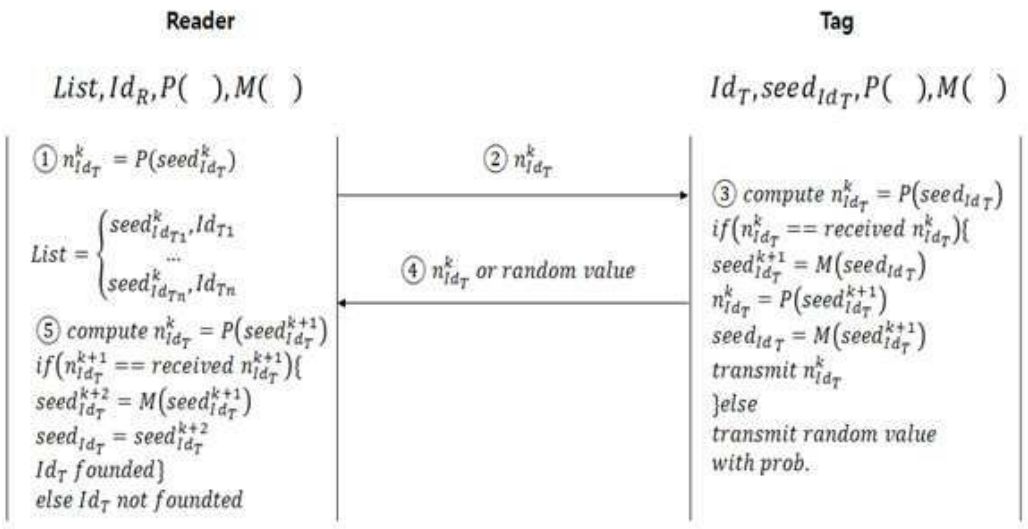
[0111]

도면

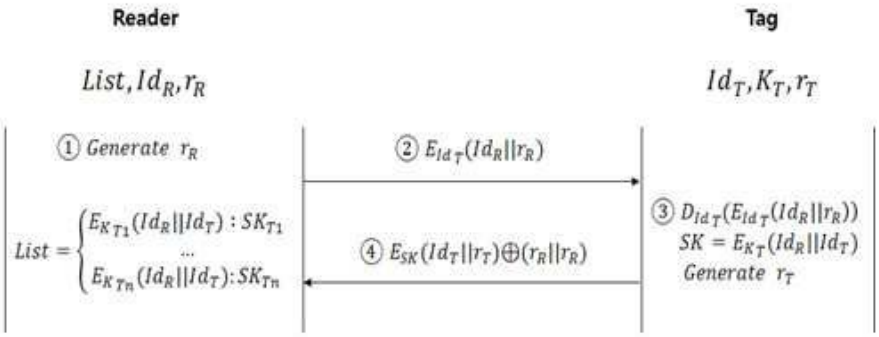
도면1a



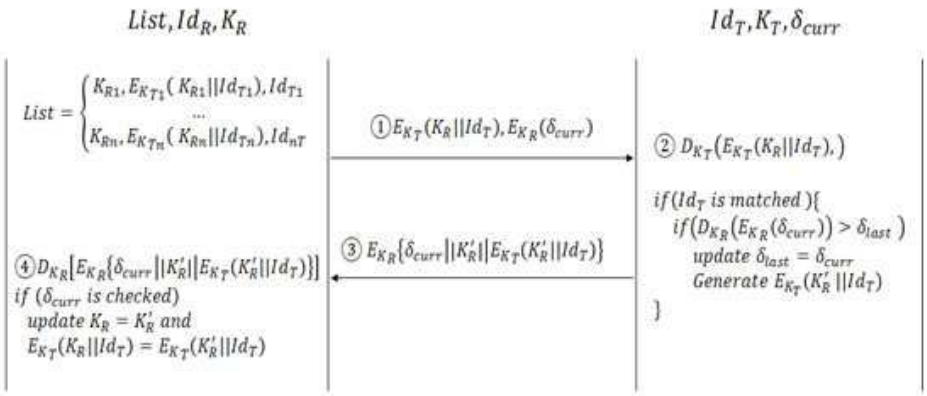
도면1b



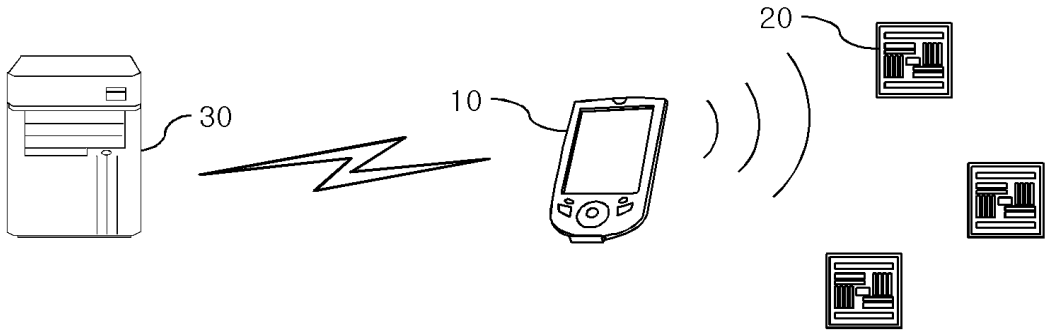
도면1c



도면1d



도면2

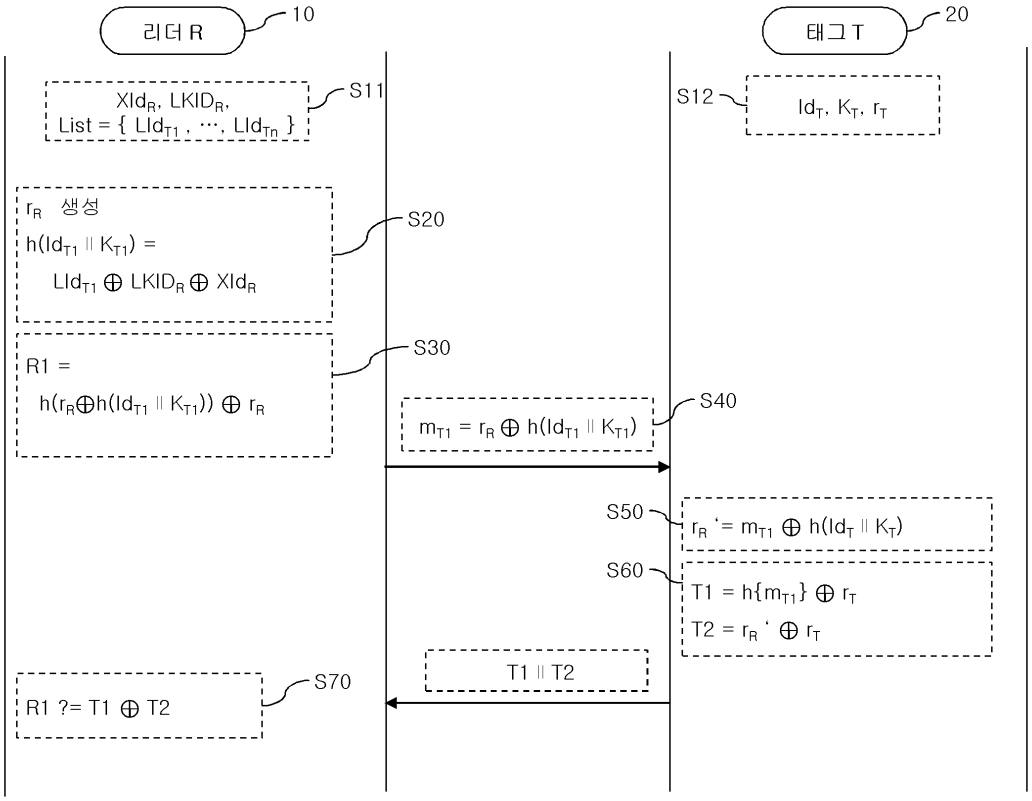


도면3

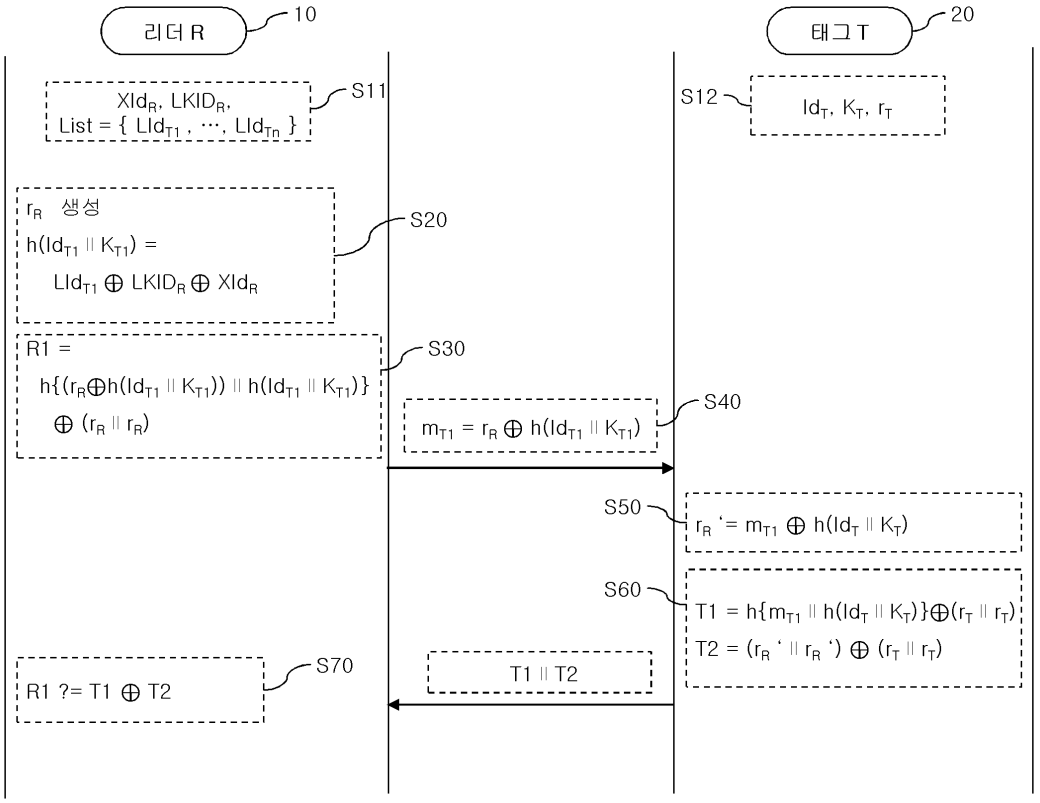
$$LKId_{R1} = h(Id_{T1}||K_{T1}) \oplus \cdots \oplus h(Id_{Tn}||K_{Tn})$$

$$List = \begin{cases} LKId_{R1} \oplus h(Id_{T1}||K_{T1}) \oplus XId_{R1} & : LId_{T1} \\ \cdots & \\ LKId_{R1} \oplus h(Id_{Tn}||K_{Tn}) \oplus XId_{R1} & : LId_{Tn} \end{cases}$$

도면4


리더 R
10
태그 T
20
XId_R, LKID_R,
List = { LId_T1 , ···, LId_Tn }
S11
S12
Id_T, K_T, r_T
r_R 생성
h(Id_T1 ‖ K_T1) =
LId_T1 ⊕ LKID_R ⊕ XId_R
S20
R1 =
h(r_R⊕h(Id_T1 ‖ K_T1)) ⊕ r_R
S30
m_T1 = r_R ⊕ h(Id_T1 ‖ K_T1)
S40
S50
r_R ' = m_T1 ⊕ h(Id_T ‖ K_T)
S60
T1 = h{m_T1} ⊕ r_T
T2 = r_R ' ⊕ r_T
T1 ‖ T2
R1 ?= T1 ⊕ T2
S70

도면5


리더 R
10
태그 T
20
XId_R, LKID_R,
List = { LId_T1 , ···, LId_Tn }
S11
S12
Id_T, K_T, r_T
r_R 생성
h(Id_T1 ‖ K_T1) =
LId_T1 ⊕ LKID_R ⊕ XId_R
S20
R1 =
h{(r_R⊕h(Id_T1 ‖ K_T1)) ‖ h(Id_T1 ‖ K_T1)}
⊕ (r_R ‖ r_R)
S30
m_T1 = r_R ⊕ h(Id_T1 ‖ K_T1)
S40
S50
r_R ' = m_T1 ⊕ h(Id_T ‖ K_T)
S60
T1 = h{m_T1 ‖ h(Id_T ‖ K_T)}⊕(r_T ‖ r_T)
T2 = (r_R ' ‖ r_R ') ⊕ (r_T ‖ r_T)
T1 ‖ T2
R1 ?= T1 ⊕ T2
S70

도면6

	선행기술 1	선행기술 3	선행기술 2	선행기술 4	본 발명
RFID 타입	정적ID	정적ID	동적ID	동적ID	동적ID
정보갱신 주체	-	-	태그	태그	서버
태그정보 갱신	-	-	O	O	-
리더정보 갱신	-	-	O	O	O
암호화지원 여부	-	O	-	O	-
태그 위장	-	-	취약	-	-
리더 위장	-	-	-	취약	-
태그 프라이버시	△	-	-	-	-
리더 프라이버시	취약	-	-	-	-
비동기화	-	-	취약	취약	-
Tag	3H+R+2X	D+2E+R+X	2P+2M	2D+2E+H+R	2H+R+3X
Server-RQ	H+R+X	E+R	P	E+R	H+R+4X
Server-Tag	-	-	-	D	-
Server-NT	N(H+X)	N(D+X)	N(P+M)	-	N(X)

*Tag : 태그 측에서의 연산량
*Server-RQ : 요청 메시지 생성시 소비되는 연산량
*Server-Tag : 응답 메시지 확인 연산량(1개의 태그만 응답하는 경우)
*Server-NT : 응답 메시지 확인 연산량(N개의 태그가 응답하는 경우)
*H : 해쉬연산
*R,P,M : 의사난수함수를 이용한 랜덤값 생성
*X : 배타적 논리연산