(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0064292
(43) 공개일자 2010년06월14일

(51) Int. Cl.
H04W 12/08 (2009.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2009-0028572
(22) 출원일자 2009년04월02일
심사청구일자 2009년04월02일
(30) 우선권주장
1020080122747 2008년12월04일 대한민국(KR)
기술이전 희망 : **기술양도**, **실시권허여**, **기술지도**

(71) 출원인
한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자
강유성
대전 유성구 신성동 대림두레아파트 108동 901호
최두호
충남 천안시 청당동 신도브래뉴아파트 101동 501호
(뒷면에 계속)
(74) 대리인
유미특허법인

전체 청구항 수 : 총 8 항

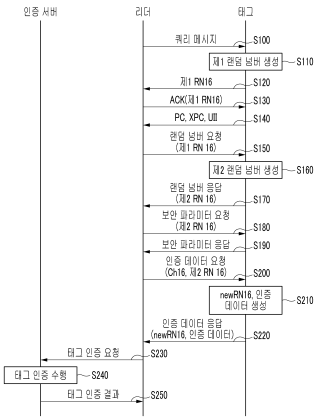
(54) 보안 모드에 따른 수동형 R F I D 보안 방법

(57) 요 약

본 발명은 보안 모드에 따른 수동형 RFID(Radio Frequency Identification) 보안 방법에 관한 것이다.

본 발명에 따르면 RFID 태그가 자신의 현재 보안 모드를 리더에 전달하기 때문에, 리더는 RFID 태그의 현재 보안 모드에 따라 보안 프로토콜을 구동시킬 수 있고, 리더가 보안 모드를 통해 태그의 능력을 알 수 있기 때문에 능력에 맞는 프로토콜을 동작시킬 수 있다. 또한, 다수의 태그가 존재하는 상황에서도 리더가 태그들과의 통신을 끝내고 계속적으로 세션을 유지할 필요가 없기 때문에, 리더와 인증 서버사이의 통신 부담도 줄일 수 있다.

대 표 도 - 도3



(72) 발명자

최용제

대전 유성구 관평동 한화꿈에그린 104동 2002호

정교일

대전 유성구 신성동 한울아파트 107동 1102호

조현숙

대전 유성구 관평동 대덕테크노밸리7단지 금성백조아파트 701동 501호

이형섭

대전 서구 만년동 강변아파트 107-904

이상연

대전 서구 둔산동 샘머리아파트 201동 1205호

이강복

대전광역시 서구 둔산동 샘머리아파트 103동 801호

신동범

대전광역시 서구 월평동 백합아파트 101동 905호

정재영

대전광역시 유성구 지족동 열매마을아파트 403동 1405호

표철식

대전광역시 서구 만년동 강변아파트 109동 701호

이 발명을 지원한 국가연구개발사업

과제고유번호	2005-S-088-04
부처명	지식경제부 및 정보통신연구진흥원
연구사업명	IT성장동력기술개발
연구과제명	안전한 RFID/USN을 위한 정보보호 기술 개발
주관기관	한국전자통신연구원
연구기간	2005.01.01~2009.02.28

특허청구의 범위

청구항 1

태그로부터 제1 랜덤 넘버, 프로토콜 컨트롤 정보, 확장 프로토콜 컨트롤 정보 및 단일 아이템 지시자 정보를 수신하면, 상기 제1 랜덤 넘버를 이용하여 제2 랜덤 넘버를 요청하는 단계;

상기 태그로부터 제2 랜덤 넘버를 수신하면, 상기 제2 랜덤 넘버를 포함하여 보안 파라미터를 요청하는 단계;

상기 태그로부터 암호화된 데이터를 수신하면, 인증 서버로 상기 암호화된 데이터의 인증 결과를 요청하는 단계; 및

상기 인증 서버로부터 수신하는 상기 암호화된 데이터의 인증 결과에 따라 상기 태그를 인증하는 단계

를 포함하는 보안 방법.

청구항 2

제1항에 있어서,

상기 인증 결과를 요청하는 단계는,

상기 보안 파라미터를 수신하면, 상기 태그로 제2 랜덤 넘버와 임의로 생성된 랜덤 넘버를 파라미터로 하여 상기 암호화된 데이터를 요청하는 단계;

상기 태그로부터 상기 암호화된 데이터 및 상기 암호화된 데이터를 생성하기 위해 사용한 암호화 랜덤 넘버를 수신하는 단계; 및

상기 인증 서버로 상기 암호화 랜덤 넘버, 임의로 생성된 랜덤 넘버 및 암호화된 인증 데이터, 단일 아이템 지시자 정보 및 제1 랜덤 넘버를 포함하여 상기 암호화된 인증 데이터의 인증 결과를 요청하는 단계

를 포함하는 보안 방법.

청구항 3

제1항에 있어서,

상기 진의 여부는,

상기 인증 서버가 미리 저장하고 있는 상기 단일 아이템 지시자 정보에 대응되는 비밀키를 확인하는 단계;

상기 제1 랜덤 넘버와 상기 비밀키를 이용하여 세션 키를 생성하는 단계;

상기 세션 키를 사용하여 상기 암호화 랜덤 넘버를 복호화하여, 랜덤 넘버를 구하는 단계;

상기 임의로 생성된 랜덤 넘버와 복호화된 상기 랜덤 넘버를 이용하여 암호화된 인증 데이터를 구하는 단계; 및

상기 구한 암호화된 인증 데이터와 상기 수신한 암호화된 인증 데이터를 비교하여 인증 결과를 생성하여 전달하는 단계

를 포함하는 보안 방법.

청구항 4

제1항에 있어서,

상기 확장 프로토콜 컨트롤 정보에는 보안 모드 지시자가 포함되어 있는 보안 방법.

청구항 5

미리 생성한 제1 랜덤 넘버를 파라미터로 하는 메시지를 리더로부터 수신하면, 상기 리더로 프로토콜 정보, 확장 프로토콜 컨트롤 정보 및 단일 아이템 지시자 정보를 전송하는 단계;

상기 제1 랜덤 넘버를 파라미터로 하는 랜덤 넘버 요청 메시지를 수신하면, 제2 랜덤 넘버를 생성하여 상기 리더로 전송하는 단계; 및

상기 제2 랜덤 넘버와 상기 리더가 임의로 생성한 랜덤 넘버를 파라미터로 하는 인증 데이터 요청 메시지를 수신하면, 상기 리더에 암호화된 인증 데이터와 암호화 랜덤 넘버를 전달하는 단계

를 포함하는 보안 방법.

청구항 6

제5항에 있어서,

상기 암호화 랜덤 넘버를 전달하는 단계는,

상기 리더가 임의로 생성한 랜덤 넘버를 파라미터로 하는 인증 데이터 요청 메시지를 수신하는 단계;

상기 암호화 랜덤 넘버를 생성하는 단계;

상기 리더가 임의로 생성하여 전송한 랜덤 넘버와 상기 랜덤 넘버를 이용하여 인증 데이터를 만들고, 이를 암호화하여 암호화된 인증 데이터를 생성하는 단계; 및

상기 리더로 암호화된 데이터와 암호화 랜덤 넘버를 전달하는 단계

를 포함하는 보안 방법.

청구항 7

제5항에 있어서,

상기 확장 프로토콜 컨트롤 정보에는 보안 모드 지시자가 포함되어 있는 보안 방법.

청구항 8

제7항에 있어서,

상기 보안 모드 지시자는 일반 모드, 인증 모드, 그룹 키 관리 모드 및 개별 키 관리 모드 중 어느 하나의 보안 모드인 보안 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 보안 모드에 따른 수동형 RFID 보안 방법에 관한 것이다.

[0002] 본 발명은 지식경제부 및 정보통신연구진흥원의 IT성장동력기술개발사업의 일환으로 수행한 연구로부터 도출된 것이다[과제관리번호: 2005-S-088-04, 과제명: 안전한 RFID/USN을 위한 정보보호 기술 개발].

배 경 기 술

[0003] 반도체 기술이 발전함에 따라 수동형 RFID(Radio Frequency IDentification, 전파식별) 태그에서도 AES(Advanced Encryption Standard) 암호 알고리즘을 구동시킬 수 있는 여건이 조성되고 있다. 이는 보안기술 적용 측면에서 데이터를 암호화할 수 있다는 것을 의미한다. 즉, 자체적인 전원이 없어 리더로부터 전원을 공급받아야 하는 수동형 RFID 태그에서 데이터 암호화를 수행할 수 있게 되면, 이를 이용하여 다양한 보안 프로토콜을 구현할 수 있게 된다.

[0004] 이 외에 수동형 RFID 태그가 보안 강도 또는 보안 기능에 따라서 다양한 보안 모드로 설정될 수 있다. 이러한 경우에는 리더가 태그의 현재 보안 모드를 확인하고, 그에 알맞은 보안 기능을 수행하여 해당 RFID 시스템이 요구하는 보안 강도를 만족시켜야 한다.

[0005] 즉, 종래에는 수동형 RFID 태그에서 암호 알고리즘의 활용이 없고, 보안 강도를 나타내는 보안 모드 활용이 없어 유연한 활용이 어렵다는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

[0006] 따라서, 본 발명은 RFID 리더가 RFID 태그의 보안 모드를 확인한 후 보안 모드에 따라 인증 프로토콜 또는 데이터 보호 프로토콜 동작을 수행하는 RFID 태그와 리더간 보안 방법을 제공한다.

과제 해결수단

[0007] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 하나의 특징인 보안 방법은,

[0008] 태그로부터 제1 랜덤 넘버, 프로토콜 컨트롤 정보, 확장 프로토콜 컨트롤 정보 및 단일 아이템 지시자 정보를 수신하면, 상기 제1 랜덤 넘버를 이용하여 제2 랜덤 넘버를 요청하는 단계; 상기 태그로부터 제2 랜덤 넘버를 수신하면, 상기 제2 랜덤 넘버를 포함하여 보안 파라미터를 요청하는 단계; 상기 태그로부터 암호화된 데이터를 수신하면, 인증 서버로 상기 암호화된 데이터의 인증 결과를 요청하는 단계; 및 상기 인증 서버로부터 수신하는 상기 암호화된 데이터의 인증 결과에 따라 상기 태그를 인증하는 단계를 포함한다.

[0009] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 또 다른 특징인 보안 방법은,

[0010] 미리 생성한 제1 랜덤 넘버를 파라미터로 하는 메시지를 리더로부터 수신하면, 상기 리더로 프로토콜 정보, 확장 프로토콜 컨트롤 정보 및 단일 아이템 지시자 정보를 전송하는 단계; 상기 제1 랜덤 넘버를 파라미터로 하는 랜덤 넘버 요청 메시지를 수신하면, 제2 랜덤 넘버를 생성하여 상기 리더로 전송하는 단계; 및 상기 제2 랜덤 넘버와 상기 리더가 임의로 생성한 랜덤 넘버를 파라미터로 하는 인증 데이터 요청 메시지를 수신하면, 상기 리더에 암호화된 인증 데이터와 암호화 랜덤 넘버를 전달하는 단계를 포함한다.

효 과

[0011] 본 발명에 따르면 RFID 태그가 자신의 현재 보안 모드를 리더에 전달하기 때문에, 리더는 RFID 태그의 현재 보안 모드에 따라 보안 프로토콜을 구동시킬 수 있고, 리더가 보안 모드를 통해 태그의 능력을 알 수 있기 때문에 능력에 맞는 프로토콜을 동작시킬 수 있다.

[0012] 또한, 다수의 태그가 존재하는 상황에서도 리더가 태그들과의 통신을 끝내고 계속적으로 세션을 유지할 필요가 없기 때문에, 리더와 인증 서버사이의 통신 부담도 줄일 수 있다.

발명의 실시를 위한 구체적인 내용

[0013] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0014] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0015] 수동형 RFID 태그가 부착되는 물품이 높은 보안 강도를 요구하여 RFID 태그 인증, RFID 태그 데이터 기밀성 보호, RFID 태그 무결성 보장 등의 보안 기능이 필요하게 되면, 이러한 보안 기능을 지원할 수 있는 연산 능력을 구비하고 그에 맞는 보안 모드를 설정할 수 있는 RFID 태그를 사용해야 하다. 만약, RFID 태그 데이터 보호가 필요 없이 단지 RFID 태그 인증만이 필요한 응용이 있다면, 그에 맞는 연산만 처리하고 해당 보안 모드를 설정하면 된다.

[0016] 즉, 본 발명의 실시예에서는 응용이 요구하는 보안 강도를 보안 모드로 설정하고, RFID 태그와 리더가 해당 보안 모드에 따라 동작함으로써 응용이 요구하는 보안 서비스를 제공하되 최적화된 연산을 수행할 수 있는 보안 기술을 제공한다. 본 발명의 실시예에서는 수동형 RFID 태그의 대표적인 표준인 ISO/IEC 18000-6 Type C 표준과 호환성을 가지도록 구성하나, 반드시 이와 같이 한정되는 것은 아니다. 이에 대해 이하 도면을 참조로 하여 설명하기로 한다.

[0017] 도 1은 본 발명의 실시예에 따른 보안 모드를 지시하는 데이터 포맷의 예시도이다.

[0018] 도 1에 도시된 바와 같이, 16비트의 확장 프로토콜 컨트롤(XPC: Extended Protocol Control) 데이터 구조가 보안 모드 지시자를 포함할 수 있다. 도 1의 보안 모드 지시자는 2 비트로 구성되며, 이 비트가 확장 프로토콜 컨트롤의 여분의 비트에 포함될 수도 있다.

[0019] 본 발명의 실시예에서는 2 비트의 보안 모드 지시자를 이용하기 때문에 총 4개의 보안 모드를 지시할 수 있다. 이에 대해 표 1에 보안 모드 별 활용 예 및 보안 모드 필드를 나타내었다. 표 1에 대해 설명하면서 본 발명의 실시예에 따른 응용 서비스별 대표적인 서비스와 그에 대한 보안 고려사항 및 태그 인증 모드의 동작 절차에 대하여 도 2 및 도 3을 참조로 설명하기로 한다.

[0020] [표 1]

[0021]

보안 모드	특징	효과	활용 예	보안 모드 필드
모드 1 (비보안 모드)	- UII 노출 - 18000-6 Type C	- 접근 패스워드 노출 가능 - 제품 종류 노출 가능 - 복제 태그 등장 가능 - 태그/리더 통신 데이터 도청 가능	- 단순 물품 인식	00
모드 2 (태그 인증 모드)	- UII 노출 - 서버가 태그 검증 - 키는 태그와 서버가 공유 - 인증 프로토콜	- 제품 이동 경로 추적 가능 - 태그/리더 통신 데이터 도청 가능 - 태그 진품 확인 - 복제 태그 방지(리더의 악의적인 복제 불가)	- 농축수산물 진품 검증 - 진품 확인이 필요한 경우	01
모드 3 (그룹키 관리 모드)	- UII 보호 - 태그/리더 통신 데이터 보호 - 리더에서 그룹키 관리 - 데이터 보호 프로토콜	- 복제 태그 방지(리더의 악의적인 태그 복제 가능) - 제품 이동 경로 추적 방지 - 태그/리더 통신 데이터 보호 - 소유자 프라이버시 보호	- 모바일 RFID - 개인간 소유권 이전이 필요한 경우	10
모드 4 (개별키 관리 모드)	- UII 보호 - 태그/리더 통신 데이터 보호 - UII 별로 키 관리	- 복제 태그 방지(리더의 악의적인 태그 복제 불가) - 제품 이동 경로 추적 방지 - 태그/리더 통신 데이터 보호 - 소유자 프라이버시 보호	- 농축수산물 진품 검증 - 모바일 RFID - 진품 확인/소유권 이전이 필요한 경우	11

[0022] 먼저 표 1에 나타낸 바와 같이 보안 모드 값이 00인 모드 1은 비보안 모드라고도 하며, 보안 기능이 없는 일반적인 ISO/IEC 18000-6 Type C 표준에서 동작하는 모드를 의미한다. 이 경우, RFID 태그는 단순히 태그의 아이디(ID) 정보만을 리더에 전달하고, 리더는 물품의 정보를 백엔드 네트워크(Backend Network)를 통해 별도의 서버로부터 수집한다.

[0023] 모드 1의 대표적인 서비스로는 영화 포스터 서비스이며 이를 포함하여 도 2를 참조로 설명하기로 한다. 도 2는 본 발명의 실시예에 따른 응용 서비스별 대표적인 서비스와 그에 대한 보안 고려사항의 예시도이다.

[0024] 도 2에 도시된 바와 같이 영화 포스터에 RFID 태그가 부착되어 있으면, 사용자는 RFID 태그를 읽고 백엔드 서버로부터 영화와 관련된 정보를 수집할 수 있다. 이러한 서비스에서는 RFID 태그의 아이디 정보가 노출되어도 상관없기 때문에, 인증 및 데이터 보호가 요구되지 않는다.

[0025] 다음 표 1의 보안 모드 값이 01인 모드 2는 태그 인증 모드라고도 하며, 이 모드의 대표적인 서비스는 한우와 같은 농축수산물 진품 검증 서비스이다. 모드 2의 동작 방법에 대해 설명하면, 한우 생산 업체는 한우에 RFID 태그를 부착하고 보안 모드 값을 01로 설정한 후, RFID 태그에 비밀키를 설정한다. 그리고 한우 생산 업체는 해당 RFID 태그의 비밀키를 안전한 인증 서버에 저장한다.

[0026] 한우 판매점에 들른 소비자는 진열된 한우에 부착된 RFID 태그를 통해 한우의 진품 여부를 확인하고자 한다. 이때, RFID 태그를 읽고 진품 검증을 수행할 수 있는 리더는 판매점의 리더 또는 소비자의 휴대 리더가 될 수 있다. 이러한 경우, RFID 태그의 비밀키가 판매점의 리더 또는 소비자의 리더에 전달되면 악의적인 판매점 또는 소비자에 의해 복제된 RFID 태그가 나타날 수 있는 위험이 존재한다.

[0027] 따라서, 모드 2에서는 리더는 인증 서버로부터 인증 결과만을 전달받아야 한다. 본 발명의 실시예에 따른 모드

2는 ISO/IEC 18000-6 Type C 표준과 호환성을 가지도록 구성된다. 리더는 인증 서버와 안전한 채널로 통신할 수 있다고 가정하고, 태그는 SecParam(Security Parameter, 보안 파라미터)을 가지고 있다고 가정한다.

[0028] 보안 파라미터는 사용되는 암호 알고리즘과 관련된 정보로 구성된 구조체이며, 본 발명의 실시예에서는 구체적인 형태에 대한 설명을 생략하기로 한다. 본 발명의 실시예에 따른 RFID 태그는 내부에 비밀키가 저장되어 있다고 가정하며, 리더는 태그의 비밀키를 알지 못하며 오직 인증 서버만이 태그의 비밀키 정보를 가지고 있다고 가정한다. 모드 2의 동작 절차에 대해 도 3을 참조로 설명하기로 한다.

[0029] 도 3은 본 발명의 실시예에 따른 태그 인증 모드의 동작을 나타낸 흐름도이다.

[0030] 도 3에 도시된 바와 같이, 리더는 태그로 쿼리 메시지를 전송한다(S100). 이때, 쿼리 메시지에 포함되어 전송되는 파라미터들(예를 들어, 쿼리, Query_Adjust, Query_Rep 등)은 이미 표준에 정의되어 있는 명령어로, 본 발명의 실시예에서는 상세한 설명을 생략하기로 한다. 쿼리 메시지를 받은 태그는 랜덤 넘버를 생성하여(S110) 제1 랜덤 넘버(RN16)로 회신한다(S120). 여기서 생성된 랜덤 넘버는 16비트이며, 이하 설명의 편의상 RN16이라고 표시한다.

[0031] 태그로부터 제1 RN16을 받은 리더는 랜덤 넘버를 받았음을 알림과 동시에 태그로부터 프로토콜 컨트롤(PC: Protocol Control), 확장 프로토콜 컨트롤(XPC: Extended Protocol Control) 및 단일 아이템 지시자(UII:Unique Item Identification) 정보를 받기 위해 ACK(Acknowledge) 메시지를 태그로 전송한다(S130). 그러면 ACK 메시지를 수신한 태그는 자신의 프로토콜 컨트롤, 확장 프로토콜 컨트롤 및 단일 아이템 지시자 정보를 포함하는 메시지를 리더에 전송한다(S140). 여기서 프로토콜 컨트롤, 확장 프로토콜 컨트롤 및 단일 아이템 지시자는 이미 알려진 사항으로, 본 발명의 실시예에서는 상세한 설명을 생략하기로 한다.

[0032] 프로토콜 컨트롤, 확장 프로토콜 컨트롤 및 단일 아이템 지시자 정보를 수신한 리더는 새로운 랜덤 넘버를 요청하는 랜덤 넘버 요청(Req_RN) 명령을 태그에 전송하는데(S150), S110 단계에서 수신한 랜덤 넘버인 제1 RN16을 파라미터로 갖고 있다. 랜덤 넘버를 파라미터로 포함하는 이유는 일종의 태그 주소 또는 세션 아이디 개념으로, 다수의 태그가 랜덤 넘버 요청 메시지를 수신한다 하더라도 S110 단계에서 제1 랜덤 넘버 RN16을 전송한 태그만이 자신에게 온 메시지임을 파악할 수 있도록 하기 위함이다.

[0033] 랜덤 넘버 요청 메시지를 수신한 태그는 새롭게 사용할 랜덤 넘버를 생성하여 리더에 회신한다(S160, S170). 이때 새로 생성한 랜덤 넘버도 16비트로 이루어지며, 제2 RN16 또는 핸들(Handle)이라 지칭하기로 한다.

[0034] 다음, S140 단계에서 태그가 리더로 전송하는 확장 프로토콜 컨트롤에 현재 지원하는 보안 모드가 지시되어 있기 때문에, 리더는 S180 단계 내지 S250 단계를 통해 태그 인증 모드로 동작을 수행한다. 즉, 도 1에서 나타낸 것처럼 전체 16비트의 확장 프로토콜 컨트롤 데이터 구조의 보안 모드 필드에 2비트로 보안 모드를 나타내는 이진수 "01"을 지시하면, 리더는 S180 단계 내지 S250 단계까지의 태그 인증 모드로 동작을 수행한다.

[0035] 먼저 리더는 태그로 보안 파라미터를 요청하는 명령인 보안 파라미터 요청 메시지(Get_SecParam)를 전송한다(S180). 이때 보안 파라미터 요청 메시지를 전송할 때, S170 단계에서 태그로부터 수신한 제2 RN16인 핸들을 포함하여 전송한다. 리더는 태그의 비밀키를 모르기 때문에, 항상 평문으로 데이터를 전송한다. 리더로부터 보안 파라미터 요청 메시지를 수신한 태그는, 보안 파라미터를 회신한다(S190).

[0036] 리더는 태그가 가지고 있는 데이터를 암호화한 암호 데이터(Auth_data)를 얻기 위해 태그에 암호 데이터 요청(Req_Auth) 명령을 전달하는데(S200), 이 명령은 챌린지(challenge)용으로 리더가 생성한 16비트의 랜덤 넘버인 Ch16과 S170 단계에서 수신한 제2 RN16인 핸들을 파라미터로 갖는다. 암호 데이터 요청 명령을 수신한 태그는 암호 데이터를 만들기 위해 새로운 랜덤 넘버인 newRN16을 생성하고, 이 newRN16과 리더로부터 수신한 Ch16을 조합하여(XOR) 인증 데이터를 만든 후, newRN16과 인증 데이터를 암호화한다(S210).

[0037] 암호화에 사용되는 세션 키는 태그가 내장하고 있는 비밀키 K와 S110 단계에서 생성한 제1 RN16으로부터 생성된다. 세션 키 생성 방법에 대해서는 다양한 알고리즘이 사용될 수 있으며, 본 발명의 실시예에서는 구체적인 방법을 규정하지는 않는다. 그 후 태그는 암호화된 newRN16과 인증 데이터를 파라미터로 포함하여 리더로 회신한다(S220). 이때 보안 파라미터 요청과 인증 데이터 요청에 대한 명령/응답 메시지 포맷은 표 2 내지 표 5와 같다.

[0038] [표 2]

[0039]

	명령(Command)	랜덤 넘버(RN)	CRC-16
크기(#of bits)	16	16	16
설명(description)	0xE101	handle	

[0040] [표 3]

[0041]

	헤더(Header)	보안 파라미터 (SecParam)	랜덤 넘버(RN)	CRC-16
크기(#of bits)	1	16	16	16
설명(description)	0 or 1	SecParam	handle	

[0042] [표 4]

[0043]

	명령(Command)	Challenge	랜덤 넘버(RN)	CRC-16
크기(#of bits)	16	16	16	16
설명(description)	0xE104	Ch16	handle	

[0044] [표 5]

[0045]

	명령 (Command)	랜덤 넘버(RN)	인증 데이터 (Auth_data)	랜덤 넘버(RN)	CRC-16
크기(#of bits)	16	16	16	16	16
설명 (description)	0xE104	newRN16	Ch16 ?? newRN16	handle	

[0046] 표 2 내지 표 5의 명령어 코드(Command Code)는 예로 든 값인데, 표준의 Reserved 영역에 있는 값 중 하나이며, 반드시 이와 같이 한정되는 것은 아니다.

[0047] 표 2는 보안 파라미터 요청 메시지로 S180 단계를 통해 리더에서 태그로 전송되는 것이고, 표 3은 보안 파라미터 요청 메시지에 대한 응답(Reply)으로 S190 단계를 통해 태그에서 리더로 전송되는 것이다. 표 4는 인증 데이터 요청으로 S200 단계를 통해 리더에서 태그로 전송되는 것이고, 표 5는 인증 데이터 요청에 대한 응답으로 S220 단계를 통해 태그에서 리더로 전송되는 것이다. 이때, 표 5의 랜덤 넘버와 인증 데이터는 암호화된 형태이며, 나머지 값들은 평문으로 전송된다.

[0048] 도 3을 이어 설명하면, 인증 데이터까지 수신한 리더는 태그와의 통신을 끝내고 인증 서버와의 통신을 통해, 태그가 보내온 값들을 검증함으로써 진품 여부를 판단한다. 즉, 리더는 인증 서버에 태그 인증 요청(Req_Verify) 메시지를 전송한다(S230). 이때 메시지에 포함되는 파라미터로는 태그의 UII, 제1 RN16, 보안 파라미터, Ch16, S220 단계에서 받은 암호화된 형태의 newRN16과 인증 데이터가 포함된다.

[0049] 인증 서버는 리더로부터 수신한 메시지를 토대로 태그에 대한 인증을 수행한다(S240). 먼저 인증 서버는 UII와 관련된 비밀키 K를 검색하고, 제1 RN16과 K로부터 세션 키를 생성한다. 세션 키 생성 방법에 대해서는 다양한 알고리즘이 사용될 수 있으나, 본 발명의 실시예에서는 태그와 리더가 동일한 알고리즘을 사용한다고 예를 들어 설명한다. 그러나, 반드시 이와 같이 한정되는 것은 아니다. 인증 서버가 세션 키를 생성한 후, 세션 키를 이용하여 암호화된 newRN16을 복호화 하여 newRN16을 찾아낸다.

[0050] Ch16과 찾아낸 newRN16을 연산하여(XOR), 인증 데이터를 구한다. 인증 서버는 자신이 자체적으로 구한 인증 데이터 값과 리더로부터 수신한 인증 데이터 값을 비교한다. 비교를 통해 만약 두 값이 동일하면 인증에 성공, 동일하지 않다면 인증에 실패했다고 판단한다. 그리고 이에 대한 결과를 리더에 회신한다(S250). 이와 같은 절차를 통해 태그 인증 모드의 동작이 수행된다.

[0051] 다음 표 1의 보안 모드 값이 10인 모드 3은 그룹 키 관리 모드라고도 하며, 이 모드의 대표적인 서비스는 모바일 RFID 기술을 활용한 개인 소유물 관리 서비스이다. RFID 태그가 부착된 제품을 개인이 구입하여 개인 소유물이 되면, 소유자가 RFID 태그에 직접 비밀키를 입력하면서 보안 모드 값을 이진수 "10"으로 설정한다.

[0052] 이 모드의 주요 특징은 개인 소유화된 RFID 태그의 단일 아이템 지시자가 암호화되어 전송된다는 것이다. 또한, 키 관리가 개인에게 맡겨지므로, 그룹 키로 관리된다는 것이다. 여기서 그룹 키로 관리된다라고 함은, 모드 3의 경우에는 비밀키를 알아야만 단일 아이템 지시자를 알 수 있는 프로토콜을 사용하기 때문에, 소유자가 RFID 태그 정보를 활용하기 위해서는 자신이 소유한 모든 태그의 비밀키를 알고 있어야만 한다. 그러나, 단일 아이템 지시자를 모르는 상황에서 소유자가 모든 태그의 비밀키를 개별적으로 관리한다는 것은 키 관리 부담이 크기 때문에, 소유자는 자신이 소유한 모든 태그에 대해서 하나의 그룹으로 인지하여 하나의 그룹 키로 관리하게 된다.

[0053] 마지막으로 표 1의 보안 모드 값이 11인 모드 4는 개별 키 관리 모드라고도 하며, 모드 2의 태그 인증 모드와 모드 3의 키 관리 모드 특징을 동시에 가진다. 모드 4는 RFID 태그 인증 및 데이터 보호가 필요한 모든 서비스에 활용될 수 있다.

[0054] 모드 4에서는 RFID 태그는 자신의 단일 아이템 지시자를 암호화하여 리더로 전달할 뿐만 아니라 RFID 태그에 저장된 데이터도 암호화되어 전송된다. 이때, 암호화에 사용되는 비밀키가 개별 RFID 태그마다 다르게 사용된다. 이러한 경우, 리더가 각각의 RFID 태그 비밀키를 사용하기 때문에 보안성이 강화된다. 본 발명의 실시예에서는 모드 2에 대한 구체적인 프로토콜은 도 3을 통해 상세히 설명하였으나, 모드 3과 모드 4에 대한 구체적인 프로토콜에 대해서는 설명을 생략하기로 한다.

[0055] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

[0056] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면의 간단한 설명

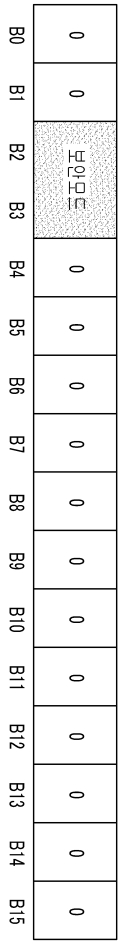
[0057] 도 1은 본 발명의 실시예에 따른 보안 모드를 지시하는 데이터 포맷의 예시도이다.

[0058] 도 2는 본 발명의 실시예에 따른 응용 서비스별 보안 취약성의 예시도이다.

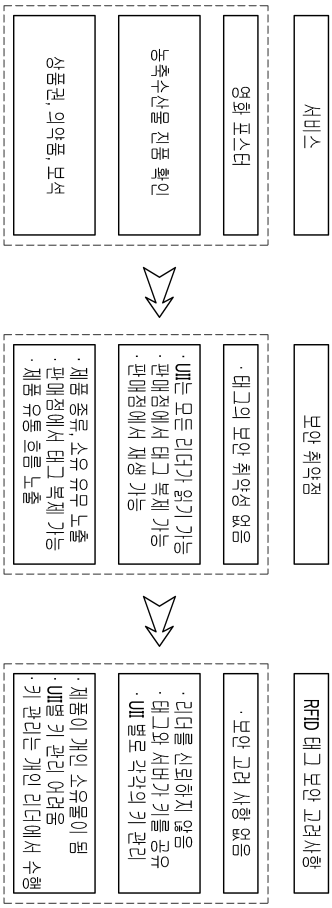
[0059] 도 3은 본 발명의 실시예에 따른 태그 인증 모드의 동작을 나타낸 흐름도이다.

도면

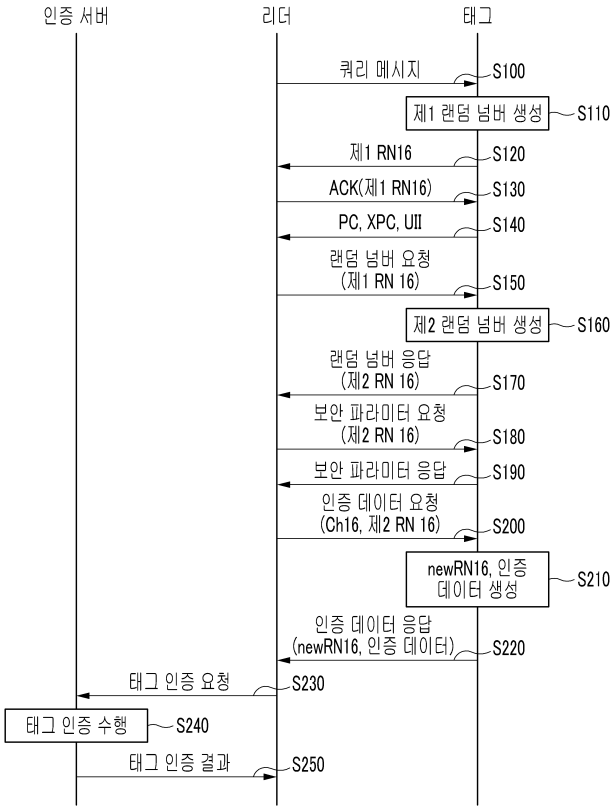
도면1


B0
B1
B2
B3
B4
B5
B6
B7
B8
B9
B10
B11
B12
B13
B14
B15
0
0
보안모드
0
0
0
0
0
0
0
0
0
0
0

도면2


서비스
영화 포스터
농축수산물 진품 확인
상품권, 의약품, 보석
보안 취약점
· 태그의 보안 취약성 없음
· UII는 모든 리더가 읽기 가능
· 판매점에서 태그 복제 가능
· 제품 종류 소유 유무 노출
· 판매점에서 태그 복제 가능
· 제품 유통 흐름 노출
RFID 태그 보안 고려사항
· 보안 고려 사항 없음
· 리더를 신뢰하지 않음
· 태그와 서버가 키를 공유
· UII별로 각각의 키 관리
· 제품이 개인 소유물이 됨
· UII별 키 관리 어려움
· 키 관리는 개인 리더에서 수행

도면3


인증 서버
리더
태그
쿼리 메시지
S100
제1 랜덤 넘버 생성
S110
제1 RN16
S120
ACK(제1 RN16)
S130
PC, XPC, UII
S140
랜덤 넘버 요청
(제1 RN 16)
S150
제2 랜덤 넘버 생성
S160
랜덤 넘버 응답
(제2 RN 16)
S170
보안 파라미터 요청
(제2 RN 16)
S180
보안 파라미터 응답
S190
인증 데이터 요청
(Ch16, 제2 RN 16)
S200
newRN16, 인증
데이터 생성
S210
인증 데이터 응답
(newRN16, 인증 데이터)
S220
태그 인증 요청
S230
태그 인증 수행
S240
태그 인증 결과
S250