



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년12월13일
(11) 등록번호 10-1686200
(24) 등록일자 2016년12월07일

(51) 국제특허분류(Int. Cl.)
G06K 7/10 (2006.01) H04L 9/32 (2006.01)
(52) CPC특허분류
G06K 7/10039 (2013.01)
H04L 9/3273 (2013.01)
(21) 출원번호 10-2015-0155943
(22) 출원일자 2015년11월06일
심사청구일자 2015년11월06일
(56) 선행기술조사문헌
KR1020120100434 A*
KR1020150122281 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이원준
서울특별시 강남구 선릉로 221, 104동 2005호 (도곡동, 도곡렉슬아파트)
이현준
서울특별시 성북구 삼선교로23가길 47, 201호 (삼선동4가)
유지은
경기도 광주시 오포읍 새말길 174-24, 101동 201호 (산하아크로빌)
(74) 대리인
특허법인엠에이피에스

전체 청구항 수 : 총 9 항

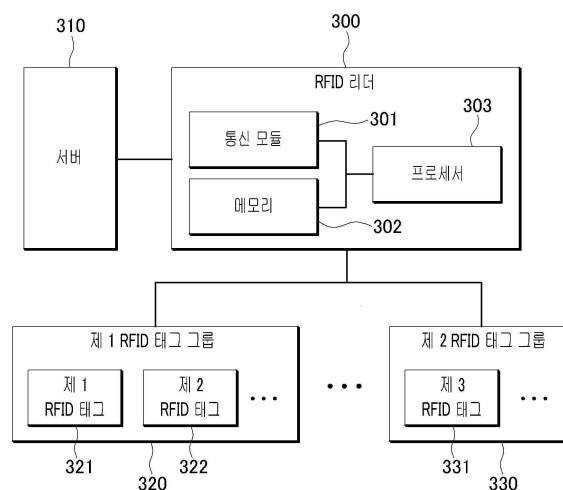
심사관 : 김병성

(54) 발명의 명칭 RFID 태그와의 상호 인증을 위한 RFID 리더 및 이를 이용한 상호 인증 방법

(57) 요약

본 발명은 RFID 태그와 통신을 수행하는 통신 모듈, 상호 인증 프로그램이 저장된 메모리 및 메모리에 저장된 프로그램을 실행하는 프로세서를 포함한다. 이때, 프로세서는 프로그램의 실행에 따라, 통신 모듈을 통하여, 미리 정해진 범위 내의 복수의 RFID 태그에 상호 인증 명령을 전송하고, 상호 인증 명령에 포함된 보안 기법 식별자에 대응하는 RFID 태그와 상호 인증을 수행한 이후, 상호 인증을 수행한 RFID 태그에 포함된 메모리에 기저장된 데이터를 읽거나, RFID 태그에 포함된 메모리에 새로운 데이터를 저장하는 것 중 어느 하나 이상을 수행한다. 그리고 RFID 태그는 복수의 RFID 태그 그룹 중 어느 하나에 포함되며, 각각 서로 상이하고 주기적으로 갱신되는 하나 이상의 보안 기법 식별자를 포함하고, RFID 태그 그룹은 복수의 RFID 태그 및 업데이트 보안 기법 식별자를 포함한다.

대표도 - 도3



(52) CPC특허분류

H04L 2209/805 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711024057

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 중견연구자지원

연구과제명 무선 네트워킹 클라우드 설계 및 성능 최적화 기술

기 여 율 1/1

주관기관 고려대학교

연구기간 2015.06.01 ~ 2016.05.31

명세서

청구범위

청구항 1

RFID 태그와 상호 인증하는 RFID 리더에 있어서,
 RFID 태그와 통신을 수행하는 통신 모듈,
 상호 인증 프로그램이 저장된 메모리 및
 상기 메모리에 저장된 프로그램을 실행하는 프로세서를 포함하고,
 상기 프로세서는 상기 프로그램의 실행에 따라, 상기 통신 모듈을 통하여, 미리 정해진 범위 내의 복수의 RFID 태그에 상호 인증 명령을 전송하고,
 상기 상호 인증 명령에 포함된 보안 기법 식별자에 대응하는 RFID 태그와 상호 인증을 수행한 이후, 상기 상호 인증을 수행한 RFID 태그에 포함된 메모리에 기저장된 데이터를 읽거나, 상기 RFID 태그에 포함된 메모리에 새로운 데이터를 저장하는 것 중 어느 하나 이상을 수행하되,
 상기 RFID 태그는 복수의 RFID 태그 그룹 중 어느 하나에 포함되며, 각각 서로 상이하고 미리 정해진 주기에 따라 주기적으로 갱신되는 하나 이상의 보안 기법 식별자를 포함하고,
 상기 미리 정해진 주기는 상기 RFID 태그 및 상기 RFID 리더에 대응하는 공격자의 공격 성공 시간에 기초하여 결정되는 것이고,
 상기 공격자의 공격 성공 시간은 상기 보안 기법 식별자의 크기 및 상기 공격자의 1회 공격 소요 시간에 기초하여 산출된 것이며,
 상기 RFID 태그 그룹은 복수의 RFID 태그 및 업데이트 보안 기법 식별자를 포함하는, RFID 리더.

청구항 2

제 1 항에 있어서,
 상기 프로세서는 미리 정해진 주기에 따라, 상기 복수의 RFID 태그 그룹 중 보안 기법 식별자 갱신 대상 RFID 태그 그룹에 대한 업데이트 보안 기법 식별자가 포함된 갱신 명령을 브로드캐스팅 하고,
 상기 브로드캐스팅 한 갱신 명령에 대응하는 RFID 태그 그룹에 포함된 복수의 RFID 태그의 보안 기법 식별자를 갱신하고, 상기 브로드캐스팅한 갱신 명령에 대응하는 RFID 태그 그룹의 업데이트 보안 기법 식별자를 갱신 하는, RFID 리더.

청구항 3

삭제

청구항 4

제 1 항에 있어서,
 상기 RFID 태그 그룹에 포함된 RFID 태그의 개수는 상기 미리 정해진 주기 및 상기 RFID 태그 그룹의 개수에 기초하여 산출되는 것인, RFID 리더.

청구항 5

제 1 항에 있어서,
 상기 RFID 태그 그룹의 업데이트 보안 기법 식별자와 상기 RFID 태그 그룹에 포함된 복수의 RFID 태그의 상기 보안 기법 식별자는 서로 상이하게 설정되는 것인, RFID 리더.

청구항 6

제 1 항에 있어서,

상기 RFID 태그 그룹의 업데이트 보안 기법 식별자는 각각 상이하게 설정되는 것인, RFID 리더.

청구항 7

RFID 리더에서 수행되는 RFID 태그와의 상호 인증 방법에 있어서,

미리 정해진 범위 내의 복수의 RFID 태그에 상호 인증 명령을 전송하는 단계;

상기 상호 인증 명령을 전송하는 단계 이후에, 상기 상호 인증 명령에 포함된 보안 기법 식별자에 대응하는 RFID 태그와 상호 인증을 수행하는 단계; 및

상기 상호 인증을 수행하는 단계 이후에, 상기 상호 인증을 수행한 RFID 태그에 포함된 메모리에 기저장된 데이터를 읽거나, 상기 RFID 태그에 포함된 메모리에 새로운 데이터를 저장하는 것 중 어느 하나 이상을 수행하는 단계를 포함하되,

상기 RFID 태그는 복수의 RFID 태그 그룹 중 어느 하나에 포함되며, 각각 서로 상이하고 상기 RFID 리더에 의해 미리 정해진 주기에 따라 주기적으로 갱신되는 하나 이상의 보안 기법 식별자를 포함하고,

상기 미리 정해진 주기는 상기 RFID 태그 및 상기 RFID 리더에 대응하는 공격자의 공격 성공 시간에 기초하여 결정되는 것이고,

상기 공격자의 공격 성공 시간은 상기 보안 기법 식별자의 크기 및 상기 공격자의 1회 공격 소요 시간에 기초하여 산출된 것이며,

상기 RFID 태그 그룹은 복수의 RFID 태그 및 업데이트 보안 기법 식별자를 포함하는, RFID 리더의 상호 인증 방법.

청구항 8

제 7 항에 있어서,

상기 RFID 태그에 상호 인증 명령을 전송하는 단계 이전에,

미리 정해진 주기에 따라, 상기 복수의 RFID 태그 그룹 중 보안 기법 식별자 갱신 대상 RFID 태그 그룹에 대한 업데이트 보안 기법 식별자가 포함된 갱신 명령을 브로드캐스팅 하는 단계;

상기 갱신 명령을 브로드캐스팅 하는 단계 이후에, 상기 브로드캐스팅한 갱신 명령에 대응하는 RFID 태그 그룹에 포함된 복수의 RFID 태그의 보안 기법 식별자를 갱신하는 단계; 및

상기 복수의 RFID 태그의 보안 기법 식별자를 갱신하는 단계 이후에, 상기 브로드캐스팅한 갱신 명령에 대응하는 RFID 태그 그룹의 업데이트 보안 기법 식별자를 갱신하는 단계를 더 포함하는, RFID 리더의 상호 인증 방법.

청구항 9

삭제

청구항 10

제 7 항에 있어서,

상기 RFID 태그 그룹에 포함된 RFID 태그의 개수는 상기 미리 정해진 주기 및 상기 RFID 태그 그룹의 개수에 기초하여 산출되는 것인, RFID 리더의 상호 인증 방법.

청구항 11

제 7 항, 제 8 항 및 제 10 항 중 어느 한 항에 기재된 방법을 컴퓨터 상에서 수행하기 위한 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

발명의 설명

기술 분야

[0001] 본 발명은 RFID 태그와의 상호 인증을 위한 RFID 리더 및 이를 이용한 상호 인증 방법에 관한 것이다.

배경 기술

[0002] EPC-C1G2(electronic product code class-1 generation-2) 표준은 GS1(global standard No. 1)의 RFID(radio-frequency identification) 연구 그룹인 EPC 글로벌(EPC global)과 ISO(international organization for standardization)를 중심으로 제정되었다. EPC C1G2 표준은 860MHz ~ 960MHz 대역에서 작동하는 RFID 시스템을 위한 것으로 RFID 리더(RFID reader)로 구현되는 interrogator 및 RFID 태그(RFID tag)로 구현되는 label을 포함할 수 있다.

[0003] RFID 리더는 초기화(initialization), 상호 인증(mutual authentication) 및 RFID 태그에 포함된 메모리를 읽고 쓸 수 있다. 이때, 상호 인증은 RFID 리더가 메모리에 접속하고자 하는 RFID 태그에 상호 인증 명령을 전송하여 수행될 수 있다. 예를 들어, RFID 리더는 메모리에 접속하고자 하는 RFID 태그에 상호 인증 방법을 포함하는 보안 기법 식별자(cryptographic suite indicator; CSI)를 포함하는 상호 인증 명령을 통보할 수 있다. 그리고 RFID 리더는 상호 인증 명령에 따라, RFID 태그와 상호 인증을 수행할 수 있다.

[0004] 이때, 보안 기법 식별자는 상호 인증 방법에 따라 상이할 수 있다. 그러나 보안 기법 식별자는 암호화되지 않으므로, 보안 기법 식별자를 재사용하여 공격하는 재사용 공격(replay attack) 및 보안 기법 식별자가 될 수 있는 가능한 모든 값을 입력하여 공격하는 무차별 대입 공격(brute force attack) 등과 같은 공격에 노출될 가능성이 높다.

[0005] 이와 관련되어, 한국 공개특허공보 제10-2013-0059054호(발명의 명칭: "RFID 액세스 단말기 및 RFID 태그 정보 인증 방법")는 RFID 태그를 이용한 인증방법을 개시하고 있다. 구체적으로 이 발명은 RFID 태그의 사용자 영역에 생산 정보 및 유통 정보를 위한 필드가 정의되며, 생산 정보 및 유통 정보는 각 생산자 및 유통자만 기록할 수 있도록 암호화한다. 그리고 이 발명은 RFID 인증장치가 서버로 TID를 전송하고 암호화 키를 제공받아 복호화한 생산 정보와 유통정보를 서버에 송신함으로써 인증을 받는다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, RFID 태그와의 상호 인증을 위하여, RFID 태그의 그룹을 생성하고, RFID 태그 그룹별로 보안 기법 식별자를 갱신하는 RFID 리더 및 RFID 리더를 이용한 상호 인증 방법을 제공한다.

[0007] 다만, 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

과제의 해결 수단

[0008] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 RFID 태그와 상호 인증하는 RFID 리더는 RFID 태그와 통신을 수행하는 통신 모듈, 상호 인증 프로그램이 저장된 메모리 및 메모리에 저장된 프로그램을 실행하는 프로세서를 포함한다. 이때, 프로세서는 프로그램의 실행에 따라, 통신 모듈을 통하여, 미리 정해진 범위 내의 복수의 RFID 태그에 상호 인증 명령을 전송하고, 상호 인증 명령에 포함된 보안 기법 식별자에 대응하는 RFID 태그와 상호 인증을 수행한 이후, 상호 인증을 수행한 RFID 태그에 포함된 메모리에 기저장된 데이터를 읽거나, RFID 태그에 포함된 메모리에 새로운 데이터를 저장하는 것 중 어느 하나 이상을 수행한다. 그리고 RFID 태그는 복수의 RFID 태그 그룹 중 어느 하나에 포함되며, 각각 서로 상이하고 주기적으로 갱신되는 하나 이상의 보안 기법 식별자를 포함하고, RFID 태그 그룹은 복수의 RFID 태그 및 업데이트 보안 기법 식별자를 포함한다.

[0009] 또한, 본 발명의 제 2 측면에 따른 RFID 리더에서 수행되는 RFID 태그와의 상호 인증 방법은 미리 정해진 범위 내의 복수의 RFID 태그에 상호 인증 명령을 전송하는 단계; 상호 인증 명령을 전송하는 단계 이후에, 상호 인증 명령에 포함된 보안 기법 식별자에 대응하는 RFID 태그와 상호 인증을 수행하는 단계; 및 상호 인증을 수행하는 단계 이후에, 상호 인증을 수행한 RFID 태그에 포함된 메모리에 기저장된 데이터를 읽거나, RFID 태그에 포함된

메모리에 새로운 데이터를 저장하는 것 중 어느 하나 이상을 수행하는 단계를 포함한다. 이때, RFID 태그는 복수의 RFID 태그 그룹 중 어느 하나에 포함되며, 각각 서로 상이하고 RFID 리더에 의해 주기적으로 갱신되는 하나 이상의 보안 기법 식별자를 포함하고, RFID 태그 그룹은 복수의 RFID 태그 및 업데이트 보안 기법 식별자를 포함한다.

발명의 효과

[0010] 본 발명은 RFID 표준에서 RFID 리더를 이용하여 상호 인증 명령의 헤더에 암호화되지 않았던 보안 기법 식별자를 암호화하는 방법을 제공한다. 또한, 본 발명은 복수의 RFID 태그를 포함하는 RFID 태그 그룹을 설정하므로, RFID 태그의 개수가 증가하더라도 RFID 태그 그룹의 업데이트 보안 기법 식별자 및 RFID 태그의 보안 기법 식별자에 대한 랜덤성을 보장할 수 있다.

[0011] 그러므로 본 발명은 공격자가 보안 기법 식별자를 수집하여 공격을 하더라도 RFID 태그에 저장된 값을 안전하게 지킬 수 있다.

도면의 간단한 설명

[0012] 도 1은 종래의 RFID 리더의 상호 인증 과정의 흐름도이다.

도 2는 종래의 RFID 태그에 저장된 보안 기법 식별자의 예시도이다.

도 3은 본 발명의 일 실시예에 따른 RFID 시스템의 블록도이다.

도 4는 본 발명의 일 실시예에 따른 RFID 태그 및 RFID 태그 그룹을 설명하기 위한 예시도이다.

도 5는 본 발명의 일 실시예에 따른 RFID 리더의 상호 인증 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 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 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한, 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.

[0015] 다음은 도 1 및 도 2를 참조하여, 종래의 RFID 리더(110)에서의 상호 인증 과정을 설명한다.

[0016] 도 1은 종래의 RFID 리더(110)의 상호 인증 과정의 흐름도이다.

[0017] EPC C1G2 표준에서 RFID 리더(110)는 인식 범위 내의 RFID 태그에 RFID 태그의 고유 번호를 포함하는 EPC를 요청한다(S100). 예를 들어, 도 1과 같이, 인식 범위 내에 제 1 RFID 태그(120), 제 2 RFID 태그(130) 및 제 3 RFID 태그(140)가 포함될 때, RFID 리더(110)는 제 1 RFID 태그(120), 제 2 RFID 태그(130) 및 제 3 RFID 태그(140)에 EPC 요청을 전송할 수 있다(S100).

[0018] RFID 리더(110)로부터 EPC 요청을 받은 제 1 RFID 태그(120), 제 2 RFID 태그(130) 및 제 3 RFID 태그(140)는 EPC 요청에 대응하여, 각각의 EPC를 RFID 리더(110)에 전송한다(S105).

[0019] RFID 리더(110)는 제 1 RFID 태그(120), 제 2 RFID 태그(130) 및 제 3 RFID 태그(140)의 EPC를 수신하면, 서버(100)로 제 1 RFID 태그(120), 제 2 RFID 태그(130) 및 제 3 RFID 태그(140)의 EPC를 전송한다(S110). 그리고 RFID 리더(110)는 서버(100)로부터 RFID 태그와의 상호 인증에 필요한 정보를 수신한다(S115). 그리고 서버(100)로부터 상호 인증에 필요한 정보를 수신한 RFID 리더(110)는 메모리에 접속하고자 하는 RFID 태그에게 상호 인증 명령을 전송한다(S120, S130, S140). 상호 인증 명령에 대응하여 RFID 태그의 상호 인증이 성공하면, RFID 리더(110)는 상호 인증을 성공한 RFID 태그의 메모리에 대한 읽기 또는 쓰기를 수행한다(S125, S135, S145).

[0020] 예를 들어 RFID 리더(110)가 제 1 RFID 태그(120)의 메모리에 대하여 읽기/쓰기를 수행하고자 한다면, 먼저

RFID 리더(110)는 제 1 RFID 태그(120)에 상호 인증 명령을 전송할 수 있다(S110). 이때, 상호 인증 명령은 도 2와 같이, 상호 인증 알고리즘에 대한 정보를 포함하는 보안 기법 식별자(cryptographic suite indicator; CSI)를 포함할 수 있다.

[0021] 도 2는 종래의 RFID 태그에 저장된 보안 기법 식별자의 예시도이다.

[0022] 이때, 상호 인증 알고리즘은 사전에 협의한 절차에 따라, RFID 리더(110) 및 RFID 태그 간의 인증을 수행할 수 있는 알고리즘이다. 이를 위하여, RFID 태그는 RFID 태그마다 하나 이상의 보안 기법 식별자를 포함할 수 있다. 이때, RFID 태그 내의 하나 이상의 보안 기법 식별자는 상호 인증 알고리즘에 따라 각각 상이한 값을 가질 수 있다.

[0023] 다시 도 1 및 도 2를 참조하면, RFID 리더(110)가 보안 기법 식별자 'CSI: 1'을 포함한 상호 인증 명령을 제 1 RFID 태그(120)에 전송하면, 제 1 RFID 태그(120)는 보안 기법 식별자 값이 'CSI: 1'인 상호 인증 알고리즘을 이용하여, RFID 리더(110)와 상호 인증을 수행할 수 있다.

[0024] 이와 같이, 종래의 RFID 리더에서의 상호 인증 방법에서는 RFID 리더(110) 및 RFID 태그가 동일한 보안 기법 식별자를 저장한다. 그러나 종래의 상호 인증 알고리즘에서는 RFID 리더(110) 및 RFID 태그 간에 상호 인증 명령이 송수신 될 때, 상호 인증 명령의 헤더를 암호화하지 못한 상태에서 전송할 수 있다. 그러므로 RFID 태그에 대한 공격자는 상호 인증 명령에 포함된 암호화되지 않은 정보를 수집하여, 공격에 사용할 수 있다.

[0025] 다음은 도 3 및 도 4에 기초하여, 본 발명의 일 실시예에 따른 RFID 리더(300)를 설명한다.

[0026] 도 3은 본 발명의 일 실시예에 따른 RFID 시스템의 블록도이다.

[0027] RFID 시스템은 RFID 리더(300), 복수의 RFID 태그(321, 322, 331) 및 서버(310)를 포함한다. 이때, 복수의 RFID 태그(321, 322, 331)는 RFID 태그 그룹핑에 따라, 각각 RFID 태그 그룹(320, 330)에 포함될 수 있다.

[0028] 예를 들어, RFID 시스템은 거리상으로 가까운 복수의 RFID 태그(321, 322, 331)를 하나의 RFID 태그 그룹으로 생성하는 RFID 태그 그룹핑을 수행하거나, RFID 시스템에 등록되는 순서에 따라 복수의 RFID 태그(321, 322, 331)를 하나의 RFID 태그 그룹으로 생성하는 RFID 태그 그룹핑을 수행할 수 있다. 또한, RFID 시스템은 RFID 시스템 관리자가 미리 설정된 방법을 통하여, RFID 태그 그룹핑을 수행할 수 있으나, 이에 한정된 것은 아니다.

[0029] 서버(310)는 RFID 리더(300) 및 RFID 태그(321, 322, 331) 간의 상호 인증을 위한 데이터를 저장할 수 있다. 구체적으로 서버(310)는 RFID 리더(300)로부터 EPC를 전송한 RFID 태그(321, 322, 331)의 EPC를 수신할 수 있다. 그리고 서버(310)는 EPC를 수신한 RFID 리더(300)에 EPC를 전송한 RFID 태그(321, 322, 331)와의 상호 인증과 관련된 데이터를 전송할 수 있다.

[0030] RFID 태그(321, 322, 331)는 RFID 태그(321, 322, 331)에 포함된 메모리에 RFID 태그(321, 322, 331)의 고유 번호를 포함하는 EPC를 저장할 수 있다. 또한, RFID 태그(321, 322, 331)는 메모리에 RFID 리더(300)와의 상호 인증을 위한 보안 기법 식별자를 저장할 수 있다. 구체적으로 RFID 태그(321, 322, 331)는 RFID 리더(300)의 EPC 요청에 대응하여 RFID 리더(300)에 고유 번호를 포함하는 EPC를 전송할 수 있다. 또한, RFID 태그(321, 322, 331)는 RFID 리더(300)의 상호 인증 요청 명령에 따라, RFID 리더(300)와 상호 인증을 수행할 수 있다.

[0031] RFID 리더(300)는 RFID 태그(321, 322, 331)에 접속하여 RFID 태그(321, 322, 331)에 포함된 메모리에 정보를 수신하거나, 정보를 기록할 수 있다. 또한, RFID 리더(300)는 RFID 태그(321, 322, 331)에 포함된 보안 기법 식별자를 갱신할 수 있다. 이때, RFID 리더(300)는 통신 모듈(301), 메모리(302) 및 프로세서(303)를 포함한다.

[0032] RFID 리더(300)의 통신 모듈(301)은 RFID 태그(321, 322, 331) 및 서버(310)와 데이터 통신을 수행한다. 이때, 통신 모듈(301)은 RFID 태그(321, 322, 331)와의 통신을 위한 RFID 통신 모듈 및 서버(310)와의 데이터 통신을 위한 데이터 통신 모듈을 포함할 수 있다.

[0033] 메모리(302)는 상호 인증 프로그램이 저장된다. 이때, 메모리(302)는 전원이 공급되지 않아도 저장된 정보를 계속 유지하는 비휘발성 저장장치 및 저장된 정보를 유지하기 위하여 전력이 필요한 휘발성 저장장치를 통칭하는 것이다.

[0034] 프로세서(303)는 메모리(302)에 상호 인증 프로그램을 실행한다. 구체적으로 프로세서(303)는 통신 모듈(301)을 통하여, 미리 정해진 범위 내의 복수의 RFID 태그(321, 322, 331)에 상호 인증 명령을 전송한다. 이때, 미리 정해진 범위는 RFID 리더(300)의 통신 모듈(301)을 통하여 인식되는 주파수에 따라 상이할 수 있다.

- [0035] 또한, 프로세서(303)가 상호 인증 명령을 전송하는 복수의 RFID 태그(321, 322, 331)는 앞에서 설명한 바와 같이, EPC C1G2 표준에 따라, 통신 모듈(301)을 통하여 프로세서(303)와 EPC를 교환한 RFID 태그(321, 322, 331)일 수 있다.
- [0036] 구체적으로 RFID 리더(300)의 프로세서(303)가 미리 정해진 범위 내의 RFID 태그(321, 322, 331)에 EPC를 요청하면, EPC 요청을 수신한 미리 정해진 범위 내의 복수의 RFID 태그(321, 322, 331)는 각각 RFID 리더(300)에 EPC를 전송할 수 있다. 그리고 프로세서(303)는 통신 모듈(301)을 통하여, 복수의 RFID 태그(321, 322, 331) 각각으로부터 EPC를 수신한 다음, 서버(310)로 수신한 EPC를 전송할 수 있다.
- [0037] 프로세서(303)는 통신 모듈(301)을 통하여, 서버(310)로부터 전송한 EPC에 대응하는 데이터를 수신할 수 있다. 이때, EPC에 대응하는 데이터는 서버(310)에 기저장된 복수의 RFID 태그(321, 322, 331)에 대한 상호 인증을 위한 데이터일 수 있다.
- [0038] 프로세서(303)는 상호 인증 명령을 전송한 이후, 상호 인증 명령에 포함된 보안 기법 식별자에 대응하는 RFID 태그(321, 322, 331)와 상호 인증을 수행할 수 있다. 상호 인증에 성공한 이후, 프로세서(303)는 RFID 태그(321, 322, 331)에 포함된 메모리(302)에 기저장된 데이터를 읽거나, 새로운 데이터를 저장하는 것 중 어느 하나 이상을 수행할 수 있다.
- [0039] 한편, 프로세서(303)가 전송하는 상호 인증 명령은 RFID 태그(321, 322, 331)에 대한 보안 기법 식별자를 포함한다. 이때, 보안 기법 식별자는 프로세서(303)에 의해 주기적으로 갱신된 후 RFID 태그(321, 322, 331)로 전송된다. 프로세서(303)는 복수의 RFID 태그(321, 322, 331)를 포함하는 RFID 태그 그룹(320, 330)을 통하여, 주기적으로 RFID 태그(321, 322, 331)에 포함된 보안 기법 식별자를 갱신할 수 있다.
- [0040] 구체적으로 프로세서(303)는 미리 정해진 주기에 따라, 복수의 RFID 태그 그룹(320, 330) 중 보안 기법 식별자 갱신 대상 RFID 태그 그룹(320, 330)에 갱신 명령을 브로드캐스팅 할 수 있다. 이때, 갱신 명령은 EPC C1G2 표준에서의 'challenge' 명령을 이용할 수 있다.
- [0041] 갱신 명령을 수신한 갱신 대상 RFID 태그 그룹에 포함된 복수의 RFID 태그는 수신한 갱신 명령에 저장되어 있는 보안 기법 식별자에 기초하여, RFID 태그의 메모리에 기저장된 보안 기법 식별자를 갱신할 수 있다. 또한, 갱신이 완료되면, RFID 태그는 상호 인증 명령 또는 다음 갱신 명령을 수신하기 전까지 대기할 수 있다.
- [0042] 한편, 프로세서(303)는 일반적인 암호 해독 시스템에서 암호를 해독하는데 까지 소요되는 시간을 예측하여, 미리 정해진 주기를 설정할 수 있다. 즉, 프로세서(303)는 RFID 태그(321, 322, 331)에서 공격자가 일정한 크기를 가지는 보안 기법 식별자를 탐지하는데 소요되는 시간을 예측하여 미리 정해진 주기를 산출할 수 있다.
- [0043] 예를 들어, 프로세서(303)는 보안 기법 식별자의 크기, RFID 시스템을 공격하는 공격자가 1회 공격을 하는데 소요되는 시간 및 공격을 성공하기까지 소요되는 시간에 기초하여 미리 정해진 주기를 산출할 수 있다. 만약, 보안 기법 식별자의 크기가 8비트(bit)이고, 공격자의 1회 공격 소요 시간이 200밀리초(millisecond)이며, [수학식 1]과 같이 Hellman의 공식에 기초하여 공격을 성공하기까지 소요되는 시간을 산출한다면, 프로세서(303)는 [수학식 2]과 같이, 미리 정해진 주기를 약 8초로 설정할 수 있다. [수학식 1]에서 O 는 공격 성공까지 소요되는 시간이며, N 은 공격하고자 하는 변수에 포함될 수 있는 값의 경우의 수가 될 수 있다. 그러므로 [수학식 1]에서 N 은 8비트 변수가 가질 수 있는 값의 경우의 수이므로, 2^8 이 될 수 있다. 이때, 미리 정해진 주기를 산출하는 일 예일뿐, 이에 한정된 것이 아니다.

수학식 1

$$O = N^{2/3}$$

[0044]

수학식 2

$$T = (2^8)^{2/3} \times 200ms$$

$$\approx 8,063.5ms$$

[0045]

[0046]

한편, 프로세서(303)가 브로드캐스팅하는 갱신 명령은 갱신 대상 RFID 태그 그룹(320, 330)의 업데이트 보안 기법 식별자(400, 410)를 포함할 수 있다. 그리고 프로세서(303)는 브로드캐스팅한 갱신 명령에 대응하는 RFID 태그 그룹에 포함된 복수의 RFID 태그(321, 322, 331)의 보안 기법 식별자를 갱신할 수 있다. RFID 태그 그룹에 포함된 복수의 RFID 태그(321, 322, 331)의 보안 기법 식별자를 갱신 한 이후, 프로세서(303)는 RFID 태그 그룹의 업데이트 보안 기법 식별자(400, 410)를 갱신할 수 있다. RFID 태그(321, 322, 331) 및 RFID 태그 그룹(320, 330)은 도 4를 참조하여 구체적으로 설명하기로 한다.

[0047]

도 4는 본 발명의 일 실시예에 따른 RFID 태그(321, 322, 331) 및 RFID 태그 그룹(320, 330)을 설명하기 위한 예시도이다.

[0048]

RFID 태그 그룹(320, 330)은 복수의 RFID 태그(321, 322, 331) 및 각각의 RFID 태그(321, 322, 331)에 대한 보안 기법 식별자 갱신을 위한 업데이트 보안 기법 식별자(400, 410)를 포함한다. 예를 들어, 제 1 RFID 태그 그룹(320)은 제 1 RFID 태그(321) 및 제 2 RFID 태그(322)와 제 1 RFID 태그 그룹(320)의 업데이트 보안 기법 식별자(400)를 포함한다. 그리고 제 2 RFID 태그 그룹(330)은 제 3 RFID 태그(331)와 제 2 RFID 태그 그룹(330)의 업데이트 보안 기법 식별자(410)를 포함할 수 있다.

[0049]

이때, RFID 태그 그룹(320, 330)은 RFID 태그 그룹(320, 330)에 포함된 복수의 RFID 태그(321, 322, 331)의 각각의 보안 기법 식별자를 갱신하기 위한 논리적인 그룹일 수 있다. 그러므로 RFID 태그 그룹(320, 330)은 RFID 태그 그룹(320, 330)에 포함된 복수의 RFID 태그(321, 322, 331)에 각각 저장된 업데이트 보안 기법 식별자(400, 410)에 의해 분류될 수 있다.

[0050]

예를 들어, 제 1 RFID 태그(321) 및 제 2 RFID 태그(322)가 동일한 업데이트 보안 기법 식별자(400)인 'CSIU: 11'을 포함한다면, 제 1 RFID 태그(321) 및 제 2 RFID 태그(322)를 동일한 그룹으로 분류할 수 있다. 또한, 제 1 RFID 태그(321)가 업데이트 보안 기법 식별자(400)인 'CSIU: 11'을 포함하고, 제 3 RFID 태그(331)가 업데이트 보안 기법 식별자(410)인 'CSIU: 12'를 포함한다면, 제 1 RFID 태그(321) 및 제 3 RFID 태그(331)는 상이한 그룹으로 분류할 수 있다.

[0051]

RFID 태그 그룹(320, 330)의 업데이트 보안 기법 식별자(400, 410)는 RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)의 보안 기법 식별자를 갱신 하기 위하여 사용될 수 있다. 즉, 프로세서(303)는 보안 기법 식별자를 갱신할 RFID 태그 그룹(320, 330)에 대한 업데이트 보안 기법 식별자(400, 410)를 포함하는 갱신 명령을 미리 정해진 범위 내의 복수의 RFID 태그(321, 322, 331)에 전송할 수 있다. 그리고 갱신 명령에 대응하는 RFID 태그 그룹(320, 330)에 포함된 복수의 RFID 태그(321, 322, 331)는 갱신 명령에 따라, 보안 기법 식별자를 갱신할 수 있다.

[0052]

이때, 복수의 RFID 태그 그룹(320, 330)의 업데이트 보안 기법 식별자(400, 410)가 동일한 경우, RFID 리더(300)의 프로세서(303)가 통신 모듈(301)을 통하여 전송한 업데이트 보안 기법 식별자(400, 410)에 복수의 RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)의 보안 기법 식별자가 동시에 변경될 수 있다. 그러므로 복수의 RFID 태그 그룹(320, 330)의 업데이트 보안 기법 식별자(400, 410)는 각각 상이하게 설정될 수 있다. 그리고 RFID 태그 그룹(320, 330)에 포함된 복수의 RFID 태그(321, 322, 331)의 업데이트 보안 기법 식별자(400, 410)는 해당 RFID 태그 그룹(320, 330)에 포함된 보안 기법 식별자와 상이하게 설정될 수 있다.

[0053]

다시 도 4를 참조하면, 제 1 RFID 태그 그룹(320)의 업데이트 보안 기법 식별자(400) 'CSIU: 11'은 제 2 RFID 태그 그룹(330)의 업데이트 보안 기법 식별자(410) 'CSIU: 12'와 상이하게 설정될 수 있다. 또한, 제 1 RFID 태그 그룹(320)의 업데이트 보안 기법 식별자(400)는 제 1 RFID 태그 그룹(320)에 포함된 제 1 RFID 태그(321)의 보안 기법 식별자 'CSI: 5' 및 'CSI: 7'과 상이하며, 제 2 RFID 태그(322)의 보안 기법 식별자 'CSI: 3' 및 'CSI: 9'와 상이할 수 있다.

[0054]

한편, 본 발명의 일 실시예에 따른 복수의 RFID 태그 그룹(320, 330)에 포함되는 RFID 태그(321, 322, 331)의

개수는 미리 정해진 주기 및 RFID 태그 그룹(320, 330)의 개수에 기초하여 산출될 수 있다. 이때, 프로세서(303)는 사용자가 요구하는 초당 상호 인증 횟수를 고려할 수 있다.

- [0055] 또는 복수의 RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)의 개수는 미리 정해진 주기, 업데이트 보안 기법 식별자(400, 410)를 결정하는 시간 및 1회 연산에 소요되는 시간에 기초하여 산출될 수 있다. 또한, 업데이트 보안 기법 식별자(400, 410)를 결정하는 시간은 RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)가 보안 기법 식별자를 결정하는 시간에 대한 기댓값에 기초하여 산출된다.
- [0056] 예를 들어, RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)의 개수는 미리 정해진 주기, 업데이트 보안 기법 식별자(400, 410)를 결정하는 시간 및 1회 연산에 소요되는 시간에 기초하여 산출된 최적화 식 및 최적화 식에서 값을 산출하기 위한 휴리스틱 검색 알고리즘(heuristic search algorithm)인 이진 검색(binary algorithm) 기반 지수 검색 알고리즘(exponential search algorithm)을 이용하여, 산출될 수 있다.
- [0057] 또한, RFID 태그 그룹(320, 330)의 수 및 RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)의 개수는 RFID 리더와 상호 인증을 수행하는 대상 RFID 태그(321, 322, 331)가 증감함에 따라, 갱신될 수 있다. 즉, RFID 리더는 미리 정해진 주기에 RFID 태그 그룹(320, 330)의 수 및 RFID 태그 그룹(320, 330)에 포함되는 RFID 태그(321, 322, 331)의 수를 변경하고, 변경된 RFID 태그 그룹(320, 330)의 수 및 RFID 태그 그룹(320, 330)에 포함될 RFID 태그(321, 322, 331)의 수에 따라, 보안 기법 식별자 및 업데이트 보안 기법 식별자(400, 410)를 갱신할 수 있다.
- [0058] 한편, RFID 태그(321, 322, 331)의 프로세서(303)는 하나의 RFID 태그 그룹(320, 330)의 업데이트 보안 기법 식별자(400, 410) 및 RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)의 보안 기법 식별자를 갱신 한 다음, 다른 RFID 태그 그룹(320, 330)의 업데이트 보안 기법 식별자(400, 410) 및 RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)의 보안 기법 식별자를 갱신할 수 있다. 이때, 프로세서(303)는 미리 정해진 대기 시간만큼 대기 후 다른 RFID 태그 그룹(320, 330)의 업데이트 보안 기법 식별자(400, 410) 및 RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)의 보안 기법 식별자를 갱신할 수 있다.
- [0059] 이때, 미리 정해진 대기 시간은 현재 갱신 중인 RFID 태그 그룹의 갱신 중 다음 RFID 태그 그룹의 갱신이 수행되지 않을 수 있도록 충분한 시간이 될 수 있다. 예를 들어, 미리 정해진 시간은 0.2초가 될 수 있다.
- [0060] 다음은 도 5를 참조하여 본 발명의 일 실시예에 따른 RFID 리더(300)에서 수행되는 RFID 태그(321, 322, 331)와의 상호 인증 방법을 설명한다.
- [0061] 도 5는 본 발명의 일 실시예에 따른 RFID 리더의 상호 인증 방법을 설명하기 위한 흐름도이다. 이때, 도 5의 각각의 단계에서 화살표의 순서는 본 발명의 일 실시예에 따른 상호 인증 방법을 설명하기 위하여 임의로 설정한 것이다. 그러므로 도 5에 의해, 본 발명이 한정 해석되는 것은 아니다.
- [0062] RFID 리더(300)는 먼저, 미리 정해진 범위 내의 하나 이상 RFID 태그(321, 322, 331)에 대하여 EPC를 요청할 수 있다. 이때, 미리 정해진 범위는 RFID 리더(300)에서 인식되는 주파수의 크기에 따라 상이할 수 있다. 예를 들어, 미리 정해진 범위 내에 제 1 RFID 태그(321), 제 2 RFID 태그(322) 및 제 3 RFID 태그(331)가 포함된다면, RFID 리더(300)는 제 1 RFID 태그(321), 제 2 RFID 태그(322) 및 제 3 RFID 태그(331)에 EPC를 요청할 수 있다(S500).
- [0063] 그리고 EPC를 요청받는 RFID 태그(321, 322, 331)는 복수의 RFID 태그 그룹(320, 330) 중 어느 하나에 포함된다. RFID 태그(321, 322, 331)는 주기적으로 갱신되는 하나 이상의 보안 기법 식별자를 포함한다.
- [0064] 복수의 RFID 태그(321, 322, 331)를 포함하는 RFID 태그 그룹(320, 330)은 복수의 RFID 태그(321, 322, 331) 및 업데이트 보안 기법 식별자(400, 410)를 포함한다. 이때, RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)의 개수는 RFID 태그(321, 322, 331)의 보안 기법 식별자를 갱신할 때 사용되는 미리 정해진 주기(500) 및 RFID 태그 그룹(320, 330)의 개수에 기초하여 산출될 수 있다.
- [0065] EPC를 요청받은 제 1 RFID 태그(321), 제 2 RFID 태그(322) 및 제 3 RFID 태그(331)는 RFID 리더(300)로 각각 EPC를 전송할 수 있다(S501).
- [0066] RFID 리더(300)는 제 1 RFID 태그(321), 제 2 RFID 태그(322) 및 제 3 RFID 태그(331)로부터 각각 EPC를 수신하면, 수신된 EPC를 서버(310)로 전송할 수 있다(S510).
- [0067] 그리고 RFID 리더(300)는 서버(310)로부터 제 1 RFID 태그(321), 제 2 RFID 태그(322) 및 제 3 RFID 태그(331)

1)에 대한 상호 인증 관련 데이터를 수신할 수 있다(S511).

- [0068] 상호 인증 관련 데이터를 수신한 다음, RFID 리더(300)는 먼저, 복수의 RFID 태그 그룹(320, 330) 중 보안 기법 식별자 갱신 대상 RFID 태그 그룹(320, 330)에 대한 업데이트 보안 기법 식별자(400, 410)가 포함된 갱신 명령을 브로드캐스팅 할 수 있다. 그리고 RFID 리더(300)는 보안 기법 식별자 갱신 대상 RFID 태그 그룹(320, 330)에 포함된 RFID 태그(321, 322, 331)의 보안 기법 식별자를 갱신할 수 있다(S520, S530)
- [0069] 예를 들어, 보안 기법 식별자 갱신 대상 RFID 태그 그룹(320, 330)이 제 1 RFID 태그 그룹(320)이라면, RFID 리더(300)는 제 1 RFID 태그 그룹(320)의 업데이트 보안 기법 식별자(400, 410)가 포함된 갱신 명령을 브로드캐스팅 한다.
- [0070] RFID 리더(300)를 통하여, 브로드캐스팅 된 갱신 명령을 수신한 제 1 RFID 태그(321), 제 2 RFID 태그(322) 및 제 3 RFID 태그(331)는 각각 저장된 업데이트 보안 기법 식별자(400, 410)를 확인하여, 보안 기법 식별자 갱신 대상 RFID 태그 그룹에 포함되는지 확인할 수 있다. 그리고 RFID 리더(300)는 보안 기법 식별자 갱신 대상 RFID 태그 그룹인 제 1 RFID 태그 그룹(320)에 포함된 제 1 RFID 태그(321) 및 제 2 RFID 태그(322)는 보안 기법 식별자를 갱신할 수 있다(S520). 제 1 RFID 태그(321) 및 제 2 RFID 태그(322)의 보안 기법 식별자가 갱신 되면, RFID 리더(300)는 제 1 RFID 태그 그룹(320)의 업데이트 보안 기법 식별자(400)를 갱신할 수 있다.
- [0071] 또한, RFID 리더(300)는 미리 정해진 대기 시간 이후, 다음 RFID 태그 그룹인 제 2 태그 RFID 태그 그룹(410)을 보안 기법 식별자 갱신 대상 RFID 태그 그룹으로 선택하고, 제 2 RFID 태그 그룹(330)의 업데이트 보안 기법 식별자(410)가 포함된 갱신 명령을 브로드 캐스팅 한다. 그리고 제 1 RFID 태그 그룹(320)의 보안 기법 식별자 갱신과 유사한 방법으로 제 2 RFID 태그 그룹(330)에 포함된 제 3 RFID 태그(331)의 보안 기법 식별자 및 제 2 RFID 태그 그룹의 업데이트 보안 기법 식별자(410)를 갱신할 수 있다.
- [0072] 그리고 RFID 리더(300)는 미리 정해진 범위 내에 포함된 RFID 태그(321, 322, 331)에 상호 인증 명령을 전송하여, 상호 인증을 수행할 수 있다. 이때, RFID 리더(300)는 보안 기법 식별자를 포함하는 상호 인증 명령을 RFID 태그(321, 322, 331)로 전송할 수 있다. 그리고 상호 인증이 성공하면, RFID 리더(300)는 상호 인증 명령을 전송한 RFID 태그(321, 322, 331)의 메모리를 읽거나 쓸 수 있다.
- [0073] 예를 들어, RFID 리더(300)가 제 1 RFID 태그(321)에 상호 인증 명령을 전송하여(S540), 제 1 RFID 태그(321)와 상호 인증을 성공하면, RFID 리더(300)는 제 1 RFID 태그(321)에 포함된 메모리의 읽기 또는 쓰기를 수행할 수 있다(S541).
- [0074] RFID 리더(300)는 미리 정해진 주기(500)에 따라, 다시 제 1 RFID 태그 그룹(320) 및 제 2 RFID 태그 그룹(330)에 포함된 보안 기법 식별자를 갱신할 수 있다(S560, S570). 이때, 미리 정해진 주기(500)는 보안 기법 식별자의 크기에 기초하여 산출될 수 있다.
- [0075] RFID 태그(321, 322, 331)와의 상호 인증을 위한 RFID 리더(300) 및 이를 이용한 상호 인증 방법은 EPC C1G2 표준에서 RFID 리더(300)를 이용하여 상호 인증 명령의 헤더에 암호화되지 않았던 보안 기법 식별자를 암호화하는 방법을 제공한다. 또한, RFID 리더(300) 및 이를 이용한 상호 인증 방법은 복수의 RFID 태그(321, 322, 331)를 포함하는 RFID 태그 그룹(320, 330)을 설정하므로, RFID 태그(321, 322, 331)의 개수가 증가하더라도 RFID 태그 그룹(320, 330)의 업데이트 보안 기법 식별자(400, 410) 및 RFID 태그(321, 322, 331)의 보안 기법 식별자에 대한 랜덤성을 보장할 수 있다.
- [0076] 그러므로 RFID 리더(300) 및 이를 이용한 상호 인증 방법은 공격자가 보안 기법 식별자를 수집하여 공격을 하더라도 RFID 태그(321, 322, 331)에 저장된 값을 안전하게 지킬 수 있다.
- [0077] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능한 기록 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독 가능한 기록 매체는 컴퓨터 저장 매체를 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다.
- [0078] 본 발명의 방법 및 시스템은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍처를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다.
- [0079] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명

의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

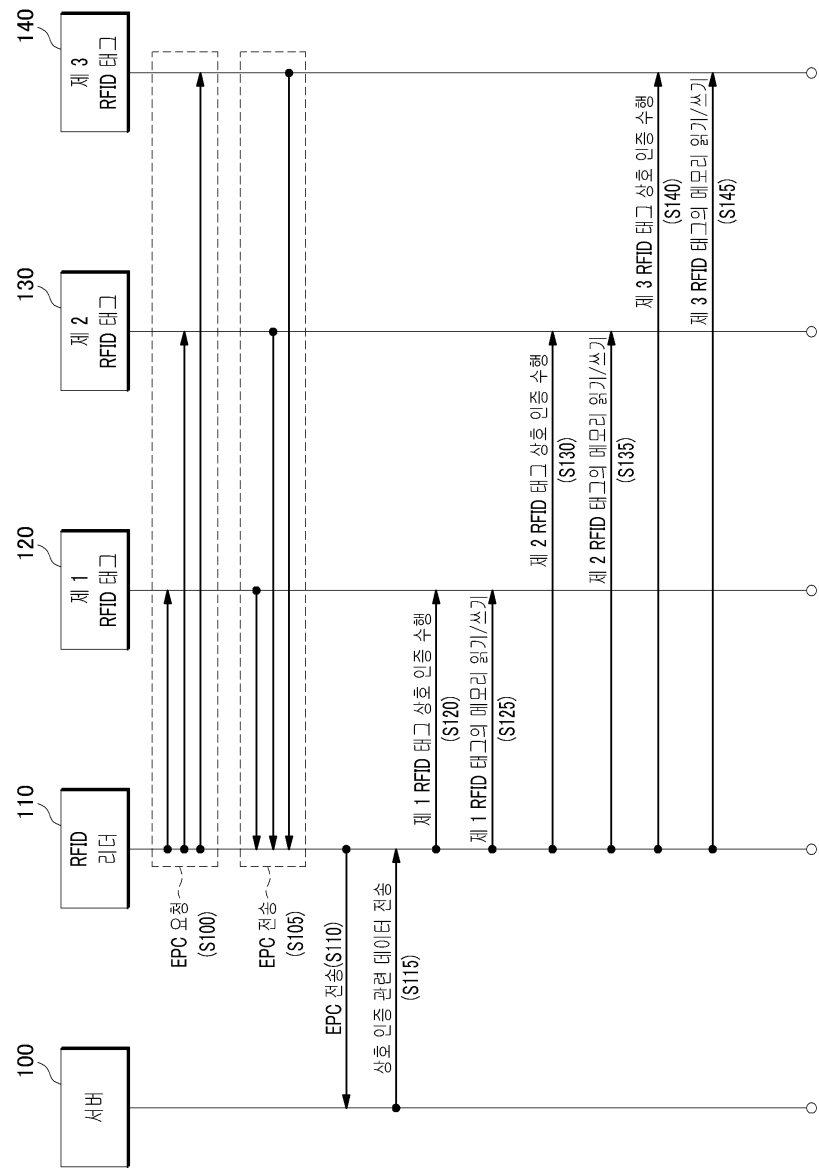
[0080] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

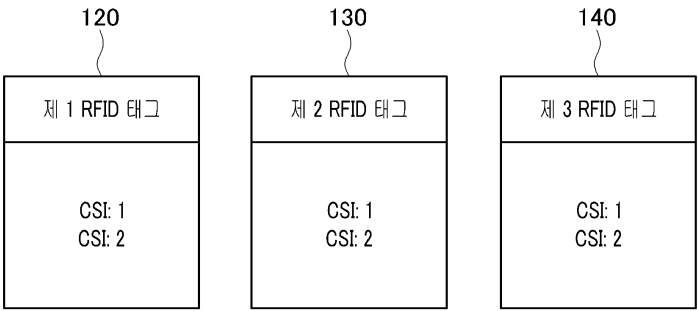
[0081] 300: 서버
301: 통신 모듈
302: 메모리
303: 프로세서
310: 서버
320: RFID 태그 그룹
303: RFID 태그

도면

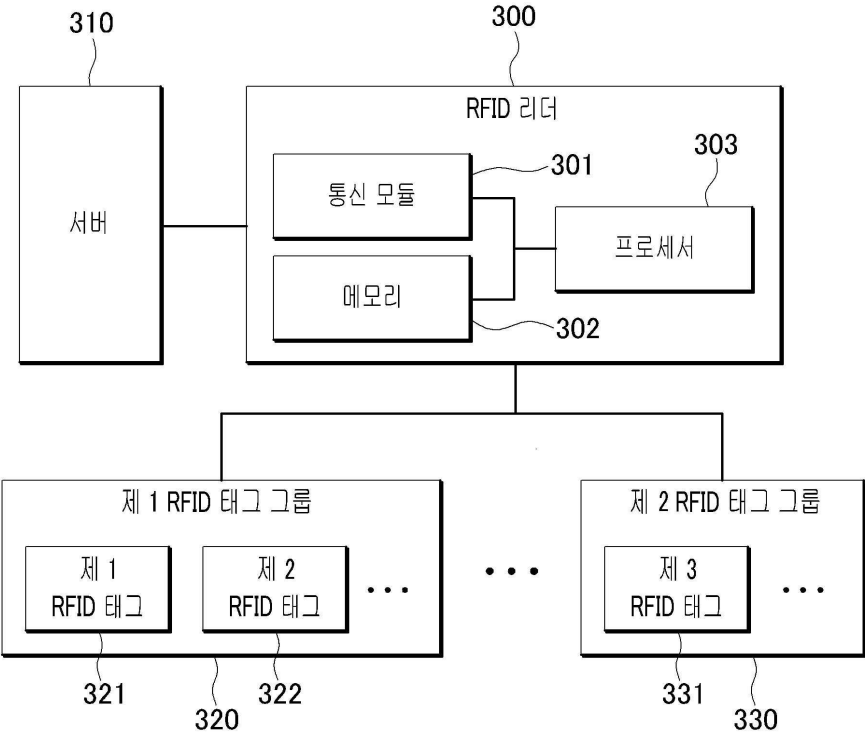
도면1



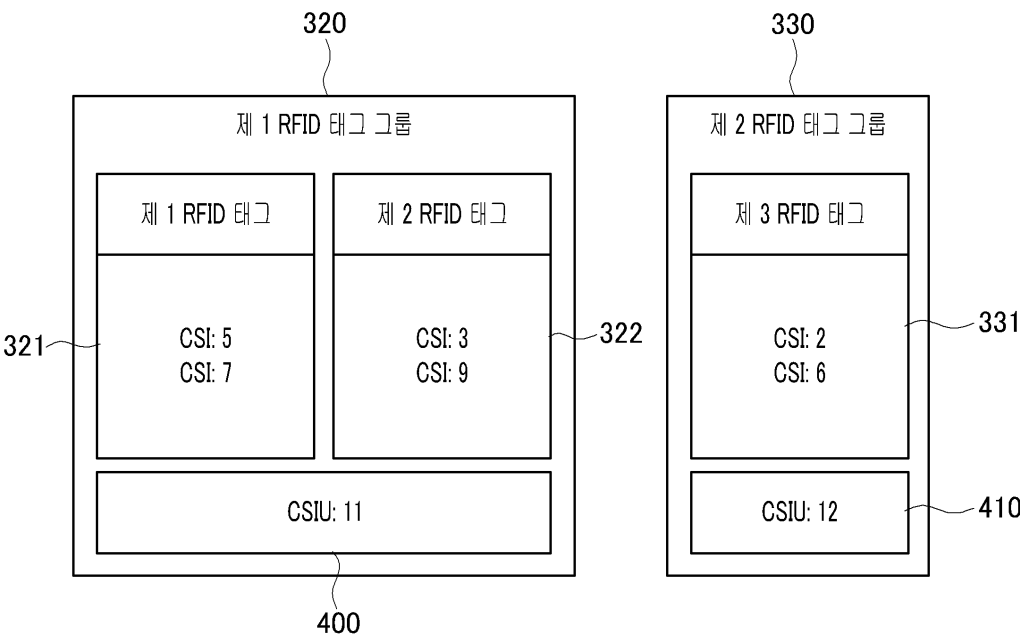
도면2



도면3



도면4



도면5

