(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년07월13일
(11) 등록번호 10-2555796
(24) 등록일자 2023년07월11일

(51) 국제특허분류(Int. Cl.)
G01S 5/02 (2010.01) *H04W 64/00* (2023.01)
(52) CPC특허분류
G01S 5/0252 (2023.05)
H04W 64/00 (2013.01)
(21) 출원번호 10-2017-7031056
(22) 출원일자(국제) 2016년03월30일
심사청구일자 2021년03월29일
(85) 번역문제출일자 2017년10월26일
(65) 공개번호 10-2017-0132263
(43) 공개일자 2017년12월01일
(86) 국제출원번호 PCT/US2016/025069
(87) 국제공개번호 WO 2016/161020
국제공개일자 2016년10월06일
(30) 우선권주장
14/673,551 2015년03월30일 미국(US)
14/673,582 2015년03월30일 미국(US)
(56) 선행기술조사문헌
JP10136436 A
JP2009087834 A

(73) 특허권자
어페로, 인크.
미국, 94022, 캘리포니아주, 로스앨토스, 엘 카미노 리얼 4970, 스위트 210
(72) 발명자
자카리아, 오마르
미국 94022 캘리포니아 로스 알토스 이엘 카미노 리얼 4970 스위트 210
(74) 대리인
특허법인 남앤남

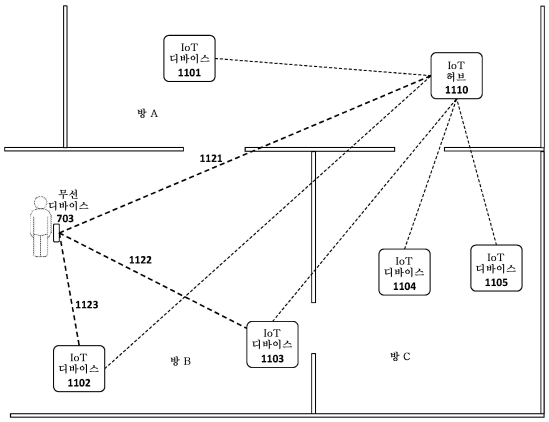
전체 청구항 수 : 총 24 항 심사관 : 나영준

(54) 발명의 명칭 **IoT 시스템에서 사용자 위치를 정확하게 감지하기 위한 시스템 및 방법**

(57) 요 약

무선 디바이스의 위치를 정확하게 검출하기 위한 시스템 및 방법이 설명된다. 예를 들어, 방법의 일 실시예는 무선 디바이스와 사용자의 집 내의 복수의 IoT 디바이스 및/또는 IoT 허브 사이의 신호 강도를 나타내는 신호 강도 데이터를 수집하는 단계; 신호 강도 데이터를 사용자 집 내의 위치들과 관련시키고 관련을 위치 데이터베이스 내에 저장하는 단계; 및 데이터베이스 내의 신호 강도 데이터를, 무선 디바이스와 복수의 IoT 디바이스 및/또는 IoT 허브 사이의 현재 신호 강도를 나타내는 현재 신호 강도 데이터와 비교함으로써 무선 디바이스의 현재 위치를 결정하는 단계를 포함한다.

대 표 도 - 도12



명 세 서

청구범위

청구항 1

시스템으로서,

무선 디바이스와 사용자의 집 또는 사업체 내의 복수의 사물 인터넷(IoT) 디바이스들 및/또는 IoT 허브들 사이의 신호 강도를 나타내는 신호 강도 데이터를 수집하기 위한 시스템 교정 모듈 - 상기 시스템 교정 모듈은 상기 신호 강도 데이터를 상기 사용자의 집 또는 사업체 내의 위치들과 관련시키고 상기 관련을 위치 데이터베이스 내에 저장함 -;

상기 위치 데이터베이스 내의 상기 신호 강도 데이터를, 상기 무선 디바이스와 상기 복수의 IoT 디바이스들 및/또는 IoT 허브들 중 하나 이상 사이의 현재 신호 강도를 나타내는 현재 신호 강도 데이터와 비교함으로써 상기 무선 디바이스의 현재 위치를 결정하기 위한 신호 강도 분석 모듈; 및

상기 무선 디바이스 상에 설치된 교정 앱을 포함하고,

상기 교정 앱은 상기 신호 강도 데이터를 수집할 때 상기 시스템 교정 모듈과 통신하고, 상기 교정 앱은 상기 사용자에게 1) 상기 사용자의 집 또는 사업체 내의 상이한 방들 및/또는 각각의 방 내의 상이한 위치들로 이동하도록 지시하고, 2) 상기 사용자가 상기 상이한 방들 및/또는 각각의 방들 내의 상이한 위치들 각각에 도달했을 때 상기 교정 앱으로 표시(indication)를 제공하도록 지시하는,

시스템.

청구항 2

삭제

청구항 3

제1항에 있어서, 상기 교정 앱은 상기 표시를 제공할 때 상기 무선 디바이스와 상기 복수의 IoT 디바이스들 및/또는 IoT 허브들 각각 사이의 현재 신호 강도 데이터를 전송하는, 시스템.

청구항 4

제1항에 있어서,

상기 시스템 교정 모듈 및 신호 강도 분석 모듈이 실행되는 IoT 허브를 추가로 포함하는, 시스템.

청구항 5

제1항에 있어서, 상기 위치 데이터베이스는 각각의 위치의 아이덴티티 및 각각의 위치와 관련된 복수의 신호 강도 값들을 포함하는, 시스템.

청구항 6

제5항에 있어서, 상기 복수의 신호 강도 값들은 각각의 위치에서 상기 무선 디바이스와 상기 복수의 IoT 디바이스들 및/또는 IoT 허브들 사이에서 측정된 수신 신호 강도 지시자(RSSI) 값들을 포함하는, 시스템.

청구항 7

제6항에 있어서, 상기 신호 강도 분석 모듈은 현재 신호 강도 값들의 세트를 수신하고 이 값들을 상기 위치 데이터베이스 내의 상기 신호 강도 데이터와 비교하여 상기 무선 디바이스의 상기 현재 위치를 결정하는, 시스템.

청구항 8

제7항에 있어서, 상기 신호 강도 분석 모듈은 상기 현재 신호 강도 값들이 상기 위치 데이터베이스 내에 지정된 상기 신호 강도 값들의 지정된 범위 내에 있는 경우 상기 무선 디바이스가 특정 위치에 있는 것으로 결정하는,

시스템.

청구항 9

제8항에 있어서, 상기 신호 강도 분석 모듈은 상기 무선 디바이스가 상기 특정 위치에 있다는 상기 결정에 응답하여 IoT 디바이스들을 제어하기 위해 하나 이상의 IoT 디바이스 커맨드들을 전송하는, 시스템.

청구항 10

제9항에 있어서, 상기 무선 디바이스가 특정 방 내에 있는 것으로 결정할 때, 상기 신호 강도 분석 모듈은 그에 응답하여 상기 방 내의 오디오 스피커들을 턴온하고/하거나 상기 방 내의 발광체들을 턴온하는, 시스템.

청구항 11

제10항에 있어서, 상기 무선 디바이스가 상기 특정 방 내에 있는 것으로 결정할 때, 상기 신호 강도 분석 모듈은 그에 응답하여 다른 방 내의 오디오 스피커들을 턴오프하고/하거나 상기 다른 방 내의 발광체들을 턴오프하는, 시스템.

청구항 12

제1항에 있어서, 상기 신호 강도 분석 모듈은 삼각 측량 기술들을 수행하여 상기 무선 디바이스의 상기 현재 위치를 결정하는, 시스템.

청구항 13

제12항에 있어서, 상기 삼각 측량 기술들은 상기 무선 디바이스와 IoT 허브, 상기 무선 디바이스와 IoT 디바이스 사이의 신호 강도 값들, 및 상기 IoT 디바이스와 상기 IoT 허브 사이의 신호 강도를 측정하는 것을 포함하는, 시스템.

청구항 14

제1항에 있어서, 상기 신호 강도 데이터는 상기 무선 디바이스에 의해 수집되어 제1 IoT 허브로 전송되는, 시스템.

청구항 15

제14항에 있어서, 상기 신호 강도 데이터는 단거리 무선 통신 표준을 이용하여 무선 통신 채널들에 대해 수집되고, 상기 신호 강도 데이터는 상이한 무선 통신 표준을 이용하여 상기 무선 디바이스로부터 상기 제1 IoT 허브로 전송되는, 시스템.

청구항 16

제15항에 있어서, 상기 단거리 무선 통신 표준은 블루투스 저에너지(BTLE)를 포함하고, 상기 상이한 무선 통신 표준은 Wifi 표준을 포함하는, 시스템.

청구항 17

방법으로서,

무선 디바이스와 사용자의 집 또는 사업체 내의 복수의 IoT 디바이스들 및/또는 IoT 허브들 사이의 신호 강도를 나타내는 신호 강도 데이터를 수집하는 단계 - 신호 강도 데이터를 수집하는 단계는 상기 무선 디바이스 상의 교정 앱이 상기 IoT 허브와 통신하는 단계를 추가로 포함하며, 상기 교정 앱은 상기 사용자에게 1) 상기 사용자의 집 또는 사업체 내의 상이한 방들 및/또는 각각의 방 내의 상이한 위치들로 이동하도록 지시하고, 2) 상기 사용자가 상기 상이한 방들 및/또는 각각의 방들 내의 상이한 위치들 각각에 도달했을 때 상기 교정 앱으로 표시를 제공하도록 지시함 -;

상기 신호 강도 데이터를 상기 사용자의 집 또는 사업체 내의 위치들과 관련시키고 상기 관련을 위치 데이터베이스 내에 저장하는 단계; 및

상기 위치 데이터베이스 내의 상기 신호 강도 데이터를, 상기 무선 디바이스와 상기 복수의 IoT 디바이스들 및/

또는 IoT 허브들 사이의 현재 신호 강도를 나타내는 현재 신호 강도 데이터와 비교함으로써 상기 집 또는 사업체 내의 상기 무선 디바이스의 현재 위치를 결정하는 단계

를 포함하는, 방법.

청구항 18

삭제

청구항 19

제17항에 있어서, 상기 교정 앱은 상기 표시를 제공할 때 상기 무선 디바이스와 상기 복수의 IoT 디바이스들 및/또는 IoT 허브들 각각 사이의 현재 신호 강도 데이터를 전송하는, 방법.

청구항 20

제17항에 있어서, 상기 위치 데이터베이스는 각각의 위치의 아이덴티티 및 각각의 위치와 관련된 복수의 신호 강도 값들을 포함하는, 방법.

청구항 21

제20항에 있어서, 상기 복수의 신호 강도 값들은 각각의 위치에서 상기 무선 디바이스와 상기 복수의 IoT 디바이스들 및/또는 IoT 허브들 사이에서 측정된 수신 신호 강도 지시자(RSSI) 값들을 포함하는, 방법.

청구항 22

제21항에 있어서, 현재 위치를 결정하는 단계는 현재 신호 강도 값들의 세트를 수신하고 이 값들을 상기 위치 데이터베이스 내의 상기 신호 강도 데이터와 비교하여 상기 무선 디바이스의 상기 현재 위치를 결정하는 단계를 추가로 포함하는, 방법.

청구항 23

제22항에 있어서, 상기 현재 위치를 결정하는 단계는 상기 현재 신호 강도 값들이 상기 위치 데이터베이스 내에 지정된 상기 신호 강도 값들의 지정된 범위 내에 있는 경우 상기 무선 디바이스가 특정 위치에 있는 것으로 결정하는 단계를 추가로 포함하는, 방법.

청구항 24

제23항에 있어서, 상기 무선 디바이스가 상기 특정 위치에 있다는 상기 결정에 응답하여 IoT 디바이스들을 제어하기 위해 하나 이상의 IoT 디바이스 커맨드들을 전송하는 단계를 추가로 포함하는, 방법.

청구항 25

제24항에 있어서, 상기 무선 디바이스가 특정 방 내에 있는 것으로 결정할 때, 그에 응답하여 상기 방 내의 오디오 스피커들을 턴온하고/하거나 상기 방 내의 발광체들을 턴온하는, 방법.

청구항 26

제25항에 있어서, 상기 무선 디바이스가 상기 특정 방 내에 있는 것으로 결정할 때, 그에 응답하여 다른 방 내의 오디오 스피커들을 턴오프하고/하거나 상기 다른 방 내의 발광체들을 턴오프하는, 방법.

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

청구항 38

삭제

청구항 39

삭제

청구항 40

삭제

청구항 41

삭제

청구항 42

삭제

청구항 43

삭제

청구항 44

삭제

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

청구항 48

삭제

청구항 49

삭제

청구항 50

삭제

청구항 51

삭제

청구항 52

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 컴퓨터 시스템의 분야에 관한 것이다. 더 구체적으로는, 본 발명은 IoT 시스템에서 사용자 위치를 정확하게 감지하기 위한 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] "사물 인터넷"은 인터넷 기반구조 내의 고유하게 식별 가능한 임베디드 디바이스들의 상호접속을 지칭한다. 궁극적으로, IoT는, 사실상 임의의 타입의 물리적인 물건이 그 자체 또는 그의 주변에 대한 정보를 제공할 수 있고 그리고/또는 인터넷을 통하여 클라이언트 디바이스를 통해 원격으로 제어될 수 있는 새로운 광범위한 타입의 애플리케이션을 생성할 것으로 예상된다.

[0003] IoT 개발 및 채택은 접속성, 전력, 및 표준화의 결여에 관련된 이슈로 인해 느렸다. 예를 들어, IoT 개발 및 채택에 대한 하나의 장애물은 개발자가 새로운 IoT 디바이스 및 서비스를 설계 및 제공하도록 허용하기 위한 어떠한 표준 플랫폼도 존재하지 않는다는 것이다. IoT 시장에 진입하기 위해, 개발자는 원하는 IoT 구현을 지원하는 데 요구되는 네트워크 프로토콜 및 기반구조, 하드웨어, 소프트웨어 및 서비스를 포함하여 처음부터 끝까지 전체 IoT 플랫폼을 설계해야 한다. 결과적으로, IoT 디바이스의 각각의 제공자는 IoT 디바이스를 설계하고 접속하기 위한 독점적인 기법을 사용하여, 다수의 타입의 IoT 디바이스의 채택을 최종 사용자에게 부담이 되게 한다. IoT 채택에 대한 다른 장애물은 IoT 디바이스들을 접속하고 전력공급하는 것과 연관된 어려움이다. 예를 들어, 냉장고, 차고 도어 오프너, 환경 센서, 집 보안 센서/제어기 등과 같은 기기를 접속시키는 것은, 각각의 접속된 IoT 디바이스에 전력공급하기 위한 전기 소스를 요구하고, 그러한 전기 소스는 종종 편리하게 위치되어 있지 않다.

[0004] 존재하는 다른 문제는 블루투스 LE와 같은 IoT 디바이스들을 상호접속하는 데 사용되는 무선 기술들이 일반적으로 단거리 기술들이라는 점이다. 따라서, IoT 구현을 위한 데이터 수집 허브가 IoT 디바이스의 범위 밖에 있는 경우, IoT 디바이스는 데이터를 IoT 허브로 전송할 수 없을 것이다(그리고 그 반대도 마찬가지다). 그 결과, IoT 디바이스가 범위 밖에 있는 IoT 허브(또는 다른 IoT 디바이스)에 데이터를 제공하는 것을 가능하게 하는 기술들이 필요하다.

도면의 간단한 설명

[0005] 아래의 도면들과 관련된 아래의 상세한 설명으로부터 본 발명의 더 양호한 이해가 얻어질 수 있다.

도 1a 및 도 1b는 IoT 시스템 아키텍처의 상이한 실시예들을 예시한다.

도 2는 본 발명의 일 실시예에 따른 IoT 디바이스를 예시한다.

도 3은 본 발명의 일 실시예에 따른 IoT 허브를 예시한다.

도 4a 및 도 4b는 IoT 디바이스들로부터 데이터를 제어 및 수집하고 통지를 생성하기 위한 본 발명의 실시예들을 예시한다.

도 5는 IoT 디바이스들로부터 데이터를 수집하고 IoT 허브 및/또는 IoT 서비스로부터 통지를 생성하기 위한 본 발명의 실시예들을 예시한다.

도 6은 현재의 무선 록 시스템들에서 사용자를 식별하는 것과 관련된 문제들을 예시한다.

도 7은 IoT 디바이스들 및/또는 IoT 허브들이 무선 록 시스템의 사용자의 위치를 정확하게 검출하는 데 사용되는 시스템을 예시한다.

도 8은 IoT 디바이스들 및/또는 IoT 허브들이 무선 록 시스템의 사용자의 위치를 정확하게 검출하는 데 사용되는 다른 실시예를 예시한다.

도 9는 위치 검출 시스템을 교정하고, 신호 강도 값들에 기초하여 사용자의 위치를 검출하기 위한 일 실시예를 예시한다.

도 10은 IoT 디바이스들 및/또는 IoT 허브들을 사용하여 무선 록 시스템을 구현하기 위한 방법을 예시한다.

도 11은 무선 록 시스템을 교정하기 위한 방법의 일 실시예를 예시한다.

도 12는 신호 강도 값들로 사용자의 위치를 결정하기 위한 본 발명의 일 실시예를 예시한다.

도 13은 위치 검출 시스템을 교정하고, 신호 강도 값들에 기초하여 사용자의 위치를 검출하기 위한 다른 실시예를 예시한다.

도 14는 암호화 및 디지털 서명과 같은 개선된 보안 기술들을 구현하는 본 발명의 실시예들을 예시한다.

도 15는 IoT 디바이스 상에 키를 저장하기 위해 가입자 식별 모듈(SIM)이 사용되는 아키텍처의 일 실시예를 예시한다.

도 16a는 IoT 디바이스가 바코드 또는 QR 코드를 사용하여 등록되는 일 실시예를 예시한다.

도 16b는 바코드 또는 QR 코드를 사용하여 페어링이 수행되는 일 실시예를 예시한다.

도 17은 IoT 허브를 사용하여 SIM을 프로그래밍하는 방법의 일 실시예를 예시한다.

도 18은 IoT 디바이스를 IoT 허브 및 IoT 서비스에 등록하는 방법의 일 실시예를 예시한다.

도 19는 IoT 디바이스로 전송될 데이터를 암호화하는 방법의 일 실시예를 예시한다.

발명을 실시하기 위한 구체적인 내용

[0006] 아래의 설명에서, 설명의 목적으로, 아래에 설명되는 본 발명의 실시예의 완전한 이해를 제공하기 위해 다수의 특정 상세들이 기재된다. 그러나, 본 발명의 실시예는 이러한 특정 상세들 중 일부 없이도 실시될 수 있다는 것이 당업자에게 명백할 것이다. 다른 경우에서, 잘 알려진 구조 및 디바이스는 본 발명의 실시예의 기본 원리를 불명확하게 하는 것을 피하기 위해 블록도 형태로 도시된다.

[0007] 본 발명의 일 실시예는 새로운 IoT 디바이스 및 애플리케이션을 설계 및 구축하기 위해 개발자에 의해 이용될 수 있는 사물 인터넷(IoT) 플랫폼을 포함한다. 특히, 일 실시예는 IoT 디바이스들이 그것을 통해 인터넷에 결합되는 미리 정의된 네트워킹 프로토콜 스택 및 IoT 허브를 포함한 IoT 디바이스들을 위한 기반 하드웨어/소프트웨어 플랫폼을 포함한다. 부가적으로, 일 실시예는 IoT 허브들 및 접속된 IoT 디바이스들이 그것을 통해 아래에 설명되는 바와 같이 액세스 및 관리될 수 있는 IoT 서비스를 포함한다. 부가적으로, IoT 플랫폼의 일 실시예는 IoT 서비스, 허브 및 접속된 디바이스들에 액세스하고 그들을 구성하기 위한 (예를 들어, 클라이언트 디

바이스 상에서 실행되는) IoT 앱 또는 웹 애플리케이션을 포함한다. 기존의 온라인 소매상 및 다른 웹사이트 운영자는 고유 IoT 기능을 기존의 사용자 기반에 쉽게 제공하기 위해 본 명세서에 설명된 IoT 플랫폼을 레버리징할 수 있다.

[0008] 도 1a는 본 발명의 실시예가 구현될 수 있는 아키텍처 플랫폼의 개요를 예시한다. 특히, 예시된 실시예는 그 자체가 인터넷(220)을 통해 IoT 서비스(120)에 통신 가능하게 결합된 중앙 IoT 허브(110)에 로컬 통신 채널(130)을 통해 통신 가능하게 결합된 복수의 IoT 디바이스(101 내지 105)를 포함한다. IoT 디바이스(101 내지 105) 각각은 로컬 통신 채널들(130) 각각을 인에이블하기 위해 (예를 들어, 아래에 설명되는 페어링 기법을 사용하여) IoT 허브(110)에 초기에 페어링될 수 있다. 일 실시예에서, IoT 서비스(120)는 각각의 사용자의 IoT 디바이스로부터 수집된 사용자 계정 정보 및 데이터를 유지하기 위한 최종 사용자 데이터베이스(122)를 포함한다. 예를 들어, IoT 디바이스가 센서(예를 들어, 온도 센서, 가속도계, 열 센서, 모션 검출기 등)를 포함하면, 데이터베이스(122)는 IoT 디바이스(101 내지 105)에 의해 수집된 데이터를 저장하도록 계속 업데이트될 수 있다. 이어서, 데이터베이스(122)에 저장된 데이터는 사용자의 디바이스(135) 상에 설치된 IoT 앱 또는 브라우저를 통해(또는 데스크톱 또는 다른 클라이언트 컴퓨터 시스템을 통해) 최종 사용자에 의해 그리고 (예를 들어, IoT 서비스(120)에 가입한 웹사이트(130)와 같은) 웹 클라이언트에 의해 액세스 가능하게 될 수 있다.

[0009] IoT 디바이스(101 내지 105)에는 그들 및 그들의 주변에 대한 정보를 수집하고 수집된 정보를 IoT 허브(110)를 통해 IoT 서비스(120), 사용자 디바이스(135) 및/또는 외부 웹사이트(130)에 제공하기 위한 다양한 타입들의 센서가 탑재될 수 있다. IoT 디바이스(101 내지 105) 중 일부는 IoT 허브(110)를 통해 전송된 제어 커맨드에 응답하여 지정된 기능을 수행할 수 있다. IoT 디바이스(101 내지 105)에 의해 수집된 정보 및 제어 커맨드의 다양한 특정 예가 아래에서 제공된다. 아래에 설명된 일 실시예에서, IoT 디바이스(101)는, 사용자 선택을 기록하고 사용자 선택을 IoT 서비스(120) 및/또는 웹사이트에 전송하도록 설계된 사용자 입력 디바이스이다.

[0010] 일 실시예에서, IoT 허브(110)는 4G(예를 들어, 모바일 WiMAX, LTE) 또는 5G 셀룰러 데이터 서비스와 같은 셀룰러 서비스(115)를 통해 인터넷(220)에 대한 접속을 설정하기 위한 셀룰러 라디오를 포함한다. 대안적으로 또는 부가적으로, IoT 허브(110)는 (예를 들어, 인터넷 서비스를 최종 사용자에게 제공하는 인터넷 서비스 제공자를 통해) IoT 허브(110)를 인터넷에 결합시키는 WiFi 액세스 포인트 또는 라우터(116)를 통해 WiFi 접속을 설정하기 위한 WiFi 라디오를 포함할 수 있다. 물론, 본 발명의 기본 원리는 임의의 특정 타입의 통신 채널 또는 프로토콜로 제한되지 않는다는 것에 유의하여야 한다.

[0011] 일 실시예에서, IoT 디바이스(101 내지 105)는 배터리 전력으로 장기간(예를 들어, 수년) 동안 동작할 수 있는 초 저전력 디바이스이다. 전력을 보전하기 위해, 로컬 통신 채널(130)은 블루투스 저에너지(LE)와 같은 저전력 무선 통신 기술을 사용하여 구현될 수 있다. 이러한 실시예에서, IoT 디바이스(101 내지 105) 각각 및 IoT 허브(110)에는 블루투스 LE 라디오 및 프로토콜 스택이 탑재된다.

[0012] 언급된 바와 같이, 일 실시예에서, IoT 플랫폼은 사용자가 접속된 IoT 디바이스(101 내지 105), IoT 허브(110), 및/또는 IoT 서비스(120)에 액세스하고 그들을 구성하도록 허용하기 위해 사용자 디바이스(135) 상에서 실행되는 IoT 앱 또는 웹 애플리케이션을 포함한다. 일 실시예에서, 앱 또는 웹 애플리케이션은 IoT 기능을 그의 사용자 기반에 제공하도록 웹사이트(130)의 운영자에 의해 설계될 수 있다. 예시된 바와 같이, 웹사이트는 각각의 사용자에 관련된 계정 기록을 포함하는 사용자 데이터베이스(131)를 유지할 수 있다.

[0013] 도 1b는 복수의 IoT 허브(110, 111, 190)에 대한 추가의 접속 옵션들 예시한다. 이러한 실시예에서, 단일 사용자는 단일 사용자 구내(premises)(180)(예를 들어, 사용자의 집 또는 사업체)에 현장 설치된 다수의 허브(110, 111)를 가질 수 있다. 이것은 예를 들어 IoT 디바이스(101 내지 105) 모두를 접속시키기 위해 필요한 무선 범위를 확장시키기 위해 행해질 수 있다. 표시된 바와 같이, 사용자가 다수의 허브(110, 111)를 갖는 경우, 그것들은 로컬 통신 채널(예를 들어, Wifi, 이더넷, 전력 라인 네트워킹 등)을 통해 접속될 수 있다. 일 실시예에서, 허브(110, 111) 각각은 (도 1b에 명시적으로 도시되지 않은) 셀룰러(115) 또는 WiFi(116) 접속을 통해 IoT 서비스(120)에 대한 직접 접속을 설정할 수 있다. 대안적으로 또는 부가적으로, IoT 허브(110)와 같은 IoT 허브들 중 하나는 (IoT 허브(110)와 IoT 허브(111)를 연결하는 점선에 의해 표시된 바와 같이) IoT 허브(111)와 같은, 사용자 구내(180) 상의 다른 IoT 허브들 모두에 접속 및/또는 로컬 서비스를 제공하는 "마스터" 허브로서 동작할 수 있다. 예를 들어, 마스터 IoT 허브(110)는 IoT 서비스(120)에 대한 직접 접속을 설정하기 위한 유일한 IoT 허브일 수 있다. 일 실시예에서, "마스터" IoT 허브(110)에만 IoT 서비스(120)에 대한 접속을 설정하기 위한 셀룰러 통신 인터페이스가 탑재된다. 그렇기 때문에, IoT 서비스(120)와 다른 IoT 허브(111) 사이의 모든 통신은 마스터 IoT 허브(110)를 통해 흐를 것이다. 이러한 역할에서, 마스터 IoT 허브(110)는 다른 IoT 허브

(111)와 (예를 들어, 가능한 경우 로컬식으로 일부 데이터 요청들을 서비스하는) IoT 서비스(120) 사이에서 교환되는 데이터에 대해 필터링 동작을 수행하기 위한 부가적인 프로그램 코드를 제공받을 수 있다.

[0014] IoT 허브(110, 111)가 어떻게 접속되는지에 관계없이, 일 실시예에서, IoT 서비스(120)는 앱이 설치된 사용자 디바이스(135)를 통해 액세스 가능한 단일의 포괄적인 사용자 인터페이스 (및/또는 브라우저-기반 인터페이스) 하에서 허브를 사용자와 논리적으로 연관시키고 부착된 IoT 디바이스(101 내지 105) 모두를 결합시킬 것이다.

[0015] 이러한 실시예에서, 마스터 IoT 허브(110) 및 하나 이상의 슬레이브 IoT 허브(111)는 WiFi 네트워크(116), 이더넷 네트워크, 및/또는 사용 전력-라인 통신(PLC) 네트워킹일 수 있는 로컬 네트워크를 통해 접속될 수 있다(예를 들어, 여기서 네트워크의 전부 또는 일부가 사용자의 전력 라인을 통해 구동됨). 부가적으로, IoT 허브(110, 111)에 대해, IoT 디바이스(101 내지 105) 각각은, 몇몇 예를 들자면, WiFi, 이더넷, PLC 또는 블루투스 LE와 같은 임의의 타입의 로컬 네트워크 채널을 사용하여 IoT 허브(110, 111)와 상호접속될 수 있다.

[0016] 도 1b는 또한 제2 사용자 구내(181)에 설치된 IoT 허브(190)를 도시한다. 사실상 제한되지 않는 수의 그러한 IoT 허브(190)가 전세계의 사용자 구내에서 IoT 디바이스(191, 192)로부터 데이터를 수집하도록 설치 및 구성될 수 있다. 일 실시예에서, 2개의 사용자 구내(180, 181)가 동일한 사용자에 대해 구성될 수 있다. 예를 들어, 하나의 사용자 구내(180)는 사용자의 주된 집일 수 있고, 다른 사용자 구내(181)는 사용자의 별장일 수 있다. 그러한 경우에, IoT 서비스(120)는 앱이 설치된 사용자 디바이스(135)를 통해 액세스 가능한 단일의 포괄적인 사용자 인터페이스 (및/또는 브라우저-기반 인터페이스)하에서 IoT 허브(110, 111, 190)를 사용자와 논리적으로 연관시키고 부착된 IoT 디바이스(101 내지 105, 191, 192) 모두를 결합시킬 것이다.

[0017] 도 2에 예시된 바와 같이, IoT 디바이스(101)의 예시적인 실시예는 프로그램 코드 및 데이터(201 내지 203)를 저장하기 위한 메모리(210) 및 프로그램 코드를 실행하고 데이터를 처리하기 위한 저전력 마이크로제어기(200)를 포함한다. 메모리(210)는 동적 랜덤 액세스 메모리(DRAM)와 같은 휘발성 메모리일 수 있거나, 플래시 메모리와 같은 비-휘발성 메모리일 수 있다. 일 실시예에서, 비-휘발성 메모리는 영속적인 저장을 위해 사용될 수 있고, 휘발성 메모리는 런타임 시에 프로그램 코드 및 데이터의 실행을 위해 사용될 수 있다. 또한, 메모리(210)는 저전력 마이크로제어기(200) 내에 통합될 수 있거나, 버스 또는 통신 패브릭(fabric)을 통해 저전력 마이크로제어기(200)에 결합될 수 있다. 본 발명의 기본 원리는 메모리(210)의 임의의 특정 구현으로 제한되지 않는다.

[0018] 예시된 바와 같이, 프로그램 코드는 IoT 디바이스(201)에 의해 수행될 기능들의 애플리케이션-특정 세트를 정의하는 애플리케이션 프로그램 코드(203), 및 IoT 디바이스(101)의 애플리케이션 개발자에 의해 이용될 수 있는 미리 정의된 빌딩 블록(building block)들의 세트를 포함하는 라이브러리 코드(202)를 포함할 수 있다. 일 실시예에서, 라이브러리 코드(202)는 각각의 IoT 디바이스(101)와 IoT 허브(110) 사이의 통신을 인에이블하기 위한 통신 프로토콜 스택(201)과 같은, IoT 디바이스를 구현하는 데 요구되는 기본 기능들의 세트를 포함한다. 언급된 바와 같이, 일 실시예에서, 통신 프로토콜 스택(201)은 블루투스 LE 프로토콜 스택을 포함한다. 이러한 실시예에서, 블루투스 LE 라디오 및 안테나(207)는 저전력 마이크로제어기(200) 내에 통합될 수 있다. 그러나, 본 발명의 기본 원리는 임의의 특정 통신 프로토콜로 제한되지 않는다.

[0019] 도 2에 도시된 특정 실시예는 또한 사용자 입력을 수신하고 사용자 입력을 저전력 마이크로제어기에 제공하기 위한 복수의 입력 디바이스 또는 센서(210)를 포함하며, 저전력 마이크로제어기는 애플리케이션 코드(203) 및 라이브러리 코드(202)에 따라 사용자 입력을 처리한다. 일 실시예에서, 입력 디바이스들 각각은 최종 사용자에게 피드백을 제공하기 위한 LED(209)를 포함한다.

[0020] 부가적으로, 예시된 실시예는 저전력 마이크로제어기에 전력을 공급하기 위한 배터리(208)를 포함한다. 일 실시예에서, 비-충전 가능 코인 셀 배터리가 사용된다. 그러나, 대안적인 실시예에서, 통합된 재충전 가능 배터리가 사용될 수 있다(예를 들어, IoT 디바이스를 AC 전력 공급부(도시되지 않음)에 접속시킴으로써 재충전 가능함).

[0021] 오디오를 생성하기 위한 스피커(205)가 또한 제공된다. 일 실시예에서, 저전력 마이크로제어기(299)는 스피커(205)에서 오디오를 생성하기 위해 (예를 들어, MPEG-4/어드밴스드 오디오 코딩(AAC) 스트림과 같은) 압축된 오디오 스트림을 디코딩하기 위한 오디오 디코딩 로직을 포함한다. 대안적으로, 저전력 마이크로제어기(200) 및/또는 애플리케이션 코드/데이터(203)는 사용자가 입력 디바이스(210)를 통해 선택을 입력할 때 언어 피드백을 최종 사용자에게 제공하기 위한 오디오의 디지털 샘플링된 단편(snippet)을 포함할 수 있다.

[0022] 일 실시예에서, 하나 이상의 다른/대안적인 I/O 디바이스 또는 센서(250)가, IoT 디바이스(101)가 그것을 위해

설계되는 특정 애플리케이션에 기초하여 IoT 디바이스(101) 상에 포함될 수 있다. 예를 들어, 온도, 압력, 습도 등을 측정하기 위해 환경 센서가 포함될 수 있다. IoT 디바이스가 보안 디바이스로서 사용되는 경우 보안 센서 및/또는 도어록 오프너가 포함될 수 있다. 물론, 이들 예는 단지 예시의 목적으로 제공된다. 본 발명의 기본 원리는 IoT 디바이스의 임의의 특정 타입으로 제한되지 않는다. 사실, 라이브러리 코드(202)가 탑재된 저전력 마이크로제어기(200)의 고도로 프로그래밍 가능한 속성을 고려해 볼 때, 애플리케이션 개발자는 사실상 임의의 타입의 IoT 애플리케이션을 위한 저전력 마이크로제어기와 인터페이싱하기 위해 새로운 애플리케이션 코드(203) 및 새로운 I/O 디바이스(250)를 쉽게 개발할 수 있다.

[0023] 일 실시예에서, 저전력 마이크로제어기(200)는 또한 통신을 암호화하고/하거나 서명을 생성하기 위한 암호화 키를 저장하기 위한 보안 키 저장소를 포함한다. 대안적으로, 키는 가입자 식별 모듈(SIM)에서 보안될 수 있다.

[0024] 일 실시예에서, IoT 디바이스가 사실상 어떠한 전력도 소비하고 있지 않은 초 저전력 상태로부터 그 IoT 디바이스를 웨이크하기 위해 웨이크업 수신기(207)가 포함된다. 일 실시예에서, 웨이크업 수신기(207)는 도 3에 도시된 바와 같이 IoT 허브(110) 상에 구성된 웨이크업 송신기(307)로부터 수신된 웨이크업 신호에 응답하여 IoT 디바이스(101)로 하여금 이러한 저전력 상태를 빠져나가게 하도록 구성된다. 특히, 일 실시예에서, 송신기(307) 및 수신기(207)는 테슬라 코일과 같은 전기 공진 변압기 회로를 함께 형성한다. 동작 시에, 허브(110)가 매우 낮은 전력 상태로부터 IoT 디바이스(101)를 웨이크할 필요가 있을 때 에너지가 라디오 주파수 신호를 통해 송신기(307)로부터 수신기(207)로 송신된다. 에너지 전달 때문에, IoT 디바이스(101)는 그것이 그것의 저전력 상태에 있을 때 사실상 어떠한 전력도 소비하지 않도록 구성될 수 있는데, 왜냐하면 (디바이스가 네트워크 신호를 통해 어웨이크되도록 허용하는 네트워크 프로토콜에서 그러한 바와 같이) 그것이 허브로부터의 신호를 계속 "청취"할 필요가 없기 때문이다. 오히려, IoT 디바이스(101)의 마이크로제어기(200)는 송신기(307)로부터 수신기(207)로 전기적으로 송신된 에너지를 사용함으로써 사실상 전력 차단된 후에 웨이크 업하도록 구성될 수 있다.

[0025] 도 3에 예시된 바와 같이, IoT 허브(110)는 또한 프로그램 코드 및 데이터(305)를 저장하기 위한 메모리(317), 및 프로그램 코드를 실행하고 데이터를 처리하기 위한 마이크로제어기와 같은 하드웨어 로직(301)을 포함한다. 광역 네트워크(WAN) 인터페이스(302) 및 안테나(310)가 IoT 허브(110)를 셀룰러 서비스(115)에 결합시킨다. 대안적으로, 위에서 언급된 바와 같이, IoT 허브(110)는 또한 근거리 네트워크 통신 채널을 설정하기 위한 WiFi 인터페이스(및 WiFi 안테나) 또는 이더넷 인터페이스와 같은 로컬 네트워크 인터페이스(도시되지 않음)를 포함할 수 있다. 일 실시예에서, 하드웨어 로직(301)은 또한 통신을 암호화하고 서명을 생성/검증하기 위한 암호화 키를 저장하기 위한 보안 키 저장소를 포함한다. 대안적으로, 키는 가입자 식별 모듈(SIM)에서 보안될 수 있다.

[0026] 로컬 통신 인터페이스(303) 및 안테나(311)가 IoT 디바이스(101 내지 105) 각각과 로컬 통신 채널을 설정한다. 위에서 언급된 바와 같이, 일 실시예에서, 로컬 통신 인터페이스(303)/안테나(311)는 블루투스 LE 표준을 구현한다. 그러나, 본 발명의 기본 원리는 IoT 디바이스(101 내지 105)와 로컬 통신 채널을 설정하기 위한 임의의 특정 프로토콜로 제한되지 않는다. 도 3에서 별개의 유닛으로서 예시되지만, WAN 인터페이스(302) 및/또는 로컬 통신 인터페이스(303)는 하드웨어 로직(301)과 동일한 칩 내에 임베딩될 수 있다.

[0027] 일 실시예에서, 프로그램 코드 및 데이터는 로컬 통신 인터페이스(303) 및 WAN 인터페이스(302)를 통해 통신하기 위한 별개의 스택을 포함할 수 있는 통신 프로토콜 스택(308)을 포함한다. 부가적으로, IoT 허브가 새로운 IoT 디바이스와 페어링하도록 허용하기 위해 디바이스 페어링 프로그램 코드 및 데이터(306)가 메모리에 저장될 수 있다. 일 실시예에서, 각각의 새로운 IoT 디바이스(101 내지 105)는 페어링 프로세스 동안 IoT 허브(110)에 통신되는 고유 코드를 할당받는다. 예를 들어, 고유 코드는 IoT 디바이스 상의 바코드에 임베딩될 수 있으며, 바코드 판독기(106)에 의해 판독될 수 있거나 로컬 통신 채널(130)을 통해 통신될 수 있다. 대안적인 실시예에서, 고유 ID 코드는 IoT 디바이스 상에 자기적으로 임베딩되며, IoT 허브는 IoT 디바이스(101)가 IoT 허브(110)로부터 수 인치 이내로 이동될 때 코드를 검출하기 위한 라디오 주파수 ID(RFID) 또는 근거리장 통신(NFC) 센서와 같은 자기 센서를 갖는다.

[0028] 일 실시예에서, 일단 고유 ID가 통신되면, IoT 허브(110)는 로컬 데이터베이스(도시되지 않음)에 질의하고/하거나, 코드가 수용 가능한지를 검증하기 위해 해시(hash)를 수행하고/하거나, ID 코드를 확인하기 위해 IoT 서비스(120), 사용자 디바이스(135) 및/또는 웹사이트(130)와 통신함으로써 고유 ID를 검증할 수 있다. 일단 확인되면, 일 실시예에서, IoT 허브(110)는 IoT 디바이스(101)를 페어링하고, (언급된 바와 같이, 비-휘발성 메모리를 포함할 수 있는) 메모리(317)에 페어링 데이터를 저장한다. 일단 페어링이 완료되면, IoT 허브(110)는 본 명세서에 설명된 다양한 IoT 기능을 수행하기 위해 IoT 디바이스(101)와 접속할 수 있다.

[0029] 일 실시예에서, IoT 서비스(120)를 구동하는 조직은 개발자가 새로운 IoT 서비스를 용이하게 설계하도록 허용하기 위해 IoT 허브(110) 및 기본적인 하드웨어/소프트웨어 플랫폼을 제공할 수 있다. 특히, IoT 허브(110)에 더하여, 개발자는 허브(110) 내에서 실행되는 프로그램 코드 및 데이터(305)를 업데이트하기 위한 소프트웨어 개발 키트(SDK)를 제공받을 수 있다. 부가적으로, IoT 디바이스(101)에 대해, SDK는 다양한 상이한 타입의 애플리케이션(101)의 설계를 용이하게 하기 위하여 기반 IoT 하드웨어(예를 들어, 도 2에 도시된 저전력 마이크로제어기(200) 및 다른 컴포넌트)에 대해 설계된 광범위한 세트의 라이브러리 코드(202)를 포함할 수 있다. 일 실시예에서, SDK는 개발자가 단지 IoT 디바이스에 대한 입력 및 출력만을 지정할 필요가 있는 그래픽 설계 인터페이스를 포함한다. IoT 디바이스(101)가 허브(110) 및 서비스(120)에 접속하도록 허용하는 통신 스택(201)을 포함한 모든 네트워킹 코드가 이미 개발자를 위해 제 위치에 있다. 부가적으로, 일 실시예에서, SDK는 또한 모바일 디바이스(예를 들어, 아이폰 및 안드로이드 디바이스)를 위한 앱의 설계를 용이하게 하기 위한 라이브러리 코드 기반을 포함한다.

[0030] 일 실시예에서, IoT 허브(110)는 IoT 디바이스(101 내지 105)와 IoT 서비스(120) 사이의 데이터의 연속적인 양방향 스트림을 관리한다. IoT 디바이스(101 내지 105)로의/로부터의 업데이트가 실시간으로 요구되는(예를 들어, 사용자가 보안 디바이스 또는 환경 측정의 현재 상태를 볼 필요가 있는) 상황에서, IoT 허브는 정기 업데이트를 사용자 디바이스(135) 및/또는 외부 웹사이트들(130)에 제공하기 위한 개방형 TCP 소켓을 유지할 수 있다. 업데이트를 제공하는 데 사용되는 특정 네트워킹 프로토콜은 기본 애플리케이션의 필요에 기초하여 미세조정될 수 있다. 예를 들어, 연속적인 양방향 스트림을 갖는 것이 타당하지 않을 수 있는 일부 경우에, 간단한 요청/응답 프로토콜이 필요할 경우 정보를 수집하는 데 사용될 수 있다.

[0031] 일 실시예에서, IoT 허브(110) 및 IoT 디바이스(101 내지 105) 둘 모두는 네트워크를 통해 자동적으로 업그레이드 가능하다. 특히, 새로운 업데이트가 IoT 허브(110)에게 이용 가능한 경우, 그것은 IoT 서비스(120)로부터 업데이트를 자동적으로 다운로드 및 설치할 수 있다. 그것은 먼저 업데이트된 코드를 로컬 메모리에 복사하고, 구동하고, 구형 프로그램 코드를 교체하기 전에 업데이트를 검증할 수 있다. 유사하게, 업데이트가 IoT 디바이스(101 내지 105) 각각에게 이용 가능한 경우, 업데이트는 초기에 IoT 허브(110)에 의해 다운로드되고 IoT 디바이스(101 내지 105) 각각에 푸시 아웃될 수 있다. 그 후, 각각의 IoT 디바이스(101 내지 105)는 IoT 허브에 대해 위에서 설명된 것과 유사한 방식으로 업데이트를 적용하고 업데이트의 결과를 IoT 허브(110)에 다시 보고할 수 있다. 업데이트가 성공적이면, IoT 허브(110)는 그것의 메모리로부터 업데이트를 삭제하고 (예를 들어, 그것이 각각의 IoT 디바이스에 대한 새로운 업데이트를 계속 체크할 수 있도록) 각각의 IoT 디바이스 상에 설치된 코드의 최신 버전을 기록할 수 있다.

[0032] 일 실시예에서, IoT 허브(110)는 A/C 전력을 통해 전력공급된다. 특히, IoT 허브(110)는 A/C 전력 코드를 통해 공급된 A/C 전압을 더 낮은 DC 전압으로 변압시키기 위한 변압기를 갖는 전력 유닛(390)을 포함할 수 있다.

[0033] 도 4a는 IoT 시스템을 사용하여 범용 원격 제어 동작을 수행하기 위한 본 발명의 일 실시예를 예시한다. 특히, 이 실시예에서, IoT 디바이스들(101 내지 103)의 세트에는 (몇 개만 예로 들자면) 에어컨/히터(430), 조명 시스템(431) 및 시청각 장비(432)를 포함한 다양한 상이한 타입의 전자 장비를 제어하기 위해 원격 제어 코드를 전송하기 위한 적외선(IR) 및/또는 라디오 주파수(RF) 블라스터들(401 내지 403)이 각각 탑재된다. 도 4a에 도시된 실시예에서, IoT 디바이스들(101 내지 103)에는 또한 후술되는 바와 같이 그들이 제어하는 디바이스들의 동작을 검출하기 위한 센서들(404 내지 406)이 각각 탑재된다.

[0034] 예를 들어, IoT 디바이스(101) 내의 센서(404)는 현재의 온도/습도를 감지하고, 그에 응답하여 현재의 원하는 온도에 기초하여 에어컨/히터(430)를 제어하기 위한 온도 및/또는 습도 센서일 수 있다. 이 실시예에서, 에어컨/히터(430)는 원격 제어 디바이스(전형적으로 그 자체가 온도 센서를 내장하고 있는 리모트 컨트롤)를 통해 제어되도록 설계된 것이다. 일 실시예에서, 사용자는 사용자 디바이스(135) 상에 설치된 앱 또는 브라우저를 통해 IoT 허브(110)에 원하는 온도를 제공한다. IoT 허브(110) 상에서 실행되는 제어 로직(412)은 센서(404)로부터 현재 온도/습도 데이터를 수신하고, 그에 응답하여 원하는 온도/습도에 따라 IR/RF 블라스터(401)를 제어하기 위해 IoT 디바이스(101)에 커맨드를 전송한다. 예를 들어, 온도가 원하는 온도보다 낮으면, 제어 로직(412)은 IR/RF 블라스터(401)를 통해 에어컨/히터에 커맨드를 전송하여 (예를 들어, 에어컨을 턴오프하거나 히터를 턴온함으로써) 온도를 높일 수 있다. 커맨드는 IoT 허브(110) 상의 데이터베이스(413) 내에 저장된 필요한 원격 제어 코드를 포함할 수 있다. 대안적으로 또는 추가적으로, IoT 서비스(421)는 지정된 사용자 선호 및 저장된 제어 코드(422)에 기초하여 전자 장비(430 내지 432)를 제어하기 위한 제어 로직(421)을 구현할 수 있다.

[0035] 예시된 예의 IoT 디바이스(102)는 조명(431)을 제어하는 데 사용된다. 특히, IoT 디바이스(102) 내의 센서(405)는 조명 설비(431)(또는 다른 조명 장치)에 의해 생성되는 광의 현재 밝기를 검출하도록 구성된 광센서 또는 광검출기일 수 있다. 사용자는 사용자 디바이스(135)를 통해 IoT 허브(110)에 원하는 조명 레벨(온 또는 오프의 지시를 포함함)을 지정할 수 있다. 이에 응답하여, 제어 로직(412)은 IR/RF 블라스터(402)에 커맨드를 전송하여, 발광체(431)의 현재 밝기 레벨을 제어할 것이다(예를 들어, 현재 밝기가 너무 낮으면 조명을 높이거나 현재 밝기가 너무 높으면 조명을 낮추거나; 단순히 발광체를 턴온 또는 턴오프함).

[0036] 예시된 예의 IoT 디바이스(103)는 시청각 장비(432)(예를 들어, 텔레비전, A/V 수신기, 케이블/위성 수신기, 애플(Apple)TV™ 등)를 제어하도록 구성된다. IoT 디바이스(103) 내의 센서(406)는 현재의 주위 볼륨 레벨을 검출하기 위한 오디오 센서(예를 들어, 마이크로폰 및 관련 로직) 및/또는 텔레비전에 의해 생성된 광에 기초하여(예를 들어, 지정된 스펙트럼 내의 광을 측정함으로써) 텔레비전이 온 또는 오프 상태인지를 검출하기 위한 광센서일 수 있다. 대안적으로, 센서(406)는 검출된 온도에 기초하여 오디오 장비가 온 또는 오프 상태인지를 검출하기 위해 시청각 장비에 접속된 온도 센서를 포함할 수 있다. 다시 한번, 사용자 디바이스(135)를 통한 사용자 입력에 응답하여, 제어 로직(412)은 IoT 디바이스(103)의 IR 블라스터(403)를 통해 시청각 장비에 커맨드를 전송할 수 있다.

[0037] 전술한 내용은 단지 본 발명의 일 실시예의 예시적인 예에 불과하다는 점에 유의해야 한다. 본 발명의 기본 원리는 IoT 디바이스에 의해 제어될 임의의 특정 타입의 센서 또는 장비로 제한되지 않는다.

[0038] IoT 디바이스들(101 내지 103)이 블루투스 LE 접속을 통해 IoT 허브(110)에 결합되는 실시예에서, 센서 데이터 및 커맨드는 블루투스 LE 채널을 통해 전송된다. 그러나, 본 발명의 기본 원리는 블루투스 LE 또는 임의의 다른 통신 표준으로 제한되지 않는다.

[0039] 일 실시예에서, 각각의 전자 장비를 제어하는 데 필요한 제어 코드는 IoT 허브(110) 상의 데이터베이스(413) 및/또는 IoT 서비스(120) 상의 데이터베이스(422)에 저장된다. 도 4b에 예시된 바와 같이, 제어 코드는 IoT 서비스(120) 상에서 유지되는 상이한 장비들에 대한 제어 코드들(422)의 마스터 데이터베이스로부터 IoT 허브(110)에 제공될 수 있다. 최종 사용자는 사용자 디바이스(135) 상에서 실행되는 앱 또는 브라우저를 통해 제어될 전자(또는 다른) 장비의 타입을 지정할 수 있으며, 그에 응답하여 IoT 허브 상의 원격 제어 코드 학습 모듈(491)은 IoT 서비스(120) 상의 원격 제어 코드 데이터베이스(492)에서 (예를 들어, 고유 ID를 갖는 각각의 전자 장비를 식별하는) 필요한 IR/RF 코드를 검색할 수 있다.

[0040] 또한, 일 실시예에서, IoT 허브(110)에는 원격 제어 코드 학습 모듈(491)이 전자 장비와 함께 제공된 원래의 리모트 컨트롤(495)로부터 직접 새로운 원격 제어 코드를 "학습"하는 것을 가능하게 하는 IR/RF 인터페이스(490)가 탑재된다. 예를 들어, 에어컨(430)과 함께 제공된 원래의 리모트 컨트롤에 대한 제어 코드가 원격 제어 데이터베이스에 포함되어 있지 않으면, 사용자는 사용자 디바이스(135) 상의 앱/브라우저를 통해 IoT 허브(110)와 상호 작용하여, 원래의 리모트 컨트롤에 의해 생성된 다양한 제어 코드(예를 들어, 온도 증가, 온도 감소 등)를 IoT 허브(110)에게 교시할 수 있다. 원격 제어 코드가 학습되면, 이들은 IoT 허브(110) 상의 제어 코드 데이터베이스(413)에 저장되고/되거나, IoT 서비스(120)로 되돌려 보내져서 중앙 원격 제어 코드 데이터베이스(492)에 포함될 수 있다(그리고 후속하여 동일한 에어컨 유닛(430)을 갖는 다른 사용자에 의해 사용됨).

[0041] 일 실시예에서, IoT 디바이스들(101 내지 103) 각각은 극히 작은 폼 팩터를 가지며, 양면 테이프, 작은 못, 자석 부착 등을 사용하여 그들 각자의 전자 장비(430 내지 432) 상에 또는 그 부근에 부착될 수 있다. 에어컨(430)과 같은 장비의 제어를 위해, 센서(404)가 집 안의 주위 온도를 정확하게 측정할 수 있도록 IoT 디바이스(101)를 충분히 멀리 배치하는 것이 바람직할 것이다(예를 들어, 에어컨 상에 직접 IoT 디바이스를 배치하는 것은 에어컨이 작동 중일 때 너무 낮거나 히터가 작동 중일 때 너무 높을 온도 측정치를 초래할 것임). 대조적으로, 조명을 제어하는 데 사용되는 IoT 디바이스(102)는 센서(405)가 현재 조명 레벨을 검출하기 위해 조명 설비(431) 상에 또는 그 부근에 배치될 수 있다.

[0042] 설명된 바와 같은 일반적인 제어 기능을 제공하는 것 외에도, IoT 허브(110) 및/또는 IoT 서비스(120)의 일 실시예는 각각의 전자 장비의 현재 상태와 관련된 통지를 최종 사용자에게 전송한다. 텍스트 메시지 및/또는 앱 특유 통지일 수 있는 통지는 이어서 사용자의 모바일 디바이스(135)의 디스플레이 상에 표시될 수 있다. 예를 들어, 사용자의 에어컨이 장기간 동안 켜져 있었지만 온도가 변하지 않은 경우, IoT 허브(110) 및/또는 IoT 서비스(120)는 에어컨이 적절히 기능하고 있지 않다는 통지를 사용자에게 전송할 수 있다. 사용자가 집에 있지 않고(이는 모션 센서를 통해 또는 사용자의 현재 검출된 위치에 기초하여 검출될 수 있음), 센서(406)가 시청각 장비(430)가 켜져 있다는 것을 지시하거나, 센서(405)가 발광체가 켜져 있다는 것을 지시하는 경우, 사용자가

시청각 장비(432) 및/또는 발광체(431)를 턴오프하기를 원하는지를 묻는 통지가 사용자에게 전송될 수 있다. 임의의 장비 타입에 대해 동일한 타입의 통지가 전송될 수 있다.

[0043] 사용자가 통지를 수신하면, 그/그녀는 사용자 디바이스(135) 상의 앱 또는 브라우저를 통해 전자 장비(430 내지 432)를 원격 제어할 수 있다. 일 실시예에서, 사용자 디바이스(135)는 터치 스크린 디바이스이고, 앱 또는 브라우저는 장비(430 내지 432)를 제어하기 위해 사용자가 선택할 수 있는 버튼을 갖는 리모트 컨트롤의 이미지를 표시한다. 통지를 수신하면, 사용자는 그래픽 리모트 컨트롤을 열고 다양한 상이한 장비를 턴오프하거나 조정할 수 있다. IoT 서비스(120)를 통해 접속되는 경우, 사용자의 선택은 IoT 서비스(120)로부터 IoT 허브(110)로 전달될 수 있으며, 이어서 IoT 허브(110)는 제어 로직(412)을 통해 장비를 제어할 것이다. 대안적으로, 사용자 입력은 사용자 디바이스(135)로부터 IoT 허브(110)로 직접 전송될 수 있다.

[0044] 일 실시예에서, 사용자는 전자 장비(430 내지 432)에 대한 다양한 자동 제어 기능을 수행하도록 IoT 허브(110) 상의 제어 로직(412)을 프로그래밍할 수 있다. 전술한 바와 같이 원하는 온도, 밝기 레벨 및 볼륨 레벨을 유지하는 것 이외에, 제어 로직(412)은 소정 조건이 검출되면 전자 장비를 자동으로 턴오프할 수 있다. 예를 들어, 제어 로직(412)이 사용자가 집에 없고 에어컨이 기능하고 있지 않다는 것을 검출하면, 그것은 자동으로 에어컨을 턴오프할 수 있다. 유사하게, 사용자가 집에 없고, 센서(406)가 시청각 장비(430)가 켜져 있음을 나타내거나 센서(405)가 발광체가 켜져 있음을 나타내면, 제어 로직(412)은 IR/RF 블라스터(403, 402)를 통해 커맨드를 자동 전송하여, 시청각 장비 및 발광체를 각각 턴오프할 수 있다.

[0045] 도 5는 전자 장비(530, 531)를 모니터링하기 위한 센서(503, 504)가 탑재된 IoT 디바이스(104, 105)의 추가 실시예를 예시한다. 특히, 이 실시예의 IoT 디바이스(104)는 스토브가 켜진 채로 있을 때를 검출하기 위해 스토브(530) 상에 또는 그 부근에 배치될 수 있는 온도 센서(503)를 포함한다. 일 실시예에서, IoT 디바이스(104)는 온도 센서(503)에 의해 측정된 현재 온도를 IoT 허브(110) 및/또는 IoT 서비스(120)에 전송한다. 스토브가 (예를 들어, 측정된 온도에 기초하여) 임계 기간을 초과하여 켜져 있는 것으로 검출되면, 제어 로직(512)은 사용자에게 스토브(530)가 켜져 있음을 알리는 통지를 최종 사용자의 디바이스(135)에 전송할 수 있다. 또한, 일 실시예에서, IoT 디바이스(104)는, 사용자로부터 지시를 수신하는 것에 응답하여 또는 (제어 로직(512)이 사용자에 의해 그렇게 하도록 프로그래밍된 경우) 자동으로, 스토브를 턴오프하기 위한 제어 모듈(501)을 포함할 수 있다. 일 실시예에서, 제어 로직(501)은 스토브(530)에 대한 전기 또는 가스를 차단하는 스위치를 포함한다. 그러나, 다른 실시예에서, 제어 로직(501)은 스토브 자체 내에 통합될 수 있다.

[0046] 도 5는 또한 세탁기 및/또는 건조기와 같은 소정 타입의 전자 장비의 모션을 검출하기 위한 모션 센서(504)를 갖는 IoT 디바이스(105)를 예시한다. 사용될 수 있는 다른 센서는 주위 볼륨 레벨을 검출하기 위한 오디오 센서(예를 들어, 마이크로폰 및 로직)이다. 전술한 다른 실시예에서와 같이, 이 실시예는 소정의 지정된 조건이 충족되면(예를 들어, 모션이 장기간 동안 검출되어, 세탁기/건조기가 턴오프되지 않았음을 나타내는 경우) 최종 사용자에게 통지를 전송할 수 있다. 도 5에 도시되지 않지만, IoT 디바이스(105)에는 자동으로 그리고/또는 사용자 입력에 응답하여 (예를 들어, 전기/가스를 스위치 오프함으로써) 세탁기/건조기(531)를 턴오프하는 제어 모듈이 또한 탑재될 수 있다.

[0047] 일 실시예에서, 제어 로직 및 스위치를 갖는 제1 IoT 디바이스는 사용자의 집 안의 모든 전력을 턴오프하도록 구성될 수 있고, 제어 로직 및 스위치를 갖는 제2 IoT 디바이스는 사용자의 집 안의 모든 가스를 턴오프하도록 구성될 수 있다. 이어서, 센서를 갖는 IoT 디바이스가 사용자의 집에 있는 전자 또는 가스 구동 장비 상에 또는 그 부근에 배치될 수 있다. 사용자가 특정 장비(예를 들어, 스토브(530))가 켜진 채로 있다는 통지를 받으면, 사용자는 손상을 방지하기 위해 집 안의 모든 전기 또는 가스를 턴오프하기 위한 커맨드를 전송할 수 있다. 대안적으로, IoT 허브(110) 및/또는 IoT 서비스(120) 내의 제어 로직(512)은 그러한 상황에서 전기 또는 가스를 자동으로 턴오프하도록 구성될 수 있다.

[0048] 일 실시예에서, IoT 허브(110) 및 IoT 서비스(120)는 주기적인 간격으로 통신한다. IoT 서비스(120)가 (예를 들어, 지정된 지속 기간 동안 IoT 허브로부터 요청 또는 응답을 수신하지 못함으로써) IoT 허브(110)에 대한 접속이 손실된 것을 검출하면, (예를 들어, 텍스트 메시지 또는 앱 특유 통지를 전송함으로써) 이러한 정보를 최종 사용자의 디바이스(135)로 통신할 것이다.

[0049] IoT 시스템에서 사용자 위치를 정확하게 감지하기 위한 장치 및 방법

[0050] 현재의 무선 "스마트" 록들 및 차고 도어 오프너들은 최종 사용자가 모바일 디바이스를 통해 록 및/또는 차고 도어를 제어하는 것을 가능케 한다. 이러한 시스템들을 동작시키기 위해, 사용자는 모바일 디바이스 상에서 앱

을 열고, 개방/언록 또는 폐쇄/록 옵션을 선택해야 한다. 그에 응답하여, 무선 신호가 원하는 동작을 구현하는 무선 록 또는 차고 도어 상에 있거나 그에 결합된 수신기로 전송된다. 아래의 논의는 무선 "록들"에 집중되지만, 용어 "록"은 본 명세서에서 표준 도어 록들, 무선 차고 도어 오프너들, 및 빌딩 또는 다른 위치에 대한 액세스를 제한하기 위한 임의의 다른 디바이스를 지칭하기 위해 광범위하게 사용된다.

[0051] 몇몇 무선 록들은 사용자가 언제 도어 밖에 있는지를 결정하고, 그에 응답하여 개방/언록 기능을 트리거링하려고 시도한다. 예를 들어 도 6은 무선 디바이스(603)로부터의 신호의 신호 강도에 기초하여 무선 디바이스(603)를 가진 사용자가 도어(601) 밖으로부터 접근하는 것에 응답하여 무선 록(602)이 트리거링되는 예를 예시한다. 예를 들어, 무선 록(602)은 무선 디바이스(603)로부터 수신 신호 강도 지시자(RSSI)를 측정할 수 있고, 그것이 임계치(예컨대, -60 dbm)에 도달할 때 도어(601)를 언록킹할 것이다.

[0052] 이러한 기술들에 관한 한 가지 분명한 문제는 RSSI 측정이 비-지향적이라는 점이다. 예를 들어, 사용자가 무선 디바이스(603)를 갖고서 집 주위에서 이동하고 무선 록(602) 또는 차고 도어 오프너 곁을 지나가서, 그것이 트리거링되게 할 수 있다. 이러한 이유로, 사용자 근접 검출에 기초하여 동작하는 무선 록들의 사용이 제한되었다.

[0053] 도 7은 IoT 허브 및/또는 IoT 디바이스(710)가 사용자의 위치를 더 큰 정밀도로 결정하는 데 사용되는 본 발명의 일 실시예를 예시한다. 특히, 본 발명의 이 실시예는 무선 디바이스(703)와 IoT 록 디바이스(702) 사이의 신호 강도를 측정하고 또한 무선 디바이스(703)와 하나 이상의 IoT 디바이스/허브(710) 사이의 신호 강도를 측정하여, 사용자가 집 밖에 있는 경우와 집 안에 있는 경우를 구별한다. 예를 들어, 사용자가 집 안에서 또는 밖에서 IoT 록(702)으로부터 특정 거리에 있는 경우, 집 안의 위치로부터의 신호 강도(761)와 집 밖에서의 신호 강도(760)가 대략 동일할 수 있다. 도 6에 예시된 것과 같은 종래의 시스템들에서는, 이러한 두 가지 경우를 구별할 방법이 없었다. 그러나, 도 7에 도시된 실시예에서, 각각, 사용자가 집 밖에 있을 때와 집 안에 있을 때 IoT 허브/디바이스(710)와 무선 디바이스(703) 사이에서 측정된, 신호 강도 측정치들(750, 751)에 있어서의 차이들은 사용자의 위치를 결정하는 데 사용된다. 예를 들어, 무선 디바이스(703)가 외부 위치에 있을 때, 신호 강도(750)는 무선 디바이스(703)가 내부 위치에 있을 때의 신호 강도(751)와는 눈에 띄게 상이할 수 있다. 대부분의 경우 집 안에서의 신호 강도(751)가 더 강해야 하지만, 신호 강도(751)가 실제로는 더 약한 경우들이 있을 수 있다. 중요한 점은 신호 강도가 2개의 위치를 구별하는 데 사용될 수 있다는 점이다.

[0054] 신호 강도 값들(760, 761, 750, 751)은 IoT 허브/디바이스(710)에서 또는 IoT 록(702)에서(그것이 이러한 평가를 수행하기 위한 지능을 갖는 경우) 평가될 수 있다. 본 논의의 나머지는 신호 강도 평가가 IoT 허브(710)에 의해 수행되고, 이어서 IoT 허브(710)가 평가의 결과들에 기초하여 무선 통신 채널(770)(예컨대, BTLE)을 통해 록 또는 언록 커맨드를 IoT 록(702)으로 전송할 수 있는 것으로(또는 이미 록킹/언록킹된 경우에는 커맨드를 전송하지 않을 수 있는 것으로) 가정할 것이다. 그러나, IoT 록(702)이 평가를 수행하기 위한 로직을 갖도록 구성되면(예를 들어, 신호 강도 값들이 IoT 록(702)에 제공되는 경우) 동일한 기본 평가 및 결과가 IoT 록(702)에 의해 직접 수행될 수 있다는 점에 유의해야 한다.

[0055] 도 8은 2개의 IoT 허브/디바이스(710, 711)로부터의 신호 강도 값들을 이용하기 때문에, 더 큰 정밀도를 제공할 수 있는 다른 실시예를 예시한다. 이 실시예에서, 신호 강도(805)는 무선 디바이스(703)와 (1) IoT 허브/디바이스(711); (2) IoT 허브/디바이스(710); 및 (3) IoT 록(702) 사이에서 측정된다. 무선 디바이스는 도 8에서는 간략함을 위해 단일 위치에 도시된다.

[0056] 일 실시예에서, 수집된 신호 강도 값들 모두가 IoT 허브 디바이스들(710, 711) 중 하나에 제공되며, 이어서 그것은 값들을 평가하여 사용자의 위치(예를 들어, 내부 또는 외부)를 결정한다. 사용자가 외부에 있는 것으로 결정되면, IoT 허브/디바이스(710)는 커맨드를 IoT 록(702)으로 전송하여 도어를 언록킹할 수 있다. 대안적으로, IoT 록(702)이 평가를 수행하기 위한 로직을 갖는 경우, IoT 허브들/디바이스들(710, 711)은 신호 강도 값들을 IoT 록(702)으로 전송할 수 있고, 그것은 신호 강도 값들을 평가하여 사용자의 위치를 결정한다.

[0057] 도 9에 예시된 바와 같이, 일 실시예에서, IoT 허브(710) 상의 교정 모듈(910)이 무선 디바이스(703) 상의 앱 또는 브라우저 기반 코드와 통신하여 신호 강도 측정들을 교정한다. 교정 동안, 시스템 교정 모듈(910) 및/또는 교정 앱은 사용자에게 도어 밖의 소정 위치 및 도어 안의 소정 위치에(예를 들어, 도어 1의 6 피트 밖에, 도어 1의 6 피트 안에, 도어 2의 6 피트 밖에 등) 서 있도록 지시할 수 있다. 사용자는 사용자 인터페이스 상의 그래픽을 선택함으로써 그/그녀가 요구되는 위치에 있다는 것을 나타낼 수 있다. 이어서, 시스템 교정 앱 및/또는 시스템 교정 모듈(910)은 수집된 신호 강도 값들(900)을 IoT 허브/디바이스(710) 상의 위치 데이터베이스(901) 내의 각각의 위치와 관련시킬 것이다.

[0058] 일단 사용자의 상이한 알려진 위치들에 대한 신호 강도 값들이 수집되어 데이터베이스(901) 내에 저장되면, 신호 강도 분석 모듈(911)이 이러한 값들을 사용하여, 검출된 신호 강도 값들에 기초하여 도어를 록킹/언록킹하기 위한 IoT 록 커맨드들(950)을 전송할지를 결정한다. 도 9에 도시된 실시예에서, 2개의 상이한 도어에 대한 4개의 예시적인 위치: 도어 1 외부, 도어 1 내부, 도어 2 외부 및 도어 2 내부가 도시된다. RSSI1 값은 무선 록과 관련되며, -60 dbm의 임계치로 설정된다. 따라서, 일 실시예에서, 신호 강도 분석 모듈(911)은 RSSI1 값이 적어도 -60 dbm이 아닌 한 사용자의 위치를 결정하기 위한 그의 평가를 수행하지 않을 것이다. RSSI2 및 RSSI3 값들은 사용자의 무선 디바이스와 2개의 상이한 IoT 허브/디바이스 사이에서 측정된 신호 강도 값들이다.

[0059] RSSI1 임계치에 도달함을 가정하면, 신호 강도 분석 모듈(911)은 IoT 허브들/디바이스들과 사용자의 무선 디바이스 사이에서 측정된 현재의 신호 강도 값들(900)을 위치 데이터베이스(901)로부터의 RSSI2/RSSI3 값들과 비교한다. 현재의 RSSI 값들이 (예를 들어, IoT 허브/디바이스(710)에 대한) RSSI2 및 (예를 들어, IoT 허브/디바이스(711)에 대한) RSSI3에 대해 데이터베이스 내에 지정된 값들의 지정된 범위 내에 있는 경우, 무선 디바이스는 관련된 위치에 또는 그 근처에 있는 것으로 결정된다. 예를 들어, (예컨대, 교정 동안 행해진 측정에 기초하여) "도어 1 외부" 위치와 관련된 RSSI2 값이 -90 dbm이기 때문에, RSSI2에 대한 현재 측정된 신호 강도가 -93 dbm 내지 -87 dbm인 경우, RSSI2 비교는 (±3 dbm의 지정된 범위를 가정하여) 검증될 수 있다. 유사하게, (예를 들어, 교정 동안 행해진 측정에 기초하여) "도어 1 외부" 위치와 관련된 RSSI3 값이 -85 dbm이기 때문에, RSSI3에 대한 현재 측정된 신호 강도가 -88 dbm 내지 -82 dbm인 경우, RSSI3 비교는 검증될 수 있다. 따라서, 사용자가 IoT 록에 대해 -60 dbm 값 내에 그리고 RSSI2 및 RSSI3에 대해 위에서 지정된 범위들 내에 있는 경우, 신호 강도 분석 모듈(911)은 록을 개방하기 위한 커맨드(950)를 전송할 것이다. 이러한 방식으로 상이한 RSSI 값들을 비교함으로써, 시스템은 사용자가 집 안으로부터 IoT 록의 -60 dbm 이내에서 지나갈 때 바람직하지 않은 "언록" 이벤트들을 피하게 되는데, 이는 RSSI2 및 RSSI3에 대한 RSSI 측정치들이 내부 및 외부 사례들을 구별하는 데 사용되기 때문이다.

[0060] 일 실시예에서, 신호 강도 분석 모듈(911)은 내부 사례와 외부 사례 사이의 가장 큰 양의 구별을 제공하는 RSSI 값들에 의존한다. 예를 들어, (예컨대, 각각, 도어 2 내부 및 도어 2 외부에 대한 -96 dbm 및 -97 dbm의 RSSI3 값들과 같이) 내부 및 외부 사례들에 대한 RSSI 값들이 동등하거나 매우 유사한 몇몇 예들이 있을 수 있다. 그러한 경우, 신호 강도 분석 모듈은 다른 RSSI 값을 사용하여 2개의 사례를 구별할 것이다. 게다가, 일 실시예에서, 신호 강도 분석 모듈(911)은 기록된 RSSI 값들이 유사할 때 비교를 위해 사용되는 RSSI 범위들을 동적으로 조정할 수 있다(예를 들어, 측정된 RSSI 값들이 더 유사할 때 범위들을 더 작게 함). 따라서, ±3 dbm이 위의 예에 대한 비교 범위로 사용되지만, RSSI 측정치들이 얼마나 유사한지에 기초하여 다양한 상이한 범위들이 비교를 위해 설정될 수 있다.

[0061] 일 실시예에서, 시스템 교정 모듈(910) 시스템은 사용자가 도어를 통해 들어올 때마다 dbm 값들을 측정함으로써 시스템을 계속 훈련시킨다. 예를 들어, 초기 교정 후에 사용자가 집에 성공적으로 들어오는 것에 응답하여, 시스템 교정 모듈(910)은 RSSI2 및 RSSI3에 대한 추가적인 RSSI 값들을 저장할 수 있다. 이러한 방식으로, 다양한 RSSI 값들이 각각의 사례에 대해 위치/신호 강도 데이터베이스(901) 내에 저장되어 내부 사례와 외부 사례를 더욱 구별할 수 있다. 최종 결과는 현재 이용 가능한 것보다 훨씬 더 정밀한 무선 록 시스템이다.

[0062] 본 발명의 일 실시예에 따른 방법이 도 10에 예시된다. 방법은 상기에 기술된 시스템 아키텍처의 맥락 내에서 구현될 수 있지만, 임의의 특정 시스템 아키텍처로 제한되지 않는다.

[0063] 1001에서, 사용자 디바이스와 IoT 록 사이의 무선 신호 강도가 측정된다. 1002에서, 신호 강도가 지정된 임계치를 초과하면(즉, 사용자가 도어 근처에 있음을 지시함), 1002에서, 사용자 디바이스와 하나 이상의 IoT 허브/디바이스 사이의 무선 신호 강도가 측정된다. 1003에서, 수집된 무선 신호 강도 값들을 이전에 수집 및 저장된 신호 강도 값들과 비교하여 사용자의 위치를 결정한다. 예를 들어, RSSI 값들이 사용자가 이전에 도어 밖에 있었을 때의 RSSI 값들의 지정된 범위 내에 있는 경우, 사용자가 현재 도어 밖에 있는 것으로 결정될 수 있다. 1004에서, 평가에 기초하여, 사용자가 도어 밖에 있는지에 대한 결정이 행해진다. 그렇다면, 1005에서, 도어가 IoT 록을 사용하여 자동으로 언록킹된다.

[0064] IoT 록 시스템을 교정하기 위한 방법이 도 11에 예시된다. 1101에서, 사용자는 도어 밖에 서 있도록 요청되고, 1102에서, 사용자 디바이스와 하나 이상의 IoT 디바이스/허브 사이에서 무선 신호 강도 데이터가 수집된다. 언급된 바와 같이, 사용자의 무선 디바이스 상에 설치된 사용자 앱을 통해 사용자에게 요청이 전송될 수 있다. 1103에서, 사용자는 도어 안에 서 있도록 요청되고, 1104에서, 사용자 디바이스와 IoT 디바이스들/허브들 사이에서 무선 신호 강도 데이터가 수집된다. 1105에서, 신호 강도 데이터가 데이터베이스 내에 저장되며, 따라서

그것은 사용자의 현재 위치를 결정하기 위해 본 명세서에서 설명되는 바와 같이 신호 강도 값들을 비교하는 데 사용될 수 있다.

[0065] 본 명세서에서는 사용자의 집이 예시적인 실시예로서 사용되지만, 본 발명의 실시예들은 소비자 응용으로 제한되지 않는다는 점에 유의한다. 예를 들어, 이러한 동일 기술들이 사업체들 또는 다른 타입의 빌딩들에 대한 액세스를 제공하는 데 사용될 수 있다.

[0066] 일 실시예에서, 전술한 것과 유사한 기술들이 사용자의 집 전반에 걸쳐 사용자를 추적하는 데 사용된다. 예를 들어, 사용자의 무선 디바이스와 사용자의 집 안의 다양한 IoT 디바이스들/허브들 사이의 RSSI 측정치들을 추적함으로써, 상이한 사용자 위치들의 "맵"이 집계될 수 있다. 이어서, 이러한 맵은 사용자 현재 위치하는 방 안의 스피커들로 오디오를 지향시키는 것과 같은 서비스들을 최종 사용자에게 제공하는 데 사용될 수 있다.

[0067] 도 12는 무선 디바이스(703)와 복수의 IoT 디바이스(1101 내지 1105) 및 IoT 허브(1110) 사이에서 측정된 RSSI 값들이 사용자가 방 A 안에 있는지, 방 B 안에 있는지, 또는 방 C 안에 있는지를 결정하는 데 사용되는 예시적인 시스템의 개요를 제공한다. 특히, 무선 디바이스(703)와 IoT 허브(1110), IoT 디바이스(1103) 및 IoT 디바이스(1102) 사이에서 측정된 RSSI 값들(1121 내지 1123)에 기초하여, IoT 허브(1110)는 예시된 바와 같이 사용자가 현재 방 B 안에 있는 것으로 결정할 수 있다. 유사하게, 사용자가 방 C 안으로 이동할 때, 무선 디바이스(703)와 IoT 디바이스들(1104, 1105) 및 IoT 허브(1110) 사이의 RSSI 측정치들이 이어서 사용자가 방 C 안에 있는 것으로 결정하는 데 사용될 수 있다. 도 12에는 3개의 RSSI 측정(1121 내지 1123)만이 도시되지만, 더 큰 정밀도를 제공하기 위해 무선 디바이스(703)의 범위 내에 있는 임의의 IoT 디바이스 또는 IoT 허브 사이에서 RSSI 측정들이 행해질 수 있다.

[0068] 일 실시예에서, IoT 허브(1110)는 그 자신과 다양한 IoT 디바이스들(1101 내지 1105) 및 무선 디바이스(703) 사이의 RSSI 값들에 기초하여 삼각 측량 기술들을 이용하여 사용자의 위치를 삼각 측량할 수 있다. 예를 들어, IoT 디바이스(1102), IoT 허브(1110) 및 무선 디바이스(703) 사이에 형성된 RSSI 삼각형을 사용하여, 삼각형의 각각의 변에 대한 RSSI 값들에 기초하여 무선 디바이스(703)의 현재 위치를 결정할 수 있다.

[0069] 일 실시예에서, 전술한 것들과 유사한 교정 기술들을 사용하여 각각의 방 안에서 신호 강도 값들을 수집할 수 있다. 도 13은, 전술한 실시예들에서와 같이, 무선 디바이스(703) 상의 앱 또는 브라우저 기반 코드와 통신하여 신호 강도 측정들을 교정하는 시스템 교정 모듈(910)을 예시한다. 교정 동안, 시스템 교정 모듈(910) 및/또는 교정 앱은 IoT 시스템이 사용되고 있는 응용들에 따라 사용자에게 상이한 방들 안에 그리고 각 방 안의 소정 위치들에 서 있도록 지시할 수 있다. 전술한 바와 같이, 사용자는 사용자 인터페이스 상의 그래픽을 선택함으로써 그/그녀가 요구되는 위치에 있다는 것을 나타낼 수 있다. 이어서, 시스템 교정 앱 및/또는 시스템 교정 모듈(910)은 수집된 신호 강도 값들(900)을 IoT 허브/디바이스(710) 상의 위치 데이터베이스(1301) 내의 각각의 위치와 관련시킬 것이다.

[0070] 일단 사용자의 상이한 알려진 위치들에 대한 신호 강도 값들이 수집되어 데이터베이스(1301) 내에 저장되면, 신호 강도 분석 모듈(911)이 이러한 값들을 사용하여 사용자의 집 주위의 다양한 IoT 디바이스들(1101 내지 1105)을 제어한다. 예를 들어, IoT 디바이스들(1101 내지 1105)이 홈 오디오 시스템을 위한 스피커들 또는 증폭기들을 포함하는 경우, 신호 강도 분석 모듈(911)은 오디오가 재생되고 있는 방들을 제어하기 위해 IoT 디바이스 커맨드들(1302)을 전송할 수 있다(예를 들어, 사용자가 존재하는 방 안의 스피커들을 턴온하고, 다른 방들 안의 스피커들을 턴오프함). 유사하게, IoT 디바이스들(1101 내지 1105)이 조명 제어 유닛들을 포함하는 경우, 신호 강도 분석 모듈(911)은 사용자가 존재하는 방 안의 발광체들을 턴온하고 다른 방들 안의 발광체들을 턴오프하기 위해 IoT 디바이스 커맨드들(1302)을 전송할 수 있다. 물론, 본 발명의 기본 원리들은 임의의 특정 최종 사용자 응용들로 제한되지 않는다.

[0071] 언급된 바와 같이, 시스템 교정 모듈(910)의 일 실시예는 응용에 기초하여 방 안의 상이한 지점들에 대한 RSSI 데이터를 수집할 것이다. 도 13에서, 사용자에게 방 안의 상이한 위치들에 서 있도록 지시함으로써 각각의 방에 대한 RSSI 범위들이 수집된다. 예를 들어, 사용자의 거실의 경우, -99 dbm 내지 -93 dbm, -111 dbm 내지 -90 dbm, 및 -115 dbm 내지 -85 dbm의 RSSI 범위들이, 각각, RSSI1, RSSI2 및 RSSI3에 대해 수집된다(즉, 3개의 상이한 IoT 디바이스/허브로부터 수집된다). 무선 디바이스(703)의 현재 위치가 이러한 범위들 각각에 속할 때, 신호 강도 분석 모듈(911)은 사용자가 거실 안에 있는 것으로 결정하고 잠재적으로 IoT 디바이스 커맨드들(1302)을 전송하여 지정된 세트의 기능들(예를 들어, 발광체 턴온, 오디오의 턴온 등)을 수행할 것이다. 게다가, 방 안의 특정 지점들에 대해, 특정 RSSI 값들이 수집될 수 있다. 예를 들어, 도 13에서, 사용자가 거실 안의 소파에 앉아 있을 때 -88 dbm, -99 dbm 및 -101 dbm의 값들이 수집되었다. 전술한 실시예들에서와 같이, 신

호 강도 분석 모듈(911)은 RSSI 값들이 저장된 RSSI 값들의 지정된 범위 내에(예를 들어, ±3 dbm 내에) 있는 경우에 사용자가 카우치(couch) 위에 있는 것으로 결정할 수 있다. 게다가, 이전의 실시예들에서와 같이, 시스템 교정 모듈(910)은 RSSI 값들이 현재 상태로 유지되는 것을 보장하기 위해 상이한 위치들에 대한 데이터를 계속 수집할 수 있다. 예를 들어, 사용자가 거실을 재배열하는 경우, 카우치의 위치가 바뀔 수 있다. 이 경우, 시스템 교정 모듈(910)은 (예를 들어, 데이터베이스 내에 저장된 것들로부터의 RSSI 값들의 유사성이 주어지는 경우) 사용자가 현재 카우치에 앉아 있는지를 사용자에게 묻고, 신호 강도 데이터베이스(1301)를 새로운 값들로 업데이트할 수 있다.

[0072] 일 실시예에서, 다양한 타입의 IoT 디바이스들과의 사용자의 상호작용을 이용하여 사용자의 위치를 결정할 수 있다. 예를 들어, 사용자의 냉장고가 IoT 디바이스를 갖추고 있는 경우, 시스템은 사용자가 냉장고 도어를 개방한 것을 검출한 때 RSSI 측정치들을 취할 수 있다. 유사하게, 조명 시스템이 IoT 시스템을 포함하는 경우, 사용자가 집 또는 사업체의 상이한 방들 내의 발광체들을 조정할 때, 시스템은 RSSI 측정치들을 자동으로 취할 수 있다. 다른 예로서, 사용자가 다양한 기기들(예를 들어, 세탁기, 건조기, 식기 건조기), 시청각 장비(예컨대, 텔레비전, 오디오 장비 등) 또는 HVAC 시스템들(예컨대, 서모스탯 조정)과 상호작용할 때, 시스템은 RSSI 측정치들을 획득하고 측정치들을 이러한 위치들과 관련시킬 수 있다.

[0073] 전술한 실시예들에서는 단일 사용자 설명되지만, 본 발명의 실시예들은 다수의 사용자에 대해 구현될 수 있다. 예를 들어, 시스템 교정 모듈(910)은 신호 강도 데이터베이스(1301) 내에 저장될 사용자 A 및 사용자 B 둘 모두에 대한 신호 강도 값들을 수집할 수 있다. 이어서, 신호 강도 분석 모듈(911)은 신호 강도 측정치들의 비교들에 기초하여 사용자 A 및 사용자 B의 현재 위치를 식별하고 IoT 커맨드들(1302)을 전송하여 사용자 A 및 사용자 B의 집 주위의 IoT 디바이스들을 제어할 수 있다(예를 들어, 사용자 A 및 사용자 B가 존재하는 방들 안의 발광체들/스피커들을 온 상태로 유지함).

[0074] 본 명세서에서 설명되는 본 발명의 실시예들에서 사용되는 무선 디바이스(703)는 스마트폰, 태블릿, 웨어러블 디바이스(예컨대, 스마트워치, 목걸이 또는 팔찌 상의 토큰), 또는 RSSI 값들을 검출할 수 있는 임의의 다른 형태의 무선 디바이스(703)일 수 있다. 일 실시예에서, 무선 디바이스(703)는 블루투스 LE(BTLE)와 같은 단거리, 저전력 무선 통신 프로토콜을 통해 IoT 디바이스들(1101 내지 1105) 및 IoT 허브(1110)와 통신한다. 게다가, 일 실시예에서, 무선 디바이스(703)는 Wifi와 같은 장거리 무선 프로토콜을 통해 IoT 허브(1110)와 통신한다. 따라서, 이 실시예에서, RSSI 값들은 무선 디바이스(703)에 의해 수집되고 장거리 프로토콜을 이용하여 다시 IoT 허브(1110)로 통신될 수 있다. 게다가, 개별 IoT 디바이스들(1101 내지 1105) 각각은 RSSI 값들을 수집하고 이러한 값들을 단거리 무선 프로토콜을 통해 다시 IoT 허브(1110)로 통신할 수 있다. 본 발명의 기본 원리들은 RSSI 값들을 수집하는 데 사용되는 임의의 특정 프로토콜 또는 기술로 제한되지 않는다.

[0075] 본 발명의 일 실시예는 본 명세서에서 설명되는 기술들을 이용하여 단거리 무선 프로토콜을 사용하여 무선 확장기가 IoT 허브(1110)의 범위를 확장하기 위한 이상적인 위치를 찾는다. 예를 들어, 일 실시예에서, 새로운 확장기를 구매한 때, 시스템 교정 모듈(910)은 (예를 들어, 무선 디바이스(703) 상의 앱에 지시를 전송함으로써) 무선 확장기 디바이스를 갖는 사용자의 집의 방들 각각 안으로 사용자가 이동하도록 지시를 전송할 것이다. 접속 마법사가 또한 무선 디바이스(703) 상에서 실행되어 사용자가 프로세스를 통과하게 할 수 있다. 시스템 교정 모듈(910)에 의해 또는 마법사로부터 지시가 전송된 후, 사용자는 각각의 방 안으로 걸어 들어가서 무선 디바이스(703) 상의 버튼을 누를 것이다. 이어서, IoT 허브(1110)는 그 자신과 확장기 사이의 신호 강도를, 그리고 또한 확장기와 시스템 내의 모든 다른 IoT 디바이스들 사이의 신호 강도를 측정할 것이다. 이어서, 시스템 교정 모듈(910) 또는 무선 디바이스 마법사는 무선 확장기를 배치할 최상의 위치들의 우선순위화된 리스트를 사용자에게 제공할 수 있다(즉, 무선 확장기와 IoT 허브(1110) 사이 및/또는 무선 확장기와 IoT 디바이스들(1101 내지 1105) 사이에서 최고의 신호 강도를 갖는 그러한 위치들을 선택함).

[0076] 전술한 본 발명의 실시예들은 현재의 IoT 시스템들에서 발견되지 않는 IoT 시스템 내에서의 미세 조정 위치 인식을 제공한다. 게다가, 위치 정밀도를 개선하기 위해, 일 실시예에서, 무선 디바이스(703) 상의 GPS 시스템이 GPS 데이터뿐만 아니라 각각의 위치에 대한 RSSI 데이터를 포함할 사용자의 집의 정밀한 맵을 제공하는 데 사용될 정밀한 GPS 데이터를 통신할 수 있다.

[0077] 개선된 보안을 위한 실시예들

[0078] 일 실시예에서, 각각의 IoT 디바이스(101)의 저전력 마이크로제어기(200) 및 IoT 허브(110)의 저전력 로직/마이크로제어기(301)는 후술되는 실시예에 의해 사용되는 암호화 키를 저장하기 위한 보안 키 저장소를 포함한다(예를 들어, 도 14 내지 도 19 및 관련 텍스트 참조). 대안적으로, 키는 아래에서 논의되는 바와 같이 가입자 식

별 모듈(SIM)에서 보안될 수 있다.

[0079] 도 14는 IoT 서비스(120), IoT 허브(110) 및 IoT 디바이스(101, 102) 간의 통신을 암호화하기 위해 공개 키 기반구조(PKI) 기술 및/또는 대칭 키 교환/암호화 기술을 사용하는 고레벨 아키텍처를 예시한다.

[0080] 공개/비공개 키 쌍을 사용하는 실시예가 먼저 설명될 것이고, 이어서 대칭 키 교환/암호화 기술을 사용하는 실시예가 설명될 것이다. 특히, PKI를 사용하는 실시예에서는, 고유 공개/비공개 키 쌍이 각각의 IoT 디바이스(101, 102), 각각의 IoT 허브(110) 및 IoT 서비스(120)와 관련된다. 일 실시예에서, 새로운 IoT 허브(110)가 설정될 때, 그것의 공개 키가 IoT 서비스(120)에 제공되고, 새로운 IoT 디바이스(101)가 설정될 때, 그것의 공개 키가 IoT 허브(110) 및 IoT 서비스(120) 둘 모두에 제공된다. 디바이스들 사이에서 공개 키를 안전하게 교환하기 위한 다양한 기술이 아래에서 설명된다. 일 실시예에서, 임의의 수신 디바이스가 서명을 확인함으로써 공개 키의 유효성을 검증할 수 있도록 모든 수신 디바이스에 알려진(즉, 인증서 형태의) 마스터 키에 의해 모든 공개 키가 서명된다. 따라서, 단지 원시 공개 키만을 교환하기보다는 이러한 인증서가 교환될 것이다.

[0081] 예시된 바와 같이, 일 실시예에서, 각각의 IoT 디바이스(101, 102)는 각각의 디바이스의 비공개 키를 보안 저장하기 위한 보안 키 저장소(1401, 1403)를 각각 포함한다. 이어서, 보안 로직(1402, 1304)은 안전하게 저장된 비공개 키를 사용하여 본 명세서에 설명된 암호화/해독 동작을 수행한다. 유사하게, IoT 허브(110)는 IoT 허브 비공개 키 및 IoT 디바이스(101, 102) 및 IoT 서비스(120)의 공개 키를 저장하기 위한 보안 저장소(1411)뿐만 아니라, 키를 사용하여 암호화/해독 동작을 수행하기 위한 보안 로직(1412)을 포함한다. 마지막으로, IoT 서비스(120)는 그 자신의 비공개 키, 다양한 IoT 디바이스 및 IoT 허브의 공개 키를 보안 저장하기 위한 보안 저장소(1421), 및 키를 사용하여 IoT 허브 및 디바이스와의 통신을 암호화/해독하기 위한 보안 로직(1413)을 포함할 수 있다. 일 실시예에서, IoT 허브(110)가 IoT 디바이스로부터 공개 키 인증서를 수신할 때, IoT 허브는 (예를 들어, 전술한 바와 같이 마스터 키를 사용하여 서명을 확인함으로써) 그것을 검증할 수 있고, 이어서 그것 내부로부터 공개 키를 추출하여 그 공개 키를 그것의 보안 키 저장소(1411)에 저장할 수 있다.

[0082] 예로서, 일 실시예에서, IoT 서비스(120)가 커맨드 또는 데이터(예를 들어, 도어를 열기 위한 커맨드, 센서를 판독하기 위한 요청, IoT 디바이스에 의해 처리/표시될 데이터 등)를 IoT 디바이스(101)로 전송할 필요가 있을 때, 보안 로직(1413)은 IoT 디바이스(101)의 공개 키를 사용하여 데이터/커맨드를 암호화하여 암호화된 IoT 디바이스 패킷을 생성한다. 일 실시예에서, 보안 로직은 이어서 IoT 허브(110)의 공개 키를 사용하여 IoT 디바이스 패킷을 암호화하여 IoT 허브 패킷을 생성하고 IoT 허브 패킷을 IoT 허브(110)로 전송한다. 일 실시예에서, 서비스(120)는 암호화된 메시지를 그것의 비공개 키 또는 상기에 언급된 마스터 키로 서명하여, 디바이스(101)는 그것이 신뢰 소스로부터 변경되지 않은 메시지를 수신하고 있는지를 검증할 수 있다. 이어서, 디바이스(101)는 비공개 키 및/또는 마스터 키에 대응하는 공개 키를 사용하여 서명을 확인할 수 있다. 전술한 바와 같이, 공개/비공개 키 암호화 대신에 대칭 키 교환/암호화 기술이 사용될 수 있다. 이들 실시예에서, 하나의 키를 비공개적으로 저장하고 대응하는 공개 키를 다른 디바이스에 제공하기보다는, 디바이스들은 각각 암호화에 사용되고 서명을 확인하는 데 사용되는 동일한 대칭 키의 사본을 제공받을 수 있다. 대칭 키 알고리즘의 일례는 진보된 암호화 표준(AES)이지만, 본 발명의 기본 원리는 임의의 타입의 특정 대칭 키로 제한되지 않는다.

[0083] 대칭 키 구현을 사용하여, 각각의 디바이스(101)는 IoT 허브(110)와 대칭 키를 교환하기 위해 보안 키 교환 프로토콜에 들어간다. 동적 대칭 키 프로비저닝 프로토콜(DSKPP)과 같은 보안 키 프로비저닝 프로토콜이 보안 통신 채널을 통해 키를 교환하는 데 사용될 수 있다(예를 들어, RFC(Request for Comments) 6063 참조). 그러나, 본 발명의 기본 원리는 임의의 특정 키 프로비저닝 프로토콜로 제한되지 않는다.

[0084] 일단 대칭 키가 교환되면, 대칭 키는 통신을 암호화하기 위해 각각의 디바이스(101) 및 IoT 허브(110)에 의해 사용될 수 있다. 유사하게, IoT 허브(110) 및 IoT 서비스(120)는 보안 대칭 키 교환을 수행 한 다음, 교환된 대칭 키를 사용하여 통신을 암호화할 수 있다. 일 실시예에서, 새로운 대칭 키가 디바이스(101)와 허브(110) 사이에서 그리고 허브(110)와 IoT 서비스(120) 사이에서 주기적으로 교환된다. 일 실시예에서, 새로운 대칭 키가 디바이스(101), 허브(110) 및 서비스(120) 사이에서 각각의 새로운 통신 세션을 이용하여 교환된다(예를 들어, 새로운 키가 생성되고 각각의 통신 세션 동안 안전하게 교환된다). 일 실시예에서, IoT 허브 내의 보안 모듈(1412)이 신뢰되는 경우, 서비스(120)는 허브 보안 모듈(1312)과 세션 키를 협상할 수 있고, 이어서 보안 모듈(1412)은 각각의 디바이스(120)와 세션 키를 협상할 것이다. 이어서, 서비스(120)로부터의 메시지가 디바이스(101)로의 전송을 위해 재암호화되기 전에 허브 보안 모듈(1412)에서 해독 및 검증될 것이다.

[0085] 일 실시예에서, 허브 보안 모듈(1412) 상의 타협(compromise)을 방지하기 위해, 설치 시에 1회(영구) 설치 키가 디바이스(101)와 서비스(120) 사이에서 협상될 수 있다. 메시지를 디바이스(101)로 전송할 때, 서비스(120)는

먼저 이 디바이스 설치 키로 암호화/MAC하고, 이어서 허브의 세션 키로 암호화/MAC할 수 있다. 이어서, 허브(110)는 암호화된 디바이스 블롭(device blob)을 검증 및 추출하여, 이를 디바이스로 전송할 것이다.

[0086] 본 발명의 일 실시예에서, 재생 공격을 방지하기 위해 카운터 메커니즘이 구현된다. 예를 들어, 디바이스(101)로부터 허브(110)로의(또는 그 반대로의) 각각의 연속적인 통신이 계속 증가하는 카운터 값을 할당받을 수 있다. 허브(110) 및 디바이스(101) 둘 모두는 이 값을 추적하고 이 값이 디바이스들 간의 각각의 연속적인 통신에서 정확한지를 검증할 것이다. 동일한 기술이 허브(110)와 서비스(120) 사이에서 구현될 수 있다. 이러한 방식으로 카운터를 사용하는 것은 (카운터 값이 부정확할 것이기 때문에) 각각의 디바이스들 간의 통신을 스푸핑(spoofing)하는 것을 더 어렵게 할 것이다. 그러나, 이것 없이도, 서비스와 디바이스 간의 공유 설치 키가 모든 디바이스에 대한 네트워크(허브) 전반적 공격을 방지할 것이다.

[0087] 일 실시예에서, 공개/비공개 키 암호화를 사용할 때, IoT 허브(110)는 그것의 비공개 키를 사용하여 IoT 허브 패킷을 해독하고 암호화된 IoT 디바이스 패킷을 생성하여, 이것을 관련 IoT 디바이스(101)로 전송한다. 이어서, IoT 디바이스(101)는 그것의 비공개 키를 사용하여 IoT 디바이스 패킷을 해독하여, IoT 서비스(120)로부터 시작되는 커맨드/데이터를 생성한다. 이어서, IoT 디바이스는 데이터를 처리하고/하거나 커맨드를 실행할 수 있다. 대칭 암호화를 사용하여, 각각의 디바이스는 공유 대칭 키를 사용하여 암호화하고 해독할 것이다. 어느 경우에나, 각각의 송신 디바이스는 또한 메시지를 그것의 비공개 키로 서명할 수 있어서, 수신 디바이스는 그것의 진정성을 검증할 수 있다.

[0088] IoT 디바이스(101)로부터 IoT 허브(110)로의 그리고 IoT 서비스(120)로의 통신을 암호화하기 위해 상이한 키 세트가 사용될 수 있다. 예를 들어, 공개/비공개 키 배열을 사용하여, 일 실시예에서, IoT 디바이스(101) 상의 보안 로직(1402)은 IoT 허브(110)의 공개 키를 사용하여, IoT 허브(110)로 전송되는 데이터 패킷을 암호화한다. 이어서, IoT 허브(110) 상의 보안 로직(1412)은 IoT 허브의 비공개 키를 사용하여 데이터 패킷을 해독할 수 있다. 유사하게, IoT 디바이스(101) 상의 보안 로직(1402) 및/또는 IoT 허브(110) 상의 보안 로직(1412)은 IoT 서비스(120)의 공개 키를 사용하여 IoT 서비스(120)로 전송되는 데이터 패킷을 암호화할 수 있다(데이터 패킷은 이어서 IoT 서비스(120) 상의 보안 로직(1413)에 의해 서비스의 비공개 키를 사용하여 해독될 수 있다). 대칭 키를 사용하는 경우, 디바이스(101) 및 허브(110)는 하나의 대칭 키를 공유할 수 있는 반면, 허브 및 서비스(120)는 상이한 대칭 키를 공유할 수 있다.

[0089] 소정의 특정 상세가 위의 설명에서 기재되지만, 본 발명의 기본 원리는 다양한 상이한 암호화 기술을 사용하여 구현될 수 있다는 점에 유의해야 한다. 예를 들어, 상기에 논의된 일부 실시예는 비대칭 공개/비공개 키 쌍을 사용하지만, 대안적인 실시예는 다양한 IoT 디바이스(101, 102), IoT 허브(110) 및 IoT 서비스(120) 사이에서 안전하게 교환되는 대칭 키를 사용할 수 있다. 더욱이, 일부 실시예에서, 데이터/커맨드 그 자체가 암호화되는 것이 아니라, 키가 데이터/커맨드(또는 다른 데이터 구조)에 대한 서명을 생성하는 데 사용된다. 이어서, 수신자는 그것의 키를 사용하여 서명을 확인할 수 있다.

[0090] 도 15에 예시된 바와 같이, 일 실시예에서, 각각의 IoT 디바이스(101) 상의 보안 키 저장소는 프로그래밍 가능 가입자 식별 모듈(SIM)(1501)을 사용하여 구현된다. 이 실시예에서, IoT 디바이스(101)는 처음에, IoT 디바이스(101) 상의 SIM 인터페이스(1500) 내에 안착되는 프로그래밍되지 않은 SIM 카드(1501)와 함께 최종 사용자에게 제공될 수 있다. 하나 이상의 암호화 키의 세트를 갖도록 SIM을 프로그래밍하기 위해, 사용자는 SIM 인터페이스(500)로부터 프로그래밍 가능 SIM 카드(1501)를 취하여, 그것을 IoT 허브(110) 상의 SIM 프로그래밍 인터페이스(1502) 안에 삽입한다. 이어서, IoT 허브 상의 프로그래밍 로직(1525)은 SIM 카드(1501)를 안전하게 프로그래밍하여, IoT 디바이스(101)를 IoT 허브(110) 및 IoT 서비스(120)에 대해 등록/페어링한다. 일 실시예에서, 공개/비공개 키 쌍이 프로그래밍 로직(1525)에 의해 무작위로 생성될 수 있고, 이어서 그 쌍의 공개 키는 IoT 허브의 보안 저장 디바이스(411)에 저장될 수 있는 반면, 비공개 키는 프로그래밍 가능 SIM(1501) 내에 저장될 수 있다. 게다가, 프로그래밍 로직(525)은 IoT 허브(110), IoT 서비스(120) 및/또는 임의의 다른 IoT 디바이스(101)의 공개 키를 (IoT 디바이스(101) 상의 보안 로직(1302)에 의해 발신 데이터를 암호화하는 데 사용되도록) SIM 카드(1401) 상에 저장할 수 있다. 일단 SIM(1501)이 프로그래밍되면, 새로운 IoT 디바이스(101)는 SIM을 보안 식별자로서 사용하여(예를 들어, SIM을 사용하여 디바이스를 등록하기 위한 기존 기술을 사용하여) IoT 서비스(120)로 프로비저닝될 수 있다. 프로비저닝 후에, IoT 허브(110) 및 IoT 서비스(120) 둘 모두는 IoT 디바이스(101)와의 통신을 암호화할 때 사용될 IoT 디바이스의 공개 키의 사본을 안전하게 저장할 것이다.

[0091] 도 15와 관련하여 전술한 기술은 새로운 IoT 디바이스를 최종 사용자에게 제공할 때 엄청난 유연성을 제공한다. 사용자가 (현재 행해지고 있는 바와 같이) 판매/구매 시에 각각의 SIM을 특정 서비스 제공자에 직접 등록할 것

을 요구하기보다는, SIM은 IoT 허브(110)를 통해 최종 사용자에 의해 직접 프로그래밍될 수 있고 프로그래밍의 결과는 IoT 서비스(120)로 안전하게 통신될 수 있다. 결과적으로, 새로운 IoT 디바이스(101)는 온라인 또는 로컬 소매상으로부터 최종 사용자에게 판매될 수 있고, 나중에 IoT 서비스(120)로 안전하게 프로비저닝될 수 있다.

[0092] 등록 및 암호화 기술이 SIM(가입자 식별 모듈)의 특정 상황에서 전술되지만, 본 발명의 기본 원리는 "SIM" 디바이스로 제한되지 않는다. 오히려, 본 발명의 기본 원리는 암호화 키 세트를 저장하기 위한 보안 저장소를 갖는 임의의 타입의 디바이스를 사용하여 구현될 수 있다. 또한, 위의 실시예가 이동 가능한 SIM 디바이스를 포함하지만, 일 실시예에서, SIM 디바이스는 이동 가능한 것이 아니라, IoT 디바이스 그 자체가 IoT 허브(110) 상의 프로그래밍 인터페이스(1502) 내에 삽입될 수 있다.

[0093] 일 실시예에서, 사용자가 SIM(또는 다른 디바이스)을 프로그래밍할 것을 요구하기보다는, SIM은 최종 사용자에게 배포되기 전에 IoT 디바이스(101) 내에 미리 프로그래밍된다. 이 실시예에서, 사용자가 IoT 디바이스(101)를 설정할 때, 본 명세서에서 설명되는 다양한 기술은 IoT 허브(110)/IoT 서비스(120)와 새로운 IoT 디바이스(101) 사이에서 암호화 키를 안전하게 교환하는 데 사용될 수 있다.

[0094] 예를 들어, 도 16a에 예시된 바와 같이, 각각의 IoT 디바이스(101) 또는 SIM(401)은 IoT 디바이스(101) 및/또는 SIM(1501)을 고유하게 식별하는 바코드 또는 QR 코드(1501)와 함께 패키징될 수 있다. 일 실시예에서, 바코드 또는 QR 코드(1601)는 IoT 디바이스(101) 또는 SIM(1001)에 대한 공개 키의 인코딩된 표현을 포함한다. 대안적으로, 바코드 또는 QR 코드(1601)는 IoT 허브(110) 및/또는 IoT 서비스(120)에 의해 공개 키를 식별하거나 생성하는 데 사용될 수 있다(예를 들어, 보안 저장소에 이미 저장된 공개 키에 대한 포인터로서 사용될 수 있다). 바코드 또는 QR 코드(601)는 (도 16a에 도시된 바와 같이) 별도의 카드 상에 인쇄될 수 있거나 IoT 디바이스 그 자체 상에 직접 인쇄될 수 있다. 바코드가 인쇄되는 곳에 관계없이, 일 실시예에서, IoT 허브(110)에는 바코드를 판독하고 결과적인 데이터를 IoT 허브(110) 상의 보안 로직(1012) 및/또는 IoT 서비스(120) 상의 보안 로직(1013)에 제공하기 위한 바코드 판독기(206)가 탑재된다. 이어서, IoT 허브(110) 상의 보안 로직(1012)은 IoT 디바이스에 대한 공개 키를 그것의 보안 키 저장소(1011) 내에 저장할 수 있고, IoT 서비스(120) 상의 보안 로직(1013)은 공개 키를 (후속 암호화된 통신에 사용되도록) 그것의 보안 저장소(1021) 내에 저장할 수 있다.

[0095] 일 실시예에서, 바코드 또는 QR 코드(1601)에 포함되는 데이터는 또한 IoT 서비스 제공자에 의해 설계된 IoT 앱 또는 브라우저 기반 애플릿이 설치된 (예를 들어, 아이폰 또는 안드로이드 디바이스와 같은) 사용자 디바이스(135)를 통해 캡처될 수 있다. 일단 캡처되면, 바코드 데이터는 (예를 들어, 보안 소켓 계층(SSL) 접속과 같은) 보안 접속을 통해 IoT 서비스(120)로 안전하게 통신될 수 있다. 바코드 데이터는 또한 보안 로컬 접속을 통해(예를 들어, 로컬 WiFi 또는 블루투스 LE 접속을 통해) 클라이언트 디바이스(135)로부터 IoT 허브(110)로 제공될 수 있다.

[0096] IoT 디바이스(101) 상의 보안 로직(1002) 및 IoT 허브(110) 상의 보안 로직(1012)은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 임의의 조합을 사용하여 구현될 수 있다. 예를 들어, 일 실시예에서, 보안 로직(1002, 1012)은 IoT 디바이스(101)와 IoT 허브(110) 사이에 로컬 통신 채널(130)을 설정하는 데 사용되는 칩(예를 들어, 로컬 채널(130)이 블루투스 LE인 경우에 블루투스 LE 칩) 내에 구현된다. 보안 로직(1002, 1012)의 특정 위치에 관계없이, 일 실시예에서, 보안 로직(1002, 1012)은 소정 타입의 프로그램 코드를 실행하기 위한 보안 실행 환경을 설정하도록 설계된다. 이것은 예를 들어 트러스트존(TrustZone) 기술(일부 ARM 프로세서 상에서 이용 가능함) 및/또는 신뢰 실행 기술(Trusted Execution Technology)(인텔(Intel)에 의해 설계됨)을 사용하여 구현될 수 있다. 물론, 본 발명의 기본 원리는 임의의 특정 타입의 보안 실행 기술로 제한되지 않는다.

[0097] 일 실시예에서, 바코드 또는 QR 코드(1501)는 각각의 IoT 디바이스(101)를 IoT 허브(110)와 페어링하는 데 사용될 수 있다. 예를 들어, 블루투스 LE 디바이스를 페어링하기 위해 현재 사용되는 표준 무선 페어링 프로세스를 사용하기보다는, 바코드 또는 QR 코드(1501) 내에 임베딩되는 페어링 코드가 IoT 허브를 대응하는 IoT 디바이스와 페어링하기 위해 IoT 허브(110)에 제공될 수 있다.

[0098] 도 16b는 IoT 허브(110) 상의 바코드 판독기(206)가 IoT 디바이스(101)와 관련된 바코드/QR 코드(1601)를 캡처하는 일 실시예를 예시한다. 언급된 바와 같이, 바코드/QR 코드(1601)는 IoT 디바이스(101) 상에 직접 인쇄될 수 있거나, IoT 디바이스(101)가 제공된 별개의 카드 상에 인쇄될 수 있다. 어느 경우에나, 바코드 판독기(206)는 바코드/QR 코드(1601)로부터 페어링 코드를 판독하고 로컬 통신 모듈(1680)에 페어링 코드를 제공한다. 일 실시예에서, 로컬 통신 모듈(1680)은 블루투스 LE 칩 및 관련 소프트웨어이지만, 본 발명의 기본 원리는 임의의 특정 프로토콜 표준으로 제한되지 않는다. 일단 페어링 코드가 수신되면, 그것은 페어링 데이터(1685)를

포함하는 보안 저장소에 저장되고, IoT 디바이스(101) 및 IoT 허브(110)는 자동적으로 페어링된다. IoT 허브가 이러한 방식으로 새로운 IoT 디바이스와 페어링될 때마다, 그러한 페어링을 위한 페어링 데이터는 보안 저장소(685) 내에 저장된다. 일 실시예에서, 일단 IoT 허브(110)의 로컬 통신 모듈(1680)이 페어링 코드를 수신하면, 그것은 IoT 디바이스(101)와의 로컬 무선 채널을 통한 통신을 암호화하기 위한 키로서 코드를 사용할 수 있다.

[0099] 유사하게, IoT 디바이스(101) 측에서, 로컬 통신 모듈(1590)은 로컬 보안 저장 디바이스(1595) 내에 IoT 허브와의 페어링을 지시하는 페어링 데이터를 저장한다. 페어링 데이터(1695)는 바코드/QR 코드(1601)에서 식별된 미리 프로그래밍된 페어링 코드를 포함할 수 있다. 페어링 데이터(1695)는 또한 보안 로컬 통신 채널을 설정하는 데 필요한, IoT 허브(110) 상의 로컬 통신 모듈(1680)로부터 수신된 페어링 데이터(예를 들어, IoT 허브(110)와의 통신을 암호화하기 위한 추가 키)를 포함할 수 있다.

[0100] 따라서, 바코드/QR 코드(1601)는 페어링 코드가 무선으로 전송되지 않기 때문에 현재 무선 페어링 프로토콜보다 훨씬 더 안전한 방식으로 로컬 페어링을 수행하는 데 사용될 수 있다. 또한, 일 실시예에서, 페어링에 사용되는 동일한 바코드/QR 코드(1601)는 IoT 디바이스(101)로부터 IoT 허브(110)로의 그리고 IoT 허브(110)로부터 IoT 서비스(120)로의 보안 접속을 구축하기 위한 암호화 키를 식별하는 데 사용될 수 있다.

[0101] 본 발명의 일 실시예에 따른 SIM 카드를 프로그래밍하는 방법이 도 17에 예시되어 있다. 방법은 전술한 시스템 아키텍처 내에서 구현될 수 있지만, 임의의 특정 시스템 아키텍처로 제한되지 않는다.

[0102] 1701에서 사용자는 블랭크(blank) SIM 카드를 갖는 새로운 IoT 디바이스를 수신하고, 1602에서 사용자는 블랭크 SIM 카드를 IoT 허브 안에 삽입한다. 1703에서, 사용자는 하나 이상의 암호화 키의 세트를 갖도록 블랭크 SIM 카드를 프로그래밍한다. 예를 들어, 전술한 바와 같이, 일 실시예에서, IoT 허브는 공개/비공개 키 쌍을 무작위로 생성하고, SIM 카드 상에 비공개 키를 저장하고 그것의 로컬 보안 저장소에 공개 키를 저장할 수 있다. 또한, 1704에서, 적어도 공개 키가 IoT 서비스로 전송되어, 그것은 IoT 디바이스를 식별하고 IoT 디바이스와의 암호화된 통신을 설정하는 데 사용될 수 있다. 전술한 바와 같이, 일 실시예에서, "SIM" 카드 이외의 프로그래밍 가능 디바이스가 도 17에 도시된 방법에서 SIM 카드와 동일한 기능을 수행하는 데 사용될 수 있다.

[0103] 새로운 IoT 디바이스를 네트워크 안에 통합하는 방법이 도 18에 예시되어 있다. 방법은 전술한 시스템 아키텍처 내에서 구현될 수 있지만, 임의의 특정 시스템 아키텍처로 제한되지 않는다.

[0104] 1801에서, 사용자는 암호화 키가 미리 할당된 새로운 IoT 디바이스를 수신한다. 1802에서, 키는 IoT 허브에 안전하게 제공된다. 전술한 바와 같이, 일 실시예에서, 이것은 디바이스에 할당된 공개/비공개 키 쌍의 공개 키를 식별하기 위해 IoT 디바이스와 관련된 바코드를 판독하는 것을 포함한다. 바코드는 IoT 허브에 의해 직접 판독되거나 모바일 디바이스를 통해 앱 또는 브라우저를 통해 캡처될 수 있다. 대안적인 실시예에서, 블루투스 LE 채널, 근거리장 통신(NFC) 채널 또는 보안 WiFi 채널과 같은 보안 통신 채널이 IoT 디바이스와 IoT 허브 사이에 설정되어 키를 교환할 수 있다. 키가 전송되는 방식에 상관없이, 일단 수신되면, 그것은 IoT 허브 디바이스의 보안 키 저장소에 저장된다. 전술한 바와 같이, 보안 엔클레이브(Secure Enclave), 신뢰 실행 기술(TXT) 및/또는 트러스트존과 같은 다양한 보안 실행 기술이 키를 저장하고 보호하기 위해 IoT 허브 상에서 사용될 수 있다. 또한, 1803에서, 키는 IoT 서비스로 안전하게 전송되며, IoT 서비스는 그 자신의 보안 키 저장소에 키를 저장한다. 이어서, IoT 서비스는 키를 사용하여 IoT 디바이스와의 통신을 암호화할 수 있다. 다시 한번, 교환은 인증서/서명된 키를 사용하여 구현될 수 있다. 허브(110) 내에서, 저장된 키의 변경/추가/제거를 방지하는 것이 특히 중요하다.

[0105] 공개/비공개 키를 사용하여 커맨드/데이터를 IoT 디바이스로 안전하게 통신하는 방법이 도 19에 예시되어 있다. 방법은 전술한 시스템 아키텍처 내에서 구현될 수 있지만, 임의의 특정 시스템 아키텍처로 제한되지 않는다.

[0106] 1901에서, IoT 서비스는 IoT 디바이스 공개 키를 사용하여 데이터/커맨드를 암호화하여 IoT 디바이스 패킷을 생성한다. 이어서 그것은 IoT 허브의 공개 키를 사용하여 IoT 디바이스 패킷을 암호화하여 IoT 허브 패킷을 생성한다(예를 들어, IoT 디바이스 패킷 주위에 IoT 허브 래퍼(wrapper)를 생성함). 1902에서, IoT 서비스는 IoT 허브 패킷을 IoT 허브로 전송한다. 1903에서, IoT 허브는 IoT 허브의 비공개 키를 사용하여 IoT 허브 패킷을 해독하여 IoT 디바이스 패킷을 생성한다. 1904에서, 그것은 이어서 IoT 디바이스 패킷을 IoT 디바이스로 전송하고, IoT 디바이스는 1905에서 IoT 디바이스 비공개 키를 사용하여 IoT 디바이스 패킷을 해독하여 데이터/커맨드를 생성한다. 1906에서, IoT 디바이스는 데이터/커맨드를 처리한다.

[0107] 대칭 키를 사용하는 실시예에서, 대칭 키 교환은 각각의 디바이스들 사이에서(예를 들어, 각각의 디바이스와 허브 사이에서 그리고 허브와 서비스 사이에서) 협상될 수 있다. 일단 키 교환이 완료되면, 각각의 송신 디바이

스는 데이터를 수신 디바이스로 송신하기 전에 대칭 키를 사용하여 각각의 송신을 암호화 및/또는 서명한다.

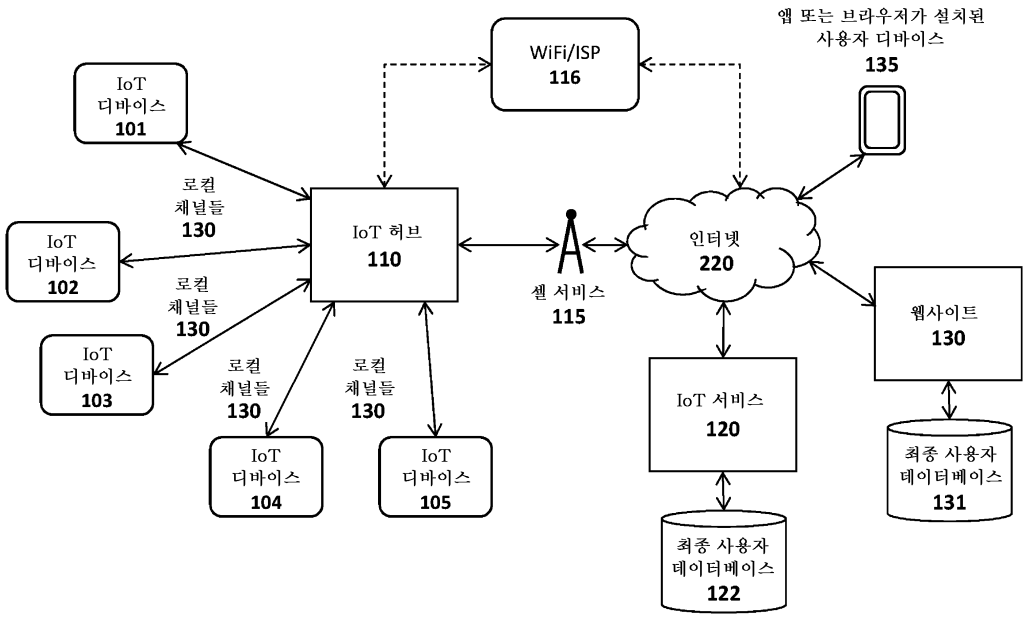
[0108] 본 발명의 실시예는 위에서 설명된 다양한 단계를 포함할 수 있다. 단계는 범용 또는 특수-목적 프로세서로 하여금 그 단계를 수행하게 하기 위해 사용될 수 있는 기계-실행 가능 명령어들로 구현될 수 있다. 대안적으로, 이들 단계는 단계를 수행하기 위한 하드와이어드 로직(hardwired logic)을 포함하는 특정 하드웨어 컴포넌트들에 의해, 또는 프로그래밍된 컴퓨터 컴포넌트와 맞춤형 하드웨어 컴포넌트의 임의의 조합에 의해 수행될 수 있다.

[0109] 본 명세서에 설명된 바와 같이, 명령어는, 소정의 동작을 수행하도록 구성되거나, 비일시적인 컴퓨터 판독 가능 매체에 수록되는 메모리에 저장된 소프트웨어 명령어 또는 미리 결정된 기능을 갖는 주문형 집적 회로(ASIC)와 같은 하드웨어의 특정한 구성을 지칭할 수 있다. 따라서, 도면에 도시된 기법은 하나 이상의 전자 디바이스(예를 들어, 최종 스테이션, 네트워크 요소 등) 상에 저장되고 그것 상에서 실행되는 코드 및 데이터를 사용하여 구현될 수 있다. 그러한 전자 디바이스는 비일시적 컴퓨터 기계 판독 가능 저장 매체(예를 들어, 자기 디스크, 광 디스크, 랜덤 액세스 메모리, 판독 전용 메모리, 플래시 메모리 디바이스, 상변화 메모리) 및 일시적 컴퓨터 기계 판독 가능 통신 매체(예를 들어, 전기, 광학, 음향 또는 다른 형태의 전파 신호 - 예를 들어, 반송파, 적외선 신호, 디지털 신호 등)와 같은 컴퓨터 기계 판독 가능 매체를 사용하여 코드 및 데이터를 저장하고 (내부적으로 그리고/또는 네트워크를 통해 다른 전자 디바이스와) 통신한다. 부가적으로, 그러한 전자 디바이스는 전형적으로 하나 이상의 저장 디바이스(비일시적 기계 판독 가능 저장 매체), 사용자 입력/출력 디바이스(예를 들어, 키보드, 터치스크린, 및/또는 디스플레이), 및 네트워크 접속부와 같은 하나 이상의 다른 컴포넌트에 결합된 하나 이상의 프로세서의 세트를 포함한다. 프로세서의 세트와 다른 컴포넌트의 결합은 전형적으로 하나 이상의 버스 및 브리지(또한 버스 제어기로 지칭됨)를 통해 이루어진다. 저장 디바이스 및 네트워크 트래픽을 반송하는 신호는 각각 하나 이상의 기계 판독 가능 저장 매체 및 기계 판독 가능 통신 매체를 대표한다. 따라서, 주어진 전자 디바이스의 저장 디바이스는 전형적으로 그 전자 디바이스의 하나 이상의 프로세서의 세트 상에서의 실행을 위한 코드 및/또는 데이터를 저장한다. 물론, 본 발명의 실시예의 하나 이상의 부분이 소프트웨어, 펌웨어, 및/또는 하드웨어의 상이한 조합을 사용하여 구현될 수 있다.

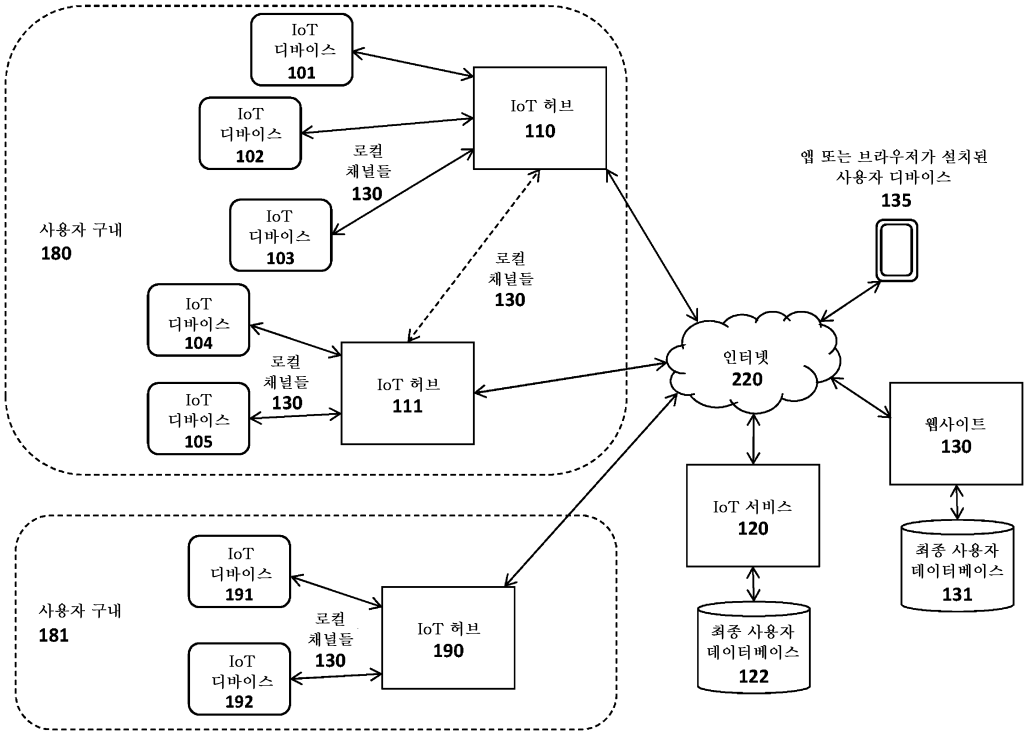
[0110] 이러한 상세한 설명 전반에 걸쳐, 설명의 목적으로, 본 발명의 완전한 이해를 제공하기 위해 다수의 특정 상세가 기술되었다. 그러나, 본 발명은 이러한 특정 상세들 중 일부 없이도 실시될 수 있다는 것이 당업자에게 명백할 것이다. 소정의 경우에, 잘 알려진 구조 및 기능은 본 발명의 주제를 불명확하게 하는 것을 피하기 위해 정성 들여 상세히 설명되지 않았다. 따라서, 본 발명의 범주 및 사상은 후속하는 청구범위의 관점에서 판단되어야 한다.

도면

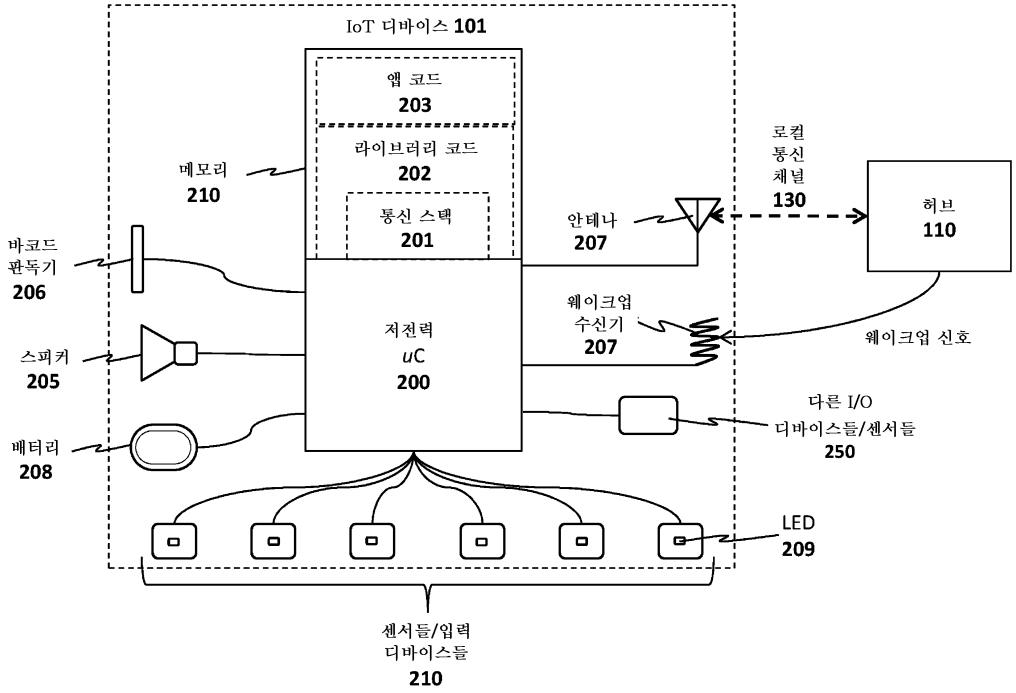
도면1a


WiFi/ISP
116
앱 또는 브라우저가 설치된
사용자 디바이스
135
IoT
디바이스
101
로컬
채널들
130
IoT 허브
110
셀 서비스
115
인터넷
220
IoT
디바이스
102
로컬
채널들
130
웹사이트
130
IoT
디바이스
103
로컬
채널들
130
로컬
채널들
130
IoT 서비스
120
최종 사용자
데이터베이스
131
IoT
디바이스
104
IoT
디바이스
105
최종 사용자
데이터베이스
122

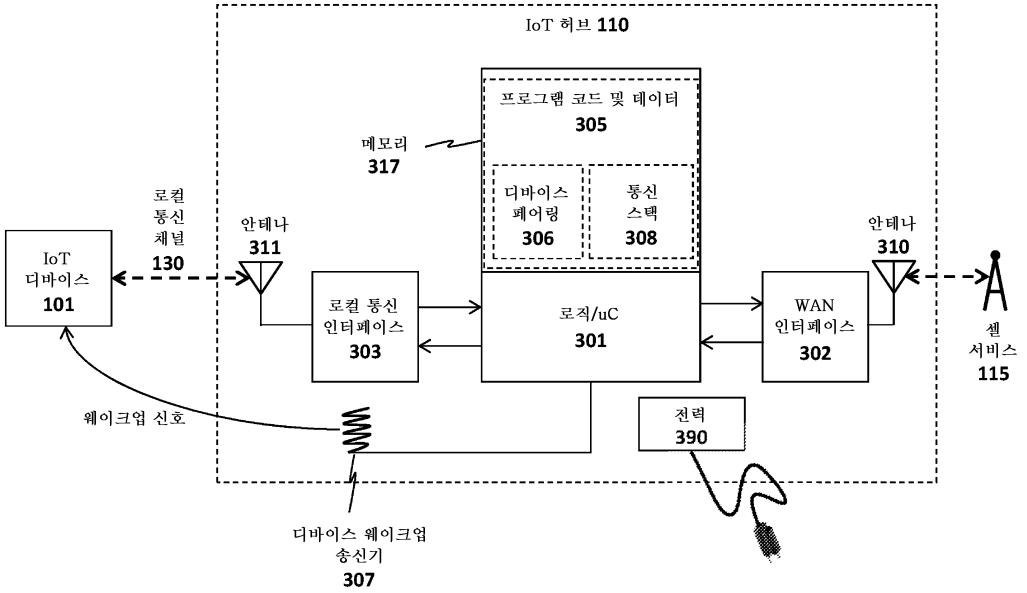
도면1b


IoT
디바이스
101
IoT 허브
110
IoT
디바이스
102
로컬
채널들
130
앱 또는 브라우저가 설치된
사용자 디바이스
135
사용자 구내
180
IoT
디바이스
103
로컬
채널들
130
IoT
디바이스
104
로컬
채널들
130
IoT 허브
111
인터넷
220
IoT
디바이스
105
웹사이트
130
IoT 서비스
120
최종 사용자
데이터베이스
131
사용자 구내
181
IoT
디바이스
191
로컬
채널들
130
IoT 허브
190
IoT
디바이스
192
최종 사용자
데이터베이스
122

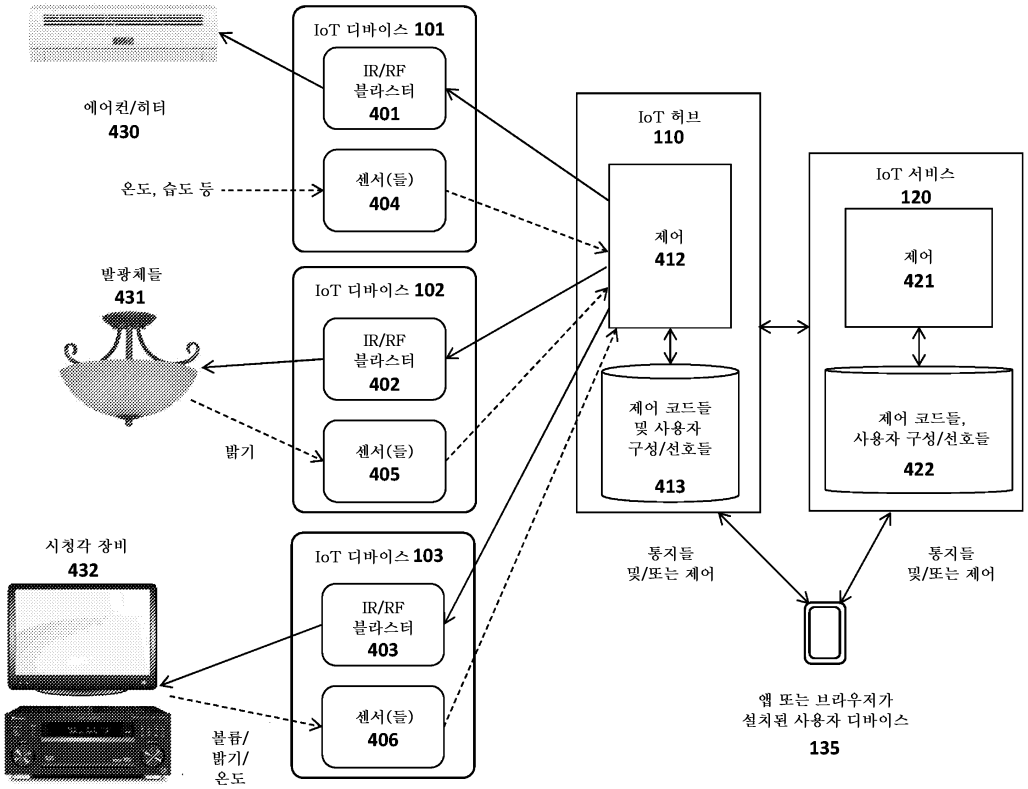
도면2


IoT 디바이스 101
앱 코드
203
라이브러리 코드
202
통신 스택
201
메모리
210
바코드
판독기
206
스피커
205
배터리
208
저전력
uC
200
안테나
207
로컬
통신
채널
130
허브
110
웨이크업
수신기
207
웨이크업 신호
다른 I/O
디바이스들/센서들
250
LED
209
센서들/입력
디바이스들
210

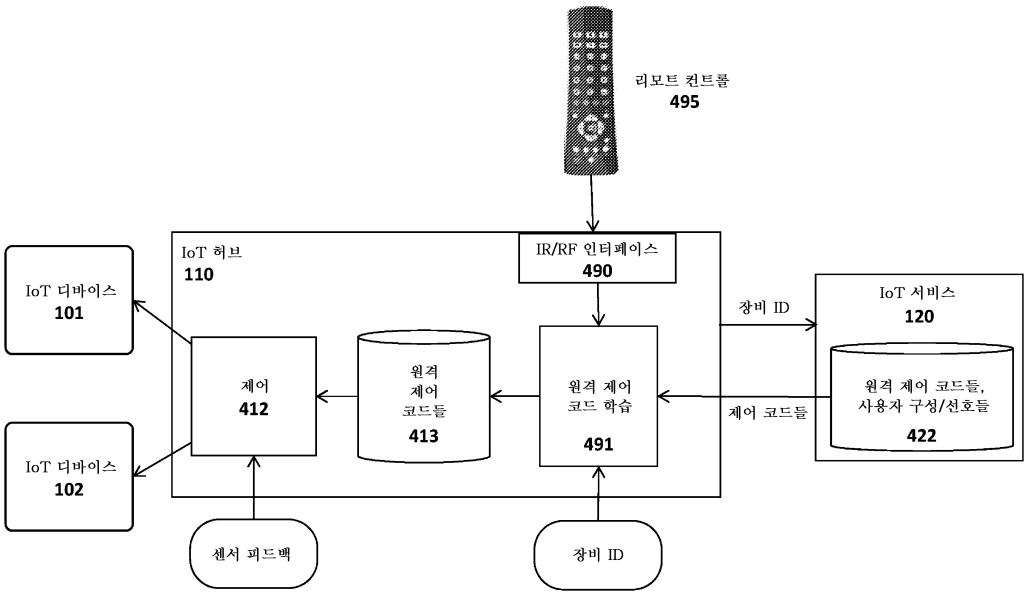
도면3


IoT 허브 110
프로그램 코드 및 데이터
305
메모리
317
디바이스
페어링
306
통신
스택
308
로컬
통신
채널
130
안테나
311
IoT
디바이스
101
로컬 통신
인터페이스
303
로직/uC
301
WAN
인터페이스
302
안테나
310
셀
서비스
115
웨이크업 신호
전력
390
디바이스 웨이크업
송신기
307

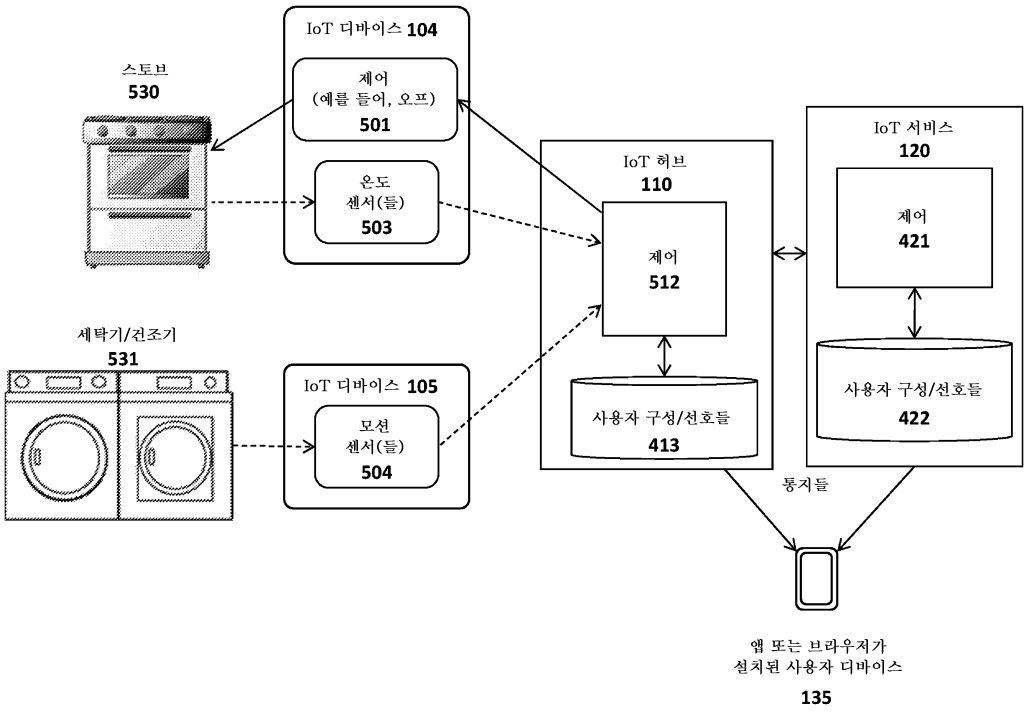
도면4a


IoT 디바이스 101
IR/RF 블라스터 401
센서(들) 404
에어컨/히터 430
온도, 습도 등
IoT 디바이스 102
IR/RF 블라스터 402
센서(들) 405
발광체들 431
밝기
IoT 디바이스 103
IR/RF 블라스터 403
센서(들) 406
시청각 장비 432
볼륨/밝기/온도
IoT 허브 110
제어 412
제어 코드들 및 사용자 구성/선호들 413
IoT 서비스 120
제어 421
제어 코드들, 사용자 구성/선호들 422
통지들 및/또는 제어
통지들 및/또는 제어
앱 또는 브라우저가 설치된 사용자 디바이스 135

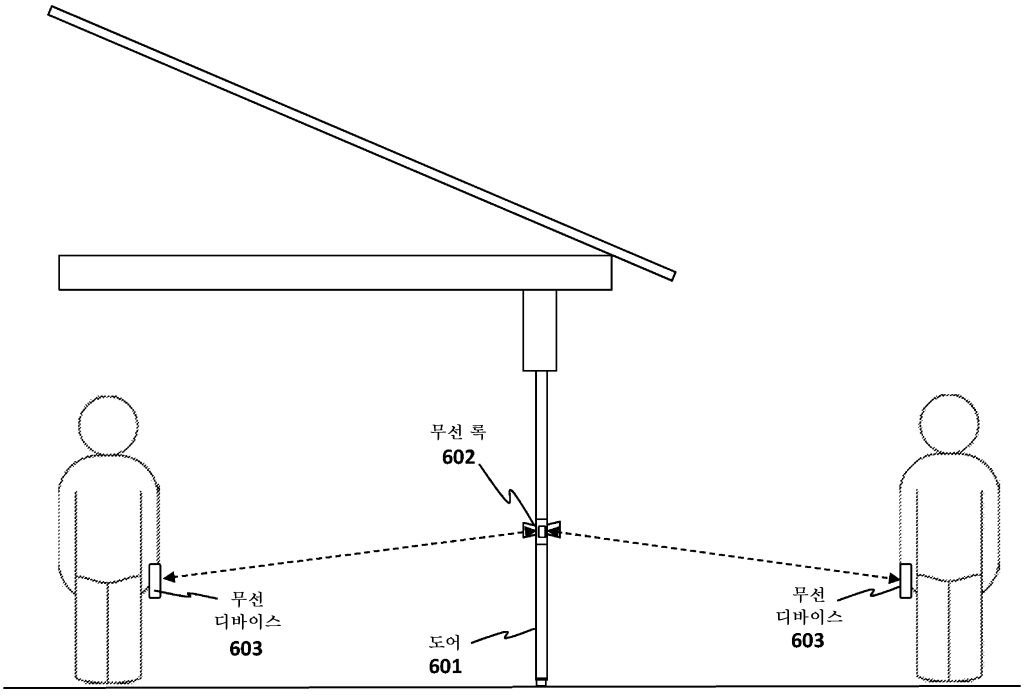
도면4b


리모트 컨트롤 495
IoT 허브 110
IR/RF 인터페이스 490
IoT 디바이스 101
IoT 디바이스 102
제어 412
원격 제어 코드들 413
원격 제어 코드 학습 491
장비 ID
제어 코드들
IoT 서비스 120
원격 제어 코드들, 사용자 구성/선호들 422
센서 피드백
장비 ID

도면5

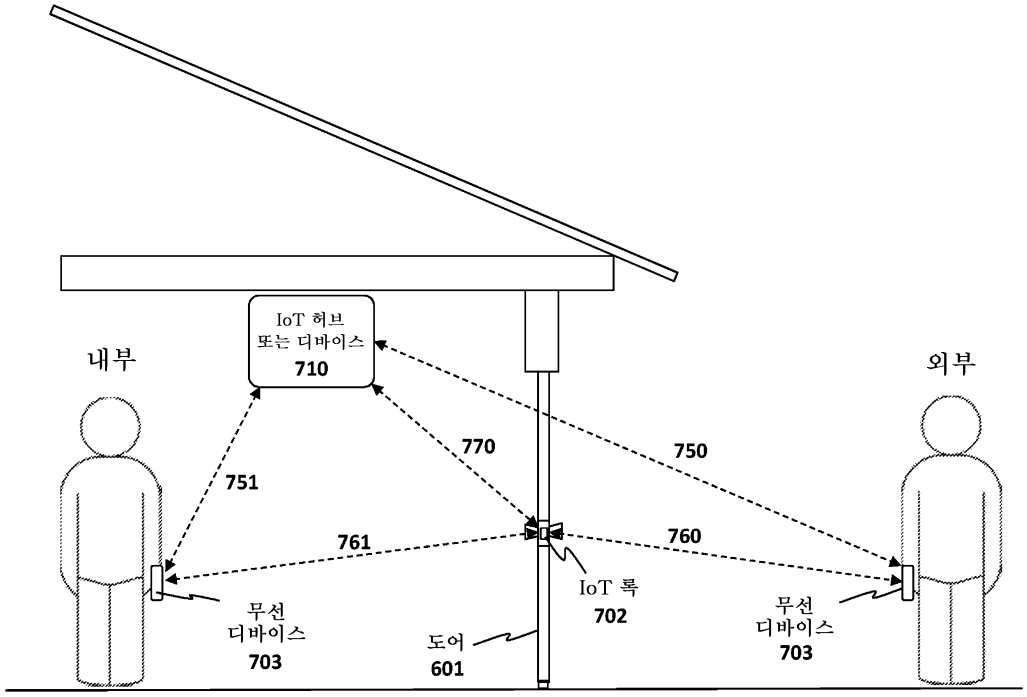

IoT 디바이스 104
스토브
530
제어
(예를 들어, 오프)
501
온도
센서(들)
503
IoT 허브
110
제어
512
사용자 구성/선호들
413
IoT 서비스
120
제어
421
사용자 구성/선호들
422
세탁기/건조기
531
IoT 디바이스 105
모션
센서(들)
504
통지들
앱 또는 브라우저가
설치된 사용자 디바이스
135

도면6

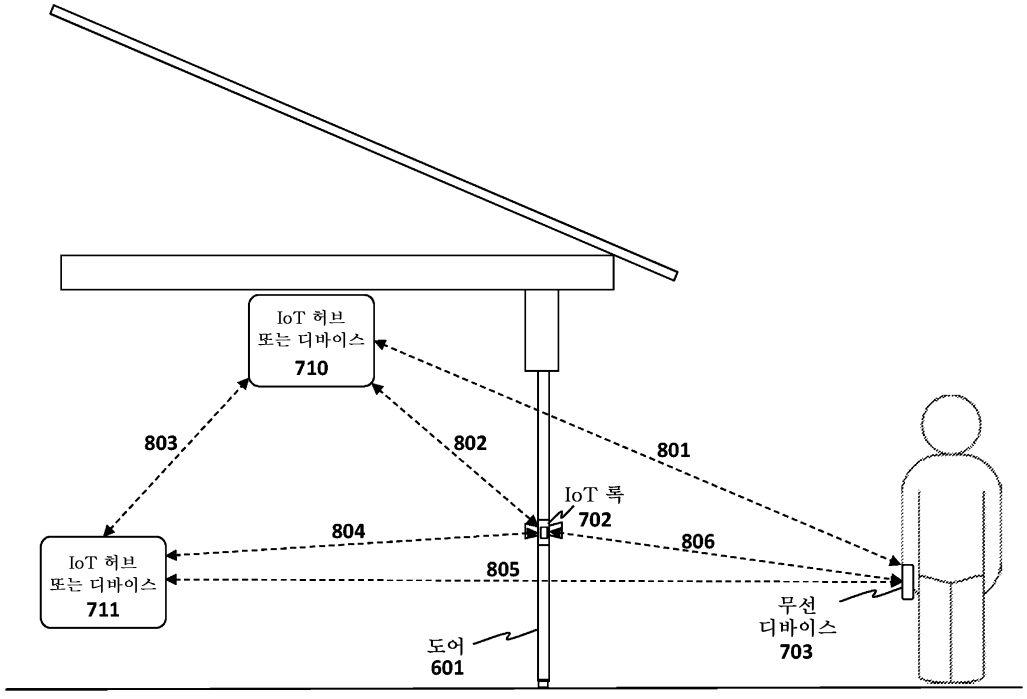

무선 폭
602
무선
디바이스
603
도어
601
무선
디바이스
603

(종래 기술)

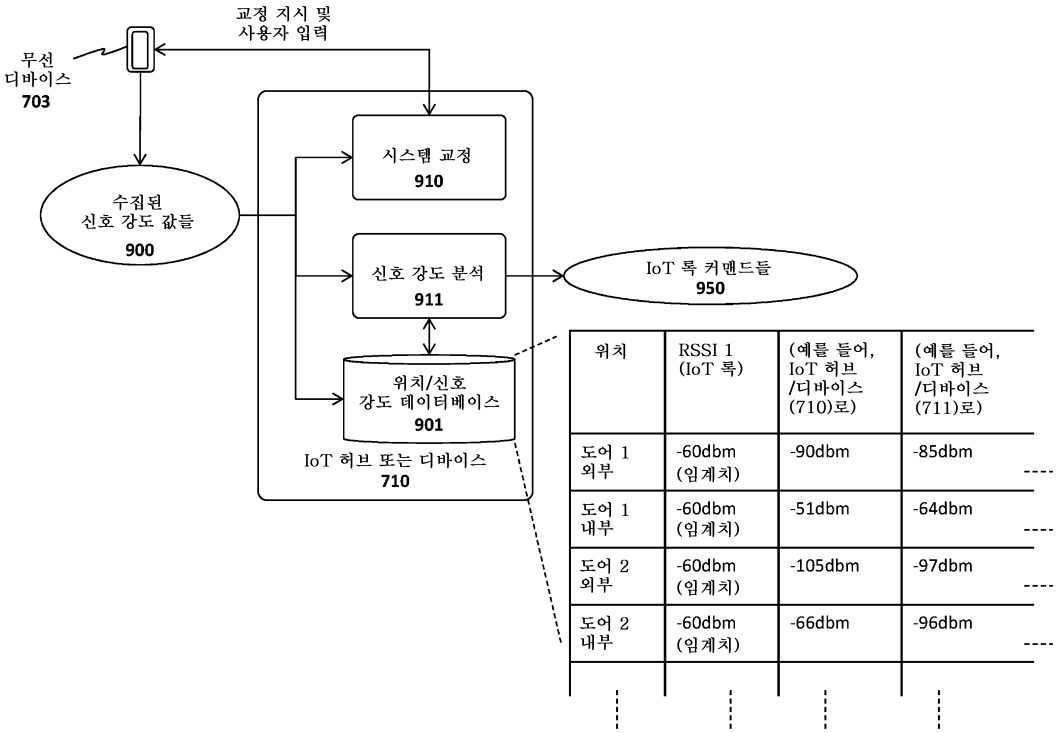
도면7


IoT 허브
또는 디바이스
710
내부
외부
770
750
751
761
760
IoT 록
702
무선
디바이스
703
도어
601
무선
디바이스
703

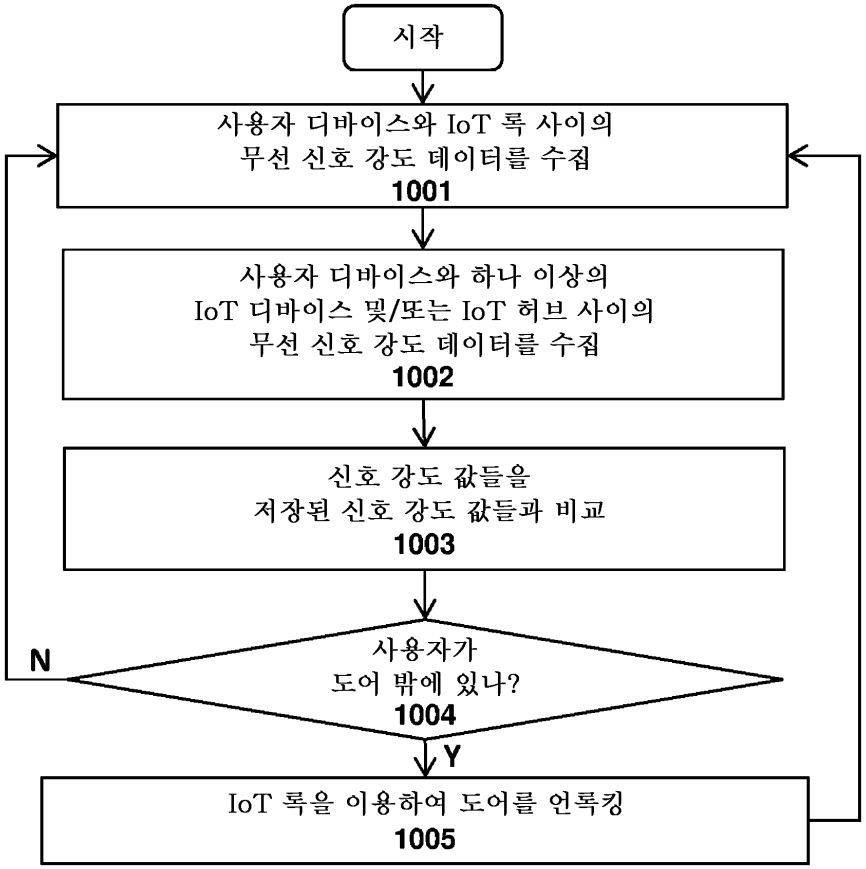
도면8


IoT 허브
또는 디바이스
710
803
802
801
IoT 록
702
804
806
805
IoT 허브
또는 디바이스
711
무선
디바이스
703
도어
601

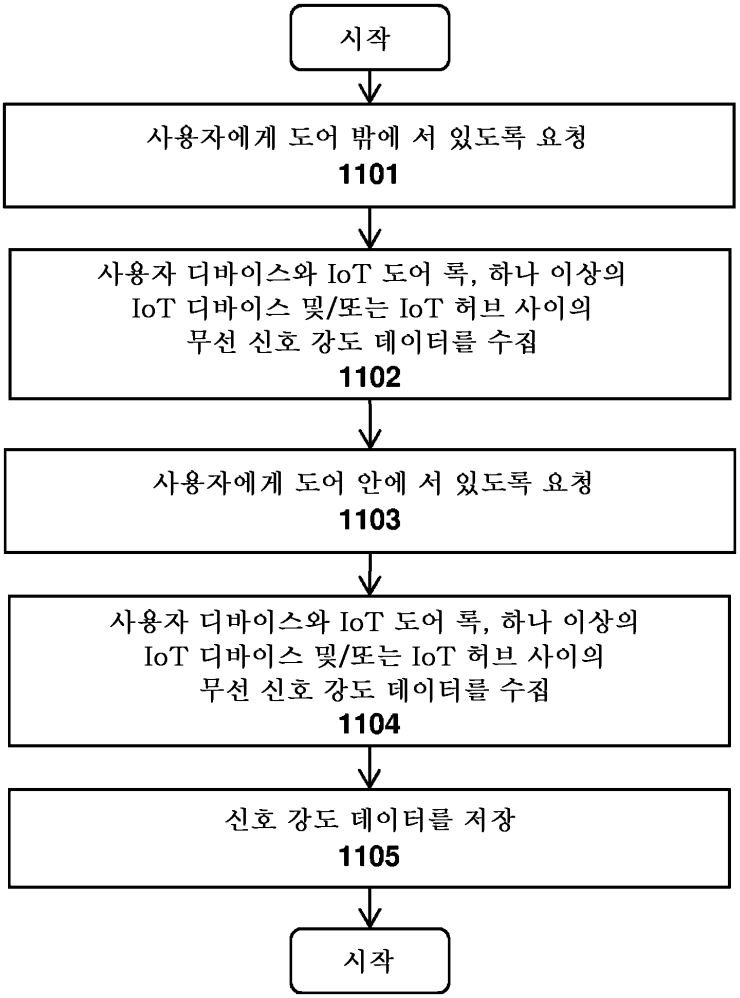
도면9


교정 지시 및
사용자 입력
무선
디바이스
703
수집된
신호 강도 값들
900
시스템 교정
910
신호 강도 분석
911
위치/신호
강도 데이터베이스
901
IoT 허브 또는 디바이스
710
IoT 록 커맨드들
950
위치
RSSI 1
(IoT 록)
(예를 들어,
IoT 허브
/디바이스
(710)로)
(예를 들어,
IoT 허브
/디바이스
(711)로)
도어 1
외부
-60dbm
(임계치)
-90dbm
-85dbm
도어 1
내부
-60dbm
(임계치)
-51dbm
-64dbm
도어 2
외부
-60dbm
(임계치)
-105dbm
-97dbm
도어 2
내부
-60dbm
(임계치)
-66dbm
-96dbm

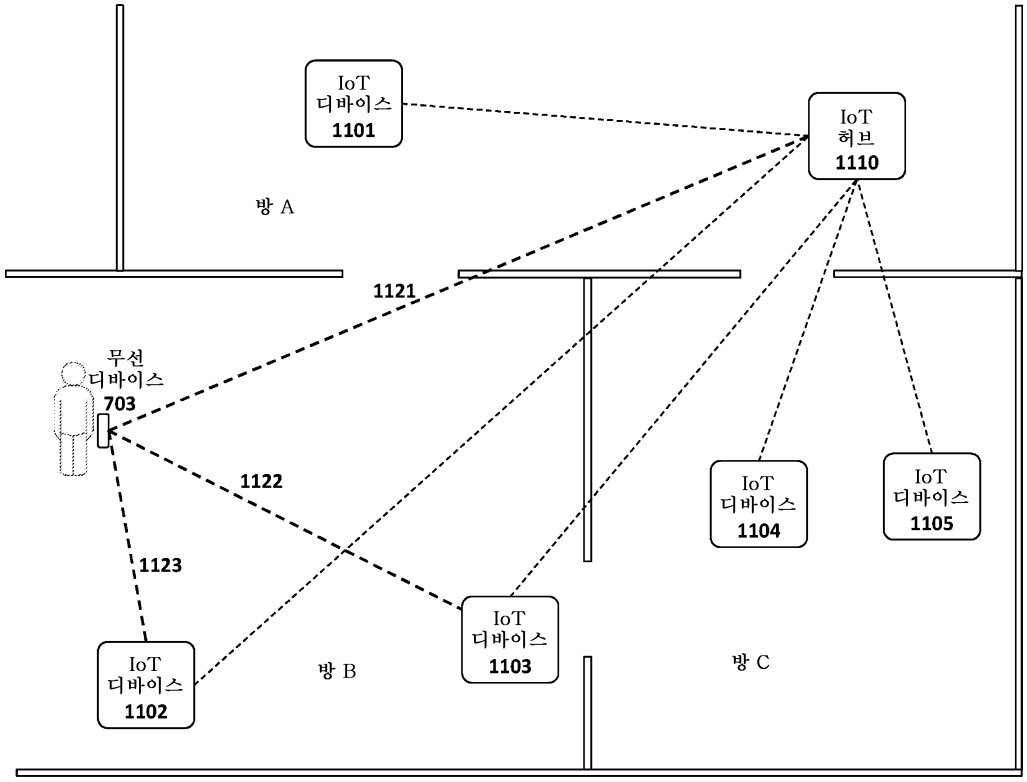
도면10


시작
사용자 디바이스와 IoT 록 사이의
무선 신호 강도 데이터를 수집
1001
사용자 디바이스와 하나 이상의
IoT 디바이스 및/또는 IoT 허브 사이의
무선 신호 강도 데이터를 수집
1002
신호 강도 값들을
저장된 신호 강도 값들과 비교
1003
사용자가
도어 밖에 있나?
1004
N
Y
IoT 록을 이용하여 도어를 언록킹
1005

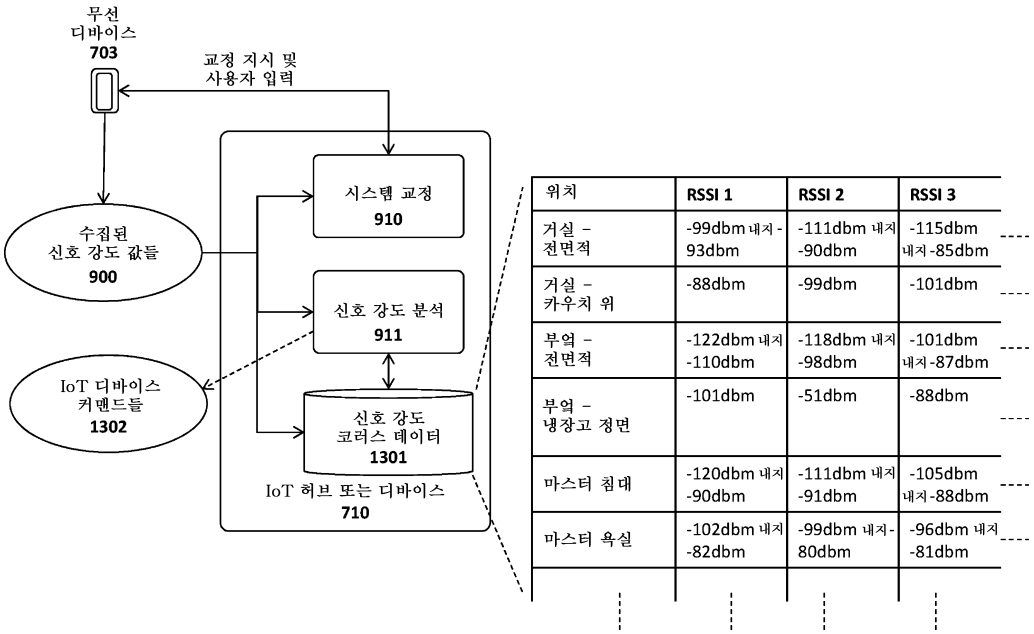
도면11


시작
사용자에게 도어 밖에 서 있도록 요청
1101
사용자 디바이스와 IoT 도어 록, 하나 이상의
IoT 디바이스 및/또는 IoT 허브 사이의
무선 신호 강도 데이터를 수집
1102
사용자에게 도어 안에 서 있도록 요청
1103
사용자 디바이스와 IoT 도어 록, 하나 이상의
IoT 디바이스 및/또는 IoT 허브 사이의
무선 신호 강도 데이터를 수집
1104
신호 강도 데이터를 저장
1105
시작

도면12

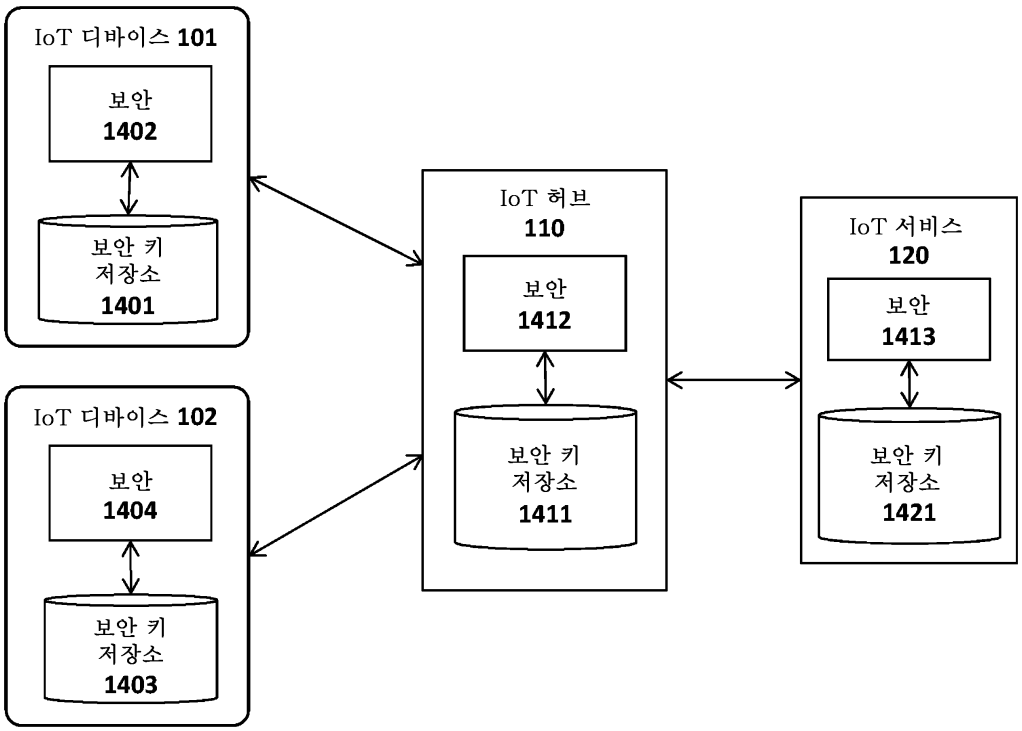


도면13

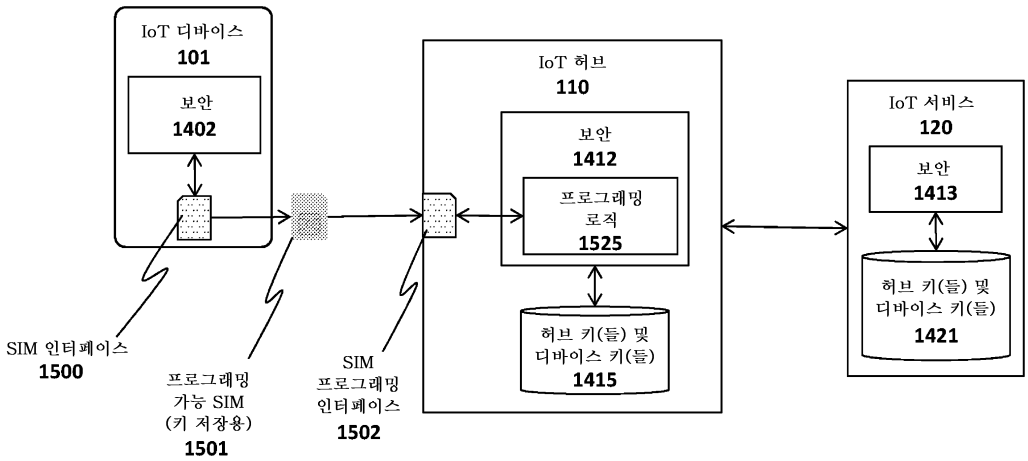


위치	RSSI 1	RSSI 2	RSSI 3
거실 – 전면적	-99dbm 내지 -93dbm	-111dbm 내지 -90dbm	-115dbm 내지 -85dbm
거실 – 카우치 위	-88dbm	-99dbm	-101dbm
부엌 – 전면적	-122dbm 내지 -110dbm	-118dbm 내지 -98dbm	-101dbm 내지 -87dbm
부엌 – 냉장고 정면	-101dbm	-51dbm	-88dbm
마스터 침대	-120dbm 내지 -90dbm	-111dbm 내지 -91dbm	-105dbm 내지 -88dbm
마스터 욕실	-102dbm 내지 -82dbm	-99dbm 내지 -80dbm	-96dbm 내지 -81dbm

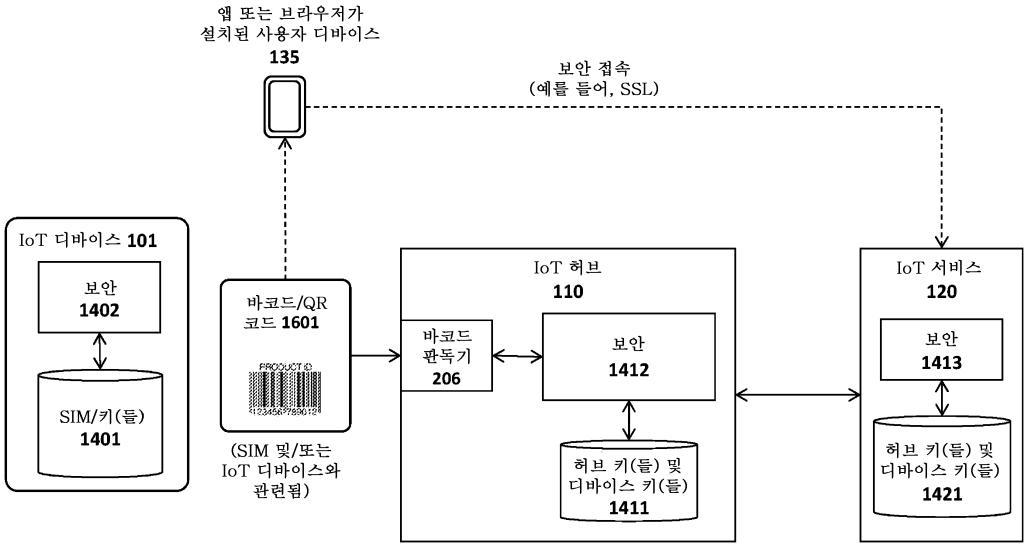
도면14


IoT 디바이스 101
보안
1402
보안 키
저장소
1401
IoT 디바이스 102
보안
1404
보안 키
저장소
1403
IoT 허브
110
보안
1412
보안 키
저장소
1411
IoT 서비스
120
보안
1413
보안 키
저장소
1421

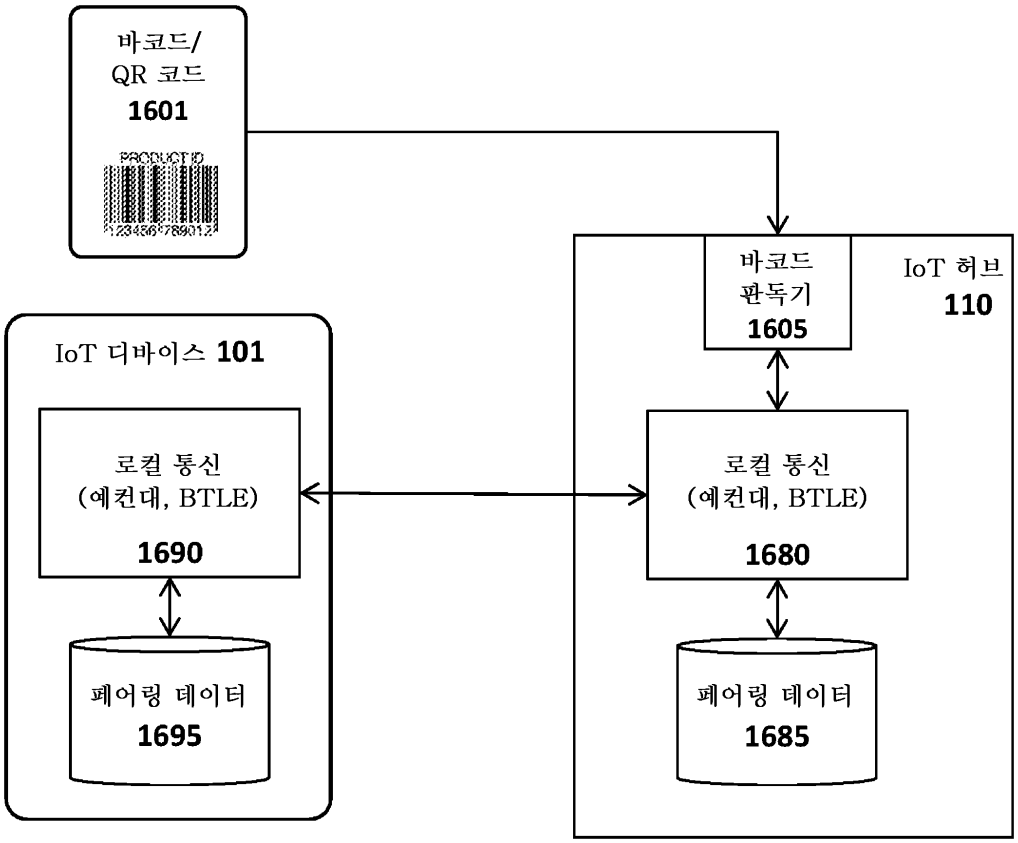
도면15


IoT 디바이스
101
보안
1402
SIM 인터페이스
1500
프로그래밍
가능 SIM
(키 저장용)
1501
SIM
프로그래밍
인터페이스
1502
IoT 허브
110
보안
1412
프로그래밍
로직
1525
허브 키(들) 및
디바이스 키(들)
1415
IoT 서비스
120
보안
1413
허브 키(들) 및
디바이스 키(들)
1421

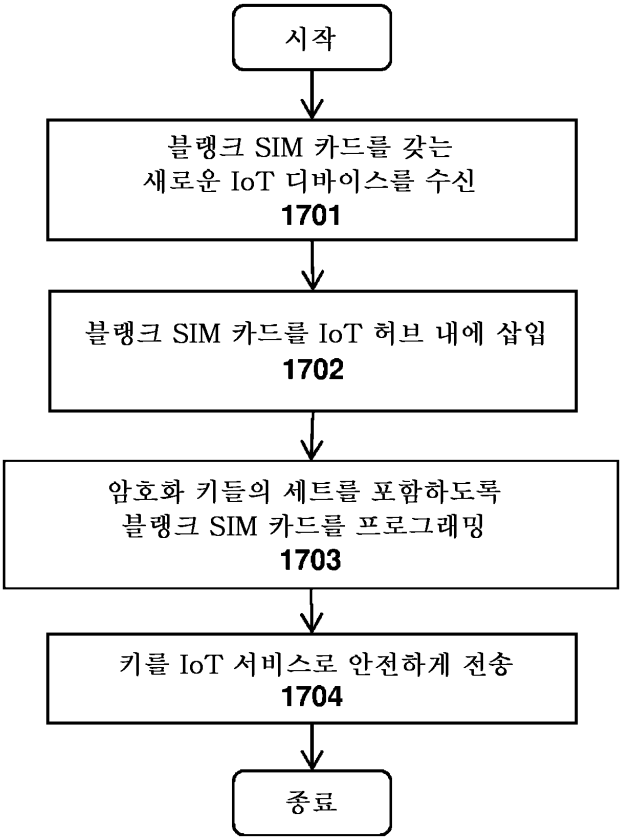
도면16a


앱 또는 브라우저가
설치된 사용자 디바이스
135
보안 접속
(예를 들어, SSL)
IoT 디바이스 101
보안
1402
SIM/키(들)
1401
바코드/QR
코드 1601
(SIM 및/또는
IoT 디바이스와
관련됨)
IoT 허브
110
바코드
판독기
206
보안
1412
허브 키(들) 및
디바이스 키(들)
1411
IoT 서비스
120
보안
1413
허브 키(들) 및
디바이스 키(들)
1421

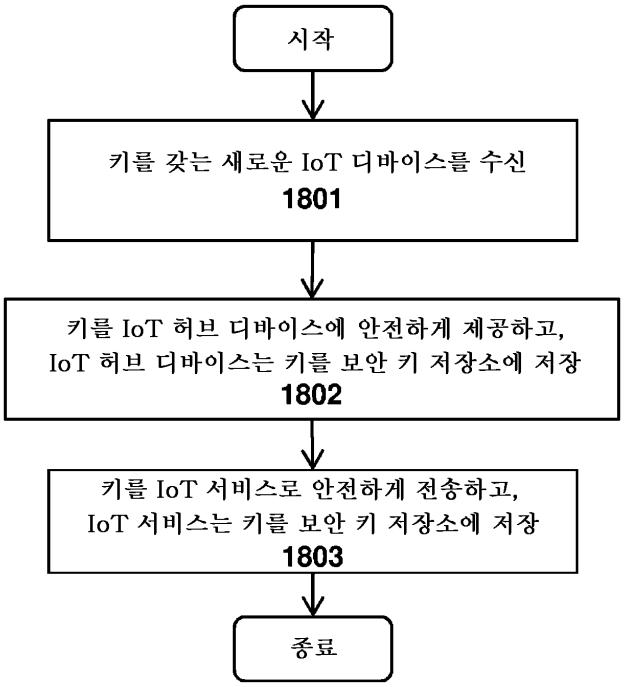
도면16b


바코드/
QR 코드
1601
IoT 디바이스 101
로컬 통신
(예컨대, BTLE)
1690
페어링 데이터
1695
바코드
판독기
1605
IoT 허브
110
로컬 통신
(예컨대, BTLE)
1680
페어링 데이터
1685

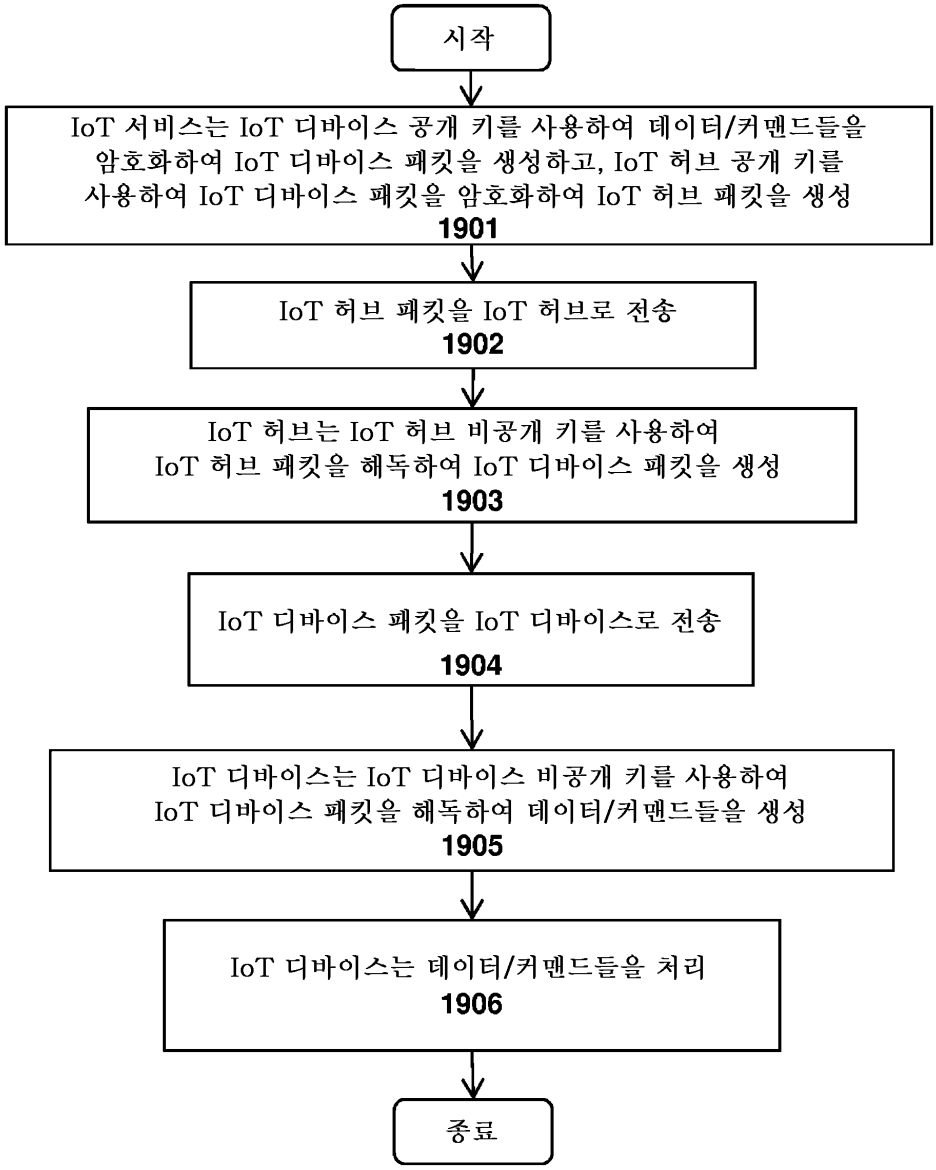
도면17


시작
블랭크 SIM 카드를 갖는
새로운 IoT 디바이스를 수신
1701
블랭크 SIM 카드를 IoT 허브 내에 삽입
1702
암호화 키들의 세트를 포함하도록
블랭크 SIM 카드를 프로그래밍
1703
키를 IoT 서비스로 안전하게 전송
1704
종료

도면18


시작
키를 갖는 새로운 IoT 디바이스를 수신
1801
키를 IoT 허브 디바이스에 안전하게 제공하고,
IoT 허브 디바이스는 키를 보안 키 저장소에 저장
1802
키를 IoT 서비스로 안전하게 전송하고,
IoT 서비스는 키를 보안 키 저장소에 저장
1803
종료

도면19


시작
IoT 서비스는 IoT 디바이스 공개 키를 사용하여 데이터/커맨드들을 암호화하여 IoT 디바이스 패킷을 생성하고, IoT 허브 공개 키를 사용하여 IoT 디바이스 패킷을 암호화하여 IoT 허브 패킷을 생성
1901
IoT 허브 패킷을 IoT 허브로 전송
1902
IoT 허브는 IoT 허브 비공개 키를 사용하여 IoT 허브 패킷을 해독하여 IoT 디바이스 패킷을 생성
1903
IoT 디바이스 패킷을 IoT 디바이스로 전송
1904
IoT 디바이스는 IoT 디바이스 비공개 키를 사용하여 IoT 디바이스 패킷을 해독하여 데이터/커맨드들을 생성
1905
IoT 디바이스는 데이터/커맨드들을 처리
1906
종료