(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0058556
(43) 공개일자 2022년05월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *H04L 101/622* (2022.01)
H04L 9/06 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 63/0421 (2013.01)
H04L 9/0643 (2013.01)
(21) 출원번호 10-2022-7009256
(22) 출원일자(국제) 2020년08월23일
심사청구일자 2022년04월07일
(85) 번역문제출일자 2022년03월21일
(86) 국제출원번호 PCT/US2020/047561
(87) 국제공개번호 WO 2021/041279
국제공개일자 2021년03월04일
(30) 우선권주장
62/891,116 2019년08월23일 미국(US)

(71) 출원인
누들 테크놀로지 인코포레이티드
미국 94115 캘리포니아 샌프란시스코 스위트 287 필모어 스트리트 2443
(72) 발명자
데이소니에르, 엘리엇 쿠엔틴 에릭
미국 캘리포니아 94115, 샌프란시스코, 스위트 287, 필모어 스트리트 2443
루와조, 루시앙
미국 캘리포니아 94115, 샌프란시스코, 스위트 287, 필모어 스트리트 2443
(뒷면에 계속)
(74) 대리인
김해중

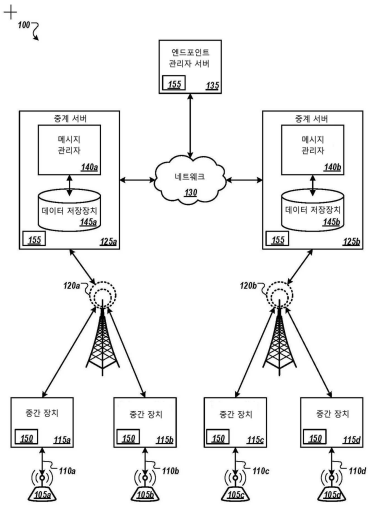
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **장치 ＩＤ의 익명화 및 랜덤화**

(57) 요 약

방법은 엔드포인트 장치에 대한 고유 식별자를 생성하는 단계를 포함할 수 있다. 고유 식별자는 엔드포인트 장치에 특별하고 적어도 하나의 반-신뢰 당사자와 함께 엔드포인트 장치를 식별하도록 구성될 수 있다. 고유 식별자는 엔드포인트 장치의 MAC 주소와 네트워크 운영자에게 알려진 운영자 비밀 둘 다를 기반으로 하는 해시 값일 수 있다. 방법은 고유 식별자를 다른 장치와 공유하는 단계를 포함할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/085 (2013.01)
H04L 2101/622 (2022.05)
H04L 2209/80 (2013.01)
(72) 발명자
베놀리엘, 미카 안테노르
미국 캘리포니아 94115, 샌프란시스코, 스위트 287, 필모어 스트리트 2443
킨스먼, 가렛 에드워드
미국 캘리포니아 94115, 샌프란시스코, 스위트 287, 필모어 스트리트 2443

명 세 서

청구범위

청구항 1

방법으로서,

엔드포인트 장치에 대한 고유 식별자를 생성하는 단계로서, 고유 식별자는 엔드포인트 장치에 특별하고 적어도 하나의 반-신뢰 당사자와 함께 엔드포인트 장치를 식별하도록 구성되는, 단계; 및

고유 식별자를 다른 장치와 공유하는 단계를 포함하는,

방법.

청구항 2

제 1 항에 있어서,

고유 식별자는 엔드포인트 장치의 MAC 주소와 네트워크 운영자에게 알려진 운영자 비밀 둘 다를 기반으로 하는 해시 값인,

방법.

청구항 3

제 2 항에 있어서,

MAC 주소는 엔드포인트 장치의 하드웨어에 의해 정의되는,

방법.

청구항 4

제 1 항에 있어서,

고유 식별자는 무선으로 공유되는,

방법.

청구항 5

제 1 항에 있어서,

고유 식별자는 네트워크 운영자에 의해 운영되는 네트워크를 통해 공유되는,

방법.

청구항 6

제 1 항에 있어서,

고유 식별자는 알고리즘: id = hash(operatorSecret, deviceMacAddress)에 따라 생성되며, 여기서 id는 고유 식별자, hash는 해싱 알고리즘, operatorSecret은 네트워크 운영자가 알고 있는 비밀, deviceMacAddress는 엔드포인트 장치의 하드웨어에 의해 정의되는 MAC 주소인,

방법.

청구항 7

제 6 항에 있어서,

해싱 알고리즘은 SHA(Secure Hash Algorithm: 보안 해시 알고리즘)인,

방법.

청구항 8

제 1 항에 있어서,

고유 식별자는 제 3자에 의해 이해될 수 없으며 네트워크 운영자에 의해 엔드포인트 장치에 연결될 수 있는,

방법.

청구항 9

제 1 항에 있어서,

고유 식별자는 엔드포인트 장치에서 생성되며, 네트워크 운영자에서 고유 식별자를 재계산하는 단계를 더 포함하는,

방법.

청구항 10

제 1 항에 있어서,

고유 식별자를 다른 장치와 공유하는 단계는 고유 식별자를 네트워크 운영자에 의해 소유된 다른 장치에 전송하는 단계를 포함하는,

방법.

청구항 11

제 2 항에 있어서,

운영자 비밀을 순환하는 단계를 더 포함하는,

방법.

청구항 12

제 11 항에 있어서,

운영자 비밀은 네트워크 운영자에게 알려진 순환 알고리즘을 기반으로 순환되는,

방법.

청구항 13

제 12 항에 있어서,

순환 알고리즘은 네트워크 운영자에게 알려진 미리 정의된 매개변수를 포함하는,

방법.

청구항 14

방법으로서,

네트워크 운영자에게 알려진 운영자 비밀을 순환하는 단계;

엔드포인트 장치에 대한 고유 식별자를 생성하는 단계로서, 고유 식별자는 엔드포인트 장치에 특별하고 엔드포인트 장치, 운영자 비밀에 기반한 고유 식별자 및 엔드포인트 장치의 식별자를 식별하도록 구성되는, 단계; 및

고유 식별자를 다른 장치와 공유하는 단계를 포함하는,

방법.

청구항 15

제 14 항에 있어서,

엔드포인트 장치의 식별자는 MAC 주소인,

방법.

청구항 16

제 15 항에 있어서,

MAC 주소는 엔드포인트 장치의 하드웨어에 의해 정의되는,

방법.

청구항 17

제 14 항에 있어서,

운영자 비밀은 네트워크 운영자에게 알려져 있는,

방법.

청구항 18

제 14 항에 있어서,

고유 식별자는 네트워크 운영자에 의해 운영되는 네트워크를 통해 무선으로 공유되는,

방법.

청구항 19

제 14 항에 있어서,

고유 식별자는 알고리즘: id = hash(operatorSecret, deviceMacAddress)에 따라 생성되며, 여기서 id는 고유 식별자, hash는 해싱 알고리즘, operatorSecret은 네트워크 운영자가 알고 있는 비밀, deviceMacAddress는 엔드포인트 장치의 하드웨어에 의해 정의되는 MAC 주소인,

방법.

청구항 20

제 19 항에 있어서,

해싱 알고리즘은 SHA(Secure Hash Algorithm: 보안 해시 알고리즘)인,

방법.

발명의 설명

기 술 분 야

[0001] 본 개시는 일반적으로 네트워크 "스마트" 장치들 사이의 통신을 위한 보안 및 프라이버시에 관한 것이다. 특히, 본 개시는 네트워크 장치에 대한 보안 및 개인 식별을 설명한다.

배 경 기 술

[0002] 사물 인터넷(IoT)은 조명 및 도어와 같은 일반 장치를 컴퓨터 네트워크에 연결하여 "지능형"으로 만드는 개념이다. 임베디드 시스템(embedded system)이나 컴퓨터는 각각의 장치를 네트워크와 인터넷에 함께 연결한다. 연결은 각각의 장치가 데이터를 수집하고 교환하게 하며, 연결이 원격으로 제어되거나 연결을 업데이트된 상태로 유지하거나 원격으로 또는 규칙이나 일련의 행위를 설정하여 제어되게 한다.

[0003] IoT 장치의 사용은 인간 생활의 많은 측면으로 확대되고 있으며 전문가들은 IoT가 2020년까지 거의 500 억 개의 장치를 갖게 될 것으로 추정한다. 점점 더 많은 IoT 장치가 병원에서의 건강관리, 의료 기기 및 제약 제조에

사용된다. 도시에서 IoT 장치는 오염을 추적하고 모니터링하는데 도움이 된다. IoT 장치는 자산 추적 및 관리를 위해서 정부, 군대, 회사 및 개인에 의해 사용될 수도 있다. 이들 용례는 상이한 목적에 사용되지만, 많은 용례에는 강력한 보안 및 프라이버시 제어를 요구한다.

[0004] 보안 및 프라이버시는 오랫동안 인터넷을 괴롭혀 왔다. 모바일 장치의 사용 증가로 인해 이들 보안 및 프라이버시 문제가 증가했으며 IoT 장치의 출현으로 보안 및 프라이버시 문제가 훨씬 높아졌다. 따라서, 본 개시는 네트워크 장치에 대한 보안 및 프라이버시에 관한 것이다.

[0005] 청구된 요지는 임의의 단점을 해결하거나 위에서 설명된 것과 같은 환경에서만 작동하는 실시예로 제한되지 않는다. 이러한 배경은 단지, 본 개시가 활용될 수 있는 예를 예시하기 위해 제공된다.

발명의 내용

[0006] 본 개시는 일반적으로, 네트워크 "스마트" 장치들 사이의 통신을 위한 보안 및 프라이버시에 관한 것이다. 특히, 본 개시는 네트워크 장치에 대한 보안 및 개인 식별을 설명한다.

[0007] 하나의 비-제한적인 예에서, 상기 방법은 엔드포인트 장치(endpoint device)에 대한 고유 식별자(unique identifier)를 생성하는 단계를 포함할 수 있다. 고유 식별자는 엔드포인트 장치에 특별할 수 있으며 적어도 하나의 반-신뢰할 수 있는 당사자와 함께 엔드포인트 장치를 식별하도록 구성될 수 있다. 고유 식별자는 엔드포인트 장치의 MAC 주소와 네트워크 운영자에게 알려진 운영자 비밀 모두를 기반으로 하는 해시 값(hashed value)일 수 있다. 상기 방법은 고유 식별자를 다른 장치와 공유하는 것을 포함할 수 있다.

[0008] 몇몇 양태들에서, MAC 주소는 엔드포인트 장치의 하드웨어에 의해 정의될 수 있다. 고유 식별자는 무선으로 공유될 수 있다. 고유 식별자는 네트워크 운영자가 운영하는 네트워크를 통해 공유될 수 있다.

[0009] 고유 식별자는 알고리즘 id = hash(operatorSecret, deviceMacAddress)에 따라 생성될 수 있으며. 여기서 id는 고유 식별자, hash는 해싱 알고리즘(hashing algorithm), operatorSecret은 네트워크 운영자에게 알려진 비밀, deviceMacAddress는 엔드포인트 장치의 하드웨어에 의해 정의된 MAC 주소이다. 해싱 알고리즘은 SHA(Secure Hash Algorithm: 보안 해시 알고리즘)일 수 있다.

[0010] 고유 식별자는 제 3자가 이해하지 못할 수 있으며 네트워크 운영자가 엔드포인트 장치에 연결될 수 있다. 고유 식별자는 엔드포인트 장치에서 생성될 수 있다. 상기 방법은 네트워크 운영자에서 고유 식별자를 재계산하는 것을 포함할 수 있다. 고유 식별자를 다른 장치와 공유하는 것은 네트워크 운영자가 소유한 다른 장치에 고유 식별자를 전송하는 것을 포함할 수 있다.

[0011] 상기 방법은 운영자 비밀(operator secret)을 교체하는 것을 포함할 수 있다. 운영자 비밀은 네트워크 운영자에게 알려진 순환 알고리즘을 기반으로 순환될 수 있다. 순환 알고리즘은 네트워크 운영자에게 알려진 미리 정의된 매개변수를 포함할 수 있다.

[0012] 다른 예에서, 상기 방법은 네트워크 운영자에게 알려진 운영자 비밀을 교체하고, 엔드포인트 장치에 대한 고유 식별자를 생성하고, 고유 식별자를 다른 장치와 공유하는 것을 포함할 수 있다. 고유 식별자는 엔드포인트 장치에 고유할 수 있고 엔드포인트 장치를 식별하도록 구성될 수 있다. 고유 식별자는 운영자 비밀 및 엔드포인트 장치의 식별자를 기반으로 할 수 있다.

[0013] 엔드포인트 장치의 식별자는 MAC 주소일 수 있다. MAC 주소는 엔드포인트 장치의 하드웨어에 의해 정의될 수 있다. 운영자 비밀은 네트워크 운영자에게 알려질 수 있다. 고유 식별자는 네트워크 사업자가 운영하는 네트워크를 통해 무선으로 공유될 수 있다.

[0014] 고유 식별자는 id = hash(operatorSecret, deviceMacAddress) 알고리즘에 따라 생성될 수 있으며, 여기서 id는 고유 식별자, hash는 해싱 알고리즘, operatorSecret은 네트워크 운영자가 알고 있는 비밀, deviceMacAddress는 엔드포인트 장치의 하드웨어에서 정의한 MAC 주소이다. 해싱 알고리즘은 SHA(Secure Hash Algorithm)일 수 있다.

[0015] 이러한 요약은 아래의 상세한 설명에서 추가로 설명되는 단순화된 형태의 개념 선택을 소개한다. 이러한 요약은 청구된 요지의 주요 특징 또는 필수 특성을 식별하기 위한 것이 아니며 청구된 요지의 범주를 결정하는데 도움을 주기 위한 것도 아니다.

도면의 간단한 설명

[0016] 도 1은 네트워크 구성의 예를 예시한다.

도 2 및 도 3은 네트워크 장치를 안전하고 개인적으로 식별하는 예시적인 방법의 흐름도를 예시한다.

도 4는 본 명세서에서 논의된 방법 중 임의의 하나 이상을 기계가 수행하게 하기 위한 명령어 세트가 실행될 수 있는 컴퓨팅 장치의 예시적인 형태의 기계의 도식적 표현을 예시한다.

발명을 실시하기 위한 구체적인 내용

[0017] 도면이 참조될 것이고 특정 언어는 본 개시의 다양한 양태를 설명하는데 사용될 것이다. 이러한 방식으로 도면 및 설명을 사용하는 것은 그 범위를 제한하는 것으로 해석되어서는 안 된다. 추가적인 양태는 청구범위를 포함한 본 개시에 비추어 자명해지거나, 실행에 의해 학습될 수 있다.

[0018] IoT(사물 인터넷) 장치의 수가 증가함에 따라서, 이들 장치와 관련된 보안 및 프라이버시 문제도 증가한다. 특히, IoT 장치가 예를 들어, 상업 및 산업 용례에서 점점 더 확장됨에 따라서 더욱 그렇다.

[0019] IoT 장치는 장치 및 그 목적에 관한 식별 정보를 포함하는 신호를 주기적으로 방출할 수 있다. 어떤 상황에서는 이들 비컨(beacon)을 기반으로 개인과 그들의 장치를 연관시키는 것이 가능할 수 있다. 이는 전화 및 태블릿뿐만 아니라, 자산 추적기, 건강 모니터링 장치, 자동차 키, 무선 시계 등과 같은 보조 장치도 포함한다.

[0020] 그러나 IoT 장치에서 식별 정보를 수집함으로써 범죄자는 어떤 장치를 가까이에서 많은 시간을 보내는지 추적하는 것만으로 개인의 물리적 위치뿐만 아니라, 어떤 개인이 어떤 장치를 소유하고 있는지 추론하거나 추정할 수 있다. 범죄자가 누가 어떤 장치를 소유하고 있는지 확인하면 해당 정보를 사용하여 장치를 흉내내고 장치와 장치 소유자를 추적할 수 있다. 몇몇 IoT 장치는 GPS(Global Positioning System: 위성 위치확인 시스템)를 사용하여 키 세트와 같이 사용자가 추적하려는 자산을 찾을 수 있다. 자산은 장치 제조업체에 송신하거나 중계할 수 있는 비컨을 전송할 수 있다. 불행히도, 범죄자는 이러한 정보를 사용하여 장치 및 관련 사용자 또는 자산의 위치를 식별할 수 있다.

[0021] IoT 장치와 이들 장치가 방출하는 신호는 프라이버시 문제로 이어질 수도 있다. 예를 들어, IoT 장치는 고유하고 변하지 않는 장치 ID를 포함하는 신호를 방출할 수 있다. 이는 장치 추적이 가능하지만 주변 장치가 고유 ID를 볼 수 있고 이러한 정보를 사용하여 허가 없이 장치를 식별하고 추적할 수 있기 때문에 취약점도 노출된다.

[0022] IoT 장치 네트워크의 운영자는 IoT 장치를 1) 고유하게 식별될 필요가 없는 장치, 및 2) 식별될 필요가 있는 장치의 두 가지 범주로 분류할 수 있다. 식별해야 하는 장치의 경우, 그러한 장치를 식별하는 일반적인 방법은 장치의 하드웨어(가장 일반적으로 블루투스 칩셋(Bluetooth chipset)에서)에 의해 정의될 수 있는 MAC 주소를 사용하는 것이다. 그러나 식별을 위해 MAC 주소를 사용하는 것은 몇 가지 중요한 단점과 관련될 수 있다.

[0023] 첫째, MAC 주소로 장치를 식별하는 것은 장치가 추적되는 것을 피하기 위해서 이러한 동일한 주소를 랜덤으로 지정할 수 없다는 것을 의미하며, 이는 보안 및 프라이버시 문제를 초래할 수 있다. 예를 들어, 장치의 소유자는 IoT 장치의 위치를 (예를 들어, GPS 또는 네트워크 연결 위치를 통해)확인하는 것만으로 간단히 추적할 수 있다. 이는 소유자가 항상 착용하도록 되어 있고 소유자가 항상 추적되도록 허용할 수 있는 시계와 같은 웨어러블 장치에 대해 중요한 문제일 수 있다. 둘째, 장치의 MAC 주소는 올바른 하드웨어 및 소프트웨어를 사용하는 다른 장치에 의해 쉽게 스푸핑될(spoofed) 수 있다. 현재, 그러한 하드웨어 및 소프트웨어는 예를 들어, 인터넷에서 쉽게 이용 가능할 수 있다.

[0024] 따라서 MAC 주소는 IoT 장치를 식별하는 좋은 방법이 아니다. MAC 주소는 스푸핑하기 쉽기 때문에 안전하지 않으며 모든 장치를 쉽게 추적할 수 있게 하기 때문에 프라이버시 문제가 있다. 따라서, 본 개시는 안전하고 사적인 방식으로 IoT 장치를 식별하기 위한 시스템 및 방법을 설명한다. 특히, 본 개시는 스푸핑하기 어렵고 제3자에게 랜덤으로 나타나는 장치 식별자를 포함하지만, 네트워크 운영자만을 위한 네트워크의 IoT 장치에 링크할 수 있다. 또한, 개시된 식별자는 구현하기 쉽고 계산이 빠르기 때문에(너무 많은 작업이 필요하지 않음) 작은 배터리와 상대적으로 낮은 성능 및 저전력 하드웨어에 의존하는 IoT 장치에서 구현하는데 적합하다.

[0025] 도 1은 본 개시가 구현될 수 있는 예시적인 네트워크 구성(100)을 예시한다. 네트워크 구성(100)은 하나 이상의 엔드포인트 장치(105), 하나 이상의 중간 장치(115), 하나 이상의 중계 서버(125), 및 하나 이상의 엔드포인트 관리자 서버(135)를 포함할 수 있다. 몇몇 실시예에서, 네트워크 구성(100)은 네트워크 클라이언트로서 기능을 할 수 있는 크라우드-소싱 중간 장치(crowd-sourced intermediate device)(115) 및 하나 이상의 중계 서

버(125)를 통해 하나 이상의 엔드포인트 장치(105)와 다양한 엔드포인트 관리자 서버(135) 사이에서 데이터를 이동할 수 있다.

[0026] 엔드포인트 장치(105)는 하나 이상의 IoT 장치를 포함할 수 있다. 엔드포인트 장치(105)는 전원, 데이터 수집 장치(예를 들어, 센서), 네트워크 장치를 포함할 수 있다. 전원 공급 장치는 배터리 또는 전력 망에 대한 연결을 포함할 수 있다. 추가로 또는 대안적으로, 전원 공급 장치는 태양 전지판, 태양 전지, 태양광 발전, 전자기 등과 같은 에너지 수확 장치를 포함할 수 있다. 적어도 몇몇 실시예에서, 엔드포인트 장치(105)는 전원을 포함하지 않을 수 있는 대신에 주변 후방 산란 기술을 사용할 수 있다. 엔드포인트 장치(105)는 또한 하나 이상의 센서를 포함할 수 있다. 하나 이상의 센서는 임의의 유형의 상태를 검출하고 검출된 상태에 기반하여 전자 데이터를 생성하도록 구성될 수 있다. 예를 들어, 엔드포인트 장치(105)는 심박수 모니터에 의해 수집된 심박수 조건을 사용하여 심박수 데이터를 생성하도록 구성된 심박수 모니터를 구비한 스마트 시계를 포함할 수 있다. 몇몇 실시예에서, 엔드포인트 장치(105)는 인터넷을 통해 통신할 수 있는 능력이 없고 근처의 중간 장치(115)와 같은 근처의 장치와 통신할 수 있는 하드웨어 및/또는 소프트웨어만을 포함한다. 다른 경우에, 엔드포인트 장치(105)는 인터넷을 통해 통신하는 하드웨어 및/또는 소프트웨어를 포함할 수 있다.

[0027] 엔드포인트 장치(105)의 네트워크 장치는 네트워크를 통해 다른 장치와 통신할 수 있는 임의의 하드웨어, 소프트웨어, 또는 이들의 조합을 포함할 수 있다. 적어도 하나의 실시예에서, 네트워크 장치는 블루투스(Bluetooth®) 또는 임의의 다른 단거리 네트워크와 같은 단거리 네트워크를 통해 통신하도록 구성된 임의의 네트워크 컨트롤러를 포함할 수 있다. 적어도 하나의 실시예에서, 네트워크 장치는 저전력 네트워크를 통해 통신하도록 구성된 임의의 네트워크 컨트롤러를 포함할 수 있다. 예시적인 엔드포인트 장치(105)는 산업용 장치, 주거용 가전제품, 상업용 장비, 재고 추적기, 스마트 시계, 웨어러블, 심박수 모니터, 물류 추적기, 환경 센서, 금전 등록기, 신용 카드 판독기, 포인트-오브-세일(POS: point-of-sale), 자전거, 전기 스쿠터, 전기 스케이트 보드, 자동차, 전기 자동차, 위성 또는 임의의 장치(모바일 및 무선 라디오 인터페이스를 포함하는 모바일 제외)를 포함하지만, 이에 한정되지 않는다. 네트워크 구성(100)은 임의의 수의 엔드포인트 장치(105)를 포함할 수 있고 네트워크 구성(100)의 엔드포인트 장치(105)는 임의의 유형의 네트워크 가능 장치를 포함하는 임의의 유형의 엔드포인트 장치(105)일 수 있다. 엔드포인트 장치(105)는 POS 또는 오염 센서와 같은 네트워크 구성(100)에서 고정되거나 상대적으로 고정될 수 있다. 추가적으로 또는 대안적으로, 엔드포인트 장치(105)는 스마트 워치, 또는 임의의 자동차 또는 차량과 같은 모바일일 수 있다.

[0028] 하나 이상의 엔드포인트 장치(105)는 적어도 하나의 무선 네트워크(110)를 통해 다른 장치와 통신하도록 구성될 수 있다. 예를 들어, 제 1 엔드포인트 장치(105a)는 무선 네트워크(110a)를 통해 제 1 중간 장치(115a)와 전자 통신할 수 있다. 하나 이상의 중간 장치(115)는 무선 네트워크(110)를 통해 엔드포인트 장치(105)와 통신할 수 있고 제 2 네트워크(120)를 통해 중계 서버(125)와 통신할 수 있는 임의의 유형의 장치를 포함할 수 있다. 적어도 하나의 실시예에서, 중간 장치(115)는 2 개의 네트워크 컨트롤러, 즉 무선 네트워크(110)를 통해 통신하기 위한 제 1 네트워크 컨트롤러 및 제 2 네트워크(120)를 통해 통신하기 위한 제 2 네트워크 컨트롤러를 포함할 수 있다. 예시적인 중간 장치(115)는 모바일 장치, 개인용 컴퓨터(PC), 랩탑, 스마트폰, 넷북, e-리더, 개인 휴대 정보 단말기(PDA), 휴대폰, 모바일폰, 태블릿, 차량, 드론, 자동차, 트럭, 웨어러블 장치, 라우터, 텔레비전 또는 셋톱 박스 등을 포함한다.

[0029] 예시된 바와 같이, 제 1 엔드포인트 장치(105a)는 무선 네트워크(110a)(예를 들어, 근거리 네트워크)를 통해 제 1 중간 장치(115a)와 전자 통신할 수 있다. 또한, 제 2 엔드포인트 장치(105b)는 다른 무선 네트워크(110b)(예를 들어, 저전력 네트워크)를 통해 제 2 중간 장치(115b)와 전자 통신할 수 있다. 제 3 엔드포인트 장치(105c)는 다른 무선 네트워크(110c)를 통해 제 3 중간 장치(115c)와 전자 통신할 수 있다. 제 4 엔드포인트 장치(105d)는 다른 무선 네트워크(110d)를 통해 제 4 중간 장치(115d)와 전자 통신할 수 있다.

[0030] 몇몇 실시예에서, 무선 네트워크(110)는 비교적 적은 양의 전력을 사용하는 임의의 네트워크일 수 있다. 예시적인 무선 네트워크(110)는 임의의 블루투스® 네트워크 유형(예를 들어, 블루투스 저에너지(BLE), 블루투스 4.0, 블루투스 5.0, 블루투스 장거리(Bluetooth Long Range)), NB-IoT, LTE 다이렉트(Direct), LTE-M, LTE M2M, 5G, Wi-Fi, Wi-Fi Aware 또는 임의의 저전력 네트워크를 포함할 수 있다. 하나 이상의 엔드포인트 장치(105)는 상이한 유형의 무선 네트워크(110)를 사용하여 다양한 중간 장치(115)에 연결할 수 있다. 예를 들어, 제 1 엔드포인트 장치(105a)는 제 1 근거리 무선 네트워크(110a)를 통해 제 1 중간 장치(115a)와 전자 통신할 수 있고, 제 2 엔드포인트 장치(105b)는 제 2 근거리 무선 네트워크(110b)를 통해 제 2 중간 장치(115b)와 전자 통신할 수 있다.

[0031] 엔드포인트 장치(105), 중간 장치(115), 또는 둘 모두는 고정되거나, 상대적으로 고정되거나 이동할 수 있다. 엔드포인트 장치(105)와 중간 장치(115)가 서로의 무선 범위에 들어갈 때, 엔드포인트 장치(105)와 중간 장치(115)는 핸드셰이크(handshake) 및/또는 인증을 수행하여 엔드포인트 장치(105)와 중간 장치(115) 사이의 데이터 교환을 개시할 수 있다.

[0032] 몇몇 실시예에서, 엔드포인트 장치(105)는 무선 네트워크(110)를 통해 데이터를 포함하는 비컨을 주기적으로 전송할 수 있다. 엔드포인트 장치(105)는 엔드포인트 장치(105)에서 실행될 수 있는 다양한 서비스를 포함할 수 있다. 예를 들어, 스마트 워치는 시계 서비스, 심박수 모니터 서비스, 모션 검출 서비스, 음악 서비스 등을 포함할 수 있다. 비컨은 이들 서비스 각각에 대해 생성되거나 단일 비컨이 생성되어 서비스의 일부 또는 전체에 대한 데이터를 포함할 수 있다.

[0033] 중간 장치(115)는 엔드포인트 장치들로부터 그러한 비컨들을 청취할 수 있다. 비컨 수신에 응답하여, 중간 장치(115)는 제 2 네트워크(120)를 통해 중계 서버(125)에 비컨을 전송할 수 있다. 적어도 하나의 실시예에서, 무선 네트워크(110) 및 제 2 네트워크(120)는 상이한 유형의 네트워크이다. 예를 들어, 무선 네트워크(110)는 Bluetooth® 네트워크일 수 있고, 제 2 네트워크(120)는 셀룰러 네트워크, Wi-Fi 또는 인터넷일 수 있다.

[0034] 제 2 네트워크(120)는 공중망(예를 들어, 인터넷), 사설망(예를 들어, LAN(Local Area Network) 또는 WAN(Wide Area Network)), 유선 네트워크(예를 들어, 이더넷 네트워크), 무선 네트워크(예를 들어, 802.xx 네트워크 또는 Wi-Fi 네트워크), 셀룰러 네트워크(예를 들어, LTE(Long Term Evolution) 또는 LTE-어드밴스드(Advanced) 네트워크, 1G, 2G, 3G, 4G, 5G 등), 라우터, 허브, 스위치, 서버 컴퓨터 및/또는 이들의 조합을 포함할 수 있다.

[0035] 중계 서버(125)는 제 3 네트워크(130)를 통해 엔드포인트 관리자 서버(135)로 비컨 또는 비컨과 관련된 정보를 전송할 수 있다. 제 3 네트워크(120)는 공중망(예를 들어, 인터넷), 사설망(예를 들어, LAN(Local Area Network) 또는 WAN(Wide Area Network)), 유선 네트워크(예를 들어, 이더넷 네트워크), 무선 네트워크(예를 들어, 802.xx 네트워크 또는 Wi-Fi 네트워크), 셀룰러 네트워크(예를 들어, LTE(Long Term Evolution) 또는 LTE-Advanced 네트워크, 1G, 2G, 3G, 4G, 5G 등), 라우터, 허브, 스위치, 서버 컴퓨터 및/또는 이들의 조합을 포함할 수 있다. 적어도 하나의 실시예에서, 제 2 네트워크(120) 및 제 3 네트워크(130)는 동일한 네트워크이거나 적어도 일부 중첩 구성요소를 포함한다.

[0036] 하나 이상의 중계 서버(125)는 랙마운트 서버(rackmount server), 라우터 컴퓨터, 서버 컴퓨터, 개인용 컴퓨터, 메인프레임 컴퓨터, 랩톱 컴퓨터, 태블릿 컴퓨터, 데스크탑 컴퓨터, 스마트폰, 자동차, 드론, 로봇, 운영 체제 등이 있는 임의의 이동 장치, 데이터 저장장치(예를 들어, 하드 디스크, 메모리, 데이터베이스), 네트워크, 소프트웨어 구성 요소 및/또는 하드웨어 구성 요소와 같은 하나 이상의 컴퓨팅 장치를 포함할 수 있다. 하나 이상의 중계 서버(125)는 중간 장치(115)로부터 비컨을 수신하도록 구성될 수 있다. 하나 이상의 중계 서버(125)는 엔드포인트 관리자 서버(135)와 관련되거나 연관된 비컨, 또는 데이터를 전송할 수 있다. 하나 이상의 중계 서버(125)는 엔드포인트 관리자 서버(135)로부터 메시지를 수신할 수 있고, 몇몇 실시예에서 엔드포인트 관리자 서버(135)로부터 중간 장치(115)로 메시지를 전송할 수 있다. 적어도 몇몇 실시예에서, 중간 장치(115)는 엔드포인트 관리자 서버(135)로부터 메시지를 수신하는 것에 응답하여 하나 이상의 작동을 수행할 수 있다. 작동은 중간 장치(115)에 국부적인 작동 및/또는 엔드포인트 관리자 서버(135)로부터 엔드포인트 장치(105)로 메시지를 전송하는 것을 포함한다.

[0037] 엔드포인트 관리자 서버(135)는 랙마운트 서버, 라우터 컴퓨터, 서버 컴퓨터, 개인용 컴퓨터, 메인프레임 컴퓨터, 랩톱 컴퓨터, 태블릿 컴퓨터, 데스크탑 컴퓨터, 스마트폰, 자동차, 드론, 로봇, 운영 체제 등이 있는 임의의 이동 장치, 데이터 저장장치(예를 들어, 하드 디스크, 메모리, 데이터베이스), 네트워크, 소프트웨어 구성 요소 및/또는 하드웨어 구성 요소와 같은 하나 이상의 컴퓨팅 장치를 포함할 수 있다. 엔드포인트 관리자 서버(135)는 하나 이상의 엔드포인트 장치(105)와 연관될 수 있다. 예를 들어, 특정 기업, 개인 또는 제조업체는 엔드포인트 장치(105)를 판매할 수 있고 엔드포인트 관리자 서버(135)를 사용하여 엔드포인트 장치(105)와 통신 및/또는 제어할 수 있다.

[0038] 엔드포인트 관리자 서버(135)는 특정 엔드포인트 장치(105) 또는 엔드포인트 장치(105)의 세트와 관련된 메시지를 전송할 수 있다. 예를 들어, 엔드포인트 관리자 서버(135)는 특정 엔드포인트 장치(105) 또는 엔드포인트 장치(105)의 세트에 업데이트(예를 들어, 펌웨어, 소프트웨어)를 송신할 수 있다. 엔드포인트 관리자 서버(135)는 특정 엔드포인트 장치(105)에 의해 생성된 비컨으로부터의 요청에 대한 응답과 같은 다른 통신을 엔드포인트 장치(105)에 전송할 수 있다.

[0039] 각각의 중계 서버(125)는 메시지 관리자(140)를 포함할 수 있다. 메시지 관리자(140)는 프로세서, (예를 들어, 하나 이상의 작동의 성능을 수행하거나 제어하기 위한)마이크로프로세서, FPGA, 또는 ASIC을 포함하는 하드웨어를 사용하여 구현될 수 있다. 몇몇 다른 경우에, 메시지 관리자(140)는 하드웨어와 소프트웨어의 조합을 사용하여 구현될 수 있다. 소프트웨어에서의 구현은 컴퓨팅 시스템(예를 들어, 중계 서버(135))의 하드웨어에 포함될 수 있는 것과 같은 하나 이상의 트랜지스터 또는 트랜지스터 요소의 신속한 활성화 및 비활성화를 포함할 수 있다. 또한, 소프트웨어 정의 명령은 트랜지스터 요소 내의 정보에 대해 작동할 수 있다. 소프트웨어 명령의 구현은 적어도 일시적으로 전자 경로를 재구성하고 컴퓨팅 하드웨어를 변환할 수 있다.

[0040] 각각의 중계 서버(125)는 데이터 저장장치(145)를 포함할 수 있다. 데이터 저장장치(145)는 임의의 메모리 또는 데이터 저장장치를 포함할 수 있다. 몇몇 실시예에서, 데이터 저장장치(145)는 컴퓨터 실행가능 명령어 또는 데이터 구조가 저장되어 있거나 운반하기 위한 컴퓨터 판독가능 저장 매체를 포함할 수 있다. 컴퓨터 판독가능 저장 매체는 프로세서와 같은 범용 또는 특수 목적 컴퓨터에 의해 액세스될 수 있는 임의의 이용 가능한 매체를 포함할 수 있다. 예를 들어, 데이터 저장장치(145)는 RAM(Random Access Memory), ROM(Read-Only Memory), 전기적 소거 및 프로그램 가능 읽기 전용 메모리(EEPROM), CD-ROM(Compact Disc Read-Only Memory) 또는 기타 광 디스크 저장 장치, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 플래시 메모리 장치(예를 들어, 솔리드 스테이트 메모리 장치), 또는 컴퓨터에서 실행할 수 있는 명령이나 데이터 구조의 형태로 원하는 프로그램 코드를 운반 또는 저장하는데 사용되고 범용 또는 특수 목적 컴퓨터에서 액세스될 수 있는 임의의 다른 저장 매체를 포함하는 유형 또는 비-일시적 컴퓨터 판독 가능 저장 매체일 수 있는 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. 위의 조합은 데이터 저장장치(145)에 포함될 수 있다. 도시된 실시예에서, 데이터 저장장치(145)는 중계 서버(125)의 일부이다. 임의의 실시예에서, 데이터 저장장치(145)는 중계 서버(125)와 분리되어 네트워크를 통해 데이터 저장장치(145)에 접근할 수 있다. 적어도 하나의 실시예에서, 데이터 저장장치(145)는 다중 데이터 저장장치를 포함할 수 있다.

[0041] 데이터 저장장치(145)는 엔드포인트 장치(105), 중간 장치(115), 및 엔드포인트 관리자 서버(135)에 관한 데이터 그리고 엔드포인트 장치(105), 중간 장치(115), 및 엔드포인트 관리자 서버(135) 사이의 관계를 포함할 수 있다. 예를 들어, 데이터 저장장치(145)는 특정 엔드포인트 관리자 서버(135)와 연관된 엔드포인트 장치의 테이블 또는 목록을 포함할 수 있다. 데이터 저장장치(145)는 비컨의 수신 타임스탬프(timestamp), 비컨의 생성과 연관된 타임스탬프, 비컨을 생성하거나 전송하는 비컨 및/또는 엔드포인트 장치(105)와 연관된 지리적 위치, 엔드포인트 장치와 관련된 센서 데이터, 엔드포인트 관리자 서버(135)와 엔드포인트 장치(105) 사이의 데이터를 송신하는 방법 및/또는 위치에 대한 라우팅 정보, 중간 장치와 엔드포인트 장치 사이의 연결 강도, 중간 장치(115)에 대한 엔드포인트 장치(105)의 근접성, 중간 장치(115) 및 엔드포인트 장치(105)를 연결하는 무선 네트워크(110)의 유형, 중간 장치(115)와 엔드포인트 장치(105) 사이의 연결 비용, 중간 장치의 현재 배터리 수준, 중간 장치의 유형 등과 같은 엔드포인트 장치로부터 수신된 비컨에 관한 데이터를 포함할 수 있다.

[0042] 메시지 관리자(140)는 엔드포인트 장치(105), 중간 장치(115) 및 엔드포인트 관리자 서버(들)(135) 사이의 통신을 처리할 수 있다. 예에서, 메시지 관리자(140)는 제 2 네트워크(120a)를 통해 중간 장치(115a)로부터 비컨을 수신할 수 있다. 비컨은 엔드포인트 장치(105a)에 의해 무선 네트워크(110a)를 통해 중간 장치로 전송될 수 있다. 비컨은 엔드포인트 장치(105)의 식별자(예를 들어, MAC 주소, 고유 ID), 엔드포인트 장치(105a)의 지리적 위치, 및 그것이 지원하는 서비스의 UUID의 광고 등을 포함하는 엔드포인트 장치(105)에 대한 특성을 포함할 수 있다. 메시지 관리자(140)는 비컨에 관한 정보를 식별하기 위해 비컨을 분석하는 것과 같이 비컨의 특성을 식별할 수 있다. 메시지 관리자(140)는 비컨의 특성에 기반하여 비컨과 연관된 엔드포인트 관리자 서버(135)를 식별하기 위해 데이터 저장장치(145)에 액세스할 수 있다. 예를 들어, 엔드포인트 장치의 식별자는 특정 엔드포인트 관리자 서버(135)를 작동하는 특정 제조업체와 연관될 수 있다. 메시지 관리자(140)는 데이터 저장장치(145)에서 이러한 특정 엔드포인트 관리자 서버(135) 및 엔드포인트 관리자 서버(135)에 도달하기 위해서 비컨을 송신하기 위한 주소 및/또는 경로를 식별할 수 있다. 적어도 몇몇 실시예에서, 메시지 관리자(140)는 제 3 네트워크(130)를 통해 엔드포인트 관리자 서버(135)에 비컨 또는 비컨 메시지를 송신할 수 있다. 비컨 메시지는 비컨을 포함할 수 있거나, 비컨을 포함하지 않을 수 있거나, 비컨에 관한 정보를 포함할 수 있다.

[0043] 적어도 하나의 실시예에서, 비컨은 엔드포인트 장치(105)와 연관된 다수의 서비스로부터의 데이터를 포함할 수 있다. 추가적으로 또는 대안적으로, 단일 엔드포인트 장치(105)로부터의 다수의 비컨이 생성되고 무선 네트워크(110)를 통해 방송될 수 있다. 예를 들어, 이들 다수의 비컨 각각은 엔드포인트 장치(105)와 연관된 상이한 서비스와 연관될 수 있다. 메시지 관리자(140)는 서비스를 식별할 수 있고, 서비스에 대한 정보에 기반하여 비컨 메시지를 수신해야 하는 적절한 엔드포인트 관리자 서버(135)를 식별할 수 있다.

[0044] 엔드포인트 관리자 서버(135)는 중계 서버(125)로부터 메시지를 수신할 수 있다. 엔드포인트 관리자 서버(135)는 메시지를 저장하고, 메시지를 처리하고, 메시지에 기반하여 보고서를 생성하고, 메시지에 기반하여 통지 또는 응답을 생성하거나, 임의의 다른 작동을 생성할 수 있다. 예를 들어, 엔드포인트 관리자 서버(135)는 비컨 메시지에 관한 응답 메시지를 생성할 수 있다. 응답 메시지는 중계 서버(125), 중간 장치(115), 비컨을 생성한 엔드포인트 장치(105), 또는 비컨을 생성하지 않은 다른 엔드포인트 장치(105) 중 하나 이상을 위한 메시지를 포함할 수 있다. 엔드포인트 관리자 서버(135)는 엔드포인트 관리자 서버(135)(예를 들어, 중계 서버(125a))에 비컨 메시지를 송신하는 동일한 중계 서버(125), 또는 비컨 메시지를 엔드포인트 관리자 서버(135)(예를 들어, 중계 서버(125b))로 송신하지 않은 상이한 중계 서버(125)로 응답 메시지를 송신할 수 있다.

[0045] 중계 서버(125)는 엔드포인트 관리자 서버(135)로부터 비컨 메시지에 관한 응답 메시지를 수신할 수 있다. 중계 서버(125)는 예컨대, 중계 서버(125)에서 작동을 수행함으로써, 다른 장치(예를 들어, 사용자 장치)로 데이터를 송신하고, 엔드포인트 장치(105)로 데이터를 송신하는 등에 의해서 응답 메시지를 처리할 수 있다.

[0046] 네트워크 구성(100)은 인터넷을 통한 종래의 통신과는 상이한 방식으로 네트워크 기반 통신이 가능한 임의의 장치들 사이에서 데이터를 교환하는데 사용될 수 있다.

[0047] 예에서, 네트워크 구성(100)은 지연-허용 연결을 생성하기 위해 기존 스마트폰 기반구조를 활용할 수 있다. 네트워크 구성(100)은 초기 지연 허용 방식으로 데이터를 클라우드로 이동할 수 있으며, 이는 펌웨어 업데이트, 상태 업데이트, 로그 파일 저장 및 소액 결제와 같은 많은 유형의 IoT 통신에 유용할 수 있다. 중간 장치는 산업용 장치, 스마트워치, 웨어러블, 물류 추적기 및 환경 센서와 같은 다른 장치(예를 들어, 엔드포인트 장치(105))를 주기적으로 스캔하기 위해 스마트폰에서 실행되는 소프트웨어를 포함할 수 있다. 이들 엔드포인트 장치(105)는 스마트폰에서 실행되는 소프트웨어 클라이언트와 연결하여 클라우드로 그리고 클라우드 내에서 데이터를 이동하기 위한 방대한 영역 전체 네트워크를 생성할 수 있다.

[0048] 또한, 인간 인구의 95%가 일종의 셀룰러 서비스에 포함되는 것으로 추정되었다. 네트워크 구성(100)은 세계 어느 곳에서나 배치될 수 있고 더 낮은 연결성의 영역이 그들의 연결성을 증가시킬 수 있게 한다. 또한, 네트워크 구성(100)은 예를 들어 (블루투스)Bluetooth® 지원 스마트폰에서 실행되는 소프트웨어를 사용하여 기존의 셀룰러 네트워크의 도달 범위를 넘어서는 범위를 제공할 수 있다. 사용자는 셀룰러 연결이 제한되거나 없는 영역으로 여행할 수 있지만, 여전히 무선 네트워크(110)를 통해 엔드포인트 장치(105)로부터 비컨을 수신할 수 있다. 예를 들어, 통신 사업자는 네트워크 구성(100)을 사용하여 이제 소프트웨어 업데이트를 사용자 장치에 쉽게 배포하여 세계의 가장 먼 지역에도 더 높은 대기 시간 IoT 연결을 제공하기 위해서 설명된 대로 엔드포인트 장치(105)와 통신을 시작할 수 있다.

[0049] 특정 예에서, 네트워크 구성(100)은 자산 추적 및 관리를 위해 사용될 수 있다. 예를 들어, 네트워크 구성(100)은 무선 라디오 칩셋이 있는 스케이트보드, 부착된 추적 비컨, 랩톱 등과 같은 엔드포인트 장치(105)로 구성된 분실물을 찾는데 사용될 수 있다. 사용자는 예를 들어, 모바일 애플리케이션 또는 웹사이트를 사용하여 아이템이 분실되었음을 엔드포인트 관리자 서버(135) 또는 중계 서버(125)에 표시함으로써 아이템이 분실되었음을 나타낼 수 있다. 제 1 실시예에서, 엔드포인트 매니저 서버(135)는 분실물을 감시하기 위해서 하나 이상의 중계 서버(125)에 메시지를 보낼 수 있다. 중계 서버(125)는 분실물 감시 목록에 분실물의 식별자를 추가할 수 있다. 중간 장치(115)가 상이한 지리적 위치로 이동함에 따라서, 그들은 상이한 종점 장치(103)로부터 비컨을 수신할 수 있다. 그 다음, 중간 장치(115)는 중계 서버(125)로 비컨을 전달한다. 중계 서버(125)가 비컨을 수신할 때, 중계 서버(125)는 비컨이 감시 목록에 있는 엔드포인트 장치(105)에서 발신되었는지를 결정하기 위해서 비컨을 분석할 수 있다. 중계 서버(125)가 감시 목록에 있는 엔드포인트 장치(105)에서 시작된 비컨을 식별할 때, 중계 서버(125)는 유실물이 발견되었음을 엔드포인트 관리자 서버(135)에 통지할 수 있다. 적어도 몇몇 실시예에서, 중계 서버(125)는 분실물이 발견되었다는 통지를 푸시 통지(push notification) 또는 풀 통지(pull notification)로서(즉, 엔드포인트 관리자 서버(135)로부터의 요청에 대한 응답으로) 보낼 수 있다. 적어도 몇몇 실시예에서, 중계 서버(125)는 아이템이 분실되었음을 나타내기 위해서 사용자에 의해 사용된 사용자 장치에 분실 아이템이 발견되었다는 통지를 보낼 수 있다.

[0050] 중간 장치(115) 및/또는 엔드포인트 장치(105)가 상이한 지리적 위치들로 이동함에 따라서, 그들이 네트워크 구성(100)에서 통신하는 방식이 변경될 수 있다. 예를 들어, 엔드포인트 장치(105) 중 하나가 중간 장치(115) 중 하나와 통신할 수 있을 만큼 더 이상 가깝지 않은 위치로 이동하는 경우에, 비컨을 수신하는 범위 내부에 장치가 없더라도 계속 비컨을 보낼 수 있다. 게다가, 엔드포인트 장치(105)는 중간 장치(115) 중 하나가 범위 내에 있을 때까지 계속해서 비컨을 보낼 수 있다. 유사하게, 중간 장치(115)는 엔드포인트 장치(105)의 범위 밖의

위치들로 이동할 수 있고, 네트워크 구성(100)은 그에 따라 적응할 수 있다.

[0051] 네트워크 구성(100)은 엔드포인트 장치(105) 중 대응하는 것에 대한 비컨을 통신 및/또는 포워딩하기 위해서 중간 장치(115) 중 하나를 선택할 수 있다. 예를 들어, 중계 서버(125) 중 하나는 엔드포인트 장치(105) 중 하나로 응답 메시지를 전송하는 것을 취급하기 위해서 중간 장치(115) 중 하나를 선택할 수 있다. 중계 서버(125)는 중간 장치(115)와 목표 엔드포인트 장치(105) 사이의 연결 강도, 중간 장치에 대한 엔드포인트 장치(105)의 근접성, 중간 장치(115)와 엔드포인트 장치(105)를 연결하는 무선 네트워크(110)의 유형, 중간 장치(115)와 엔드포인트 장치(105) 사이의 연결 비용, 중간 장치의 현재 배터리 잔량, 중간 장치의 유형 장치 등과 같은 응답 메시지를 송신하는데 사용할 중간 장치(115)를 선택하기 위해서 임의의 선택 기준을 사용할 수 있다.

[0052] 몇몇 상황에서, 중간 장치(115b) 중 2 개는 엔드포인트 장치(105) 중 하나의 범위 내에 있을 수 있고 둘 다 엔드포인트 장치(105)로부터 동일한 비컨을 수신할 수 있다. 또한, 중간 장치(115) 모두는 엔드포인트 장치(105)의 비컨을 중계 서버들(125) 중 하나로 전달할 수 있다. 중복성, 네트워크 트래픽(network traffic), 배터리 영향 등을 줄이기 위해서, 중계 서버(125)는 중간 장치(115) 중 하나를 선택하여 엔드포인트 장치(105)와의 통신을 처리하고, 선택되지 않은 중간 장치가 엔드포인트 장치(105)로부터의 비컨을 무시하도록 지시하고, 엔드포인트 장치(105)로부터 비컨을 폐기하고, 엔드포인트 장치(105)로부터 비컨 송신을 중지하거나, 네트워크 혼잡을 감소시킬 수 있는 임의의 다른 작업, 데이터 저장 공간 확보, 프로세서 능력 확보 등을 수행할 수 있다.

[0053] 더 많은 중간 장치(115)가 데이터 전송에 이용 가능하게 됨에 따라서, 특정 중간 장치(115)에 대한 데이터 전송 주파수는 감소할 수 있다. 장기적으로, 강화된 밀도 중간 장치(115) 및 기계 학습 기반 프로토콜을 사용하여 본 명세서에 설명된 기술은 중간 장치(115)의 배터리 수명을 크게 개선하고, 네트워크 혼잡을 줄이며, 전역 연결성을 개선할 수 있다. 중계 서버(125)는 엔드포인트 장치(105)와 통신하는데 사용할 중간 장치(105)와 엔드포인트 장치(105)에 관한 통신을 중단할 중간 장치(115)를 선택하기 위한 임의의 선택 기준, 예컨대 중간 장치(115)와 타겟 엔드포인트 장치(105) 사이의 연결 강도, 중간 장치(115)에 대한 엔드포인트 장치(105)의 근접성, 중간 장치(115)와 엔드포인트 장치(105)를 연결하는 무선 네트워크(110)의 유형, 중간 장치(115)와 엔드포인트 장치(105) 사이의 연결 비용, 중간 장치(115)의 현재 배터리 잔량, 중간 장치(115)의 유형 등을 사용할 수 있다.

[0054] 네트워크 운영자는 엔드포인트 장치(105)와 같은 네트워크 구성(100)의 장치 중 일부를 고유하게 식별하는 것이 바람직할 수 있다. 엔드포인트 장치(105)가 식별되는 한 가지 방법은 엔드포인트 장치(105)의 하드웨어(예를 들어, 블루투스 칩셋)에 의해 정의될 수 있는 MAC 주소에 의한 방법이다. 그러나 식별을 위해서 MAC 주소를 사용하는 것은 몇 가지 중요한 단점과 관련될 수 있다.

[0055] 먼저, 엔드포인트 장치(105)를 MAC 주소로 식별한다는 것은 엔드포인트 장치(105)가 제 3자에 의해 추적되는 것을 피하기 위해서 이러한 동일한 주소가 랜덤화될 수 없다는 것을 의미하며, 이는 보안 및 프라이버시 문제를 초래할 수 있다. 예를 들어, 엔드포인트 장치(105)의 소유자는 엔드포인트 장치(105)가 어디에 위치하는지 (예를 들어, GPS 또는 네트워크 연결 위치를 통해)단순히 체크함으로써 추적될 수 있다. 이는 소유자가 항상 착용하도록 되어 있고 소유자가 항상 추적되도록 허용할 수 있는 시계와 같은 웨어러블 장치에 대한 중요한 문제일 수 있다. 둘째, 장치의 MAC 주소는 올바른 하드웨어 및 소프트웨어를 사용하는 다른 장치에 의해 쉽게 스푸핑될 수 있다. 따라서 MAC 주소는 보안 및 프라이버시 문제로 인해 장치를 식별하는 우수한 방법이 아니다.

[0056] 따라서, 도 1의 임의의 장치(예를 들어, 엔드포인트 장치(105), 중간 장치(115), 중계 서버(125), 엔드포인트 관리자 서버(135) 등)는 MAC 주소 이외의 식별자를 사용하여 식별될 수 있다. 특히, 본 개시는 네트워크 운영자만을 위한 네트워크 장치에 링크될 수 있는 동안 스푸핑하기 어렵고 제 3자에게 랜덤으로 나타나는 식별자를 포함한다. 또한, 개시된 식별자는 비교적 구현하기 쉽고(너무 많은 작업을 필요로 하지 않고) 계산이 빠르므로 소형 배터리 및 상대적으로 낮은 성능 및 저전력 하드웨어에 의존하는 장치에서 구현하는데 적합하다.

[0057] 적어도 하나의 실시예에서, 엔드포인트 장치(105) 및/또는 중간 장치(115)는 장치 ID 생성기(150)를 포함할 수 있다. 장치 ID 생성기(150)는 프로세서, (예를 들어, 하나 이상의 작동을 수행하거나 성능을 제어하기 위한)마이크로프로세서, FPGA, 또는 ASIC을 포함하는 하드웨어를 사용하여 구현될 수 있다. 몇몇 다른 경우에, 장치 ID 생성기(150)는 하드웨어 및 소프트웨어의 조합을 사용하여 구현될 수 있다. 소프트웨어에서의 구현은 컴퓨팅 시스템의 하드웨어(예를 들어, 엔드포인트 장치(105) 및/또는 중간 장치(115))에 포함될 수 있는 하나 이상의 트랜지스터 또는 트랜지스터 요소의 신속한 활성화 및 비활성화를 포함할 수 있다. 또한 소프트웨어 정의 명령은 트랜지스터 요소 내의 정보에 대해 작동할 수 있다. 소프트웨어 명령의 구현은 적어도 일시적으로 전자 경로를 재구성하고 컴퓨팅 하드웨어를 변환할 수 있다.

[0058] 장치 ID 생성기(150)는 제 3자가 이해할 수 없지만 네트워크 운영자, 중계 서버(125) 및/또는 엔드포인트 관리자 서버(135)에 의해 장치에 쉽게 링크될 수 있는 장치가 상주하는 장치에 대한 고유 식별자를 생성할 수 있다. 장치 ID 생성기(150)는 도 2 및 도 3에 설명된 방법을 사용하여 고유 식별자를 생성할 수 있는 고유 식별자를 생성할 수 있다.

[0059] 적어도 하나의 실시예에서, 중계 서버(들)(125) 및/또는 엔드포인트 관리자 서버(135)는 장치 ID 디코더(155)를 포함할 수 있다. 장치 ID 디코더(155)는 프로세서, (예를 들어, 하나 이상의 작동의 성능을 수행하거나 제어하기 위한)마이크로프로세서, FPGA, 또는 ASIC을 포함하는 하드웨어를 사용하여 구현될 수 있다. 몇몇 다른 경우에, 장치 ID 디코더(155)는 하드웨어 및 소프트웨어의 조합을 사용하여 구현될 수 있다. 소프트웨어의 구현은 컴퓨팅 시스템(예를 들어, 중계 서버(들)(125) 및/또는 엔드포인트 관리자 서버(135))의 하드웨어에 포함될 수 있는 것과 같은 하나 이상의 트랜지스터 또는 트랜지스터 요소의 신속한 활성화 및 비활성화를 포함할 수 있다. 또한 소프트웨어 정의 명령은 트랜지스터 요소 내의 정보에 대해 작동할 수 있다. 소프트웨어 명령의 구현은 적어도 일시적으로 전자 경로를 재구성하고 컴퓨팅 하드웨어를 변환할 수 있다.

[0060] 장치 ID 디코더(155)는 엔드포인트장치(105) 및/또는 중간 장치(115)로부터 수신된 고유 식별자를 디코딩할 수 있다. 고유 식별자는 엔드포인트 장치(105) 및/또는 중간 장치(115) 중 적어도 하나에 대응할 수 있다.

[0061] 장치 ID 생성기(150) 및 장치 ID 디코더(155)는 네트워크 장치를 안전하고 사적으로 식별하기 위한 노력으로 서로 통신할 수 있다. 예를 들어, 장치 ID 생성기(150)와 장치 ID 디코더(155)는 운영자 비밀을 서로 통신할 수 있다. 적어도 하나의 실시예에서, 운영자 비밀은 장치 ID 디코더(155)에서 정의되고 엔드포인트 장치(105) 및/또는 중간 장치(115) 각각으로 송신된다. 차례로, 엔드포인트 장치(105) 및/또는 중간 장치(115)의 장치 ID 생성기(150)는 장치의 MAC 주소 및 운영자 비밀 둘 모두에 기초한 해시 값을 포함할 수 있는 고유 식별자를 생성하기 위해서 운영자 비밀을 사용할 수 있다. 추가 세부사항은 도 2 및 도 3과 함께 추가로 설명된다.

[0062] 본 개시의 범위를 벗어나지 않고 네트워크 구성(100)에 수정, 추가 또는 생략이 이루어질 수 있다. 본 개시는 하나 이상의 엔드포인트 장치(105), 하나 이상의 무선 네트워크, 하나 이상의 중간 장치(115), 하나 이상의 제 2 네트워크(120), 하나 이상의 중계 서버(125), 하나 이상의 제 3 네트워크(130), 및 하나 이상의 엔드포인트 관리자 서버(135) 또는 이들의 임의의 조합을 포함을 포함하는 네트워크 구성(100)에 보다 일반적으로 적용된다.

[0063] 더욱이, 설명된 다양한 구성요소의 분리는 이들 모두에서 분리가 발생함을 나타내는 것을 의미하지 않는다. 또한, 설명된 구성요소가 단일 구성요소로 함께 통합되거나 다중 구성요소로 분리될 수 있다는 것이 본 개시의 이점으로 이해될 수 있다.

[0064] 도 2 및 도 3은 네트워크 장치를 안전하고 개인적으로 식별하는 예시적인 방법의 흐름도를 도시한다. 설명된 방법은 악의적인 제 3자가 장치에서 방출하는 비컨을 인식하지 못하도록 하는데 사용될 수 있다. 이러한 방법은 장치의 보안 및 프라이버시 그리고 그러한 장치와 관련된 사용자를 보호하기 위해서 구현될 수 있다.

[0065] 상기 방법은 하드웨어(회로, 전용 논리 등), (범용 컴퓨터 시스템 또는 전용 기계에서 실행되는 것과 같은)소프트웨어, 또는 둘의 조합을 포함할 수 있는 처리 논리에 의해 수행될 수 있으며, 이러한 처리 논리는 엔드포인트 장치(105), 중간 장치(115) 및/또는 도 1의 중계 서버(125), 또는 다른 컴퓨터 시스템 또는 장치에 포함될 수 있다. 그러나 다른 시스템 또는 시스템 조합을 사용하여 방법을 수행할 수 있다.

[0066] 설명의 편의를 위해서, 본 명세서에 설명된 방법이 일련의 행위로 묘사되고 설명된다. 그러나, 본 개시에 따른 행위는 다양한 순서로 및/또는 동시에, 그리고 제시 및 설명되지 않은 다른 행위와 함께 발생할 수 있다. 또한, 설명된 모든 행위가 개시된 요지에 따라서 방법을 구현하는데 사용될 수 있는 것은 아니다. 또한, 당업자는 상기 방법이 상태 다이어그램 또는 이벤트를 통해 일련의 상호 관련된 상태로 대안적으로 표시될 수 있음을 이해하고 인식할 것이다. 또한, 본 명세서에 개시된 방법은 비-일시적 컴퓨터 판독 가능 매체와 같은 제조 물품에 저장되어 이러한 방법을 컴퓨팅 장치로 전송하고 이송할 수 있다. 본 명세서에서 사용된 제조 물품이라는 용어는 임의의 컴퓨터 판독 가능 장치 또는 저장 매체에서 액세스할 수 있는 컴퓨터 프로그램을 포함하도록 의도된다. 이산 블록으로 예시되어 있지만, 원하는 구현에 따라 다양한 블록이 추가 블록으로 분할되거나 더 적은 수의 블록으로 조합되거나 제거될 수 있다.

[0067] 도 2는 네트워크 장치를 안전하고 사적으로 식별하기 위한 예시적인 방법(200) 방법의 흐름도를 도시한다. 예를 들어, 예시적인 방법(200)은 도 1의 엔드포인트 장치(105) 중 적어도 하나에 의해 수행되어 네트워크 장치를 안전하고 사적으로 식별할 수 있다. 상기 방법(200)은 고유 식별자가 생성될 수 있는 블록(202)에서 시작할 수

있다. 몇몇 경우에, 고유 식별자는 엔드포인트 장치(105) 중 하나와 같은 장치에서 생성될 수 있다.

[0068] 몇몇 양태에서, 고유 식별자는 제한된 수의 반-신뢰 당사자들(예를 들어, 네트워크 운영자 및/또는 IoT 연결 제공자)과 함께 장치를 식별하도록 설계된 각각의 장치에 특정한 고유 정적(Unique Static) ID(USID)일 수 있다. 그러한 구성에서는 제 3자가 이해할 수 없지만, 네트워크 운영자가 장치에 쉽게 연결할 수 있는 고유 식별자를 생성하는 것이 바람직할 수 있다.

[0069] 몇몇 실시예에서, 고유 식별자는 id = hash(operatorSecret, deviceMacAddress) 알고리즘을 기반으로 생성될 수 있다. 알고리즘에서 "id"는 장치의 식별자이거나 제 3자와 공유될 수 있는 USID일 수 있다. "해시"는 해싱 알고리즘, 예를 들어 SHA(Secure Hash Algorithm) 또는 기타 적절한 해싱 알고리즘일 수 있다. "OperatorSecret"은 네트워크 또는 장치 운영자가 알고 있는 비밀일 수 있다. "DeviceMacAddress"는 장치 하드웨어의 MAC 주소일 수 있다. 몇몇 구성에서 장치는 패킷을 대중 또는 다른 장치에 보낼 때 랜덤화 MAC 주소를 사용할 수 있다. 그러한 구성에서, 장치는 고유 식별자를 생성하기 위해서 장치의 하드웨어 MAC 주소를 계속 사용하여 네트워크 운영자와 자신을 식별할 수 있다.

[0070] 그러한 구성에서 반-신뢰 당사자는 고유 식별자(예를 들어, USID)만 볼 수 있지만, 운영자의 비밀(예를 들어, OperatorSecret)을 가져오거나 장치의 MAC 주소(예를 들어, DeviceMacAddress)를 가져올 수도 없다. 그러나 네트워크 운영자는 자신이 정의한 운영자의 비밀(예를 들어, OperatorSecret)과 해당 장치의 MAC 주소(예를 들어, DeviceMacAddress)를 알고 있다. 예를 들어, 네트워크 운영자는 장치 제조업체로부터 장치의 MAC 주소를 얻을 수 있다. 이러한 정보를 기반으로, 네트워크 운영자는 각각의 장치의 고유 식별자(예를 들어, USID)를 다시 계산하고 제 3자의 도구에서 관련 데이터를 검색할 수 있다.

[0071] 따라서 고유 식별자는 장치의 MAC 주소(임의로 할당되지 않고 하드웨어에 의해 정의될 수 있음)와 운영자 비밀 모두를 기반으로 하는 해시된 값이다. 고유 식별자는 장치의 MAC 주소와 운영자 비밀을 기반으로 한 해시 값을 포함할 수 있으므로, 고유 식별자는 네트워크 운영자가 식별할 수 있는 동안 제 3자에게 랜덤으로 나타난다. 또한 USID는 반-신뢰할 수 있는 제 3자와 공유할 수 있으므로, 장치의 MAC 주소나 운영자의 비밀을 공개하지 않고도 반-신뢰할 수 있는 제 3자가 장치를 식별할 수 있다. 또한, 고유 식별자는 다른 사람이 운영자의 비밀을 알지 못하므로, 다른 사람이 USID(다른 사람이 장치의 MAC 주소를 알고 있는지 여부)를 생성할 수 없기 때문에 위장하기 어렵다. 또한 고유 식별자의 해시 값은 소형 배터리에 의존하고 상대적으로 성능이 낮고 하드웨어가 저전력인 IoT 장치에서도 쉽고 빠르게 계산할 수 있다.

[0072] 블록(204)에서, 고유 식별자는 다른 장치와 공유될 수 있다. 예를 들어, 고유 식별자는 제한된 수의 반-신뢰 당사자(예를 들어, 네트워크 운영자 및/또는 IoT 연결 제공자)와 공유될 수 있다. 고유 식별자는 예를 들어, 네트워크 운영자, 장치 운영자 또는 반-신뢰된 제 3자가 소유한 다른 장치로 전송될 수 있다. 고유 식별자(예를 들어, USID)는 예를 들어, 블루투스 또는 다른 적절한 연결을 통해 무선으로 장치로부터 비컨의 일부로 전송될 수 있다.

[0073] 위에서 언급한 바와 같이, 방법(200)은 제한된 수의 반-신뢰 당사자로 장치를 식별하는데 사용될 수 있다. 그러나 몇몇 상황에서는 장치를 무제한의 당사자와 식별하는 것이 바람직할 수 있으며 그 중 적어도 일부는 신뢰할 수 없는 당사자일 수 있다. 적어도 일 실시예에서, 고유 식별자(예를 들어, USID)는 어떻게든 고유 식별자(예를 들어, USID)에 대한 액세스를 획득하는 악의적인 사용자를 추가로 위협할 수 있는 주기적으로 재생성되고 공유될 수 있다.

[0074] 도 3은 네트워크 장치를 안전하고 사적으로 식별하기 위한 예시적인 방법(300)의 흐름도를 도시한다. 몇몇 양태들에서, 방법(300)은 무제한의 비-신뢰 당사자들과 함께 장치를 식별하는데 사용될 수 있다. 방법(300)은 고유 식별자(예를 들어, USID)가 광고되거나 공개적으로 방송될 때 구현될 수 있다. 예를 들어, 고유 식별자는 지리적 위치 또는 기타 애플리케이션 또는 구성을 위해 블루투스 비컨 내부에 내장되어 공개적으로 방송될 수 있다.

[0075] 방법(200)과 유사하게, 방법(300)은 고유 식별자가 생성될 수 있는 블록(302) 및 고유 식별자가 다른 장치와 공유될 수 있는 블록(304)을 포함할 수 있다. 그러나, 방법(300)은 또한 운영자 비밀이 순환되는 블록(301)을 포함할 수 있다. 몇몇 구성에서 운영자 비밀은 고유 식별자가 생성되기 전이나 생성될 때 순환될 수 있다.

[0076] 몇몇 양태들에서, 운영자 비밀은 순환 알고리즘에 기초하여 순환될 수 있다. 순환 알고리즘은 미리 정의될 수 있으며 장치 및/또는 네트워크 운영자만 알 수 있다. 또한, 순환 알고리즘은 미리 정의된 매개변수에 기초하여 운영자 비밀을 순환할 수 있으며, 미리 정의된 매개변수는 장치 및/또는 네트워크 운영자에게만 알려질 수

있다. 또한, 몇몇 상황에서 순환 알고리즘 및/또는 미리 정의된 매개변수는 신뢰할 수 있는 제 3자(네트워크 운영자 이외에)에게 알려질 수 있다. 순환 알고리즘은 id = hash(operatorSecret, deviceMacAddress)와 같은 고유 식별자를 생성하는데 사용되는 운영자 비밀을 순환하거나 변경하는데 사용할 수 있다. 순환 알고리즘 및/또는 미리 정의된 매개변수는 네트워크 운영자 및/또는 신뢰할 수 있는 제 3자가 장치를 식별할 수 있도록 고유 식별자를 디코딩하는데 사용될 수 있다.

[0077] 그러한 구성에서, 고유 식별자(예를 들어, USID)는 외부 관찰자 및 제 3자에게 랜덤으로 표시되지만 여전히 장치 운영자, 네트워크 운영자 및/또는 소유자가 장치를 식별하는데 사용될 수 있다. 방법(200)의 고유 식별자는 일반적으로 동일하게 유지될 수 있지만, 방법(300)의 고유 식별자는 순환 운영자 비밀에 기초하여 변경된다. 따라서 제 3자에게 무작위로 나타난다. 또한 제 3자는 운영자의 비밀(예를 들어, OperatorSecret) 또는 장치의 MAC 주소(예를 들어, DeviceMacAddress)를 얻을 수 없다.

[0078] 그러나 네트워크 운영자는 자신이 정의한 운영자의 비밀(예를 들어, OperatorSecret)과 해당 장치의 MAC 주소(예를 들어, DeviceMacAddress)를 알고 있다. 네트워크 운영자는 순환 알고리즘과 해당 매개변수도 알고 있으므로, 순환 운영자의 비밀을 다시 계산할 수 있다. 이러한 정보를 기반으로, 네트워크 운영자는 각각의 장치의 고유 식별자(예를 들어, USID)를 다시 계산하고 제 3자의 도구에서 관련 데이터를 검색할 수 있다.

[0079] 따라서, 방법(300)의 고유 식별자는 장치의 MAC 주소(랜덤으로 할당되기 보다는 하드웨어에 의해 정의될 수 있음) 및 순환 운영자 비밀 둘 모두에 기반한 해시 값을 포함할 수 있다. 고유 식별자는 장치의 MAC 주소와 순환 운영자 비밀을 기반으로 하는 해시 값이므로, 고유 식별자는 네트워크 운영자가 식별할 수 있는 동안 제 3자에게 랜덤으로 나타난다. 적어도 일 실시예에서, 고유 식별자는 장치의 MAC 주소, 운영자 비밀, 및 미리 정의된 매개변수들 중 둘 이상에 기반하여 생성될 수 있는 해시된 값을 포함할 수 있다. 운영자 비밀은 순환될 수 있다. 추가적으로 또는 대안적으로, 미리 정의된 매개변수가 변경될 수 있으며, 이는 고유 식별자도 변경할 수 있다. 또한, 고유 식별자는 다른 사람들이 교환 알고리즘이나 운영자의 비밀을 순환하는데 사용되는 매개변수를 알지 못하기 때문에, 다른 사람들이 USID(다른 사람들이 장치의 MAC 주소를 알고 있는지 여부)를 생성할 수 없으므로 스푸핑하기 어렵다.

[0080] 위에서 언급했듯이, 몇몇 장치는 MAC 주소로 식별될 수 있다. 몇몇 상황에서 MAC 주소는 장치와 관련된 하드웨어(예를 들어, 블루투스 하드웨어)에 의해 정의될 수 있다. 그러나 다른 상황에서는 MAC 주소가 랜덤으로 지정될 수 있다. 예를 들어, 장치의 MAC 주소는 임의로 할당 및 재할당될 수 있으므로 장치를 식별하는데 사용할 수 없다. 이는 장치의 보안 및 프라이버시를 보호하기 위해 수행될 수 있다. 그럼에도 불구하고, 몇몇 상황에서 IoT 네트워크의 사용자 또는 가입자는 장치를 식별할 수 있기를 원할 수 있으므로 비-랜덤화 식별자를 가질 수 있다. 예를 들어, 비-랜덤화 식별자를 사용하여 어떤 장치가 어떤 데이터를 수집했는지 알 수 있다. 따라서 본 명세서에 설명된 고유 식별자를 사용하여 프라이버시 및 보안을 유지하면서 장치를 식별할 수 있다. 설명된 고유 식별자(예를 들어, USID)는 고유하고 정적이지만, 네트워크 구성원에게 개인 데이터를 노출하지 않는다.

[0081] 이들 고유 식별자는 에지 노드의 MAC 주소를 고객의 개발자 키로 해싱하고 원하는 소프트웨어 개발 키트를 시작할 때 런타임 식별자(RID)를 교체하여 생성할 수 있다. 몇몇 경우에, 이러한 구성은 특수한 사용 사례를 위한 옵트-인(opt-in) 전용 시스템일 수 있다. 네트워크 가입자가 소프트웨어 개발 키트를 구성할 때 이러한 종류의 고유 식별자를 활성화하면, 이러한 장치별 고유 식별자(예를 들어, USID)로 수집한 데이터를 필터링할 수 있는데, 이는 네트워크가 해시된 고유 식별자만 볼 수 있으므로 네트워크의 임의의 구성원도 고유 식별자를 생성하는데 사용된 MAC 주소를 검색할 수 없기 때문이지만, 네트워크 가입자는 고유한 MAC 주소 목록과 개발자 키를 사용하여 에지 노드에서 사용된 고유 식별자를 재생성하고 에지 노드에서 어떤 IoT 장치를 검출했는지 정확하게 알 수 있다.

[0082] 도 4는 기계가 본 명세서에서 논의된 방법들 중 임의의 하나 이상을 수행하게 하기 위한 명령어 세트가 실행될 수 있는 컴퓨팅 장치(700)의 예시적인 형태의 기계의 도식적 표현을 예시한다. 컴퓨팅 장치(700)는 본 명세서에서 논의된 방법 중 하나 이상을 기계가 수행하도록 하는 명령 세트가 실행될 수 있는, 휴대폰, 스마트폰, 넷북 컴퓨터, 랙마운트 서버(rackmount server), 라우터 컴퓨터(router computer), 서버 컴퓨터, 개인용 컴퓨터, 메인프레임 컴퓨터, 랩톱 컴퓨터, 태블릿 컴퓨터, 데스크톱 컴퓨터 등을 포함할 수 있다. 대안적으로, 기계는 LAN, 인트라넷, 엑스트라넷 또는 인터넷의 다른 기계에 연결(예를 들어, 네트워크)될 수 있다. 기계는 클라이언트-서버 네트워크 환경에서 서버 기계의 용량으로 작동할 수 있다. 기계에는 개인용 컴퓨터(PC), 셋톱 박스(STB), 서버, 네트워크 라우터, 스위치 또는 브리지, 그 기계에 의해 취해지는 행위를 지정하는 (순차적이든 아

니든)명령어 세트를 실행할 수 있는 임의의 기계를 포함할 수 있다. 또한, 단일 기계만이 예시되어 있지만, 용어 "기계"는 본 명세서에서 논의된 방법 중 임의의 하나 이상을 수행하기 위해서 명령어 세트(또는 다중 세트)를 개별적으로 또는 공동으로 실행하는 기계의 임의의 집합체를 포함할 수도 있다.

[0083] 예시적인 컴퓨팅 장치(700)는 버스(708)를 통해 서로 통신하는, 프로세싱 장치(예를 들어, 프로세서)(702), 메인 메모리(704)(예를 들어, 읽기 전용 메모리(ROM), 플래시 메모리, 동기식 DRAM(SDRAM)와 같은 동적 랜덤 액세스 메모리(DRAM)), 정적 메모리(706)(예를 들어, 플래시 메모리, 정적 랜덤 액세스 메모리(SRAM)) 및 데이터 저장 장치(716)를 포함한다.

[0084] 프로세싱 장치(702)는 마이크로프로세서, 중앙 처리 장치 등과 같은 하나 이상의 범용 처리 장치를 나타낸다. 더 구체적으로, 프로세싱 장치(702)는 복합 명령어 세트 컴퓨팅(CISC) 마이크로프로세서, RISC(Reduced Instruction Set Computing) 마이크로프로세서, VLIW(Very Long Instruction Word) 마이크로프로세서, 또는 다른 명령어 세트를 구현하는 프로세서 또는 명령어 세트의 조합을 구현하는 프로세서를 포함할 수 있다. 프로세싱 장치(702)는 또한, ASIC(application-specific integrated circuit), FPGA(field programmable gate array), DSP(디지털 신호 프로세서), 네트워크 프로세서 등과 같은 하나 이상의 특수 목적 처리 장치를 포함할 수 있다. 처리 장치(702)는 본 명세서에서 논의된 작동 및 단계를 수행하기 위한 명령어(726)를 실행하도록 구성된다.

[0085] 컴퓨팅 장치(700)는 네트워크(718)와 통신할 수 있는 네트워크 인터페이스 장치(722)를 더 포함할 수 있다. 컴퓨팅 장치(700)는 또한, 디스플레이 장치(710)(예를 들어, 액정 디스플레이(LCD) 또는 음극선관(CRT)), 영숫자 입력 장치(712)(예를 들어, 키보드), 커서 제어 장치(714)(예를 들어, 마우스) 및 신호 생성 장치(720)(예를 들어, 스피커)를 포함한다. 적어도 일 실시예에서, 디스플레이 장치(710), 영숫자 입력 장치(712), 및 커서 제어 장치(714)는 단일 구성요소 또는 장치(예를 들어, LCD 터치 스크린)로 조합될 수 있다.

[0086] 데이터 저장 장치(716)는 본 명세서에서 설명된 방법 또는 기능 중 임의의 하나 이상을 구현하는 명령어(726)의 하나 이상의 세트가 저장된 컴퓨터 판독가능 저장 매체(724)를 포함할 수 있다. 명령어(726)는 또한, 컴퓨터 판독 가능 매체를 구성하는 컴퓨팅 장치(700), 메인 메모리(704) 및 프로세싱 장치(702)에 의한 실행 동안 메인 메모리(704) 및/또는 처리 장치(702) 내에 완전히 또는 적어도 부분적으로 상주할 수 있다. 명령어는 네트워크 인터페이스 장치(722)를 통해 네트워크(718)를 통해 추가로 전송 또는 수신될 수 있다.

[0087] 컴퓨터 판독 가능 저장 매체(726)가 예시적인 실시예에서 단일 매체인 것으로 도시되어 있지만, "컴퓨터 판독 가능 저장 매체"라는 용어는 하나 이상의 명령어 세트를 저장하는 단일 매체 또는 다중 매체(예를 들어, 중앙 집중식 또는 분산형 데이터베이스 및/또는 관련 캐시 및 서버)를 포함할 수 있다. "컴퓨터 판독 가능 저장 매체"라는 용어는 또한, 기계에 의한 실행을 위한 명령 세트를 저장, 인코딩 또는 전달할 수 있고 기계가 본 개시의 방법 중 임의의 하나 이상을 수행하게 하는 임의의 매체를 포함할 수 있다. 따라서 "컴퓨터 판독 가능 저장 매체"라는 용어는 고체 상태 메모리, 광학 매체 및 자기 매체를 포함하지만, 이에 제한되지 않는 것으로 간주될 수 있다.

[0088] 일 예에서, 상기 방법은 엔드포인트 장치에 대한 고유 식별자를 생성하는 것을 포함할 수 있다. 고유 식별자는 엔드포인트 장치에 고유할 수 있으며 적어도 하나의 반-신뢰할 수 있는 당사자와 함께 엔드포인트 장치를 식별하도록 구성될 수 있다. 고유 식별자는 엔드포인트 장치의 MAC 주소와 네트워크 운영자에게 알려진 운영자 비밀 둘 다를 기반으로 하는 해시된 값일 수 있다. 상기 방법은 고유 식별자를 다른 장치와 공유하는 것을 포함할 수 있다.

[0089] 몇몇 양태들에서, MAC 주소는 엔드포인트 장치의 하드웨어에 의해 정의될 수 있다. 고유 식별자는 무선으로 공유될 수 있다. 고유 식별자는 네트워크 사업자가 운영하는 네트워크를 통해 공유될 수 있다.

[0090] 고유 식별자는 알고리즘 id = hash(operatorSecret, deviceMacAddress)에 따라 생성될 수 있으며, 여기서 id는 고유 식별자, hash는 해싱 알고리즘, operatorSecret은 네트워크 운영자가 알고 있는 비밀, deviceMacAddress는 엔드포인트 장치의 하드웨어에서 정의한 MAC 주소이다. 해싱 알고리즘은 SHA(Secure Hash Algorithm)일 수 있다.

[0091] 고유 식별자는 제 3자가 이해하지 못할 수 있으며 네트워크 운영자가 엔드포인트 장치에 연결할 수 있다. 고유 식별자는 엔드포인트 장치에서 생성될 수 있다. 상기 방법은 네트워크 운영자에서 고유 식별자를 재계산하는 단계를 포함할 수 있다. 고유 식별자를 다른 장치와 공유하는 것은 고유 식별자를 네트워크 운영자가 소유한 다른 장치에 전송하는 것을 포함할 수 있다.

[0092] 상기 방법은 운영자 비밀을 교체하는 단계를 포함할 수 있다. 운영자 비밀은 네트워크 운영자에게 알려진 순환 알고리즘을 기반으로 순환될 수 있다. 순환 알고리즘은 네트워크 운영자에게 알려진 미리 정의된 매개변수를 포함할 수 있다.

[0093] 다른 예에서, 상기 방법은 네트워크 운영자에게 알려진 운영자 비밀을 교체하고, 엔드포인트 장치에 대한 고유 식별자를 생성하고, 고유 식별자를 다른 장치와 공유하는 것을 포함할 수 있다. 고유 식별자는 엔드포인트 장치에 고유할 수 있고 엔드포인트 장치를 식별하도록 구성될 수 있다. 고유 식별자는 운영자 비밀 및 엔드포인트 장치의 식별자를 기반으로 할 수 있다.

[0094] 엔드포인트 장치의 식별자는 MAC 주소일 수 있다. MAC 주소는 엔드포인트 장치의 하드웨어에 의해 정의될 수 있다. 운영자 비밀은 네트워크 운영자에게 알려질 수 있다. 고유 식별자는 네트워크 사업자가 운영하는 네트워크를 통해 무선으로 공유될 수 있다.

[0095] 고유 식별자는 알고리즘 id = hash(operatorSecret, deviceMacAddress)에 따라 생성될 수 있으며, 여기서 id는 고유 식별자, hash는 해싱 알고리즘, operatorSecret은 네트워크 운영자가 알고 있는 비밀, deviceMacAddress는 엔드포인트 장치의 하드웨어에서 정의한 MAC 주소이다. 해싱 알고리즘은 SHA(Secure Hash Algorithm)일 수 있다.

[0096] 본 명세서, 특히 첨부된 청구범위에서 사용된 용어(예를 들어, 첨부된 청구범위의 본문)는 일반적으로 "개방형" 용어로 의도된다(예를 들어, "포함하는"이라는 용어는 "포함하지만 이에 제한되지 않는"으로 해석될 수 있으며, "가지는"이라는 용어는 "적어도 가진"으로 해석될 수 있고, "포함하다"라는 용어는 "포함하지만 이에 제한되지 않는" 등으로 해석될 수 있다.

[0097] 또한, 특정 수의 도입된 청구항 인용을 의도하는 경우, 그러한 의도는 청구항에서 명시적으로 인용되며, 그러한 인용이 없을 경우 그러한 의도는 존재하지 않는다. 예를 들어, 이해를 돕기 위해서 다음 첨부된 청구범위에는 청구항 인용을 도입하기 위해서 "적어도 하나" 및 "하나 이상"이라는 도입 문구의 사용이 포함될 수 있다. 그러나 동일한 청구항에 "하나 이상" 또는 "적어도 하나"라는 도입구와 "a" 또는 "an"과 같은 부정관사가 포함되더라도(예를 들어, "a" 및/또는 "an"은 "적어도 하나" 또는 "하나 이상"을 의미하는 것으로 해석될 수 있음), 그러한 문구의 사용은 부정관사("a" 또는 "an")에 의한 청구항 인용의 도입이 그러한 도입된 청구항 인용을 포함하는 특정 청구범위를 그러한 인용을 하나만 포함하는 것으로 제한한다는 의미로 해석되어서는 안 되며, 청구항 인용을 도입하는데 사용되는 정관사를 사용하는 경우에도 마찬가지이다.

[0098] 또한, 도입된 청구항 인용의 특정 수가 명시적으로 인용된 경우에도, 당업자는 그러한 인용이 적어도 인용된 수를 의미하는 것으로 해석될 수 있음을 인식할 것이다(예를 들어, 다른 수식어 없이 "두 개 인용"은 적어도 2 개 인용 또는 2 개 이상 인용을 의미한다). 또한, "A, B, C 등 중 적어도 하나" 또는 또는 "A, B, C 등 중 하나 이상"과 유사한 관행이 있는 경우, 일반적으로 그러한 구성은 A 단독, B 단독, C 단독, A와 B를 함께, A와 C를 함께, B와 C를 함께, 또는 A, B 및 C를 함께 등을 포함하도록 의도된다. 예를 들어, "및/또는"이라는 용어의 사용은 이러한 방식으로 구성되도록 의도된다.

[0099] 또한, 설명, 청구범위 또는 도면에서 둘 이상의 대안적인 용어를 제시하는 임의의 분리 단어 또는 구는 용어 중 하나, 용어 중 하나 또는 두 용어 모두를 포함하는 가능성을 고려하는 것으로 이해될 수 있다. 예를 들어, "A 또는 B"라는 문구는 "A" 또는 "B" 또는 "A 및 B"의 가능성을 포함하는 것으로 이해될 수 있다.

[0100] 본 명세서에 설명된 실시예는 컴퓨터 실행 가능 명령어 또는 데이터 구조가 저장되어 있거나 전달하기 위한 컴퓨터 판독 가능 매체를 사용하여 구현될 수 있다. 그러한 컴퓨터 판독 가능 매체는 범용 또는 특수 목적 컴퓨터에 의해 액세스될 수 있는 임의의 이용 가능한 매체일 수 있다. 예로서 그리고 그에 제한됨이 없이, 그러한 컴퓨터 판독 가능 매체는 RAM(Random Access Memory), ROM(Read-Only Memory), EEPROM(Electrically Erasable Programmable Read-Only Memory: 전기적 소거 및 프로그램 가능 읽기 전용 메모리), CD-ROM(Compact Disc Read-Only Memory) 또는 기타 광학 디스크 저장 장치, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 플래시 메모리 장치(예를 들어, 솔리드 스테이트 메모리 장치), 또는 컴퓨터 실행 가능 명령어 또는 데이터 구조의 형태로 원하는 프로그램 코드를 휴대하거나 저장하는데 사용될 수 있고 범용 또는 특수 목적 컴퓨터에서 액세스할 수 있는 임의의 다른 저장 매체를 포함하는 비-일시적 컴퓨터 판독 가능 저장 매체를 포함할 수 있지만 이에 제한되지 않는다. 위의 조합은 또한, 컴퓨터 판독 가능 매체의 범주 내에 포함될 수 있다.

[0101] 컴퓨터 실행 가능 명령은 예를 들어, 범용 컴퓨터, 특수 목적 컴퓨터 또는 특수 목적 프로세싱 장치(예를 들어, 하나 이상의 프로세서)가 특정 기능 또는 기능 그룹을 수행하게 하는 명령어 및 데이터를 포함할 수 있다. 요

지가 구조적 특징 및/또는 방법론적 행위에 특정한 언어로 설명되지만, 첨부된 청구범위에 정의된 요지가 반드시 위에서 설명된 특정 특징 또는 행위로 제한되지 않는다는 것을 이해해야 한다. 오히려, 위에서 설명된 특정 특징 및 작용은 청구범위를 구현하는 예시적인 형태로 개시된다.

[0102] 본 명세서에서 사용된 용어 "모듈" 또는 "구성요소"는 컴퓨팅 시스템의 범용 하드웨어(예를 들어, 컴퓨터 판독 가능 매체, 처리 장치 등)에 저장 및/또는 실행될 수 있는 모듈 또는 구성요소 및/또는 소프트웨어 객체 또는 소프트웨어 루틴의 작업을 수행하도록 구성된 특정 하드웨어 구현을 지칭할 수 있다. 몇몇 실시예에서, 본 명세서에서 설명된 다른 구성요소, 모듈, 엔진 및 서비스는 컴퓨팅 시스템(예를 들어, 별도의 스레드)에서 실행되는 객체 또는 프로세스로 구현될 수 있다. 본 명세서에서 설명된 시스템 및 방법 중 일부는 일반적으로 소프트웨어로 구현되는 것으로 설명되지만(범용 하드웨어에 저장 및/또는 실행됨), 특정 하드웨어 구현 또는 소프트웨어와 특정 하드웨어 구현의 조합도 가능하고 고려된다. 이러한 설명에서, "컴퓨팅 엔티티(computing entity)"는 이전에 정의된 바와 같은 임의의 컴퓨팅 시스템, 또는 컴퓨팅 시스템에서 실행되는 임의의 모듈 또는 변조기의 조합일 수 있다.

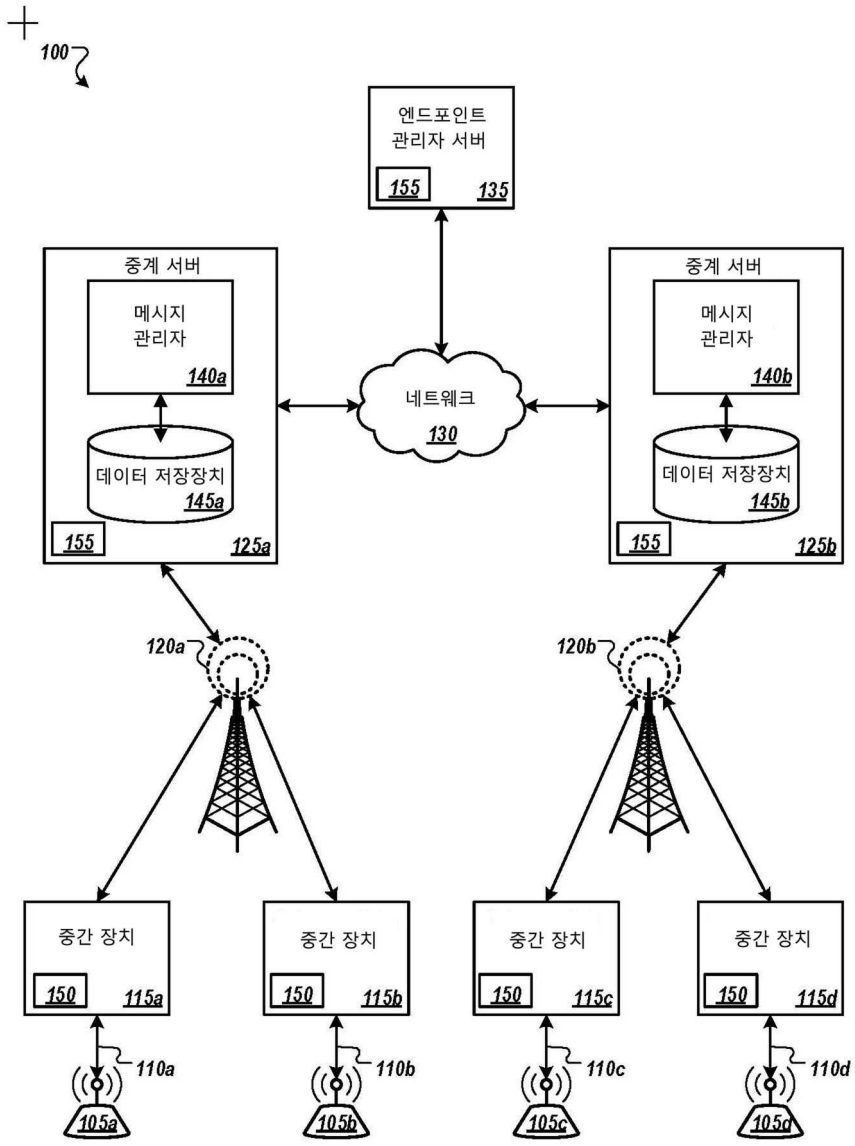
[0103] 개시된 프로세스 및/또는 방법에 대해, 프로세스 및 방법에서 수행되는 기능은 문맥에 의해 지시될 수 있는 바와 같이 상이한 순서로 구현될 수 있다. 또한, 요약된 단계 및 작동은 예시로만 제공되며, 일부 단계 및 작동은 선택 사항이거나 더 적은 수의 단계 및 작동으로 조합되거나 추가 단계 및 작동으로 확장될 수 있다.

[0104] 본 개시는 때때로 상이한 다른 구성요소 내에 포함되거나 이들과 연결된 상이한 구성요소를 예시할 수 있다. 그러한 도시된 구성은 단지 예시일 뿐이며, 동일하거나 유사한 기능을 달성하는 많은 다른 구성이 구현될 수 있다.

[0105] 본 개시의 양태는 그 사상 또는 본질적인 특징을 벗어남이 없이 다른 형태로 구현될 수 있다. 설명된 양태는 모든 면에서 예시적인 것으로 간주되어야 하며 제한적인 것이 아니다. 청구된 요지는 전술한 설명보다는 첨부된 청구범위에 의해 나타난다. 청구범위의 동등성의 의미 및 범위 내에서 발생하는 모든 변경은 그들의 범주 내에 포함되어야 한다.

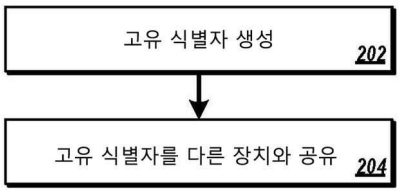
도면

도면1


100
엔드포인트
관리자 서버
155
135
중계 서버
메시지
관리자
140a
데이터 저장장치
145a
155
125a
네트워크
130
중계 서버
메시지
관리자
140b
데이터 저장장치
145b
155
125b
120a
120b
중간 장치
150
115a
중간 장치
150
115b
중간 장치
150
115c
중간 장치
150
115d
110a
110b
110c
110d
105a
105b
105c
105d

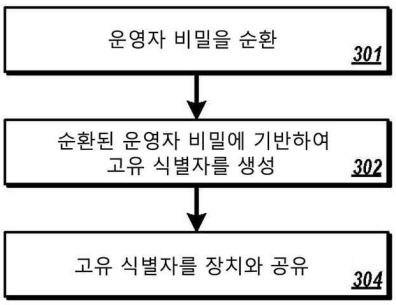
도면2


200

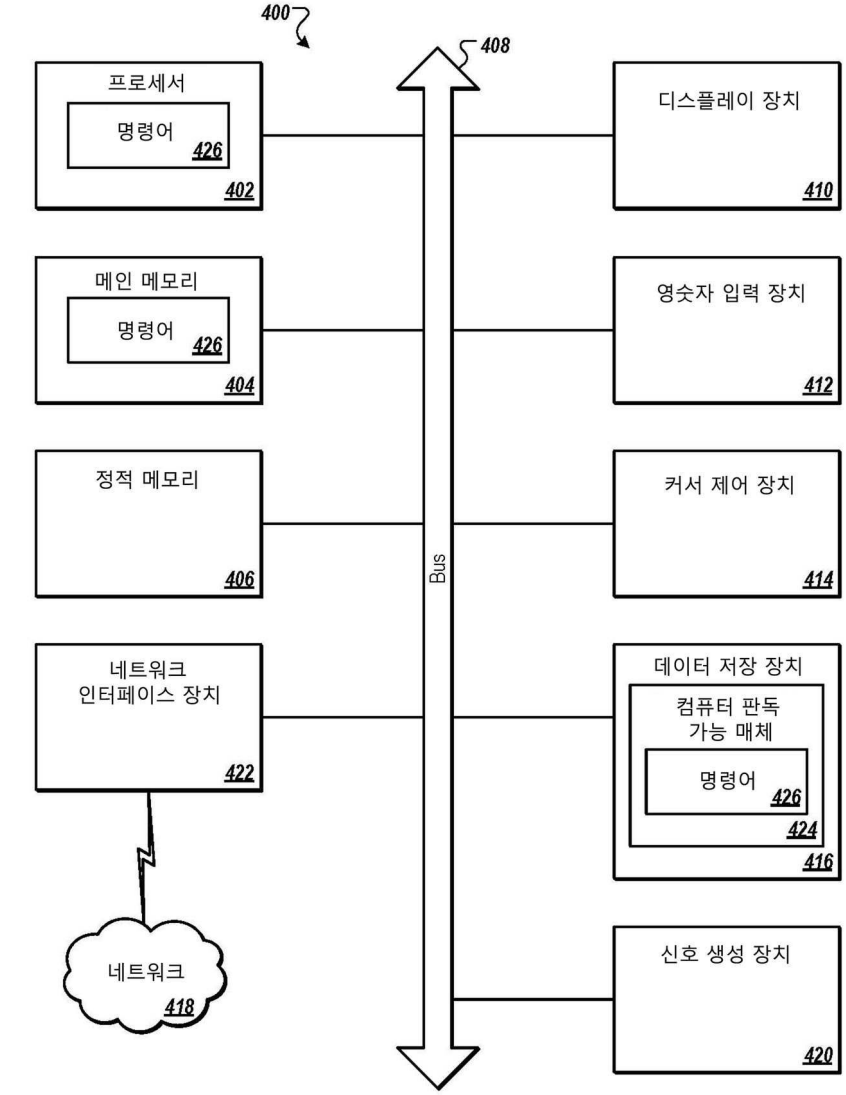

고유 식별자 생성
202
고유 식별자를 다른 장치와 공유
204

도면3


300


운영자 비밀을 순환
301
순환된 운영자 비밀에 기반하여
고유 식별자를 생성
302
고유 식별자를 장치와 공유
304

도면4


400
408
프로세서
명령어
426
402
메인 메모리
명령어
426
404
정적 메모리
406
네트워크
인터페이스 장치
422
네트워크
418
Bus
디스플레이 장치
410
영숫자 입력 장치
412
커서 제어 장치
414
데이터 저장 장치
컴퓨터 판독
가능 매체
명령어
426
424
416
신호 생성 장치
420