(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년03월06일
(11) 등록번호 10-1712158
(24) 등록일자 2017년02월24일

(51) 국제특허분류(Int. Cl.)
*H04W 4/00* (2009.01) *H04W 12/06* (2009.01)
*H04W 12/08* (2009.01) *H04W 12/10* (2009.01)
(21) 출원번호 10-2014-7010758(분할)
(22) 출원일자(국제) 2010년12월28일
심사청구일자 2015년12월23일
(85) 번역문제출일자 2014년04월22일
(65) 공개번호 10-2014-0074357
(43) 공개일자 2014년06월17일
(62) 원출원 특허 10-2012-7020010
원출원일자(국제) 2010년12월28일
심사청구일자 2012년07월30일
(86) 국제출원번호 PCT/US2010/062196
(87) 국제공개번호 WO 2011/082150
국제공개일자 2011년07월07일
(30) 우선권주장
61/290,482 2009년12월28일 미국(US)
*(뒷면에 계속)*
(56) 선행기술조사문헌
KR1020070100580 A*
KR1020090124979 A
JP2004171274 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
**인터디지탈 패튼 홀딩스, 인크**
미국, 델라웨어주 19809, 윌밍턴, 벨뷰 파크웨이 200, 스위트 300
(72) 발명자
**파타르 수디르 비**
미국 뉴저지주 08054 마운트 로렐 앤 드라이브 17
**차 인혁**
대한민국 서울 137 830 강남구 14-1 삼성동 102동 202-에이치 중앙 헤이츠 빌리지
*(뒷면에 계속)*
(74) 대리인
**김태홍**

전체 청구항 수 : 총 28 항 심사관 : 양종필

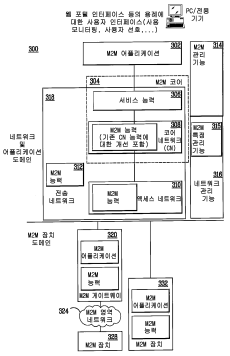
(54) 발명의 명칭 **사물 지능 통신 게이트웨이 아키텍처**

## (57) 요 약

복수의 장치에 서비스를 제공하기 위해 네트워크 도메인 외부에 게이트웨이를 제공하는 시스템, 방법 및 수단이 개시된다. 예를 들면, 게이트웨이는 관리 엔티티 또는 네트워크 도메인을 위한 프록시로서 동작할 수 있다. 관리 엔티티로서, 게이트웨이는 복수의 장치 각각에 관한 보안 기능을 행할 수 있다. 게이트웨이는 네트워크 도메

(뒷면에 계속)

*대 표 도* - 도3



인이 참여하지 않거나 특정 장치에 대한 지식을 갖지 않고도 보안 기능을 수행할 수 있다. 네트워크를 위한 프록시로서, 게이트웨이는 복수의 장치 각각에 관한 보안 기능을 수행하도록 네트워크 도메인으로부터 명령을 수신할 수 있다. 네트워크는 복수의 장치 각각의 아이덴티티를 알 수 있다. 게이트웨이는 복수의 장치 각각에 대해 보안 기능을 수행하고 관련 정보를 종합한 후 네트워크 도메인으로 전송할 수 있다.

(72) 발명자

**샤 요겐드라 씨**

미국 펜실베니아주 19341 엑스톤 리젠시 코트 10

**슈미트 안드레아스**

독일 65929 프랑크푸르트 암 마인 투토넨베그 37

**레이처 안드레아스**

독일 60385 프랑크푸르트 하이데스트라쎄 131

**치트라푸 프라바카 알**

미국 펜실베니아주 19422 블루 벨 브로찬트 드라이브 135

**케이스 로렌스**

미국 텍사스주 78734 오스틴 티모시 서클 5002

(30) 우선권주장

61/293,599 2010년01월08일 미국(US)

61/311,089 2010년03월05일 미국(US)

# 명 세 서

## 청구범위

### 청구항 1

네트워크 도메인 외부의 사물지능통신(machine-to-machine: M2M) 게이트웨이에 의해, 상기 네트워크 도메인의 특정 기능을 상기 M2M 게이트웨이에 분담(offloading)시키는 방법에 있어서,

관리 엔티티로서 네트워크 도메인과 신뢰를 구축하는 단계;

복수의 M2M 장치 각각과의 연결을 구축하는 단계;

상기 네트워크 도메인의 제어와 독립적으로, 상기 복수의 M2M 장치 각각에 대해 보안 기능을 수행하는 단계; 및

상기 복수의 M2M 장치 각각에 관하여 상기 네트워크 도메인에 정보를 리포팅(report)하는 단계

를 포함하는 네트워크 도메인의 특정 기능 분담 방법.

### 청구항 2

제1항에 있어서, 상기 정보는 상기 복수의 M2M 장치 각각으로부터 종합되는(aggregated) 것인 네트워크 도메인의 특정 기능 분담 방법.

### 청구항 3

삭제

### 청구항 4

제1항에 있어서, 상기 리포팅하는 단계는 상기 네트워크 도메인으로부터의 요청에 응답하는 것인, 네트워크 도메인의 특정 기능 분담 방법.

### 청구항 5

제1항에 있어서, 상기 리포팅하는 단계는 주기적으로 수행되는 것인, 네트워크 도메인의 특정 기능 분담 방법.

### 청구항 6

제1항에 있어서, 상기 보안 기능은 상기 네트워크 도메인에 상기 복수의 M2M 장치 각각을 등록하고 인증하는(authenticate) 것을 포함하는 것인 네트워크 도메인의 특정 기능 분담 방법.

### 청구항 7

제6항에 있어서, 상기 등록 및 인증은 부트스트래핑된 크리덴셜(bootstrapped credential)을 이용하는 것을 포함하는 것인 네트워크 도메인의 특정 기능 분담 방법.

### 청구항 8

제1항에 있어서, 상기 보안 기능은 상기 복수의 M2M 장치 각각에 크리덴셜의 제공(provisioning) 및 이송(migration)을 포함하는 것인 네트워크 도메인의 특정 기능 분담 방법.

### 청구항 9

제1항에 있어서, 상기 보안 기능은 상기 복수의 M2M 장치 각각에 보안 정책을 제공하는 것을 포함하는 것인 네트워크 도메인의 특정 기능 분담 방법.

### 청구항 10

제1항에 있어서, 상기 보안 기능은 상기 복수의 M2M 장치 각각에 신뢰할만한 기능(functionality)을 구축하는 것을 포함하고, 상기 복수의 M2M 장치 각각에 대한 무결성 검증(integrity validation)이 수행되는 것인, 네트

워크 도메인의 특정 기능 분담 방법.

**청구항 11**

제1항에 있어서, 상기 보안 기능은 상기 복수의 M2M 장치 각각에 대해 장치 관리를 제공하는 것을 포함하는 것인 네트워크 도메인의 특정 기능 분담 방법.

**청구항 12**

제1항에 있어서, 상기 보안 기능은, 상기 복수의 M2M 장치 각각에 대해 무결성 검증(integrity validatioin)을 수행하고,

상기 복수의 M2M 장치 중 하나 이상의 장치가 무결성 검증에 실패하면, 상기 하나 이상의 M2M 장치의 리스트를 상기 네트워크 도메인에 전송하는 것인 네트워크 도메인의 특정 기능 분담 방법.

**청구항 13**

제1항에 있어서, 상기 보안 기능은 상기 복수의 M2M 장치 중 적어도 하나에 대해, 보안 연관, 통신 채널 또는 통신 링크 중 적어도 하나를 구축하는 것을 포함하는 것인 네트워크 도메인의 특정 기능 분담 방법.

**청구항 14**

제1항에 있어서,

상기 복수의 M2M 장치 중 하나 이상의 장치에 연관된 무결성 위반(integrity breach) 또는 실패를 결정하는 단계와;

상기 복수의 M2M 장치 중 상기 하나 이상의 장치를 격리(quarantining)시키는 단계

를 더 포함하는 네트워크 도메인의 특정 기능 분담 방법.

**청구항 15**

제1항에 있어서, 상기 보안 기능은 네트워크 도메인 참여없이 상기 네트워크 도메인을 대행하여 수행되는 것인 네트워크 도메인의 특정 기능 분담 방법.

**청구항 16**

네트워크 도메인의 외부에 있는 사물지능통신 (machine-to-machine: M2M) 게이트웨이에 있어서,

관리 엔티티로서 네트워크 도메인과 신뢰를 구축하고;

상기 네트워크 도메인과 연관된 복수의 M2M 장치 각각과의 연결을 구축하고;

상기 네트워크 도메인의 제어와는 독립적으로, 상기 복수의 M2M 장치 각각에 대해 보안 기능을 수행하며;

상기 복수의 M2M 장치 각각에 관하여 상기 네트워크 도메인에 정보를 리포팅하도록 구성되는 M2M 게이트웨이.

**청구항 17**

제16항에 있어서, 상기 정보는 상기 복수의 M2M 장치 각각으로부터 종합되는 것인 M2M 게이트웨이.

**청구항 18**

삭제

**청구항 19**

제16항에 있어서, 상기 리포팅은 상기 네트워크 도메인으로부터의 요청에 응답하는 것인 M2M 게이트웨이.

**청구항 20**

제16항에 있어서, 상기 리포팅은 주기적으로 수행되는 것인 M2M 게이트웨이.

**청구항 21**

제16항에 있어서, 상기 보안 기능은 상기 네트워크 도메인에 상기 복수의 M2M 장치 각각을 등록하고 인증하는 것을 포함하는 것인 M2M 게이트웨이.

**청구항 22**

제21항에 있어서, 상기 등록 및 인증은 부트스트래핑된 크리덴셜을 이용하는 것을 포함하는 것인 M2M 게이트웨이.

**청구항 23**

제16항에 있어서, 상기 보안 기능은 상기 복수의 M2M 장치 각각에 크리덴셜의 제공 및 이송을 포함하는 것인 M2M 게이트웨이.

**청구항 24**

제16항에 있어서, 상기 보안 기능은 상기 복수의 M2M 장치 각각에 보안 정책을 제공하는 것을 포함하는 것인 M2M 게이트웨이.

**청구항 25**

제16항에 있어서, 상기 보안 기능은 상기 복수의 M2M 장치 각각에 신뢰할만한 기능을 구축하는 것을 포함하고, 상기 복수의 M2M 장치 각각에 대한 무결성 검증이 수행되는 것인 M2M 게이트웨이.

**청구항 26**

제16항에 있어서, 상기 보안 기능은 상기 복수의 M2M 장치 각각에 대해 장치 관리를 제공하는 것을 포함하는 것인 M2M 게이트웨이.

**청구항 27**

제16항에 있어서, 상기 보안 기능은, 상기 복수의 M2M 장치 각각에 대해 무결성 검증(integrity validatioin)을 수행하고,

상기 복수의 M2M 장치 중 하나 이상의 장치가 무결성 검증에 실패하면, 상기 하나 이상의 M2M 장치의 리스트를 상기 네트워크 도메인에 전송하는 것인 M2M 게이트웨이.

**청구항 28**

제16항에 있어서, 상기 보안 기능은 상기 복수의 M2M 장치 중 적어도 하나에 대해, 보안 연관, 통신 채널 또는 통신 링크 중 적어도 하나를 구축하는 것을 포함하는 것인 M2M 게이트웨이.

**청구항 29**

제16항에 있어서, 상기 M2M 게이트웨이는 또한,

상기 복수의 M2M 장치 중 하나 이상의 장치에 연관된 무결성 위반 또는 실패를 결정하고;

상기 복수의 M2M 장치 중 상기 하나 이상의 장치를 격리시키도록 구성되는 것인, M2M 게이트웨이.

**청구항 30**

제16항에 있어서, 상기 보안 기능은 네트워크 도메인 참여없이 상기 네트워크 도메인을 대행하여 수행되는 것인 M2M 게이트웨이.

## *발명의 설명*

### *기 술 분 야*

[0001] 본 출원은 사물 지능 통신 게이트웨이 아키텍처에 관한 것이다.

## 배 경 기 술

[0002] 관련 출원의 상호 참조

[0003] 본 출원은 그 내용이 참조로 여기에 포함되는 2009년 12월 28일자 출원된 미국 가특허 출원 번호 제61/290,482호, 2010년 1월 8일자 출원된 미국 가특허 출원 번호 제61/293,599호, 2010년 3월 5일자 출원된 미국 가특허 출원 번호 제61/311,089호을 기초로 하고 해당 출원들에 대한 우선권을 주장한다.

[0004] 배경기술

[0005] 사물 지능 통신(machine-to-machine: M2M) 아키텍처는 네트워크 및 어플리케이션 도메인에 대한 M2M 장치 연동 및 상호 접속을 보장하는 M2M 능력(capability)을 이용한 장비로서 기술될 수 있는 M2M 게이트웨이를 사용할 수 있다. M2M 게이트웨이는 또한 M2M 어플리케이션을 구동할 수 있고 M2M 장치와 함께 배치될 수 있다. 현재의 M2M 게이트웨이 아키텍처는 단점을 가지고 있다.

## 발명의 내용

### 해결하려는 과제

[0006] 복수의 장치에 서비스를 제공하기 위해 네트워크 도메인 외부에 게이트웨이를 제공하는 시스템, 방법 및 수단이 개시된다. 게이트웨이는 네트워크 도메인을 위한 장치에 서비스 능력을 제공할 수 있고, 이는 네트워크 도메인에 의해 제공될 필요가 있을 수 있는 기능을 감소시킬 수 있다.

### 과제의 해결 수단

[0007] 게이트웨이는 관리 엔티티로서 작용할 수 있다. 게이트웨이는 네트워크 도메인에 대해 신뢰를 구축할 수 있다. 예를 들면, 게이트웨이는 게이트웨이가 네트워크 도메인과 상호 작용하도록 하기 위해 네트워크 도메인에 대해 일정 수준의 신뢰를 형성할 수 있다. 게이트웨이는 복수의 장치 각각에 대한 연결을 구축할 수 있다. 게이트웨이는 각각의 장치에 관한 보안 기능을 행할 수 있다. 게이트웨이는 네트워크 도메인을 위한 것일 수 있는 보안 기능을 행할 수 있다. 게이트웨이는 네트워크 도메인이 직접 참여하지 않거나 최소한으로 참여하여 보안 기능을 수행할 수 있다. 게이트웨이는 네트워크가 특정 장치에 대한 지식을 갖지 않고도 보안 기능을 수행할 수 있다. 게이트웨이는 각각의 장치에 관한 네트웨크 도메인에 장치 정보를 리포팅(report)할 수 있다.

[0008] 게이트웨이는 네트워크를 위한 프록시로서 작용할 수 있다. 게이트웨이는 네트워크 도메인에 대해 신뢰를 구축할 수 있다. 예를 들면, 게이트웨이는 게이트웨이가 네트워크 도메인과 상호 작용하도록 하기 위해 네트워크 도메인에 대해 일정 수준의 신뢰를 형성할 수 있다. 게이트웨이는 복수의 장치 각각에 관한 보안 기능을 수행하도록 네트워크 도메인으로부터 명령을 수신할 수 있다. 예를 들면, 게이트웨이는 네트워크 도메인으로부터 단일 명령을 수신할 수 있고, 이에 응하여 다중 장치에 대한 보안 기능을 수행할 수 있다. 네트워크는 복수의 장치 각각의 아이덴티티를 인지할 수 있다. 게이트웨이는 복수의 장치 각각에 대해 보안 기능을 수행할 수 있다. 게이트웨이는 수행된 보안 기능에 관련된 복수의 장치 각각으로부터 정보를 종합한 후 해당 종합된 정보를 네트워크 도메인으로 전송할 수 있다. 게이트웨이는 종합된 정보를 처리한 후 해당 처리된 종합 정보를 네트워크 도메인으로 전송할 수 있다.

[0009] 게이트웨이에 의해 수행되는 보안 기능은 다음 중 하나 이상을 포함할 수 있다: 부트스트래핑된 크리덴셜(boostrapped credentials)을 사용하거나 사용하지 않고 네트워크 도메인에의 장치의 등록 및 인증; 크리덴셜의 제공 및 복수의 장치로의 이송(migration); 복수의 장치 각각으로의 보안 정책 제공; 복수의 장치 각각의 인증 수행; 복수의 장치 각각에 신뢰할만한 기능성을 설정하는 기능으로서, 복수의 장치 각각에 대해 무결성 검증(integrity validation)이 수행되는, 기능성 설정; 복수의 장치 각각에 대해, 결함 탐색 및 결함 교정을 포함할 수 있는 장치 관리의 제공; 또는 복수의 장치 중 적어도 하나에 대해, 보안 연관(security association), 통신 채널 또는 통신 링크 중 적어도 하나를 설정.

### 발명의 효과

[0010] 복수의 장치에 서비스를 제공하기 위해 네트워크 도메인 외부에 게이트웨이를 제공하는 시스템, 방법 및 수단이 개시된다. 게이트웨이는 네트워크 도메인을 위한 장치에 서비스 능력을 제공할 수 있고, 이는 네트워크 도메인에 의해 제공될 필요가 있을 수 있는 기능을 감소시킬 수 있다.

## 도면의 간단한 설명

[0011] 하기의 첨부 도면과 함께 예시로써 주어진 아래의 설명으로부터 보다 구체적으로 이해할 수 있다. 도면에서:

도 1은 예시적인 무선 통신 시스템을 나타내며;

도 2는 예시적인 WTRU 및 노드-B를 나타내며;

도 3은 예시적인 M2M 아키텍쳐를 나타내며;

도 4는 예시적인 케이스 3의 게이트웨이 기능성을 나타내며;

도 5는 케이스 3의 접속 장치에 대한 예시적인 부트스트래핑 및 등록 흐름을 나타내며;

도 6은 케이스 4의 접속 장치에 대한 예시적인 부트스트래핑 및 등록 흐름을 나타내며;

도 7은 예시적인 계층적 연결 아키텍쳐를 나타내며;

도 8은 케이스 3과 4의 장치 무결성 검증을 위한 예시적인 호 흐름 다이어그램을 나타내며;

도 9는 케이스 1의 장치 무결성 및 등록을 위한 예시적인 호 흐름 다이어그램을 나타내며;

도 10은 케이스 2의 장치 및 게이트웨이 무결성 및 등록을 위한 예시적인 호 흐름 다이어그램을 나타내며;

도 11은 케이스 3의 장치 및 게이트웨이 무결성 및 등록을 위한 예시적인 호 흐름 다이어그램을 나타내며;

도 12는 케이스 4의 장치 및 게이트웨이 무결성 및 등록을 위한 예시적인 호 흐름 다이어그램을 나타내며;

도 13은 계층화된 검증을 위한 예시적인 시나리오를 나타내며;

도 14는 예시적인 M2M 아키텍쳐를 나타내며;

도 15는 M2M 네트워크 계층의 서비스 능력의 예시적인 아키텍쳐를 나타내며;

도 16a 및 도 16b는 M2M 게이트웨이 및 인터페이스의 예시적인 아키텍쳐를 나타내며;

도 17a는 하나 이상의 개시된 실시예가 구현된 예시적인 통신 시스템의 시스템 다이어그램이고;

도 17b는 도 17a에 예시된 통신 시스템 내에 사용될 수 있는 예시적인 무선 송수신 유닛(WTRU)의 시스템 다이어그램이고;

도 17c는 도 17a에 예시된 통신 시스템 내에 사용될 수 있는 예시적인 무선 액세스 네트워크와 예시적인 코어 네트워크의 시스템 다이어그램이다.

## 발명을 실시하기 위한 구체적인 내용

[0012] 도 1 내지 도 17은 개시된 시스템, 방법 및 수단이 구현될 수 있는 예시적인 실시예에 관한 것일 수 있다. 그러나, 본 발명은 예시적인 실시예와 관련하여 설명되지만, 그것에 한정되지 않으며, 다른 실시예들도 사용될 수 있거나, 개시된 실시예를 벗어나지 않고 본 발명의 동일한 기능을 수행하기 위해 설명된 실시예에 대해 변형 또는 부가를 행할 수 있음을 이해하여야 한다. 예를 들면, 개시된 시스템, 방법 및 수단은 M2M 구성을 참조로 예시될 수 있지만, 구성은 그것에 한정되지 않는다. 추가로, 개시된 시스템, 방법 및 수단은 무선 방식의 구성을 참조로 예시될 수 있지만, 구성은 그에 한정되지 않는다. 예를 들면, 개시된 시스템, 방법 및 수단은 유선 통신에 적용될 수 있다. 또한, 도면에는 호 흐름이 예시될 수 있지만, 이는 예시적임을 의미한다. 다른 실시예들도 사용될 수 있음을 알아야 한다. 또한, 흐름도 순서는 적절한 경우 변경될 수 있다. 추가로, 흐름은 필요치 않은 경우 생략될 수 있고 추가의 흐름을 추가할 수 있다.

[0013] 이후의 설명을 참조하면, "무선 송수신 유닛(WTRU)"이란 용어는 한정되는 것은 아니지만 사용자 장비(UE), 이동국(mobile station), 고정 및 이동 가입자 유닛, 페이저, 휴대 전화, 휴대 정보 단말기(PDA), 컴퓨터 또는 무선 환경에서 동작할 수 있는 임의의 다른 종류의 사용자 장치를 포함할 수 있다. 이후의 설명을 참조하면, "기지국(base station)"이란 용어는 한정되는 것은 아니지만 노드-B, 사이트-컨트롤러(site-controller), 액세스 포인트(AP) 또는 무선 환경에서 동작될 수 있는 임의의 다른 종류의 인터페이싱 장치를 포함할 수 있다.

[0014] 도 1은 복수의 WTRU(110), 노드-B(120)와 같은 기지국, 컨트롤링 무선 네트워크 제어기(CRNC)(130), 서빙 무선 네트워크 제어기(SRNC)(140) 및 코어 네트워크(150)를 포함하는 예시적인 무선 통신 시스템(100)을 보여준다.

노드-B(120)와 CRNC(130)는 총괄적으로 UTRAN으로 지칭될 수 있다.

[0015] 도 1에 도시된 바와 같이, WTRU(110)는 CRNC(130) 및 SRNC(140)와 연결된 노드-B(120)와 연결될 수 있다. 도 1에는 3개의 WTRU(110), 하나의 노드-B(120), 하나의 CRNC(130) 및 하나의 SRNC(140)가 예시되고 있지만, 유무선 장치의 어떤 조합도 무선 통신 시스템(100) 내에 포함될 수 있음을 알아야 한다.

[0016] 도 2는 도 1의 무선 통신 시스템(100)의 예시적인 WTRU(110) 및 노드-B(120)의 기능적 블록 다이어그램이다. 도 2에 예시된 바와 같이, WTRU(110)는 노드-B(20)와 연결되며, 양자 모두는 네트워크 및 어플리케이션 도메인에 대해 M2M 장치 연동 및 상호 연결을 보장하도록 M2M 능력을 이용하는 사물 지능 통신(M2M) 게이트웨이를 지원하도록 구성될 수 있다.

[0017] 통상의 WTRU에서 볼 수 있는 구성 성분 이외에, WTRU(110)는 프로세서(115), 수신기(116), 송신기(117), 메모리(118) 및 안테나(119)를 포함할 수 있다. 메모리(118)는 운영 시스템, 어플리케이션 및 기타 기능적 모듈을 포함하는 소프트웨어를 저장할 수 있다. 프로세서(115)는 독자적으로 또는 상기 소프트웨어와 함께, 네트워크 및 어플리케이션 도메인에 대해 M2M 장치 연동 및 상호 연결을 보장하도록 M2M 능력을 이용하는 사물 지능 통신(M2M) 게이트웨이를 지원하는 방법을 수행할 수 있다. 수신기(116)와 송신기(117)는 프로세서(115)와 연결될 수 있다. 안테나(119)는 무선 데이터의 송수신을 용이하게 하기 위해 수신기(116)와 송신기(117) 모두에 연결될 수 있다.

[0018] 통상의 기지국에서 볼 수 있는 구성 성분 이외에, 노드-B(120)는 프로세서(125), 수신기(126), 송신기(127) 및 안테나(128)를 포함할 수 있다. 프로세서(125)는 네트워크 및 어플리케이션 도메인에 대해 M2M 장치 연동 및 상호 연결을 보장하도록 M2M 능력을 이용하는 사물 지능 통신(M2M) 게이트웨이와 함께 동작하도록 구성될 수 있다. 수신기(126)와 송신기(127)는 프로세서(125)와 연결될 수 있다. 안테나(128)는 무선 데이터의 송수신을 용이하게 하기 위해 수신기(126)와 송신기(127) 모두에 연결될 수 있다.

[0019] 복수의 장치에 서비스를 제공하기 위해 네트워크 도메인 외부에 게이트웨이를 제공하는 시스템, 방법 및 수단이 개시된다. 게이트웨이는 네트워크 도메인을 위한 장치에 서비스 능력을 제공할 수 있고, 이는 네트워크 도메인에 의해 제공될 필요가 있을 수 있는 기능을 감소시킬 수 있다.

[0020] 게이트웨이는 관리 엔티티로서 작용할 수 있다. 게이트웨이는 네트워크 도메인에 대해 신뢰를 구축할 수 있다. 예를 들면, 게이트웨이는 게이트웨이가 네트워크 도메인과 상호 작용하도록 하기 위해 네트워크 도메인에 대해 일정 수준의 신뢰를 형성할 수 있다. 게이트웨이는 복수의 장치 각각에 대한 연결을 구축할 수 있다. 게이트웨이는 각각의 장치에 관한 보안 기능을 행할 수 있다. 게이트웨이는 네트워크 도메인을 위한 것일 수 있는 보안 기능을 행할 수 있다. 게이트웨이는 네트워크 도메인이 직접 참여하지 않거나 최소한으로 참여하여 보안 기능을 수행할 수 있다. 게이트웨이는 네트워크가 특정 장치에 대한 지식을 갖지 않고도 보안 기능을 수행할 수 있다. 게이트웨이는 각각의 장치에 관한 네트웨크 도메인에 장치 정보를 리포팅할 수 있다.

[0021] 게이트웨이는 네트워크를 위한 프록시로서 작용할 수 있다. 게이트웨이는 네트워크 도메인에 대해 신뢰를 구축할 수 있다. 예를 들면, 게이트웨이는 게이트웨이가 네트워크 도메인과 상호 작용하도록 하기 위해 네트워크 도메인에 대해 일정 수준의 신뢰를 형성할 수 있다. 게이트웨이는 복수의 장치 각각에 관한 보안 기능을 수행하도록 네트워크 도메인으로부터 명령을 수신할 수 있다. 예를 들면, 게이트웨이는 네트워크 도메인으로부터 단일 명령을 수신할 수 있고, 이에 응하여 다중 장치에 대한 보안 기능을 수행할 수 있다. 네트워크는 복수의 장치 각각의 아이덴티티를 인지할 수 있다. 게이트웨이는 복수의 장치 각각에 대해 보안 기능을 수행할 수 있다. 게이트웨이는 수행된 보안 기능에 관련된 복수의 장치 각각으로부터 정보를 종합한 후 해당 종합된 정보를 네트워크 도메인으로 전송할 수 있다. 게이트웨이는 종합된 정보를 처리한 후 해당 처리된 종합 정보를 네트워크 도메인으로 전송할 수 있다.

[0022] 게이트웨이에 의해 수행되는 보안 기능은 다음 중 하나 이상을 포함할 수 있다: 부트스트래핑된 크리덴셜(boostrapped credentials)을 사용하거나 사용하지 않고 네트워크 도메인에의 장치의 등록 및 인증; 복수의 장치로의 크리덴셜 제공 및 이송(migration); 복수의 장치 각각으로의 보안 정책 제공; 복수의 장치 각각의 인증 수행; 복수의 장치 각각에 신뢰할만한 기능성을 설정하는 기능으로서, 복수의 장치 각각에 대해 무결성 검증이 수행되는, 기능성 설정; 복수의 장치 각각에 대해, 결함 탐색 및 결함 교정을 포함할 수 있는 장치 관리의 제공; 또는 복수의 장치 중 적어도 하나에 대해, 보안 연관(security association), 통신 채널 또는 통신 링크 중 적어도 하나를 설정.

[0023] 도 3은 개시된 시스템, 방법 및 수단에 사용될 수 있는 일 실시예의 M2M 아키텍처를 예시한다. M2M 게이트웨이

(320)는 M2M 영역 네트워크(324)를 통해 그것에 연결된 M2M 장치(328)와 같은 M2M 장치를 위한 집선기(aggregator)로서 동작하도록 구성될 수 있다. M2M 게이트웨이(320)에 연결된 각각의 M2M 장치는 M2M 네트워크에 의한 M2M 장치 식별 및 인증을 포함할 수 있다.

[0024] M2M 장치 도메인(360)에는 M2M 능력 및 네트워크 도메인 기능을 이용하여 어플리케이션(들)을 구동시키는 M2M 장치(332)가 존재한다. M2M 장치는 액세스 네트워크(310)에 직접 연결되거나(예, M2M 장치(332)), M2M 영역 네트워크(324)를 통해 M2M 게이트웨이(320)에 인터페이스 연결될 수 있다(예, M2M 장치(328)). M2M 영역 네트워크(324)는 M2M 장치와 M2M 게이트웨이 사이의 연결을 제공할 수 있다. M2M 영역 네트워크의 예로는: IEEE 802.15와 같은 개인 영역 네트워크 기술, 지그비(zigbee), 블루투스 및 기타 유사한 기술을 포함한다. M2M 영역 네트워크와 M2M 모세관 네트워크(capillary network)라는 용어는 호환적으로 사용될 수 있다. M2M 게이트웨이(320)는 네트워크 및 어플리케이션 도메인(350)으로도 지칭될 수 있는 네트워크 도메인(350)에 대해 M2M 장치 연동 및 상호 연결을 보장하는 M2M 능력을 이용하는 장비일 수 있다. M2M 게이트웨이(320)는 M2M 어플리케이션도 구동시킬 수 있다. M2M 게이트웨이 기능은 M2M 장치(들)와 공동 배치될 수 있다. 예로써, M2M 게이트웨이(320)와 같은 M2M 게이트웨이는 다양한 정보 소스의 수집 및 처리(예, 센서와 맥락 관련 파라미터로부터)에 기인하는 자동화 처리의 활성화를 위해 국소적 지능(local intelligence)을 구현할 수 있다.

[0025] 네트워크 도메인(350)에는 M2M 장치 도메인(360)이 코어 네트워크(308)와 통신이 이루어지도록 할 수 있는 M2M 액세스 네트워크(310)가 존재한다. 기존의 액세스 네트워크에 기초한 M2M 능력은 M2M 서비스의 전달의 개선을 위해 필요할 수 있다. 액세스 네트워크의 예로는: 디지털 가입자 회선 기술(xDSL), 혼합 광섬유-동축 케이블 접속망(hybrid fiber-coaxial: HFC), 전력선 통신(PLC), 위성, EDGE 전송 표준 무선 액세스 네트워크(GERAN)용 GSM, 제3 세대 휴대 전화 시스템(UMTS) UTRAN, eUTRAN, 무선 로컬 영역 네트워크(W-LAN) 및 WiMAX를 포함한다.

[0026] 네트워크 도메인(350) 내에서 데이터의 전송을 허용할 수 있는 전송 네트워크(318)와 같은 전송 네트워크도 존재할 수 있다. 기존의 전송 네트워크를 기초로 한 M2M 능력은 M2M 서비스의 전달을 개선하는데 필요할 수 있다. M2M 코어(304)는 코어 네트워크(308)와 서비스 능력으로 구성된다. M2M 코어 네트워크(308)는 IP 연결성, 서비스 및 네트워크 제어 기능, 상호 연결(다른 네트워크와의), 로밍(PLMN 용) 등을 제공할 수 있다. 다른 코어 네트워크는 다른 능력 세트를 제공할 수 있다. 기존 코어 네트워크에 기초한 M2M 능력은 M2M 서비스의 전달을 개선하는데 필요할 수 있다. 코어 네트워크의 예로는 3GPP 코어 네트워크(예, GPRS, EPC), ESTI TISPAN 코어 네트워크를 포함할 수 있다. IP 서비스 제공자 네트워크의 경우, 코어 네트워크는 제한된 기능을 제공할 수 있다.

[0027] 서비스 능력(306)은 다른 어플리케이션에 의해 공유될 수 있는 기능을 제공한다. 서비스 능력(306)은 개방 인터페이스 세트를 통해 기능성을 노출한다. 추가로, 서비스 능력(306)은 코어 네트워크 기능을 이용할 수 있다. 서비스 능력(306)은 어플리케이션 개발 및 전개를 최적화하고 어플리케이션에 대한 네트워크 사양을 숨기기 위해 이용될 수 있다. 서비스 능력(306)은 M2M 특정 또는 M2M 이외의 어플리케이션에 지원을 제공하는 M2M 범용일 수 있다. 해당 예로는 데이터 저장 및 집합, 유니캐스트 또는 멀티캐스트 메시지 전달 등을 포함한다.

[0028] M2M 어플리케이션(302)은 서비스 로직을 구동시키고 개방 인터페이스를 통해 액세스 가능한 서비스 능력을 이용하는 어플리케이션을 포함할 수 있다. 네트워크 관리 기능(316)은 권한 설정(provisioning), 감독, 결함 관리 및 다른 유사 기능과 같은 관련 M2M 능력을 포함하여, 액세스 네트워크(310), 전송 네트워크(318) 및 코어 네트워크(308)를 관리하는데 필요한 기능을 포함할 수 있다. M2M 특정 관리 기능(315)은 액세스 네트워크(310), 전송 네트워크(318) 및 코어 네트워크(308)에서 M2M 능력을 관리하기 위해 네트워크 관리 기능(316) 내에 포함될 수 있다. M2M 관리 기능(314)은 M2M 장치 및 게이트웨이(예, M2M 게이트웨이(320), M2M 장치(328), M2M 장치(332) 등)의 기능은 물론, M2M 어플리케이션(302)과 서비스 능력(306)의 관리에 필요한 기능을 포함할 수 있다. M2M 장치 및 게이트웨이의 관리는 서비스 기능(예, 장치 관리 서비스 능력)을 이용할 수 있다. M2M 관리 기능(314)은 M2M 장치(328) 또는 M2M 게이트웨이(320)의 결함 탐색 및 결합 교정을 위한 기능을 포함할 수 있다.

[0029] M2M 아키텍처와 다중 M2M 장치 연결 방법이 여기에 제시된다. M2M 장치는 다양한 방법으로 M2M 네트워크에 연결될 수 있다. 4가지 경우의 예가 예시된다. 제1의 경우(케이스 1), M2M 장치는 액세스 네트워크를 통해 직접 M2M 시스템에 연결된다. M2M 장치는 M2M 시스템에 등록 및 인증된다. 제2의 경우(케이스 2), M2M 장치는 M2M 게이트웨이 영역 네트워크를 통해 M2M 시스템에 연결된다. M2M 게이트웨이는 액세스 네트워크를 통해 M2M 시스템에 연결된다. M2M 장치는 M2M 게이트웨이를 통해 M2M 시스템에 인증된다. 영역 네트워크는 무선 통신망, WLAN, BT 및 기타 시스템이거나 그렇지 않을 수 있다. 제2 경우, M2M 게이트웨이는 단지 M2M 장치를 위한 터널로서 작용할 수 있다. M2M 장치의 등록, 인증, 허가(authorization), 관리 및 권한 설정과 같은 절차가 M2M 네

트워크에 의해 수행된다.

[0030] 2가지 추가의 경우가 아래 제시된다. 제3의 경우(케이스 3), M2M 게이트웨이(320)와 같은 게이트웨이는 관리 엔티티로서 작용할 수 있다. M2M 장치(328)와 같은 M2M 장치는 예컨대 M2M 영역 네트워크(324)를 통해 M2M 게이트웨이(320)에 연결될 수 있다. M2M 게이트웨이(320)는 액세스 네트워크(310)를 통해 연결이 행해질 수 있는 M2M 네트웨크 도메인(350)에 연결되어 해당 도메인과 신뢰를 구축할 수 있다. M2M 게이트웨이(320)는 예컨대 영역 네트워크(310)에 의해 제공된 등록, 인증, 허가, 관리 및 권한 설정의 기존의 방법을 재사용하는 것에 의해 M2M 네트워크 도메인(350)의 제어에 무관한 방식으로 M2M 게이트웨이에 연결되는 M2M 장치를 관리할 수 있다. 이러한 게이트웨이에 연결되는 장치는 M2M 네트워크 도메인(350)에 의해 주소 지정 가능하거나 그렇지 않을 수 있다. M2M 영역 네트워크(324)는 무선 통신 네트워크, WLAN, BT 또는 기타 유사한 네트워크이거나 그렇지 않을 수 있다. 게이트웨이는 해당 게이트웨이에 연결된 각각의 M2M 장치에 대해 보안 기능을 수행할 수 있다. 게이트웨이는 M2M 네트워크 도메인(350)이 직접 특정 장치에 참여 또는 해당 장치에 대한 지식을 갖지 않거나, M2M 네트워크 도메인(350)에 의해 최소한 참여하여 상기 보안 기능을 수행할 수 있다. M2M 게이트웨이(320)는 수행된 보안 기능에 대한 각각의 장치에 관련된 네트워크 도메인에 정보를 리포팅할 수 있다.

[0031] 제4의 경우(케이스 4), M2M 게이트웨이(320)와 같은 게이트웨이는 예컨대 네트워크 도메인(350)과 같은 네트워크를 위한 프록시로서 작용할 수 있다. M2M 장치(328)와 같은 M2M 장치는 예컨대 M2M 영역 네트워크(324)를 통해 M2M 게이트웨이(320)에 연결된다. 이러한 게이트웨이에 연결된 장치들은 M2M 네트워크에 의해 주소 지정되거나 그렇지 않을 수 있다. M2M 게이트웨이(320)는 액세스 네트워크(310)를 통해 연결이 이루어질 수 있는 M2M 네트워크 도메인(350)에 연결되어 해당 네트워크 도메인과 신뢰를 구축할 수 있다. M2M 게이트웨이(320)는 해당 게이트웨이에 연결되는 M2M 장치(328)와 같은 M2M 장치를 향한 M2M 네트워크 도메인(350)를 위한 프록시로서 작용한다. 이러한 M2M 게이트웨이는 이에 연결된 각각의 M2M 장치에 관한 보안 기능의 수행을 위해 네트워크 도메인으로부터 명령을 수신할 수 있다. 예를 들면, 게이트웨이는 네트워크 도메인으로부터 단일 명령을 수신할 수 있으며, 이에 응하여 다중 장치에 대해 보안 기능을 수행할 수 있다. 게이트웨이는 보안 기능을 수행할 수 있다. 게이트웨이는 인증, 허가, 등록, 장치 관리 및 권한 설정과 같은 절차를 수행할 수 있으며, M2M 네트워크를 대신하여 어플리케이션도 실행할 수 있다. 게이트웨이는 수행된 보안 기능에 관한 복수의 장치 각각으로부터 정보를 종합하고 해당 종합된 정보를 M2M 네트워크 도메인(350)으로 전송할 수 있다. 게이트웨이는 종합된 정보를 처리하고 해당 처리된 종합 정보를 네트워크 도메인으로 전송할 수 있다.

[0032] 도 4는 케이스 3의 게이트웨이 기능의 예를 예시한다. M2M 네트워크 도메인(350)에 연결될 수 있는 M2M 게이트웨이(410)는 M2M 영역 네트워크(예, 모세관 네트워크)에 의해 연결되는 M2M 장치(430)를 위해 로컬 AAA 서버(420)를 유지한다. AAA 서버(420)는 로컬 등록, 인증, 허가, 계정(accounting) 및 장치 무결성 검증을 용이하게 한다.

[0033] 케이스 3의 연결 장치의 경우, 등록, 인증, 허가 및 장치 관리를 위한 M2M 영역 네트워크 프로토콜 및 절차가 이용된다. 장치는 `M2M 네트워크 도메인(350)에 의해 주소 지정되거나 그렇지 않을 수 있다. 게이트웨이는 M2M 네트워크에 대해 M2M 장치로서 등장하여 등록과 인증을 수행한다. 도 5는 케이스 3의 연결 장치 또는 연결 시나리오에 대한 예시적인 부트스트래핑과 등록 흐름을 나타낸다.

[0034] 도 5는 M2M 장치(502), M2M 게이트웨이(504), 액세스 네트워크(504)(예, 네트워크 망 운용 서비스와 관련됨), 인증 서버(508)(예, 네트워크 망 운용 서비스와 관련됨), 보안 능력(510), AAA/GMAE(512) 및 기타 능력(514)을 나타낸다. 522에서, M2M 게이트웨이(504)는 액세스 네트워크(506)를 통해 네트워크를 획득한다. 524 및 528에서, M2M 게이트웨이(504)와 액세스 네트워크(506) 사이와 액세스 네트워크(506)와 인증 서버(508) 사이에 액세스 인증이 수행될 수 있다. 526에서, M2M 게이트웨이(504)와 액세스 네트워크(506) 사이에 링크 및 네트워크 세션 셋업이 수행될 수 있다. 부트스트래핑은 529 및 530에서의 흐름을 포함한다. 부트스트래핑은 권한 설정 중에 성능이 제한될 수 있다. 529에서 M2M 게이트웨이(504)와 보안 능력(510) 사이에 부트스트래핑 요청이 수행될 수 있다. 530에서, M2M 게이트웨이(504)와 보안 능력(510) 사이에 M2M 보안 부트스트래핑이 수행될 수 있다. 536에서, 보안 능력(510)과 AAA/GMAE(512) 사이에 장치 권한 설정(예, M2M 네트워크 어드레스 식별자(NAI) 및 루트 키(root key)와 같은 데이터 또는 기타 서비스 또는 어플리케이션-레벨 파라미터 또는 데이터의 권한 설정)이 수행될 수 있다. 532에서, M2M 게이트웨이(504)와 보안 능력(510) 사이에 세션 키의 인증 및 생성을 포함하는 M2M 등록이 행해진다. 538에서, M2M 장치, 서비스 능력, 일련의 서비스 능력 또는 하나 이상의 어플리케이션을 인증할 수 있는 M2M 인증이 보안 능력(510)과 AAA/GMAE(512) 사이에 행해질 수 있다. 540에서, 보안 능력(510)은 다른 능력(514)에 대해 암호화 키를 제공할 수 있다. 534에서, M2M 장치(502)와 M2M 게이트

웨이(504) 사이에 영역 프로토콜, 등록, 인증 및 권한 설정이 행해질 수 있다.

[0035] 케이스 4의 연결 장치의 경우, 등록 인증, 허가 및 장치 관리를 위한 절차 및 영역 네트워크 프로토콜이 사용될 수 있다. M2M 네트워크 명령을 M2M 장치로 옮기는 망 연동 기능이 M2M 게이트웨이에 존재할 수 있다. 장치들은 M2M 네트워크 도메인에 의해 주소 지정되거나 그렇지 않을 수 있다. 도 6은 케이스 4의 연결 장치에 대한 예시적인 부트스트래핑 및 등록 흐름을 나타낸다. 도 6에 예시된 케이스 4의 흐름은 도 5의 흐름을 포함한다. 추가로, 644에서, M2M 게이트웨이(504)와 M2M 네트워크 도메인의 보안 능력(510) 사이에 장치 등록/인증 상태 리포팅이 행해질 수 있다.

[0036] 여전히 케이스 4의 예를 참조하면, M2M 게이트웨이는 네트워크를 위한 프록시로서 작용하도록 네트워크 내에 신뢰를 구축하기 위해 네트워크에 대해 등록과 인증을 수행한다. 이러한 경우, M2M 게이트웨이는: 네트워크 측으로 자체를 입증하고; M2M 액세스 네트워크에 부착된 장치를 입증하고; M2M 장치의 보안 연관을 관리라고 유지하는 것으로 포함하여 M2M 장치의 인증 및 아이덴티티 관리를 포함하는 보안 및 신뢰를 관리하고; 로컬 IP 액세스 라우팅을 수행할 수 있도록, M2M 장치 로컬 등록(로컬 영역 인증을 포함) 및 아이덴티티 관리를 수행하고; M2M 인증(예, 하나 이상의 M2M 장치, M2M 장치의 하나 이상의 서비스, 또는 M2M 장치의 하나 이상의 어플리케이션 등의), 허가 및 계정을 수행하고; M2M 장치 무결성 검증을 수행하고; 네트워크를 위한 프록시로서 작용할 수 있다.

[0037] 이러한 M2M 게이트웨이는 다수의 어플리케이션에 사용될 수 있다. 제한적이지 않은 예를 들면, 유선 또는 무선의 역 전송(back haul)의 발전된 펨토 셀, 발전된 Home 노트-B 또는 Home 노드-B의 구현에 이용될 수 있다. 네트워크 및/또는 사용자를 위한 디지털 프록시로서 이용될 수도 있다. 네트워크는 M2M 장치를 인지하지 못할 수 있으며; 게이트웨이는 M2M 장치 연결을 관리하고 유지하는데 네트워크 대신에 동작할 수 있다. 디지털 프록시로서 동작하는 M2M 게이트웨이는 핸드셋 또는 기타 휴대용 단말기 형상 인자를 가질 수 있다. 센서와 액츄에이터가 M2M 게이트웨이에 연결된 eHealth 시나리오에 이용될 수도 있다. 센서/액츄에이터는 M2M 네트워크 도메인에 대해 등록과 인증을 행하지 않을 수 있다. 대신에, 이들 M2M 장치(센서/액츄에이터)는 M2M 게이트웨이에 기록을 행할 수 있다. 이들 어플리케이션에서, M2M 게이트웨이는 PDA 또는 휴대 전화와 같은 휴대용 장치이거나 액세스 포인트 또는 라우터와 같은 트래픽 집선기(aggregator)일 수 있다. 연결은 M2M 게이트웨이가 서브세트의 연결된 M2M 장치와 게이트웨이에 연결된 다른 M2M 장치에 대해 프록시 기능을 수행하고 케이스 2의 M2M 게이트웨이로서 기능을 행할 수 있도록 행해질 수 있다. 연결은 M2M 게이트웨이가 M2M 액세스 네트워크와 코어 네트워크에 대해 케이스 1의 연결 M2M 장치로서 동작 및 등장하고 M2M 게이트웨이에 연결된 M2M 장치가 M2M 게이트웨이에 의해 독립적으로 관리될 수 있도록 행해질 수 있다. 연결은 M2M 게이트웨이가 도 7에 예시된 바와 같이 M2M 게이트웨이(710)에 대해 M2M 장치로서 동작하도록 행해질 수 있는데, 예컨대, M2M 게이트웨이(720)는 M2M 게이트웨이(710)에 대해 M2M 장치로서 동작할 수 있다. M2M 게이트웨이(710)는 M2M 영역 네트워크(모세관 네트워크로도 알려짐)에 의해 연결된 M2M 장치(712)를 위한 로컬 AAA 서버(715)를 유지할 수 있다. M2M 게이트웨이(720)는 M2M 영역 네트워크(예, 모세관 네트워크)에 의해 연결된 M2M 장치(722)를 위한 로컬 AAA 서버(725)를 유지할 수 있다.

[0038] 무결성 검증은 리포팅을 포함하여 국부화된 동작과 국부적으로 수행되는 측정을 기초로 한 원격 동작을 포함할 수 있는데, 예컨대 검증은 암시적이거나 시그널링을 통해 명시적일 수 있다. 장치 무결성 확인 및 검증을 실현하기 위해 M2M 장치는 신뢰되는 실행 환경을 포함할 수 있다. 신뢰되는 실행 환경으로부터 장치는 장치의 소프트웨어의 무결성을 확인하고, 보안 부트 처리에 의한 로딩 및 실행에 앞서 신뢰된 기준 값에 대해 무결성을 입증할 수 있다. 이들 신뢰된 기준 값은 신뢰되는 제3자 또는 신뢰되는 제조자에 의해 발생될 수 있고, 검증될 장치의 측정 값(예, 해시 값(hash value))이다. 소프트웨어의 무결성의 검증은 국부적으로(예, 자율적 검증) 또는 원격으로(예, 반 자율적인 검증 및 완전 원격 검증) 행해질 수 있다. 장치 무결성 검증이 원격으로 수행되면, 검증을 행하는 엔티티는 M2M 게이트웨이 또는 검증 엔티티로서 동작하는 M2M 게이트웨이의 지정된 엔티티 또는 프록시일 수 있다. 검증 대상이 M2M 게이트웨이에 연결된 M2M 장치 및/또는 M2M 네트워크 또는 M2M 네트워크의 지정된 엔티티 또는 프록시에 대한 네트워크-기초한 검증 엔티티이면, 검증 대상은 M2M 장치 또는 M2M 게이트웨이, 또는 이들의 소정의 조합일 수 있다.

[0039] 완전 원격 검증시, 대상 엔티티(그 무결성이 검증될)는 국부적으로 수행된 검증의 증거 또는 결과 없이 검증 엔티티에 대해 무결성의 측정치를 전송할 수 있다. 다른 한편, 반 자율적 검증의 경우, 대상 엔티티는 무결성을 측정하고 해당 측정치를 일정 정도 검증/어써트할 수 있으며, 검증 엔티티에 검증의 결과에 관한 증거 또는 정보를 전송할 수 있다.

[0040] 무결성 확인 처리가 국부적으로 수행되면, 신뢰되는 기준값은 보안 메모리에 저장될 수 있고, 허가된 액세스로 액세스가 제한될 수 있다. 검증이 원격 검증 엔티티(예, 검증 엔티티로서 동작하는 M2M 게이트웨이 또는 M2M 네트워크 상의 네트워크-기초한 검증 엔티티)에서 수행되면, 게이트웨이 또는 네트워크-기초한 검증 엔티티는 검증 처리 중에 신뢰되는 제3자 또는 신뢰되는 제조자로부터 이들 신뢰된 기준값을 페칭(fetch)하거나 예비 페칭한 후 국부적으로 저장할 수 있다. 디들 신뢰된 기준값은 오퍼레이터 또는 사용자에 의해 M2M 게이트웨이 또는 M2M 네트워크 내의 검증 엔티티에 제공될 수도 있다. 이러한 신뢰된 기준값은 방송으로, 유선으로 또는 사용자 또는 오퍼레이터가 M2M 게이트웨이(예, 반 자율적 검증의 경우) 또는 M2M 장치(예, 자율적 검증의 경우)에 보안 매체를 삽입할 수 있는 보안 USB, 보안 스마트 카드, 보안 디지털(SD) 카드와 같은 보안 매체를 통해 신뢰되는 제3자 또는 신뢰되는 제조자에 의해 보내질 수 있다. M2M 네트워크에 기초한 반 자율적 검증의 경우, 검증 엔티티는 이러한 정보를 신뢰되는 제조자 또는 신뢰되는 제3자로부터 직접 얻을 수 있다.

[0041] 장치로부터 M2M 게이트웨이 내의 검증 엔티티까지 무결성 결과를 보내기 위해서는 M2M 영역 네트워크 프로토콜에 대해 새로운 업데이트가 필요할 수 있다. 이것은 프로토콜 필드를 업데이트하거나 무결성 결과와 측정 함수를 포함하는 데이터그램을 초기 랜덤 액세스 메시지에 전송하는 것에 의해 또는 알고 있거나 알고 있지 않은 형태의 연결을 세팅한 후에 실시될 수 있다.

[0042] 장치 무결성 검증은 다음의 예시적인 방법 중 하나 이상의 방법을 이용하여 자율적으로 또는 반 자율적으로 수행될 수 있다.

[0043] 장치 검증 절차는 케이스 1의 장치에 대해 제공될 수 있다.

[0044] 이 경우, 장치는 코어 네트워크를 통해 직접 M2M 네트워크에 연결될 수 있다. 자율적 검증이 지원되는 장치에서, 장치에 의해 액세스 네트워크로의 최초 액세스는 국부적 무결성 확인 및 검증의 결과를 포함할 수 있다. 장치가 네트워크 내의 등록을 시도했다는 사실에 의해, 네트워크는 장치 무결성 검증이 성공한 것으로 추정할 수 있다. 장치 무결성 확인이 실패한 경우, 실패된 엔티티 또는 기능의 리스트가 장애 신호(distress signal)에 포함될 수 있으며, 네트워크는 장치의 교정 또는 복구를 위한 필요 절차를 행할 수 있다.

[0045] 반 자율적 검증의 경우, 검증 엔티티는 액세스 네트워크 또는 M2M 네트워크 또는 양자 모두에 필요할 수 있다. 이러한 검증 엔티티는 플랫폼 검증 엔티티일 수 있고 인증, 허가 및 계정 (AAA) 서버와 함께 배치될 수 있다. 국부적 엔티티 확인의 결과는 무결성 확인의 통과 또는 실패 여부를 결정하는 플랫폼 검증 엔티티(PVE)로 전송될 수 있다. 성공적인 확인의 경우, PVE는 장치가 액세스 네트워크 및/또는 M2M 서비스 능력 계층 또는 M2M 네트워크 내에 등록될 수 있게 한다. 실패된 확인의 경우, PVE는 업데이트 또는 페치를 다운로딩하기 위해 교정 서버로 장치를 리디렉션(redirect)할 수 있다. 실패된 확인의 경우, PVE는 장치를 격리시키고 장치를 고치기 위해 담당자를 보내도록 OAM에 신호를 보낼 수 있다.

[0046] 장치 검증 절차는 케이스 2의 장치와 게이트웨이에 대해 제공될 수 있다.

[0047] 이 경우, 장치는 M2M 게이트웨이를 통해 M2M 네트워크에 연결될 수 있다. 장치는 M2M 네트워크에 의해 주소 지정될 수 있다. M2M 게이트웨이는 이러한 경우 터널 제공자로서 동작한다. 게이트웨이와 장치의 무결성 확인을 별도로 고려하는 것이 유용할 수 있다. 우선, 게이트웨이는 장치가 게이트웨이로 대체되는 경우 여기에 설명된 바와 같이 반 자율적으로 또는 자율적으로 무결성이 검증될 수 있다. 게이트웨이의 성공적인 무결성 확인 후에 장치는 M2M 게이트웨이에 연결되는 것이 허용될 수 있다. 장치의 무결성 확인이 이후 수행될 수 있다. 이것은 액세스 네트워크 내에서 PVE에 의해, M2M 서비스 능력 계층 또는 M2M 네트워크에 의해 자율적으로 또는 반 자율적으로 수행될 수 있다.

[0048] 반 자율적 검증의 경우, M2M 게이트웨이는 M2M 장치에 대한 액세스 제어를 행할 수 있는 보안 게이트웨이의 임무를 수행할 수 있다. 게이트웨이는 장치 무결성 검증 절차가 M2M 장치에 대해 완료되기까지 PVE에 대한 액세스를 억제할 수 있으며, M2M 장치 무결성 확인이 실패되는 경우, 액세스 제어를 수행하고 M2M 장치를 단절하거나 교정 엔티티로의 액세스를 제한하는 것에 의해 M2M 장치의 액세스를 제한할 수 있다.

[0049] 장치 검증 절차는 케이스 3 및 케이스 4의 장치 및 게이트웨이에 대해 제공될 수 있다.

[0050] 장치는 장치 무결성이 게이트웨이 또는 네트워크에 의해 내재적으로 확인 및 검증될 수 있는 자율적 검증을 수행할 수 있다. 장치는 장치가 검증 엔티티에 대해 무결성 확인 결과 또는 해당 결과의 요약(예, 무결성 확인 실패된 성분에 대응하는 실패된 기능의 리스트)을 전송하는 반 자율적 또는 완전 원격 검증을 수행할 수 있다.

[0051] 케이스 3의 연결의 경우, M2M 장치에 대한 검증 엔티티는 M2M 게이트웨이일 수 있다. M2M 네트워크(및/또는 액세스 네트워크)는 M2M 게이트웨이의 무결성을 위한 검증 엔티티로서 동작하는 다른 엔티티(또는 무결성 검증이 M2M 네트워크와 액세스 네트워크 모두에 대해 별도로 행해지는 것이 필요한 경우에는 엔티티들)를 필요로 할 수 있다. M2M 네트워크 및/또는 액세스 네트워크는 무결성 검증 후의 게이트웨이가 M2M 장치의 무결성을 검증하는 자신의 역할을 수행하는 것이 "신뢰"될 수 있는 경우 M2M 게이트웨이의 무결성을 검증하는 것에 의해 간접적인 방식으로 M2M 장치의 무결성을 "검증"할 수 있다.

[0052] 케이스 4의 연결의 경우, M2M 장치의 무결성에 대한 검증 엔티티의 역할은 M2M 게이트웨이와 M2M 네트워크 사이에서 분할될 수 있다. M2M 게이트웨이의 무결성을 위한 검증 엔티티의 역할은 M2M 네트워크 또는 액세스 네트워크 상의 엔티티에 의해 취해질 필요가 있을 수 있다. (검증 엔티티) 역할이 M2M 게이트웨이와 M2M 네트워크(및/또는 액세스 네트워크) 간에 분할되는지 여부와 (그 정도를 포함하는) 방법은 하나 이상의 정책에 의해 정의될 수 있다. 트리형 구조를 사용한 분할 검증(예, 트리-형성된 검증)이 이용되면, 정책은 M2M 게이트웨이가 장치에 대해 대략적인 무결성 검증을 수행하고 그 결과를 M2M 네트워크(및/또는 액세스 네트워크) 내의 검증 엔티티 또는 엔티티들에 리포팅한다. 검증 엔티티는 이들 결과를 확인 및 평가한 후 평가의 결과와 자체의 정책에 따라 게이트웨이를 통해 정확한 무결성 검증을 직접 또는 간접적으로 수행할 수 있다.

[0053] 하나의 이러한 정책은 M2M 오퍼레이터로부터일 수 있고, 다른 이러한 정책은 액세스 네트워크 오퍼레이터로부터일 수 있다. 다른 이해 관계자도 자체의 정책을 채용하고 이용할 수 있다.

[0054] 장치 무결성 확인이 통과되면, 장치는 네트워크에 대한 등록 및 인증을 계속할 수 있다. 장치의 등록 및 인증은 케이스 3의 연결에 대한 M2M 영역 네트워크 내에서 국부적으로 수행될 수 있다. 이러한 작업을 수행하는 엔티티들은 케이스 4의 연결에 대해 M2M 게이트웨이와 M2M 네트워크(및/또는 액세스 네트워크) 사이에서 분할될 수 있다.

[0055] 케이스 3과 케이스 4의 연결 모두의 경우, 설정된 정책에 기초하여, M2M 게이트웨이는 M2M 장치가 M2M 게이트웨이에 등록되기 전에 M2M 액세스 네트워크와 M2M 코어 네트워크에 대해 비동기적으로 등록 및 인증이 행해질 수 있다. M2M 게이트웨이는 장치가 인증을 완료한 후까지 M2M 액세스 네트워크와 M2M 코어 네트워크에 대한 등록 및 인증을 지연할 수 있다. 장치로부터의 등록의 허용 및 M2M 코어/M2M 액세스 네트워크에 대한 등록 시작 전에, M2M 장치는 자체의 무결성 확인 및 검증 과정을 예컨대 자율적으로 또는 반 자율적으로 수행할 수 있다.

[0056] 케이스 3과 케이스 4의 장치 무결성 검증은 도 8에 예시된 흐름 중 하나 이상을 포함할 수 있다. 도 8은 M2M 장치(들)(802), M2M 게이트웨이(804)(로컬 AAA를 포함할 수 있음), 네트워크 오퍼레이터(806)(액세스 네트워크를 포함할 수 있음) 및 M2M 오퍼레이터(808)(M2M 코어(GMAE/DAR)를 포함할 수 있음)를 예시한다. 820에서, M2M 게이트웨이(804)는 자체의 무결성 확인 및 검증을 자율적으로 또는 반 자율적으로 수행할 수 있다. 824에서, M2M 장치(들)(802)는 자체의 무결성 확인 및 검증을 수행한 후 그것이 성공적이면 828에서 게이트웨이 획득, 등록 및 인증을 수행할 수 있다. 게이트웨이는: 1) 자체의 무결성 확인 및 검증을 완료하자마자; 또는 2) M2M 액세스 네트워크 및/또는 M2M 코어 네트워크에 대한 등록 이후에 장치 등록 및 인증 요청의 허용을 시작할 수 있다. 832에서, 게이트웨이는 M2M 액세스 네트워크(예, 네트워크 오퍼레이터(806)) 및/또는 M2M 코어 네트워크(M2M 오퍼레이터(808))에 대한 등록 및 인증을 M2M 장치 등록 및 인증과 비동기적으로 상관없이 수행할 수 있거나, M2M 장치(들)(802)가 M2M 게이트웨이(804)에서 등록 및 인증될 때까지 등록 및 인증을 지연할 수 있다.

[0057] 836에서, M2M 등록 및 인증은 M2M 게이트웨이(804)와 M2M 오퍼레이터(808) 사이에서 수행될 수 있다. M2M 게이트웨이(804)에 연결된 하나 이상의 장치가 장치 무결성 확인에 실패하면, 실패한 장치의 리스트 또는 실패한 기능(예, 장치가 센서인 경우)의 리스트가 M2M 게이트웨이(804)로부터 M2M 코어 네트워크(M2M 오퍼레이터(808))로 전송될 수 있다. 이러한 실패(예, 전체적인 실패 또는 특정 기능의 실패)에 의존하여, 무결성 확인에 실패한 것으로 확인된 장치는 네트워크 액세스가 거부되거나 액세스가 제한될 수 있다(예, 시간, 종류 또는 범위와 관련하여). 개인 영역 네트워크(body area network) 또는 다른 무선 센서 영역 네트워크와 같은 소정의 경우, 임의의 하나의 또는 다중의 장치가 무결성 확인에 실패한 것으로 확인되면, M2M 게이트웨이(804)는, 이러한 능력이 모세관 네트워크와 게이트웨이에 존재하는 경우, 남아있는 장치의 기능 또는 위상(topology) 업데이트를 시도함으로써 남아있는 장치 상의 새로운 위상 또는 새로운 기능이 무결성 확인에 실패한 장치의 실패 또는 감소된 기능을 보상할 수 있다. 네트워크가 M2M 영역 네트워크(예, 모세관 네트워크) 내에 있는 장치에 대해 높은 레벨의 보장이 필요한 경우, M2M 게이트웨이는 M2M 영역 네트워크 내의 하나 이상의 장치에 대한 무결성 위반(integrity breach) 또는 실패를 검출한 후 스스로 또는 M2M 네트워크 도메인으로부터의 감독과 병행하거나 감

독하에 M2M 영역 네트워크 또는 그 서브세트 내의 모든 장치를 단절하도록 조치할 수 있다.

[0058] 케이스 4의 연결의 경우, 840에서, M2M 게이트웨이(804)와 네트워크 오퍼레이터(806) 사이에서 보다 정밀한 무결성 검증이 수행될 수 있다. 844에서, M2M 게이트웨이(804)와 M2M 장치(들)(802) 사이에 보다 정밀한 무결성 검증이 수행될 수 있다. 848에서, 844의 결과는 네트워크 오퍼레이터(806)에 리포팅될 수 있다.

[0059] 852에서, 장치 런타임 무결성 실패가 결정/리포팅될 수 있고 및/또는 장치 등록 해제가 M2M 장치(들)(802)와 M2M 게이트웨이(804) 사이에 수행될 수 있다. 856에서, 업데이트된 기능 및/또는 업데이트된 장치 리스트가 M2M 게이트웨이(804)와 M2M 오퍼레이터(808) 사이에 리포팅될 수 있다.

[0060] 케이스 1의 장치 무결성 및 등록은 도 9에 예시된 흐름 중 하나 이상을 포함할 수 있다. 도 9는 M2M 장치(902), 네트워크 오퍼레이터 액세스 네트워크(904), 네트워크 오퍼레이터 인증 서버(906)(플랫폼 검증 엔티티로서 수행할 수 있음), 보안 능력(908), AAA/GMAE(910) 및 기타 능력(912)을 나타낸다. 케이스 1의 연결의 경우, M2M 장치(902)는 M2M 액세스 네트워크, 네트워크 오퍼레이터 액세스 네트워크(904)에 직접 연결될 수 있다.

[0061] 920에서, M2M 장치(902)는 무결성 확인을 수행할 수 있다. 922에서, M2M 장치(902)는 네트워크 오퍼레이터 액세스 네트워크(904)를 획득할 수 있다. 924에서, 네트워크 오퍼레이터 액세스 네트워크(904)와 네트워크 오퍼레이터 인증 서버(906) 사이에 (무결성 검증 정보를 포함할 수 있는) 액세스 인증이 구축될 수 있다. 928에서, M2M 장치(902)와 네트워크 오퍼레이터 액세스 네트워크(904) 사이에 (무결성 검증 정보를 포함할 수 있는) 액세스 인증이 구축될 수 있다. 보안 부트 처리를 이용하여, M2M 장치(902)는 자율적 검증 또는 반 자율적 검증에 포함된 단계를 시동 및 수행할 수 있다. 반 자율적 검증의 대안으로서, 원격 검증 절차가 수행될 수도 있다.

[0062] 자율적 검증이 M2M 장치(902)에 이용되는 경우, 장치 무결성 확인 및 검증 후에 장치는 M2M 액세스 네트워크를 획득하도록 진행되고 M2M 액세스 네트워크로의 연결 및 등록을 시도할 수 있다.

[0063] 반 자율적 검증이 M2M 장치(902)에 이용된 경우, 장치는 국부적 장치 무결성 확인을 수행하고, 네트워크 획득 이후, 장치는 국부적 장치 무결성 확인의 결과를 어떤 것이 적용 가능하던지 M2M 네트워크 오퍼레이터 및/또는 M2M 액세스 네트워크 플랫폼 검증 인티티로 전송할 수 있다. 플랫폼 검증 엔티티는 도 9의 흐름 다이어그램에 예시된 바와 같이 오퍼레이터의 인증 서버(M2M 오퍼레이터 또는 액세스 네트워크 오퍼레이터)와 공동 배치될 수 있으나, 플랫폼 검증 엔티티는 네트워크 내에서 별도의 엔티티일 수 있다. 장치 무결성 확인의 결과는 실패된 성분, 모듈 또는 기능의 리스트일 수 있다. 플랫폼 검증 엔티티는 장치 무결성 검증을 행한 후 장치 인증을 수행할 수 있다.

[0064] 장치에 의해 사용되는 아이덴티티는 액세스 네트워크 또는 M2M 오퍼레이터 네트워크 비밀 키가 아직 부트스트래핑되지 않은 경우 신뢰되는 플랫폼 식별자일 수 있다. 상기 비밀 키가 존재하면, 해당 키는 추가로 또는 개별적으로 사용될 수도 있다.

[0065] 인증이 성공적이면, 930에서 링크와 네트워크 세션 셋업이 후속될 수 있다. M2M 액세스 네트워크 인증이 성공적이면, 이 결과는 926에서 단일의 개시 신호(sign-on)에 대해 M2M 시스템에 사용될 수 있다. 따라서, M2M 액세스 네트워크 아이덴티티와 인증 결과는 M2M 시스템 아이덴티티와 인증에 이용될 수 있다. M2M 액세스 네트워크에 의한 성공적인 인증은 다른 M2M 액세스 네트워크, M2M 시스템 또는 M2M 코어, 또는 M2M 네트워크 또는 다른 서비스 제공자에 의해 제공되는 소정의 서비스 능력 또는 어플리케이션에 의한 성공적인 식별 및 인증을 의미할 수 있다. 부트스트래핑과 M2M 등록이 후속할 수 있다. 예를 들면, 932에서 M2M 장치(902)는 보안 능력(908)에 M2M 부트스트래핑을 요청할 수 있다. 934에서, M2M 장치(902)와 보안 능력(908) 사이에 M2M 보안 부트스트래핑이 행해질 수 있다. 936에서, 보안 능력(908)과 AAA/GMAE(910) 사이에 장치 권한 설정(M2M NAI 및 루트 키)이 행해질 수 있다. 938에서, M2M 장치(902)와 보안 능력(908) 사이에 인증 및 세션 키를 포함할 수 있는 M2M 등록이 행해질 수 있다. 940에서, 보안 능력(908)과 AAA/GMAE(910) 사이에 M2M 인증이 행해질 수 있다. 942에서, 보안 능력(908)은 암호화 키를 다른 능력(912)에 제공할 수 있다.

[0066] 케이스 2의 장치 및 게이트웨이의 무결성 및 등록은 도 10에 예시된 흐름 중 하나 이상을 포함할 수 있다. 도 10은 M2M 장치(1002), M2M 게이트웨이(1004), 액세스 네트워크(1006)(예, 네트워크 오퍼레이터와 관련된), 인증 서버(1008)(예, 네트워크 오퍼레이터와 관련됨), 보안 능력(1010), AAA/GMAE(1012) 및 기타 능력(1014)을 나타낸다.

[0067] 1020에서, M2M 장치(1002)는 국부적 무결성 확인을 수행할 수 있다. 1024에서, M2M 게이트웨이(1004)는 국부적 무결성 확인을 수행할 수 있다. 1028에서, 무결성 검증 정보는 M2M 게이트웨이(1004)와 액세스 네트워크(1006)

사이에서 공유될 수 있다. 1032에서, M2M 장치(902)는 액세스 네트워크(1006)를 획득할 수 있다. 1036에서, M2M 장치(1002)와 액세스 네트워크(1006) 사이에 액세스 인증(무결성 검증 정보를 포함할 수 있음)이 구축될 수 있다. 1040에서, 액세스 네트워크(1006)와 인증 서버(1008) 사이에 액세스 인증(무결성 검증 정보를 포함할 수 있음)이 구축될 수 있다. 케이스 2의 연결에서, M2M 장치는 M2M 게이트웨이를 통해 M2M 시스템에 연결될 수 있다. 무결성 확인 및 검증은 M2M 장치 및/또는 M2M 게이트웨이에서 수행되어야 할 것이다. M2M 게이트웨이는 자율적 검증 또는 반 자율적 검증을 수행할 수 있다. 이것은 장치에서 자율적 또는 반 자율적 검증에 무관하게 실행될 수 있다.

[0068] 게이트웨이는 보안 부트 처리를 이용하여 국부적 무결성 확인을 수행할 수 있고 자율적 검증이 이용된 경우 국부적 무결성 확인의 결과에 대한 검증을 국부적으로 수행할 수 있다. 반 자율적 검증이 이용된 경우, 게이트웨이는 국부적 무결성 확인의 결과를 오퍼레이터의 네트워크 내에서 플랫폼 검증 엔티티로 전송할 수 있다. 플랫폼 검증 엔티티는 오퍼레이터의 AAA 서버, 예컨대 AAA/GMAE(1012)와 공동으로 배치될 수 있다. 성공적인 무결성 확인 및 검증에 후속하여, 게이트웨이는 서비스를 제공하기 위해 M2M 장치에 유효할 수 있는 대기 상태로 시동될 수 있다. M2M 장치는 보안 부트 처리를 이용하여 국부적 무결성 확인을 수행할 수 있고, 자율적 검증이 이용된 경우, 국부적 무결성 확인의 결과에 대한 검증을 국부적으로 행할 수 있다. 반 자율적 검증이 이용된 경우, M2M 장치는 M2M 게이트웨이를 탐색하고 그 결과를 오퍼레이터의 네트워크에서 플랫폼 검증 엔티티로 전송하는 것에 의해 네트워크를 획득할 수 있다. M2M 게이트웨이는 보안 게이트웨이로서 동작하여 M2M 장치에 대해 장치 무결성 검증 절차로 제한될 수 있는 네트워크로의 액세스를 제공하도록 액세스 제어를 수행할 수 있다. 플랫폼 검증 엔티티는 장치 무결성 검증을 수행하고 장치 및 게이트웨이에 그 결과를 알려줄 수 있다. 결과가 성공적이면, 1048에서, 액세스 네트워크와 코어 네트워크에 대한 부트스트래핑, 등록 및 인증의 절차를 위해 M2M 장치(1002)와 액세스 네트워크(1006) 사이에 링크 및 네트워크 세션 셋업이 형성될 수 있다. M2M 액세스 인증이 성공적이면, 1044에서 이 결과는 단일의 개시 신호에 대해 M2M 시스템에 사용될 수 있다. M2M 액세스 네트워크 아이덴티티 및 인증 결과는 M2M 시스템 아이덴티티 및 인증에 이용될 수 있다. M2M 액세스 네트워크(1006)에 의한 성공적인 인증은 다른 M2M 영역 네트워크에서, M2M 시스템 또는 M2M 코어, 또는 M2M 네트워크 또는 다른 서비스 제공자에 의해 제공되는 하나 이상의 서비스 능력 또는 어플리케이션에 의한 성공적인 식별 및 인증을 의미할 수 있다. 부트스트래핑과 M2M 등록이 후속할 수 있다. 예를 들면, 1052에서 M2M 장치(1002)는 보안 능력(1010)에 M2M 부트스트래핑을 요청할 수 있다. 1056에서, M2M 장치(1002)와 보안 능력(1010) 사이에 M2M 보안 부트스트래핑이 행해질 수 있다. 1060에서, 보안 능력(1010)과 AAA/GMAE(1012) 사이에 장치 권한 설정(M2M NAI 및 루트 키)이 행해질 수 있다. 1064에서, M2M 장치(1002)와 보안 능력(1010) 사이에 인증 및 세션 키를 포함할 수 있는 M2M 등록이 행해질 수 있다. 1068에서, 보안 능력(1010)과 AAA/GMAE(1012) 사이에 M2M 인증이 행해질 수 있다. 1072에서, 보안 능력(1010)은 암호화 키를 다른 능력(1014)에 제공할 수 있다.

[0069] 케이스 3의 장치 및 게이트웨이의 무결성 및 등록은 도 11에 예시된 흐름 중 하나 이상을 포함할 수 있다. 도 11은 M2M 장치(1102), M2M 게이트웨이(1104), 액세스 네트워크(1106)(예, 네트워크 오퍼레이터와 관련된), 인증 서버(1108)(예, 네트워크 오퍼레이터와 관련됨), 보안 능력(1110), AAA/GMAE(1112) 및 기타 능력(1114)을 나타낸다.

[0070] 1120에서, M2M 장치(1102)는 국부적 무결성 확인을 수행할 수 있다. 1124에서, M2M 게이트웨이(1104)는 국부적 무결성 확인을 수행할 수 있다. 1128에서, 무결성 검증 정보를 포함할 수 있는 액세스 인증이 M2M 게이트웨이(1104)와 인증 서버(1108) 사이에서 행해질 수 있다. 1132에서, M2M 장치(1102)와 M2M 게이트웨이(1104) 사이에 장치 무결성 검증을 포함할 수 있는 모세관 등록 및 인증이 행해질 수 있다.

[0071] 1136에서, M2M 게이트웨이(1104)는 액세스 네트워크(1106)를 획득할 수 있다. 1140에서, M2M 게이트웨이(1104)와 액세스 네트워크(1106) 사이에 액세스 인증(무결성 검증 정보를 포함할 수 있음)이 구축될 수 있다. 1144에서, 액세스 네트워크(1106)와 인증 서버(1108) 사이에 액세스 인증(무결성 검증 정보를 포함할 수 있음)이 구축될 수 있다. M2M 액세스 네트워크 인증이 성공적이면, 1148에서, 이 결과는 단일의 개시 신호에 대해 M2M 시스템에 사용될 수 있다.

[0072] 케이스 3의 연결에서, M2M 게이트웨이는 네트워크를 향하는 M2M 장치로서 동작할 수 있다. 도 11에 예시된 바와 같이, 다음의 무결성 확인 및 검증 절차 중 하나 이상의 절차가 후속될 수 있다.

[0073] 게이트웨이는 보안 부트 처리를 이용하여 국부적 무결성 확인을 수행할 수 있고 자율적 검증이 이용된 경우 국부적 무결성 확인의 결과에 대한 검증을 국부적으로 수행할 수 있다. 반 자율적 검증이 이용된 경우, 게이트웨이는 국부적 무결성 확인의 결과를 오퍼레이터의 네트워크(액세스 네트워크 오퍼레이터 또는 M2M 네트워크 오퍼

레이터) 내에서 플랫폼 검증 엔티티로 전송할 수 있다. 플랫폼 검증 엔티티는 오퍼레이터(액세스 네트워크 오퍼레이터 또는 M2M 네트워크 오퍼레이터)의 AAA 서버와 공동으로 배치될 수 있다. 성공적인 무결성 확인 및 검증에 후속하여, 게이트웨이는 서비스를 제공하기 위해 M2M 장치에 유효할 수 있는 대기 상태로 시동될 수 있다. 이 경우, M2M 게이트웨이는 케이스 1의 연결에 의해 연결되는 네트워크에 대한 M2M 장치로서 등장함에 유의하라. 전술된 케이스 1의 연결의 경우에 기술된 절차는 M2M 장치로서 동작하는 M2M 게이트웨이에 의해 후속될 수 있다.

[0074] M2M 게이트웨이가 M2M 액세스 네트워크 및 M2M 서비스 능력에 의한 자체의 무결성 확인 및 검증이 완료된 후, 이는 게이트웨이에 연결되는 것을 원할 수 있는 M2M 장치에 대해 유효해질 수 있다. M2M 장치는 보안 부트 처리를 이용하여 국부적 무결성 확인을 수행할 수 있고, 자율적 검증이 이용된 경우, 국부적 무결성 확인의 결과에 대한 검증을 국부적으로 행할 수 있다. 반 자율적 검증이 이용된 경우, M2M 장치는 M2M 게이트웨이를 탐색하고 그 결과를 M2M 게이트웨이로 전송하는 것에 의해 네트워크를 획득할 수 있다. M2M 게이트웨이는 플랫폼 검증 엔티티로서 동작하여 장치 무결성 검증 절차를 수행하고 장치에 그 결과를 알려줄 수 있다. 결과가 성공적이면, 1152에서, M2M 게이트웨이에 대한 부트스트래핑, 등록 및 인증의 절차를 위해 M2M 게이트웨이(1104)와 액세스 네트워크(1106) 사이에 링크 및 네트워크 세션 셋업이 형성될 수 있다.

[0075] M2M 장치는 액세스 네트워크 및/또는 코어 네트워크에 대해 부트스트래핑, 등록 및 인증의 절차를 수행할 수 있다. 예를 들면, 1156에서 M2M 게이트웨이(1104)는 보안 능력(1110)에 M2M 부트스트래핑을 요청할 수 있다. 1160에서, M2M 게이트웨이(1104)와 보안 능력(1110) 사이에 M2M 보안 부트스트래핑이 행해질 수 있다. 1164에서, 보안 능력(1110)과 AAA/GMAE(1112) 사이에 장치 권한 설정(M2M NAI 및 루트 키)이 행해질 수 있다. 1068에서, M2M 게이트웨이(1104)와 보안 능력(1110) 사이에 인증 및 세션 키를 포함할 수 있는 M2M 등록이 행해질 수 있다. 1172에서, 보안 능력(1110)과 AAA/GMAE(1112) 사이에 M2M 인증이 행해질 수 있다. 1176에서, 보안 능력(1110)은 암호화 키를 다른 능력(1114)에 제공할 수 있다.

[0076] 케이스 3의 연결에서, M2M 게이트웨이에 연결된 M2M 장치는 M2M 시스템에는 보여지지 않을 수 있다. 대안적으로, M2M 장치 또는 M2M 장치의 서브세트는 독립적인 M2M 장치로서 M2M 시스템에 보여질 수 있다. 이 경우, M2M 게이트웨이는 네트워크 프록시로서 작업을 수행하고 인증을 행하며 게이트웨이에 연결된 장치 또는 서브 세트의 장치에 대해 플랫폼 무결성 검증 엔티티로서 동작할 수 있다.

[0077] 케이스 4의 장치 및 게이트웨이의 무결성 및 등록은 도 12에 예시된 흐름 중 하나 이상을 포함할 수 있다. 도 12는 M2M 장치(1202), M2M 게이트웨이(1204), 액세스 네트워크(1206)(예, 네트워크 오퍼레이터와 관련된), 인증 서버(1208)(예, 네트워크 오퍼레이터와 관련됨), 보안 능력(1210), AAA/GMAE(1212) 및 기타 능력(1214)을 나타낸다.

[0078] 1220에서, M2M 장치(1202)는 국부적 무결성 확인을 수행할 수 있다. 1224에서, M2M 게이트웨이(1204)는 국부적 무결성 확인을 수행할 수 있다. 1228에서, 무결성 검증 정보를 포함할 수 있는 액세스 인증이 M2M 게이트웨이(1204)와 인증 서버(1208) 사이에서 행해질 수 있다. 1232에서, M2M 장치(1202)와 M2M 게이트웨이(1204) 사이에 장치 무결성 검증을 포함할 수 있는 모세관 등록 및 인증이 행해질 수 있다.

[0079] 1236에서, M2M 게이트웨이(1204)는 액세스 네트워크(1206)를 획득할 수 있다. 1240에서, M2M 게이트웨이(1204)와 액세스 네트워크(1206) 사이에 액세스 인증(무결성 검증 정보를 포함할 수 있음)이 구축될 수 있다. 1244에서, 액세스 네트워크(1206)와 인증 서버(1208) 사이에 액세스 인증(무결성 검증 정보를 포함할 수 있음)이 구축될 수 있다. M2M 액세스 네트워크 인증이 성공적이면, 1248에서, 이 결과는 이 결과는 단일의 개시 신호에 대해 M2M 시스템에 사용될 수 있다.

[0080] 케이스 4의 연결에서, M2M 게이트웨이는 장치를 향하는 네트워크용 프록시로서 동작할 수 있다. 도 12에 예시된 바와 같이, 다음의 무결성 확인 및 검증 절차 중 하나 이상의 절차가 후속될 수 있다.

[0081] 게이트웨이는 보안 부트 처리를 이용하여 국부적 무결성 확인을 수행할 수 있고 자율적 검증이 이용된 경우 국부적 무결성 확인의 결과에 대한 검증을 국부적으로 수행할 수 있다. 반 자율적 검증이 이용된 경우, 게이트웨이는 국부적 무결성 확인의 결과를 오퍼레이터의 네트워크(액세스 네트워크 오퍼레이터 또는 M2M 네트워크 오퍼레이터) 내에서 플랫폼 검증 엔티티로 전송할 수 있다. 플랫폼 검증 엔티티는 오퍼레이터(액세스 네트워크 오퍼레이터 또는 M2M 네트워크 오퍼레이터)의 AAA 서버와 공동으로 배치될 수 있다. 성공적인 무결성 확인 및 검증에 후속하여, 게이트웨이는 서비스를 제공하기 위해 M2M 장치에 유효할 수 있는 대기 상태로 시동될 수 있다. M2M 게이트웨이가 M2M 액세스 네트워크에 의한 자체의 무결성 확인 및 검증이 완료된 후, 이는 게이트웨이에 연

결되는 것을 원할 수 있는 M2M 장치에 대해 유효해질 수 있다.

[0082] M2M 장치는 보안 부트 처리를 이용하여 국부적 무결성 확인을 수행할 수 있고, 자율적 검증이 이용된 경우, 국부적 무결성 확인의 결과에 대한 검증을 국부적으로 행할 수 있다. 반 자율적 검증이 이용된 경우, M2M 장치는 M2M 게이트웨이를 탐색하고 그 결과를 M2M 게이트웨이로 전송하는 것에 의해 네트워크를 획득할 수 있다. 장치의 검증은 분할된 형태의 M2M 게이트웨이와 M2M 액세스 네트워크 및 M2M 서비스 계층 능력의 플랫폼 검증 엔티티에 의해 수행될 수 있다. 예시적인 검증 처리 방법은: M2M 게이트웨이에서 배타적으로 처리되고; 액세스 네트워크에 의해 처리되고; 검증 엔티티에 배치된 M2M 서비스 계층 능력에 의해 처리되거나; 검증의 정교성(granularity)이 분할된 형태로 수행되는 검증 엔티티에 의해 수행될 수 있다.

[0083] M2M 게이트웨이의 플랫폼 검증 엔티티는 대략적인 검증 후에 높은 수준의 검증 엔티티에 의한 정밀한 검증이 또는 그 반대로 수행될 수 있다. 정밀한 무결성 검증은 M2M 게이트웨이(1204)와 인증 서버(1208) 사이에 행해질 수 있다. M2M 장치(1202)와 M2M 게이트웨이(1204) 사이에 영역 네트워크 프로토콜 메시지를 사용하는 정밀 무결성 검증이 행해질 수 있다. 이러한 메커니즘은 장치 무결성 확인 결과가 장치 아키텍처를 반영하는 트리 형태로 수집되는 트리형 검증에 사용될 수 있다. 트리는 부모 노드(parent node)의 검증이 리프 노드(leaf node) 모듈을 나타낼 수 있도록 구성될 수 있다. 이러한 개념은 루트 노드가 형성되고 루트 노드 측정의 확인이 전체 트리를 검증하여 소프트웨어 모듈을 나타내는 리프 노드를 검증할 때까지 순환적으로 적용될 수 있다. 서브 트리는 소프트웨어 구조에 따라 구성될 수 있다. M2M 게이트웨이 검증 엔티티는 일련의 서브 트리를 확인하는 것에 의해 낮은 정교성의 확인을 수행할 수 있다. 이러한 정보는 액세스의 검증 엔티티 또는 M2M 오퍼레이터의 검증 엔티티로 전달될 수 있다. 네트워크 내의 검증 엔티티는 그 결과를 평가할 수 있고 그 평가를 기초로 정밀한 검증의 수행을 결정할 수 있다. 검증 엔티티는 M2M 게이트웨이 내의 검증 엔티티에 대해 정밀한 검증 시험의 결과를 획득하도록 지시할 수 있다. 리포팅 결과는 M2M 게이트웨이(1204)와 인증 서버(1208) 사이에서 교환될 수 있다. 따라서, M2M 게이트웨이는 계층화된 형태로 플랫폼 검증 엔티티로서 동작할 수 있고, 네트워크를 위한 프록시로서 등장하며, 장치 무결성 검증 절차를 수행할 수 있고, 장치에 대해 그 결과를 알려줄 수 있다. 결과가 성공적이면, 1252에서, 장치는 M2M 게이트웨이(1204)에 대한 부트스트래핑, 등록 및 인증의 절차를 위해 M2M 게이트웨이(1204)와 액세스 네트워크(1206) 사이에 링크 및 네트워크 세션 셋업을 시작할 수 있다. 대안적으로, 장치는 액세스 네트워크와 코어 네트워크에 대한 부트스트래핑, 등록 및 인증의 절차를 시작할 수 있다. M2M 게이트웨이에 연결된 M2M 장치는 M2M 시스템에는 보여지지 않을 수 있다. 대안적으로, M2M 장치 또는 M2M 장치의 서브세트는 독립적인 M2M 장치로서 M2M 시스템에 보여질 수 있다. 이 경우, M2M 게이트웨이는 네트워크 프록시로서 작업을 수행하고 인증을 행하며 게이트웨이에 연결된 장치 또는 서브 세트의 장치에 대해 플랫폼 무결성 검증 엔티티로서 동작할 수 있다.

[0084] M2M 네트워크는 많은 장치 그룹의 무결성, 예컨대 전체 네트워크에 상당하는 장치와 그 게이트웨이의 무결성을 M2M 게이트웨이에 의해 용이하게 될 수 있는 계층화된 검증 방법을 이용하여 검증할 수 있다.

[0085] M2M 게이트웨이는 우선 게이트웨이에 연결된 장치(예, 모든 장치, 여러 그룹의 장치, 서브 세트의 장치 등)로부터 개별 장치의 무결성 증거(예, 해시)를 수집할 수 있다. 무결성 증거는 개별 트리의 루트가 개별 장치의 장치 무결성의 최고 수준의 요약을 나타내는 반면, 그 가지는 개별 장치의 기능 또는 능력을 나타내고 트리의 잎은 제한되는 것은 아니지만 SW 이진 파일, 설정 파일 또는 하드웨어 성분 무결성의 개별 표지와 같은 개별 파일/성분을 나타낼 수 있는 트리 구조의 형태일 수 있다.

[0086] M2M 게이트웨이의 개시 또는 M2M 서버(검증 서버, Home eNode-B에서의 플랫폼 검증 엔티티(PVE), 또는 M2M에서의 플랫폼 검증 권한(PVA)일 수 있음)의 개시에 의해, M2M 게이트웨이는 1) 자체의 게이트웨이 기능의 장치 무결성에 대한 종합 정보와 2) M2M 게이트웨이에 연결된 M2M 장치(예, 모든 장치, 여러 그룹의 장치, 서브 세트의 장치 등)의 무결성에 대한 높은 수준의 요약 정보를 M2M 서버로 전송할 수 있다.

[0087] M2M 게이트웨이로부터 정보를 수신하고 평가한 후, M2M 서버는 그 무결성이 이전에 리포팅된 M2M 게이트웨이 또는 M2M 장치(예, 모든 장치, 여러 그룹의 장치, 서브세트의 장치 등)의 무결성에 대한 보다 상세한 정보를 요청할 수 있다. 이러한 요청을 수신한 후, M2M 게이트웨이는 예컨대, 1) 게이트웨이 자체 또는 게이트웨이가 이미 사전에 수집하여 그 저장소에 가지고 있는 M2M 장치의 무결성에 대한 보다 상세한 정보를 M2M 서버로 전송하거나, 2) 그러한 상세한 정보를 수집한 후 M2M 서버로 전송할 수 있다. 이러한 "보다 상세한 정보"는 트리의 루트가 M2M 게이트웨이와 해당 게이트웨이에 연결된 M2M 장치(예, 모든 장치, 여러 그룹의 장치, 서브세트의 장치 등)로 이루어진 전체 서브 네트워크의 무결성에 대한 높은 레벨의 요약을 보여주고 하부 노드와 잎은 장치에 대한 기능과 같이 낮은 레벨의 보다 상세한 정보를 나타낼 수 있는 트리 또는 트리형 구조의 데이터로부터 찾을

수 있다. 도 13은 계층화된 검증의 예시적인 시나리오를 나타낸다. 큰 삼각형(1310)은 삼각형의 정점이 M2M 게이트웨이(1300)에 의해 조직된 전체 서브 네트워크의 전반적인 건강성을 나타내는 무결성 데이터의 높은 수준의 요약 버전을 표현하고 있는 트리 또는 트리형 구조를 나타낼 수 있다. 큰 트리는 그 일부로서 하나 이상의 작은 삼각형 형상(1315)을 포함할 수 있으며, 각각은 삼각형 형상은 M2M 게이트웨이(1300)에 의해 조직된 서브 네트를 포함하는 장치(1330) 중 하나 이상의 장치에 대한 무결성 정보를 나타낼 수 있다.

[0088] 또한, M2M 게이트웨이(1300)는 종류, 등급, 또는 기타의 기술자(descriptor)를 기초로 연결 장치를 그룹화하고, 가능하게는 그 무결성 트리에 대해 그룹 인증을 행할 수 있다. 이것은 내부에 인증서를 갖는 작은 삼각형 1317에 의해 도 13에 표현된다. 이러한 신뢰되는 인증서의 사용은 멀티-네트워크 운용(MNO) 네트워크(1320)가 리포팅된 무결성 값에 보다 큰 신뢰를 갖도록 하는 것을 용이하게 할 수 있다.

[0089] 전술한 시나리오는 M2M 장치가 서로 또는 전용 검정 노드가 존재할 수 있는 검정 노드를 갖는 클러스터 내에서, 또는 임의의 노드가 검정 노드의 역할을 할 수 있는 애드-혹(ad-hoc) 노드에서 트리 또는 트리형 무결성 제공 데이터 구조를 교환하고 증명하는 피어-투-피어(peer-to-peer)(P2P) 접근에 적용되거나 그러한 접근을 포함할 수 있다.

[0090] 네트워크와 어플리케이션 도메인의 서비스 능력에서 서비스 능력(SC)은: 키 관리, 인증 및 세션 키 관리 또는 장치 무결성 검증 중 하나 이상을 제공할 수 있다.

[0091] 키 관리는 인증을 위해 장치 내의 보안 키(예, 미리 공유된 보안 키, 인증서 등)의 부트스트래핑에 의해 보안 키를 어떻게 관리하는 것을 포함할 수 있다.

[0092] 인증 및 세션 키 관리는 다음 중 하나 이상을 수행하도록 구성될 수 있다: 인증을 통한 계층 등록 서비스; M2M 장치/M2M 게이트웨이와 SC 사이의 세션 키 관리 서비스; 서비스 제공 전 어플리케이션의 인증; M2M 장치와 M2M 게이트웨이 간의 교환된 데이터 상의 암호화/무결성 보호를 수행(메시지 능력에 의해)하도록 메시지 능력에 대해 협상된 세션 키의 전달; 또는 어플리케이션이 터널 보안(예, 홈 게이트웨이와 메시징을 위한 서비스 능력 엔티티 사이의 터널)을 필요로 하는 경우 M2M 게이트웨이와 장치로부터 보안 터널 세션의 셋업. 장치 무결성 검증은 장치 또는 게이트웨이의 무결성을 검증하도록 구성될 수 있다.

[0093] M2M 장치 또는 M2M 게이트웨이 내의 SC는 다음 중 하나 이상을 수행하도록 구성될 수 있다: 인증을 위해 장치 내의 보안 키(예, 미리 공유된 보안 키 또는 인증서)의 부트스트래핑에 의해 보안 키의 관리; 어플리케이션에 의해 필요시 세션 구축 전에 인증의 실시; 시그널링 메시지를 위해 무결성 보호와 트래픽의 암호화와 같은 세션 보안 관련 기능; (가능한 장치/게이트웨이의 경우) 장치(또는 게이트웨이)의 무결성의 측정, 검증 및/또는 리포팅의 수행; 보안 시간 동기화의 절차의 지원; 적용 가능한 보안 특정 서비스 클래스 특성의 협상 및 이용; 결함 복구 메커니즘의 지원; 또는 M2M 장치의 M2M 코어로의 액세스 제어의 지원.

[0094] 다양한 특징 및 요소가 특정 조합으로 전술되었지만, 각각의 특징 또는 요소는 그밖의 특징 및 요소 없이 단독으로 또는 다른 특징 및 요소를 갖거나 갖지 않고 다양한 조합으로 사용될 수 있다. 여기 제공된 방법 또는 흐름은 범용 컴퓨터 또는 프로세서에 의한 실행을 위해 컴퓨터 판독 가능 저장 매체에 포함된 컴퓨터 프로그램, 소프트웨어, 또는 펌웨어로 실행될 수 있다. 컴퓨터 판독 가능 저장 매체의 예로는 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 레지스터, 캐시 메모리, 반도체 메모리 소자, 내장 하드 디스크와 분리 가능한 디스크와 같은 자기 매체, 광자기 매체 및 CD-ROM 디스크와 DVDs와 같은 광학 매체를 포함한다.

[0095] 예로써, 적절한 프로세서는 범용 프로세서, 특수 목적 프로세서, 통상의 프로세서, 디지털 신호 프로세서(DSP), 복수의 마이크로프로세서, DSP 코어와 결합된 하나 이상의 마이크로프로세서, 컨트롤러, 마이크로컨트롤러, 주문현 반도체(ASICs), 필드 프로그래밍 가능한 게이트 어레이(FPGAs) 회로, 임의의 다른 종류의 집적 회로(IC), 및/또는 상태 머신(state machine)을 포함한다.

[0096] 소프트웨어와 결합된 프로세서는 무선 송수신 유닛(WTRU), 사용자 장비(UE), 단말기, 기지국, 무선 네트워크 제어기(RNC) 또는 임의의 호스트 컴퓨터에 사용되는 무선 주파수 송수신기의 구현에 사용될 수 있다. WTRU는 카메라, 비디오 카메라 모듈, 비디오폰, 스피커폰, 진동 장치, 스피커, 마이크로폰, 텔레비젼 수상기, 핸즈프리 헤드셋, 키보드, 블루투스 모듈, 주파수 변조(FM) 라디오 유닛, LCD 디스플레이 장치, 유기발광 다이오드(OLED) 디스플레이 장치, 디지털 음악 플레이어, 미디어 플레이어, 비디오 게임 플레이어 모듈, 인터넷 브라우저, 및/또는 임의의 무선 근거리 네트워크(WLAN) 또는 초광대역(UWB) 모듈과 같은 하드웨어 및/또는 소프트웨어로 실현되는 모듈과 함께 사용될 수 있다.

[0097] 전술한 개시물과 함께 또는 그 일부로서 실현될 수 있는 시스템, 방법 및 수단을 이하에 개시한다.

[0098] 도 14는 예시적인 M2M 아키텍처를 보여준다. 해당 다이어그램은 사물 지능 통신(machine-to-machine: M2M) 네트워크 상의 M2M 서비스 능력(1430)과 M2M 장치/게이트웨이 엔티티를 포함한다. 도 14는 M2M 장치/M2M 게이트웨이(1410), 능력 레벨 인터페이스(1460), M2M 서비스 능력(1430), M2M 어플리케이션(1420), 리소스 인터페이스(1490), 코어 네트워크 A(1440), 코어 네트워크 B(1450)를 포함한다. M2M 장치/M2M 게이트웨이(1410)는 M2M 어플리케이션(1412), M2M 능력(1414), 및 통신 모듈(1416)을 포함할 수 있다. M2M 서비스 능력(1430)은 범용 M2M 어플리케이션 가능 능력(1470)은 물론, 능력(C1, C2, C3, C4, C5)을 포함할 수 있다.

[0099] 도 15는 M2M 네트워크 계층의 M2M 서비스 능력의 예시적인 내부 기능 아키텍처를 예시한다. 예시된 바와 같이, 도 15는 도 14의 성분을 포함할 수 있다. 도 15에서, M2M 네트워크 서비스 계층은 : 범용 메시지 전달(GM); 도달성(reachability)(60), 어드레싱 및 장치 어플리케이션 저장소(RADAR)(30); 네트워크 및 통신 서비스 선택(NCSS)(20); M2M 장치 및 M2M 게이트웨이 관리(MGDM)(10); 이력화(historization) 및 데이터 보유(HDR)(70); 범용 M2M 어플리케이션 가능(GMAE)(1470); 보안 능력(SC)(50); 또는 트랜잭션 관리(TM)(40)를 포함하는, 하나 이상의 능력을 포함할 수 있다.

[0100] 케이스 A의 연결의 경우, M2M 장치는 서비스 능력의 관점으로부터 보면 M2M 액세스 네트워크에 직접 연결될 수 있다. 이러한 의미에서, 여기 설명된 케이스 1과 케이스 2의 연결은 케이스 A의 연결의 예로 간주될 수 있다. M2M 네트워크가 모세관 네트워크를 통해 알 수 없는 주변 장치에 연결되면서도 M2M 액세스 네트워크에 연결되는 M2M 게이트웨이가 존재한다면, 이러한 M2M 게이트웨이는 M2M 액세스 네트워크에 직접 연결되어 예컨대 케이스 1의 연결을 달성하는 M2M 장치로 간주될 수 있다.

[0101] 케이스 B의 연결의 경우, M2M 게이트웨이는 네트워크 프록시로서 동작하여 게이트웨이에 연결된 M2M 장치의 인증, 허가, 등록, 장치 관리 및 권한 설정의 절차를 수행할 수 있고, M2M 네트워크와 어플리케이션을 대신하여 어플리케이션을 실행할 수 있다. 케이스 B의 연결의 경우, M2M 게이트웨이는 국부적으로 M2M 장치 상의 어플리케이션으로부터 나오거나 M2M 네트워크 및 어플리케이션 도메인으로 발신되는 라우딩 서비스 계층 요청에 대해 결정을 행할 수 있다. 여기 설명된 연결 케이스 3과 4는 연결 케이스 B의 예일 수 있다.

[0102] M2M 게이트웨이를 위한 서비스 능력에 대한 새로운 아키텍처와 특정 기능을 이하에 상세히 설명한다.

[0103] 도 16a와 도 16b는 M2M 게이트웨이와 그 인터페이스의 예시적인 기능적 아키텍처를 보여준다. 도 16a와 도 16b는 여기 설명되는 추가의 성분은 물론, 게이트웨이 M2M 서비스 능력(1610), 네트워크 M2M 서비스 능력(1650), M2M 어플리케이션(1612), M2M 어플리케이션(1652), 능력 레벨 인터페이스(1615), 능력 레벨 인터페이스(1655), M2M 장치(1630), 모세관 네트워크(1635), 및 모세관 네트워크(1675)를 포함한다. 고려되는 서비스 능력은 gGMAE(1620), gGM(26), gMDGM(21), gNCSS(22), gRADAR(23) 및 gSC(24)를 포함할 수 있다. 이들 능력 각각은 M2M 코어의 (1650), GM(65), MDGM(61), NCSS(62), RADAR(63) 및 SC(64)의 능력 각각에 대응하고 프록시로서 동작하는 M2M 게이트웨이의 능력일 수 있다.

[0104] M2M 네트워크의 프록시로서 동작하는 M2M 게이트웨이에 적용 가능한 각각의 이들 M2M 게이트웨이 능력에 대한 높은 레벨의 기능성을 이하 상세히 설명한다.

[0105] gGMAE(1620)는 네트워크 및 어플리케이션 도메인(NAD)의 GMAE(1660)의 프록시로서 동작하고, 1) 네트워크 프록시 M2M 게이트웨이에 연결되는 M2M 장치를 위한 어플리케이션과 2) M2M 게이트웨이 자체를 위한 어플리케이션을 제공할 수 있는 M2M 게이트웨이의 능력이다.

[0106] gGM(26)은 NAD의 GM(65)의 프록시로서 동작하는 M2M 게이트웨이 능력으로서, 다음의 대상체 중 하나 이상의 사이에서 메시지를 전송할 수 있는 능력을 제공할 수 있다: M2M 장치, 네트워크-프록시 M2M 게이트웨이, 네트워크-프록시 M2M 게이트웨이에 상주하는 프록시 서비스 능력, gGMAE(1620)에 의해 인에이블되는 M2M 어플리케이션, NAD의 서비스 능력, NAD에 상주하는 M2M 어플리케이션.

[0107] gMDGM(21)은 NAD의 MDGM(61)의 프록시로서 동작하는 M2M 게이트웨이 능력으로서, M2M 게이트웨이 자체의 모든 능력 및 인터페이스는 물론, 해당 요소에 연결된 M2M 장치 양자에 대해 설정 관리(CM), 성능 관리(PM), 및 결함 관리(FM)와 같은 관리 기능을 제공할 수 있다.

[0108] gNCSS(22)는 NAD의 NCSS(62)의 프록시로서 동작하는 M2M 게이트웨이 능력으로서, M2M 게이트웨이 자체에는 물론 해당 요소에 연결된 M2M 장치에 대해 통신 및 네트워크 서비스 선택 능력을 제공할 수 있다.

[0109] gRADAR(23)는 NAD의 RADAR(63)의 프록시로서 동작하는 M2M 게이트웨이 능력이다. 해당 기능은 아래의 설명을

포함한다.

[0110] gSC(24)는 NAD의 SC(64)의 프록시로서 동작하는 M2M 게이트웨이 능력이다.

[0111] NAD 내에 대응 요소를 갖는 이들 능력 외에, 포함될 수 있는 gMMC(25)로 지칭되는 M2M 게이트웨이 능력은 서비스 및 어플리케이션 도메인에서 M2M 게이트웨이에 걸친 M2M 장치의 이동(mobility)을 관리하기 위한 기능을 수행한다. 이러한 능력 gMMC(25)는 상기의 도 15에도 보이지 않지만, 그럼에도 네트워크-프록시 게이트웨이에 상주하는 것으로 간주될 수 있다.

[0112] 게이트웨이 서비스 능력은 도 16a에 나타낸 바와 같이 "_DG", "_G", "_GN"으로 지시된 다중(예, 3개) 서브-능력을 포함할 수 있다. "gX" 기능의 경우, "gX_DG"는 게이트웨이에 연결된 M2M 장치와 상호 작용을 담당하는 서브-능력을 지시하고, "gX_G"는 "gX"의 능력의 일부인 게이트웨이의 자율적 기능을 담당하는 서브-능력을 지시하며, "gX_GN"은 M2M 서비스 코어와의 상호 작용을 담당하는 서브-능력을 지시할 수 있다.

[0113] 이들 능력 외에, 도 16a와 도 16b에 예시된 바와 같이, 네트워크-프록시 M2M 게이트웨이의 아키텍처는 M2M 장치 또는 M2M 네트워크 및 그 다양한 능력을 위한 네트워크-프록시 M2M 게이트웨이로부터의 인터페이스는 물론, 전술한 능력 사이에 다수의 인터페이스를 포함할 수 있다. 예시적인 인터페이스 명칭은 도 16a와 도 16b에 예시된다.

[0114] 다음 중 하나 이상이 게이트웨이 범용 M2M 어플리케이션 가능(gGMAE) 능력에 적용될 수 있다.

[0115] M2M 어플리케이션은 M2M 장치, M2M 게이트웨이나 M2M 네트워크 및 어플리케이션 도메인에 상주할 수 있다.

[0116] gGMAE(1620)과 같은 gGMAE의 기능은 네트워크-기초한 GMAE(1660)을 위한 다음의 것 중 하나 이상을 포함할 수 있다.

[0117] gGMAE는 도 16a의 gIa와 같은 단일 인터페이스를 통해 M2M 코어의 서비스 능력과 M2M 게이트웨이의 네트워크-프록시 서비스 능력에 구현되는 기능을 노출시킬 수 있다. gGMAE는 게이트웨이 서비스 위상을 숨김으로써 M2M 게이트웨이의 다른 네트워크-프록시 서비스 능력을 이용하기 위해 M2M 어플리케이션에 의해 필요한 정보는 gGMAE 능력의 어드레스로 제한될 수 있다. gGMAE는 M2M 어플리케이션이 게이트웨이 서비스 능력에 등록되도록 하는 것을 허용할 수 있다.

[0118] 또한, gGMAE는 특정 세트의 능력에의 액세스를 허용하기 전에 M2M 어플리케이션의 인증 및 허가를 수행하도록 구성될 수 있다. M2M 어플리케이션이 액세스할 수 있는 능력 세트는 M2M 어플리케이션 제공자와 서비스 능력 운용 제공자 간의 사전 승낙을 취하여야 할 것이다. M2M 어플리케이션과 서비스 능력이 동일한 엔티티에 의해 운용되는 경우, 인증 요건은 완화될 수 있다. 인터페이스(gIa)에 대한 특정 요청이 해당 요청을 다른 능력으로 라우팅하기 전에 유효한지도 확인할 수 있다. 요청이 유효하지 않으면, M2M 어플리케이션으로 에러가 리포팅될 수 있다.

[0119] gGMAE는 또한 M2M 어플리케이션과 프록시 서비스 능력 중의 능력 간에 라우팅을 수행하도록 구성될 수 있다. 라우팅은 특정 요청이 특별한 능력으로 전송되도록 하는 메커니즘 또는 예컨대 로드(load) 밸런싱이 실현될 때 해당 능력의 경우에 의해 정해질 수 있다. gGMAE는 다른 프록시 서비스 능력 간에 라우팅을 수행할 수 있다. 또한, gGMAE는 서비스 능력의 사용에 속하는 차징 기록(charging records)을 생성할 수 있다.

[0120] 추가로, M2M 게이트웨이의 gGMAE 능력은 M2M 장치의 등록, 인증 및 허가의 상태 및/또는 결과를 M2M NAD에서의 GMAE 능력으로 리포팅하는 것을 수행하도록 구성될 수 있다. 이러한 리포팅은 다음 중 하나 이상에 의해 수행될 수 있다:

[0121] 장치 내에 국부적으로 및/또는 외부 타이밍 동기화에 제공되는 타이머를 주기적으로 사용한 자체의 개시에 의해.

[0122] M2M 네트워크의 GMAE 능력으로부터의 명령에 응답하여(예, 온-디맨드(on-demand) 방식).

[0123] 요청에 대한 자체의 개시 및 NAD의 GMAE로부터의 응답을 후속으로 수신하는 것에 의해.

[0124] 다음 중 하나 이상은 RADAR(reachability, addressing and device application repository) 능력에 적용할 수 있다.

[0125] gRADAR(23)와 같은 M2M 게이트웨이 내의 RADAR 능력은 M2M 네트워크 및 어플리케이션 도메인의 정책 및/또는 명령에 따라 M2M 네트워크 및 어플리케이션에서의 서비스 능력으로부터 기본적인 모세관 네트워크 위상, 어드레싱

및 라우팅을 드러내거나 감추는 능력을 제공하도록 구성될 수 있다. 또한, 해당 능력은 M2M 어플리케이션과 서비스 계층 메시지 및 데이터를 릴레이하는 것에 의해 M2M 게이트웨이를 통한 M2M 장치 이동을 지원할 수 있다.

[0126] 또한, gRADAR(23)와 같은 M2M 게이트웨이 내의 RADAR 능력은 장치 어플리케이션 저장소 내에 M2M 장치의 M2M 장치 어플리케이션 등록 정보를 저장하고 해당 정보를 현재까지 유지하는 것에 의해 게이트웨이 장치 어플리케이션 저장소(gDAR)를 유지하는 기능을 제공하도록 구성될 수 있다. 추가로, 해당 능력은 네트워크 및 어플리케이션 도메인에 상주하는 엔티티가 M2M 장치 어플리케이션 등록 정보를 검색할 수 있도록 해당 엔티티를 인증 및 허가하는 질의 인터페이스를 제공하는 것에 의해 기능을 제공할 수 있다. 추가로, 해당 능력은 요청시 해당 정보를 네트워크 및 어플리케이션 도메인에 상주하는 엔티티에 제공하여, 예컨대 요청 엔티티가 이러한 질의를 수행하도록 인증되고 허가되는 것으로 간주하는 것에 의해 기능을 제공할 수 있다.

[0127] (NAD의) gRADAR(23)와 RADAR(63)은 모두 다음 중 하나 이상을 제공하도록 구성될 수 있다: 1) 구름형의 네트워크-기초한 어플리케이션 실행, 2) 다운로드 가능한 어플리케이션-저장형의 어플리케이션 저장소, 또는 3) DRM 권한 발행과 유사한 방식으로, 장치 상의 권한 설정된 어플리케이션의 사용을 등록 및 허가/활성화.

[0128] 다음 중 하나 이상은 네트워크 및 통신 서비스 선택(NCSS) 능력에 적용될 수 있다.

[0129] NCSS(62)와 같은 NCSS 능력은 다음의 기능 중 하나 이상을 포함할 수 있다.

[0130] NCSS 능력은 M2M 어플리케이션으로부터 네트워크 어드레스의 사용을 숨기도록 구성될 수 있다. 해당 능력은 M2M 장치 또는 M2M 게이트웨이가 여러 서브스크립션을 통해 여러 네트워크를 통해 도달될 수 있을 때 네트워크 선택을 제공할 수 있다. 추가로, M2M 장치 또는 M2M 게이트웨이가 여러 네트워크 어드레스를 가지고 있을 때 통신 서비스 선택을 제공할 수 있다.

[0131] 추가로, NCSS 능력은 네트워크 및 통신 서비스 선택을 위해 요청된 서비스 클래스를 고려하도록 구성될 수 있다. 또한, 해당 능력은 통신 실패 후 예컨대, 1차로 선택된 네트워크 또는 통신 서비스를 이용하여 다른 네트워크 또는 통신 서비스 선택을 제공할 수 있다.

[0132] gNCSS(22)와 같은 M2M 게이트웨이 내의 NCSS 능력은 M2M 어플리케이션 및 서비스 계층으로부터 액세스 네트워크의 사용을 숨기도록 구성될 수 있다. 해당 능력은 다중 액세스 네트워크가 유용한 경우 액세스 네트워크 선택을 제공할 수 있다.

[0133] 또한, gNCSS는 네트워크 및 통신 서비스 선택을 위해 요청된 서비스 클래스를 고려하도록 구성될 수 있다. 또한, 해당 능력은 통신 실패 후 예컨대, 1차로 선택된 네트워크 또는 통신 서비스를 이용하여 다른 네트워크 또는 통신 서비스 선택을 제공할 수 있다.

[0134] 다음 중 하나 이상은 보안 능력(SC)에 적용될 수 있다.

[0135] SC(64)와 같은, 네트워크 및 어플리케이션 도메인의 서비스 능력의 SC는 다음 중 하나 이상을 제공하도록 구성될 수 있다: 키 관리, 인증 및 세션 키 관리 또는 장치 무결성 검증.

[0136] 키 관리는 인증을 위해 장치 내의 보안 키(예, 미리 공유된 보안 키, 인증서 등)의 부트스트래핑을 이용하여 보안 키를 관리하는 것을 포함할 수 있다. 또한, 키 관리는 어플리케이션으로부터 권한 설정 정보를 획득하고 필요한 오퍼레이터 네트워크를 알려주는 것을 포함할 수 있다.

[0137] 인증 및 세션 키 관리는 인증을 통해 서비스 계층 등록을 수행하는 것을 포함할 수 있다. 또한, 해당 관리는 M2M 장치/M2M 게이트웨이와 SC 사이에 서비스 세션 키 관리를 수행하는 것을 포함할 수 있다. 또한, 해당 관리는 서비스 제공 전에 어플리케이션을 인증하는 것을 포함할 수 있다.

[0138] 인증 및 세션 키 관리는 M2M 장치 어플리케이션 또는 M2M 게이트웨이 어플리케이션 인증 및 세션 키 관리를 수행하는데 필요한 인증 데이터를 획득하도록 AAA 서버와 인터페이스 연결하는 것을 추가로 포함할 수 있다. SC는 AAA의 용어에서 "인증 기호"로서 사용될 수 있다. 또한, 해당 관리는 M2M 장치와 M2M 게이트웨이 사이에서 교환되는 데이터 상에 암호화/무결성 보호를 수행하도록(메시징 능력에 의해) 협상된 세션 키를 메시지 능력에 전달할 수 있다.

[0139] 인증 및 세션 키 관리는 어플리케이션이 터널 보안(예, 홈 게이트웨이와 서비스 능력 엔티티 사이의 터널: 메시징)이 필요한 경우, M2M 게이트웨이와 장치로부터 보안 터널 세션을 셋업하는 것을 더 포함할 수 있다.

[0140] 장치 무결성 검증은 M2M 네트워크가 장치 무결성 검증을 지원하는 M2M 장치 및 게이트웨이에 대한 장치 및 게이트웨이의 인티그리티를 검증하는 것을 포함할 수 있다. 추가로, M2M 네트워크는 액세스 제어와 같은 사후-검증 동작을 기동시킬 수 있다.

[0141] M2M 장치 또는 M2M 게이트웨이의 SC는 인증을 위해 장치 내의 보안 키(예, 미리 공유된 보안 키, 인증서 등)의 부트스트래핑에 의해 보안 키를 관리하도록 구성될 수 있다. 또한, 해당 능력은 어플리케이션으로부터 권한 설정 정보를 획득하고 필요한 오퍼레이터 네트워크를 알릴 수 있다. 해당 능력은 예컨대 어플리케이션에 의해 필요시 세션 구축 전에 인증을 수행하도록 구성될 수도 있다.

[0142] M2M 장치 또는 M2M 게이트웨이에서의 SC는 메시지의 시그널링을 위해 트래픽의 암호화와 무결성 보호와 같은 세션 보안 관련 기능을 수행하도록 구성될 수 있다. 또한, (가능한 장치/게이트웨이의 경우) 해당 능력은 장치 또는 게이트웨이의 무결성의 검증 및/또는 리포팅을 수행할 수 있다. 추가로, 해당 능력은 (가능한 장치/게이트웨이의 경우) 보안 시간 동기화의 절차를 지원할 수 있다.

[0143] M2M 장치 또는 M2M 게이트웨이에서의 SC는 적용 가능한 보안 특정 서비스 클래스 특성을 협상 및 이용하도록 구성될 수도 있다. 또한, 오퍼레이터의 정책을 조건으로, 해당 능력은 무결성 검증을 수행할 수 있는 M2M 장치가 이 절차에서 실패하면, 임의의 M2M 장치가 네트워크 및 어플리케이션 도메인에 대해 액세스하는 것을 차단할 수 있다.

[0144] NAD-기초 SC는 전술한 기능 외에 M2M 장치의 펌웨어 또는 소프트웨어를 업데이트하기 위해 MDGM 능력을 개시하도록 구성될 수 있다.

[0145] 추가로, 네트워크-프록시 M2M 게이트웨이의 게이트웨이 보안 능력(gSC)을 위해, SC는 M2M 장치 또는 M2M 어플리케이션에 의한 사용을 위해 보안 키를 관리하도록 구성될 수 있다.

[0146] SC는 M2M 장치(NAD에서의 SC의 인증 기능을 위한 프록시로서)의 서비스-레벨 인증을 수행하고 그 결과 서비스 계층과 어플리케이션 등록을 지원할 수 있다.

[0147] SC는 이러한 인증의 결과를 개별 M2M 장치 또는 그룹 단위로 NAD에서의 보안 능력으로 리포팅할 수 있다. SC는 NAD에서의 SC 측으로 자체의 서비스-레벨 인증을 수행할 수 있다.

[0148] SC는 어플리케이션이 이러한 터널 방식의 보안을 필요로 하는 경우 (M2M 장치(들) 또는 M2M 코어 측으로) M2M 게이트웨이로부터 보안 터널 세션을 셋업 및 연동시킬 수 있다. 추가로, SC는 NAD의 SC를 대신하여 M2M 장치의 무결성을 확인 및 검증하는 절차를 수행할 수 있다.

[0149] SC는 개별 M2M 장치 또는 그룹 단위로 이러한 확인 및 검증의 결과를 NAD의 보안 능력으로 리포팅하도록 더 구성될 수 있다. 추가로, SC는 자체의 무결성을 NAD의 보안 능력에 대해 증명하는 절차를 수행할 수 있다. 추가로, SC는 M2M 장치의 펌웨어 또는 소프트웨어를 업데이트하기 위해 (NAD 내의) MDGM 또는 gMDGM 능력의 개시를 포함하는 액세스 제어 및 교정과 같은 M2M 장치를 위한 사후-검정 동작을 시동시킬 수 있다.

[0150] SC는 다음 기능 중 하나 이상을 수행하도록 더 구성될 수 있다: 1) M2M NAD의 능력으로부터 시작되는 명령에 대한 응답, 2) M2M 게이트웨이로부터 자율적으로 생성되는 실행 요청에 후속하여 M2M NAD로부터 수신하는 명령에 대한 응답, 또는 3) gSC가 M2M NAD의 능력(들)에 대한 실행의 절차 또는 결과(들)에 대해 나중에 리포팅을 행하도록 기능에 대하여 자율적으로 개시되는 실행.

[0151] 다양한 특징 및 요소가 특정 조합으로 전술되었지만, 각각의 특징 또는 요소는 그밖의 특징 및 요소 없이 단독으로 또는 다른 특징 및 요소를 갖거나 갖지 않고 다양한 조합으로 사용될 수 있다. 여기 제공된 방법 또는 흐름은 범용 컴퓨터 또는 프로세서에 의한 실행을 위해 컴퓨터 판독 가능 저장 매체에 포함된 컴퓨터 프로그램, 소프트웨어, 또는 펌웨어로 실행될 수 있다. 컴퓨터 판독 가능 저장 매체의 예로는 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 레지스터, 캐시 메모리, 반도체 메모리 소자, 내장 하드 디스크와 분리 가능한 디스크와 같은 자기 매체, 광자기 매체 및 CD-ROM 디스크와 DVDs와 같은 광학 매체를 포함한다.

[0152] 예로써, 적절한 프로세서는 범용 프로세서, 특수 목적 프로세서, 통상의 프로세서, 디지털 신호 프로세서(DSP), 복수의 마이크로프로세서, DSP 코어와 결합된 하나 이상의 마이크로프로세서, 컨트롤러, 마이크로컨트롤러, 주문형 반도체(ASICs), 필드 프로그래밍 가능한 게이트 어레이(FPGAs) 회로, 임의의 다른 종류의 집적 회로(IC), 및/또는 상태 머신을 포함한다.

[0153] 소프트웨어와 결합된 프로세서는 무선 송수신 유닛(WTRU), 사용자 장비(UE), 단말기, 기지국, 무선 네트워크 제

어기(RNC) 또는 임의의 호스트 컴퓨터에 사용되는 무선 주파수 송수신기의 구현에 사용될 수 있다. WTRU는 카메라, 비디오 카메라 모듈, 비디오폰, 스피커폰, 진동 장치, 스피커, 마이크로폰, 텔레비젼 수상기, 핸즈프리 헤드셋, 키보드, 블루투스 모듈, 주파수 변조(FM) 라디오 유닛, LCD 디스플레이 장치, 유기발광 다이오드(OLED) 디스플레이 장치, 디지털 음악 플레이어, 미디어 플레이어, 비디오 게임 플레이어 모듈, 인터넷 브라우저, 및/또는 임의의 무선 근거리 네트워크(WLAN) 또는 초광대역(UWB) 모듈과 같은 하드웨어 및/또는 소프트웨어로 실현되는 모듈과 함께 사용될 수 있다.

[0154] 다양한 특징 및 요소가 특정 조합으로 전술되었지만, 당업자는 각각의 특징 또는 요소가 독자적으로 또는 그밖의 특징 및 요소와 임의의 조합으로 사용될 수 있음을 알 것이다. 추가로, 여기 설명되는 방법은 컴퓨터 또는 프로세서에 의한 실행을 위해 컴퓨터 판독 가능 저장 매체에 포함된 컴퓨터 프로그램, 소프트웨어, 또는 펌웨어로 실행될 수 있다. 컴퓨터 판독 가능 저장 매체의 예로는 전자 신호(유선 또는 무선 연결로 전송된) 및 컴퓨터 판독 가능 저장 매체를 포함한다. 컴퓨터 판독 가능 매체의 예로는 한정되는 것은 아니지만, 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 레지스터, 캐시 메모리, 반도체 메모리 소자, 내장 하드 디스크와 분리가능한 디스크와 같은 자기 매체, 광자기 매체 및 CD-ROM 디스크와 DVDs와 같은 광학 매체를 포함한다. 소프트웨어와 결합된 프로세서는 WTRU, UE, 단말기, 기지국, RNC 또는 임의의 호스트 컴퓨터에 사용되는 무선 주파수 송수신기의 구현에 사용될 수 있다.

[0155] 도 17a는 하나 이상의 개시된 실시예가 구현될 수 있는 일례의 통신 시스템(1700)의 다이어그램이다. 통신 시스템(1700)은 음성, 데이터, 비디오, 메시지, 방송 등의 콘텐츠를 다중 무선 사용자에게 제공하는 다중 액세스 시스템일 수 있다. 통신 시스템(1700)은 다중 무선 사용자가 무선 대역폭을 포함하는 시스템 리소스의 공유를 통해 이러한 콘텐츠에 액세스 가능하게 할 수 있다. 예를 들면, 통신 시스템(1700)은 CDMA, TDMA, FDMA, OFDMA, SC-FDMA 등과 같은 하나 이상의 채널 액세스 방법을 채용할 수 있다.

[0156] 도 17a에 예시된 바와 같이, 통신 시스템(1700)은, 개시된 실시예들은 임의의 갯수의 WTRUs, 기지국, 네트워크 및/또는 네트워크 요소를 고려할 수 있지만, 무선 송수신 유닛(WTRUs)(1702a, 1702b, 1702c, 1702d), 무선 액세스 네트워크(RAN)(1704), 코어 네트워크(1706), 공중 교환 전화 네트워크(PSTN)(1708), 인터넷(1710) 등을 포함할 수 있다. WTRUs(1702a, 1702b, 1702c, 1702d) 각각은 무선 환경에서 동작 및/또는 통신하도록 구성된 임의의 종류의 장치일 수 있다. 예컨대, WTRUs(1702a, 1702b, 1702c, 1702d)는 무선 신호를 송신 및/또는 수신하도록 구성될 수 있으며, 사용자 장비(UE), 이동국, 고정 또는 이동 가입자 유닛, 페이저, 휴대 전화, 개인 정보 단말기(PDA), 스마트폰, 랩톱, 노트북, 개인용 컴퓨터, 무선 센서, 가전 제품 등을 포함할 수 있다.

[0157] 또한, 통신 시스템(1700)은 기지국(1714a)과 기지국(1714b)을 포함할 수 있다. 각각의 기지국(1714a, 1714b)은 코어 네트워크(1706), 인터넷(1710) 및/또는 네트워크(1712)와 같은 하나 이상의 통신 네트워크에 접속이 용이하도록 WTRUs(1702a, 1702b, 1702c, 1702d) 중 적어도 하나와 무선 인터페이스 연결되도록 구성된 임의의 종류의 장치일 수 있다. 예로써, 기지국(1714a, 1714b)은 송수신기 기지국(BTS), Node-B, eNode B, Home Node B, Home eNode B, 사이트 컨트롤러, 액세스 포인트(AP), 무선 라우터 등일 수 있다. 기지국(1714a, 1714b)은 각각 단일 요소로 묘사되고 있지만, 기지국(1714a, 1714b)은 임의의 수의 상호 연결된 기지국 및/또는 네트워크 요소를 포함할 수 있음을 알 것이다.

[0158] 기지국(1714a)은 기지국 제어기(BSC), 무선 네트워크 제어기(RNC), 릴레이 노드 등과 같은 다른 기지국 및/또는 네트워크 요소(도시 생략)를 역시 포함할 수 있는 RAN(1704)의 일부일 수 있다. 기지국(1714a) 및/또는 기지국(1714b)은 셀(도시 생략)로 지칭될 수 있는 특정 지리적 영역 내에서 무선 신호를 송신 및/또는 수신하도록 구성될 수 있다. 셀은 셀 섹터로 세분될 수 있다. 예를 들면, 기지국(1714a)과 연관된 셀은 3개의 섹터로 분할될 수 있다. 따라서, 일 실시예에서, 기지국(1714a)은 3개의 송수신기, 즉 셀의 각 섹터 당 하나의 송수신기를 포함할 수 있다. 다른 실시예에서, 기지국(1714a)은 다중-입력 다중-출력 (MIMO) 기술을 채용할 수 있어서 셀의 각 섹터마다 다중 송수신기를 활용할 수 있다.

[0159] 기지국(1714a, 1714b)은 임의의 적절한 무선 통신 링크(예, 무선 주파수(RF), 마이크로파, 적외선(IR), 자외선(UV), 가시광선 등)일 수 있는 무선 인터페이스(1716)를 통해 하나 이상의 WTRUs(1702a, 1702b, 1702c, 1702d)와 통신할 수 있다. 무선 인터페이스(1716)는 임의의 적절한 무선 액세스 기술(RAT)을 이용하여 구축될 수 있다.

[0160] 보다 구체적으로, 전술한 바와 같이, 통신 시스템(1700)은 다중 액세스 시스템일 수 있고, CDMA, TDMA, OFDMA, SC-FDMA 등의 하나 이상의 채널 액세스 구성을 채용할 수 있다. 예를 들면, RAN(1704)과 WTRUs(1702a, 1702b, 1702c) 내의 기지국(1714a)은 광대역 CDMA(WCDMA)를 이용하여 무선 인터페이스(1716)를 구축할 수 있는 UMTS

UTRA와 같은 무선 기술을 실현할 수 있다. WCDMA는 HSPA, 및/또는 HSPA+와 같은 통신 프로토콜을 포함할 수 있다. HSPA는 HSDPA 및/또는 HSUPA를 포함할 수 있다.

[0161] 다른 실시예에서, 기지국(1714a)과 WTRUs(1702a, 1702b, 1702c)는 LTE 및/또는 LTE-A를 이용하여 무선 인터페이스(1716)를 구축할 수 있는 E-UTRA와 같은 무선 기술을 실현할 수 있다.

[0162] 다른 실시예에서, 기지국(1714a)과 WTRUs(1702a, 1702b, 1702c)은 IEEE 802.16(즉, WiMAX), CDMA2000, CDMA2000 1X, CDMA2000 EV-DO, 인터림 표준 2000(IS-2000), 인터림 표준 95(IS-95), 인터림 표준 856(IS-856), GSM, EDGE, GERAN 등과 같은 무선 기술을 실현할 수 있다.

[0163] 도 17a의 기지국(1714b)은 예컨대, 무선 라우터, Home Node B, Home eNode B 또는 액세스 포인트일 수 있고, 사무실, 가정, 차량, 캠퍼스 등의 장소와 같은 로컬 영역에서 무선 연결을 용이하게 하기 위해 임의의 적절한 RAT를 활용할 수 있다. 일 실시예에서, 기지국(1714b)과 WTRUs(1702c, 1702d)는 무선 로컬 영역 네트워크(WLAN)을 구축하는 IEEE 802.11과 같은 무선 기술을 실현할 수 있다. 다른 실시에에서, 기지국(1714b)과 WTRUs(1702c, 1702d)는 무선 개인 영역 네트워크(WPAN)을 구축하는 IEEE 802.15와 같은 무선 기술을 실현할 수 있다. 또 다른 실시예에서, 기지국(1714b)과 WTRUs(1702c, 1702d)는 피코셀 또는 펨토셀을 구축하는 셀-기반의 RAT(예, WCDMA, CDMA2000, GSM, LTE, LTE-A 등)를 활용할 수 있다. 도 17a에 예시된 바와 같이, 기지국(1714b)은 인터넷(1710)과 직접 연결될 수 있다. 따라서, 기지국(1714b)은 코어 네트워크(1706)를 통해 인터넷(1710)에 액세스할 필요가 없을 수 있다.

[0164] RAN(1704)은 음성, 데이터, 어플리케이션 및/또는 인터넷을 통한 음성 프로토콜(VoIP) 서비스를 WTRUs(1702a, 1702b, 1702c, 1702d) 중 하나 이상으로 제공하도록 구성된 임의의 종류의 네트워크일 수 있는 코어 네트워크(1706)와 통신 상태일 수 있다. 예를 들면, 코어 네트워크(1706)는 콜 제어, 빌링 서비스, 모바일 위치-기반 서비스, 선불 콜링, 인터넷 연결, 비디오 배포, 등을 제공하거나 및/또는 사용자 인증 등의 높은 수준의 보안 기능을 수행할 수 있다. 도 17a에는 예시되지 않고 있지만, RAN(1704) 및/또는 코어 네트워크(1706)는 RAN(1704)과 동일한 RAT 또는 상이한 RAT를 채용하는 다른 RAN들과 직접 또는 간접적인 통신 상태일 수 있음을 알 것이다. 예를 들면, E-UTRA 무선 기술을 활용할 수 있는 RAN(1704)에 연결되는 것 외에, 코어 네트워크(1706)는 GSM 무선 기술을 채용하는 다른 RAN(도시 생략)과 통신 상태에 있을 수 있다.

[0165] 코어 네트워크(1706)는 PSTN(1708), 인터넷(1710) 및/또는 다른 네트워크(1712)를 액세스하기 위해 WTRUs(1702a, 1702b, 1702c, 1702d)를 위한 게이트웨이로서 사용될 수도 있다. PSTN(1708)은 재래식 단순 전화 서비스(POTS)를 제공하는 회선 교환 전화 네트워크를 포함할 수 있다. 인터넷(1710)은 TCP/IP 인터넷 프로토콜 묶음 중 전송 제어 프로토콜(TCP), 사용자 데이터그램 프로토콜(UDP) 및 인터넷 프로토콜(IP)과 같은 공통 통신 프로토콜을 사용하는 상호 연결된 컴퓨터 네트워크 및 장치의 글로벌 시스템을 포함할 수 있다. 네트워크(1712)는 다른 서비스 제공자에 의해 소유 및/또는 운용되는 유선 또는 무선 통신 네트워크를 포함할 수 있다. 예를 들면, 네트워크(1712)는 RAN(1704)과 동일한 RAT 또는 다른 RAT를 채용할 수 있는 하나 이상의 RAN에 연결된 다른 코어 네트워크를 포함할 수 있다.

[0166] 통신 시스템(1700)에서 WTRUs(1702a, 1702b, 1702c, 1702d) 중 일부 또는 전부는 다중 모드 능력을 포함할 수 있는데, 즉 WTRUs(1702a, 1702b, 1702c, 1702d)는 다른 무선 링크를 통해 다른 무선 네트워크와 통신하기 위한 다중 송수신기를 포함할 수 있다. 예를 들면, 도 17a에 예시된 WTRU(1702c)는 셀-기반의 무선 기술을 채용할 수 있는 기지국(1714a)과 통신하고 IEEE 802 무선 기술을 채용할 수 있는 기지국(1714b)과 통신하도록 구성될 수 있다.

[0167] 도 17b는 일례의 WTRU(1702)의 시스템 다이어그램이다. 도 17b에 예시된 바와 같이, WTRU(1702)는 프로세서(1718), 송수신기(1720), 송신/수신 요소(1722), 스피커/마이크로폰(1724), 키패드(1726), 디스플레이/터치패드(1728), 고정형 메모리(1706), 분리형 메모리(1732), 전원(1734), GPS 칩셋(1736) 및 기타 주변 장치(1738)를 포함할 수 있다. WTRU(1702)는 실시예와의 일관성을 유지하면서 전술한 요소들의 임의의 서브-조합을 포함할 수 있음을 알 것이다.

[0168] 프로세서(1718)는 범용 프로세서, 특수 목적 프로세서, 통상적 프로세서, 디지털 신호 프로세서(DSP), 복수의 마이크로프로세서, DSP 코어와 결합된 하나 이상의 마이크로프로세서, 컨트롤러, 마이크로컨트롤러, 주문형 반도체(ASICs), 필드 프로그래밍 가능한 게이트 어레이(FPGAs) 회로, 임의의 다른 종류의 집적 회로(IC), 상태 머신 등일 수 있다. 프로세서(1718)는 신호 코딩, 데이터 처리, 전력 제어, 입/출력 처리, 및/또는 WTRU(1702)가 무선 환경에서 동작할 수 있게 하는 임의의 다른 기능을 수행할 수 있다. 프로세서(1718)는 송수신기(1720)에

결합될 수 있고, 송수신기는 송신/수신 요소(1722)에 결합될 수 있다. 도 17b는 프로세서(1718)와 송수신기(1720)를 별개 성분으로 표현하고 있지만, 프로세서(1718)와 송수신기(1720)는 전자 패키지 또는 칩으로 함께 일체화될 수 있음을 알 것이다.

[0169] 송신/수신 요소(1722)는 무선 인터페이스(1716)를 통해 기지국(예, 기지국(1714a))에 대해 신호를 송신 및 수신하도록 구성될 수 있다. 예를 들면, 일 실시예에서, 송신/수신 요소(1722)는 RF 신호를 송신 및/또는 수신하도록 구성된 안테나일 수 있다. 다른 실시예에서, 송신/수신 요소(1722)는 예컨대 적외선(IR), 자외선(UV) 또는 가시광선 신호를 송신 및/또는 수신하도록 구성된 에미터/검출기일 수 있다. 또 다른 실시예에서, 송신/수신 요소(1722)는 RF 신호와 광 신호 모두를 송신 및 수신하도록 구성될 수 있다. 송신/수신 요소(1722)는 임의의 조합의 무선 신호를 송신 및/또는 수신하도록 구성될 수 있음을 알 것이다.

[0170] 추가로, 송신/수신 요소(1722)는 도 17b에 단일 요소로 표현되고 있지만, WTRU(1702)는 임의의 갯수의 송신/수신 요소(1722)를 포함할 수 있다. 보다 구체적으로, WTRU(1702)는 MIMO 기술을 채용할 수 있다. 따라서, 일 실시예에서, WTRU(1702)는 무서 인터페이스(1716)를 통해 무선 신호를 송신 및 수신하기 위해 2개 이상의 송신/수신 요소(1722)(예, 다중 안테나)를 포함할 수 있다.

[0171] 송수신기(1720)는 송신/수신 요소(1722)에 의해 송신될 신호를 변조하고 송신/수신 요소(1722)에 의해 수신되는 신호를 복조하도록 구성될 수 있다. 전술한 바와 같이, WTRU(1702)는 다중 모드 능력을 가질 수 있다. 따라서, 송수신기(1720)는 WTRU(1702)가 예컨대 UTRA와 IEEE 802.11과 같은 다중 RAT를 통해 통신 가능하도록 하기 위해 다중 송수신기를 포함할 수 있다.

[0172] WTRU(1702)의 프로세서(1718)는 스피커/마이크로폰(1724), 키패드(1726) 및/또는 디스플레이/터치패드(1728)(예, LCD 디스플레이 유닛 또는 OLED 디스플레이 유닛)에 결합될 수 있고 이로부터 사용자 입력 데이터를 수신할 수 있다. 또한, 프로세서(1718)는 스피커/마이크로폰(1724), 키패드(1726) 및/또는 디스플레이/터치패드(1728)로 사용자 데이터를 출력할 수 있다. 추가로, 프로세서(1718)는 고정형 메모리(1706) 및/또는 분리형 메모리(1732)와 같은 임의의 종류의 적절한 메모리로부터 정보를 액세스하고 해당 메모리에 데이터를 저장할 수 있다. 고정형 lapahfl(1706)는 랜덤 액세스 메모리(RAM), 읽기 전용 메모리(ROM), 하드 디스크 또는 임의의 다른 종류의 메모리 저장 장치를 포함할 수 있다. 분리형 메모리(1732)는 가입자 식별 모듈(SIM) 카드, 메모리 스틱, 보안 디지털(SD) 메모리 카드 등을 포함할 수 있다. 다른 실시예에서, 프로세서(1718)는 예컨대 서버 또는 가정용 컴퓨터(도시 생략) 등의 WTRU(1702) 상에 물리적으로 위치되지 않은 메모리로부터 정보를 액세스하고 해당 메모리에 데이터를 저장할 수 있다.

[0173] 프로세서(1718)는 전원(1734)으로부터 전력을 수신할 수 있고, 해당 전력을 WTRU(1702) 내의 다른 성분으로 분배 및/또는 제어하도록 구성될 수 있다. 전원(1734)은 WTRU(1702)에 전력을 공급하는 임의의 적절한 장치일 수 있다. 예를 들면, 전원(1734)은 하나 이상의 건전지(예, NiCd, NiZn, NiMH, Li-ion 등), 태양 전지, 연료 전지 등을 포함할 수 있다.

[0174] 또한, 프로세서(1718)는 GPS 칩셋(1736)에도 결합될 수 있는데, GPS 칩셋은 WTRU(1702)의 현재 위치에 관한 위치 정보(예, 위도 및 경도)를 제공하도록 구성될 수 있다. GPS 칩셋(1736)으로부터의 정보 외에 또는 해당 정보 대신에, WTRU(1702)는 기지국(예, 기지국(1714a))으로부터 무선 인터페이스(1716)를 통해 위치 정보를 수신하고 및/또는 2곳 이상의 인접 기지국으로부터 수신되는 신호의 타이밍을 기초로 그 위치를 결정할 수 있다. WTRU(1702)는 실시예와의 일관성을 유지하면서 임의의 적절한 위치-결정 방법으로 위치 정보를 획득할 수 있음을 알 것이다.

[0175] 프로세서(1718)는 다른 주변 장치(1738)에 추가로 결합될 수 있는데, 해당 주변 장치는 추가의 특징, 기능 및/또는 유무선 연결을 제공하는 하나 이상의 소프트웨어 및/또는 하드웨어 모듈을 포함할 수 있다. 예를 들면, 주변 장치(1738)는 가속도계, 전자-나침반, 위성 송수신기, 디지털 카메라(사진 또는 비디오용), USB 포트, 진동 소자, 텔레비젼 수상기, 핸즈프리 헤드셋, 블루투스 모듈, 주파수 변조(FM) 라디오 유닛, 디지털 음악 플레이어, 미디어 플레이어, 비디오 게임 플레이어 모듈, 인터넷 브라우저 등을 포함할 수 있다.

[0176] 도 17c는 일 실시예에 따른 RAN(1704)과 코어 네트워크(1706)의 시스템 다이어그램이다. 전술한 바와 같이, RAN(1704)은 무선 인터페이스(1716)를 통해 WTRUs(1702a, 1702b, 1702c)와 통신하기 위해 UTRA 무선 기술을 채용할 수 있다. 또한, RAN(1704)은 코어 네트워크(1706)와 통신 상태에 있을 수 있다. 도 17c에 예시된 바와 같이, RAN(1704)은 무선 인터페이스(1716)를 통해 WTRUs(1702a, 1702b, 1702c)와 통신하기 위해 각각 하나 이상의 송수신기를 포함할 수 있는 Node-B(1740a, 1740b, 1740c)를 포함할 수 있다. Node-B(1740a, 1740b,

1740c)는 각각 RAN(1704) 내의 특정 셀(도시 생략)과 연관될 수 있다. 또한, RAN(1704)은 RNC(1742a, 1742b)를 포함할 수 있다. RAN(1704)은 실시예와의 일관성을 유지하면서 임의의 갯수의 Node-B와 RNC를 포함할 수 있음을 알 것이다.

[0177] 도 17c에 예시된 바와 같이, Node-B(1740a, 1740b)는 RNC(1742a)와 통신 상태에 있을 수 있다. 추가로, Node-B(1740c)는 RNC(1742b)와 통신 상태에 있을 수 있다. Node-B(1740a, 1740b, 1740c)는 Iub 인터페이스를 통해 각각의 RNC(1742a, 1742b)와 통신할 수 있다. RNC(1742a, 1742b)는 Iur 인터페이스를 통해 서로 통신할 수 있다. RNC(1742a, 1742b) 각각은 해당 RNC가 연결되는 각각의 Node-B(1740a, 1740b, 1740c)를 제어하도록 구성될 수 있다. 추가로, RNC(1742a, 1742b) 각각은 외부 루프 전력 제어, 부하 제어, 승인 제어, 패킷 스케줄링, 핸드오버 제어, 매크로다이버시티(macrodiversity), 보안 기능, 데이터 암호화 등과 같은 다른 기능을 수행하거나 지원하도록 구성될 수 있다.

[0178] 도 17c에 예시된 코어 네트워크(1706)는 미디어 게이트웨이(MGW)(1744), 이동 통신 교환국(MSC)(1746), 패킷 교환 지원 노드(SGSN)(1748) 및/또는 패킷 관문 지원 노드(GGSN)(1750)를 포함할 수 있다. 전술한 요소 각각은 코어 네트워크(1706)의 일부로 묘사되고 있지만, 이들 요소 중 임의의 한 요소는 코어 네트워크 오퍼레이터가 아닌 엔티티에 의해 소유 및/또는 동작될 수 있음을 알아야 한다.

[0179] RAN(1704) 내의 RNC(1742a)는 IuCS 인터페이스를 통해 코어 네트워크(1706) 내의 MSC(1746)에 연결될 수 있다. MSC(1746)는 MGW(1744)에 연결될 수 있다. MSC(1746)와 MGW(1744)는 WTRU(1702a, 1702b, 1702c)와 전통적인 지상 통신 장치 간의 통신을 용이하게 하기 위해 WTRU(1702a, 1702b, 1702c)가 PSTN(1708)과 같은 회선 교환 네트워크에 액세스되도록 할 수 있다.

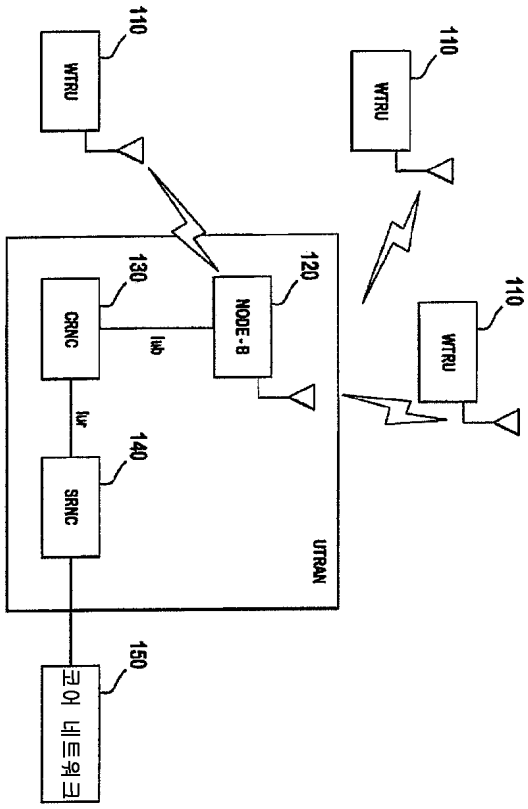
[0180] 또한, RAN(1704) 내의 RNC(1742a)는 IuPS 인터페이스를 통해 코어 네트워크(1706) 내의 SGSN(1748)에 연결될 수 있다. SGSN(1748)은 GGSN(1750)에 연결될 수 있다. SGSN(1748)과 GGSN(1750)은 WTRU(1702a, 1702b, 1702c)와 IP-인에이블 장치 간의 통신을 용이하게 하기 위해 WTRU(1702a, 1702b, 1702c)가 인터넷(1710)과 같은 패킷 교환 네트워크에 액세스되도록 할 수 있다.

[0181] 전술한 바와 같이, 코어 네트워크(1706)는 다른 서비스 제공자에 의해 소유 및/또는 동작되는 다른 유선 또는 무선 네트워크를 포함할 수 있는 네트워크(1712)에도 연결될 수 있다.

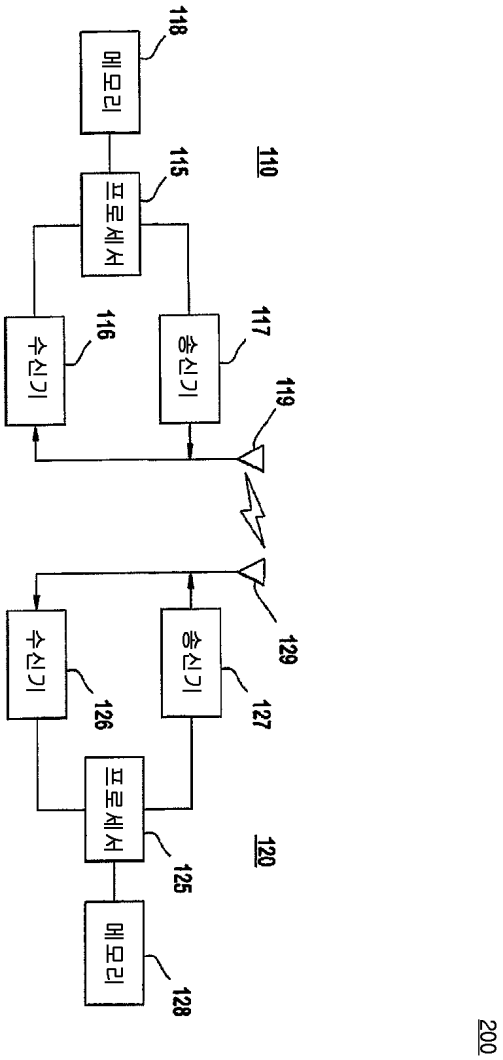
[0182] 다양한 특징 및 요소가 특정 조합으로 전술되었지만, 당업자는 각각의 특징 또는 요소가 독자적으로 또는 그밖의 특징 및 요소와 임의의 조합으로 사용될 수 있음을 알 것이다. 추가로, 여기 설명되는 방법은 컴퓨터 또는 프로세서에 의한 실행을 위해 컴퓨터 판독 가능 저장 매체에 포함된 컴퓨터 프로그램, 소프트웨어, 또는 펌웨어로 실행될 수 있다. 컴퓨터 판독 가능 저장 매체의 예로는 전자 신호(유선 또는 무선 연결로 전송된) 및 컴퓨터 판독 가능 저장 매체를 포함한다. 컴퓨터 판독 가능 매체의 예로는 한정되는 것은 아니지만, 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 레지스터, 캐시 메모리, 반도체 메모리 소자, 내장 하드 디스크와 분리 가능한 디스크와 같은 자기 매체, 광자기 매체 및 CD-ROM 디스크와 DVDs와 같은 광학 매체를 포함한다. 소프트웨어와 결합된 프로세서는 WTRU, UE, 단말기, 기지국, RNC 또는 임의의 호스트 컴퓨터에 사용되는 무선 주파수 송수신기의 구현에 사용될 수 있다.

## 도면

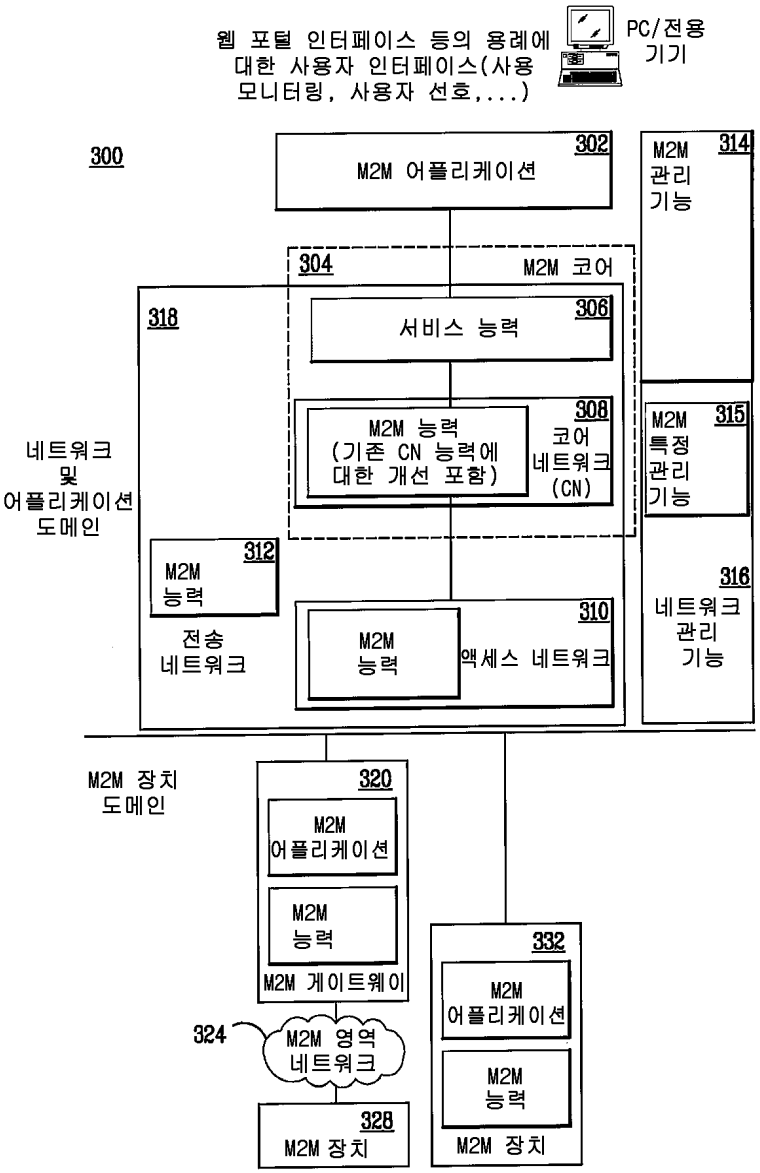
### 도면1


110
WTRU
110
WTRU
110
WTRU
130
CRNC
120
NODE-B
Iub
Iur
140
SRNC
UTRAN
150
코어 네트워크
100

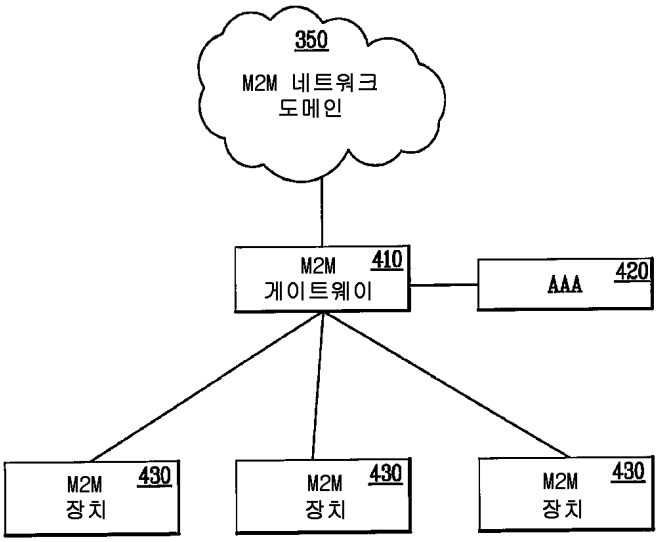
도면2


200
110
118
메모리
115
프로세서
116
수신기
117
송신기
119
129
수신기
126
송신기
127
120
프로세서
125
메모리
128

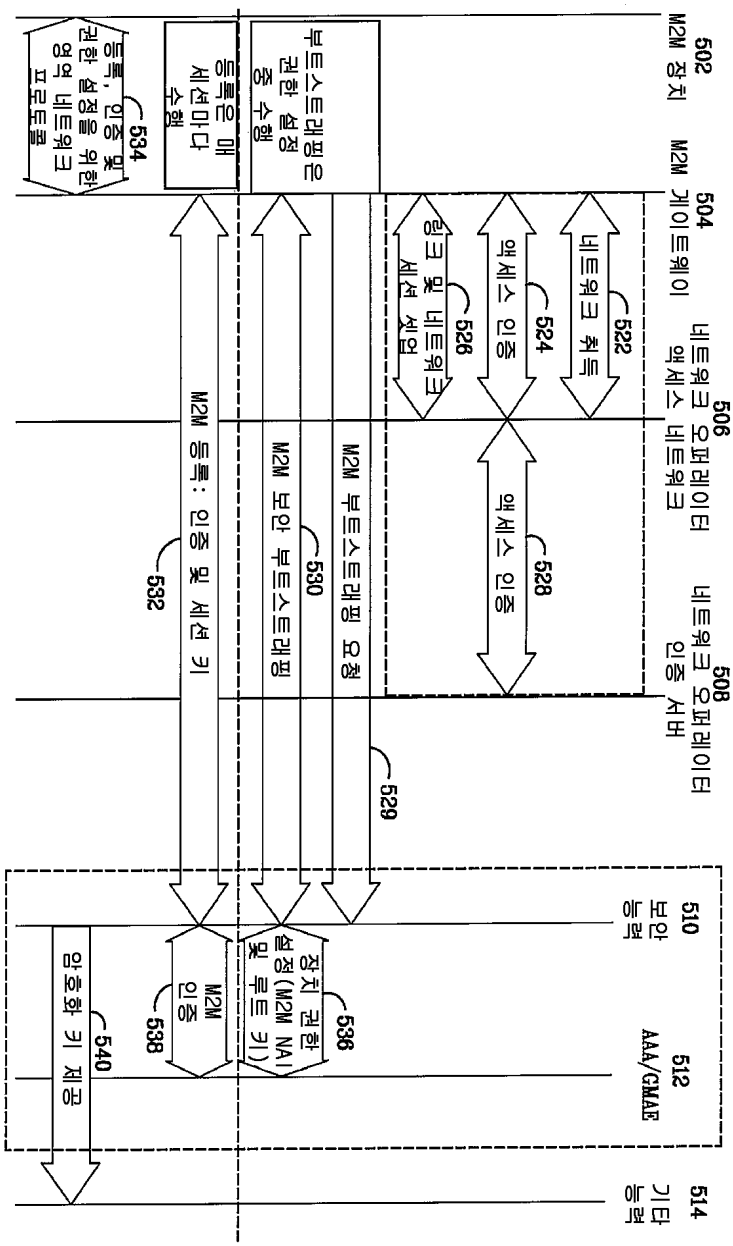
도면3


웹 포털 인터페이스 등의 용례에 대한 사용자 인터페이스(사용 모니터링, 사용자 선호,...)
PC/전용 기기
300
302
M2M 어플리케이션
314
M2M 관리 기능
304
M2M 코어
318
306
서비스 능력
308
M2M 능력 (기존 CN 능력에 대한 개선 포함)
코어 네트워크 (CN)
315
M2M 특정 관리 기능
네트워크 및 어플리케이션 도메인
312
M2M 능력
316
네트워크 관리 기능
전송 네트워크
310
M2M 능력
액세스 네트워크
M2M 장치 도메인
320
M2M 어플리케이션
M2M 능력
M2M 게이트웨이
332
M2M 어플리케이션
M2M 능력
M2M 장치
324
M2M 영역 네트워크
328
M2M 장치

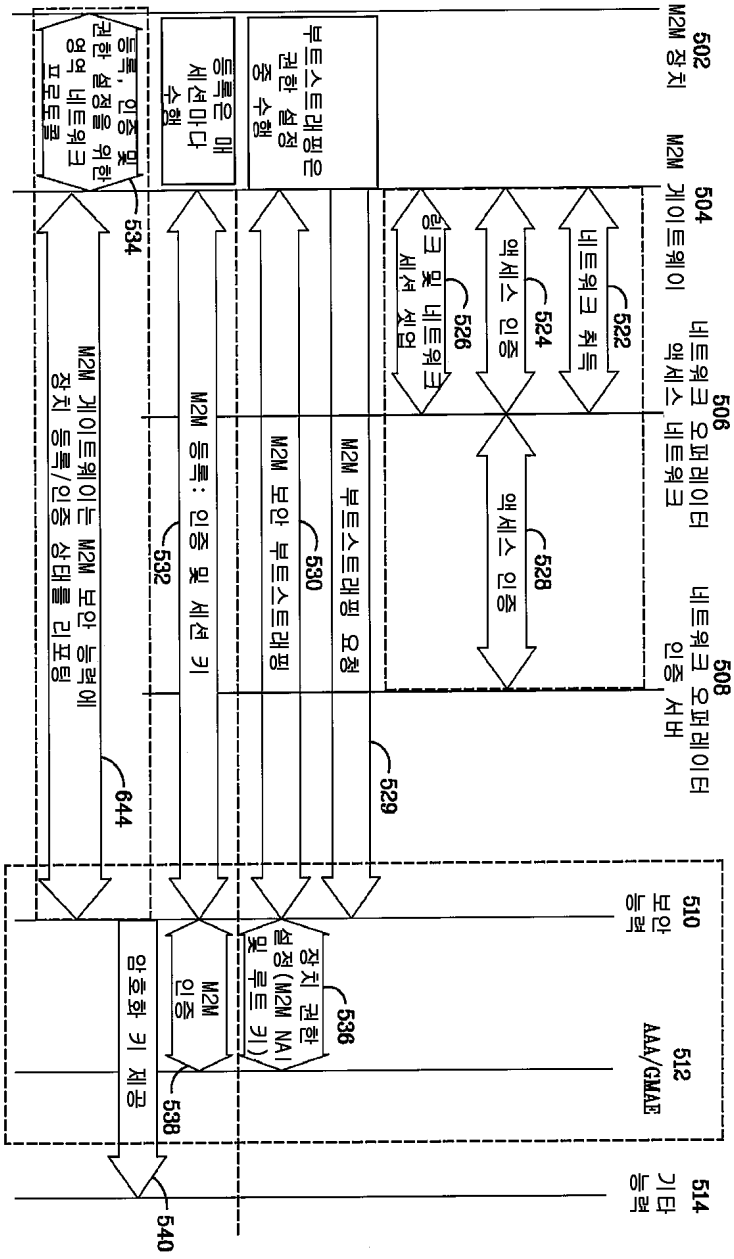
도면4


350
M2M 네트워크
도메인
M2M
게이트웨이
410
AAA
420
M2M
장치
430
M2M
장치
430
M2M
장치
430

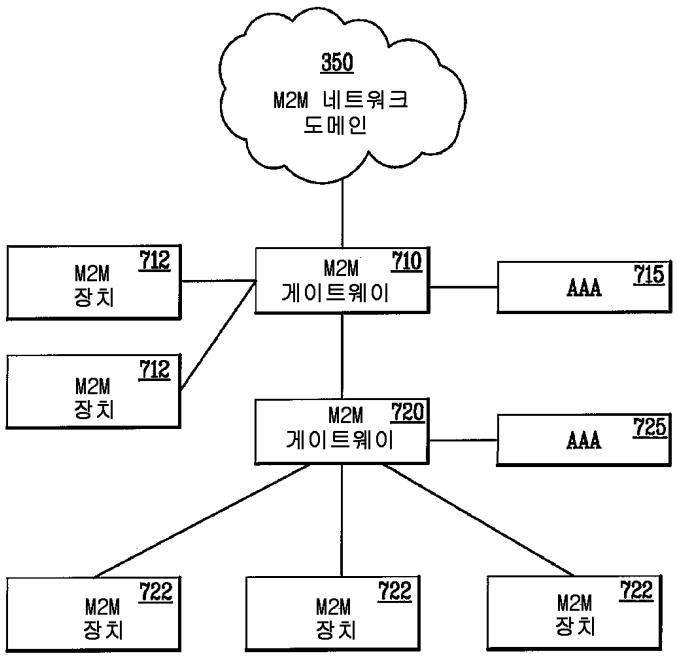
도면5


502
M2M 장치
504
M2M 게이트웨이
506
네트워크 오퍼레이터 네트워크
508
네트워크 오퍼레이터 인증 서버
510
보안 등록
512
AAA/GMAE
514
기타 등록
등록은 매 세션마다 수행
부트스트래핑은 권한 설정 중 수행
등록, 인증 및 권한 설정을 위한 영역 네트워크 프로토콜
534
네트워크 취득
522
액세스 인증
524
링크 및 네트워크 세션 셋업
526
액세스 인증
528
M2M 부트스트래핑 요청
529
M2M 보안 부트스트래핑
530
M2M 등록: 인증 및 세션 키
532
장치 권한 설정(M2M NAI 및 루트 키)
536
M2M 인증
538
암호화 키 제공
540

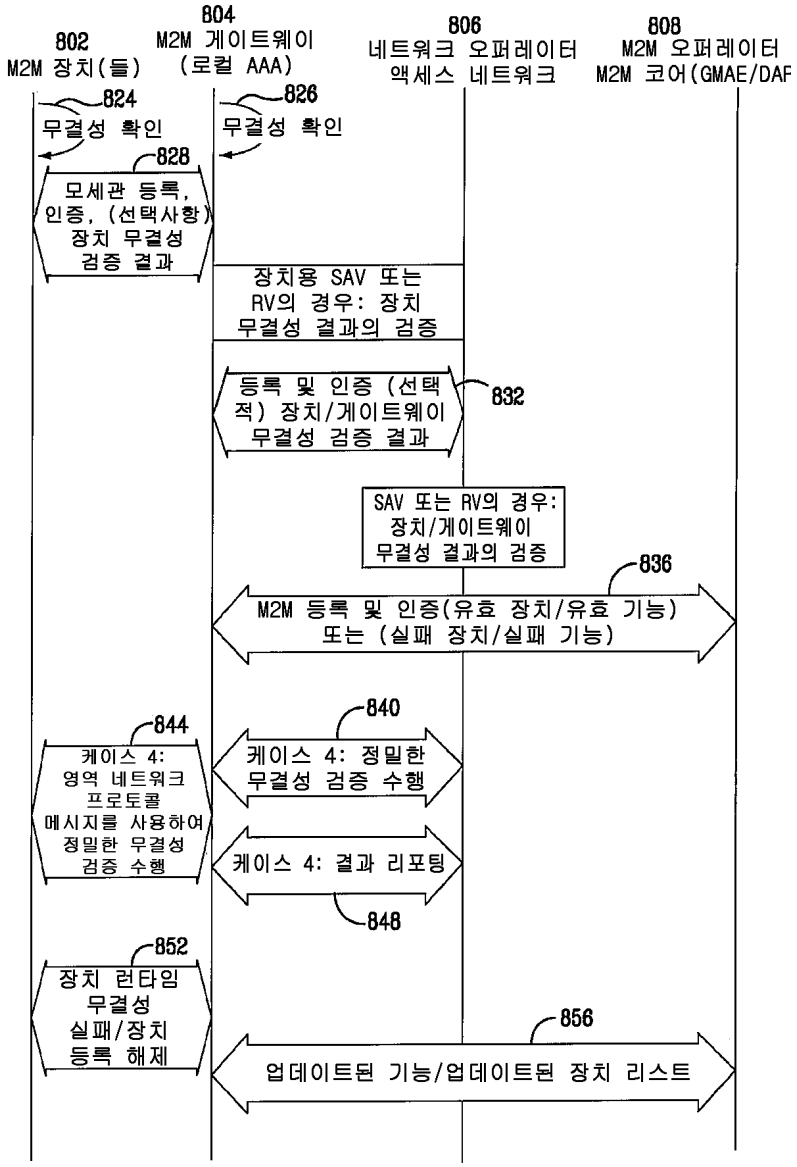
도면6


502
M2M 장치
504
M2M 게이트웨이
506
네트워크 오퍼레이터 액세스 네트워크
508
네트워크 오퍼레이터 인증 서버
510
보안 등록
512
AAA/GMAE
514
기타 등록
522
네트워크 취득
524
액세스 인증
526
링크 및 네트워크 세션 셋업
528
액세스 인증
529
M2M 부트스트래핑 요청
530
M2M 보안 부트스트래핑
532
M2M 등록: 인증 및 세션 키
534
등록, 인증 및 권한 설정을 위한 영역 네트워크 프로토콜
536
장치 권한 설정(M2M NAI 및 루트 키)
538
M2M 인증
540
암호화 키 제공
644
M2M 게이트웨이는 M2M 보안 등록에 장치 등록/인증 상태를 리포팅
부트스트래핑은 권한 설정 중 수행
등록은 매 세션마다 수행

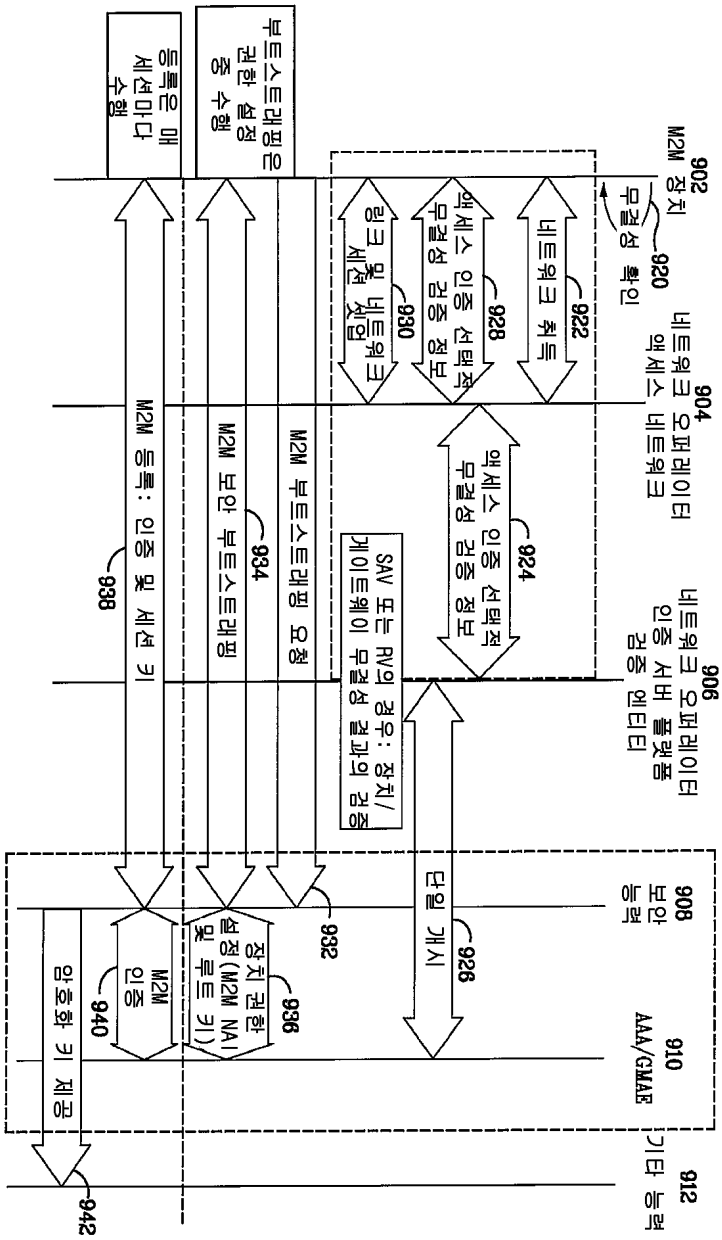
도면7


350
M2M 네트워크
도메인
712
M2M
장치
712
M2M
장치
710
M2M
게이트웨이
715
AAA
720
M2M
게이트웨이
725
AAA
722
M2M
장치
722
M2M
장치
722
M2M
장치

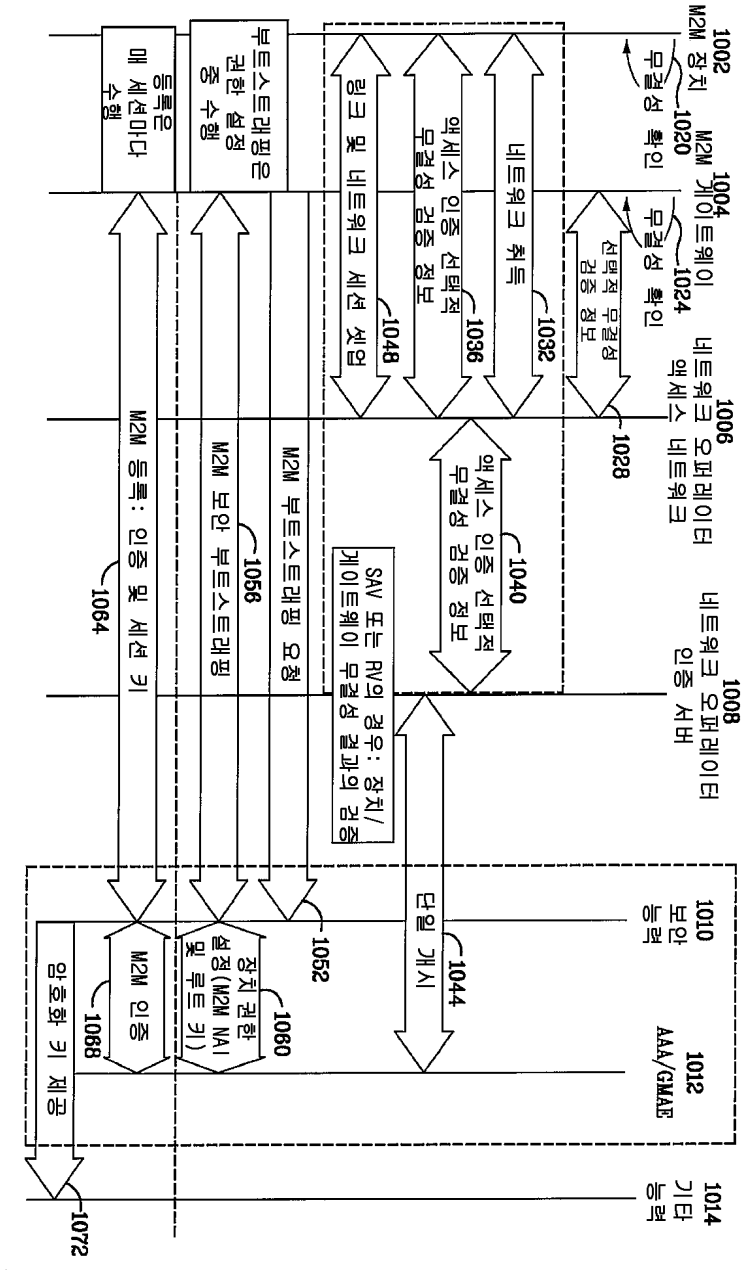
도면8


802
M2M 장치(들)
804
M2M 게이트웨이
(로컬 AAA)
806
네트워크 오퍼레이터
액세스 네트워크
808
M2M 오퍼레이터
M2M 코어(GMAE/DAF
824
무결성 확인
826
무결성 확인
828
모세관 등록,
인증, (선택사항)
장치 무결성
검증 결과
장치용 SAV 또는
RV의 경우: 장치
무결성 결과의 검증
등록 및 인증 (선택
적) 장치/게이트웨이
무결성 검증 결과
832
SAV 또는 RV의 경우:
장치/게이트웨이
무결성 결과의 검증
836
M2M 등록 및 인증(유효 장치/유효 기능)
또는 (실패 장치/실패 기능)
840
케이스 4: 정밀한
무결성 검증 수행
844
케이스 4:
영역 네트워크
프로토콜
메시지를 사용하여
정밀한 무결성
검증 수행
케이스 4: 결과 리포팅
848
852
장치 런타임
무결성
실패/장치
등록 해제
856
업데이트된 기능/업데이트된 장치 리스트

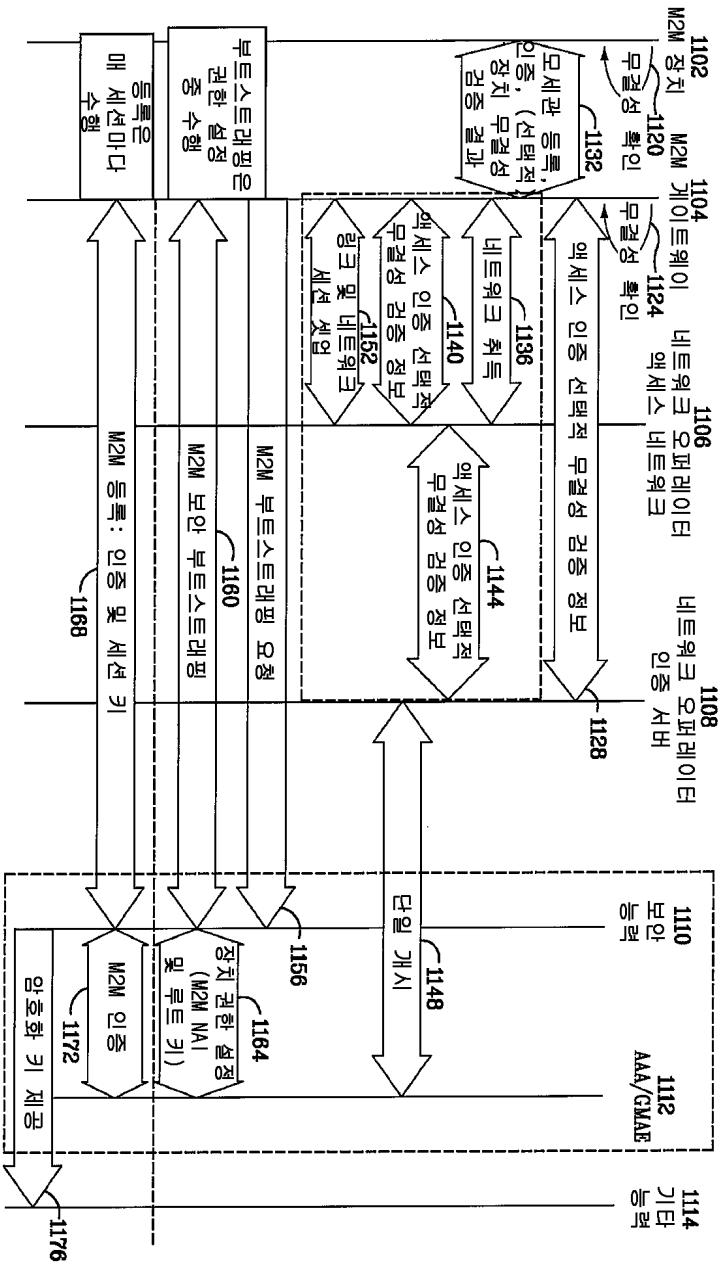
도면9


902
M2M 장치
920
무결성 확인
922
네트워크 취득
928
액세스 인증 선택적 무결성 검증 정보
930
링크 및 네트워크 세션 셋업
904
네트워크 오퍼레이터 액세스 네트워크
924
액세스 인증 선택적 무결성 검증 정보
906
네트워크 오퍼레이터 인증 서버 플랫폼 검증 엔티티
SAV 또는 RV의 경우: 장치/게이트웨이 무결성 결과의 검증
908
보안 등록
910
AAA/GMAB
912
기타 등록
926
단일 게시
932
M2M 부트스트래핑 요청
934
M2M 보안 부트스트래핑
936
장치 권한 설정(M2M NAI 및 루트 키)
940
M2M 인증
942
암호화 키 제공
938
M2M 등록: 인증 및 세션 키
부트스트래핑은 권한 설정 중 수행
등록은 매 세션마다 수행

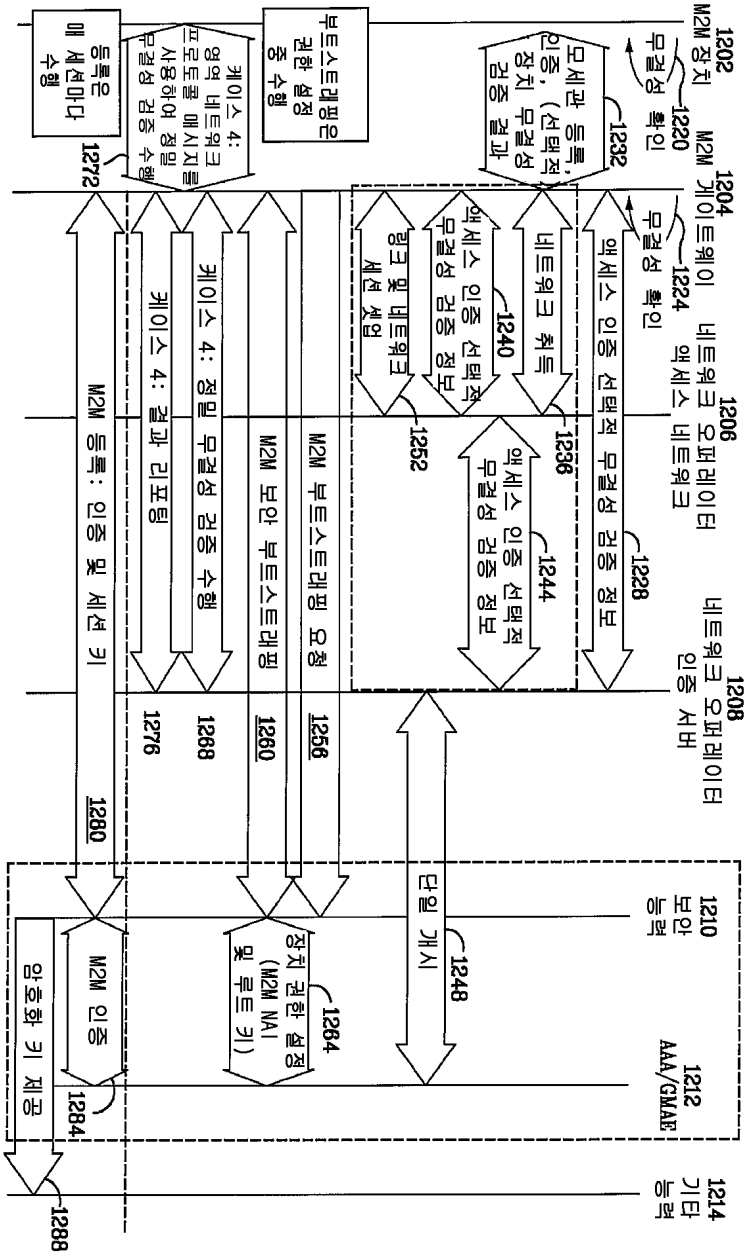
도면10


1002
M2M 장치
1020
무결성 확인
1004
게이트웨이
1024
무결성 확인
선택적 무결성 검증 정보
1028
네트워크 액세스 오퍼레이터 네트워크
네트워크 취득
1032
액세스 인증 선택적 무결성 검증 정보
1036
링크 및 네트워크 세션 셋업
1048
1006
네트워크 오퍼레이터 인증 서버
1008
액세스 인증 선택적 무결성 검증 정보
1040
SAV 또는 RV의 경우 : 장치/게이트웨이 무결성 결과의 검증
M2M 부트스트래핑 요청
1052
M2M 보안 부트스트래핑
1056
M2M 등록 : 인증 및 세션 키
1064
부트스트래핑은 권한 설정 중 수행
등록은 매 세션마다 수행
단일 개시
1044
1010
보안 능력
1012
AAA/GMAE
장치 권한 설정(M2M NAI 및 루트 키)
1060
M2M 인증
1068
암호화 키 제공
1072
1014
기타 능력

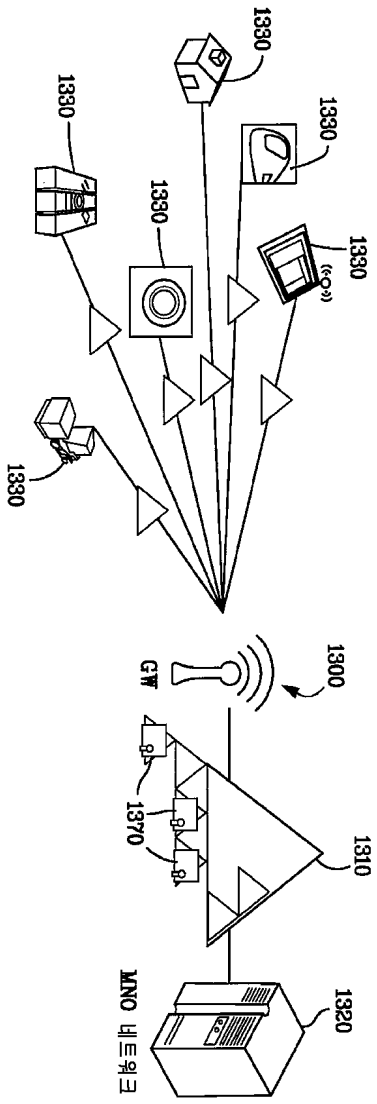
도면11


1102 M2M 장치
1104 M2M 게이트웨이
1106 네트워크 오퍼레이터 액세스 네트워크
1108 네트워크 오퍼레이터 인증 서버
1110 보안 능력
1112 AAA/GMAE
1114 기타 능력
1120 무결성 확인
1124 무결성 확인
1128 액세스 인증 선택적 무결성 검증 정보
1132 모세관 등록, 인증, (선택적) 장치 무결성 검증 결과
1136 네트워크 취득
1140 액세스 인증 선택적 무결성 검증 정보
1144 액세스 인증 선택적 무결성 검증 정보
1148 단일 개시
1152 링크 및 네트워크 세션 셋업
1156 M2M 부트스트래핑 요청
1160 M2M 보안 부트스트래핑
1164 장치 권한 설정 (M2M NAI 및 루트 키)
1168 M2M 등록: 인증 및 세션 키
1172 M2M 인증
1176 암호화 키 제공
부트스트래핑은 권한 설정 중 수행
등록은 매 세션마다 수행

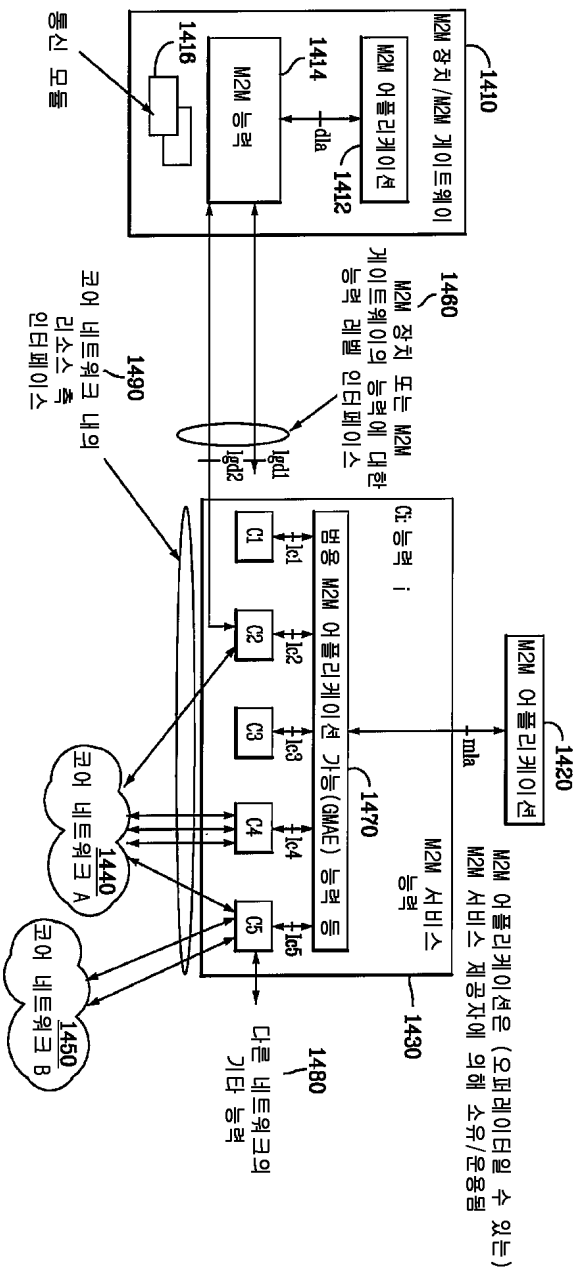
도면12


1202
M2M 장치
1204
게이트웨이
1206
네트워크 오퍼레이터
네트워크
1208
네트워크 오퍼레이터
인증 서버
1210
보안
능력
1212
AAA/GMAF
1214
기타
능력
1220
무결성 확인
1224
무결성 확인
1232
모세관 등록;
인증, (선택적)
장치 무결성
검증 결과
1240
네트워크 취득
1252
링크 및 네트워크
세션 셋업
1236
액세스 인증 선택적
무결성 검증 정보
1244
액세스 인증 선택적
무결성 검증 정보
1228
액세스 인증 선택적 무결성 검증 정보
부트스트래핑은
권한 설정
중 수행
등록은
매 세션마다
수행
1272
케이스 4:
영역 네트워크
프로토콜 메시지를
사용하여 정밀
무결성 검증 수행
M2M 등록; 인증 및 세션 키
1280
케이스 4: 정밀 무결성 검증 수행
1268
케이스 4: 결과 리포팅
1276
M2M 보안 부트스트래핑
1260
M2M 부트스트래핑 요청
1256
단일 게시
1248
장치 권한 설정
(M2M NAI
및 루트 키)
1264
M2M 인증
1284
암호화 키 제공
1288

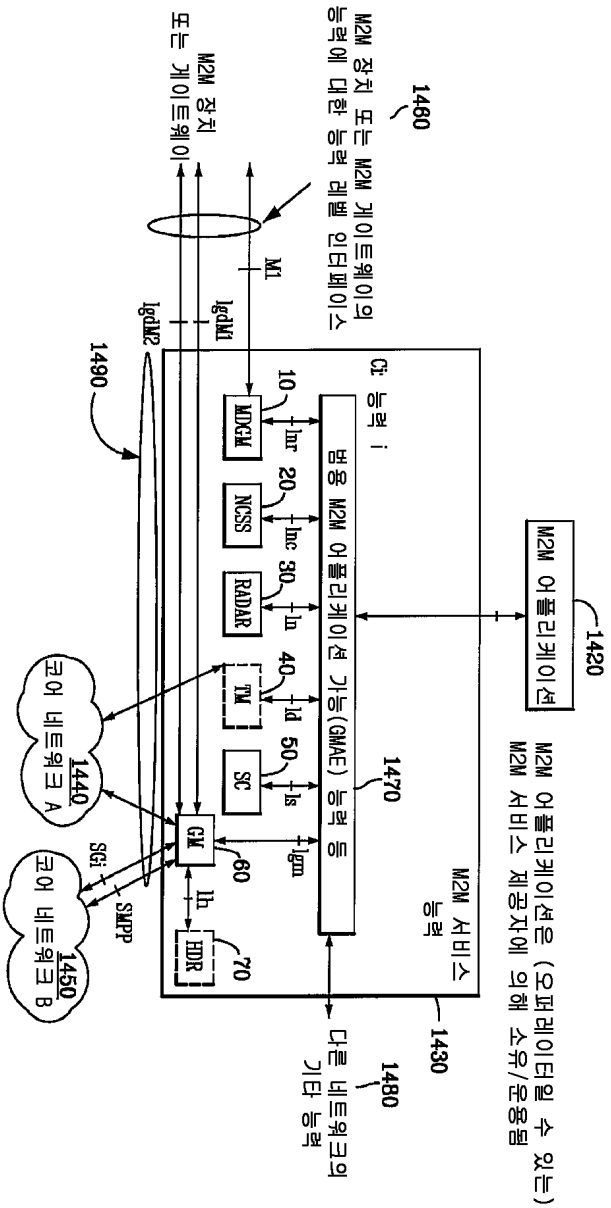
도면13



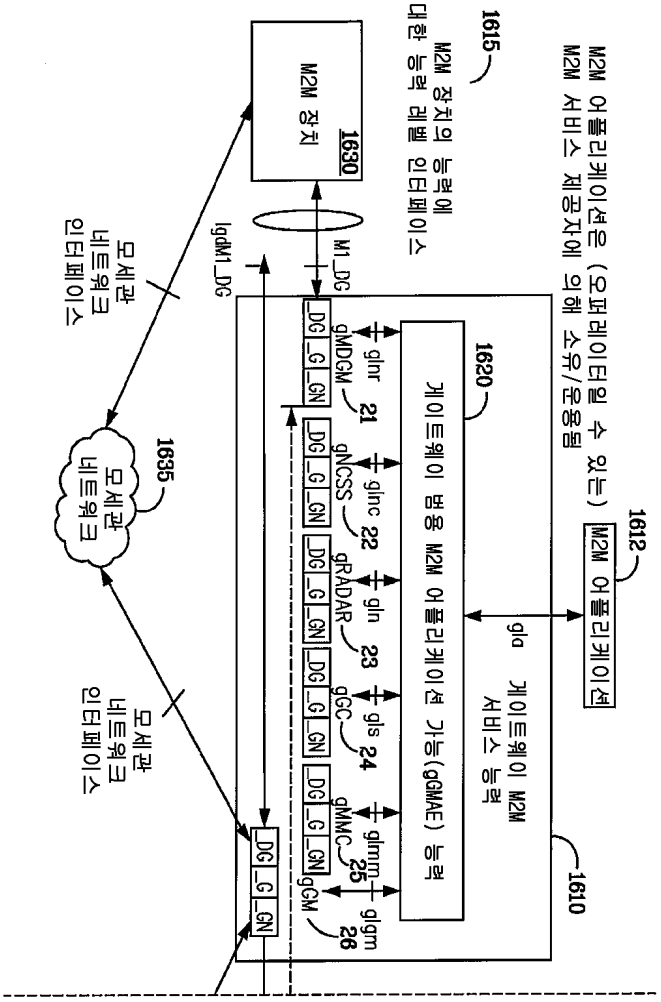
도면14


M2M 장치/M2M 게이트웨이
1410
M2M 어플리케이션
1412
M2M 능력
1414
통신 모듈
1416
dla
M2M 장치 또는 M2M 게이트웨이의 능력에 대한 레벨 인터페이스
1460
lgd1
lgd2
코어 네트워크 내의 리소스 촉 인터페이스
1490
C1
C2
C3
C4
C5
lc1
lc2
lc3
lc4
lc5
범용 M2M 어플리케이션 기능(GMAE) 능력 등
1470
M2M 서비스 능력
1430
Ci: 능력 i
mla
M2M 어플리케이션
1420
M2M 어플리케이션은 (오퍼레이터일 수 있는) M2M 서비스 제공자에 의해 소유/운용됨
코어 네트워크 A
1440
코어 네트워크 B
1450
다른 네트워크의 기타 능력
1480

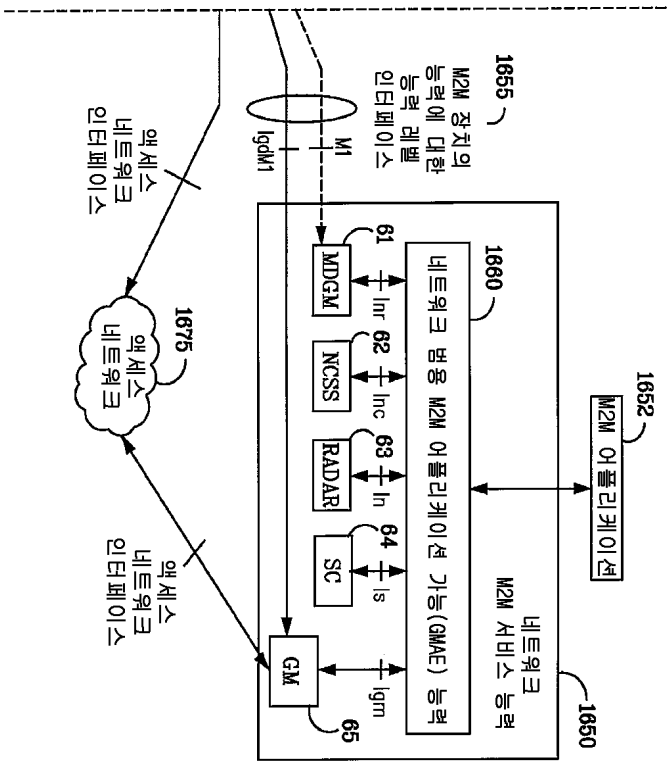
도면15


M2M 장치 또는 M2M 게이트웨이의 능력에 대한 능력 레벨 인터페이스
1480
M2M 장치 또는 게이트웨이
M1
1gdM1
1gdM2
1490
Ct: 능력 i
10
mr
MDGM
20
mc
NCSS
30
m
RADAR
40
d
TM
50
s
SC
범용 M2M 어플리케이션 가능(GMAE) 능력 등
1470
M2M 서비스 능력
gm
60
GM
h
70
HDR
1430
M2M 어플리케이션
1420
M2M 어플리케이션은 (오퍼레이터일 수 있는) M2M 서비스 제공자에 의해 소유/운용됨
다른 네트워크의 기타 능력
1480
코어 네트워크 A
1440
코어 네트워크 B
1450
SGi
SMPP

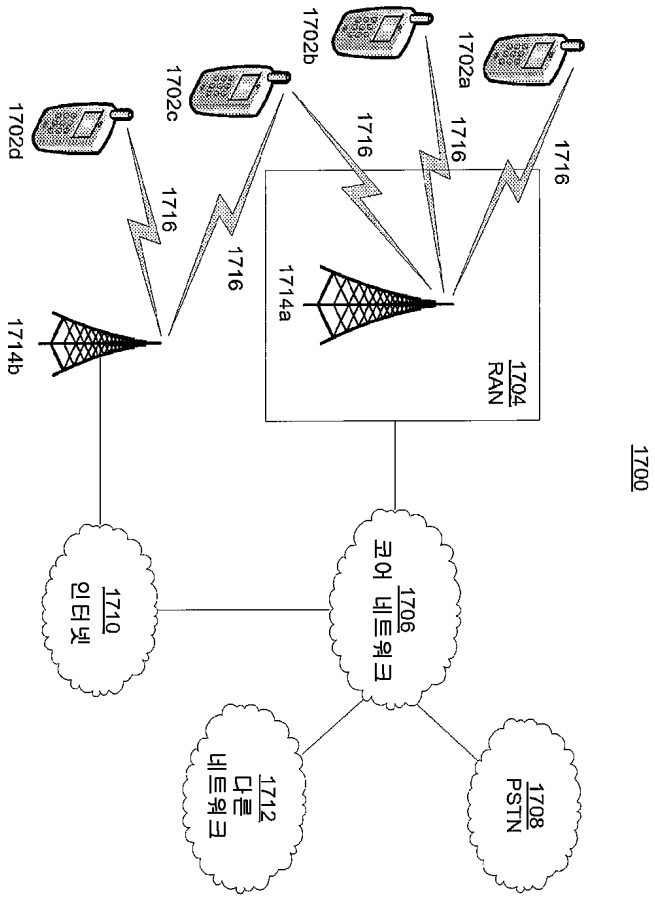
도면16a


M2M 어플리케이션을 (오퍼레이터일 수 있는)
M2M 서비스 제공자에 의해 소유/운용됨
1612
M2M 어플리케이션
gla
게이트웨이 M2M
서비스 능력
1610
게이트웨이 범용 M2M 어플리케이션 가능(gGMAE) 능력
1620
M2M 장치의 능력에
대한 등록 레벨 인터페이스
1615
M2M 장치
1630
M1_DG
lgdM1_DG
모세관
네트워크
인터페이스
1635
모세관
네트워크
인터페이스
glnr
glnc
gln
gls
glmm
glgm
21
22
23
24
25
26
gMDGM
gNCSS
gRADAR
gCC
gMMC
gGM
_DG
_G
_GN

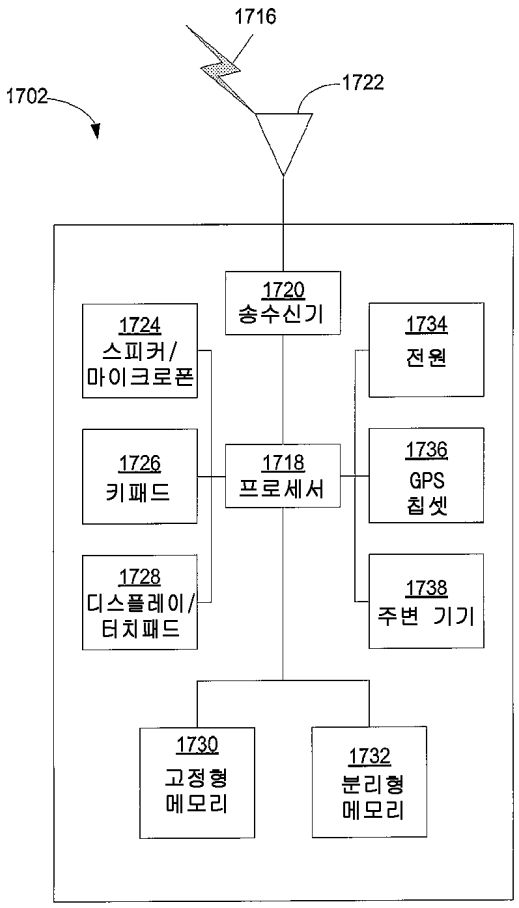
도면16b


1655
M2M 장치의 등록에 대한 레퍼런스 인터페이스
IgdM1
M1
액세스 네트워크 인터페이스
1675
액세스 네트워크
액세스 네트워크 인터페이스
1660
네트워크 범용 M2M 어플리케이션 가능(GMAE) 능력
61
MDGM
Inr
62
NCSS
Inc
63
RADAR
In
64
SC
Is
GM
Igm
65
1650
네트워크 M2M 서비스 능력
1652
M2M 어플리케이션

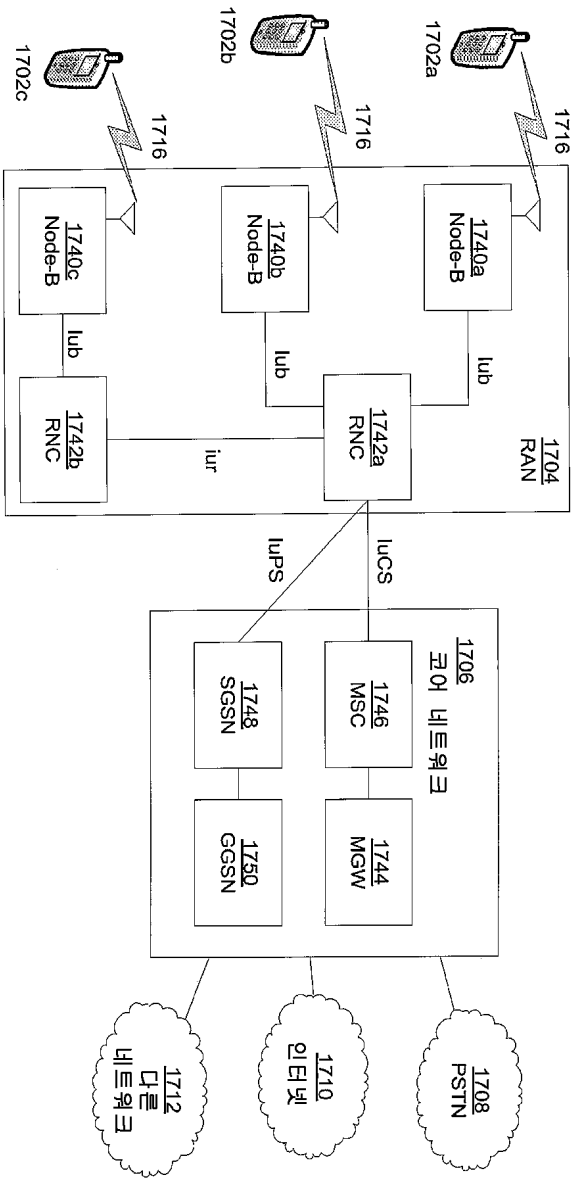
도면17a


1702b
1702a
1702c
1702d
1716
1716
1716
1716
1716
1714a
1714b
1704
RAN
1700
1710
인터넷
1706
코어 네트워크
1712
다른
네트워크
1708
PSTN

도면17b


1716
1722
1702
1720
송수신기
1724
스피커/
마이크로폰
1734
전원
1726
키패드
1718
프로세서
1736
GPS
칩셋
1728
디스플레이/
터치패드
1738
주변 기기
1730
고정형
메모리
1732
분리형
메모리

도면17c


1702c
1702b
1702a
1716
1716
1716
1740c Node-B
1740b Node-B
1740a Node-B
Iub
Iub
Iub
1742b RNC
1742a RNC
Iur
1704 RAN
IuPS
IuCS
1706 코어 네트워크
1748 SGSN
1746 MSC
1750 GGSN
1744 MGW
1712 다른 네트워크
1710 인터넷
1708 PSTN