(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0038572
(43) 공개일자 2018년04월16일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04L 29/06* (2006.01)
H04L 29/08 (2006.01) *H04W 12/04* (2009.01)
H04W 4/70 (2018.01)
(52) CPC특허분류
H04W 12/06 (2013.01)
H04L 63/0428 (2013.01)
(21) 출원번호 10-2018-7009288(분할)
(22) 출원일자(국제) 2014년05월22일
심사청구일자 없음
(62) 원출원 특허 10-2015-7036120
원출원일자(국제) 2014년05월22일
심사청구일자 2015년12월21일
(85) 번역문제출일자 2018년04월02일
(86) 국제출원번호 PCT/US2014/039205
(87) 국제공개번호 WO 2014/190186
국제공개일자 2014년11월27일
(30) 우선권주장
61/826,176 2013년05월22일 미국(US)

(71) 출원인
콘비다 와이어리스, 엘엘씨
미국 19809-3727 델라웨어주 윌밍턴 스위트 300 벨레뷰 파크웨이 200
(72) 발명자
스타시닉, 마이클, 에프.
미국 18940 펜실베이니아주 뉴타운 앤드류 드라이브 190
루, 구앙, 엑스.
캐나다 엘4제이 9비6 온타리오주 톤힐 멘델 크레센트 1
(뒷면에 계속)
(74) 대리인
양영준, 백만기, 정은진

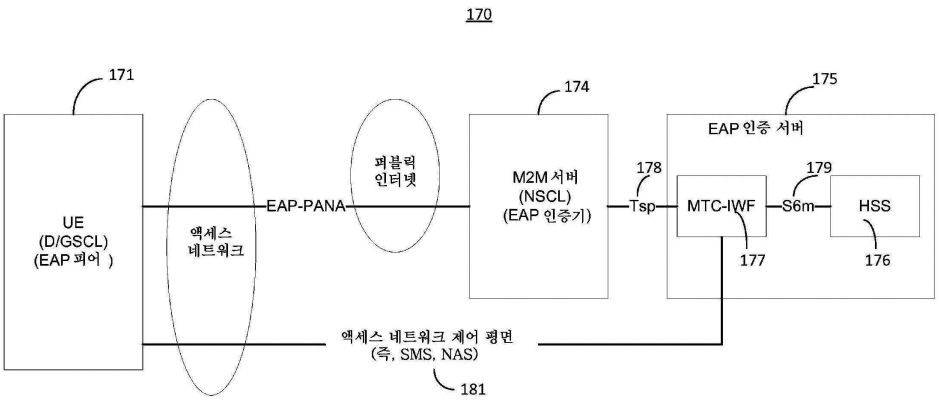
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 **머신-투-머신 통신을 위한 네트워크 지원형 부트스트랩핑**

(57) 요 약

액세스 네트워크에 의해 이미 요구되는 것을 넘어 공급을 요구하지 않고도 디바이스 상의 애플리케이션들이 머신-투-머신 서버와 부트스트랩할 수 있도록 서비스 레이어가 액세스 네트워크 인프라구조에 영향을 줄 수 있다.

대 표 도



(52) CPC특허분류
H04L 63/0876 (2013.01)
H04L 63/164 (2013.01)
H04L 67/34 (2013.01)
H04W 12/04 (2013.01)
H04W 4/70 (2018.02)
(72) 발명자
팔라니사미, 수레쉬
인도 637019 타밀나두 스테이트 나마칼 디스트릭트 셀라팜 파티 비아 사우스 우두팜 포스트 센고담팔라얌 2/3
리, 킹
미국 08550-2029 뉴저지주 프린스톤 정션 호우톤 드라이브 25
시드, 데일, 엔.
미국 18104 펜실베이니아주 알렌타운 노스 36번 스트리트 229

명 세 서

청구범위

청구항 1

명세서 또는 도면에 기재된 방법 및 장치.

발명의 설명

배 경 기 술

[0001] <관련 출원들에 대한 상호 참조>

[0002] 본 출원은 2013년 5월 22일자 "ACCESS NETWORK ASSISTED BOOTSTRAPPING"이라는 제목으로 출원된 미국 가특허 출원 61/826176호의 이익을 주장하며, 그 내용들은 본 명세서에 참조로써 원용된다.

[0003] M2M(Machine-to-Machine) 기술들은, 디바이스들이 유선 및 무선 통신 시스템들을 사용하여 상호 더 직접적으로 통신하게 한다. M2M 기술들은 IoT(Internet of Things), 고유하게 식별가능한 오브젝트들의 시스템, 및, 인터넷과 같은, 네트워크를 통해 상호 통신하는 이러한 오브젝트들의 가상 표현들의 추가 실현을 가능하게 한다. IoT는, 심지어, 식료품 상점에서의 제품들 또는 가정에서의 가전제품들과 같은, 일상적인 매일의 오브젝트들과의 통신을 촉진할 수 있고, 이에 의하면 이러한 오브젝트들의 지식을 향상시키는 것에 의해 비용과 낭비를 절감할 수 있다. 예를 들어, 상점들은 재고에 있을 수 있거나 또는 판매되었을 수 있는 오브젝트들과 통신할 수 있거나, 또는 이들로부터 데이터를 얻을 수 있는 것에 의해 매우 정확한 재고 데이터를 유지할 수 있다.

[0004] 머신 투 머신 통신을 위한 표준화된 아키텍처들을 개발하려는 여러가지 노력들이 행해져 왔다. 이들은 3GPP(3rd Generation Partnership Project) MTC(Machine Type Communication) 아키텍처, ETSI M2M 아키텍처, 및 oneM2M 아키텍처를 포함한다. 이러한 아키텍처들이 이하 간략히 요약된다.

[0005] 3GPP EPC(Evolved Packet Core) 네트워크는, 머신들, 또는 디바이스들이, 스마트 미터링, 홈 오토메이션, eHealth, 소비자 제품들, 차량 관리(fleet management) 등에 연관되는 통신과 같이, 네트워크를 통해 상호 통신하는, M2M(Machine-to-Machine) 통신(MTC(Machine Type Communication)라고도 함)을 취급하는데 최적화되는 방식으로 본래 설계되지 않았다. 따라서, 3GPP 사양들의 R11(Release 11)에서, 3GPP는 머신 타입 통신/머신 투 머신 통신을 위한 UMTS 코어 네트워크의 인터워킹 능력들(interworking capabilities)을 향상시켰다. 인터워킹이란, 정보를 교환하거나, 디바이스들을 제어하거나, 또는 디바이스들을 모니터링하거나, 또는 디바이스들과 통신할 목적으로 코어 네트워크에 인터페이스하는 서버, 또는 애플리케이션을 말한다. 도 1은 TS 23.682 V11.5.0에서 3GPP에 의해 제시되는 MTC 아키텍처의 부분들을 도시한다.

[0006] 도 1에 도시된 바와 같이, 사용자 장비(314)는, E-UTRAN(LTE 액세스 네트워크)를 포함할 수 있는, RAN(Radio Access Network)(319)을 통해 EPC에 접속할 수 있다. eNodeB(evolved NodeB)(3)는 LTE 라디오에 대한 기지국이다. 본 도면에서, EPC는, 서빙 GW(Serving Gateway)(310), PDN GW 또는 P-GW(Packet Data Network Gateway)(353), MME(Mobility Management Entity)(312) 및 HSS(Home Subscriber Server)(357)를 포함하는, 다수의 네트워크 엘리먼트들을 포함한다.

[0007] HSS(357)는 사용자 관련된 및 가입자 관련된 정보를 포함하는 데이터베이스이다. 이는 모빌리티 관리, 콜 및 세션 셋업, 사용자 인증 및 액세스 승인에서의 지원 기능들을 또한 제공한다.

[0008] 게이트웨이들(S-GW(310) 및 P-GW(352))은 사용자 평면을 다룬다. 이들은 UE(User Equipment)(314)와 외부 네트워크(들) 사이에서 IP 데이터 트래픽을 전송한다. S-GW(310)는 라디오 사이드와 EPC 사이의 상호접속의 포인트이다. 그 명칭이 나타내는 바와 같이, 이러한 게이트웨이는 인입(incoming) 및 인출(outgoing) IP 패킷들을 라우팅하는 것에 의해 UE를 서비스한다. 이는 인트라-LTE 모빌리티에 대한(즉, RAN(319)에서 eNodeB들 사이의 핸드오버의 경우에) 및 LTE와 다른 3GPP 액세스들 사이의 앵커 포인트(anchor point)이다. 이는 나머지 게이트웨이, PGW(353)에 논리적으로 접속된다.

[0009] P-GW(353)는 EPC와 인터넷과 같은 외부 IP 네트워크들 사이의 상호접속의 포인트이다. 이러한 네트워크들은 그 명칭들인 PDN들(Packet Data Networks)이라 한다. P-GW(353)는 패킷들을 PDN들에 및 이로부터 라우트한다.

P-GW(353)는 IP 어드레스 / IP 프리픽스 할당 또는 정책 제어 및 충전과 같은 다양한 기능들을 또한 수행한다. 3GPP는 이러한 게이트웨이들이 독립적으로 동작하는 것을 명시하지만 실제로 이들은 네트워크 벤더들에 의해 단일 "박스(box)"로 조합될 수 있다.

[0010] MME(312)는 제어 평면을 다룬다. 이는 E-UTRAN 액세스에 대한 모빌리티 및 보안에 관련되는 시그널링을 취급한다. 이러한 MME는 아이들 모드에 있는 UE들의 추적 및 페이징을 담당한다. 이는 또한 NAS(Non-Access Stratum)의 종료 포인트이다.

[0011] 위에 언급된 바와 같이, UE(314)는 E-UTRAN을 사용하여 EPC에 도달할 수 있지만, 이것이 지원되는 유일한 액세스 기술은 아니다. 3GPP는 다수의 액세스 기술들의 지원을 명시하며 또한 이러한 액세스들 사이의 핸드오버를 명시한다. 이러한 아이디어는 다수의 액세스 기술들을 통해 다양한 IP 기반의 서비스들을 제공하는 고유한 코어 네트워크를 사용하는 수렴을 야기하는 것이다. 기존 3GPP 라디오 액세스 네트워크들이 지원된다. 3GPP 사양들은, E-UTRAN(LTE 및 LTE-Advanced), GERAN(Radio Access Network of GSM/GPRS) 및 UTRAN(Radio Access Network of UMTS-based technologies WCDMA and HSPA) 사이에 어떻게 인터워킹이 달성되는지 정의한다.

[0012] 이러한 아키텍처는 또한 논-3GPP 기술들이 UE와 EPC를 상호접속하게 한다. 논-3GPP는 이러한 액세스들이 3GPP에 명시되지 않았다는 것을 의미한다. 이러한 기술들은, 예를 들어, WiMAX, cdma2000®, WLAN 또는 고정형 네트워크들을 포함한다. 논-3GPP 액세스들은 2가지 카테고리들: "신뢰형(trusted)" 및 "비신뢰형(untrusted)" 카테고리들로 나뉠 수 있다. 신뢰형 논-3GPP 액세스들은 EPC와 직접 상호작용할 수 있다. 비신뢰형 논-3GPP 액세스들은 ePDG(for Evolved Packet Data Gateway)(도시되지 않음)라 하는 네트워크 엔티티를 통해 EPC와 인터워킹한다. ePDG의 주요 역할은 비신뢰형 논-3GPP 액세스를 통해 UE와의 접속들의 IPsec 터널링과 같은 보안 메커니즘들을 제공하는 것이다. 3GPP는 어느 논-3GPP 기술들이 신뢰형 또는 비신뢰형으로 고려되어야 하는지 명시하지 않는다. 이러한 결정은 오퍼레이터에 의해 이루어진다.

[0013] 도 1에 또한 도시되는 바와 같이, SCS(Service Capability Server)(361)는 코어 네트워크, 디바이스들 및 애플리케이션들에 서비스들을 제공할 수 있다. SCS는, M2M 서버, MTC 서버, SCL(Service Capability Layer), 또는 CSE(Common Services Entity)라 불릴 수도 있다. SCS(361)는 HPLMN(Home Public Land Mobile Network)에 의해 또는 MTC 서비스 프로바이더에 의해 제어될 수 있다. SCS는 오퍼레이터 도메인 내부에 또는 외부에 배치될 수 있다. SCS가 오퍼레이터 도메인 내부에 배치되면, 이러한 SCS는, 내부 네트워크 기능일 수 있고, 오퍼레이터에 의해 제어될 수 있다. SCS가 오퍼레이터 도메인 외부에 배치되면, 이러한 SCS는 MTC 서비스 프로바이더에 의해 제어될 수 있다.

[0014] 도 1의 MTC 아키텍처에서, SCS(361)는 Tsp 참조 포인트(즉, 인터페이스)(308)를 통해 MTC-IWF(MTC(Machine Type Communication) Interworking Function)(359)와 통신할 수 있다. Tsp 참조 포인트는 코어 네트워크와 인터워킹하는데 사용되는 인터페이스의 일 예이다.

[0015] UE는, RAN(Radio Access Network)(319)을 포함하는, PLMN(Public Land Mobile Network)을 통해 SCS(들) 및/또는 다른 MTC UE(들)과 통신할 수 있다. MTC UE(214)는 하나 이상의 MTC 애플리케이션들(316)을 관리할 수 있다. MTC 애플리케이션들은 하나 이상의 AS(Application Servers)(예를 들어, AS(320)) 상에서 또한 관리될 수 있다. MTC 애플리케이션(316)은, SCS(361), AS MTC 애플리케이션들, 또는 다른 UE MTC 애플리케이션들과 상호작용할 수 있는 MTC 통신 엔드포인트일 수 있다.

[0016] AS(Application Server)(예를 들어, AS(320)) 또한 하나 이상의 MTC 애플리케이션들을 관리할 수 있다. AS(320)는 SCS(161)과 인터페이스할 수 있고, SCS(361)는 AS(320) 상에서 실행되는 애플리케이션(들)에 서비스를 제공할 수 있다. AS 상의 MTC 애플리케이션들은, SCS들, UE MTC 애플리케이션들, 또는 다른 MTC 애플리케이션들과 인터페이스할 수 있다.

[0017] MTC-IWF(MTC Inter Working Function)(359)는 SCS(361)에게 내부 PLMN 토폴로지를 숨긴다. MTC-IWF는 PLMN에서 MTC 기능성(예를 들어, MTC UE 트리거링)을 지원하기 위해 (예를 들어, Tsp 참조 포인트(308)를 통해) 자신과 SCS 사이에 사용되는 시그널링 프로토콜들을 중계 및/또는 해석할 수 있다. 예를 들어, SCS는 MTC-IWF가 MTC 디바이스에 트리거를 보낼 것을 요청할 수 있다. MTC-IWF는, 예를 들어, SMS(도시되지 않음)를 통해 MTC 디바이스(314)에 MTC 트리거를 전달할 수 있다. MTC 디바이스(316)는, 이러한 트리거에 기초하여, SCS(312)에 응답할 수 있다. MTC 디바이스(314)는, 예를 들어, 센서 판독으로 응답할 수 있다. MTC 디바이스(214)가 SCS(312)에 응답할 때, MTC 디바이스는, P-GW(353)를 통해, SCS(316)과 통신하는데, PDN(Packet Data Network)/PDP(Packet Data Protocol)을 사용할 수 있다. MTC 디바이스는 IP 접속을 사용하여 SCS와 접속할 수

있다.

[0018] MTC-IWF(359)는, SCS가 3GPP 네트워크와 통신을 수립하기 이전에, SCS(361)를 승인할 수 있다. 예를 들어, SCS(359)가 Tsp 참조 포인트에 대한 트리거 요청을 행할 때, MTC-IWF(359)는, SCS가 이러한 트리거 요청을 보내는 것이 승인되는지 및 SCS가 트리거 제출들의 자신의 한도 또는 비율을 초과하지 않는지를 점검할 수 있다.

[0019] ETSI M2M 아키텍처가 도 2에 도시된다. 이러한 ETSI M2M 아키텍처에서, SCL(Service Capability Layer)는 네트워크에 서비스 능력들을 제공하는데 노출된 인터페이스들의 세트를 통한 코어 네트워크 기능성들을 사용한다. SCL은 하나 또는 여러가지 상이한 코어 네트워크들에 인터페이스할 수 있다.

[0020] 이러한 ETSI M2M 아키텍처에서, 네트워크는 M2M 디바이스들(예를 들어, 디바이스(145)), M2M 게이트웨이들(예를 들어, 게이트웨이(140)), 및 M2M 서버들(예를 들어, M2M 서버(125))를 포함한다. DA(Device Application)가 M2M 디바이스 상에서 실행중일 수 있고, GA(Gateway Application)가 M2M 게이트웨이 상에서 실행중일 수 있으며, NA(Network Application)가 M2M 서버 상에서 실행중일 수 있다. 또한 도시되는 바와 같이, 디바이스(예를 들어, 디바이스(145))는 DSCL(Device Service Capabilities Layer)(예를 들어, DSCL(146))을 사용하여 M2M 서비스 능력들을 구현할 수 있고, 게이트웨이는 GSCL(Gateway SCL)(141)을 구현할 수 있으며, 서버는 NSCL(Network SCL)(예를 들어, NSCL(126))을 구현할 수 있다.

[0021] mIa 참조 포인트는 네트워크 애플리케이션이 M2M 서버에서의 M2M 서비스 능력들에 액세스하게 한다.

[0022] dIa 참조 포인트는 M2M 디바이스에 상주하는 디바이스 애플리케이션이 동일 M2M 디바이스에서의 또는 M2M 게이트웨이에서의 상이한 M2M 서비스 능력들을 액세스하게 하고; M2M 게이트웨이에 상주하는 게이트웨이 애플리케이션이 동일 M2M 게이트웨이에서의 상이한 M2M 서비스 능력들을 액세스하게 한다.

[0023] mId 참조 포인트는 M2M 디바이스 또는 M2M 게이트웨이에 상주하는 M2M 서비스 능력들 레이어가 네트워크에서의 M2M 서비스 능력들 레이어와 통신하게 한다. mId 참조 포인트는 하위 레이어로서 코어 네트워크 접속성 기능들을 사용한다.

[0024] 또한 ETSI M2M 아키텍처에 따르면, M2M 엔티티(예를 들어, 하드웨어 및/또는 소프트웨어의 조합에 의해 구현될 수 있는 디바이스, 게이트웨이, 또는 서버/플랫폼과 같은 M2M 기능성 엔티티)가 애플리케이션 또는 서비스를 제공할 수 있다. 예를 들어, 광 센서는 검출되는 광 레벨들을 나타내는 데이터를 제공할 수 있고, 온도조절기(thermostat)는 온도 데이터 및 에어컨 제어들을 조절하는 능력을 제공할 수 있다. 이러한 데이터는, 다른 M2M 엔티티들에 의해 액세스될 수 있고 본질적으로 M2M 엔티티들 사이에 데이터를 교환하는 수단으로서 역할을 하는 "리소스"로서 사용가능하게 될 수 있다. 리소스는 URI(Universal Resource Indicator) 또는 URL(Universal Resource Locator)을 사용하여 어드레싱될 수 있는 데이터의 고유하게 어드레싱될 수 있는 표현일 수 있다. 이러한 리소스들의 사용가능성은 M2M SCL(Service Capabilities Layer)를 통해 M2M 엔티티들 사이에서 통신될 수 있다.

[0025] M2M SCL 또한 하드웨어 및 소프트웨어의 조합을 사용하여 구현될 수 있고 참조 포인트들(즉, M2M 엔티티들 사이의 기능성 인터페이스들) 상에 노출되는 기능들을 제공하는 기능성 엔티티이다. 예를 들어, M2M SCL은 상이한 M2M 애플리케이션들 및/또는 서비스들에 의해 공유되거나 또는 공동으로 사용되는 공동 (서비스) 기능들을 제공할 수 있다. M2M 서비스 능력들은, 노출된 인터페이스들(예를 들어, 3GPP, 3GPP2, ETSI TISPAN 등에 의해 명시되는 기존 인터페이스들)을 통해 3GPP 코어 네트워크 아키텍처의 기능들 및 능력들을 사용할 수 있고, 또한 하나 이상의 다른 코어 네트워크들에 인터페이스할 수 있다. M2M 디바이스들 및 엔티티들은 통상적으로 M2M 네트워크 도메인들 내에 조직화된다. 많은 구현들에서, NSCL(Network SCL) 엔티티와 함께 구성되는 M2M 서버(예를 들어, M2M 서버(125))는 동일 M2M 네트워크 도메인에서의 다른 디바이스들(예를 들어, 다른 M2M 디바이스들 및 M2M 게이트웨이들)에 의한 사용을 위해 리소스들 및 리소스 데이터를 유지할 수 있다.

[0026] 여전히 도 2를 참조하면, NSCL(126)은 네트워크 도메인(122)에 있을 수 있으며 M2M 서버 플랫폼(125)에서 NA(Network Application)(127)과 함께 구성될 수 있다. NA(127) 및 NSCL(126)은 참조 포인트 mIa(128)를 통해 통신할 수 있다. mIa 참조 포인트들은 NA가 M2M 도메인에서 NSCL로부터 사용가능한 M2M 서비스 능력들을 액세스하게 한다. 또한 네트워크 도메인(122) 내에는 M2M 게이트웨이 디바이스(140)에 구성될 수 있는 GSCL(141) 및 GA(Gateway Application)(142)가 있을 수 있다. GSCL(141) 및 GA(142)는 참조 포인트 dIa(143)를 사용하여 통신할 수 있다. 또한 네트워크 도메인(122) 내에는 M2M 디바이스(145)에 구성될 수 있는 DSCL(146) 및 DA(Device Application)(147)가 있을 수 있다. DSCL(146) 및 DA(147)는 참조 포인트 dIa(148)를 사용하여 통신할 수 있다. GSCL(141) 및 DSCL(146) 각각은 참조 포인트 mId(124)를 사용하여 NSCL(126)과 통신할 수

있다. 일반적으로, dIa 참조 포인트들은 디바이스 및 게이트웨이 애플리케이션들이 그들 각각의 로컬 서비스 능력들(즉, 각각 DSCL 및 GSCL에서 사용가능한 서비스 능력들)과 통신하게 한다. mId 참조 포인트는 M2M 디바이스(예를 들어, DSCL(146)) 또는 M2M 게이트웨이(예를 들어, GSCL(141))에 상주하는 M2M SCL이 네트워크 도메인에서의 M2M 서비스 능력들과 또는 그 역으로(예를 들어, NSCL(126)) 통신하게 한다.

[0027] 통상적으로, 디바이스(145), 게이트웨이(140), 및 M2M 서버 플랫폼(125)은, 도 8c 및 도 8d에 도시되고 이하 설명되는 디바이스들과 같은, 컴퓨팅 디바이스들을 포함한다. NSCL, DSCL, GSCL, NA, GA, 및 DA 엔티티들은 통상적으로, 시스템(120)에서 그들 각각의 기능들을 수행하도록, 하위 디바이스 또는 플랫폼 상에서 실행되는, 소프트웨어의 형태로 구현되는 논리적 엔티티들이다. ETSI M2M 아키텍처의 M2M 서버(125)는 3GPP MTC 아키텍처에서의 SCS(예를 들어, 도 1의 SCS(361))일 수 있다.

[0028] 또한 도 2에 도시된 바와 같이, NSCL(131)이 NA(132)와 함께 도메인(130)에 있을 수 있다. NA(132) 및 NSCL(131)은 mIa 참조 포인트(133)를 통해 통신할 수 있다. 네트워크 도메인(135)에서의 NSCL(136) 및 네트워크 도메인(138)에서의 NSCL(139)이 있을 수 있다. mIm 참조 포인트(123)는, 네트워크 도메인(122)에서의 NSCL(126), 네트워크 도메인(130)에서의 NSCL(131), 네트워크 도메인(135)에서의 NSCL(136), 또는 네트워크 도메인(138)에서의 NSCL(139)과 같은, 상이한 네트워크 도메인들에서의 M2M 네트워크 노드들이 상호 통신하게 하는 도메인간 참조 포인트가 존재할 수 있다. 본 명세서에서는 간단히, SCS(Service Capability Server), NSCL, 애플리케이션 서버, NA, 또는 MTC 서버를 나타내는데 "M2M 서버"라는 용어가 사용될 수 있다. 또한, UE(User Equipment)라는 용어는, 본 명세서에 논의되는 바와 같이, GA, GSCL, DA, 또는 DSCL에 적용될 수 있다. UE는, M2M 또는 MTC 디바이스 또는 게이트웨이와 같은, 3GPP 또는 다른 무선 네트워크에서 통신할 수 있고, 예를 들어, 머신들, 센서들, 기기들, 또는 그와 유사한 것, 모바일 스테이션, 고정형 또는 모바일 가입자 유닛, 페이저, PDA(Personal Digital Assistant), 컴퓨터, 모바일 폰 또는 스마트 폰, 또는 유선 또는 무선 환경에서 동작할 수 있는 임의의 다른 타입의 디바이스를 포함할 수 있는 임의의 무선 디바이스를 포함할 수 있다.

[0029] 3GPP MTC 및 ETSI M2M 아키텍처들이 본 명세서에서 배경기술을 통해 설명되며 이하 설명되는 다양한 실시예들을 예시하는데 사용될 수 있지만, 이하 설명되는 실시예들의 구현은 본 개시내용의 범위 내에 남아 있으면서 변경될 수 있다는 점이 이해된다. 통상의 기술자는 개시되는 실시예들이 위에 논의된 3GPP 또는 ETSI M2M 아키텍처들을 사용하는 실시예들에만 제한되는 것이 아니라, oneM2M, MQTT(MQ Telemetry Transport), 및 다른 관련된 M2M 시스템들 및 아키텍처들과 같은, 다른 아키텍처들 및 시스템들에 구현될 수 있다는 점 또한 인식할 것이다.

[0030] M2M 시스템들에서 종종 수행되는 하나의 프로세스는 부트스트랩핑이라 불리운다. 부트스트랩핑은 그에 의해 엔티티들(예를 들어, 최종 사용자 디바이스 또는 서버)이 그들 사이의 안전한 통신들을 가능하게 하는 관계를 수립하기 위해 상호 인증 및 키 공유(key agreement)를 수행하는 프로세스이다. 상호 인증은 각 당사자가 자신의 아이덴티티를 다른 것에게 증명하는 프로시저이다. 인증은 악의적 디바이스가 정당한 최종 사용자 디바이스로 가장하여 서버에 등록하는 것을 방지하는 것을 돕는다. 인증은 부당한 서버가 정당한 서버인 것으로 가장하여 최종 사용자 디바이스와 접속을 수립하는 부당한 서버를 구성할 수 있는 중간자 공격(man-in-the-middle attack)을 수행하는 것을 방지하는 것을 또한 돕는다.

[0031] 키 공유는 통신 엔티티들이, 예를 들어, 보안 키를 사용하는 암호화 프로세스에 의해, 그들 사이의 통신들을 안전하게 하는데 나중에 사용할 수 있는 보안 키를 유도하는 프로시저이다. 키 공유 메커니즘의 특징은 키가 송신되지 않는다는 점이다. 키 유도 기능은, 예를 들어, 최종 사용자 디바이스 및 서버만이 아는 것을 의미하는 공유된 비밀 값에 기초할 수 있다. 이러한 공유된 비밀 또한 송신되지 않는다. 키 유도 기능은, 공유된 비밀을 알지 못하는, 엿듣는 사람(eavesdropper)이 키 공유 프로시저 동안 송신되는 메시지들을 관찰하는 것에 의해 키를 계산해 낼 엄두를 못낼 만큼 계산적으로 복잡하게 설계된다. 일부 인증 및 키 공유 메커니즘들의 개요가 본 명세서에 논의된다. EAP(Extensible Authentication Protocol) 및 PANA(Protocol for carrying Authentication for Network Access)와 같은, 일부 인증 및 키 공유 메커니즘들의 개요가 개시되는 실시예들에 추가적 정황을 제공하도록 이하 논의된다.

[0032] EAP(Extensible Authentication Protocol)는 자체로 인증 방법은 아니지만, 구체적 인증 방법들을 구현하는데 사용될 수 있는 공동 인증 프레임워크이다. 환언하면, EAP는, Peer, Authenticator, 및 Authentication Server가 어떠한 인증 방법이 사용될지 협상하게 하는 프로토콜이다. 선택된 인증 방법은 그리고 나서 EAP 프로토콜의 내부에서 실행된다. EAP는 RFC 3748에 정의된다. RFC 3748은 원하는 인증 메커니즘의 협상과 같은 기본 기능들 뿐만 아니라 EAP 패킷 포맷, 프로시저들을 설명한다.

[0033] 도 4는 기본 EAP 아키텍처를 도시한다. 도 4에 도시되고 RFC 3748에 설명되는 바와 같이, EAP 인증기(163)(예를 들어, 액세스 포인트)를 통해 인증 서버(162)에 접촉할 수 있는 EAP 피어(161)가 존재한다. EAP는 Radius 또는 Diameter 프로토콜들을 사용할 수 있다. IETF에 의해 정의되는 많은 EAP 방법들이 존재한다. 본 명세서에는 UMTS(Universal Mobile Telecommunications System)-AKA에 기초하고 RFC 4187에 정의되는 EAP-AKA(Authentication and Key Agreement)라 불리우는 EAP 방법이 논의된다. 그렇지만, 본 명세서에 제시되는 아이디어들 중 많은 것은 선택된 EAP 인증 방법에 무관하게 사용될 수 있다. EAP는 링크 레이어(Layer 2) 프로토콜로서 설계되었다. PANA는 IP 네트워크를 통해 EAP 메시지들을 전달하는데 사용될 수 있는 프로토콜이다. 환언하면, PANA는 EAP에 대한 전송수단이다. PANA는 네트워크(IP) 레이어의 상위 상에서 실행된다. PANA는 RFC5191에 정의된다. PANA는 다이나믹 서비스 프로바이더 선택을 허용하고, 다양한 인증 방법들을 지원하고, 사용자들을 로밍하는데 적합하며, 링크 레이어 메커니즘들로부터 독립적이다.

발명의 내용

[0034] 부트스트랩핑은 원하는 레벨의 보안을 달성하기 위해 비밀 키들 또는 인증서들이 디바이스에 공급될 것을 종종 요구한다는 점에서 값비싼 프로세스일 수 있다. 이는 SCS, 또는 M2M 서버와 부트스트랩하는데 요구되는 다수의 디바이스들 때문에 머신 투 머신 필드에서 특히 중요한 문제이다. 본 명세서에는 적어도 2개의 부트스트랩핑 접근방식들을 위한 방법들, 디바이스들 및 시스템들이 개시된다. 일 실시예에서는, 액세스 네트워크에 의해 이미 요구되는 것을 넘어 공급을 요구하지 않고도 D/GSCL들이 M2M 서버와 부트스트랩할 수 있도록 서비스 레이어가 액세스 네트워크 인프라구조에 영향을 줄 수 있다. 이러한 접근방식에서, MTC-IWF는 액세스 네트워크의 AAA 서버로의 안전한 접속을 제공할 수 있다. UE가 액세스 네트워크에 속할 때 액세스 네트워크의 AAA 서버에 의해 서비스 레이어 키 재료가 M2M 서버에 제공될 수 있다. 다른 실시예에서는, M2M 서버가 디바이스를 인증 및 승인하는데 코어 네트워크의 인프라구조를 사용하도록 프로시저들이 정의된다. 예를 들어, UE 및 M2M 서버가 EAP-AKA-PANA 인증을 수행할 수 있도록 EAP-PANA 기반의 접근방식이 EAP 인증 서버로서 HSS를 사용할 수 있다.

[0035] 이러한 개요는 하기의 상세한 설명에서 더 설명되는 개념들 중 선택된 것들을 간단한 형태로 소개하기 위해 제공된다. 이러한 개요는 청구되는 주제의 주요 특징들 또는 핵심 특징들을 식별하기 위해 의도되는 것은 아니며, 청구되는 주제의 범위를 제한하는데 사용되도록 의도되는 것도 아니다. 또한, 청구되는 주제는 본 개시내용의 임의의 부분에서 언급되는 임의의 또는 모든 단점들을 해결하는 한정들에 제한되는 것이 아니다.

도면의 간단한 설명

[0036] 첨부 도면들과 함께 예를 통해 주어지는 이하의 설명으로부터 보다 상세한 이해가 이루어질 수 있다.

도 1은 3GPP MTC(Machine Type Communication) 아키텍처를 도시하는 블록도이다.

도 2는 ETSI M2M 아키텍처를 도시하는 블록도이다.

도 3은 일반적 EAP 아키텍처를 도시한다.

도 4는 M2M을 위한 EAP-PANA-AKA 아키텍처를 도시한다.

도 5는 EAP-PANA D/GSCL 부트스트랩핑의 흐름도를 도시한다.

도 6은 M2M을 위한 EAP 액세스 네트워크 기반의 서비스 레이어 부트스트랩핑을 도시한다.

도 7a는 액세스 네트워크 EAP 기반의 D/GSCL 부트스트랩핑의 흐름도를 도시한다.

도 7b는 도 7a로부터 계속되는 액세스 네트워크 EAP 기반의 D/GSCL 부트스트랩핑의 흐름도를 도시한다.

도 8a는 하나 이상의 개시되는 실시예들이 구현될 수 있는 예시적인 M2M(Machine-to-Machine) 또는 IoT(Internet of Things) 통신 시스템의 시스템 도면이다.

도 8b는 도 8a에 도시되는 M2M/IoT 통신 시스템 내에 사용될 수 있는 예시적인 아키텍처의 시스템 도면이다.

도 8c는 도 8a에 도시되는 통신 시스템 내에 사용될 수 있는 예시적인 M2M/IoT 단말 또는 게이트웨이 디바이스의 시스템 도면이다.

도 8d는 도 8a의 통신 시스템의 양상들이 구현될 수 있는 예시적인 컴퓨팅 시스템의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0037] 진행에 앞서, 본 명세서에 기재되는 실시예들은 REST(Representational State Transfer) 아키텍처의 관점에서 설명될 수 있고, 설명되는 컴포넌트들 및 엔티티들은 REST 아키텍처(RESTful 아키텍처)의 제약들에 따른다는 점이 주목되어야 한다. RESTful 아키텍처는 사용되는 물리적 컴포넌트 구현 또는 통신 프로토콜들의 관점에서보다는 오히려 아키텍처에 사용되는 컴포넌트들, 엔티티들, 커넥터들, 및 데이터 엘리먼트들에 적용되는 제약들의 관점에서 설명된다. 따라서, 이러한 컴포넌트들, 엔티티들, 커넥터들, 및 데이터 엘리먼트들의 역할들 및 기능들이 설명될 것이다.

[0038] RESTful 아키텍처에서, 고유하게 어드레싱가능한 리소스들의 표현들은 엔티티들 사이에 이동된다. ETSI M2M 사양(예를 들어, 본 명세서에 논의되는 바와 같은 TS 102 921 및 TS 102 690)은 SCL 상에 상주하는 리소스 구조를 표준화하였다. RESTful 아키텍처에서 리소스들을 취급할 때, Create(자식 리소스들을 생성함), Retrieve(리소스의 콘텐츠를 판독함), Update(리소스의 콘텐츠를 기입함) 또는 Delete(리소스를 삭제함)와 같은, 리소스들에 적용될 수 있는 기본 메소드들이 존재한다. 통상의 기술자는 즉각적인 실시예들의 구현들이 본 개시내용의 범위 내에 남아 있으면서 변경될 수 있다는 점을 인식할 것이다. 통상의 기술자는, 개시되는 실시예들이 예시적인 실시예들을 설명하기 위해 본 명세서에 설명되는 ETSI M2M 아키텍처를 사용하는 구현들에 제한되는 것은 아니라는 점을 또한 인식할 것이다. 개시되는 실시예들은, oneM2M 및 다른 M2M 시스템들 및 아키텍처들과 같은, 다른 아키텍처들 및 시스템들에 마찬가지로 구현될 수 있다.

[0039] 본 명세서에 논의되는 EAP-PANA 접근 방식 및 EAP 액세스 네트워크 기반의 접근 방식은 서비스 레이어가 보다 경량이 되게 할 수 있다. EAP-PANA 접근 방식 및 EAP 액세스 네트워크 기반의 접근 방식에서는, M2M 서버의 NSCL로부터 액세스 네트워크까지 인터페이스가 제공되지만, 이러한 인터페이스가 ETSI M2M 사양들에 의해 완전히 정의되는 것은 아니다. ETSI M2M 아키텍처 사양의 섹션 8.3.2 및 ETMS M2M mIa, dIa, mId 사양의 섹션 6.2를 포함하는, ETSI M2M 사양들은, 본 명세서에 논의되는 바와 같이, 액세스 네트워크 지원형 부트스트랩핑 방법들을 위한 지원을 제공한다. 본 명세서에 개시되는 키 공유 예들은 M2M 서비스 레이어 루트 키(kmr)을 유도하는 D/GSCL 및 M2M 서버를 포함한다.

[0040] 본 명세서에 개시되는 부트스트랩핑 접근방식들은 ETSI M2M 아키텍처 사양의 섹션 8.3.2, ETSI TS 102 690, 및 ETSI TS 102 921에 개요가 서술되는 액세스 네트워크 지원형 M2M 부트스트랩 프로시저들과 유사하다. 이하 더욱 상세히 논의되는 바와 같이, ETSI M2M 아키텍처는, 베이스라인으로서 사용되고, 프로세서들을 보다 효율적이게 하고 액세스 네트워크의 능력들을 보다 우수하게 개발하도록 확장된다. 액세스 네트워크는 가입자들을 그들의 직속 애플리케이션 서비스 프로바이더에게 접속시키는 전기통신 네트워크의 부분으로 일반적으로 고려될 수 있다.

[0041] 본 명세서에 개시되는 각각의 부트스트랩핑 방법은, (i) UE의 D/GSCL(이하, UE D/GSCL)이 M2M 서버의 NSCL(이하 M2M 서버)와 상호 인증을 수행하게 코어 네트워크 인프라구조에 영향을 줄 수 있고; (ii) 부트스트랩핑 프로세스의 일부로서, 서비스 레이어 루트 키, Kmr을 유도하도록 코어 네트워크 인프라 구조(예를 들어, 홈 퍼블릭 랜드 모바일 네트워크(home public land mobile network))에 영향을 줄 수 있고; (iii) 부트스트랩핑 프로세스가 완료될 때, UE D/GSCL이 M2M 서버에 등록되도록, 등록 프로세스를 통합할 수 있다.

[0042] 본 명세서에 개시되는 부트스트랩핑 접근방식들 중 하나는 EAP-PANA 기반의 접근방식이다. 요약하면, EAP-PANA 기반의 접근 방식은 UE D/GSCL 및 M2M 서버가 EAP-AKA-PANA 인증을 수행할 수 있도록 HSS(Home Subscriber Server)를 EAP 인증 서버(예를 들어, 인증 서버(162))로서 사용할 수 있다. 이러한 접근방식에서, UE D/GSCL은 EAP 피어(예를 들어, EAP 피어(161))로 고려되고, M2M 서버는 EAP 인증기(예를 들어, EAP 인증기(163))로 고려된다. M2M 서버는 MTC-IWF(Machine Type Communication Inter-Working Function)를 통해 EAP 인증 서버(예를 들어, HSS)에 접촉한다.

[0043] 도 4는 셀룰러 액세스 네트워크와 인터워킹하는 EAP-PANA-AKA 아키텍처(170)를 나타낸다(EAP-PANA 접근방식). UE D/GSCL(171)은 EAP-PANA를 사용하여 M2M 서버(174)와 통신가능하게 접속된다. M2M 서버(174)는 Tsp 참조 포인트(178)를 통해 EAP 인증 서버(175)에 통신가능하게 접속된다. EAP 인증 서버(175)는 MTC-IWF(177) 및 HSS(176)을 포함하는데, 이들은 S6m 참조 포인트(179)를 통해 접속된다. EAP 인증 서버(175)는, NAS(Non-Access-Stratum) 및 SMS(Short Messaging Service)와 같은, 액세스 네트워크 제어 평면(181)을 통해 UE(171)에 통신가능하게 접속된다. 이러한 아키텍처에서, UE D/GSCL(171)은 EAP 피어이고, M2M 서버(174)는 EAP 인증기이며, HSS(176)과 함께 MTC-IWF(177)는 EAP 인증 서버(175) 내에 통합되는 것으로 고려된다.

[0044] MTC-IWF(177)는 M2M 서버(174)에게 코어 네트워크 토폴로지를 숨긴다. 따라서, EAP 인증 서버(175)는, AAA(Authentication, Authorization, and Accounting) 서버(도시되지 않음)와 같은, HSS(176) 이외의 엔티티를

포함할 수 있다. ETSI 전문용어들에서, MTC-IWF(177)는 MAS(M2M Authentication Server) 또는 MAS에 대한 인터페이스이다. MSBF(M2M Service Bootstrap Function)는 M2M 서버(174)의 부분이다.

[0045] 도 4에 도시된 바와 같은 EAP-PANA 기반의 아키텍처를 참조하여, AKA가 사용되면, 인증 키 Ki가 UICC(Universal Integrated Circuit Card)(도시되지 않음) 및 HSS(176)에서 공급되지 않기 때문에 HSS(176)는 인증 서버로서 사용된다. 인증 키가 UE D/GSCL(171) 상의 어느 다른 매체에 저장되어 AAA 서버와 같은 다른 네트워크 노드에서 공급되면, 동일한 아키텍처가 적용된다.

[0046] EAP-PANA-AKA 부트스트랩핑 프로시저의 호출 흐름이 도 5에 도시되고 이하 논의된다. 도 5는 EAP-PANA-AKA를 사용하여 M2M 서버(192)를 부트스트랩핑하여 이에 등록하는 UE D/GSCL(191)의 흐름(190)을 도시한다. 단계 195에서는, PCI(PANA-Client-Initiation) 메시지가 UE D/GSCL(191)에 의해 M2M 서버(192)에 송신된다. PCI 메시지는 PANA 사양, IETF RFC 5191에서 정의된다. 단계 195에서 송신된 PCI 메시지는 등록 요청이다. PCI 메시지의 목적지 IP 어드레스는 M2M 서버(192)의 IP 어드레스이고, 목적지 포트 번호는 PANA 포트 번호(예를 들어, 포트 716)일 수 있다. M2M 서버(192)는 PANA 메시지들을 위해 UE D/GSCL(191)이 듣는 IP 어드레스 및 포트 번호를 결정하는데 메시지의 소스 IP 어드레스 및 포트 번호를 사용한다. 일 실시예에서, M2M 서버(192)가, UE D/GSCL(191)의 IP 어드레스를 알고, PANA 메시지들을 위해 자신이 듣는 포트 번호를 알면, M2M 서버(192)는 부트스트랩핑을 착수할 수 있다. 예를 들어, M2M 서버(192)가 UE(191) 상에서 자신이 요구하는 일부 서비스들을 발견하면 이러한 것이 바람직할 수 있다. PANA 사양은 PCI 메시지에서의 AVP들(Attribute Value Pairs)을 정의하지 않는다. 그러나, ETSI 사양, ETSI TS 102 921는, PCI 메시지를 위해 사용될 수 있는 AVP들을 정의한다. 표 1은 사용될 수 있는 AVP들 중 일부의 예들을 나타낸다. MSM-MSBF-ID, M2M-NSCL-ID, M2M-D/GSCL-ID, 및 M2M-SP-ID는, D/GSCL이 타겟 등록을 특정의 MSBF들, NSCL들, 또는 서비스 프로바이더들에 제한하기 원하면 사용되는 옵션의 AVP들이다.

표 1

PCI 메시지를 위한 AVP들

AVP	설명
M2M-Usage-Type	부트스트랩핑시 “M2M Bootstrapping” 으로 설정될 수 있음.
M2M-Node-ID	M2M-Node-ID는 디바이스 식별자를 전달함. 3GPP 가능 디바이스들이 이 값을 자신들의 M2M-Node-ID 외부 식별자로 설정할 수 있음.
MSM-MSBF-ID	MSM-MSBF-ID는 MSBF (M2M Service Bootstrap Function) 식별자를 전달함. MSM-MSBF-ID AVP는 NSCL에게 인증 서버의 아이덴티티를 알림. 이 필드는 3GPP 디바이스들이 부트스트랩핑할 때 필요하지 않음. 3GPP 디바이스들에서, 인증 서버는 MTC-IWF/HSS임. MTC-IWF 아이덴티티는 M2M-Node-ID 상의 DNS(Domain Name Service) 룩업을 통해 유도될 것임.
M2M-NSCL-ID	M2M-NSCL-ID는 NSCL을 식별함.
M2M-D/GSCL-ID	M2M-D/GSCL-ID는 D/GSCL을 식별함. M2M-D/GSCL-ID는 요청된 D/GSCL 식별자임.
M2M_SP-ID	M2M_SP-ID는 서비스 프로바이더를 식별함.

[0047]

[0048] 단계 196에서는, PAR(PANA-Auth-Request) 메시지가 UE D/GSCL(191)에 송신된다. PAR(PANA-Auth-Request) 메시지는 IETF RFC 5191(PANA 사양)에서 정의된다. M2M 서버(192)가 UE D/GSCL(191)의 IP 어드레스를 알지 못하면, PAR 메시지는 UE D/GSCL(191)이 도달될 수 있는 어드레스에 브로드캐스트(broadcast), 멀티캐스트(multicast), 또는 임의 캐스트(anycast)될 수 있다. 단계 197에서는, PANA 사양에서 정의되는, PAN(PANA-Auth-Answer) 메시지가 M2M 서버(192)에 송신된다. PAN 메시지는 "M2M Bootstrapping"으로 설정되는 M2M-Usage-Type AVP를 갖는다.

[0049] 단계 198에서는, M2M 서버(192)가 MTC-IWF(193)에 디바이스 인증 요청을 행한다. 디바이스 인증 요청은 디바이스의 3GPP 외부 디바이스 식별자를 포함한다. 이러한 경우, 본 명세서에 보다 상세히 논의되는, DIR(Device-Information-Request) 커맨드는 실행되는 커맨드일 수 있다. DIR 커맨드는, IETF RFC 4187(EAP-AKA 사양)에서 정의되는 EAP-Response/AKA-Identity 메시지를 전달하는, EAP_Payload AVP를 포함할 수 있다. EAP 페이로드는 EAP-Response 메시지 또는 AKA-Identity 메시지와 동일하다. DIR 커맨드는, External ID, M2M 서버 ID(SCS ID), 및 Requested Param을 또한 포함할 수 있으며, 이들 모두는 EAP AKA 키 재료(EAP_AKA_KEY_MATERIAL)이다.

[0050] 단계 199에서는, MTC-IWF(193)가 단계 198과 관련된 디바이스 인증 요청을 HSS(194)에 송신한다. 디바이스 인증 요청을 수신한 후, HSS(194)는, 단계 200에서, AUTN(Authentication TokeN), RAND(RANDom challenge), XRES(eXpected authentication RESponse), MAC(Message Authentication Code), 및 M2M Root Key를 생성하는 AKA 알고리즘을 실행한다. 단계 201에서는, HSS(194)가 MTC-IWF(193)에 EAP-AKA 부트스트랩핑 정보를 송신한다. 본 명세서에 보다 상세히 논의되는, DIA(Device-Information-Answer) 커맨드는 실행되는 커맨드일 수 있다. DIA 커맨드는, External ID, M2M 서버 ID, 및 Requested Param을 포함할 수 있고, 이들 모두는 EAP AKA 키 재료(EAP_AKA_KEY_MATERIAL)이다. DIA 커맨드는 또한 RAND, XRES, AUTN, MAC, 및 M2M Root Key와 동일한 키 재료를 포함할 수 있다.

[0051] 단계 202에서는, MTC-IWF(193)가 M2M 서버(192)에 EAP-AKA 부트스트랩핑 정보를 보낸다. DIA 커맨드는 EAP_Payload AVP를 포함할 수 있다. 논의된 바와 같이, EAP_Payload AVP는 EAP-Request/AKA-Challenge 메시지를 전달하는데, 이는 EAP-AKA 사양에서 정의된다. 단계 202에서의 메시지는 랜덤 챌린지(AT_RAND), AUTN, 및 MAC를 전달한다. MTC-IWF(193)는 XRES 및 M2M Root Key(Kmr)를 보유한다. XRES는 M2M 서버(192)에 전달되지 않는다.

[0052] 단계 203에서는, UE D/GSCL(191)이 PAR 메시지를 수신한다. 이러한 PAR 메시지의 EAP_Payload는 단계 202로부터의 EAP-Request/AKA-Challenge 메시지를 전달한다. 단계 204에서는, UE D/GSCL(191)이, AKA 알고리즘을 실행하고, RAND(RANDom challenge)에 대한 RES(RESponse)를 생성하고, 이는 M2M 서버(192)를 인증하는데 AUTN을 사용한다. UE D/GSCL(191)은 ETSI TS 102 921에 의해 정의되는 바와 같이 M2M 루트 키, Kmr을 또한 유도한다. 단계 205에서는, M2M 서버(192)가 EAP-AKA 사양에서 정의되는 EAP-Response/AKA-Challenge 메시지를 전달하는 PAN 메시지를 수신한다. 단계 206에서는, M2M 서버(192)가 UE D/GSCL(191)로부터의 RES가 올바르다는 것을 점검하기 위해 MTC-IWF(193)에 다른 디바이스 인증 요청을 행한다. 단계 206에서의 요청은 UE D/GSCL(191)의 3GPP External Device Identifier를 포함한다. 단계 206에서는, DIR 커맨드가 송신될 수 있고 이는 External ID, M2M 서버 ID, EAP_Payload, 및 Requested Param AVP들을 포함할 수 있다. Requested Param은 EAP_AKA_KEY_MATERIAL로 설정될 수 있는데, 이는 External ID, M2M 서버 ID, 및 Requested Param을 포함한다. EAP_Payload AVP는 EAP Response 메시지 또는 AKA 챌린지 메시지와 동일할 수 있다.

[0053] MTC-IWF(193)가 단계 206의 요청을 수신한 후, MTC-IWF(193)은, 단계 207에서, RES를 XRES에 비교한다. 단계 208에서는, M2M 서버(192)가 EAP_AKA_KEY_MATERIAL(= External ID, SCS ID, 및 Requested Param) 및 EAP_Payload(=EAP-Success 또는 EAP-Failure, Kmr인 Key-Material)를 포함하는 응답을 수신한다. EAP-Success 메시지 및 EAP-Failure 메시지는 EAP 사양, IETF RFC 3748에서 정의된다. 단계 208에서는, EAP 성공 메시지가 수신되는 것으로 가정된다.

[0054] 단계 209에서는, UE D/GSCL(191)이 단계 208과 관련된 EAP-Success 메시지(또는 EAP-Failure 메시지)를 전달하는 PAR 메시지를 수신한다. 단계 209의 PAR 메시지는, M2M-Bootstrap-Result, M2M-Node-ID(Node-ID에 할당되는 서비스 프로바이더를 전달함), M2M-D/GSCL-ID, 및 M2M-NSCL-ID와 같은, 추가 정보를 포함할 수 있다. 단계 210에서는, PAN 메시지가 PANA를 통해 EAP-AKA 프로토콜을 사용하여 M2M 서버(192)를 부트스트랩핑하는 것 및 이에 등록하는 것이 성공적이라는 것을 나타내는 정보(예를 들어, 설정 완료, 또는 "C", 비트)를 전달할 수 있

다.

[0055] 2번째 부트스트랩핑 접근방식이 이제 설명될 것이다. 이러한 2번째 접근방식은 서비스 레이어 부트스트랩핑 및 등록을 위한 EAP 기반의 액세스 네트워크 등록(이하 EAP 액세스 네트워크 기반의 접근방식)에 영향을 준다. 요약하면, EAP 액세스 네트워크 기반의 접근방식은 UE D/GSCL이 액세스 네트워크와 인증하는데 EAP 방법들을 사용하는 경우에 사용될 수 있다. 이러한 접근방식에서, MTC-IWF는 액세스 네트워크 인증 서버에 안전한 접속을 제공한다. UE D/GSCL이 액세스 네트워크에 속할 때 서비스 레이어 키 재료는 액세스 네트워크의 AAA 서버에 의해 M2M 서버에 제공될 수 있다. 보안 키들을 교환하는데 이러한 접근방식을 사용하는 것에 의해, M2M 서버 및 UE D/GSCL이 아직 안전하지 않은 인터페이스를 통해 보안 키들을 협상할 필요성이 회피된다. 이러한 접근방식은 디바이스를 M2M 서버에 접속하는 프로세스를 간소화할 수 있다.

[0056] 신뢰형 WLAN(Wireless Local Area Network)를 통한 승인 및 인증은 3GPP TS 33.402에서 정의된다. 도 6은, 본 실시예에 따라, 서비스 레이어 부트스트랩핑 및 등록을 위한 EAP 기반의 액세스 네트워크 등록에 영향을 주는 아키텍처를 도시한다. 액세스 네트워크(222)에 관한 키들이 생성될 때 서비스 레이어 루트 키들이 AAA 서버 / HSS(224)에 의해 생성된다. MTC-IWF(225)는 M2M 서버(229)에 키 재료를 전달하는데 사용될 것이다. 이하 보다 상세히 논의되는, 호출 흐름이 도 7a 및 도 7b에 도시된다.

[0057] D/GSCL들을 액세스 네트워크와 부트스트랩핑하는데 EAP, 또는 유사한, 인증 방법들이 사용될 때, M2M 서버의 서비스 레이어는 디바이스와 부트스트랩핑하는 프로세스에 영향을 줄 수 있다. 일부 액세스 네트워크들은 액세스 네트워크 등록을 위해 EAP 방법들을 사용한다. 예를 들어, 도 6을 참조하면, UE D/GSCL(221)이 신뢰형 WLAN(223)을 통해 EPS(Evolved Packet System)과 접속할 때, UE D/GSCL(221)은 EAP-AKA'를 사용하여 코어 네트워크와 인증한다. AKA'(AKA-프라임)은 RFC 5488에서 정의된다. AKA'은 유도되는 키들(즉, M2M 루트 키)이 액세스 네트워크 명칭에 기초하는 AKA의 변수이다. EAP 액세스 네트워크 기반의 접근방식에 대해, 도 3에서의 EAP 액터들(actors)은, 각각, 도 6에 도시되는 바와 같은 액터들에 따르는 것으로서 맵핑될 것이다. EAP 피어(161)는 UE D/GSCL(221)과 맵핑될 수 있고, EAP 인증기(163)는 WLAN 액세스 포인트(223)와 맵핑될 수 있으며, 인증 서버(162)는 HSS(224)에 맵핑될 수 있다.

[0058] 도 7a 내지 도 7b는 3GPP TS 33.402의 도 6.2-1에 기초한다. 3GPP TS 33.402의 도 6.2-1은 신뢰형 논-3GPP 액세스 포인트를 통해 접속할 때 UE가 3GPP 액세스 네트워크와 어떻게 인증하고 키 공유를 수행하는지를 도시한다. 도 7a 내지 도 7b는, 이하 논의와 함께, UE D/GSCL(221)이 동시에 M2M 서버(229)를 부트스트랩핑하고, 이와 키 공유를 수행하며, 이에 등록할 수 있도록 프로세스들이 어떻게 확장되는지를 도시한다.

[0059] 이하의 메시지 설명들은 서비스 레이어 부트스트랩핑을 지원하기 위해 호출 흐름이 어떻게 확장되는지를 보여준다. 기존 단계들의 보다 상세한 설명에 대해서는 3GPP TS 33.402의 도 6.2-1를 참조하라. 도 7a 내지 도 7b는 신뢰형 논-3GPP 네트워크를 통한 UE D/GSCL 인증에 기초하지만(예를 들어, 직경 접속(diameter Connection) - SWm을 포함함), 서비스 레이어 부트스트랩핑을 위한 향상들은 EAP 기반의 방법들 또는 다른 유사한 수단을 통해 디바이스가 인증하게 하는 임의의 액세스 네트워크에 적용될 수 있다는 점에 주목하자.

[0060] 도 7a를 참조하면, 단계 247에서는, UE D/GSCL(241)이 액세스 포인트(242)와 접속하는데, 이는 신뢰형 논-3GPP 액세스 포인트이다. 단계 248에서는, 액세스 포인트(242)가 UE D/GSCL(241)의 아이덴티티를 요청한다. 단계 249에서는, UE D/GSCL(241)이 단계 248의 아이덴티티 요청에 대해 EAP 응답을 송신한다. UE D/GSCL(241)의 아이덴티티는 자신의 NAI(Network Access Identity)일 수 있다. 단계 249의 응답은 액세스 네트워크 퍼블릭 ID(예를 들어, 3GPP 외부 식별자), 서비스 프로바이더 식별자, 또는 UE D/GSCL(241) 상의 애플리케이션의 애플리케이션 ID를 포함하는 파라미터들을 전달하는 AVP들을 또한 포함할 수 있다. 서비스 프로바이더 식별자는 디바이스가 접속하기 원하는 서비스 레이어들을 제공하는 회사의 명칭일 수 있거나 또는 이는 디바이스가 접속하기 원하는 특정 서비스 레이어(예를 들어 NSCL ID)를 명명할 수 있다. 애플리케이션 ID(예를 들어, 3GPP에 대한 D/GSCL ID; onM2M에 대한 DA 또는 NA)는 요청 애플리케이션(GA, DA, DSCL, 또는 GSCL)이 할당되기를 요청하는 명칭일 수 있다.

[0061] 단계 250에서는, 액세스 포인트(242)가 단계 249로부터의 정보를 액세스 네트워크 AAA 서버(243)에 송신하는데, 이 또한 HSS일 수 있다. 단계 251 내지 단계 254는 AKA'이 사용될 때, 특히 UE D/GSCL(241)과 AAA 서버(243) 사이의 노드들이 단계 249의 본래 EAP 아이덴티티 응답 메시지에서의 사용자 아이덴티티를 변경하면, 일반적으로 행해진다. 단계 251에서는, AAA 서버(243)가 UE D/GSCL(241)의 AKA' 아이덴티티를 요청한다. 단계 252에서는, 단계 251의 요청이 UE D/GSCL(241)에 송신된다. 단계 253에서는, UE D/GSCL(241)이 자신의 아이덴티티로 응답한다(단계 249와 유사함). 단계 254에서는, 액세스 포인트(242)가 단계 253으로부터의 정보를 액세스

네트워크 AAA 서버(243)에 송신한다.

[0062] 단계 255에서는, HSS로부터의 가입자 정보에 기초하여, AAA 서버(243)가, UE D/GSCL(241)이 EPC를 액세스하는 것이 허용되는 것을 확인하고, UE D/GSCL(241)이 이전 단계에서 명명된 M2M 서버(246)에 등록하는 것이 허용되는 것을 확인한다. 더욱 명확히 하기 위해, 일반적으로 HSS는 가입자 정보를 유지하는 데이터베이스로 고려될 수 있다. 여기서 AAA 서버(243)는 HSS를 액세스하여 HSS에서의 정보에 기초하여 AAA 결정들을 행하는 것이 허용되는 서버이다. 단계 256에서는, UE D/GSCL(241)이 액세스 네트워크를 액세스하는 것이 허용되면, AKA 알고리즘이 실행될 것이다. 또한, "Attachment Block Enabled" 플래그가 인에이블되면 또는 NSCL ID가 단계 253에서 제공되었으면, AAA 서버(243)는 가입자 데이터에서 제공되는 MTC-IWF(245)의 어드레스에 메시지를 송신할 것이다. 이하 보다 상세히 설명되는, DPR(Device-Permission-Request) 커맨드는 Action-Type = Device Attach Request, External-ID, SCS-Identifier에 의해 실행될 수 있다. 단계 256에서의 메시지는 S6m 참조 포인트를 통해 송신된다. 이러한 메시지의 목적은 UE D/GSCL(241)이 부속되는 것이 허용되어야 하는지를 또는 M2M 서버(246)가 부속할 요청이 거절되기를 원하는지를 알아보는 것이다. UE D/GSCL(241)의 명칭이 단계 253에서 제공되었으면, 이러한 메시지는 UE D/GSCL(241)이 등록될 수 있도록 UE D/GSCL(241)의 명칭을 M2M 서버(246)에 제시하는데 또한 사용된다.

[0063] 단계 257에서는, UE D/GSCL(241)이 부속되는 것이 허용되어야 하는지를 결정하기 위한 메시지를 MTC-IWF(245)가 M2M 서버(246)에 송신한다. 이러한 메시지는 Tsp 참조 포인트를 통해 송신된다. DPR 커맨드는 Action-Type = Device Attach Request, External-ID에 의해 실행될 수 있다. 단계 258에서는, UE D/GSCL(241)이 부속하는 것이 허용되어야 하는지 여부의 표시에 의해 M2M 서버(246)가 응답한다. UE D/GSCL(241)이 부속되는 것이 허용되지 말아야 한다는 것을 M2M 서버(246)가 나타내면, M2M 서버(246)는 MTC-IWF(245)에게 이유를 제공하고, M2M 서버(246)는 MTC-IWF(245)에게 백오프 시간(backoff time)을 제공할 수 있다. UE D/GSCL(241)의 명칭이 제공되면(예를 들어, 단계 257에서 DPR을 통해), M2M 서버(246)로부터의 응답은 UE D/GSCL(241)의 명칭을 포함한다. M2M 서버(246)가 제시된 명칭을 수용하면, 동일한 명칭이 MTC-IWF에 다시 제공된다. DPA(Device-Permission-Answer) 커맨드가 단계 258에 대해 실행될 수 있다.

[0064] 단계 259에서는, UE D/GSCL(241)이 부속되는 것이 허용되어야 하는지를 M2M 서버(246)가 원하는지 여부의 표시를 MTC-IWF(245)가 AAA 서버(243)에 보낸다. UE D/GSCL(241)이 이 시점에 부속될 필요는 없다고 M2M 서버(246)가 나타내면, MTC-IWF(245)는 그 이유 및 백-오프 시간을 AAA 서버(243)에 제공한다. 이러한 메시지는 S6m 참조 포인트를 통해 송신되는데, 이는 DPA 커맨드를 사용하여 실행될 수 있다. 단계 260에서는, EAP MSK 및 EMSK가 생성된다. EAP MSK 및 EMSK는 EAP 알고리즘에서 빠져 나오는 표준 키들이다. 서비스 레이어 루트 키(Kmr)가 ETSI M2M Architecture Specification, ETSI TS 102 690의 섹션 8.3.2.3에 설명되는 바와 같이 AAA 서버에 의해 생성될 수 있다. Kmr은 (EMSK, "ETSI M2M Device-Network Root Key" | M2M-Node-ID | M2M-SP-ID)의 Hash와 동일하다.

[0065] 단계 261에서는, AAA 서버(243)가 UE D/GSCL(241)을 향해 EAP-Request를 송신한다. EAP 방법이 AKA'이면, 이러한 메시지는, RAND(RANDom challenge), AUTN(network authentication vector), 및 MAC(Message Authentication Code)를 포함한다. 아이덴티티 응답은, 액세스 네트워크 퍼블릭 ID, NSCL ID, 또는 할당된 애플리케이션 ID(예를 들어, D/GSCL ID)와 같은, 파라미터들을 전달하는 AVP들을 포함할 수 있다. 액세스 네트워크 퍼블릭 ID는 Kmr을 생성하는데 사용되는 M2M-Node_ID로서 사용될 수 있다. NSCL ID는 UE 애플리케이션(DA, GA, DSCL, 또는 GSCL)이 접속되어야 하는 특정 서비스 레이어를 나타내고, 이는 Kmr을 생성하는데 사용되는 M2M-SP-ID이다. 할당된 애플리케이션 ID는 NSCL에 의해 애플리케이션에 할당된 특정 식별자를 나타낸다. 이러한 값은 Kmr을 생성하는데 사용되는 M2M-Node_ID로서 사용될 수 있다. 단계 262에서는, 액세스 포인트(242)가 단계 261의 메시지를 UE D/GSCL(241)에 송신한다.

[0066] 도 7a의 흐름의 연속인, 도 7b에 도시된 바와 같이, 단계 263에서는, UE D/GSCL(241)이, AKA 알고리즘을 실행하고, AUTN이 네트워크를 인증하는데 올바른지 확인한다. 네트워크가 확인된 후, UE D/GSCL(214)은 RES에 대한 응답을 생성한다. 서비스 레이어 루트 키(예를 들어, Kmr)가, ETSI M2M 아키텍처 사양의 섹션 8.3.2.3에 설명된 바와 같이, UE D/GSCL(241)에 의해 생성될 수 있다. Kmr은 (EMSK, "ETSI M2M Device-Network Root Key" | M2M-Node-ID | M2M-SP-ID)의 Hash와 동일하다. 단계 264에서는, UE D/GSCL(241)이 RES를 랜덤 챌린지에 송신한다. 단계 265에서는, AAA 서버(243)가 단계 264의 RES를 수신한다. 단계 266에서는, AAA 서버(243)가 RES가 XRES와 동일한지 확인한다.

[0067] 도 7b를 참조하면, 단계 267에서는, "Reachable Indicators Enabled" 플래그가 인에이블되면 또는 NSCL ID가

단계 253에서 제공되면, AAA 서버(243)는 UE D/GSCL(241)를 위해 가입자 데이터에서 제공되었던 MTC-IWF(245)의 어드레스에 메시지를 보낸다. DNR(Device-Notification-Request) 커맨드는, 이하 보다 상세히 논의되는 바와 같이, Action-Type = Device Attach Event, External-ID, M2M-Identifier, Key-Material, UE Service Layer ID에 의해 실행될 수 있다. 단계 267에서의 메시지는, S6m 참조 포인트를 통해 송신되고, UE D/GSCL(241)이 부속되었다는 것을 M2M 서버(246)에 결국 알릴 것이다.

[0068] 단계 268에서는, M2M 서버(246)가 Tsp 참조 포인트를 통해 부속 통지를 수신한다. DNR 커맨드는 Action-Type = Device Attach Event, Key-Material, External-ID에 의해 실행될 수 있다. 단계 269에서는, M2M 서버(246)가 단계 268의 수신된 통지를 수신확인한다. 이하 보다 상세히 논의되는, DNA 커맨드가 단계 269에서 실행될 수 있다. 단계 270에서는, MTC-IWF(245)가 S6m 참조 포인트를 통해 AAA 서버(243)에 단계 269의 수신확인을 송신한다.

[0069] 단계 251 내지 단계 254와 유사하게, 블록 271에 있는 단계들은 AKA'가 사용중일때만 일반적으로 수행된다. 단계 272에서는, AAA 서버(243) 및 UE D/GSCL(241)이 보호된 성공적 결과 표시들을 사용하고 있으면, AAA 서버(243)는 EAP-Success 메시지를 송신하기 전에 UE D/GSCL(241)에 EAP-Request/AKA'-Notification 메시지를 송신한다. 단계 273에서는, 액세스 포인트(242)가 단계 272의 응답을 UE D/GSCL(241)에 송신한다. 단계 275에서는, UE D/GSCL(241)이 EAP-Response/AKA'-Notification 메시지를 송신하는데, 이는 단계 274에서 AAA 서버(243)에 전달된다. 단계 276에서는, AAA 서버(243)가 EAP-Success 메시지를 송신하는데, 이는 단계 277에서 UE D/GSCL(241)에 전달된다. 단계 278에서는, UE D/GSCL(241)가 등록되지만, M2M 서버는 UE D/GSCL(241)의 IP 어드레스를 알지 못할 수 있다. UE D/GSCL(241)가 mId를 통해 통신을 시작할 수 있거나 또는 M2M 서버(246)가 디바이스 트리거를 송신하는 것에 의해 통신을 시작할 수 있다.

[0070] 액세스 네트워크가 부트스트랩핑을 돕기 때문에, 이러한 특징을 사용하는 것이 허용되는 디바이스들의 가입 정보에 추가 정보가 보유될 수 있다. 서비스 레이어 부트스트랩핑의 승인을 지원하기 위해 새로운 액세스 네트워크 가입 정보가 HSS에 추가된다.

[0071] 도 8a는 하나 이상의 개시되는 실시예들이 구현될 수 있는 예시적인 M2M(Machine-to machine) 또는 IoT(Internet of Things), 또는 WoT(Web of Things) 통신 시스템(10)의 도면이다. 일반적으로, M2M 기술들은 IoT/WoT에 대한 빌딩 블록들을 제공하고, 임의의 M2M 디바이스, 게이트웨이, 또는 서비스 플랫폼은 IoT/WoT 뿐만 아니라 IoT/WoT 서비스 레이어 등의 컴포넌트일 수 있다.

[0072] 도 8a에 도시된 바와 같이, M2M/IoT/WoT 통신 시스템(10)은 통신 네트워크(12)를 포함한다. 통신 네트워크(12)는 고정 네트워크(예를 들어, Ethernet, Fiber, ISDN, PLC 등) 또는 무선 네트워크(예를 들어, WLAN, 셀룰러 등) 또는 이종 네트워크들의 네트워크일 수 있다. 예를 들어, 통신 네트워크(12)는, 음성, 데이터, 비디오, 메시징, 방송 등과 같은 콘텐츠를 다수의 사용자들에게 제공하는 다수의 액세스 네트워크들로 구성될 수 있다. 예를 들어, 통신 네트워크(12)는, CDMA(Code Division Multiple Access), TDMA(Time Division Multiple Access), FDMA(Frequency Division Multiple Access), OFDMA(Orthogonal FDMA), SC-FDMA(Single-Carrier FDMA) 등과 같은 하나 이상의 채널 액세스 방법들을 채택할 수 있다. 또한, 통신 네트워크(12)는, 예를 들어, 코어 네트워크, 인터넷, 센서 네트워크, 산업적 제어 네트워크, 개인 영역 네트워크, 융합된 개인 네트워크, 위성 네트워크, 홈 네트워크, 또는 기업 네트워크와 같은 다른 네트워크들을 포함할 수 있다.

[0073] 도 8a에 도시된 바와 같이, M2M/IoT/WoT 통신 시스템(10)은 Infrastructure Domain 및 Field Domain을 포함할 수 있다. Infrastructure Domain은 엔드-투-엔드(end-to-end) M2M 배치의 네트워크 사이드를 말하며, Field Domain은 일반적으로 M2M 게이트웨이 뒤에 있는 영역 네트워크들을 말한다. Field Domain은 M2M 게이트웨이들(14) 및 단말 디바이스들(18)을 포함할 수 있다. 임의의 수의 M2M 게이트웨이 디바이스들(14) 및 M2M 단말 디바이스들(18)이 원하는 바에 따라 M2M/IoT/WoT 통신 시스템(10)에 포함될 수 있다는 점이 이해될 것이다. M2M 게이트웨이 디바이스들(14) 및 M2M 단말 디바이스들(18) 각각은 통신 네트워크(12) 또는 직접 무선 링크를 통해 신호들을 송신 및 수신하도록 구성된다. M2M 게이트웨이 디바이스(14)는 고정 네트워크 M2M 디바이스들(예를 들어, PLC) 뿐만 아니라 무선 M2M 디바이스들(예를 들어, 셀룰러 및 논-셀룰러)이, 통신 네트워크(12) 또는 직접 무선 링크와 같은, 오퍼레이터 네트워크들을 통해, 통신하게 한다. 예를 들어, M2M 디바이스들(18)은, 통신 네트워크(12) 또는 직접 무선 링크를 통해, 데이터를 수집할 수 있고, M2M 애플리케이션(20) 또는 M2M 디바이스들(18)에 송신할 수 있다. M2M 디바이스들(18)은 또한 M2M 애플리케이션(20) 또는 M2M 디바이스(18)로부터 데이터를 수신할 수 있다. 또한, 데이터 및 신호들은, 이하 설명되는 바와 같이, M2M 서비스 레이어(22)를 통해 M2M 애플리케이션(20)에 송신될 수 있고 이로부터 수신될 수 있다. M2M 디바이스들(18) 및

게이트웨이들(14)은, 예를 들어, 셀룰러, WLAN, WPAN(예를 들어, 지그비(Zigbee), 6LoWPAN, 블루투스(Bluetooth)), 직접 무선 링크, 및 유선을 포함하는 다양한 네트워크들을 통해 통신할 수 있다.

[0074] 도 8b를 참조하면, 필드 도메인에 도시되는 M2M 서비스 레이어(22)(예를 들어, 본 명세서에 설명되는 바와 같은 NSCL(Network Service Capability Layer))는, M2M 애플리케이션(20), M2M 게이트웨이 디바이스들(14), 및 M2M 단말 디바이스들(18) 및 통신 네트워크(12)에 대한 서비스들을 제공한다. M2M 서비스 레이어(22)는 원하는 바에 따라 임의의 수의 M2M 애플리케이션들, M2M 게이트웨이 디바이스들(14), M2M 단말 디바이스들(18), 및 통신 네트워크들(12)과 통신할 수 있다는 점이 이해될 것이다. M2M 서비스 레이어(22)는, 하나 이상의 서버들, 컴퓨터들 등에 의해 구현될 수 있다. M2M 서비스 레이어(22)는 M2M 단말 디바이스들(18), M2M 게이트웨이 디바이스들(14) 및 M2M 애플리케이션들(20)에 적용되는 서비스 능력들을 제공한다. M2M 서비스 레이어(22)의 기능들은, 예를 들어, 웹 서버로서, 셀룰러 코어 네트워크에서, 클라우드에서 등 다양한 방식들로 구현될 수 있다.

[0075] 도시된 M2M 서비스 레이어(22)와 유사하게, 인프라구조 도메인에 M2M 서비스 레이어(22')가 존재한다. M2M 서비스 레이어(22')는 인프라구조 도메인에서의 M2M 애플리케이션(20') 및 하위 통신 네트워크(12')에 대한 서비스들을 제공한다. M2M 서비스 레이어(22')는 필드 도메인에서의 M2M 게이트웨이 디바이스들(14) 및 M2M 단말 디바이스들(18)에 대한 서비스들을 또한 제공한다. M2M 서비스 레이어(22')는 임의의 수의 M2M 애플리케이션들, M2M 게이트웨이 디바이스들 및 M2M 단말 디바이스들과 통신할 수 있다는 점이 이해될 것이다. M2M 서비스 레이어(22')는 상이한 서비스 프로바이더에 의한 서비스 레이어와 상호작용할 수 있다. M2M 서비스 레이어(22')는 하나 이상의 서버들, 컴퓨터들, 가상 머신들(예를 들어, 클라우드/컴퓨트/스토리지 팜들 등) 등에 의해 구현될 수 있다.

[0076] 또한, 도 8b를 참조하면, M2M 서비스 레이어(22 및 22')는, 다양한 애플리케이션들 및 버티컬들(verticals)이 영향을 줄 수 있는 서비스 전달 능력들의 코어 세트를 제공한다. 이러한 서비스 능력들은, M2M 애플리케이션들(20 및 20')이, 디바이스들과 상호작용하여, 데이터 수집, 데이터 분석, 디바이스 관리, 보안, 빌링(billing), 서비스/디바이스 발견 등과 같은 기능들을 수행할 수 있게 한다. 본질적으로, 이러한 서비스 능력들은 이러한 기능들을 구현하는 부담에서 애플리케이션들을 자유롭게 하며, 따라서 애플리케이션 개발을 단순하게 하며, 시장에 대한 비용 및 시간을 줄여준다. 서비스 레이어(22 및 22')는, 또한, M2M 애플리케이션들(20 및 20')이, 서비스 레이어(22 및 22')가 제공하는 서비스들과 관련하여 다양한 네트워크들(12 및 12')을 통해 통신할 수 있게 한다.

[0077] 일부 실시예들에서, M2M 애플리케이션들(20 및 20')은 본 명세서에 논의되는 바와 같이 EAP를 사용하여 통신하는 원하는 애플리케이션들을 포함할 수 있다. M2M 애플리케이션들(20 및 20')은, 이에 제한되는 것은 아니지만, 수송, 건강 및 건강관리, 접속된 가정, 에너지 관리, 자산 추적, 및 보안 및 감시와 같은, 다양한 산업들에서의 애플리케이션들을 포함할 수 있다. 위에 언급된 바와 같이, 시스템의 디바이스들, 게이트웨이들, 및 다른 서버들에 걸쳐 실행되는, M2M 서비스 레이어는, 예를 들어, 데이터 수집, 디바이스 관리, 보안, 빌링(billing), 위치 추적/지오펜싱(geofencing), 디바이스/서비스 발견, 및 레거시 시스템들 통합과 같은 기능들을 지원하고, 이러한 기능들을 서비스들로서 M2M 애플리케이션들(20 및 20')에 제공한다.

[0078] 본 출원에 사용되는 EAP 관련된 접근방식들(예를 들어, EAP-PANA 또는 EAP 액세스 네트워크 기반의 접근방식)은 서비스 레이어의 부분으로서 구현될 수 있다. 이러한 서비스 레이어(예를 들어, UE D/GSCL(191))는 API들(Application Programming Interfaces) 및 하위 네트워킹 인터페이스들의 세트를 통해 부가 가치의 서비스 능력들을 지원하는 소프트웨어 미들웨어 레이어이다. M2M 엔티티(예를 들어, 하드웨어 및 소프트웨어의 조합에 의해 구현될 수 있는 디바이스, 게이트웨이, 또는 서비스/플랫폼과 같은 M2M 기능성 엔티티)는 애플리케이션 또는 서비스를 제공할 수 있다. ETSI M2M 및 oneM2M 양자 모두 본 발명의 EAP 관련된 접근방식들을 포함할 수 있는 서비스 레이어를 사용한다. ETSI M2M의 서비스 레이어는 SCL(Service Capability Layer)라 한다. 이러한 SCL은, M2M 디바이스(DSCL(Device SCL)이라 함), 게이트웨이(GSCL(Gateway SCL)이라 함) 및/또는 네트워크 노드(NSCL(Network SCL)이라 함) 내에 구현될 수 있다. oneM2M 서비스 레이어는 CSF들(Common Service Functions)(즉, 서비스 능력들)의 세트를 지원한다. 하나 이상의 특정 타입들의 CSF들의 세트의 예시화는 상이한 타입들의 네트워크 노드들(예를 들어, 인프라구조 노드, 중간 노드, 애플리케이션 특정 노드) 상에서 관리될 수 있는 CSE(Common Services Entity)라 한다. 또한, 본 출원의 EAP 관련된 접근방식들은 본 출원의 EAP 관련된 접근방식들과 같은 서비스들을 액세스하는데 SOA(Service Oriented Architecture) 및/또는 ROA(Resource-Oriented Architecture)를 사용하는 M2M 네트워크의 부분으로서 구현될 수 있다.

[0079] 도 8c는, 예를 들어, M2M 단말 디바이스(18) 또는 M2M 게이트웨이 디바이스(14)와 같은, 예시적인 M2M 디바이스

(30)의 시스템 도면이다. 도 8c에 도시된 바와 같이, M2M 디바이스(30)는, 프로세서(32), 송수신기(34), 송신/수신 엘리먼트(36), 스피커/마이크로폰(38), 키패드(40), 디스플레이/터치패드(42), 비-분리형 메모리(44), 분리형 메모리(46), 전원(48), GPS(Global Positioning System) 칩셋(50), 및 다른 주변기기들(52)을 포함할 수 있다. M2M 디바이스(30)는 실시예에 부합하면서 전술한 엘리먼트들의 임의의 서브-조합을 포함할 수 있다는 점이 이해될 것이다. 이러한 디바이스는 EAP-PANA를 사용하여 부트스트랩핑하기 위해 개시된 시스템들 및 방법들을 사용하는 디바이스일 수 있다.

[0080] 프로세서(32)는, 범용 프로세서, 특수 목적 프로세서, 종래의 프로세서, DSP(Digital Signal Processor), 복수의 마이크로프로세서들, DSP 코어와 관련된 하나 이상의 마이크로프로세서들, 컨트롤러, 마이크로컨트롤러, ASIC들(Application Specific Integrated Circuits), FPGA(Field Programmable Gate Array) 회로들, 임의의 다른 타입의 IC(Integrated Circuit), 상태 머신 등일 수 있다. 프로세서(32)는, 신호 코딩, 데이터 처리, 전력 제어, 입력/출력 처리, 및/또는 M2M 디바이스(30)가 무선 환경에서 동작할 수 있게 하는 임의의 다른 기능을 수행할 수 있다. 프로세서(32)는 송신/수신 엘리먼트(36)에 연결될 수 있는 송수신기(34)에 연결될 수 있다. 도 8c는 프로세서(32)와 송수신기(34)를 별도의 컴포넌트들로서 묘사하지만, 프로세서(32)와 송수신기(34)는 전자 패키지 또는 칩 내에 함께 통합될 수 있다는 점이 이해될 것이다. 프로세서(32)는 애플리케이션-레이어 프로그램들(예를 들어, 브라우저들) 및/또는 RAN(Radio Access-Layer) 프로그램들 및/또는 통신을 수행할 수 있다. 프로세서(32)는, 예를 들어, 액세스 레이어 및/또는 애플리케이션 레이어에서와 같은, 인증, 보안 키 승낙, 및/또는 암호화 동작들과 같은, 보안 동작들을 수행할 수 있다.

[0081] 송신/수신 엘리먼트(36)는 M2M 서비스 플랫폼(22)에 신호들을 송신하도록, 또는 이로부터의 신호들을 수신하도록 구성될 수 있다. 예를 들어, 일 실시예에서, 송신/수신 엘리먼트(36)는 RF 신호들을 송신 및/또는 수신하도록 구성되는 안테나일 수 있다. 송신/수신 엘리먼트(36)는, WLAN, WPAN, 셀룰러 등과 같은, 다양한 네트워크들 및 에어 인터페이스들을 지원할 수 있다. 일 실시예에서, 송신/수신 엘리먼트(36)는, 예를 들어, IR, UV, 또는 가시광 신호들을 송신 및/또는 수신하도록 구성되는 이미터/검출기일 수 있다. 또 다른 실시예에서, 송신/수신 엘리먼트(36)는 RF 및 광 신호들 양자 모두를 송신 및 수신하도록 구성될 수 있다. 송신/수신 엘리먼트(36)는 무선 또는 유선 신호들의 임의의 조합을 송신 및/또는 수신하도록 구성될 수 있다는 점이 이해될 것이다.

[0082] 또한, 송신/수신 엘리먼트(36)가 단일 엘리먼트로서 도 8c에 묘사되지만, M2M 디바이스(30)는 임의의 수의 송신/수신 엘리먼트들(36)을 포함할 수 있다. 보다 구체적으로, M2M 디바이스(30)는 MIMO 기술을 채택할 수 있다. 따라서, 일 실시예에서, M2M 디바이스(30)는 무선 신호들을 송신 및 수신하기 위한 2개 이상의 송신/수신 엘리먼트들(36)(예를 들어, 다수의 안테나들)을 포함할 수 있다.

[0083] 송수신기(34)는, 송신/수신 엘리먼트(36)에 의해 송신될 신호들을 변조하도록, 및 송신/수신 엘리먼트(36)에 의해 수신되는 신호들을 복조하도록 구성될 수 있다. 위에 언급된 바와 같이, M2M 디바이스(30)는 다수 모드의 능력들을 가질 수 있다. 따라서, 송수신기(34)는, M2M 디바이스(30)가, 예를 들어, UTRA 및 IEEE 802.11과 같은, 다수의 RAT들을 통해 통신할 수 있게 하는 다수의 송수신기들을 포함할 수 있다.

[0084] 프로세서(32)는, 비-분리형 메모리(44) 및/또는 분리형 메모리(46)와 같은, 임의의 타입의 적절한 메모리로부터 정보를 액세스할 수 있고, 거기에 데이터를 저장할 수 있다. 비-분리형 메모리(44)는, RAM(Random-Access Memory), ROM(Read-Only Memory), 하드 디스크, 또는 다른 타입의 메모리 스토리지 디바이스를 포함할 수 있다. 분리형 메모리(46)는, SIM(Subscriber Identity Module) 카드, 메모리 스틱, SD(Secure Digital) 메모리 카드 등을 포함할 수 있다. 다른 실시예들에서, 프로세서(32)는, 서버 또는 가정용 컴퓨터와 같은, M2M 디바이스(30) 상에 물리적으로 위치되지 않는 메모리로부터 정보를 액세스할 수 있고, 거기에 데이터를 저장할 수 있다. 프로세서(32)는, 본 명세서에서 설명되는 실시예들의 일부에서의 부트스트랩핑(예를 들어, EAP를 사용하는 부트스트랩핑)이 성공적인지 또는 성공적이지 못한지, 또는 리소스 전파 프로세스들의 상태를 다른 방식으로 나타내는지에 응답하여, 디스플레이 또는 인디케이터들(42) 상의 점등 패턴들, 이미지들, 또는 컬러들을 제어하도록 구성될 수 있다. 디스플레이(42)를 통해 보여지는 사용자 인터페이스는 인증을 위해 EAP-PANA, EAP 액세스 네트워크 기반의 접근방식, GBA 등을 사용하는 옵션을 사용자에게 제공할 수 있다.

[0085] 프로세서(32)는, 전원(48)으로부터 전력을 수신할 수 있고, M2M 디바이스(30) 내의 다른 컴포넌트들에 전력을 분배 및/또는 제어하도록 구성될 수 있다. 전원(48)은 M2M 디바이스(30)에 전력을 공급하에 적절한 임의의 디바이스일 수 있다. 예를 들어, 전원(48)은, 하나 이상의 드라이 셀 배터리들(예를 들어, 니켈-카드뮴(NiCd), 니켈-아연(NiZn), 니켈 금속 수소화물(NiMH), 리튬-이온(Li-이온) 등), 태양광 전지들, 연료 전지들 등을 포함할 수 있다.

[0086] 프로세서(32)는, 또한, M2M 디바이스(30)의 현재 위치에 관한 위치 정보(예를 들어, 경도와 위도)를 제공하도록 구성되는, GPS 칩셋(50)에 연결될 수 있다. M2M 디바이스(30)는, 일 실시예에 부합하면서, 임의의 적절한 위치-결정 방법에 의해 위치 정보를 취득할 수 있다는 점이 이해될 것이다.

[0087] 프로세서(32)는 다른 주변기기들(52)에 더 연결될 수 있는데, 이러한 주변기기들은, 추가적 특징들, 기능, 및/또는 유선 또는 무선 접속을 제공하는 하나 이상의 소프트웨어 및/또는 하드웨어 모듈들을 포함할 수 있다. 예를 들어, 주변기기들(52)은, 가속도계, e-컴파스, 위성 송수신기, 센서, (사진들 또는 비디오를 위한) 디지털 카메라, USB(Universal Serial Bus) 포트, 진동 디바이스, 텔레비전 송수신기, 핸즈 프리 헤드셋, Bluetooth® 모듈, FM(Frequency Modulated) 무선 유닛, 디지털 음악 플레이어, 미디어 플레이어, 비디오 게임 플레이어 모듈, 인터넷 브라우저 등을 포함할 수 있다.

[0088] 도 8d는, 예를 들어, 도 8a 및 도 8b의 M2M 서비스 플랫폼(22)이 구현될 수 있는 예시적인 컴퓨팅 시스템(90)의 블록도이다. 컴퓨팅 시스템(90)은, 컴퓨터 또는 서버를 포함할 수 있고, 주로 컴퓨터 판독가능 명령어들에 의해 제어될 수 있는데, 이러한 컴퓨터 판독가능 명령어들은, 소프트웨어의 형태일 수 있거나, 이러한 소프트웨어가 저장되거나 액세스되는, 어디서든지, 또는 어느 것에 의해 있을 수 있다. 이러한 컴퓨터 판독가능 명령어들은, 컴퓨팅 시스템(90)으로 하여금 작업하게 하도록 CPU(Central Processing Unit)(91) 내에서 실행될 수 있다. 많은 알려진 워크스테이션들, 서버들, 및 퍼스널 컴퓨터들에서, 중앙 처리 유닛(91)은 마이크로프로세서라 불리우는 단일 칩 CPU에 의해 구현된다. 다른 머신들에서, 중앙 처리 유닛(91)은 다수의 프로세서들을 포함할 수 있다. 코프로세서(81)는, 메인 CPU(91)와는 구별되며, 추가적 기능들을 수행하거나 또는 CPU(91)를 도와주는 옵션의 프로세서이다. CPU(91) 및/또는 코프로세서(81)는, 디바이스 인증 메시지들을 교환하는 것과 같은, EAP를 위해 개시된 시스템 및 방법들에 관련된 데이터를, 수신하고, 생성하고, 처리할 수 있다.

[0089] 동작시에, CPU(91)는, 명령어들을, 페치, 디코딩, 및 실행하고, 컴퓨터의 메인 데이터 전송 경로, 시스템 버스(80)를 통해 다른 리소스들에 및 이들로부터 정보를 전송한다. 이러한 시스템 버스는, 컴퓨팅 시스템(90) 내의 컴포넌트들을 접속시키고, 데이터 교환을 위한 매체를 정의한다. 시스템 버스(80)는, 데이터를 보내기 위한 데이터 라인들, 어드레스들을 보내기 위한 어드레스 라인들, 인터럽트들을 보내고 시스템 버스를 동작시키기 위한 제어 라인들을 통상적으로 포함한다. 이러한 시스템 버스(80)의 일 예는 PCI(Peripheral Component Interconnect) 버스이다.

[0090] 시스템 버스(80)에 연결되는 메모리 디바이스들은 RAM(Random Access Memory)(82) 및 ROM(Read Only Memory)(93)을 포함한다. 이러한 메모리들은 정보가 저장 및 검색되게 하는 회로를 포함한다. ROM들(93)은 쉽게 수정될 수 없는 저장된 데이터를 일반적으로 포함한다. RAM(82)에 저장되는 데이터는 CPU(91) 또는 다른 하드웨어 디바이스들에 의해 판독 또는 변경될 수 있다. RAM(82) 및/또는 ROM(93)에 대한 액세스는 메모리 제어기(92)에 의해 제어될 수 있다. 메모리 제어기(92)는 명령어들이 실행될 때 가상 어드레스들을 물리적 어드레스들로 변환하는 어드레스 변환 기능을 제공할 수 있다. 메모리 제어기(92)는, 또한, 시스템 내의 프로세스들을 격리시키고, 시스템 프로세스들을 사용자 프로세스들로부터 격리시키는 메모리 보호 기능을 제공할 수 있다. 따라서, 제1 모드에서 실행하는 프로그램은 자기 자신의 프로세스 가상 어드레스 공간에 의해 맵핑되는 메모리만을 액세스할 수 있다; 프로세스들 사이에 공유하는 메모리가 셋업되지 않으면 다른 프로세스의 가상 어드레스 공간 내의 메모리를 액세스할 수 없다.

[0091] 또한, 컴퓨팅 시스템(90)은, 프린터(94), 키보드(84), 마우스(95), 및 디스크 드라이브(85)와 같은, 주변기기들에 CPU(91)로부터의 명령어들을 통신하는 것을 담당하는 주변기기 제어기(83)를 포함할 수 있다.

[0092] 디스플레이 제어기(96)에 의해 제어되는 디스플레이(86)는, 컴퓨팅 시스템(90)에 의해 생성되는 가시적 출력을 디스플레이하는데 사용된다. 이러한 가시적 출력은, 텍스트, 그래픽, 애니메이션 그래픽, 및 비디오를 포함할 수 있다. 디스플레이(86)는, CRT 기반의 비디오 디스플레이, LCD 기반의 평면 패널 디스플레이, 가스 플라즈마 기반의 평면 패널 디스플레이, 또는 터치 패널로 구현될 수 있다. 디스플레이 제어기(96)는 디스플레이(86)에 보내어지는 비디오 신호를 생성하는데 요구되는 전자 컴포넌트들을 포함한다.

[0093] 또한, 컴퓨팅 시스템(90)은, 도 8a 및 도 8b의 네트워크(12)와 같은, 외부 통신 네트워크에 컴퓨팅 시스템(90)을 접속하는 데 사용될 수 있는 네트워크 어댑터(97)를 포함할 수 있다.

[0094] 본 명세서에 설명되는 시스템들, 방법들, 및 처리들 중 임의의 것 또는 모두는, 컴퓨터 판독가능 스토리지 매체상에 저장되는 컴퓨터 실행가능 명령어들(즉 프로그램 코드)의 형태로 구현될 수 있고, 이러한 명령어들은, 컴퓨터, 서버, M2M 단말 디바이스, M2M 게이트웨이 디바이스 등과 같은, 머신에 의해 실행될 때, 본 명세서에 설

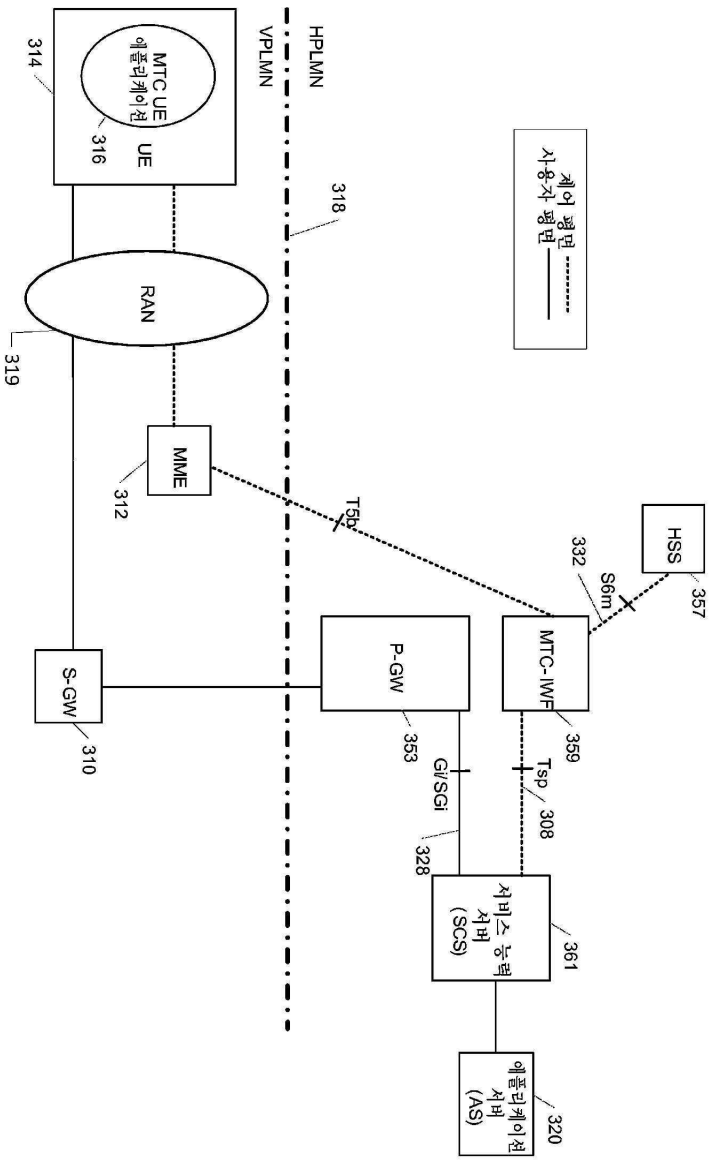
명되는 시스템들, 방법들, 및 프로세스들을 수행 및/또는 구현한다는 점이 이해된다. 특히, 위에 설명된 단계들, 동작들, 또는 기능들 중 임의의 것이 이러한 컴퓨터 실행가능 명령어들의 형태로 구현될 수 있다. 컴퓨터 판독가능 스토리지 매체는, 정보의 저장을 위해 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성, 분리형 및 비-분리형 매체 양자 모두를 포함하지만, 이러한 컴퓨터 판독가능 스토리지 매체가 신호들을 포함하는 것은 아니다. 컴퓨터 판독가능 스토리지 매체는, RAM, ROM, EEPROM, 플래시 메모리, 또는 다른 메모리 기술, CD-ROM, DVD(Digital Versatile Disk) 또는 다른 광 디스크 스토리지, 자기 카세트들, 자기 테이프, 자기 디스크 스토리지 또는 다른 자기 스토리지 디바이스들, 또는 원하는 정보를 저장하는데 사용될 수 있고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 물리적 매체를 포함하지만, 이에 제한되는 것은 아니다.

[0095] 본 개시내용의 대상의 바람직한 실시예들을 설명함에 있어서, 도면들에 도시된 바와 같이, 명료성을 위해 특정 용어가 채택된다. 그러나, 청구되는 대상은, 그렇게 선택된 특정 용어에 제한되는 것으로 의도된 것은 아니며, 각각의 특정 엘리먼트는 유사한 목적을 달성하기 위해 유사한 방식으로 동작하는 모든 기술적 균등물을 포함한다는 점이 이해되어야 한다.

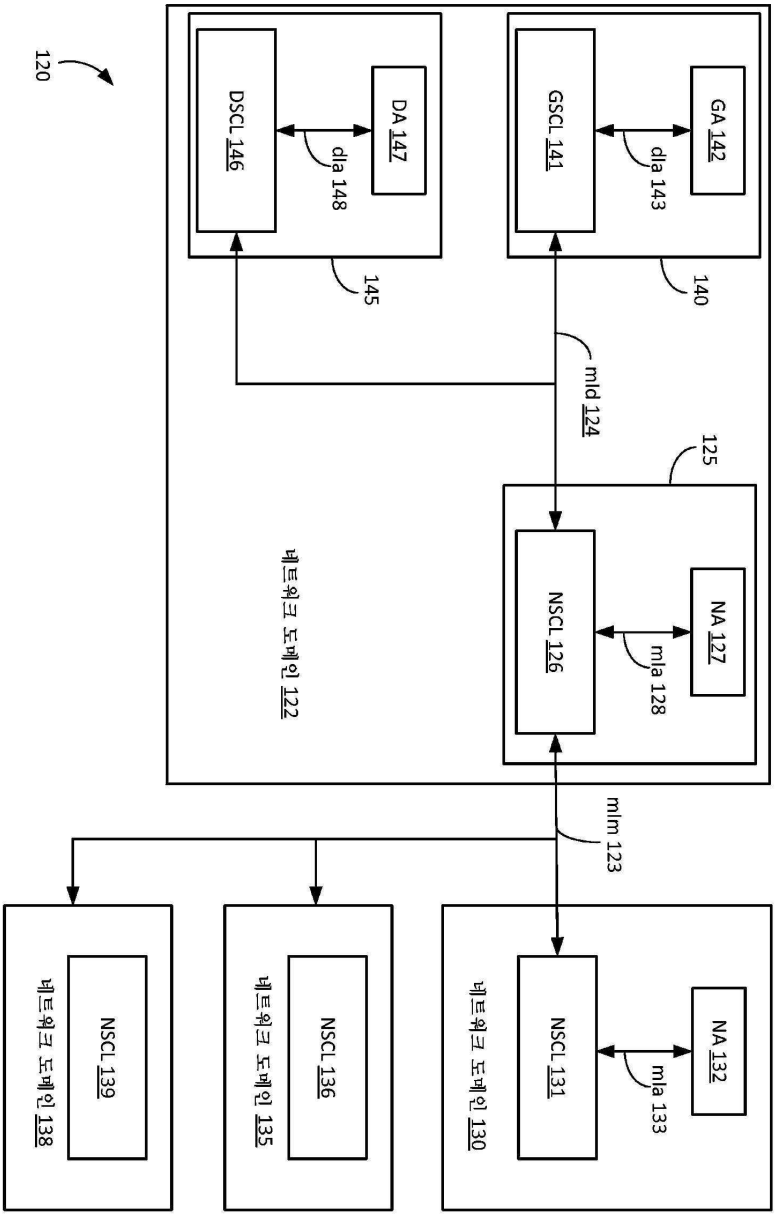
[0096] 본 작성된 설명은, 최상의 모드를 포함하여, 본 발명을 개시하는, 또한 통상의 기술자가, 임의의 디바이스들 또는 시스템들을 제조하고 사용하여, 임의의 포함되는 방법들을 수행하는 것을 포함하여, 본 발명을 실시할 수 있게 하는, 예들을 사용한다. 본 발명의 특허가능한 범위는, 청구항들에 의해 정의되며, 통상의 기술자에게 떠오르는 다른 예들을 포함할 수 있다. 이러한 다른 예들은, 그들이 청구항들의 기재와 다르지 않은 구조적 엘리먼트들을 가지는 경우에 또는 그들이 청구항들의 기재와의 미미한 차이를 갖는 등가의 구조적 엘리먼트들을 포함하는 경우에, 청구항들의 범위 내에 있는 것으로 의도된다.

도면

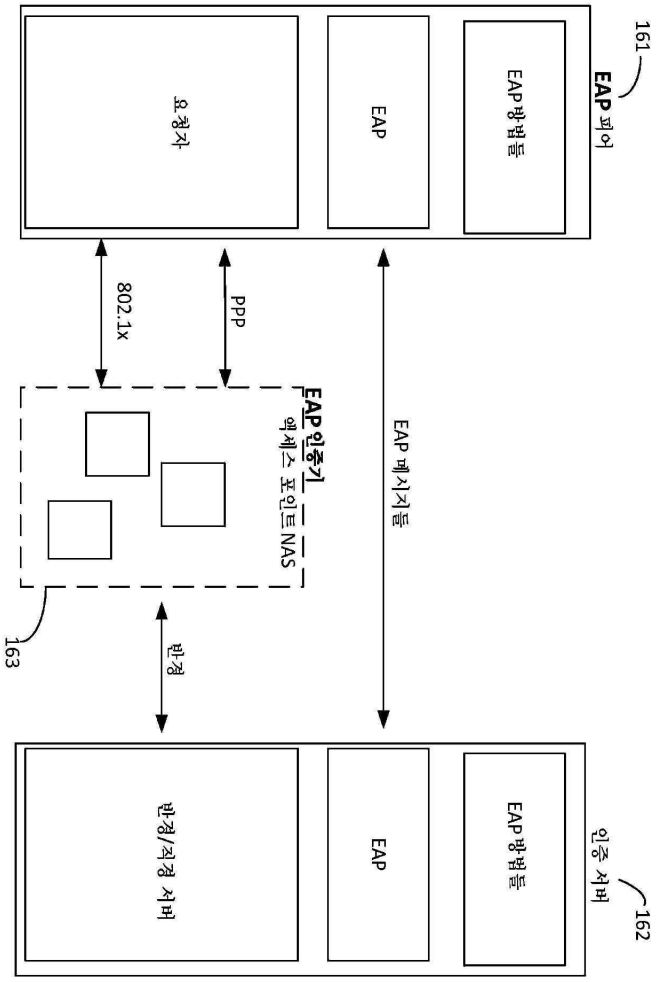
도면1


제어 평면
사용자 평면
HPLMN
VPLMN
318
314
MTC UE
애플리케이션
316
UE
RAN
319
MME
312
T5b
HSS
332
S6m
357
S-GW
310
P-GW
353
MTC-IWF
359
Gi/SGi
328
Tsp
308
서비스 능력
서버
(SCS)
361
애플리케이션
서버
(AS)
320

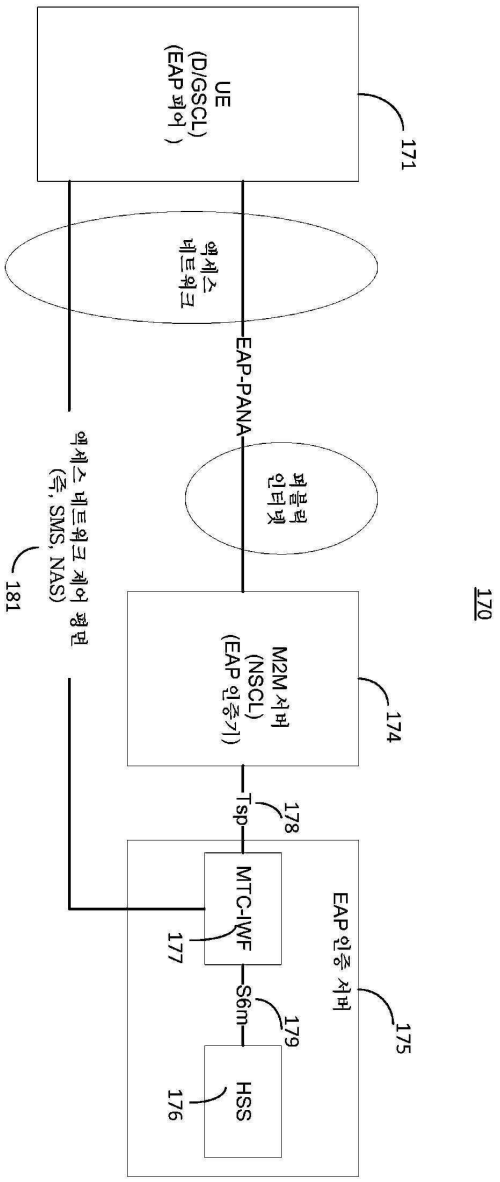
도면2


120
네트워크 도메인 122
GSCL 141
GA 142
dla 143
140
DSCL 146
DA 147
dla 148
145
mld 124
125
NSCL 126
NA 127
mla 128
mlm 123
네트워크 도메인 130
NSCL 131
NA 132
mla 133
네트워크 도메인 135
NSCL 136
네트워크 도메인 138
NSCL 139

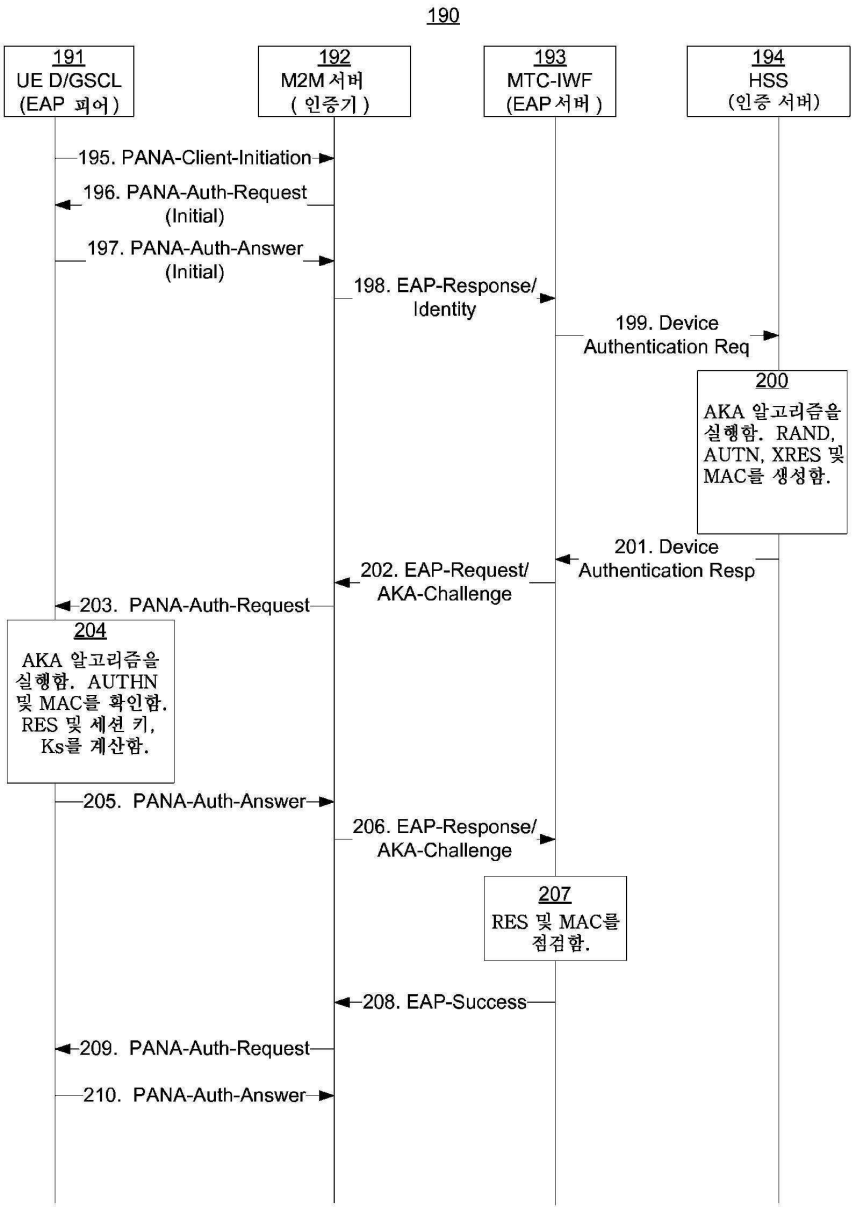
도면3


161
EAP 피어
요청자
EAP
EAP방법들
802.1x
PPP
EAP 메시지들
EAP 인증기
액세스 포인트 NAS
163
반경
반경/적경 서버
EAP
EAP방법들
인증 서버
162

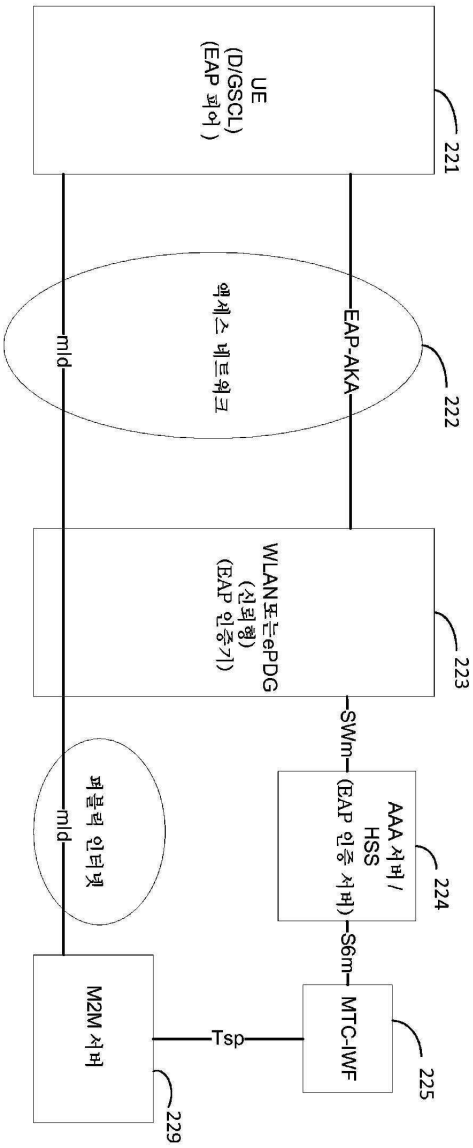
도면4


UE
(D/GSCL)
(EAP 피어)
171
액세스
네트워크
EAP-PANA
퍼블릭
인터넷
액세스 네트워크 제어 평면
(즉, SMS, NAS)
181
M2M 서버
(NSCL)
(EAP 인증기)
174
Tsp
178
EAP 인증 서버
175
MTC-IWF
177
S6m
179
HSS
176
170

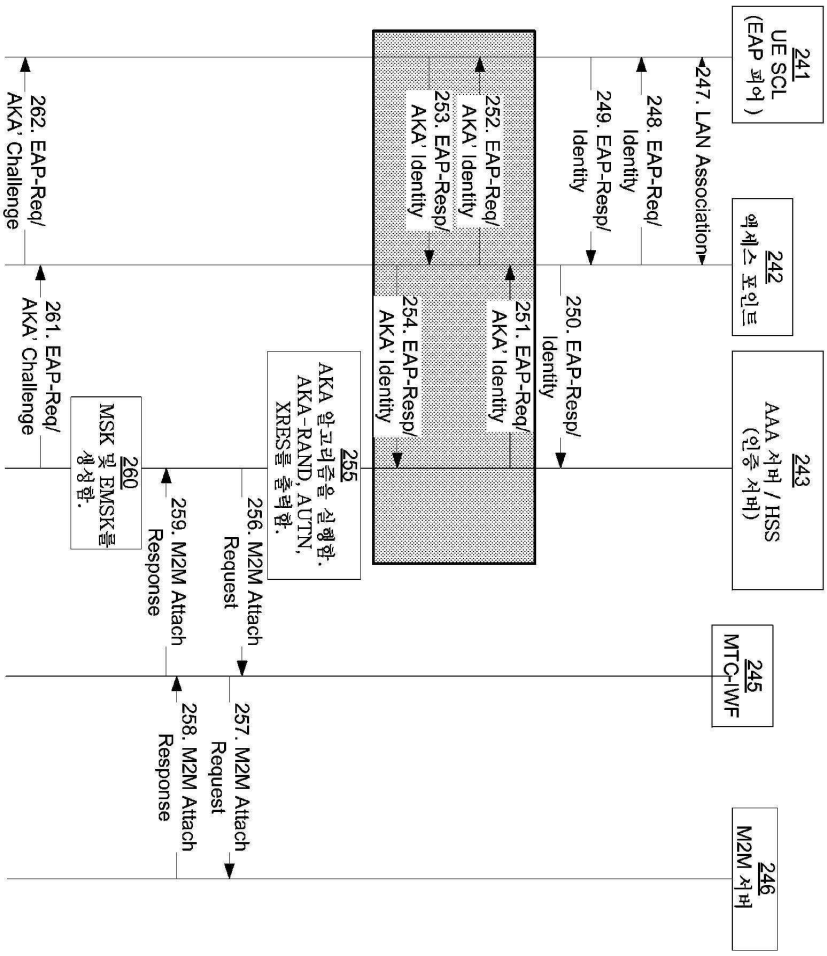
도면5


190
191
UE D/GSCL
(EAP 피어)
192
M2M 서버
(인증기)
193
MTC-IWF
(EAP 서버)
194
HSS
(인증 서버)
195. PANA-Client-Initiation
196. PANA-Auth-Request
(Initial)
197. PANA-Auth-Answer
(Initial)
198. EAP-Response/
Identity
199. Device
Authentication Req
200
AKA 알고리즘을 실행함. RAND, AUTN, XRES 및 MAC를 생성함.
201. Device
Authentication Resp
202. EAP-Request/
AKA-Challenge
203. PANA-Auth-Request
204
AKA 알고리즘을 실행함. AUTHN 및 MAC를 확인함. RES 및 세션 키, Ks를 계산함.
205. PANA-Auth-Answer
206. EAP-Response/
AKA-Challenge
207
RES 및 MAC를 점검함.
208. EAP-Success
209. PANA-Auth-Request
210. PANA-Auth-Answer

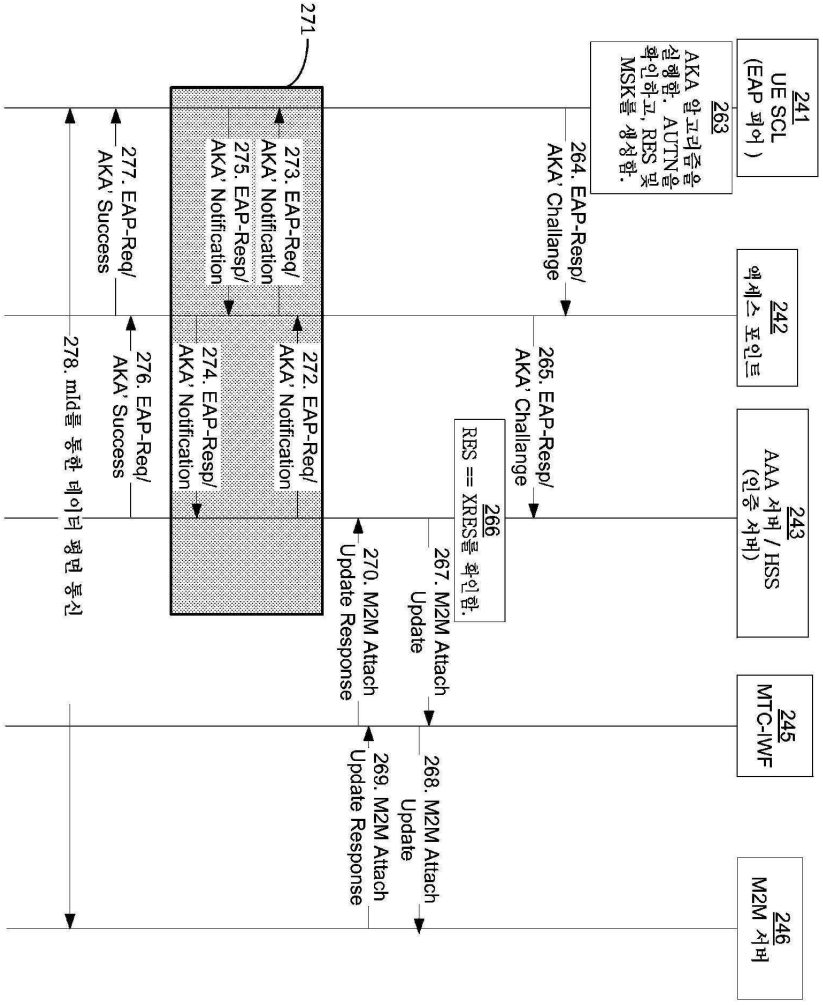
도면6


UE
(D/GSCL)
(EAP 피어)
221
액세스 네트워크
222
EAP-AKA
mId
WLAN또는ePDG
(신뢰형)
(EAP 인증기)
223
SWm
AAA 서버 /
HSS
(EAP 인증 서버)
224
S6m
MTC-IWF
225
Tsp
M2M 서버
229
mId
퍼블릭 인터넷

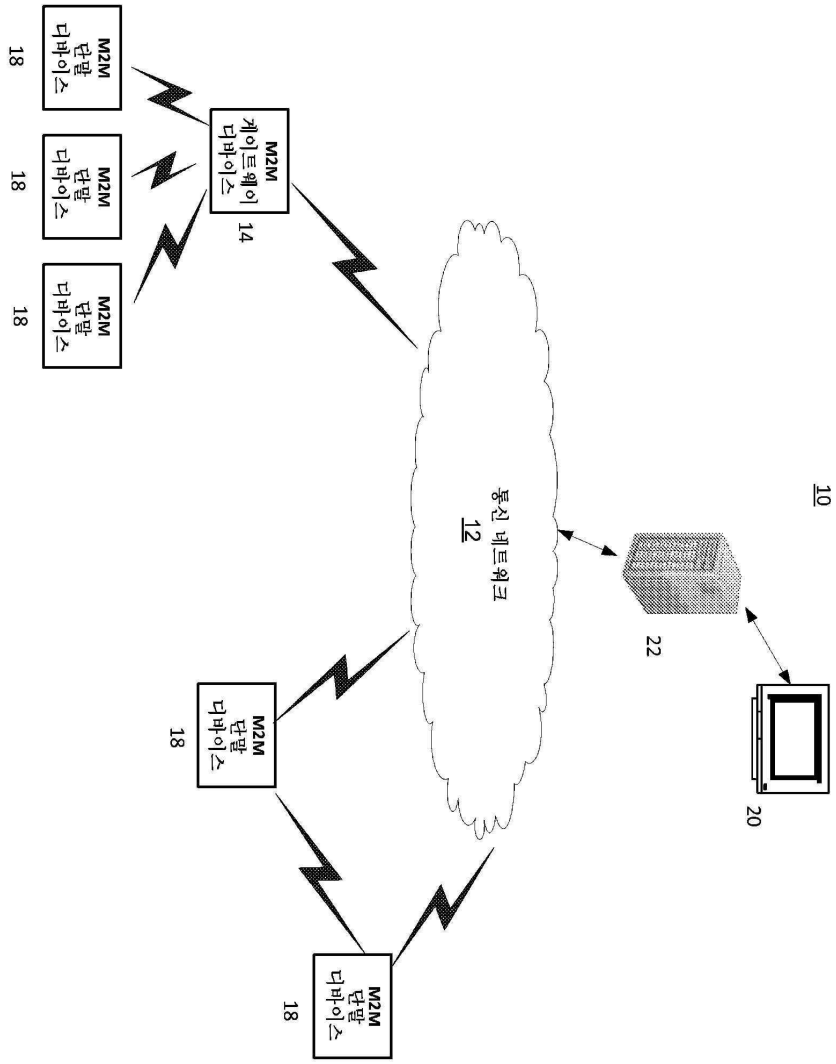
도면7a


241
UE SCL
(EAP 피어)
242
액세스 포인트
243
AAA 서버 / HSS
(인증 서버)
245
MTC-IWF
246
M2M 서버
247. LAN Association
248. EAP-Req/
Identity
249. EAP-Resp/
Identity
250. EAP-Resp/
Identity
251. EAP-Req/
AKA' Identity
252. EAP-Req/
AKA' Identity
253. EAP-Resp/
AKA' Identity
254. EAP-Resp/
AKA' Identity
255
AKA 알고리즘을 실행함.
AKA-RAND, AUTN,
XRES를 출력함.
256. M2M Attach
Request
257. M2M Attach
Request
258. M2M Attach
Response
259. M2M Attach
Response
260
MSK 및 EMSK를
생성함.
261. EAP-Req/
AKA' Challenge
262. EAP-Req/
AKA' Challenge

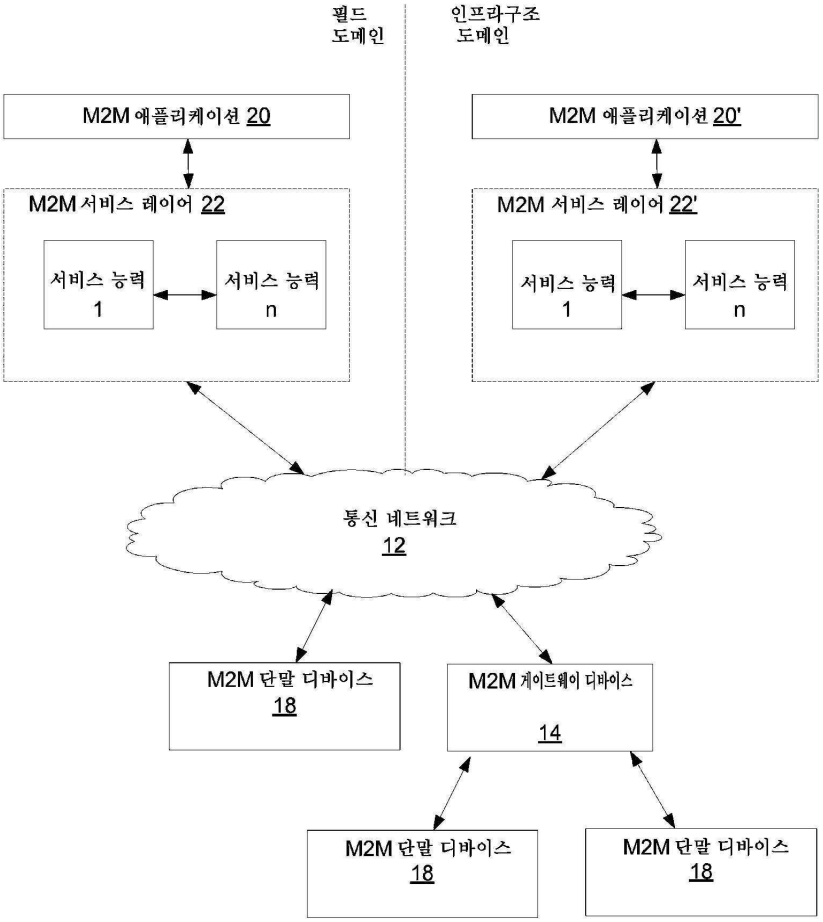
도면7b


241
UE SCL
(EAP 피어)
242
액세스 포인트
243
AAA 서버 / HSS
(인증 서버)
245
MTC-IWF
246
M2M 서버
263
AKA 알고리즘을 실행함. AUTN을 확인하고, RES 및 MSK를 생성함.
264. EAP-Resp/
AKA' Challange
265. EAP-Resp/
AKA' Challange
266
RES == XRES를 확인 함.
267. M2M Attach
Update
268. M2M Attach
Update
269. M2M Attach
Update Response
270. M2M Attach
Update Response
271
272. EAP-Req/
AKA' Notification
273. EAP-Req/
AKA' Notification
274. EAP-Resp/
AKA' Notification
275. EAP-Resp/
AKA' Notification
276. EAP-Req/
AKA' Success
277. EAP-Req/
AKA' Success
278. mId를 통한 데이터 평면 통신

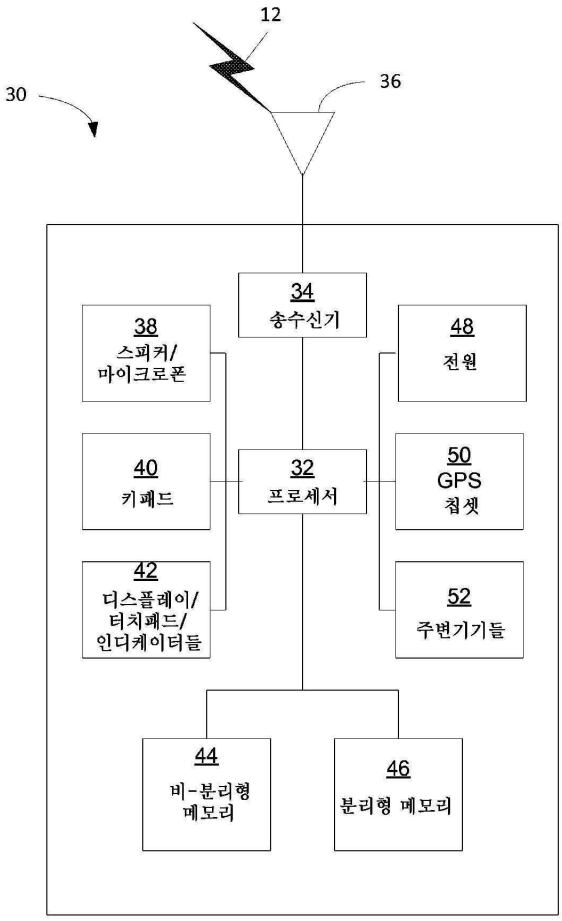
도면8a


M2M 단말 디바이스
18
M2M 단말 디바이스
18
M2M 단말 디바이스
18
M2M 게이트웨이 디바이스
14
통신 네트워크
12
10
22
20
M2M 단말 디바이스
18
M2M 단말 디바이스
18

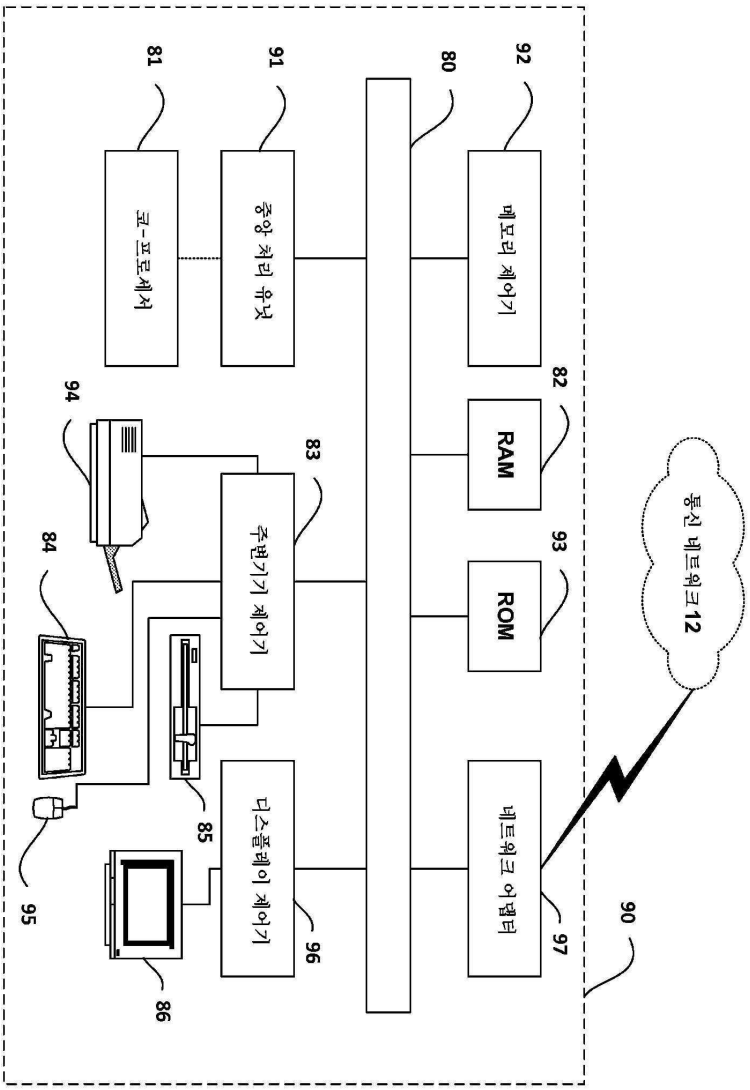
도면8b


필드
도메인
인프라구조
도메인
M2M 애플리케이션 20
M2M 애플리케이션 20'
M2M 서비스 레이어 22
M2M 서비스 레이어 22'
서비스 능력
1
서비스 능력
n
서비스 능력
1
서비스 능력
n
통신 네트워크
12
M2M 단말 디바이스
18
M2M 게이트웨이 디바이스
14
M2M 단말 디바이스
18
M2M 단말 디바이스
18

도면8c


12
30
36
34
송수신기
38
스피커/
마이크로폰
48
전원
40
키패드
32
프로세서
50
GPS
칩셋
42
디스플레이/
터치패드/
인디케이터들
52
주변기기들
44
비-분리형
메모리
46
분리형 메모리

도면8d


81
91
80
92
코-프로세서
중앙 처리 유닛
메모리 제어기
94
82
RAM
83
주변기기 제어기
84
93
ROM
통신 네트워크12
85
디스플레이 제어기
네트워크 어댑터
95
96
97
90
86