(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0098251
(43) 공개일자 2018년09월03일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
H04L 9/08 (2006.01) *H04L 9/14* (2006.01)
H04W 12/04 (2009.01) *H04W 12/10* (2009.01)
H04W 4/70 (2018.01)
(52) CPC특허분류
H04L 63/0428 (2013.01)
H04L 63/062 (2013.01)
(21) 출원번호 10-2018-7016964
(22) 출원일자(국제) 2016년12월14일
심사청구일자 없음
(85) 번역문제출일자 2018년06월15일
(86) 국제출원번호 PCT/US2016/066702
(87) 국제공개번호 WO 2017/112491
국제공개일자 2017년06월29일
(30) 우선권주장
62/387,499 2015년12월23일 미국(US)
15/199,924 2016년06월30일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
이 수범
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
팔라니고운데르 아난드
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
에스콧 애드리안 에드워드
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인코리아나

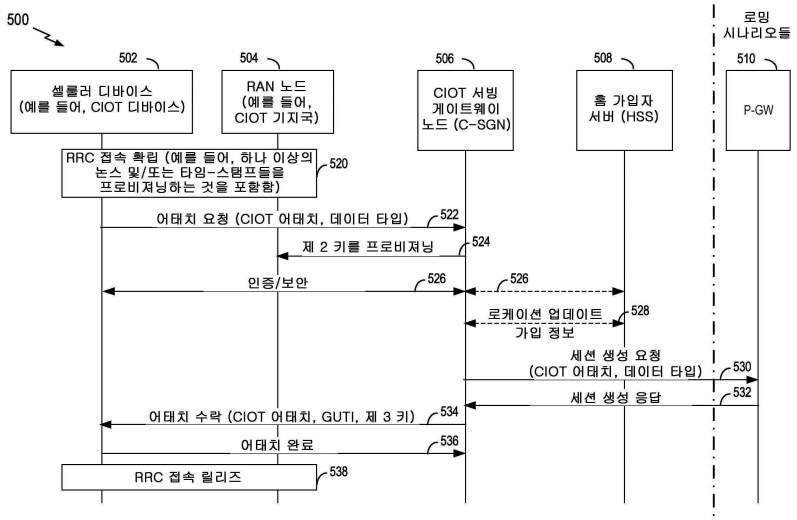
전체 청구항 수 : 총 30 항

(54) 발명의 명칭 **셀룰러 사물 인터넷에 대한 무상태 액세스 계층 보안**

(57) 요 약

보안 스킴들 (예를 들어, 무결성 보호, 암호화, 또는 양자 모두) 의 양태들이 설명된다. 액세스 계층 보안의 측정은 셀룰러 사물 인터넷 (CIoT) 기지국 (C-BS) 에서 셀룰러-디바이스-마다의 액세스 계층 보안 콘텍스트를 확립 및/또는 유지하는 것과 연관된 오버헤드 없이 실현될 수 있다. 게이트웨이 (예를 들어, CIoT 서빙 게이트웨이 노드 (C-SGN)) 는 제 1 키를 유도할 수도 있다. 제 1 키는 C-SGN 에만 알려져 있을 수도 있다. C-SGN 은 제 1 키 및 C-BS 에 고유한 파라미터로부터 제 2 키를 유도할 수도 있다. C-SGN 은 또한, 제 2 키 및 셀룰러 디바이스의 아이덴티티로부터 제 3 키를 유도할 수도 있다. C-SGN 은 제 2 및 제 3 키들을 각각 C-BS 및 셀룰러 디바이스로 전송할 수도 있다. 셀룰러 디바이스에 의해 암호화된 및/또는 무결성 보호된 스몰 데이터 메시지들은 C-BS 에 의해 해독 및/또는 검증될 수도 있다.

대 표 도



(52) CPC특허분류
H04L 63/123 (2013.01)
H04L 63/16 (2013.01)
H04L 63/205 (2013.01)
H04L 67/12 (2013.01)
H04L 9/0822 (2013.01)
H04L 9/14 (2013.01)
H04W 12/04 (2013.01)
H04W 12/10 (2013.01)
H04W 4/70 (2018.02)

명 세 서

청구범위

청구항 1

통신의 방법으로서,

게이트웨이에서, 상기 게이트웨이에만 알려져 있는 제 1 키를 획득하는 단계;

상기 게이트웨이에서, 상기 제 1 키 및 무선 액세스 네트워크 (RAN) 노드에 고유한 파라미터에 기초하는 제 2 키를 획득하는 단계;

상기 게이트웨이에 의해, 상기 제 2 키를 상기 RAN 노드에 프로비져닝하는 단계;

상기 게이트웨이에서, 상기 제 2 키 및 셀룰러 디바이스에 고유한 파라미터에 기초하여 제 3 키를 획득하는 단계; 및

상기 게이트웨이에 의해, 상기 제 3 키를 상기 셀룰러 디바이스에 프로비져닝하는 단계를 포함하는, 통신의 방법.

청구항 2

제 1 항에 있어서,

상기 게이트웨이는 셀룰러 사물 인터넷 서빙 게이트웨이 노드 (C-SGN) 인, 통신의 방법.

청구항 3

제 1 항에 있어서,

상기 제 1 키는 어떤 다른 키로부터 획득되지 않고 및/또는 상기 게이트웨이에서 랜덤으로 생성되는, 통신의 방법.

청구항 4

제 1 항에 있어서,

상기 RAN 노드는 셀룰러 사물 인터넷 (CIoT) 기지국 (C-BS) 또는 진화된 노드 B (eNodeB) 이고, 그리고 상기 RAN 노드에 고유한 상기 파라미터는 C-BS 아이덴티티 또는 eNodeB 아이덴티티인, 통신의 방법.

청구항 5

제 1 항에 있어서,

상기 제 2 키는 비-액세스 계층 (NAS) 메시지에서 상기 RAN 노드에 프로비져닝되는, 통신의 방법.

청구항 6

제 1 항에 있어서,

상기 제 3 키는 비-액세스 계층 (NAS) 메시지에서 상기 셀룰러 디바이스에 프로비져닝되는, 통신의 방법.

청구항 7

제 6 항에 있어서,

상기 NAS 메시지는 보안 NAS 메시지인, 통신의 방법.

청구항 8

제 1 항에 있어서,

상기 제 3 키는 상기 셀룰러 디바이스에 암호화된 정보 엘리먼트 (IE) 로서 프로비져닝되는, 통신의 방법.

청구항 9

제 8 항에 있어서,

상기 IE 는 상기 IE 를 암호화는데 이용되는 알고리즘을 식별하는 알고리즘 식별자를 포함하는, 통신의 방법.

청구항 10

통신 장치로서,

통신 네트워크의 노드들과 통신하기 위한 통신 인터페이스;

상기 통신 인터페이스에 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

상기 통신 장치에만 알려져 있는 제 1 키를 획득하고;

상기 제 1 키 및 무선 액세스 네트워크 (RAN) 노드에 고유한 파라미터에 기초하는 제 2 키를 획득하고;

상기 제 2 키를 상기 RAN 노드에 프로비져닝하고;

상기 제 2 키 및 셀룰러 디바이스에 고유한 파라미터에 기초하여 제 3 키를 획득하고; 그리고

상기 제 3 키를 상기 셀룰러 디바이스에 프로비져닝하도록 적응된, 통신 장치.

청구항 11

제 10 항에 있어서,

상기 프로세싱 회로는,

상기 제 1 키를 어떤 다른 키로부터 획득할 수 없을 시에 상기 제 1 키를 획득하고; 및/또는

상기 통신 장치에서 상기 제 1 키를 랜덤으로 생성하는 것에 의해 상기 제 1 키를 획득하도록 추가로 적응되는, 통신 장치.

청구항 12

제 10 항에 있어서,

상기 프로세싱 회로는,

비-액세스 계층 (NAS) 메시지에서 상기 제 2 키를 상기 RAN 노드에 프로비져닝하도록 추가로 적응되는, 통신 장치.

청구항 13

제 10 항에 있어서,

상기 프로세싱 회로는,

비-액세스 계층 (NAS) 메시지에서 상기 제 3 키를 상기 셀룰러 디바이스에 프로비져닝하도록 추가로 적응되는, 통신 장치.

청구항 14

제 10 항에 있어서,

상기 프로세싱 회로는,

암호화된 정보 엘리먼트 (IE) 에서 상기 제 3 키를 상기 셀룰러 디바이스에 프로비져닝하도록 추가로 적응되는, 통신 장치.

청구항 15

장치로서,

통신 네트워크의 노드들과 통신하기 위한 통신 인터페이스;

상기 통신 인터페이스에 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

제 1 키 및 상기 장치에 고유한 파라미터에 기초하는 제 2 키를 획득하고;

디바이스 아이덴티티 및 제 1 무결성 보호 값을 포함하는 스몰 (small) 데이터 메시지를 획득하고;

상기 제 2 키 및 상기 디바이스 아이덴티티에 기초하는 제 3 키를 획득하고;

상기 제 3 키에 기초하는 제 2 무결성 보호 값을 획득하고;

상기 제 1 무결성 보호 값과 상기 제 2 무결성 보호 값을 비교하고;

상기 제 1 무결성 보호 값이 상기 제 2 무결성 보호 값과 동일하지 않다는 것을 비교 결과가 표시하면 상기 스몰 데이터 메시지를 폐기하고; 그리고

상기 제 1 무결성 보호 값이 상기 제 2 무결성 보호 값과 동일하다는 것을 상기 비교 결과가 표시하면 상기 스몰 데이터 메시지를 게이트웨이로 전송하도록 적응된, 장치.

청구항 16

제 15 항에 있어서,

상기 제 1 무결성 보호 값 및 상기 제 2 무결성 보호 값은 적어도 하나의 논스 (nonce) 및/또는 타임 스탬프를 이용하여 획득되고, 그리고 상기 스몰 데이터 메시지를 획득하기 이전에, 상기 프로세싱 회로는,

상기 디바이스 아이덴티티에 의해 식별된 디바이스에 제 1 논스 및/또는 상기 타임 스탬프를 프로비져닝하고; 및/또는

상기 디바이스로부터 제 2 논스를 획득하도록 추가로 적응되는, 장치.

청구항 17

제 16 항에 있어서,

상기 프로세싱 회로는,

랜덤 액세스 프로시저 동안에 상기 제 1 논스 및/또는 상기 타임 스탬프를 프로비져닝하고 그리고 상기 제 2 논스를 획득하도록 추가로 적응되는, 장치.

청구항 18

제 15 항에 있어서,

상기 스몰 데이터 메시지는 상기 제 3 키로 암호화되고, 그리고 상기 프로세싱 회로는,

상기 제 3 키를 이용하여 상기 스몰 데이터 메시지를 해독하도록 추가로 적응되는, 장치.

청구항 19

제 15 항에 있어서,

상기 스몰 데이터 메시지를 획득하기 이전에, 상기 프로세싱 회로는,

트래픽 부하 값을 모니터링하고;

상기 트래픽 부하 값이 미리결정된 임계값을 초과한다는 것을 검출하고; 그리고

상기 트래픽 부하 값이 상기 미리결정된 임계값을 초과한다는 것을 검출하는 것에 응답하여, 상기 디바이스 아이덴티티에 의해 식별되는 디바이스로, 상기 장치로 전송된 다음의 하나 이상의 메시지들에 상기 제 1 무결성

보호 값을 포함시킬 것을 상기 디바이스에 요청하는 메시지를 전송하도록 추가로 적응되는, 장치.

청구항 20

제 19 항에 있어서,

네트워크가 상기 미리결정된 임계값을 구성하는, 장치.

청구항 21

제 15 항에 있어서,

상기 프로세싱 회로는,

게이트웨이로부터 상기 제 2 키를 획득하도록 추가로 적응되는, 장치.

청구항 22

제 21 항에 있어서,

상기 게이트웨이는 셀룰러 사물 인터넷 서빙 게이트웨이 노드 (C-SGN) 인, 장치.

청구항 23

제 15 항에 있어서,

상기 장치는 셀룰러 사물 인터넷 (CIoT) 기지국 (C-BS) 또는 진화된 노드 B (eNodeB) 이고, 그리고 장치에 고유한 상기 파라미터는 C-BS 아이덴티티 또는 eNodeB 아이덴티티인, 장치.

청구항 24

제 15 항에 있어서,

상기 프로세싱 회로는,

적어도 하나의 논스 및/또는 타임 스탬프를 이용하여 상기 제 1 무결성 보호 값 및 상기 제 2 무결성 보호 값을 획득하도록 추가로 적응되는, 장치.

청구항 25

제 15 항에 있어서,

상기 프로세싱 회로는,

디바이스와 초기 어태치 프로시저 동안에 액세스 계층 보안 구성을 협상하도록 추가로 적응되고, 상기 액세스 계층 보안 구성은, 보안 없이, 무결성 보호로, 암호화로, 무결성 보호 및 암호화로, 및/또는 온디맨드 무결성 보호로 스몰 데이터 메시지들이 상기 디바이스로부터 전송되는지 여부를 특정하고, 무결성 보호 및 암호화는 상기 제 3 키를 이용하여 수행되는, 장치.

청구항 26

장치로서,

통신 네트워크의 노드들과 통신하기 위한 통신 인터페이스;

상기 통신 인터페이스에 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

제 2 키 및 상기 장치에 고유한 파라미터에 기초하는 제 3 키를 획득하고;

액세스 계층 보안 구성을 협상하고;

상기 제 3 키를 이용하여 상기 액세스 계층 보안 구성에 기초한 스몰 데이터 메시지를 보호하고; 그리고

상기 제 3 키를 이용하여 보호된 상기 스몰 데이터 메시지를 전송하도록 적응된, 장치.

청구항 27

제 26 항에 있어서,

상기 프로세싱 회로는,

RAN 노드와 상기 액세스 계층 보안 구성을 협상하고; 그리고

상기 제 3 키를 이용하여 보호된 상기 스몰 데이터 메시지를 상기 RAN 노드로 전송하도록 추가로 적응되는, 장치.

청구항 28

제 26 항에 있어서,

상기 프로세싱 회로는,

게이트웨이로부터 상기 제 3 키를 획득하도록 추가로 적응되고, 상기 제 2 키는 제 1 키 및 RAN 노드에 고유한 파라미터에 기초하고, 그리고 상기 제 1 키는 상기 게이트웨이에만 알려져 있는, 장치.

청구항 29

제 26 항에 있어서,

상기 프로세싱 회로는,

초기 어태치 프로시저 동안에 상기 액세스 계층 보안 구성을 협상하도록 추가로 적응되는, 장치.

청구항 30

제 26 항에 있어서,

상기 프로세싱 회로는,

디바이스와 초기 어태치 프로시저 동안에 액세스 계층 보안 구성을 협상하도록 추가로 적응되고, 상기 액세스 계층 보안 구성은, 보안 없이, 무결성 보호로, 암호화로, 무결성 보호 및 암호화로, 및/또는 온디맨드 무결성 보호로 스몰 데이터 메시지들이 상기 디바이스로부터 전송되는지 여부를 특정하고, 무결성 보호 및 암호화는 상기 제 3 키를 이용하여 수행되는, 장치.

발명의 설명

기 술 분 야

[0001] **관련 출원에 대한 상호-참조**

[0002] 본 출원은 2015년 12월 23일자로 미국 특허청에 출원된 가출원 제62/387,499호, 및 2016년 6월 30일자로 미국 특허청에 출원된 정규출원 제15/199,924호에 대해 우선권을 주장하고 이들의 이익을 주장하며, 그 전체 내용은 모든 적용가능한 목적들을 위해 그리고 전부 이하에 완전히 기재된 것처럼 본 명세서에 참조로 통합된다.

[0003] 본 개시의 양태들은 일반적으로 무선 통신에 관한 것으로, 특히, 그러나 비배타적으로는, 셀룰러 사물 인터넷 (CIoT) 메시지들에 대해 무상태 (stateless) 방식으로 액세스 계층 보안을 달성하기 위한 기법들에 관한 것이다.

배 경 기 술

[0004] 국제 전기통신 연합 (International Telecommunications Union; ITU) 은 상호운용성 정보 및 통신 기술들에 기초하여 물리적 사물 (physical thing) 과 가상 사물 (virtual thing) 을 연결하는 인트라스트럭처로서 사물 인터넷 (Internet of Things; IoT) 을 설명한다. 본 명세서에서 사용한 바와 같이, 그리고 IoT 의 콘텍스트에서, "사물 (thing)" 은 통신 네트워크들에 식별 및 통합되는 것이 가능한 물리적 세계 (예를 들어, 물리적 사물) 또는 정보 세계 (예를 들어, 가상 사물) 에서의 오브젝트이다. Recommendation ITU-T Y.2060. 무선 광역 네트워크들 (WWAN) 및/또는 무선 로컬-영역 네트워크들 (무선 LAN) 과 같은 무선 통신 네트워크들은

IoT 디바이스들과 상호운용가능한 정보 및 통신 기술들 중 하나이다.

[0005] 롱 텀 에볼루션 (Long Term Evolution; LTE) 패러다임에 따르면, 무선 접속을 위해 2 개의 모드들이 정의되어 있다: 접속된 모드; 및 아이들 모드. 접속된 모드에서, 셀룰러 디바이스는 데이터를 전송 및 수신 중이다. 사용자 장비 (UE) 콘텍스트 ("UE 콘텍스트") 또는 "무선 리소스 제어 (RRC) 접속" 이 접속된 모드에서 확립된다. UE 콘텍스트의 경우, 무선 베어러가 셀룰러 디바이스와 코어 네트워크 (예를 들어, 진화된 패킷 코어 (evolved packet core; EPC)) 사이에서 데이터를 중계하도록 확립된다. 진화된 무선 액세스 베어러 (eRAB) 로 지칭되는, 무선 베어러는, 무선 베어러 부분 및 S1 베어러 부분을 포함한다. 무선 베어러는 LTE-Uu 레퍼런스 포인트 위에서 셀룰러 디바이스와 진화된 노드 B (eNodeB) 사이에 확립된다. S1 베어러는 S1 레퍼런스 포인트 위에서 eNodeB 와 서빙 게이트웨이 (S-GW) 사이에 확립된다. 그 통신들을 안전하게 하기 위해 보안 콘텍스트가 확립된다.

[0006] 아이들 모드에서, eRAB 베어러 (무선 베어러 및 S1 베어러) 가 릴리즈되고 보안 콘텍스트가 드롭된다. 이렇게 하여, 불필요한 무선 리소스들이 릴리즈된다. 무선 베어러들 및 보안 콘텍스트들은, 단지 전송/수신될 데이터가 있을 때 (즉, 접속된 모드에서) 확립 및 유지된다. 셀룰러 디바이스가 (예를 들어, 아이들 모드로부터) 웨이크 업할 때, eNodeB 는 새로운 UE 콘텍스트 및 보안 콘텍스트를 이동성 관리 엔티티 (MME) 로의 서비스 요청을 통해 확립하고 접속된 모드에 진입한다. 셀룰러 디바이스가 아이들 상태가 될 때, eNodeB 는 UE 콘텍스트 (예를 들어, eRAB 베어러) 및 보안 콘텍스트를 제거하고 아이들 모드에 진입한다.

[0007] LTE 이동성 관리 및 세션 관리 프로시저들은, UE 콘텍스트를 확립하기 위한 시그널링 지연이 CIoT 디바이스 웨이크업 주기를 연장시킬 것이기 때문에 예를 들어, 에너지 소비 면에서 셀룰러 사물 인터넷 (CIoT) 디바이스 및 그 CIoT 디바이스를 지원하는 네트워크에 대해 상당한 오버헤드를 초래할 수도 있다. 오버헤드는 추가된 레이턴시와 관련되며, 이는 또한 바람직하지 않다.

[0008] 오버헤드 및 레이턴시를 감소시키기 위해, 셀룰러 디바이스를 통과하는 다른 통신들에 대한 요건들과 비교한, CIoT 의 이동성 관리 및 보안 기능들에 대한 상이한 요건들이 제안되었다. 이들 상이한 요건들은 셀룰러 네트워크에서 동작하는 IoT 디바이스들의 이동성 관리 및 보안 기능들에 관련된 오버헤드를 감소시킬 수도 있다.
그러나, 상이한 요건들은 무선 액세스 네트워크 (RAN) 노드 및 코어 네트워크 노드들을 예를 들어 서비스 거부 (DoS) 및/또는 패킷 플러딩 공격 (packet flooding attack) 들과 같은 바람직하지 않은 취약성들에 오픈된 상태로 둘 수도 있다. 따라서, 오버헤드 및 레이턴시를 증가시키지 않고 이들 바람직하지 않은 취약성들을 극복 또는 방지하기 위한 방식들을 발견하는 것이 바람직하다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0009] 다음은 본 개시의 일부 양태들의 단순화된 개요를 이러한 양태들의 기본적인 이해를 제공하기 위하여 제시한다.
이 개요는 본 개시의 모든 고려된 피처들의 광범위한 개관이 아니며, 본 개시의 모든 양태들의 핵심적인 또는 결정적인 엘리먼트들을 식별하는 것으로도, 본 개시의 임의의 또는 모든 양태들의 범위를 기술하는 것으로도 의도되지 않는다. 그 유일한 목적은 본 개시의 일부 양태들의 다양한 개념들을 추후에 제시되는 보다 상세한 설명에 대한 서두 (prelude) 로서 단순화된 형태로 제시하는 것이다.

[0010] 일부 구현들에서, 통신의 방법은 게이트웨이에서, 그 게이트웨이에만 알려져 있을 수도 있는 제 1 키를 유도하는 단계를 포함할 수도 있다. 게이트웨이는 또한 제 1 키 및 무선 액세스 네트워크 (RAN) 의 노드에 고유할 수도 있는 파라미터에 기초할 수도 있는 제 2 키를 유도할 수도 있다. 게이트웨이는 제 2 키를 RAN 의 노드로 전송할 수도 있다. 게이트웨이는 또한 제 3 키를 유도할 수도 있다. 제 3 키는 제 2 키 및 셀룰러 디바이스에 고유할 수도 있는 파라미터에 기초할 수도 있다. 게이트웨이는 그 후 제 3 키를 셀룰러 디바이스로 전송할 수도 있다.

[0011] 일부 구현들에서, 통신 장치는 통신 네트워크의 노드들과 통신할 수도 있는 통신 인터페이스 및 그 통신 인터페이스에 커플링될 수도 있는 프로세싱 회로를 포함할 수도 있다. 프로세싱 회로는 통신 장치에만 알려져 있을 수도 있는 제 1 키를 유도하도록 고안 (constructing), 적응 (adapting), 및/또는 구성 (configuring) 될

수도 있다. 프로세싱 회로는 또한, 제 1 키 및 무선 액세스 네트워크 (RAN) 의 노드에 고유할 수도 있는 파라미터에 기초할 수도 있는 제 2 키를 유도할 수도 있다. 프로세싱 회로는, 통신 장치로 하여금, 제 2 키를 RAN 의 노드로 전송하게 할 수도 있다. 프로세싱 회로는 또한, 제 2 키 및 셀룰러 디바이스에 고유한 파라미터에 기초할 수도 있는 제 3 키를 유도할 수도 있다. 프로세싱 회로는, 통신 장치로 하여금, 제 3 키를 셀룰러 디바이스로 전송하게 할 수도 있다.

[0012] 일부 구현들에서, 무결성 보호된 통신의 방법은 무선 액세스 네트워크 (RAN) 노드에서, 제 2 키를 수신하는 단계를 포함할 수도 있다. 제 2 키는 제 1 키 및 RAN 노드에 고유한 파라미터에 기초할 수도 있다. 그 방법은 또한, RAN 노드에서, 디바이스 아이덴티티 및 제 1 무결성 보호 값 (예를 들어, 메시지 인증 코드 (MAC) 또는 토큰에 주어진 값) 을 포함하는 스몰 (small) 데이터 메시지를 수신하는 단계를 포함할 수도 있다. RAN 노드는 제 2 키 및 디바이스 아이덴티티에 기초할 수도 있는 제 3 키를 유도할 수도 있다. RAN 노드는 그 후 제 3 키를 이용하여 제 2 무결성 보호 값을 유도할 수도 있다. 제 1 무결성 보호 값과 제 2 무결성 보호 값의 비교가 수행될 수도 있다. 제 1 및 제 2 무결성 보호 값들이 동일하지 않다는 것을 그 비교의 결과가 표시하면, RAN 노드는 스몰 데이터 메시지를 폐기할 수도 있다. 그러나, 제 1 및 제 2 무결성 보호 값들이 동일하다는 것을 그 비교의 결과가 표시하면, RAN 노드는 스몰 데이터 메시지를 게이트웨이로 전송할 수도 있다.

[0013] 일부 구현들에서, 무상태 액세스 계층 보호의 방법이 실시될 수도 있다. 그 방법은 무선 액세스 네트워크 (RAN) 노드에서 제 2 키를 수신하는 단계를 포함할 수도 있다. 제 2 키는 제 1 키 및 RAN 노드에 고유한 파라미터에 기초할 수도 있다. RAN 노드는 디바이스 아이덴티티를 포함하는 암호화된 스몰 데이터 메시지를 수신할 수도 있다. 스몰 데이터 메시지는 제 3 키로 암호화될 수도 있다. RAN 노드는 제 2 키 및 디바이스 아이덴티티에 기초할 수도 있는 제 3 키를 유도할 수도 있다. RAN 노드는 그 후 제 3 키를 이용하여 스몰 데이터 메시지를 해독할 수도 있다.

[0014] 일부 구현들에서, 무상태 액세스 계층 보안의 다른 방법이 실시될 수도 있다. 그 방법은 무선 액세스 네트워크 (RAN) 노드에서 제 2 키를 수신하는 단계를 포함할 수도 있다. 제 2 키는 제 1 키 및 RAN 노드에 고유한 파라미터에 기초할 수도 있다. RAN 노드는 디바이스 아이덴티티를 포함하는 스몰 데이터 메시지를 수신할 수도 있다. 스몰 데이터 메시지는 제 3 키를 이용하여 암호화될 수도 있고 스몰 데이터 메시지는 무결성 보호 값을 포함할 수도 있고, 여기서 무결성 보호가 제 3 키를 이용하여 구현되었다. RAN 노드는 제 2 키 및 디바이스 아이덴티티에 기초할 수도 있는 제 3 키를 유도할 수도 있다. 스몰 데이터 메시지는 제 3 키를 이용하여 RAN 노드에서 해독될 수도 있다. 추가적으로, 무결성 보호 값은 제 3 키를 이용하여 RAN 노드에서 검증될 수도 있다.

[0015] 일부 구현들에서, 온디맨드 (on-demand) 무결성 보호의 방법이 제공될 수도 있다. 그 방법은, 무선 액세스 네트워크 (RAN) 노드에 의해, 트래픽 부하 값을 모니터링하는 단계를 포함할 수도 있다. RAN 노드는 트래픽 부하 값이 미리결정된 임계값을 초과한다는 것을 검출할 수도 있다. RAN 노드는, 트래픽 부하 값이 미리결정된 임계값을 초과한다는 것을 검출하는 것에 응답하여, 셀룰러 디바이스로 메시지를 전송할 수도 있다. 메시지는 RAN 노드로 전송된 다음의 하나 이상의 메시지들에 토큰을 포함시킬 것을 셀룰러 디바이스에 요청할 수도 있다,

[0016] 일부 구현들에서, 통신 장치와 같은 장치는 통신 네트워크의 노드들과 통신하기 위한 통신 인터페이스 및 그 통신 인터페이스에 커플링된 프로세싱 회로를 포함할 수도 있다. 장치는 무결성 보호된 통신을 위해 이용될 수도 있다. 일부 구현들에서, 프로세싱 회로는 제 2 키를 수신하도록 고안, 적응, 및/또는 구성될 수도 있다. 제 2 키는 제 1 키 및 장치에 고유한 파라미터에 기초할 수도 있다. 프로세싱 회로는 또한, 디바이스 아이덴티티 및 제 1 무결성 보호 값을 포함하는 스몰 데이터 메시지를 수신할 수도 있다. 프로세싱 회로는 제 2 키 및 디바이스 아이덴티티에 기초할 수도 있는 제 3 키를 유도할 수도 있다. 프로세싱 회로는 그 후 제 3 키를 이용하여 제 2 무결성 보호 값을 유도할 수도 있다. 제 1 무결성 보호 값과 제 2 무결성 보호 값의 비교는 프로세싱 회로에서 수행될 수도 있다. 제 1 및 제 2 무결성 보호 값들이 동일하지 않다는 것을 그 비교의 결과가 표시하면, 프로세싱 회로는, 장치로 하여금, 스몰 데이터 메시지를 폐기하게 할 수도 있다. 그러나, 제 1 및 제 2 무결성 보호 값들이 동일하다는 것을 그 비교의 결과가 표시하면, 프로세싱 회로는, 장치로 하여금, 스몰 데이터 메시지를 게이트웨이로 전송하게 할 수도 있다.

[0017] 일부 구현들에서, 통신 장치와 같은 장치는 통신 네트워크의 노드들과 통신하기 위한 통신 인터페이스 및 그 통신 인터페이스에 커플링된 프로세싱 회로를 포함할 수도 있다. 장치는 무상태 액세스 계층 보안을 실시하는

데 이용될 수도 있다. 일부 구현들에서, 프로세싱 회로는 제 2 키를 수신하도록 고안, 적응, 및/또는 구성될 수도 있다. 제 2 키는 제 1 키 및 장치에 고유한 파라미터에 기초할 수도 있다. 프로세싱 회로는 또한, 디바이스 아이덴티티를 포함하는 암호화된 스몰 데이터 메시지를 수신할 수도 있다. 일부 구현들에서, 스몰 데이터 메시지는 제 3 키로 암호화될 수도 있다. 프로세싱 회로는 제 3 키를 유도할 수도 있다. 제 3 키는 제 2 키 및 디바이스 아이덴티티에 기초할 수도 있다. 프로세싱 회로는 그 후 제 3 키를 이용하여 스몰 데이터 메시지를 해독할 수도 있다.

[0018] 일부 구현들에서, 통신 장치와 같은 장치는 통신 네트워크의 노드들과 통신하기 위한 통신 인터페이스 및 그 통신 인터페이스에 커플링된 프로세싱 회로를 포함할 수도 있다. 장치는 또한, 무상태 액세스 계층 보안을 실시하는데 이용될 수도 있다. 일부 구현들에서, 프로세싱 회로는 제 2 키를 수신하도록 고안, 적응, 및/또는 구성될 수도 있다. 제 2 키는 제 1 키 및 장치에 고유한 파라미터에 기초할 수도 있다. 프로세싱 회로는 또한, 디바이스 아이덴티티를 포함하는 스몰 데이터 메시지를 수신할 수도 있다. 스몰 데이터 메시지는 제 3 키로 암호화될 수도 있고 스몰 데이터 메시지는 제 3 키를 이용하여 유도된 무결성 보호 값을 포함할 수도 있다. 프로세싱 회로는 제 2 키 및 디바이스 아이덴티티에 기초할 수도 있는 제 3 키를 유도할 수도 있다. 프로세싱 회로는 제 3 키를 이용하여 스몰 데이터 메시지를 해독할 수도 있다. 프로세싱 회로는 또한 제 3 키를 이용하여 무결성 보호 값을 검증할 수도 있다.

[0019] 일부 구현들에서, 통신 장치와 같은 장치는 통신 네트워크의 노드들과 통신하기 위한 통신 인터페이스 및 그 통신 인터페이스에 커플링된 프로세싱 회로를 포함할 수도 있다. 장치는 온디맨드 무결성 보호된 통신을 위해 이용될 수도 있다. 일부 구현들에서, 프로세싱 회로는 트래픽 부하 값을 모니터링하도록 고안, 적응, 및/또는 구성될 수도 있다. 프로세싱 회로는 트래픽 부하 값이 미리결정된 임계값을 초과한다는 것을 검출할 수도 있다. 프로세싱 회로는 그 후 장치로 하여금, 트래픽 부하 값이 미리결정된 임계값을 초과한다는 것을 검출하는 것에 응답하여, 장치로 전송된 다음의 하나 이상의 메시지들에 토큰을 포함시킬 것을 셀룰러 디바이스에 요청하는 메시지를 셀룰러 디바이스로 전송하게 할 수도 있다.

[0020] 일부 구현들에서, 통신의 방법은 셀룰러 디바이스에서, 제 3 키를 수신하는 단계를 포함할 수도 있다. 제 3 키는 제 2 키 및 셀룰러 디바이스의 아이덴티티에 기초할 수도 있고, 제 2 키는 제 1 키 및 무선 액세스 네트워크 (RAN) 노드 아이덴티티에 기초할 수도 있다. 그 방법은 초기 어태치 프로시저 동안에 보안 프로토콜을 구성 및/또는 협상하는 단계를 더 포함할 수도 있다. 보안 프로토콜은 보안 없이, 무결성 보호로, 암호화로, 무결성 보호 및 암호화로, 및/또는 온디맨드 무결성 보호로 셀룰러 디바이스가 스몰 데이터 메시지들을 전송할 수도 있는지 여부를 결정할 수도 있다. 일부 구현들에서, 무결성 보호 및 암호화는 제 3 키에 기초할 수도 있다.

[0021] 일부 구현들에서, 통신 장치와 같은 장치는 통신 네트워크의 노드들과 통신하기 위한 통신 인터페이스 및 그 통신 인터페이스에 커플링된 프로세싱 회로를 포함할 수도 있다. 일부 구현들에서, 프로세싱 회로는 제 3 키를 수신하도록 고안, 적응, 및/또는 구성될 수도 있다. 제 3 키는 제 2 키 및 장치의 아이덴티티에 기초할 수도 있다. 제 2 키는 제 1 키 및 무선 액세스 네트워크 (RAN) 노드 아이덴티티에 기초할 수도 있다. 프로세싱 회로는 초기 어태치 프로시저 동안에 보안 프로토콜을 구성 및/또는 협상하도록 추가로 고안, 적응, 및/또는 구성될 수도 있다. 일부 구현들에서, 보안 프로토콜은 보안 없이, 무결성 보호로, 암호화로, 무결성 보호 및 암호화로, 및/또는 온디맨드 무결성 보호로 장치가 스몰 데이터 메시지들을 전송하는지 여부를 결정할 수도 있다. 일부 구현들에서, 무결성 보호 및 암호화는 제 3 키에 기초할 수도 있다.

[0022] 일부 구현들에서, 통신 장치와 같은 장치는 통신 네트워크의 노드들과 통신하기 위한 통신 인터페이스 및 그 통신 인터페이스에 커플링된 프로세싱 회로를 포함할 수도 있다. 그 장치는 또한, 무상태 액세스 계층 보안을 실시하는데 이용될 수도 있다. 일부 구현들에서, 프로세싱 회로는 제 2 키 및 장치에 고유한 파라미터에 기초하는 제 3 키를 획득하고, 액세스 계층 보안 구성을 협상하고, 제 3 키를 이용하여 액세스 계층 보안 구성에 기초한 스몰 데이터 메시지를 보호하고, 그리고 제 3 키를 이용하여 보호된 스몰 데이터 메시지를 전송하도록 고안, 적응, 및/또는 구성될 수도 있다. 일부 구현들에서, 프로세싱 회로는 RAN 노드와 액세스 계층 보안 구성을 협상하고, 그리고 제 3 키를 이용하여 보호된 스몰 데이터 메시지를 RAN 노드로 전송하도록 추가로 적응될 수도 있다. 일부 구현들에서, 프로세싱 회로는 게이트웨이로부터 제 3 키를 획득하도록 추가로 적응될 수도 있으며, 여기서 제 2 키는 제 1 키 및 RAN 노드에 고유한 파라미터에 기초하고, 제 1 키는 게이트웨이에만 알려져 있다. 일부 양태들에서, 프로세싱 회로는 초기 어태치 프로세서 동안에 액세스 계층 보안 구성을 협상하도록 추가로 적응될 수도 있다. 일부 양태들에서, 프로세싱 회로는 디바이스와 초기 어태치 프로시저 동안에 액세스 계층 보안 구성을 협상하도록 추가로 적응될 수도 있고, 여기서 액세스 계층 보안 구성은 보안

없이, 무결성 보호로, 암호화로, 무결성 보호 및 암호화로, 및/또는 온디맨드 무결성 보호로 스몰 데이터 메시지들이 디바이스로부터 전송되는지 여부를 특정하고, 여기서 무결성 보호 및 암호화는 제 3 키를 이용하여 수행된다.

도면의 간단한 설명

[0023] 다양한 피처들, 본성, 및 이점들은, 유사한 참조 부호들이 전반에 걸쳐 대응하여 식별하는 도면들과 함께 취해질 때 이하에 기재된 상세한 설명으로부터 명백해질 수도 있다.

도 1 은 본 개시의 양태들이 애플리케이션을 발견할 수도 있는 통신 네트워크의 일 예를 예시하는 다이어그램이다.

도 2 는 본 개시의 양태들이 애플리케이션을 발견할 수도 있는 통신 네트워크의 다른 예를 예시하는 다이어그램이다.

도 3 은 본 개시의 양태들이 애플리케이션을 발견할 수도 있는 통신 네트워크의 또 다른 예를 예시하는 다이어그램이다.

도 4 는 본 개시의 일부 양태들에 따른 액세스 계층 보안 키 유도 및 프로비져닝 프로세스의 일 예를 예시하는 플로우 다이어그램이다.

도 5 는 본 개시의 일부 양태들에 따른 셀룰러 사물 인터넷 (CIoT) 하의 연관된 어태치 프로시저의 일 예를 예시하는 호출 플로우 다이어그램이다.

도 6 은 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 및 보안 키들의 획득, 프로비져닝, 및 이용 중 하나 이상을 지원할 수도 있는 장치의 하드웨어 구현의 일 예를 예시하는 블록 다이어그램이다.

도 7 은 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 프로세스의 일 예를 예시하는 플로우 다이어그램이다.

도 8 은 본 개시의 하나 이상의 양태들에 따른 무상태 액세스 계층 보안 및 보안 키들의 획득, 프로비져닝, 및 이용 중 하나 이상을 지원할 수도 있는 장치의 하드웨어 구현의 다른 예를 예시하는 블록 다이어그램이다.

도 9 는 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 프로세스의 다른 예를 예시하는 플로우 다이어그램이다.

도 10 은 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 프로세스의 다른 예를 예시하는 플로우 다이어그램이다.

도 11 은 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 프로세스의 다른 예를 예시하는 플로우 다이어그램이다.

도 12 는 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 프로세스의 다른 예를 예시하는 플로우 다이어그램이다.

도 13 은 본 개시의 하나 이상의 양태들에 따른 무상태 액세스 계층 보안 및 보안 키들의 획득, 프로비져닝, 및 이용 중 하나 이상을 지원할 수도 있는 장치의 하드웨어 구현의 다른 예를 예시하는 블록 다이어그램이다.

도 14 는 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 프로세스의 다른 예를 예시하는 플로우 다이어그램이다.

도 15 는 본 개시의 일부 양태들에서 나타날 수도 있는 바와 같은 다수의 통신 엔티티들을 포함하는 무선 통신 네트워크의 개략적 예시이다.

발명을 실시하기 위한 구체적인 내용

[0024] IoT 디바이스들은 통신의 능력들 및 센싱, 액추에이션, 데이터 캡처, 데이터 저장, 및/또는 데이터 프로세싱의 옵션적 능력들을 가진 임의의 피스의 장비를 포함할 수도 있지만, 이들에 제한되지는 않는다. 셀룰러 디바이스 (예를 들어, 칩 컴포넌트, 무선 디바이스, 모바일 디바이스, 사용자 장비 (UE), 단말기) 는 IoT 디바이스와 인터페이스할 수도 있다. 인터페이스는 직접적으로 (예를 들어, IoT 디바이스는 셀룰러 디바이스와 일체형일 수도 있다) 또는 간접적으로 (예를 들어, IoT 디바이스는 블루투스와 같은 로컬 영역 네트워크를 통해 셀

룰러 디바이스에 인터페이스할 수도 있다) 달성될 수도 있다. 참조의 용이함을 위해, 본 명세서에서 행해진 셀룰러 디바이스에 대한 언급은, 다르게 특정하지 않는 한, IoT 디바이스 (즉, CIoT 디바이스) 에 인터페이스된 셀룰러 디바이스에 대한 언급인 것으로 이해될 것이다.

[0025] 본 명세서에서 사용한 바와 같이, 단어 "획득하다 (obtain)" 는 유도하다, 생성하다, 컴퓨팅하다, 취출하다, 수신하다, 요청하다 등등을 행하는 것을 의미할 수도 있고, 로컬로 획득하는 것 및/또는 원격으로 획득하는 것을 포괄할 수도 있다. 본 명세서에서 사용한 바와 같이, 단어 "획득하다" 는 부분적으로 획득하는 것 및/또는 완전히 획득하는 것을 포괄할 수도 있다.

[0026] 본 명세서에서 사용한 바와 같이, 어구 "온-더-플라이로 (on-the-fly)" 는 동적으로, 또는 필요에 따라 일어날 수도 있는 액션을 설명할 수도 있다.

[0027] **개관**

[0028] UE 가 아이들 모드로부터 접속된 모드로 트랜지션할 때, UE 및 그 UE 를 지원하는 네트워크는 전통적으로 UE 보안 콘텍스트 (예를 들어, 셀룰러-디바이스-마다의 (per-cellular-device) 액세스 계층 (access stratum; AS) 보안 콘텍스트) 및 eRAB 베어러를 확립한다. 그러나, 셀룰러 사물 인터넷 (CIoT) 디바이스들 (예를 들어, IoT 디바이스들과 인터페이스된 UE들) 에 대해, 오버헤드를 감소시키기 위해, 파티 (party) 들은 액세스 계층 (AS) 보안 콘텍스트의 확립을 제거하고 이동성 관리를 제거할 것을 제안하고 있다. 이동성 관리의 제거 (예를 들어, MME 를 제거) 는 네트워크 아키텍처에 있어서 변화를 필요로 한다. 이에 따라, CIoT 아키텍처는 CIoT 서빙 게이트웨이 노드 (C-SGN) 로 지칭된 새로운 노드를 도입한다. C-SGN 은 MME 로부터 남은 임의의 필요한 기능성을 서빙-게이트웨이 (S-GW) 의 기능성과 결합한다.

[0029] 그러나, CIoT 디바이스들에 대한 액세스 계층 (AS) 보안 및 이동성 관리를 제거하는 것은 무선 액세스 네트워크 (RAN) 노드 (예를 들어, eNB) 및 코어 네트워크 노드들을 이를 테면 서비스 거부 (DoS) 및/또는 패킷 플러딩 공격 (packet flooding attack) 들과 같은 바람직하지 않은 취약성들에 오픈된 상태로 둘 수도 있다.

[0030] 본 개시는 일부 양태들에서, 셀룰러 사물 인터넷 (CIoT) 기지국 (C-BS) 에서와 같은 RAN 노드에서 셀룰러-디바이스-마다의 액세스 계층 (AS) 보안 콘텍스트를 확립 및/또는 유지하지 않고 달성될 수 있는 보안 스킴들 (예를 들어, 무결성 보호, 암호화, 또는 양자 모두) 에 관한 것이다. 액세스 계층 보안의 적어도 일부 측정 (measure) 이 셀룰러-디바이스-마다의 액세스 계층 보안 콘텍스트를 확립 및/또는 유지하는 것과 연관된 오버헤드 없이 실현될 수 있다.

[0031] 게이트웨이, 예를 들어, C-SGN 은 3 개의 키들을 획득할 수도 있다. 제 1 키는 어떤 다른 키로부터 유도되지 않을 수도 있고 제 1 키는 C-SGN 에만 알려져 있을 수도 있다. 제 1 키는, 예를 들어, C-SGN 에 의해 랜덤으로 생성될 수 있다. 제 2 키는 제 1 키 및 무선 액세스 네트워크 (RAN) 노드에 고유한 파라미터 (예를 들어, C-BS 의 eNB 의 아이덴티티) 에 기초할 (예를 들어, 이들을 이용하여 유도될, 이들을 이용하여 생성될) 수도 있다. 제 3 키는 제 2 키 및 셀룰러 디바이스의 아이덴티티에 기초할 수도 있다. 아이덴티티는, 예를 들어, SAE-임시 모바일 가입자 아이덴티티 (S-TMSI) 일 수도 있다.

[0032] C-SGN 은 제 2 키를 RAN 노드에 그리고 제 3 키를 셀룰러 디바이스에 프로비져닝 (예를 들어, 제공, 전송, 전달) 할 수도 있다. 제 3 키는 예를 들어, 보안 NAS 메시지를 통해 셀룰러 디바이스에 프로비져닝될 수도 있다.

[0033] 셀룰러 디바이스가 CIoT 메시지 ("스몰 데이터 메시지" 로 지칭됨) 를 전송할 때, 셀룰러 디바이스는 CIoT 메시지에 무결성 보호 및/또는 암호화를 추가할 수도 있다. 무결성 보호 및/또는 암호화는 제 3 키를 이용하여 수행될 수도 있다. 서술한 바와 같이, 제 3 키는 제 2 키 및 디바이스의 아이덴티티에 기초할 (예를 들어, 이들을 이용하여 유도될, 이들을 이용하여 생성될) 수도 있다. 셀룰러 디바이스는 무결성 보호된 및/또는 암호화된 CIoT 메시지 (예를 들어, 스몰 데이터 메시지) 를 RAN 노드로 전송한다.

[0034] 일부 구현들에서, RAN 노드는 디바이스 (예를 들어, UE 보안 콘텍스트) 와 액세스 계층 (AS) 보안 콘텍스트를 확립 및/또는 유지하지 않을 수도 있다. 액세스 계층 보안 콘텍스트를 확립 및/또는 유지하는 것은 상태 테이블들 및 그 상태 테이블들과 연관된 데이터의 프로세싱의 이용을 요구한다; 이 오버헤드는 바람직하지 않다.

일부 구현들에서, RAN 노드는 RRC 시그널링을 이용하여 CIoT 메시지에 대한 액세스 계층 보안 구성 (예를 들어, 사이퍼링 (ciphering) 또는 무결성 보호) 을 인에이블/디스에이블하도록 디바이스를 구성할 수도 있다. 액세스 계층 보안 구성은 또한, 액세스 계층 보안 보호 구성으로 지칭될 수도 있다. 액세스 계층 보안 구성은 트리거링 이벤트 시에 C-SGN 에 의해 또는 RAN 노드에 의해 트리거링될 수도 있다. 트리거링

이벤트는, 예를 들어, 위조 (예를 들어, 진짜가 아닌 가짜, 모조) 패킷 인젝션의 검출 또는 서비스 거부 공격과 같은 공격의 검출을 포함할 수도 있다.

[0035] 액세스 계층 보안이, 본 명세서에서 제시된 예들에서 설명되는 바와 같이, 트리거링 또는 이용될 때, RAN 노드는 온-더-플라이로, 제 3 키의 듀플리케이트 (duplicate) 를 획득 (예를 들어, 유도, 생성) 하기 위해 제 2 키 (C-SGN 에 의해 RAN 노드에 프로비져닝되었음) 및 셀룰러 디바이스의 아이덴티티를 이용할 수도 있다. 셀룰러 디바이스의 아이덴티티는 RAN 노드에서 획득된 모든 스몰 데이터 메시지와 함께 포함되고 제 2 키는 셀룰러 디바이스의 아이덴티티에 독립적이다; 이에 따라, 보안 스킴은 상태 테이블이 필요하지 않다는 점에서 무상태이다. 제 3 키를 이용하면, RAN 노드는 구성에 기초하여 스몰 데이터를 검증, 해독, 또는 양자 모두를 행할 수 있다. 하나의 양태에서, RAN 노드는 제 3 키에 의해 보호된 (무결성 보호된 및/또는 암호화된) 스몰 데이터 메시지를 수신할 수도 있고 그 후 (즉, 스몰 데이터 메시지가 C-SGN 으로부터 제 3 키를 획득한 디바이스로부터 전송되었다는 것을 검증하기 위해) 스몰 데이터 메시지의 무결성 보호를 검증하고 및/또는 스몰 데이터 메시지를 해독할 수도 있다.

[0036] **예시적인 동작 환경**

[0037] 도 1 은 본 개시의 양태들이 애플리케이션을 발견할 수도 있는 통신 네트워크 (100) 의 일 예를 예시하는 다이어그램이다. 무선 액세스 네트워크 (RAN) 는 하나 이상의 네트워크 액세스 노드들 (예를 들어, 셀룰러 사물 인터넷 (CIoT) 기지국 (C-BS), eNodeB) (RAN 노드 (102) 로 지칭됨) 을 포함할 수도 있다. 본 명세서에서 제시된 기법들은 RAN 노드 (102) (예를 들어, C-BS, eNodeB), 셀룰러 디바이스 (116, 122), 및/또는 CIoT 디바이스 (136, 142) 에 키들을 프로비져닝하는데 이용될 수도 있다. 키들 (예를 들어, 암호키들, 수학적으로 유도된 키들) 은 스몰 데이터 메시지들을 무결성 보호 및/또는 암호화하는데 이용될 수도 있다. 스몰 데이터 메시지들의 무결성 보호 및/또는 암호화는 통신 네트워크 (100) 에 액세스 계층 보안 및 보호를 바람직하게 추가한다.

[0038] 도 1 의 예에서, RAN 노드 (102) 는 다수의 안테나 그룹들을 포함할 수도 있으며, 하나의 그룹은 안테나들 (104 및 106) 을 포함하고, 다른 그룹은 안테나들 (108 및 110) 을 포함하고, 그리고 추가적인 그룹은 안테나들 (112 및 114) 을 포함한다. 도 1 에는, 2 개의 안테나들이 각각의 안테나 그룹을 위해 도시된다; 그러나 더 많거나 또는 더 적은 안테나들이 각각의 안테나 그룹에 대해 활용될 수도 있다. 셀룰러 디바이스 (116) 는 안테나들 (112 및 114) 과 통신하고 있을 수도 있고, 여기서 안테나들 (112 및 114) 은 순방향 링크 (120) (예를 들어, 다운링크) 를 통해 셀룰러 디바이스 (116) 에 정보를 송신하고 역방향 링크 (118) (예를 들어, 업링크) 를 통해 셀룰러 디바이스 (116) 로부터 정보를 수신한다. 셀룰러 디바이스 (112) 는 안테나들 (104 및 106) 과 통신하고 있을 수도 있고, 여기서 안테나들 (104 및 106) 은 순방향 링크 (126) 를 통해 셀룰러 디바이스 (122) 에 정보를 송신하고 역방향 링크 (124) 를 통해 셀룰러 디바이스 (122) 로부터 정보를 수신한다. RAN 노드 (102) 는 또한, 예를 들어, 사물 인터넷 (IoT) 디바이스들과 인터페이스할 수도 있는, 다른 셀룰러 디바이스들과 통신하고 있을 수도 있다. 예를 들어, IoT 디바이스 (150) 는 셀룰러 디바이스 (116) 와 통신하고 있을 수도 있고, 여기서 정보는 순방향 링크 (121) 를 통해 IoT 디바이스 (150) 에 송신될 수도 있고 정보는 역방향 링크 (119) 를 통해 IoT 디바이스 (150) 로부터 셀룰러 디바이스 (116) 로 전송될 수도 있다. IoT 디바이스 (셀룰러 사물 인터넷 (CIoT) 디바이스 (136) 또는 CIoT 디바이스 (136) 로 통칭됨) 에 (예를 들어, 직접적으로 또는 간접적으로) 인터페이스된 셀룰러 디바이스는 RAN 노드 (102) 의 하나 이상의 다른 안테나들과 통신하고 있을 수도 있고, 여기서 안테나들은 순방향 링크 (140) 를 통해 CIoT 디바이스 (136) 에 정보를 송신하고 역방향 링크 (138) 를 통해 CIoT 디바이스 (136) 로부터 정보를 수신한다. CIoT 디바이스 (142) 는 RAN 노드 (102) 의 하나 이상의 다른 안테나들과 통신하고 있을 수도 있고, 여기서 안테나들은 순방향 링크 (146) 를 통해 CIoT 디바이스 (142) 에 정보를 송신하고 역방향 링크 (144) 를 통해 CIoT 디바이스 (142) 로부터 정보를 수신한다. RAN 노드 (102) 는 하나 이상의 통신 링크들 및/또는 레퍼런스 포인트들 (128) 에 의해 코어 네트워크 (130) 에 커플링될 수도 있다.

[0039] 본 개시 전반에 걸쳐 제시된 다양한 개념들은 다양한 전기통신 시스템들, 네트워크 아키텍처들, 및 통신 표준들에 걸쳐서 구현될 수도 있다. 예를 들어, 제 3 세대 파트너십 프로젝트 (3GPP) 는 롱-텀 에볼루션 (LTE) 네트워크들로 빈번히 지칭되는, 진화된 패킷 시스템 (EPS) 을 수반하는 네트워크들에 대한 여러 무선 통신 표준들을 정의하는 표준 바디이다. 제 5 세대 (5G) 네트워크와 같은 LTE 네트워크의 진화된 버전들은, 웹 브라우징, 비디오 스트리밍, VoIP, 임무 결정적 애플리케이션들, 멀티-홉 네트워크들, 실시간 피드백을 가진 원격 동작들 (예를 들어, 원격 수술) 등을 포함하지만, 이들에 제한되지는 않는, 많은 상이한 타입들의 서비스들 또는 애플리케이션들을 위해 제공될 수도 있다. LTE 네트워크의 진화는 계속 진행중인 프로세스이다. 그 진

화는 IoT 디바이스들에 인터페이스된 셀룰러 디바이스들을 포함한, 모든 셀룰러 디바이스들과의 개선된 상호운용성을 위해 이루어진 변화들/수정들/대안들을 포함한다. 이에 따라, 디바이스들 (116, 122, 150, 136, 142), RAN 노드 (102) 및 코어 네트워크 (130) 내의 노드들에 대한 변화들/수정들/대안들의 예들이 본 명세서에서 설명된다.

[0040] 무선 셀룰러 통신 네트워크들은 2 개의 레벨들에서 보안을 다룬다. 이들 레벨들은 액세스 계층 (AS) 및 비-액세스 계층 (non-access stratum; NAS) 으로 지칭된다. 일 예로서 롱 텀 에볼루션 (LTE) 을 이용하면, 액세스 계층은 RAN 과 셀룰러 디바이스 사이의 무선 전기통신 프로토콜 스택들에서의 기능 레이어로서 설명될 수도 있다. 액세스 계층 프로토콜 레이어는 RAN 과 셀룰러 디바이스 사이의 무선 접속을 통해 데이터를 전송하는 것 그리고 무선 리소스들을 관리하는 것을 담당할 수도 있다. 비-액세스 계층은 코어 네트워크와 셀룰러 디바이스 사이의 무선 전기통신 프로토콜 스택들에서의 기능 레이어일 수도 있다. 비-액세스 계층 프로토콜 레이어는 통신 세션들의 확립을 관리하고 셀룰러 디바이스가 이동할 때 그 셀룰러 디바이스와의 계속적인 통신을 유지하기 위해 이용될 수도 있다. 비-액세스 계층 프로토콜 레이어는 또한, 셀룰러 디바이스와 코어 네트워크 (예를 들어, MME 또는 C-SGN) 의 노드 사이의 메시지들의 통과를 위해 이용될 수도 있고, 여기서 그 메시지들은 RAN 을 통하여 투명하게 통과된다. NAS 메시지들의 예들은 업데이트 (Updata) 메시지들, 어태치 요청 (Attach Request) 메시지들, 어태치 수락 (Attach Accept) 메시지들, 인증 (Authentication) 메시지들, 및 서비스 요청 (Service Request) 들을 포함한다.

[0041] 오버헤드 및 레이턴시를 감소시키기 위해, 3GPP 표준 세팅 바디는 셀룰러 디바이스를 통과하는 다른 통신들에 대한 요건들과 비교하여, CIoT 에 대해 상이한 요건들을 제안하였다. 그러나, 이들 요건들은 RAN 노드 및 코어 네트워크를 바람직하지 않은 취약성들에 오픈된 상태로 둘 수도 있다.

[0042] 상이한 요건들 중에는 액세스 계층 보안의 제거가 있다. 액세스 계층 보안은 셀룰러 디바이스와 eNodeB 사이의 공중 인터페이스에서의 보안에 관한 것이다. CIoT 메시지들은 제어 평면에서, NAS 레이어에서, 셀룰러 디바이스로부터 코어 네트워크로 전송되도록 제안된다. 스몰 데이터 메시지들로 본 명세서에서 지칭되는, CIoT 메시지들은 따라서 기존의 NAS 보안에 의해 보호된다. 그러나, 이하에 설명되는 바와 같이, AS 보안을 제거하는 것은 RAN 노드 및 코어 네트워크를 바람직하지 않은 취약성들에 오픈된 상태로 둘 수도 있다.

[0043] 또한, 상이한 요건들 중에는 CIoT 에 대한 이동성 지원의 제거가 있다. IoT 디바이스들은 하루종일 주기적 레포트들을 전송하는 것에 의해 동작할 수도 있다; 그들은 오랜 시간 동안 코어 네트워크에 접속된 상태로 유지되지 않는다. 많은 IoT 디바이스들은 정지식이고, 그들은 셀들을 통하여 이동하지 않고, 오히려 그들은 하나의 셀의 경계들 내의 고정된 로케이션에 남아 있다. 다른 IoT 디바이스들, 이를 테면 자동차들, 인간들, 소포들 등에 커플링된 것들은 셀들을 통하여 이동한다, 즉 그들은 로밍된다. IoT 디바이스들이 네트워크를 통하여 로밍되기 때문에, 그들이 레포트를 전송해야 할 시간이 도래할 때, 그들은 셀에서 웨이크 업하고 그들의 레포트를 그 셀 내로부터 전송한다; 셀-투-셀 접속된 모드 이동성은 요구되지 않을 수도 있다.

[0044] 따라서, 접속된 모드 이동성은 CIoT 아키텍처에서 지원되지 않을 수도 있다. 이동성 관리의 제거는 RAN 에서의 eNodeB 와 코어 네트워크에서의 MME 양자 모두에 대해 오버헤드의 감소를 제공한다. 이에 따라, CIoT 아키텍처는 CIoT 서빙 게이트웨이 노드 (C-SGN) 로 지칭되는 새로운 노드를 도입한다. C-SGN 은 MME 로부터 남은 임의의 필요한 기능성을 서빙-게이트웨이 (S-GW) 의 기능성과 결합한다. C-SGN 은 3G 에서 서빙 범용 패킷 무선 서비스 (GPRS) 지원 노드 (SGSN) 와 등가일 수도 있다.

[0045] 도 2 는 본 개시의 양태들이 애플리케이션을 발견할 수도 있는 통신 네트워크 (200) 의 다른 예를 예시하는 다이어그램이다. 예를 들어, 본 명세서에서 제시된 기법들은 게이트웨이 (202) (예를 들어, C-SGN) 에 의해, 제 1 RAN 노드 (204) (예를 들어, C-BS) 및 CIoT 디바이스 (206) 에 키들을 프로비져닝하는데 이용될 수도 있다. 도 2 의 예시적인 예시는 CIoT 디바이스 (206) 를 수반하는 비-로밍 시나리오에 대한 CIoT 아키텍처를 나타낸다. 도 2 의 양태에서, 패킷 데이터 네트워크 게이트웨이 (P-GW) 의 기능들은 게이트웨이 (202) (예를 들어, C-SGN) 의 것과 통합될 수 있다. 추가적으로 또는 대안적으로, 구현 옵션 (240) 으로서, P-GW 의 기능들은 P-GW (237) 에서 게이트웨이 (202) 로부터 분리될 수 있다. 구현 옵션 (240) 에 따르면, S5 레퍼런스 포인트 (239) 는 게이트웨이 (202) (예를 들어, C-SGN) 와 P-GW (237) 사이에서 이용될 수도 있다. S5 레퍼런스 포인트는 게이트웨이 (202) (예를 들어, C-SGN) 와 P-GW (237) 사이에 사용자 평면 터널링 및 터널 관리를 제공할 수도 있다. S5 레퍼런스 포인트는 예를 들어, 게이트웨이 (202) (예를 들어, C-SGN) 가 패킷 데이터 네트워크 접속성을 위해 비-병치된 P-GW (237) 에 접속하면 이용될 수도 있다. 따라서, 도 2 의 예시적인 비-로밍 시나리오에서도, 게이트웨이 (202) (예를 들어, C-SGN) 및 P-GW (237) 는 옵션적으로는 별도의

엔티티들일 수도 있다 (예를 들어, 그들은 병치되지 않을 수도 있다).

[0046] 도 2 의 예시적인 예시에서, 게이트웨이 (202) 에 의해 프로비져닝된 키들은 스몰 데이터 메시지들을 무결성 보호 및/또는 암호화여, 이로써 통신 네트워크 (200) 에 액세스 계층 보호를 제공하는데 이용될 수도 있다.

[0047] 도 2 의 예에서, CIoT 디바이스 (206) 는 셀룰러 디바이스 (210) 에 인터페이스된 IoT 디바이스 (208) 로서 표현될 수도 있다. 인터페이스는 직접적 (예를 들어, IoT 디바이스 (208) 는 셀룰러 디바이스 (210) 에 하드 와이어링될 수도 있다) 또는 간접적 (예를 들어, IoT 디바이스 (208) 는 블루투스 무선 네트워크와 같은 중간 통신 네트워크를 통해 셀룰러 디바이스 (210) 에 커플링될 수도 있다) 일 수도 있다. CIoT 디바이스 (206) 는 C-Uu 레퍼런스 포인트 (212) (레퍼런스 포인트들은 또한 네트워크 인터페이스들로 지칭될 수도 있다) 위에서 제 1 RAN 노드 (204) (예를 들어, C-BS) 와 무선으로 통신할 수도 있다. 제 1 RAN 노드 (204) (예를 들어, C-BS) 는 S1, 또는 등가의, 레퍼런스 포인트 위에서 게이트웨이 (202) (예를 들어, C-SGN) 와 통신할 수도 있다. 일부 양태들에서, 도 2 에 예시한 바와 같이, 제 1 RAN 노드 (204) 는 S1-라이트 (lite) (214) 레퍼런스 포인트 위에서 게이트웨이 (202) 와 통신할 수도 있다. S1-라이트는 스몰 데이터 메시지들에 대해 최적화되는 S1 의 "경량 (light-weight)" 버전이다. 예를 들어, 단지 CIoT 프로시저들을 지원하는데 필요한 S1 애플리케이션 프로토콜 (S1AP) 메시지들 및 정보 엘리먼트들 (IE들) 만이 S1-라이트에 포함될 수도 있다. 일반적으로, 레퍼런스 포인트 (예를 들어, 네트워크 인터페이스) 는 S1, S1-라이트 (214), 또는 등가물일 수도 있다.

[0048] 도 2 에는 또한, 롱 텀 에볼루션 (LTE) 또는 머신 타입 통신 (MTC) 셀룰러 디바이스 (216) 가 묘사되어 있다. LTE 또는 MTC 셀룰러 디바이스 (216) 는 LTE Uu (eMTC) 레퍼런스 포인트 (218) 위에서 제 2 RAN 노드 (220) (예를 들어, eNodeB) 와 무선으로 통신할 수도 있다.

[0049] 제 2 RAN 노드 (220) 는 S1 레퍼런스 포인트 위에서 게이트웨이 (202) 와 통신할 수도 있다. 일부 양태들에서, 도 2 에 예시한 바와 같이, 제 2 RAN 노드 (220) 는 S1-라이트 (222) 레퍼런스 포인트 위에서 게이트웨이 (202) 와 통신할 수도 있다.

[0050] 게이트웨이 (202) 는 홈 가입자 서버 (224) (HSS) 와 통신할 수도 있다. HSS (224) 는 사용자 가입 정보를 포함하는 데이터베이스를 저장 및 업데이트할 수도 있고 사용자 아이덴티티 키들로부터 보안 정보를 생성한다. HSS (224) 는 S6a (226) 레퍼런스 포인트 위에서 게이트웨이 (202) 와 통신할 수도 있다. S6a (226) 레퍼런스 포인트는 통신 네트워크 (200) 에 사용자 액세스를 인증/인가하기 위해 가입 및 인증 데이터의 전송을 인에이블한다. 게이트웨이 (202) 는 단문 메시지 서비스 (short message service; SMS) 게이트웨이 모바일 스위칭 센터 (SMS-GMSC)/인터 워킹 모바일 스위칭 센터 (IWMSC)/SMS 라우터 (즉, SMS-GMSC/IWMSC/SMS 라우터 (228)) 와 통신할 수도 있다. 일반적으로, SMS-GMSC/IWMSC/SMS 라우터 (228) 는 다른 네트워크들과 단문 메시지 서비스를 위한 콘택 포인트이다. SMS-GMSC/IWMSC/SMS 라우터 (228) 는 Gd/Gdd (230) 레퍼런스 포인트 위에서 게이트웨이 (202) 와 통신할 수도 있다. 게이트웨이 (202) 는 애플리케이션 서버 (232) 와 통신할 수도 있다.

[0051] 일반적으로, 애플리케이션 서버 (232) 는 서비스 제공자들의 애플리케이션들을 호스팅할 수도 있다. 애플리케이션 서버 (232) 는 패킷 데이터 네트워크 (예를 들어, 인터넷) 에 로케이트될 수도 있다. 애플리케이션 서버 (232) 는 SGi (234) 레퍼런스 포인트 위에서 게이트웨이 (202) 와 통신할 수도 있다. SGi (234) 는 게이트웨이 (202) (예를 들어, C-SGN) 와 패킷 데이터 네트워크 사이의 레퍼런스 포인트이다.

[0052] 도 3 은 본 개시의 양태들이 애플리케이션을 발견할 수도 있는 통신 네트워크 (300) 의 또 다른 예를 예시하는 다이어그램이다. 예를 들어, 본 명세서에서 제시된 기법들은 게이트웨이 (302) (예를 들어, C-SGN) 에 의해, 제 1 RAN 노드 (304) (예를 들어, C-BS) 와 CIoT 디바이스 (306) 에 키들을 프로비져닝하는데 이용될 수도 있다. 도 3 의 예시적인 예시는 CIoT 디바이스 (306) 를 수반하는 로밍 시나리오에 대한 CIoT 아키텍처를 나타낸다.

[0053] 도 3 의 예시적인 예시에서, 게이트웨이 (302) 에 의해 프로비져닝된 키들은 스몰 데이터 메시지들을 무결성 보호 및/또는 암호화하여, 이로써 통신 네트워크 (300) 에 액세스 계층 보호를 제공하는데 이용될 수도 있다.

[0054] 도 3 의 노드들은, 게이트웨이 (302) (예를 들어, C-SGN) 외부의, 및/또는 그 게이트웨이와 병치되지 않은, 패킷 데이터 네트워크 (PDN) 게이트웨이 (P-GW) (336) 노드의 추가를 제외하고는, 도 2 의 노드들과 동일 또는 유사하다. 도 3 의 설명이 완전성을 위해 후속된다.

[0055] 도 3 의 예에서, CIoT 디바이스 (306) 는 셀룰러 디바이스 (310) 에 인터페이스된 IoT 디바이스 (308) 로서 표

현될 수도 있다. 인터페이스는 직접적 (예를 들어, IoT 디바이스 (308) 는 셀룰러 디바이스 (310) 에 하드 와이어링될 수도 있다) 또는 간접적 (예를 들어, IoT 디바이스 (308) 는 블루투스 무선 네트워크와 같은 중간 통신 네트워크를 통해 셀룰러 디바이스 (310) 에 커플링될 수도 있다) 일 수도 있다. CIoT 디바이스 (306) 는 C-Uu 레퍼런스 포인트 (312) (레퍼런스 포인트들은 또한 네트워크 인터페이스들로 지칭될 수도 있다) 위에서 제 1 RAN 노드 (304) (예를 들어, C-BS) 와 무선으로 통신할 수도 있다. 제 1 RAN 노드 (304) (예를 들어, C-BS) 는 S1 레퍼런스 포인트 위에서 게이트웨이 (302) (예를 들어, C-SGN) 와 통신할 수도 있다. 일부 양태들에서, 도 3 에 예시한 바와 같이, 제 1 RAN 노드 (304) 는 S1-라이트 (314) 레퍼런스 포인트 위에서 게이트웨이 (302) 와 통신할 수도 있다. S1-라이트는 스몰 데이터 메시지들에 대해 최적화되는 S1 의 버전이다. 예를 들어, 단지 CIoT 프로시저들을 지원하는데 필요한 S1 애플리케이션 프로토콜 (S1AP) 메시지들 및 정보 엘리먼트들 (IE들) 이 S1-라이트에 포함될 수도 있다. 일반적으로, 레퍼런스 포인트 (예를 들어, 네트워크 인터페이스) 는 S1, S1-라이트 (314), 또는 등가물일 수도 있다.

[0056] 도 3 에는 또한, 롱 텀 에볼루션 (LTE) 또는 머신 타입 통신 (MTC) 셀룰러 디바이스 (316) 가 묘사되어 있다. LTE 또는 MTC 셀룰러 디바이스 (316) 는 LTE Uu (eMTC) 레퍼런스 포인트 (318) 위에서 제 2 RAN 노드 (320) (예를 들어, eNodeB) 와 무선으로 통신할 수도 있다.

[0057] 제 2 RAN 노드 (320) 는 S1 레퍼런스 포인트 위에서 게이트웨이 (302) 와 통신할 수도 있다. 일부 양태들에서, 도 3 에 예시한 바와 같이, 제 2 RAN 노드 (320) 는 S1-라이트 (322) 레퍼런스 포인트 위에서 게이트웨이 (302) 와 통신할 수도 있다.

[0058] 게이트웨이 (302) 는 홈 가입자 서버 (324) (HSS) 와 통신할 수도 있다. HSS (324) 는 사용자 가입 정보를 포함하는 데이터베이스를 저장 및 업데이트할 수도 있고 사용자 아이덴티티 키들로부터 보안 정보를 생성한다. HSS (324) 는 S6a (326) 레퍼런스 포인트 위에서 게이트웨이 (302) 와 통신할 수도 있다. S6a (326) 레퍼런스 포인트는 통신 네트워크 (300) 에 사용자 액세스를 인증/인가하기 위한 가입 및 인증 데이터의 전송을 인에이블한다. 게이트웨이 (302) 는 단문 메시지 서비스 (SMS) 게이트웨이 모바일 스위칭 센터 (SMS-GMSC)/인터 워킹 모바일 스위칭 센터 (IWMSC)/SMS 라우터 (즉, SMS-GMSC/IWMSC/SMS 라우터 (328)) 와 통신할 수도 있다. 일반적으로, SMS-GMSC/IWMSC/SMS 라우터 (328) 는 다른 네트워크들과 단문 메시지 서비스를 위한 콘택 포인트이다. SMS-GMSC/IWMSC/SMS 라우터 (328) 는 Gd/Gdd (330) 레퍼런스 포인트 위에서 게이트웨이 (302) 와 통신할 수도 있다. 게이트웨이 (302) 는 애플리케이션 서버 (332) 와 통신할 수도 있다.

[0059] 일반적으로, 애플리케이션 서버 (332) 는 서비스 제공자들의 애플리케이션들을 호스팅할 수도 있다. 애플리케이션 서버 (332) 는 패킷 데이터 네트워크 (예를 들어, 인터넷) 에 로케이트될 수도 있다. 애플리케이션 서버 (332) 는 SGi (334) 레퍼런스 포인트 위에서 P-GW (336) 와 통신할 수도 있다. SGi (334) 는 패킷 데이터 네트워크에서 P-GW (336) 와 애플리케이션 서버 (332) 사이의 레퍼런스 포인트이다. P-GW (336) 는 S8 (338) 레퍼런스 포인트 위에서 게이트웨이 (302) (예를 들어, C-SGN) 와 통신할 수도 있다. S8 (338) 레퍼런스 포인트는, 일반적으로 방문자 공중 육상 모바일 네트워크 (Visitor Public Land Mobile Network; VPLMN) 에서의 서빙 GW (또는 도 3 의 경우에, C-SGN) 와 홈 공중 육상 모바일 네트워크 (HPLMN) 에서의 P-GW 사이에 사용자 및 제어 평면 인터페이스를 제공하는, 인터-공중 육상 모바일 네트워크 (인터-PLMN) 레퍼런스 포인트이다.

[0060] 도 3 의 양태에서, P-GW 기능들은 P-GW (336) 에서 게이트웨이 (302) 로부터, 또는 P-GW (337) 에서 구현 옵션 (340) 으로서 분리될 수 있다. 구현 옵션 (340) 의 경우에, S5 레퍼런스 포인트 (339) 는 게이트웨이 (302) (예를 들어, C-SGN) 와 P-GW (337) 사이에 이용될 수도 있다. S5 레퍼런스 포인트는 게이트웨이 (302) (예를 들어, C-SGN) 와 P-GW (337) 사이에 사용자 평면 터널링 및 터널 관리를 제공할 수도 있다. S5 레퍼런스 포인트는 예를 들어, 게이트웨이 (302) (예를 들어, C-SGN) 가 패킷 데이터 네트워크 접속성을 위해 비-병치된 P-GW (237) 에 접속하면 이용될 수도 있다.

[0061] 본 명세서에서 설명된 예시적인 양태들에서, 셀룰러 디바이스는 사물 인터넷 (IoT) 디바이스에 인터페이스될 수도 있다. 예시적인 양태들은 셀룰러 디바이스를 통해 IoT 디바이스와 코어 네트워크 사이에 전송된 데이터 메시지들 (예를 들어, 스몰 데이터 메시지들) 에 관하여 설명된다; 그러나, 본 명세서에서 설명된 양태들은 스몰 데이터 메시지들에 제한되지 않고 다른 타입들의 데이터 메시지들에 적용가능성을 갖는다.

[0062] **예시적인 무상태 액세스 계층 보안 프로세스들**

[0063] 도 4 는 본 개시의 일부 양태들에 따른 액세스 계층 보안 키 유도 및 프로비져닝 프로세스 (400) 의 일 예를 예

시하는 플로우 다이어그램이다. 게이트웨이는 먼저 제 1 키를 획득 (402) (예를 들어, 유도, 생성, 컴퓨팅, 취출, 수신, 요청 등) 할 수도 있다. 게이트웨이는 CIoT 서빙 게이트웨이 노드 (C-SGN) 일 수도 있다. C-SGN 은 CIoT 사용 케이스들에 대한 기능성을 지원하도록 구현될 수 있는 게이트웨이일 수도 있다. C-SGN 은 CIoT 사용 케이스들에 대해 유용한 LTE 이동성 관리 엔티티 (MME), LTE 서빙 게이트웨이 (S-GW), 및 LTE 패킷 데이터 네트워크 게이트웨이 (P-GW) 의 그 양태들을 통합할 수도 있다. 본 명세서에서의 C-SGN 에 대한 언급은 편의를 위한 것이다. 본 명세서에서 설명된 양태들은 게이트웨어로서 C-SGN 을 이용하는 구현들에 제한되지 않는다. 일부 양태들에서, 용어들 C-SGN 및 게이트웨이는 본 명세서에서 상호교환가능하게 사용될 수도 있다.

[0064] 제 1 키는 마스터 액세스 계층 보안 키 (Master Access Stratum security Key; MASK) 로 지칭될 수도 있다. 일부 양태들에서, 제 1 키는 어떤 다른 키로부터 획득되지 않는다. 예를 들어, 제 1 키는 다른 키 재료로부터 유도되지 않는다. 일부 양태들에서, 제 1 키는 C-SGN 에서 랜덤으로 획득될 수도 있다. 예를 들어, 일부 양태들에서, 제 1 키는 C-SGN 에서 랜덤으로 생성될 수도 있다. 제 1 키는 C-SGN 에만 알려져 있을 수도 있다.

[0065] C-SGN 은 다음에 제 2 키를 획득 (404) 할 수도 있다. 제 2 키는 기지국 액세스 계층 보안 키 (BASK) 로 지칭될 수도 있다. 제 2 키는 제 1 키 (예를 들어, MASK) 및 무선 액세스 네트워크 (RAN) 노드 (예를 들어, eNodeB, C-BS) 에 고유한 파라미터로부터 획득될 수도 있다. RAN 노드에 고유한 파라미터는 RAN 노드의 아이덴티티일 수도 있다. 하나의 양태에서, RAN 노드의 아이덴티티는 CIoT 기지국 아이덴티티 (C-BS ID) 일 수도 있다. C-BS ID 는 예를 들어, LTE 에서의 eNodeB ID 와 등가일 수도 있다. 제 2 키는 키 유도 함수 (KDF) 를 이용하여 획득될 수도 있다. 예를 들어, 제 2 키는 다음으로서 주어질 수도 있다:

[0066] 제 2 키 = KDF (MASK, C-BS ID),

[0067] 여기서 KDF 는 키 유도 함수이고, MASK 는 제 1 키이고, 그리고 C-BS ID 는 CIoT 기지국 아이덴티티이다.

[0068] 제 2 키는 게이트웨이에 의해 RAN 노드 (예를 들어, C-BS) 에 프로비져닝 (406) 될 수도 있다. 적어도 제 2 키는 제 1 키 및 무선 액세스 네트워크 (RAN) 노드에 고유한 파라미터에 기초하기 때문에, 제 2 키는 셀룰러 네트워크로의 셀룰러 디바이스의 초기 어태치먼트 전에, 동안, 또는 후에 RAN 노드에 프로비져닝될 수도 있다.

[0069] C-SGN 은 여전히 추가로 제 3 키를 획득할 수도 있다. 제 3 키는 디바이스 액세스 계층 보안 키 (Device Access Stratum security Key; DASK) 로 지칭될 수도 있다. 제 3 키는 제 2 키 (예를 들어, BASK) 및 셀룰러 디바이스에 고유한 파라미터로부터 획득될 수도 있다. 셀룰러 디바이스에 고유한 파라미터는 셀룰러 디바이스의 아이덴티티일 수도 있다. 셀룰러 디바이스의 아이덴티티는 예를 들어, SAE-임시 모바일 가입자 아이덴티티 (S-TMSI) 일 수도 있다.

[0070] 제 3 키는 키 유도 함수 (KDF) 를 이용하여 획득될 수도 있다. 예를 들어, 제 3 키는 다음으로서 주어질 수도 있다:

[0071] 제 3 키 = KDF (BASK, 셀룰러 디바이스 ID),

[0072] 여기서 KDF 는 키 유도 함수이고, BASK 는 제 2 키이며, 그리고 셀룰러 디바이스 ID 는 셀룰러 디바이스의 아이덴티티이다.

[0073] 일부 양태들에서, 게이트웨이 (예를 들어, C-GSN) 는 제 3 키 (예를 들어, DASK) 를 셀룰러 디바이스에 프로비져닝 (410) 할 수도 있다.

[0074] 일부 양태들에서, 셀룰러 디바이스는 스몰 데이터 메시지에 무결성 보호를 추가할 수도 있고, 여기서 무결성 보호는 예를 들어, 제 3 키 (예를 들어, DASK) 및 디바이스의 아이덴티티에 기초할 수도 있다. 셀룰러 디바이스는 추가적으로 또는 대안적으로 스몰 데이터 메시지를 암호화할 수도 있고, 여기서 암호화는 제 3 키 (예를 들어, DASK) 를 이용하여 수행될 수도 있다. 무결성 보호된 및/또는 암호화된 스몰 데이터 메시지는 셀룰러 디바이스로부터 RAN 노드로 전송될 수도 있다.

[0075] 제 3 키는 보안 비-액세스 계층 (NAS) 메시지를 통해 셀룰러 디바이스에 프로비져닝 (예를 들어, 전송) 될 수도 있다 (즉, NAS 보안 모드 커맨드는 완료된다). 보안 NAS 메시지의 하나의 예는 초기 어태치 프로시저의 성공적인 완료 시에 셀룰러 디바이스로 전송된, 어태치 수락 메시지일 수도 있다. 대안으로서, 제 3 키는 암호화된 정보 엘리먼트 (IE) 로서 셀룰러 디바이스로 전송될 수도 있다. 이 대안에서, IE 는 IE 를 암호화하

는데 이용되는 알고리즘을 식별하는 알고리즘 식별자를 포함할 수도 있다.

[0076] 일부 양태들에서, RAN 노드는 디바이스와 액세스 계층 보안 콘텍스트를 확립 및/또는 유지하지 않는다. 액세스 계층 보안 콘텍스트를 확립 및/또는 유지하는 것은 상태 테이블들 및 그 상태 테이블들과 연관된 데이터의 프로세싱의 이용을 요구할 수도 있다. 상태 테이블 및 연관된 프로세싱은, 예를 들어, CIoT 에서 바람직하지 않은, 오버헤드의 소비를 표현할 수도 있다. 실제로, 본 명세서에는 무상태 보안 스킴의 양태들이 개시되어 있다. 예를 들어, RAN 노드는, 게이트웨이 (예를 들어, C-SGN) 에 의해 RAN 노드에 프로비져닝되었던 제 2 키 (예를 들어, BASK) 를 프로세싱한다. 하나의 예에서, RAN 노드는 제 2 키 (예를 들어, BASK) 및 셀룰러 디바이스의 아이덴티티로부터 온-더-플라이로 (예를 들어, 동적으로, 필요에 따라) 제 3 키 (예를 들어, DASK) 를 획득할 수도 있다. 셀룰러 디바이스의 아이덴티티는 RAN 노드에서 획득된 모든 스몰 데이터 메시지와 함께 포함되고 제 2 키는 셀룰러 디바이스의 아이덴티티에 독립적이다; 이에 따라, 보안 스킴은 적어도, 상태 테이블이 필요하지 않다는 점에서 무상태이다.

[0077] RAN 노드는 그 후 디바이스로부터 획득되는 스몰 데이터 메시지들의 무결성을 검증하고 및/또는 그 스몰 데이터 메시지들을 해독하기 위해, 온-더-플라이로 획득 (예를 들어, 유도, 생성) 한 제 3 키 (예를 들어, DASK) 를 이용할 수도 있다. 본 명세서에서 설명된 예시적인 키 생성 및 프로비져닝 스킴들을 이용하면, AS 보안의 측정이 기존의 메시지들의 도움으로 구현될 수도 있다. 오버헤드는 증가되지 않는다. RAN 노드는 그 자체 및 코어 네트워크를 서비스 거부 및/또는 플러딩 공격들과 같은 취약성들로부터 보호할 수도 있다.

[0078] 도 5 는 본 개시의 일부 양태들에 따른 셀룰러 사물 인터넷 (CIoT) 하의 어태치 프로시저의 일 예를 예시하는 호출 플로우 다이어그램 (500) 이다. 도 5 의 양태에는, 셀룰러 디바이스 (502) (예를 들어, CIoT 디바이스), RAN 노드 (504) (예를 들어, C-BS), 코어 네트워크 게이트웨이 (예를 들어, CIoT 서빙 게이트웨이 노드 (C-SGN) (506)), 홈 가입자 서버 (HSS) (508), 및 P-GW (510) 가 포함되어 있다. P-GW (510) 는 셀룰러 디바이스 (502) 가 로밍중인 시나리오들을 위해 묘사된다.

[0079] 도 5 의 예시적인 호출 플로우는 RRC 접속 확립 프로시저가 수행 (520) 될 때 시작될 수도 있다. RRC 접속 확립 프로시저의 수행 동안에, 셀룰러 디바이스 (502) 및 RAN 노드 (504) 는 본 명세서에서 추후에 설명되는 바와 같이 하나 이상의 논스 (nonce) 값들 (예를 들어, 논스-디바이스, 논스-RAN) 및/또는 하나 이상의 타임 스탬프 값들을 서로에 제공할 수도 있다. 셀룰러 디바이스 (502) 는 어태치 요청 (522) 을 전송하는 것에 의해 표시된 어태치 프로시저를 수행할 수도 있다. 어태치 프로시저 동안에, 셀룰러 디바이스 (502) 는 어태치먼트가 CIoT 스몰 데이터 메시지에 대한 것임을 표시할 수도 있다 (예를 들어, "CIoT 어태치 (Attach)" 는 어태치 요청 (522) 의 파라미터로서 포함될 수도 있다). RAN 노드 (504) (예를 들어, C-BS) 는 셀룰러 디바이스 표시에 기초하여 또는 사전-구성에 기초하여 CIoT 에 대해 최적화된 C-SGN (506) 을 선택할 수도 있다. 셀룰러 디바이스 (502) 는 또한 특정 데이터 타입 (예를 들어, IP 및/또는 비-IP 및/또는 SMS) 을 표시할 수도 있다. 액세스 포인트 명칭 (APN) 이 표시될 수도 있다. APN 은 셀룰러 디바이스 (502) 가 접속성을 요청하는 P-GW (510) 및/또는 C-SGN (506) 을 식별할 수도 있고, 그리고 C-SGN (506) 이 로케이트되는 공중 육상 모바일 네트워크 (PLMN) 및/또는 P-GW (510) 가 로케이트되는 PLMN 을 식별하는 APN 오퍼레이터 식별자를 포함할 수도 있다.

[0080] 위에서 표시한 바와 같이, C-SGN (506) 은 RAN 노드 (504) (예를 들어, C-BS) 에 대한 제 2 키 (예를 들어, BASK) 를 획득할 수도 있다. C-SGN (506) 은 NAS 메시지 (524) 에서 RAN 노드 (504) (예를 들어, C-BS) 에 제 2 키를 프로비져닝할 수도 있다.

[0081] C-SGN (506) 은 임의의 필요한 인증/보안 프로시저들 (526) 을 수행할 수도 있다.

[0082] C-SGN (506) 은, 홈 가입자 서버 (508) (HSS) 와, 로케이션 업데이트를 수행할 수도 있고 가입 정보 (528) 를 취출할 수도 있다.

[0083] C-SGN (506) 은 어태치 요청 (522) 을 프로세싱할 수도 있고, 어태치 요청 (522) 과 함께 제공된 파라미터들에 기초하여, IP 베어러 서비스를 확립할 필요성이 있는지를 결정할 수도 있다. 데이터 타입 파라미터가 "IP" 로서 식별되면, PDN 타입은 할당될 IP 어드레스의 타입 (즉, IPv4, IPv6) 을 표시한다. C-SGN (506) 은 어태치 요청 (522) 에서의 PDN 타입에 기초하여 IP 어드레스를 할당할 수도 있다. NAS 세션 관리 시그널링은 필요하지 않을 수도 있다. 로밍 시나리오에서, C-SGN (506) 은 이것이 CIoT 어태치 요청임을 표시하고 데이터 타입 (530) 을 표시하는 세션 생성 요청 (Create Session Request) (또는 새로운 제어 메시지) 를 P-GW 로 전송할 수도 있다. P-GW 는 어태치 요청에서의 PDN 타입에 기초하여 IP 어드레스를 할당할 수도 있다.

[0084] 로밍 시나리오 단독에서, 데이터 타입에 의존하여, P-GW 는 C-SGN (532) 으로 세션 생성 응답 (Create Session response) (또는 새로운 제어 메시지) 을 전송할 수도 있다. IP 데이터 케이스 (예를 들어, 데이터 타입 = IP) 에 대해, 세션 생성 응답은 할당된 IP 어드레스를 포함할 수도 있다.

[0085] C-SGN 은 어떤 세션 관리 메시지 없이 셀룰러 디바이스 (502) 로 어태치 수락 메시지 (534) 를 전송하는 것에 의해 응답할 수도 있다. 데이터 타입 = IP 에 대해, 할당된 IP 어드레스는 셀룰러 디바이스 (502) 로 전송될 수도 있다. 어태치 수락 메시지는 GUTI (Globally Unique Temporary Identifier) 를 포함할 수도 있다. GUTI 는 셀룰러 디바이스 (502) 의 초기 어태치 프로시저 동안에 C-SGN (또는 C-SGN 의 MME 기능) 에 의해 배정될 수도 있다.

[0086] 위에서 표시한 바와 같이, 어태치 프로시저 (예를 들어, 초기 어태치) 동안에, C-SGN (506) 은 셀룰러 디바이스 (502) 에 대한 제 3 키 (예를 들어, DASK) 를 획득할 수도 있다. 일부 양태들에 따르면, C-SGN (506) 은 NAS 메시지에서 (예를 들어, 어태치 수락 메시지 (534) 에서) 셀룰러 디바이스에 제 3 키를 프로비져닝할 수도 있다.

[0087] 셀룰러 디바이스 (502) 는 어태치 완료 메시지 (536) 로 응답할 수도 있다.

[0088] RRC 접속은 릴리즈 (538) 될 수도 있다.

[0089] 도 6 은 본 개시의 양태들에 따른 무상태 액세스 계층 보안 및 보안 키들의 획득 (예를 들어, 유도, 생성, 컴퓨팅, 취출, 수신, 요청 등), 프로비져닝, 및 이용 중 하나 이상을 지원할 수 있는 장치 (600) (예를 들어, 전자 디바이스) 의 하드웨어 구현의 일 예를 예시하는 블록 다이어그램이다. 장치 (600) 는 게이트웨이 (예를 들어, C-SGN), RAN 노드 (예를 들어, 기지국, eNB, C-BS), 셀룰러 디바이스 (예를 들어, CIoT 디바이스), 또는 모바일 폰, 스마트 폰, 태블릿, 휴대용 컴퓨터, 서버, 개인 컴퓨터, 센서, 엔터테인먼트 디바이스, 의료 디바이스, 또는 무선 통신 회로부를 갖는 임의의 다른 전자 디바이스와 같은 무선 통신을 지원하는 일부 다른 타입의 디바이스 내에서 구현될 수 있다.

[0090] 장치 (600) (예를 들어, 통신 장치) 는 통신 인터페이스 (602) (예를 들어, 적어도 하나의 트랜시버), 저장 매체 (604), 사용자 인터페이스 (606), 메모리 디바이스 (608) (예를 들어, 하나 이상의 보안 키들 (618) 을 저장), 및 프로세싱 회로 (610) 를 포함할 수도 있다. 다양한 구현들에서, 사용자 인터페이스 (606) 는, 키패드, 디스플레이, 스피커, 마이크로폰, 터치스크린 디스플레이, 또는 사용자로부터 입력을 수신하거나 또는 사용자로 출력을 전송하기 위한 일부 다른 회로부 중 하나 이상을 포함할 수도 있다.

[0091] 이들 컴포넌트들은 도 6 에서의 접속 라인들로 일반적으로 표현된, 시그널링 버스 (640) 또는 다른 적합한 컴포넌트를 통해 서로에 커플링되고 및/또는 서로 전기 통신하여 배치될 수 있다. 시그널링 버스 (640) 는 프로세싱 회로 (610) 의 특정 애플리케이션 및 전체 설계 제약들에 의존하여 임의의 수의 상호접속 버스들 및 브리지 (bridge) 들을 포함할 수도 있다. 시그널링 버스 (640) 는 통신 인터페이스 (602), 저장 매체 (604), 사용자 인터페이스 (606), 및 메모리 디바이스 (608) 의 각각이 프로세싱 회로 (610) 에 커플링되고 및/또는 그 프로세싱 회로 (610) 와 전기 통신하고 있도록 다양한 회로들을 함께 링크한다. 시그널링 버스 (640) 는 또한, 당업계에 잘 알려져 있기 때문에, 더 이상 설명되지 않을 타이밍 소스들, 주변기기들, 전압 레귤레이터들, 및 전력 관리 회로들과 같은 다양한 다른 회로들 (미도시) 을 링크할 수도 있다.

[0092] 통신 인터페이스 (602) 는 장치 (600) 의 무선 통신을 용이하게 하도록 적응될 수도 있다. 예를 들어, 통신 인터페이스 (602) 는 네트워크에서 하나 이상의 통신 디바이스들에 대하여 양방향으로 정보의 통신을 용이하게 하도록 적응된 회로부 및/또는 프로그래밍을 포함할 수도 있다. 일부 구현들에서, 통신 인터페이스 (602) 는 유선-기반 통신을 위해 고안, 적응, 및/또는 구성될 수도 있다. 일부 구현들에서, 통신 인터페이스 (602) 는 무선 통신 시스템 내에서의 무선 통신을 위해 하나 이상의 안테나들 (612) 에 커플링될 수도 있다. 통신 인터페이스 (602) 는 하나 이상의 스탠드얼론 수신기들 및/또는 송신기들 뿐만 아니라 하나 이상의 트랜시버들로 고안, 적응, 및/또는 구성될 수도 있다. 예시된 예에서, 통신 인터페이스 (602) 는 송신기 (614) 및 수신기 (616) 를 포함한다.

[0093] 메모리 디바이스 (608) 는 하나 이상의 메모리 디바이스들을 표현할 수도 있다. 표시한 바와 같이, 메모리 디바이스 (608) 는 장치 (600) 에 의해 이용되는 다른 정보와 함께 보안 키들 (618) 을 유지할 수도 있다. 일부 구현들에서, 메모리 디바이스 (608) 및 저장 매체 (604) 는 공통 메모리 컴포넌트로서 구현된다. 메모리 디바이스 (608) 는 또한, 프로세싱 회로 (610) 또는 장치 (600) 의 일부 다른 컴포넌트에 의해 조작되는 데이터를 저장하기 위해 이용될 수도 있다.

[0094] 저장 매체 (604) 는 프로세서 실행가능 코드 또는 명령들 (예를 들어, 소프트웨어, 펌웨어), 전자 데이터, 데이터베이스들, 또는 다른 디지털 정보와 같은 프로그래밍을 저장하기 위한 하나 이상의 비일시적 컴퓨터 판독가능, 머신 판독가능, 및/또는 프로세서 판독가능 디바이스들을 표현할 수도 있다. 저장 매체 (604) 는 또한, 프로그래밍을 실행할 때 프로세싱 회로 (610) 에 의해 조작되는 데이터를 저장하기 위해 이용될 수도 있다. 저장 매체 (604) 는 휴대용 또는 고정된 저장 디바이스들, 광 저장 디바이스들, 및 프로그래밍을 저장, 포함 또는 반송하는 것이 가능한 다양한 다른 매체를 포함하는, 범용 또는 특수 목적 프로세서에 의해 액세스될 수 있는 임의의 이용가능한 매체들일 수도 있다.

[0095] 제한이 아닌 일 예로, 저장 매체 (604) 는 자기 저장 디바이스 (예를 들어, 하드 디스크, 플로피 디스크, 자기 스트립), 광 디스크 (예를 들어, 콤팩트 디스크 (CD) 또는 디지털 다기능 디스크 (DVD)), 스마트 카드, 플래시 메모리 디바이스 (예를 들어, 카드, 스틱, 또는 키 드라이브), 랜덤 액세스 메모리 (RAM), 판독 전용 메모리 (ROM), 프로그래밍가능 ROM (PROM), 소거가능한 PROM (EPROM), 전기적으로 소거가능한 PROM (EEPROM), 레지스터, 착탈식 디스크, 및 컴퓨터에 의해 액세스 및 판독될 수도 있는 소프트웨어 및/또는 명령들을 저장하기 위한 임의의 다른 적합한 매체를 포함할 수도 있다. 저장 매체 (604) 는 제조물 (예를 들어, 컴퓨터 프로그램 제품) 에서 구현될 수도 있다. 일 예로, 컴퓨터 프로그램 제품은 패키징 재료들에 컴퓨터 판독가능 매체를 포함시킬 수도 있다. 상기 관점에서, 일부 구현들에서, 저장 매체 (604) 는 비일시적 (예를 들어, 유형의) 저장 매체일 수도 있다.

[0096] 저장 매체 (604) 는 프로세싱 회로 (610) 가 저장 매체 (604) 로부터 정보를 판독하고 그 저장 매체에 정보를 기입할 수 있도록 프로세싱 회로 (610) 에 커플링될 수도 있다. 즉, 저장 매체 (604) 는 적어도 하나의 저장 매체가 프로세싱 회로 (610) 와 일체형인 예들 및/또는 적어도 하나의 저장 매체가 프로세싱 회로 (610) 와 별개인 (예를 들어, 장치 (600) 에 상주하는, 장치 (600) 외부에 있는, 다수의 엔티티들에 걸쳐 분산되는 등등인) 예들을 포함하여, 저장 매체 (604) 가 프로세싱 회로 (610) 에 의해 적어도 액세스가능하도록 프로세싱 회로 (610) 에 커플링될 수 있다.

[0097] 저장 매체 (604) 에 의해 저장된 프로그래밍은, 프로세싱 회로 (610) 에 의해 실행될 때, 프로세싱 회로 (610) 로 하여금, 본 명세서에서 설명된 다양한 기능들 및/또는 프로세스 동작들 중 하나 이상을 수행하게 한다. 예를 들어, 저장 매체 (604) 는 프로세싱 회로 (610) 의 하나 이상의 하드웨어 블록들에서의 동작들을 레귤레이팅하기 위해, 뿐만 아니라 예를 들어 그들 개별의 통신 프로토콜들을 활용하는 무선, 또는 일부 구현들에서 유선 통신을 위해 통신 인터페이스 (602) 를 활용하도록 구성된 동작들을 포함할 수도 있다.

[0098] 프로세싱 회로 (610) 는 일반적으로 저장 매체 (604) 상에 저장된 이러한 프로그래밍의 실행을 포함하는, 프로세싱을 위해 적응된다. 본 명세서에서 사용한 바와 같이, 용어들 "코드" 또는 "프로그래밍" 은, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 하드웨어 기술 언어, 또는 다른 것으로 지칭되든 간에, 명령들, 명령 세트들, 데이터, 코드, 코드 세그먼트들, 프로그램 코드, 프로그램들, 프로그래밍, 서브프로그램들, 소프트웨어 모듈들, 애플리케이션들, 소프트웨어 애플리케이션들, 소프트웨어 패키지들, 루틴들, 서브루틴들, 오브젝트들, 실행가능물들, 실행 스레드들, 프로시저들, 함수들 등을 제한 없이 포함하는 것으로 광범위하게 해석되어야 한다.

[0099] 프로세싱 회로 (610) 는 데이터, 제어 데이터 액세스 및 스토리지를 획득, 프로세싱 및/또는 전송하고, 커맨드들을 이슈하고, 그리고 다른 원하는 동작들을 제어하도록 배열될 수도 있다. 프로세싱 회로 (610) 는 적어도 하나의 예에서 적절한 매체들에 의해 제공된 원하는 프로그래밍을 구현하도록 고안, 적응, 및/또는 구성된 회로부를 포함할 수도 있다. 예를 들어, 프로세싱 회로 (610) 는 하나 이상의 프로세서들, 하나 이상의 제어기들, 및/또는 실행가능 프로그래밍을 실행하도록 고안, 적응, 및/또는 구성된 다른 구조로서 구현될 수도 있다. 프로세싱 회로 (610) 의 예들은 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적 회로 (ASIC), 필드 프로그래밍가능 게이트 어레이 (FPGA) 또는 다른 프로그래밍가능 로직 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본 명세서에서 설명된 기능들을 수행하도록 설계된 그 임의의 조합을 포함할 수도 있다. 범용 프로세서는 마이크로프로세서, 뿐만 아니라 임의의 종래의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신을 포함할 수도 있다. 프로세싱 회로 (610) 는 또한 DSP 와 마이크로프로세서의 조합, 다수의 마이크로프로세서들, DSP 코어, ASIC 및 마이크로프로세서와 결합된 하나 이상의 마이크로프로세서들, 또는 임의의 다른 수의 다양한 구성들과 같은 컴퓨팅 컴포넌트들의 조합으로서 구현될 수도 있다. 프로세싱 회로 (610) 의 이들 예들은 예시를 위한 것이며 본 개시의 범위 내의 다른 적합한 구성들이 고려된다.

[0100] 본 개시의 하나 이상의 양태들에 따르면, 프로세싱 회로 (610) 는 본 명세서에서 설명된 장치들 중 임의의 것 또는 전부에 대한 피처들, 프로세스들, 기능들, 동작들 및/또는 루틴들 중 임의의 것 또는 전부를 수행하도록 적응될 수도 있다. 예를 들어, 프로세싱 회로 (610) 는 도 4, 도 5, 도 7, 도 9 내지 도 12, 및 도 14 에 대하여 식별된 블록들에서 설명된 동작들 중 임의의 하나를 수행 및/또는 이행하도록 적응될 수도 있다. 본 명세서에서 사용한 바와 같이, 프로세싱 회로 (610) 에 관한 용어 "적응된" 은 프로세싱 회로 (610) 가 본 명세서에서 설명된 다양한 피처들에 따라 특정한 프로세스, 기능, 동작, 및/또는 루틴을 수행하도록 고안, 구성, 채용, 구현, 및/또는 프로그래밍되는 것 중 하나 이상을 행하는 것을 지칭할 수도 있다.

[0101] 프로세싱 회로 (610) 는 도 4, 도 5, 도 7, 도 9 내지 도 12, 및 도 14 에 대하여 식별된 블록들에서 설명된 동작들 중 임의의 하나를 수행 및/또는 이행하기 위한 수단 (예를 들어, 위한 구조) 로서 서빙하는 주문형 집적 회로 (ASIC) 와 같은 전문화된 프로세서일 수도 있다. 프로세싱 회로 (610) 는 송신하기 위한 수단 및/또는 수신하기 위한 수단의 하나의 예로서 서빙할 수도 있다.

[0102] 장치 (600) 의 적어도 하나의 예에 따르면, 프로세싱 회로 (610) 는 통신하기 위한 회로/모듈 (620), 결정하기 위한 회로/모듈 (622), 프로비져닝하기 위한 회로/모듈 (624), 전송하기 위한 회로/모듈 (626), 대기하기 위한 회로/모듈 (628), 또는 획득하기 위한 회로/모듈 (629) 중 하나 이상을 포함할 수도 있다.

[0103] 위에서 언급한 바와 같이, 저장 매체 (604) 에 의해 저장된 프로그래밍은, 프로세싱 회로 (610) 에 의해 실행될 때, 프로세싱 회로 (610) 로 하여금, 본 명세서에서 설명된 다양한 기능들 및/또는 프로세스 동작들 중 하나 이상을 수행하게 한다. 예를 들어, 저장 매체 (604) 는 통신하기 위한 코드 (630), 결정하기 위한 코드 (632), 프로비져닝하기 위한 코드 (634), 전송하기 위한 코드 (636), 대기하기 위한 코드 (638), 또는 획득하기 위한 코드 (639) 중 하나 이상을 포함할 수도 있다.

[0104] 도 7 은 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 프로세스 (700) 의 일 예를 예시하는 플로우 다이어그램이다. 무상태 액세스 계층 보안 프로세스 (700) 는 게이트웨이 (예를 들어, C-SGN) 또는 일부 다른 적합한 장치에 로케이트될 수도 있는, 프로세싱 회로 (예를 들어, 도 6 의 프로세싱 회로 (610)) 내에서 일어날 수도 있다. 이에 따라, 무상태 액세스 계층 보안 프로세스 (700) 는 게이트웨이 (예를 들어, C-SGN) 또는 일부 다른 적합한 장치에서 동작가능할 수도 있다. 본 개시의 범위 내의 다양한 양태들에서, 무상태 액세스 계층 보안 프로세스 (700) 는 본 개시의 하나 이상의 양태들에 따른 보안 키들을 획득, 프로비져닝, 및 이용 중 하나 이상을 포함하여 무상태 액세스 계층 보안을 지원하는 것이 가능한 임의의 적합한 장치에 의해 구현될 수도 있다.

[0105] 일부 양태들에 따르면, 무상태 액세스 계층 보안 프로세스 (700) 는 장치 (예를 들어, 게이트웨이, C-SGN) 에서, 장치에만 알려져 있는 제 1 키를 획득 (702) 하는 것을 포함할 수도 있는, 통신의 방법으로서 설명될 수도 있다. 장치에서, 제 1 키 및 무선 액세스 네트워크 (RAN) 노드에 고유한 파라미터에 기초하는 (예를 들어, 이들을 이용하여 유도되는, 이들을 이용하여 생성되는) 제 2 키를 획득 (704) 하는 것. 장치에 의해, 제 2 키를 RAN 노드에 프로비져닝 (706) 하는 것. 장치에서, 제 2 키 및 셀룰러 디바이스에 고유한 파라미터에 기초하는 제 3 키를 획득 (708) 하는 것. 그리고 장치에 의해, 제 3 키를 셀룰러 디바이스에 프로비져닝 (710) 하는 것을 더 포함할 수도 있다.

[0106] 일부 양태들에 따르면, 장치 (예를 들어, 게이트웨이, C-SGN, 통신 장치) 는 장치에만 알려져 있는 제 1 키 (예를 들어, 마스터 액세스 계층 보안 키 - MASK) 를 획득 (702) 할 수도 있다. 일부 양태들에서, 제 1 키는 어떤 다른 키로부터 획득되지 않을 수도 있다. 다시 말해서, 장치는 어떤 다른 키로부터 제 1 키를 획득할 수 없을 시에 제 1 키를 획득할 수도 있다. 일부 양태들에서, 장치는 제 1 키를 랜덤으로 생성할 수도 있다. 다시 말해서, 장치는 장치에서 제 1 키를 랜덤으로 생성하는 것에 의해 제 1 키를 획득할 수도 있다. 일부 양태들에서, 장치는 셀룰러 사물 인터넷 서빙 게이트웨이 노드 (C-SGN) 일 수도 있다. 일부 양태들에서, 단지 장치 (예를 들어, 게이트웨이, C-SGN) 만이 제 1 키 (예를 들어, MASK) 를 알고 있다. 다시 말해서, 일부 양태들에서, 제 1 키는 장치에만 알려져 있다.

[0107] 장치는 제 1 키 및 무선 액세스 네트워크 (RAN) 노드에 고유한 파라미터에 기초할 수도 있는 제 2 키 (예를 들어, 마스터 액세스 계층 보안 키 - MASK) 를 획득 (704) 할 수도 있다. 일부 양태들에서, RAN 노드에 고유한 파라미터는 RAN 노드의 아이덴티티일 수도 있다. 일부 양태들에서, RAN 노드는 CIoT 기지국 (C-BS) 또는 진화된 노드 B (eNodeB) 일 수 있고, 그리고 RAN 노드에 고유한 파라미터는 C-BS 아이덴티티 또는 eNodeB 아이덴티티일 수 있다. 일부 양태들에서, 키 유도 함수는 제 2 키를 획득 (예를 들어, 유도, 생성) 하는데 이용

될 수도 있다.

[0108] 장치는 제 2 키를 RAN 노드에 프로비져닝 (706) 할 수도 있다. 일부 양태들에서, 장치는 비-액세스 계층 (NAS) 메시지에서 제 2 키를 RAN 노드에 프로비져닝할 수도 있다. 일부 양태들에서, 비-액세스 계층 메시지는 보안 NAS 메시지일 수도 있다.

[0109] 장치는 제 2 키 및 셀룰러 디바이스에 고유한 파라미터에 기초할 수도 있는 제 3 키 (예를 들어, 디바이스 액세스 계층 보안 키 - DASK) 를 획득 (708) 할 수도 있다. 일부 양태들에서, 셀룰러 디바이스에 고유한 파라미터는 셀룰러 디바이스 아이덴티티일 수도 있다. 일부 양태들에서, 셀룰러 디바이스에 고유한 파라미터는 시스템 아키텍처 진화 (System Architecture Evolution; SAE) 임시 모바일 가입자 아이덴티티 (S-TMSI) 일 수도 있다. S-TMSI 는 MME 그룹 내의 셀룰러 디바이스를 로컬로 식별하는데 이용될 수도 있다. S-TMSI 는 셀룰러 디바이스를 페이징하는데 있어서 이용될 수도 있다. S-TMSI 는 MME 코드 및 MME 모바일 가입자 아이덴티티 (M-TMSI) 로 구성될 수도 있다. 일부 양태들에서, 키 유도 함수는 제 3 키를 획득 (예를 들어, 유도, 생성) 하는데 이용될 수도 있다.

[0110] 장치는 제 3 키를 셀룰러 디바이스에 프로비져닝 (710) 할 수도 있다. 일부 양태들에서, 장치는 비-액세스 계층 (NAS) 메시지에서 제 3 키를 셀룰러 디바이스에 프로비져닝할 수도 있다. 일부 양태들에서, 비-액세스 계층 메시지는 보안 NAS 메시지일 수도 있다. 일부 양태들에서, 비-액세스 계층 메시지는 어태치 수락 메시지일 수도 있다. 일부 양태들에서, 장치는 암호화된 정보 엘리먼트 (IE) 로서 제 3 키를 셀룰러 디바이스에 프로비져닝할 수도 있다. IE 는 IE 를 암호화하는데 이용되는 알고리즘을 식별하는 알고리즘 식별자를 포함할 수도 있다.

[0111] 도 8 은 본 개시의 양태들에 따른 무상태 액세스 계층 보안 및 보안 키들의 획득, 프로비져닝, 및 이용 중 하나 이상을 지원할 수도 있는 장치 (800) (예를 들어, 전자 디바이스, 통신 장치) 의 하드웨어 구현의 다른 예를 예시하는 블록 다이어그램이다. 장치 (800) 는 게이트웨이 (예를 들어, C-SGN), RAN 노드 (예를 들어, eNB, C-BS), 셀룰러 디바이스 (예를 들어, CIoT 디바이스), 또는 모바일 폰, 스마트 폰, 태블릿, 휴대용 컴퓨터, 서버, 개인 컴퓨터, 센서, 엔터테인먼트 디바이스, 의료 디바이스, 또는 무선 통신 회로부를 갖는 임의의 다른 전자 디바이스와 같은 무선 통신을 지원하는 일부 다른 타입의 디바이스 내에서 구현될 수 있다.

[0112] 장치 (800) 는 통신 인터페이스 (예를 들어, 적어도 하나의 트랜시버) (802), 저장 매체 (804), 사용자 인터페이스 (806), 메모리 디바이스 (808) (예를 들어, 하나 이상의 보안 키들 (818) 을 저장), 및 프로세싱 회로 (810) 를 포함할 수도 있다. 다양한 구현들에서, 사용자 인터페이스 (806) 는, 키패드, 디스플레이, 스피커, 마이크로폰, 터치스크린 디스플레이, 또는 사용자로부터 입력을 수신하거나 또는 사용자로 출력을 전송하기 위한 일부 다른 회로부 중 하나 이상을 포함할 수도 있다. 일반적으로, 도 8 의 컴포넌트들은 도 6 의 장치 (600) 의 대응하는 컴포넌트들과 유사할 수도 있다.

[0113] 본 개시의 하나 이상의 양태들에 따르면, 프로세싱 회로 (810) 는 본 명세서에서 설명된 장치들 중 임의의 것 또는 전부에 대한 피처들, 프로세스들, 기능들, 동작들, 및/또는 루틴들 중 임의의 것 또는 전부를 수행하도록 적응될 수도 있다. 예를 들어, 프로세싱 회로 (810) 는 도 4, 도 5, 도 7, 도 9 내지 도 12, 및 도 14 에 대하여 설명된 블록들 중 임의의 것을 수행하도록 적응될 수도 있다. 본 명세서에서 사용한 바와 같이, 프로세싱 회로 (810) 에 관한 용어 "적응된" 은 프로세싱 회로 (810) 가 본 명세서에서 설명된 다양한 피처들에 따라 특정한 프로세스, 기능, 동작, 및/또는 루틴을 수행하도록 고안, 구성, 채용, 구현, 및/또는 프로그래밍되는 것 중 하나 이상을 행하는 것을 지칭할 수도 있다.

[0114] 프로세싱 회로 (810) 는 도 4, 도 5, 도 7, 도 9 내지 도 12, 및 도 14 와 함께 설명된 동작들 중 임의의 하나를 이행하기 위한 수단 (예를 들어, 위한 구조) 로서 서빙하는 주문형 집적 회로 (ASIC) 와 같은 전문화된 프로세서일 수도 있다. 프로세싱 회로 (810) 는 송신하기 위한 수단 및/또는 수신하기 위한 수단의 하나의 예로서 서빙할 수도 있다.

[0115] 장치 (800) 의 적어도 하나의 예에 따르면, 프로세싱 회로 (810) 는 통신하기 위한 회로/모듈 (820), 수신하기 위한 회로/모듈 (822), 비교하기 위한 회로/모듈 (824), 폐기하기 위한 회로/모듈 (826), 전송하기 위한 회로/모듈 (828), 획득하기 위한 회로/모듈 (830), 해독하기 위한 회로/모듈 (832), 검증하기 위한 회로/모듈 (834), 검출하기 위한 회로/모듈 (836), 또는 모니터링하기 위한 회로/모듈 (838) 중 하나 이상을 포함할 수도 있다.

[0116] 위에서 언급한 바와 같이, 저장 매체 (804) 에 의해 저장된 프로그래밍은, 프로세싱 회로 (810) 에 의해 실행될 때, 프로세싱 회로 (810) 로 하여금, 본 명세서에서 설명된 다양한 기능들 및/또는 프로세스 동작들 중 하나 이

상을 수행하게 할 수도 있다. 예를 들어, 저장 매체 (804) 는 통신하기 위한 코드 (840), 수신하기 위한 코드 (842), 비교하기 위한 코드 (844), 폐기하기 위한 코드 (846), 전송하기 위한 코드 (848), 획득하기 위한 코드 (850), 해독하기 위한 코드 (852), 검증하기 위한 코드 (854), 검출하기 위한 코드 (856), 또는 모니터링하기 위한 코드 (858) 중 하나 이상을 포함할 수도 있다.

[0117] 도 9 는 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 보호된 통신의 방법 (900) 의 일 예를 예시하는 플로우 다이어그램이다. 무상태 액세스 계층 보안 보호된 통신의 방법 (900) 은 무선 액세스 네트워크 (RAN) 노드 (예를 들어, eNB, C-BS) 또는 일부 다른 적합한 장치에 로케이트될 수도 있는 프로세싱 회로 (예를 들어, 도 8 의 프로세싱 회로 (810)) 내에서 일어날 수도 있다. 이에 따라, 무상태 액세스 계층 보안 보호된 통신의 방법 (900) 은 RAN 노드 또는 일부 다른 적합한 장치에서 동작가능할 수도 있다. 본 개시의 범위 내의 다양한 양태들에서, 무상태 액세스 계층 보안 보호된 통신의 방법 (900) 은 본 개시의 하나 이상의 양태들에 따른 보안 키들을 획득하는 것, 프로비져닝하는 것, 및 이용하는 것 중 하나 이상을 포함하여 무상태 액세스 계층 보안을 지원하는 것이 가능한 임의의 적합한 장치에 의해 구현될 수도 있다.

[0118] 도 9 의 양태에서, 셀룰러 디바이스가 RAN 노드 (예를 들어, eNB, C-BS) 로 스몰 데이터 메시지를 전송할 때, 셀룰러 디바이스는 초기 어태치 프로시저 동안에 게이트웨이 (예를 들어, C-SGN) 에 의해 셀룰러 디바이스에 프로비져닝된 제 3 키 (예를 들어, DASK) 를 이용하여 스몰 데이터 메시지를 보호 (예를 들어, 무결성 보호 및/또는 암호화) 할 수도 있다. 제 3 키로 보호된 (예를 들어, 무결성 보호된 및/또는 암호화된) 스몰 데이터 메시지는 본 명세서에서 "보호된 메시지" 로 지칭될 수도 있다. 제 3 키는 제 2 키 (예를 들어, BASK) 및 셀룰러 디바이스의 아이덴티티에 기초할 수도 있다. 제 2 키는 디바이스가 보호된 메시지를 RAN 노드로 전송하기 전에, 동안, 또는 후에 게이트웨이에 의해 RAN 노드에 프로비져닝될 수도 있다. 제 2 키는 RAN 노드에서, 예를 들어, 장기 메모리 디바이스 (예를 들어, 도 8 의 메모리 디바이스 (808)), 임시 메모리, 또는 캐시에 저장될 수도 있다.

[0119] RAN 노드가 셀룰러 디바이스로부터 보호된 메시지를 수신할 때, RAN 노드는 메시지가 무결성 보호 값 (예를 들어, 메시지 인증 코드 (MAC), 토큰) 을 포함한다고 결정할 수도 있다. RAN 노드는, 예를 들어, RAN 노드가 RAN 노드에 알려지거나 또는 이용가능한 아이템들 (예를 들어, 제 2 키, 디바이스 ID) 로부터 온-더-플라이로 획득 (예를 들어, 유도, 생성) 할 수도 있는 제 3 키를 이용하여 무결성 보호 값을 검증할 수도 있다. 예를 들어, 서술한 바와 같이, 제 3 키는 제 2 키 (예를 들어, BASK) 및 셀룰러 디바이스의 아이덴티티 (예를 들어, 디바이스 ID, S-TMSI) 에 기초할 (예를 들어, 이들을 이용하여 유도될, 이들을 이용하여 생성될) 수도 있다. 제 2 키는 게이트웨이로부터 RAN 노드에 프로비져닝될 수도 있는 한편, 셀룰러 디바이스의 아이덴티티 (예를 들어, S-TMSI) 는 RAN 노드에 의해 수신된 스몰 데이터 메시지에 포함될 수도 있다.

[0120] 본 명세서에서 설명된 예시적인 양태들에 따르면, 제 2 키 (예를 들어, BASK) 는 셀룰러-디바이스-특정적 (cellular-device-specific) 이 아닐 수도 있다 (예를 들어, 제 2 키는 주어진 셀룰러 디바이스에 고유하지 않을 수도 있다). 비록 제 3 키가 셀룰러-디바이스-특정적일 수도 있더라도, RAN 노드 (예를 들어, 기지국, eNB, C-BS) 는 액세스 계층 보안을 구현하기 위해 셀룰러 디바이스에 대한 보안 콘텍스트 (UE 상태, 셀룰러 디바이스 상태) 를 유지하도록 강요되지 않는다. 그 대신, 셀룰러 디바이스로부터의 보호된 메시지를 검증 및/또는 해독하기 위해, RAN 노드는 제 2 키 (예를 들어, BASK) 및 디바이스 ID 를 이용하여 제 3 키를 온-더-플라이로 획득하고, 제 3 키를 이용하여 셀룰러 디바이스로부터의 보호된 메시지를 검증 및/또는 해독할 수도 있다. 제 2 키는 RAN 노드가 연관되는 각각의 게이트웨이 (예를 들어, C-SGN) 에 의해 RAN 노드에 제공될 수도 있다. 디바이스 ID 는, 검증 및/또는 해독될 스몰 데이터 메시지와 함께 포함될 수도 있다. RAN 노드는 RAN 노드가 셀룰러 디바이스로부터 보호된 메시지를 수신할 때 온-더-플라이로 셀룰러 디바이스의 제 3 키를 획득 (예를 들어, 유도, 생성, 컴퓨팅, 취출, 수신, 요청 등) 할 수도 있다. 이에 따라, 제 3 키 (예를 들어, DASK) 를 획득하는 것에 관련된 예시적인 액세스 계층 보안 스킴은 무상태이다.

[0121] 일부 구현들에서, 제 2 키는 RAN-노드-특정적 (RAN-node-specific) 일 수도 있다. 다른 구현들에서, 제 2 키는 RAN-노드-그룹-특정적일 수도 있다 (예를 들어, 복수의 RAN 노드들은 공통 그룹 식별자를 가질 수도 있다). 제 2 키가 RAN-노드-그룹-특정적인 구현들에서, 제 2 키는 주어진 그룹에서 복수의 RAN 노드들 간에 공유될 수도 있다. 제 2 키가 복수의 RAN 노드들 간에 공유될 때, 셀룰 디바이스가 주어진 그룹에서 상이한 RAN 노드들에 접속하는 경우라도, 셀룰러 디바이스는 주어진 그룹에서 조우되는 각각의 RAN 노드에 대해 게이트웨이 (예를 들어, C-SGN) 로부터 새로운 제 3 키 (예를 들어, DASK) 를 획득할 필요가 없을 수도 있다. 따라서, 제 1 키 (예를 들어, MASK) 및 RAN 노드 아이덴티티 (예를 들어, eNB ID) 에 기초하여 제 2 키 (예를 들어, BASK) 를 획득 (예를 들어, 유도, 생성) 하는 대신에, 게이트웨이 (예를 들어, C-SGN) 는 제 1 키 (예를 들

어, MASK) 및 RAN 노드 그룹 아이덴티티로부터 제 2 키 (예를 들어, BASK) 를 획득할 수도 있다. 다시 말해서, 주어진 RAN 노드 그룹 (즉, 주어진 RAN 노드 그룹) 의 커버리지 내에서, 주어진 그룹의 RAN 노드들은 동일한 제 2 키 (예를 들어, BASK) 를 공유한다. 이에 따라, 셀룰러 디바이스 (예를 들어, CIoT 디바이스, UE) 는 주어진 RAN 노드 그룹의 커버리지 내에서 전송된 스몰 데이터 메시지들을 보호하기 위해 (및/또는 그 커버리지 내에서 수신된 스몰 데이터 메시지들을 검증 및/또는 해독하기 위해) 주어진 RAN 노드 그룹에서 복수의 RAN 노드들에 공통인 제 3 키 (예를 들어, DASK) 를 이용할 수 있다. 일부 구현들에서, 네트워크는 RAN 노드 그룹을 구성하고 RAN 노드 그룹의 이용가능성을 시스템 정보 (SI) 의 부분으로서 공지할 수도 있다.

[0122] 일부 양태들에 따르면, 무상태 액세스 계층 보안 보호된 통신의 방법 (900) 은 보안 보호된 통신의 방법으로서 설명될 수도 있다. 무상태 액세스 계층 보안 보호된 통신은 예를 들어, 무결성 보호 및/또는 사이퍼링 (일반적으로 본 명세서에서는 암호화 또는 해독으로 지칭됨) 으로 통신을 보호할 수도 있다. 그 방법은, 장치 (예를 들어, RAN 노드, C-BS, eNB) 에서, 제 1 키 및 장치에 고유한 파라미터에 기초하는 (예를 들어, 이들을 이용하여 유도되는, 이들을 이용하여 생성되는) 제 2 키를 획득 (902) 하는 단계를 포함할 수도 있다. 장치에서, 디바이스 아이덴티티 및 제 1 무결성 보호 값을 포함하는 스몰 데이터 메시지를 획득 (904) 하는 것. 장치에서, 제 2 키 및 디바이스 아이덴티티에 기초하는 제 3 키를 획득 (906) 하는 것. 장치에서, 제 3 키를 이용하여 획득된 (예를 들어, 유도된, 생성된) 제 2 무결성 보호 값을 획득 (908) 하는 것. 무결성 보호 프로세스들은 제 3 키를 이용하여 (무결성 보호 값들을 산출하기 위해) 수행될 수도 있고, 예를 들어, 보호되는 디바이스 아이덴티티, 하나 이상의 논스들, 및 스몰 데이터 메시지를 이용하여 추가로 수행될 수도 있다. 장치에서, 제 1 무결성 보호 값과 제 2 무결성 보호 값을 비교 (910) 하는 것. 비교 결과를 획득/제 1 무결성 보호 값이 제 2 무결성 보호 값과 동일한지를 결정 (912) 하는 것. 장치로부터, 제 1 무결성 보호 값이 제 2 무결성 보호 값과 동일하지 않다는 것을 비교 결과가 표시하면 스몰 데이터 메시지를 폐기 (914) 하는 것. 대안적으로, 장치로부터, 제 1 무결성 보호 값이 제 2 무결성 보호 값과 동일하다는 것을 비교 결과가 표시하면 스몰 데이터 메시지를 게이트웨이로 전송 (916) 하는 것.

[0123] 일부 양태들에 따르면, 장치 (예를 들어, RAN 노드, C-BS, eNB) 는 제 2 키 (예를 들어, BASK) 를 획득할 수도 있고, 여기서 제 2 키는 제 1 키 및 장치에 고유한 파라미터에 기초한다 (902). 일부 양태들에서, 제 2 키는 게이트웨이로부터 획득된다. 일부 양태들에서, 제 1 키는 게이트웨이에만 알려져 있다. 일부 양태들에서, 게이트웨이는 C-SGN 이다. 일부 양태들에서, RAN 노드에 고유한 파라미터는 RAN 노드의 아이덴티티이다. 예를 들어, RAN 노드는 CIoT 기지국 (C-BS) 또는 진화된 노드 B (eNodeB) 일 수도 있고, RAN 노드에 고유한 파라미터는 C-BS 아이덴티티 또는 eNodeB 아이덴티티일 수도 있다.

[0124] 장치 (편의를 위해 "장치" 로 지칭되거나 또는 대안적으로는 다음에 오는 도 9 의 설명과 연관하여 "RAN 노드" 로 지칭됨) 는 디바이스 아이덴티티 및 제 1 무결성 보호 값을 포함하는 스몰 데이터 메시지를 수신 (904) 할 수도 있다.

[0125] 장치는 제 2 키 및 디바이스 아이덴티티에 기초하는 제 3 키 (예를 들어, DASK) 를 획득 (906) 할 수도 있다.

[0126] 장치는 제 3 키를 이용하여 제 2 무결성 보호 값을 획득 (908) 할 수도 있다.

[0127] 하나의 양태에서, 제 1 및 제 2 무결성 보호 값들은 토큰에 주어진 (예를 들어, 이에 기인한, 이로부터 계산된) 값들일 수도 있다. 하나의 양태에서, 제 1 및 제 2 무결성 보호 값들은 메시지 인증 코드 (MAC) 에 주어진 값들일 수도 있다. 본 명세서에서 사용한 바와 같이, 토큰 및/또는 MAC 은 무결성 보호 파라미터로 지칭될 수도 있다. 예를 들어, 본 명세서에서 설명된 AS 보안 보호의 양태들이 (예를 들어, 디바이스로부터 RAN 노드로의) 업링크 트래픽을 위해 이용되는 시나리오들에서, RAN 노드는 AS 보안 보호에서의 이용을 위해 디바이스에 논스 (예를 들어, 논스-RAN) 를 제공할 필요가 있을 수도 있다. 이러한 시나리오에서, 아래에 나타낸 바와 같은 MAC 이 이용될 수도 있다:

[0128] MAC = F (DASK, S-TMSI | 논스-RAN | 메시지).

[0129] 하나의 대안에 따르면, MAC 를 획득하기 위한 다른 방식은 다음의 식들을 이용할 수도 있다:

[0130] K_{MAC} = KDF (DASK, 논스-RAN), 여기서 K_{MAC} 는 DASK 및 논스-RAN 에 기초하여 획득된 원-타임 (one-time) MAC 생성 키이고; KDF 는 키 유도 함수이다.

[0131] MAC = F (K_{MAC}, 메시지).

[0132] 또 다른 대안에 따르면, 다수의 메시지들이 단일 접속 (예를 들어, RRC 접속) 을 위해 전송되는 경우를 고려하

기 위해, 카운터가 각각의 메시지의 MAC, 즉,

[0133] MAC = F (K_{MAC}, 카운터 | 메시지)

[0134] 를 생성하도록 통합될 수도 있고, 여기서 카운터는 새로운 키 (즉, K_{MAC}) 가 유도될 때 (예를 들어, 0 으로) 초기화되고 접속을 위한 모든 단일 메시지에 대해 소정의 값 (예를 들어, 1) 만큼 증가된다.

[0135] 또 다른 대안에서, 본 명세서에서 설명된 AS 보안 보호의 양태들이 (예를 들어, 디바이스로부터 RAN 노드로의) 업링크 트래픽 및/또는 (예를 들어, RAN 노드로부터 디바이스로의) 다운링크 트래픽을 위해 이용되는 시나리오들에서, 디바이스는 AS 보안 보호에서의 이용을 위해 RAN 노드에 논스 (예를 들어, 논스-디바이스) 를 제공할 필요가 있을 수도 있다. 이러한 시나리오에서, 아래에 나타낸 바와 같은 MAC 이 이용될 수도 있으며:

[0136] MAC = F (DASK, S-TMSI | 논스-디바이스 | 논스-RAN | 메시지),

[0137] 여기서 위에서 나타낸 모든 식들에 대해, F 는 MAC 생성 함수 (예를 들어, CMAC, HMAC) 이고 ("F" 는 대안적으로는 본 명세서에서 무결성 보호 알고리즘으로 지칭될 수도 있다), DASK 는 제 2 키의 일 예이고, S-TMSI 는 셀룰러 디바이스의 아이덴티티의 일 예이고, 논스-디바이스는 한번만 사용될 수도 있고 디바이스에 의해 제공되는 제 1 임의의 수 (arbitrary number) 이고, 논스-RAN 은 한번만 사용될 수도 있고 RAN 노드에 의해 제공되는 제 2 임의의 수이고, 그리고 메시지는 전송되는 메시지 (예를 들어, 스몰 데이터 메시지) 이다.

[0138] 다른 대안에 따르면, MAC 를 획득하기 위한 다른 방식이 다음의 식들을 이용할 수도 있다:

[0139] K_{MAC} = KDF (DASK, S-TMSI | 논스-디바이스 | 논스-RAN), 여기서 K_{MAC} 은 DASK, 논스-디바이스 및 논스-RAN 에 기초하여 획득된 원-타임 MAC 생성 키이고; 그리고 KDF 는 키 유도 함수이다.

[0140] MAC = F (K_{MAC}, 메시지)

[0141] 또 다른 대안에 따르면, 다수의 메시지들이 단일 접속 (예를 들어, RRC 접속) 을 위해 전송되는 경우를 고려하기 위해, 카운터가 각각의 메시지의 MAC, 즉

[0142] MAC = F (K_{MAC}, 카운터 | 메시지)

[0143] 를 생성하도록 통합될 수도 있고, 여기서 카운터는 새로운 키 (즉, K_{MAC}) 가 유도될 때 (예를 들어, 0 으로) 초기화되고 접속을 위한 모든 단일 메시지에 대해 소정의 값 (예를 들어, 1) 만큼 증가된다.

[0144] 무결성 보호 파라미터 (예를 들어, MAC, 토큰) 는 재전송 공격 (reply attack) 들을 방지하기 위해 하나 이상의 논스 (예를 들어, 논스-디바이스 및/또는 논스-RAN) 를 통합할 수도 있다. 다시 말해서, 하나 이상의 논스는 재전송 보호를 위해 이용될 수도 있다. 논스-디바이스 및/또는 논스-RAN 은 랜덤 액세스 프로시저 동안에 디바이스와 RAN 노드 사이에서 교환될 수도 있다. 예를 들어, 디바이스는 랜덤 액세스 프로시저의 메시지 3 (RRC 접속 요청) 에서 RAN 노드로 논스-디바이스를 전송할 수도 있고 RAN 노드는 랜덤 액세스 프로시저의 메시지 4 (RRC 접속 셋업) 에서 디바이스로 논스-RAN 을 전송할 수도 있다. 1 초과의 메시지가 전송되고 있다면, 논스 (예를 들어, 논스-디바이스 및/또는 논스-RAN) 는 각각의 메시지에 대해 미리결정된 고정된 양 (예를 들어, 1) 만큼 증분될 수도 있다.

[0145] 논스 (예를 들어, 논스-디바이스 및/또는 논스-RAN) 에 대한 대안으로서, (예를 들어, 재전송 공격들을 방지하기 위해) 교환될 수도 있는 임의의 랜덤 수가 용인된다. 일부 양태들에서, 논스는 타임스탬프로 교체 (예를 들어, 대체) 될 수도 있다. 타임스탬프는 셀룰러 디바이스 및 장치 (예를 들어, RAN 노드, C-BS) 가 타이머를 갖는 경우에 이용될 수도 있다. 이에 따라, 일부 양태들에서, 그리고 일 예로, 위에서 제공된 예시적인 MAC들에서의 논스 (예를 들어, 논스-디바이스 및/또는 논스-RAN) 중 하나 이상은 랜덤으로 선택된 수 및/또는 타임스탬프로 교체 (예를 들어, 대체) 될 수도 있다.

[0146] 또 다른 대안으로서, 일부 양태들에서, 위에서 제공된 예시적인 MAC들에서의 논스 (예를 들어, 논스-디바이스 및/또는 논스-RAN) 중 하나 이상은 셀-무선 네트워크 임시 아이덴티티 (C-RNTI) 로 교체 (예를 들어, 대체) 될 수도 있다. C-RNTI 는 RRC 접속을 식별하기 위해 그리고 특정한 셀룰러 디바이스에 전용되는 (예를 들어, 디바이스-고유인) 스케줄링을 위해 이용되는 고유 ID (identification) 일 수도 있다. 이러한 시나리오에서, 예를 들어, 제 1 및 제 2 무결성 보호 파라미터들은 논스-디바이스 및 논스-RAN 대신에 파라미터 C-RNTI 를 이용하여 획득된 메시지 인증 코드 (MAC) 일 수도 있다. 예를 들어,

[0147] MAC = F (DASK, S-TMSI | C-RNTI | 메시지),

[0148] 여기서 F 는 MAC 생성 함수 (예를 들어, CMAC, HMAC) 이고, DASK 는 제 2 키의 일 예이고, S-TMSI 는 셀룰러 디바이스의 아이덴티티의 일 예이고, C-RNTI 는 RRC 접속 확립 동안에 디바이스에 배정되는 아이덴티티이고, 그리고 메시지는 전송되는 메시지 (예를 들어, 스몰 데이터 메시지) 이다. 이 대안의 이용은 S-TMSI 및 C-RNTI 식별자들을 배정하는데 있어서 네트워크에 의해 이용되는 프라이버시 폴리시들의 강도에 의해 영향을 받을 수도 있다. 예를 들어, 이 대안은 네트워크가 그 식별자들을 배정하기 위해 양호한 프라이버시 폴리시들을 갖는다는 가정 하에서 이용될 수도 있다.

[0149] K_{MAC} = KDF (DASK, S-TMSI | C-RNTI),

[0150] 여기서 K_{MAC} 는 DASK, S-TMSI 및 C-RNTI 에 기초하여 획득된 원-타임 MAC 생성 키이고; 그리고 KDF 는 키 유도 함수이다.

[0151] MAC = F (K_{MAC}, 메시지)

[0152] 다수의 메시지들이 단일 접속 (예를 들어, RRC 접속) 을 위해 전송되는 경우를 고려하기 위해, 카운터가 각각의 메시지의 MAC, 즉,

[0153] MAC = F (K_{MAC}, 카운터 | 메시지)

[0154] 를 생성하도록 통합될 수도 있다.

[0155] 여기서 카운터는 새로운 키 (즉, K_{MAC}) 가 유도될 때 (예를 들어, 0 으로) 초기화되고 접속을 위한 모든 단일 메시지에 대해 소정의 값 (예를 들어, 1) 만큼 증가된다.

[0156] 위에서 설명된 예시적인 대안들에서, 무결성 보호 파라미터 (예를 들어, MAC, 토큰) 를 획득 (예를 들어, 유도, 생성) 하는데 이용되는 무결성 보호 알고리즘 (예를 들어, 함수 F) 은 네트워크에 의해 결정되고 디바이스에 공지될 수도 있다. 이것은 또한, 아래에 설명되는 바와 같이, 사이퍼링 알고리즘들에 적용된다.

[0157] 이에 따라, 일부 양태들에서, 제 1 무결성 보호 파라미터 및 제 2 무결성 보호 파라미터는 하나 이상의 논스, 랜덤 수들, 타임 스탬프들, 및/또는 네트워크 배정된 고유 (예를 들어, C-RNTI) 파라미터들을 통합할 수도 있다. RAN 노드에서 동작가능한 방법은, RAN 노드에 의해, 논스 (예를 들어, 논스-RAN), 랜덤 수, 타임 스탬프, 및/또는 네트워크 배정된 고유 (예를 들어, C-RNTI) 파라미터를 셀룰러 디바이스에 프로비져닝하는 단계를 포함할 수도 있다. RAN 노드에서 동작가능한 방법은, RAN 노드에 의해, 랜덤 액세스 프로시저 동안에 논스 (예를 들어, 논스-RAN), 랜덤 수, 타임 스탬프, 및/또는 네트워크 배정된 고유 (예를 들어, C-RNTI) 파라미터를 셀룰러 디바이스에 프로비져닝하는 단계를 포함할 수도 있다. 디바이스에서 동작가능한 방법은 디바이스에 의해, 논스 (예를 들어, 논스-디바이스), 랜덤 수, 타임 스탬프, 및/또는 네트워크 배정된 고유 파라미터를 RAN 노드에 프로비져닝하는 단계를 포함할 수도 있다. 디바이스에서 동작가능한 방법은 디바이스에 의해, 랜덤 액세스 프로시저 동안에 논스 (예를 들어, 논스-RAN), 랜덤 수, 타임 스탬프, 및/또는 네트워크 배정된 고유 파라미터를 RAN 노드에 프로비져닝하는 단계를 포함할 수도 있다.

[0158] 장치는 제 1 무결성 보호 값과 제 2 무결성 보호 값을 비교 (910) 할 수도 있다.

[0159] 장치는 제 1 무결성 보호 값이 제 2 무결성 보호 값과 동일하지 않다는 것을 비교 결과가 표시하면 스몰 데이터 메시지를 폐기 (914) 할 수도 있다.

[0160] 장치는 제 1 무결성 보호 값이 제 2 무결성 보호 값과 동일하다는 것을 비교 결과가 표시하면 스몰 데이터 메시지를 게이트웨이 (예를 들어, 다음의 홉) 로 전송할 수도 있다.

[0161] 위에서 표시한 바와 같이, 일부 양태들에서 제 1 무결성 보호 파라미터 및 제 2 무결성 보호 파라미터는 재전송 공격들을 방지하기 위해 랜덤 수 및/또는 타임 스탬프를 통합할 수도 있다. 일부 양태들에서, RAN 노드는 디바이스 아이덴티티에 의해 식별되는 디바이스로부터 스몰 데이터 메시지를 수신할 수도 있고, RAN 노드는 랜덤 수를 디바이스에 프로비져닝한다. 예를 들어, 스몰 데이터 메시지는 디바이스 아이덴티티에 의해 식별되는 디바이스로부터 획득될 수도 있고 랜덤 수는 랜덤 액세스 프로시저 동안에 RAN 노드에 의해 디바이스에 프로비져닝된 논스일 수도 있다. 논스는 RAN 노드로부터 디바이스로 전송된 각각의 메시지에 대해 미리결정된 고정된 양만큼 증분될 수도 있다.

[0162] 다음의 프로세스는 또한, 보안 보호된 통신의 방법을 구현하는데 이용될 수도 있다. 방법은, 무선 액세스 네트워크 (RAN) 노드에서, 제 1 키 및 RAN 노드에 고유한 파라미터에 기초하는 제 2 키를 획득하는 단계, RAN 노드에서, 디바이스 아이덴티티 및 제 1 무결성 보호 값을 포함하는 스몰 데이터 메시지를 획득하는 단계, RAN 노드에서, 제 2 키 및 디바이스 아이덴티티에 기초하는 제 3 키를 획득하는 단계, RAN 노드에서, 제 3 키에 기초하여 제 2 무결성 보호 값을 획득하는 단계, RAN 노드에서, 제 1 무결성 보호 값과 제 2 무결성 보호 값을 비교하는 단계, RAN 노드로부터, 제 1 무결성 보호 값이 제 2 무결성 보호 값과 동일하지 않다는 것을 비교 결과가 표시하면 스몰 데이터 메시지를 폐기하는 단계, 및 RAN 노드로부터, 제 1 무결성 보호 값이 제 2 무결성 보호 값과 동일하다는 것을 비교 결과가 표시하면 스몰 데이터 메시지를 게이트웨이로 전송하는 단계를 포함할 수도 있다. 일부 양태들에 따르면, 제 2 키는 게이트웨이로부터 획득된다. 일부 양태들에 따르면, 게이트웨이는 셀룰러 사물 인터넷 서빙 게이트웨이 노드 (C-SGN) 이다. 일부 양태들에 따르면, RAN 노드는 셀룰러 사물 인터넷 (CIoT) 기지국 (C-BS) 또는 진화된 노드 B (eNodeB) 이고, RAN 노드에 고유한 파라미터는 C-BS 아이덴티티 또는 eNodeB 아이덴티티이다. 일부 양태들에 따르면, 제 1 무결성 보호 값 및 제 2 무결성 보호 값은 적어도 하나의 논스 및/또는 타임 스탬프를 이용하여 획득된다. 일부 양태들에 따르면, 디바이스 아이덴티티는 디바이스를 식별하고, 그 방법은 디바이스에 제 1 논스 및/또는 타임 스탬프를 프로비져닝하는 단계 및/또는 디바이스로부터 제 2 논스를 획득하는 단계를 더 포함한다. 일부 양태들에 따르면, 제 1 논스 및/또는 타임 스탬프를 프로비져닝하는 단계 및 제 2 논스를 획득하는 단계는 랜덤 액세스 프로시저 동안에 일어난다. 일부 양태들에 따르면, 스몰 데이터 메시지는 제 3 키로 암호화되고, 그 방법은 RAN 노드에서, 제 3 키를 이용하여 스몰 데이터 메시지를 해독하는 단계를 더 포함한다. 일부 양태들에 따르면, 스몰 데이터 메시지를 획득하기 이전에, 방법은 RAN 노드에 의해, 트래픽 부하 값을 모니터링하는 단계; RAN 노드에 의해, 트래픽 부하 값이 미리결정된 임계값을 초과한다는 것을 검출하는 단계; 및 트래픽 부하 값이 미리결정된 임계값을 초과한다는 것을 검출하는 것에 응답하여, 디바이스 아이덴티티에 의해 식별되는 디바이스로, RAN 노드로 전송된 다음의 하나 이상의 메시지들에 제 1 무결성 보호 값을 포함시킬 것을 디바이스에 요청하는 메시지를 전송하는 단계를 더 포함한다. 일부 양태들에 따르면, 네트워크는 미리결정된 임계값을 구성한다. 일부 양태들에 따르면, 스몰 데이터 메시지를 획득하기 이전에, 그 방법은 디바이스 아이덴티티에 의해 식별되는 디바이스와 초기 어태치 프로시저 동안에 액세스 계층 보안 구성을 구성 및/또는 협상하는 단계를 더 포함하고, 여기서 액세스 계층 보안 구성은 보안 없이, 무결성 보호로, 암호화로, 무결성 보호 및 암호화로, 및/또는 온디맨드 무결성 보호로 스몰 데이터 메시지들이 디바이스로부터 전송되는지 여부를 특정하며, 여기서 무결성 보호 및 암호화는 제 3 키를 이용하여 수행된다.

[0163] 도 10 은 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 프로세스 (1000) 의 다른 예를 예시하는 플로우 다이어그램이다. 무상태 액세스 계층 보안 프로세스 (1000) 는 무선 액세스 네트워크 (RAN) 노드 (예를 들어, C-BS) 또는 일부 다른 적합한 장치에 로케이트될 수도 있는 프로세싱 회로 (예를 들어, 도 8 의 프로세싱 회로 (810)) 내에서 일어날 수도 있다. 이에 따라, 무상태 액세스 계층 보안 프로세스 (1000) 는 RAN 노드 (예를 들어, C-BS) 또는 일부 다른 적합한 장치에서 동작가능할 수도 있다. 물론, 본 개시의 범위 내의 다양한 양태들에서, 무상태 액세스 계층 보안 프로세스 (1000) 는 본 개시의 하나 이상의 양태들에 따른 보안 키들을 획득하는 것, 프로비져닝하는 것, 및 이용하는 것 중 하나 이상을 포함하여 무상태 액세스 계층 보안을 지원하는 것이 가능한 임의의 적합한 장치에 의해 구현될 수도 있다.

[0164] 도 10 의 양태에서, 셀룰러 디바이스가 RAN 노드 (예를 들어, C-BS) 로 스몰 데이터 메시지를 전송할 때, 셀룰러 디바이스는 초기 어태치 프로시저 동안에 게이트웨이 (예를 들어, C-SGN) 에 의해 셀룰러 디바이스에 프로비져닝된 제 3 키 (예를 들어, DASK) 를 이용하여 스몰 데이터 메시지를 암호화할 수도 있다. RAN 노드 (예를 들어, C-BS) 가 셀룰러 디바이스로부터 스몰 데이터 메시지를 수신할 때, RAN 노드는 게이트웨이에 의해 RAN 노드에 프로비져닝될 수도 있는 제 2 키 (예를 들어, BASK) 및 RAN 노드에 의해 획득된 암호화된 스몰 데이터 메시지와 함께 반송될 수도 있는 셀룰러 디바이스의 아이덴티티를 이용하여 온-더-플라이로 제 3 키 (예를 들어, DASK) 를 획득할 수도 있다. 예를 들어, 암호화된 스몰 데이터 메시지는 셀룰러 디바이스의 S-TMSI 와 함께 반송될 수도 있다.

[0165] 암호화는 랜덤 액세스 프로시저 동안에 RAN 노드 (예를 들어, C-BS) 에 의해 셀룰러 디바이스에 제공된 논스를 이용할 수도 있다. 하나의 양태에서, 논스는 초기화 벡터 (IV) 로서 제공될 수도 있다. 예를 들어:

[0166] 사이퍼텍스트 (Ciphertext) = Enc (DASK, IV, 메시지),

[0167] 여기서 Enc 는 암호화 함수 (예를 들어, AES-CTR, ...) 이고, DASK 는 제 2 키의 일 예이고, 그리고 IV 는 초

기화 벡터로서 제공된 논스이다.

[0168] 원-타임 키를 이용한 암호화의 대안의 방식은, 앞서와 같이:

[0169] K_{Enc} = KDF (DASK, 논스) 이고,

[0170] 여기서 K_{Enc} 는 DASK 및 S-TMSI, C-RNTI, 논스-디바이스, 논스-RAN 또는 그 조합에 기초하여 획득된 원-타임 암호화 키이고; 그리고 KDF 는 키 유도 함수이다.

[0171] 사이퍼텍스트 = Enc (K_{Enc}, IV, 메시지),

[0172] 여기서 IV 는 소정의 값 (예를 들어, 0, 또는 S-TMSI, C-RNTI, 논스-RAN, 논스-디바이스, 또는 그 조합에 기초하여 획득된 값) 으로 초기화된다.

[0173] 다수의 메시지들이 단일 접속 (예를 들어, RRC 접속) 을 위해 전송되는 경우를 고려하기 위해, 카운터가 각각의 메시지의 사이퍼텍스트, 즉,

[0174] 사이퍼텍스트 = Enc (K_{Enc}, IV, 메시지)

[0175] 를 생성하도록 통합될 수도 있으며, 여기서 IV 는 새로운 키 (즉, K_{Enc}) 가 유도될 때 초기화되고 (예를 들어, 0, 또는 S-TMSI, C-RNTI, 논스-RAN, 논스-디바이스, 또는 그 조합에 기초하여 획득된 값), 접속을 위한 모든 단일 메시지에 대해 소정의 값 (예를 들어, 1) 만큼 증가된다.

[0176] 앞서와 같이, RAN 노드는 제 2 키 (예를 들어, BASK) 및 셀룰러 디바이스의 아이덴티티에 기초하여 제 3 키 (예를 들어, DASK) 를 획득할 수도 있다.

[0177] 일부 양태들에서, 메시지에의 IV 의 포함은 RAN 노드 (예를 들어, C-BS) 가 짧은 양의 시간 동안 (예를 들어, RRC 접속의 지속기간 동안) 논스 (예를 들어, IV 로서 이용되는/IV 로 설정되는 논스) 를 저장할 수 있기 때문에 옵션적이다.

[0178] 일부 양태들에서, 논스는 랜덤 액세스 프로시저 동안에 장치 (예를 들어, RAN 노드, C-BS) 에 의해 셀룰러 디바이스에 제공되는 랜덤으로 선택된 수이다. 1 초과의 메시지가 전송되고 있다면, 논스는 각각의 메시지에 대해 미리결정된 고정된 양 (예를 들어, 1) 만큼 증분될 수도 있다. 대안으로, 장치 (예를 들어, RAN 노드, C-BS) 에 의해 셀룰러 디바이스에 제공되고 (예를 들어, 재전송 공격들을 방지하기 위해) 변화될 수도 있는 임의의 랜덤 수가 용인된다. 일부 양태들에서, 논스는 C-RNTI 로 교체될 수도 있다. 일부 양태들에서, 논스는 타임스탬프로 교체될 수도 있다. 타임스탬프는 셀룰러 디바이스 및 장치 (예를 들어, RAN 노드, C-BS) 가 타이머를 갖는 경우에 이용될 수도 있다.

[0179] 이제 도 10 으로 돌아가면, 장치 (예를 들어, RAN 노드, C-BS) 는 제 2 키 (예를 들어, BASK) 를 수신할 수도 있고, 여기서 제 2 키는 제 1 키 및 장치 (예를 들어, RAN 노드, C-BS) 에 고유한 파라미터에 기초한다 (1002). 일부 양태들에서, RAN 노드는 게이트웨이로부터 제 2 키를 수신하고, 제 1 키는 게이트웨이에만 알려져 있다. 일부 양태들에서, 게이트웨이는 C-SGN 이다. 일부 양태들에서, RAN 노드에 고유한 파라미터는 RAN 노드의 아이덴티티이다. 예를 들어, RAN 노드는 CIoT 기지국 (C-BS) 또는 진화된 노드 B (eNodeB) 일 수도 있고, RAN 노드에 고유한 파라미터는 C-BS 아이덴티티 또는 eNodeB 아이덴티티일 수도 있다.

[0180] 장치는 디바이스 아이덴티티를 포함하는 암호화된 스몰 데이터 메시지를 수신할 수도 있다. 일부 양태들에서 스몰 데이터 메시지는 제 3 키 (예를 들어, DASK) 로 암호화 (1004) 된다.

[0181] 장치는 제 2 키 및 디바이스 아이덴티티에 기초하는 제 3 키 (예를 들어, DASK) 를 획득 (1006) 할 수도 있다.

[0182] 장치는 제 3 키를 이용하여 스몰 데이터 메시지를 해독 (1008) 할 수도 있다.

[0183] 일부 양태들에서, 암호화 및 해독은 재전송 공격들을 방지하기 위해 랜덤 수 및/또는 타임 스탬프를 통합할 수도 있다. 일부 양태들에서, 스몰 데이터 메시지는 디바이스 아이덴티티에 의해 식별되는 디바이스로부터 획득될 수도 있고 RAN 노드는 랜덤 수를 디바이스에 프로비져닝한다. 예를 들어, 스몰 데이터 메시지는 디바이스 아이덴티티에 의해 식별되는 디바이스로부터 획득될 수도 있고 랜덤 수는 랜덤 액세스 프로시저 동안에 RAN 노드에 의해 디바이스에 프로비져닝된 논스일 수도 있다. 논스는 RAN 노드로부터 디바이스로 전송된 각각의 메시지에 대해 미리결정된 고정된 양만큼 증분될 수도 있다.

[0184] 도 11 은 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 프로세스 (1100) 의 다른 예를 예시하는 플로우 다이어그램이다. 무상태 액세스 계층 보안 프로세스 (1100) 는 무선 액세스 네트워크 (RAN) 노드 (예를 들어, C-BS) 또는 일부 다른 적합한 장치에 로케이트될 수도 있는 프로세싱 회로 (예를 들어, 도 8 의 프로세싱 회로 (810)) 내에서 일어날 수도 있다. 이에 따라, 무상태 액세스 계층 보안 프로세스 (1100) 는 RAN 노드 (예를 들어, C-BS) 또는 일부 다른 적합한 장치에서 동작가능할 수도 있다. 물론, 본 개시의 범위 내의 다양한 양태들에서, 무상태 액세스 계층 보안 프로세스 (1100) 는 본 개시의 하나 이상의 양태들에 따른 보안 키들을 획득하는 것, 프로비져닝하는 것, 및 이용하는 것 중 하나 이상을 포함하여 무상태 액세스 계층 보안을 지원하는 것이 가능한 임의의 적합한 장치에 의해 구현될 수도 있다.

[0185] 도 11 의 양태에서, 암호화 및 무결성 보호 양자 모두가 인에이블될 수도 있다. 암호화 및 무결성 보호 양자 모두가 이용을 위해 구성될 때, AEAD (Authenticated Encryption With Associated Data) 사이퍼가 이용될 수도 있다. 액세스 계층 보안은 초기 어태치 프로시저 동안에 구성 및/또는 협상될 수도 있다.

[0186] 이제 도 11 로 돌아가면, 장치 (예를 들어, 무선 액세스 네트워크 (RAN) 노드, C-BS) 는 제 2 키 (예를 들어, BASK) 를 수신할 수도 있고, 여기서 제 2 키는 제 1 키 및 장치 (예를 들어, RAN 노드, C-BS) 에 고유한 파라미터에 기초한다 (1102). 일부 양태들에서, RAN 노드는 게이트웨이로부터 제 2 키를 수신하고, 그리고 제 1 키는 게이트웨이에만 알려져 있다. 일부 양태들에서, 게이트웨이는 C-SGN 이다. 일부 양태들에서, RAN 노드에 고유한 파라미터는 RAN 노드의 아이덴티티이다. 예를 들어, RAN 노드는 CIoT 기지국 (C-BS) 또는 진화된 노드 B (eNodeB) 일 수도 있고, RAN 노드에 고유한 파라미터는 C-BS 아이덴티티 또는 eNodeB 아이덴티티일 수도 있다.

[0187] 장치는 디바이스 아이덴티티를 포함하는 스몰 데이터 메시지를 수신할 수도 있다. 일부 양태들에서, 스몰 데이터 메시지는 제 3 키 (예를 들어, DASK) 로 암호화될 수도 있고 스몰 데이터 메시지는 제 3 키를 이용하여 유도 또는 생성된 무결성 보호 값을 포함할 수도 있다 (1104).

[0188] 장치는 제 2 키 및 디바이스 아이덴티티에 기초하는 제 3 키 (예를 들어, DASK) 를 획득 (1106) 할 수도 있다.

[0189] 디바이스는 제 3 키를 이용하여 스몰 데이터 메시지를 해독 (1108) 할 수도 있다.

[0190] 디바이스는 제 3 키를 이용하여 무결성 보호 값을 검증 (1110) 할 수도 있다.

[0191] 도 12 는 본 개시의 일부 양태들에 따른 무상태 액세스 계층 보안 프로세스 (1200) 의 다른 예를 예시하는 플로우 다이어그램이다. 무상태 액세스 계층 보안 프로세스 (1200) 는 무선 액세스 네트워크 (RAN) 노드 (예를 들어, C-BS) 또는 일부 다른 적합한 장치에 로케이트될 수도 있는 프로세싱 회로 (예를 들어, 도 8 의 프로세싱 회로 (810)) 내에서 일어날 수도 있다. 이에 따라, 무상태 액세스 계층 보안 프로세스 (1200) 는 RAN 노드 (예를 들어, C-BS) 또는 일부 다른 적합한 장치에서 동작가능할 수도 있다. 물론, 본 개시의 범위 내의 다양한 양태들에서, 무상태 액세스 계층 보안 프로세스 (1200) 는 본 개시의 하나 이상의 양태들에 따른 보안 키들을 획득하는 것, 프로비져닝하는 것, 및 이용하는 것 중 하나 이상을 포함하여 무상태 액세스 계층 보안을 지원하는 것이 가능한 임의의 적합한 장치에 의해 구현될 수도 있다.

[0192] 도 12 의 양태에서, 토큰을 채용하는 일 예시적인 온디맨드 무결성 보호 프로세스가 묘사된다. 하나의 양태에 따르면, 정상 또는 제 1 동작 모드에서는, 어떤 액세스 계층 보안도 구성되지 않는다; 제 2 동작 모드에서, 액세스 계층 보안이 구성된다. 예를 들어, 혼잡 (congestion) 및/또는 오버헤드가 RAN 노드 (예를 들어, C-BS) 또는 일부 다른 네트워크 노드에서 검출될 때, RAN 노드 (예를 들어, C-BS) 는 셀룰러 디바이스로 메시지 (예를 들어, 표시, 요청, 명령, 커맨드) 를 전송할 수도 있다. 메시지는 RAN 노드 (예를 들어, C-BS) 로 전송된 하나 이상의 메시지들 (예를 들어, 스몰 데이터 메시지들) 과 함께 토큰을 포함하도록 셀룰러 디바이스를 야기할 수도 있다 (또는 트리거링할 수도 있다). 하나의 예에서, 혼잡 및/또는 오버로드가 많은 양의 스몰 데이터 메시지 전송들에 기초하여 검출될 수도 있다. 하나의 예에서, 트래픽 부하가 주어진 임계치를 초과할 때, 혼잡 및/또는 오버로드가 검출될 수도 있고, 그리고 표시/요청/명령/커맨드의 전송이 트리거링될 수도 있다. 일부 양태들에서, 임계치는 미리정의될 수도 있다. 일부 양태들에서, 네트워크는 임계치를 구성할 수도 있다.

[0193] 일부 양태들에 따르면, 토큰은 무결성을 위한 MAC 와 동일한 방식으로 생성될 수도 있다; 그러나, 무결성을 위한 MAC 와 달리, 이 양태에 따른 토큰은 RAN 노드로부터 온디맨드로 제공 (예를 들어, RAN 노드로부터의 디맨드에 응답하여 제공) 된다.

[0194] 예를 들어, 랜덤 액세스 프로시저 동안에, RAN 노드 (예를 들어, C-BS) 및 디바이스는 이전에 설명한 바와 같이 개별의 논스 (예를 들어, 논스-RAN, 논스-디바이스) 를 교환할 수도 있다. 추가적으로, RAN 노드는 전송된 다음의 하나 이상의 스몰 데이터 메시지들과 함께 토큰을 전송하기 위해 셀룰러 디바이스에 표시/요청/명령/커맨드를 제공할 수도 있다. 토큰은 다음으로서 생성될 수도 있으며,

[0195] 토큰 = F (DASK, S-TMSI | 논스-디바이스 | 논스-RAN | 메시지),

[0196] 여기서 F 는 토큰 생성 함수 (예를 들어, CMAC, HMAC) 이고, DASK 는 제 3 키이고, S-TMSI 는 셀룰러 디바이스의 아이덴티티 (셀룰러 디바이스를 식별하는 다른 파라미터들이 이용될 수도 있다) 이고, 논스-디바이스, 및 논스-RAN 은 위에서 설명되었고, 메시지는 전송되는 메시지이다. 1 초과의 메시지가 전송되고 있다면, 논스는 각각의 메시지에 대해 고정된 양 (예를 들어, 1) 만큼 증분될 수도 있다.

[0197] RAN 노드 (예를 들어, C-BS) 가 셀룰러 디바이스로부터 토큰을 반송하는 메시지를 수신할 때, RAN 노드는 온-더-플라이로 제 3 키 (예를 들어, DASK) 를 획득할 수도 있고, 여기서 제 3 키는 제 2 키 (예를 들어, BASK) 및 셀룰러 디바이스의 아이덴티티에 기초할 수도 있다. RAN 노드는 그 후, 예를 들어, 위에서 제공된 식에 따라 제 2 토큰을 획득 (예를 들어, 유도, 생성) 하고 수신된 토큰과 제 2 토큰을 비교하는 것에 의해, 토큰을 검증할 수도 있다.

[0198] 일부 양태들에서, 논스는 셀룰러 디바이스 메시지에서 반송되거나 또는 RAN 노드 (예를 들어, C-BS) 에 일시적으로 저장될 수도 있다.

[0199] 다양한 구현들에서, 토큰을 채용하는 이 온디맨드 무결성 보호 프로세스는 혼잡/오버로드 동안에 트리거링되기 때문에, 온디맨드 무결성 보호 프로세스는, 액세스 계층 보안 (예를 들어, LTE 액세스 계층 보안) 이 항상 활성화되었다면, 셀룰러 디바이스 및 RAN 노드 (예를 들어, C-BS) 에 다르게 초래될 컴퓨테이션 오버헤드를 최소화한다.

[0200] 이제 도 12 로 돌아가면, 장치 (예를 들어, 무선 액세스 네트워크 (RAN) 노드) 는 트래픽 부하 값을 모니터링 (1202) 할 수도 있다.

[0201] 장치는 트래픽 부하 값이 미리결정된 임계값을 초과한다는 것을 검출 (1204) 할 수도 있다. 하나의 예에서, 네트워크 (예를 들어, 코어 네트워크) 는 미리결정된 임계값을 구성할 수도 있다.

[0202] 장치는 트래픽 부하 값이 미리결정된 임계값을 초과한다는 것을 검출하는 것에 응답하여, 장치 (RAN 노드, C-BS) 로 전송된 다음의 하나 이상의 메시지들에 토큰을 포함시킬 것을 셀룰러 디바이스에 요청하는 메시지 (예를 들어, 표시, 요청, 명령, 커맨드) 를 셀룰러 디바이스 (예를 들어, CIoT 디바이스) 로 전송할 수도 있다.

[0203] 도 13 은 본 개시의 하나 이상의 양태들에 따른 무상태 액세스 계층 보안 및 보안 키들을 획득하는 것, 프로비져닝하는 것, 및 이용하는 것 중 하나 이상을 지원할 수도 있는 장치 (1300) (예를 들어, 셀룰러 디바이스, CIoT 디바이스, 전자 디바이스, 통신 장치) 의 하드웨어 구현의 다른 예를 예시하는 블록 다이어그램이다. 장치 (1300) 는 게이트웨이 (예를 들어, C-SGN), RAN 노드 (예를 들어, 기지국, eNB, C-BS), 셀룰러 디바이스, CIoT 디바이스, 또는 모바일 폰, 스마트 폰, 태블릿, 휴대용 컴퓨터, 서버, 개인 컴퓨터, 센서, 엔터테인먼트 디바이스, 의료 디바이스, 또는 무선 통신 회로부를 갖는 임의의 다른 전자 디바이스와 같은 무선 통신을 지원하는 일부 다른 타입의 디바이스 내에서 구현될 수 있다.

[0204] 장치 (1300) 는 통신 인터페이스 (예를 들어, 적어도 하나의 트랜시버) (1302), 저장 매체 (1304), 사용자 인터페이스 (1306), 메모리 디바이스 (1308) (예를 들어, 하나 이상의 보안 키들 (1318) 을 저장), 및 프로세싱 회로 (1310) 를 포함한다. 다양한 구현들에서, 사용자 인터페이스 (1306) 는 키패드, 디스플레이, 스피커, 마이크로폰, 터치스크린 디스플레이, 또는 사용자로부터 입력을 수신하거나 또는 사용자로 출력을 전송하기 위한 일부 다른 회로부 중 하나 이상을 포함할 수도 있다. 일반적으로, 도 13 의 컴포넌트들은 도 6 의 장치 (600) 의 대응하는 컴포넌트들과 유사할 수도 있다.

[0205] 본 개시의 하나 이상의 양태들에 따르면, 프로세싱 회로 (1310) 는 본 명세서에서 설명된 장치들 중 임의의 것 또는 전부에 대한 피처들, 프로세스들, 기능들, 동작들, 및/또는 루틴들 중 임의의 것 또는 전부를 수행하도록 적응될 수도 있다. 예를 들어, 프로세싱 회로 (1310) 는 도 4, 도 5, 도 7, 도 9 내지 도 12, 및 도 14 에 대하여 설명된 블록들, 단계들, 기능들, 및/또는 프로세스들 중 임의의 것을 수행하도록 적응될 수도 있다. 본 명세서에서 사용한 바와 같이, 프로세싱 회로 (1310) 에 관한 용어 "적응된" 은 프로세싱 회로 (1310) 가 본 명세서에서 설명된 다양한 피처들에 따라 특정한 프로세스, 기능, 동작, 및/또는 루틴을 수행하도록 고안,

구성, 채용, 구현, 및/또는 프로그래밍되는 것 중 하나 이상을 행하는 것을 지칭할 수도 있다.

[0206] 프로세싱 회로 (1310) 는 도 4, 도 5, 도 7, 도 9 내지 도 12, 및 도 14 와 함께 설명된 동작들 중 임의의 하나를 이행하기 위한 수단 (예를 들어, 위한 구조) 으로서 서빙하는 주문형 집적 회로 (ASIC) 와 같은 전문화된 프로세서일 수도 있다. 프로세싱 회로 (1310) 는 송신하기 위한 수단 및/또는 수신하기 위한 수단의 하나의 예로서 서빙할 수도 있다.

[0207] 장치 (1300) 의 적어도 하나의 예에 따르면, 프로세싱 회로 (1310) 는 통신하기 위한 회로/모듈 (1320), 수신하기 위한 회로/모듈 (1322), 구성하기 위한 회로/모듈 (1324), 협상하기 위한 회로/모듈 (1326), 전송하기 위한 회로/모듈 (1328), 무결성 파라미터를 획득하기 위한 회로/모듈 (1330), 또는 암호화하기 위한 회로/모듈 (1332) 중 하나 이상을 포함할 수도 있다.

[0208] 위에서 언급한 바와 같이, 저장 매체 (1304) 에 의해 저장된 프로그래밍은, 프로세싱 회로 (1310) 에 의해 실행될 때, 프로세싱 회로 (1310) 로 하여금, 본 명세서에서 설명된 다양한 기능들 및/또는 프로세스 동작들 중 하나 이상을 수행하게 한다. 예를 들어, 저장 매체 (1304) 는 통신하기 위한 코드 (1340), 수신하기 위한 코드 (1342), 구성하기 위한 코드 (1344), 협상하기 위한 코드 (1346), 전송하기 위한 코드 (1348), 무결성 파라미터를 획득하기 위한 코드 (1350), 또는 암호화하기 위한 코드 (1352) 중 하나 이상을 포함할 수도 있다.

[0209] 도 14 는 본 개시의 양태들에 따른 무상태 액세스 계층 보안 프로세스 (1400) 의 다른 예를 예시하는 플로우 다이어그램이다. 무상태 액세스 계층 보안 프로세스 (1400) 는 셀룰러 디바이스 (예를 들어, CIoT 디바이스) 또는 일부 다른 적합한 장치에 로케이트될 수도 있는 프로세싱 회로 (예를 들어, 도 13 의 프로세싱 회로 (1310)) 내에서 일어날 수도 있다. 이에 따라, 무상태 액세스 계층 보안 프로세스 (1400) 는 셀룰러 디바이스 또는 일부 다른 적합한 장치에서 동작가능할 수도 있다. 물론, 본 개시의 범위 내의 다양한 양태들에서, 무상태 액세스 계층 보안 프로세스 (1400) 는 본 개시의 하나 이상의 양태들에 따른 보안 키들을 획득하는 것, 프로비져닝하는 것, 및 이용하는 것 중 하나 이상을 포함하여 무상태 액세스 계층 보안을 지원하는 것이 가능한 임의의 적합한 장치에 의해 구현될 수도 있다.

[0210] 이제 도 14 로 돌아가면, 장치 (예를 들어, 셀룰러 디바이스, CIoT 디바이스) 는 제 2 키 (예를 들어, BASK) 및 장치에 고유한 파라미터에 기초하는 제 3 키 (예를 들어, DASK) 를 획득 (1402) 할 수도 있다. 일부 양태들에서, 장치에 고유한 파라미터는 장치의 아이덴티티 (예를 들어, 셀룰러 디바이스의 아이덴티티, 셀룰러 디바이스 ID, CIoT 디바이스 ID) 일 수도 있다. 일부 양태들에서, 제 2 키는 제 1 키 및 RAN 노드 아이덴티티 또는 RAN 노드 그룹 아이덴티티에 기초할 수도 있다. 장치는 제 2 키 및 제 1 키를 알고 있지 않을 수도 있다. 일부 양태들에서, 예를 들어, 제 2 키는 제 1 키 및 RAN 노드에 고유한 파라미터에 기초할 수도 있고, 제 1 키 는 게이트웨이에만 알려져 있을 수도 있다.

[0211] 장치는 액세스 계층 보안 구성을 구성 및/또는 협상 (1404) 할 수도 있다. 일부 양태들에서, 장치는 RAN 노드와 액세스 계층 보안 구성을 협상할 수도 있다. 일부 양태들에서, 장치는 초기 어태치 프로시저 동안에 액세스 계층 보안 구성을 협상할 수도 있다. 일부 양태들에서, 장치는 초기 어태치 프로시저 동안에 RAN 노드와 액세스 계층 보안 구성을 협상할 수도 있다. 일부 양태들에 따르면, 액세스 계층 보안 구성은 보안 없이, 무결성 보호로, 암호화로, 무결성 보호 및 암호화로, 및/또는 온디맨드 무결성 보호로 스몰 데이터 메시지들이 셀룰러 디바이스로부터 전송되는지 여부를 특정할 수도 있고, 여기서 무결성 보호 및 암호화는 제 3 키를 이용하여 수행될 수도 있다.

[0212] 장치는 제 3 키를 이용하여 액세스 계층 보안 구성에 기초한 스몰 데이터 메시지를 보호 (1406) 할 수도 있다. 장치는 제 3 키를 이용하여 무결성 보호 및/또는 암호화로 스몰 데이터 메시지를 보호할 수도 있다. 장치는 제 3 키를 이용하여 보호된 스몰 데이터 메시지를 전송 (1408) 할 수도 있다. 일부 양태들에서, 장치는 제 3 키를 이용하여 보호된 스몰 데이터 메시지를 RAN 노드로 전송할 수도 있다.

[0213] 본 명세서에서 설명된 모든 양태들 및 구현들에 대하여, 게이트웨이 (예를 들어, C-SGN) 는 제 1 키 (예를 들어, MASK) 를 주기적으로 변화시킬 수도 있다. 일부 양태들에 따르면, 제 1 키는 제 1 인덱스 (예를 들어, MASK 인덱스) 와 연관될 수도 있다. 예를 들어, 제 1 키는 제 1 인덱스에 의해 결정될 수도 있다. 하나의 양태에서, 제 1 키가 변화하는 시간마다 (주기마다), 제 1 인덱스는 변화할 수도 있다.

[0214] 일부 양태들에 따르면, 제 2 키 (예를 들어, BASK) 는 제 2 인덱스 (예를 들어, BASK 인덱스) 와 연관될 수도 있다. 제 2 인덱스는 제 1 인덱스 (예를 들어, MASK 인덱스) 에 의해 결정될 수도 있다. 예를 들어, RAN 노드 (예를 들어, C-BS) 에는, 현재 유효한 (예를 들어, 만료되지 않은, 액티브인) 제 1 인덱스에 대응하는

제 2 인덱스를 갖는 제 2 키가 프로비져닝될 수도 있다.

[0215] 일부 양태들에 따르면, 제 3 키 (예를 들어, DASK) 는 제 3 인덱스 (예를 들어, DASK 인덱스) 와 연관될 수도 있다. 제 3 인덱스는 제 2 인덱스 (예를 들어, BASK 인덱스) 에 의해 결정될 수도 있다. 예를 들어, 셀룰러 디바이스 (예를 들어, CIoT 디바이스) 에는, 현재 유효한 (예를 들어, 만료되지 않은, 액티브인) 제 2 인덱스에 대응하는 제 3 인덱스를 갖는 제 3 키가 프로비져닝될 수도 있다.

[0216] 제 3 키 인덱스 (예를 들어, DASK 인덱스) 는, 본 명세서에서 설명된 양태들에 따라 스몰 데이터 메시지를 획득하는 엔티티 (예를 들어, RAN 노드, C-BS) 가 액세스 계층 보안 검증 및/또는 해독을 위해 이용되어야 하는 제 3 키 (예를 들어, DASK) 를 획득 (예를 들어, 유도, 생성) 할 수 있도록 스몰 데이터 메시지에 포함될 수도 있다.

[0217] 임의의 키 (예를 들어, 제 1, 제 2, 및/또는 제 3 키) 의 변화는, 예를 들어, 시간 만료, 보안, 유지보수, 키 타협의 검출, 또는 악의적인 디바이스(들)의 검출로 인한 것일 수도 있다.

[0218] 하나의 양태에 따르면, 키가 (예를 들어, 시간 만료, 보안, 유지보수, 키 타협의 검출, 악의적인 디바이스(들)의 검출로 인해) 유효하지 않을 때, 에러 메시지가 셀룰러 디바이스 및/또는 게이트웨이 (예를 들어, C-SGN) 로 전송될 수도 있다.

[0219] 셀룰러 디바이스에서, 에러 메시지를 획득 시에, 셀룰러 디바이스는 게이트웨이 (예를 들어, C-SGN) 로 제 3 키 (예를 들어, DASK) 에 대한 요청을 전송할 수도 있다. 제 3 키에 대한 요청은 키 요청 메시지로 지칭될 수도 있다 (그리고 대안적으로 DASK 업데이트 메시지로 지칭될 수도 있다). 키 요청 메시지는 본 명세서에서 설명된 양태들에서 논의한 바와 같이 액세스 계층 보안에 의해 보호되지 않을 수도 있다.

[0220] 키 요청 메시지 및/또는 에러 메시지는, 예를 들어, 보안 NAS 제어 메시지를 이용하여 셀룰러 디바이스로 새로운 제 3 키 (예를 들어, 새로운 DASK) 를 전송 (예를 들어, 푸시) 하도록 게이트웨이를 트리거링하기 위해, 게이트웨이로 전송될 수도 있다. 하나의 양태에서, 게이트웨이가 주어진 셀룰러 디바이스에 대한 키를 변화시킬 때 (예를 들어, 새로운 제 3 키를 전송), 게이트웨이는 다른 셀룰러 디바이스들 (예를 들어, 제 3 키들이 타협된 제 2 키에 기초할 수도 있는 디바이스들) 에 개별의 새로운 키들을 동시에 프로비져닝할 수도 있다. 그러나, 다른 양태들에 따르면, 게이트웨이가 주어진 셀룰러 디바이스에 대한 키를 변화시킬 때 (예를 들어, 새로운 제 3 키를 전송), 게이트웨이는 다른 셀룰러 디바이스들에 개별의 새로운 키들을 동시에 프로비져닝하지 않을 수도 있다.

[0221] 대안적으로, 키 요청 메시지 (예를 들어, DASK 업데이트) 는 게이트웨이 (예를 들어, C-SGN) 로 구 (old) 키로 보호된 메시지를 전송하는 것에 의해 디바이스에 의해 트리거링될 수도 있다.

[0222] 게이트웨이 (예를 들어, C-SGN) 는 다수의 상이한 제 1 키들 (예를 들어, MASK들) 및 대응하는 상이한 제 2 키들 (예를 들어, BASK들) 을 동시에 이용할 수도 있다. 상이한 제 1 키들 및 대응하는 상이한 제 2 키들의 동시 이용은, 예를 들어, 키 변화들의 영향을 감소 및/또는 일반적으로 보안을 개선시킬 수도 있다.

[0223] 일부 양태들에 따르면, 액세스 계층 보안 보호된 메시지는 RAN 노드 (예를 들어, C-BS) 에서 액세스 계층 보안 보호를 이용하지 않는 메시지보다 더 큰 우선순위를 획득할 수도 있다 (예를 들어, 그에 비해 우선순위화될 수도 있다). 일부 양태들에 따르면, 액세스 계층 보안 보호된 메시지는 RAN 노드 (예를 들어, C-BS) 가 혼잡 또는 오버로드될 때 RAN 노드에서 액세스 계층 보안 보호를 이용하지 않는 메시지보다 더 큰 우선순위를 획득할 수도 있다 (예를 들어, 그에 비해 우선순위화될 수도 있다).

[0224] 일부 양태들에 따르면, CIoT 는 접속된 모드 이동성 (즉, 핸드오버 프로시저) 을 지원하지 않을 수도 있다. 이에 따라, 본 명세서에서 설명된 일부 양태들에 따른 액세스 계층 보안은 접속된 모드 이동성을 또한 지원하지 않을 수도 있다.

[0225] 본 명세서에서 설명된 일부 양태들에 따르면, 셀룰러 디바이스 (예를 들어, CIoT 디바이스) 가 새로운 RAN 노드 (예를 들어, C-BS) 에 어태치될 때, 셀룰러 디바이스는 위에서 설명한 바와 같이 키 요청 메시지를 전송할 수도 있다. 예를 들어, 셀룰러 디바이스는 새로운 RAN 노드로 키 요청 메시지를 전송할 수도 있다. 일부 양태들에 따르면, 셀룰러 디바이스가 이전에 어태치된 RAN 노드 (예를 들어, C-BS) 에 어태치되면, 셀룰러 디바이스는 (제 3 키가 제거되지 않으면 및/또는 어떤 연관된 키 인덱스도 변화되지 않으면) 이전에 어태치된 RAN 노드와 연관된 제 3 키 (예를 들어, DASK) 를 이용할 수 있다.

[0226] 도 15 는 본 개시의 일부 양태들에서 나타날 수도 있는 바와 같은 RAN (1502) 및 다수의 통신 엔티티들을 포함

하는 무선 통신 네트워크 (1500) 의 부분의 개략적 예시이다. 본 명세서에서 설명한 바와 같이, 셀룰러 디바이스, CIoT 디바이스, LTE 무선 셀룰러 디바이스, 및/또는 머신-타입 통신 무선 셀룰러 디바이스는 예를 들어, IoT 디바이스 (1504), 스마트 알람 (1506), 원격 센서 (1508), 스마트 폰 (1510), 모바일 폰 (1512), 스마트 미터 (1514), 개인 휴대 정보 단말기 (PDA) (1516), 개인 컴퓨터 (1518), 메시 노드 (1520), 및/또는 태블릿 컴퓨터 (1522) 에 상주하거나, 또는 그 일부일 수도 있다. 물론, 예시된 디바이스들 또는 컴포넌트들은 예들이며, 임의의 적합한 노드 또는 디바이스는 본 개시의 범위 내의 무선 통신 네트워크 내에서 나타날 수도 있다. 이들 예들은 본 개시의 소정의 개념들을 예시하기 위해 제공된다. 당업자들은 이들이 사실상 예시적이며, 다른 예들이 본 개시 및 첨부된 청구항들의 범위에 포함될 수도 있다는 것을 인식할 것이다.

[0227] 당업자들은 본 개시 전반에 걸쳐 설명된 다양한 양태들이 임의의 적합한 전기통신 시스템, 네트워크 아키텍처, 및 통신 표준으로 확장될 수도 있다는 것을 쉽게 인식할 것이다. 일 예로, 다양한 양태들은 W-CDMA, TD-SCDMA, 및 TD-CDMA 와 같은 UMTS 시스템들에 적용될 수도 있다. 다양한 양태들은 또한, 롱 텀 에볼루션 (LTE) (FDD, TDD, 또는 양자의 모드들에서), LTE-어드밴스드 (LTE-A) (FDD, TDD, 또는 양자의 모드들에서), CDMA 2000, EV-DO (Evolution-Data Optimized), 울트라 모바일 브로드밴드 (UMB), IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, 울트라-광대역 (UWB), 블루투스를 채용하는 시스템들, 및/또는 아직 정의되지 않은 광역 네트워크 표준들에 의해 설명된 것들을 포함한 다른 적합한 시스템들에 적용될 수도 있다. 채용된 실제 전기통신 표준, 네트워크 아키텍처, 및/또는 통신 표준은 특정 애플리케이션 및 시스템에 부과된 전체 설계 제약들에 의존할 것이다.

[0228] 본 개시 내에서, 단어 "예시적인" 은 "일 예, 인스턴스, 또는 예시로서 서빙하는 것" 을 의미하는데 사용된다. 본 명세서에서 "예시적인" 으로서 설명된 임의의 구현 또는 양태는 반드시 본 개시의 다른 양태들에 비해 유리하거나 또는 선호되는 것으로서 해석될 필요는 없다. 마찬가지로, 용어 "양태들" 은 본 개시의 모든 양태들이 논의된 피처, 이점, 또는 동작 모드를 포함하는 것을 요구하지 않는다. 용어 "커플링된" 은 본 명세서에서 2 개의 오브젝트들 간의 직접 또는 간접 기계적 및/또는 전기적 커플링을 지칭하는데 사용된다. 예를 들어, 오브젝트 A 가 오브젝트 B 와 물리적으로 터치 및/또는 전기적으로 통신하고, 오브젝트 B 가 오브젝트 C 와 물리적으로 터치 및/또는 전기적으로 통신하면, 오브젝트들 A 와 C 는 - 그들이 서로 직접 물리적으로 터치 및/또는 전기적으로 통신하지 않는 경우라도 - 여전히 서로 커플링되는 것으로 간주될 수도 있다. 예를 들어, 제 1 다이는 그 제 1 다이가 제 2 다이와 절대 직접 물리적으로 접촉하고 있지 않더라도 패키지 내의 제 2 다이에 커플링될 수도 있다. 용어들 "회로" 및 "회로부" 는 광범위하게 사용되며, 접속 및 구성될 때, 전자 회로들의 타입에 대한 제한 없이, 본 개시에서 설명된 기능들의 수행을 인에이블하는 전기 디바이스들 및 컨덕터들의 하드웨어 구현들, 뿐만 아니라 프로세서에 의해 실행될 때, 본 개시에서 설명된 기능들의 수행을 인에이블하는 정보 및 명령들의 소프트웨어 구현들 양자 모두를 포함하도록 의도된다.

[0229] 위에서 예시된 컴포넌트들, 블록들, 피처들, 및/또는 기능들 중 하나 이상은 단일 컴포넌트, 블록, 피처, 또는 기능으로 재배열 및/또는 결합되거나 또는 여러 컴포넌트들, 블록들, 피처들, 및/또는 기능들로 구현될 수도 있다. 추가적인 컴포넌트들, 블록들, 피처들, 및/또는 기능들은 또한, 본 명세서에서 개시된 신규한 피처들로부터 벗어남 없이 추가될 수도 있다. 위에서 예시된 장치, 디바이스들, 및/또는 컴포넌트들은 본 명세서에서 설명된 방법들, 블록들, 피처들, 및/또는 기능들 중 하나 이상을 수행하도록 적응 (예를 들어, 고안, 구성, 채용, 구현, 및/또는 프로그래밍) 될 수도 있다. 본 명세서에서 설명된 알고리즘들은 또한 효율적으로 소프트웨어에서 구현 및/또는 하드웨어에 임베딩될 수도 있다.

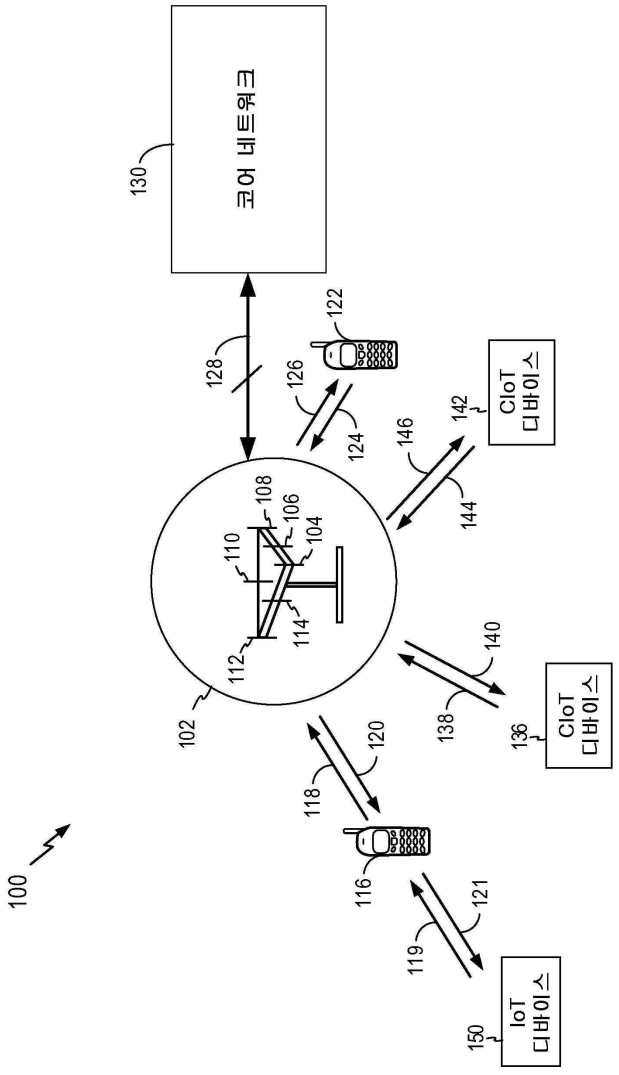
[0230] 개시된 방법들에서의 블록들의 특정 순서 또는 계위 (hierarchy) 는 예시적인 프로세스들의 예시인 것으로 이해되어야 한다. 방법들에서의 블록들의 특정 순서 또는 계위는 재배열될 수도 있는 것으로 이해된다. 첨부하는 방법 청구항들은 샘플 순서로 다양한 블록들의 엘리먼트들을 제시하고, 본 명세서에서 구체적으로 열거되지 않는 한 제시된 특정 순서 또는 계위에 제한되도록 의도되지 않는다.

[0231] 이전의 설명은 임의의 당업자가 본 명세서에서 설명된 다양한 양태들을 실시하는 것을 인에이블하기 위해 제공된다. 이들 양태들에 대한 다양한 수정들은 당업자들에게 용이하게 명백할 것이며, 본 명세서에서 정의된 일반적인 원리들은 다른 양태들에 적용될 수도 있다. 따라서, 청구항들은 본 명세서에서 나타낸 양태들에 제한되도록 의도되지 않고, 청구항들의 언어 (language) 에 부합하는 최광의 범위를 부여받게 하려는 것이며, 여기서 단수로의 엘리먼트에 대한 언급은 구체적으로 그렇게 서술하지 않는 한 "하나 및 단 하나" 를 의미하도록 의도되지 않고, 오히려 "하나 이상" 을 의미한다. 구체적으로 다르게 서술하지 않는 한, 용어 "일부" 는 하나 이상을 지칭한다. 아이템들의 리스트 "중 적어도 하나" 를 지칭하는 어구는 단일 멤버들을 포함하는, 그 아이템들의 임의의 조합을 지칭한다. 일 예로서, "a, b, 또는 c 중 적어도 하나" 는 a; b; c; a 및 b; a

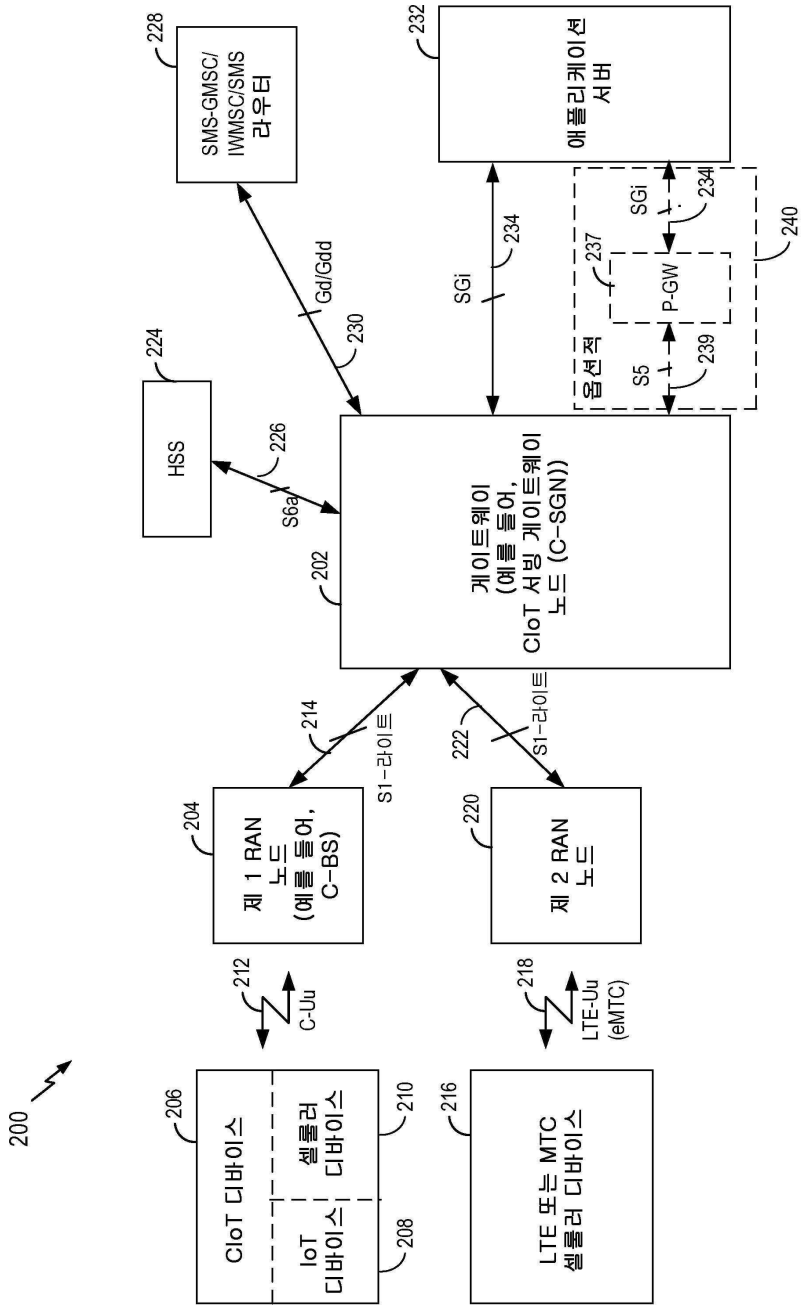
및 c; b 및 c; 및 a, b, 및 c 를 커버하도록 의도된다. 당업자들에게 알려져 있거나 또는 추후에 알려지게 될 본 개시 전반에 걸쳐 설명된 다양한 양태들의 엘리먼트들에 대한 모든 구조적 및 기능적 등가물들은 본 명세서에 참조로 분명히 통합되고 청구항들에 의해 포괄되도록 의도된다. 더욱이, 본 명세서에서 개시된 어떤 것도 이러한 개시가 청구항들에서 명시적으로 열거되는지 여부에 관계없이 공공에게 전용되도록 의도되지 않는다. 어떤 청구항 엘리먼트도, 그 엘리먼트가 어구 "위한 수단" 을 이용하여 분명히 열거되지 않거나, 또는 방법 청구항의 경우에, 엘리먼트가 어구 "위한 단계" 를 이용하여 열거되지 않는 한, 35 U.S.C. §112(f) 의 프로비젼들 하에서 해석되어서는 안된다.

도면

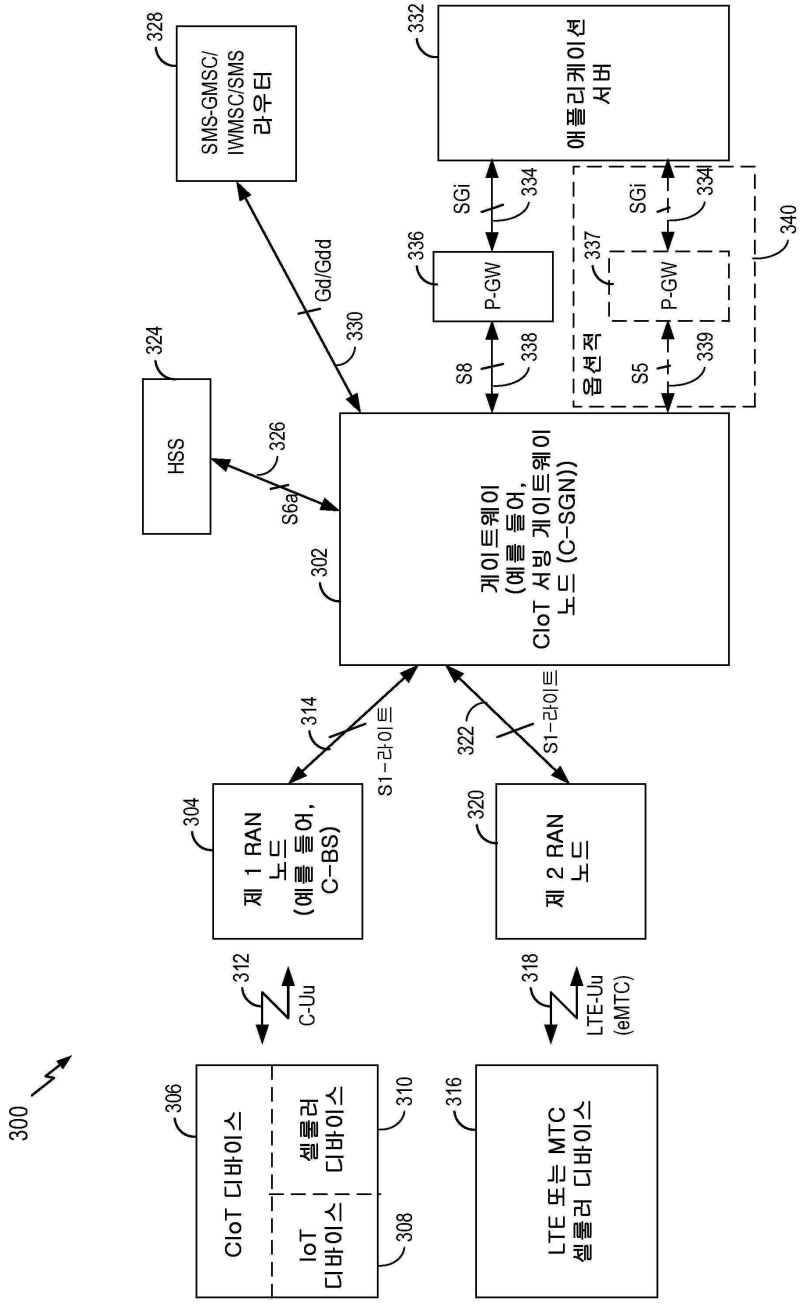
도면1



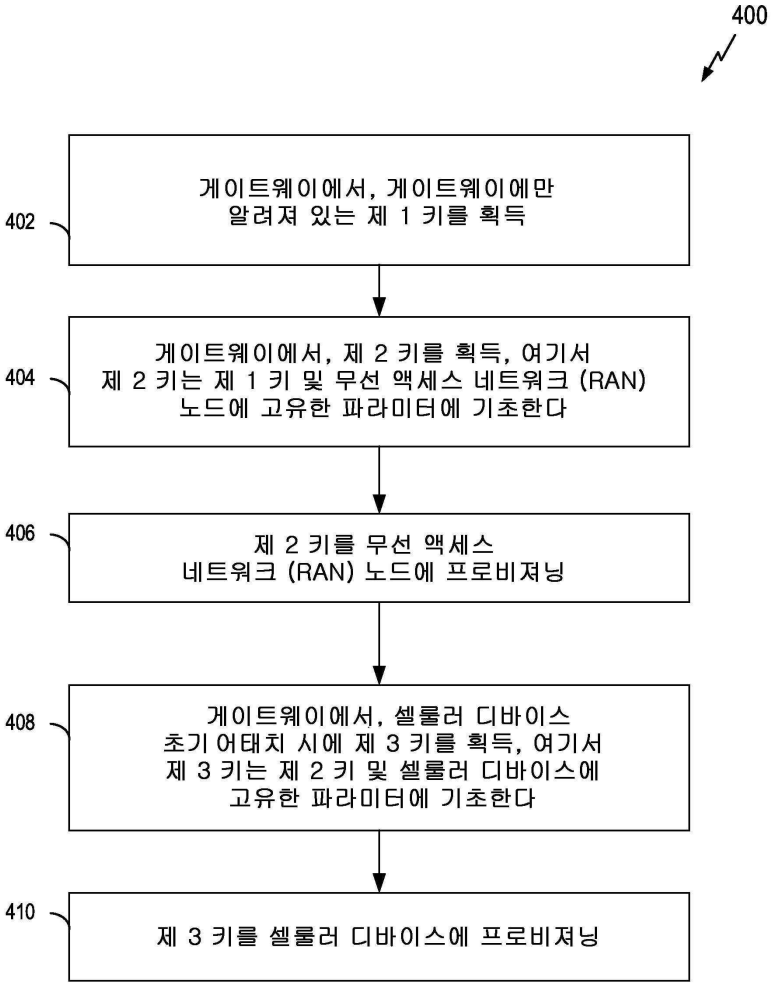
도면2


200
206
CIoT 디바이스
IoT 디바이스
셀룰러 디바이스
210
208
212
C-Uu
204
제 1 RAN 노드 (예를 들어, C-BS)
214
S1-라이트
202
게이트웨이 (예를 들어, CIoT 서빙 게이트웨이 노드 (C-SGN))
224
HSS
226
S6a
228
SMS-GMSC/ IWMSC/SMS 라우터
Gd/Gdd
230
232
애플리케이션 서버
SGi
234
240
옵션적
237
P-GW
SGi
234
S5
239
222
S1-라이트
220
제 2 RAN 노드
218
LTE-Uu (eMTC)
216
LTE 또는 MTC 셀룰러 디바이스

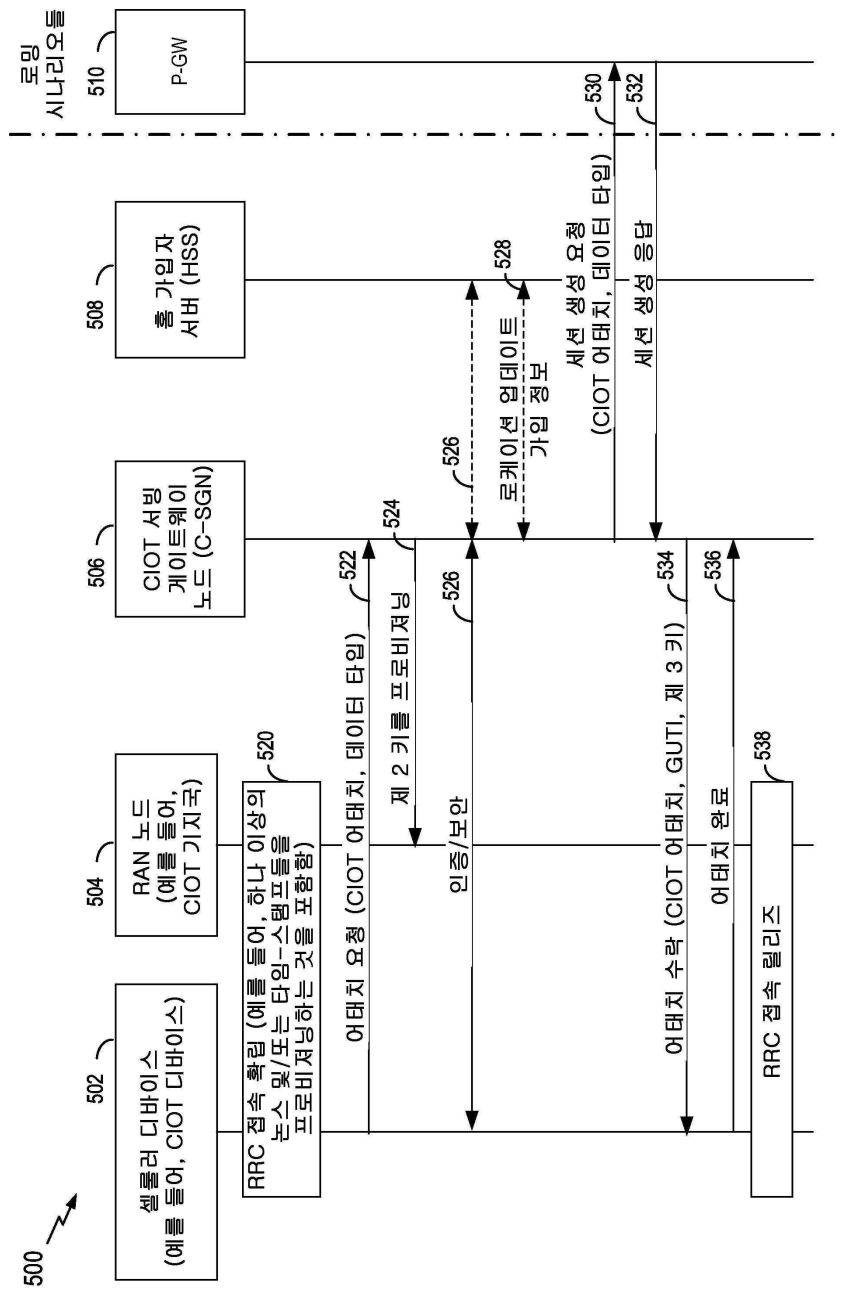
도면3


300
306
CIoT 디바이스
310
셀룰러 디바이스
308
IoT 디바이스
316
LTE 또는 MTC 셀룰러 디바이스
312
C-Uu
318
LTE-Uu (eMTC)
304
제 1 RAN 노드 (예를 들어, C-BS)
320
제 2 RAN 노드
314
S1-라이트
322
S1-라이트
302
게이트웨이 (예를 들어, CIoT 서빙 게이트웨이 노드 (C-SGN))
326
S6a
324
HSS
330
Gd/Gdd
328
SMS-GMSC/ IWMSC/SMS 라우터
336
P-GW
338
S8
334
SGi
332
애플리케이션 서버
340
옵션적
337
P-GW
339
S5
334
SGi

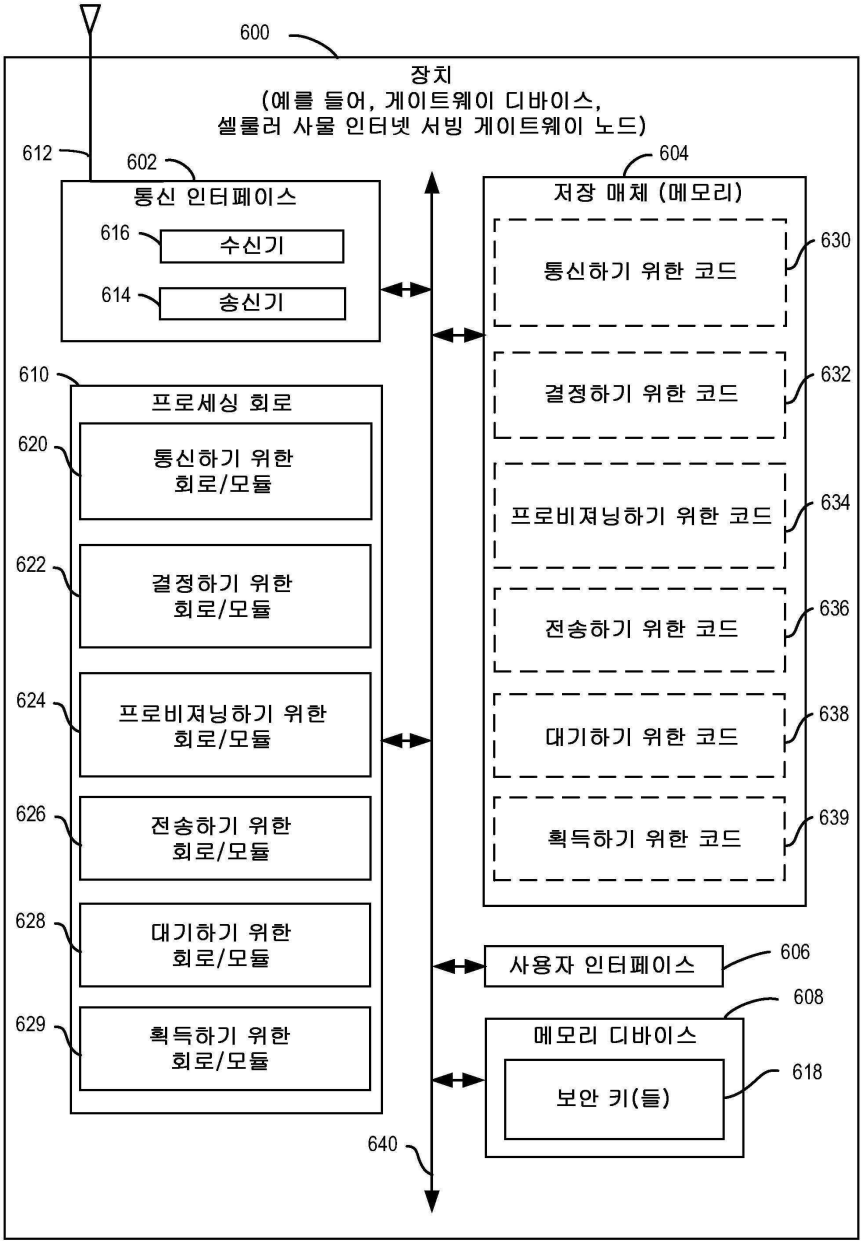
도면4


400
402
게이트웨이에서, 게이트웨이에만 알려져 있는 제 1 키를 획득
404
게이트웨이에서, 제 2 키를 획득, 여기서 제 2 키는 제 1 키 및 무선 액세스 네트워크 (RAN) 노드에 고유한 파라미터에 기초한다
406
제 2 키를 무선 액세스 네트워크 (RAN) 노드에 프로비져닝
408
게이트웨이에서, 셀룰러 디바이스 초기 어태치 시에 제 3 키를 획득, 여기서 제 3 키는 제 2 키 및 셀룰러 디바이스에 고유한 파라미터에 기초한다
410
제 3 키를 셀룰러 디바이스에 프로비져닝

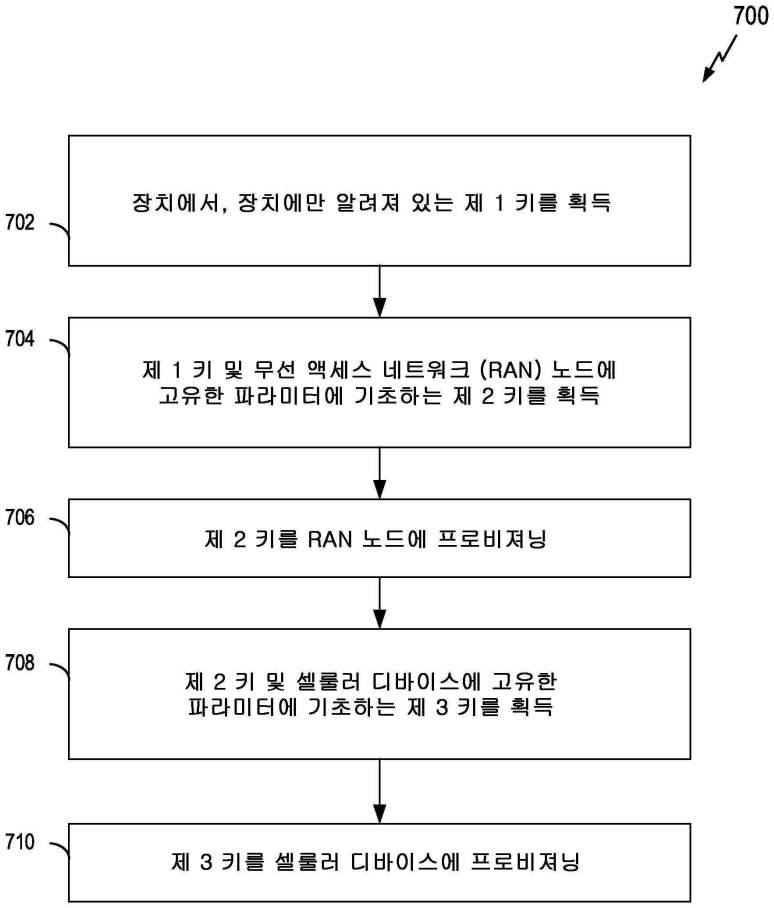
도면5


500
셀룰러 디바이스
(예를 들어, CIOT 디바이스)
502
RAN 노드
(예를 들어,
CIOT 기지국)
504
CIOT 서빙
게이트웨이
노드 (C-SGN)
506
홈 가입자
서버 (HSS)
508
P-GW
510
로밍
시나리오들
RRC 접속 확립 (예를 들어, 하나 이상의
논스 및/또는 타임-스탬프들을
프로비져닝하는 것을 포함함)
520
어태치 요청 (CIOT 어태치, 데이터 타입)
522
제 2 키를 프로비져닝
524
인증/보안
526
로케이션 업데이트
가입 정보
528
세션 생성 요청
(CIOT 어태치, 데이터 타입)
530
세션 생성 응답
532
어태치 수락 (CIOT 어태치, GUTI, 제 3 키)
534
어태치 완료
536
RRC 접속 릴리즈
538

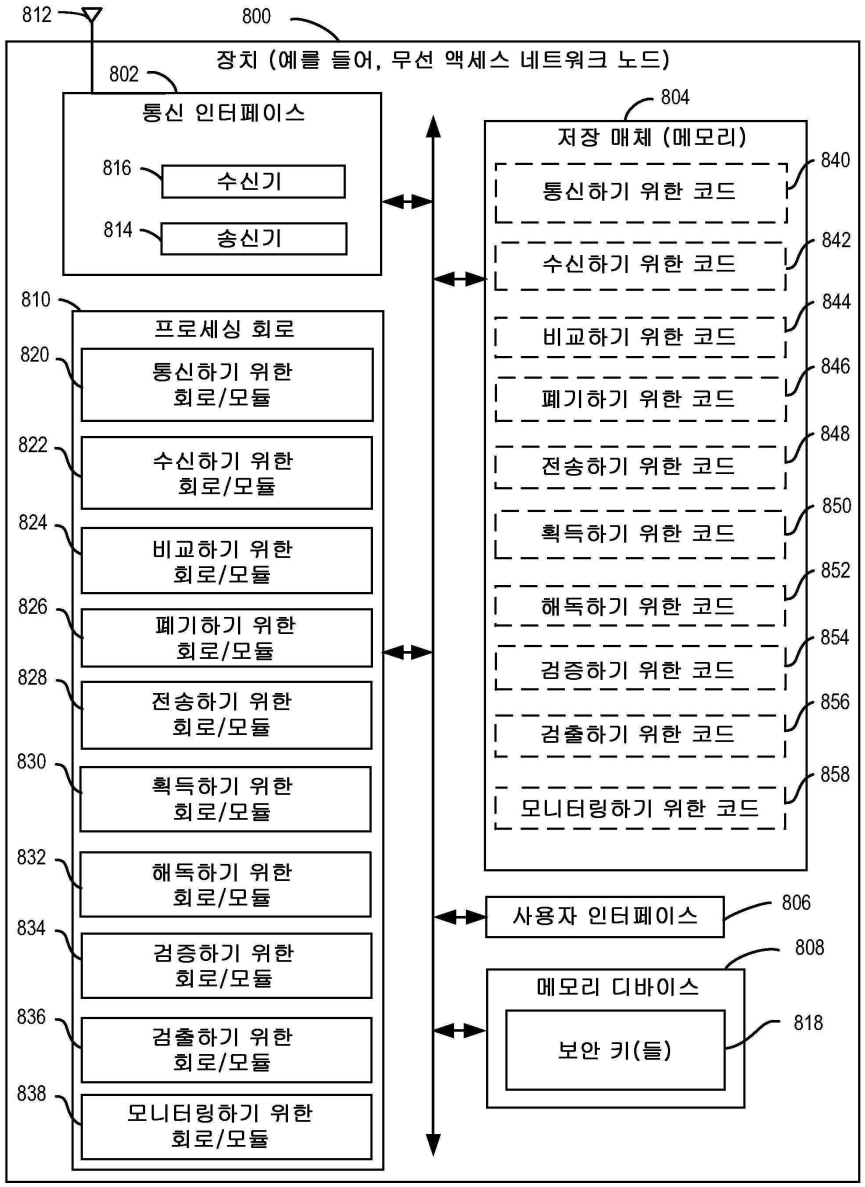
도면6


600
장치
(예를 들어, 게이트웨이 디바이스,
셀룰러 사물 인터넷 서빙 게이트웨이 노드)
612
602
통신 인터페이스
616
수신기
614
송신기
604
저장 매체 (메모리)
630
통신하기 위한 코드
632
결정하기 위한 코드
634
프로비져닝하기 위한 코드
636
전송하기 위한 코드
638
대기하기 위한 코드
639
획득하기 위한 코드
610
프로세싱 회로
620
통신하기 위한
회로/모듈
622
결정하기 위한
회로/모듈
624
프로비져닝하기 위한
회로/모듈
626
전송하기 위한
회로/모듈
628
대기하기 위한
회로/모듈
629
획득하기 위한
회로/모듈
606
사용자 인터페이스
608
메모리 디바이스
618
보안 키(들)
640

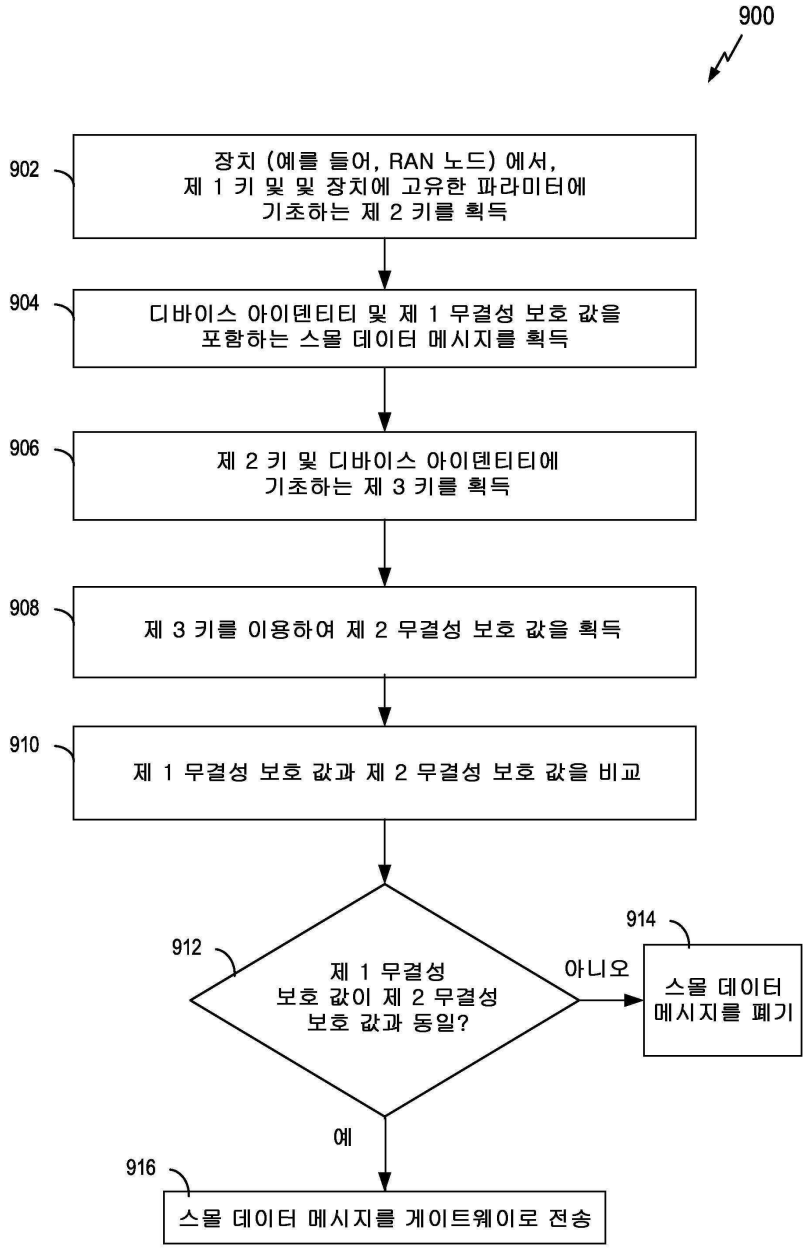
도면7


700
702
장치에서, 장치에만 알려져 있는 제 1 키를 획득
704
제 1 키 및 무선 액세스 네트워크 (RAN) 노드에 고유한 파라미터에 기초하는 제 2 키를 획득
706
제 2 키를 RAN 노드에 프로비져닝
708
제 2 키 및 셀룰러 디바이스에 고유한 파라미터에 기초하는 제 3 키를 획득
710
제 3 키를 셀룰러 디바이스에 프로비져닝

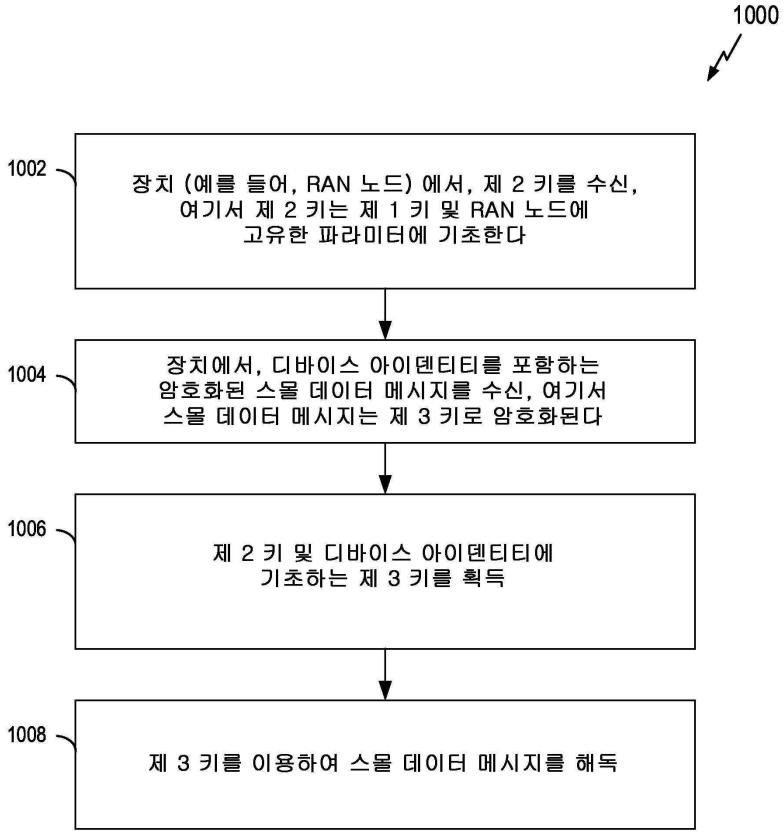
도면8


812
800
장치 (예를 들어, 무선 액세스 네트워크 노드)
802
통신 인터페이스
816
수신기
814
송신기
804
저장 매체 (메모리)
840
통신하기 위한 코드
842
수신하기 위한 코드
844
비교하기 위한 코드
846
폐기하기 위한 코드
848
전송하기 위한 코드
850
획득하기 위한 코드
852
해독하기 위한 코드
854
검증하기 위한 코드
856
검출하기 위한 코드
858
모니터링하기 위한 코드
810
프로세싱 회로
820
통신하기 위한 회로/모듈
822
수신하기 위한 회로/모듈
824
비교하기 위한 회로/모듈
826
폐기하기 위한 회로/모듈
828
전송하기 위한 회로/모듈
830
획득하기 위한 회로/모듈
832
해독하기 위한 회로/모듈
834
검증하기 위한 회로/모듈
836
검출하기 위한 회로/모듈
838
모니터링하기 위한 회로/모듈
사용자 인터페이스
806
808
메모리 디바이스
보안 키(들)
818

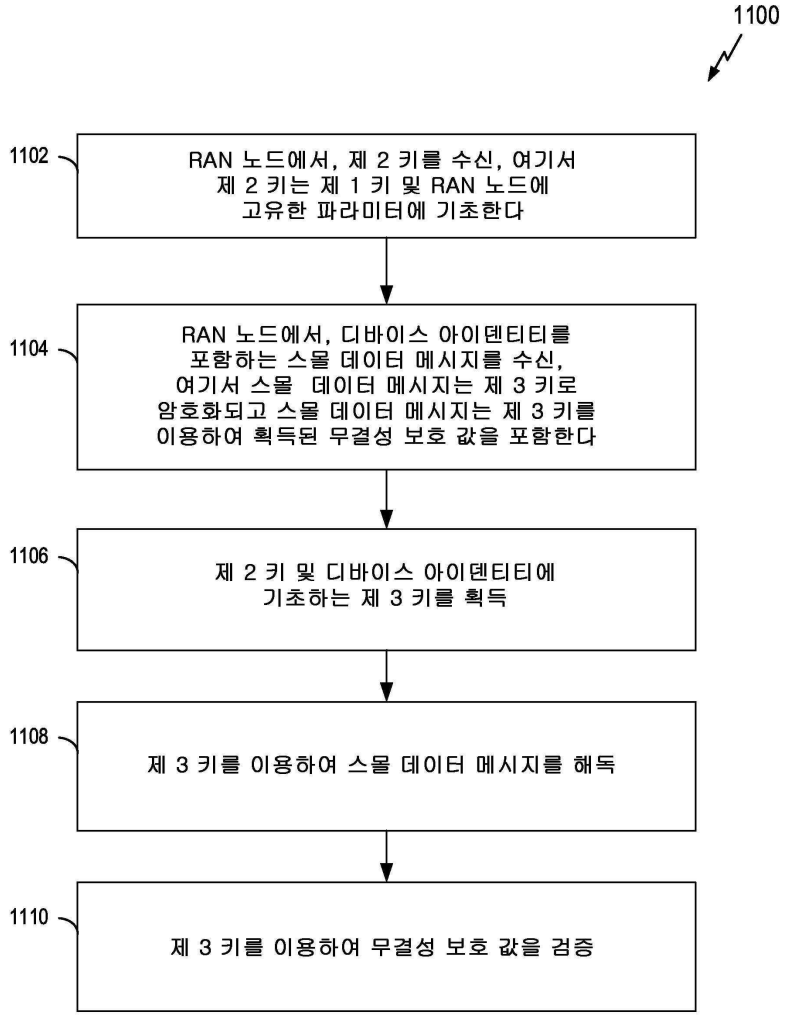
도면9


900
902
장치 (예를 들어, RAN 노드) 에서,
제 1 키 및 및 장치에 고유한 파라미터에
기초하는 제 2 키를 획득
904
디바이스 아이덴티티 및 제 1 무결성 보호 값을
포함하는 스몰 데이터 메시지를 획득
906
제 2 키 및 디바이스 아이덴티티에
기초하는 제 3 키를 획득
908
제 3 키를 이용하여 제 2 무결성 보호 값을 획득
910
제 1 무결성 보호 값과 제 2 무결성 보호 값을 비교
912
제 1 무결성
보호 값이 제 2 무결성
보호 값과 동일?
아니오
914
스몰 데이터
메시지를 폐기
예
916
스몰 데이터 메시지를 게이트웨이로 전송

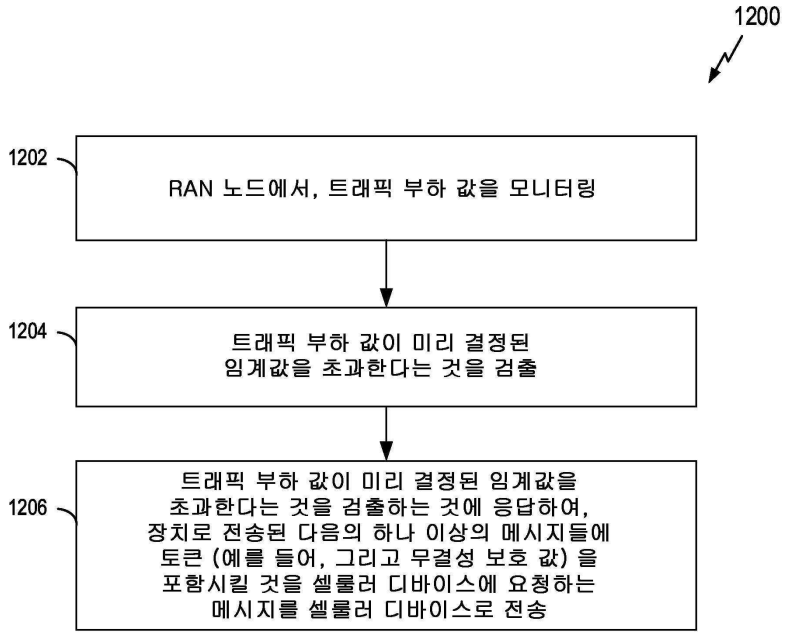
도면10


1000
1002
장치 (예를 들어, RAN 노드) 에서, 제 2 키를 수신, 여기서 제 2 키는 제 1 키 및 RAN 노드에 고유한 파라미터에 기초한다
1004
장치에서, 디바이스 아이덴티티를 포함하는 암호화된 스몰 데이터 메시지를 수신, 여기서 스몰 데이터 메시지는 제 3 키로 암호화된다
1006
제 2 키 및 디바이스 아이덴티티에 기초하는 제 3 키를 획득
1008
제 3 키를 이용하여 스몰 데이터 메시지를 해독

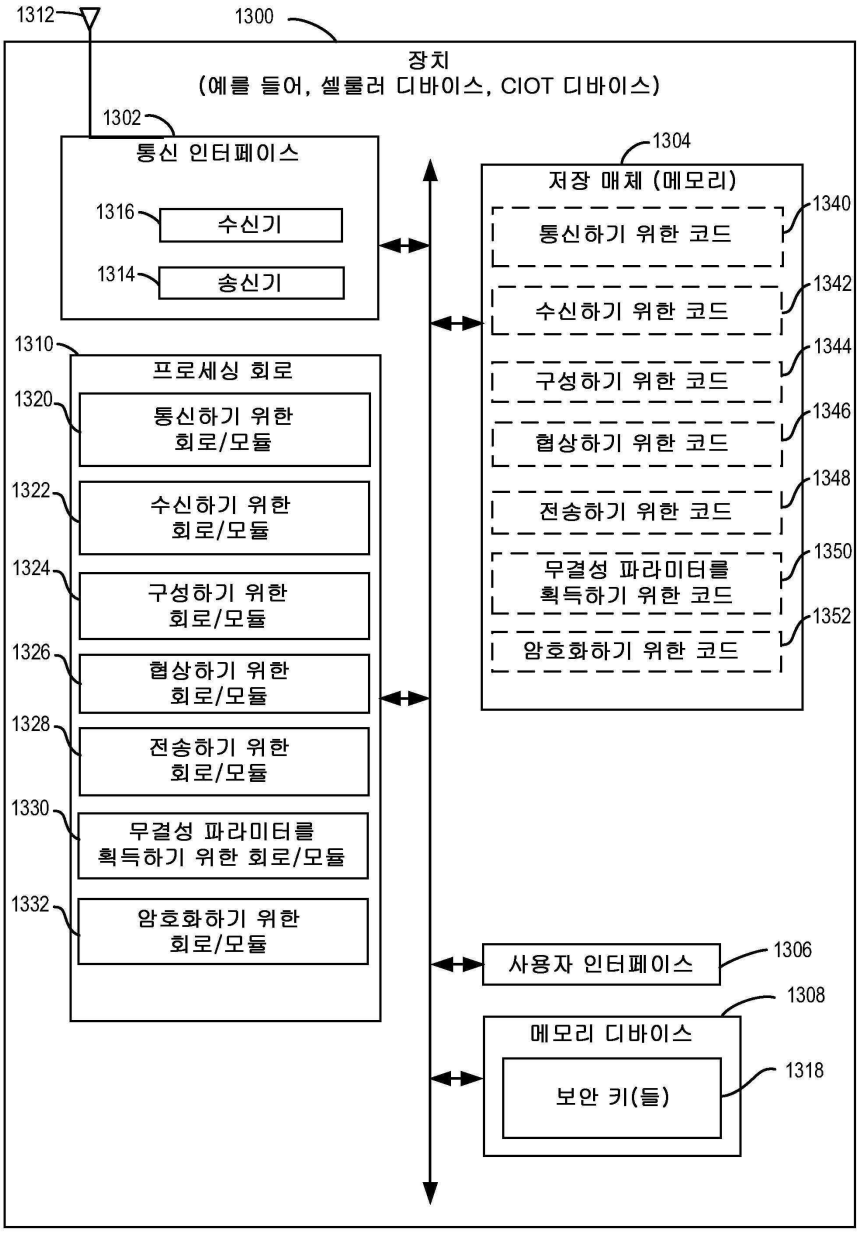
도면11


1100
1102
RAN 노드에서, 제 2 키를 수신, 여기서 제 2 키는 제 1 키 및 RAN 노드에 고유한 파라미터에 기초한다
1104
RAN 노드에서, 디바이스 아이덴티티를 포함하는 스몰 데이터 메시지를 수신, 여기서 스몰 데이터 메시지는 제 3 키로 암호화되고 스몰 데이터 메시지는 제 3 키를 이용하여 획득된 무결성 보호 값을 포함한다
1106
제 2 키 및 디바이스 아이덴티티에 기초하는 제 3 키를 획득
1108
제 3 키를 이용하여 스몰 데이터 메시지를 해독
1110
제 3 키를 이용하여 무결성 보호 값을 검증

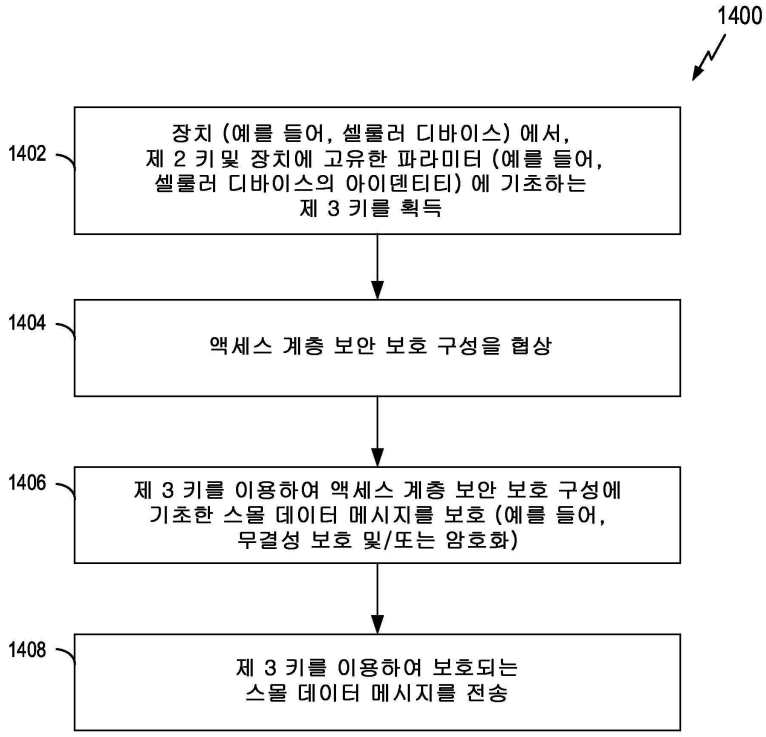
도면12


1200
1202
RAN 노드에서, 트래픽 부하 값을 모니터링
1204
트래픽 부하 값이 미리 결정된 임계값을 초과한다는 것을 검출
1206
트래픽 부하 값이 미리 결정된 임계값을 초과한다는 것을 검출하는 것에 응답하여, 장치로 전송된 다음의 하나 이상의 메시지들에 토큰 (예를 들어, 그리고 무결성 보호 값) 을 포함시킬 것을 셀룰러 디바이스에 요청하는 메시지를 셀룰러 디바이스로 전송

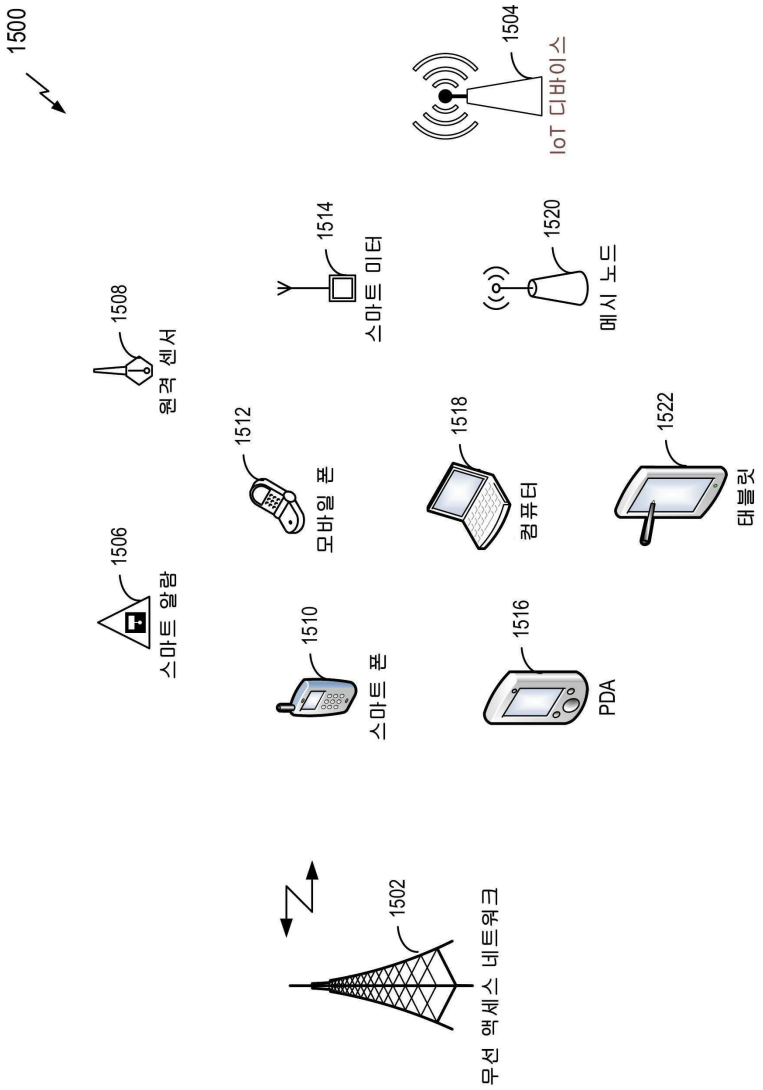
도면13


1312
1300
장치
(예를 들어, 셀룰러 디바이스, CIOT 디바이스)
1302
통신 인터페이스
1316
수신기
1314
송신기
1304
저장 매체 (메모리)
1340
통신하기 위한 코드
1342
수신하기 위한 코드
1344
구성하기 위한 코드
1346
협상하기 위한 코드
1348
전송하기 위한 코드
1350
무결성 파라미터를 획득하기 위한 코드
1352
암호화하기 위한 코드
1310
프로세싱 회로
1320
통신하기 위한 회로/모듈
1322
수신하기 위한 회로/모듈
1324
구성하기 위한 회로/모듈
1326
협상하기 위한 회로/모듈
1328
전송하기 위한 회로/모듈
1330
무결성 파라미터를 획득하기 위한 회로/모듈
1332
암호화하기 위한 회로/모듈
사용자 인터페이스
1306
1308
메모리 디바이스
1318
보안 키(들)

도면14


1400
1402
장치 (예를 들어, 셀룰러 디바이스) 에서,
제 2 키 및 장치에 고유한 파라미터 (예를 들어,
셀룰러 디바이스의 아이덴티티) 에 기초하는
제 3 키를 획득
1404
액세스 계층 보안 보호 구성을 협상
1406
제 3 키를 이용하여 액세스 계층 보안 보호 구성에
기초한 스몰 데이터 메시지를 보호 (예를 들어,
무결성 보호 및/또는 암호화)
1408
제 3 키를 이용하여 보호되는
스몰 데이터 메시지를 전송

도면15


1500
1504
IoT 디바이스
1514
스마트 미터
1520
메시 노드
1508
원격 센서
1512
모바일 폰
1518
컴퓨터
1522
태블릿
1506
스마트 알람
1510
스마트 폰
1516
PDA
1502
무선 액세스 네트워크