



등록특허 10-2727663



(19) 대한민국특허청(KR)  
(12) 등록특허공보(B1)

(45) 공고일자 2024년11월06일  
(11) 등록번호 10-2727663  
(24) 등록일자 2024년11월04일

- (51) 국제특허분류(Int. Cl.)  
*H04W 12/04* (2021.01) *H04L 9/40* (2022.01)  
*H04W 12/10* (2021.01)
- (52) CPC특허분류  
*H04W 12/041* (2021.01)  
*H04L 63/062* (2013.01)
- (21) 출원번호 10-2020-7009116
- (22) 출원일자(국제) 2018년09월29일  
심사청구일자 2021년09월01일
- (85) 번역문제출일자 2020년03월30일
- (65) 공개번호 10-2020-0061348
- (43) 공개일자 2020년06월02일
- (86) 국제출원번호 PCT/US2018/053661
- (87) 국제공개번호 WO 2019/070542  
국제공개일자 2019년04월11일
- (30) 우선권주장  
62/567,086 2017년10월02일 미국(US)  
16/146,709 2018년09월28일 미국(US)

- (56) 선행기술조사문헌  
비특허문헌1(3GPP S3\_171605)\*  
비특허문헌2(3GPP S3\_172010)\*  
비특허문헌3(3GPP S3\_171053)\*
- \*는 심사관에 의하여 인용된 문헌

전체 청구항 수 : 총 47 항

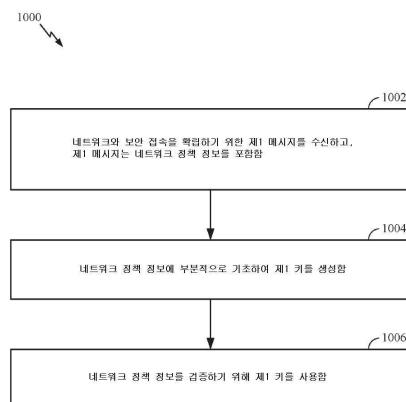
심사관 : 이준석

- (54) 발명의 명칭 키 생성에서 네트워크 정책들의 통합

**(57) 요 약**

본 개시는 예를 들어, 보안 방식으로 네트워크 정책 정보를 제공하기 위해 적용될 수 있는 기술들을 제공한다. 일부 경우들에서, UE는 네트워크와 보안 접속을 확립하기 위한 제1 메시지를 수신하고 – 제1 메시지는 네트워크 정책 정보를 포함함 –, 네트워크 정책 정보에 부분적으로 기초하여 제1 키를 생성하고, 제1 키를 사용하여 네트워크 정책 정보를 검증할 수 있다.

대 표 도 - 도10



(52) CPC특허분류

*H04L 63/123* (2013.01)

*H04L 63/20* (2013.01)

*H04W 12/106* (2021.01)

---

## 명세서

### 청구범위

#### 청구항 1

사용자 장비(UE)에 의한 무선 통신을 위한 방법으로서,

네트워크와 보안 접속을 확립하기 위한 제1 메시지를 수신하는 단계 – 상기 제1 메시지는 네트워크 정책 정보를 포함하고, 그리고 상기 네트워크 정책 정보는 상기 네트워크의 보안 특징들을 포함함 –;

키 유도 함수(KDF)에 의해 제1 키를 생성하는 단계 – 제2 키 및 상기 네트워크 정책 정보는 상기 KDF에 대한 입력들임 –; 및

상기 제1 키에 적어도 부분적으로 기초하여 상기 네트워크 정책 정보를 검증하는 단계를 포함하는, 무선 통신을 위한 방법.

#### 청구항 2

제1 항에 있어서,

상기 네트워크 정책 정보를 검증하는 것은 상기 제1 키에 부분적으로 기초하여 상기 제1 메시지가 유효한지 여부를 결정하는 것을 포함하는, 무선 통신을 위한 방법.

#### 청구항 3

제2 항에 있어서,

상기 제1 메시지는 제3 키로부터 유도된 보호 키로 무결성 보호되고; 그리고

상기 제1 메시지가 유효한지 여부를 결정하는 것은 상기 제1 키에 기초하여 상기 제1 메시지의 무결성 검증을 수행하는 것을 포함하는, 무선 통신을 위한 방법.

#### 청구항 4

제2 항에 있어서,

상기 결정이 상기 제1 메시지가 유효한 것으면, 상기 네트워크와 보안 접속을 확립하는 단계를 더 포함하는, 무선 통신을 위한 방법.

#### 청구항 5

제1 항에 있어서,

상기 제1 메시지는 상기 네트워크 정책 정보가 유효한 시간의 양을 더 포함하는, 무선 통신을 위한 방법.

#### 청구항 6

제5 항에 있어서,

상기 제1 키는 AMF(access and mobility management function) 키이고 그리고 상기 제2 키는 상기 네트워크 내의 상기 UE와 SEAF(security anchor function) 사이에 공유되는 앵커(anchor) 키인, 무선 통신을 위한 방법.

#### 청구항 7

제6 항에 있어서,

상기 방법은, 상기 제1 메시지를 수신하기 전에, 상기 SEAF와 인증 또는 등록 절차 중 적어도 하나를 수행하는 단계를 더 포함하고, 상기 앵커 키는 상기 인증 또는 등록 절차 중 적어도 하나에 기초하여 확립되는, 무선 통신을 위한 방법.

### 청구항 8

제1 항에 있어서,

상기 네트워크 정책 정보는, 상기 UE가 상기 네트워크와 통신 세션을 확립할 때 상기 네트워크 내의 SMF(session management function)로부터 세션 관리 토큰을 수신할지 여부의 표시를 포함하는, 무선 통신을 위한 방법.

### 청구항 9

제1 항에 있어서,

상기 제1 메시지는 상기 네트워크 내의 AMF(access and mobility management function)로부터 수신되는, 무선 통신을 위한 방법.

### 청구항 10

제9 항에 있어서,

상기 네트워크 정책 정보는 상기 AMF가 상기 네트워크 내의 SEAF(security anchor function)와 코로케이트되는지 여부의 표시를 포함하는, 무선 통신을 위한 방법.

### 청구항 11

제9 항에 있어서,

상기 네트워크 정책 정보는 상기 AMF의 보안 레벨을 포함하는, 무선 통신을 위한 방법.

### 청구항 12

제1 항에 있어서,

상기 제1 메시지는 상기 네트워크 내의 AMF(access and mobility management function)로부터 수신되고; 그리고

상기 보안 접속을 확립하는 것은 상기 AMF에 제2 메시지를 전송하는 것을 포함하는, 무선 통신을 위한 방법.

### 청구항 13

제12 항에 있어서,

상기 제1 메시지는 SMC(security mode command) 메시지이고; 그리고

상기 제2 메시지는 SMC 완료 메시지인, 무선 통신을 위한 방법.

### 청구항 14

제12 항에 있어서,

상기 보안 접속은 NAS(non-access stratum) 보안 접속을 포함하는, 무선 통신을 위한 방법.

### 청구항 15

제1 항에 있어서,

상기 방법은, 상기 네트워크에 UE 정책 정보를 전송하는 단계를 더 포함하고, 상기 UE 정책 정보는 UE 능력 정보 또는 UE 보안 정보 중 적어도 하나를 포함하는, 무선 통신을 위한 방법.

### 청구항 16

제15 항에 있어서,

상기 제1 키를 생성하는 것은 상기 네트워크에 전송되는 상기 UE 정책 정보에 기초하는, 무선 통신을 위한 방법.

### 청구항 17

제15 항에 있어서,

상기 네트워크 정책 정보는 상기 UE 정책 정보에 기초하는, 무선 통신을 위한 방법.

### 청구항 18

SEAF(security anchor function)에 의한 무선 통신을 위한 방법으로서,

키 유도 함수(KDF)에 제2 키 및 네트워크 정책 정보를 입력함으로써 네트워크 노드에 대한 제1 키를 생성하는 단계 – 상기 네트워크 정책 정보는 네트워크의 보안 특징들을 포함하고, 그리고 상기 제1 키는 사용자 장비(UE)와 상기 네트워크 노드 사이의 보안 접속을 확립하기 위해 사용가능함 –; 및

상기 네트워크 노드에 상기 제1 키를 전송하는 단계를 포함하는, 무선 통신을 위한 방법.

### 청구항 19

제18 항에 있어서,

상기 방법은, 상기 제1 키를 생성하기 전에 상기 UE와의 인증 절차 또는 등록 절차 중 적어도 하나에 참여하는 단계를 더 포함하고, 상기 참여하는 것은 상기 UE와 상기 SEAF 사이에 공유될 앵커 키를 확립하는 것을 포함하는, 무선 통신을 위한 방법.

### 청구항 20

제19 항에 있어서,

상기 제1 키는 AMF(access and mobility management function) 키이고 그리고 상기 제2 키는 상기 앵커 키인, 무선 통신을 위한 방법.

### 청구항 21

제20 항에 있어서,

상기 네트워크 노드에 상기 네트워크 정책 정보를 전송하는 단계를 더 포함하는, 무선 통신을 위한 방법.

### 청구항 22

제18 항에 있어서,

상기 네트워크 정책 정보는 상기 네트워크 노드가 상기 네트워크 내의 상기 SEAF와 코로케이트되는지 여부의 표시를 포함하는, 무선 통신을 위한 방법.

### 청구항 23

제18 항에 있어서,

상기 네트워크 정책 정보는 상기 네트워크 노드의 보안 레벨을 포함하는, 무선 통신을 위한 방법.

### 청구항 24

제18 항에 있어서,

상기 네트워크 정책 정보는, 상기 네트워크 내의 SMF(session management function)가 상기 UE와 상기 네트워크 사이의 통신 세션에 대한 세션 관리 토큰을 생성하고 그리고 상기 UE에 상기 세션 관리 토큰을 송신할 것인지 여부의 표시를 포함하는, 무선 통신을 위한 방법.

### 청구항 25

제18 항에 있어서,

상기 방법은, 상기 UE의 정책 정보를 포함하는 메시지를 수신하는 단계를 더 포함하고, 상기 UE 정책 정보는 UE

능력 정보 또는 UE 보안 정보 중 적어도 하나를 포함하는, 무선 통신을 위한 방법.

### 청구항 26

제25 항에 있어서,

상기 제1 키는 상기 UE 정책 정보에 추가로 기초하여 생성되는, 무선 통신을 위한 방법.

### 청구항 27

제25 항에 있어서,

상기 메시지는 등록 메시지 또는 어태치 요청 메시지를 포함하는, 무선 통신을 위한 방법.

### 청구항 28

제25 항에 있어서,

상기 네트워크 정책 정보는 상기 UE 정책 정보에 기초하여 결정되는, 무선 통신을 위한 방법.

### 청구항 29

제18 항에 있어서,

상기 네트워크 노드는 상기 네트워크 내의 AMF(access and mobility management function)인, 무선 통신을 위한 방법.

### 청구항 30

사용자 장비(UE)로서,

명령들을 저장하기 위한 메모리; 및

프로세서를 포함하고,

상기 프로세서가 상기 명령들을 실행할 때, 상기 프로세서는:

네트워크와 보안 접속을 확립하기 위한 제1 메시지를 수신하고 — 상기 제1 메시지는 네트워크 정책 정보를 포함하고, 그리고 상기 네트워크 정책 정보는 상기 네트워크의 보안 특징들을 포함함 —;

키 유도 함수(KDF)에 의해 제1 키를 생성하고 — 제2 키 및 상기 네트워크 정책 정보는 상기 KDF에 대한 입력들임 —; 그리고

상기 제1 키에 적어도 부분적으로 기초하여 상기 네트워크 정책 정보를 검증하도록 구성되는, 사용자 장비(UE).

### 청구항 31

제30 항에 있어서,

상기 프로세서는, 상기 제1 키에 부분적으로 기초하여 상기 제1 메시지가 유효한지 여부를 결정함으로써 상기 네트워크 정책 정보를 검증하도록 구성되는, 사용자 장비(UE).

### 청구항 32

제31 항에 있어서,

상기 제1 메시지는 제3 키로부터 유도된 보호 키로 무결성 보호되고; 그리고

상기 프로세서는, 상기 제1 키에 기초하여 상기 제1 메시지의 무결성 검증을 수행함으로써 상기 제1 메시지가 유효한지 여부를 결정하도록 구성되는, 사용자 장비(UE).

### 청구항 33

제31 항에 있어서,

상기 프로세서는, 상기 결정이 상기 제1 메시지가 유효한 것이면, 상기 네트워크와 보안 접속을 확립하도록 구성되는, 사용자 장비(UE).

#### 청구항 34

제30 항에 있어서,

상기 제1 키는 AMF(access and mobility management function) 키이고 그리고 상기 제2 키는 상기 네트워크 내의 상기 UE와 SEAF(security anchor function) 사이에 공유되는 앵커(anchor) 키인, 사용자 장비(UE).

#### 청구항 35

제34 항에 있어서,

상기 프로세서는, 상기 제1 메시지를 수신하기 전에, 상기 SEAF와 인증 또는 등록 절차 중 적어도 하나를 수행하도록 구성되고, 상기 앵커 키는 상기 인증 또는 등록 절차 중 적어도 하나에 기초하여 확립되는, 사용자 장비(UE).

#### 청구항 36

제30 항에 있어서,

상기 네트워크 정책 정보는 AMF(access and mobility function)의 보안 레벨을 포함하는, 사용자 장비(UE).

#### 청구항 37

제30 항에 있어서,

상기 제1 메시지는 상기 네트워크 내의 AMF(access and mobility management function)로부터 수신되고; 그리고

상기 프로세서는, 상기 AMF에 제2 메시지를 전송함으로써 상기 보안 접속을 확립하도록 구성되는, 사용자 장비(UE).

#### 청구항 38

제37 항에 있어서,

상기 제1 메시지는 SMC(security mode command) 메시지이고; 그리고

상기 제2 메시지는 SMC 완료 메시지인, 사용자 장비(UE).

#### 청구항 39

SEAF(security anchor function)로서,

명령들을 저장하기 위한 메모리; 및

프로세서를 포함하고,

상기 프로세서가 상기 명령들을 실행할 때, 상기 프로세서는:

키 유도 함수(KDF)에 제2 키 및 네트워크 정책 정보를 입력함으로써 네트워크 노드에 대한 제1 키를 생성하고 – 상기 네트워크 정책 정보는 네트워크의 보안 특징들을 포함하고, 그리고 상기 제1 키는 사용자 장비(UE)와 상기 네트워크 노드 사이의 보안 접속을 확립하기 위해 사용가능함 –; 그리고

상기 네트워크 노드에 상기 제1 키를 전송하도록

구성되는, SEAF.

#### 청구항 40

제39 항에 있어서,

상기 프로세서는, 상기 제1 키를 생성하기 전에 상기 UE와의 인증 절차 또는 등록 절차 중 적어도 하나에 참여

하도록 구성되고, 상기 참여하는 것은 상기 UE와 상기 SEAF 사이에 공유될 앵커 키를 확립하는 것을 포함하는, SEAF.

#### 청구항 41

제40 항에 있어서,

상기 제1 키는 AMF(access and mobility management function) 키이고 그리고 상기 제2 키는 상기 앵커 키인, SEAF.

#### 청구항 42

제39 항에 있어서,

상기 프로세서는 상기 네트워크 노드에 상기 네트워크 정책 정보를 전송하도록 구성되는, SEAF.

#### 청구항 43

제39 항에 있어서,

상기 네트워크 정책 정보는 상기 네트워크 노드가 상기 네트워크 내의 상기 SEAF와 코로케이트되는지 여부의 표시를 포함하는, SEAF.

#### 청구항 44

제39 항에 있어서,

상기 네트워크 정책 정보는 상기 네트워크 노드의 보안 레벨을 포함하는, SEAF.

#### 청구항 45

제39 항에 있어서,

상기 프로세서는, 상기 UE의 정책 정보를 포함하는 메시지를 수신하도록 구성되고, 상기 UE 정책 정보는 UE 능력 정보 또는 UE 보안 정보 중 적어도 하나를 포함하는, SEAF.

#### 청구항 46

제45 항에 있어서,

상기 메시지는 등록 메시지 또는 어태치 요청 메시지를 포함하는, SEAF.

#### 청구항 47

제39 항에 있어서,

상기 네트워크 노드는 AMF(access and mobility management function)인, SEAF.

### 발명의 설명

#### 기술 분야

[0001] 본 출원은, 2017년 10월 2일에 출원된 미국 가특허 출원 일련번호 제62/567,086호에 대한 이익을 주장하는, 2018년 9월 28일에 출원된 미국 출원 제16/146,709호에 대해 우선권을 주장하며, 상기 출원은 그 전체가 인용에 의해 본원에 통합된다.

[0002] 본 개시의 특정 양상들은 일반적으로 무선 통신들에 관한 것이고, 더 상세하게는, 네트워크에서 보안 통신들을 확립하기 위한 방법들 및 장치에 관한 것이다.

#### 배경 기술

[0003] 무선 통신 시스템들은 텔레포니(telephony), 비디오, 데이터, 메시징, 및 브로드캐스트들과 같은 다양

한 전기통신 서비스들을 제공하도록 널리 배치되어 있다. 통상적인 무선 통신 시스템들은 이용가능한 시스템 자원들(예를 들어, 대역폭, 송신 전력)을 공유함으로써 다수의 사용자들과의 통신을 지원할 수 있는 다중-액세스 기술들을 이용할 수 있다. 이러한 다중-액세스 기술들의 예들은 LTE(Long Term Evolution) 시스템들, CDMA(code division multiple access) 시스템들, TDMA(time division multiple access) 시스템들, FDMA(frequency division multiple access) 시스템들, OFDMA(orthogonal frequency division multiple access) 시스템들, SC-FDMA(single-carrier frequency division multiple access) 시스템들, 및 TD-SCDMA(time division synchronous code division multiple access) 시스템들을 포함한다.

[0004]

[0004] 일부 예들에서, 무선 다중 액세스 통신 시스템은, 달리 UE(user equipment)들로 공지된 다수의 통신 디바이스들에 대한 통신을 각각 동시에 지원하는 다수의 기지국들을 포함할 수 있다. LTE 또는 LTE-A 네트워크에서, 하나 이상의 기지국들의 세트가 eNodeB(eNB)를 정의할 수 있다. 다른 예들에서(예를 들어, 차세대 또는 5G 네트워크에서), 무선 다중 액세스 통신 시스템은 다수의 CU(central unit)들(예를 들어, CN(central node)들, ANC(access node controller)들 등)과 통신하는 다수의 DU(distributed unit)들(예를 들어, EU(edge unit)들, EN(edge node)들, RH(radio head)들, SRH(smart radio head)들, TRP(transmission reception point)들 등)을 포함할 수 있고, 여기서, 중앙 유닛과 통신하는 하나 이상의 분산형 유닛들의 세트는 액세스 노드(예를 들어, NR BS(new radio base station), NR NB(new radio node-B), 네트워크 노드, 5G NB, gNB 등)를 정의할 수 있다. 기지국 또는 DU는, (예를 들어, 기지국으로부터의 또는 UE로의 송신들을 위한) 다운링크 채널들 및 (예를 들어, UE로부터 기지국 또는 분산형 유닛으로의 송신들을 위한) 업링크 채널들 상에서 UE들의 세트와 통신할 수 있다.

[0005]

[0005] 이러한 다중 액세스 기술들은 상이한 무선 디바이스들이, 도시 레벨, 국가 레벨, 지역 레벨, 및 심지어 글로벌 레벨 상에서 통신할 수 있게 하는 공통 프로토콜을 제공하기 위해 다양한 전기통신 표준들에서 채택되어 왔다. 신흥 전기통신 표준의 예는 NR(new radio), 예를 들어, 5G 라디오 액세스이다. NR은 3GPP(Third Generation Partnership Project)에 의해 공표된 LTE 모바일 표준에 대한 향상들의 세트이다. 이는, 스펙트럼 효율을 개선하고, 비용들을 낮추고, 서비스들을 개선하고, 새로운 스펙트럼을 이용하고, DL(downlink) 상에서 그리고 UL(uplink) 상에서 CP(cyclic prefix)를 갖는 OFDMA를 사용하는 다른 개방형 표준들과 더 양호하게 통합함으로써 모바일 브로드밴드 인터넷 액세스를 더 양호하게 지원할 뿐만 아니라 빔형성, MIMO(multiple-input multiple-output) 안테나 기술 및 캐리어 어그리게이션을 지원하도록 설계된다.

[0006]

[0006] 그러나, 모바일 브로드밴드 액세스에 대한 요구가 계속 증가함에 따라, NR 기술에서의 추가적인 개선들에 대한 필요성이 존재한다. 바람직하게, 이러한 개선들은 다른 다중-액세스 기술들 및 이러한 기술들을 이용하는 전기통신 표준들에 적용가능해야 한다.

## 발명의 내용

[0007]

[0007] 본 개시의 시스템들, 방법들 및 디바이스들 각각은 몇몇 양상들을 갖고, 이 양상들 중 어떠한 단일 양상도 본 발명의 바람직한 속성을 단독으로 담당하지 않는다. 후속하는 청구항들에 의해 표현되는 바와 같은 본 개시의 범위를 제한하지 않고, 이제 일부 특징들이 간략하게 논의될 것이다. 이러한 논의를 고려한 이후, 그리고 특히 "상세한 설명"으로 명명된 섹션을 관독한 이후, 당업자는, 본 개시내용의 특징들이 무선 네트워크에서 개선된 통신들을 포함하는 이점들을 어떻게 제공하는지를 이해할 것이다.

[0008]

[0008] 본 개시의 특정 양상들은 UE(user equipment)에 의한 무선 통신들을 위한 방법을 제공한다. 방법은 일반적으로 네트워크와 보안 접속을 확립하기 위한 제1 메시지를 수신하는 단계를 포함하고, 제1 메시지는 네트워크 정책 정보를 포함한다. 방법은 또한 네트워크 정책 정보에 부분적으로 기초하여 제1 키를 생성하는 단계를 포함한다. 방법은 네트워크 정보를 검증하기 위해 제1 키를 사용하는 단계를 더 포함한다.

[0009]

[0009] 본 개시의 특정 양상들은 SEAF(security anchor function)와 같은 네트워크 노드에 의한 무선 통신들을 위한 방법을 제공한다. 방법은 일반적으로 네트워크 정책 정보에 적어도 부분적으로 기초하여 네트워크 노드에 대한 키를 생성하는 단계를 포함한다. 키는 UE와 네트워크 노드 사이의 보안 접속을 확립하기 위해 사용된다. 방법은 또한 네트워크 노드에 키를 전송하는 단계를 포함한다.

[0010]

[0010] 본 개시의 특정 양상들은 UE(user equipment)에 의한 무선 통신들을 위한 방법을 제공한다. 방법은 일반적으로 네트워크와 인증 절차에 기초하여, 네트워크 내의 UE와 SEAF(security anchor function) 사이에 공유되는 앵커 키를 확립하는 단계를 포함한다. 방법은 또한 네트워크와 보안 접속을 확립하기 위해 제1 메시지를 수신하는 단계를 포함하고, 제1 메시지는 상기 네트워크와의 통신 세션에 대한 네트워크 정책 토큰, 네트워크 정책 정보, 제1 키가 유효한 시간의 제1 양 및 상기 네트워크 정책 토큰이 유효한 시간의 제2 양을 포함한다.

방법은 네트워크와 보안 접속을 확립하기 전에, 공유된 앵커 키로부터 유도된 키, 네트워크 정책 정보, 시간의 제1 양 및 시간의 제2 양에 기초하여 네트워크 정책 토큰이 유효한지 여부를 결정하는 단계를 더 포함한다.

[0011] 본 개시의 특정 양상들은 SEAF(security anchor function)와 같은 네트워크 노드에 의한 무선 통신들을 위한 방법을 제공한다. 방법은 일반적으로 UE와의 인증 절차에 기초하여, 네트워크 내의 SEAF와 UE 사이에 공유되는 앵커 키를 확립하는 단계를 포함한다. 방법은 또한 앵커 키, 네트워크 정책 정보 및 네트워크 정책 토큰이 유효한 시간의 제1 양에 부분적으로 기초하여 네트워크 정책 토큰을 생성하는 단계를 포함한다. 방법은 다른 네트워크 노드에 대한 키를 생성하는 단계, 및 키, 네트워크 정책 정보, 및 네트워크 정책 토큰을 다른 네트워크 노드에 전송하는 단계를 더 포함한다.

[0012] 앞서 설명된 동작들을 수행할 수 있는 방법들, 장치, 시스템들, 컴퓨터 프로그램 제품들 및 프로세싱 시스템들을 포함하는 다수의 다른 양상들이 제공된다.

[0013] 상술한 목적 및 관련되는 목적의 달성을 위해서, 하나 이상의 양상들은, 아래에서 완전히 설명되고 특히 청구항들에서 언급되는 특징들을 포함한다. 하기 설명 및 부가된 도면들은 하나 이상의 양상들의 특정한 예시적인 특징들을 상세히 기술한다. 그러나, 이 특징들은, 다양한 양상들의 원리들이 사용될 수 있는 다양한 방식들 중 일부만을 나타내고, 이 설명은 모든 이러한 양상을 및 이들의 균등물들을 포함하는 것으로 의도된다.

### 도면의 간단한 설명

[0014] 본 개시의 상기 인용된 특징들이 상세히 이해될 수 있는 방식으로, 상기 간략하게 요약된 더 구체적인 설명이 양상들을 참조하여 행해질 수 있으며, 그 양상들 중 일부는 첨부된 도면들에 예시되어 있다. 그러나, 상기 설명이 다른 균등하게 유효한 양상들에 허용될 수 있기 때문에, 첨부된 도면들이 본 개시의 특정한 통상적인 양상들만을 예시하며, 따라서, 본 개시의 범위를 제한하는 것으로 고려되지 않음을 주목해야 한다.

[0015] 도 1은, 본 개시의 특정 양상들에 따른 예시적인 전기통신 시스템을 개념적으로 예시하는 블록도이다.

[0016] 도 2는 본 개시의 특정 양상들에 따른 분산형 RAN의 예시적인 논리적 아키텍처를 예시하는 블록도이다.

[0017] 도 3은 본 개시의 특정 양상들에 따른 분산형 RAN의 예시적인 물리적 아키텍처를 예시하는 도면이다.

[0018] 도 4는 본 개시의 특정 양상들에 따른 예시적인 BS 및 UE(user equipment)의 설계를 개념적으로 예시하는 블록도이다.

[0019] 도 5는 본 개시의 특정 양상들에 따른 통신 프로토콜 스택을 구현하기 위한 예들을 도시하는 도면이다.

[0020] 도 6은 본 개시의 특정 양상들에 따른 DL-중심 서브프레임의 예를 예시한다.

[0021] 도 7은 본 개시의 특정 양상들에 따른 UL-중심 서브프레임의 예를 예시한다.

[0022] 도 8 및 도 9는 본 개시의 특정 양상들에 따라 하나 이상의 코로케이트되지 않은 네트워크 노드들을 갖는 예시적인 5G 아키텍처들을 예시한다.

[0023] 도 10은 본 개시의 특정 양상들에 따른 네트워크에서 무선 통신들을 위한 예시적인 동작들을 예시하는 흐름도이다.

[0024] 도 11은 본 개시의 특정 양상들에 따른 네트워크에서 무선 통신들을 위한 예시적인 동작들을 예시하는 흐름도이다.

[0025] 도 12는 본 개시의 특정 양상들에 따른 예시적인 등록 절차를 예시하는 흐름도이다.

[0026] 도 13은 본 개시의 특정 양상들에 따른 네트워크에서 무선 통신들을 위한 예시적인 동작들을 예시하는 흐름도이다.

[0027] 도 14는 본 개시의 특정 양상들에 따른 네트워크에서 무선 통신들을 위한 예시적인 동작들을 예시하는 흐름도이다.

[0028] 도 15는 본 개시의 특정 양상들에 따른 예시적인 등록 절차를 예시하는 흐름도이다.

[0029] 이해를 용이하게 하기 위해, 가능한 경우, 도면들에 공통된 동일한 엘리먼트들을 지정하기 위해 동일한 참조 부호들이 사용되었다. 일 실시예에서 개시된 엘리먼트들은, 특정 인용이 없이도 다른 실시예들 상에서 유리하게 활용될 수 있는 것으로 고려된다.

## 발명을 실시하기 위한 구체적인 내용

- [0015] [0030] 본 개시의 양상들은 NR(new radio)(새로운 라디오 액세스 기술 또는 5G 기술) 무선 네트워크들과 같은 무선 네트워크들에 대한 장치, 방법들, 프로세싱 시스템들 및 컴퓨터 판독가능 매체들을 제공한다.
- [0016] [0031] NR은 다양한 무선 통신 서비스들, 예를 들어, 넓은 대역폭(예를 들어, 80 MHz 초과)을 타겟팅하는 eMBB(enhanced mobile broadband), 높은 캐리어 주파수(예를 들어, 60 GHz)를 타겟팅하는 밀리미터파(mmW), 역호환불가능한 MTC 기술들을 타겟팅하는 mMTC(massive MTC) 및/또는 URLLC(ultra reliable low latency communications)를 타겟팅하는 미션 크리티컬(mission critical)을 지원할 수 있다. 이러한 서비스들은 레이턴시 및 신뢰도 요건들을 포함할 수 있다. 이러한 서비스들은 또한 각각의 QoS(quality of service) 요건들을 충족하기 위해 상이한 TTI(transmission time intervals)를 가질 수 있다. 또한, 이러한 서비스들은 동일한 서브프레임에서 공존할 수 있다.
- [0017] [0032] NR은 네트워크 슬라이싱의 개념을 도입한다. 예를 들어, 네트워크는 상이한 서비스들, 예를 들어, IoE(internet of everything), URLLC, eMBB, V2V(vehicle-to-vehicle) 통신을 등을 지원할 수 있는 다수의 슬라이스들을 가질 수 있다. 슬라이스는 특정 네트워크 능력들 및 네트워크 특성들을 제공하기 위해 필요한 네트워크 기능들 및 대응하는 자원들의 세트를 포함하는 완전한 로직 네트워크로서 정의될 수 있다.
- [0018] [0033] 일부 양상들에서, 5G NR 시스템은 다양한 상이한 배치 시나리오들을 지원할 수 있다. 특히, 5G 기술 및/또는 서비스 요건들은 진화를 계속하기 때문에, 5G 네트워크에서 하나 이상의 네트워크 노드들에 의해 수행되는 서비스들, 능력들 및/또는 기능들은 달라질 수 있다. 네트워크 아키텍처에서의 변화들이 UE에 알려지지 않을 수 있기 때문에, 특정한 네트워크 구성, 능력들, 보안 구성 등에 대해 UE에 통지하는 것이 유리할 수 있다. 그러나, 현재 기술들을 사용하여 네트워크가 보안 방식으로 네트워크(보안) 구성, 능력들 및 정책들에 대해 UE에 통지하는 것은 가능하지 않을 수 있다.
- [0019] [0034] 예를 들어, 5G 시스템에서, 통상적으로 UE와 서빙 네트워크 사이에는 단일 제어 평면 인터페이스(N1)이 존재한다. 이러한 N1 인터페이스는 일반적으로 UE와 AMF(access and mobility management function) AMF 사이의 NAS(non-access stratum) 접속을 확립하기 위해 사용된다. 그러나, 일부 배치 시나리오들에서, AMF는 네트워크에서 보안 기능들을 담당하지(또는 그에 대한 액세스를 갖지) 않을 수 있다. 따라서, AMF는 UE와의 시그널링 접속을 갖는 유일한 엔티티일 수 있기 때문에, (사기적 또는 악의적) AMF가 네트워크 구성 정보를 인터셉트하고 UE에 제공되는 네트워크 구성 정보를 수정하여 UE와 네트워크 사이의 접속/통신을 손상시킬 수 있는 경우들이 존재할 수 있다. 따라서, 본 개시의 양상들은 네트워크(보안) 구성, 능력들, 네트워크 정책들 등에 대해 UE에 안전하게 통지하기 위한 기술들을 제공한다.
- [0020] [0035] 본 개시의 다양한 양상들은 첨부된 도면들을 참조하여 아래에서 더 완전히 설명된다. 그러나, 본 개시는 많은 상이한 형태들로 구현될 수 있고, 본 개시 전반에 걸쳐 제시되는 임의의 특정 구조 또는 기능에 제한되는 것으로 해석되어서는 안된다. 오히려, 이러한 양상들은, 본 개시가 철저하고 완전해지도록, 그리고 당업자들에게 본 개시의 범위를 완전히 전달하도록 제공된다. 본원의 교시들에 기초하여, 당업자는, 본 개시의 범위가, 본 개시의 임의의 다른 양상과는 독립적으로 구현되든 또는 임의의 다른 양상과 결합되어 구현되든, 본원에 개시된 개시의 임의의 양상을 커버하도록 의도됨을 인식해야 한다. 예를 들어, 본원에서 기술된 임의의 수의 양상들을 사용하여 장치가 구현될 수 있거나 방법이 실시될 수 있다. 또한, 본 개시의 범위는, 본원에 기술된 본 개시의 다양한 양상들에 추가로 또는 그 이외의 다른 구조, 기능 또는 구조 및 기능을 사용하여 실시되는 이러한 장치 또는 방법을 커버하도록 의도된다. 본원에서 개시되는 본 개시의 임의의 양상은 청구항의 하나 이상의 엘리먼트들에 의해 구현될 수 있음을 이해해야 한다.
- [0021] [0036] "예시적인"이라는 단어는, "예, 예증 또는 예시로서 기능하는" 것을 의미하도록 본 명세서에서 사용된다. 본 명세서에서 "예시적인" 것으로 설명되는 임의의 양상은 반드시 다른 양상들에 비해 선호되거나 유리한 것으로 해석될 필요는 없다.
- [0022] [0037] 특정한 양상들이 본 명세서에서 설명되지만, 이 양상들의 많은 변경들 및 치환들은 본 개시의 범위 내에 속한다. 선호되는 양상들의 일부 이익들 및 이점들이 언급되지만, 본 개시의 범위는 특정한 이점들, 사용들 또는 목적들로 제한되도록 의도되지 않는다. 오히려, 본 개시의 양상들은, 상이한 무선 기술들, 시스템 구성을, 네트워크들 및 송신 프로토콜들에 광범위하게 적용가능하도록 의도되고, 이들 중 일부는, 선호되는 양상들의 하기 설명 및 도면들에서 예시의 방식으로 예시된다. 상세한 설명 및 도면들은 제한적이기 보다는 본 개시의 단지 예시이고, 본 개시의 범위는 첨부된 청구항들 및 이들의 균등물들에 의해 정의된다.

[0023]

[0038] 본 명세서에서 설명되는 기술들은 CDMA, TDMA, FDMA, OFDMA, SC-FDMA 및 다른 네트워크들과 같은 다양한 무선 통신 네트워크들에 대해 사용될 수 있다. 용어 "네트워크" 및 "시스템"은 종종 상호교환가능하게 사용된다. CDMA 네트워크는, UTRA(universal terrestrial radio access), cdma2000 등과 같은 라디오 기술을 구현할 수 있다. UTRA는 WCDMA(wideband CDMA), TD-SCDMA(time division synchronous CDMA), 및 CDMA의 다른 변형들을 포함한다. cdma2000은 IS-2000, IS-95 및 IS-856 표준들을 커버한다. TDMA 네트워크는 GSM(global system for mobile communications)과 같은 라디오 기술을 구현할 수 있다. OFDMA 네트워크는, E-UTRA(evolved UTRA), UMB(ultra mobile broadband), IEEE 802.11(Wi-Fi), IEEE 802.16(WiMAX), IEEE 802.20, Flash-OFDM® 등과 같은 라디오 기술을 구현할 수 있다. UTRA 및 E-UTRA는 UMTS(universal mobile telecommunication system)의 일부이다. FDD(frequency division duplex) 및 TDD(time division duplex) 둘 모두에서 3GPP LTE(Long Term Evolution) 및 LTE-A(LTE Advanced)는 다운링크 상에서 OFDMA를 그리고 업링크 상에서 SC-FDMA를 이용하는 E-UTRA를 사용하는 UMTS의 새로운 레릴리스들이다. UTRA, E-UTRA, UMTS, LTE, LTE-A 및 GSM은 "3GPP(3rd Generation Partnership Project)"로 명명된 조직으로부터의 문서들에 기술되어 있다. cdma2000 및 UMB는 "3GPP2(3rd Generation Partnership Project 2)"로 명명된 조직으로부터의 문서들에 기술되어 있다. 본 명세서에서 설명되는 기술들은 위에서 언급된 무선 네트워크들 및 라디오 기술들뿐만 아니라, 다른 무선 네트워크들 및 라디오 기술들, 예를 들어, 5G 차세대/NR 네트워크에도 사용될 수 있다.

[0024]

예시적인 무선 통신 시스템

[0025]

[0039] 도 1은 예를 들어, UE 네트워크(보안) 정책 정보(예를 들어, 네트워크 구성, 보안 정보, 능력들 등)를 안전하게 제공하기 위해 본 개시의 양상들이 수행될 수 있는 예시적인 무선 네트워크(100), 예를 들어, NR(new radio) 또는 5G 네트워크를 예시한다. 일부 경우들에서, 네트워크(100)는 멀티-슬라이스 네트워크일 수 있고, 여기서 각각의 슬라이스는 적절히 구성된 네트워크 기능들, 네트워크 애플리케이션들, 및 특정 사용 사례 또는 비즈니스 모델의 요건을 충족하기 위해 함께 번들링되는 기본적 클라우드 인프라구조들의 구성요소로서 정의된다.

[0026]

[0040] 도 1에 예시된 바와 같이, 무선 네트워크(100)는 다수의 BS들(110) 및 다른 네트워크 엔티티들을 포함할 수 있다. BS는 UE들과 통신하는 스테이션일 수 있다. 각각의 BS(110)는 특정 지리적 커버리지 영역에 대한 통신 커버리지를 제공할 수 있다. 3GPP에서, "셀"이라는 용어는, 그 용어가 사용되는 상황에 따라, 노드 B의 커버리지 영역 및/또는 이러한 커버리지 영역을 서빙하는 노드 B 서브시스템을 지칭할 수 있다. NR 시스템들에서, "셀" 및 eNB, 노드 B, 5G NB, AP, NR BS, NR BS, 또는 TRP라는 용어는 상호교환가능할 수 있다. 일부 예들에서, 셀은 필수적으로 정적은 아닐 수 있고, 셀의 지리적 영역은 모바일 기지국의 위치에 따라 이동할 수 있다. 일부 예들에서, 기지국들은 임의의 적합한 전송 네트워크를 사용하여 직접 물리적 접속, 가상 네트워크 등과 같은 다양한 타입들의 백홀 인터페이스들을 통해 서로 및/또는 무선 네트워크(100)의 하나 이상의 다른 기지국들 또는 네트워크 노드들(도시되지 않음)에 상호접속될 수 있다.

[0027]

[0041] 일반적으로, 임의의 수의 무선 네트워크들이 주어진 지리적 영역에 배치될 수 있다. 각각의 무선 네트워크는 특정 RAT(radio access technology)를 지원할 수 있고 하나 이상의 주파수들 상에서 동작할 수 있다. RAT는 또한 라디오 기술, 에어 인터페이스 등으로 지칭될 수 있다. 주파수는 또한, 캐리어, 주파수 채널 등으로 지칭될 수 있다. 각각의 주파수는 상이한 RAT들의 무선 네트워크들 사이에서 간섭을 회피하기 위해 주어진 지리적 영역에서 단일 RAT를 지원할 수 있다. 일부 경우들에서, 멀티-슬라이스 네트워크 아키텍처를 이용하는 NR 또는 5G RAT 네트워크들이 배치될 수 있다.

[0028]

[0042] BS는 매크로 셀, 피코 셀, 웨토 셀 및/또는 다른 타입들의 셀에 대한 통신 커버리지를 제공할 수 있다. 매크로 셀은, 비교적 넓은 지리적 영역(예를 들어, 반경 수 킬로미터)을 커버할 수 있고, 서비스 가입을 한 UE들에 의한 제한없는 액세스를 허용할 수 있다. 피코 셀은 비교적 작은 지리적 영역을 커버할 수 있고, 서비스 가입을 한 UE들에 의한 제한없는 액세스를 허용할 수 있다. 웨토 셀은 비교적 작은 지리적 영역(예를 들어, 집)을 커버할 수 있고, 웨토 셀과의 연관을 갖는 UE들(예를 들어, CSG(Closed Subscriber Group) 내의 UE들, 집에 있는 사용자들에 대한 UE들 등)에 의한 제한적 액세스를 허용할 수 있다. 매크로 셀에 대한 BS는 매크로 BS로 지칭될 수 있다. 피코 셀에 대한 BS는 피코 BS로 지칭될 수 있다. 웨토 셀에 대한 BS는 웨토 BS 또는 홈 BS로 지칭될 수 있다. 도 1에 도시된 예에서, BS들(110a, 110b 및 110c)은 각각 매크로 셀들(102a, 102b 및 102c)에 대한 매크로 BS들일 수 있다. BS(110x)는 피코 셀(102x)에 대한 피코 BS일 수 있다. BS들(110y 및 110z)은 각각 웨토 셀들(102y 및 102z)에 대한 웨토 BS들일 수 있다. BS는 하나의 또는 다수의(예를 들어, 3개의) 셀들을 지원할 수 있다.

- [0029] [0043] 무선 네트워크(100)는 또한 중계국들을 포함할 수 있다. 중계국은, 업스트림 스테이션(예를 들어, BS 또는 UE)으로부터 데이터 및/또는 다른 정보의 송신을 수신하고 다운스트림 스테이션(예를 들어, UE 또는 BS)으로 데이터 및/또는 다른 정보의 송신을 전송하는 스테이션이다. 또한, 중계국은 다른 UE들에 대한 송신들을 중계하는 UE일 수 있다. 도 1에 도시된 예에서, 중계국(110r)은 BS(110a)와 UE(120r) 사이의 통신을 용이하게 하기 위해 BS(110a) 및 UE(120r)와 통신할 수 있다. 중계국은 또한 중계 BS, 중계기 등으로 지칭될 수 있다.
- [0030] [0044] 무선 네트워크(100)는 상이한 타입들의 BS들, 예를 들어, 매크로 BS, 피코 BS, 펨토 BS, 중계기들 등을 포함하는 이종 네트워크일 수 있다. 이러한 상이한 타입들의 BS들은 상이한 송신 전력 레벨들, 상이한 커버리지 영역들 및 무선 네트워크(100)에서의 간섭에 대한 상이한 영향을 가질 수 있다. 예를 들어, 매크로 BS는 높은 송신 전력 레벨(예를 들어, 20 와트)을 가질 수 있는 반면, 피코 BS, 펨토 BS 및 중계기들은 더 낮은 송신 전력 레벨(예를 들어, 1 와트)을 가질 수 있다.
- [0031] [0045] 무선 네트워크(100)는 동기식 또는 비동기식 동작을 지원할 수 있다. 동기식 동작의 경우, BS들은 유사한 프레임 타이밍을 가질 수 있으며, 상이한 BS들로부터의 송신들이 대략 시간 정렬될 수 있다. 비동기식 동작의 경우, BS들은 상이한 프레임 타이밍을 가질 수 있으며, 상이한 BS들로부터의 송신들이 시간상 정렬되지 않을 수 있다. 본 명세서에서 설명되는 기술들은 동기식 및 비동기식 동작 둘 모두를 위해 사용될 수 있다.
- [0032] [0046] 네트워크 제어기(130)는 BS들의 세트에 커플링될 수 있고, 이러한 BS들에 대한 조정 및 제어를 제공할 수 있다. 네트워크 제어기(130)는 백홀을 통해 BS들(110)과 통신할 수 있다. BS들(110)은 또한, 예를 들어, 무선 또는 유선 백홀을 통해 간접적으로 또는 직접적으로 서로 통신할 수 있다.
- [0033] [0047] UE들(120)(예를 들어, 120x, 120y 등)은 무선 네트워크(100) 전반에 걸쳐 산재되어 있을 수 있고, 각각의 UE는 고정형 또는 이동형일 수 있다. UE는 또한 모바일 스테이션, 단말, 액세스 단말, 가입자 유닛, 스테이션, CPE(Customer Premises Equipment), 셀룰러 폰, 스마트 폰, PDA(personal digital assistant), 무선 모뎀, 무선 통신 디바이스, 핸드헬드 디바이스, 랩톱 컴퓨터, 코드리스 폰, WLL(wireless local loop) 스테이션, 태블릿, 카메라, 게이밍 디바이스, 넷북, 스마트북, 울트라북, 의료 디바이스 또는 의료 장비, 생체인식 센서/디바이스, 웨어러블 디바이스, 예를 들어, 스마트 시계, 스마트 의류, 스마트 안경, 스마트 손목 밴드, 스마트 보석류(예를 들어, 스마트 반지, 스마트 팔찌 등), 엔터테인먼트 디바이스(예를 들어, 뮤직 디바이스, 비디오 디바이스, 위성 라디오 등), 차량 컴퓨트 또는 센서, 스마트 계측기/센서, 산업용 제조 장비, 글로벌 포지셔닝 시스템 디바이스 또는 무선 또는 유선 매체를 통해 통신하도록 구성되는 임의의 다른 적합한 디바이스로 지칭될 수 있다. 일부 UE들은 이볼브드 또는 MTC(machine-type communication) 디바이스들 또는 eMTC(evolved MTC) 디바이스들로 고려될 수 있다. MTC 및 eMTC UE들은, BS, 다른 디바이스(예를 들어, 원격 디바이스) 또는 일부 다른 엔티티와 통신할 수 있는, 예를 들어, 로봇들, 드론들, 원격 디바이스들, 센서들, 계측기들, 모니터들, 위치 태그들 등을 포함한다. 무선 노드는, 예를 들어, 유선 또는 무선 통신 링크를 통해 네트워크(예를 들어, 인터넷 또는 셀룰러 네트워크와 같은 광역 네트워크)에 대한 또는 네트워크로의 접속을 제공할 수 있다. 일부 UE들은 IoT(Internet-of-Things) 디바이스들로 고려될 수 있다.
- [0034] [0048] 도 1에서, 양방향 화살표들을 갖는 실선은, 다운링크 및/또는 업링크 상에서 UE를 서빙하도록 지정된 BS인 서빙 BS와 UE 사이의 원하는 송신들을 표시한다. 양방향 화살표들을 갖는 파선은 UE와 BS 사이의 간접 송신들을 표시한다.
- [0035] [0049] 특정 무선 네트워크들(예를 들어, LTE)은, 다운링크 상에서는 OFDM(orthogonal frequency division multiplexing)을 활용하고, 업링크 상에서는 SC-FDM(single-carrier frequency division multiplexing)을 활용한다. OFDM 및 SC-FDM은, 톤(tone)들, 빈(bin)들 등으로 일반적으로 또한 지칭되는 다수(K개)의 직교 서브캐리어들로 시스템 대역폭을 분할한다. 각각의 서브캐리어는 데이터와 변조될 수 있다. 일반적으로, 변조 심볼들은 OFDM에 의해 주파수 도메인에서 그리고 SC-DMA에 의해 시간 도메인에서 전송된다. 인접한 서브캐리어들 사이의 간격은 고정될 수 있고, 서브캐리어들의 총 수(K)는 시스템 대역폭에 의존할 수 있다. 예를 들어, 서브캐리어들의 간격은 15 kHz일 수 있고, 최소 자원 할당(‘자원 블록’으로 지칭됨)은 12개의 서브캐리어들(또는 180 kHz)일 수 있다. 결국, 공칭 FFT 크기는, 1.25, 2.5, 5, 10 또는 20메가헤르츠(MHz)의 시스템 대역폭에 대해 각각 128, 256, 512, 1024 또는 2048과 동일할 수 있다. 시스템 대역폭은 또한 서브대역들로 파티셔닝될 수 있다. 예를 들어, 서브대역은 1.08MHz(즉, 6개의 자원 블록들)를 커버할 수 있으며, 각각, 1.25, 2.5, 5, 10 또는 20MHz의 시스템 대역폭에 대해 1, 2, 4, 8 또는 16개의 서브대역들이 존재할 수 있다.
- [0036] [0050] 본원에 설명된 예들의 양상들은 LTE 기술들과 연관될 수 있지만, 본 개시의 양상들은 NR/5G와 같은 다른

른 무선 통신 시스템들과 적용가능할 수 있다.

- [0037] [0051] NR은 업링크 및 다운링크 상에서 CP를 갖는 OFDM을 활용할 수 있고 TDD를 사용하는 하프-듀플렉스 동작에 대한 지원을 포함할 수 있다. 100 MHz의 단일 컴포넌트 캐리어 대역폭이 지원될 수 있다. NR 자원 블록들은 0.1 ms 지속기간에 걸쳐 75 kHz의 서브캐리어 대역폭을 갖는 12개의 서브캐리어들에 걸쳐 있을 수 있다. 각각의 라디오 프레임은 10 ms의 길이를 갖는 50개의 서브프레임들로 이루어질 수 있다. 결국, 각각의 서브프레임은 0.2 ms의 길이를 가질 수 있다. 각각의 서브프레임은 데이터 송신을 위한 링크 방향(즉, DL 또는 UL)을 표시할 수 있고, 각각의 서브프레임에 대한 링크 방향은 동적으로 스위칭될 수 있다. 각각의 서브프레임은 DL/UL 데이터 뿐만 아니라 DL/UL 제어 데이터를 포함할 수 있다. NR에 대한 UL 및 DL 서브프레임들은 도 6 및 도 7에 대해 아래에서 더 상세히 설명되는 바와 같을 수 있다. 범형성이 지원될 수 있고 범 방향은 동적으로 구성될 수 있다. 프리코딩을 갖는 MIMO 송신들이 또한 지원될 수 있다. DL에서 MIMO 구성들은 최대 8개의 스트림들 및 최대 2개의 UE당 스트림들을 갖는 다중-층 DL 송신들을 갖는 최대 8개의 송신 안테나들을 지원할 수 있다. 최대 2개의 UE당 스트림들을 갖는 다중-층 송신들이 지원될 수 있다. 다수의 셀들의 어그리게이션이 최대 8개의 서빙 셀들에 대해 지원될 수 있다. 대안적으로, NR은 OFDM-기반 이외의 상이한 에어 인터페이스를 지원할 수 있다. NR 네트워크들은 CU들 및/또는 DU들과 같은 엔티티들을 포함할 수 있다.
- [0038] [0052] 일부 예들에서, 에어 인터페이스에 대한 액세스가 스케줄링될 수 있고, 스케줄링 엔티티(예를 들어, 기지국)는 자신의 서비스 영역 또는 셀 내의 일부의 또는 모든 디바이스들 및 장비 사이의 통신을 위해 자원들을 할당한다. 본 개시 내에서, 아래에서 추가로 논의되는 바와 같이, 스케줄링 엔티티는 하나 이상의 하위 엔티티들에 대한 자원들을 스케줄링, 할당, 재구성 및 해제하는 것을 담당할 수 있다. 즉, 스케줄링된 통신에 대해, 하위 엔티티들은 스케줄링 엔티티에 의해 할당된 자원들을 활용한다. 기지국들은 스케줄링 엔티티로서 기능할 수 있는 유일한 엔티티들이 아니다. 즉, 일부 예들에서, UE가 하나 이상의 하위 엔티티들(예를 들어, 하나 이상의 다른 UE들)에 대한 자원들을 스케줄링하는 스케줄링 엔티티로서 기능할 수 있다. 이러한 예에서, UE는 스케줄링 엔티티로서 기능하고 있고, 다른 UE들은 무선 통신을 위해 UE에 의해 스케줄링된 자원들을 활용한다. UE는 P2P(peer-to-peer) 네트워크에서 및/또는 메시(mesh) 네트워크에서 스케줄링 엔티티로서 기능할 수 있다. 메시 네트워크 예에서, UE들은 선택적으로, 스케줄링 엔티티와 통신하는 것에 추가로 서로 직접 통신할 수 있다.
- [0039] [0053] 따라서, 시간-주파수 자원들에 대한 스케줄링된 액세스를 갖고 셀룰러 구성, P2P 구성 및 메시 구성을 갖는 무선 통신 네트워크에서, 스케줄링 엔티티 및 하나 이상의 하위 엔티티들은 스케줄링된 자원들을 활용하여 통신할 수 있다.
- [0040] [0054] 앞서 언급된 바와 같이, RAN은 CU 및 DU들을 포함할 수 있다. NR BS(예를 들어, gNB, 5G 노드 B, 노드 B, TRP(transmission reception point), AP(access point))는 하나의 또는 다수의 BS들에 대응할 수 있다. NR 셀들은 액세스 셀(ACells) 또는 데이터 전용 셀(DCells)들로 구성될 수 있다. 예를 들어, RAN(예를 들어, 중앙 유닛 또는 분산형 유닛)은 셀들을 구성할 수 있다. DCells들은 캐리어 어그리게이션 또는 듀얼 접속성을 위해 사용되지만, 초기 액세스, 셀 선택/재선택 또는 핸드오버에 대해서는 사용되지 않는 셀들일 수 있다. 일부 경우들에서, DCells들은 동기화 신호들을 송신하지 않을 수 있고, 일부 경우들에서, DCells들은 SS를 송신할 수 있다. NR BS들은 셀 태입을 표시하는 UE들에 다운링크 신호들을 송신할 수 있다. 셀 태입 표시에 기초하여, UE는 NR BS와 통신할 수 있다. 예를 들어, UE는 표시된 셀 태입에 기초하여 셀 선택, 액세스, 핸드오버 및/또는 측정을 위해 고려할 NR BS들을 결정할 수 있다.
- [0041] [0055] 도 2는 도 1에 예시된 무선 통신 시스템에서 구현될 수 있는 분산형 RAN(radio access network)(200)의 예시적인 논리적 아키텍처를 예시한다. 5G 액세스 노드(206)는 ANC(access node controller)(202)를 포함할 수 있다. ANC는 분산형 RAN(200)의 CU(central unit)일 수 있다. NG-CN(next generation core network)(204)에 대한 백홀 인터페이스는 ANC에서 종료될 수 있다. 이웃 NG-AN(next generation access node)들에 대한 백홀 인터페이스는 ANC에서 종료될 수 있다. ANC는 하나 이상의 TRP들(208)(이는 또한 BS들, NR BS들, 노드 B들, 5G NB들, AP들 또는 일부 다른 용어로 지칭될 수 있음)을 포함할 수 있다. 앞서 설명된 바와 같이, TRP는 "셀"과 상호교환가능하게 사용될 수 있다.
- [0042] [0056] TRP들(208)은 DU일 수 있다. TRP들은 하나의 ANC(ANC(202)) 또는 하나 초파의 ANC(예시되지 않음)에 접속될 수 있다. 예를 들어, RAN 공유, RaaS(radio as a service) 및 서비스 특정 AND 배치들의 경우, TRP는 하나 초파의 ANC에 접속될 수 있다. TRP는 하나 이상의 안테나 포트들을 포함할 수 있다. TRP들은 UE에 대한 트래픽을 개별적으로(예를 들어, 동적 선택) 또는 공동으로(예를 들어, 공동 송신) 서빙하도록 구성될 수 있다.

- [0043] [0057] 로컬 아키텍처(200)는 프론트홀(fronthaul) 정의를 예시하기 위해 사용될 수 있다. 상이한 배치 탑입들에 걸쳐 프론트홀 솔루션들을 지원하는 아키텍처가 정의될 수 있다. 예를 들어, 아키텍처는 송신 네트워크 능력들(예를 들어, 대역폭, 레이턴시 및/또는 지터(jitter))에 기초할 수 있다.
- [0044] [0058] 아키텍처는 특징들 및/또는 컴포넌트들을 LTE와 공유할 수 있다. 양상들에 따르면, NG-AN(next generation AN)(210)은 NR과의 듀얼 접속을 지원할 수 있다. NG-AN은 LTE 및 NR에 대한 공통 프론트홀을 공유 할 수 있다.
- [0045] [0059] 아키텍처는 TRP들(208) 사이에서의 협력을 가능하게 할 수 있다. 예를 들어, 협력은 TRP 내에서 및/또는 ANC(202)를 통해 TRP들에 걸쳐 미리 설정될 수 있다. 양상들에 따르면, 어떠한 TRP-간 인터페이스도 필요/존재하지 않을 수 있다.
- [0046] [0060] 양상들에 따르면, 분리된 논리적 기능들의 동적 구성이 아키텍처(200) 내에서 존재할 수 있다. 도 5를 참조하여 더 상세히 설명될 바와 같이, RRC(Radio Resource Control) 계층, PDCP(Packet Data Convergence Protocol) 계층, RLC(Radio Link Control) 계층, MAC(Medium Access Control) 계층 및 물리(PHY) 계층들이 DU 또는 CU(예를 들어, 각각 TRP 또는 ANC)에 적응적으로 배치될 수 있다. 특정 양상들에 따르면, BS는 CU(central unit)(예를 들어, ANC(202)) 및/또는 하나 이상의 분산형 유닛들(예를 들어, 하나 이상의 TRP들(208))을 포함할 수 있다.
- [0047] [0061] 도 3은 본 개시의 양상들에 따른 분산형 RAN(300)의 예시적인 물리적 아키텍처를 예시한다. C-CU(centralized core network unit)(302)가 코어 네트워크 기능들을 호스팅할 수 있다. C-CU는 중앙집중형으로 배치될 수 있다. C-CU 기능은 피크 용량을 핸들링하기 위한 노력으로, (예를 들어, AWS(advanced wireless services)에) 분담될 수 있다.
- [0048] [0062] C-RU(centralized RAN unit)(304)가 하나 이상의 ANC 기능들을 호스팅할 수 있다. 선택적으로, C-RU는 코어 네트워크 기능들을 로컬로 호스팅할 수 있다. C-RU는 분산형 배치를 가질 수 있다. C-RU는 네트워크 애지에 더 가까울 수 있다.
- [0049] [0063] DU(306)는 하나 이상의 TRP들(EN(edge node), EU(edge unit), RH(radio head), SRH(smart radio head) 등)을 호스팅할 수 있다. DU는 RF(radio frequency) 기능을 갖는 네트워크의 애지들에 로케이트될 수 있다.
- [0050] [0064] 도 4는 본 개시의 양상들을 구현하기 위해 사용될 수 있는, 도 1에 예시된 BS(110) 및 UE(120)의 예시적인 컴포넌트들을 예시한다. 앞서 설명된 바와 같이, BS는 TRP를 포함할 수 있다. BS(110) 및 UE(120)의 하나 이상의 컴포넌트들은, 본 개시의 양상들을 실시하기 위해 사용될 수 있다. 예를 들어, UE(120)의 안테나들(452), Tx/Rx(222), 프로세서들(466, 458, 464) 및/또는 제어기/프로세서(480) 및/또는 BS(110)의 안테나들(434), 프로세서들(460, 420, 438) 및/또는 제어기/프로세서(440)는 본원에 설명되고 도 10 내지 도 15를 참조하여 예시된 동작들을 수행하기 위해 사용될 수 있다.
- [0051] [0065] 제한된 연관 시나리오에 대한 양상들에 따르면, 기지국(110)은 도 1의 매크로 BS(110c)일 수 있고, UE(120)는 UE(120y)일 수 있다. 기지국(110)은 또한 일부 다른 타입의 기지국일 수 있다. 기지국(110)은 안테나들(434a 내지 434t)을 구비할 수 있고, UE(120)는 안테나들(452a 내지 452r)을 구비할 수 있다.
- [0052] [0066] 기지국(110)에서, 송신 프로세서(420)는 데이터 소스(412)로부터의 데이터 및 제어기/프로세서(440)로부터의 제어 정보를 수신할 수 있다. 제어 정보는 PBCH(Physical Broadcast Channel), PCFICH(Physical Control Format Indicator Channel), PHICH(Physical Hybrid ARQ Indicator Channel), PDCCH(Physical Downlink Control Channel) 등에 대한 것일 수 있다. 데이터는 PDSCH(Physical Downlink Shared Channel) 등에 관한 것일 수 있다. 프로세서(420)는 데이터 및 제어 정보를 프로세싱(예를 들어, 인코딩 및 심볼 맵핑)하여, 데이터 심볼들 및 제어 심볼들을 각각 획득할 수 있다. 프로세서(420)는 또한, 예를 들어, PSS, SSS, 및 셸-특정 기준 신호에 대해 기준 심볼들을 생성할 수 있다. 송신(TX) 다중입력 다중출력(MIMO) 프로세서(430)는, 적용가능하다면, 데이터 심볼들, 제어 심볼들 및/또는 기준 심볼들에 대해 공간 프로세싱(예를 들어, 프리코딩)을 수행할 수 있고, 출력 심볼 스트림들을 변조기들(MOD들)(432a 내지 432t)에 제공할 수 있다. 각각의 변조기(432)는 각각의 출력 심볼 스트림을 (예를 들어, OFDM 등을 위해) 프로세싱하여 출력 샘플 스트림을 획득할 수 있다. 각각의 변조기(432)는 출력 샘플 스트림을 추가 프로세싱(예를 들어, 아날로그로 변환, 증폭, 필터링 및 상향 변환)하여 다운링크 신호를 획득할 수 있다. 변조기들(432a 내지 432t)로부터의 다운링크 신호들은 안테나들(434a 내지 434t)을 통해 각각 송신될 수 있다.

- [0053] [0067] UE(120)에서, 안테나들(452a 내지 452r)은 기지국(110)으로부터 다운링크 신호들을 수신할 수 있고, 수신된 신호들을 복조기들(DEMOD들)(454a 내지 454r)에 각각 제공할 수 있다. 각각의 복조기(454)는 각각의 수신된 신호를 컨디셔닝(예를 들어, 필터링, 증폭, 하향변환 및 디지털화)하여, 입력 샘플들을 획득할 수 있다. 각각의 복조기(454)는 입력 샘플들을 (예를 들어, OFDM 등을 위해) 추가로 프로세싱하여, 수신된 심볼들을 획득할 수 있다. MIMO 검출기(456)는 모든 복조기들(454a 내지 454r)로부터의 수신된 심볼들을 획득하고, 적용가능하다면 수신된 심볼들에 대해 MIMO 검출을 수행하고, 검출된 심볼들을 제공할 수 있다. 수신 프로세서(458)는 검출된 심볼들을 프로세싱(예를 들어, 복조, 디인터리빙 및 디코딩)하고, UE(120)에 대한 디코딩된 데이터를 데이터 싱크(460)에 제공하고, 디코딩된 제어 정보를 제어기/프로세서(480)에 제공할 수 있다.
- [0054] [0068] 업링크 상에서는, UE(120)에서, 송신 프로세서(464)가 데이터 소스(462)로부터의 (예를 들어, PUSCH(Physical Uplink Shared Channel)에 대한) 데이터 및 제어기/프로세서(480)로부터의 (예를 들어, PUCCH(Physical Uplink Control Channel)에 대한) 제어 정보를 수신 및 프로세싱할 수 있다. 송신 프로세서(464)는 또한 기준 신호에 대한 기준 심볼들을 생성할 수 있다. 송신 프로세서(464)로부터의 심볼들은 적용가능하다면 TX MIMO 프로세서(466)에 의해 프리코딩되고, 복조기들(454a 내지 454r)에 의해 (예를 들어, SC-FDM 등을 위해) 추가로 프로세싱되고, 기지국(110)에 송신될 수 있다. BS(110)에서, UE(120)에 의해 전송된 데이터 및 제어 정보에 대한 디코딩된 데이터 및 제어 정보를 획득하기 위해, UE(120)로부터의 업링크 신호들은 안테나들(434)에 의해 수신되고, 변조기들(432)에 의해 프로세싱되고, 적용가능하다면 MIMO 검출기(436)에 의해 검출되고, 수신 프로세서(438)에 의해 추가로 프로세싱될 수 있다. 수신 프로세서(438)는 디코딩된 데이터를 데이터 싱크(439)에 제공할 수 있고, 디코딩된 제어 정보를 제어기/프로세서(440)에 제공할 수 있다.
- [0055] [0069] 제어기들/프로세서들(440 및 480)은 기지국(110) 및 UE(120)에서의 동작을 각각 지시(direct)할 수 있다. 기지국(110)의 프로세서(440) 및/또는 다른 프로세서들 및 모듈들은 예를 들어, 본원에 설명된 기술들에 대한 프로세스들을 수행 또는 지시할 수 있다. UE(120)에서의 프로세서(480) 및/또는 다른 프로세서들 및 모듈들은 또한, 예를 들어, 도 10, 도 12, 도 13 및/또는 도 15에 예시된 기능 블록들 및/또는 본 명세서에서 설명된 기술들에 대한 다른 프로세스들의 실행을 수행 또는 지시할 수 있다. 메모리들(442 및 482)은 BS(110) 및 UE(120)에 대한 데이터 및 프로그램 코드들을 각각 저장할 수 있다. 스케줄러(444)는 다운링크 및/또는 업링크를 통한 데이터 송신을 위해 UE들을 스케줄링할 수 있다.
- [0056] [0070] 도 5는 본 개시의 양상들에 따른 통신 프로토콜 스택을 구현하기 위한 예들을 도시하는 도면(500)을 예시한다. 예시된 통신 프로토콜 스택들은 5G 시스템(예를 들어, 업링크 기반 모빌리티를 지원하는 시스템)에서 동작하는 디바이스들에 의해 구현될 수 있다. 도면(500)은 RRC(Radio Resource Control) 계층(510), PDCP(Packet Data Convergence Protocol) 계층(515), RLC(Radio Link Control) 계층(520), MAC(Medium Access Control) 계층(525), 및 물리(PHY) 계층(530)을 포함하는 통신 프로토콜 스택을 예시한다. 다양한 예들에서 프로토콜 스택의 계층들은 소프트웨어의 별개의 모듈들, 프로세서 또는 ASIC의 부분들, 통신 링크에 의해 접속되는 코로케이트되지 않은 디바이스들의 부분들 또는 이들의 다양한 조합들로서 구현될 수 있다. 예를 들어, 네트워크 액세스 디바이스(예를 들어, AN들, CU들 및/또는 DU들) 또는 UE에 대한 프로토콜 스택에서 코로케이트된 그리고 코로케이트되지 않은 구현들이 사용될 수 있다.
- [0057] [0071] 제1 옵션(505-a)은 프로토콜 스택의 분리된 구현을 도시하고, 여기서 프로토콜 스택의 구현은 중앙집중형 네트워크 액세스 디바이스(예를 들어, 도 2의 ANC(202))와 분산형 네트워크 액세스 디바이스(예를 들어, 도 2의 DU(208)) 사이에 분리될 수 있다. 제1 옵션(505-a)에서, RRC 계층(510) 및 PDCP 계층(515)은 중앙 유닛에 의해 구현될 수 있고, RLC 계층(520), MAC 계층(525) 및 PHY 계층(530)은 DU에 의해 구현될 수 있다. 다양한 예들에서, CU 및 DU는 코로케이트될 수 있거나 코로케이트되지 않을 수 있다. 제1 옵션(505-a)은 매크로 셀, 마이크로 셀 또는 피코 셀 배치에서 유용할 수 있다.
- [0058] [0072] 제2 옵션(505-b)은 프로토콜 스택의 단일화된 구현을 도시하고, 여기서 프로토콜 스택은 단일 네트워크 액세스 디바이스(예를 들어, AN(access node), NR BS(new radio base station), NR NB(new radio Node-B), NN(network node) 등)에서 구현된다. 제2 옵션에서, RRC 계층(510), PDCP 계층(515), RLC 계층(520), MAC 계층(525) 및 PHY 계층(530) 각각은 AN에 의해 구현될 수 있다. 제2 옵션(505-b)은 웹토 셀 배치에서 유용할 수 있다.
- [0059] [0073] 네트워크 액세스 디바이스가 프로토콜 스택 중 일부를 구현하는지 또는 전부를 구현하는지와 무관하게, UE는 전체 프로토콜 스택(예를 들어, RRC 계층(510), PDCP 계층(515), RLC 계층(520), MAC 계층(525) 및 PHY 계층(530))을 구현할 수 있다.

- [0060] [0074] 도 6은 무선 네트워크(100)에서 통신하기 위해 사용될 수 있는 DL-중심 서브프레임의 예를 도시하는 도면(600)이다. DL-중심 서브프레임은 제어 부분(602)을 포함할 수 있다. 제어 부분(602)은 DL-중심 서브프레임의 초기 또는 시작 부분에 존재할 수 있다. 제어 부분(602)은 DL-중심 서브프레임의 다양한 부분들에 대응하는 다양한 스케줄링 정보 및/또는 제어 정보를 포함할 수 있다. 일부 구성들에서, 제어 부분(602)은 도 6에 표시된 바와 같이, PDCCH(physical DL control channel)일 수 있다. DL-중심 서브프레임은 또한 DL 데이터 부분(604)을 포함할 수 있다. DL 데이터 부분(604)은 때때로 DL-중심 서브프레임의 페이로드로 지칭될 수 있다. DL 데이터 부분(604)은 스케줄링 엔티티(예를 들어, UE 또는 BS)로부터 하위 엔티티(예를 들어, UE)에 DL 데이터를 통신하기 위해 활용되는 통신 자원들을 포함할 수 있다. 일부 구성들에서, DL 데이터 부분(604)은 PDSCH(physical DL shared channel)일 수 있다.
- [0061] [0075] DL-중심 서브프레임은 또한 공통 UL 부분(606)을 포함할 수 있다. 공통 UL 부분(606)은 때때로 UL 버스트, 공통 UL 버스트 및/또는 다양한 다른 적합한 용어들로 지칭될 수 있다. 공통 UL 부분(606)은 DL-중심 서브프레임의 다양한 다른 부분들에 대응하는 피드백 정보를 포함할 수 있다. 예를 들어, 공통 UL 부분(606)은 제어 부분(602)에 대응하는 피드백 정보를 포함할 수 있다. 피드백 정보의 비제한적인 예들은 ACK 신호, NACK 신호, HARQ 표시자 및/또는 다양한 다른 적합한 타입들의 정보를 포함할 수 있다. 공통 UL 부분(606)은 추가적인 또는 대안적인 정보, 예를 들어, RACH(random access channel) 절차들과 관련된 정보, SR(scheduling request)들 및 다양한 다른 적합한 타입들의 정보를 포함할 수 있다. 도 6에 예시된 바와 같이, DL 데이터 부분(604)의 끝은 공통 UL 부분(606)의 시작으로부터 시간상 분리될 수 있다. 이러한 시간 분리는 때때로, 캡, 가드 기간, 가드 인터벌 및/또는 다양한 다른 적합한 용어들로 지칭될 수 있다. 이러한 분리는 DL 통신(예를 들어, 하위 엔티티(예를 들어, UE)에 의한 수신 동작)으로부터 UL 통신(예를 들어, 하위 엔티티(예를 들어, UE)에 의한 송신)으로의 스위치-오버를 위한 시간을 제공한다. 당업자는, 전술한 내용이 DL-중심 서브프레임의 단지 일례이며, 본원에 설명된 양상들로부터 반드시 벗어남이 없이 유사한 특징들을 갖는 대안적인 구조들이 존재할 수 있음을 이해할 것이다.
- [0062] [0076] 도 7은 무선 네트워크(100)에서 통신하기 위해 사용될 수 있는 UL-중심 서브프레임의 예를 도시하는 도면(700)이다. UL-중심 서브프레임은 제어 부분(702)을 포함할 수 있다. 제어 부분(702)은 UL-중심 서브프레임의 초기 또는 시작 부분에 존재할 수 있다. 도 7의 제어 부분(702)은 도 6을 참조하여 앞서 설명된 제어 부분과 유사할 수 있다. UL-중심 서브프레임은 또한 UL 데이터 부분(704)을 포함할 수 있다. UL 데이터 부분(704)은 때때로 UL-중심 서브프레임의 페이로드로 지칭될 수 있다. UL 부분은 하위 엔티티(예를 들어, UE)로부터 스케줄링 엔티티(예를 들어, UE 또는 BS)에 UL 데이터를 통신하기 위해 활용되는 통신 자원들을 지칭할 수 있다. 일부 구성들에서, 제어 부분(702)은 PDCCH(physical DL control channel)일 수 있다.
- [0063] [0077] 도 7에 예시된 바와 같이, 제어 부분(702)의 끝은 UL 데이터 부분(704)의 시작으로부터 시간상 분리될 수 있다. 이러한 시간 분리는 때때로, 캡, 가드 기간, 가드 인터벌 및/또는 다양한 다른 적합한 용어들로 지칭될 수 있다. 이러한 분리는 DL 통신(예를 들어, 스케줄링 엔티티에 의한 수신 동작)으로부터 UL 통신(예를 들어, 스케줄링 엔티티에 의한 송신)으로의 스위치-오버를 위한 시간을 제공한다. UL-중심 서브프레임은 또한 공통 UL 부분(706)을 포함할 수 있다. 도 7b의 공통 UL 부분(706)은 도 6을 참조하여 앞서 설명된 공통 UL 부분(606)과 유사할 수 있다. 공통 UL 부분(706)은 추가적으로 또는 대안적으로 CQI(channel quality indicator)와 관련된 정보, SRS(sound reference signal)들, 및 다양한 다른 적합한 타입들의 정보를 포함할 수 있다. 당업자는, 전술한 내용이 UL-중심 서브프레임의 단지 일례이며, 본원에 설명된 양상들로부터 반드시 벗어남이 없이 유사한 특징들을 갖는 대안적인 구조들이 존재할 수 있음을 이해할 것이다.
- [0064] [0078] 일부 환경들에서, 둘 이상의 하위 엔티티들(예를 들어, UE들)은 사이드링크 신호들을 사용하여 서로 통신할 수 있다. 이러한 사이드링크 통신들의 실세계 애플리케이션들은 공공 안전, 근접 서비스들, UE-대-네트워크 중계, V2V(vehicle-to-vehicle) 통신들, IoE(Internet of Everything) 통신들, IoT 통신들, 미션-크리티컬 메시 및/또는 다양한 다른 적합한 애플리케이션들을 포함할 수 있다. 일반적으로, 사이드링크 신호는, 스케줄링 엔티티가 스케줄링 및/또는 제어 목적들로 활용될 수 있더라도, 스케줄링 엔티티(예를 들어, UE 또는 BS)를 통한 그 통신을 중계함이 없이 하나의 하위 엔티티(예를 들어, UE1)로부터 다른 하위 엔티티(예를 들어, UE2)에 통신되는 신호를 지칭할 수 있다. 일부 예들에서, 사이드링크 신호들은 면허 스펙트럼을 사용하여 통신될 수 있다(통상적으로 비면허 스펙트럼을 사용하는 무선 로컬 영역 네트워크들과 상이함).
- [0065] [0079] UE는 자원들의 전용 세트를 사용하여 송신하는 것과 연관된 구성(예를 들어, RRC(radio resource control) 전용 상태 등) 또는 자원들의 공통 세트를 사용하여 파일럿들을 송신하는 것과 연관된 구성(예를 들어, RRC 공통 상태 등)을 포함하는 다양한 라디오 자원 구성들에서 동작할 수 있다. RRC 전용 상태에서 동작

하는 경우, UE는 네트워크에 파일럿 신호를 송신하기 위한 자원들의 전용 세트를 선택할 수 있다. RRC 공통 상태에서 동작하는 경우, UE는 네트워크에 파일럿 신호를 송신하기 위한 자원들의 공통 세트를 선택할 수 있다. 어느 경우이든, UE에 의해 송신된 파일럿 신호는 AN 또는 DU 또는 이를 중 일부들과 같은 하나 이상의 네트워크 액세스 디바이스들에 의해 수신될 수 있다. 각각의 수신 네트워크 액세스 디바이스는 자원들의 공통 세트 상에서 송신된 파일럿 신호들을 수신 및 측정하고, 또한 네트워크 액세스 디바이스가 UE에 대한 네트워크 액세스 디바이스들의 모니터링 세트의 멤버인 UE들에 할당된 자원들의 전용 세트들 상에서 송신된 파일럿 신호들을 수신 및 측정하도록 구성될 수 있다. 수신 네트워크 액세스 디바이스들 중 하나 이상, 또는 수신 네트워크 액세스 디바이스(들)가 파일럿 신호들의 측정들을 송신하는 CU는 UE들에 대한 서빙 셀들을 식별하기 위해 또는 UE들 중 하나 이상에 대한 서빙 셀의 변화를 개시하기 위해 측정들을 사용할 수 있다.

[0066] 키 생성에서 네트워크 정책들의 예시적인 통합

[0067] [0080] 앞서 언급된 바와 같이, 넓은 대역폭(예를 들어, 80 MHz 초과)을 타겟팅하는 eMBB(Enhanced mobile broadband), 높은 캐리어 주파수(예를 들어, 60 GHz)를 타겟팅하는 밀리미터파(mmW), 역호환불가능한 MTC 기술들을 타겟팅하는 mMTC(massive MTC) 및/또는 URLLC(ultra reliable low latency communications)를 타겟팅하는 미션 크리티컬(mission critical)을 포함하는 특징들을 포함하는 새로운 에어 인터페이스가 5G에 도입되고 있다.

[0068] [0081] 5G에 대한 서비스들 및 기술들이 진화를 계속하기 때문에, 5G는 다양한 상이한 배치 시나리오들을 지원할 수 있다. 예를 들어, 현재 5G 아키텍처에서, 네트워크에서 상이한 기능들을 수행하는 것을 담당하는 하나 이상의 네트워크 노드들(예를 들어, SEAF(security anchor function), AMF(access and mobility management function), SMF(session management function) 등)은 코로케이트되거나 물리적으로 분리될 수 있다.

[0069] [0082] AMF를 네트워크 에지 가까이로 이동 및/또는 코로케이트할 필요성이 존재하더라도, 물리적으로 안전한 위치에 보안 앵커를 유지하기 위해 SEAF가 5G에서 도입되었다(예를 들어, RAN). 따라서, 일부 배치들에서, SEAF는 AMF와 코로케이트될 수 있고, 다른 배치들에서, SEAF는 AMF와 분리될 수 있다(예를 들어, SEAF 및 AMF 각각은 독립형 기능들을 가질 수 있다). 유사하게, SMF는 AMF 및 SEAF와 분리될 수 있다. 일부 경우들에서, SMF는 AMF와 물리적으로 분리될 수 있고, AMF와는 상이한 보안 도메인 내에 있을 수 있다(예를 들어, 네트워크 공유 시나리오의 경우). 일부 경우들에서, SMF는 슬라이스 특정적일 수 있다.

[0070] [0083] 도 8은 본 개시의 특정 양상들에 따라 하나 이상의 네트워크 노드들이 물리적으로 분리될 수 있는 5G 아키텍처(800)의 참조 예를 예시한다. 특히, 아키텍처(800)는 (예를 들어, 다른 배치 시나리오들에서 코로케이트된 SEAF/AMF와 반대로) SEAF가 AMF로부터 물리적으로 분리되는 배치 시나리오의 참조 예를 예시한다.

[0071] [0084] 도시된 바와 같이, 5G 아키텍처(800)는 다수의 슬라이스들을 포함할 수 있다. 각각의 슬라이스는 상이한 서비스들, 예를 들어, IoE(internet of everything), URLLC, eMBB, 차량 통신들(즉, V2X, 예를 들어, V2V(vehicle-to-vehicle), V2I(vehicle-to-infrastructure), V2P(vehicle-to-pedestrian), V2N(vehicle-to-network)) 등을 지원할 수 있다.

[0072] [0085] 슬라이스는, 5G-AN 및 5G-CN 둘 모두를 포함할 수 있는 특정 네트워크 능력들 및 네트워크 특성들을 제공하기 위해 필요한 네트워크 기능들 및 대응하는 자원들의 세트를 포함하는 완전한 로직 네트워크로서 정의될 수 있다. 더 구체적으로, 슬라이스는 적절히 구성된 네트워크 기능들, 네트워크 애플리케이션들, 및 특정 사용 사례 또는 비즈니스 모델의 요건을 충족하기 위해 함께 번들링되는 기본적 클라우드 인프라구조들의 구성요소일 수 있다. 일부 경우들에서, 상이한 슬라이스들은 분리된 자원들을 할당받을 수 있고 레이턴시 및/또는 전력과 같은 상이한 요건들을 가질 수 있다.

[0073] [0086] 이러한 예에서, AMF는 다수의 슬라이스들을 동시에 서빙하도록 구성될 수 있다. 예를 들어, AMF는 UE와 네트워크 슬라이스들 사이에 모빌리티 관리 NAS 보안 앵커를 제공할 수 있다. SMF는 일반적으로 서비스(슬라이스) 특정 PDU 세션 확립을 지원하기 위해 서비스 인가/인증을 수행하도록 구성된다. SMF는 또한 UPF(user plane function)와 RAN 사이에 유지되는 터널(들)을 포함하는 기능들, 예를 들어, 수정 및 해제를 수행할 수 있다. 사용자 평면 보안은 UDF에서 종단될 수 있다. 일부 경우들에서, SMF는 서비스 특정 QoS를 지원할 수 있다.

[0074] [0087] 도 9는 본 개시의 특정 양상들에 따라 하나 이상의 네트워크 노드들(예를 들어, SEAF, AMF, SMF 등)이 물리적으로 분리될 수 있는 5G 아키텍처(900)의 다른 참조 예를 예시한다. 일부 경우들에서, 5G 보안 아키텍처는 본질적으로 PDU 세션 인가를 위한 제3자 AUSF(authentication server function)(예를 들어, 제3자 AAA)를

이용한 2차 인증을 지원하도록 설계될 수 있다. 서비스 인증은 서비스 특정 PDU 세션의 확립을 가능하게 한다. 도 8과 유사하게, 사용자 평면 보안은 UPF에서 종단될 수 있고, 서비스 특정 QoS가 지원될 수 있다. SMF는 제3자 AAA에 직접 인터페이싱하고 SEAF를 통해 제3자 AAA와 상호작용할 수 있다.

[0075] [0088] 언급된 바와 같이, 5G 네트워크는 진화를 계속할 수 있기 때문에, 특정 네트워크 구성, 능력들, 보안 정보 등에 관한 정보(본 명세서에서 집합적으로 네트워크 정책 정보로 지칭됨)를 UE에 제공하는 것이 바람직할 수 있다. 그러나, 현재 아키텍처들에서, UE와 서빙 네트워크 사이의 유일한 제어 평면 인터페이스는 N1이고 이는 UE와 AMF 사이의 NAS 접속을 위해 사용되기 때문에, 현재 기술들을 사용하여 보안 방식으로 네트워크 정책 정보를 UE에 제공하는 것은 가능하지 않을 수 있다.

[0076] [0089] 예를 들어, 아키텍처(800)를 참조하면, AMF는 (예를 들어, NAS 시그널링에 기초하여) UE와 시그널링 접속을 갖는 유일한 엔티티일 수 있기 때문에, AMF는 다른 네트워크 노드(예를 들어, SEAF, SMF 등)로부터 수신된 임의의 네트워크 보안 정책 정보에 관해 UE에 잘못 통지할 수 있다. 따라서, 네트워크 정책 정보가 AMF 및 SEAF가 분리된다는 정보를 포함하면, 현재 기술들은 AMF 및 SEAF가 분리된다는 것을 UE에 안전하게 통지하지 못 할 수 있는데, 이는, UE가 (예를 들어, 또한 SEAF와 시그널링 접속을 갖는 것과는 반대로) 단지 AMF와 시그널링 접속을 가질 수 있기 때문이다.

[0077] [0090] 이러한 경우, 독립형(사기적) AMF는 자신이 SEAF와 코로케이트된다고 주장할 수 있는데, 이는 UE에 의해 검출될 수 없는 시나리오이다. 이러한 독립형 AMF(사기적)는 UE와 네트워크 사이의 접속/세션을 순상시키기 위해, 네트워크 보안 능력들, 세션 관리 NAS 보호, 슬라이스 특정 보안 능력들/요건들 등을 수정할 수 있다.

[0078] [0091] 추가로, 정확한(보안) 네트워크 정책 정보가 없다면, UE는 (예를 들어, PDU 세션 확립 시에) 비딩 다운 공격(bidding down attack)들에 취약할 수 있다. 비딩 다운 시나리오의 일례에서, AMF는 SMF와는 상이한 보안 도메인에 있을 수 있다. 예를 들어, 하나의 경우에, AMF는 서빙 네트워크에서 UE(또는 RAN)에 가깝게 로케이트 될 수 있는 한편(예를 들어, 덜 안전한 위치일 수 있음), SMF는 네트워크 내에 깊이 로케이트될 수 있다. 하나의 경우에, AMF는 서빙 네트워크(예를 들어, VPLMN)에 있을 수 있는 한편, SMF는 홈 네트워크에 있다.

[0079] [0092] 그러나, AMF가 SMF와는 상이한 보안 도메인에 있을 수 있는 동안, SMF는 (예를 들어, AMF에 의해 액세스될 수 없는 슬라이스 특정 가입 정보에 기초하여) 슬라이스 특정 PDU 세션 생성을 인가하는 것을 여전히 담당 할 수 있다. SMF는 예를 들어, 통상적으로 AMF로부터 논리적으로 별개의 네트워크 기능이고 PDU 세션 인가 및 관리를 담당한다. 앞서 언급된 바와 같이, SMF는 슬라이스 특정적일 수 있고, 따라서 UE와 슬라이스 특정 PDU 세션 파라미터들을 교환할 수 있다.

[0080] [0093] 그러나, UE에 의해 요청되고 SMF에 의해 구성되는 PDU 세션 파라미터들, 예를 들어, 인가된 QoS 규칙, SSC 모드, S-S-NSSAI, 할당된 IPv4 어드레스 등은 UE와 SMF 사이의 중간 노드(예를 들어, AMF를 포함함)에 의해 수정되지 않아야 한다. 오히려, 이러한 파라미터들은, SEAF로부터 획득되고 동일한 SMF 키를 유도함으로써 UE에서 검증가능한 특정 키를 사용하여 SMF에 의해 보호되어야 한다. 따라서, AMF가 SEAF로부터 분리되는 상황들에서, (악의적 또는 손상된) AMF는 예를 들어, 보안, QoS 또는 다른 패킷 처리를 격하시키기 위해, UE에 의해 요청되거나 SMF에 의해 인가된 세션 정보를 수정할 수 있다.

[0081] [0094] 따라서, 본 명세서에 제시된 양상들은 예를 들어, 비딩 다운 공격들 최소화하기 위해, 네트워크 정책 정보를 UE에 안전하게 통지하기 위한 기술들을 제공한다. 특히, 양상들은 네트워크 정책 정보를 UE와 AMF 사이의 NAS 접속을 보안하기 위해 사용되는 키(예를 들어,  $K_{AMF}$ ) 유도로 통합하기 위한 기술들을 제공한다. 아래에서 설명되는 바와 같이, 네트워크 정책 정보를 키 유도로 통합함으로써, UE는 AMF로부터의 임의의 수신된 네트워크 정책 정보가 변경/수정/손상되었는지 여부를 검출할 수 있다.

[0082] [0095] 본원에 설명된 기술들은 PDU 세션 확립의 비딩 다운 공격들에 대해 보호하기 위해 사용될 수 있는 한편, 본원에 제시된 양상들은 또한 SEAF와 UE 사이의 노드(들)에 의한 UE 정책 비딩 다운에 대해 보호하기 위해 사용될 수 있음을 주목한다. 즉, 아래에서 설명되는 바와 같이, 본원에 제시된 양상들은 또한, 예를 들어, UE 정책 정보를 키(예를 들어,  $K_{AMF}$ ) 유도에 통합함으로써 UE 정책 정보(예를 들어, 네트워크 능력들, 보안 능력들 또는 이들의 임의의 조합을 포함하는 UE 보안 특징들 및/또는 UE 능력들)를 보호하기 위해 사용될 수 있다. UE 정책 정보는 등록/어태치 요청 메시지에서 네트워크에 제공될 수 있다.

[0083] [0096] 특정 양상들에 따르면,  $K_{AMF}$  유도는 네트워크에서 교환되는 파라미터(들)를 보호하기 위해 사용될 수 있다. 특히, UE가 네트워크에 등록할 때, SEAF는 네트워크 정책 정보 및/또는 UE 정책 정보를 키(예를 들어,

$K_{AMF}$  유도 내에 통합함으로써 네트워크(보안) 정책 정보(예를 들어, 네트워크 구성, 능력들, 보안 특징들 등) 및/또는 UE 정책 정보(예를 들어, UE에 의해 수신됨)를 UE에 통지할 수 있다.

[0084] [0097] 예를 들어, SEAF는 네트워크 정책 정보, UE 정책 정보, 프레시니스 파라미터들 또는 이들의 임의의 조합에 기초하여 AMF 키(예를 들어,  $K_{AMF}$ )를 유도하고, 키를 AMF에 전송할 수 있어서, AMF 및 UE는 NAS 보안 콘텍스트를 확립할 수 있고 SEAF는 또한 UE로부터 수신된 UE 정책 정보를 UE에 통지할 수 있다. AMF 및 UE는  $K_{AMF}$ 로부터 암호화 및 무결성 보호 키들을 유도하고 (예를 들어, N1 인터페이스를 통해) NAS 메시지들을 보호할 수 있다.

[0085] [0098] 네트워크 정책 정보를  $K_{AMF}$  유도에 통합함으로써, AMF는, 네트워크 정책 정보에서의 변화가 UE에서 상이한  $K_{AMF}$  유도를 초래할 때, SEAF로부터 유도된 네트워크 정책 정보를 수정함으로써 네트워크 특징들을 비딩 다운하는 것과 같은 미인가된 거동들이 방지될 수 있다. 유사하게, UE 정책 정보를  $K_{AMF}$  유도에 통합함으로써, UE와 SEAF 사이의 네트워크 노드들은, UE 능력들에서의 변화가 또한 상이한  $K_{AMF}$  유도를 초래할 때, UE 능력들을 수정함으로써 UE 능력들을 비딩 다운하는 것이 방지될 수 있다.

[0086] [0099] 도 10은 무선 통신들에 대한 예시적인 동작들(1000)을 예시한다. 특정 양상들에 따르면, 동작들(1000)은 네트워크와 보안(예를 들어, NAS) 접속을 확립하기 위한 사용자 장비에 의해 수행될 수 있다.

[0087] [0100] 동작들(1000)은 UE가 네트워크와 보안 접속을 확립하기 위한 제1 메시지(예를 들어, SMC(security mode command) 메시지)를 (예를 들어, AMF로부터) 수신하는 1002에서 시작할 수 있다. 제1 메시지는 네트워크 정책 정보(예를 들어, 네트워크 구성, 능력들, 보안 특징들 등)를 포함한다. 1004에서, UE는 네트워크 정책 정보에 부분적으로 기초하여 제1 키(예를 들어,  $K_{AMF}$ )를 생성한다.

[0088] [0101] 일부 양상들에서, 네트워크 정책 정보는, UE가 네트워크와 통신 세션을 확립할 때 네트워크 내의 SMF로부터 세션 관리 토큰을 수신할지 여부의 표시를 포함한다. 일부 양상들에서, 네트워크 정책 정보는 AMF가 네트워크 내의 SEAF와 코로케이트되는지 여부의 표시를 포함한다. 일부 양상들에서, 네트워크 정책 정보는 AMF의 보안 레벨을 포함한다. 일부 양상들에서, 네트워크 정책 정보는 SEAF의 보안 도메인, AMF의 보안 도메인 또는 이들의 임의의 조합을 포함한다. 일부 양상들에서, 네트워크 정책 정보는 UE로부터 네트워크에 전송된 UE 정책 정보에 대한 응답으로 형성되었을 수 있다. 일부 양상들에서, 제1 키는 네트워크에 전송된 UE 정책 정보에 기초하여 결정될 수 있다.

[0089] [0102] 1006에서, UE는 네트워크 정책 정보가 유효하다고 검증하기 위해 제1 키를 사용한다. 예를 들어, 일부 경우들에서, UE는 제1 키에 부분적으로 기초하여 제1 메시지(네트워크 정책 정보를 포함함)가 유효한지 여부를 결정할 수 있다.

[0090] [0103] 아래에서 더 상세히 설명되는 바와 같이, 일부 경우들에서, 제1 메시지는 제2 키(예를 들어, SEAF로부터 AMF에 제공되는  $K_{AMF}$ )에 기초하여 유도된 보호 키로 무결성 보호되는 SMC 메시지일 수 있다. UE는 제1 키에 기초하여 제1 메시지의 무결성 검증을 수행함으로써 제1 메시지(및/또는 그 안에 포함된 네트워크 정책 정보)가 유효한지 여부를 결정할 수 있다. 일부 양상에서, UE는 제1 메시지의 무결성 검증이 정확하면 제1 메시지가 유효하다고 결정할 수 있다.

[0091] [0104] 제1 키가 제2 키와 동일하다고 UE가 결정하면, UE는, 제1 메시지의 무결성 검증이 정확하다고 결정할 수 있다. UE는 제1 키가 제2 키와 동일하다는 결정에 기초하여 네트워크 정책 정보가 유효하다고 결정할 수 있다. 마찬가지로, UE는 제1 메시지의 무결성 검증이 부정확하면 제1 메시지가 무효라고 결정할 수 있다. 제1 키가 제2 키와 상이하면, UE는, 제1 메시지의 무결성 검증이 부정확하다고 결정할 수 있다. UE는 제1 키가 제2 키와 상이하다는 결정에 기초하여 네트워크 정책 정보가 무효라고 결정할 수 있다.

[0092] [0105] 도 11은 무선 통신들에 대한 예시적인 동작들(1100)을 예시한다. 특정 양상들에 따르면, 동작들(1100)은 네트워크 정책 정보를 UE에 안전하게 제공하기 위해, 예를 들어, 네트워크 노드(예를 들어, SEAF)에 의해 수행될 수 있다.

[0093] [0106] 동작들(1100)은 네트워크 노드가 네트워크 정책 정보에 적어도 부분적으로 기초하여 다른 네트워크 노드(예를 들어, AMF)에 대한 키(예를 들어,  $K_{AMF}$ )를 생성하는 1102에서 시작할 수 있다. 언급된 바와 같이, 네트워크 정책 정보는 다른 네트워크 노드(예를 들어, AMF)가 네트워크 노드와 코로케이트되는지 여부의 표시를 포함한다.

함할 수 있다. 일부 경우들에서, 네트워크 정책 정보는, 네트워크 노드의 보안 레벨, 또는 네트워크 내의 SMF 가 UE와 네트워크 사이에서 통신 세션에 대한 SM 토큰을 생성하고 SM 토큰을 UE에 전송할지 여부의 표시 중 적어도 하나를 포함할 수 있다. 키는 UE와 네트워크 노드 사이의 보안 접속을 확립하기 위해 사용된다.

[0094] [0107] 일부 양상들에서, 네트워크 노드는 UE 정책(또는 능력) 정보를 포함하는 등록 메시지/어태치 요청 메시지를 수신할 수 있다. 네트워크 노드는 수신된 UE 정책 정보를 다른 네트워크 노드에 대한 키(예를 들어,  $K_{AMF}$ ) 유도에 통합할 수 있다. 예를 들어, 도 11의 1102에서, 네트워크 노드는 네트워크 정책 정보, 프레시니스 파라미터들, UE 정책 정보 또는 이들의 임의의 조합에 부분적으로 기초하여 다른 네트워크 노드(예를 들어, AMF)에 대한 키(예를 들어,  $K_{AMF}$ )를 생성할 수 있다.

[0095] [0108] 1104에서, 네트워크 노드는 다른 네트워크 노드에 키를 전송한다. 일부 양상들에서, 네트워크 노드는 네트워크 정책 정보 또는 네트워크 정책 정보가 유효한 시간의 양 중 적어도 하나를 네트워크 노드에 추가로 전송할 수 있다.

[0096] [0109] 도 12는 본 개시의 특정 양상들에 따라 SEAF가 (예를 들어, 정책 정보 및/또는 UE 정책 정보를 키 유도에 통합함으로써) 네트워크(보안) 정책 정보 및/또는 UE 정책 정보를 UE에 안전하게 통지하도록 허용하는 예시적인 등록 절차를 예시하는 호출 흐름도이다.

[0097] [0110] 일부 양상들에서, 도시된 바와 같이, UE는 초기에 등록 요청/어태치 요청을 네트워크(예를 들어, AMF, SEAF 등)에 전송할 수 있다. 등록 요청/어태치 요청은 UE 정책(능력들)을 포함한다. 그 다음, 단계 1에서, UE는 네트워크와 인증/등록 절차를 수행한다. UE 및 SEAF는 새로운 인증에 기초하여 또는 이전 인증에 기초하여 공유된 앵커 키( $K_{SEAF}$ )를 확립할 수 있다. 등록 동안, AMF는 SEAF로부터 키( $K_{AMF}$ )를 요청할 수 있다.

[0098] [0111] 단계 2에서, SEAF는 AMF에 대해, UE를 네트워크에 등록하기 위한  $K_{AMF}$ 를 생성(예를 들어, 유도)한다.  $K_{AMF}$  유도는 네트워크 정책 정보(예를 들어, 네트워크 구성, 능력들, 보안 특징들 등) 및/또는 UE 정책 정보를 통합한다. 일 양상에서, 네트워크 정책 정보는 AMF 타입, 예를 들어, 코로케이트된 AMF/SEAF, 독립형 AMF 등을 포함할 수 있다.

[0099] [0112] 예를 들어, 네트워크 정책 정보는 하나 이상의 SEAF/AMF 분리 비트들을 포함할 수 있다.  $K_{AMF}$ 를 요청하는 AMF가 독립형 SEAF로부터 분리된 독립형 AMF이면, SEAF는 SEAF/AMF 분리 비트(들)를 제1 값(예를 들어, 1)으로 설정할 수 있다.  $K_{AMF}$ 를 요청하는 AMF가 코로케이트된 AMF/SEAF이면, SEAF는 SEAF/AMF 분리 비트(들)를 상이한 제2 값(예를 들어, 0)으로 설정할 수 있다. 일 양상에서,  $K_{AMF}$  유도는 또한 리플레이 공격들을 방지하기 위해 사용되는 하나 이상의 프레시니스 파라미터들을 통합할 수 있다. 이러한 프레시니스 파라미터들의 예들은 카운터(들)(UE 및 SEAF 둘 모두에서 유지됨), UE와 SEAF 사이에서 교환되는 랜덤 값들 또는 이들의 임의의 조합을 포함할 수 있다. 일 양상에서, SEAF는  $K_{AMF}$ 를 생성(유도)하기 위해 하기 수식 (1)을 사용할 수 있다:

$$K_{AMF} = KDF(K_{SEAF}, \text{프레시니스 파라미터(들)}, \text{네트워크 정책 정보}, \text{UE 정책}) \quad (1)$$

[0101] 여기서, KDF는 키 유도 함수(예를 들어, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512, PRF-X(출력 크기가 X인 의사 랜덤 함수))이고,  $K_{SEAF}$ 는 서빙 네트워크 내의(그리고 SEAF에서 유지되는) 앵커 보호 키이고, 프레시니스 파라미터들은 리플레이 공격들을 방지하기 위해 사용되는 랜덤 값(들)인 카운터(들)이고, 네트워크 정책 정보는 네트워크 구성, 능력들, 보안 특징들 등을 포함하고, UE 정책은 UE 능력 정보 및/또는 UE 보안 정보 중 적어도 하나를 포함한다.

[0102] [0113] 단계 3에서, SEAF는  $K_{AMF}$ , 프레시니스 파라미터(들) 및 네트워크 정책 정보를 AMF에 제공한다. 일부 양상들에서, SEAF는 또한 단계 3에서의 UE 정책을 AMF에 제공(예를 들어, 반복)할 수 있다. 단계 4에서, AMF는 NAS 보안 모드 커맨드(SMC)를 UE에 전송한다. 일부 양상들에서, AMF는 또한 단계 4에서의 UE 정책을 UE에 제공(예를 들어, 반복)할 수 있다. NAS SMC는 SEAF로부터 획득된 프레시니스 파라미터(들) 및 네트워크 정책 정보를 포함할 수 있고, NAS SMC는  $K_{AMF}$ 에 기초하여 무결성 보호될 수 있다. 예를 들어, SEAF로부터  $K_{AMF}$ 를 수신할 때, AMF는  $K_{AMF}$ 에 기초하여 NAS 무결성 보호 키(예를 들어,  $K_{NASINT}$ )를 유도하고, NAS SMC 메시지를 무결성 보호하기 위해  $K_{NASINT}$ 를 사용할 수 있다.

- [0103] [0114] 단계 5에서, UE는  $K_{SEAF}$  및 NAS SMC 메시지 내의 정보(예를 들어, 서비스 파라미터(들), 네트워크 정책 정보 등)를 사용하여  $K_{AMF}$ 를 생성(예를 들어, 유도)하고, NAS SMC 메시지를 검증한다. 즉, UE는 네트워크 정책 정보에 대한 (예를 들어, AMF에 의한) 임의의 변화들이 존재했는지 여부를 검출할 수 있는데, 이는, 네트워크 정책 정보에서의 임의의 변화들이 UE에서 상이한  $K_{AMF}$  유도를 초래할 것이기 때문이다. UE가  $K_{AMF}$ 를 사용하여 NAS SMC의 무결성 보호와 UE에 의해 생성된  $K_{AMF}$ 를 비교함으로써 사용하는 NAS SMC의 무결성 보호를 체크할 때, UE는 이러한 변화들을 검출할 수 있다. 따라서, SMC의 무결성 검증이 정확하다는 결정은, UE에 의해 생성된  $K_{AMF}$  및 (SEAF로부터) AMF에 제공되는  $K_{AMF}$ 가 동일하다는 것을 의미하며, 이는 결국 (AMF로부터) UE에 제공된 네트워크 정책 정보가 유효함을 의미한다.
- [0104] [0115] SMC의 검증이 정확하다고 가정하면, (단계 6에서) UE가 NAS 보안 모드 완료 메시지를 AMF를 전송한다. 일부 양상들에서, UE는 또한 (네트워크에 제공된) UE 정책 정보가 중간 네트워크 노드들 중 임의의 것에 의해 수정되었는지 여부를 검출할 수 있다. 즉, 일부 양상들에서, UE는 (예를 들어, UE에 의해 생성된  $K_{AMF}$  및 (SEAF로부터) AMF에 제공된  $K_{AMF}$ 가 동일한지 여부에 기초하여) UE 정책 정보가 수정되었는지 여부를 결정하기 위해 (예를 들어, 네트워크 정책 정보에 추가로 또는 대안적으로) UE 정책 정보에 기초하여  $K_{AMF}$ 를 생성할 수 있다.
- [0105] [0116] 도 12의 호출 흐름은 네트워크 정책 정보를 UE에 안전하게 통지하기 위해 네트워크 정책 정보를 키 유도에 통합하는 것을 설명하지만, 본원에 제시된 기술들은 또한 UE 보안 특징들을 보호하기 위해 사용될 수 있음을 주목한다. 즉, 네트워크 정책 정보에 추가로 또는 대안적으로, 키( $K_{AMF}$ ) 유도는 UE 능력들(UE 보안 특징들을 포함함)을 통합할 수 있고, UE 능력들은 등록/어태치 요청 메시지에서 네트워크에 제공된다.
- [0106] [0117] 도 10 내지 도 12에서 설명된 기술들은 키 유도에서 키 사용을 제한함으로써 AMF가 UE에 중계하는 임의의 네트워크 능력 파라미터들을 수정하는 것을 방지하기 위해 사용될 수 있다. 그러나, 이러한 기술들은 네트워크 능력들의 비딩 다운을 방지하기 위해 유용할 수 있지만, 이러한 기술들은 PDU 세션 파라미터(들) 비딩 다운(예를 들어, SM NAS 토큰)을 방지하기에는 충분하지 않을 수 있다.
- [0107] [0118] 따라서, 본원에 제시된 양상들은 비딩 다운 공격들을 방지하기 위해 사용될 수 있는 기술들(예를 들어, PDU 세션 확립 및/또는 네트워크 능력 파라미터들)을 제공한다.
- [0108] [0119] 더 구체적으로, UE가 네트워크에 등록할 때, SEAF는 네트워크 정책 정보(예를 들어, 네트워크 구성, (보안) 능력들 등) 및 무결성 보호된 네트워크 정책 정보(예를 들어, 네트워크 정책 토큰)을  $K_{AMF}$ 와 함께 AMF에 제공한다. 네트워크 정책 정보는  $K_{SEAF}$ 를 사용하여 무결성 보호된다. 네트워크 정책 토큰은 NAS 보안 모드 커맨드 상에서 폐기백되고 UE에 제공된다. 네트워크 정책 토큰은 SEAF와 UE 사이에 있는 임의의 네트워크 기능들이 네트워크 능력들을 수정하는 것을 방지한다.
- [0109] [0120] 도 13은 무선 통신들에 대한 예시적인 동작들(1300)을 예시한다. 특정 양상들에 따르면, 동작들(1300)은 예를 들어, 네트워크와 보안(예를 들어, NAS) 접속을 확립하기 위한 사용자 장비에 의해 수행될 수 있다.
- [0110] [0121] 동작들(1300)은, UE가 네트워크와의 인증 절차에 기초하여, 네트워크에서 UE와 SEAF 사이에 공유되는 앵커 키(예를 들어,  $K_{SEAF}$ )를 확립하는 1302에서 시작할 수 있다. 1304에서, UE는 네트워크와 보안 접속을 확립하기 위한 제1 메시지(예를 들어, SMC 메시지)를 수신한다. 제1 메시지는 네트워크와 통신 세션에 대한 네트워크 정책 토큰, 네트워크 정책 정보, 네트워크 정책 정보가 유효한 시간의 제1 양 및 보안 접속을 위해 사용된 제1 키가 유효한 시간의 제2 양을 포함한다. 네트워크 정책 토큰은 네트워크 정책 정보와 연관된 무결성 보호 정보를 포함한다.
- [0111] [0122] 1306에서, UE는 네트워크와 보안 접속을 확립하기 전에, 공유된 앵커 키로부터 유도된 키, 네트워크 정책 정보, 시간의 제1 양 및 시간의 제2 양에 기초하여 네트워크 정책 토큰이 유효한지 여부를 결정한다. 일부 양상들에서, 네트워크 정책 토큰이 유효한지 여부를 결정하는 단계는 공유된 앵커 키로부터 유도된 키에 기초하여 무결성 보호 정보를 검증하는 단계를 포함한다. 일부 양상들에서, UE는 UE 정책 정보(예를 들어, UE 능력 정보, UE 보안 정보 등)를 네트워크에 전송할 수 있다. UE는 네트워크에 전송되는 UE 정책 정보에 기초하여 키를 생성할 수 있다. 일부 경우들에서, 네트워크 정책 정보는 UE 정책 정보에 기초할 수 있다.
- [0112] [0123] 도 14는 무선 통신들에 대한 예시적인 동작들(1400)을 예시한다. 특정 양상들에 따르면, 동작들(1400)은 네트워크 정책 정보를 UE에 안전하게 제공하기 위해, 예를 들어, 네트워크 노드(예를 들어, SEAF)에 의해

수행될 수 있다.

- [0113] [0124] 동작들(1400)은, 네트워크 노드가 UE와의 인증 절차에 기초하여, 네트워크에서 네트워크 노드와 UE 사이에 공유되는 앵커 키(예를 들어,  $K_{SEAF}$ )를 확립하는 1402에서 시작할 수 있다. 1404에서, 네트워크 노드는 앵커 키, 네트워크 정책 정보 및 네트워크 정책 토큰이 유효한 시간의 제1 양에 부분적으로 기초하여 네트워크 정책 토큰(예를 들어,  $K_{token}$ )을 생성한다. 네트워크 정책 토큰은 네트워크 정책 정보와 연관된 무결성 보호 정보를 포함한다. 1406에서, 네트워크 노드는 다른 네트워크 노드(예를 들어, AMF)에 대한 키(예를 들어,  $K_{AMF}$ )를 생성한다. 1408에서, 네트워크 노드는 키, 네트워크 정책 정보, 및 네트워크 정책 토큰을 다른 네트워크 노드에 전송한다.
- [0114] [0125] 일부 양상들에서, 앞서 설명된 바와 같이, 네트워크 노드는, 예를 들어, 중간 노드들이 UE로부터 수신된 UE 정책 정보를 수정하는 것을 방지하기 위해, UE 정책 정보를 키(예를 들어,  $K_{AMF}$ ) 유도에 통합할 수 있다. 언급된 바와 같이, 네트워크 노드는 등록/어태치 요청 메시지를 통해 UE 정책 정보를 수신할 수 있다.
- [0115] [0126] 도 15는 본 개시의 특정 양상들에 따라 SEAF가 PDU 세션 확립 시에 비딩 다운 공격들을 방지하도록 허용하는 예시적인 등록 절차를 예시하는 호출 흐름도이다.
- [0116] [0127] 도시된 바와 같이, 단계 1에서, UE는 네트워크와 등록 절차를 수행한다. UE 및 SEAF는 새로운 인증에 기초하여 또는 이전 인증에 기초하여 공유된 앵커 키( $K_{SEAF}$ )를 확립할 수 있다. 등록 동안, AMF는 SEAF로부터 키( $K_{AMF}$ )를 요청할 수 있다. 도시되지 않지만, 일부 경우들에서, UE는 등록/어태치 요청 메시지를 통해 UE 정책 정보(예를 들어, UE 능력 정보, UE 보안 정보 등)를 네트워크에 제공할 수 있다.
- [0117] [0128] 단계 2에서, SEAF는 AMF에 대해, UE를 네트워크에 등록하기 위한  $K_{AMF}$ 를 생성한다. SEAF는  $K_{SEAF}$  및 하나 이상의 제1 프레시니스 파라미터들을 사용하여  $K_{AMF}$ 를 생성할 수 있다. 추가적으로, SEAF는  $K_{SEAF}$ , (예를 들어, 리플레이 공격들을 방지하기 위한) 하나 이상의 제2 프레시니스 파라미터들, 및 네트워크 정책 정보를 사용하여 네트워크 정책 토큰을 생성한다. 언급된 바와 같이, 네트워크 정책 토큰은 네트워크 정책 정보의 메시지 인증 코드(또는 무결성 보호 정보)이다. 도 12와 유사하게, 네트워크 정책 정보는 하나 이상의 SEAF/AMF 분리 비트들을 포함할 수 있다. 일부 양상들에서, SEAF는 UE 정책 정보에 추가로 기초하여  $K_{AMF}$ 를 생성할 수 있다.
- [0118] [0129] 단계 3에서, SEAF는  $K_{AMF}$ , 제1 및 제2 프레시니스 파라미터(들), 네트워크 정책 토큰 및 네트워크 정책 정보를 AMF에 제공한다. 단계 4에서, AMF는 NAS 보안 모드 커맨드를 UE에 전송한다. NAS 보안 모드 커맨드는 네트워크 정책 정보, 제1 및 제2 프레시니스 파라미터들 및 SEAF로부터 획득된 네트워크 정책 토큰을 포함한다.
- [0119] [0130] 단계 5에서, UE는  $K_{SEAF}$ 를 사용하여 네트워크 정책 토큰에 대한 검증 절차를 수행한다. 검증이 성공적이면, UE는  $K_{SEAF}$ 를 사용하여  $K_{AMF}$ 를 유도하고, 유도된  $K_{AMF}$ 를 사용하여 NAS 보안 모드 커맨드에 대한 검증 절차를 수행한다. NAS 보안 모드 커맨드가 검증된다고 가정하면, UE는 (단계 6에서) NAS 보안 모드 완료 메시지를 AMF에 전송한다. 이러한 방식으로, (UE와 SEAF 사이의 키에 기초하여 토큰이 생성 및 검증될 때) SEAF는 네트워크 능력들을 보안 방식으로 UE에 직접 표시할 수 있다.
- [0120] [0131] 일부 양상들에서, (도 15에 대한) SEAF는 리플레이 공격들을 방지하기 위해 네트워크 정책 생성에 대한 UE의 (도 12의 SEAF에 비해) 추가적인 상태(예를 들어, 프레시니스 파라미터)를 유지해야 할 수 있음을 주목한다. 이는, 디싱킹(desyncing)을 겪을 수 있는 접속인, UE와 SEAF 사이의 접속 상태를 유지하는 것과 유사할 수 있다. 추가로, 도 13 내지 도 15에 설명된 기술들과 유사한 기술들이 또한 UE 정책 정보(UE 보안 정보 및/또는 UE 능력 정보를 포함함)에 대한 비딩 다운 공격들을 보호하기 위해 사용될 수 있음을 주목한다.
- [0121] [0132] 본 명세서에 개시된 방법들은 설명된 방법을 달성하기 위한 하나 이상의 단계들 또는 동작들을 포함한다. 방법 단계들 및/또는 동작들은 청구항들의 범위를 벗어나지 않고 서로 교환될 수 있다. 즉, 단계들 또는 동작들의 특정한 순서가 규정되지 않으면, 특정 단계들 및/또는 동작들의 순서 및/또는 사용은 청구항들의 범위를 벗어나지 않고 변형될 수 있다.
- [0122] [0133] 본 명세서에서 사용되는 바와 같이, 아이템들의 리스트 "중 적어도 하나"로 지칭되는 구문은 단일 멤버들을 포함하여 그 아이템들의 임의의 조합을 지칭한다. 예를 들어, "a, b 또는 c 중 적어도 하나"는 a, b, c, a-b, a-c, b-c, 및 a-b-c 뿐만 아니라 다수의 동일한 엘리먼트의 임의의 결합(예를 들어, a-a, a-a-a, a-a-b,

a-a-c, a-b-b, a-c-c, b-b, b-b-b, b-b-c, c-c, 및 c-c-c 또는 a, b, 및 c의 임의의 다른 순서화)을 커버하는 것으로 의도된다.

[0123] [0134] 본 명세서에서 사용되는 용어 "결정"은 광범위한 동작들을 포함한다. 예를 들어, "결정"은 계산, 컴퓨팅, 프로세싱, 유도, 검사, 검색(예를 들어, 표, 데이터베이스 또는 다른 데이터 구조에서의 검색), 확인 등을 포함할 수 있다. 또한, "결정"은 수신(예를 들어, 정보 수신), 액세스(예를 들어, 메모리 내의 데이터에 액세스) 등을 포함할 수 있다. 또한, "결정"은 해결, 선택, 선정, 설정 등을 포함할 수 있다.

[0124] [0135] 일부 경우들에서, 프레임을 실제로 송신하기 보다는, 디바이스는 송신을 위해 프레임을 출력하기 위한 인터페이스를 가질 수 있다. 예를 들어, 프로세서는 버스 인터페이스를 통해 프레임을, 송신을 위해 RF 프론트 엔드에 출력할 수 있다. 유사하게, 프레임을 실제로 수신하기 보다는, 디바이스는 다른 디바이스로부터 수신된 프레임을 획득하기 위한 인터페이스를 가질 수 있다. 예를 들어, 프로세서는 송신을 위해 RF 프론트 엔드로부터 버스 인터페이스를 통해 프레임을 획득(또는 수신)할 수 있다.

[0125] [0136] 앞서 설명된 방법들의 다양한 동작들은 대응하는 기능들을 수행할 수 있는 임의의 적절한 수단에 의해 수행될 수 있다. 이 수단은, 회로, ASIC(application specific integrated circuit) 또는 프로세서를 포함하는(그러나, 이에 제한되지는 않는) 다양한 하드웨어 및/또는 소프트웨어 컴포넌트(들) 및/또는 모듈(들)을 포함할 수 있다. 일반적으로, 도면들에 도시된 동작들이 존재하는 경우, 이 동작들은 유사한 넘버링을 갖는 상응하는 대응 수단-및-기능(means-plus-function) 컴포넌트들을 가질 수 있다.

[0126] [0137] 예를 들어, 송신하기 위한 수단, 수신하기 위한 수단, 결정하기 위한 수단, 수행하기 위한 수단, 참여하기 위한 수단, 표시하기 위한 수단, 확립하기 위한 수단, 검증하기 위한 수단, 전송하기 위한 수단, 통신하기 위한 수단, 저장하기 위한 수단, 입력하기 위한 수단, 보호하기 위한 수단, 방지하기 위한 수단, 빠져 나가기 위한 수단, 생성하기 위한 수단, 포워딩하기 위한 수단 및/또는 제공하기 위한 수단은 BS(110) 또는 UE(120)의 하나 이상의 프로세서들 또는 안테나들, 예를 들어, BS(110)의 송신 프로세서(420), 제어기/프로세서(440), 수신 프로세서(438) 또는 안테나(434), 및/또는 UE(120)의 송신 프로세서(464), 제어기/프로세서(480), 수신 프로세서(458) 또는 안테나들(452)을 포함할 수 있다.

[0127] [0138] 본 개시와 관련하여 설명되는 다양한 예시적인 논리 블록들, 모듈들, 및 회로들이 범용 프로세서, 디지털 신호 프로세서(DSP), 주문형 집적회로(ASIC), 필드 프로그래밍가능 게이트 어레이(FPGA) 또는 다른 프로그래밍가능 논리 디바이스(PLD), 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들 또는 본 명세서에 설명된 기능들을 수행하도록 설계된 이들의 임의의 조합으로 구현 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안으로 프로세서는 임의의 상업적으로 이용가능한 프로세서, 제어기, 마이크로제어기 또는 상태 머신일 수도 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합, 예를 들어 DSP 및 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 이상의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

[0128] [0139] 하드웨어로 구현되는 경우, 예시적인 하드웨어 구성은 무선 노드 내의 프로세싱 시스템을 포함할 수 있다. 프로세싱 시스템은 버스 아키텍처를 통해 구현될 수 있다. 버스는 프로세싱 시스템의 특정 애플리케이션 및 전체적인 설계 제약들에 따라, 임의의 개수의 상호접속 버스들 및 브리지들을 포함할 수 있다. 버스는 프로세서, 머신-판독가능 매체, 및 버스 인터페이스를 포함하는 다양한 회로들을 함께 링크시킬 수 있다. 버스 인터페이스는 버스를 통해 프로세싱 시스템에, 특히 네트워크 어댑터를 접속시키기 위해 사용될 수 있다. 네트워크 어댑터는 PHY층의 신호 프로세싱 기능들을 구현하기 위해 사용될 수 있다. 사용자 단말(120)(도 1 참조)의 경우, 사용자 인터페이스(예를 들어, 키패드, 디스플레이, 마우스, 조이스틱 등)는 또한 버스에 접속될 수 있다. 버스는 또한 타이밍 소스들, 주변장치들, 전압 레귤레이터들, 전력 관리 회로들 등과 같은 다양한 다른 회로들을 링크시킬 수 있고, 이들은 당해 기술분야에 공지되어 있어, 더 이상 설명되지 않을 것이다. 프로세서는 하나 이상의 범용 및/또는 특수 목적 프로세서들을 사용하여 구현될 수 있다. 예들은 마이크로프로세서들, 마이크로제어기들, DSP 프로세서들, 및 소프트웨어를 실행할 수 있는 다른 회로를 포함한다. 당업자는 전체 시스템에 부과된 전체 설계 제약들 및 특정 애플리케이션에 따라 프로세싱 시스템에 대해 설명된 기능성을 최상으로 구현하는 방법을 인지할 것이다.

[0129] [0140] 소프트웨어로 구현되는 경우, 상기 기능들은 컴퓨터 판독가능 매체 상에 하나 이상의 명령 또는 코드로서 저장되거나 이를 통해 송신될 수 있다. 소프트웨어는, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 하드웨어 기술 언어로서 또는 이와 달리 언급되든지 간에, 명령들, 데이터 또는 이들의 임의의 결합을 의미하도록 넓게 해석될 것이다. 컴퓨터 판독가능 매체들은 컴퓨터 저장 매체들, 및 일 장소에서 다른 장소로 컴퓨터 프로

그램의 이전을 용이하게 하는 임의의 매체들을 포함하는 통신 매체 둘 모두를 포함한다. 프로세서는, 머신-판독가능 저장 매체에 저장된 소프트웨어 모듈들의 실행을 비롯하여, 버스의 관리 및 일반적 프로세싱을 담당할 수 있다. 컴퓨터-판독가능 저장 매체는, 프로세서가 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기록할 수 있도록 프로세서에 커플링될 수 있다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다. 예를 들어, 머신-판독가능 매체는 송신선, 데이터에 의해 변조된 반송파, 및/또는 무선 노드와는 별개로 명령들이 저장된 컴퓨터 판독가능 저장 매체를 포함할 수 있고, 이를 모두는 버스 인터페이스를 통해 프로세서에 의해 액세스될 수 있다. 대안적으로 또는 추가적으로, 머신-판독가능 매체, 또는 그것의 임의의 부분은, 캐시 및/또는 범용 레지스터 파일에서 흔히 있듯이, 프로세서에 통합될 수 있다. 머신-판독가능 저장 매체의 예들은, 예를 들어, RAM (Random Access Memory), 플래시 메모리, ROM(Read Only Memory), PROM(Programmable Read-Only Memory), EPROM(Erasable Programmable Read-Only Memory), EEPROM(Electrically Erasable Programmable Read-Only Memory), 레지스터들, 자기 디스크들, 광학 디스크들, 하드 드라이브들, 또는 임의의 다른 적절한 저장 매체, 또는 이들의 임의의 결합을 포함할 수 있다. 머신-판독가능 매체는 컴퓨터-프로그램 제품에서 구체화될 수 있다.

[0130]

[0141] 소프트웨어 모듈은 단일 명령 또는 다수의 명령들을 포함할 수 있고, 다수의 저장 매체에 걸쳐 상이한 프로그램들 사이에서 몇몇 상이한 코드 세그먼트들에 걸쳐 분산될 수 있다. 컴퓨터-판독가능 매체는 다수의 소프트웨어 모듈들을 포함할 수 있다. 소프트웨어 모듈들은, 프로세서와 같은 장치에 의해 실행되는 경우, 프로세싱 시스템으로 하여금 다양한 기능들을 수행하게 하는 명령들을 포함한다. 소프트웨어 모듈들은 전송 모듈 및 수신 모듈을 포함할 수 있다. 각각의 소프트웨어 모듈은 단일 저장 디바이스에 상주할 수 있거나, 다수의 저장 디바이스들에 걸쳐 분배될 수 있다. 예를 들어, 소프트웨어 모듈은 트리거링 이벤트가 발생하는 경우 하드 드라이브로부터 RAM으로 로딩될 수 있다. 소프트웨어 모듈의 실행 동안, 프로세서는 액세스 속도를 증가시키기 위해 캐시 내로 명령들의 일부를 로딩할 수 있다. 하나 이상의 캐시 라인들은 이후 프로세서에 의한 실행을 위해 범용 레지스터 파일로 로딩될 수 있다. 하기에서 소프트웨어 모듈의 기능성을 참조하는 경우, 이러한 기능성이 해당 소프트웨어 모듈로부터의 명령들을 실행할 때 프로세서에 의해 구현될 수 있다는 점이 이해될 것이다.

[0131]

[0142] 또한, 임의의 접속이 컴퓨터 판독가능 매체로 적절히 지정된다. 예를 들어, 소프트웨어가 동축 케이블, 광섬유 케이블, 연선, DSL(digital subscriber line), 또는 적외선(IR), 라디오 및 마이크로파와 같은 무선 기술들을 사용하여 웹사이트, 서버 또는 다른 원격 소스로부터 전송된다면, 동축 케이블, 광섬유 케이블, 연선, DSL, 또는 적외선, 라디오 및 마이크로파와 같은 무선 기술들이 매체의 정의에 포함된다. 본 명세서에서 사용된 것과 같은 디스크(disk 및 disc)는 CD(compact disc), 레이저 디스크(laser disc), 광 디스크(optical disc), DVD(digital versatile disc), 플로피 디스크(floppy disk) 및 블루레이 디스크(Blu-ray® disc)를 포함하며, 여기서 디스크(disk)들은 보통 데이터를 자기적으로 재생하는 한편, 디스크(disc)들은 데이터를 레이저들에 의해 광학적으로 재생한다. 따라서, 일부 양상들에서, 컴퓨터-판독가능 매체는 비-일시적 컴퓨터-판독가능 매체(예를 들어, 유형의(tangible) 매체)를 포함할 수 있다. 추가로, 다른 양상들에 대해, 컴퓨터-판독가능 매체는 일시적 컴퓨터-판독가능 매체(예를 들어, 신호)를 포함할 수 있다. 상기의 것들의 결합들이 또한 컴퓨터 판독가능 매체의 범위 내에 포함되어야 한다.

[0132]

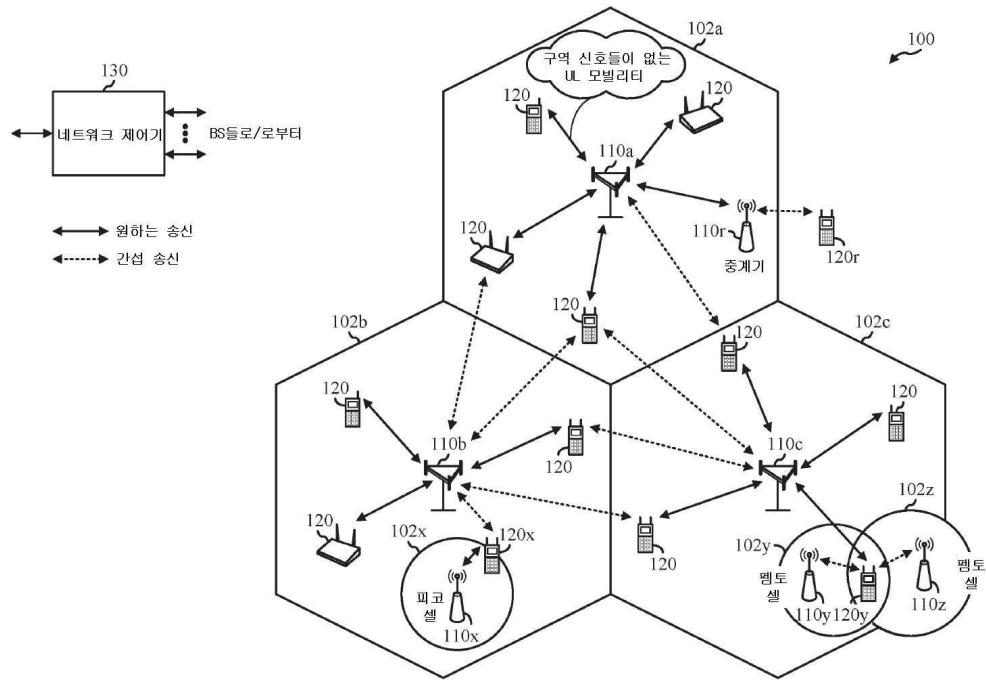
[0143] 또한, 여기서 설명된 방법들 및 기법들을 수행하기 위한 모듈들 및/또는 다른 적절한 수단이 적용 가능한 경우 사용자 단말 및/또는 기지국에 의해 다운로드되고 그리고/또는 이와 다르게 획득될 수 있다는 점이 이해되어야 한다. 예를 들어, 이러한 디바이스는 여기서 설명된 방법들을 수행하기 위한 수단의 전달을 용이하게 하기 위해 서버에 커플링될 수 있다. 대안적으로, 여기서 설명된 다양한 방법들은, 저장 수단(예를 들어, RAM, ROM, CD(compact disc) 또는 플로피 디스크와 같은 물리적 저장 매체 등)을 통해 제공될 수 있고, 따라서, 사용자 단말 및/또는 기지국은 디바이스에 저장 수단을 커플링시키거나 제공할 시에 다양한 방법들을 획득할 수 있다. 또한, 여기에 설명된 방법들 및 기법들을 디바이스에 제공하기 위한 임의의 다른 적절한 기법이 활용될 수 있다.

[0133]

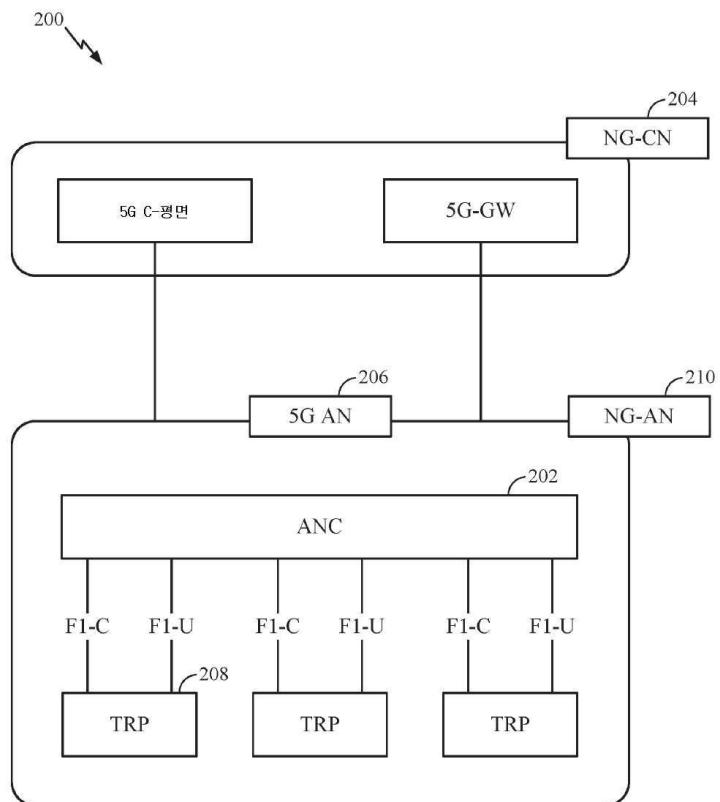
[0144] 청구항들이 위에서 예시된 정확한 구성 및 컴포넌트들에 제한되지 않는다는 점이 이해될 것이다. 다양한 수정들, 변화들 및 변경들은 청구항들의 범위로부터 벗어나지 않고 전술된 방법들 및 장치의 어레인지먼트(arrangement), 동작 및 상세항목들 내에서 이루어질 수 있다.

## 도면

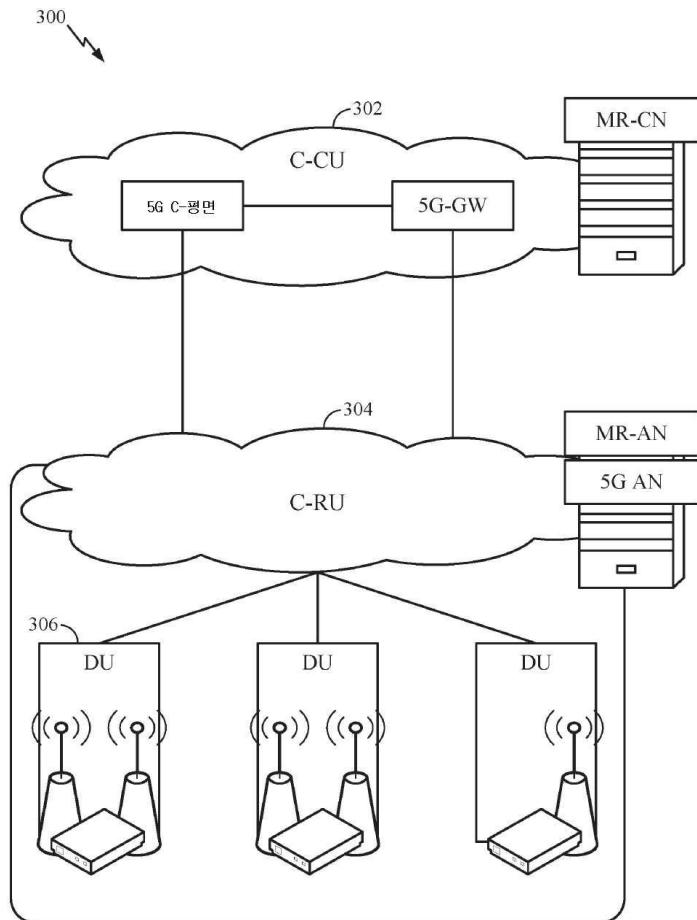
## 도면1



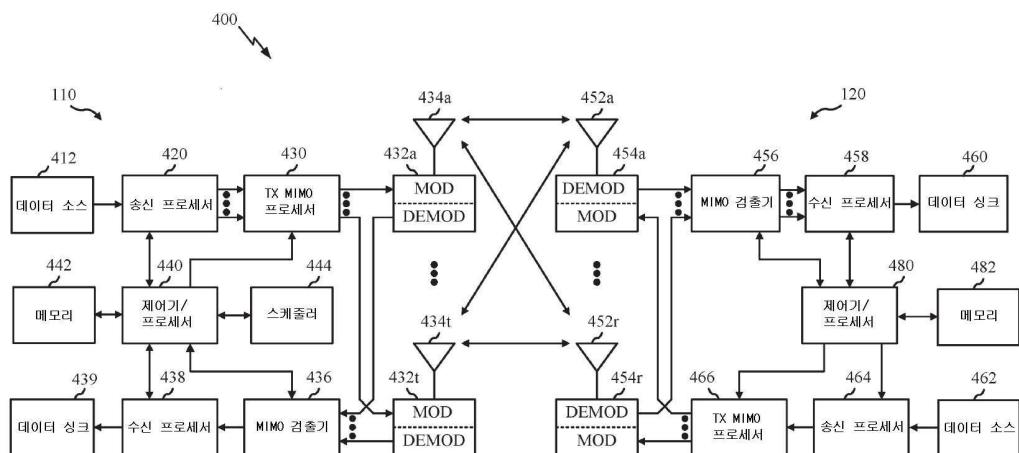
## 도면2



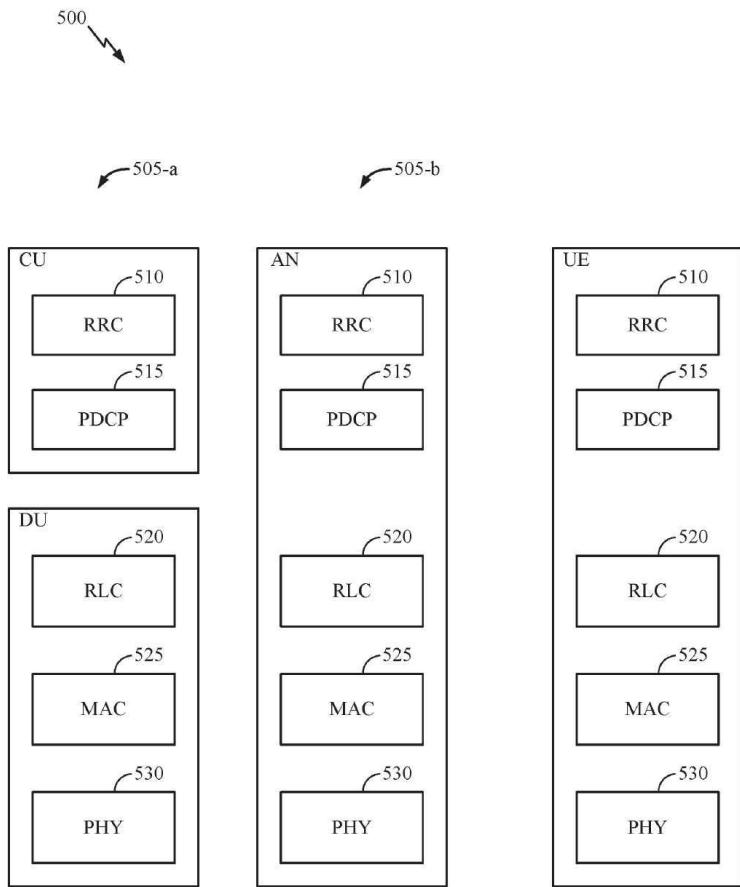
## 도면3



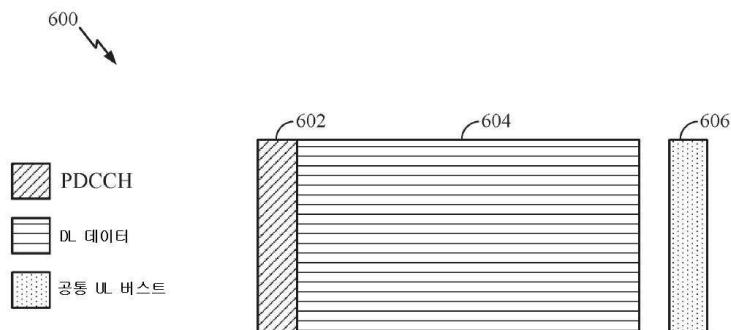
## 도면4



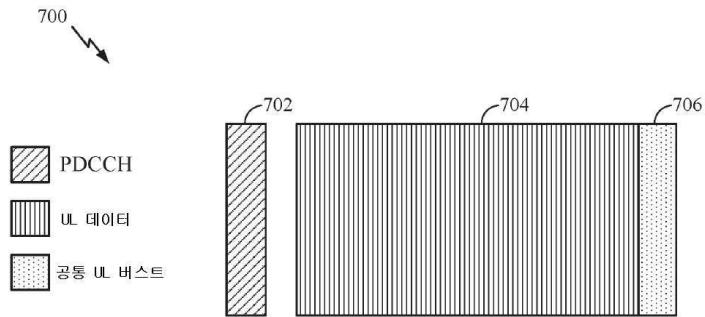
## 도면5



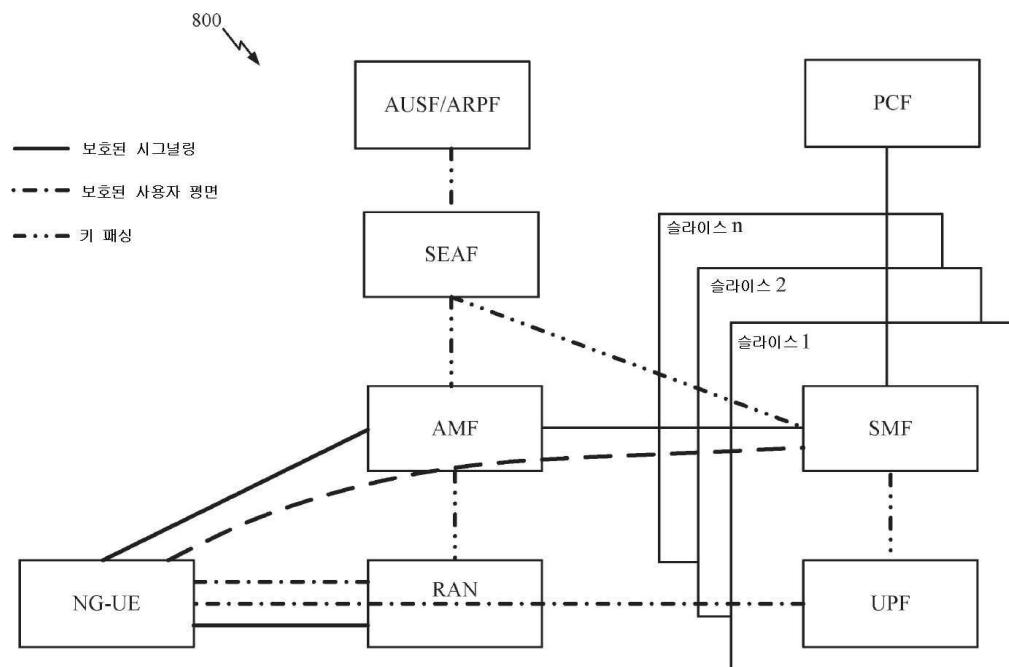
## 도면6



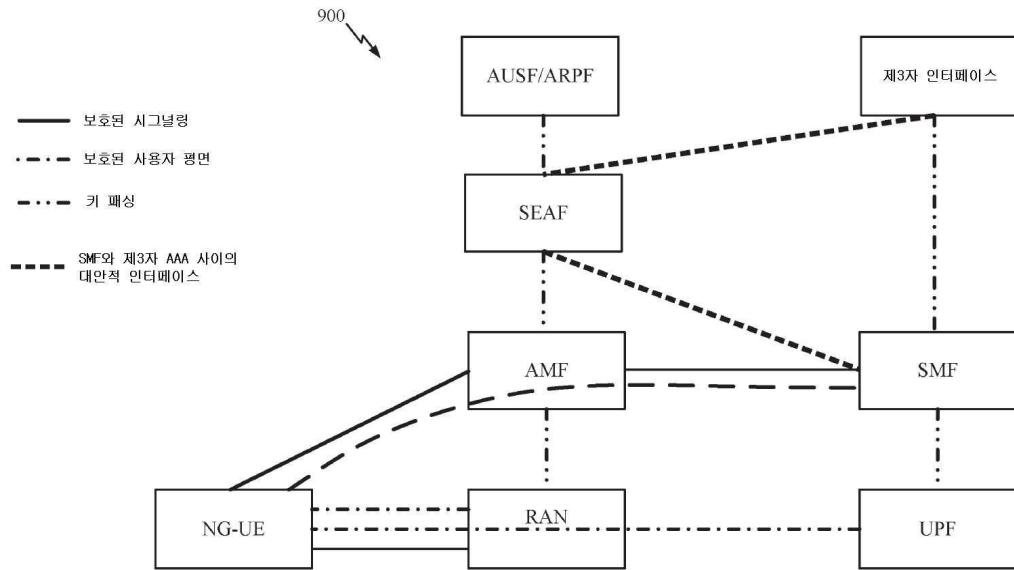
도면7



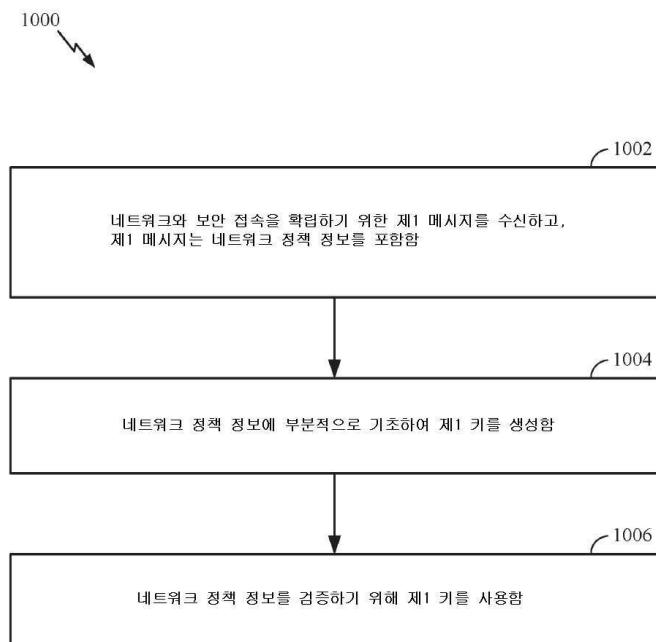
도면8

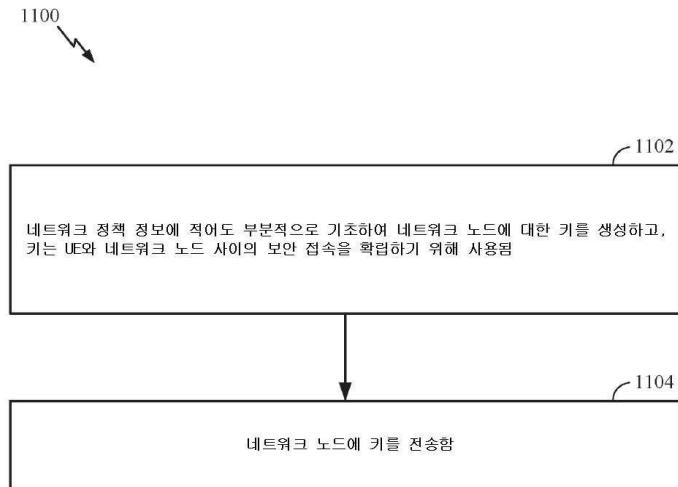
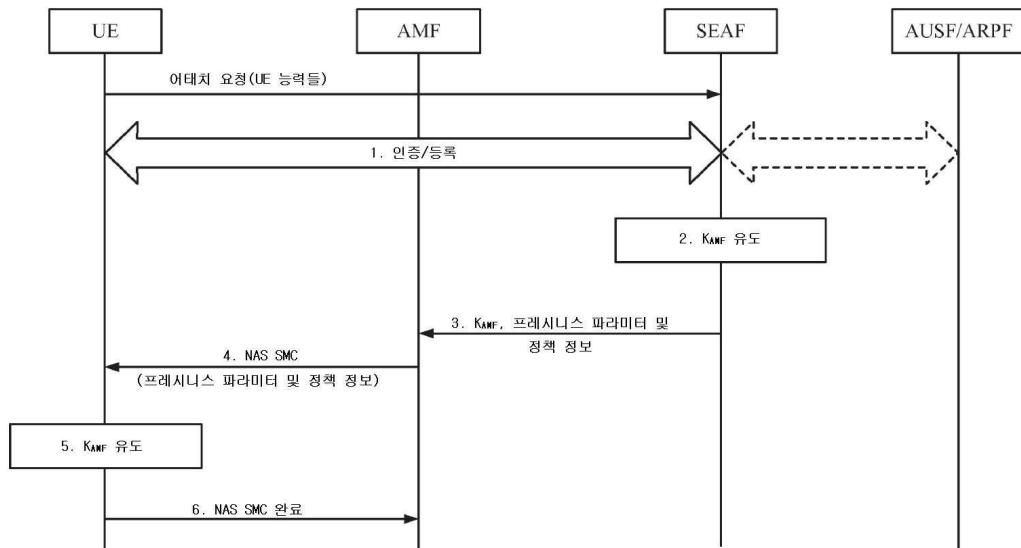


도면9

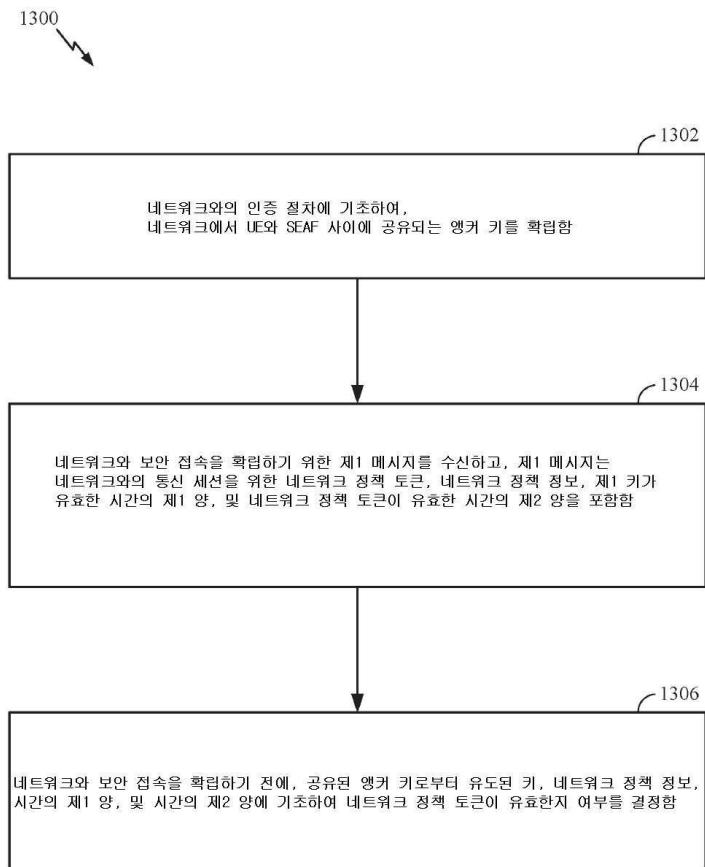


도면10

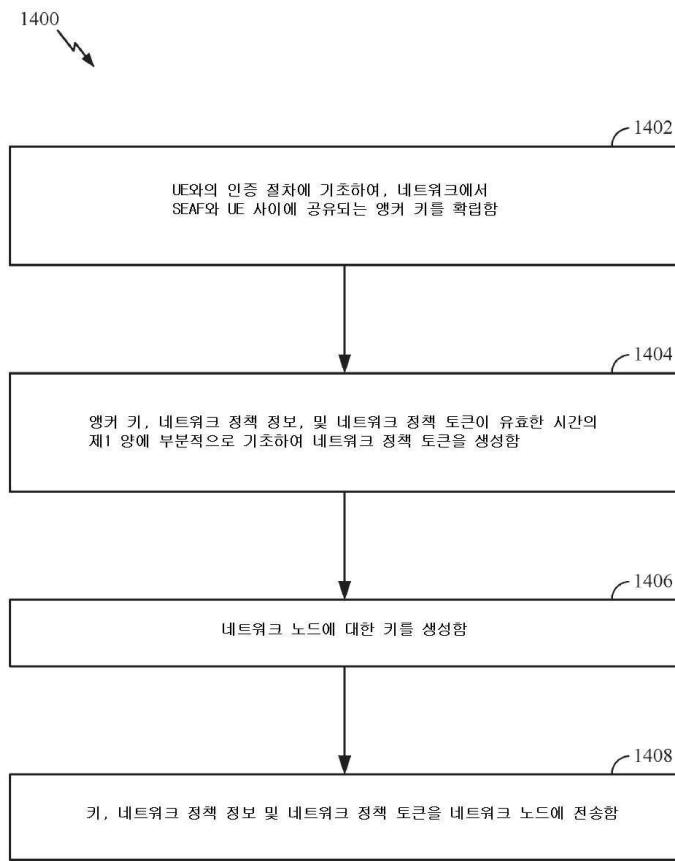


**도면11****도면12**

## 도면13



## 도면14



## 도면15

