



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0022013
(43) 공개일자 2025년02월14일

(51) 국제특허분류(Int. Cl.)
H04W 12/033 (2021.01) H04W 12/04 (2021.01)
H04W 12/63 (2021.01) H04W 64/00 (2023.01)
H04W 8/00 (2009.01)
(52) CPC특허분류
H04W 12/033 (2021.01)
H04W 12/04 (2021.01)
(21) 출원번호 10-2024-7039318
(22) 출원일자(국제) 2023년05월12일
심사청구일자 없음
(85) 번역문제출일자 2024년11월26일
(86) 국제출원번호 PCT/US2023/021977
(87) 국제공개번호 WO 2023/244368
국제공개일자 2023년12월21일
(30) 우선권주장
20220100499 2022년06월16일 그리스(GR)

(71) 출원인
켈컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
이, 수 범
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
지시모폴로스, 해리스
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
특허법인(유)남아이피그룹

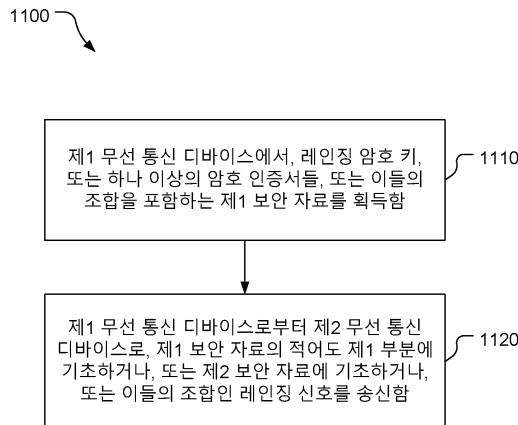
전체 청구항 수 : 총 30 항

(54) 발명의 명칭 모바일-투-모바일 포지셔닝을 위한 보안

(57) 요약

포지셔닝 세션 시그널링 방법은, 제1 무선 통신 디바이스에서, 레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하는 단계; 및 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하는 단계를 포함한다.

대표도 - 도11



(52) CPC특허분류

H04W 12/069 (2021.01)

H04W 12/104 (2021.01)

H04W 12/63 (2022.08)

H04W 64/00 (2013.01)

H04W 8/005 (2013.01)

(72) 발명자

마실로프스키, 댄

미국 92121 캘리포니아주 샌 디에고 모어하우스 드
라이브 5775

청, 홍

미국 92121 캘리포니아주 샌 디에고 모어하우스 드
라이브 5775

명세서

청구범위

청구항 1

제1 무선 통신 디바이스로서,

트랜시버;

메모리; 및

상기 트랜시버 및 상기 메모리에 통신가능하게 커플링된 프로세서를 포함하고, 상기 프로세서는,

레인징 암호 키(ranging cryptographic key), 또는 하나 이상의 암호 인증서(cryptographic certificate)들, 또는 이들의 조합을 포함하는 제1 보안 자료(security material)를 획득하도록; 그리고

상기 트랜시버를 통해, 제2 무선 통신 디바이스로, 상기 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하도록 구성되는, 제1 무선 통신 디바이스.

청구항 2

제1항에 있어서, 상기 제1 보안 자료는 대칭 암호 키인 상기 레인징 암호 키를 포함하고, 상기 레인징 신호는, 기본(base) 포지셔닝 기준 신호 및 상기 레인징 암호 키에 기초하는 수정된 포지셔닝 기준 신호를 포함하는, 제1 무선 통신 디바이스.

청구항 3

제1항에 있어서, 상기 제1 보안 자료는 제1 비대칭 암호 키를 포함하는 제1 암호로 서명된(cryptographically-signed) 인증서를 포함하고, 상기 프로세서는,

상기 트랜시버를 통해 상기 제2 무선 통신 디바이스로, 상기 제1 암호로 서명된 인증서를 송신하도록; 그리고

상기 제2 무선 통신 디바이스로부터 상기 트랜시버를 통해, 제2 비대칭 암호 키를 포함하는 제2 암호로 서명된 인증서를 수신하도록 추가로 구성되고;

상기 레인징 신호를 송신하기 위해, 상기 프로세서는, 상기 제1 비대칭 암호 키 및 상기 제2 비대칭 암호 키에 기초하는 대칭 암호 키에 기초하여 암호화된 상기 레인징 신호를 암호화된 유니캐스트 레인징 신호로서 송신하도록 구성되는, 제1 무선 통신 디바이스.

청구항 4

제3항에 있어서, 상기 프로세서는, 상기 제1 무선 통신 디바이스의 현재 위치가 상기 제1 암호로 서명된 인증서와 연관된 유효성 구역(validity region) 내에 있는 것에 기초하여 상기 제1 암호로 서명된 인증서를 송신하도록 구성되는, 제1 무선 통신 디바이스.

청구항 5

제1항에 있어서, 상기 프로세서는, 상기 트랜시버를 통해, 상기 레인징 암호 키를 수신하도록 추가로 구성되고, 상기 제2 보안 자료는 상기 레인징 암호 키를 포함하는, 제1 무선 통신 디바이스.

청구항 6

제1항에 있어서, 상기 프로세서는, 상기 트랜시버를 통해 상기 제2 무선 통신 디바이스로, 상기 제1 보안 자료의 적어도 제2 부분에 기초하는 발견 메시지(discovery message)를 송신하도록 추가로 구성되는, 제1 무선 통신 디바이스.

청구항 7

제6항에 있어서, 상기 제1 보안 자료의 상기 제1 부분은 상기 제1 보안 자료의 상기 제2 부분과 동일한, 제1 무선 통신 디바이스.

청구항 8

제1항에 있어서, 상기 제1 보안 자료는 상기 레인징 암호 키를 포함하고, 상기 프로세서는,

상기 트랜시버를 통해 상기 제2 무선 통신 디바이스로, 상기 제2 무선 통신 디바이스가 상기 레인징 암호 키를 위해 네트워크 엔티티에 연락(contact)하도록 하는 표시를 송신하도록; 그리고

상기 제1 무선 통신 디바이스에 저장된 기본 암호 키에 기초하여 상기 레인징 암호 키를 결정하도록 추가로 구성되는, 제1 무선 통신 디바이스.

청구항 9

제1항에 있어서,

상기 제1 보안 자료는, 상기 제1 무선 통신 디바이스 및 상기 제2 무선 통신 디바이스와는 별개인 엔티티에 의해 암호로 서명된 상기 제1 무선 통신 디바이스의 공개 암호 키를 포함하는 복수의 암호로 서명된 인증서들을 포함하고;

상기 프로세서는, 상기 트랜시버를 통해 상기 제2 무선 통신 디바이스로, 상기 제1 무선 통신 디바이스에 의해 암호로 서명되고 인증서 선택 정책에 기초하여 상기 복수의 암호로 서명된 인증서들 중 적어도 하나를 포함하는 발견 메시지를 송신하도록 추가로 구성되는, 제1 무선 통신 디바이스.

청구항 10

제9항에 있어서, 상기 프로세서는, 그룹 형성 동안 상기 제2 무선 통신 디바이스와 상기 레인징 암호 키를 협상하도록 추가로 구성되고, 상기 레인징 신호는, 기본 포지셔닝 기준 신호, 또는 상기 레인징 암호 키, 또는 선도 파라미터(freshness parameter), 또는 이들 중 2개 이상의 조합에 기초하는 수정된 포지셔닝 기준 신호를 포함하고, 상기 선도 파라미터는 타이머, 카운터, 시스템 프레임 수(system frame number), 슬롯 수(slot number), 심볼 수(symbol number), 또는 이들 중 2개 이상의 임의의 조합을 포함하는, 제1 무선 통신 디바이스.

청구항 11

포지셔닝 세션 시그널링 방법으로서,

제1 무선 통신 디바이스에서, 레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하는 단계; 및

상기 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 상기 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하는 단계를 포함하는, 포지셔닝 세션 시그널링 방법.

청구항 12

제11항에 있어서, 상기 제1 보안 자료는 대칭 암호 키인 상기 레인징 암호 키를 포함하고, 상기 레인징 신호는, 기본 포지셔닝 기준 신호 및 상기 레인징 암호 키에 기초하는 수정된 포지셔닝 기준 신호를 포함하는, 포지셔닝 세션 시그널링 방법.

청구항 13

제11항에 있어서, 상기 제1 보안 자료는 제1 비대칭 암호 키를 포함하는 제1 암호로 서명된 인증서를 포함하고, 상기 포지셔닝 세션 시그널링 방법은,

상기 제1 무선 통신 디바이스로부터 상기 제2 무선 통신 디바이스로, 상기 제1 암호로 서명된 인증서를 송신하는 단계; 및

상기 제2 무선 통신 디바이스로부터 상기 제1 무선 통신 디바이스에서, 제2 비대칭 암호 키를 포함하는 제2 암호로 서명된 인증서를 수신하는 단계를 추가로 포함하고;

상기 레인징 신호를 송신하는 단계는, 상기 제1 비대칭 암호 키 및 상기 제2 비대칭 암호 키에 기초하는 대칭 암호 키에 기초하여 암호화된 상기 레인징 신호를 암호화된 유니캐스트 레인징 신호로서 송신하는 단계를 포함하는, 포지셔닝 세션 시그널링 방법.

청구항 14

제13항에 있어서, 상기 제1 암호로 서명된 인증서는, 상기 제1 무선 통신 디바이스의 현재 위치가 상기 제1 암호로 서명된 인증서와 연관된 유효성 구역 내에 있는 것에 기초하여 송신되는, 포지셔닝 세션 시그널링 방법.

청구항 15

제11항에 있어서, 상기 제2 무선 통신 디바이스 또는 네트워크 엔티티로부터 상기 제1 무선 통신 디바이스에서, 상기 레인징 암호 키를 수신하는 단계를 추가로 포함하고, 상기 제2 보안 자료는 상기 레인징 암호 키를 포함하는, 포지셔닝 세션 시그널링 방법.

청구항 16

제11항에 있어서, 상기 제1 무선 통신 디바이스로부터 상기 제2 무선 통신 디바이스로, 상기 제1 보안 자료의 적어도 제2 부분에 기초하는 발견 메시지를 송신하는 단계를 추가로 포함하는, 포지셔닝 세션 시그널링 방법.

청구항 17

제16항에 있어서, 상기 제1 보안 자료의 상기 제1 부분은 상기 제1 보안 자료의 상기 제2 부분과 동일한, 포지셔닝 세션 시그널링 방법.

청구항 18

제11항에 있어서, 상기 제1 보안 자료는 상기 레인징 암호 키를 포함하고, 상기 포지셔닝 세션 시그널링 방법은,

상기 제1 무선 통신 디바이스로부터 상기 제2 무선 통신 디바이스로, 상기 제2 무선 통신 디바이스가 상기 레인징 암호 키를 위해 네트워크 엔티티에 연락하도록 하는 표시를 송신하는 단계; 및

상기 제1 무선 통신 디바이스에서, 상기 제1 무선 통신 디바이스에 저장된 기본 암호 키에 기초하여 상기 레인징 암호 키를 결정하는 단계를 추가로 포함하는, 포지셔닝 세션 시그널링 방법.

청구항 19

제11항에 있어서,

상기 제1 보안 자료는, 상기 제1 무선 통신 디바이스 및 상기 제2 무선 통신 디바이스와는 별개인 엔티티에 의해 암호로 서명된 상기 제1 무선 통신 디바이스의 공개 암호 키를 포함하는 복수의 암호로 서명된 인증서들을 포함하고;

상기 포지셔닝 세션 시그널링 방법은, 상기 제1 무선 통신 디바이스로부터 상기 제2 무선 통신 디바이스로, 상기 제1 무선 통신 디바이스에 의해 암호로 서명되고 인증서 선택 정책에 기초하여 상기 복수의 암호로 서명된 인증서들 중 적어도 하나를 포함하는 발견 메시지를 송신하는 단계를 추가로 포함하는, 포지셔닝 세션 시그널링 방법.

청구항 20

제19항에 있어서, 상기 제1 무선 통신 디바이스가 그룹 형성 동안 상기 제2 무선 통신 디바이스와 상기 레인징 암호 키를 협상하는 단계를 추가로 포함하고, 상기 레인징 신호는, 기본 포지셔닝 기준 신호, 또는 상기 레인징 암호 키, 또는 선도 파라미터, 또는 이들 중 2개 이상의 조합에 기초하는 수정된 포지셔닝 기준 신호를 포함하고, 상기 선도 파라미터는 타이머, 카운터, 시스템 프레임 수, 슬롯 수, 심볼 수, 또는 이들 중 2개 이상의 임의의 조합을 포함하는, 포지셔닝 세션 시그널링 방법.

청구항 21

제1 무선 통신 디바이스로서,

레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하기 위한 수단; 및

제2 무선 통신 디바이스로, 상기 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하기 위한 수단을 포함하는, 제1 무선 통신 디바이스.

청구항 22

제21항에 있어서, 상기 제1 보안 자료는 대칭 암호 키인 상기 레인징 암호 키를 포함하고, 상기 레인징 신호는, 기본 포지셔닝 기준 신호 및 상기 레인징 암호 키에 기초하는 수정된 포지셔닝 기준 신호를 포함하는, 제1 무선 통신 디바이스.

청구항 23

제21항에 있어서, 상기 제1 보안 자료는 제1 비대칭 암호 키를 포함하는 제1 암호로 서명된 인증서를 포함하고, 상기 제1 무선 통신 디바이스는,

상기 제2 무선 통신 디바이스로, 상기 제1 암호로 서명된 인증서를 송신하기 위한 수단; 및

상기 제2 무선 통신 디바이스로부터, 제2 비대칭 암호 키를 포함하는 제2 암호로 서명된 인증서를 수신하기 위한 수단을 추가로 포함하고;

상기 레인징 신호를 송신하기 위한 수단은, 상기 제1 비대칭 암호 키 및 상기 제2 비대칭 암호 키에 기초하는 대칭 암호 키에 기초하여 암호화된 상기 레인징 신호를 암호화된 유니캐스트 레인징 신호로서 송신하기 위한 수단을 포함하는, 제1 무선 통신 디바이스.

청구항 24

제23항에 있어서, 상기 제1 암호로 서명된 인증서를 송신하기 위한 수단은, 상기 제1 무선 통신 디바이스의 현재 위치가 상기 제1 암호로 서명된 인증서와 연관된 유효성 구역 내에 있는 것에 기초하여 상기 제1 암호로 서명된 인증서를 송신하기 위한 수단을 포함하는, 제1 무선 통신 디바이스.

청구항 25

제21항에 있어서, 상기 제2 무선 통신 디바이스 또는 네트워크 엔티티로부터, 상기 레인징 암호 키를 수신하기 위한 수단을 추가로 포함하고, 상기 제2 보안 자료는 상기 레인징 암호 키를 포함하는, 제1 무선 통신 디바이스.

청구항 26

제21항에 있어서, 상기 제2 무선 통신 디바이스로, 상기 제1 보안 자료의 적어도 제2 부분에 기초하는 발견 메시지를 송신하기 위한 수단을 추가로 포함하는, 제1 무선 통신 디바이스.

청구항 27

제26항에 있어서, 상기 제1 보안 자료의 상기 제1 부분은 상기 제1 보안 자료의 상기 제2 부분과 동일한, 제1 무선 통신 디바이스.

청구항 28

제21항에 있어서, 상기 제1 보안 자료는 상기 레인징 암호 키를 포함하고, 상기 제1 무선 통신 디바이스는,

상기 제2 무선 통신 디바이스로, 상기 제2 무선 통신 디바이스가 상기 레인징 암호 키를 위해 네트워크 엔티티에 연락하도록 하는 표시를 송신하기 위한 수단; 및

상기 제1 무선 통신 디바이스에 저장된 기본 암호 키에 기초하여 상기 레인징 암호 키를 결정하기 위한 수단을 추가로 포함하는, 제1 무선 통신 디바이스.

청구항 29

제21항에 있어서,

상기 제1 보안 자료는, 상기 제1 무선 통신 디바이스 및 상기 제2 무선 통신 디바이스와는 별개인 엔티티에 의해 암호로 서명된 상기 제1 무선 통신 디바이스의 공개 암호 키를 포함하는 복수의 암호로 서명된 인증서들을 포함하고;

상기 제1 무선 통신 디바이스는, 상기 제2 무선 통신 디바이스로, 상기 제1 무선 통신 디바이스에 의해 암호로 서명되고 인증서 선택 정책에 기초하여 상기 복수의 암호로 서명된 인증서들 중 적어도 하나를 포함하는 발견 메시지를 송신하기 위한 수단을 추가로 포함하는, 제1 무선 통신 디바이스.

청구항 30

프로세서 판독가능 명령들을 포함하는 비일시적 프로세서 판독가능 저장 매체로서, 상기 프로세서 판독가능 명령들은, 제1 무선 통신 디바이스의 프로세서로 하여금,

레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하게 하도록; 그리고

제2 무선 통신 디바이스로, 상기 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하게 하도록 구성되는, 비일시적 프로세서 판독가능 저장 매체.

발명의 설명

기술 분야

[0001] 관련 출원들에 대한 상호 참조

[0002] 본 출원은 "SECURITY FOR MOBILE-TO-MOBILE POSITIONING"이라는 명칭으로 2022년 6월 16일자로 출원된 그리스 특허 출원 일련 번호 제20220100499호의 이익을 주장하며, 이는 본 출원의 양수인에게 양도되며, 그 전체 내용이 이로써 모든 목적들을 위해 참고로 본 명세서에 통합된다.

배경 기술

[0003] 무선 통신 시스템들은 1세대 아날로그 무선 전화 서비스(1G), 2세대(2G) 디지털 무선 전화 서비스(중간 2.5G 및 2.75G 네트워크들을 포함함), 3세대(3G) 고속 데이터, 인터넷 가능 무선 서비스, 4세대(4G) 서비스(예컨대, 롱 텀 에볼루션(Long Term Evolution, LTE) 또는 WiMax®), 5세대(5G) 서비스(예컨대, 5G 뉴 라디오(New Radio, NR)) 등을 포함하여 다양한 세대들을 통해 개발되어 왔다. 셀룰러 및 개인 통신 서비스(Personal Communications Service, PCS) 시스템들을 포함하여, 현재 사용 중인 많은 상이한 타입들의 무선 통신 시스템들이 있다. 알려진 셀룰러 시스템들의 예들은 셀룰러 아날로그 어드밴스드 모바일 전화 시스템(Advanced Mobile Phone System, AMPS), 및 코드 분할 다중 액세스(Code Division Multiple Access, CDMA), 주파수 분할 다중 액세스(Frequency Division Multiple Access, FDMA), 직교 주파수 분할 다중 액세스(Orthogonal Frequency Division Multiple Access, OFDMA), 시간 분할 다중 액세스(Time Division Multiple Access, TDMA), TDMA의 GSM(Global System for Mobile access) 변형 등에 기초한 디지털 셀룰러 시스템들을 포함한다.

[0004] 5세대(5G) 모바일 표준은 다른 개선들 중에서도, 더 높은 데이터 전송 속도들, 더 많은 수들의 연결들, 및 더 우수한 커버리지를 요구한다. 차세대 모바일 네트워크 연합(Next Generation Mobile Networks Alliance)에 따른 5G 표준은, 사무실 층에 있는 수십 명의 작업자들에게 초당 1기가비트로, 수만 명의 사용자들 각각에게 초당 수십 메가비트의 데이터 레이트들을 제공하도록 설계된다. 대규모 센서 배치들을 지원하기 위해서는 수십만 개의 동시 연결들이 지원되어야 한다. 결과적으로, 5G 모바일 통신들의 스펙트럼 효율은 현재 4G 표준에 비해 상당히 향상되어야 한다. 또한, 현재 표준들에 비해 시그널링 효율들이 향상되어야 하고 레이턴시가 크게 감소되어야 한다.

발명의 내용

[0005] 예시적인 제1 무선 통신 디바이스는, 트랜시버; 메모리; 및 트랜시버 및 메모리에 통신가능하게 커플링된 프로세서를 포함하고, 프로세서는, 레인징 암호 키(ranging cryptographic key), 또는 하나 이상의 암호 인증서(cryptographic certificate)들, 또는 이들의 조합을 포함하는 제1 보안 자료(security material)를 획득하도록; 그리고 트랜시버를 통해 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하도록 구성된다.

[0006] 예시적인 포지셔닝 세션 시그널링 방법은, 제1 무선 통신 디바이스에서, 레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하는 단계; 및 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하는 단계를 포함한다.

[0007] 다른 예시적인 제1 무선 통신 디바이스는, 레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하기 위한 수단; 및 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하기 위한 수단을 포함한다.

[0008] 예시적인 비밀시적 프로세서 판독가능 저장 매체는 프로세서 판독가능 명령들을 포함하고, 프로세서 판독가능 명령들은, 제1 무선 통신 디바이스의 프로세서로 하여금, 레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하게 하도록; 그리고 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하게 하도록 구성된다.

도면의 간단한 설명

[0009] 도 1은 예시적인 무선 통신 시스템의 간략화된 도면이다.
 도 2는 도 1에 도시된 예시적인 사용자 장비의 컴포넌트들의 블록도이다.
 도 3은 예시적인 송신/수신 포인트(transmission/reception point, TRP)의 컴포넌트들의 블록도이다.
 도 4는 예시적인 서버의 컴포넌트들의 블록도이며, 그의 다양한 실시 형태들이 도 1에 도시되어 있다.
 도 5는 예시적인 사용자 장비의 간략화된 블록도이다.
 도 6은 예시적인 네트워크 엔티티의 간략화된 블록도이다.
 도 7은 사이드링크 포지셔닝을 위한 간략화된 환경의 도면이다.
 도 8은 사이드링크 포지셔닝을 위한 시그널링 및 프로세스 흐름이다.
 도 9는 네트워크 보조된/관리된 그룹 형성 및 브로드캐스트 또는 유니캐스트 사이드링크 포지셔닝을 위한 시그널링 및 프로세스 흐름이다.
 도 10은 사용자 장비 기반 그룹 형성 및 브로드캐스트 또는 유니캐스트 사이드링크 포지셔닝을 위한 시그널링 및 프로세스 흐름이다.
 도 11은 포지셔닝 세션 시그널링 방법의 블록 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0010] 무선 디바이스들 사이의 포지셔닝(예컨대, 사이드링크 포지셔닝)에 보안(예컨대, 기밀성 및/또는 무결성)을 제공하기 위한 기법들이 본 명세서에서 논의된다. 무선 디바이스들 중 하나 이상은, 사용자 장비(user equipment, UE)라고 불릴 수 있는 모바일 무선 통신 디바이스일 수 있고, 하나 이상의 암호 키들(대칭 및/또는 비대칭 키들) 및/또는 하나 이상의 디지털 인증서들과 같은 보안 자료를 저장할 수 있다. 본 명세서에서의 논의가 모바일 무선 통신 디바이스들에 초점을 맞추지만, 그 논의는 하나 이상의 비-모바일 디바이스들(예컨대, 노변 유닛(Roadside Unit, RSU))의 사용에 적용된다. 보안 자료는, 예컨대, 네트워크 엔티티로부터 다운로드되거나 또는 다른 UE로부터 수신된 것과 같이 다른 무선 통신 디바이스로부터 수신되는 것에 의해, 제조 동안 그리고/또는 제조 이후 모바일 무선 통신 디바이스에 저장될 수 있다. UE는 기밀성-보호된 통신들(이들은 보안 자료의 암호 키를 사용하여 암호화되거나, 또는 보안 자료로부터 유도됨) 및/또는 무결성-보호된 통신들(이들은 암호로 서명되고(cryptographically signed) 그리고/또는 암호 서명(cryptographic signature)을 포함함)을 사용하는 하나 이상의 다른 UE들을 발견할 수 있지만, 발견 메시징은 선택적이다. UE는 메시지들 및 포지셔닝 기준 신호(positioning reference signal, PRS)가 기밀성 및/또는 무결성 보호되는 경우 메시지들 및 PRS 전송을 통해 다른 UE와의 레인징에 관여할 수 있다. 예를 들어, 포지셔닝 신호들(포지셔닝 메시지들을 포함함)은, 보안 자료에 포함되거나 또는 보안 자료로부터 유도되는 암호 키를 사용하여 암호화될 수 있고, 그리고/또는 보안 자료에 포함되거나 또는 보안 자료로부터 유도되는 암호 키를 사용하여 서명될 수 있다. 그러나, 다른 예들이

구현될 수 있다.

- [0011] 본 명세서에 설명된 항목들 및/또는 기법들은 다음의 능력들 중 하나 이상뿐만 아니라, 언급되지 않은 다른 능력들도 제공할 수 있다. 포지셔닝 시그널링에 포함된 민감 정보(Sensitive information)가 원하지 않는 엔티티들에 의해 발견되는 것으로부터 보호될 수 있다. 발견 시그널링의 경우, 아이덴티티 프라이버시 및/또는 서비스 식별/프라이버시가 제공될 수 있고, 그리고/또는 가짜 서비스 공지들/요청들이 작용되지 않게 방지될 수 있다. PRS 이전(pre-PRS) 메시지들의 경우, 아이덴티티 프라이버시가 제공될 수 있고, (예컨대, 타깃화된/최적화된 공격들로부터의) 파라미터 유출(parameter leakage)이 억제(예컨대, 방지)될 수 있고, 그리고/또는 파라미터 수정(서비스 거부(denial of service, DoS) 또는 서비스 저하(service degradation)를 초래함)이 억제(예컨대, 방지)될 수 있다. PRS 응답들을 위해 아이덴티티 프라이버시가 제공될 수 있다. PRS 주입으로 인한 포지셔닝 에러들이 억제(예컨대, 방지)되어, 부정확한(과대(over)/과소(under)) 범위 추정들을 회피할 수 있다. PRS 이후(post-PRS) 메시지들의 경우, 위치 프라이버시가 제공될 수 있고 그리고/또는 위치 에러를 초래하는 측정 결과 수정이 억제(예컨대, 방지)될 수 있다. 다른 능력들이 제공될 수 있고, 본 개시내용에 따른 모든 구현이 논의된 능력들 전부는 물론이고 임의의 것을 제공해야 하는 것은 아니다.
- [0012] 무선 네트워크에 액세스하고 있는 모바일 디바이스들의 위치들을 획득하는 것은, 예를 들어, 긴급 통화들, 개인 내비게이션, 소비자 자산 추적, 친구 또는 가족 구성원 위치확인 등을 포함한 많은 애플리케이션들에 유용할 수 있다. 기존 포지셔닝 방법들은 기지국들 및 액세스 포인트들과 같은 무선 네트워크 내의 SV(satellite vehicle)들 및 지상 라디오 소스들을 포함한 다양한 디바이스들 또는 엔티티들로부터 송신된 라디오 신호들을 측정하는 것에 기초한 방법들을 포함한다. 5G 무선 네트워크들에 대한 표준화는, LTE 무선 네트워크들이 현재 포지션 결정을 위한 포지셔닝 기준 신호(PRS)들 및/또는 셀-특정 기준 신호(Cell-specific Reference Signal, CRS)들을 활용하는 것과 유사한 방식으로 기지국들에 의해 송신된 기준 신호들을 활용할 수 있는 다양한 포지셔닝 방법들에 대한 지원을 포함할 것으로 예상된다.
- [0013] 본 명세서에서의 설명은 예를 들어, 컴퓨팅 디바이스의 엘리먼트들에 의해 수행될 액션들의 시퀀스들을 언급할 수 있다. 본 명세서에 설명된 다양한 액션들은 특정 회로들(예컨대, 주문형 집적 회로(application specific integrated circuit, ASIC))에 의해, 하나 이상의 프로세서들에 의해 실행되는 프로그램 명령들에 의해, 또는 둘 모두의 조합에 의해 수행될 수 있다. 본 명세서에 설명된 액션들의 시퀀스들은, 실행 시에, 연관된 프로세서로 하여금, 본 명세서에 설명된 기능을 수행하게 할 컴퓨터 명령들의 대응하는 세트를 저장한 비일시적 컴퓨터 판독가능 매체 내에 구현될 수 있다. 따라서, 본 명세서에 설명된 다양한 예들은 다수의 상이한 형태들로 구현될 수 있으며, 그 형태들 모두는 청구된 청구 대상을 포함하여 본 개시내용의 범주 내에 있다.
- [0014] 본 명세서에 사용된 바와 같이, 용어들 "사용자 장비"(UE) 및 "기지국"은 달리 언급되지 않는 한 임의의 특정 라디오 액세스 기술(Radio Access Technology, RAT)에 특정되거나 또는 달리 그것으로 제한되지 않는다. 일반적으로, UE는 무선 통신 네트워크를 통해 통신하는 데 사용되는 임의의 무선 통신 디바이스(예컨대, 모바일 전화, 라우터, 태블릿 컴퓨터, 랩톱 컴퓨터, 소비자 자산 추적 디바이스, 사물 인터넷(Internet of Things, IoT) 디바이스 등)일 수 있다. UE는 이동식일 수 있거나 또는 (예컨대, 특정 시간들에) 고정식일 수 있고, 라디오 액세스 네트워크(Radio Access Network, RAN)와 통신할 수 있다. 본 명세서에 사용된 바와 같이, 용어 "UE"는 "액세스 단말기" 또는 "AT", "클라이언트 디바이스", "무선 디바이스", "가입자 디바이스", "가입자 단말기", "가입자 스테이션", "사용자 단말기" 또는 UT, "모바일 단말기", "모바일 스테이션", "모바일 디바이스", 또는 이들의 변형들로 상호교환가능하게 지칭될 수 있다. 일반적으로, UE들은 RAN을 통해 코어 네트워크와 통신할 수 있으며, 그 코어 네트워크를 통해, UE들은 인터넷과 같은 외부 네트워크들과 그리고 다른 UE들과 연결될 수 있다. 물론, 코어 네트워크 및/또는 인터넷에 연결하는 다른 메커니즘들이 또한, 이를테면, 유선 액세스 네트워크들, WiFi® 네트워크들(예컨대, IEEE(Institute of Electrical and Electronics Engineers) 802.11 등에 기초함) 등을 통해 UE들에 대해 가능하다.
- [0015] 기지국은, 자신이 배치되는 네트워크에 따라 UE들과 통신하는 여러 RAT들 중 하나에 따라 동작할 수 있다. 기지국의 예들은 액세스 포인트(Access Point, AP), 네트워크 노드(Network Node), NodeB, 진화된 NodeB(evolved NodeB, eNB), 또는 일반 Node B(gNodeB, gNB)를 포함한다. 추가로, 일부 시스템들에서, 기지국은 순수 예지 노드 시그널링 기능들을 제공할 수 있는 한편, 다른 시스템들에서는, 추가적인 제어 및/또는 네트워크 관리 기능들을 제공할 수 있다.
- [0016] UE들은 인쇄 회로(printed circuit, PC) 카드들, 콤팩트 플래시 디바이스들, 외부 또는 내부 모듈들, 무선 또는 와이어라인(wireline) 전화들, 스마트폰들, 태블릿들, 소비자 자산 추적 디바이스들, 자산 태그들 등을 포함하

지만, 이들로 제한되지 않는 다수의 타입들의 디바이스들 중 임의의 것에 의해 구현될 수 있다. UE들이 RAN으로 신호들을 전송할 수 있는 통신 링크는 업링크 채널(예컨대, 역방향 트래픽 채널, 역방향 제어 채널, 액세스 채널 등)로 불린다. RAN이 UE들로 신호들을 전송할 수 있는 통신 링크는 다운링크 또는 순방향 링크 채널(예컨대, 페이징 채널, 제어 채널, 브로드캐스트 채널, 순방향 트래픽 채널 등)로 불린다. 본 명세서에 사용된 바와 같이, 용어 트래픽 채널(traffic channel, TCH)은 업링크/역방향 또는 다운링크/순방향 트래픽 채널을 지칭할 수 있다.

[0017] 본 명세서에 사용된 바와 같이, 용어 "셀" 또는 "섹터"는 맥락에 따라 기지국의 복수의 셀들 중 하나, 또는 기지국 그 자체에 대응할 수 있다. 용어 "셀"은 (예를 들어, 캐리어를 통한) 기지국과의 통신을 위해 사용되는 논리적 통신 엔티티를 지칭할 수 있고, 동일한 또는 상이한 캐리어를 통해 동작하는 이웃 셀들을 구별하기 위한 식별자(예를 들어, PCID(physical cell identifier), VCID(virtual cell identifier))와 연관될 수 있다. 일부 예들에서, 캐리어는 다수의 셀들을 지원할 수 있고, 상이한 셀들은 상이한 타입들의 디바이스들에 대한 액세스를 제공할 수 있는 상이한 프로토콜 타입들(예를 들어, MTC(machine-type communication), 협대역 사물 인터넷(NB-IoT), eMBB(enhanced mobile broadband) 등)에 따라 구성될 수 있다. 일부 예들에서, 용어 "셀"은 논리적 엔티티가 동작하는 지리적 커버리지 영역의 일부(예를 들어, 섹터)를 지칭할 수 있다.

[0018] 도 1을 참조하면, 통신 시스템(100)의 일 예는 UE(105), UE(106), 라디오 액세스 네트워크(RAN), 여기서는 5세대(5G) NG-RAN(Next Generation(NG) RAN)(135), 5G 코어 네트워크(5GC)(140), 및 서버(150)를 포함한다. UE(105) 및/또는 UE(106)는, 예컨대 IoT 디바이스, 위치 추적기 디바이스, 휴대 전화, 차량(예컨대, 자동차, 트럭, 버스, 보트 등) 또는 다른 디바이스일 수 있다. 5G 네트워크는 또한, 뉴 라디오(NR) 네트워크로 지칭될 수 있고; NG-RAN(135)은 5G RAN 또는 NR RAN으로 지칭될 수 있고; 5GC(140)는 NG 코어 네트워크(NG Core network, NGC)로 지칭될 수 있다. NG-RAN 및 5GC의 표준화는 3GPP(3rd Generation Partnership Project)에서 진행 중이다. 따라서, NG-RAN(135) 및 5GC(140)는 3GPP로부터의 5G 지원을 위한 현재 또는 미래 표준들을 따를 수 있다. NG-RAN(135)은 다른 타입의 RAN, 예컨대, 3G RAN, 4G 롱 텀 에볼루션(LTE) RAN 등일 수 있다. UE(106)는 UE(105)와 유사하게 시스템(100) 내의 유사한 다른 엔티티들로/로부터 신호들을 전송 및/또는 수신하도록 구성 및 커플링될 수 있지만, 그러한 시그널링은 도면의 단순화를 위해 도 1에 표시되지 않는다. 유사하게, 논의는 단순화를 위해 UE(105)에 초점을 맞춘다. 통신 시스템(100)은, 글로벌 포지셔닝 시스템(Global Positioning System, GPS), 글로벌 내비게이션 위성 시스템(GLONASS), 갈릴레오(Galileo), 또는 베이더우(Beidou)와 같은 위성 포지셔닝 시스템(Satellite Positioning System, SPS)(예컨대, 글로벌 내비게이션 위성 시스템(Global Navigation Satellite System, GNSS)) 또는 일부 다른 로컬 또는 지역 SPS, 이를테면, IRNSS(Indian Regional Navigational Satellite System), EGNOS(European Geostationary Navigation Overlay Service) 또는 WAAS(Wide Area Augmentation System)에 대한 SV들(190, 191, 192, 193)의 성상도(constellation)(185)로부터의 정보를 활용할 수 있다. 통신 시스템(100)의 추가적인 컴포넌트들이 아래에서 설명된다. 통신 시스템(100)은 추가적인 또는 대안적인 컴포넌트들을 포함할 수 있다.

[0019] 도 1에 도시된 바와 같이, NG-RAN(135)은 NR nodeB(gNB)들(110a, 110b) 및 차세대 eNodeB(ng-eNB)(114)를 포함하고, 5GC(140)는 AMF(Access and Mobility Management Function)(115), SMF(Session Management Function)(117), LMF(Location Management Function)(120), 및 GMLC(Gateway Mobile Location Center)(125)를 포함한다. gNB들(110a, 110b) 및 ng-eNB(114)는 서로 통신가능하게 커플링되고, 각각 UE(105)와 양방향으로 무선 통신하도록 구성되고, 각각 AMF(115)에 통신가능하게 커플링되고 이와 양방향으로 통신하도록 구성된다. gNB들(110a, 110b) 및 ng-eNB(114)는 기지국(BS)들로 지칭될 수 있다. AMF(115), SMF(117), LMF(120) 및 GMLC(125)는 서로 통신가능하게 커플링되고, GMLC는 외부 클라이언트(130)에 통신가능하게 커플링된다. SMF(117)는 미디어 세션들을 생성, 제어 및 삭제하기 위한 SCF(Service Control Function)(도시되지 않음)의 초기 접점(initial contact point)의 역할을 할 수 있다. gNB들(110a, 110b) 및/또는 ng-eNB(114)와 같은 기지국들은 매크로 셀(예컨대, 고전력 셀룰러 기지국), 또는 소형 셀(예컨대, 저전력 셀룰러 기지국), 또는 액세스 포인트(예컨대, WiFi®, WiFi® 다이렉트(WiFi®-Direct, WiFi®-D), Bluetooth®, Bluetooth® 저 에너지(BLE), Zigbee® 등과 같은 단거리(short-range) 기술과 통신하도록 구성된 단거리 기지국)일 수 있다. 하나 이상의 기지국들, 예컨대, ng-eNB(114) 및/또는 gNB들(110a, 110b) 중 하나 이상은 다수의 캐리어들을 통해 UE(105)와 통신하도록 구성될 수 있다. gNB들(110a, 110b) 및 ng-eNB(114) 각각은 각자의 지리적 구역, 예컨대, 셀에 대한 통신 커버리지를 제공할 수 있다. 각각의 셀은 기지국 안테나들의 기능에 따라 다수의 섹터들로 분할될 수 있다.

[0020] 도 1은 다양한 컴포넌트들의 일반화된 예시를 제공하며, 이들 중 임의의 것 또는 전부는 적절하게 활용될 수 있

고, 그 각각은 필요에 따라 중복되거나 생략될 수 있다. 구체적으로, 하나의 UE(105)가 예시되어 있지만, 많은 UE들(예컨대, 수백, 수천, 수백만 개 등)이 통신 시스템(100)에서 활용될 수 있다. 유사하게, 통신 시스템(100)은 더 많은(또는 더 적은) 수의 SV들(즉, 도시된 4개의 SV들(190 내지 193)보다 더 많거나 더 적음), gNB들(110a, 110b), ng-eNB들(114), AMF들(115), 외부 클라이언트들(130) 및/또는 다른 컴포넌트들을 포함할 수 있다. 통신 시스템(100)의 다양한 컴포넌트들을 연결하는 예시된 연결들은 추가적인(중개) 컴포넌트들, 직접 또는 간접 물리적 및/또는 무선 연결들, 및/또는 추가적인 네트워크들을 포함할 수 있는 데이터 및 시그널링 연결들을 포함한다. 더욱이, 컴포넌트들은 원하는 기능에 따라 재배열, 조합, 분리, 대체 및/또는 생략될 수 있다.

[0021] 도 1은 5G 기반 네트워크를 예시하지만, 유사한 네트워크 구현들 및 구성들이 3G, 롱 텀 에볼루션(LTE) 등과 같은 다른 통신 기술들을 위해 사용될 수 있다. 본 명세서에 설명된 구현들(5G 기술에 대한 것이든 그리고/또는 하나 이상의 다른 통신 기술들 및/또는 프로토콜들에 대한 것이든)은 방향성 동기화 신호(synchronization signal, SS)들을 송신(또는 브로드캐스팅)하고, UE들(예컨대, UE(105))에서 방향성 신호들을 수신 및 측정하고 그리고/또는 (GMLC(125) 또는 다른 위치 서버를 통해) UE(105)에 위치 보조를 제공하고 그리고/또는 그러한 방향으로 송신된 신호들에 대해 UE(105)에서 수신된 측정 수량들에 기초하여 UE(105), gNB(110a, 110b), 또는 LMF(120)와 같은 위치 가능 디바이스(location-capable device)에서 UE(105)에 대한 위치를 컴퓨팅하는 데 사용될 수 있다. GMLC(125), LMF(120), AMF(115), SMF(117), ng-eNB(eNodeB)(114) 및 gNB(gNodeB)들(110a, 110b)은 예들이며, 다양한 실시 형태들에서, 각각 다양한 다른 위치 서버 기능 및/또는 기지국 기능에 의해 대체되거나 또는 이들을 포함할 수 있다.

[0022] 시스템(100)은 시스템(100)의 컴포넌트들이 직접 또는 간접적으로, 예컨대, gNB들(110a, 110b), ng-eNB(114) 및/또는 5GC(140)(및/또는 하나 이상의 다른 베이스 트랜시버 스테이션들과 같은, 도시되지 않은 하나 이상의 다른 디바이스들)를 통해 (적어도 몇 번은 무선 연결들을 사용하여) 서로 통신할 수 있다는 점에서 무선 통신이 가능하다. 간접 통신들의 경우, 예컨대, 데이터 패킷들의 헤더 정보를 변경하기 위해, 포맷을 변경하는 등을 위해 하나의 엔티티로부터 다른 엔티티로의 송신 동안 통신들이 변경될 수 있다. UE(105)는 다수의 UE들을 포함할 수 있고 모바일 무선 통신 디바이스일 수 있지만, 무선으로 그리고 유선 연결들을 통해 통신할 수 있다. UE(105)는 다양한 디바이스들, 예컨대, 스마트폰, 태블릿 컴퓨터, 차량 기반 디바이스 등 중 임의의 것일 수 있지만, 이들은 UE(105)가 이러한 구성들 중 임의의 것일 필요가 없으므로 예들일 뿐이며, UE들의 다른 구성들이 사용될 수 있다. 다른 UE들은 웨어러블 디바이스들(예컨대, 스마트 워치들, 스마트 보석류, 스마트 안경들 또는 헤드셋들 등)을 포함할 수 있다. 현재 존재하든 미래에 개발되든, 또 다른 UE들이 사용될 수 있다. 또한, 다른 무선 디바이스들(모바일이든 아니든)은 시스템(100) 내에서 구현될 수 있고, 서로 그리고/또는 UE(105), gNB들(110a, 110b), ng-eNB(114), 5GC(140) 및/또는 외부 클라이언트(130)와 통신할 수 있다. 예를 들어, 그러한 다른 디바이스들은 사물 인터넷(IoT) 디바이스들, 의료 디바이스들, 홈 엔터테인먼트 및/또는 자동화 디바이스들 등을 포함할 수 있다. 5GC(140)는 외부 클라이언트(130)(예컨대, 컴퓨터 시스템)와 통신하여, 예컨대, 외부 클라이언트(130)가 (예컨대 GMLC(125)를 통해) UE(105)에 관한 위치 정보를 요청 및/또는 수신하도록 허용할 수 있다.

[0023] UE(105) 또는 다른 디바이스들은 다양한 네트워크들에서 그리고/또는 다양한 목적들을 위해 그리고/또는 다양한 기술들(예컨대, 5G, Wi-Fi® 통신, Wi-Fi® 통신의 다중 주파수들, 위성 포지셔닝, 하나 이상의 타입들의 통신들(예컨대, GSM(Global System for Mobiles), 코드 분할 다중 액세스(CDMA), 롱 텀 에볼루션(LTE), 차량-대-사물(Vehicle-to-Everything, V2X, 예컨대, 차량-대-보행자(Vehicle-to-Pedestrian, V2P), 차량-대-인프라구조(Vehicle-to-Infrastructure, V2I), 차량-대-차량(Vehicle-to-Vehicle, V2V) 등), IEEE 802.11p 등)을 사용하여 통신하도록 구성될 수 있다. V2X 통신들은 셀룰러(셀룰러-V2X(Cellular-V2X, C-V2X)) 및/또는 WiFi®(예컨대, DSRC(Dedicated Short-Range Connection))일 수 있다. 시스템(100)은 다수의 캐리어들(상이한 주파수들의 파형 신호들) 상에서의 동작을 지원할 수 있다. 다중-캐리어 송신기들은 변조된 신호들을 다수의 캐리어들 상에서 동시에 송신할 수 있다. 각각의 변조된 신호는 코드 분할 다중 액세스(CDMA) 신호, 시간 분할 다중 액세스(TDMA) 신호, 직교 주파수 분할 다중 액세스(OFDMA) 신호, 단일-캐리어 주파수 분할 다중 액세스(Single-Carrier Frequency Division Multiple Access, SC-FDMA) 신호 등일 수 있다. 각각의 변조된 신호는 상이한 캐리어 상에서 전송될 수 있고, 파일럿, 오버헤드 정보, 데이터 등을 반송할 수 있다. UE들(105, 106)은 물리 사이드링크 동기화 채널(physical sidelink synchronization channel, PSSCH), 물리 사이드링크 브로드캐스트 채널(physical sidelink broadcast channel, PSBCH) 또는 물리 사이드링크 제어 채널(physical sidelink control channel, PSCCH)과 같은 하나 이상의 사이드링크 채널들을 통해 송신함으로써 UE-투-UE(UE-to-UE) 사이드링크(sidelink, SL) 통신들을 통해 서로 통신할 수 있다. 네트워크를 거치지 않는 직접 무선 디바이스-대-무선 디

바이스 통신들은 일반적으로, 통신들을 특정 프로토콜로 제한함이 없는 사이드링크 통신들로 지칭될 수 있다.

[0024] UE(105)는 디바이스, 모바일 디바이스, 무선 디바이스, 모바일 단말기, 단말기, 모바일 스테이션(mobile station, MS), SET(Secure User Plane Location(SUPL) Enabled Terminal)를 포함할 수 있고 그리고/또는 이들로 또는 일부 다른 명칭에 의해 지칭될 수 있다. 또한, UE(105)는 휴대폰, 스마트폰, 랩톱, 태블릿, PDA, 소비자 자산 추적 디바이스, 내비게이션 디바이스, 사물 인터넷(IoT) 디바이스, 헬스 모니터들, 보안 시스템들, 스마트 시티 센서들, 스마트 계측기들, 웨어러블 추적기들 또는 일부 다른 휴대용 또는 이동가능 디바이스에 대응할 수 있다. 통상적으로, 반드시 그런 것은 아니지만, UE(105)는 GSM(Global System for Mobile communication), 코드 분할 다중 액세스(CDMA), 광대역 CDMA(Wideband CDMA, WCDMA), LTE, HRPD(High Rate Packet Data), IEEE 802.11 WiFi®(WiFi®로도 지칭됨), Bluetooth®(BT), WiMax®(Worldwide Interoperability for Microwave Access), 5G 뉴 라디오(NR)(예컨대, NG-RAN(135) 및 5GC(140)를 사용함) 등과 같은 하나 이상의 라디오 액세스 기술(RAT)들을 사용하여 무선 통신을 지원할 수 있다. UE(105)는 예를 들어 디지털 가입자 회선(Digital Subscriber Line, DSL) 또는 패킷 케이블을 사용하여 다른 네트워크들(예컨대, 인터넷)에 연결할 수 있는 무선 로컬 영역 네트워크(Wireless Local Area Network, WLAN)를 사용하여 무선 통신을 지원할 수 있다. 이러한 RAT들 중 하나 이상의 사용은 UE(105)가 (예컨대, 도 1에 도시되지 않은 5GC(140)의 엘리먼트들을 통해, 또는 가능하게는 GMLC(125)를 통해) 외부 클라이언트(130)와 통신하도록 허용하고 그리고/또는 외부 클라이언트(130)가 (예컨대, GMLC(125)를 통해) UE(105)에 관한 위치 정보를 수신하도록 허용할 수 있다.

[0025] UE(105)는 단일 엔티티를 포함할 수 있거나 또는 사용자가 오디오, 비디오 및/또는 데이터 입력/출력(I/O) 디바이스들 및/또는 신체 센서들 및 별개의 와이어라인 또는 무선 모뎀을 채용할 수 있는 개인 영역 네트워크에서와 같은 다수의 엔티티들을 포함할 수 있다. UE(105)의 위치의 추정치는 위치, 위치 추정치, 위치 픽스(fix), 픽스, 포지션, 포지션 추정치 또는 포지션 픽스로 지칭될 수 있고, 지리적일 수 있으며, 따라서 고도 성분(예컨대, 해수면 위의 높이, 지면 위의 높이 또는 지면 아래의 깊이, 바닥 레벨, 또는 지하실 레벨)을 포함할 수 있거나 포함하지 않을 수 있는 UE(105)에 대한 위치 좌표들(예컨대, 위도 및 경도)을 제공할 수 있다. 대안적으로, UE(105)의 위치는 도시(civic) 위치로서(예컨대, 우편 주소 또는 특정 방 또는 층과 같은 건물 내의 일부 포인트 또는 작은 영역의 지정으로서) 표현될 수 있다. UE(105)의 위치는 UE(105)가 어떤 확률 또는 신뢰 레벨(예컨대, 67%, 95% 등)로 위치될 것으로 예상되는 영역 또는 볼륨(지리적으로 또는 도시 형태로 정의됨)으로서 표현될 수 있다. UE(105)의 위치는 예를 들어, 알려진 위치로부터의 거리 및 방향을 포함하는 상대 위치로서 표현될 수 있다. 상대 위치는 예컨대 지리적으로, 도시 용어들로, 또는 예컨대 맵, 평면도, 또는 건물 평면도에 표시된 포인트, 영역 또는 볼륨에 대한 참조에 의해 정의될 수 있는 알려진 위치에서의 일부 원점을 기준으로 정의된 상대 좌표들(예컨대, X, Y(및 Z) 좌표들)로서 표현될 수 있다. 본 명세서에 포함된 설명에서, 용어 위치의 사용은 달리 나타내지 않는 한 이러한 변형들 중 임의의 것을 포함할 수 있다. UE의 위치를 컴퓨팅할 때, 로컬 x, y 및 가능하게는 z 좌표들의 해를 찾고, 이어서, 원하는 경우, 로컬 좌표들을 절대 좌표들(예컨대, 위도, 경도 및 평균 해수면 위 또는 아래의 고도)로 컨버팅하는 것이 일반적이다.

[0026] UE(105)는 다양한 기술들 중 하나 이상을 사용하여 다른 엔티티들과 통신하도록 구성될 수 있다. UE(105)는 하나 이상의 디바이스-투-디바이스(device-to-device, D2D) P2P(peer-to-peer) 링크들을 통해 하나 이상의 통신 네트워크들에 간접적으로 연결하도록 구성될 수 있다. D2D P2P 링크들은 LTE 다이렉트(LTE Direct, LTE-D), WiFi® 다이렉트(WiFi®-D), Bluetooth® 등과 같은 임의의 적절한 D2D 라디오 액세스 기술(RAT)로 지원될 수 있다. D2D 통신들을 활용하는 UE들의 그룹 중 하나 이상은 ng-eNB(114), 및/또는 gNB들(110a, 110b) 중 하나 이상과 같은 송신/수신 포인트(TRP)의 지리적 커버리지 영역 내에 있을 수 있다. 그러한 그룹 내의 다른 UE들은 그러한 지리적 커버리지 영역들 밖에 있을 수 있거나, 또는 달리 기지국으로부터 송신들을 수신할 수 없을 수 있다. D2D 통신들을 통해 통신하는 UE들의 그룹들은, 각각의 UE가 그룹 내의 다른 UE들로 송신할 수 있는 일대다(1:M) 시스템을 활용할 수 있다. TRP는 D2D 통신들을 위한 리소스들의 스케줄링을 용이하게 할 수 있다. 다른 경우들에서, D2D 통신들은 TRP의 개입 없이 UE들 간에 수행될 수 있다. D2D 통신들을 활용하는 UE들의 그룹 중 하나 이상은 TRP의 지리적 커버리지 영역 내에 있을 수 있다. 그러한 그룹 내의 다른 UE들은 그러한 지리적 커버리지 영역들 밖에 있을 수 있거나, 또는 달리 기지국으로부터 송신들을 수신할 수 없을 수 있다. D2D 통신들을 통해 통신하는 UE들의 그룹들은, 각각의 UE가 그룹 내의 다른 UE들로 송신할 수 있는 일대다(1:M) 시스템을 활용할 수 있다. TRP는 D2D 통신들을 위한 리소스들의 스케줄링을 용이하게 할 수 있다. 다른 경우들에서, D2D 통신들은 TRP의 개입 없이 UE들 간에 수행될 수 있다.

[0027] 도 1에 도시된 NG-RAN(135) 내의 기지국(BS)들은 gNB들(110a, 110b)로 지칭되는 NR Node B들을 포함한다. NG-

RAN(135) 내의 gNB들(110a, 110b)의 쌍들은 하나 이상의 다른 gNB들을 통해 서로 연결될 수 있다. 5G 네트워크에 대한 액세스는 UE(105)와 gNB들(110a, 110b) 중 하나 이상의 gNB들 사이의 무선 통신을 통해 UE(105)에 제공되며, 이는 5G를 사용하여 UE(105)를 대신하여 5GC(140)에 대한 무선 통신 액세스를 제공할 수 있다. 도 1에서, UE(105)에 대한 서빙 gNB는 gNB(110a)인 것으로 가정되지만, 다른 gNB(예컨대, gNB(110b))가, UE(105)가 다른 위치로 이동하는 경우 서빙 gNB로서 작용할 수 있거나 또는 추가적인 처리량 및 대역폭을 UE(105)에 제공하기 위한 2차 gNB로서 작용할 수 있다.

[0028] 도 1에 도시된 NG-RAN(135) 내의 기지국(BS)들은 차세대 진화된 Node B로도 지칭되는 ng-eNB(114)를 포함할 수 있다. ng-eNB(114)는, 가능하게는 하나 이상의 다른 gNB들 및/또는 하나 이상의 다른 ng-eNB들을 통해 NG-RAN(135) 내의 gNB들(110a, 110b) 중 하나 이상에 연결될 수 있다. ng-eNB(114)는 LTE 무선 액세스 및/또는 진화된 LTE(evolved LTE, eLTE) 무선 액세스를 UE(105)에 제공할 수 있다. ng-eNB(114) 및/또는 gNB들(110a, 110b) 중 하나 이상은, UE(105)의 포지션을 결정하는 것을 보조하기 위해 신호들을 송신할 수 있지만 UE(105)로부터 또는 다른 UE들로부터 신호들을 수신하지 않을 수 있는 포지셔닝 전용 비콘들로서 기능하도록 구성될 수 있다.

[0029] gNB들(110a, 110b) 및/또는 ng-eNB(114)는 하나 이상의 TRP들을 각각 포함할 수 있다. 예를 들어, BS의 셀 내의 각각의 섹터는 TRP를 포함할 수 있지만, 다수의 TRP들이 하나 이상의 컴포넌트들을 공유할 수 있다(예컨대, 프로세서를 공유하지만 별개의 안테나들을 가짐). 시스템(100)은 매크로 TRP들만을 포함할 수 있거나, 또는 시스템(100)은 상이한 타입들의 TRP들, 예컨대, 매크로, 피코, 및/또는 펌토 TRP들 등을 가질 수 있다. 매크로 TRP는 비교적 큰 지리적 영역(예컨대, 반경이 수 킬로미터임)을 커버할 수 있고, 서비스 가입된 단말기들에 의한 제한없는 액세스를 허용할 수 있다. 피코 TRP는 비교적 작은 지리적 영역(예컨대, 피코 셀)을 커버할 수 있고, 서비스 가입된 단말기들에 의한 제한없는 액세스를 허용할 수 있다. 펌토 또는 홈 TRP는 비교적 작은 지리적 영역(예컨대, 펌토 셀)을 커버할 수 있고, 펌토 셀과의 연관성을 갖는 단말기들(예컨대, 홈 내의 사용자들을 위한 단말기들)에 의한 제한된 액세스를 허용할 수 있다.

[0030] ng-eNB(114) 및/또는 gNB들(110a, 110b) 각각은 라디오 유닛(radio unit, RU), 분산 유닛(distributed unit, DU), 및 중앙 유닛(central unit, CU)을 포함할 수 있다. 예를 들어, gNB(110b)는 RU(111), DU(112) 및 CU(113)를 포함한다. RU(111), DU(112) 및 CU(113)는 gNB(110b)의 기능을 분할한다. gNB(110b)는 단일 RU, 단일 DU 및 단일 CU로 도시되어 있지만, gNB는 하나 이상의 RU들, 하나 이상의 DU들 및/또는 하나 이상의 CU들을 포함할 수 있다. CU(113)와 DU(112) 사이의 인터페이스는 F1 인터페이스로 지칭된다. RU(111)는 디지털 프런트 엔드(digital front end, DFE) 기능들(예컨대, 아날로그-디지털(analog-to-digital) 컨버전, 필터링, 전력 증폭, 송신/수신) 및 디지털 빔포밍을 수행하도록 구성되고, 물리(PHY) 계층의 일부를 포함한다. RU(111)는 대용량 MIMO(multiple input/multiple output)를 사용하여 DFE를 수행할 수 있고, gNB(110b)의 하나 이상의 안테나들과 통합될 수 있다. DU(112)는 gNB(110b)의 라디오 링크 제어(Radio Link Control, RLC), 매체 액세스 제어(Medium Access Control, MAC) 및 물리 계층들을 호스팅한다. 하나의 DU는 하나 이상의 셀들을 지원할 수 있고, 각각의 셀은 단일 DU에 의해 지원된다. DU(112)의 동작은 CU(113)에 의해 제어된다. CU(113)는 사용자 데이터의 전송, 이동성 제어, 라디오 액세스 네트워크 공유, 포지셔닝, 세션 관리 등을 위한 기능들을 수행하도록 구성되지만, 일부 기능들은 DU(112)에만 할당된다. CU(113)는 gNB(110b)의 라디오 리소스 제어(Radio Resource Control, RRC), 서비스 데이터 적응 프로토콜(Service Data Adaptation Protocol, SDAP) 및 패킷 데이터 수렴 프로토콜(Packet Data Convergence Protocol, PDCP) 프로토콜들을 호스팅한다. UE(105)는 RRC, SDAP 및 PDCP 계층들을 통해 CU(113)와 통신하고, RLC, MAC 및 PHY 계층들을 통해 DU(112)와 통신하고, PHY 계층을 통해 RU(111)와 통신할 수 있다.

[0031] 언급된 바와 같이, 도 1은 5G 통신 프로토콜들에 따라 통신하도록 구성된 노드들을 도시하지만, 예를 들어, LTE 프로토콜 또는 IEEE 802.11x 프로토콜과 같은 다른 통신 프로토콜들에 따라 통신하도록 구성된 노드들이 사용될 수 있다. 예를 들어, UE(105)에 LTE 무선 액세스를 제공하는 진화된 패킷 시스템(Evolved Packet System, EPS)에서, RAN은 진화된 Node B(eNB)들을 포함하는 기지국들을 포함할 수 있는 진화된 범용 모바일 원격통신 시스템 지상 라디오 액세스 네트워크(Evolved Universal Mobile Telecommunications System(UMTS) Terrestrial Radio Access Network, E-UTRAN)를 포함할 수 있다. EPS에 대한 코어 네트워크는 EPC(Evolved Packet Core)를 포함할 수 있다. EPS는 E-UTRAN 플러스 EPC를 포함할 수 있으며, 도 1에서 E-UTRAN은 NG-RAN(135)에 대응하고 EPC는 5GC(140)에 대응한다.

[0032] gNB들(110a, 110b) 및 ng-eNB(114)는, 포지셔닝 기능을 위해 LMF(120)와 통신하는 AMF(115)와 통신할 수 있다. AMF(115)는 셀 변경 및 핸드오버를 포함하여 UE(105)의 이동성을 지원할 수 있고, UE(105)에 대한 시그널링 연

결 및 가능하게는 UE(105)에 대한 데이터 및 음성 베어러들을 지원하는 데 참여할 수 있다. LMF(120)는 예컨대, 무선 통신들을 통해 UE(105)와 직접 통신하거나, 또는 gNB들(110a, 110b) 및/또는 ng-eNB(114)와 직접 통신할 수 있다. LMF(120)는, UE(105)가 NG-RAN(135)에 액세스할 때 UE(105)의 포지셔닝을 지원할 수 있고, A-GNSS(Assisted GNSS), 관측된 도달 시간 차이(Observed Time Difference of Arrival, OTDOA)(예컨대, 다운링크(DL) OTDOA 또는 업링크(UL) OTDOA), 왕복 시간(Round Trip Time, RTT), 다중-셀 RTT, RTK(Real Time Kinematics), PPP(Precise Point Positioning), DGNSS(Differential GNSS), E-CID(Enhanced Cell ID), 도달 각도(angle of arrival, AoA), 출발 각도(angle of departure, AoD), 및/또는 다른 포지션 방법들과 같은 포지션 절차들/방법들을 지원할 수 있다. LMF(120)는 예컨대, AMF(115)로부터 또는 GMLC(125)로부터 수신된 UE(105)에 대한 위치 서비스 요청들을 프로세싱할 수 있다. LMF(120)는 AMF(115)에 그리고/또는 GMLC(125)에 연결될 수 있다. LMF(120)는 LM(Location Manager), LF(Location Function), CLMF(Commercial LMF), 또는 VLMF(Value Added LMF)와 같은 다른 명칭들로 지칭될 수 있다. LMF(120)를 구현하는 노드/시스템은 E-SMLC(Enhanced Serving Mobile Location Center) 또는 SLP(Secure User Plane Location(SUPL) Location Platform)와 같은 다른 타입들의 위치 지원 모듈들을 추가적으로 또는 대안적으로 구현할 수 있다. (UE(105)의 위치의 유도를 포함하는) 포지셔닝 기능의 적어도 일부가 (예컨대, 무선 노드들, 이를테면, gNB들(110a, 110b) 및/또는 ng-eNB(114)에 의해 송신된 신호들에 대해 UE(105)에 의해 획득된 신호 측정치들, 및/또는 예컨대, LMF(120)에 의해 UE(105)에 제공된 보조 데이터를 사용하여) UE(105)에서 수행될 수 있다. AMF(115)는 UE(105)와 5GC(140) 간의 시그널링을 프로세싱하는 제어 노드의 역할을 할 수 있고, QoS(Quality of Service) 흐름 및 세션 관리를 제공할 수 있다. AMF(115)는 셀 변경 및 핸드오버를 포함하여 UE(105)의 이동성을 지원할 수 있고, UE(105)에 대한 시그널링 연결을 지원하는 데 참여할 수 있다.

[0033] 서버(150), 예컨대, 클라우드 서버는 UE(105)의 위치 추정치들을 획득하여 외부 클라이언트(130)에 제공하도록 구성된다. 서버(150)는, 예를 들어, UE(105)의 위치 추정치를 획득하는 마이크로서비스/서비스를 실행하도록 구성될 수 있다. 예를 들어, 서버(150)는 UE(105), ng-eNB(114) 및/또는 (예컨대, RU(111), DU(112) 및 CU(113)를 통한) gNB들(110a, 110b) 중 하나 이상, 및/또는 LMF(120)로부터 (예컨대, 이들로 위치 요청을 전송함으로써) 위치 추정치를 가져올 수 있다. 다른 예로서, UE(105), (예컨대, RU(111), DU(112) 및 CU(113)를 통한) gNB들(110a, 110b) 중 하나 이상, 및/또는 LMF(120)는 UE(105)의 위치 추정치를 서버(150)에 푸시할 수 있다.

[0034] GMLC(125)는 서버(150)를 통해 외부 클라이언트(130)로부터 수신된 UE(105)에 대한 위치 요청을 지원할 수 있고, AMF(115)에 의해 LMF(120)로 포워딩하기 위해 그러한 위치 요청을 AMF(115)로 포워딩할 수 있거나, 또는 위치 요청을 LMF(120)로 직접 포워딩할 수 있다. LMF(120)로부터의 위치 응답(예컨대, UE(105)에 대한 위치 추정치를 포함함)은 직접 또는 AMF(115)를 통해 GMLC(125)에 반환될 수 있으며, 이어서 GMLC(125)는 위치 응답(예컨대, 위치 추정치를 포함함)을 서버(150)를 통해 외부 클라이언트(130)에 반환할 수 있다. GMLC(125)는 AMF(115) 및 LMF(120) 둘 모두에 연결된 것으로 도시되어 있지만, 일부 구현들에서는 AMF(115) 또는 LMF(120)에 연결되지 않을 수 있다.

[0035] 도 1에 추가로 예시된 바와 같이, LMF(120)는 3GPP 기술 규격(Technical Specification, TS) 38.455에 정의될 수 있는 뉴 라디오 포지션 프로토콜 A(이는 NPPa 또는 NRPPa로 지칭될 수 있음)를 사용하여 gNB들(110a, 110b) 및/또는 ng-eNB(114)와 통신할 수 있다. NRPPa는 3GPP TS 38.455에 정의된 LTE 포지셔닝 프로토콜 A(LPPa)와 동일하거나, 이와 유사하거나, 또는 이의 확장일 수 있으며, 이때 NRPPa 메시지들은 AMF(115)를 통해, gNB(110a)(또는 gNB(110b))와 LMF(120) 사이에서 그리고/또는 ng-eNB(114)와 LMF(120) 사이에서 전송된다. 도 1에 추가로 예시된 바와 같이, LMF(120)와 UE(105)는 3GPP TS 38.355에 정의될 수 있는 LTE 포지셔닝 프로토콜(LPP)을 사용하여 통신할 수 있다. LMF(120)와 UE(105)는 또한 또는 그 대신에, LPP와 동일하거나, 이와 유사하거나, 이의 확장일 수 있는 뉴 라디오 포지셔닝 프로토콜(이는 NPP 또는 NRPP로 지칭될 수 있음)을 사용하여 통신할 수 있다. 여기서, LPP 및/또는 NPP 메시지들은 AMF(115) 및 UE(105)에 대한 서빙 gNB(110a, 110b) 또는 서빙 ng-eNB(114)를 통해 UE(105)와 LMF(120) 사이에서 전송될 수 있다. 예를 들어, LPP 및/또는 NPP 메시지들은 5G 위치 서비스 애플리케이션 프로토콜(Location Services Application Protocol, LCS AP)을 사용하여 LMF(120)와 AMF(115) 사이에서 전송될 수 있고, 5G NAS(Non-Access Stratum) 프로토콜을 사용하여 AMF(115)와 UE(105) 사이에서 전송될 수 있다. LPP 및/또는 NPP 프로토콜은 A-GNSS, RTK, OTDOA 및/또는 E-CID와 같은 UE 보조 및/또는 UE 기반 포지션 방법들을 사용하여 UE(105)의 포지셔닝을 지원하기 위해 사용될 수 있다. NRPPa 프로토콜은 (예컨대, gNB(110a, 110b) 또는 ng-eNB(114)에 의해 획득된 측정치들과 함께 사용될 때) E-CID와 같은 네트워크 기반 포지션 방법들을 사용하여 UE(105)의 포지셔닝을 지원하기 위해 사용될 수 있고 그리고/또는 gNB들(110a, 110b) 및/또는 ng-eNB(114)로부터의 방향성 SS 또는 PRS 송신들을 정의하는 파라미터들과 같은,

gNB들(110a, 110b) 및/또는 ng-eNB들(114)로부터의 위치 관련 정보를 획득하기 위해 LMF(120)에 의해 사용될 수 있다. LMF(120)는 gNB 또는 TRP와 공동위치되거나 통합될 수 있거나, 또는 gNB 및/또는 TRP로부터 원격으로 배치되고 gNB 및/또는 TRP와 직접 또는 간접적으로 통신하도록 구성될 수 있다.

[0036] UE 보조 포지션 방법을 사용하여, UE(105)는 위치 측정치들을 획득하고 그 측정치들을 UE(105)에 대한 위치 추정치의 컴퓨테이션을 위해 위치 서버(예컨대, LMF(120))로 전송할 수 있다. 예를 들어, 위치 측정치들은 gNB들(110a, 110b), ng-eNB(114) 및/또는 WLAN AP에 대한 수신 신호 강도 표시(Received Signal Strength Indication, RSSI), 왕복 신호 전파 시간(Round Trip signal propagation Time, RTT), 기준 신호 시간 차이(Reference Signal Time Difference, RSTD), 기준 신호 수신 전력(Reference Signal Received Power, RSRP) 및/또는 기준 신호 수신 품질(Reference Signal Received Quality, RSRQ) 중 하나 이상을 포함할 수 있다. 위치 측정치들은 또한 또는 그 대신에 SV들(190 내지 193)에 대한 GNSS 의사범위(pseudorange), 코드 위상 및/또는 캐리어 위상의 측정치들을 포함할 수 있다.

[0037] UE 기반 포지션 방법을 사용하여, UE(105)는 위치 측정치들(예컨대, 이는 UE 보조 포지션 방법에 대한 위치 측정치들과 동일하거나 유사할 수 있음)을 획득할 수 있고, (예컨대, LMF(120)와 같은 위치 서버로부터 수신되거나 또는 gNB들(110a, 110b), ng-eNB(114), 또는 다른 기지국들 또는 AP들에 의해 브로드캐스팅된 보조 데이터의 도움으로) UE(105)의 위치를 컴퓨팅할 수 있다.

[0038] 네트워크 기반 포지션 방법을 사용하여, 하나 이상 기지국들(예컨대, gNB들(110a, 110b) 및/또는 ng-eNB(114)) 또는 AP들은 위치 측정치들(예컨대, UE(105)에 의해 송신된 신호들에 대한 RSSI, RTT, RSRP, RSRQ 또는 도달 시간(Time of Arrival, ToA)의 측정치들)을 획득할 수 있고 그리고/또는 UE(105)에 의해 획득된 측정치들을 수신할 수 있다. 하나 이상의 기지국들 또는 AP들은 그 측정치들을 UE(105)에 대한 위치 추정치의 컴퓨테이션을 위해 위치 서버(예컨대, LMF(120))로 전송할 수 있다.

[0039] NRPPa를 사용하여 gNB들(110a, 110b) 및/또는 ng-eNB(114)에 의해 LMF(120)에 제공된 정보는 위치 좌표들 및 방향성 SS 또는 PRS 송신들에 대한 타이밍 및 구성 정보를 포함할 수 있다. LMF(120)는 이 정보의 일부 또는 전부를 NG-RAN(135) 및 5GC(140)를 통해 LPP 및/또는 NPP 메시지에서 보조 데이터로서 UE(105)에 제공할 수 있다.

[0040] LMF(120)로부터 UE(105)로 전송된 LPP 또는 NPP 메시지는 원하는 기능에 따라 다양한 것들 중 임의의 것을 수행하도록 UE(105)에 명령할 수 있다. 예를 들어, LPP 또는 NPP 메시지는 UE(105)가 GNSS(또는 A-GNSS), WLAN, E-CID 및/또는 OTDOA(또는 일부 다른 포지션 방법)에 대한 측정치들을 획득하기 위한 명령을 포함할 수 있다. E-CID의 경우에, LPP 또는 NPP 메시지는 ng-eNB(114) 및/또는 gNB들(110a, 110b) 중 하나 이상에 의해 지원되는(또는 eNB 또는 WiFi® AP와 같은 일부 다른 타입의 기지국에 의해 지원되는) 특정 셀들 내에서 송신된 방향성 신호들의 하나 이상의 측정 수량들(예컨대, 빔 ID, 빔 폭, 평균 각도, RSRP, RSRQ 측정치들)을 획득하도록 UE(105)에 명령할 수 있다. UE(105)는 서빙 gNB(110a)(또는 서빙 ng-eNB(114)) 및 AMF(115)를 통해 (예컨대, 5G NAS 메시지 내부의) LPP 또는 NPP 메시지에서 측정 수량들을 다시 LMF(120)로 전송할 수 있다.

[0041] 언급된 바와 같이, 통신 시스템(100)은 5G 기술과 관련하여 설명되지만, 통신 시스템(100)은 (예컨대, 음성, 데이터, 포지셔닝 및 다른 기능들을 구현하기 위해) UE(105)와 같은 모바일 디바이스들을 지원하고 이들과 상호작용하기 위해 사용되는 GSM, WCDMA, LTE 등과 같은 다른 통신 기술들을 지원하도록 구현될 수 있다. 일부 그러한 실시 형태들에서, 5GC(140)는 상이한 에어(air) 인터페이스들을 제어하도록 구성될 수 있다. 예를 들어, 5GC(140)는 5GC(140) 내의 N3IWF(Non-3GPP InterWorking Function, 도 1에 도시되지 않음)를 사용하여 WLAN에 연결될 수 있다. 예를 들어, WLAN은 UE(105)에 대한 IEEE 802.11 WiFi® 액세스를 지원할 수 있고 하나 이상의 WiFi® AP들을 포함할 수 있다. 여기서, N3IWF는 WLAN에 그리고 AMF(115)와 같은 5GC(140) 내의 다른 엘리먼트들에 연결할 수 있다. 일부 실시 형태들에서, NG-RAN(135) 및 5GC(140) 둘 모두는 하나 이상의 다른 RAN들 및 하나 이상의 다른 코어 네트워크들에 의해 대체될 수 있다. 예를 들어, EPS에서, NG-RAN(135)은 eNB들을 포함하는 E-UTRAN에 의해 대체될 수 있고, 5GC(140)는 AMF(115) 대신 MME(Mobility Management Entity), LMF(120) 대신 E-SMLC, 및 GMLC(125)와 유사할 수 있는 GMLC를 포함하는 EPC에 의해 대체될 수 있다. 그러한 EPS에서, E-SMLC는 NRPPa 대신 LPPa를 사용하여 E-UTRAN 내의 eNB들로 그리고 이들로부터 위치 정보를 전송 및 수신할 수 있고, LPP를 사용하여 UE(105)의 포지셔닝을 지원할 수 있다. 이러한 다른 실시 형태들에서, 방향성 PRS들을 사용하는 UE(105)의 포지셔닝은, gNB들(110a, 110b), ng-eNB(114), AMF(115), 및 LMF(120)에 대해 본 명세서에 설명된 기능들 및 절차들이 일부 경우들에서, eNB들, WiFi® AP들, MME 및 E-SMLC와 같은 다른 네트워크 엘리먼트들에 대신 적용될 수 있다는 차이를 가지고, 5G 네트워크에 대해 본 명세서에 설명된 것과 유사한

방식으로 지원될 수 있다.

- [0042] 언급된 바와 같이, 일부 실시 형태들에서, 포지셔닝 기능은 포지션이 결정될 UE(예컨대, 도 1의 UE(105))의 범위 내에 있는 기지국들(이를테면, gNB들(110a, 110b) 및/또는 ng-eNB(114))에 의해 전송되는 방향성 SS 또는 PRS 빔들을 사용하여 적어도 부분적으로 구현될 수 있다. UE는, 일부 인스턴스들에서, UE의 포지션을 컴퓨팅하기 위해 복수의 기지국들(이를테면, gNB들(110a, 110b), ng-eNB(114) 등)로부터의 방향성 SS 또는 PRS 빔들을 사용할 수 있다.
- [0043] 또한 도 2를 참조하면, UE(200)는 UE들(105, 106) 중 하나의 일 예일 수 있고, 프로세서(210), 소프트웨어(SW)(212)를 포함하는 메모리(211), 하나 이상의 센서들(213), (무선 트랜시버(240) 및 유선 트랜시버(250)를 포함하는) 트랜시버(215)에 대한 트랜시버 인터페이스(214), 사용자 인터페이스(216), 위성 포지셔닝 시스템(SPS) 수신기(217), 카메라(218), 및 포지션 디바이스(position device, PD)(219)를 포함하는 컴퓨팅 플랫폼을 포함할 수 있다. 프로세서(210), 메모리(211), 센서(들)(213), 트랜시버 인터페이스(214), 사용자 인터페이스(216), SPS 수신기(217), 카메라(218), 및 포지션 디바이스(219)는 버스(220)(이는 예컨대, 광 및/또는 전기 통신을 위해 구성될 수 있음)에 의해 서로 통신가능하게 커플링될 수 있다. 도시된 장치 중 하나 이상(예컨대, 카메라(218), 포지션 디바이스(219), 및/또는 센서(들)(213) 중 하나 이상 등)은 UE(200)로부터 생략될 수 있다. 프로세서(210)는 하나 이상의 지능형 하드웨어 디바이스들, 예컨대, 중앙 프로세싱 유닛(central processing unit, CPU), 마이크로제어기, 주문형 집적 회로(ASIC) 등을 포함할 수 있다. 프로세서(210)는 범용/애플리케이션 프로세서(230), 디지털 신호 프로세서(Digital Signal Processor, DSP)(231), 모뎀 프로세서(232), 비디오 프로세서(233) 및/또는 센서 프로세서(234)를 포함하는 다수의 프로세서들을 포함할 수 있다. 프로세서들(230 내지 234) 중 하나 이상은 다수의 디바이스들(예컨대, 다수의 프로세서들)을 포함할 수 있다. 예를 들어, 센서 프로세서(234)는, 예컨대, 라디오 주파수(RF) 감지(이때 하나 이상의 (셀룰러) 무선 신호들이 송신되고 반사(들)가 객체를 식별, 맵핑, 및/또는 추적하기 위해 사용됨), 및/또는 초음파 등을 위한 프로세서들을 포함할 수 있다. 모뎀 프로세서(232)는 이중 SIM/이중 연결(또는 훨씬 더 많은 SIM들)을 지원할 수 있다. 예를 들어, SIM(Subscriber Identity Module 또는 Subscriber Identification Module)은 OEM(Original Equipment Manufacturer)에 의해 사용될 수 있고, 다른 SIM이 연결을 위해 UE(200)의 최종 사용자에게 의해 사용될 수 있다. 메모리(211)는 랜덤 액세스 메모리(random access memory, RAM), 플래시 메모리, 디스크 메모리, 및/또는 판독 전용 메모리(read-only memory, ROM) 등을 포함할 수 있는 비일시적 저장 매체일 수 있다. 메모리(211)는, 실행될 때, 프로세서(210)로 하여금, 본 명세서에 설명된 다양한 기능들을 수행하게 하도록 구성될 수 있는 명령들을 포함하는 프로세서 판독가능, 프로세서 실행가능 소프트웨어 코드일 수 있는 소프트웨어(212)를 저장할 수 있다. 대안적으로, 소프트웨어(212)는 프로세서(210)에 의해 직접 실행가능할 수 있는 것이 아니라, 예컨대, 컴파일링 및 실행될 때, 프로세서(210)로 하여금, 기능들을 수행하게 하도록 구성될 수 있다. 본 명세서에서의 설명은 프로세서(210)가 기능을 수행하는 것을 언급할 수 있지만, 이것은 프로세서(210)가 소프트웨어 및/또는 펌웨어를 실행하는 경우와 같은 다른 구현들을 포함한다. 본 명세서에서의 설명은, 프로세서들(230 내지 234) 중 하나 이상이 기능을 수행하는 것에 대한 약칭으로서, 프로세서(210)가 기능을 수행하는 것을 언급할 수 있다. 본 명세서에서의 설명은, UE(200)의 하나 이상의 적절한 컴포넌트들이 기능을 수행하는 것에 대한 약칭으로서, UE(200)가 기능을 수행하는 것을 언급할 수 있다. 프로세서(210)는 메모리(211)에 더하여 그리고/또는 그 대신에 명령들이 저장된 메모리를 포함할 수 있다. 프로세서(210)의 기능은 아래에서 더 완전히 논의된다.
- [0044] 도 2에 도시된 UE(200)의 구성은 청구항들을 포함하는 본 개시내용의 제한이 아닌 일 예이며, 다른 구성들이 사용될 수 있다. 예를 들어, UE의 예시적인 구성은 프로세서(210)의 프로세서들(230 내지 234) 중 하나 이상, 메모리(211), 및 무선 트랜시버(240)를 포함할 수 있다. 다른 예시적인 구성들은 프로세서(210)의 프로세서들(230 내지 234) 중 하나 이상, 메모리(211), 무선 트랜시버, 및 센서(들)(213), 사용자 인터페이스(216), SPS 수신기(217), 카메라(218), PD(219), 및/또는 유선 트랜시버 중 하나 이상을 포함할 수 있다.
- [0045] UE(200)는 트랜시버(215) 및/또는 SPS 수신기(217)에 의해 수신되고 다운컨버팅된 신호들의 기저대역 프로세싱을 수행가능할 수 있는 모뎀 프로세서(232)를 포함할 수 있다. 모뎀 프로세서(232)는 트랜시버(215)에 의한 송신을 위해 업컨버팅된 신호들의 기저대역 프로세싱을 수행할 수 있다. 또한 또는 대안적으로, 범용/애플리케이션 프로세서(230) 및/또는 DSP(231)에 의해 기저대역 프로세싱이 수행될 수 있다. 그러나, 다른 구성들이 기저대역 프로세싱을 수행하는 데 사용될 수 있다.
- [0046] UE(200)는, 예를 들어, 하나 이상의 관성 센서들, 하나 이상의 자력계들, 하나 이상의 환경 센서들, 하나 이상의 광 센서들, 하나 이상의 중량 센서들 및/또는 하나 이상의 라디오 주파수(RF) 센서들 등과 같은 다양한 타입

들의 센서들 중 하나 이상을 포함할 수 있는 센서(들)(213)를 포함할 수 있다. 관성 측정 유닛(inertial measurement unit, IMU)은, 예를 들어, 하나 이상의 가속도계들(예컨대, 3차원에서 UE(200)의 가속도에 집합적으로 응답함) 및/또는 하나 이상의 자이로스코프들(예컨대, 3차원 자이로스코프(들))을 포함할 수 있다. 센서(들)는, 다양한 목적들 중 임의의 목적을 위해, 예컨대, 하나 이상의 나침반 애플리케이션들을 지원하기 위해, 사용될 수 있는 (예컨대, 자북(magnetic north) 및/또는 진북(true north)에 대한) 배향을 결정하기 위한 하나 이상의 자력계들(예컨대, 3차원 자력계(들))을 포함할 수 있다. 환경 센서(들)는, 예를 들어, 하나 이상의 온도 센서들, 하나 이상의 기압 센서들, 하나 이상의 주변 광 센서들, 하나 이상의 카메라 이미지들, 및/또는 하나 이상의 마이크로폰들 등을 포함할 수 있다. 센서(들)(213)는 아날로그 및/또는 디지털 신호들을 생성할 수 있는데, 이들의 표시들이 예를 들어, 포지셔닝 및/또는 내비게이션 동작들과 관련된 애플리케이션들과 같은 하나 이상의 애플리케이션들의 지원으로 메모리(211)에 저장되고 DSP(231) 및/또는 범용/애플리케이션 프로세서(230)에 의해 프로세싱될 수 있다. 센서(들)(213)는 하나 이상의 광 센서들, 하나 이상의 중량 센서들, 및/또는 하나 이상의 라디오 주파수(RF) 센서들 등과 같은 다른 다양한 타입들의 센서들 중 하나 이상을 포함할 수 있다.

[0047] 센서(들)(213)는 상대 위치 측정들, 상대 위치 결정, 모션 결정 등에 사용될 수 있다. 센서(들)(213)에 의해 검출된 정보는 모션 검출, 상대 변위, 추측 항법(dead reckoning), 센서 기반 위치 결정, 및/또는 센서 보조 위치 결정을 위해 사용될 수 있다. 센서(들)(213)는 UE(200)가 고정되는지(고정식) 또는 이동식인지 그리고/또는 UE(200)의 이동성에 관한 특정 유용한 정보를 LMF(120)에 보고할지 여부를 결정하는 데 유용할 수 있다. 예를 들어, 센서(들)(213)에 의해 획득된/측정된 정보에 기초하여, UE(200)는, UE(200)가 이동했다는 것을 검출했다는 것 또는 UE(200)가 이동했다는 것을 LMF(120)에 통지/보고하고, (예컨대, 센서(들)(213)에 의해 인에이블된 센서 보조 위치 결정, 또는 센서 기반 위치 결정, 또는 추측 항법을 통해) 상대 변위/거리를 보고할 수 있다. 다른 예에서, 상대 포지셔닝 정보의 경우, 센서들/IMU는 UE(200) 등에 대한 다른 디바이스의 각도 및/또는 배향을 결정하는 데 사용될 수 있다.

[0048] IMU는 상대 위치 결정에 사용될 수 있는, UE(200)의 모션 방향 및/또는 모션 속도에 관한 측정치들을 제공하도록 구성될 수 있다. 예를 들어, IMU(270)의 하나 이상의 가속도계들(273) 및/또는 하나 이상의 자이로스코프들(274)은 각각 UE(200)의 선형 가속도 및 회전 속도를 검출할 수 있다. UE(200)의 선형 가속도 및 회전 속도 측정치들은 UE(200)의 변위뿐만 아니라 순간적인 모션 방향을 결정하기 위해 시간에 대해 적분될 수 있다. 순간적인 모션 방향과 변위가 적분되어 UE(200)의 위치를 추적할 수 있다. 예를 들어, UE(200)의 기준 위치는, 예컨대, 순간의 시간 동안 SPS 수신기(217)를 사용하여(그리고/또는 일부 다른 수단에 의해) 결정될 수 있고, 이 순간의 시간 이후 취해진 가속도계(들)(273) 및 자이로스코프(들)(274)로부터의 측정치들은 기준 위치에 대한 UE(200)의 이동(방향 및 거리)에 기초하여 UE(200)의 현재 위치를 결정하기 위해 추측 항법에서 사용될 수 있다.

[0049] 자력계(들)(271)는 UE(200)의 배향을 결정하기 위해 사용될 수 있는 상이한 방향들의 자기장 강도들을 결정할 수 있다. 예를 들어, 배향은 UE(200)에 대해 디지털 나침반을 제공하는 데 사용될 수 있다. 자력계(들)는 2개의 직교 차원들에서 자기장 강도의 표시들을 검출 및 제공하도록 구성된 2차원 자력계를 포함할 수 있다. 자력계(들)는 3개의 직교 차원들에서 자기장 강도의 표시들을 검출 및 제공하도록 구성된 3차원 자력계를 포함할 수 있다. 자력계(들)(271)는, 자기장을 감지하고 자기장의 표시들을, 예컨대, 프로세서(210)에 제공하기 위한 수단을 제공할 수 있다.

[0050] 트랜시버(215)는 각각 무선 연결들 및 유선 연결들을 통해 다른 디바이스들과 통신하도록 구성된 무선 트랜시버(240) 및 유선 트랜시버(250)를 포함할 수 있다. 예를 들어, 무선 트랜시버(240)는, 무선 신호들(248)을 (예컨대, 하나 이상의 업링크 채널들 및/또는 하나 이상의 사이드링크 채널들 상에서) 송신하고/하거나 (예컨대, 하나 이상의 다운링크 채널들 및/또는 하나 이상의 사이드링크 채널들 상에서) 수신하고 신호들을 무선 신호들(248)로부터 유선(예컨대, 전기 및/또는 광) 신호들로 그리고 유선(예컨대, 전기 및/또는 광) 신호들로부터 무선 신호들(248)로 변환하기 위해 안테나(246)에 커플링된 무선 송신기(242) 및 무선 수신기(244)를 포함할 수 있다. 무선 송신기(242)는 적절한 컴포넌트들(예컨대, 전력 증폭기 및 디지털-아날로그 컨버터)을 포함한다. 무선 수신기(244)는 적절한 컴포넌트들(예컨대, 하나 이상의 증폭기들, 하나 이상의 주파수 필터들 및 아날로그-디지털 컨버터)을 포함한다. 무선 송신기(242)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 송신기들을 포함할 수 있고, 그리고/또는 무선 수신기(244)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 수신기들을 포함할 수 있다. 무선 트랜시버(240)는 5G 뉴 라디오(NR), GSM, 범용 모바일 원격통신 시스템(1UMTS), 어드밴스드 모바일 전화 시스템(AMPS), 코드 분할 다중 액세스(CDMA), 광대역

CDMA(WCDMA), 롱 텀 에볼루션(LTE), LTE 다이렉트(LTE-D), 3GPP LTE-V2X(PC5), IEEE 802.11(IEEE 802.11p를 포함함), WiFi®, WiFi® 다이렉트(WiFi®-D), Bluetooth®, Zigbee® 등과 같은 다양한 라디오 액세스 기술(RAT)들에 따라 (예컨대, TRP들 및/또는 하나 이상의 다른 디바이스들과) 신호들을 통신하도록 구성될 수 있다. 뉴 라디오는 mm-과 주파수들 및/또는 서브-6 GHz 주파수들을 사용할 수 있다. 유선 트랜시버(250)는, 유선 통신을 위해 구성된 유선 송신기(252) 및 유선 수신기(254), 예컨대, NG-RAN(135)과 통신하여 NG-RAN(135)으로 통신들을 전송하고 이로부터 통신들을 수신하기 위해 활용될 수 있는 네트워크 인터페이스를 포함할 수 있다. 유선 송신기(252)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 송신기들을 포함할 수 있고, 그리고/또는 유선 수신기(254)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 수신기들을 포함할 수 있다. 유선 트랜시버(250)는 예컨대, 광 통신 및/또는 전기 통신을 위해 구성될 수 있다. 트랜시버(215)는 예컨대, 광 및/또는 전기 연결에 의해 트랜시버 인터페이스(214)에 통신가능하게 커플링될 수 있다. 트랜시버 인터페이스(214)는 트랜시버(215)와 적어도 부분적으로 통합될 수 있다. 무선 송신기(242), 무선 수신기(244) 및/또는 안테나(246)는 적절한 신호들을 각각 전송 및/또는 수신하기 위해 다수의 송신기들, 다수의 수신기들 및/또는 다수의 안테나들을 각각 포함할 수 있다.

[0051] 사용자 인터페이스(216)는 예를 들어 스피커, 마이크로폰, 디스플레이 디바이스, 진동 디바이스, 키보드, 터치 스크린 등과 같은 여러 디바이스들 중 하나 이상을 포함할 수 있다. 사용자 인터페이스(216)는 이들 디바이스들 중 임의의 것을 하나 초과 포함할 수 있다. 사용자 인터페이스(216)는 사용자가 UE(200)에 의해 호스팅되는 하나 이상의 애플리케이션들과 상호작용할 수 있게 하도록 구성될 수 있다. 예를 들어, 사용자 인터페이스(216)는 사용자로부터의 액션에 응답하여 DSP(231) 및/또는 범용/애플리케이션 프로세서(230)에 의해 프로세싱될 아날로그 및/또는 디지털 신호들의 표시들을 메모리(211)에 저장할 수 있다. 유사하게, UE(200) 상에 호스팅된 애플리케이션들은 출력 신호를 사용자에게 제시하기 위해 아날로그 및/또는 디지털 신호들의 표시들을 메모리(211)에 저장할 수 있다. 사용자 인터페이스(216)는 예를 들어, 스피커, 마이크로폰, 디지털-아날로그 회로부, 아날로그-디지털 회로부, 증폭기 및/또는 이득 제어 회로부(이들 디바이스들 중 임의의 것을 하나 초과 포함함)를 포함하는 오디오 입력/출력(I/O) 디바이스를 포함할 수 있다. 오디오 I/O 디바이스의 다른 구성들이 사용될 수 있다. 또한 또는 대안적으로, 사용자 인터페이스(216)는 예컨대, 사용자 인터페이스(216)의 키보드 및/또는 터치 스크린 상의 터치 및/또는 압력에 반응하는 하나 이상의 터치 센서들을 포함할 수 있다.

[0052] SPS 수신기(217)(예컨대, 글로벌 포지셔닝 시스템(GPS) 수신기)는 SPS 안테나(262)를 통해 SPS 신호들(260)을 수신 및 포착가능할 수 있다. SPS 안테나(262)는 SPS 신호들(260)을 무선 신호들로부터 유선 신호들, 예컨대, 전기 또는 광 신호들로 변환하도록 구성되고, 안테나(246)와 통합될 수 있다. SPS 수신기(217)는 UE(200)의 위치를 추정하기 위해, 포착된 SPS 신호들(260)을 전체적으로 또는 부분적으로 프로세싱하도록 구성될 수 있다. 예를 들어, SPS 수신기(217)는 SPS 신호들(260)을 사용한 삼변측량(trilateration)에 의해 UE(200)의 위치를 결정하도록 구성될 수 있다. 범용/애플리케이션 프로세서(230), 메모리(211), DSP(231) 및/또는 하나 이상의 특수 프로세서들(도시되지 않음)은 포착된 SPS 신호들을 전체적으로 또는 부분적으로 프로세싱하기 위해 그리고/또는 SPS 수신기(217)와 함께 UE(200)의 추정된 위치를 계산하기 위해 활용될 수 있다. 메모리(211)는 포지셔닝 동작들을 수행하는 데 사용하기 위한 SPS 신호들(260) 및/또는 다른 신호들(예컨대, 무선 트랜시버(240)로부터 포착된 신호들)의 표시들(예컨대, 측정치들)을 저장할 수 있다. 범용/애플리케이션 프로세서(230), DSP(231), 및/또는 하나 이상의 특수 프로세서들 및/또는 메모리(211)는 UE(200)의 위치를 추정하기 위해 측정치들을 프로세싱하는 데 사용하기 위한 위치 엔진을 제공 또는 지원할 수 있다.

[0053] UE(200)는 정지 또는 움직이는 이미저리를 캡처하기 위한 카메라(218)를 포함할 수 있다. 카메라(218)는 예를 들어, 이미징 센서(예컨대, 전하 결합 디바이스 또는 CMOS(Complementary Metal-Oxide Semiconductor) 이미저), 렌즈, 아날로그-디지털 회로부, 프레임 버퍼들 등을 포함할 수 있다. 캡처된 이미지들을 표현하는 신호들의 추가적인 프로세싱, 컨디셔닝, 인코딩 및/또는 압축은 범용/애플리케이션 프로세서(230) 및/또는 DSP(231)에 의해 수행될 수 있다. 또한 또는 대안적으로, 비디오 프로세서(233)는 캡처된 이미지들을 표현하는 신호들의 컨디셔닝, 인코딩, 압축 및/또는 조작을 수행할 수 있다. 비디오 프로세서(233)는 예컨대, 사용자 인터페이스(216)의 디스플레이 디바이스(도시되지 않음) 상의 제시를 위해 저장된 이미지 데이터를 디코딩/압축해제할 수 있다.

[0054] 포지션 디바이스(PD)(219)는 UE(200)의 포지션, UE(200)의 모션, 및/또는 UE(200)의 상대 포지션 및/또는 시간을 결정하도록 구성될 수 있다. 예를 들어, PD(219)는 SPS 수신기(217)와 통신하고, 그리고/또는 이의 일부 또는 전부를 포함할 수 있다. PD(219)는 하나 이상의 포지셔닝 방법들의 적어도 일부를 수행하기 위해 적절하게 프로세서(210) 및 메모리(211)와 함께 작동할 수 있지만, 본 명세서에서의 설명은 PD(219)가 포지셔닝 방법

(들)에 따라 수행하도록 구성되거나 수행하는 것을 언급할 수 있다. PD(219)는 또한 또는 대안적으로, 삼변측량을 위해, SPS 신호들(260)을 획득하고 사용하는 것을 보조하기 위해, 또는 둘 모두를 위해 지상 기반 신호들(예컨대, 무선 신호들(248)의 적어도 일부)을 사용하여 UE(200)의 위치를 결정하도록 구성될 수 있다. PD(219)는 서빙 기지국의 셀(예컨대, 셀 센터) 및/또는 E-CID와 같은 다른 기법에 기초하여 UE(200)의 위치를 결정하도록 구성될 수 있다. PD(219)는 카메라(218)로부터의 하나 이상의 이미지들 및 랜드마크들(예컨대, 자연 랜드마크들, 이를테면 산들 및/또는 인공 랜드마크들, 이를테면 건물들, 다리들, 거리들 등)의 알려진 위치들과 조합된 이미지 인식을 사용하여 UE(200)의 위치를 결정하도록 구성될 수 있다. PD(219)는 UE(200)의 위치를 결정하기 위한 하나 이상의 다른 기법들(예컨대, UE의 자체 보고된 위치(예컨대, UE의 포지션 비콘의 일부)에 의존함)을 사용하도록 구성될 수 있고, UE(200)의 위치를 결정하기 위해 기법들의 조합(예컨대, SPS 및 지상 포지셔닝 신호들)을 사용할 수 있다. PD(219)는, UE(200)의 배향 및/또는 모션을 감지하고 프로세서(210)(예컨대, 범용/애플리케이션 프로세서(230) 및/또는 DSP(231))가 UE(200)의 모션(예컨대, 속도 벡터 및/또는 가속도 벡터)을 결정하기 위해 사용하도록 구성될 수 있다는 그것의 표시들을 제공할 수 있는 센서들(213)(예컨대, 자이로스코프(들), 가속도계(들), 자력계(들) 등) 중 하나 이상을 포함할 수 있다. PD(219)는 결정된 포지션 및/또는 모션의 불확실성 및/또는 에러의 표시들을 제공하도록 구성될 수 있다. PD(219)의 기능은 예컨대, 범용/애플리케이션 프로세서(230), 트랜시버(215), SPS 수신기(217) 및/또는 UE(200)의 또 다른 컴포넌트에 의해 다양한 방식들 및/또는 구성들로 제공될 수 있으며, 하드웨어, 소프트웨어, 펌웨어 또는 이들의 다양한 조합들에 의해 제공될 수 있다.

[0055] 또한 도 3을 참조하면, gNB들(110a, 110b) 및/또는 ng-eNB(114)의 TRP(300)의 일 예는 프로세서(310), 소프트웨어(SW)(312)를 포함하는 메모리(311) 및 트랜시버(315)를 포함하는 컴퓨팅 플랫폼을 포함한다. 프로세서(310), 메모리(311) 및 트랜시버(315)는 버스(320)(이는 예컨대, 광 및/또는 전기 통신을 위해 구성될 수 있음)에 의해 서로 통신가능하게 커플링될 수 있다. 도시된 장치 중 하나 이상(예컨대, 무선 트랜시버)은 TRP(300)로부터 생략될 수 있다. 프로세서(310)는 하나 이상의 지능형 하드웨어 디바이스들, 예컨대, 중앙 프로세싱 유닛(CPU), 마이크로제어기, 주문형 집적 회로(ASIC) 등을 포함할 수 있다. 프로세서(310)는 (예컨대, 도 2에 도시된 바와 같은 범용/애플리케이션 프로세서, DSP, 모뎀 프로세서, 비디오 프로세서 및/또는 센서 프로세서를 포함하는) 다수의 프로세서들을 포함할 수 있다. 메모리(311)는 랜덤 액세스 메모리(RAM), 플래시 메모리, 디스크 메모리, 및/또는 판독 전용 메모리(ROM) 등을 포함할 수 있는 비일시적 저장 매체일 수 있다. 메모리(311)는, 실행될 때, 프로세서(310)로 하여금, 본 명세서에 설명된 다양한 기능들을 수행하게 하도록 구성되는 명령들을 포함하는 프로세서 판독가능, 프로세서 실행가능 소프트웨어 코드일 수 있는 소프트웨어(312)를 저장할 수 있다. 대안적으로, 소프트웨어(312)는 프로세서(310)에 의해 직접 실행가능할 수 있는 것이 아니라, 예컨대, 컴파일링 및 실행될 때, 프로세서(310)로 하여금, 기능들을 수행하게 하도록 구성될 수 있다.

[0056] 본 명세서에서의 설명은 프로세서(310)가 기능을 수행하는 것을 언급할 수 있지만, 이것은 프로세서(310)가 소프트웨어 및/또는 펌웨어를 실행하는 경우와 같은 다른 구현들을 포함한다. 본 명세서에서의 설명은, 프로세서(310)에 포함된 프로세서들 중 하나 이상이 기능을 수행하는 것에 대한 약칭으로서, 프로세서(310)가 기능을 수행하는 것을 언급할 수 있다. 본 명세서에서의 설명은 TRP(300)의 (그리고 따라서 ng-eNB(114) 및/또는 gNB들(110a, 110b) 중 하나의) 하나 이상의 적절한 컴포넌트들(예컨대, 프로세서(310) 및 메모리(311))이 기능을 수행하는 것에 대한 약칭으로서, TRP(300)가 기능을 수행하는 것을 언급할 수 있다. 프로세서(310)는 메모리(311)에 더하여 그리고/또는 그 대신에 명령들이 저장된 메모리를 포함할 수 있다. 프로세서(310)의 기능은 아래에서 더 완전히 논의된다.

[0057] 트랜시버(315)는 각각 무선 연결들 및 유선 연결들을 통해 다른 디바이스들과 통신하도록 구성된 무선 트랜시버(340) 및/또는 유선 트랜시버(350)를 포함할 수 있다. 예를 들어, 무선 트랜시버(340)는, 무선 신호들(348)을 (예컨대, 하나 이상의 업링크 채널들 및/또는 하나 이상의 다운링크 채널들 상에서) 송신하고/하거나 (예컨대, 하나 이상의 다운링크 채널들 및/또는 하나 이상의 업링크 채널들 상에서) 수신하고 신호들을 무선 신호들(348)로부터 유선(예컨대, 전기 및/또는 광) 신호들로 그리고 유선(예컨대, 전기 및/또는 광) 신호들로부터 무선 신호들(348)로 변환하기 위해 하나 이상의 안테나들(346)에 커플링된 무선 송신기(342) 및 무선 수신기(344)를 포함할 수 있다. 따라서, 무선 송신기(342)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 송신기들을 포함할 수 있고, 그리고/또는 무선 수신기(344)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 수신기들을 포함할 수 있다. 무선 트랜시버(340)는 5G 뉴 라디오(NR), GSM, 범용 모바일 원격통신 시스템(UMTS), 어드밴스드 모바일 전화 시스템(AMPS), 코드 분할 다중 액세스(CDMA), 광대역 CDMA(WCDMA), 롱 텀 에볼루션(LTE), LTE 다이렉트(LTE-D), 3GPP LTE-V2X(PC5), IEEE 802.11(IEEE 802.11p를 포함함), WiFi®, WiFi® 다이렉트(WiFi®-D), Bluetooth®, Zigbee® 등과 같은 다양한 라디오 액세스 기술

(RAT)들에 따라 (예컨대, UE(200), 하나 이상의 다른 UE들, 및/또는 하나 이상의 다른 디바이스들과) 신호들을 통신하도록 구성될 수 있다. 유선 트랜시버(350)는, 유선 통신을 위해 구성된 유선 송신기(352) 및 유선 수신기(354), 예컨대, NG-RAN(135)과 통신하여 예를 들어, LMF(120), 및/또는 하나 이상의 다른 네트워크 엔티티들로 통신들을 전송하고 이들로부터 통신들을 수신하기 위해 활용될 수 있는 네트워크 인터페이스를 포함할 수 있다. 유선 송신기(352)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 송신기들을 포함할 수 있고, 그리고/또는 유선 수신기(354)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 수신기들을 포함할 수 있다. 유선 트랜시버(350)는 예컨대, 광 통신 및/또는 전기 통신을 위해 구성될 수 있다.

[0058] 도 3에 도시된 TRP(300)의 구성은 청구항들을 포함하는 본 개시내용의 제한이 아닌 일 예이며, 다른 구성들이 사용될 수 있다. 예를 들어, 본 명세서에서의 설명은, TRP(300)가 여러 기능들을 수행하거나 수행하도록 구성될 수 있지만, 이러한 기능들 중 하나 이상은 LMF(120) 및/또는 UE(200)에 의해 수행될 수 있음(즉, LMF(120) 및/또는 UE(200)는 이러한 기능들 중 하나 이상을 수행하도록 구성될 수 있음)을 논의한다.

[0059] 또한 도 4를 참조하면, LMF(120)가 일 예일 수 있는 서버(400)는 프로세서(410), 소프트웨어(SW)(412)를 포함하는 메모리(411) 및 트랜시버(415)를 포함하는 컴퓨팅 플랫폼을 포함할 수 있다. 프로세서(410), 메모리(411) 및 트랜시버(415)는 버스(420)(이는 예컨대, 광 및/또는 전기 통신을 위해 구성될 수 있음)에 의해 서로 통신가능하게 커플링될 수 있다. 도시된 장치 중 하나 이상(예컨대, 무선 트랜시버)은 서버(400)로부터 생략될 수 있다. 프로세서(410)는 하나 이상의 지능형 하드웨어 디바이스들, 예컨대, 중앙 프로세싱 유닛(CPU), 마이크로제어기, 주문형 집적 회로(ASIC) 등을 포함할 수 있다. 프로세서(410)는 (예컨대, 도 2에 도시된 바와 같은 범용/애플리케이션 프로세서, DSP, 모뎀 프로세서, 비디오 프로세서 및/또는 센서 프로세서를 포함하는) 다수의 프로세서들을 포함할 수 있다. 메모리(411)는 랜덤 액세스 메모리(RAM), 플래시 메모리, 디스크 메모리, 및/또는 판독 전용 메모리(ROM) 등을 포함할 수 있는 비일시적 저장 매체일 수 있다. 메모리(411)는, 실행될 때, 프로세서(410)로 하여금, 본 명세서에 설명된 다양한 기능들을 수행하게 하도록 구성되는 명령들을 포함하는 프로세서 판독가능, 프로세서 실행가능 소프트웨어 코드일 수 있는 소프트웨어(412)를 저장할 수 있다. 대안적으로, 소프트웨어(412)는 프로세서(410)에 의해 직접 실행가능할 수 있는 것이 아니라, 예컨대, 컴파일링 및 실행될 때, 프로세서(410)로 하여금, 기능들을 수행하게 하도록 구성될 수 있다. 본 명세서에서의 설명은 프로세서(410)가 기능을 수행하는 것을 언급할 수 있지만, 이것은 프로세서(410)가 소프트웨어 및/또는 펌웨어를 실행하는 경우와 같은 다른 구현들을 포함한다. 본 명세서에서의 설명은, 프로세서(410)에 포함된 프로세서들 중 하나 이상이 기능을 수행하는 것에 대한 약칭으로서, 프로세서(410)가 기능을 수행하는 것을 언급할 수 있다. 본 명세서에서의 설명은, 서버(400)의 하나 이상의 적절한 컴포넌트들이 기능을 수행하는 것에 대한 약칭으로서, 서버(400)가 기능을 수행하는 것을 언급할 수 있다. 프로세서(410)는 메모리(411)에 더하여 그리고/또는 그 대신에 명령들이 저장된 메모리를 포함할 수 있다. 프로세서(410)의 기능은 아래에서 더 완전히 논의된다.

[0060] 트랜시버(415)는 각각 무선 연결들 및 유선 연결들을 통해 다른 디바이스들과 통신하도록 구성된 무선 트랜시버(440) 및/또는 유선 트랜시버(450)를 포함할 수 있다. 예를 들어, 무선 트랜시버(440)는, 무선 신호들(448)을 (예컨대, 하나 이상의 다운링크 채널들 상에서) 송신하고/하거나 (예컨대, 하나 이상의 업링크 채널들 상에서) 수신하고 신호들을 무선 신호들(448)로부터 유선(예컨대, 전기 및/또는 광) 신호들로 그리고 유선(예컨대, 전기 및/또는 광) 신호들로부터 무선 신호들(448)로 변환하기 위해 하나 이상의 안테나들(446)에 커플링된 무선 송신기(442) 및 무선 수신기(444)를 포함할 수 있다. 따라서, 무선 송신기(442)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 송신기들을 포함할 수 있고, 그리고/또는 무선 수신기(444)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 수신기들을 포함할 수 있다. 무선 트랜시버(440)는 5G 뉴 라디오(NR), GSM, 범용 모바일 원격통신 시스템(UMTS), 어드밴스드 모바일 전화 시스템(AMPS), 코드 분할 다중 액세스(CDMA), 광대역 CDMA(WCDMA), 롱 텀 에볼루션(LTE), LTE 다이렉트(LTE-D), 3GPP LTE-V2X(PC5), IEEE 802.11(IEEE 802.11p를 포함함), WiFi®, WiFi® 다이렉트(WiFi®-D), Bluetooth®, Zigbee® 등과 같은 다양한 라디오 액세스 기술(RAT)들에 따라 (예컨대, UE(200), 하나 이상의 다른 UE들, 및/또는 하나 이상의 다른 디바이스들과) 신호들을 통신하도록 구성될 수 있다. 유선 트랜시버(450)는, 유선 통신을 위해 구성된 유선 송신기(452) 및 유선 수신기(454), 예컨대, NG-RAN(135)과 통신하여 예를 들어, TRP(300), 및/또는 하나 이상의 다른 네트워크 엔티티들로 통신들을 전송하고 이들로부터 통신들을 수신하기 위해 활용될 수 있는 네트워크 인터페이스를 포함할 수 있다. 유선 송신기(452)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 송신기들을 포함할 수 있고, 그리고/또는 유선 수신기(454)는 별개의 컴포넌트들 또는 조합된/통합된 컴포넌트들일 수 있는 다수의 수신기들을 포함할 수 있다. 유선 트랜시버(450)는 예컨대, 광 통신 및/또는 전

기 통신을 위해 구성될 수 있다.

[0061] 본 명세서에서의 설명은 프로세서(410)가 기능을 수행하는 것을 언급할 수 있지만, 이것은 프로세서(410)가 소프트웨어(메모리(411)에 저장됨) 및/또는 펌웨어를 실행하는 경우와 같은 다른 구현들을 포함한다. 본 명세서에서의 설명은 서버(400)의 하나 이상의 적절한 컴포넌트들(예컨대, 프로세서(410) 및 메모리(411))이 기능을 수행하는 것에 대한 약칭으로서, 서버(400)가 기능을 수행하는 것을 언급할 수 있다.

[0062] 도 4에 도시된 서버(400)의 구성은 청구항들을 포함하는 본 개시내용의 제한이 아닌 일 예이며, 다른 구성들이 사용될 수 있다. 예를 들어, 무선 트랜시버(440)는 생략될 수 있다. 또한 또는 대안으로, 본 명세서에서의 설명은 서버(400)가 여러 기능들을 수행하거나 수행하도록 구성되지만, 이러한 기능들 중 하나 이상은 TRP(300) 및/또는 UE(200)에 의해 수행될 수 있음(즉, TRP(300) 및/또는 UE(200)는 이러한 기능들 중 하나 이상을 수행하도록 구성될 수 있음)을 논의한다.

[0063] 포지셔닝 기법들

[0064] 셀룰러 네트워크들에서 UE의 지상 포지셔닝을 위해, AFLT(Advanced Forward Link Trilateration) 및 관측된 도달 시간 차이(OTDOA)와 같은 기법들은 종종, 기지국에 의해 송신된 기준 신호들의 측정치들(예컨대, PRS, CRS 등)이 UE에 의해 취해지고 이어서 위치 서버에 제공되는 "UE 보조" 모드에서 동작한다. 위치 서버는 측정치들 및 기지국들의 알려진 위치들에 기초하여 UE의 포지션을 계산한다. 이러한 기법들은 UE 자체가 아닌, UE의 포지션을 계산하기 위해 위치 서버를 사용하기 때문에, 이러한 포지셔닝 기법들은, 대신에 통상적으로 위성 기반 포지셔닝에 의존하는, 자동차 또는 휴대폰 내비게이션과 같은 애플리케이션들에서 자주 사용되지 않는다.

[0065] UE는 PPP 또는 RTK 기술을 사용한 고정밀 포지셔닝을 위해 위성 포지셔닝 시스템(SPS)(글로벌 내비게이션 위성 시스템(GNSS))을 사용할 수 있다. 이러한 기술들은 지상-기반 스테이션(ground-based station)들로부터의 측정치들과 같은 보조 데이터를 사용한다. LTE 릴리스(Relase) 15는 데이터가 암호화되도록 허용하여 서비스에 가입된 UE들만이 정보를 판독할 수 있도록 한다. 그러한 보조 데이터는 시간에 따라 변한다. 따라서, 서비스에 가입된 UE는, 가입 비용을 지불하지 않은 다른 UE들에 데이터를 전달함으로써 쉽게 다른 UE들에 대한 "암호화를 해독할" 수 없을 수 있다. 그 전달은 보조 데이터가 변경될 때마다 반복될 필요가 있을 것이다.

[0066] UE 보조 포지셔닝에서, UE는 측정치들(예컨대, TDOA, 도달 각도(AoA) 등)을 포지셔닝 서버(예컨대, LMF/eSMLC)로 전송한다. 포지셔닝 서버는 셀당 하나의 레코드씩, 다수의 '엔트리들' 또는 '레코드들'을 포함하는 BSA(base station almanac)를 가지며, 여기서 각각의 레코드는 지리적 셀 위치를 포함하지만 다른 데이터를 또한 포함할 수 있다. BSA 내의 다수의 '레코드들' 중의 '레코드'의 식별자가 참조될 수 있다. BSA 및 UE로부터의 측정치들은 UE의 포지션을 컴퓨팅하는 데 사용될 수 있다.

[0067] 종래의 UE 기반 포지셔닝에서, UE는 그 자신의 포지션을 컴퓨팅하고, 따라서 네트워크(예컨대, 위치 서버)로 측정치들을 전송하는 것을 회피하는데, 이는 결국 레이턴시 및 확장성을 개선한다. UE는 네트워크로부터의 관련 BSA 레코드 정보(예컨대, gNB들(더 광범위하게는 기지국들)의 위치들)를 사용한다. BSA 정보는 암호화될 수 있다. 그러나, BSA 정보는 예를 들어, 이전에 설명된 PPP 또는 RTK 보조 데이터보다 훨씬 덜 자주 변하기 때문에, 복호화 키들에 가입하지 않고 그에 대한 비용을 지불하지 않았던 UE들에게 (PPP 또는 RTK 정보에 비해) BSA 정보를 이용가능하게 하는 것이 더 쉬울 수 있다. gNB들에 의한 기준 신호들의 송신들은 BSA 정보를 클라우드 소싱(crowd-sourcing) 또는 워 드라이빙(war-driving)에 잠재적으로 액세스할 수 있게 하여, 본질적으로 현장(in-the-field) 및/또는 오버더톱(over-the-top) 관측들에 기초하여 BSA 정보가 생성될 수 있게 한다.

[0068] 포지셔닝 기법들은 포지션 결정 정확도 및/또는 레이턴시와 같은 하나 이상의 기준들에 기초하여 특성화 및/또는 평가될 수 있다. 레이턴시는 포지션 관련 데이터의 결정을 트리거하는 이벤트와 포지셔닝 시스템 인터페이스, 예컨대 LMF(120)의 인터페이스에서의 그 데이터의 이용가능성 사이에 경과된 시간이다. 포지셔닝 시스템의 초기화에서, 포지션 관련 데이터의 이용가능성에 대한 레이턴시는 TTFF(time to first fix)로 불리며, TTFF 이후의 레이턴시들보다 더 크다. 2개의 연속적인 포지션 관련 데이터 이용가능성들 사이에 경과된 시간의 역(inverse)은 업데이트 레이트, 즉 제1 픽스 이후 포지션 관련 데이터가 생성되는 레이트로 불린다. 레이턴시는 예컨대, UE의 프로세싱 능력에 따라 달라질 수 있다. 예를 들어, UE는 272 PRB(Physical Resource Block) 할당을 가정하여 T 시간량(예컨대, T ms)마다 UE가 프로세싱할 수 있는 시간 단위(예컨대, 밀리초)의 DL PRS 심볼들의 지속시간으로서 UE의 프로세싱 능력을 보고할 수 있다. 레이턴시에 영향을 미칠 수 있는 능력들의 다른 예들은 UE가 PRS를 프로세싱할 수 있는 TRP들의 수, UE가 프로세싱할 수 있는 PRS의 수 및 UE의 대역폭이다.

[0069] 많은 상이한 포지셔닝 기법들(포지셔닝 방법들로도 불림) 중 하나 이상은 UE들(105, 106) 중 하나의 UE와 같은

엔티티의 포지션을 결정하는 데 사용될 수 있다. 예를 들어, 알려진 포지션 결정 기법들은 RTT, 다중-RTT, OTDOA(TDOA로도 불리며 UL-TDOA 및 DL-TDOA를 포함함), E-CID, DL-AoD, UL-AoA 등을 포함한다. RTT는 신호가 하나의 엔티티로부터 다른 엔티티로 이동하고 다시 돌아오는 데 걸리는 시간을 사용하여 2개의 엔티티들 사이의 범위를 결정한다. 그 범위와 더불어, 엔티티들 중 제1 엔티티의 알려진 위치 및 2개의 엔티티들 사이의 각도(예컨대, 방위각)가 엔티티들 중 제2 엔티티의 위치를 결정하는 데 사용될 수 있다. 다중-RTT(다중-셀 RTT로도 불림)에서는, 하나의 엔티티(예컨대, UE)로부터 다른 엔티티들(예컨대, TRP들)까지의 다수의 범위들 및 다른 엔티티들의 알려진 위치들이 하나의 엔티티의 위치를 결정하는 데 사용될 수 있다. TDOA 기법들에서, 하나의 엔티티와 다른 엔티티들 사이의 이동 시간들의 차이는 다른 엔티티들로부터의 상대 범위들을 결정하는 데 사용될 수 있으며, 다른 엔티티들의 알려진 위치들과 조합된 것들이 하나의 엔티티의 위치를 결정하는 데 사용될 수 있다. 도달 각도 및/또는 출발 각도는 엔티티의 위치를 결정하는 것을 돕는 데 사용될 수 있다. 예를 들어, (신호, 예컨대, 신호의 이동 시간, 신호의 수신 전력 등을 사용하여 결정된) 디바이스들 사이의 범위와 조합된 신호의 도달 각도 또는 출발 각도 및 디바이스들 중 하나의 디바이스의 알려진 위치가 다른 디바이스의 위치를 결정하는 데 사용될 수 있다. 도달 또는 출발 각도는 진북과 같은 기준 방향에 대한 방위각일 수 있다. 도달 또는 출발 각도는 엔티티로부터 바로 위쪽에 대한(즉, 지구 중심으로부터 반경 방향으로 바깥쪽에 대한) 천정각일 수 있다. E-CID는 서빙 셀의 아이덴티티, 타이밍 어드벤스(즉, UE에서의 수신 시간과 송신 시간 사이의 차이), 검출된 이웃 셀 신호들의 추정된 타이밍 및 전력, 그리고 가능하게는(예컨대, 기지국으로부터의 UE에서의 또는 그 반대의 신호의) 도달 각도를 사용하여 UE의 위치를 결정한다. TDOA에서, 소스들의 알려진 위치들 및 소스들로부터의 송신 시간들의 알려진 오프셋과 함께 상이한 소스들로부터의 신호들의 수신 디바이스에서의 도달 시간들의 차이는 수신 디바이스의 위치를 결정하는 데 사용된다.

[0070] 네트워크 중심 RTT 추정에서, 서빙 기지국은 2개 이상의 이웃 기지국들(및 통상적으로 서빙 기지국, 이는 적어도 3개의 기지국들이 필요하기 때문임)의 서빙 셀들 상에서 RTT 측정 신호들(예컨대, PRS)을 스캔/수신하도록 UE에 명령한다. 하나 이상의 기지국들은 네트워크(예컨대, LMF(120)와 같은 위치 서버)에 의해 할당된 낮은 채널 리소스들(예컨대, 시스템 정보를 송신하기 위해 기지국에 의해 사용되는 리소스들) 상에서 RTT 측정 신호들을 송신한다. UE는(예컨대, UE에 의해 그의 서빙 기지국으로부터 수신된 DL 신호로부터 유도된 바와 같은) UE의 현재 다운링크 타이밍에 대한 각각의 RTT 측정 신호의 도달 시간(수신 시간(receive time), 수신 시간(reception time), 수신 시간(time of reception) 또는 도달 시간(ToA)으로도 지칭됨)을 기록하고, 공통 또는 개별 RTT 응답 메시지(예컨대, 포지셔닝을 위한 사운딩 기준 신호(sounding reference signal, SRS), 즉 UL-PRS)를 하나 이상의 기지국들로(예컨대, 그의 서빙 기지국에 의해 명령될 때) 송신하고, 각각의 RTT 응답 메시지의 페이로드에 RTT 측정 신호의 ToA와 RTT 응답 메시지의 송신 시간 사이의 시간 차이 T_{Rx-Tx} (즉, UE T_{Rx-Tx} 또는 UE_{Rx-Tx})를 포함할 수 있다. RTT 응답 메시지는 기지국이 RTT 응답의 ToA를 추론할 수 있는 기준 신호를 포함할 것이다. 기지국으로부터의 RTT 측정 신호의 송신 시간과 기지국에서의 RTT 응답의 ToA 사이의 차이 T_{Tx-Rx} 를 UE-보고된 시간 차이 T_{Rx-Tx} 와 비교하고 UE_{Rx-Tx} 를 감산함으로써, 기지국은 기지국과 UE 사이의 전파 시간을 추론할 수 있으며, 이로부터 기지국은 이 전파 시간 동안의 광속을 가정하여 UE와 기지국 사이의 거리를 결정할 수 있다.

[0071] UE 중심 RTT 추정은, UE가 UE의 이웃에 있는 다수의 기지국들에 의해 수신되는 업링크 RTT 측정 신호(들)를(예컨대, 서빙 기지국에 의해 명령될 때) 송신하는 것을 제외하고는, 네트워크 기반 방법과 유사하다. 각각의 연루된 기지국은 다운링크 RTT 응답 메시지로 응답하며, 이는 RTT 응답 메시지 페이로드에 기지국에서의 RTT 측정 신호의 ToA와 기지국으로부터의 RTT 응답 메시지의 송신 시간 사이의 시간 차이를 포함할 수 있다.

[0072] 네트워크 중심 및 UE 중심 절차들 둘 모두에서, RTT 계산을 수행하는 측(네트워크 또는 UE)은 통상적으로(항상 그런 것은 아니지만) 제1 메시지(들) 또는 신호(들)(예컨대, RTT 측정 신호(들))를 송신하는 한편, 다른 측은 제1 메시지(들) 또는 신호(들)의 ToA와 RTT 응답 메시지(들) 또는 신호(들)의 송신 시간 사이의 차이를 포함할 수 있는 하나 이상의 RTT 응답 메시지(들) 또는 신호(들)로 응답한다.

[0073] 다중-RTT 기법은 포지션을 결정하는 데 사용될 수 있다. 예를 들어, 제1 엔티티(예컨대, UE)는(예컨대, 기지국으로부터 유니캐스팅, 멀티캐스팅, 또는 브로드캐스팅된) 하나 이상의 신호들을 전송할 수 있고, 다수의 제2 엔티티들(예컨대, 다른 TSP들, 이를테면 기지국(들) 및/또는 UE(들))은 제1 엔티티로부터 신호를 수신하고 이 수신된 신호에 응답할 수 있다. 제1 엔티티는 다수의 제2 엔티티들로부터 응답들을 수신한다. 제1 엔티티(또는 LMF와 같은 다른 엔티티)는 제2 엔티티들로부터의 응답들을 사용하여 제2 엔티티들에 대한 범위들을 결정할

수 있고, 제2 엔티티들의 다수의 범위들 및 알려진 위치들을 사용하여, 삼변측량에 의해 제1 엔티티의 위치를 결정할 수 있다.

[0074] 일부 경우들에서, 추가적인 정보는 직선 방향(예컨대, 이는 수평면에 또는 3차원에 있을 수 있음) 또는 가능하게는 (예컨대, 기지국의 위치들로부터 UE에 대한) 일정 범위의 방향들을 정의하는 도달 각도(AoA) 또는 출발 각도(AoD)의 형태로 획득될 수 있다. 2개의 방향들의 교차는 UE에 대한 위치의 다른 추정치를 제공할 수 있다.

[0075] 포지셔닝 기준 신호(PRS) 신호들(예컨대, TDOA 및 RTT)을 사용한 포지셔닝 기법들의 경우, 다수의 TRP들에 의해 전송된 PRS 신호들이 측정되고, 신호들의 도달 시간들, 알려진 송신 시간들 및 TRP들의 알려진 위치들이 UE로부터 TRP들까지의 범위들을 결정하는 데 사용된다. 예를 들어, 기준 신호 시간 차이(RSTD)가 다수의 TRP들로부터 수신된 PRS 신호들에 대해 결정되고, UE의 포지션(위치)을 결정하기 위해 TDOA 기법에서 사용될 수 있다. 포지셔닝 기준 신호는 PRS 또는 PRS 신호로 지칭될 수 있다. PRS 신호들은 통상적으로 동일한 전력을 사용하여 전송되고, 동일한 신호 특성들(예컨대, 동일한 주파수 시프트)을 갖는 PRS 신호들은 서로 간섭할 수 있어서, 더 먼 TRP로부터의 PRS 신호가 더 가까운 TRP로부터의 PRS 신호에 의해 압도될 수 있고, 그에 따라 더 먼 TRP로부터의 신호가 검출되지 않을 수 있다. PRS 뮤팅(muting)은 일부 PRS 신호들을 뮤팅하여(PRS 신호의 전력을 예컨대 제로로 감소시켜 PRS 신호를 송신하지 않음) 간섭을 감소시키는 것을 돕는 데 사용될 수 있다. 이러한 방식으로, (UE에서) 더 약한 PRS 신호는, 더 강한 PRS 신호가 더 약한 PRS 신호를 간섭하지 않으면서 UE에 의해 더 쉽게 검출될 수 있다. 용어 RS 및 이의 변형들(예컨대, PRS, SRS, CSI-RS(Channel State Information - Reference Signal))은 하나의 기준 신호 또는 하나 초과개의 기준 신호를 지칭할 수 있다.

[0076] 포지셔닝 기준 신호(PRS)들은 다운링크 PRS(DL PRS, 종종 단순히 PRS로 지칭됨)와 업링크 PRS(UL PRS)(이는 포지셔닝을 위한 사운드 기준 신호(SRS)로 불릴 수 있음)를 포함한다. PRS는 PN 코드(의사 난수 코드)를 포함하거나 또는 (예컨대, PN 코드로 캐리어 신호를 변조함으로써) PN 코드를 사용하여 생성될 수 있어서, PRS의 소스가 의사-위성(pseudo-satellite)(의사위성(pseudolite))의 역할을 할 수 있도록 할 수 있다. PN 코드는 (상이한 PRS 소스들로부터의 동일한 PRS가 중첩되지 않도록 적어도 특정된 영역 내에서) PRS 소스에 대해 고유할 수 있다. PRS는 주파수 계층의 PRS 리소스들 및/또는 PRS 리소스 세트들을 포함할 수 있다. DL PRS 포지셔닝 주파수 계층(또는 단순히 주파수 계층)은 상위 계층 파라미터들인 *DL-PRS-PositioningFrequencyLayer*, *DL-PRS-ResourceSet*, 및 *DL-PRS-Resource*에 의해 구성된 공통 파라미터들을 갖는 PRS 리소스(들)를 갖는, 하나 이상의 TRP들로부터의 DL PRS 리소스 세트들의 집합이다. 각각의 주파수 계층은 주파수 계층에서의 DL PRS 리소스들 및 DL PRS 리소스 세트들에 대한 DL PRS 서브캐리어 간격(subcarrier spacing, SCS)을 갖는다. 각각의 주파수 계층은 주파수 계층에서의 DL PRS 리소스들 및 DL PRS 리소스 세트들에 대한 DL PRS 사이클릭 프리픽스(cyclic prefix, CP)를 갖는다. 5G에서, 리소스 블록은 12개의 연속적인 서브캐리어들 및 특정된 수의 심볼들을 점유한다. 공통 리소스 블록들은 채널 대역폭을 점유하는 리소스 블록들의 세트이다. 대역폭 부분(bandwidth part, BWP)은 인접한 공통 리소스 블록들의 세트이고, 채널 대역폭 내의 모든 공통 리소스 블록들 또는 공통 리소스 블록들의 서브세트를 포함할 수 있다. 또한, DL PRS 포인트 A 파라미터는 기준 리소스 블록(및 리소스 블록의 최하위 서브캐리어)의 주파수를 정의하며, 이때 동일한 DL PRS 리소스 세트에 속하는 DL PRS 리소스들은 동일한 포인트 A를 갖고 동일한 주파수 계층에 속하는 모든 DL PRS 리소스 세트들은 동일한 포인트 A를 갖는다. 주파수 계층은 또한, 동일한 DL PRS 대역폭, 동일한 시작 PRB(및 중심 주파수) 및 동일한 값의 콤(comb) 크기(즉, 콤-N의 경우, 매 N번째 리소스 엘리먼트가 PRS 리소스 엘리먼트가 되도록 하는 심볼당 PRS 리소스 엘리먼트들의 주파수)를 갖는다. PRS 리소스 세트는 PRS 리소스 세트 ID에 의해 식별되고, 기지국의 안테나 패널에 의해 송신된 특정 TRP(셀 ID에 의해 식별됨)와 연관될 수 있다. PRS 리소스 세트의 PRS 리소스 ID는 전방향성 신호와, 그리고/또는 단일 기지국(여기서 기지국은 하나 이상의 빔들을 송신할 수 있음)으로부터 송신된 단일 빔(및/또는 빔 ID)과 연관될 수 있다. PRS 리소스 세트의 각각의 PRS 리소스는 상이한 빔 상에서 송신될 수 있고, 따라서 PRS 리소스(또는 단순히 리소스)는 빔으로도 지칭될 수 있다. 이는 PRS가 송신되는 기지국들 및 빔들이 UE에 알려져 있는지 여부에 어떠한 영향도 미치지 않는다.

[0077] TRP는 예컨대, 서버로부터 수신된 명령들에 의해 그리고/또는 TRP 내의 소프트웨어에 의해, 스케줄에 따라 DL PRS를 전송하도록 구성될 수 있다. 스케줄에 따르면, TRP는 DL PRS를 간헐적으로, 예컨대 초기 송신부터 일정한 간격을 두고 주기적으로 전송할 수 있다. TRP는 하나 이상의 PRS 리소스 세트들을 전송하도록 구성될 수 있다. 리소스 세트는 하나의 TRP에 걸친 PRS 리소스들의 집합이고, 이때 리소스들은 슬롯들에 걸쳐 동일한 주기성, 공통 뮤팅 패턴 구성(존재하는 경우) 및 동일한 반복 인자를 갖는다. PRS 리소스 세트들 각각은 다수의 PRS 리소스들을 포함하고, 이때 각각의 PRS 리소스는 슬롯 내의 N개의(하나 이상의) 연속적인 심볼(들) 내의 다수의 리소스 블록(Resource Block, RB)들에 있을 수 있는 다수의 OFDM(Orthogonal Frequency Division

Multiplexing) 리소스 엘리먼트(Resource Element, RE)들을 포함한다. PRS 리소스들(또는 일반적으로 기준 신호(RS) 리소스들)은 OFDM PRS 리소스들(또는 OFDM RS 리소스들)로 지칭될 수 있다. RB는 시간 도메인에서의 일정 수량의 하나 이상의 연속적인 심볼들 및 주파수 도메인에서의 일정 수량(5G RB의 경우 12개)의 연속적인 서브캐리어들에 걸쳐 있는 RE들의 집합이다. 각각의 PRS 리소스는 RE 오프셋, 슬롯 오프셋, 슬롯 내의 심볼 오프셋, 및 PRS 리소스가 슬롯 내에서 점유할 수 있는 연속적인 심볼들의 수로 구성된다. RE 오프셋은 주파수에서 DL PRS 리소스 내의 제1 심볼의 시작 RE 오프셋을 정의한다. DL PRS 리소스 내의 나머지 심볼들의 상대적인 RE 오프셋들은 초기 오프셋에 기초하여 정의된다. 슬롯 오프셋은 대응하는 리소스 세트 슬롯 오프셋에 대한 DL PRS 리소스의 시작 슬롯이다. 심볼 오프셋은 시작 슬롯 내의 DL PRS 리소스의 시작 심볼을 결정한다. 송신된 RE들은 슬롯들에 걸쳐 반복될 수 있으며, 이때 각각의 송신은 PRS 리소스에서 다수의 반복들이 존재할 수 있도록 하는 반복으로 불린다. DL PRS 리소스 세트 내의 DL PRS 리소스들은 동일한 TRP와 연관되고 각각의 DL PRS 리소스는 DL PRS 리소스 ID를 갖는다. DL PRS 리소스 세트 내의 DL PRS 리소스 ID는 단일 TRP로부터 송신된 단일 빔과 연관된다(단, TRP는 하나 이상의 빔들을 송신할 수 있음).

[0078] PRS 리소스는 의사 공동위치(quasi-co-location) 및 시작 PRB 파라미터들에 의해 정의될 수 있다. 의사 공동위치(QCL) 파라미터는 다른 기준 신호들과 함께 DL PRS 리소스의 임의의 의사 공동위치 정보를 정의할 수 있다. DL PRS는 서빙 셀 또는 비-서빙(non-serving) 셀로부터 DL PRS 또는 SS/PBCH(동기화 신호/물리 브로드캐스트 채널(Physical Broadcast Channel)) 블록을 갖는 QCL 타입 D로 구성될 수 있다. DL PRS는 서빙 셀 또는 비-서빙 셀로부터 SS/PBCH 블록을 갖는 QCL 타입 C로 구성될 수 있다. 시작 PRB 파라미터는 기준 포인트 A에 대한 DL PRS 리소스의 시작 PRB 인덱스를 정의한다. 시작 PRB 인덱스는 하나의 PRB의 입도(granularity)를 가지며, 0의 최소 값 및 2176개의 PRB들의 최대 값을 가질 수 있다.

[0079] PRS 리소스 세트는 슬롯들에 걸쳐 동일한 주기성, 동일한 뉀팅 패턴 구성(존재하는 경우) 및 동일한 반복 인자를 갖는 PRS 리소스들의 집합이다. PRS 리소스 세트의 모든 PRS 리소스들의 모든 반복들이 송신되도록 구성되는 모든 시간은 "인스턴스(instance)"로 지칭된다. 따라서, PRS 리소스 세트의 "인스턴스"는 각각의 PRS 리소스에 대한 특정된 수의 반복들 및 PRS 리소스 세트 내의 특정된 수의 PRS 리소스들이어서, 일단 특정된 수의 반복들이 특정된 수의 PRS 리소스들 각각에 대해 송신되면, 인스턴스가 완료되도록 한다. 인스턴스는 "오케이션"으로도 지칭될 수 있다. DL PRS 송신 스케줄을 포함하는 DL PRS 구성은 UE가 DL PRS를 측정하는 것을 용이하게(또는 심지어 가능하게) 하기 위해 UE에 제공될 수 있다.

[0080] PRS의 다수의 주파수 계층들은 개별적으로 계층들의 대역폭들 중 임의의 대역폭보다 더 큰 유효 대역폭을 제공하도록 어그리게이팅될 수 있다. 의사 공동위치되는(QCL되는) 것, 및 동일한 안테나 포트를 갖는 것과 같은 기준들을 충족하는 (연속적이고 그리고/또는 분리될 수 있는) 컴포넌트 캐리어들의 다수의 주파수 계층들이 (DL PRS 및 UL PRS에 대한) 더 큰 유효 PRS 대역폭을 제공하기 위해 스티칭되어, 증가된 도달 시간 측정 정확도를 초래할 수 있다. 스티칭은 스티칭된 PRS가 단일 측정으로부터 취해진 것으로 취급될 수 있도록 개별 대역폭 프래그먼트들에 대한 PRS 측정치들을 통합된 조각으로 조합하는 것을 포함한다. QCL되면, 상이한 주파수 계층들은 유사하게 거동하여, PRS의 스티칭이 더 큰 유효 대역폭을 산출할 수 있게 한다. 어그리게이팅된 PRS의 대역폭 또는 어그리게이팅된 PRS의 주파수 대역폭으로 지칭될 수 있는 더 큰 유효 대역폭은 (예컨대, TDOA의) 더 우수한 시간 도메인 분해능을 제공한다. 어그리게이팅된 PRS는 PRS 리소스들의 집합을 포함하고, 어그리게이팅된 PRS의 각각의 PRS 리소스는 PRS 컴포넌트로 불릴 수 있으며, 각각의 PRS 컴포넌트는 상이한 컴포넌트 캐리어들, 대역들, 또는 주파수 계층들 또는 동일한 대역의 상이한 부분들 상에서 송신될 수 있다.

[0081] RTT 포지셔닝은, RTT가 TRP들에 의해 UE들로 그리고 (RTT 포지셔닝에 참여하고 있는) UE들에 의해 TRP들로 전송된 포지셔닝 신호들을 사용한다는 점에서 능동 포지셔닝 기법이다. TRP들은 UE들에 의해 수신되는 DL-PRS 신호들을 전송할 수 있고, UE들은 다수의 TRP들에 의해 수신되는 사운딩 기준 신호(SRS) 신호들을 전송할 수 있다. 사운딩 기준 신호는 SRS 또는 SRS 신호로 지칭될 수 있다. 5G 다중-RTT에서, UE가 각각의 TRP에 대해 포지셔닝을 위한 별개의 UL-SRS를 전송하는 대신 다수의 TRP들에 의해 수신되는 포지셔닝을 위한 단일 UL-SRS를 전송하는, 조정된 포지셔닝이 사용될 수 있다. 다중-RTT에 참여하는 TRP는 통상적으로 그 TRP에 현재 캠프 온되는 UE들(서빙된 UE들, 이때 TRP는 서빙 TRP임), 그리고 또한 이웃 TRP들에 캠프 온되는 UE들(이웃 UE들)을 검색할 것이다. 이웃 TRP들은 단일 BTS(Base Transceiver Station)(예컨대, gNB)의 TRP들일 수 있거나, 또는 하나의 BTS의 TRP 및 별개의 BTS의 TRP일 수 있다. 다중-RTT 포지셔닝을 포함하는 RTT 포지셔닝의 경우, RTT를 결정하는 데 사용되는(그리고 따라서 UE와 TRP 사이의 범위를 결정하는 데 사용되는) 포지셔닝 신호 쌍을 위한 PRS/SRS에서의 포지셔닝 신호에 대한 DL-PRS 신호 및 UL-SRS는, UE 모션 및/또는 UE 클록 드리프트 및/또는 TRP 클록 드리프트로 인한 에러들이 허용가능한 한계들 내에 있도록 서로 시간적으로 가깝게 발생할 수 있다. 예를

들어, 포지셔닝 신호 쌍을 위한 PRS/SRS에서의 신호들은 서로 약 10 ms 이내에서 각각 TRP 및 UE로부터 송신될 수 있다. 포지셔닝을 위한 SRS가 UE들에 의해 전송되고, 포지셔닝을 위한 PRS 및 SRS가 서로 시간적으로 가깝게 전달되는 경우, 특히 많은 UE들이 동시에 포지셔닝을 시도하는 경우 라디오 주파수(RF) 신호 혼잡이 초래될 수 있고(이는 과도한 잡음 등을 야기할 수 있음) 그리고/또는 동시에 많은 UE들을 측정하려고 시도하고 있는 TRP들에서 컴퓨테이션 혼잡이 초래될 수 있다는 것이 확인되었다.

[0082] RTT 포지셔닝은 UE 기반 또는 UE 보조일 수 있다. UE 기반 RTT에서, UE(200)는 TRP들(300)에 대한 범위들 및 TRP들(300)의 알려진 위치들에 기초하여 TRP들(300) 각각에 대한 RTT 및 대응하는 범위 및 UE(200)의 포지션을 결정한다. UE 보조 RTT에서, UE(200)는 포지셔닝 신호들을 측정하고 측정 정보를 TRP(300)에 제공하고, TRP(300)는 RTT 및 범위를 결정한다. TRP(300)는 위치 서버, 예컨대, 서버(400)에 범위들을 제공하고, 서버는 예컨대, 상이한 TRP들(300)에 대한 범위들에 기초하여 UE(200)의 위치를 결정한다. RTT 및/또는 범위는 UE(200)로부터 신호(들)를 수신한 TRP(300)에 의해, 하나 이상의 다른 디바이스들, 예컨대 하나 이상의 다른 TRP들(300) 및/또는 서버(400)와 조합한 이 TRP(300)에 의해, 또는 UE(200)로부터 신호(들)를 수신한 TRP(300) 이외의 하나 이상의 디바이스들에 의해 결정될 수 있다.

[0083] 5G NR에서는 다양한 포지셔닝 기법들이 지원된다. 5G NR에서 지원되는 NR 네이티브(native) 포지셔닝 방법들은 DL 전용 포지셔닝 방법들, UL 전용 포지셔닝 방법들, 및 DL+UL 포지셔닝 방법들을 포함한다. 다운링크 기반 포지셔닝 방법들은 DL-TDOA 및 DL-AoD를 포함한다. 업링크 기반 포지셔닝 방법들은 UL-TDOA 및 UL-AoA를 포함한다. 조합된 DL+UL 기반 포지셔닝 방법들은 하나의 기지국을 이용한 RTT 및 다수의 기지국들을 이용한 RTT(다중-RTT)를 포함한다.

[0084] (예컨대, UE에 대한) 포지션 추정치는 위치 추정치, 위치, 포지션, 포지션 픽스, 픽스 등과 같은 다른 명칭들로 지칭될 수 있다. 포지션 추정치는 측지적(geodetic)이고 좌표들(예컨대, 위도, 경도 및 가능하게는 고도)을 포함할 수 있거나, 또는 도시적이고 거리 주소, 우편 주소 또는 위치의 일부 다른 구두 설명을 포함할 수 있다. 포지션 추정치는 추가로 일부 다른 알려진 위치에 대해 정의되거나 절대적인 용어들(예컨대, 위도, 경도 및 가능하게는 고도를 사용하여)로 정의될 수 있다. 포지션 추정치는 (예컨대, 위치가 일부 특정된 또는 디폴트 신뢰 레벨로 포함될 것으로 예상되는 영역 또는 볼륨을 포함함으로써) 예상된 에러 또는 불확실성을 포함할 수 있다. 포지션 정보는 (예컨대, 하나 이상의 위성 신호들의, PRS의, 그리고/또는 하나 이상의 다른 신호들의) 하나 이상의 포지셔닝 신호 측정치들, 및/또는 하나 이상의 포지셔닝 신호 측정치들에 기초한 하나 이상의 값들 (예컨대, 하나 이상의 범위들(가능하게는 하나 이상의 의사범위들을 포함함), 및/또는 하나 이상의 포지션 추정치들 등)을 포함할 수 있다.

[0085] 사이드링크 포지셔닝 보안

[0086] 또한 도 5를 참조하면, UE(500)는 버스(540)에 의해 서로 통신가능하게 커플링된 프로세서(510), 트랜시버(520) 및 메모리(530)를 포함한다. UE(500)는 도 5에 도시된 컴포넌트들을 포함할 수 있다. UE(500)는 UE(200)가 UE(500)의 일 예일 수 있도록 도 2에 도시된 것들 중 임의의 것과 같은 하나 이상의 다른 컴포넌트들을 포함할 수 있다. 예를 들어, 프로세서(510)는 프로세서(210)의 컴포넌트들 중 하나 이상을 포함할 수 있다. 트랜시버(520)는 트랜시버(215)의 컴포넌트들 중 하나 이상, 예컨대, 무선 송신기(242) 및 안테나(246), 또는 무선 수신기(244) 및 안테나(246), 또는 무선 송신기(242), 무선 수신기(244) 및 안테나(246)를 포함할 수 있다. 또한 또는 대안적으로, 트랜시버(520)는 유선 송신기(252) 및/또는 유선 수신기(254)를 포함할 수 있다. 메모리(530)는, 예컨대, 프로세서(510)로 하여금 기능들을 수행하게 하도록 구성된 프로세서 판독가능 명령들을 갖는 소프트웨어를 포함하여, 메모리(211)와 유사하게 구성될 수 있다.

[0087] 본 명세서에서의 설명은 프로세서(510)가 기능을 수행하는 것을 언급할 수 있지만, 이것은 프로세서(510)가 소프트웨어(메모리(530)에 저장됨) 및/또는 펌웨어를 실행하는 경우와 같은 다른 구현들을 포함한다. 본 명세서에서의 설명은 UE(500)의 하나 이상의 적절한 컴포넌트들(예컨대, 프로세서(510) 및 메모리(530))이 기능을 수행하는 것에 대한 약칭으로서, UE(500)가 기능을 수행하는 것을 언급할 수 있다. 프로세서(510)는 (가능하게는 메모리(530), 및 적절하게는 트랜시버(520)와 함께) SL 포지셔닝 유닛(550)을 포함한다. SL 포지셔닝 유닛(550)은 아래에서 추가로 논의되며, 설명은 일반적으로 프로세서(510), 또는 일반적으로 UE(500)가 SL 포지셔닝 유닛(550)의 기능들 중 임의의 것을 수행하는 것으로 언급할 수 있다. UE(500)는 본 명세서에 논의된 SL 포지셔닝 유닛(550)의 기능들을 수행하도록 구성된다.

[0088] 또한 도 6을 참조하면, 네트워크 엔티티(600)는 버스(640)에 의해 서로 통신가능하게 커플링된 프로세서(610), 트랜시버(620) 및 메모리(630)를 포함한다. 네트워크 엔티티(600)는 도 6에 도시된 컴포넌트들을 포함할 수 있

다. 네트워크 엔티티(600)는 TRP(300) 및/또는 서버(400)가 네트워크 엔티티(600)의 일 예일 수 있도록 도 3 및/또는 도 4에 도시된 것들 중 임의의 것과 같은 하나 이상의 다른 컴포넌트들을 포함할 수 있다. 예를 들어, 프로세서(610)는 프로세서(310) 및/또는 프로세서(410)의 컴포넌트들 중 하나 이상을 포함할 수 있다. 트랜시버(620)는 트랜시버(315) 및/또는 트랜시버(415)의 컴포넌트들 중 하나 이상을 포함할 수 있다. 메모리(630)는, 예컨대, 프로세서(610)로 하여금 기능들을 수행하게 하도록 구성된 프로세서 판독가능 명령들을 갖는 소프트웨어를 포함하여, 메모리(311) 및/또는 메모리(411)와 유사하게 구성될 수 있다.

[0089] 본 명세서에서의 설명은 프로세서(610)가 기능을 수행하는 것을 언급할 수 있지만, 이것은 프로세서(610)가 소프트웨어(메모리(630)에 저장됨) 및/또는 펌웨어를 실행하는 경우와 같은 다른 구현들을 포함한다. 본 명세서에서의 설명은 네트워크 엔티티(600)의 하나 이상의 적절한 컴포넌트들(예컨대, 프로세서(610) 및 메모리(630))이 기능을 수행하는 것에 대한 약칭으로서, 네트워크 엔티티(600)가 기능을 수행하는 것을 언급할 수 있다. 프로세서(610)는 (가능하게는 메모리(630), 및 적절하게는 트랜시버(620)와 함께) RKMF(Ranging Key Management Function)(650)를 포함한다. RKMF(650)는 아래에서 추가로 논의되며, 설명은 일반적으로 프로세서(610), 또는 일반적으로 네트워크 엔티티(600)가 RKMF(650)의 기능들 중 임의의 것을 수행하는 것으로 언급할 수 있다. 네트워크 엔티티(600)는 본 명세서에 논의된 RKMF(650)의 기능들을 수행하도록 구성된다.

[0090] 또한 도 7을 참조하면, SL 포지셔닝이 UE들 사이의 범위들 및/또는 UE들의 위치들을 결정하기 위해 환경(700)에서 수행될 수 있다. UE들의 범위들 및/또는 위치들은 충돌 회피, 내비게이션, 소비자 자산 추적, 긴급 도움 요청들을 위한 디바이스들의 선택 등과 같은 다양한 이유들 중 하나 이상을 위해 사용될 수 있다. 환경(700)은 UE들(711, 712, 713, 714) 및 기지국들(721, 722)을 포함한다. 이러한 예에서, UE들(711 내지 713)은 스마트폰들이고 UE(714)는 차량이지만, 이들은 본 개시내용의 제한이 아닌 예들이다. UE들(711 내지 714)은 하나 이상의 목적들, 예컨대, 포지셔닝, 통신 등을 위해 PC5 인터페이스를 통해 SL 신호들을 전송하도록 구성된다. V2X 및 UE-투-UE는 약간 상이한 프로토콜들을 사용하지만, 둘 모두는 UE들 사이의 인터페이스인 PC5 링크를 사용한다. UE들(711 내지 714) 및 기지국들(721, 722)은 Uu 인터페이스들을 통해 서로 통신하도록 구성된다.

[0091] 또한 도 8을 참조하면, SL 포지셔닝을 위한 프로세싱 및 신호 흐름(800)은 도시된 스테이지들을 포함하며, 그에 따라 UE들(711 내지 714) 중 임의의 것이 다른 UE들(711 내지 714) 중 하나 이상과의 SL 포지셔닝에 관여할 수 있다. UE, 예컨대, UE(711)는 UE들(712 내지 714) 중 하나와의 일대일 포지셔닝에 관여할 수 있거나 또는 예컨대, 모든 UE들(712 내지 714)과의 일대N 포지셔닝에 관여할 수 있고, 포지셔닝은 연루된 UE들 사이의 공지-기반 핸드셰이킹 또는 요청-응답 핸드셰이킹에 의해 조정될 수 있다. 도 8에 도시된 바와 같이, 개시자 UE(801)는 타겟 UE(802)와의 SL 포지셔닝에 관여하고, 이때 타겟 UE(802)는 (예컨대, UE(801)에 대한 그리고/또는 지구의 좌표계와 같은 기준 좌표계에 대한) 포지션이 결정될 UE이다. 포지셔닝 프로세스는 2개의 부분들, 즉 발견 부분(810) 및 포지셔닝 세션 부분(820)으로 분할된다.

[0092] 발견 부분(810)은 선택적이며, 포함된 경우, 공지 발견 또는 요청-응답 발견일 수 있다. 공지 발견에서, UE들(801, 802)에 의해 전송된 발견 메시지(discovery message)들(812)은 SL 포지셔닝을 지원하기 위한 각각의 UE의 능력을 브로드캐스팅하는 유사한 발견 메시지들이다. 요청-응답 발견에서, 개시자 UE(801) 및 타겟 UE(802)에 의해 전송된 발견 메시지들(812)은 상이하다. 개시자 UE(801)는 SL 포지셔닝 지원을 위한 PRS 요청을 송신(브로드캐스팅)하고, 타겟 UE(802)는 타겟 UE(802)가 SL 포지셔닝을 지원한다는 것을 표시하는 PRS 응답을 송신함으로써 PRS 요청을 수신하는 것에 응답한다. 발견 부분(810) 및 포지셔닝 세션 부분(820) 둘 모두에서의 신호 전송은, 기밀성 보호가 부재하는 경우 추적 또는 타겟화된 공격들의 대상이 되는 프라이버시-민감 정보(privacy-sensitive information), 및 무결성/재생(replay) 보호가 부재하는 경우 서비스 다운그레이드(service downgrade)들 또는 심지어 서비스 거부를 초래할 수 있는 변조-방지-요망 정보(tamper-resistant-desired information)를 포함한다. 시그널링이 보호되지 않으면, 공격자에 의해 프라이버시-민감 정보가 판독될 수 있고 변조-방지-요망 정보가 전송될 수 있어 서비스의 다운그레이드 또는 중단(거부)을 야기할 수 있다. 기밀성 보호(예컨대, 암호화)는 프라이버시-민감 정보를 보호할 수 있는 한편, 무결성 보호는 정보를 기밀로 유지하지 않으면서, 정보가 신뢰된 소스로부터의 또는 의도된(purported) 소스로부터의 것이거나 또는 변경되지 않았음을 보장하는 데 도움이 될 수 있다. 공지 발견 메시지들의 경우, 프라이버시-민감 정보는 예컨대, SL 포지셔닝을 위한 V2X 서비스 식별자 및 UE 소스 사용자 정보(예컨대, 개시자 ID)를 포함하고, 변조-방지-요망 정보는 예컨대, PRS 캐리어(예컨대, 면허, 비면허, ITS(지능형 교통 시스템)), 및 앵커 UE로서 서빙하기 위한 UE의 능력의 표시(타겟 UE의 포지션을 결정하는 것을 돕는 데 사용될 수 있는 알려진 위치를 가짐)를 포함한다. 요청-응답 발견을 위한 PRS 요청 메시지의 경우, 프라이버시-민감 정보는 예컨대, SL 포지셔닝을 위한 V2X 서비스 식별자 및 UE 소스 사용자 정보를 포함하고, 변조-방지-요망 정보는 예컨대, PRS 캐리어, 앵커 UE로서 서빙

하기 위한 UE의 능력의 표시, 및 PRS 포맷(예컨대, 콤 수(comb number), 심볼들의 수, TDM/FDM(Time Division Multiplexed/Frequency Division Multiplexed))을 포함한다. 요청-응답 발견을 위한 PRS 응답 메시지의 경우, 프라이버시-민감 정보는 예컨대, 레인징 세션 ID 및 타깃 애플리케이션-계층 ID를 포함하고, 변조-방지-요망 정보는 예컨대, PRS에 대한 지원된 캐리어 및 원하는 범위 또는 포지션을 포함한다.

[0093] 포지셔닝 세션 부분(820)은 그룹 형성 스테이지(825), PRS 이전 스테이지(830), PRS 응답 스테이지(840), PRS 스테이지(850), 및 PRS 이후 스테이지(860)를 포함한다. 그룹 형성 스테이지(825)에서, 발견된 UE들은 그룹을 형성하기로 결정하기 위해 서로 통신하며, 이는 그룹 내의 UE들 사이의 시그널링의 보호를 위한 보안 정보를 결정하기 위한 기초일 수 있다. PRS 이전 메시지(832)의 경우, 프라이버시-민감 정보는 예컨대, 개시자-할당 세션 ID, 개시자 ID, 및 타깃 UE ID(들)의 리스트를 포함하고, 변조-방지-요망 정보는 예컨대, PRS 캐리어, PRS 주기성, 주기적 PRS에 대한 시간 지속기간, 개시자 UE의 가장 이른 PRS Tx 시간, PRS 응답 요구 표시, 및 앵커 UE 능력 표시를 포함한다. PRS 응답 메시지(842)의 경우, 프라이버시-민감 정보는 예컨대, 레인징 세션 ID 및 타깃 애플리케이션-계층 ID를 포함하고, 변조-방지-요망 정보는 예컨대, PRS에 대한 지원된 캐리어 및 원하는 범위 또는 포지션을 포함한다. PRS(852)는 프라이버시-민감 정보 또는 변조-방지-요망 정보를 포함하지 않지만, 공격들, 예컨대, PRS의 스푸핑에 대해 경계하는 것을 돕도록 보호될 수 있다. PRS 이후 응답 메시지(862)의 경우, 프라이버시-민감 정보는 예컨대, 레인징 세션 ID 및 타깃 애플리케이션-계층 ID를 포함하고, 변조-방지-요망 정보는 예컨대, PRS Rx-Tx 차이들의 리스트(포지셔닝 세션에서 각각의 개시자 UE에 대해 하나씩), UE 기준 포지션, PRS Tx 시간에서 UE 기준 포지션으로부터의 안테나의 오프셋, PRS Tx 시간에서의 UE 속도 및 연관된 정확도, PRS Tx 시간에서의 UE 가속도 및 연관된 정확도, 및 수신된 PRS에 대한 도달 각도 및 연관된 정확도를 포함한다.

[0094] ProSe(proximity services) 디바이스들에 대한 흐름(800)에서 전송된 신호들은 다양한 위협들에 취약하다. ProSe 디바이스는 PC5 인터페이스 및 UE들 간의 시그널링을 지원하는 디바이스이다. 발견 메시지들은, 전송된 경우, 브로드캐스팅되고, PRS 이전 메시지(832), PRS 응답 메시지(842), PRS(852), 및 PRS 이후 메시지(862)는 브로드캐스팅(또는 그룹캐스팅) 또는 유니캐스팅될 수 있다. 그룹캐스트 시그널링은 예컨대, 신호(예컨대, 메시지, PRS 등) 소스로부터 관리되거나, 심지어 그 소스로부터의 거리에 기초할 수 있다. 발견 메시지들(812)은 아이덴티티 프라이버시, 서비스 식별/프라이버시, 및 가짜 서비스 공지/요청 공격들에 취약하다. PRS 이전 메시지들(832)은 아이덴티티 프라이버시, 파라미터 유출(타깃화됨/최적화됨), 및 파라미터 수정(DoS/서비스 저하) 공격들에 취약하다. 파라미터 유출 공격에서, 공격자는 파라미터(들)를 판독하고, 그 파라미터(들)를 사용하여, 예컨대, 상이한 파라미터 값들을 갖는 공격 메시지를 주입할 수 있다. 예를 들어, 공격자는 메시지를 스푸핑하고 상이한 파라미터 값들을 사용하도록 수신자에게 명령할 수 있거나 또는 다른 메시지를 변경(예컨대, 오버라이딩)할 수 있다. PRS 응답 메시지들(842)은 아이덴티티 프라이버시 공격들에 취약하다. PRS(852)는 PRS 주입 공격들에 취약하여, 예컨대, 범위(거리) 과대/과소 추정을 초래한다. PRS 이후 메시지들(862)은 위치 프라이버시 공격들, 및 위치 에러를 초래할 수 있는 측정 결과 수정 공격들(예컨대, 부정확한 범위의 주입)에 취약하다. 메시지 공격들에 대처하기 위해, 암호화, 무결성 보호, 및/또는 재생 보호가 브로드캐스트 및 유니캐스트 메시지들에 대해 사용될 수 있다. PRS 주입 공격들에 대처하기 위해, PRS 신호 랜덤화가 사용될 수 있다. 애플리케이션 및/또는 시나리오에 따라, 기밀성 및/또는 무결성 보호가 제공될 수 있다.

[0095] 레인징/포지셔닝 시그널링(메시지 전송 및/또는 비-메시지 신호 전송을 포함함)에 대한 보안 보호(예컨대, 기밀성 및/또는 무결성 보호)를 제공하기 위해, 보안 자료가 UE들에 프로비저닝될 수 있다. 보안 자료는 하나 이상의 암호 키들(예컨대, 하나 이상의 대칭 키들 및/또는 하나 이상의 비대칭 키들) 및/또는 하나 이상의 암호 인증서들을 포함할 수 있다. RKMF(650)는 레인징 서비스들을 위한 UE들에 보안 자료를 프로비저닝하도록 구성된다. RKMF(650)는 UE들이 포지셔닝을 위한 그룹을 형성하기 위해 서로를 발견하기 전에 UE들에 보안 자료를 사전-프로비저닝할 수 있거나, 또는 요구 시(on demand), 예컨대, 포지셔닝을 위한 그룹이 형성되는 것에 기초한 요청에 응답하여 보안 자료를 프로비저닝할 수 있다. 보안 자료는 예컨대, 브로드캐스트 보호와 멀티캐스트/그룹캐스트 보호 사이의 구별없이, 비-유니캐스트 메시지 보호, 즉, 브로드캐스트 메시지 보호 및/또는 멀티캐스트/그룹캐스트 메시지 보호를 위해 프로비저닝될 수 있다. 본 명세서에서의 논의는 브로드캐스트 보호를 언급할 수 있고, 그러한 논의는 멀티캐스트/그룹캐스트 보호에도 적용된다.

[0096] 브로드캐스트 메시지 보호를 위해, 현재 PRS 세션 내의 UE들(예컨대, UE들(801, 802))은 암호화 및 무결성 보호 키들을 공유한다. 예를 들어, RKMF(650)는 UE들(801, 802) 각각이 네트워크 엔티티(600)의 커버리지 내에 있을 때 UE들(801, 802)에 키들을 프로비저닝할 수 있으며, 이는 동시에 발생하지 않을 수 있다. 네트워크 엔티티(600)는 예를 들어, 5GC(140) 내의 서버 또는 인터넷 내의 애플리케이션 서버일 수 있다. 다른 예로서, 보호

키들은 그룹 형성 프로세스의 일부로서 확립될 수 있다. 이러한 경우에, RKMF(650)는 UE들(801, 802)이 보호 키들을 확립(예컨대, 유도)하기 위해 사용하는 인증서들을 UE들(801, 802)에 (그룹 형성 이전에 또는 그룹 형성과 동시에) 프로비저닝할 수 있으며, 이는 RKMF(650)에 의해 직접 보호 키들을 프로비저닝받는 것보다 더 많은 프로세싱 전력을 사용할 수 있다. 동일한 그룹 내의 UE들, 예컨대, UE들(801, 802)은 암호화 및 무결성 키들을 공유할 수 있다. 키들은 그룹 형성에 앞서 사전-프로비저닝될 수 있고, 키들의 손상 위험은 그룹 크기가 증가함에 따라 커진다. 그룹 형성은 발견 이후에 그리고 PRS 전송을 보호하기 위한 하나 이상의 키들의 확립 이전에 발생할 수 있다.

[0097] 브로드캐스트 PRS 보호의 경우, PRS 세션 내의 UE들은 PRS 시퀀스를 생성하기 위해 사용되는 암호 키를 공유할 수 있다. 동일한 그룹 내의 UE들은 PRS 시퀀스를 생성하기 위해 사용되는 키를 공유한다. 키 및/또는 선도 파라미터(freshness parameter)(예컨대, 타이머, 카운터, 시스템 프레임 수(system frame number), 슬롯 수(slot number), 심볼 수(symbol number), 또는 이들 중 2개 이상의 임의의 조합) 및/또는 기본 PRS는 랜덤화된 PRS의 시퀀스를 생성하기 위한 알고리즘에 대한 하나 이상의 입력들로서 사용될 수 있다. 이는 공격자(또는 기본 PRS 및 키에 대한 지식이 없는 임의의 엔티티)가, 그룹 내의 UE들 중 하나 이상이 범위, 및 따라서 타겟 UE의 위치를 결정하기 위해 사용하는 PRS를 주입하는 것을 억제할 수 있다. 암호 키는, 예컨대, RKMF(650)에 의한 그룹 형성에 앞서, RKMF(650)에 의한 요구 시, 브로드캐스트 메시지 보호를 위한 키들의 프로비저닝과 유사하게 프로비저닝되거나, 또는 그룹 형성에 앞서, 또는 이와 동시에 RKMF(650)에 의해 프로비저닝된 하나 이상의 인증서들에 기초하여 그룹 형성 동안 유도될 수 있다.

[0098] 유니캐스트 메시지 및/또는 비-메시지 신호 보호를 위해, UE들, 예컨대, UE들(801, 802)은 서로를 인증하고, UE들(801, 802)에만 알려진 대칭 암호 키를 확립할 수 있다. 대칭 키는 시그널링(예컨대, 메시지들 및/또는 PRS)의 기밀성 및 무결성 보호를 제공하기 위해 사용될 수 있는 한편, 비대칭 개인 키는 기밀성 보호 없이 무결성 보호를 제공하기 위해 사용될 수 있다. 비대칭 개인 키는 무결성 보호를 제공하기 위해 신호(예컨대, 메시지 또는 PRS)에 서명하는 데 사용될 수 있으며, 이때 수신 엔티티는 그 개인 키에 대응하는 공개 키를 사용하여, 수신된 메시지를 인증한다. 암호 키들은 그룹 형성 동안 또는 그룹 형성 이전에 RKMF(650)에 의해 프로비저닝될 수 있으며, 이때 UE들(801, 802)은, 반드시 동시에 일어나는 것은 아니지만, 네트워크 엔티티(600)에 연결된 동안 그 키들을 수신한다. RKMF(650)는 연루될 UE들(801, 802)에 대한 지식 없이 암호 키들을 사전-프로비저닝할 수 있다. 그러한 경우에, 다수의 대칭 키들이 UE들(801, 802)에 대해 프로비저닝될 수 있으며, 각각의 키는 특정 다른 UE에 대응하여, UE들(801, 802)이, UE들(801, 802)이 서로를 발견할 때 적절한 대칭 키를 가질 가능성이 높게 될 것이다. 그룹 형성 동안 요구 시 키들을 프로비저닝하는 것은 그룹을 위한 원하는 UE들이 알려져 있기 때문에 대량의 키들을 저장하는 것을 회피하는 데 도움이 될 수 있다. 확장성을 제공하기 위해 공개 키 기반 암호법(cryptography)이 사용될 수 있다. RKMF(650)는 그룹 형성에 앞서, UE들(801, 802)에 인증서들을 발행하거나, 또는 (신뢰된 인증 기관(certificate authority, CA)들의 리스트가 UE들(801, 802)에 제공된 상태에서) 신뢰된 서비스에 의해 발행된 인증서들을 보증할 수 있다. 인증서들은 (예컨대, 아래에서 추가로 논의된 바와 같이) 대칭 암호 키를 결정하기 위해 UE들(801, 802)에 의해 사용될 수 있다. 대칭 키가 확립되면, 3GPP 기술 규격 33.536에 의해 정의된 바와 같은 V2X를 위한 유니캐스트 링크 셋업 절차가 UE들(801, 802) 사이의 유니캐스트 링크를 확립하는 데 사용될 수 있다.

[0099] 네트워크 보조된/관리된 그룹 형성

[0100] 또한 도 9를 참조하면, 네트워크 보조된/관리된 그룹 형성 및 그룹 내의 브로드캐스트 또는 유니캐스트 SL 포지셔닝을 위한 프로세싱 및 신호 흐름(900)은 도시된 스테이지들을 포함한다. 네트워크 엔티티(600), 예컨대, RKMF(650)는, 개시자 UE(901) 및 타겟 UE(902)가 그룹을 형성하도록 보조하고, 발견 동안 그리고/또는 포지셔닝 세션 동안 시그널링을 기밀성 보호 및/또는 무결성 보호하기 위한 적절한 보안 자료를 가질 수 있다. 흐름(900)은 일 예이고, 다른 흐름들이 사용될 수 있다. 예를 들어, 스테이지(940)는, PRS 응답 메시지들, PRS, 및 PRS 이후 메시지들의 브로드캐스트/그룹캐스트 송신이 유니캐스트 송신 대신에 사용되는 경우 생략될 수 있다. 다른 예로서, 스테이지(950)는, 유니캐스트 포지셔닝 세션에 대한 레인징 키가 요구 시 요청되지 않는 경우 생략될 수 있다.

[0101] 스테이지(910)에서, UE들(901, 902)에는 적절한 보안 자료가 프로비저닝된다. UE들(901, 902)은 발견 메시지들을 위한 보안 자료를 요청하는 발견 요청들(911, 912)을 네트워크 엔티티(600)로 전송할 수 있다. 네트워크 엔티티(600), 예컨대, RKMF(650)는 발견 메시지들을 위한 보안 자료를 포함하는 발견 응답들(913, 914)을 전송함으로써 발견 요청들(911, 912)에 응답할 수 있다. 또한 또는 대안적으로, UE들(901, 902)은 (포지셔닝 메시지들 및 PRS를 포함하는) 포지셔닝 시그널링을 위한 보안 자료를 요청하는 레인징 보호 요청들(915, 916)을 네트

워크 엔티티(600)로 전송할 수 있다. 네트워크 엔티티(600), 예컨대, RKM(650)는 레인징 메시지들 및 PRS를 위한 보안 자료를 포함하는 레인징 보호 응답들(917, 918)을 전송함으로써 레인징 보호 요청들(915, 916)에 응답할 수 있다. 발견 및 레인징 둘 모두를 위해 동일한 보안 자료가 사용될 수 있거나, 또는 발견 및 레인징을 위해 별개의 보안 자료들이 제공될 수 있다. 일부 실시 형태들에서, 발견 보안 자료가 제공되는 한편 레인징 보안 자료는 제공되지 않는다. 일부 실시 형태들에서, 레인징 보안 자료가 제공되고 발견 보안 자료는 제공되지 않는다.

[0102] 보안 자료는 그룹 형성에 앞서 또는 요구 시 제공될 수 있다. 보안 자료는 UE들(901, 902)을 포함하는 그룹의 형성 이전에 제공될 수 있으며, 이때 보안 자료는 긴 유효성 시간(validity time)을 갖는다. 보안 자료는 예컨대, 하나 이상의 지리적 위치들 및/또는 구역들 및/또는 TAI(Tracking Area Identities)의 리스트에 의해 식별된 하나 이상의 표시된 영역들에 대해 유효할 수 있다. 보안 자료가 그룹 형성에 앞서 제공되는 경우, UE들(901, 902)은 그룹 형성 시에 그리고/또는 포지셔닝 세션 동안(포지셔닝 세션 부분(820) 참조) 네트워크 커버리지 밖에 있을 수 있다. 요구 시 보안 자료의 프로비저닝을 위해, UE(예컨대, UE(901) 및/또는 UE(902))는 포지셔닝 세션에 참여하기 위해 보안 자료를 요청한다. UE(또는 TRP 및/또는 AMF)는, 네트워크 엔티티(600)가 그룹을 형성하는 것을 돕기 위해 UE에 대한 대략적인 위치 정보(예컨대, 현재 TAC(Tracking Area Code), 현재 셀 ID)를 제공할 수 있다. 네트워크 엔티티(600), 예컨대, RKM(650)는 요구 시 보안 자료 프로비저닝을 위한 UE들(901, 902)에 대한 그룹 관리자로서 작용한다. 보안 자료는 특정 그룹을 위해 네트워크 엔티티(600)에 의해 제공될 수 있으며, 예컨대, 이때 상이한 그룹들은 상이한 보안 자료를 수신한다.

[0103] 보안 자료는 하나 이상의 암호 키들 및/또는 하나 이상의 디지털 인증서들(이들은 암호 인증서들 또는 인증서들로 불릴 수 있음)을 포함할 수 있다. 예를 들어, 네트워크 엔티티(600)는 UE들(901, 902) 둘 모두에 대해 동일한 대칭 암호 키(대칭 키로도 불림)를 프로비저닝할 수 있다. 다른 예로서, 보안 자료는 UE들(901, 902) 중 하나 이상에 대한 하나 이상의 암호 인증서들(또는 단순히 인증서들)을 포함할 수 있다. 각각의 디지털 인증서는 공개 키(이는 공개 암호 키 또는 공개 비대칭 암호 키로 불릴 수 있음)를 포함하며, 개인 키(이는 개인 암호 키 또는 개인 비대칭 암호 키로 불릴 수 있음)와 연관된다. 예를 들어, 각자의 UE는 공개/개인 키 쌍을 생성하고, 공개 키를 네트워크 엔티티(600)에 제공함으로써 인증서를 요청할 수 있다. 네트워크 엔티티(600)는 네트워크 엔티티(600)의 개인 키를 사용하여 인증서에 서명한다. 다른 예로서, 네트워크 엔티티(600)는 각자의 디지털 인증서(즉, 네트워크 엔티티에 의해 서명된 UE의 공개 키)를 UE들(901, 902) 각각에 프로비저닝할 수 있다. 네트워크 엔티티(600)는 UE에 대한 공개/개인 키 쌍을 생성하고, 인증서를 생성하기 위해 UE 공개 키에 서명하고, 개인 키 및 인증서를 UE에 제공할 수 있다. 이러한 경우에, 각각의 인증서는 네트워크 엔티티(600)의 개인 키를 사용하여 네트워크 엔티티(600)에 의해 서명된 각자의 UE의 공개 키이다. 다른 예로서, UE의 제조자는 공개/개인 키를 생성하거나 또는 달리 제공하고, 제조 동안 UE에 대한 키들을 프로비저닝할 수 있다.

[0104] 브로드캐스트/그룹캐스트 시그널링 보호

[0105] 브로드캐스트 메시지들에는, UE들(901, 902) 둘 모두가 동일한 대칭 키를 갖는 경우 기밀성 및/또는 무결성 보호가 제공될 수 있다. 기밀성 보호는 모바일-투-모바일 포지셔닝을 위한 시그널링을 보호하기 위해, 5G ProSe, 3GPP 기술 표준 33.503에 따라 네트워크 엔티티(600), 예컨대, RKM(650)에 의해 프로비저닝된 보안 자료에 의해 제공될 수 있다. 보안 자료는 그룹 내의 UE들, 예컨대, UE들(901, 902)에 대해 유효하다. 보안 자료는 DUSK(Discovery User Scrambling Key), DUCK(Discovery User Confidentiality Key), DUIK(Discovery User Integrity Key)를 포함할 수 있다. DUSK, DUCK, 및 DUIK는, 각각, 전체 메시지들을 암호화하고, 메시지의 하나 이상의 부분들을 암호화하고, 메시지의 무결성을 보호하는 데 사용될 수 있다. DUCK을 갖는 UE들만이 메시지의 DUCK-암호화된 부분(들)을 해독할 수 있다. DUIK는 전체 메시지의 무결성을 보호하는 데 사용될 수 있으며, 예컨대, 이때 송신 UE는 DUIK로 메시지에 서명하고 수신 UE는 DUIK를 사용하여 무결성을 확인한다. DUSK, DUCK, 및 DUIK는 그룹 형성 스테이지(925) 동안 형성된 그룹에 기초하여 스테이지(920)에서의 발견 메시지들(922) 및/또는 스테이지(930)에서의 PRS 이전 메시지들(932)을 보호하는 데 사용될 수 있다. 동일한 키가 발견 보호 및 PRS 이전 보호를 위해 사용될 수 있거나, 또는 키(예컨대, 그룹 키)가 구체적으로 PRS 이전 보호를 위한 것일 수 있으며, 이때 그러한 키는 DUSK, DUCK 또는 DUIK를 포함하지 않는다. 그룹 키(예컨대, 네트워크 엔티티(600)에 의해 UE들의 그룹에 대해 프로비저닝된 암호 키)는 그룹캐스트 보호를 위해 사용될 수 있다. 예를 들어, UE들(901, 902)은 AS-계층(Access Stratum layer) 그룹캐스트 보안을 위해, 예컨대, 공공 안전 사용 사례들을 위해 그룹 키를 사용할 수 있다. AS-계층은 에어 인터페이스를 통한 UE와 UE 사이 또는 UE와 gNB 사이의 프로토콜 계층이다. PRS 이전 보호를 위해 사용되는 브로드캐스트/그룹캐스트 키(들)는 또한, 유니캐스트 링크가 UE들(901, 902) 사이에서 확립되지 않거나 사용되지 않는 경우 스테이지(960)에서의 PRS 응답 메시지들

(962), 스테이지(970)에서 송신된 PRS(972), 및/또는 스테이지(980)에서 송신된 PRS 이후 메시지들(982)을 보호하는 데 사용될 수 있다.

[0106] 브로드캐스트 또는 그룹캐스트 PRS 송신을 위해, 프로비저닝된 키가 레인징 시그널링을 보호하기 위해 레인징 키로서 사용될 수 있다. 브로드캐스트/그룹캐스트 레인징을 위해, 레인징 키는 PRS를 랜덤화하는 데 사용될 수 있다. 예를 들어, 동일한 그룹 키가 발견 보호를 위해 그리고 PRS를 랜덤화하기 위해 사용될 수 있다. UE들(901, 902) 중 어느 하나의 SL 포지셔닝 유닛(550)은 그룹 키 및 하나 이상의 다른 항목들(예컨대, 시간(또는 프레임 수 및/또는 슬롯 수), 그룹/서비스 ID)을 포지셔닝 세션에 대한 PRS 시퀀스를 생성하기 위한 함수에 대한 입력들로서 사용할 수 있다. 시퀀스 내의 각각의 PRS는 상이할 것이고, 그룹 키, 함수, 및 함수에 대한 입력들의 이해를 갖는 각각의 UE에 알려질(이에 의해 생성될) 것이다. 레인징 키는, 예를 들어, 발견 응답들(913, 914) 또는 레인징 보호 응답들(917, 918)에서 제공될 수 있으며, 이때 PRS를 랜덤화하기 위한 기법이 UE들(901, 902)에 의해 알려진다. 다른 예로서, PRS를 랜덤화하기 위한 기법의 표시(및/또는 그 기법에서 어느 입력들이 사용될 것인지를 표시)는 발견 응답들(913, 914) 및/또는 레인징 보호 응답들(917, 918)에서 표시될 수 있다.

[0107] 유니캐스트 시그널링 보호

[0108] 유니캐스트 링크가 스테이지(940)에서 확립되고 레인징 암호 키, 예컨대, 대칭 키가 스테이지들(960, 970, 980)에서 모바일-투-모바일 포지셔닝을 위한 유니캐스트 시그널링을 보호하기 위해 확립되거나 또는 달리 획득될 수 있다. 레인징 암호 키는, 키가 UE들 사이의 PC5 인터페이스를 통한 시그널링을 보호하기 위해 사용되므로 PC5 레인징 키로 불릴 수 있다. 레인징 키는, 예를 들어, 요구 시 네트워크 엔티티(600)로부터 획득되거나, 또는 유니캐스트 링크의 확립에 앞서, 또는 UE들(901, 902)의 인증서들에 기초하여, 네트워크 엔티티(600)로부터 획득될 수 있다.

[0109] 요구 시 레인징 키의 획득을 위해, UE(902)는 스테이지(950)에서 네트워크 엔티티(600)와 통신하여, 네트워크 엔티티(600), 예컨대, RKMF(650)로부터 레인징 키를 요청 및 수신한다. 예를 들어, 스테이지(940) 동안, UE(902)는 UE(901)와의 유니캐스트 포지셔닝 세션을 갖도록 UE(901)로 요청을 전송한다. UE(901)는 UE(902)가 UE(901)와의 유니캐스트 포지셔닝 세션을 위해 네트워크 엔티티(600)로부터 레인징 키를 요청하도록 하는 명령을 UE(902)로 전송함으로써 응답한다. 스테이지(950)에서, UE(902)가, 네트워크 엔티티(600)가 속하는 네트워크의 커버리지 내에 있는 상태에서, UE(902)의 SL 포지셔닝 유닛(550)은 UE(902)와 UE(901) 사이의 유니캐스트 레인징을 위한 레인징 키에 대한 요청을 네트워크 엔티티(600)로 송신한다. 네트워크 엔티티(600)는 레인징 키, 예컨대, RRUK(Ranging Remote User Key)를 제공함으로써 응답한다. 레인징 키는, 예컨대, 현재 시간 동안 UE들(901, 902)에 대해, 세션-특정적인 쌍별(pairwise) 대칭 키이다. RKMF(650)는 UE(901)에 프로비저닝된 암호 키를 알고, UE(901)에 프로비저닝된 키로부터 레인징 키를 유도하며, 레인징 키를 UE(902)에 제공한다. UE(901)의 SL 포지셔닝 유닛(550)은 (UE(901)가 네트워크 엔티티(600)를 포함하는 네트워크의 커버리지 내에 있었던 동안) RKMF(650)에 의해 이전에 프로비저닝된 암호 키로부터 레인징 키를 유도한다. UE들(901, 902)은, UE들(901, 902) 둘 모두가 레인징 키를 획득했음(예컨대, 이를 UE(901)가 유도했고 UE(902)가 수신했음)을 확인하기 위해 서로에게 비밀 모드 커맨드 메시지들을 송신한다.

[0110] 레인징 키는 스테이지(940)에 앞서 UE들(901, 902)에 제공되어, 사전-프로비저닝될 수 있다. 네트워크 엔티티(600) 또는 다른 엔티티는 각자의 UE들과의 포지셔닝 세션에 사용하기 위한 다수의 레인징 키들을 UE들(901, 902)에 각각 프로비저닝할 수 있다. 스테이지(940)에 응답하여, UE(901)는 UE(902)와의 포지셔닝 세션에 전용되는 레인징 키를 메모리로부터 추출할 수 있고, UE(902)는 UE(901)와의 포지셔닝 세션에 전용되는 레인징 키를 메모리로부터 추출할 수 있다.

[0111] 레인징 키는 UE들(901, 902)의 인증서들에 기초하여 UE들(901, 902)에 의해 획득될 수 있다. UE들(901, 902) 각각은, 네트워크 엔티티(600)를 포함하는 네트워크의 커버리지 내에 있을 때, 네트워크 엔티티(600)로부터 인증서를 수신할 수 있다. UE들(901, 902)은, 동시에, 또는 포지셔닝 세션이 확립되고 있을 때 커버리지 내에 있지 않을 수 있다. UE들(901, 902) 각각은 각자의 UE(901, 902)의 공개 키를 네트워크 엔티티(600)로 전송한다. 네트워크 엔티티(600)는 인증서를 형성하기 위해 네트워크 엔티티(600)의 개인 키를 사용하여 UE 공개 키에 서명하고 인증서를 각자의 UE(901, 902)로 전송한다. 따라서, 인증서들 각각은 네트워크 엔티티(600)의 개인 비 대칭 키에 의해 서명된 각자의 UE(901, 902)의 공개 키를 포함한다. 인증서들은 예컨대, 특정 지리적 구역 및/또는 특정된 시간 윈도우로 제한되어, 사용에 대한 하나 이상의 제한들을 가질 수 있다. UE들(901, 902)은 그들 각자의 인증서들을 교환한다. UE(901)는 네트워크 엔티티(600)의 공개 키를 사용하여, 수신된 인증서 내의

UE(902)의 공개 키가 진짜임을 검증하고, UE(902)는 UE(901)의 공개 키에 대해 동일한 것을 행한다. UE들(901, 902)의 SL 포지셔닝 유닛들(550)은 검증된 공개 키들을 사용하여 (예컨대, EAP-TLS(Extensible Authentication Protocol - Transport Layer Security)에 따라) 대칭 키를 유도한다. UE들(901, 902)은 이러한 대칭 키를 사용하여, 포지셔닝 세션에, 예컨대, PRS 응답 메시지(962), PRS(972), 및 PRS 이후 메시지(982)에 기밀성 및/또는 무결성 보호를 제공할 수 있다. PRS 이전 메시지(932)가 UE(901)로부터 UE(902)로 가는 것으로 도시되고, PRS 응답 메시지(962)가 UE(902)로부터 UE(901)로 가는 것으로 도시되지만, PRS 이전 메시지는 UE(902)로부터 UE(901)로 전송될 수 있고, PRS 응답 메시지는 UE(901)로부터 UE(902)로 전송될 수 있다. 이러한 방식으로 대칭 키를 유도하는 것은 포지셔닝 세션들에 대한 대칭 키들을 결정하기 위한 확장가능한 기법을 제공한다.

[0112] UE 기반 자율 그룹 형성

[0113] 또한 도 10을 참조하면, 개시자 UE(1001) 및 타겟 UE(1002)에 대한 UE 기반 그룹 형성, 및 그룹 내의 브로드캐스트 또는 유니캐스트 SL 포지셔닝을 위한 프로세싱 및 신호 흐름(1000)은 도시된 스테이지들을 포함한다. 흐름(1000)은 일 예이며, 다른 흐름들이 사용될 수 있다. 예를 들어, 스테이지(1040)는, PRS 응답 메시지들, PRS, 및 PRS 이후 메시지들의 브로드캐스트/그룹캐스트 송신이 유니캐스트 송신 대신에 사용되는 경우 생략될 수 있다.

[0114] 스테이지(1010)에서, UE들(1001, 1002)에는 적절한 보안 자료가 프로비저닝된다. UE들(1001, 1002)은 발견 메시지를 위한 보안 자료를 요청하는 발견 요청들(1011, 1012)을 네트워크 엔티티(600)로 전송할 수 있다. 네트워크 엔티티(600), 예컨대, RKMF(650)는 발견 메시지들을 위한 보안 자료를 포함하는 발견 응답들(1013, 1014)을 전송함으로써 발견 요청들(1011, 1012)에 응답할 수 있다. 또한 또는 대안적으로, UE들(1001, 1002)은 (포지셔닝 메시지들 및 PRS를 포함하는) 포지셔닝 시그널링을 위한 보안 자료를 요청하는 레인징 보호 요청들(1015, 1016)을 네트워크 엔티티(600)로 전송할 수 있다. 네트워크 엔티티(600), 예컨대, RKMF(650)는 레인징 메시지들 및 PRS를 위한 보안 자료를 포함하는 레인징 보호 응답들(1017, 1018)을 전송함으로써 레인징 보호 요청들(1015, 1016)에 응답할 수 있다. 네트워크 엔티티(600)는 자율 그룹 형성을 위해, 또는 네트워크 기반 그룹 형성 또는 자율 그룹 형성 둘 모두를 위해, 네트워크 커버리지 밖에 있을 때 자율 기반 그룹 형성을 사용하기 위한 표시(및/또는 네트워크 커버리지 내에 있을 때 네트워크 기반 그룹 형성을 사용하기 위한 표시)를 UE들(1001, 1002)에 프로비저닝할 수 있다. 발견 및 레인징 둘 모두를 위해 동일한 보안 자료가 사용될 수 있거나, 또는 발견 및 레인징을 위해 별개의 보안 자료가 제공될 수 있다. 일부 실시 형태들에서, 발견 보안 자료가 제공되는 한편 레인징 보안 자료는 제공되지 않는다. 일부 실시 형태들에서, 레인징 보안 자료가 제공되고 발견 보안 자료는 제공되지 않는다.

[0115] 보안 자료는 그룹 형성에 앞서 제공되고, UE들(1001, 1002) 각각에 대한 하나 이상의 인증서들을 포함하며, 이때 보안 자료는 긴 유효성 시간을 갖는다. UE들(1001, 1002)에 대한 인증서들은 각각 네트워크 엔티티(600)에 의해 서명된 UE(1001)의 공개 키 및 네트워크 엔티티(600)에 의해 서명된 UE(1002)의 공개 키를 포함한다. 다수의 인증서들이 UE들(1001, 1002) 각각에 대해 제공될 수 있으며, 이때 다수의 인증서들을 사용하기 위한 시퀀스가 UE들(1001, 1002)에 의해 알려져 있다(예컨대, 프로토콜은 사전-프로그래밍되거나, 또는 예컨대, 유니캐스트 링크 셋업 동안, UE들(1001, 1002)에 의해 합의된 로컬 정책임). 다수의 인증서들 및 인증서 롤오버 프로토콜을 사용하는 것은 UE들의 통신들의 추적을 억제하는 데 도움이 될 수 있는데, 이는 UE(1001)(또는 UE(1002))에 의한 인증서의 사용이 다른 엔티티들에 가시적이고, 그 다른 엔티티들이 다수의 통신들에서 동일한 아이덴티티 정보 및 키 ID를 인식함으로써 통신들을 추적할 수 있기 때문이다. 인증서를 변경하는 것은 UE에 대한 통신들을 추적하는 것을 더 어렵게 만든다. 스테이지(1010) 동안, UE들(1001, 1002)에는, 다른 서비스 제공자들, 예컨대, 다른 MNO(Mobile Network Operator)들과의 상호운용성을 보조하기 위해 신뢰된 인증 기관(CA) 리스트가 프로비저닝될 수 있다.

[0116] 브로드캐스트/그룹캐스트 시그널링 보호

[0117] 브로드캐스트 메시지들에는, 프로비저닝된 인증서들을 사용하여 무결성 또는 진정성(authenticity) 보호가 제공될 수 있다. 예를 들어, UE들(1001, 1002) 중 어느 하나에 의해 적절하게 전송된 각각의 브로드캐스트 메시지(예컨대, 각각 스테이지(1020)에서의 발견 메시지(1022), 스테이지(1030)에서의 PRS 이전 메시지(1032), 스테이지(1060)에서의 PRS 응답(1062), 스테이지(1070)에서의 PRS(1072), 및/또는 스테이지(1080)에서의 PRS 이후 메시지(1082))는 각자의 UE의 개인 키를 사용하여 각자의 UE에 의해 서명된다. 인증서(또는 인증서 체인)는 수신 UE에 의한 검증을 위해 메시지에서 반송된다. 수신 UE는 메시지를 송신한 UE의 공개 키를 사용하여 메시지를 검증하고, RKMF(650)의 공개 키를 사용하여 송신 UE의 공개 키를 검증한다. 그룹이 스테이지(1020)에서의 발견

에 기초하여 서로를 인식하는 UE들에 기초하여 그룹 형성 스테이지(1025)에서 형성되고, 이때 그룹은 시그널링 보호를 위한 보안 정보를 확립하는 데 사용된다(예컨대, 브로드캐스트/그룹캐스트 신호 보호를 위한 그룹 키 확립). 그룹 형성은 네트워크 엔티티(600)로부터의 입력 없이 PC5 링크를 사용하여 발생한다.

[0118] 브로드캐스트 또는 그룹캐스트 PRS 송신을 위해(발견 및/또는 레인징을 위해), 프로비저닝된 키 또는 프로비저닝된 키로부터 유도된 키가 레인징 시그널링을 보호하기 위해 레인징 키로서 사용될 수 있다. 브로드캐스트/그룹캐스트 레인징을 위해, 그룹 키(예컨대, 레인징 키)가 예컨대, 위에서 논의된 바와 같이(예컨대, 시간(또는 프레임 수 및/또는 슬롯 수), 그룹/서비스 ID, 및 그룹 키가 포지셔닝 세션에 대한 PRS 시퀀스를 생성하기 위한 함수에 대한 입력들로서 사용되는 것에 기초하여) PRS를 랜덤화하는 데 사용될 수 있고, 이때 그룹 키는 레인징 보호 응답들(1017, 1018)에서 네트워크 엔티티(600)로부터 획득된다. 대안적으로, 그룹 키는 그룹 형성 동안 UE들(1001, 1002)에 의해, 예컨대, 유니캐스트 링크 셋업 이후 PRS 세션 키를 분배하는 그룹 리더(예컨대, 개시자 UE(1001))와, 예컨대, 그룹 형성 동안 확립된 그룹 디피-헬먼(Diffie-Hellman) 키로 협상될 수 있다. 예를 들어, 그룹 키가 네트워크 엔티티(600)에 의해 프로비저닝되지 않았거나 또는 달리 이용가능하지 않은 경우, 하나의 UE는 각각의 다른 그룹 멤버에 대한 보안 유니캐스트 링크를 통해 그룹의 다른 멤버(들)에 그룹 키를 프로비저닝할 수 있다.

[0119] 유니캐스트 시그널링 보호

[0120] 유니캐스트 링크가 스테이지(1040)에서 확립되고 레인징 암호 키, 예컨대, 대칭 키가 스테이지들(1060, 1070, 1080)에서 모바일-투-모바일 포지셔닝을 위한 유니캐스트 시그널링을 보호하기 위해 확립되거나 또는 달리 획득될 수 있다. 레인징 암호 키는, 키가 UE들 사이의 PC5 인터페이스를 통한 시그널링을 보호하기 위해 사용되므로 PC5 레인징 키로 불릴 수 있다. 레인징 키는, 예를 들어, (UE들(1001, 1002)이 각각의 인증서들을 다른 UE(1001, 1002)에 제공하고 UE들(1001, 1002)의 공개 키들에 기초하여 대칭 키를 결정하는) 유니캐스트 송신들을 위한 인증서-기반 키 결정 및 보호에 대한 상기 논의와 유사하게, UE들(1001, 1002)의 인증서들에 기초하여 획득될 수 있다.

[0121] 동작

[0122] 도 1 내지 도 10을 추가로 참조하여, 도 11을 참조하면, 포지셔닝 세션 시그널링 방법(1100)은 도시된 스테이지들을 포함한다. 그러나, 방법(1100)은 제한이 아닌 일 예이다. 방법(1100)은, 예컨대, 스테이지들을 추가하고, 제거하고, 재배열하고, 조합하고, 동시에 수행함으로써, 그리고/또는 단일의 스테이지들을 다수의 스테이지들로 분할함으로써 변경될 수 있다.

[0123] 스테이지(1110)에서, 방법(1100)은, 제1 무선 통신 디바이스에서, 레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하는 단계를 포함한다. 예를 들어, UE(500)(예컨대, UE(901), UE(902), UE(1001), 또는 UE(1002))의 SL 포지셔닝 유닛(550)은, 예컨대, 보안 자료에 대한 요청에 응답하여, 스테이지(910 또는 1010) 동안 네트워크 엔티티(600)로부터 트랜시버(520)를 통해 보안 자료(예컨대, 대칭 키)를 획득할 수 있다. 요청은, 제1 UE(예컨대, 타겟 UE(902))에 의해, 제2 UE(예컨대, 개시자 UE(901))가 보안 자료(예컨대, 대칭 키)를 획득하기 위해 네트워크 엔티티(600)(예컨대, RKMF(650))에 연락(contact)하도록 제1 UE에 명령하는 것에 응답하여 전송될 수 있다. 다른 예로서, SL 포지셔닝 유닛(550)은, 메모리(530)로부터 보안 자료를 추출함으로써 보안 자료를 획득할 수 있으며, 예컨대, 이때 보안 자료는 네트워크 엔티티(600)로부터 이전에 수신되었거나 또는 예컨대, UE(500)의 제조 동안, 메모리(530)에 사전-저장되었다. 프로세서(510)는, 가능하게는 메모리(530)와 조합하여, 가능하게는 트랜시버(520)(예컨대, 무선 수신기(244) 및 안테나(246))와 조합하여, 제1 보안 자료를 획득하기 위한 수단을 포함할 수 있다.

[0124] 스테이지(1120)에서, 방법(1100)은, 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하는 단계를 포함한다. 제1 보안 자료는 스테이지(910)에서 (요구 시 또는 사전에) 프로비저닝되고 그리고/또는 제2 보안 자료는 스테이지들(940, 950)에서 프로비저닝될 수 있다. 예를 들어, UE(901) 또는 UE(902)는 스테이지(910)에서 프로비저닝되거나, 또는 유니캐스트 시그널링을 위해 스테이지(950)에서 프로비저닝된 레인징 키에 기초하여 PRS(972)를 브로드캐스팅할 수 있다. 제2 보안 자료는 요구 시 또는 그룹 형성 전에 프로비저닝될 수 있다. 제1 보안 정보의 제1 부분은 레인징을 위해 사용되는 발견 키일 수 있거나 또는 레인징-특정 키일 수 있다. 레인징 신호는 (예컨대, 유니캐스트 링크가 스테이지(940) 또는 스테이지(1040)에서 셋업되는 경우) 브로드캐스팅, 그룹캐스팅, 또는 유니캐스팅될 수 있다. 프로세서(510)는, 가능하게는 메모리(530)와 조합하여, 트랜시버(520)(예컨대, 무선 송신기(242) 및 안테나(246))와 조합하여, 레인징 신호를 송신(및 제1 보안 자료의

적어도 제1 부분에 기초하여 그리고/또는 제2 보안 자료에 기초하여 레인징 신호를 결정)하기 위한 수단을 포함할 수 있다.

[0125] 방법(1100)의 구현들은 다음의 특징들 중 하나 이상을 포함할 수 있다. 예시적인 구현에서, 제1 보안 자료는 대칭 암호 키인 레인징 암호 키를 포함하고, 레인징 신호는, 기본 포지셔닝 기준 신호 및 레인징 암호 키에 기초하는 수정된 포지셔닝 기준 신호를 포함한다. 예를 들어, 수정된 PRS는 랜덤화되는 기본 PRS(예컨대, 초기 PRS 또는 이전(예컨대, 가장 최근의) PRS)(예컨대, 이때 이전 PRS는 랜덤화된 PRS의 체인에서 가장 최근의 랜덤화된 PRS임)일 수 있다. 레인징 암호 키는 발견 암호 키와 동일한 키일 수 있다. 다른 예시적인 구현에서, 제1 보안 자료는 제1 비대칭 암호 키를 포함하는 제1 암호로 서명된 인증서를 포함하고, 포지셔닝 세션 시그널링 방법은, 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제1 암호로 서명된 인증서를 송신하는 단계; 및 제2 무선 통신 디바이스로부터 제1 무선 통신 디바이스에서, 제2 비대칭 암호 키를 포함하는 제2 암호로 서명된 인증서를 수신하는 단계를 추가로 포함하고; 여기서 레인징 신호를 송신하는 단계는, 제1 비대칭 암호 키 및 제2 비대칭 암호 키에 기초하는 대칭 암호 키에 기초하여 암호화된 레인징 신호를 암호화된 유니캐스트 레인징 신호로서 송신하는 단계를 포함한다. 예를 들어, 제1 보안 자료는 RKM(650)의 개인 키에 의해 서명된 제1 UE(예컨대, UE(901), UE(902), UE(1001), 또는 UE(1002))의 공개 키를 포함하는 인증서일 수 있다. UE(예컨대, UE(901))는, 다른 UE(예컨대, UE(902))로 인증서를 송신하도록 구성될 수 있고 그리고 이를 송신할 수 있고, (RKM(650)에 의해 서명된 다른 UE의 공개 키의) 다른 UE로부터의 유사한 인증서를 수신하도록 구성될 수 있고 그리고 이를 수신할 수 있다. 제1 UE는 (예컨대, 알고리즘, 예컨대, EAP-TLS 프로세스에 대한 입력들로서 UE들의 공개 키들을 사용함으로써) 인증서들로부터 결정된 대칭 키를 사용하여 암호화된 레인징 신호를 송신할 수 있다. 프로세서(510)는, 가능하게는 메모리(530)와 조합하여, 트랜시버(520)(예컨대, 무선 송신기(242) 및 안테나(246))와 조합하여, 제1 암호로 서명된 인증서를 송신하기 위한 수단을 포함할 수 있다. 프로세서(510)는, 가능하게는 메모리(530)와 조합하여, 트랜시버(520)(예컨대, 무선 수신기(244) 및 안테나(246))와 조합하여, 제2 암호로 서명된 인증서를 수신하기 위한 수단을 포함할 수 있다. 추가의 예시적인 구현에서, 제1 암호로 서명된 인증서는, 제1 무선 통신 디바이스의 현재 위치가 제1 암호로 서명된 인증서와 연관된 유효성 구역(validity region) 내에 있는 것에 기초하여 송신된다. 예를 들어, SL 포지셔닝 유닛(550)은, UE(500)가 UE(500)에 의한 송신을 위해 인증서 인가된 구역 내에 UE(500)가 현재 배치되지 않는 한, UE(500)의 서명된 공개 키의 인증서를 송신하지 않도록 구성될 수 있다.

[0126] 또한 또는 대안적으로, 방법(1100)의 구현들은 다음의 특징들 중 하나 이상을 포함할 수 있다. 예시적인 구현에서, 방법(1100)은, 제2 무선 통신 디바이스 또는 네트워크 엔티티로부터 제1 무선 통신 디바이스에서, 레인징 암호 키를 수신하는 단계를 추가로 포함하고, 제2 보안 자료는 레인징 암호 키를 포함한다. 예를 들어, 스테이지(950)에서, UE(902)는 네트워크 엔티티(600)로부터 암호 키(예컨대, 대칭 키)를 수신한다. 다른 예로서, 스테이지(940)에서, UE(901)는 UE(902)로부터 (UE(902)가 스테이지(950)에서 네트워크 엔티티(600)로부터 수신한) 암호 키를 수신한다. UE(901, 902)는 레인징 암호 키를 사용하여 레인징 신호를 보호(예컨대, 암호화함으로써 기밀성 보호 및/또는 서명함으로써 보안 보호)하기 위해 레인징 암호 키를 사용할 수 있다. 프로세서(510)는, 가능하게는 메모리(530)와 조합하여, 가능하게는 트랜시버(520)(예컨대, 무선 수신기(244) 및 안테나(246))와 조합하여, 레인징 암호 키를 수신하기 위한 수단을 포함할 수 있다. 다른 예시적인 구현에서, 방법(1100)은, 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제2 부분에 기초하는 발견 메시지를 송신하는 단계를 추가로 포함한다. 제1 보안 자료의 제1 및 제2 부분들은 동일할 수 있거나(예컨대, 대칭 그룹 키), 또는 제1 보안 자료의 제1 및 제2 부분들은 대칭 키; 비대칭 키; 또는 인증서 중 임의의 2개일 수 있다. 예를 들어, UE(902)는, 대칭 키로 암호화되거나, 또는 비대칭 개인 키를 사용하여 서명되거나, 또는 인증서를 포함하는 발견 메시지를 송신할 수 있다. 프로세서(510)는, 가능하게는 메모리(530)와 조합하여, 가능하게는 트랜시버(520)(예컨대, 무선 송신기(242) 및 안테나(246))와 조합하여, 발견 메시지를 송신(및 발견 메시지를 암호화 및/또는 이에 서명)하기 위한 수단을 포함할 수 있다. 추가의 예시적인 구현에서, 제1 보안 자료의 제1 부분은 제1 보안 자료의 제2 부분과 동일하다.

[0127] 또한 또는 대안적으로, 방법(1100)의 구현들은 다음의 특징들 중 하나 이상을 포함할 수 있다. 예시적인 구현에서, 제1 보안 자료는 레인징 암호 키를 포함하고, 포지셔닝 세션 시그널링 방법은, 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제2 무선 통신 디바이스가 레인징 암호 키를 위해 네트워크 엔티티에 연락하도록 하는 표시를 송신하는 단계; 및 제1 무선 통신 디바이스에서, 제1 무선 통신 디바이스에 저장된 기본 암호 키에 기초하여 레인징 암호 키를 결정하는 단계를 추가로 포함한다. 예를 들어, 개시자 UE(901)는, 타겟 UE(902)가 레인징 암호 키를 획득하기 위해 네트워크 엔티티(600)에 연락하도록 하는 표시를 유니캐스트 링크 셋업의 스테이지(940) 동안 타겟 UE(902)로 송신한다. 표시는 개시자 UE(901)의 ID 및 선도 파라미터를 포함할

수 있고, 네트워크 엔티티(600)(예컨대, RKMF(650))에 의해 개시자 UE(901)에 프로비저닝된 암호 키(예컨대, 기본 키)의 표시를 포함할 수 있다. 개시자 UE(901)는 RKMF(650)에 의해 개시자 UE(901)에 프로비저닝되고 메모리(530)에 저장된 암호 키, 및 기본 암호 키가 입력으로서 사용되는 개시자 UE(901)와 RKMF(650) 둘 모두에 의해 알려진 프로토콜 또는 알고리즘에 기초하여 레인징 키를 결정할 수 있다. 기본 암호 키는 개시자 UE(901) 및 네트워크 엔티티(600) 둘 모두에 의해 저장된다. 기본 암호 키는 초기 키일 수 있거나 또는 초기 키로부터 이전에 유도되었던 키 또는 초기 키에 다시 도달하는 키들의 체인에 있는 다른 키일 수 있다. 예를 들어, 제1 및 제2 UE들은 그들 사이의 유니캐스트 보안을 위한 대칭 키를 갖기를 원한다. 제1 UE에는 기본 키가 프로비저닝된다. 제1 UE 및 RKMF(650)는 대칭 키를 결정하기 위한 키 유도 함수(key derivation function, KDF)에 대한 입력들로서 기본 키 및 선도 파라미터들(예컨대, 제1 UE에 의해 생성된 제1 난수 및 RKMF(650)에 의해 생성된 제2 난수)을 사용한다. 제1 UE는 제1 난수를 RKMF(650)로 전송하고, RKMF(650)는 제2 난수를 제1 UE로 전송한다. 제1 UE 및 RKMF(650) 둘 모두는 기본 키 및 제1 및 제2 난수들을 알고 대칭 키를 생성할 수 있다. 프로세서(510)는, 가능하게는 메모리(530)와 조합하여, 가능하게는 트랜시버(520)(예컨대, 무선 송신기(242) 및 안테나(246))와 조합하여, 제2 UE가 레인징 암호 키를 위해 네트워크 엔티티에 연락하도록 하는 표시를 송신하기 위한 수단을 포함할 수 있다. 프로세서(510)는, 가능하게는 메모리(530)와 조합하여, 기본 암호 키에 기초하여 레인징 암호 키를 결정하기 위한 수단을 포함할 수 있다.

[0128] 또한 또는 대안적으로, 방법(1100)의 구현들은 다음의 특징들 중 하나 이상을 포함할 수 있다. 예시적인 구현에서, 제1 보안 자료는, 제1 무선 통신 디바이스 및 제2 무선 통신 디바이스와는 별개인 엔티티에 의해 암호로 서명된 제1 무선 통신 디바이스의 공개 암호 키를 포함하는 복수의 암호로 서명된 인증서들을 포함하고, 포지셔닝 세션 시그널링 방법은, 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제1 무선 통신 디바이스에 의해 암호로 서명되고 인증서 선택 정책에 기초하여 복수의 암호로 서명된 인증서들 중 적어도 하나를 포함하는 발견 메시지를 송신하는 단계를 추가로 포함한다. 예를 들어, 자율 그룹 형성을 위해, 개시자 UE(1001)는 메모리(530)에 저장된 다수의 인증서들을 가질 수 있다(이때 각각의 인증서는 네트워크 엔티티(600)의 개인 키에 의해 서명된 개시자 UE(1001)의 공개 키임). 스테이지(1020)에서, 개시자 UE(1001)는 개시자 UE(1001)에 의해 서명되고 네트워크 엔티티(600)에 의해 서명된 인증서들 중 하나 이상을 포함하는 발견 메시지(1022)를 전송할 수 있다. 발견 메시지(1022) 내의 인증서(들)는 UE들(1001, 1002) 둘 모두에 알려진 인증서 선택 정책에 따라 개시자 UE(1001)에 의해 선택될 수 있다. 프로세서(510)는, 가능하게는 메모리(530)와 조합하여, 가능하게는 트랜시버(520)(예컨대, 무선 송신기(242) 및 안테나(246))와 조합하여, 제2 UE로 발견 메시지를 송신하기 위한 수단을 포함할 수 있다. 추가의 예시적인 구현에서, 방법(1100)은, 제1 무선 통신 디바이스가 그룹 형성 동안 제2 무선 통신 디바이스와 레인징 암호 키를 협상하는 단계를 추가로 포함하고, 레인징 신호는, 기본 포지셔닝 기준 신호, 또는 레인징 암호 키, 또는 선도 파라미터, 또는 이들의 조합에 기초하는 수정된 포지셔닝 기준 신호를 포함하고, 선도 파라미터는 타이머, 카운터, 시스템 프레임 수, 슬롯 수, 심볼 수, 또는 이들 중 2개 이상의 임의의 조합을 포함한다. 따라서, 기본 PRS, 또는 레인징 암호 키, 또는 선도 파라미터는 랜덤화된 PRS를 생성하기 위한 알고리즘에 대한 입력으로서 사용될 수 있다. 대안적으로, 기본 PRS 및 레인징 암호 키, 또는 기본 PRS 및 선도 파라미터, 또는 레인징 암호 키 및 선도 파라미터, 또는 기본 PRS 및 레인징 암호 키 및 선도 파라미터는 랜덤화된 PRS를 생성하기 위한 알고리즘에 대한 입력들로서 사용될 수 있다. 예를 들어, 개시자 UE(1001)에 의해 타겟 UE(1002)로(또는 타겟 UE(1002)로부터 개시자 UE(1001)로) 송신된 PRS는 PRS를 랜덤화하기 위한 알고리즘에 대한 적어도 하나의 입력으로서 그룹 형성(여기서, UE들(1001, 1002)은 포지셔닝 세션에 대한 그룹인 것으로 결정됨) 동안 UE들(1001, 1002)에 의해 협상된 암호 키를 사용함으로써 랜덤화될 수 있다. 선도 파라미터는 또한 또는 대안적으로, 키 대신에 또는 그에 더하여 알고리즘에 대한 입력으로서 사용될 수 있다. 선도 파라미터는 타이머, 카운터, 시스템 프레임 수, 슬롯 수, 심볼 수, 또는 이들 중 2개 이상의 임의의 조합(예컨대, 타이머 및 시스템 프레임 수; 또는 카운터, 슬롯 수, 및 심볼 수; 등)일 수 있다. 프로세서(510)는, 가능하게는 메모리(530)와 조합하여, 가능하게는 트랜시버(520)(예컨대, 무선 송신기(242), 무선 수신기(244) 및 안테나(246))와 조합하여, 레인징 암호 키를 협상하기 위한 수단을 포함할 수 있다.

[0129] 또한 또는 대안적으로, 방법(1100)의 구현들은 다음의 특징들 중 하나 이상을 포함할 수 있다. 예시적인 구현에서, 제1 보안 자료는 서비스 확립에 응답하여 획득된다. 예를 들어, 제1 보안 자료는 사전-프로비저닝되고 PRS 세션에 합류할 때 사용될 수 있다. 다른 예시적인 구현에서, 제1 보안 자료는 레인징 세션에 합류하는 것에 응답하여 획득된다. 예를 들어, 제1 보안 자료는 제1 무선 통신 디바이스가 요구 시 PRS 세션에 합류하는 것에 응답하여 획득될 수 있다.

[0130] **구현 예들**

- [0131] 구현 예들은 다음의 번호가 매겨진 조항들에서 제공된다.
- [0132] 조항 1. 제1 무선 통신 디바이스로서,
- [0133] 트랜시버;
- [0134] 메모리; 및
- [0135] 트랜시버 및 메모리에 통신가능하게 커플링된 프로세서를 포함하고, 프로세서는,
- [0136] 레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하도록; 그리고
- [0137] 트랜시버를 통해 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하도록 구성되는, 제1 무선 통신 디바이스.
- [0138] 조항 2. 조항 1에 있어서, 제1 보안 자료는 대칭 암호 키인 레인징 암호 키를 포함하고, 레인징 신호는, 기본 포지셔닝 기준 신호 및 레인징 암호 키에 기초하는 수정된 포지셔닝 기준 신호를 포함하는, 제1 무선 통신 디바이스.
- [0139] 조항 3. 조항 1에 있어서, 제1 보안 자료는 제1 비대칭 암호 키를 포함하는 제1 암호로 서명된 인증서를 포함하고, 프로세서는,
- [0140] 트랜시버를 통해 제2 무선 통신 디바이스로, 제1 암호로 서명된 인증서를 송신하도록; 그리고
- [0141] 제2 무선 통신 디바이스로부터 트랜시버를 통해, 제2 비대칭 암호 키를 포함하는 제2 암호로 서명된 인증서를 수신하도록 추가로 구성되고;
- [0142] 레인징 신호를 송신하기 위해, 프로세서는, 제1 비대칭 암호 키 및 제2 비대칭 암호 키에 기초하는 대칭 암호 키에 기초하여 암호화된 레인징 신호를 암호화된 유니캐스트 레인징 신호로서 송신하도록 구성되는, 제1 무선 통신 디바이스.
- [0143] 조항 4. 조항 3에 있어서, 프로세서는, 제1 무선 통신 디바이스의 현재 위치가 제1 암호로 서명된 인증서와 연관된 유효성 구역 내에 있는 것에 기초하여 제1 암호로 서명된 인증서를 송신하도록 구성되는, 제1 무선 통신 디바이스.
- [0144] 조항 5. 조항 1에 있어서, 프로세서는, 트랜시버를 통해, 레인징 암호 키를 수신하도록 추가로 구성되고, 제2 보안 자료는 레인징 암호 키를 포함하는, 제1 무선 통신 디바이스.
- [0145] 조항 6. 조항 1에 있어서, 프로세서는, 트랜시버를 통해 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제2 부분에 기초하는 발견 메시지를 송신하도록 추가로 구성되는, 제1 무선 통신 디바이스.
- [0146] 조항 7. 조항 6에 있어서, 제1 보안 자료의 제1 부분은 제1 보안 자료의 제2 부분과 동일한, 제1 무선 통신 디바이스.
- [0147] 조항 8. 조항 1에 있어서, 제1 보안 자료는 레인징 암호 키를 포함하고, 프로세서는,
- [0148] 트랜시버를 통해 제2 무선 통신 디바이스로, 제2 무선 통신 디바이스가 레인징 암호 키를 위해 네트워크 엔티티에 연락하도록 하는 표시를 송신하도록; 그리고
- [0149] 제1 무선 통신 디바이스에 저장된 기본 암호 키에 기초하여 레인징 암호 키를 결정하도록 추가로 구성되는, 제1 무선 통신 디바이스.
- [0150] 조항 9. 조항 1에 있어서,
- [0151] 제1 보안 자료는, 제1 무선 통신 디바이스 및 제2 무선 통신 디바이스와는 별개인 엔티티에 의해 암호로 서명된 제1 무선 통신 디바이스의 공개 암호 키를 포함하는 복수의 암호로 서명된 인증서들을 포함하고;
- [0152] 프로세서는, 트랜시버를 통해 제2 무선 통신 디바이스로, 제1 무선 통신 디바이스에 의해 암호로 서명되고 인증서 선택 정책에 기초하여 복수의 암호로 서명된 인증서들 중 적어도 하나를 포함하는 발견 메시지를 송신하도록 추가로 구성되는, 제1 무선 통신 디바이스.
- [0153] 조항 10. 조항 9에 있어서, 프로세서는, 그룹 형성 동안 제2 무선 통신 디바이스와 레인징 암호 키를 협상하도록

록 추가로 구성되고, 레인징 신호는, 기본 포지셔닝 기준 신호, 또는 레인징 암호 키, 또는 선도 파라미터, 또는 이들 중 2개 이상의 조합에 기초하는 수정된 포지셔닝 기준 신호를 포함하고, 선도 파라미터는 타이머, 카운터, 시스템 프레임 수, 슬롯 수, 심볼 수, 또는 이들 중 2개 이상의 임의의 조합을 포함하는, 제1 무선 통신 디바이스.

- [0154] 조항 11. 조항 1에 있어서, 프로세서는 서비스 확립에 응답하여 제1 보안 자료를 획득하도록 구성되는, 제1 무선 통신 디바이스.
- [0155] 조항 12. 조항 1에 있어서, 프로세서는 레인징 세션에 합류하는 것에 응답하여 제1 보안 자료를 획득하도록 구성되는, 제1 무선 통신 디바이스.
- [0156] 조항 13. 포지셔닝 세션 시그널링 방법으로서,
- [0157] 제1 무선 통신 디바이스에서, 레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하는 단계; 및
- [0158] 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하는 단계를 포함하는, 포지셔닝 세션 시그널링 방법.
- [0159] 조항 14. 조항 13에 있어서, 제1 보안 자료는 대칭 암호 키인 레인징 암호 키를 포함하고, 레인징 신호는, 기본 포지셔닝 기준 신호 및 레인징 암호 키에 기초하는 수정된 포지셔닝 기준 신호를 포함하는, 포지셔닝 세션 시그널링 방법.
- [0160] 조항 15. 조항 13에 있어서, 제1 보안 자료는 제1 비대칭 암호 키를 포함하는 제1 암호로 서명된 인증서를 포함하고, 포지셔닝 세션 시그널링 방법은,
- [0161] 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제1 암호로 서명된 인증서를 송신하는 단계; 및
- [0162] 제2 무선 통신 디바이스로부터 제1 무선 통신 디바이스에서, 제2 비대칭 암호 키를 포함하는 제2 암호로 서명된 인증서를 수신하는 단계를 추가로 포함하고;
- [0163] 레인징 신호를 송신하는 단계는, 제1 비대칭 암호 키 및 제2 비대칭 암호 키에 기초하는 대칭 암호 키에 기초하여 암호화된 레인징 신호를 암호화된 유니캐스트 레인징 신호로서 송신하는 단계를 포함하는, 포지셔닝 세션 시그널링 방법.
- [0164] 조항 16. 조항 15에 있어서, 제1 암호로 서명된 인증서는, 제1 무선 통신 디바이스의 현재 위치가 제1 암호로 서명된 인증서와 연관된 유효성 구역 내에 있는 것에 기초하여 송신되는, 포지셔닝 세션 시그널링 방법.
- [0165] 조항 17. 조항 13에 있어서, 제2 무선 통신 디바이스 또는 네트워크 엔티티로부터 제1 무선 통신 디바이스에서, 레인징 암호 키를 수신하는 단계를 추가로 포함하고, 제2 보안 자료는 레인징 암호 키를 포함하는, 포지셔닝 세션 시그널링 방법.
- [0166] 조항 18. 조항 13에 있어서, 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제2 부분에 기초하는 발견 메시지를 송신하는 단계를 추가로 포함하는, 포지셔닝 세션 시그널링 방법.
- [0167] 조항 19. 조항 18에 있어서, 제1 보안 자료의 제1 부분은 제1 보안 자료의 제2 부분과 동일한, 포지셔닝 세션 시그널링 방법.
- [0168] 조항 20. 조항 13에 있어서, 제1 보안 자료는 레인징 암호 키를 포함하고, 포지셔닝 세션 시그널링 방법은,
- [0169] 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제2 무선 통신 디바이스가 레인징 암호 키를 위해 네트워크 엔티티에 연락하도록 하는 표시를 송신하는 단계; 및
- [0170] 제1 무선 통신 디바이스에서, 제1 무선 통신 디바이스에 저장된 기본 암호 키에 기초하여 레인징 암호 키를 결정하는 단계를 추가로 포함하는, 포지셔닝 세션 시그널링 방법.
- [0171] 조항 21. 조항 13에 있어서,
- [0172] 제1 보안 자료는, 제1 무선 통신 디바이스 및 제2 무선 통신 디바이스와는 별개인 엔티티에 의해 암호로 서명된 제1 무선 통신 디바이스의 공개 암호 키를 포함하는 복수의 암호로 서명된 인증서들을 포함하고;

- [0173] 포지셔닝 세션 시그널링 방법은, 제1 무선 통신 디바이스로부터 제2 무선 통신 디바이스로, 제1 무선 통신 디바이스에 의해 암호로 서명되고 인증서 선택 정책에 기초하여 복수의 암호로 서명된 인증서들 중 적어도 하나를 포함하는 발견 메시지를 송신하는 단계를 추가로 포함하는, 포지셔닝 세션 시그널링 방법.
- [0174] 조항 22. 조항 21에 있어서, 제1 무선 통신 디바이스가 그룹 형성 동안 제2 무선 통신 디바이스와 레인징 암호 키를 협상하는 단계를 추가로 포함하고, 레인징 신호는, 기본 포지셔닝 기준 신호, 또는 레인징 암호 키, 또는 선도 파라미터, 또는 이들 중 2개 이상의 조합에 기초하는 수정된 포지셔닝 기준 신호를 포함하고, 선도 파라미터는 타이머, 카운터, 시스템 프레임 수, 슬롯 수, 심볼 수, 또는 이들 중 2개 이상의 임의의 조합을 포함하는, 포지셔닝 세션 시그널링 방법.
- [0175] 조항 23. 조항 13에 있어서, 제1 보안 자료는 서비스 확립에 응답하여 획득되는, 포지셔닝 세션 시그널링 방법.
- [0176] 조항 24. 조항 13에 있어서, 제1 보안 자료는 레인징 세션에 합류하는 것에 응답하여 획득되는, 포지셔닝 세션 시그널링 방법.
- [0177] 조항 25. 제1 무선 통신 디바이스로서,
- [0178] 레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하기 위한 수단; 및
- [0179] 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하기 위한 수단을 포함하는, 제1 무선 통신 디바이스.
- [0180] 조항 26. 조항 25에 있어서, 제1 보안 자료는 대칭 암호 키인 레인징 암호 키를 포함하고, 레인징 신호는, 기본 포지셔닝 기준 신호 및 레인징 암호 키에 기초하는 수정된 포지셔닝 기준 신호를 포함하는, 제1 무선 통신 디바이스.
- [0181] 조항 27. 조항 25에 있어서, 제1 보안 자료는 제1 비대칭 암호 키를 포함하는 제1 암호로 서명된 인증서를 포함하고, 제1 무선 통신 디바이스는,
- [0182] 제2 무선 통신 디바이스로, 제1 암호로 서명된 인증서를 송신하기 위한 수단; 및
- [0183] 제2 무선 통신 디바이스로부터, 제2 비대칭 암호 키를 포함하는 제2 암호로 서명된 인증서를 수신하기 위한 수단을 추가로 포함하고;
- [0184] 레인징 신호를 송신하기 위한 수단은, 제1 비대칭 암호 키 및 제2 비대칭 암호 키에 기초하는 대칭 암호 키에 기초하여 암호화된 레인징 신호를 암호화된 유니캐스트 레인징 신호로서 송신하기 위한 수단을 포함하는, 제1 무선 통신 디바이스.
- [0185] 조항 28. 조항 27에 있어서, 제1 암호로 서명된 인증서를 송신하기 위한 수단은, 제1 무선 통신 디바이스의 현재 위치가 제1 암호로 서명된 인증서와 연관된 유효성 구역 내에 있는 것에 기초하여 제1 암호로 서명된 인증서를 송신하기 위한 수단을 포함하는, 제1 무선 통신 디바이스.
- [0186] 조항 29. 조항 25에 있어서, 제2 무선 통신 디바이스 또는 네트워크 엔티티로부터, 레인징 암호 키를 수신하기 위한 수단을 추가로 포함하고, 제2 보안 자료는 레인징 암호 키를 포함하는, 제1 무선 통신 디바이스.
- [0187] 조항 30. 조항 25에 있어서, 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제2 부분에 기초하는 발견 메시지를 송신하기 위한 수단을 추가로 포함하는, 제1 무선 통신 디바이스.
- [0188] 조항 31. 조항 30에 있어서, 제1 보안 자료의 제1 부분은 제1 보안 자료의 제2 부분과 동일한, 제1 무선 통신 디바이스.
- [0189] 조항 32. 조항 25에 있어서, 제1 보안 자료는 레인징 암호 키를 포함하고, 제1 무선 통신 디바이스는,
- [0190] 제2 무선 통신 디바이스로, 제2 무선 통신 디바이스가 레인징 암호 키를 위해 네트워크 엔티티에 연락하도록 하는 표시를 송신하기 위한 수단; 및
- [0191] 제1 무선 통신 디바이스에 저장된 기본 암호 키에 기초하여 레인징 암호 키를 결정하기 위한 수단을 추가로 포함하는, 제1 무선 통신 디바이스.

- [0192] 조항 33. 조항 25에 있어서,
- [0193] 제1 보안 자료는, 제1 무선 통신 디바이스 및 제2 무선 통신 디바이스와는 별개인 엔티티에 의해 암호로 서명된 제1 무선 통신 디바이스의 공개 암호 키를 포함하는 복수의 암호로 서명된 인증서들을 포함하고;
- [0194] 제1 무선 통신 디바이스는, 제2 무선 통신 디바이스로, 제1 무선 통신 디바이스에 의해 암호로 서명되고 인증서 선택 정책에 기초하여 복수의 암호로 서명된 인증서들 중 적어도 하나를 포함하는 발견 메시지를 송신하기 위한 수단을 추가로 포함하는, 제1 무선 통신 디바이스.
- [0195] 조항 34. 조항 33에 있어서, 그룹 형성 동안 제2 무선 통신 디바이스와 레인징 암호 키를 협상하기 위한 수단을 추가로 포함하고, 레인징 신호는, 기본 포지셔닝 기준 신호, 또는 레인징 암호 키, 또는 선도 파라미터, 또는 이들 중 2개 이상의 조합에 기초하는 수정된 포지셔닝 기준 신호를 포함하고, 선도 파라미터는 타이머, 카운터, 시스템 프레임 수, 슬롯 수, 심볼 수, 또는 이들 중 2개 이상의 임의의 조합을 포함하는, 제1 무선 통신 디바이스.
- [0196] 조항 35. 조항 25에 있어서, 제1 보안 자료를 획득하기 위한 수단은 서비스 확립에 응답하여 제1 보안 자료를 획득하기 위한 수단을 포함하는, 제1 무선 통신 디바이스.
- [0197] 조항 36. 조항 25에 있어서, 제1 보안 자료를 획득하기 위한 수단은 레인징 세션에 합류하는 것에 응답하여 제1 보안 자료를 획득하기 위한 수단을 포함하는, 제1 무선 통신 디바이스.
- [0198] 조항 37. 프로세서 판독가능 명령들을 포함하는 비밀시적 프로세서 판독가능 저장 매체로서, 프로세서 판독가능 명령들은, 제1 무선 통신 디바이스의 프로세서로 하여금,
- [0199] 레인징 암호 키, 또는 하나 이상의 암호 인증서들, 또는 이들의 조합을 포함하는 제1 보안 자료를 획득하게 하도록; 그리고
- [0200] 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제1 부분에 기초하거나, 또는 제2 보안 자료에 기초하거나, 또는 이들의 조합인 레인징 신호를 송신하게 하도록 구성되는, 비밀시적 프로세서 판독가능 저장 매체.
- [0201] 조항 38. 조항 37에 있어서, 제1 보안 자료는 대칭 암호 키인 레인징 암호 키를 포함하고, 레인징 신호는, 기본 포지셔닝 기준 신호 및 레인징 암호 키에 기초하는 수정된 포지셔닝 기준 신호를 포함하는, 비밀시적 프로세서 판독가능 저장 매체.
- [0202] 조항 39. 조항 37에 있어서, 제1 보안 자료는 제1 비대칭 암호 키를 포함하는 제1 암호로 서명된 인증서를 포함하고, 프로세서 판독가능 명령들은, 프로세서로 하여금,
- [0203] 제2 무선 통신 디바이스로, 제1 암호로 서명된 인증서를 송신하게 하도록; 그리고
- [0204] 제2 무선 통신 디바이스로부터, 제2 비대칭 암호 키를 포함하는 제2 암호로 서명된 인증서를 수신하게 하도록 구성된 프로세서 판독가능 명령들을 추가로 포함하고,
- [0205] 프로세서로 하여금, 레인징 신호를 송신하게 하도록 구성된 프로세서 판독가능 명령들은, 프로세서로 하여금, 제1 비대칭 암호 키 및 제2 비대칭 암호 키에 기초하는 대칭 암호 키에 기초하여 암호화된 레인징 신호를 암호화된 유니캐스트 레인징 신호로서 송신하게 하도록 구성된 프로세서 판독가능 명령들을 포함하는, 비밀시적 프로세서 판독가능 저장 매체.
- [0206] 조항 40. 조항 39에 있어서, 프로세서로 하여금, 제1 암호로 서명된 인증서를 송신하게 하도록 구성된 프로세서 판독가능 명령들은, 프로세서로 하여금, 제1 무선 통신 디바이스의 현재 위치가 제1 암호로 서명된 인증서와 연관된 유효성 구역 내에 있는 것에 기초하여 제1 암호로 서명된 인증서를 송신하게 하도록 구성된 프로세서 판독가능 명령들을 포함하는, 비밀시적 프로세서 판독가능 저장 매체.
- [0207] 조항 41. 조항 37에 있어서, 프로세서 판독가능 명령들은, 프로세서로 하여금, 제2 무선 통신 디바이스 또는 네트워크 엔티티로부터, 레인징 암호 키를 수신하게 하도록 구성된 프로세서 판독가능 명령들을 추가로 포함하고, 제2 보안 자료는 레인징 암호 키를 포함하는, 비밀시적 프로세서 판독가능 저장 매체.
- [0208] 조항 42. 조항 37에 있어서, 프로세서 판독가능 명령들은, 프로세서로 하여금, 제2 무선 통신 디바이스로, 제1 보안 자료의 적어도 제2 부분에 기초하는 발견 메시지를 송신하게 하도록 구성된 프로세서 판독가능 명령들을 추가로 포함하는, 비밀시적 프로세서 판독가능 저장 매체.

- [0209] 조항 43. 조항 42에 있어서, 제1 보안 자료의 제1 부분은 제1 보안 자료의 제2 부분과 동일한, 비밀시적 프로세서 판독가능 저장 매체.
- [0210] 조항 44. 조항 37에 있어서, 제1 보안 자료는 레인징 암호 키를 포함하고, 프로세서 판독가능 명령들은, 프로세서로 하여금,
- [0211] 제2 무선 통신 디바이스로, 제2 무선 통신 디바이스가 레인징 암호 키를 위해 네트워크 엔티티에 연락하도록 하는 표시를 송신하게 하도록; 그리고
- [0212] 제1 무선 통신 디바이스에 저장된 기본 암호 키에 기초하여 레인징 암호 키를 결정하게 하도록 구성된 프로세서 판독가능 명령들을 추가로 포함하는, 비밀시적 프로세서 판독가능 저장 매체.
- [0213] 조항 45. 조항 37에 있어서,
- [0214] 제1 보안 자료는, 제1 무선 통신 디바이스 및 제2 무선 통신 디바이스와는 별개인 엔티티에 의해 암호로 서명된 제1 무선 통신 디바이스의 공개 암호 키를 포함하는 복수의 암호로 서명된 인증서들을 포함하고;
- [0215] 프로세서 판독가능 명령들은, 프로세서로 하여금, 제2 무선 통신 디바이스로, 제1 무선 통신 디바이스에 의해 암호로 서명되고 인증서 선택 정책을 기초하여 복수의 암호로 서명된 인증서들 중 적어도 하나를 포함하는 발견 메시지를 송신하게 하도록 구성된 프로세서 판독가능 명령들을 추가로 포함하는, 비밀시적 프로세서 판독가능 저장 매체.
- [0216] 조항 46. 조항 45에 있어서, 프로세서 판독가능 명령들은, 프로세서로 하여금, 그룹 형성 동안 제2 무선 통신 디바이스와 레인징 암호 키를 협상하게 하도록 구성된 프로세서 판독가능 명령들을 추가로 포함하고, 레인징 신호는, 기본 포지셔닝 기준 신호, 또는 레인징 암호 키, 또는 선도 파라미터, 또는 이들 중 2개 이상의 조합에 기초하는 수정된 포지셔닝 기준 신호를 포함하고, 선도 파라미터는 타이머, 카운터, 시스템 프레임 수, 슬롯 수, 심볼 수, 또는 이들 중 2개 이상의 임의의 조합을 포함하는, 비밀시적 프로세서 판독가능 저장 매체.
- [0217] 조항 47. 조항 37에 있어서, 프로세서로 하여금, 제1 보안 자료를 획득하게 하도록 구성된 프로세서 판독가능 명령들은, 프로세서로 하여금, 서비스 확립에 응답하여 제1 보안 자료를 획득하게 하도록 구성된 프로세서 판독가능 명령들을 포함하는, 비밀시적 프로세서 판독가능 저장 매체.
- [0218] 조항 48. 조항 37에 있어서, 프로세서로 하여금, 제1 보안 자료를 획득하게 하도록 구성된 프로세서 판독가능 명령들은, 프로세서로 하여금, 레인징 세션에 합류하는 것에 응답하여 제1 보안 자료를 획득하게 하도록 구성된 프로세서 판독가능 명령들을 포함하는, 비밀시적 프로세서 판독가능 저장 매체.
- [0219] **다른 고려사항들**
- [0220] 다른 예들 및 구현들이 본 개시내용 및 첨부된 청구항들의 범주 내에 있다. 예를 들어, 소프트웨어 및 컴퓨터들의 속성으로 인해, 위에서 설명된 기능들은 프로세서에 의해 실행되는 소프트웨어, 하드웨어, 펌웨어, 하드와이어링, 또는 이들 중 임의의 것의 조합을 사용하여 구현될 수 있다. 기능들을 구현하는 특징들은 또한, 기능들의 일부들이 상이한 물리적 위치들에서 구현되도록 분산되는 것을 포함하여, 다양한 포지션들에 물리적으로 위치될 수 있다.
- [0221] 본 명세서에 사용된 바와 같이, 단수형들 "a", "an" 및 "the"는 문맥상 명백하게 달리 나타내지 않는 한 복수형들도 포함한다. 따라서, 청구항들을 포함하여, 단수형의 디바이스(예컨대, "디바이스(a device)", "디바이스(the device)")에 대한 언급은, 그러한 디바이스들 중 하나 이상을 포함한다(예컨대, "프로세서(a processor)"는 하나 이상의 프로세서들을 포함하고, "프로세서(the processor)"는 하나 이상의 프로세서들을 포함하고, "메모리(a memory)"는 하나 이상의 메모리들을 포함하고, "메모리(the memory)"는 하나 이상의 메모리들을 포함하는 등임). 본 명세서에 사용된 바와 같은 용어들 "포함하다(comprises)", "포함하는(comprising)", "포함하다(includes)" 및/또는 "포함하는(including)"은 명시된 특징들, 정수들, 단계들, 동작들, 엘리먼트들 및/또는 컴포넌트들의 존재를 특정하지만, 하나 이상의 다른 특징들, 정수들, 단계들, 동작들, 엘리먼트들, 컴포넌트들 및/또는 이들의 그룹들의 존재 또는 추가를 배제하지 않는다.
- [0222] 또한, 본 명세서에 사용된 바와 같이, 항목들의 리스트(가능하게는 "~중 적어도 하나"로 시작되거나 또는 "~중 하나 이상"으로 시작됨)에 사용된 바와 같은 "또는"은, 예를 들어, "A, B, 또는 C 중 적어도 하나"의 리스트 또는 "A, B, 또는 C 중 하나 이상"의 리스트 또는 "A 또는 B 또는 C"의 리스트가 A, 또는 B, 또는 C, 또는 AB(A 및 B), 또는 AC(A 및 C), 또는 BC(B 및 C), 또는 ABC(즉, A 및 B 및 C), 또는 하나 초과와 특징과의 조합들(예

컨대, AA, AAB, ABBC 등)을 의미하도록 하는 이접적 리스트를 나타낸다. 따라서, 항목, 예컨대, 프로세서가 A 또는 B 중 적어도 하나에 관한 기능을 수행하도록 구성된다는 언급, 또는 항목이 기능 A 또는 기능 B를 수행하도록 구성된다는 언급은 항목이 A에 관한 기능을 수행하도록 구성될 수 있거나, 또는 B에 관한 기능을 수행하도록 구성될 수 있거나, 또는 A와 B에 관한 기능을 수행하도록 구성될 수 있다는 것을 의미한다. 예를 들어, "A 또는 B 중 적어도 하나를 측정하도록 구성된 프로세서" 또는 "A를 측정하거나 B를 측정하도록 구성된 프로세서"의 어구는 프로세서가 A를 측정하도록 구성될 수 있거나(그리고 B를 측정하도록 구성될 수 있거나 또는 구성되지 않을 수 있음), 또는 B를 측정하도록 구성될 수 있거나(그리고 A를 측정하도록 구성될 수 있거나 또는 구성되지 않을 수 있음), 또는 A를 측정하고 B를 측정하도록 구성될 수 있다(그리고 A와 B 중 어느 것을 측정할지 또는 둘 모두를 측정할지를 선택하도록 구성될 수 있음)는 것을 의미한다. 유사하게, A 또는 B 중 적어도 하나를 측정하기 위한 수단의 언급은 A를 측정하기 위한 수단(이는 B를 측정가능할 수 있거나 또는 측정가능하지 않을 수 있음), 또는 B를 측정하기 위한 수단(그리고 A를 측정하도록 구성될 수 있거나 또는 구성되지 않을 수 있음), 또는 A와 B를 측정하기 위한 수단(이는 A와 B 중 어느 것을 측정할지 또는 둘 모두를 측정할지를 선택가능할 수 있음)을 포함한다. 다른 예로서, 항목, 예컨대, 프로세서가 기능 X를 수행하거나 기능 Y를 수행하는 것 중 적어도 하나를 행하도록 구성된다는 언급은 항목이 기능 X를 수행하도록 구성될 수 있거나, 또는 기능 Y를 수행하도록 구성될 수 있거나, 또는 기능 X를 수행하도록 그리고 기능 Y를 수행하도록 구성될 수 있다는 것을 의미한다. 예를 들어, "X를 측정하거나 Y를 측정하는 것 중 적어도 하나를 행하도록 구성된 프로세서"의 어구는 프로세서가 X를 측정하도록 구성될 수 있거나(그리고 Y를 측정하도록 구성될 수 있거나 또는 구성되지 않을 수 있음), 또는 Y를 측정하도록 구성될 수 있거나(그리고 X를 측정하도록 구성될 수 있거나 또는 구성되지 않을 수 있음), 또는 X를 측정하도록 그리고 Y를 측정하도록 구성될 수 있다(그리고 X와 Y 중 어느 것을 측정할지 또는 둘 모두를 측정할지를 선택하도록 구성될 수 있음)는 것을 의미한다.

[0223] 본 명세서에 사용된 바와 같이, 달리 언급되지 않는 한, 기능 또는 동작이 항목 또는 조건"에 기초한다"는 설명은, 기능 또는 동작이 명시된 항목 또는 조건에 기초하고, 명시된 항목 또는 조건에 더하여 하나 이상의 항목들 및/또는 조건들에 기초할 수 있다는 것을 의미한다.

[0224] 특정 요건들에 따라 상당한 변형들이 이루어질 수 있다. 예를 들어, 맞춤형 하드웨어가 또한 사용될 수 있고, 그리고/또는 특정 엘리먼트들이 하드웨어, 프로세서에 의해 실행되는 소프트웨어(휴대용 소프트웨어, 이를테면, 애플릿들 등을 포함함) 또는 둘 모두로 구현될 수 있다. 또한, 네트워크 입력/출력 디바이스들과 같은 다른 컴퓨팅 디바이스들에 대한 연결이 채용될 수 있다. 서로 연결되거나 통신하는 것으로 도면들에 도시되고/되거나 본 명세서에 논의된, 기능적인 또는 다른 방식의 컴포넌트들은, 달리 언급되지 않는 한 통신가능하게 커플링된다. 즉, 그들은 직접 또는 간접적으로 연결되어 그들 간의 통신을 가능하게 할 수 있다.

[0225] 위에서 논의된 시스템들 및 디바이스들은 예들이다. 다양한 구성들은 다양한 절차들 또는 컴포넌트들을 적절하게 생략, 대체, 또는 추가할 수 있다. 예를 들어, 특정 구성들과 관련하여 설명된 특징들은 다양한 다른 구성들에서 조합될 수 있다. 구성들의 상이한 양태들 및 엘리먼트들은 유사한 방식으로 조합될 수 있다. 또한, 기술이 진화하며, 따라서 많은 엘리먼트들은 예들이며 본 개시내용 또는 청구항들의 범주를 제한하지 않는다.

[0226] 무선 통신 시스템은, 통신들이 무선 통신 디바이스들 사이에서, 무선으로, 즉, 유선 또는 다른 물리적 연결을 통하기보다는 대기 공간을 통해 전파되는 전자기와 및/또는 음파에 의해 전달되는 시스템이다. 무선 통신 시스템(무선 통신 시스템(wireless communications system), 무선 통신 네트워크(wireless communication network), 또는 무선 통신 네트워크(wireless communications network)라고도 불림)은 모든 통신들이 무선으로 송신되게 하는 것은 아닐 수 있지만, 적어도 일부 통신들이 무선으로 송신되게 하도록 구성된다. 또한, 용어 "무선 통신 디바이스" 또는 유사한 용어는 디바이스의 기능이 배타적으로 또는 심지어 주로, 통신을 위한 것이거나, 또는 무선 통신 디바이스를 사용한 통신이 배타적으로 또는 심지어 주로, 무선이거나, 또는 디바이스가 모바일 디바이스일 것을 요구하는 것이 아니라, 디바이스가 무선 통신 능력(단방향 또는 양방향)을 포함하는 것, 예컨대, 무선 통신을 위한 적어도 하나의 라디오(각각의 라디오는 송신기, 수신기, 또는 트랜시버의 일부임)를 포함하는 것을 표시한다. UE는 모바일 무선 통신 디바이스이고, 용어 "UE"는 본 명세서에서의 설명을 넘어서는 특정 형태의 모바일 무선 통신 디바이스를 요구하지 않는다. 용어 "모바일"은 모바일 무선 통신 디바이스가 움직이고 있을 것을 요구하지 않는다. 모바일 무선 통신 디바이스는 이동성, 예컨대, 태블릿 컴퓨터 또는 스마트폰인 것과 같이, 경량이고 운반하기 적합한 크기인 것으로 구성되지만, 모바일 무선 통신 디바이스는 이러한 형태들의 디바이스들로 제한되지 않는다.

[0227] 예시적인 구성들(구현들을 포함함)의 철저한 이해를 제공하기 위해 설명에서 특정 세부사항들이 제공된다. 그러나, 구성들은 이러한 특정 세부사항들 없이 실시될 수 있다. 예를 들어, 구성들을 모호하게 하는 것을 회피

하기 위해 잘 알려진 회로들, 프로세스들, 알고리즘들, 구조들, 및 기법들은 불필요한 세부사항 없이 도시되었다. 본 명세서에서의 설명은 예시적인 구성들을 제공하며, 청구항들의 범주, 적용가능성, 또는 구성들을 제한하지 않는다. 오히려, 구성들의 이전 설명은 설명된 기법들을 구현하기 위한 설명을 제공한다. 엘리먼트들의 기능과 배열에 있어서 다양한 변경들이 이루어질 수 있다.

[0228] 본 명세서에 사용된 바와 같은 용어들 "프로세서 관독가능 매체", "머신 관독가능 매체" 및 "컴퓨터 관독가능 매체"는 머신으로 하여금 특정 방식으로 동작하게 하는 데이터를 제공하는 데 참여하는 임의의 매체를 지칭한다. 컴퓨팅 플랫폼을 사용하면, 다양한 프로세서 관독가능 매체들은 실행을 위해 프로세서(들)에 명령들/코드를 제공하는 것에 연루될 수 있고 그리고/또는 그러한 명령들/코드를 (예컨대, 신호들로서) 저장 및/또는 반송하는 데 사용될 수 있다. 많은 구현들에서, 프로세서 관독가능 매체는 물리적 및/또는 유형의(tangible) 저장 매체이다. 그러한 매체는, 비휘발성 매체들 및 휘발성 매체들을 포함하지만 이들로 제한되지 않는 많은 형태들을 취할 수 있다. 비휘발성 매체들은 예를 들어, 광 및/또는 자기 디스크들을 포함한다. 휘발성 매체들은, 제한 없이, 동적 메모리를 포함한다.

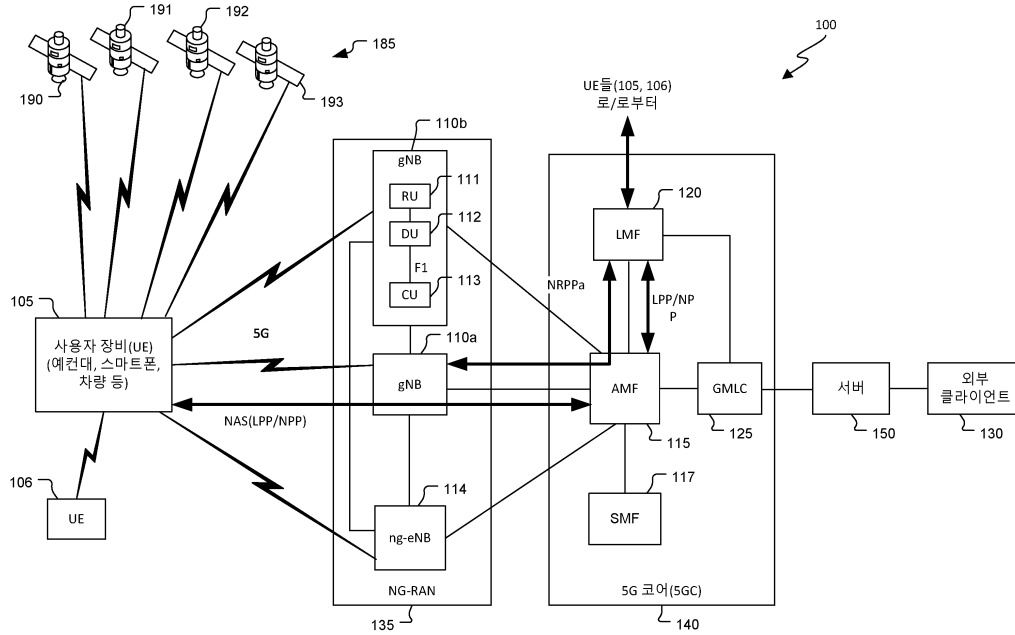
[0229] 여러 예시적인 구성들을 설명했지만, 다양한 수정들, 대안적인 구성들, 및 등가물들이 사용될 수 있다. 예를 들어, 위의 엘리먼트들은 더 큰 시스템의 컴포넌트들일 수 있으며, 여기서 다른 규칙들이 본 개시내용의 적용에 우선할 수 있거나 또는 달리 그 적용을 수정할 수 있다. 또한, 위의 엘리먼트들이 고려되기 이전, 동안, 또는 이후 다수의 동작들이 착수될 수 있다. 따라서, 위의 설명은 청구항들의 범주를 제한하지 않는다.

[0230] 달리 나타내지 않는 한, 양, 시간적 지속기간 등과 같은 측정가능 값을 언급할 때 본 명세서에 사용된 바와 같은 "약" 및/또는 "대략"은 본 명세서에 설명된 시스템들, 디바이스들, 회로들, 방법들, 및 다른 구현들의 맥락에서 적절하게 특정된 값으로부터 $\pm 20\%$ 또는 $\pm 10\%$, $\pm 5\%$, 또는 $+0.1\%$ 의 변동들을 포괄한다. 달리 나타내지 않는 한, 양, 시간적 지속기간, (주파수와 같은) 물리적 속성 등과 같은 측정가능 값을 언급할 때 본 명세서에 사용된 바와 같은 "실질적으로"는 또한, 본 명세서에 설명된 시스템들, 디바이스들, 회로들, 방법들, 및 다른 구현들의 맥락에서 적절하게 특정된 값으로부터 $\pm 20\%$ 또는 $\pm 10\%$, $\pm 5\%$, 또는 $+0.1\%$ 의 변동들을 포괄한다.

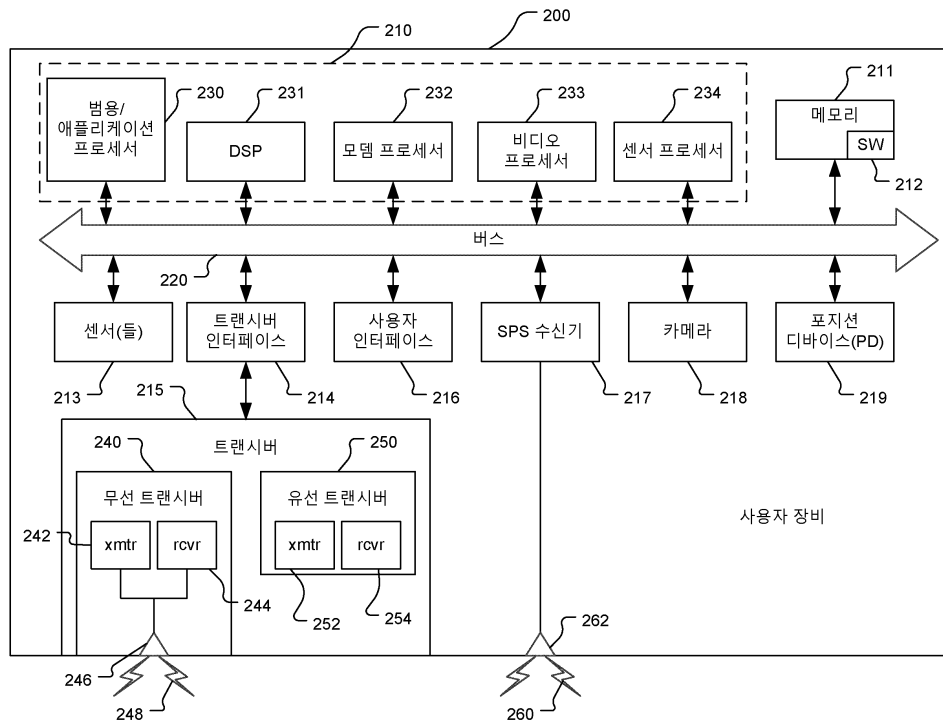
[0231] 값이 제1 임계 값을 초과한다는 (또는 그보다 많거나 위라는) 설명은 값이 제1 임계 값보다 약간 더 큰 제2 임계 값을 충족하거나 초과한다는 설명과 동일하고, 예컨대, 제2 임계 값은 컴퓨팅 시스템의 분해능에서 제1 임계 값보다 더 높은 하나의 값이다. 값이 제1 임계 값보다 작다는 (또는 그 이내이거나 아래라는) 설명은 값이 제1 임계 값보다 약간 더 낮은 제2 임계 값 이하라는 설명과 동일하고, 예컨대, 제2 임계 값은 컴퓨팅 시스템의 분해능에서 제1 임계 값보다 더 낮은 하나의 값이다.

도면

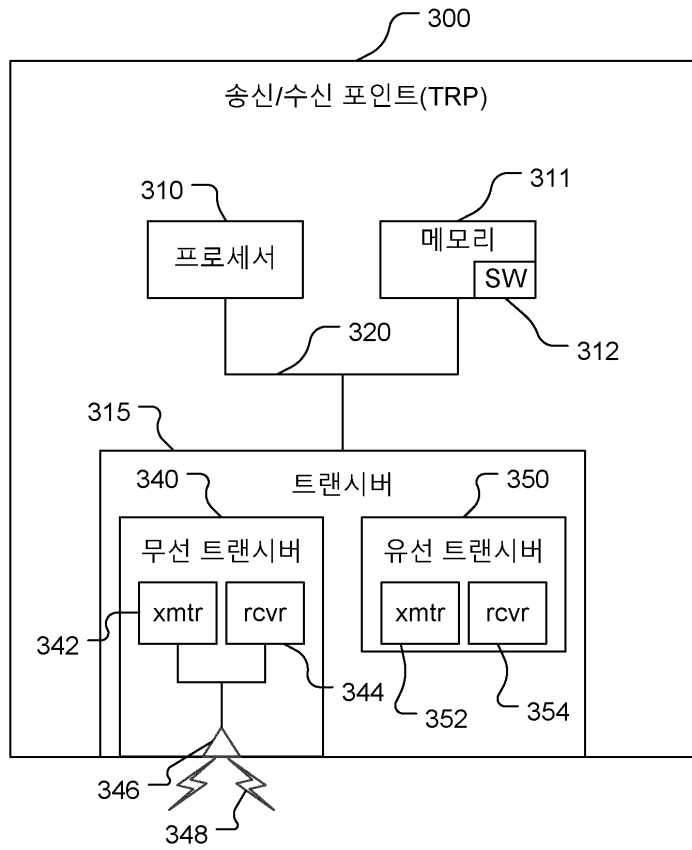
도면1



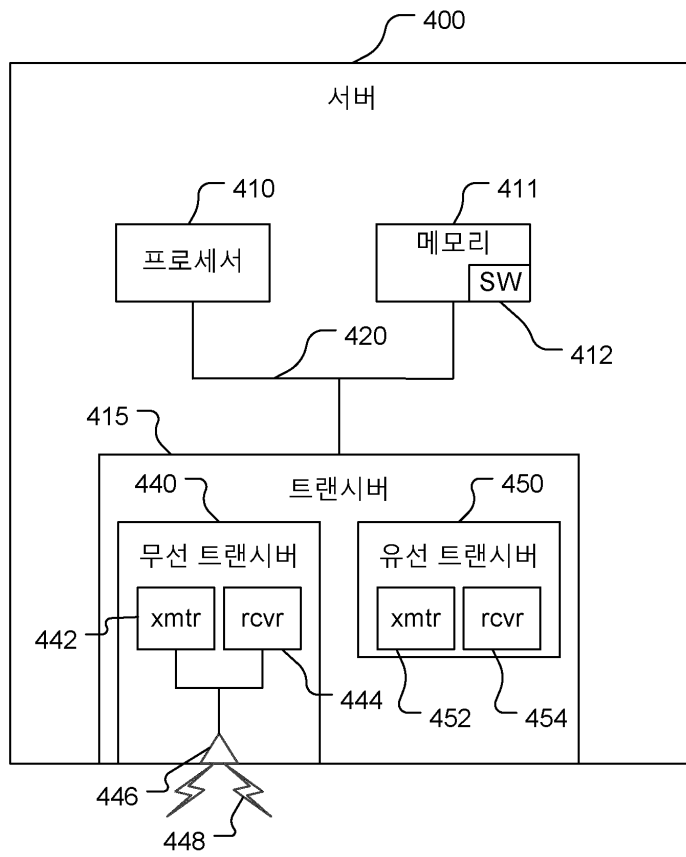
도면2



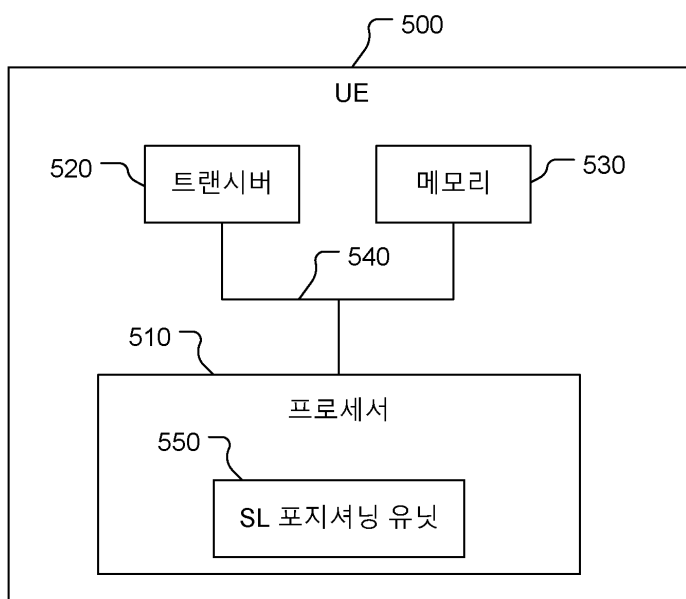
도면3



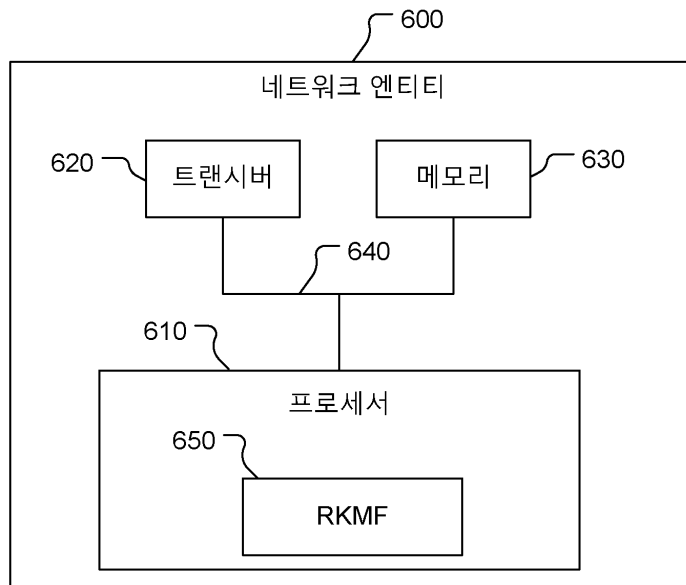
도면4



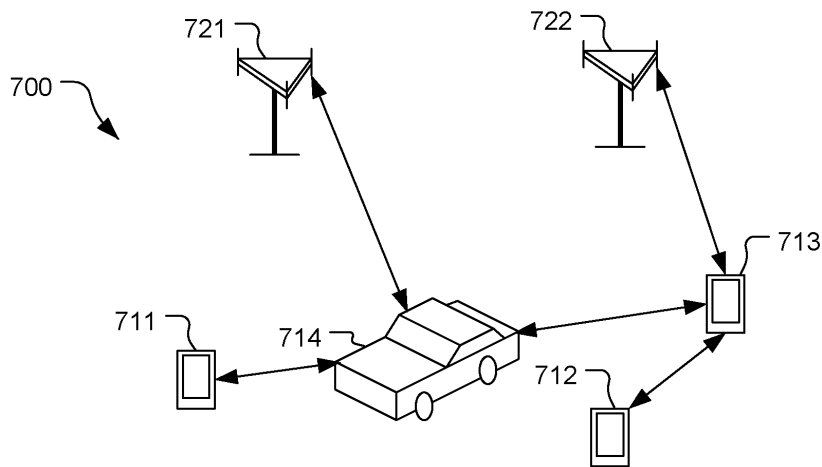
도면5



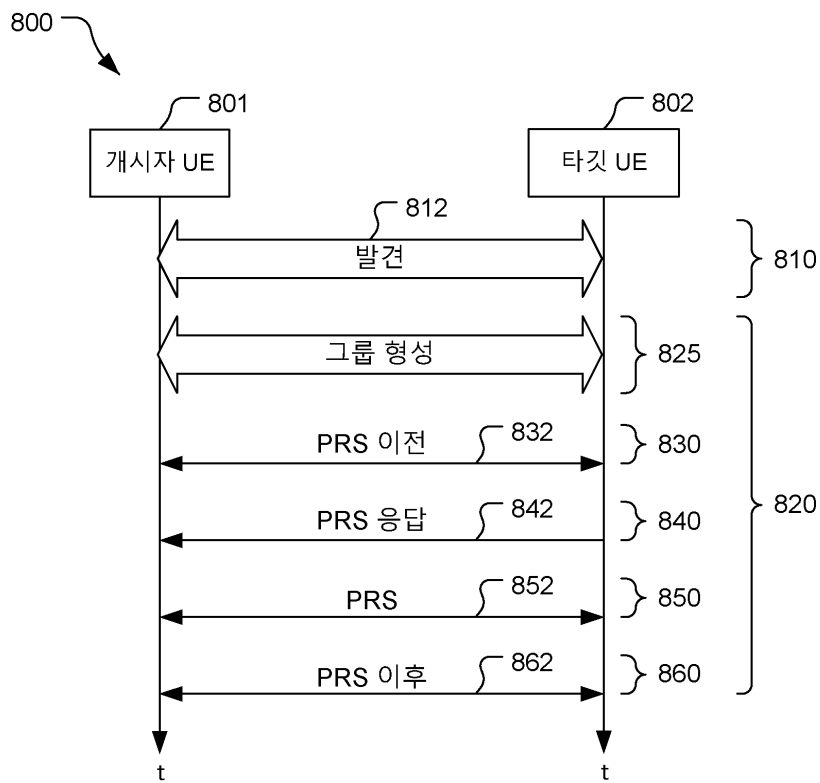
도면6



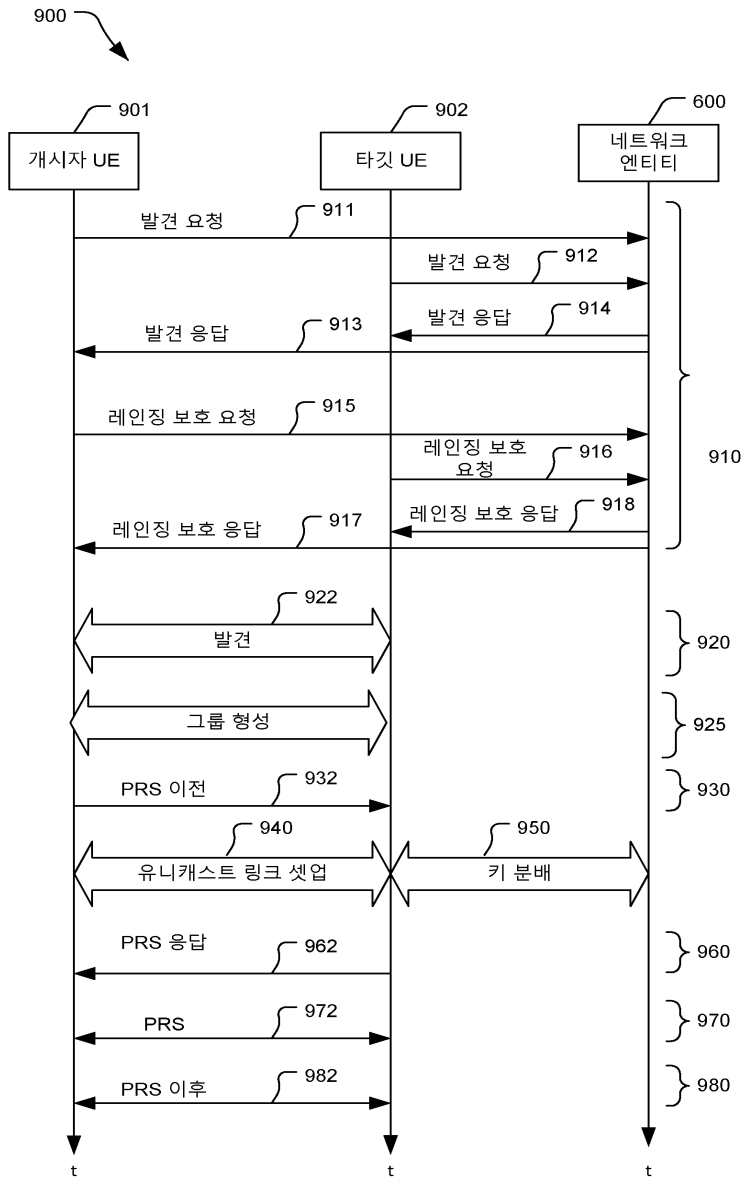
도면7



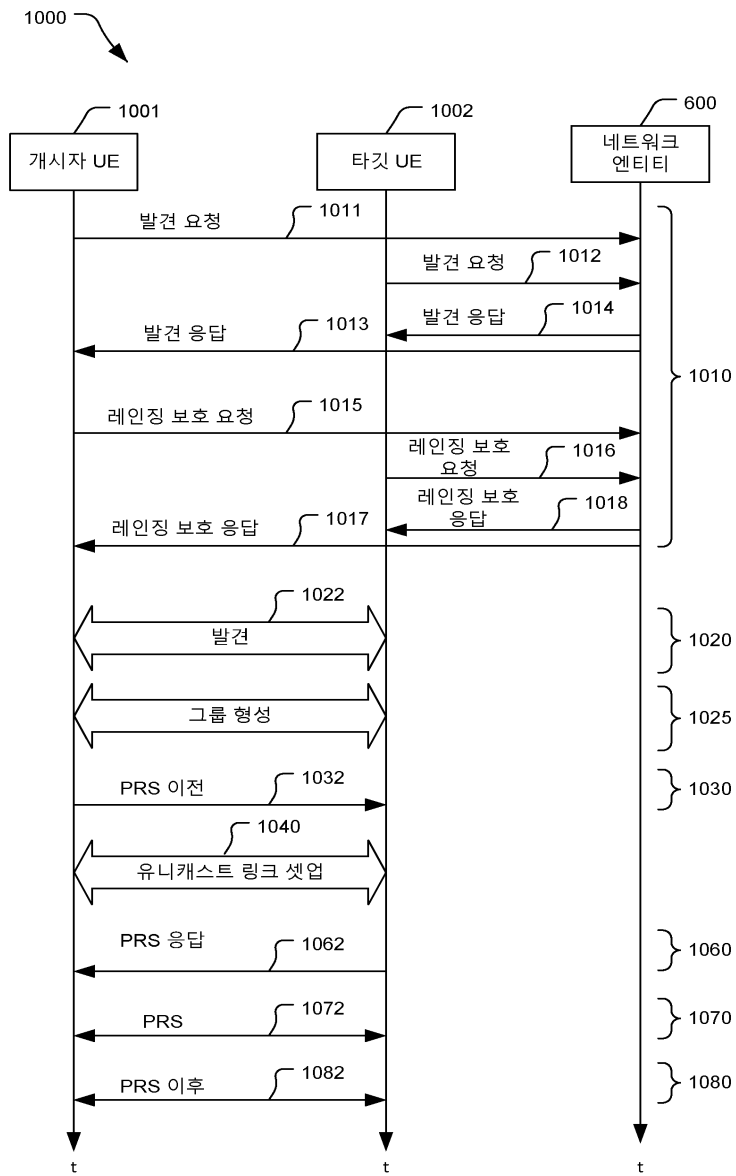
도면8



도면9



도면10



도면11

