(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0011690
(43) 공개일자 2024년01월26일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *H04L 67/12* (2022.01)
(52) CPC특허분류
H04L 63/14 (2013.01)
H04L 63/1441 (2013.01)
(21) 출원번호 10-2023-7039062
(22) 출원일자(국제) 2022년03월30일
심사청구일자 없음
(85) 번역문제출일자 2023년11월13일
(86) 국제출원번호 PCT/US2022/022624
(87) 국제공개번호 WO 2022/245432
국제공개일자 2022년11월24일
(30) 우선권주장
17/327,429 2021년05월21일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
다스, 소우먀
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
네쿠이, 모하마드
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
특허법인 남앤남

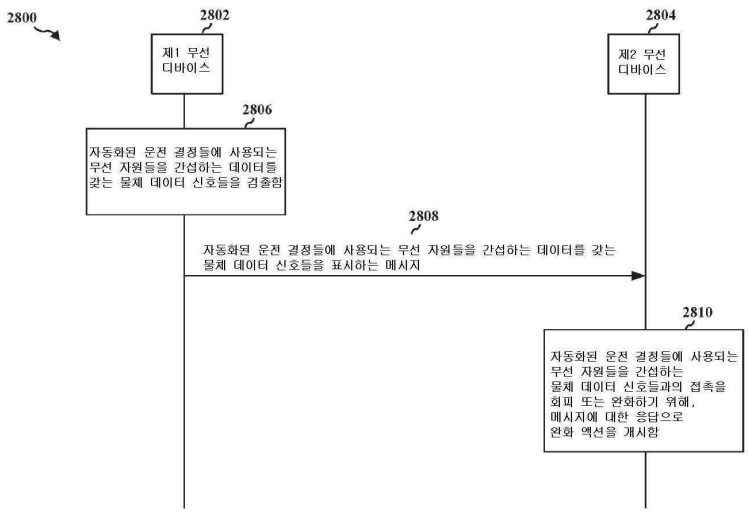
전체 청구항 수 : 총 40 항

(54) 발명의 명칭 **센서 공유를 사용한 협력적 조기 위협 검출**

(57) 요 약

협력적 조기 위협 검출을 위한 방법 및 장치. 일부 양상들에서, 장치는 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 검출한다. 장치는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 적어도 제2 무선 디바이스에 송신한다. 하나 이상의 물체 데이터 신호들은 오작동 무선 디바이스에 대응할 수 있다. 오작동 무선 디바이스의 데이터는 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 타당하지 않은 데이터를 포함할 수 있다.

대 표 도



(52) CPC특허분류
H04L 63/1458 (2013.01)
H04L 67/12 (2022.05)
H04L 2209/84 (2013.01)
(72) 발명자
바실로브스키, 댄
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
수만, 모하메드 아타우르 라만
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
마쉬에, 씬 빈센트
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

명 세 서

청구범위

청구항 1

제1 무선 디바이스에서의 무선 통신을 위한 장치로서,

메모리;

적어도 하나의 트랜시버; 및

상기 메모리 및 상기 적어도 하나의 트랜시버에 통신가능하게 접속된 적어도 하나의 프로세서를 포함하고,

상기 적어도 하나의 프로세서는,

자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 검출하고; 그리고

자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 상기 데이터를 갖는 상기 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 적어도 제2 무선 디바이스에 송신하도록 구성되는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 2

제1 항에 있어서,

상기 하나 이상의 물체 데이터 신호들은 오작동 무선 디바이스에 대응하고, 상기 오작동 무선 디바이스의 데이터는 상기 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 타당하지 않은 데이터를 포함하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 3

제2 항에 있어서,

상기 오작동 무선 디바이스의 상기 적어도 하나의 특성과 관련된 상기 타당하지 않은 데이터는 위치, 속력 또는 진로 또는 이들의 조합 중 적어도 하나를 포함하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 4

제2 항에 있어서,

상기 오작동 무선 디바이스는 오작동 차량을 포함하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 5

제1 항에 있어서,

상기 하나 이상의 물체 데이터 신호들은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물에 대응하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 6

제5 항에 있어서,

상기 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 상기 장애물의 상기 하나 이상의 물체 데이터 신호들은 RSSI(reference signal strength indicator) 임계치보다 큰 RSSI를 갖고 송신되는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 7

제5 항에 있어서,

상기 하나 이상의 물체 데이터 신호들은 DoS(denial of service) 공격자, 재머, 또는 OOB(out of band) 간섭자를 포함하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 8

제1 항에 있어서,

상기 메시지는 검출된 상기 하나 이상의 물체 데이터 신호들에 대응하는 적어도 하나의 IE(information element)를 추가로 표시하고, 상기 적어도 하나의 IE는 검출된 오작동 무선 디바이스, DoS(denial of service) 공격자, 검출된 재머 또는 검출된 OOB 간섭자 또는 이들의 조합 중 적어도 하나의 검출된 특성들을 포함하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 9

제8 항에 있어서,

상기 적어도 하나의 IE는 검출된 물체들의 클래스들을 포함하고, 검출된 물체들의 각각의 클래스는 상기 검출된 오작동 무선 디바이스, 상기 DoS(denial of service) 공격자, 상기 검출된 재머 및 상기 검출된 OOB 간섭자 중 개개의 하나에 대한 검출된 특성들을 포함하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 10

제1 항에 있어서,

상기 메시지는 협력적 또는 자동화된 운전 결정들을 방해하는 상기 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해 적어도 상기 제2 무선 디바이스에서 완화 액션을 트리거링하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 11

제1 항에 있어서,

상기 메시지는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 상기 데이터를 갖는 상기 하나 이상의 물체 데이터 신호들을 송신하고 있는 물체를 식별하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 12

제11 항에 있어서,

상기 물체는 VRU(vulnerable road user), 검출된 차량 또는 무선 장애물 중 하나를 포함하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 13

제1 항에 있어서,

상기 제2 무선 디바이스는 무선 차량, RSU(roadside unit) 또는 VRU(vulnerable road user) 중 적어도 하나를 포함하는, 제1 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 14

제1 무선 디바이스의 무선 통신 방법으로서,

자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 검출하는 단계; 및

자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 상기 데이터를 갖는 상기 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 적어도 제2 무선 디바이스에 송신하는 단계를 포함하는, 제1 무선 디바이스의 무선 통신 방법.

청구항 15

제14 항에 있어서,

상기 하나 이상의 물체 데이터 신호들은 오작동 무선 디바이스에 대응하고, 상기 오작동 무선 디바이스의 데이터는 상기 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 타당하지 않은 데이터를 포함하는, 제1 무선 디바이스의 무선 통신 방법.

청구항 16

제14 항에 있어서,

상기 하나 이상의 물체 데이터 신호들은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물에 대응하는, 제1 무선 디바이스의 무선 통신 방법.

청구항 17

제16 항에 있어서,

상기 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 상기 장애물의 상기 하나 이상의 물체 데이터 신호들은 RSSI(reference signal strength indicator) 임계치보다 큰 RSSI를 갖고 송신되는, 제1 무선 디바이스의 무선 통신 방법.

청구항 18

제14 항에 있어서,

상기 메시지는 검출된 상기 하나 이상의 물체 데이터 신호들에 대응하는 적어도 하나의 IE(information element)를 추가로 표시하고, 상기 적어도 하나의 IE는 검출된 오작동 무선 디바이스, DoS(denial of service) 공격자, 검출된 재머 또는 검출된 간섭자 또는 이들의 조합 중 적어도 하나의 검출된 특성들을 포함하는, 제1 무선 디바이스의 무선 통신 방법.

청구항 19

제14 항에 있어서,

상기 메시지는 협력적 또는 자동화된 운전 결정들을 방해하는 상기 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해 적어도 상기 제2 무선 디바이스에서 완화 액션을 트리거링하는, 제1 무선 디바이스의 무선 통신 방법.

청구항 20

제14 항에 있어서,

상기 메시지는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 상기 데이터를 갖는 상기 하나 이상의 물체 데이터 신호들을 송신하고 있는 물체를 식별하는, 제1 무선 디바이스의 무선 통신 방법.

청구항 21

제2 무선 디바이스에서의 무선 통신을 위한 장치로서,

메모리;

적어도 하나의 트랜시버; 및

상기 메모리 및 상기 적어도 하나의 트랜시버에 통신가능하게 접속된 적어도 하나의 프로세서를 포함하고,

상기 적어도 하나의 프로세서는,

자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 수신하고; 그리고

자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 상기 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해, 상기 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시하도록 구성되는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 22

제21 항에 있어서,

상기 하나 이상의 물체 데이터 신호들은 오작동 무선 디바이스에 대응하고, 상기 오작동 무선 디바이스의 데이터는 상기 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 타당하지 않은 데이터를 포함하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 23

제22 항에 있어서,

상기 오작동 무선 디바이스의 상기 적어도 하나의 특성과 관련된 상기 타당하지 않은 데이터는 위치, 속력 또는 진로 또는 이들의 조합 중 적어도 하나를 포함하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 24

제22 항에 있어서,

상기 오작동 무선 디바이스는 오작동 차량을 포함하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 25

제21 항에 있어서,

상기 하나 이상의 물체 데이터 신호들은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물에 대응하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 26

제25 항에 있어서,

상기 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 상기 장애물의 상기 하나 이상의 물체 데이터 신호들은 RSSI(reference signal strength indicator) 임계치보다 큰 RSSI를 갖고 송신되는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 27

제25 항에 있어서,

상기 하나 이상의 물체 데이터 신호들은 DoS(denial of service) 공격자, 재머, 또는 OOB(out of band) 간섭자를 포함하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 28

제21 항에 있어서,

상기 메시지는 검출된 상기 하나 이상의 물체 데이터 신호들에 대응하는 적어도 하나의 IE(information element)를 추가로 표시하고, 상기 적어도 하나의 IE는 검출된 오작동 무선 디바이스, DoS(denial of service) 공격자, 검출된 재머 또는 검출된 OOB 간섭자 또는 이들의 조합 중 적어도 하나의 검출된 특성들을 포함하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 29

제28 항에 있어서,

상기 적어도 하나의 IE는 검출된 물체들의 클래스들을 포함하고, 검출된 물체들의 각각의 클래스는 상기 검출된 오작동 무선 디바이스, 상기 DoS(denial of service) 공격자, 상기 검출된 재머 및 상기 검출된 OOB 간섭자 중 개개의 하나에 대한 검출된 특성들을 포함하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 30

제21 항에 있어서,

상기 메시지는 협력적 또는 자동화된 운전 결정들을 방해하는 상기 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해 적어도 상기 제2 무선 디바이스에서 완화 액션을 트리거링하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 31

제21 항에 있어서,

상기 메시지는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 상기 데이터를 갖는 상기 하나 이상의 물체 데이터 신호들을 송신하고 있는 물체를 식별하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 32

제31 항에 있어서,

상기 물체는 VRU(vulnerable road user), 검출된 차량 또는 무선 장애물 중 하나를 포함하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 33

제31 항에 있어서,

상기 제2 무선 디바이스는 무선 차량, RSU(roadside unit) 또는 VRU(vulnerable road user) 중 적어도 하나를 포함하는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 34

제31 항에 있어서,

상기 메시지는 제1 무선 디바이스로부터 또는 RSU(roadside unit)로부터 수신되는, 제2 무선 디바이스에서의 무선 통신을 위한 장치.

청구항 35

제2 무선 디바이스의 무선 통신 방법으로서,

자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 수신하는 단계; 및

자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 상기 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해, 상기 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시하는 단계를 포함하는, 제2 무선 디바이스의 무선 통신 방법.

청구항 36

제35 항에 있어서,

상기 하나 이상의 물체 데이터 신호들은 오작동 무선 디바이스에 대응하고, 상기 오작동 무선 디바이스의 데이터는 상기 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 타당하지 않은 데이터를 포함하는, 제2 무선 디바이스의 무선 통신 방법.

청구항 37

제35 항에 있어서,

상기 하나 이상의 물체 데이터 신호들은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물에 대응하는, 제2 무선 디바이스의 무선 통신 방법.

청구항 38

제37 항에 있어서,

상기 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 상기 장애물의 상기 하나 이상의 물체 데이터 신호들은 RSSI(reference signal strength indicator) 임계치보다 큰 RSSI를 갖고 송신되는, 제2 무선 디바이스의 무선 통신 방법.

청구항 39

제35 항에 있어서,

상기 메시지는 검출된 상기 하나 이상의 물체 데이터 신호들에 대응하는 적어도 하나의 IE(information element)를 추가로 표시하고, 상기 적어도 하나의 IE는 검출된 오작동 무선 디바이스, DoS(denial of service) 공격자, 검출된 재머 또는 검출된 OOB 간섭자 또는 이들의 조합 중 적어도 하나의 검출된 특성들을 포함하는, 제2 무선 디바이스의 무선 통신 방법.

청구항 40

제35 항에 있어서,

상기 메시지는 협력적 또는 자동화된 운전 결정들을 방해하는 상기 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해 적어도 상기 제2 무선 디바이스에서 완화 액션을 트리거링하는, 제2 무선 디바이스의 무선 통신 방법.

발명의 설명

기 술 분 야

[0001] [0001] 본 출원은, 2021년 5월 21일에 출원되고 발명의 명칭이 "COOPERATIVE EARLY THREAT DETECTION USING SENSOR SHARING"인 미국 정규 특허 출원 일련번호 제17/327,429호의 이익을 주장하며, 상기 출원은 그 전체가 인용에 의해 본원에 명백히 통합된다.

[0002] [0002] 본 개시는 일반적으로 통신 시스템들에 관한 것이고, 더 상세하게는 협력적 조기 위협 검출을 위한 구성에 관한 것이다.

배 경 기 술

[0003] [0003] 무선 통신 시스템들은 텔레포니(telephony), 비디오, 데이터, 메시징, 및 브로드캐스트들과 같은 다양한 전기통신 서비스들을 제공하도록 널리 배치되어 있다. 통상적인 무선 통신 시스템들은 이용가능한 시스템 자원들을 공유함으로써 다수의 사용자들과의 통신을 지원할 수 있는 다중-액세스 기술들을 이용할 수 있다. 이러한 다중-액세스 기술들의 예들은 CDMA(code division multiple access) 시스템들, TDMA(time division multiple access) 시스템들, FDMA(frequency division multiple access) 시스템들, OFDMA(orthogonal frequency division multiple access) 시스템들, SC-FDMA(single-carrier frequency division multiple access) 시스템들, 및 TD-SCDMA(time division synchronous code division multiple access) 시스템들을 포함한다.

[0004] [0004] 이러한 다중 액세스 기술들은 상이한 무선 디바이스들이, 도시 레벨, 국가 레벨, 지역 레벨, 및 심지어 글로벌 레벨로 통신할 수 있게 하는 공통 프로토콜을 제공하기 위해 다양한 전기통신 표준들에서 채택되어 왔다. 예시적인 전기통신 표준은 5G NR(New Radio)이다. 5G NR은 레이턴시, 신뢰도, 보안, (예를 들어, IoT(Internet of Things)에 의한) 확장가능성 및 다른 요건들과 연관된 새로운 요건들을 충족시키기 위해, 3GPP(Third Generation Partnership Project)에 의해 공표된 연속적인 모바일 브로드밴드 에볼루션의 일부이다. 5G NR은 eMBB(enhanced mobile broadband), mMTC(massive machine type communications) 및 URLLC(ultra reliable low latency communications)와 연관된 서비스들을 포함한다. 5G NR의 일부 양상들은 4G LTE(Long Term Evolution) 표준에 기초할 수 있다. 무선 통신의 양상들은 V2X, V2V 및/또는 D2D 통신에서와 같이 디바이스들 사이의 직접 통신을 포함할 수 있다. V2X, V2V 및/또는 D2D 기술에서의 추가적인 개선들에 대한 요구가 존재한다. 이러한 개선들은 또한 다른 다중-액세스 기술들 및 이러한 기술들을 이용하는 전기통신 표준들에 적용가능할 수 있다.

발명의 내용

[0005] [0005] 다음은, 이러한 양상들의 기본적인 이해를 제공하기 위해 하나 이상의 양상들의 간략화된 요약을 제시한

다. 이러한 요약은 모든 고려된 양상들의 포괄적인 개관이 아니며, 모든 양상들의 핵심적인 또는 중요한 엘리먼트들을 식별하거나 임의의 또는 모든 양상들의 범위를 서술하도록 의도되지 않는다. 이러한 요약의 유일한 목적은, 이후에 제시되는 더 상세한 설명에 대한 서론으로서 간략화된 형태로 하나 이상의 양상들의 일부 개념들을 제시하는 것이다.

[0006] [0006] 본 개시의 양상에서, 방법, 컴퓨터 판독가능 매체 및 장치가 제공된다. 장치는 제1 무선 디바이스에서의 디바이스일 수 있다. 디바이스는 제1 무선 디바이스의 프로세서 및/또는 모뎀 또는 제1 무선 디바이스 그 자체일 수 있다. 장치는 BSM(basic safety message)들의 송신을 간섭하는 데이터를 송신하는 위협 엔티티를 검출한다. 장치는 위협 엔티티의 타입과 관련된 정보를 표시하는 메시지를 제2 무선 디바이스에 송신한다.

[0007] [0007] 본 개시의 양상에서, 방법, 컴퓨터 판독가능 매체 및 장치가 제공된다. 장치는 제2 무선 디바이스에서의 디바이스일 수 있다. 디바이스는 제2 무선 디바이스의 프로세서 및/또는 모뎀 또는 제2 무선 디바이스 그 자체일 수 있다. 장치는 제1 무선 디바이스로부터 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신하고, 위협 엔티티는 BSM(basic safety message)들의 송신을 간섭하는 데이터를 송신한다. 장치는 제1 무선 디바이스로부터 위협 엔티티와 관련된 정보를 표시하는 메시지에 적어도 부분적으로 기초하여 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정한다. 장치는 결정된 후보 자원 상에서 BSM을 적어도 제3 무선 디바이스에 송신한다.

[0008] [0008] 본 개시의 양상에서, 방법, 컴퓨터 판독가능 매체 및 장치가 제공된다. 장치는 제1 무선 디바이스에서의 디바이스일 수 있다. 디바이스는 제1 무선 디바이스의 프로세서 및/또는 모뎀 또는 제1 무선 디바이스 그 자체일 수 있다. 장치는 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 구역 내의 위협 엔티티를 검출하고, 위협 엔티티는 협력적 또는 자동 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해한다. 장치는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 적어도 하나의 제2 무선 디바이스에 송신한다.

[0009] [0009] 본 개시의 양상에서, 방법, 컴퓨터 판독가능 매체 및 장치가 제공된다. 장치는 제2 무선 디바이스에서의 디바이스일 수 있다. 디바이스는 제2 무선 디바이스의 프로세서 및/또는 모뎀 또는 제2 무선 디바이스 그 자체일 수 있다. 장치는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신하고, 위협 엔티티는 협력적 또는 자동 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해한다. 장치는 위협 엔티티와의 접촉을 회피 또는 완화하기 위해 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시한다.

[0010] [0010] 본 개시의 양상에서, 방법, 컴퓨터 판독가능 매체 및 장치가 제공된다. 장치는 제1 무선 디바이스에서의 디바이스일 수 있다. 디바이스는 제1 무선 디바이스의 프로세서 및/또는 모뎀 또는 제1 무선 디바이스 그 자체일 수 있다. 장치는 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 검출한다. 장치는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 적어도 제2 무선 디바이스에 송신한다.

[0011] [0011] 본 개시의 양상에서, 방법, 컴퓨터 판독가능 매체 및 장치가 제공된다. 장치는 제2 무선 디바이스에서의 디바이스일 수 있다. 디바이스는 제2 무선 디바이스의 프로세서 및/또는 모뎀 또는 제2 무선 디바이스 그 자체일 수 있다. 장치는, 제1 무선 디바이스로부터, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 수신한다. 장치는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해, 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시한다.

[0012] [0012] 상술한 목적 및 관련되는 목적의 달성을 위해서, 하나 이상의 양상들은, 아래에서 완전히 설명되고 특히 청구항들에서 언급되는 특징들을 포함한다. 하기 설명 및 부가된 도면들은 하나 이상의 양상들의 특정한 예시적인 특징들을 상세히 기술한다. 그러나, 이 특징들은, 다양한 양상들의 원리들이 사용될 수 있는 다양한 방식들 중 일부만을 나타내고, 이 설명은 모든 이러한 양상들 및 이들의 균등물들을 포함하는 것으로 의도된다.

도면의 간단한 설명

[0013] [0013] 도 1은 무선 통신 시스템 및 액세스 네트워크의 예를 예시하는 도면이다.

[0014] [0014] 도 2는 사이드링크 슬롯 구조의 예시적인 양상들을 예시한다.

[0015] [0015] 도 3은 예컨대, V2V, V2X 및/또는 디바이스-투-디바이스 통신에 기초한 무선 통신에 수반되는 제1 디바이스 및 제2 디바이스의 예를 예시하는 도면이다.

[0016] 도 4는 예컨대, 사이드링크 통신에 기초한 무선 통신에 수반되는 디바이스들의 예를 예시하는 도면이다.

[0017] 도 5a 내지 도 5d는 협력적 및 자동화된 운전 시스템들을 위한 센서-공유의 예들을 예시하는 도면들이다.

[0018] 도 6은 협력적 및 자동화된 운전 시스템들을 위한 센서-공유의 예를 예시하는 도면이다.

[0019] 도 7은 협력적 및 자동화된 운전 시스템들을 위한 센서-공유의 예를 예시하는 도면이다.

[0020] 도 8은 위협 엔티티의 검출의 예를 예시하는 도면이다.

[0021] 도 9는 위협 엔티티의 검출의 예를 예시하는 도면이다.

[0022] 도 10a 및 도 10b는 위협 엔티티의 검출 및 보고의 예를 예시하는 도면들이다.

[0023] 도 11은 센서 데이터 공유 메시지 구조의 예를 예시하는 도면이다.

[0024] 도 12는 센서 데이터 공유 메시지 구조의 예를 예시하는 도면이다.

[0025] 도 13은 센서 데이터 공유 메시지에서 검출된 물체들에 대한 정보 엘리먼트들의 예를 예시하는 도면이다.

[0026] 도 14는 센서 데이터 공유 메시지들에서 검출된 물체들에 대한 파라미터들의 예를 예시하는 도면이다.

[0027] 도 15는 제1 무선 디바이스, 제2 무선 디바이스 및 제3 무선 디바이스 사이의 시그널링의 호출 흐름도이다.

[0028] 도 16은 무선 통신 방법의 흐름도이다.

[0029] 도 17은 예시적인 장치에 대한 하드웨어 구현의 예를 예시하는 도면이다.

[0030] 도 18은 무선 통신 방법의 흐름도이다.

[0031] 도 19는 무선 통신 방법의 흐름도이다.

[0032] 도 20은 예시적인 장치에 대한 하드웨어 구현의 예를 예시하는 도면이다.

[0033] 도 21은 제1 무선 디바이스, 제2 무선 디바이스 및 제3 무선 디바이스 사이의 시그널링의 호출 흐름도이다.

[0034] 도 22는 무선 통신 방법의 흐름도이다.

[0035] 도 23은 무선 통신 방법의 흐름도이다.

[0036] 도 24는 예시적인 장치에 대한 하드웨어 구현의 예를 예시하는 도면이다.

[0037] 도 25는 무선 통신 방법의 흐름도이다.

[0038] 도 26은 무선 통신 방법의 흐름도이다.

[0039] 도 27은 예시적인 장치에 대한 하드웨어 구현의 예를 예시하는 도면이다.

[0040] 도 28은 제1 무선 디바이스와 제2 무선 디바이스 사이의 시그널링의 호출 흐름도이다.

[0041] 도 29는 무선 통신 방법의 흐름도이다.

[0042] 도 30은 예시적인 장치에 대한 하드웨어 구현의 예를 예시하는 도면이다.

[0043] 도 31은 무선 통신 방법의 흐름도이다.

[0044] 도 32는 예시적인 장치에 대한 하드웨어 구현의 예를 예시하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0014] [0045] 첨부 도면들과 관련하여 아래에 기술되는 상세한 설명은 다양한 구성들의 설명으로 의도되며, 본 명세서에서 설명된 개념들이 실시될 수 있는 유일한 구성들을 표현하도록 의도되는 것은 아니다. 상세한 설명은 다양한 개념들의 철저한 이해를 제공할 목적으로 특정 세부사항들을 포함한다. 그러나, 이러한 특정 세부사항들 없이도 이러한 개념들이 실시될 수 있음은 당업자들에게 자명할 것이다. 일부 예들에서, 이러한 개념들을 불명료

하게 하는 것을 피하기 위해, 잘 알려진 구조들 및 컴포넌트들은 블록도 형태로 도시된다.

[0015] [0046] 이제 전기통신 시스템들의 몇몇 양상들이 다양한 장치 및 방법들을 참조하여 제시될 것이다. 이러한 장치 및 방법들은, 다양한 블록들, 컴포넌트들, 회로들, 프로세스들, 알고리즘들 등(집합적으로, "엘리먼트들"로 지칭됨)에 의해 다음의 상세한 설명에서 설명되고 첨부한 도면들에서 예시될 것이다. 이러한 엘리먼트들은 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이들의 임의의 조합을 사용하여 구현될 수 있다. 이러한 엘리먼트들이 하드웨어로서 구현될지 또는 소프트웨어로서 구현될지는 특정한 애플리케이션 및 전체 시스템에 부과된 설계 제약들에 의존한다.

[0016] [0047] 예로서, 엘리먼트, 또는 엘리먼트의 임의의 일부, 또는 엘리먼트들의 임의의 조합은, 하나 이상의 프로세서들을 포함하는 "프로세싱 시스템"으로서 구현될 수도 있다. 프로세서들의 예들은 마이크로프로세서들, 마이크로제어기들, GPU들(graphics processing units), CPU들(central processing units), 애플리케이션 프로세서들, DSP들(digital signal processors), RISC(reduced instruction set computing) 프로세서들, SoC(systems on a chip), 기저대역 프로세서들, FPGA들(field programmable gate arrays), PLD들(programmable logic devices), 상태 머신들, 게이팅된 로직, 이산적 하드웨어 회로들, 및 본 개시 전반에 걸쳐 설명되는 다양한 기능을 수행하도록 구성되는 다른 적절한 하드웨어를 포함한다. 프로세싱 시스템의 하나 이상의 프로세서들은 소프트웨어를 실행할 수 있다. 소프트웨어는, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 하드웨어 디스크립션 언어, 또는 다른 용어로서 지칭되는지에 관계없이, 명령들, 명령 세트들, 코드, 코드 세그먼트들, 프로그램 코드, 프로그램들, 서브프로그램들, 소프트웨어 컴포넌트들, 애플리케이션들, 소프트웨어 애플리케이션들, 소프트웨어 패키지들, 루틴들, 서브루틴들, 오브젝트들, 실행가능물들, 실행 스레드들, 절차들, 함수들 등을 의미하도록 광범위하게 해석되어야 한다.

[0017] [0048] 따라서, 하나 이상의 예시적인 실시예들에서, 설명된 기능들은 하드웨어, 소프트웨어, 또는 이들의 임의의 조합으로 구현될 수 있다. 소프트웨어로 구현되면, 기능들은 컴퓨터 판독가능 매체 상에 하나 이상의 명령 또는 코드로서 저장되거나 이로서 인코딩될 수 있다. 컴퓨터 판독가능 매체들은 컴퓨터 저장 매체들을 포함한다. 저장 매체들은 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체들일 수 있다. 제한이 아닌 예로써, 이러한 컴퓨터-판독가능 매체는 RAM(random-access memory), ROM(read-only memory), EEPROM(electrically erasable programmable ROM), 광학 디스크 저장소, 자기 디스크 저장소, 다른 자기 저장 디바이스들, 전술한 타입들의 컴퓨터 판독가능 매체의 조합들, 또는 컴퓨터에 의해 액세스될 수 있는 명령들 또는 데이터 구조들의 형태로 컴퓨터 실행가능 코드를 저장하기 위해 사용될 수 있는 임의의 다른 매체를 포함할 수 있다.

[0018] [0049] 도 1은 무선 통신 시스템 및 액세스 네트워크(100)의 예를 예시하는 도면이다. 무선 통신 시스템(또한 WWAN(wireless wide area network)으로 지칭됨)은 기지국들(102), UE들(104), EPC(Evolved Packet Core)(160) 및 코어 네트워크(예컨대, 5GC)(190)를 포함한다. 기지국들(102)은 매크로 셀들(고전력 셀룰러 기지국) 및/또는 소형 셀들(저전력 셀룰러 기지국)을 포함할 수 있다. 매크로 셀들은 기지국들을 포함한다. 소형 셀들은 펨토셀들, 피코셀들 및 마이크로셀들을 포함한다.

[0019] [0050] 4G LTE에 대해 구성된 기지국들(102)(총괄적으로 E-UTRAN(Evolved UMTS(Universal Mobile Telecommunications System) Terrestrial Radio Access Network)으로 지칭됨)은 백홀 링크들(132)(예를 들어, S1 인터페이스)을 통해 EPC(160)와 인터페이싱할 수 있다. NR을 위해 구성된 기지국들(102)(집합적으로 NG-RAN(Next Generation RAN)으로 지칭됨)은 백홀 링크들(184)을 통해 코어 네트워크(190)와 인터페이싱할 수 있다. 다른 기능들에 추가로, 기지국들(102)은 하기 기능들, 즉, 사용자 데이터의 전송, 라디오 채널 암호화 및 암호해독, 무결성 보호, 헤더 압축, 모빌리티 제어 기능들(예를 들어, 핸드오버, 듀얼 접속), 셀간 간섭 조정, 접속 셋업 및 해제, 로드 밸런싱, NAS(non-access stratum) 메시지들에 대한 분배, NAS 노드 선택, 동기화, RAN(radio access network) 공유, MBMS(multimedia broadcast multicast service), 가입자 및 장비 트레이스, RIM(RAN information management), 페이징, 포지셔닝 및 경고 메시지들의 전송 중 하나 이상을 수행할 수 있다. 기지국들(102)은 백홀 링크들(134)(예를 들어, X2 인터페이스)을 통해 서로 (예를 들어, EPC(160) 또는 코어 네트워크(190)를 통해) 간접적으로 또는 직접적으로 통신할 수 있다. 백홀 링크들(134)은 유선 또는 무선일 수 있다.

[0020] [0051] 기지국들(102)은 UE들(104)과 무선으로 통신할 수 있다. 기지국들(102) 각각은 각각의 지리적 커버리지 영역(110)에 대한 통신 커버리지를 제공할 수 있다. 중첩하는 지리적 커버리지 영역들(110)이 존재할 수 있다. 예를 들어, 소형 셀(102')은 하나 이상의 매크로 기지국들(102)의 커버리지 영역(110)과 중첩하는 커버리지 영역(110')을 가질 수 있다. 소형 셀 및 매크로 셀들 둘 모두를 포함하는 네트워크는 이종 네트워크로 공지될 수

있다. 이종 네트워크는 또한, CSG(closed subscriber group)로 공지된 제한된 그룹에 서비스를 제공할 수 있는 HeNB들(Home eNBs(Evolved Node Bs))을 포함할 수 있다. 기지국들(102)과 UE들(104) 사이의 통신 링크들(120)은 UE(104)로부터 기지국(102)으로의 UL(uplink)(또한 역방향 링크로 지칭됨) 송신들 및/또는 기지국(102)으로부터 UE(104)로의 DL(downlink)(또한 순방향 링크로 지칭됨) 송신들을 포함할 수 있다. 통신 링크들(120)은 공간 멀티플렉싱, 빔형성 및/또는 송신 다이버시티를 포함하는 MIMO(multiple-input and multiple-output) 안테나 기술을 사용할 수 있다. 통신 링크들은 하나 이상의 캐리어들을 통할 수 있다. 기지국들(102)/UE들(104)은 각각의 방향에서 송신을 위해 사용되는 총 Yx MHz(x 컴포넌트 캐리어들)까지의 캐리어 어그리게이션에서 할당되는 캐리어 당 Y MHz(예를 들어, 5, 10, 15, 20, 100, 400 MHz 등) 대역폭까지 스펙트럼을 사용할 수 있다. 캐리어들은 서로 인접할 수 있거나 인접하지 않을 수 있다. 캐리어들의 할당은 DL 및 UL에 대해 비대칭일 수 있다(예를 들어, 더 많거나 더 적은 캐리어들이 UL보다 DL에 대해 할당될 수 있다). 컴포넌트 캐리어들은 1차 컴포넌트 캐리어 및 하나 이상의 2차 컴포넌트 캐리어들을 포함할 수 있다. 1차 컴포넌트 캐리어는 1차 셀(PCell)로 지칭될 수 있고, 2차 컴포넌트 캐리어는 2차 셀(SCell)로 지칭될 수 있다.

[0021] [0052] 특정 UE들(104)은 D2D(device-to-device) 통신 링크(158)를 사용하여 서로 통신할 수 있다. D2D 통신 링크(158)는 DL/UL WWAN 스펙트럼을 사용할 수 있다. D2D 통신 링크(158)는 하나 이상의 사이드링크(sidelink) 채널들, 예를 들어, PSBCH(physical sidelink broadcast channel), PSDCH(physical sidelink discovery channel), PSSCH(physical sidelink shared channel), 및 PSCCH(physical sidelink control channel)를 사용할 수 있다. D2D 통신은 IEEE 802.11 표준, LTE, 또는 NR에 기초하여, 예를 들어, FlashLinQ, WiMedia, Bluetooth, ZigBee, Wi-Fi와 같은 다양한 무선 D2D 통신 시스템들을 통할 수 있다.

[0022] [0053] 무선 통신 시스템은 5 GHz의 비면허 주파수 스펙트럼에서 통신 링크들(154)을 통해 Wi-Fi 스테이션들(STA들)(152)과 통신하는 Wi-Fi AP(access point)(150)를 더 포함할 수 있다. 비면허 주파수 스펙트럼에서 통신하는 경우, STA들(152)/AP(150)는, 채널이 이용가능한지 여부를 결정하기 위해 통신하기 전에 CCA(clear channel assessment)를 수행할 수 있다.

[0023] [0054] 소형 셀(102')은 면허 및/또는 비면허 주파수 스펙트럼에서 동작할 수 있다. 비면허 주파수 스펙트럼에서 동작하는 경우, 소형 셀(102')은 NR을 이용할 수 있고, Wi-Fi AP(150)에 의해 사용되는 것과 동일한 5 GHz 비면허 주파수 스펙트럼을 사용할 수 있다. 비면허 주파수 스펙트럼에서 NR을 이용하는 소형 셀(102')은 액세스 네트워크에 대한 커버리지를 부스팅하고 그리고/또는 용량을 증가시킬 수 있다.

[0024] [0055] 기지국(102)은 소형 셀(102')이든 또는 대형 셀(예를 들어, 매크로 기지국)이든, eNB, gNodeB(gNB) 또는 다른 타입의 기지국을 포함할 수 있다. 일부 기지국들, 예를 들어, gNB(180)는 UE(104)와의 통신에서 종래의 서브 6 GHz 스펙트럼, mmW(millimeter wave) 주파수들 및/또는 준 mmW 주파수들에서 동작할 수 있다. gNB(180)가 mmW 또는 준 mmW 주파수들에서 동작하는 경우, gNB(180)는 mmW 기지국으로 지칭될 수 있다. EHF(extremely high frequency)는 전자기 스펙트럼에서 RF의 일부이다. EHF는 30 GHz 내지 300 GHz의 범위 및 1 밀리미터 내지 10 밀리미터의 파장을 갖는다. 이 대역의 라디오 파들은 밀리미터파로 지칭될 수 있다. 준 mmW는 100 밀리미터의 파장을 갖는 3 GHz의 주파수까지 아래로 확장될 수 있다. SHF(super high frequency) 대역은 3 GHz 내지 30 GHz로 확장되고 또한 센티미터파로 지칭된다. mmW/준 mmW 라디오 주파수 대역을 사용하는 통신들은 극도로 높은 경로 손실 및 짧은 범위를 갖는다. mmW 기지국(180)은 극도로 높은 경로 손실 및 짧은 범위를 보상하기 위해 UE(104)와의 빔형성(182)을 활용할 수 있다.

[0025] [0056] 디바이스들은 빔형성을 사용하여 통신을 송신 및 수신할 수 있다. 예를 들어, 도 1은 기지국(180)이 하나 이상의 송신 방향들(182')에서 UE(104)에 빔형성된 신호를 송신할 수 있는 것을 예시한다. UE(104)는 하나 이상의 수신 방향들(182")에서 기지국(180)으로부터 빔형성된 신호를 수신할 수 있다. UE(104)는 또한 빔형성된 신호를 하나 이상의 송신 방향들에서 기지국(180)에 송신할 수 있다. 기지국(180)은 하나 이상의 수신 방향들에서 UE(104)로부터 빔형성된 신호를 수신할 수 있다. 기지국(180)/UE(104)는 기지국(180)/UE(104) 각각에 대한 최상의 수신 및 송신 방향들을 결정하기 위해 빔 트레이닝을 수행할 수 있다. 기지국(180)에 대한 송신 및 수신 방향들은 동일할 수 있거나 동일하지 않을 수 있다. UE(104)에 대한 송신 및 수신 방향들은 동일할 수 있거나 동일하지 않을 수 있다. 빔형성된 신호들이 UE(104)와 기지국(102/180) 사이에서 예시되지만, 빔형성의 양상들은 유사하게, 이를테면 사이드링크 통신, 이를테면, V2X, 또는 D2D 통신에 기초하여 다른 UE(104) 또는 RSU(107)와 통신하기 위해 UE(104) 또는 RSU(107)에 의해 적용될 수 있다.

[0026] [0057] EPC(160)는 MME(Mobility Management Entity)(162), 다른 MME들(164), 서빙 게이트웨이(166), MBMS(Multimedia Broadcast Multicast Service) 게이트웨이(168), BM-SC(Broadcast Multicast Service

Center)(170) 및 PDN(Packet Data Network) 게이트웨이(172)를 포함할 수 있다. MME(162)는 HSS(Home Subscriber Server)(174)와 통신할 수 있다. MME(162)는 UE들(104)과 EPC(160) 사이의 시그널링을 프로세싱하는 제어 노드이다. 일반적으로, MME(162)는 베어러 및 접속 관리를 제공한다. 모든 사용자 IP(Internet protocol) 패킷들은, 자체로 PDN 게이트웨이(172)에 연결된 서빙 게이트웨이(166)를 통해 전송된다. PDN 게이트웨이(172)는 UE IP 어드레스 할당 뿐만 아니라 다른 기능들을 제공한다. PDN 게이트웨이(172) 및 BM-SC(170)는 IP 서비스들(176)에 연결된다. IP 서비스들(176)은 인터넷, 인트라넷, IMS(IP Multimedia Subsystem), PS 스트리밍 서비스 및/또는 다른 IP 서비스들을 포함할 수 있다. BM-SC(170)는 MBMS 사용자 서비스 프로비저닝(provisioning) 및 전달을 위한 기능들을 제공할 수 있다. BM-SC(170)는 콘텐츠 제공자 MBMS 송신을 위한 엔트리 포인트로서 기능할 수 있고, PLMN(public land mobile network) 내의 MBMS 베어러 서비스들을 인가 및 개시하기 위해 사용될 수 있으며, MBMS 송신들을 스케줄링하기 위해 사용될 수 있다. MBMS 게이트웨이(168)는, 특정 서비스를 브로드캐스트하는 MBSFN(Multicast Broadcast Single Frequency Network) 영역에 속하는 기지국들(102))에 MBMS 트래픽을 분배하기 위해 사용될 수 있고, 세션 관리(시작/중단)를 담당하고 eMBMS 관련 과금 정보를 수집하는 것을 담당할 수 있다.

[0027] [0058] 코어 네트워크(190)는 AMF(Access and Mobility Management Function)(192), 다른 AMF들(193), SMF(Session Management Function)(194) 및 UPF(User Plane Function)(195)를 포함할 수 있다. AMF(192)는 UDM(Unified Data Management)(196)과 통신할 수 있다. AMF(192)는 UE들(104)과 코어 네트워크(190) 사이의 시그널링을 프로세싱하는 제어 노드이다. 일반적으로, AMF(192)는 QoS 흐름 및 세션 관리를 제공한다. 모든 사용자 IP(Internet protocol) 패킷들은 UPF(195)를 통해 전송된다. UPF(195)는 UE IP 어드레스 할당 뿐만 아니라 다른 기능들을 제공한다. UPF(195)는 IP 서비스들(197)에 접속된다. IP 서비스들(197)은 인터넷, 인트라넷, IMS(IP Multimedia Subsystem), PS 스트리밍 서비스 및/또는 다른 IP 서비스들을 포함할 수 있다.

[0028] [0059] 기지국은 또한, gNB, 노드 B, eNB(evolved Node B), 액세스 포인트, 베이스 트랜시버 스테이션, 라디오 기지국, 라디오 트랜시버, 트랜시버 기능부, BSS(basic service set), ESS(extended service set), TRP(transmit reception point) 또는 일부 다른 적절한 용어로 지칭될 수 있다. 기지국(102)은 UE(104)에 대해 EPC(160) 또는 코어 네트워크(190)로의 액세스 포인트를 제공한다. UE들(104)의 예들은 셀룰러 폰, 스마트 폰, SIP(session initiation protocol) 폰, 랩톱, PDA(personal digital assistant), 위성 라디오, 글로벌 포지셔닝 시스템, 멀티미디어 디바이스, 비디오 디바이스, 디지털 오디오 플레이어(예를 들어, MP3 플레이어), 카메라, 게임 콘솔, 태블릿, 스마트 디바이스, 웨어러블 디바이스, 차량, 전기 검침기, 가스 펌프, 대형 또는 소형 주방 기기, 헬스케어 디바이스, 임플란트, 센서/액추에이터, 디스플레이 또는 임의의 다른 유사한 기능 디바이스를 포함한다. UE들(104) 중 일부는 IoT 디바이스들(예를 들어, 주차 검침기, 가스 펌프, 토스터(toaster), 차량들, 심장 모니터 등)로 지칭될 수 있다. UE(104)는 또한 스테이션, 이동국, 가입자국, 모바일 유닛, 가입자 유닛, 무선 유닛, 원격 유닛, 모바일 디바이스, 무선 디바이스, 무선 통신 디바이스, 원격 디바이스, 모바일 가입자국, 액세스 단말, 모바일 단말, 무선 단말, 원격 단말, 핸드셋, 사용자 에이전트, 모바일 클라이언트, 클라이언트, 또는 다른 어떤 적당한 전문용어로 지칭될 수 있다.

[0029] [0060] 무선 통신 네트워크들의 일부 예들은 V2V(vehicle-to-vehicle), V2I(vehicle-to-infrastructure)(예컨대, 차량-기반 통신 디바이스로부터 RSU(Road Side Unit)와 같은 도로 인프라구조 노드들로), V2N(vehicle-to-network)(예컨대, 차량-기반 통신 디바이스로부터 기지국과 같은 하나 이상의 네트워크 노드들로), C-V2X(cellular-vehicle-to everything), e-V2X(enhanced V2X), 및/또는 이들의 조합, 및/또는 V2X(vehicle-to-anything) 통신들로 집합적으로 지칭될 수 있는 다른 디바이스들과 통신할 수 있는 차량-기반 통신 디바이스들을 포함할 수 있다. 도 1을 다시 참조하면, 특정 양상들에서, UE(104), 예컨대 송신 VUE(Vehicle User Equipment) 또는 다른 UE는 다른 UE(104)에 직접적으로 메시지들을 송신하도록 구성될 수 있다. 통신은 V2X 또는 다른 D2D 통신, 이를테면, ProSe(Proximity Services) 등에 기초할 수 있다. V2X 및/또는 D2D 통신에 기초한 통신은 또한 RSU(Road side Unit)(107) 등과 같은 다른 송신 및 수신 디바이스들에 의해 송신 및 수신될 수 있다. 통신의 양상들은, 예컨대, 도 2의 예와 관련하여 설명된 바와 같이, PC5 또는 사이드링크 통신에 기초할 수 있다. 다음의 설명이 5G NR과 관련된 V2X/D2D 통신에 대한 예들을 제공할 수 있지만, 본원에서 설명된 개념들은 다른 유사한 영역들, 이를테면 LTE, LTE-A, CDMA, GSM, 및 다른 무선 기술들에 적용가능할 수 있다.

[0030] [0061] 도 1을 다시 참조하면, 특정 양상들에서, UE(104)는, 다른 무선 디바이스들이 위협 엔티티를 가상으로 감지할 수 있도록, 검출된 위협 엔티티의 정보를 위협 엔티티의 구역을 넘어선 다른 무선 디바이스들과 공유하도록 구성될 수 있다. 예를 들어, UE(104)는, 다른 무선 디바이스들이 위협 엔티티를 가상으로 감지할 수 있도록, 검출된 위협 엔티티의 정보를 위협 엔티티의 구역을 넘어선 다른 무선 디바이스들(예컨대, 104')과 공유하

도록 구성된 검출 컴포넌트(198)을 포함할 수 있다. 특정 양상들에서, UE(104)는, 다른 무선 디바이스가 예방 조치들을 사전에 취할 수 있도록, 검출된 위협 엔티티와 관련된 정보를 위협 엔티티의 위협 구역을 넘어선 다른 무선 디바이스들과 공유하도록 구성될 수 있다. 예를 들어, UE(104)는 다른 무선 디바이스가 예방 조치들을 사전에 취할 수 있도록, 검출된 위협 엔티티와 관련된 정보를 위협 엔티티의 위협 구역을 넘어선 다른 무선 디바이스들(예컨대, 104')과 공유하도록 구성된 검출 컴포넌트(198)을 포함할 수 있다. 특정 양상들에서, UE(104)는 검출된 위협 엔티티와 관련된 정보를 다른 무선 디바이스들과 공유하도록 구성될 수 있다. 예를 들어, UE(104)는 검출된 위협 엔티티와 관련된 정보를 다른 무선 디바이스들(예컨대, UE(104'))과 공유하도록 구성된 검출 컴포넌트(198)를 포함할 수 있다.

[0031] [0062] 도 1을 다시 참조하면, 특정 양상들에서, UE(104')는 위협 엔티티를 가상으로 감지하는 것에 기초하여 BSM을 송신할 서브채널을 결정하도록 구성될 수 있다. 예를 들어, UE(104')는 위협 엔티티를 가상으로 감지하는 것에 기초하여 BSM을 송신할 서브채널을 결정하도록 구성된 BSM 컴포넌트(199)를 포함할 수 있다. 특정 양상들에서, UE(104')는 제1 무선 디바이스에 의해 검출된 위협 엔티티를 가상으로 감지하는 것에 기초하여 완화 액션을 개시하도록 구성될 수 있다. 예를 들어, UE(104')는 제1 무선 디바이스(예를 들어, 104)에 의해 검출된 위협 엔티티를 가상으로 감지하는 것에 기초하여 완화 액션을 개시하도록 구성된 완화 컴포넌트(199)를 포함할 수 있다. 특정 양상들에서, UE(104')는 위협 장애물의 위협 구역을 넘어선 동안 제1 무선 디바이스에 의해 검출된 위협 장애물의 통지를 수신하는 것에 대한 응답으로 완화 액션을 개시하도록 구성될 수 있다. 예를 들어, UE(104')는 위협 장애물의 위협 구역을 넘어선 동안 제1 무선 디바이스(예컨대, 104)에 의해 검출된 위협 장애물의 통지를 수신하는 것에 대한 응답으로 완화 액션을 개시하도록 구성된 완화 컴포넌트(199)를 포함할 수 있다.

[0032] [0063] 도 2는, 예컨대, UE들(104) 사이, UE와 인프라구조 사이, UE와 RSU 사이 등에서 사이드링크 통신을 위해 사용될 수 있는 프레임 구조 내의 사이드링크 서브프레임을 예시하는 예시적인 도면(200)을 예시한다. 프레임 구조는 LTE 프레임 구조 내에 있을 수 있다. 다음의 설명이 LTE에 초점이 맞춰질 수 있지만, 본원에 설명된 개념들은 5G NR, LTE-A, CDMA, GSM 및 다른 무선 기술들과 같은 다른 유사한 영역들에 적용가능할 수 있다. 이는 단지 일 예이고, 다른 무선 통신 기술들은 상이한 프레임 구조 및/또는 상이한 채널들을 가질 수 있다. 프레임(10 ms)은 10개의 동등한 크기의 서브프레임들(1 ms)로 분할될 수 있다. 각각의 서브프레임은 2개의 슬롯들을 포함할 수 있다. 각각의 슬롯은 7개의 SC-FDMA 심볼들을 포함할 수 있다. 슬롯 구성 0에 대해, 각각의 슬롯은 14개의 심볼들을 포함할 수 있고, 슬롯 구성 1에 대해, 각각의 슬롯은 7개의 심볼들을 포함할 수 있다. 도면(200)이 단일 RB 서브프레임을 예시하지만, 사이드링크 통신은 다수의 RB들을 포함할 수 있다.

[0033] [0064] 자원 그리드는 프레임 구조를 표현하기 위해 사용될 수 있다. 각각의 시간 슬롯은 12개의 연속적인 서브캐리어들로 확장되는 RB(resource block)(또한 PRB(physical RB)들로 지칭됨)를 포함할 수 있다. 자원 그리드는 다수의 RE들(resource elements)로 분할된다. 각각의 RE에 의해 반송되는 비트들의 수는 변조 방식에 의존한다. 도 2에 예시된 바와 같이, RE들 중 일부는 DMRS(demodulation RS)와 같은 기준 신호를 포함할 수 있다. 본원에 설명된 바와 같이, 적어도 하나의 심볼이 피드백을 위해 사용될 수 있다. 피드백 이전 및/또는 피드백 이후의 심볼은 데이터의 수신과 피드백의 송신 사이의 턴어라운드를 위해 사용될 수 있다. 예컨대, 서브프레임의 끝에 있는 다른 심볼은 송신/수신 없이 가드 심볼로서 사용될 수 있다. 가드는 디바이스가, 예컨대, 후속 서브프레임에서, 수신 디바이스로서 동작하도록 준비하기 위해 송신 디바이스로서 동작하는 것으로부터 스위칭하는 것을 가능하게 한다. 예시된 바와 같이, 데이터 또는 제어는 나머지 RE들에서 송신될 수 있다. 예를 들어, 데이터는 PSSCH에서 반송될 수 있고, 제어 정보는 PSCCH에서 반송될 수 있다. 제어 정보는 SCI(Sidelink Control Information)를 포함할 수 있다. 기준 신호들, 제어 및 데이터 중 임의의 것의 포지션은 도 2에 예시된 예와 상이할 수 있다.

[0034] [0065] 도 2는 단지 사용될 수 있는 프레임 구조의 하나의 비제한적인 예를 예시한다. 본원에 설명된 양상들은 다른 상이한 프레임 포맷들을 사용하는 통신에 적용될 수 있다.

[0035] [0066] 도 3은 예컨대, V2V/V2X/다른 통신을 통해 제2 무선 통신 디바이스(350)와 통신하는 제1 무선 통신 디바이스(310)의 블록도(300)이다. 디바이스(310)는 수신 디바이스, 예컨대 디바이스(350)와 통신하는 송신 디바이스를 포함할 수 있다. 통신은, 예컨대 사이드링크에 기초할 수 있다. 송신 디바이스(310)는 UE, RSU 등을 포함할 수 있다. 수신 디바이스는 UE, RSU 등을 포함할 수 있다. 패킷들은 계층 3 및 계층 2 기능을 구현하는 제어기/프로세서(375)에 제공될 수 있다. 계층 3은 RRC(radio resource control) 계층을 포함하고, 계층 2는 PDCP(packet data convergence protocol) 계층, RLC(radio link control) 계층 및 MAC(medium access

control) 계층을 포함한다.

[0036] [0067] 송신(TX) 프로세서(316) 및 수신(RX) 프로세서(370)는 다양한 신호 프로세싱 기능들과 연관된 계층 1 기능을 구현한다. 물리(PHY) 계층을 포함하는 계층 1은 전송 채널들 상에서 에러 검출, 전송 채널들의 FEC(forward error correction) 코딩/디코딩, 인터리빙, 레이트 매칭, 물리 채널들 상으로의 맵핑, 물리 채널들의 변조/복조 및 MIMO 안테나 프로세싱을 포함할 수 있다. TX 프로세서(316)는 다양한 변조 방식들(예를 들어, BPSK(binary phase-shift keying), QPSK(quadrature phase-shift keying), M-PSK(M-phase-shift keying), M-QAM(M-quadrature amplitude modulation))에 기초한 신호 성상도(constellation)들로의 맵핑을 핸들링한다. 그 다음, 코딩되고 변조된 심볼들은 병렬적 스트림들로 분할될 수 있다. 그 다음, 각각의 스트림은, OFDM 서브캐리어에 맵핑되고, 시간 및/또는 주파수 도메인에서 기준 신호(예를 들어, 파일럿)와 멀티플렉싱될 수 있고, 그 다음, IFFT(Inverse Fast Fourier Transform)를 사용하여 함께 결합되어, 시간 도메인 OFDM 심볼 스트림을 반송하는 물리 채널을 생성할 수 있다. OFDM 스트림은 다수의 공간 스트림들을 생성하기 위해 공간적으로 프리코딩된다. 채널 추정기(374)로부터의 채널 추정치들은 코딩 및 변조 방식을 결정하기 위해 뿐만 아니라 공간 프로세싱을 위해 사용될 수 있다. 채널 추정치는, 기준 신호 및/또는 디바이스(350)에 의해 송신된 채널 조건 피드백으로부터 도출될 수 있다. 그 다음, 각각의 공간 스트림은 별개의 송신기(318TX)를 통해 상이한 안테나(320)에 제공될 수 있다. 각각의 송신기(318TX)는 송신을 위해 각각의 공간 스트림으로 RF 캐리어를 변조할 수 있다.

[0037] [0068] 디바이스(350)에서, 각각의 수신기(354RX)는 자신의 각각의 안테나(352)를 통해 신호를 수신한다. 각각의 수신기(354RX)는 RF 캐리어 상으로 변조된 정보를 복원하고, 그 정보를 수신(RX) 프로세서(356)에 제공한다. TX 프로세서(368) 및 RX 프로세서(356)는 다양한 신호 프로세싱 기능들과 연관된 계층 1 기능을 구현한다. RX 프로세서(356)는 정보에 대해 공간 프로세싱을 수행하여, 디바이스(350)를 목적지로 하는 임의의 공간 스트림들을 복원할 수 있다. 다수의 공간 스트림들이 디바이스(350)를 목적지로 하면, 이들은 RX 프로세서(356)에 의해 단일 OFDM 심볼 스트림으로 결합될 수 있다. 그 다음, RX 프로세서(356)는 FFT(Fast Fourier Transform)를 사용하여 OFDM 심볼 스트림을 시간-도메인으로부터 주파수 도메인으로 변환한다. 주파수 도메인 신호는, OFDM 신호의 각각의 서브캐리어에 대한 별개의 OFDM 심볼 스트림을 포함한다. 각각의 서브캐리어 상의 심볼들, 및 기준 신호는 디바이스(310)에 의해 송신된 가장 가능성있는 신호 성상도 포인트들을 결정함으로써 복원 및 복조된다. 이러한 연판정들은, 채널 추정기(358)에 의해 컴퓨팅된 채널 추정치들에 기초할 수 있다. 그 다음, 연판정들은, 물리 채널 상에서 디바이스(310)에 의해 원래 송신되었던 데이터 및 제어 신호들을 복원하기 위해 디코딩 및 디인터리빙된다. 그 다음, 데이터 및 제어 신호들은, 계층 3 및 계층 2 기능을 구현하는 제어기/프로세서(359)에 제공된다.

[0038] [0069] 제어기/프로세서(359)는 프로그램 코드들 및 데이터를 저장하는 메모리(360)와 연관될 수 있다. 메모리(360)는 컴퓨터 판독가능 매체로 지칭될 수 있다. 제어기/프로세서(359)는, 전송 채널과 로직 채널 사이의 디멀티플렉싱, 패킷 리어셈블리, 암호해독, 헤더 압축해제, 및 제어 신호 프로세싱을 제공할 수 있다. 제어기/프로세서(359)는 또한, HARQ 동작들을 지원하기 위해 ACK 및/또는 NACK 프로토콜을 사용하여 에러 검출을 담당한다.

[0039] [0070] 디바이스(310)에 의한 송신과 관련하여 설명된 기능과 유사하게, 제어기/프로세서(359)는 시스템 정보(예를 들어, MIB, SIB들) 포착, RRC 접속들 및 측정 보고와 연관된 RRC 계층 기능; 헤더 압축/압축해제 및 보안(암호화, 암호해독, 무결성 보호, 무결성 검증)과 연관된 PDCP 계층 기능; 상위 계층 PDU들의 전송, ARQ를 통한 에러 정정, 연접, 세그먼트화 및 RLC SDU들의 리어셈블리, RLC 데이터 PDU들의 리-세그먼트화, 및 RLC 데이터 PDU들의 재순서화와 연관된 RLC 계층 기능; 및 로직 채널들과 전송 채널들 사이의 맵핑, TB들 상으로의 MAC SDU들의 멀티플렉싱, TB들로부터 MAC SDU들의 디멀티플렉싱, 스케줄링 정보 보고, HARQ를 통한 에러 정정, 우선순위 핸들링 및 로직 채널 우선순위화와 연관된 MAC 계층 기능을 제공할 수 있다.

[0040] [0071] 기준 신호 또는 디바이스(310)에 의해 송신된 피드백으로부터 채널 추정기(358)에 의해 도출된 채널 추정치들은, 적절한 코딩 및 변조 방식들을 선택하고 공간 프로세싱을 용이하게 하기 위해 TX 프로세서(368)에 의해 사용될 수 있다. TX 프로세서(368)에 의해 생성된 공간 스트림들은 별개의 송신기들(354TX)을 통해 상이한 안테나(352)에 제공될 수 있다. 각각의 송신기(354TX)는 송신을 위해 각각의 공간 스트림으로 RF 캐리어를 변조할 수 있다.

[0041] [0072] 송신은, 디바이스(350)의 수신기 기능과 관련하여 설명된 것과 유사한 방식으로 디바이스(310)에서 프로세싱된다. 각각의 수신기(318RX)는 자신의 각각의 안테나(320)를 통해 신호를 수신한다. 각각의 수신기

(318RX)는 RF 캐리어 상으로 변조된 정보를 복원하고, 그 정보를 RX 프로세서(370)에 제공한다.

[0042] [0073] 제어기/프로세서(375)는 프로그램 코드들 및 데이터를 저장하는 메모리(376)와 연관될 수 있다. 메모리(376)는 컴퓨터 판독가능 매체로 지칭될 수 있다. 제어기/프로세서(375)는, 전송 채널과 로직 채널 사이의 디멀티플렉싱, 패킷 리어셈블리, 암호해독, 헤더 압축해제, 제어 신호 프로세싱을 제공한다. 제어기/프로세서(375)는 또한, HARQ 동작들을 지원하기 위해 ACK 및/또는 NACK 프로토콜을 사용하여 에러 검출을 담당한다.

[0043] [0074] 디바이스(350)의 TX 프로세서(368), RX 프로세서(356) 또는 제어기/프로세서(359) 또는 TX(316), RX 프로세서(370) 또는 제어기/프로세서(375) 중 적어도 하나는 도 1의 198 또는 199와 관련하여 설명된 양상들을 수행하도록 구성될 수 있다.

[0044] [0075] 도 4는 V2X 또는 다른 D2D 통신과 같은 사이드링크 통신에 기초한 디바이스들 사이의 무선 통신의 예(400)를 예시한다. 통신은 도 2와 관련하여 설명된 양상들을 포함하는 슬롯 구조에 기초할 수 있다. 예를 들어, 송신 UE(402)는 예컨대, 제어 채널 및/또는 대응하는 데이터 채널을 포함하는 송신(414)을 송신할 수 있으며, 이는 수신 UE들(404, 406, 408)에 의해 수신될 수 있다. 적어도 하나의 UE는 자율 주행 차량 또는 무인 항공기를 포함할 수 있다. 제어 채널은 데이터 채널을 디코딩하기 위한 정보를 포함할 수 있고, 또한, 데이터 송신 동안 점유된 자원들 상에서 송신하는 것을 억제함으로써 간섭을 회피하기 위해 수신 디바이스에 의해 사용될 수 있다. 데이터 송신에 의해 점유될 RB들 뿐만 아니라 TTI들의 수는 송신 디바이스로부터의 제어 메시지에 표시될 수 있다. UE들(402, 404, 406, 408) 각각은 수신 디바이스로서 동작하는 것에 부가하여 송신 디바이스로서 동작하는 것이 가능할 수 있다. 따라서, UE들(406, 408)은 송신들(416, 420)을 송신하는 것으로 예시된다. 송신들(414, 416, 420)은 인근 디바이스들에 브로드캐스트 또는 멀티캐스트될 수 있다. 예를 들어, UE(414)는 UE(414)의 범위(401) 내의 다른 UE들에 의한 수신을 위해 의도된 통신을 송신할 수 있다. 추가적으로/대안적으로, RSU(407)는 UE들(402, 404, 406, 408)로부터 통신을 수신하고 그리고/또는 그들에 통신을 송신할 수 있다.

[0045] [0076] UE(402, 404, 406, 408) 또는 RSU(407)는 도 1과 관련하여 설명된 198과 유사한 검출 컴포넌트를 포함할 수 있다. UE(402, 404, 406, 408) 또는 RSU(407)는 또한 도 1과 관련하여 설명된 199와 유사한 BSM 또는 완화 컴포넌트를 포함할 수 있다.

[0046] [0077] V2X 통신들과 같은 무선 통신들에서, V2X 엔티티들은 협력적 및 자동화된 운전을 위해 다른 V2X 엔티티들과의 센서 공유를 수행할 수 있다. 예를 들어, 도 5a의 도면(500)을 참조하면, 호스트 차량(HV)(502)은 자신의 환경 내의 다수의 아이템들을 검출할 수 있다. 예를 들어, HV(502)는 비-V2X 엔티티(NV)(506)의 존재를 검출할 수 있다. HV(502)는, 제1 원격 차량(RV1)(504) 및/또는 노변 유닛(RSU)(508)이 스스로 NV(506)를 검출할 수 없는 경우 RV1(504) 또는 RSU(508)와 같은 다른 엔티티들에 NV(506)의 존재에 대해 통지할 수 있다. NV(506)에 관해 RV1(504) 및/또는 RSU(508)에 통지하는 HV(502)는 센서 정보의 공유이다. 도 5b의 도면(510)을 참조하면, HV(502)는 RV1(504) 및/또는 RSU(508)에 의해 아직 검출되지 않은 HV(502) 및/또는 RV1(504)의 경로에서 장애물일 수 있는 물리적 장애물(512), 이를테면 포트홀, 잔해, 또는 물체를 검출할 수 있다. HV(502)는 장애물(512)을 회피할 수 있도록 장애물(512)을 RV1 및/또는 RSU(508)에 통지할 수 있다. 도 5c의 도면(520)을 참조하면, HV(502)는 VRU(vulnerable road user)(522)의 존재를 검출할 수 있고, RSU(508) 및/또는 RV1(504)이 VRU(522)를 검출하지 못할 수 있는 경우들에서 VRU(522)의 검출을 RV1(504) 및 RSU(508)와 공유할 수 있다. 도 5d의 도면(530)을 참조하면, HV는 인근 엔티티(예컨대, NV, VRU, 장애물)의 검출 시에, 엔티티의 검출을 공유하기 위해 SDSM(sensor data shared message)(532)을 RV 및/또는 RSU에 송신할 수 있다. SDSM(532)은 HV 부근 내의 임의의 수신 디바이스가 메시지를 수신할 수 있도록 하는 브로드캐스트 메시지일 수 있다. 일부 경우들에서, 공유된 정보는 RV들과 같은 다른 엔티티들에 중계될 수 있다. 예를 들어, 도 6의 도면(600)을 참조하면, HV(602)는 NV(606) 및/또는 VRU(622)의 존재를 검출할 수 있다. HV(602)는 NV(606) 및/또는 VRU(622)의 검출을 보고하기 위해 SDSM(610)을 RSU(608)에 브로드캐스트할 수 있다. RSU(608)는, 원격 차량들이 NV(606) 및/또는 VRU(622)의 존재를 인식하도록 HV(602)로부터 수신된 SDSM(610)을 원격 차량들에 중계할 수 있다. 예를 들어, RSU(608)는 SDSM(612)을 RV1(604)에 송신할 수 있으며, 여기서 SDSM(612)은 NV(606) 및/또는 VRU(622)의 검출과 관련된 정보를 포함한다. 일부 경우들에서, 원격 차량들은 반복적으로 업데이트될 수 있다. 예를 들어, 도 7의 도면(700)을 참조하면, HV(702)는 NV1(706) 및/또는 NV2(708)를 검출할 수 있고, NV1(706) 및/또는 NV2(708)의 존재를 RV(704)와 공유할 수 있다. HV(702)는 HV(702)에 의해 수집된 원시 데이터를 통지하는 SDSM(710)을 송신할 수 있다. RV(704)는 HV(702)에 의해 통지된 원시 데이터에 가입하기 위한 요청을 포함할 수 있는 SDSM(712)을 송신할 수 있다. 응답으로, HV는 원시 데이터 교환(714)을 RV(704)에 송신할 수 있다. 특정 물체들에 관련된 정보는 SDSM에 포함될 수 있다. 예를 들어, SDSM은 비-V2X 차량들, 장애물들 또는 VRU들에 관련된 정보를 포함할 수 있다. 이들은, 물리적으로 검출될 수 있고 V2X 차량

의 경로에 대한 물리적 장애물 또는 배리어를 제기할 수 있는 물체들이다. 그러나, 일부 물체들은 V2X 차량들의 협력적 및 자동화된 운전 결정들에 위험을 제기할 수 있다.

[0047] [0078] C-V2X 통신들과 같은 무선 통신들에서, C-V2X 분산형 스케줄링 방식들(예컨대, LTE-V2X에 대한 모드 4 또는 NR-V2X에 대한 모드 2)은 서브채널 배제를 위한 물리적 감지를 활용하고, 예비하는 동안 은닉 노드들에 의해 점유되는 자원들을 고려하지 않을 수 있다. 지속적인 은닉 재머들 또는 Wi-Fi OOB(out of band) 간섭자들은 특히 브로드캐스트 범위의 에지에서 성공적인 패킷 수신을 감소시킬 수 있으며, 이는 C-V2X 통신들의 유효 범위를 감소시킬 수 있다. 이는, 장애물들 및/또는 건물들의 존재로 인해 보이지 않게 될 수 있는 도시 VANET(vehicular ad hoc network)들에서의 근거리 은닉 노드들의 존재에 의해 악화될 수 있다. 은닉 노드들은 자동화된 운전 결정들에 활용되는 자원들을 방해하거나 또는 이들에 대한 간섭을 야기할 수 있다. 은닉 노드들은 C-V2X 안전 애플리케이션들을 의도적으로 공격하려고 시도하는 악의적인 엔티티들이 아닐 수 있다. 그러나, 일부 은닉된 노드들은 악의적인 또는 위협 엔티티들일 수 있고, DoS(denial of service) 공격, 재밍, 또는 심지어 의도적이지 않고 C-V2X에 대한 알려진 위협인 OOB 간섭의 형태로 공격들을 제기할 수 있다. 악의적이든 아니든, 이들 엔티티들로부터의 이러한 공격들은 C-V2X 가능 안전 애플리케이션들의 유용성을 실질적으로 방해할 수 있다. 이러한 엔티티들로부터의 공격들이 제 시간에 검출되지 않고 적절하게 완화 또는 회피되지 않으면, 그러한 공격들은 도로 사용자들에게 즉각적인 위험을 제기할 수 있다.

[0048] [0079] 본원에서 제공되는 양상들은 센서 공유를 사용한 협력적 조기 위협 검출을 위한 구성을 제공한다. 예를 들어, 제1 무선 디바이스는 검출된 위협 엔티티와 관련된 정보를 다른 무선 디바이스들과 공유할 수 있다. 일부 양상들에서, 제1 무선 디바이스는, 다른 무선 디바이스들이 위협 엔티티를 가상으로 감지하도록, 검출된 위협 엔티티의 정보를 위협 엔티티의 구역을 넘어선 다른 무선 디바이스들과 공유할 수 있다. 일부 양상들에서, 제1 무선 디바이스는, 다른 무선 디바이스들이 예방 조치들을 사전에 취할 수 있도록, 검출된 위협 엔티티와 관련된 정보를 위협 엔티티의 위협 구역을 넘어선 다른 무선 디바이스들과 공유할 수 있다.

[0049] [0080] 도 8은 위협 엔티티의 검출의 예를 예시하는 도면(800)이다. 일부 경우들에서, VV(victim vehicle)(802)는 V2X 엔티티일 수 있고 위협 엔티티(804)에 직면할 수 있다. VV(802)는 위협 엔티티(804)의 위협 구역(806) 내에 있는 동안 위협 엔티티(804)와 직면할 수 있다. VV(802)는 위협 엔티티(804)의 존재를 검출할 뿐만 아니라 위협 엔티티(804)의 특성들을 검출할 수 있다. 일부 경우들에서, 위협 엔티티(804)는 DoS 공격, 재머, 오작동 차량, OOB(out of band) 간섭자, WAN(wide area network) 재머 또는 GNSS(global navigation satellite systems) 재머의 형태일 수 있다. 도 8의 도면(800)은 VV(802)에 위협을 제기할 수 있는 하나의 위협 엔티티(804)를 개시한다. 그러나, 일부 양상들에서, VV(802)에 대한 위협은 하나 이상의 위협 엔티티들에 의해 제기될 수 있다. 하나 이상의 위협 엔티티들은 고정식 또는 이동식일 수 있다. 예를 들어, 고정식 위협 엔티티는 인근 건물에 또는 거리 또는 교차로 근처의 건물 외부에 로케이트될 수 있는 반면, 모바일 위협 엔티티는 차량을 포함할 수 있다.

[0050] [0081] VV(802)가 위협 엔티티(804)를 검출하면, VV(802)의 운전자는 통지를 수신할 수 있고, 정상적인 C-V2X 동작이 중단될 수 있다. C-V2X 동작은 위협 엔티티(804)가 협력적 및 자동화된 운전 결정들에서 사용되는 무선 자원들 또는 스펙트럼을 방해 또는 간섭하는 것으로 인해 위협 엔티티(804)의 검출 시에 중단될 수 있다. 예를 들어, 다른 도로 사용자들에게 위험을 제기할 수 있는 C-V2X 동작의 안전 특징들이 방해될 수 있다. 이에 따라, 위협 엔티티(804)의 검출 시에 BSM(basic safe message)들의 송신이 중단될 수 있다.

[0051] [0082] 위협 엔티티(804)는 사이버 위협일 수 있고, 도 5a 내지 도 7에서 검출된 NV들, VRU들 또는 물리적 장애물들과 유사한 방식으로 새로운 클래스의 검출된 물체들로 간주될 수 있다. 따라서, 위협 엔티티(804)의 검출은, 위협 엔티티(804)가 물리적 장애물이 아니라 스펙트럼 및/또는 보안 장애물인 것으로 인해 SDSM 또는 CPM(cooperative perception message)으로서 인코딩될 수 있다. SDSM 또는 CPM은 위협 엔티티(804)의 위협 구역(806) 외부에 있는 RV(remote vehicle)들(810)에 도달하기 위해 VV(802)에 의해 브로드캐스트될 수 있다. 일부 양상들에서, VV(802)는 SDSM 또는 CPM을 PC5 링크(812)를 통해 RV(810)에 브로드캐스트할 수 있다. RV(810)는 PC5 링크(812)를 통해 SDSM 또는 CPM을 수신하기 위해 VV(802)의 사이드링크 송신의 범위 내에 있을 수 있다. 일부 양상들에서, RV(816)는 VV(802)의 사이드링크 송신 범위를 넘어설 수 있다. 이러한 경우들에서, VV(802)는, RSU(808)가 위협 구역(806) 외부에 있고 그리고/또는 VV(802)의 사이드링크 송신 범위를 넘어선 RV(816) 및 다른 RV들에 SDSM 또는 CPM을 중계할 수 있도록, PC5 인터페이스(814)를 통해 네트워크 엔티티(예컨대, RSU(808))에 SDSM 또는 CPM을 브로드캐스트할 수 있다.

[0052] [0083] 위협 엔티티(804)의 검출 이후, VV(802)는 위협 엔티티(804)의 타입을 DoS 공격자, 오작동 차량, 재머,

OOB 간섭자, WAN 재머, 또는 GNSS 재머 중 적어도 하나인 것으로 분류하도록 구성될 수 있다. VV(802)는 위협 엔티티(804)로부터 수신된 데이터에 기초하여 위협 엔티티(804)의 타입을 분류할 수 있다. 위협 엔티티(804)로부터 수신된 데이터는 무선 디바이스들에 대한 투사된 데이터와 일치하지 않는 데이터를 포함할 수 있다. 예를 들어, 데이터는 잘못된 또는 타당하지 않은 로케이션 데이터를 포함할 수 있거나 또는 실제 속력 또는 진로를 훨씬 넘어선 위협 엔티티(804)의 속력 또는 진로에 대한 값들을 포함할 수 있다. VV(802)는 위협 엔티티(804)의 분류와 연관된 신뢰도 값을 포함할 수 있다. 일부 양상들에서, 위협 엔티티(804)의 분류는, 이를테면 VV(802)의 전체 대역폭(예컨대, 광대역)에 걸쳐 또는 각각의 서브채널(예컨대, 협대역)에 걸쳐 위협 엔티티(804)의 측정된 RSSI에 기초할 수 있다.

[0053] [0084] 일부 양상들에서, 위협 엔티티(804)의 특성들을 보고하기 위해, 위협 엔티티(804)의 특성들의 보고를 포함하는 계층적 데이터 구조가 사용될 수 있다. 일부 경우들에서, 보고는 VV(802)의 로케이션, 속력, 진로 또는 타임스탬프에 관련된 정보를 포함할 수 있다. VV(802)에서의 위협 엔티티(804)의 측정된 RSSI와 관련된 정보가 보고에 포함될 수 있다. 예를 들어, 도 11의 도면(1100)을 참조하면, 소스 데이터(1102)는 VV(802)와 관련된 정보를 포함할 수 있는 한편, 검출된 물체 데이터(1104)는 검출된 위협 엔티티(804)와 관련된 정보를 포함할 수 있다. 검출된 물체 데이터(1104)는 위협과 관련된 공통 데이터를 포함할 수 있고, 위협이 오작동 차량인지, 재머인지 또는 간섭자인지에 따라 특정 위협과 관련된 전용 정보(1106)를 더 포함할 수 있다. 도 12의 도면(1200)을 참조하면, 검출된 물체 데이터(1202)는 물리적 장애물들(1204)(예컨대, 포트홀들, VRU, 비-V2X 차량들)을 포함할 수 있고, 협력적 및 자동화된 운전 결정들에서 사용되는 무선 자원들 또는 스펙트럼을 간섭하는 검출된 물체들(1206)을 또한 포함할 수 있다. 예를 들어, 1206은 오작동 차량 데이터, 재머 데이터 또는 간섭자 데이터를 포함할 수 있다. 도 13의 도면(1300)을 참조하면, 검출된 물체들에 대한 최상위 레벨 IE(information elements)(1302)은 검출된 물체의 특정 검출된 특성들을 포함할 수 있다. 예를 들어, 데이터 엘리먼트들(1304)은 비-V2X 차량 데이터, VRU 데이터, 물리적 장애물 데이터를 포함할 수 있는 한편, 데이터 엘리먼트들(1306)은 차량 특정 검출 특성들인 오작동 차량 데이터, 검출된 재머 데이터 및 검출된 간섭자 데이터를 포함할 수 있다. 도 14의 도면(1400)을 참조하면, 도 14는 검출된 물체들의 파라미터들(1402)의 예를 제공한다. 예를 들어, 파라미터들(1402)은 위협의 포지션, 속력 및 진로를 포함할 수 있다. 검출된 재머 또는 간섭자에 대해, 파라미터들(1402)은 RSSI 값들을 포함할 수 있다. DoS 공격의 경우, 파라미터들(1402)은 포지션, 속력 또는 진로를 포함할 수 있다. 일부 양상들에서, 예를 들어, 검출된 재머 또는 간섭자에 대해, 파라미터들(1402)은 위협이 잠재적으로 상주할 수 있는 포지션 주위의 반경을 더 포함할 수 있다. 일부 양상들에서, 재밍이 일반적으로 광대역이기 때문에, 전체 C-V2X 및/또는 NR 대역폭에 걸쳐 평균 측정된 RSSI가 보고될 수 있다. 일부 양상들에서, 예를 들어, OOB 방출 및/또는 협대역 재밍을 분류하기 위해, 윈도우에 걸쳐 평균화된 각각의 서브채널에 대한 RSSI는 특정 서브채널에 대한 RSSI가 임계치를 초과하는 경우들에 대한 보고에 포함될 수 있다. 일부 양상들에서, 예를 들어, DoS 공격 및/또는 오작동 차량을 분류하기 위해, VV(802)에서의 위협 엔티티(804)의 측정된 RSSI는 관련이 없을 수 있어서, 위협 엔티티(804)의 계층 2(L2) 어드레스가 포함될 수 있고, RV들(예컨대, 810, 816)이 모뎀 계층에서 임의의 수신된 DoS 패킷들을 사전 필터링할 수 있다. 일부 양상들에서, VV(802)는, 위협 엔티티(804)가 미리 구성된 시간 인터벌에 걸쳐 검출되는 경우들에서, 위협 엔티티(804)의 검출을 보고할 수 있다. 일부 양상들에서, VV(802)는 위협 엔티티(804)의 로케이션의 측정을 결정하기 위해 위협 엔티티(804)의 측정된 RSSI를 VV(802)의 다른 센서들(예컨대, 카메라, 레이더, LIDAR)로부터의 판독들과 조합할 수 있다. 일부 양상들에서, VV(802)는 위협 엔티티(804)의 로케이션의 측정을 결정하기 위해 위협 엔티티(804)의 측정된 RSSI를 V2I 메시지들(예를 들어, MAP 정보)과 조합할 수 있다. VV(802)는 위협 엔티티(804)의 로케이션의 측정 및 위협 엔티티(804)의 로케이션의 측정의 연관된 신뢰도 값을 보고에 포함할 수 있다.

[0054] [0085] 일부 양상들에서, RV(816)는 SDSM 또는 CPM을 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. RV(816)는 위협 엔티티(804)와의 접촉을 회피 또는 완화하기 위해 SDSM 또는 CPM을 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 위협 엔티티(804)는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해할 수 있다. 일부 양상들에서, 완화 액션은 위협 엔티티(804)를 회피하기 위한 대안적인 경로(820)를 선택하는 것을 포함할 수 있다. 예를 들어, RV(816)는 스케줄링된 또는 계획된 경로(818)를 가질 수 있고, 위협 엔티티(804)의 존재를 보고하는 SDSM을 수신하는 것에 대한 응답으로 위협 엔티티(804)를 회피하기 위한 대안적인 경로(820)를 선택할 수 있다. 위협 엔티티(804)는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 실질적으로 저하시킬 수 있다. 협력적 또는 자동화된 운전 결정들은 안전 목적들을 위해 높은 신뢰도를 요구할 수 있다. 일부 양상들에서, RV(816)는 검출된 위협 엔티티 또는 임의의 위협 엔티티에 의해 영향을 가장 적게 받는 것으로 주행의 스케줄링된 루트 또는 경로(818)를 변경하기로 결정할 수 있다. RV(816)는, RV(816)가 네트워크 엔티티(808)(예컨대, 기지국)로부터 위협 엔티티(80

4)를 표시하는 SDSM을 수신하는 인스턴스들에서 위협 엔티티(804)와의 접촉을 회피 또는 완화할 수 있다. VV(802)로부터 떨어져 있는 RV(816)는 PC5를 통해 VV(802)로부터 직접 SDSM을 수신하기 위한 범위 내에 있지 않을 수 있어서, RV(816)는 Uu 링크(814)를 통해 네트워크 엔티티(808)(예컨대, 기지국)로부터 중계된 SDSM을 수신한다. RV(816)가 VV(802)로부터 떨어져 있는 것은, 위협 엔티티(804)를 회피하기 위해 대안적인 경로(820)를 취하거나, 더 견고한 MCS를 활용하거나, 또는 위협 엔티티를 가상 감지하는 것과 같은(그러나 이에 제한되지는 않음) 완화 액션을 준비하기에 충분한 시간을 RV(816)에 제공할 수 있다. 일부 양상들에서, 네트워크 엔티티(808)는 거리 교차로들에 있는 Wi-Fi 액세스 포인트들과 같은 알려진 위협들(예컨대, 정적)의 상세한 RF 핑거프린트를 제공하고 제2 무선 디바이스에 송신될 수 있는 Uu를 통해 클라우드 엔드포인트에 송신하도록 구성될 수 있는 셀룰러 액세스 포인트, 이를테면 기지국 또는 MEC(multi-access edge computing) 시스템(이에 제한되지 않음)을 포함할 수 있다. 일부 경우들에서, RSU 또는 MEC는 부분적으로 더 높은 컴퓨테이셔널 자원들 및/또는 감각 입력들을 갖는 RSU 또는 MEC로 인해 VV(802)보다 위협 엔티티(804)의 개선된 로컬화를 획득할 수 있다. 또한, RSU 또는 MEC는 위협 엔티티(804)를 보고하는 메시지를 PC5 및/또는 Uu 인터페이스들을 통해 RV(816)에 송신할 수 있다.

[0055] [0086] 일부 양상들에서, 예를 들어 도 9의 도면(900)에 도시된 바와 같이, VV1(902)은 위협 엔티티(904)의 로케이션의 측정을 결정하기 위해 동일한 위협 엔티티(904)를 보고하는 다른 VV들(예컨대, VV2(908) 및/또는 VV3(908))로부터 보고들을 수신할 수 있다. VV1(902)은 위협 엔티티(904)의 로케이션의 측정을 위협 엔티티(904)의 로케이션의 측정과 연관된 신뢰도 값과 함께 RV(910)에 송신된 보고에 포함시킬 수 있다. VV2(908) 및 VV3(908)는 또한 위협 엔티티(904)의 위협 구역(906) 내에 있을 수 있어서, VV2(908) 및 VV3(908)은 동일한 위협 엔티티를 VV1(902)에 보고한다. 일부 양상들에서, VV1(902)은 위협 엔티티(904)의 추정된 로케이션을 결정하기 위해 VV2(908) 및 VV3(908)으로부터의 보고를 위협 엔티티(904)의 측정된 RSSI 및 VV1(902)의 다른 센서들로부터의 판독들과 조합할 수 있다.

[0056] [0087] 도 10a 및 도 10b는 위협 엔티티의 검출 및 보고의 예를 예시하는 도면들(1000, 1050)이다. 예를 들어, 도면(1000)은 고속도로 시나리오의 예인 반면, 도면(1050)은 도시 시나리오의 예이다. 일부 양상들에서, VV(1002)는 검출된 위협 엔티티(1004)를, 위협 엔티티(1004)의 위협 구역(1006)을 넘어서 있을 수 있는 RV(1008)에 보고할 수 있어서, RV(1008)는 위협 엔티티(1004)를 가상으로 감지할 수 있다. 도 10a의 도면(1000)의 고속도로 시나리오와 같은 일부 경우들에서, RV(1008)는 거리에 기초하여 위협 엔티티(1004)의 위협 구역(1006)을 넘어설 수 있다. 도 10b의 도면(1050)의 도시 시나리오와 같은 일부 경우들에서, 고 손실 건물(1016)이 RV(1008)와 위협 엔티티(1004) 사이에 있기 때문에, RV(1008)는 위협 엔티티(1004)의 위협 구역을 넘어서 있을 수 있고, 따라서 고 손실 건물(1016)은 위협 엔티티(1004)의 신호가 RV(1008)의 로케이션에 도달하는 것을 차단한다.

[0057] [0088] RV(1008)는 VV(1002)로부터 수신된 보고(예컨대, SDSM(1012))에 기초하여 위협 엔티티(1004)를 가상으로 감지하고 위협 엔티티(1004)를 가상으로 감지하는 것에 기초하여 BSM을 송신할 하나 이상의 서브채널들을 결정할 수 있다. 일부 양상들에서, VV(1002)는 위협 엔티티(1004)로 인해 RSSI 임계치보다 큰 RSSI를 갖는 BSM들이 통신되는 서브채널들을 검출할 수 있다. VV(1002)는 위협 엔티티(1004)의 존재를 검출하고 관련 정보를 추출할 수 있다. 관련 정보는 위협 엔티티(1004)에 기초하여 변할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 제1 서브세트는 서브채널들의 서브세트에 대한 RSSI의 평균에 기초하여 검출될 수 있다. 이러한 양상들에서, 관련 정보는 재머 디바이스에 대응할 수 있어서, 위협 엔티티(1004)는 재머 디바이스이다. 일부 양상들에서, RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트 내의 각각의 서브채널에 대해 검출될 수 있다. 이러한 양상들에서, 관련 정보는 위협 엔티티(1004)가 OOB 간섭자이도록 OOB 간섭자에 대응할 수 있다. 관련 정보는 SDSM(1012)의 RV(1008)와 공유될 수 있다.

[0058] [0089] 일부 양상들에서, RV(1008)는 BSM(1014)을 송신할 서브채널들의 세트 중 하나 이상의 서브채널들을 결정할 수 있다. RV(1008)는 서브채널들의 제1 서브세트를 표시하는 SDSM(1012)에 적어도 부분적으로 기초하여 BSM(1014)을 송신할 서브채널들의 세트의 하나 이상의 서브채널들을 결정할 수 있다. 일부 양상들에서, 서브채널들의 제1 서브세트를 표시하는 SDSM(1012)에 적어도 부분적으로 기초한 서브채널들의 세트의 서브채널의 결정은 서브채널들의 제1 서브세트를 표시하는 추가적인 메시지들이 다른 무선 디바이스들로부터 수신되는지 여부에 추가로 기초할 수 있다. 예를 들어, RV(1008)는 위협 엔티티를 보고하는 하나 이상의 다른 VV들로부터 RV(1008)가 수신하는 추가적인 메시지들에 기초하여 어느 서브채널들이 BSM을 송신하기 위해 배제되는지를 결정할 수 있다. 다수의 VV들이 위협 엔티티(1004)에 의해 영향을 받는 위협 구역(1006) 내에 있고, RV(1008)가 위

협 엔티티(1004)의 존재를 보고하는 다수의 메시지들을 VV들로부터 수신하는 경우들에서, 다수의 메시지들의 수신은 위협 엔티티(1004)의 존재의 신뢰가능한 보고를 표시할 수 있다. 다수의 VV들이 위협 엔티티(1004)에 의해 영향을 받는 위협 구역(1006) 내에 있고, RV(1008)가 위협 엔티티(1004)의 존재를 보고하는 하나의 SDSM(1012)(또는 다수의 VV들의 수보다 훨씬 더 적은 최소량의 메시지들)을 수신하는 경우들에서, 하나의 SDSM(1012)(또는 다수의 제1 무선 디바이스의 수보다 훨씬 더 적은 최소량의 메시지들)의 수신은 신뢰가능하지 않은 보고를 표시한다. 이러한 경우들에서, RV(1008)는 BSM(1014)을 송신할 수 있지만, 보고(예컨대, SDSM)의 소스가 신뢰할 수 없다면, 위협 엔티티를 회피하기 위한 BSM(1014)의 스케줄링을 허용하도록 착수된 완화가 발동되지 않을 수 있다. RV(1008)는 결정된 적어도 하나의 서브채널 상에서 BSM(1014)을 적어도 HV(1010)에 송신할 수 있다. 송신된 BSM(1014)이 RV(1008)의 부근 내의 임의의 무선 디바이스에 송신되고 그에 의해 수신될 수 있도록, 송신된 BSM(1014)은 브로드캐스트 메시지일 수 있다. 일부 양상들에서, BSM(1014)은 하나 초과의 서브채널을 통해 송신될 수 있다.

[0059] [0090] 도 15는 제1 무선 디바이스(1502), 제2 무선 디바이스(1504) 및 제3 무선 디바이스(1506) 사이의 예시적인 통신 흐름(1500)을 예시한다. 통신은 송신 디바이스로부터 수신 디바이스로의 직접적인 V2X, V2V 또는 D2D 기반 통신에 기초할 수 있다. 디바이스(1502, 1504)로부터 송신하는 통신은 도 4와 관련하여 설명된 바와 같이, 특정 송신 디바이스의 범위 내의 다수의 수신 디바이스들에 의해 브로드캐스트 및 수신될 수 있다. 제1 무선 디바이스(1502)는 제1 UE에 대응할 수 있고, 제2 무선 디바이스(1504)는 제2 UE에 대응할 수 있다. 제1 무선 디바이스(1502), 제2 무선 디바이스(1504) 및/또는 제3 무선 디바이스(1506)는 C-V2X 엔티티에 대응할 수 있다. 예를 들어, 도 1의 상황에서, 제1 무선 디바이스(1502)는 적어도 UE(104)에 대응할 수 있고, 제2 무선 디바이스(1504)는 적어도 104'에 대응할 수 있다. 다른 예에서, 도 3의 상황에서, 제1 무선 디바이스(1502)는 디바이스(350)에 대응할 수 있고, 제2 무선 디바이스(1504)는 디바이스(310)에 대응할 수 있다.

[0060] [0091] 1508에 예시된 바와 같이, 제1 무선 디바이스(1502)는 BSM들의 송신을 간섭하는 데이터를 송신하는 위협 엔티티를 검출할 수 있다. 제1 무선 디바이스는 위협 엔티티의 존재를 검출하고 위협 엔티티와 관련된 관련 정보를 추출할 수 있다. 관련 정보는 위협 엔티티에 기초하여 변할 수 있다. 일부 양상들에서, 위협 엔티티는 DoS 공격자, 재머, 오작동 차량, OOB 간섭자, WAN 재머 또는 GNSS 재머를 포함할 수 있다. 관련 정보는 제1 무선 디바이스에 의해, 위협 엔티티의 위협 구역을 넘어선 다른 무선 디바이스들과 공유될 수 있다.

[0061] [0092] 1510에 예시된 바와 같이, 제1 무선 디바이스(1502)는 위협 엔티티의 타입과 관련된 정보를 표시하는 메시지를 송신할 수 있다. 제1 무선 디바이스는 위협 엔티티의 타입과 관련된 정보를 표시하는 메시지를 적어도 제2 무선 디바이스에 송신할 수 있다. 제2 무선 디바이스(1504)는 제1 무선 디바이스(1502)로부터 메시지를 수신할 수 있다. 일부 양상들에서, 메시지 내의 정보는 RSSI 임계치보다 큰 기준 RSSI를 갖는 서브채널들의 서브세트를 포함할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 기준 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트에 대한 RSSI의 평균에 기초할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 기준 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트 내의 각각의 서브채널에 대한 RSSI의 평균에 기초할 수 있다. 메시지 내의 정보는 서브채널들의 서브세트에 대한 평균 RSSI, 서브채널들의 서브세트 내의 각각의 서브채널에 대한 평균 RSSI, RSSI 임계치, RSSI 윈도우 시간 길이, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 또는 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 또는 이들의 조합 중 적어도 하나를 더 표시할 수 있다. 일부 양상들에서, 송신된 메시지는 SDSM, I2V 메시지 또는 CPM일 수 있다. 송신된 메시지가 제1 무선 디바이스의 부근 내의 임의의 무선 디바이스에 의해 수신될 수 있도록, 송신된 메시지는 브로드캐스트 메시지일 수 있다.

[0062] [0093] 1512에 예시된 바와 같이, 제2 무선 디바이스(1504)는 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정할 수 있다. 제2 무선 디바이스(1504)는 장치는 제1 무선 디바이스로부터 위협 엔티티와 관련된 정보를 표시하는 메시지에 적어도 부분적으로 기초하여 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정할 수 있다. 일부 양상들에서, 메시지 내의 정보는 RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트를 포함할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트에 대한 RSSI의 평균에 기초할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트 내의 각각의 서브채널에 대한 RSSI의 평균에 기초할 수 있다. 메시지 내의 정보는 서브채널들의 서브세트의 평균 RSSI, 서브채널들의 서브세트 내의 각각의 서브채널에 대한 평균

RSSI, RSSI 임계치, RSSI 윈도우 시간 길이, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 또는 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 또는 이들의 조합 중 적어도 하나를 더 표시할 수 있다. 일부 양상들에서, 후보 자원들은 후보 CSR(single-subframe resource)을 포함할 수 있고, 후보 자원들의 세트는 CSR들의 세트를 포함할 수 있다. CRM은 후보 자원들의 세트의 하나 이상의 서브채널들을 포함할 수 있다. 일부 양상들에서, 후보 자원들의 세트 중 후보 자원의 결정은, 제1 무선 디바이스로부터의 메시지에 표시된 바와 같이, 위협 구역에 대한 위협 엔티티를 표시하는 추가적인 메시지들이 다른 무선 디바이스들로부터 수신되는지 여부에 추가로 기초할 수 있다. 예를 들어, 제2 무선 디바이스는, 제2 무선 디바이스가 위협 엔티티를 보고하는 하나 이상의 다른 무선 디바이스들로부터 수신하는 추가적인 메시지들에 기초하여, BSM을 송신하기 위해 어느 후보 자원들이 배제될 수 있는지를 결정할 수 있다. 다수의 무선 디바이스들(예컨대, 피해 차량들)이 위협 엔티티에 의해 영향을 받는 구역 내에 있고, 제2 무선 디바이스가 위협 엔티티의 존재를 보고하는 다수의 무선 디바이스들(예컨대, 피해 차량들)로부터 다수의 메시지들을 수신하는 경우들에서, 다수의 메시지들 중 하나는 위협 엔티티의 존재에 대한 신뢰할 수 있는 보고를 표시할 수 있다. 다수의 무선 디바이스들(예컨대, 피해 차량들)이 위협 엔티티에 의해 영향을 받는 구역 내에 있고 제2 무선 디바이스가 위협 엔티티의 존재를 보고하는 하나의 메시지(또는 다수의 제1 무선 디바이스들의 수보다 훨씬 더 적은 최소량의 메시지들)를 수신하는 경우들에서, 하나의 메시지(또는 다수의 무선 디바이스들의 수보다 훨씬 더 적은 최소량의 메시지들)의 수신은 신뢰할 수 없는 보고를 표시할 수 있다. 이러한 경우들에서, 제2 무선 디바이스는 BSM을 송신할 수 있지만, 보고(예컨대, SDSM)의 소스가 신뢰할 수 없다면, 위협 엔티티를 회피하기 위한 BSM의 스케줄링을 허용하도록 착수된 완화가 발동되지 않을 수 있다.

[0063] [0094] 일부 양상들에서, 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정하기 위해, 제2 무선 디바이스(1504)는 후보 자원들의 세트가 LTE-V2X인지 또는 NR-V2X인지를 결정할 수 있다. 후보 자원들이 LTE-V2X인 경우들에서, 제2 무선 디바이스(1504)는 후보 자원들의 세트에서 각각의 후보 자원에 대한 투사된 RSRP(reference signal received power)가 RSRP 임계치를 초과하는 것에 기초하여 후보 자원들의 세트에서 하나 이상의 후보 자원들을 배제할 수 있다. 제2 무선 디바이스(1504)는 후보 자원들의 제1 서브세트를 결정하기 위해 RSRP 임계치를 초과하는 투사된 RSRP에 기초하여 하나 이상의 후보 자원들을 배제할 수 있다. 일부 양상들에서, 후보 자원들은 선택 풀(예컨대, 후보 자원들의 세트)에 특정 양의 후보 자원들이 남아 있을 때까지 RSRP에 기초하여 배제될 수 있다. 일부 양상들에서, 특정 양은 후보 자원들의 세트의 20%를 포함할 수 있다. 일부 양상들에서, 특정 양은 후보 자원들의 세트의 20% 초과일 수 있다. 일부 양상들에서, 제2 무선 디바이스는 또한 자신의 하프-듀플렉스 동작에 기초하여 CSR들 중 일부를 배제할 수 있다.

[0064] [0095] 일부 양상들에서, 제2 무선 디바이스(1504)는 후보 자원들의 제2 서브세트를 획득하기 위해 가중된 RSSI 랭킹에 기초하여 후보 자원들의 제1 서브세트를 랭킹할 수 있다. 후보 자원들의 제2 서브세트는 가장 낮은 가중된 RSSI를 가질 수 있다. 제2 서브세트의 후보 자원들은 후보 자원들의 제1 서브세트의 일부일 수 있다. 일부 양상들에서, 가중된 RSSI는 물리적으로 감지된 후보 자원들 및 가상으로 감지된 후보 자원들로 구성될 수 있다. 물리적으로 감지된 후보 자원들은 감지 윈도우 내에서 제2 무선 디바이스에 의해 측정된 후보 자원들을 포함할 수 있다. 가상으로 감지된 후보 자원들은 제1 무선 디바이스에 의해 측정되고 제1 무선 디바이스로부터 제2 무선 디바이스에 의해 수신된 메시지 내에 표시된 서브채널들을 포함할 수 있다. 일부 양상들에서, 가상으로 감지된 후보 자원들은 후보 자원들의 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 위협 엔티티와 연관된 로케이션 신뢰도 반경, 제1 무선 디바이스로부터 수신된 메시지와 연관된 타임스탬프, 제2 무선 디바이스의 속도, 제2 무선 디바이스의 가속도, 위협 엔티티의 로케이션과 관련된 제2 무선 디바이스의 주행 방향, 도로 기하구조와 관련된 정보, 또는 BSM과 연관된 송신 요건들, 또는 이들의 조합 중 적어도 하나에 기초할 수 있다. 일부 양상들에서, 가중된 RSSI 랭킹은 임계치를 초과하는 RSRP를 갖는 후보 자원들의 배제 이후에 남은 후보 자원들 및 하프-듀플렉스 동작으로 인한 후보 자원들의 배제 이후에 남은 후보 자원들에 기초할 수 있다.

[0065] [0096] 제2 무선 디바이스(1504)는, 가장 높은 가중된 RSSI를 갖는 제1 서브세트로부터의 후보 자원들이 선택 풀로부터 배제되도록, 가장 낮은 가중된 RSSI를 갖는 후보 자원들의 제2 서브세트를 획득하기 위해 가중된 RSSI 랭킹에 기초하여 후보 자원들의 제1 서브세트를 랭크할 수 있다. 가장 높은 가중된 RSSI를 갖는 제1 서브세트의 후보 자원들은 자원들의 특정 양(예를 들어, 20%)이 선택 풀에 남아 있을 때까지 배제될 수 있다. BSM을 송신할 후보 자원은 후보 자원들의 제2 서브세트로부터 결정될 수 있다. 후보 자원들의 제1 서브세트의 랭킹은, (예를 들어, 가상으로 감지된) 제1 무선 디바이스로부터의 메시지에서 표시된 서브채널들의 제1 서브세트에 대한 측정된 RSSI에 기초할 수 있는 가중된 RSSI에 기초할 수 있고, (예컨대, 물리적으로 감지된) 감지 윈도우에서 제2 무선 디바이스에 의한 측정들에 기초하여 후보 자원들의 투사된 RSSI에 기초할 수 있다. 제2 무선 디바이스는 감지 윈도우 동안 후보 자원들의 RSSI 측정들을 획득함으로써 물리적 감지를 수행할 수 있고, 값들이 임

계치를 초과하면 선택 풀로부터 대응하는 후보 자원들을 배제한다. 제2 무선 디바이스는 제1 무선 디바이스(예컨대, 피해 차량)로부터 수신된 메시지(예를 들어, SDSM 메시지) 내에서 보고된 RSSI 측정들에 기초하여 가상 감지를 수행하고, 재밍된 또는 간섭된 자원들(예컨대, 서브채널들)을 배제할 수 있다. 제2 무선 디바이스는 제1 무선 디바이스에 의해 보고된 재밍된 또는 간섭된 자원들(예컨대, 서브채널들)을 검출하지 못할 수 있고, 그러한 재밍된 또는 간섭된 서브채널들을 배제하기 위해 제1 무선 디바이스(예컨대, 피해 차량)에 의해 공유된 메시지 내의 정보를 활용할 수 있다. 가장 높은 가중된 RSSI를 갖는 후보 자원들의 제1 서브세트의 후보 자원들은 특정 양의 자원들이 선택 풀에 남아 있을 때까지 배제될 수 있다. 후보 자원 x의 가중된 RSSI는 하기 수식에 기초하여 결정될 수 있고:

[0066] $$RSSI_x = \alpha RSSI_{x,phy} + \beta RSSI_{x,virt}$$

[0067] 여기서, $RSSI_{x,phy}$는 물리적으로 감지된 후보 자원 x의 RSSI이고, $RSSI_{x,virt}$는 가상으로 감지된 후보 자원 x의 RSSI이고, $\alpha = 1$의 값이고, $0 \leq \beta \leq 1$이다. β의 값은 은닉된 위협 노드들에 대한 보호 레벨에 기초하여 설정될 수 있다. β의 값은, 서브채널들의 서브세트들 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 제1 무선 디바이스로부터 수신된 메시지와 연관된 타임스탬프, 제2 무선 디바이스의 속도, 제2 무선 디바이스의 가속도, 위협 엔티티의 로케이션과 관련된 제2 무선 디바이스의 주행 방향, 도로 기하구조와 관련된 정보(예컨대, MAP 정보), 또는 BSM과 연관된 송신 요건들, 또는 이들의 조합 중 적어도 하나에 기초할 수 있다. 예를 들어, 제2 무선 디바이스가 위협 엔티티로부터 멀어지게 주행하는 경우들에서 β의 값이 0에 더 가까울 수 있어서, 평균 RSSI는 물리적으로 감지된 후보 자원들에 더 의존할 수 있다. 일부 양상들에서, 제2 무선 디바이스가 위협 엔티티에 가까울 수 있고 위협 엔티티에 대한 보호를 증가시킬 수 있는 경우들에서 β의 값은 1에 더 가까울 수 있어서, 가상으로 감지된 자원들은 평균 RSSI에서 고려된다.

[0068] [0097] 일부 양상들에서, 제2 무선 디바이스는 BSM의 송신을 위해 후보 자원들의 제2 서브세트로부터 후보 자원을 선택할 수 있다.

[0069] [0098] 후보 자원들이 NR-V2X인 경우들에서, 제2 무선 디바이스(1504)는 후보 자원들의 세트에서 하나 이상의 가상으로 감지된 후보 자원들을 배제할 수 있다. 제2 무선 디바이스(1504)는, 사전-필터 임계치를 초과하는 RSSI를 갖는 후보 자원들의 세트에서 하나 이상의 가상으로 감지된 후보 자원들을 배제할 수 있다. 제2 무선 디바이스는, 사전-필터 임계치를 초과하지 않는 후보 자원들의 필터링된 서브세트를 획득하기 위해, 사전-필터 임계치를 초과하는 RSSI를 갖는 하나 이상의 가상으로 감지된 후보 자원들을 배제할 수 있다. 일부 양상들에서, 하나 이상의 가상으로 감지된 후보 자원들은 제1 무선 디바이스에 의해 측정되고 제1 무선 디바이스로부터 제2 무선 디바이스에 의해 수신된 메시지 내에 표시될 수 있다. 예를 들어, 제1 무선 디바이스는 위협 엔티티에 의해 영향을 받을 수 있는 하나 이상의 서브채널들을 물리적으로 감지할 수 있고, 제2 무선 디바이스에 송신되는 메시지에 이러한 정보를 포함할 수 있어서, 제2 무선 디바이스는 하나 이상의 서브채널들을 가상으로 감지한다. 일부 양상들에서, 가상으로 감지된 후보 자원들은 서브채널들의 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 위협 엔티티와 연관된 로케이션 신뢰도 반경, 제1 무선 디바이스로부터 수신된 메시지와 연관된 타임스탬프, 제2 무선 디바이스의 속도, 제2 무선 디바이스의 가속도, 위협 엔티티의 로케이션과 관련된 제2 무선 디바이스의 주행 방향, 도로 기하구조와 관련된 정보, 또는 BSM과 연관된 송신 요건들, 또는 이들의 조합 중 적어도 하나에 기초할 수 있다. 제2 무선 디바이스는 임계치(예컨대, $Thresh_{virt}$)를 초과하는 RSSI를 갖는 가상으로 감지된 자원들을 미리 필터링할 수 있다. 임계치를 초과하는 RSSI를 갖는 가상으로 감지된 자원들은, RSRP-기반 배제가 수행되기 전에 후보 자원들의 풀로부터 생략될 수 있다. 일부 양상들에서, 제2 무선 디바이스는, 특정 양의 후보 자원들이 후보 자원들의 선택 풀에서 이용가능하게 남아있을 때까지 제1 무선 디바이스에 의해 제공된 하나 이상의 서브채널들의 가상으로 감지된 RSSI 측정들에 기초하여, 가상으로 감지된 후보 자원들을 미리 필터링할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 자원들의 특정 양의 20%가 선택 풀(예컨대, 필터링된 서브세트)에서 이용가능하게 남아있을 때까지 가상으로 감지된 후보 자원들을 미리 필터링할 수 있다. 20 퍼센트인 특정 양은 단지 예일 뿐이며, 본원에서 제공된 예로 제한되도록 의도되지 않는다. 일부 양상들에서, 특정 양은 20% 초과일 수 있다.

[0070] [0099] 일부 양상들에서, 제2 무선 디바이스(1504)는 RSRP 임계치를 초과하지 않는 후보 자원들의 제2 서브세트

를 획득하기 위해, RSRP 임계치를 초과하는 사전-필터 임계치를 초과하지 않는, 후보 자원들의 필터링된 서브세트 내의 후보 자원들을 배제할 수 있다. 일부 양상들에서, 후보 자원들의 제2 서브세트는, 사전-필터 임계치를 초과하지 않는, 선택 풀 내의 총 후보 자원들의 미리 구성된 비율을 포함할 수 있다. 일부 양상들에서, 사전-필터 임계치는, 후보 자원들의 제2 서브세트가 선택 풀 내의 총 후보 자원들의 미리 구성된 비율 미만의 후보 자원들의 양을 포함하면 조정될 수 있다. 사전-필터 임계치는, 후보 자원들의 제2 서브세트가 선택 풀 내의 총 후보 자원들의 미리 구성된 비율을 포함할 때까지 추가로 조정될 수 있다. 일부 양상들에서, 선택 풀 내의 총 후보 자원들의 미리 구성된 비율은 20%를 포함할 수 있다. 일부 양상들에서, 선택 풀 내의 총 후보 자원들의 미리 구성된 비율은 20% 초과를 포함할 수 있다. 일부 양상들에서, RSRP 임계치는 후보 자원들의 제2 서브세트가 선택 풀에서 총 후보 자원들의 미리 구성된 비율을 포함하도록 조정될 수 있다. RSRP 임계치는, 사전-필터 임계치를 조정하는 것에 추가하여 또는 이에 대한 대안으로 조정될 수 있다.

[0071] [0100] BSM을 송신할 적어도 하나의 서브채널을 포함하는 후보 자원은 후보 자원들의 제2 서브세트로부터 결정될 수 있다. 일부 양상들에서, 제2 무선 디바이스는 BSM을 송신할 후보 자원을 선택하기 전에, 자신의 하프 듀플렉스 동작에 기초하여 후보 자원들 중 일부를 배제할 수 있다. 사전-필터 임계치(예컨대, $Thresh_{virt}$)는 위에서 논의된 β 파라미터와 유사한 방식으로 기능할 수 있다. 예를 들어, 사전-필터 임계치(예컨대, $Thresh_{virt}$)는 가상으로 감지된 자원들에 대한 보호 레벨에 기초하여 조정될 수 있다. 예를 들어, 가상으로 감지된 자원들에 대한 더 많은 보호가 요구되면, 사전-필터 임계치의 값이 감소될 수 있다. 사전-필터 임계치를 감소시키는 것은 가상으로 감지된 자원들을 더 많이 배제할 수 있다. 일부 양상들에서, 사전-필터 임계치는, 서브채널들의 서브세트들 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 제1 무선 디바이스로부터 수신된 메시지와 연관된 타임스탬프, 제2 무선 디바이스의 속도, 제2 무선 디바이스의 가속도, 위협 엔티티의 로케이션과 관련된 제2 무선 디바이스의 주행 방향, 도로 기하구조와 관련된 정보, 또는 BSM과 연관된 송신 요건들, 또는 이들의 조합 중 적어도 하나에 기초할 수 있다.

[0072] [0101] 일부 양상들에서, 사전-필터 임계치(예컨대, $Thresh_{virt}$)에 기초한 가상으로 감지된 자원들의 사전-필터링은 RSRP-기반 배제와 협력할 수 있다. 예를 들어, RSRP-기반 배제 후에 특정 양(예컨대, 20%) 미만의 자원들이 선택 풀(예컨대, 후보 자원들의 제2 서브세트)에서 이용가능하면, 제2 무선 디바이스는, 더 적은 자원들이 배제되고 특정 양(예컨대, 20%)의 자원들이 선택 풀(예컨대, 후보 자원들의 제2 서브세트)에서 이용가능하도록, 임계치(예컨대, $Thresh_{virt}$)의 값을 조정할 수 있다. 이 방식은 또한 NR-V2X의 경우 지속적인 비-은닉(예컨대, 물리적으로 감지된) 위협 엔티티들을 회피하는 데 사용될 수 있다.

[0073] [0102] 일부 양상들에서, 제2 무선 디바이스(1504)는 BSM의 송신을 위해 후보 자원들의 제2 서브세트로부터 후보 자원을 선택할 수 있다.

[0074] [0103] 1514에 예시된 바와 같이, 제2 무선 디바이스(1504)는 결정된 후보 자원 상에서 적어도 제3 무선 디바이스(1506)에 BSM을 송신할 수 있다. 제3 무선 디바이스(1506)는 제2 무선 디바이스(1504)로부터 BSM을 수신할 수 있다. 송신된 BSM이 제2 무선 디바이스(1504)의 부근 내의 임의의 무선 디바이스에 송신되고 그에 의해 수신될 수 있도록, 송신된 BSM은 브로드캐스트 메시지일 수 있다. 일부 양상들에서, BSM은 후보 자원 상에서 송신될 수 있으며, 여기서 후보 자원은 하나 이상의 서브채널들을 포함할 수 있다.

[0075] [0104] 도 16은 무선 통신 방법의 흐름도(1600)이다. 방법은 UE 또는 UE의 컴포넌트에 의해 수행될 수 있다(예컨대, UE(104); 장치(1702); 메모리(360)를 포함할 수 있고 전체 UE(350) 또는 UE(350)의 컴포넌트, 이를테면 TX 프로세서(368), RX 프로세서(356) 및/또는 제어기/프로세서(359)일 수 있는 셀룰러 기저대역 프로세서(1704)). 예시된 동작들 중 하나 이상은 선택적이거나, 생략되거나, 전치되거나, 또는 동시적일 수 있다. 방법은, 다른 무선 디바이스들이 위협 엔티티를 가상으로 감지하도록, 제1 무선 디바이스가 검출된 위협 엔티티의 정보를 위협 엔티티의 위협 구역을 넘어선 다른 무선 디바이스들과 공유하게 할 수 있다.

[0076] [0105] 1602에서, 제1 무선 디바이스는 BSM들의 송신을 간섭하는 데이터를 송신하는 위협 엔티티를 검출할 수 있다. 예를 들어, 1602는 장치(1702)의 검출 컴포넌트(1740)에 의해 수행될 수 있다. 제1 무선 디바이스는 위협 엔티티의 존재를 검출하고 위협 엔티티와 관련된 관련 정보를 추출할 수 있다. 관련 정보는 위협 엔티티에 기초하여 변할 수 있다. 일부 양상들에서, 위협 엔티티는 DoS 공격자, 재머, 오작동 차량, OOB 간섭자, WAN 재머 또는 GNSS 재머를 포함할 수 있다. 관련 정보는 제1 무선 디바이스에 의해, 위협 엔티티의 위협 구역을 넘

어선 다른 무선 디바이스들과 공유될 수 있다.

[0077] [0106] 1604에서, 제1 무선 디바이스는 위협 엔티티의 타입과 관련된 정보를 표시하는 메시지를 송신할 수 있다. 예를 들어, 1604는 장치(1702)의 메시지 컴포넌트(1742)에 의해 수행될 수 있다. 제1 무선 디바이스는 위협 엔티티의 타입과 관련된 정보를 표시하는 메시지를 적어도 제2 무선 디바이스에 송신할 수 있다. 일부 양상들에서, 메시지 내의 정보는 RSSI 임계치보다 큰 기준 RSSI를 갖는 서브채널들의 서브세트를 포함할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 기준 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트에 대한 RSSI의 평균에 기초할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 기준 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트 내의 각각의 서브채널에 대한 RSSI의 평균에 기초할 수 있다. 메시지 내의 정보는 서브채널들의 서브세트에 대한 평균 RSSI, 서브채널들의 서브세트 내의 각각의 서브채널에 대한 평균 RSSI, RSSI 임계치, RSSI 윈도우 시간 길이, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 또는 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 또는 이들의 조합 중 적어도 하나를 더 표시할 수 있다. 일부 양상들에서, 송신된 메시지는 SDSM, I2V 메시지 또는 CPM일 수 있다. 송신된 메시지가 제1 무선 디바이스의 부근 내의 임의의 무선 디바이스에 의해 수신될 수 있도록, 송신된 메시지는 브로드캐스트 메시지일 수 있다.

[0078] [0107] 도 17은 장치(1702)에 대한 하드웨어 구현의 예를 예시하는 도면(1700)이다. 장치(1702)는 UE이고, 셀룰러 RF 트랜시버(1722) 및 하나 이상의 SIM(subscriber identity module) 카드들(1720)에 커플링된 셀룰러 기저대역 프로세서(1704)(또한 모뎀으로 지칭됨), SD(secure digital) 카드(1708) 및 스크린(1710)에 커플링된 애플리케이션 프로세서(1706), 블루투스 모듈(1712), WLAN(wireless local area network) 모듈(1714), GNSS 모듈(1716) 및 전력 공급 장치(1718)를 포함한다. GNSS 모듈(1716)은 다양한 위성 포지셔닝 시스템들을 포함할 수 있다. 예를 들어, GNSS 모듈은 GPS(Global Positioning System), GLONASS(Global Navigation Satellite System), Galileo, BDS(BeiDou Navigation Satellite System), WAAS(Wide Area Augmentation System), EGNOS(European Geostationary Navigation Overlay Service), GAGAN(GPS Aided GEO Augmented Navigation), MSAS(MTSAT(Multifunctional Transport Satellites) Satellite Augmentation System), QZSS(Quasi-Zenith Satellite System), 또는 NavIC(Navigation with Indian Constellation)에 대응할 수 있다. 셀룰러 기저대역 프로세서(1704)는 셀룰러 RF 트랜시버(1722)를 통해 UE(104) 및/또는 BS(102/180)와 통신한다. 셀룰러 기저대역 프로세서(1704)는 컴퓨터 판독가능 매체/메모리를 포함할 수 있다. 컴퓨터 판독가능 매체/메모리는 비일시적일 수 있다. 셀룰러 기저대역 프로세서(1704)는, 컴퓨터 판독가능 매체/메모리 상에 저장된 소프트웨어의 실행을 포함하는 일반적인 프로세싱을 담당한다. 소프트웨어는, 셀룰러 기저대역 프로세서(1704)에 의해 실행될 때, 셀룰러 기저대역 프로세서(1704)로 하여금, 위에서 설명된 다양한 기능들을 수행하게 한다. 컴퓨터 판독가능 매체/메모리는 또한, 소프트웨어를 실행하는 경우 셀룰러 기저대역 프로세서(1704)에 의해 조작되는 데이터를 저장하기 위해 사용될 수 있다. 셀룰러 기저대역 프로세서(1704)는 수신 컴포넌트(1730), 통신 관리자(1732) 및 송신 컴포넌트(1734)를 더 포함한다. 통신 관리자(1732)는 하나 이상의 예시된 컴포넌트들을 포함한다. 통신 관리자(1732) 내의 컴포넌트들은 컴퓨터 판독가능 매체/메모리에 저장되고 그리고/또는 셀룰러 기저대역 프로세서(1704) 내의 하드웨어로서 구성될 수 있다. 셀룰러 기저대역 프로세서(1704)는 UE(350)의 컴포넌트일 수 있고, 메모리(360) 및/또는 TX 프로세서(368), RX 프로세서(356) 및 제어기/프로세서(359) 중 적어도 하나를 포함할 수 있다. 일 구성에서, 장치(1702)는 모뎀 칩일 수 있고, 단지 기저대역 프로세서(1704)를 포함할 수 있고, 다른 구성에서, 장치(1702)는 전체 UE(예컨대, 도 3의 350 참조)일 수 있고, 장치(1702)의 앞서 논의된 추가적인 모듈들을 포함할 수 있다.

[0079] [0108] 통신 관리자(1732)는 예컨대, 도 16의 1602와 관련하여 설명된 바와 같이, BSM들의 송신을 간섭하는 데이터를 송신하는 위협 엔티티를 검출하도록 구성된 검출 컴포넌트(1740)를 포함한다. 통신 관리자(1732)는 예컨대, 도 16의 1604와 관련하여 설명된 바와 같이, 위협 엔티티의 타입과 관련된 정보를 표시하는 메시지를 송신하도록 구성되는 메시지 컴포넌트(1742)를 더 포함한다.

[0080] [0109] 장치는 도 16의 전술된 흐름도에서의 알고리즘의 블록들 각각을 수행하는 추가적인 컴포넌트들을 포함할 수 있다. 따라서, 도 16의 전술된 흐름도에서의 각각의 블록은 컴포넌트에 의해 수행될 수 있고, 장치는 그러한 컴포넌트들 중 하나 이상을 포함할 수 있다. 컴포넌트들은, 언급된 프로세스들/알고리즘을 수행하도록 특정적으로 구성된 하나 이상의 하드웨어 컴포넌트들일 수 있거나, 언급된 프로세스들/알고리즘을 수행하도록 구성된 프로세서에 의해 구현될 수 있거나, 프로세서에 의한 구현을 위해 컴퓨터 판독가능 매체 내에 저장될 수 있거나, 이들의 일부 조합일 수 있다.

[0081] [0110] 일 구성에서, 장치(1702), 및 특히 셀룰러 기저대역 프로세서(1704)는 BSM들의 송신을 간섭하는 데이터를 송신하는 위협 엔티티를 검출하기 위한 수단을 포함한다. 장치는 위협 엔티티의 타입과 관련된 정보를 표시하는 메시지를 제2 무선 디바이스에 송신하기 위한 수단을 포함한다. 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 장치(1702)의 전술된 컴포넌트들 중 하나 이상일 수 있다. 위에서 설명된 바와 같이, 장치(1702)는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)를 포함할 수 있다. 따라서, 일 구성에서, 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)일 수 있다.

[0082] [0111] 도 18은 무선 통신 방법의 흐름도(1800)이다. 방법은 UE 또는 UE의 컴포넌트에 의해 수행될 수 있다(예컨대, UE(104); 장치(2002); 메모리(360)를 포함할 수 있고 전체 UE(350) 또는 UE(350)의 컴포넌트, 이를테면 TX 프로세서(368), RX 프로세서(356) 및/또는 제어기/프로세서(359)일 수 있는 셀룰러 기저대역 프로세서(2004)). 예시된 동작들 중 하나 이상은 선택적이거나, 생략되거나, 전치되거나, 또는 동시적일 수 있다. 방법은, 위협 엔티티를 가상으로 감지하는 것에 기초하여 제2 무선 디바이스가 BSM을 송신할 후보 자원을 결정하게 할 수 있다.

[0083] [0112] 1802에서, 제2 무선 디바이스는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신할 수 있다. 예를 들어, 1802는 장치(2002)의 메시지 컴포넌트(2040)에 의해 수행될 수 있다. 위협 엔티티는 BSM들의 송신을 간섭하는 데이터를 송신할 수 있다. 제2 무선 디바이스는 제1 무선 디바이스로부터 메시지를 수신할 수 있다. 일부 양상들에서, 제1 무선 디바이스로부터 수신된 메시지는 SDSM, I2V 메시지 또는 CPM을 포함할 수 있다. 일부 양상들에서, 위협 엔티티는 DoS 공격자, 재머, 오작동 차량, OOB 간섭자, WAN 재머 또는 GNSS 재머를 포함할 수 있다.

[0084] [0113] 1804에서, 제2 무선 디바이스는 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정할 수 있다. 예를 들어, 1804는 장치(2002)의 결정 컴포넌트(2042)에 의해 수행될 수 있다. 제2 무선 디바이스는 장치는 제1 무선 디바이스로부터 위협 엔티티와 관련된 정보를 표시하는 메시지에 적어도 부분적으로 기초하여 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정할 수 있다. 일부 양상들에서, 메시지 내의 정보는 RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트를 포함할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트에 대한 RSSI의 평균에 기초할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트 내의 각각의 서브채널에 대한 RSSI의 평균에 기초할 수 있다. 메시지 내의 정보는 서브채널들의 서브세트의 평균 RSSI, 서브채널들의 서브세트 내의 각각의 서브채널에 대한 평균 RSSI, RSSI 임계치, RSSI 윈도우 시간 길이, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 또는 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 또는 이들의 조합 중 적어도 하나를 더 표시할 수 있다. 일부 양상들에서, 후보 자원들은 CSR을 포함할 수 있고, 후보 자원들의 세트는 CSR들의 세트를 포함할 수 있다. CRM은 후보 자원들의 세트의 하나 이상의 서브채널들을 포함할 수 있다. 일부 양상들에서, 후보 자원들의 세트 중 후보 자원의 결정은, 제1 무선 디바이스로부터의 메시지에 표시된 바와 같이, 위협 구역에 대한 위협 엔티티를 표시하는 추가적인 메시지들이 다른 무선 디바이스들로부터 수신되는지 여부에 추가로 기초할 수 있다. 예를 들어, 제2 무선 디바이스는, 제2 무선 디바이스가 위협 엔티티를 보고하는 하나 이상의 다른 무선 디바이스들로부터 수신하는 추가적인 메시지들에 기초하여, BSM을 송신하기 위해 어느 후보 자원들이 배제될 수 있는지를 결정할 수 있다. 다수의 무선 디바이스들(예컨대, 피해 차량들)이 위협 엔티티에 의해 영향을 받는 구역 내에 있고, 제2 무선 디바이스가 위협 엔티티의 존재를 보고하는 다수의 무선 디바이스들(예컨대, 피해 차량들)로부터 다수의 메시지들을 수신하는 경우들에서, 다수의 메시지들 중 하나는 위협 엔티티의 존재에 대한 신뢰할 수 있는 보고를 표시할 수 있다. 다수의 무선 디바이스들(예컨대, 피해 차량들)이 위협 엔티티에 의해 영향을 받는 구역 내에 있고 제2 무선 디바이스가 위협 엔티티의 존재를 보고하는 하나의 메시지(또는 다수의 무선 디바이스들의 수보다 훨씬 더 적은 최소량의 메시지들)를 수신하는 경우들에서, 하나의 메시지(또는 다수의 무선 디바이스들의 수보다 훨씬 더 적은 최소량의 메시지들)의 수신은 신뢰할 수 없는 보고를 표시할 수 있다. 이러한 경우들에서, 제2 무선 디바이스는 BSM을 송신할 수 있지만, 보고(예컨대, SDSM)의 소스가 신뢰할 수 없다면, 위협 엔티티를 회피하기 위한 BSM의 스케줄링을 허용하도록 착수된 완화가 발동되지 않을 수 있다.

[0085] [0114] 1806에서, 제2 무선 디바이스는 결정된 후보 자원 상에서 BSM을 송신할 수 있다. 예를 들어, 1806은 장치(2002)의 BSM 컴포넌트(2044)에 의해 수행될 수 있다. 제2 무선 디바이스는 결정된 후보 자원 상에서 적어도

제3 무선 디바이스에 BSM을 송신할 수 있다. 송신된 BSM이 제2 무선 디바이스의 부근 내의 임의의 무선 디바이스에 송신되고 그에 의해 수신될 수 있도록, 송신된 BSM은 브로드캐스트 메시지일 수 있다. 일부 양상들에서, BSM은 후보 자원 상에서 송신될 수 있으며, 여기서 후보 자원은 하나 이상의 서브채널들을 포함할 수 있다.

[0086] [0115] 도 19는 무선 통신 방법의 흐름도(1900)이다. 방법은 UE 또는 UE의 컴포넌트에 의해 수행될 수 있다(예컨대, UE(104); 장치(2002); 메모리(360)를 포함할 수 있고 전체 UE(350) 또는 UE(350)의 컴포넌트, 이를테면 TX 프로세서(368), RX 프로세서(356) 및/또는 제어기/프로세서(359)일 수 있는 셀룰러 기저대역 프로세서(2004)). 예시된 동작들 중 하나 이상은 선택적이거나, 생략되거나, 전치되거나, 또는 동시적일 수 있다. 방법은, 위협 엔티티를 가상으로 감지하는 것에 기초하여 제2 무선 디바이스가 BSM을 송신할 후보 자원을 결정하게 할 수 있다.

[0087] [0116] 1902에서, 제2 무선 디바이스는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신할 수 있다. 예를 들어, 1902는 장치(2002)의 메시지 컴포넌트(2040)에 의해 수행될 수 있다. 위협 엔티티는 BSM들의 송신을 간섭하는 데이터를 송신할 수 있다. 제2 무선 디바이스는 제1 무선 디바이스로부터 메시지를 수신할 수 있다. 일부 양상들에서, 제1 무선 디바이스로부터 수신된 메시지는 SDSM, I2V 메시지 또는 CPM을 포함할 수 있다. 일부 양상들에서, 위협 엔티티는 DoS 공격자, 재머, 오작동 차량, OOB 간섭자, WAN 재머 또는 GNSS 재머를 포함할 수 있다.

[0088] [0117] 1904에서, 제2 무선 디바이스는 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정할 수 있다. 예를 들어, 1904는 장치(2002)의 결정 컴포넌트(2042)에 의해 수행될 수 있다. 제2 무선 디바이스는 장치는 제1 무선 디바이스로부터 위협 엔티티와 관련된 정보를 표시하는 메시지에 적어도 부분적으로 기초하여 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정할 수 있다. 일부 양상들에서, 메시지 내의 정보는 RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트를 포함할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트에 대한 RSSI의 평균에 기초할 수 있다. 일부 양상들에서, RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트는, 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 서브채널들의 서브세트 내의 각각의 서브채널에 대한 RSSI의 평균에 기초할 수 있다. 메시지 내의 정보는 서브채널들의 서브세트에 대한 평균 RSSI, 서브채널들의 서브세트 내의 각각의 서브채널에 대한 평균 RSSI, RSSI 임계치, RSSI 윈도우 시간 길이, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 또는 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 또는 이들의 조합 중 적어도 하나를 더 표시할 수 있다. 일부 양상들에서, 후보 자원들은 CSR을 포함할 수 있고, 후보 자원들의 세트는 CSR들의 세트를 포함할 수 있다. CRM은 후보 자원들의 세트의 하나 이상의 서브채널들을 포함할 수 있다. 일부 양상들에서, 후보 자원들의 세트 중 후보 자원의 결정은, 제1 무선 디바이스로부터의 메시지에 표시된 바와 같이, 위협 구역에 대한 위협 엔티티를 표시하는 추가적인 메시지들이 다른 무선 디바이스들로부터 수신되는지 여부에 추가로 기초할 수 있다. 예를 들어, 제2 무선 디바이스는, 제2 무선 디바이스가 위협 엔티티를 보고하는 하나 이상의 다른 무선 디바이스들로부터 수신하는 추가적인 메시지들에 기초하여, BSM을 송신하기 위해 어느 후보 자원들이 배제될 수 있는지를 결정할 수 있다. 다수의 무선 디바이스들(예컨대, 피해 차량들)이 위협 엔티티에 의해 영향을 받는 구역 내에 있고, 제2 무선 디바이스가 위협 엔티티의 존재를 보고하는 다수의 무선 디바이스들(예컨대, 피해 차량들)로부터 다수의 메시지들을 수신하는 경우들에서, 다수의 메시지들 중 하나는 위협 엔티티의 존재에 대한 신뢰할 수 있는 보고를 표시할 수 있다. 다수의 무선 디바이스들(예컨대, 피해 차량들)이 위협 엔티티에 의해 영향을 받는 구역 내에 있고 제2 무선 디바이스가 위협 엔티티의 존재를 보고하는 하나의 메시지(또는 다수의 무선 디바이스들의 수보다 훨씬 더 적은 최소량의 메시지들)를 수신하는 경우들에서, 하나의 메시지(또는 다수의 무선 디바이스들의 수보다 훨씬 더 적은 최소량의 메시지들)의 수신은 신뢰할 수 없는 보고를 표시할 수 있다. 이러한 경우들에서, 제2 무선 디바이스는 BSM을 송신할 수 있지만, 보고(예컨대, SDSM)의 소스가 신뢰할 수 없다면, 위협 엔티티를 회피하기 위한 BSM의 스케줄링을 허용하도록 착수된 완화가 발동되지 않을 수 있다.

[0089] [0118] 일부 양상들에서, 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정하기 위해, 제2 무선 디바이스는 후보 자원들의 세트가 LTE-V2X인지 또는 NR-V2X인지를 결정할 수 있다. 후보 자원들이 LTE-V2X인 경우들에서, 제2 무선 디바이스는 1908에서 후보 자원들의 세트에서 하나 이상의 후보 자원들을 배제할 수 있다. 예를 들어, 1908은 장치(2002)의 결정 컴포넌트(2042)에 의해 수행될 수 있다. 제2 무선 디바이스는 후보 자원들의 세트에서 각각의 후보 자원에 대한 투사된 RSRP가 RSRP 임계치를 초과하는 것에 기초하여 후보 자원들의 세트에서 하나 이상의 후보 자원들을 배제할 수 있다. 제2 무선 디바이스는 후보 자원들의 제1 서브세트를 결정하기

위해 RSRP 임계치를 초과하는 투사된 RSRP에 기초하여 하나 이상의 후보 자원들을 배제할 수 있다. 일부 양상들에서, 후보 자원들은 선택 풀(예컨대, 후보 자원들의 세트)에 특정 양의 후보 자원들이 남아 있을 때까지 RSRP에 기초하여 배제될 수 있다. 일부 양상들에서, 특정 양은 후보 자원들의 세트의 20%를 포함할 수 있다. 일부 양상들에서, 특정 양은 후보 자원들의 세트의 20% 초과일 수 있다. 일부 양상들에서, 제2 무선 디바이스는 또한 자신의 하프-듀플렉스 동작에 기초하여 CSR들 중 일부를 배제할 수 있다.

[0090] [0119] 1910에서, 제2 무선 디바이스는 가중된 RSSI 랭킹에 기초하여 후보 자원들의 제1 서브세트를 랭킹할 수 있다. 예를 들어, 1910은 장치(2002)의 결정 컴포넌트(2042)에 의해 수행될 수 있다. 제2 무선 디바이스는 후보 자원들의 제2 서브세트를 획득하기 위해 가중된 RSSI 랭킹에 기초하여 후보 자원들의 제1 랭킹된 서브세트를 랭킹할 수 있다. 후보 자원들의 제2 서브세트는 가장 낮은 가중된 RSSI를 가질 수 있다. 제2 서브세트의 후보 자원들은 후보 자원들의 제1 서브세트의 일부일 수 있다. 일부 양상들에서, 가중된 RSSI는 물리적으로 감지된 후보 자원들 및 가상으로 감지된 후보 자원들로 구성될 수 있다. 물리적으로 감지된 후보 자원들은 감지 윈도우 내에서 제2 무선 디바이스에 의해 측정된 후보 자원들을 포함할 수 있다. 가상으로 감지된 후보 자원들은 제1 무선 디바이스에 의해 측정되고 제1 무선 디바이스로부터 제2 무선 디바이스에 의해 수신된 메시지 내에 표시된 서브채널들을 포함할 수 있다. 일부 양상들에서, 가상으로 감지된 후보 자원들은 후보 자원들의 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 위협 엔티티와 연관된 로케이션 신뢰도 반경, 제1 무선 디바이스로부터 수신된 메시지와 연관된 타임스탬프, 제2 무선 디바이스의 속도, 제2 무선 디바이스의 가속도, 위협 엔티티의 로케이션과 관련된 제2 무선 디바이스의 주행 방향, 도로 기하구조와 관련된 정보, 또는 BSM과 연관된 송신 요건들, 또는 이들의 조합 중 적어도 하나에 기초할 수 있다. 일부 양상들에서, 가중된 RSSI 랭킹은 임계치를 초과하는 RSRP를 갖는 후보 자원들의 배제 이후에 남은 후보 자원들 및 하프-듀플렉스 동작으로 인한 후보 자원들의 배제 이후에 남은 후보 자원들에 기초할 수 있다.

[0091] [0120] 제2 무선 디바이스는, 가장 높은 가중된 RSSI를 갖는 제1 서브세트로부터의 후보 자원들이 선택 풀로부터 배제되도록, 가장 낮은 가중된 RSSI를 갖는 후보 자원들의 제2 서브세트를 획득하기 위해 가중된 RSSI 랭킹에 기초하여 후보 자원들의 제1 랭킹된 서브세트를 랭크할 수 있다. 가장 높은 가중된 RSSI를 갖는 제1 서브세트의 후보 자원들은 자원들의 특정 양(예를 들어, 20%)이 선택 풀에 남아 있을 때까지 배제될 수 있다. BSM을 송신할 후보 자원은 후보 자원들의 제2 서브세트로부터 결정될 수 있다. 후보 자원들의 제1 서브세트의 랭킹은, (예를 들어, 가상으로 감지된) 제1 무선 디바이스로부터의 메시지에서 표시된 서브채널들의 제1 서브세트에 대한 측정된 RSSI에 기초할 수 있는 가중된 RSSI에 기초할 수 있고, (예컨대, 물리적으로 감지된) 감지 윈도우에서 제2 무선 디바이스에 의한 측정들에 기초하여 후보 자원들의 투사된 RSSI에 기초할 수 있다. 제2 무선 디바이스는 감지 윈도우 동안 후보 자원들의 RSSI 측정들을 획득함으로써 물리적 감지를 수행할 수 있고, 값들이 임계치를 초과하면 선택 풀로부터 대응하는 후보 자원들을 배제한다. 제2 무선 디바이스는 제1 무선 디바이스(예컨대, 피해 차량)로부터 수신된 메시지(예를 들어, SDSM 메시지) 내에서 보고된 RSSI 측정들에 기초하여 가상 감지를 수행하고, 재밍된 또는 간섭된 자원들(예컨대, 서브채널들)을 배제할 수 있다. 제2 무선 디바이스는 제1 무선 디바이스에 의해 보고된 재밍된 또는 간섭된 자원들(예컨대, 서브채널들)을 검출하지 못할 수 있고, 그러한 재밍된 또는 간섭된 서브채널들을 배제하기 위해 제1 무선 디바이스(예컨대, 피해 차량)에 의해 공유된 메시지 내의 정보를 활용할 수 있다. 가장 높은 가중된 RSSI를 갖는 후보 자원들의 제1 서브세트의 후보 자원들은 특정 양의 자원들이 선택 풀에 남아 있을 때까지 배제될 수 있다. 후보 자원 x의 가중된 RSSI는 하기 수식에 기초하여 결정될 수 있고:

[0092] $$RSSI_x = \alpha RSSI_{x,phy} + \beta RSSI_{x,virt}$$

[0093] 여기서, $RSSI_{x,phy}$는 물리적으로 감지된 후보 자원 x의 RSSI이고, $RSSI_{x,virt}$는 가상으로 감지된 후보 자원 x의 RSSI이고, $\alpha = 1$의 값이고, 그리고 0 $0 \leq \beta \leq 1$이다. β의 값은 은닉된 위협 노드들에 대한 보호 레벨에 기초하여 설정될 수 있다. β의 값은, 서브채널들의 서브세트들 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 제1 무선 디바이스로부터 수신된 메시지와 연관된 타임스탬프, 제2 무선 디바이스의 속도, 제2 무선 디바이스의 가속도, 위협 엔티티의 로케이션과 관련된 제2 무선 디바이스의 주행 방향, 도로 기하구조와 관련된 정보(예컨대, MAP 정보), 또는 BSM과 연관된 송신 요건들, 또는 이들의 조합 중 적어도 하나에 기초할 수 있다. 예를 들어, 제2 무선 디바이스가 위협 엔티티로부터 멀어지게 주행하는 경우들에서 β의 값이

0에 더 가까울 수 있어서, 평균 RSSI는 물리적으로 감지된 후보 자원들에 더 의존할 수 있다. 일부 양상들에서, 제2 무선 디바이스가 위협 엔티티에 가까울 수 있고 위협 엔티티에 대한 보호를 증가시킬 수 있는 경우들에서 β의 값은 1에 더 가까울 수 있어서, 가상으로 감지된 자원들은 평균 RSSI에서 고려된다.

[0094] [0121] 1912에서, 제2 무선 디바이스는 후보 자원을 선택할 수 있다. 예를 들어, 1912는 장치(2002)의 결정 컴포넌트(2042)에 의해 수행될 수 있다. 제2 무선 디바이스는 BSM의 송신을 위해 후보 자원들의 제2 서브세트로부터 후보 자원을 선택할 수 있다.

[0095] [0122] 후보 자원들이 NR-V2X인 경우들에서, 제2 무선 디바이스는 1914에서 후보 자원들의 세트에서 하나 이상의 가상으로 감지된 후보 자원들을 배제할 수 있다. 예를 들어, 1914는 장치(2002)의 결정 컴포넌트(2042)에 의해 수행될 수 있다. 제2 무선 디바이스는, 사전-필터 임계치를 초과하는 RSSI를 갖는 후보 자원들의 세트에서 하나 이상의 가상으로 감지된 후보 자원들을 배제할 수 있다. 제2 무선 디바이스는, 사전-필터 임계치를 초과하지 않는 후보 자원들의 필터링된 서브세트를 획득하기 위해, 사전-필터 임계치를 초과하는 RSSI를 갖는 하나 이상의 가상으로 감지된 후보 자원들을 배제할 수 있다. 일부 양상들에서, 하나 이상의 가상으로 감지된 후보 자원들은 제1 무선 디바이스에 의해 측정되고 제1 무선 디바이스로부터 제2 무선 디바이스에 의해 수신된 메시지 내에 표시될 수 있다. 예를 들어, 제1 무선 디바이스는 위협 엔티티에 의해 영향을 받을 수 있는 하나 이상의 서브채널들을 물리적으로 감지할 수 있고, 제2 무선 디바이스에 송신되는 메시지에 이러한 정보를 포함할 수 있어서, 제2 무선 디바이스는 하나 이상의 서브채널들을 가상으로 감지한다. 일부 양상들에서, 가상으로 감지된 후보 자원들은 서브채널들의 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 위협 엔티티와 연관된 로케이션 신뢰도 반경, 제1 무선 디바이스로부터 수신된 메시지와 연관된 타임스탬프, 제2 무선 디바이스의 속도, 제2 무선 디바이스의 가속도, 위협 엔티티의 로케이션과 관련된 제2 무선 디바이스의 주행 방향, 도로 기하구조와 관련된 정보, 또는 BSM과 연관된 송신 요건들, 또는 이들의 조합 중 적어도 하나에 기초할 수 있다. 제2 무선 디바이스는 임계치(예컨대, $Thresh_{virt}$)를 초과하는 RSSI를 갖는 가상으로 감지된 자원들을 미리 필터링할 수 있다. 임계치를 초과하는 RSSI를 갖는 가상으로 감지된 자원들은, RSRP-기반 배제가 수행되기 전에 후보 자원들의 풀로부터 생략될 수 있다. 일부 양상들에서, 제2 무선 디바이스는, 특정 양의 후보 자원들이 후보 자원들의 선택 풀에서 이용가능하게 남아있을 때까지 제1 무선 디바이스에 의해 제공된 하나 이상의 서브채널들의 가상으로 감지된 RSSI 측정들에 기초하여, 가상으로 감지된 후보 자원들을 미리 필터링할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 자원들의 특정 양의 20%가 선택 풀(예컨대, 필터링된 서브세트)에서 이용가능하게 남아있을 때까지 가상으로 감지된 후보 자원들을 미리 필터링할 수 있다. 20 퍼센트인 특정 양은 단지 예일 뿐이며, 본원에서 제공된 예로 제한되도록 의도되지 않는다. 일부 양상들에서, 특정 양은 20% 초과일 수 있다.

[0096] [0123] 1916에서, 제2 무선 디바이스는 후보 자원들의 필터링된 서브세트 내에서 후보 자원들을 배제할 수 있다. 예를 들어, 1916은 장치(2002)의 결정 컴포넌트(2042)에 의해 수행될 수 있다. 제2 무선 디바이스는 RSRP 임계치를 초과하는 사전-필터 임계치를 초과하지 않는, 후보 자원들의 필터링된 서브세트 내의 후보 자원들을 배제할 수 있다. 제2 무선 디바이스는 RSRP 임계치를 초과하지 않는 후보 자원들의 제2 서브세트를 획득하기 위해, 사전-필터 임계치를 초과하지 않지만 RSRP 임계치를 초과하는, 후보 자원들의 필터링된 서브세트 내의 후보 자원들을 배제할 수 있다. 일부 양상들에서, 후보 자원들의 제2 서브세트는, 사전-필터 임계치를 초과하지 않는, 선택 풀 내의 총 후보 자원들의 미리 구성된 비율을 포함할 수 있다. 일부 양상들에서, 사전-필터 임계치는, 후보 자원들의 제2 서브세트가 선택 풀 내의 총 후보 자원들의 미리 구성된 비율 미만의 후보 자원들의 양을 포함하면 조정될 수 있다. 사전-필터 임계치는, 후보 자원들의 제2 서브세트가 선택 풀 내의 총 후보 자원들의 미리 구성된 비율을 포함할 때까지 추가로 조정될 수 있다. 일부 양상들에서, 선택 풀 내의 총 후보 자원들의 미리 구성된 비율은 20%를 포함할 수 있다. 일부 양상들에서, 선택 풀 내의 총 후보 자원들의 미리 구성된 비율은 20% 초과를 포함할 수 있다. 일부 양상들에서, RSRP 임계치는 후보 자원들의 제2 서브세트가 선택 풀에서 총 후보 자원들의 미리 구성된 비율을 포함하도록 조정될 수 있다. RSRP 임계치는, 사전-필터 임계치를 조정하는 것에 추가하여 또는 이에 대한 대안으로 조정될 수 있다.

[0097] [0124] BSM을 송신할 적어도 하나의 서브채널을 포함하는 후보 자원은 후보 자원들의 제2 서브세트로부터 결정될 수 있다. 일부 양상들에서, 제2 무선 디바이스는 BSM을 송신할 후보 자원을 선택하기 전에, 자신의 하프 듀플렉스 동작에 기초하여 후보 자원들 중 일부를 배제할 수 있다. 사전-필터 임계치(예컨대, $Thresh_{virt}$)는 위에서 논의된 β 파라미터와 유사한 방식으로 기능할 수 있다. 예를 들어, 사전-필터 임계치(예컨대, $Thresh_{virt}$)는 가상으로 감지된 자원들에 대한 보호 레벨에 기초하여 조정될 수 있다. 예를 들어, 가상으로

감지된 자원들에 대한 더 많은 보호가 요구되면, 사전-필터 임계치의 값이 감소될 수 있다. 사전-필터 임계치를 감소시키는 것은 가상으로 감지된 자원들을 더 많이 배제할 수 있다. 일부 양상들에서, 사전-필터 임계치는, 서브채널들의 서브세트들 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 제1 무선 디바이스로부터 수신된 메시지와 연관된 타임스탬프, 제2 무선 디바이스의 속도, 제2 무선 디바이스의 가속도, 위협 엔티티의 로케이션과 관련된 제2 무선 디바이스의 주행 방향, 도로 기하구조와 관련된 정보, 또는 BSM과 연관된 송신 요건들, 또는 이들의 조합 중 적어도 하나에 기초할 수 있다.

[0098] [0125] 일부 양상들에서, 임계치(예컨대, $Thresh_{virt}$)에 기초한 가상으로 감지된 자원들의 사전-필터링은 RSRP-기반 배제와 협력할 수 있다. 예를 들어, RSRP-기반 배제 후에 특정 양(예컨대, 20%) 미만의 자원들이 선택 풀(예컨대, 후보 자원들의 제2 서브세트)에서 이용가능하면, 제2 무선 디바이스는, 더 적은 자원들이 배제되고 특정 양(예컨대, 20%)의 자원들이 선택 풀(예컨대, 후보 자원들의 제2 서브세트)에서 이용가능하도록, 임계치(예컨대, $Thresh_{virt}$)의 값을 조정할 수 있다. 이 방식은 또한 NR-V2X의 경우 지속적인 비-은닉(예컨대, 물리적으로 감지된) 위협 엔티티들을 회피하는 데 사용될 수 있다.

[0099] [0126] 1918에서, 제2 무선 디바이스는 후보 자원을 선택할 수 있다. 예를 들어, 1918은 장치(2002)의 결정 컴포넌트(2042)에 의해 수행될 수 있다. 제2 무선 디바이스는 BSM의 송신을 위해 후보 자원들의 제2 서브세트로부터 후보 자원을 선택할 수 있다.

[0100] [0127] 1906에서, 제2 무선 디바이스는 결정된 후보 자원 상에서 BSM을 송신할 수 있다. 예를 들어, 1906은 장치(2002)의 BSM 컴포넌트(2044)에 의해 수행될 수 있다. 제2 무선 디바이스는 결정된 후보 자원 상에서 적어도 제3 무선 디바이스에 BSM을 송신할 수 있다. 송신된 BSM이 제2 무선 디바이스의 부근 내의 임의의 무선 디바이스에 송신되고 그에 의해 수신될 수 있도록, 송신된 BSM은 브로드캐스트 메시지일 수 있다. 일부 양상들에서, BSM은 후보 자원 상에서 송신될 수 있으며, 여기서 후보 자원은 하나 이상의 서브채널들을 포함할 수 있다.

[0101] [0128] 도 20은 장치(2002)에 대한 하드웨어 구현의 예를 예시하는 도면(2000)이다. 장치(2002)는 UE이고, 셀룰러 RF 트랜시버(2022) 및 하나 이상의 SIM(subscriber identity module) 카드들(2020)에 커플링된 셀룰러 기저대역 프로세서(2004)(또한 모뎀으로 지칭됨), SD(secure digital) 카드(2008) 및 스크린(2010)에 커플링된 애플리케이션 프로세서(2006), 블루투스 모듈(2012), WLAN(wireless local area network) 모듈(2014), GNSS 모듈(2016) 및 전력 공급 장치(2018)를 포함한다. GNSS 모듈(2016)은 다양한 위성 포지셔닝 시스템들을 포함할 수 있다. 예를 들어, GNSS 모듈은 GPS(Global Positioning System), GLONASS(Global Navigation Satellite System), Galileo, BDS(BeiDou Navigation Satellite System), WAAS(Wide Area Augmentation System), EGNOS(European Geostationary Navigation Overlay Service), GAGAN(GPS Aided GEO Augmented Navigation), MSAS(MTSAT(Multifunctional Transport Satellites) Satellite Augmentation System), QZSS(Quasi-Zenith Satellite System), 또는 NavIC(Navigation with Indian Constellation)에 대응할 수 있다. 셀룰러 기저대역 프로세서(2004)는 셀룰러 RF 트랜시버(2022)를 통해 UE(104) 및/또는 BS(102/180)와 통신한다. 셀룰러 기저대역 프로세서(2004)는 컴퓨터 판독가능 매체/메모리를 포함할 수 있다. 컴퓨터 판독가능 매체/메모리는 비일시적일 수 있다. 셀룰러 기저대역 프로세서(2004)는, 컴퓨터 판독가능 매체/메모리 상에 저장된 소프트웨어의 실행을 포함하는 일반적인 프로세싱을 담당한다. 소프트웨어는, 셀룰러 기저대역 프로세서(2004)에 의해 실행될 때, 셀룰러 기저대역 프로세서(2004)로 하여금, 위에서 설명된 다양한 기능들을 수행하게 한다. 컴퓨터 판독가능 매체/메모리는 또한, 소프트웨어를 실행하는 경우 셀룰러 기저대역 프로세서(2004)에 의해 조작되는 데이터를 저장하기 위해 사용될 수 있다. 셀룰러 기저대역 프로세서(2004)는 수신 컴포넌트(2030), 통신 관리자(2032) 및 송신 컴포넌트(2034)를 더 포함한다. 통신 관리자(2032)는 하나 이상의 예시된 컴포넌트들을 포함한다. 통신 관리자(2032) 내의 컴포넌트들은 컴퓨터 판독가능 매체/메모리에 저장되고 그리고/또는 셀룰러 기저대역 프로세서(2004) 내의 하드웨어로서 구성될 수 있다. 셀룰러 기저대역 프로세서(2004)는 UE(350)의 컴포넌트일 수 있고, 메모리(360) 및/또는 TX 프로세서(368), RX 프로세서(356) 및 제어기/프로세서(359) 중 적어도 하나를 포함할 수 있다. 일 구성에서, 장치(2002)는 모뎀 칩일 수 있고, 단지 기저대역 프로세서(2004)를 포함할 수 있고, 다른 구성에서, 장치(2002)는 전체 UE(예컨대, 도 3의 350 참조)일 수 있고, 장치(2002)의 앞서 논의된 추가적인 모듈들을 포함할 수 있다.

[0102] [0129] 통신 관리자(2032)는 예컨대, 도 18의 1802 또는 도 19의 1902와 관련하여 설명된 바와 같이, 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신하도록 구성되는 메시지 컴포넌트(2040)를 포함한다. 통신 관리자(2032)는, 예컨대, 도 18의 1804 또는 도 19의 1904와 관련하여 설명된 바와 같이, 후보 자원들의 세트 중 BSM

을 송신할 후보 자원을 결정하도록 구성되는 결정 컴포넌트(2042)를 더 포함한다. 결정 컴포넌트(2042)는 예컨대, 도 19의 1908과 관련하여 설명된 바와 같이, 후보 자원들의 세트에서 하나 이상의 후보 자원들을 배제하도록 구성될 수 있다. 결정 컴포넌트(2042)는 예컨대, 도 19의 1910과 관련하여 설명된 바와 같이, 가중된 RSSI 랭킹에 기초하여 후보 자원들의 제1 서브세트를 랭킹하도록 구성될 수 있다. 결정 컴포넌트(2042)는 예컨대, 도 19의 1912와 관련하여 설명된 바와 같이, 후보 자원을 선택하도록 구성될 수 있다. 결정 컴포넌트(2042)는 예컨대, 도 19의 1914와 관련하여 설명된 바와 같이, 후보 자원들의 세트에서 하나 이상의 가상으로 감지된 후보 자원들을 배제하도록 구성될 수 있다. 결정 컴포넌트(2042)는 예컨대, 도 19의 1916과 관련하여 설명된 바와 같이, 후보 자원들의 필터링된 서브세트 내에서 후보 자원들을 배제하도록 구성될 수 있다. 결정 컴포넌트(2042)는 예컨대, 도 19의 1918과 관련하여 설명된 바와 같이, 후보 자원을 선택하도록 구성될 수 있다. 통신 관리자(2032)는, 예컨대, 도 18의 1806 또는 도 19의 1906과 관련하여 설명된 바와 같이, 결정된 후보 자원 상에서 BSM을 송신하도록 구성되는 BSM 컴포넌트(2044)를 더 포함한다.

[0103] [0130] 장치는 도 18 또는 도 19의 전술된 흐름도들에서의 알고리즘의 블록들 각각을 수행하는 추가적인 컴포넌트들을 포함할 수 있다. 따라서, 도 18 또는 도 19의 전술된 흐름도들에서의 각각의 블록은 컴포넌트에 의해 수행될 수 있고, 장치는 그러한 컴포넌트들 중 하나 이상을 포함할 수 있다. 컴포넌트들은, 언급된 프로세스들/알고리즘을 수행하도록 특정적으로 구성된 하나 이상의 하드웨어 컴포넌트들일 수 있거나, 언급된 프로세스들/알고리즘을 수행하도록 구성된 프로세서에 의해 구현될 수 있거나, 프로세서에 의한 구현을 위해 컴퓨터 판독가능 매체 내에 저장될 수 있거나, 이들의 일부 조합일 수 있다.

[0104] [0131] 일 구성에서, 장치(2002), 및 특히 셀룰러 기저대역 프로세서(2004)는 제1 무선 디바이스로부터, 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신하기 위한 수단을 포함한다. 위협 엔티티는 BSM들의 송신을 간섭하는 데이터를 송신한다. 장치는 제1 무선 디바이스로부터 위협 엔티티와 관련된 정보를 표시하는 메시지에 적어도 부분적으로 기초하여 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정하기 위한 수단을 포함한다. 장치는 결정된 후보 자원 상에서 BSM을 적어도 제3 무선 디바이스에 송신하기 위한 수단을 포함한다. 장치는 후보 자원들의 제1 서브세트를 결정하기 위해 후보 자원들의 세트에서 각각의 후보 자원에 대한 투사된 RSRP가 RSRP 임계치를 초과하는 것에 기초하여 후보 자원들의 세트에서 하나 이상의 후보 자원들을 배제하기 위한 수단을 더 포함한다. 장치는 가장 낮은 가중된 RSSI를 갖는 후보 자원들의 제2 서브세트를 획득하기 위해 가중된 RSSI 랭킹에 기초하여 후보 자원들의 제1 서브세트를 랭킹하기 위한 수단을 더 포함한다. 제2 서브세트의 후보 자원들은 후보 자원들의 제1 서브세트의 일부이다. 장치는 후보 자원들의 제2 서브세트로부터 후보 자원을 선택하기 위한 수단을 더 포함한다. 장치는, 사전-필터 임계치를 초과하지 않는 후보 자원들의 필터링된 서브세트를 획득하기 위해, 사전-필터 임계치를 초과하는 RSSI를 갖는 후보 자원들의 세트에서 하나 이상의 가상으로 감지된 후보 자원들을 배제하기 위한 수단을 더 포함한다. 장치는 RSRP 임계치를 초과하지 않는 후보 자원들의 제2 서브세트를 획득하기 위해, RSRP 임계치를 초과하는 사전-필터 임계치를 초과하지 않는, 후보 자원들의 필터링된 서브세트 내의 후보 자원들을 배제하기 위한 수단을 더 포함한다. 장치는 후보 자원들의 제2 서브세트로부터 후보 자원을 선택하기 위한 수단을 더 포함한다. 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 장치(2002)의 전술된 컴포넌트들 중 하나 이상일 수 있다. 위에서 설명된 바와 같이, 장치(2002)는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)를 포함할 수 있다. 따라서, 일 구성에서, 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)일 수 있다.

[0105] [0132] 도 21은 제1 무선 디바이스(2102), 제2 무선 디바이스(2104) 및 제3 무선 디바이스(2106) 사이의 예시적인 통신 흐름(2100)을 예시한다. 통신은 송신 디바이스로부터 수신 디바이스로의 직접적인 V2X, V2V 또는 D2D 기반 통신에 기초할 수 있다. 디바이스(2102, 2104, 2106)로부터 송신하는 통신은 도 4와 관련하여 설명된 바와 같이, 특정 송신 디바이스의 범위 내의 다수의 수신 디바이스들에 의해 브로드캐스트 및 수신될 수 있다. 제1 무선 디바이스(2102)는 제1 UE에 대응할 수 있고, 제2 무선 디바이스(2104)는 제2 UE에 대응할 수 있다. 제1 무선 디바이스(2102), 제2 무선 디바이스(2104) 및/또는 제3 무선 디바이스(2106)는 C-V2X 엔티티에 대응할 수 있다. 예를 들어, 도 1의 상황에서, 제1 무선 디바이스(2102)는 적어도 UE(104)에 대응할 수 있고, 제2 무선 디바이스(2104)는 적어도 104'에 대응할 수 있다. 다른 예에서, 도 3의 상황에서, 제1 무선 디바이스(2102)는 디바이스(350)에 대응할 수 있고, 제2 무선 디바이스(2104)는 디바이스(310)에 대응할 수 있다.

[0106] [0133] 2108에 예시된 바와 같이, 제1 무선 디바이스(2102)는 위협 구역 내의 위협 엔티티를 검출할 수 있다. 제1 무선 디바이스(2102)는 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 구역 내에서 위협 엔티티를 검출할 수 있다. 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들

을 방해할 수 있다. 일부 양상들에서, 위협 엔티티로부터 수신된 데이터 신호들은 무선 디바이스들에 대한 투사된 데이터와 일치하지 않는 데이터를 포함할 수 있다. 예를 들어, 데이터 신호들은 무선 디바이스들에 대해 현실적이지 않거나 예상되지 않는 데이터를 포함할 수 있다. 데이터 신호들은 예상보다 훨씬 더 높은 속력의 값, 무의미하거나 또는 제1 무선 디바이스의 부근 내에 있지 않은 포지션 정보를 표시할 수 있거나, 또는 제1 무선 디바이스를 오버로딩(overload)하는 많은 양의 데이터를 포함할 수 있다. 데이터 신호들은, 본 개시가 본원에 제공된 예들로 제한되는 것으로 의도되지 않도록 다른 타입들의 일관되지 않거나 부정확한 데이터를 포함할 수 있다. 일부 양상들에서, 데이터 신호들은 오작동 무선 디바이스의 데이터를 포함할 수 있다. 오작동 무선 디바이스의 데이터는 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 잘못된 또는 타당하지 않은 데이터를 포함한다. 일부 양상들에서, 위협 엔티티의 타입은 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 제1 무선 디바이스에 의해 결정될 수 있다. 위협 엔티티의 타입은 DoS 공격자, 재머, 오작동 차량, OOB 간섭자, WAN 재머 또는 GNSS 재머를 포함할 수 있다.

[0107] [0134] 2114에 예시된 바와 같이, 제1 무선 디바이스(2102)는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 송신할 수 있다. 제1 무선 디바이스(2102)는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 적어도 하나의 제2 무선 디바이스(2104)에 송신할 수 있다. 제2 무선 디바이스(2104)는 제1 무선 디바이스(2102)로부터 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신할 수 있다. 검출된 위협 엔티티가 새로운 클래스의 검출된 물체로 간주될 수 있어서, 위협 엔티티가 물리적 장애물과는 반대로 스펙트럼 또는 보안 문제인 것으로 인해, 위협 엔티티를 표시하는 메시지는 SDSM(sensor data sharing message) 또는 CPM(collective perception message)으로서 인코딩될 수 있다. 메시지는 위협 구역 외부의 적어도 하나의 제2 무선 디바이스(2104)뿐만 아니라 제1 무선 디바이스 부근 내의 임의의 다른 무선 디바이스로 브로드캐스트될 수 있다. 메시지는 사이드링크 통신(예컨대, PC5)을 통해 적어도 하나의 제2 무선 디바이스에 브로드캐스트될 수 있다. 제2 무선 디바이스가 제1 무선 디바이스로부터 위협 엔티티를 표시하는 메시지를 수신하는 것은, 제2 무선 디바이스가 위협 엔티티의 위협 구역을 넘어선 것으로 인해 제2 무선 디바이스가 검출할 수 없는 위협 엔티티를 제2 무선 디바이스가 가상으로 감지할 수 있게 한다. 일부 양상들에서, 예를 들어, SPS(semi-persistent scheduling)에서, 제2 무선 디바이스는 예비들을 하기 위해 감지 윈도우 동안 데이터를 반송하는 서브채널들의 RSRP 및/또는 RSSI를 측정할 수 있다. 제2 무선 디바이스는, 측정된 RSRP/RSSI가 임계치를 초과하면, 후보 CSR들의 리스트로부터 CSR들을 배제할 수 있다. CRM들은 하나 이상의 서브채널들을 포함할 수 있다. 또한, 제1 무선 디바이스로부터의 위협 엔티티를 표시하는 메시지를 사용하는 제2 무선 디바이스는 제1 무선 디바이스로부터의 위협 엔티티를 표시하는 메시지에서 보고된 RSSI 측정들에 기초하여 재밍 또는 간섭된 서브채널들을 배제할 수 있다. 이러한 가상 감지는, 특히 제2 무선 디바이스가 연장된 시간 기간 동안 SPS 예비들에 매달릴 가능성이 있는 경우, 제2 무선 디바이스에 의해 송신되는 메시지들의 수신 확률을 개선할 수 있다.

[0108] [0135] 일부 양상들에서, 제1 무선 디바이스(2102)는 Uu 링크를 통해 네트워크 엔티티(예컨대, 기지국)에 메시지(예컨대, SDSM)를 송신할 수 있다. 이러한 경우들에서, 네트워크 엔티티는 제1 무선 디바이스로부터의 메시지를 위협 구역 외부의 다른 무선 디바이스들에 중계할 수 있어서, 다른 무선 디바이스들은 예방 조치들을 사전에 취할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 네트워크 엔티티로부터 위협 엔티티를 표시하는 메시지를 수신할 수 있다. 이러한 경우들에서, 제1 무선 디바이스는 위협 엔티티의 위협 구역 내에 있는 동안 위협 엔티티를 물리적으로 검출하였다. 제1 무선 디바이스는, 위협 구역 외부에 있고 위협 엔티티를 검출한 제1 무선 디바이스로부터의 송신 범위를 넘어선 다른 디바이스들 및 적어도 제2 무선 디바이스에 네트워크 엔티티가 메시지를 중계하도록 허용하기 위해, 검출된 위협 엔티티를 보고하는 메시지를 네트워크 엔티티에 송신할 수 있다. 메시지는 적어도 하나의 다른 무선 디바이스로부터 수신된 위협 엔티티의 보고들의 수, 위협 엔티티의 심각도, 위협 엔티티 및 제1 무선 디바이스를 분리하는 거리, 또는 적어도 하나의 제2 무선 디바이스가 위협 구역에 접근하는 시간, 또는 이들의 조합 중 적어도 하나에 기초하여 송신될 수 있다. 메시지는 위협 엔티티의 데이터 신호들의 듀티 사이클을 포함할 수 있다. 위협 엔티티의 데이터 신호의 듀티 사이클의 정보는 제2 무선 디바이스가 송신 예비들/구성들을 할 때 위협 엔티티의 듀티 사이클을 고려하게 할 수 있다. 일부 양상들에서, 메시지는 위협 엔티티를 검출한 제1 무선 디바이스의 안테나 엘리먼트들 중에서 피크 RSSI 검출을 포함할 수 있다. 제1 무선 디바이스는, 위협 엔티티의 송신들의 도달각을 검출하도록 구성될 수 있는 지향성 수신 안테나 어레이들을 갖도록 구성될 수 있으며, 이는 위협 엔티티의 로케이션의 결정을 향상시킬 수 있고 메시지에 포함된 위협 구역을 제한하는 것을 보조할 수 있다.

[0109] [0136] 메시지는 위협 엔티티와의 접촉을 회피 또는 완화시키기 위해 제2 무선 디바이스에서 완화 액션을 트리거링할 수 있다. 메시지는, 적어도 하나의 제2 무선 디바이스가 위협 엔티티를 물리적으로 감지하기 위해 위협 엔티티의 위협 구역 내에 있지 않을 수 있더라도, 제2 무선 디바이스가 위협 엔티티를 가상으로 감지할 수 있게

한다.

[0110] [0137] 메시지는 위협 엔티티의 특성들과 관련된 정보를 포함할 수 있다. 일부 양상들에서, 메시지는 위협 엔티티의 타입과 연관된 신뢰도 값을 포함할 수 있다. 메시지는 적어도 제1 무선 디바이스의 대역폭에 걸쳐 측정된 RSSI의 평균을 포함할 수 있다. 재밍은 일반적으로 광대역이며, 제1 무선 디바이스의 전체 대역폭에 걸쳐 측정된 RSSI의 평균은 위협 엔티티를 재밍 디바이스인 것으로 표시할 수 있다. 일부 양상들에서, 메시지는 RSSI 임계치를 초과하는 각각의 서브채널에 대해 측정된 RSSI의 평균을 포함할 수 있다. 각각의 서브채널에 대한 RSSI의 평균은 시간 윈도우에 걸쳐 측정될 수 있다. 각각의 서브채널에 대해 측정된 RSSI의 평균은 위협 엔티티를 OOB 엔티티 또는 협대역 재머로서 표시할 수 있다. 메시지는 위협 엔티티로부터 수신된 데이터 신호들의 듀티 사이클을 포함할 수 있다. 위협 엔티티로부터의 데이터 신호의 듀티 사이클 정보는 무선 디바이스들이 듀티 사이클 동안 수신된 데이터를 무시하도록 허용할 수 있다. 일부 양상들에서, 메시지는 위협 엔티티의 계층 2(L2) 어드레스를 포함할 수 있다. 일부 경우들, 예를 들어, DoS 공격 또는 오작동 무선 디바이스(예컨대, 오작동 차량)에서, RSSI 보고는 관련이 없을 수 있다. 따라서, 메시지는 적어도 하나의 제2 무선 디바이스가 모뎀 계층에서 수신된 DoS 패킷들을 사전-필터링하도록 허용하기 위해 위협 엔티티의 L2 어드레스를 포함할 수 있다. 메시지는 위협 엔티티에 대응하는 적어도 하나의 IE(information element)를 추가로 표시할 수 있다. 적어도 하나의 IE는 위협 엔티티의 검출된 특성들을 포함할 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 포지션, 속력, 또는 진로, 또는 이들의 조합 중 적어도 하나를 포함할 수 있다. 예를 들어, 위협 엔티티의 포지션, 속력 및/또는 진로가 DoS 공격에 포함될 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 위협 엔티티의 포지션 주위의 반경을 포함할 수 있다. 예를 들어, 재머 또는 간섭자에 대해, 포지션 주위의 반경과 관련된 정보가 제공될 수 있다. 일부 양상들에서, 제1 무선 디바이스는 그의 다른 센서들(예컨대, 카메라, 레이더, LIDAR)로부터의 정보 및/또는 동일한 위협 엔티티를 검출하는 다른 무선 디바이스들로부터 수신된 메시지들(예컨대, SDSM 또는 MAP)을 조합하여 위협 엔티티의 특성들을 결정할 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 위협 엔티티의 측정된 RSSI와 관련된 정보를 포함할 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 위협 엔티티와 연관된 하나 이상의 계층들과 관련된 정보, 인증서 다이제스트, 셀 식별자 또는 PLMN(public land mobile network)을 포함할 수 있다. 메시지는 위협 엔티티를 위협 엔티티의 데이터 신호들을 송신하는 물체로서 식별할 수 있다. 일부 양상들에서, 물체는 VRU(vulnerable road user), 검출된 차량 또는 무선 장애물 중 하나를 포함할 수 있다.

[0111] [0138] 검출된 위협 타입이 C-V2X 재머인 경우들에서, IE(예컨대, DetectedJammerData)는 제1 무선 디바이스의 전체 대역폭 및 RSSI 평균 윈도우 크기에 걸친 RSSI의 평균과 관련된 정보를 포함할 수 있다. 일부 양상들에서, IE(예컨대, DetectedobjectCommonData)는 위협 엔티티의 위협 구역의 반경과 관련된 정보 뿐만 아니라 제1 무선 디바이스의 다른 센서들(예컨대, 카메라, 레이더, LIDAR)에 대한 조합된 정보를 포함할 수 있다. 검출된 위협 타입이 OOB 간섭자인 경우들에서, IE(예컨대, DetectedInterfererData)는 각각의 서브채널 또는 대역에 대한 측정된 RSSI, RSSI 보고 임계치, RSSI 평균 윈도우 크기 또는 위협 엔티티의 듀티 사이클을 포함할 수 있다. 검출된 위협 타입이 오작동 차량인 경우들에서, IE(예컨대, MisbehavingVehicleData)는 L2 어드레스 또는 인증서 다이제스트를 포함할 수 있다. 검출된 위협 타입이 WAN 재머인 경우들에서, IE(예컨대, DetectedJammerData)는 EARFCN(E-UTRA absolute radio frequency channel number), 셀 식별자들 또는 PLMN과 관련된 정보를 포함할 수 있다. 검출된 위협 타입이 GNSS 재머인 경우들에서, IE(예컨대, DetectedJammerData)는 GNSS 대역, 계층 1(L1), L2 또는 계층 5(L5)와 관련된 정보를 포함할 수 있다.

[0112] [0139] 2118에 예시된 바와 같이, 제2 무선 디바이스(2104)는 메시지(예컨대, SDSM)를 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 제2 무선 디바이스(2104)는 위협 엔티티와의 접촉을 회피 또는 완화하기 위해 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해할 수 있다. 일부 양상들에서, 완화 액션은 위협 엔티티를 회피하기 위한 대안적인 경로를 선택하는 것, 더 견고한 MCS를 활용하는 것, 또는 위협 엔티티의 가상 감지를 포함할 수 있다. 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 실질적으로 저하시킬 수 있다. 협력적 또는 자동화된 운전 결정들은 안전 목적들을 위해 높은 신뢰도를 요구할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 검출된 위협 엔티티 또는 임의의 위협 엔티티에 의해 영향을 가장 적게 받는 것으로 주행의 스케줄링된 루트 또는 경로를 변경하기로 결정할 수 있다. 제2 무선 디바이스는, 제2 무선 디바이스가 네트워크 엔티티(예컨대, RSU)로부터 위협 엔티티를 표시하는 메시지를 수신하는 경우들에서 위협 엔티티와의 접촉을 회피 또는 완화할 수 있다. 제1 무선 디바이스로부터 이격된 제2 무선 디바이스는 PC5를 통해 제1 무선 디바이스로부터 직접 메시지를 수신하기 위한 범위 내에 있지 않을 수 있어서, 제2 무선 디바이스는 Uu 링크를 통해 네트워크 엔티티(예컨대, 기지국)로부터 중계된 메시지를 수신한다. 제1

무선 디바이스로부터 떨어져 있는 제2 무선 디바이스는, 위협 엔티티를 회피하기 위해 대안적인 경로를 취하거나, 더 견고한 MCS를 활용하거나, 또는 위협 엔티티의 가상 감지와 같은 완화 액션을 준비하기에 충분한 시간을 제2 무선 디바이스에 제공할 수 있다. 일부 양상들에서, 네트워크 엔티티는 거리 교차로들에 있는 액세스 포인트들과 같은 알려진 위협들(예컨대, 정적)의 상세한 RF 핑거프린트를 제공하고 제2 무선 디바이스에 송신될 수 있는 Uu를 통해 클라우드 엔드포인트에 송신하도록 구성될 수 있는 RSU 또는 MEC(multi-access edge computing) 시스템을 포함할 수 있다. RSU 또는 MEC는 부분적으로 더 높은 컴퓨테이셔널 자원들 및/또는 감각 입력들을 갖는 RSU 또는 MEC로 인해 제1 무선 디바이스보다 위협 엔티티의 개선된 로컬화를 획득할 수 있다. 또한, RSU 또는 MEC는 위협 엔티티를 보고하는 메시지를 PC5 및/또는 Uu 인터페이스들을 통해 제2 무선 디바이스에 송신할 수 있다.

[0113] [0140] 일부 양상들에서, 예를 들어, 2112에서, 제1 무선 디바이스는 제1 무선 디바이스에 의해 획득된 다른 데이터와 함께 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 엔티티의 로케이션의 추정된 측정을 결정할 수 있다. 일부 양상들에서, 위협 엔티티로부터 수신된 데이터 신호들은 제1 무선 디바이스의 하나 이상의 센서들로부터 수신된 데이터와 조합될 수 있다. 예를 들어, 제1 무선 디바이스는 위협 엔티티의 추정된 로케이션을 결정하기 위해 제1 무선 디바이스의 센서들(예컨대, 카메라, 레이더, LIDAR)로부터의 판독들 및/또는 V2I 메시지들(예컨대, MAP)과 위협 엔티티의 RSSI 측정들을 조합할 수 있다. 메시지는 위협 엔티티의 추정된 로케이션 및 위협 엔티티의 추정된 로케이션과 연관된 신뢰도 값을 포함할 수 있다.

[0114] [0141] 일부 양상들에서, 예를 들어, 2110에서, 제1 무선 디바이스(2102)는 제3 무선 디바이스(2106)로부터, 위협 엔티티를 표시하는 보고를 수신할 수 있다. 제1 무선 디바이스는 보고의 수신에 대한 응답으로 위협 엔티티의 추정된 로케이션을 결정할 수 있다. 일부 양상들에서, 제1 무선 디바이스(2102)는 보고의 수신에 대한 응답으로 위협 엔티티의 추정된 로케이션을 결정하도록 트리거링될 수 있다. 일부 양상들에서, 제1 무선 디바이스(2102)는 위협 엔티티의 추정된 로케이션을 결정하기 위해 제1 무선 디바이스가 위협 엔티티로부터 수신한 데이터 신호들과 함께 제3 무선 디바이스(2106)로부터의 보고에 제공된 정보를 활용할 수 있다. 일부 양상들에서, 제3 무선 디바이스로부터의 보고는 제3 무선 디바이스에 의해 결정된 위협 엔티티의 추정된 로케이션, 제3 무선 디바이스에 의해 측정된 위협 엔티티의 신호 강도 측정들, 또는 위협 엔티티의 다른 특성들을 포함할 수 있다. 일부 양상들에서, 제3 무선 디바이스로부터의 보고는 제3 무선 디바이스의 특성들, 이를테면 로케이션, 속력, 진로 및 타임스탬프(그러나 이에 제한되지 않음)를 포함할 수 있다. 제1 무선 디바이스는 하나 초과의 제3 무선 디바이스로부터 검출된 위협 엔티티와 관련된 보고를 수신하고, 위협 엔티티의 추정된 로케이션을 결정하기 위해 이러한 정보를 조합할 수 있다.

[0115] [0142] 일부 양상들에서, 예를 들어, 2116에서, 제2 무선 디바이스(2104)는 메시지의 수신에 대한 응답으로 송신 파라미터들을 조정할 수 있다. 제2 무선 디바이스는 BSM을 송신하기 위해 메시지의 수신에 대한 응답으로 송신 파라미터들을 조정할 수 있다. 일부 양상들에서, 조정된 송신 파라미터들은 송신 전력의 증가 또는 더 견고한 MCS의 사용, 또는 이들의 조합 중 적어도 하나를 포함할 수 있다. 더 견고한 MCS를 사용하는 것은 더 낮은 MCS로 스위칭하는 것을 포함할 수 있다. 일부 양상들에서, 송신 파라미터들을 조정하는 것은 위협 엔티티의 영향을 완화시킬 수 있지만, 확장된 범위 및/또는 증가된 오버-디-에어 송신 시간으로 인해 다른 무선 디바이스들과의 패킷 충돌 확률을 증가시킬 수 있다. 이러한 경우들에서, MCS 인덱스 및 송신 전력은 무선 디바이스 밀도 및 위협 신호 강도에 기초하여 조정될 수 있다.

[0116] [0143] 도 22는 무선 통신 방법의 흐름도(2200)이다. 방법은 UE 또는 UE의 컴포넌트에 의해 수행될 수 있다(예컨대, UE(104); 장치(2402); 메모리(360)를 포함할 수 있고 전체 UE(350) 또는 UE(350)의 컴포넌트, 이를테면 TX 프로세서(368), RX 프로세서(356) 및/또는 제어기/프로세서(359)일 수 있는 셀룰러 기저대역 프로세서(2404)). 예시된 동작들 중 하나 이상은 선택적이거나, 생략되거나, 전치되거나, 또는 동시적일 수 있다. 방법은, 제1 무선 디바이스가, 다른 무선 디바이스가 예방 조치들을 사전에 취할 수 있도록, 검출된 위협 엔티티와 관련된 정보를 위협 엔티티의 위협 구역을 넘어선 다른 무선 디바이스들과 공유하도록 허용할 수 있다.

[0117] [0144] 2202에서, 제1 무선 디바이스는 위협 구역 내의 위협 엔티티를 검출할 수 있다. 예를 들어, 2202는 장치(2402)의 검출 컴포넌트(2440)에 의해 수행될 수 있다. 제1 무선 디바이스는 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 구역 내에서 위협 엔티티를 검출할 수 있다. 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해할 수 있다. 일부 양상들에서, 위협 엔티티로부터 수신된 데이터 신호들은 무선 디바이스들에 대한 투사된 데이터와 일치하지 않는 데이터를 포함할 수 있다. 예를 들어, 데이터 신호들은 무선 디바이스들에 대해 현실적이지 않거나 예상되지 않는 데이터를 포함할 수 있다. 데이터 신호들은 예상보다 훨씬 더 높은 속력의 값, 무의미하거나 또는 제1 무선 디바이스의 부근 내에 있지 않

은 포지션 정보를 표시할 수 있거나, 또는 제1 무선 디바이스를 오버로딩하는 많은 양의 데이터를 포함할 수 있다. 데이터 신호들은, 본 개시가 본원에 제공된 예들로 제한되는 것으로 의도되지 않도록 다른 타입들의 일관되지 않거나 부정확한 데이터를 포함할 수 있다. 일부 양상들에서, 데이터 신호들은 오작동 무선 디바이스의 데이터를 포함할 수 있다. 오작동 무선 디바이스의 데이터는 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 잘못된 또는 타당하지 않은 데이터를 포함한다. 일부 양상들에서, 위협 엔티티의 타입은 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 제1 무선 디바이스에 의해 결정될 수 있다. 위협 엔티티의 타입은 DoS 공격자, 재머, 오작동 차량, OOB 간섭자, WAN 재머 또는 GNSS 재머를 포함할 수 있다.

[0118] [0145] 2204에서, 제1 무선 디바이스는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 송신할 수 있다. 예를 들어, 2204는 장치(2402)의 메시지 컴포넌트(2446)에 의해 수행될 수 있다. 제1 무선 디바이스는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 적어도 하나의 제2 무선 디바이스에 송신할 수 있다. 검출된 위협 엔티티가 새로운 클래스의 검출된 물체로 간주될 수 있어서, 위협 엔티티가 물리적 장애물과는 반대로 스펙트럼 또는 보안 문제인 것으로 인해, 위협 엔티티를 표시하는 메시지는 SDSM 또는 CPM으로서 인코딩될 수 있다. 메시지는 위협 구역 외부의 적어도 하나의 제2 무선 디바이스뿐만 아니라 제1 무선 디바이스 부근 내의 임의의 다른 무선 디바이스로 브로드캐스트될 수 있다. 메시지는 사이드링크 통신(예컨대, PC5)을 통해 적어도 하나의 제2 무선 디바이스에 브로드캐스트될 수 있다. 일부 양상들에서, 메시지는 Uu 인터페이스를 통해 네트워크 엔티티(예컨대, 기지국)에 송신될 수 있다. 이러한 경우들에서, 네트워크 엔티티(예컨대, 기지국)는 위협 구역 외부의 다른 무선 디바이스들에 메시지를 중계할 수 있어서, 다른 무선 디바이스들은 예방 조치들을 사전에 취할 수 있다. 메시지는 적어도 하나의 제3 무선 디바이스로부터 수신된 위협 엔티티의 보고들의 수, 위협 엔티티의 심각도, 위협 엔티티 및 제1 무선 디바이스를 분리하는 거리, 또는 적어도 하나의 제2 무선 디바이스가 위협 구역에 접근하는 시간, 또는 이들의 조합 중 적어도 하나에 기초하여 송신될 수 있다. 메시지(예컨대, SDSM)는 위협 엔티티와의 접촉을 회피 또는 완화시키기 위해 적어도 하나의 제2 무선 디바이스에서 완화 액션을 트리거링할 수 있다. 메시지는, 적어도 하나의 제2 무선 디바이스가 위협 엔티티를 물리적으로 감지하기 위해 위협 엔티티의 위협 구역 내에 있지 않을 수 있더라도, 적어도 하나의 제2 무선 디바이스가 위협 엔티티를 가상으로 감지할 수 있게 한다.

[0119] [0146] 메시지는 위협 엔티티의 특성들과 관련된 정보를 포함할 수 있다. 일부 양상들에서, 메시지는 위협 엔티티의 타입과 연관된 신뢰도 값을 포함할 수 있다. 메시지는 적어도 제1 무선 디바이스의 대역폭에 걸쳐 측정된 RSSI의 평균을 포함할 수 있다. 재밍은 일반적으로 광대역이며, 제1 무선 디바이스의 전체 대역폭에 걸쳐 측정된 RSSI의 평균은 위협 엔티티를 재밍 디바이스인 것으로 표시할 수 있다. 일부 양상들에서, 메시지는 RSSI 임계치를 초과하는 각각의 서브채널에 대해 측정된 RSSI의 평균을 포함할 수 있다. 각각의 서브채널에 대한 RSSI의 평균은 시간 윈도우에 걸쳐 측정될 수 있다. 각각의 서브채널에 대해 측정된 RSSI의 평균은 위협 엔티티를 OOB 엔티티 또는 협대역 재머로서 표시할 수 있다. 메시지는 위협 엔티티로부터 수신된 데이터 신호들의 듀티 사이클을 포함할 수 있다. 위협 엔티티로부터의 데이터 신호의 듀티 사이클 정보는 무선 디바이스들이 듀티 사이클 동안 수신된 데이터를 무시하도록 허용할 수 있다. 일부 양상들에서, 메시지는 위협 엔티티의 L2 어드레스를 포함할 수 있다. 일부 경우들, 예를 들어, DoS 공격 또는 오작동 무선 디바이스(예컨대, 오작동 차량)에서, RSSI 보고는 관련이 없을 수 있다. 따라서, 메시지는 적어도 하나의 제2 무선 디바이스가 모뎀 계층에서 수신된 DoS 패킷들을 사전-필터링하도록 허용하기 위해 위협 엔티티의 L2 어드레스를 포함할 수 있다. 메시지는 위협 엔티티에 대응하는 적어도 하나의 IE를 추가로 표시할 수 있다. 적어도 하나의 IE는 위협 엔티티의 검출된 특성들을 포함할 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 포지션, 속력, 또는 진로, 또는 이들의 조합 중 적어도 하나를 포함할 수 있다. 예를 들어, 위협 엔티티의 포지션, 속력 및/또는 진로가 DoS 공격에 포함될 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 위협 엔티티의 포지션 주위의 반경을 포함할 수 있다. 예를 들어, 재머 또는 간섭자에 대해, 포지션 주위의 반경과 관련된 정보가 제공될 수 있다. 일부 양상들에서, 제1 무선 디바이스는 그의 다른 센서들(예컨대, 카메라, 레이더, LIDAR)로부터의 정보 및/또는 동일한 위협 엔티티를 검출하는 다른 무선 디바이스들로부터 수신된 메시지들(예컨대, SDSM 또는 MAP)을 조합하여 위협 엔티티의 특성들을 결정할 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 위협 엔티티의 측정된 RSSI와 관련된 정보를 포함할 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 위협 엔티티와 연관된 하나 이상의 계층들과 관련된 정보, 인증서 다이제스트, 셀 식별자 또는 PLMN을 포함할 수 있다. 메시지는 위협 엔티티를 위협 엔티티의 데이터 신호들을 송신하는 물체로서 식별할 수 있다. 일부 양상들에서, 물체는 VRU, 검출된 차량 또는 무선 장애물 중 하나를 포함할 수 있다.

[0120] [0147] 검출된 위협 타입이 C-V2X 재머인 경우들에서, IE(예컨대, DetectedJammerData)는 제1 무선 디바이스의 전체 대역폭 및 RSSI 평균 윈도우 크기에 걸친 RSSI의 평균과 관련된 정보를 포함할 수 있다. 일부

양상들에서, IE(예컨대, DetectedobjectCommonData)는 위협 엔티티의 위협 구역의 반경과 관련된 정보 뿐만 아니라 제1 무선 디바이스의 다른 센서들(예컨대, 카메라, 레이더, LIDAR)에 대한 조합된 정보를 포함할 수 있다. 검출된 위협 타입이 OOB 간섭자인 경우들에서, IE(예컨대, DetectedInterfererData)는 각각의 서브채널 또는 대역에 대한 측정된 RSSI, RSSI 보고 임계치, RSSI 평균 윈도우 크기 또는 위협 엔티티의 듀티 사이클을 포함할 수 있다. 검출된 위협 타입이 오작동 차량인 경우들에서, IE(예컨대, MisbehavingVehicleData)는 L2 어드레스 또는 인증서 다이제스트를 포함할 수 있다. 검출된 위협 타입이 WAN 재머인 경우들에서, IE(예컨대, DetectedJammerData)는 EARFCN, 셀 식별자들 또는 PLMN과 관련된 정보를 포함할 수 있다. 검출된 위협 타입이 GNSS 재머인 경우들에서, IE(예컨대, DetectedJammerData)는 GNSS 대역, L1, L2 또는 L5와 관련된 정보를 포함할 수 있다.

[0121] [0148] 도 23은 무선 통신 방법의 흐름도(2300)이다. 방법은 UE 또는 UE의 컴포넌트에 의해 수행될 수 있다(예컨대, UE(104); 장치(2402); 메모리(360)를 포함할 수 있고 전체 UE(350) 또는 UE(350)의 컴포넌트, 이를테면 TX 프로세서(368), RX 프로세서(356) 및/또는 제어기/프로세서(359)일 수 있는 셀룰러 기저대역 프로세서(2404)). 예시된 동작들 중 하나 이상은 선택적이거나, 생략되거나, 전치되거나, 또는 동시적일 수 있다. 방법은, 제1 무선 디바이스가, 다른 무선 디바이스가 예방 조치들을 사전에 취할 수 있도록, 검출된 위협 엔티티와 관련된 정보를 위협 엔티티의 위협 구역을 넘어선 다른 무선 디바이스들과 공유하도록 허용할 수 있다.

[0122] [0149] 2302에서, 제1 무선 디바이스는 위협 구역 내의 위협 엔티티를 검출할 수 있다. 예를 들어, 2302는 장치(2402)의 검출 컴포넌트(2440)에 의해 수행될 수 있다. 제1 무선 디바이스는 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 구역 내에서 위협 엔티티를 검출할 수 있다. 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해할 수 있다. 일부 양상들에서, 위협 엔티티로부터 수신된 데이터 신호들은 무선 디바이스들에 대한 투사된 데이터와 일치하지 않는 데이터를 포함할 수 있다. 예를 들어, 데이터 신호들은 무선 디바이스들에 대해 현실적이지 않거나 예상되지 않는 데이터를 포함할 수 있다. 데이터 신호들은 예상보다 훨씬 더 높은 속력의 값, 무의미하거나 또는 제1 무선 디바이스의 부근 내에 있지 않은 포지션 정보를 표시할 수 있거나, 또는 제1 무선 디바이스를 오버로딩하는 많은 양의 데이터를 포함할 수 있다. 데이터 신호들은, 본 개시가 본원에 제공된 예들로 제한되는 것으로 의도되지 않도록 다른 타입들의 일관되지 않거나 부정확한 데이터를 포함할 수 있다. 일부 양상들에서, 데이터 신호들은 오작동 무선 디바이스의 데이터를 포함할 수 있다. 오작동 무선 디바이스의 데이터는 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 잘못된 또는 타당하지 않은 데이터를 포함한다. 일부 양상들에서, 위협 엔티티의 타입은 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 제1 무선 디바이스에 의해 결정될 수 있다. 위협 엔티티의 타입은 DoS 공격자, 재머, 오작동 차량, OOB 간섭자, WAN 재머 또는 GNSS 재머를 포함할 수 있다.

[0123] [0150] 2304에서, 제1 무선 디바이스는 제1 무선 디바이스에 의해 획득된 다른 데이터와 함께 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 엔티티의 추정된 로케이션을 결정할 수 있다. 예를 들어, 2304는 장치(2402)의 결정 컴포넌트(2442)에 의해 수행될 수 있다. 일부 양상들에서, 위협 엔티티로부터 수신된 데이터 신호들은 제1 무선 디바이스의 하나 이상의 센서들로부터 수신된 데이터와 조합될 수 있다. 예를 들어, 제1 무선 디바이스는 위협 엔티티의 로케이션을 결정하기 위해 제1 무선 디바이스의 센서들(예컨대, 카메라, 레이더, LIDAR)로부터의 판독들 및/또는 V2I 메시지들(예컨대, MAP)과 위협 엔티티의 RSSI 측정들을 조합할 수 있다. 메시지는 위협 엔티티의 추정된 로케이션 및 위협 엔티티의 추정된 로케이션과 연관된 신뢰도 값을 포함할 수 있다.

[0124] [0151] 2306에서, 제1 무선 디바이스는 제3 무선 디바이스로부터, 위협 엔티티를 표시하는 보고를 수신할 수 있다. 예를 들어, 2306은 장치(2402)의 보고 컴포넌트(2444)에 의해 수행될 수 있다. 제1 무선 디바이스는 보고의 수신에 대한 응답으로 위협 엔티티의 추정된 로케이션을 결정할 수 있다. 일부 양상들에서, 제1 무선 디바이스는 보고의 수신에 대한 응답으로 위협 엔티티의 추정된 로케이션을 결정하도록 트리거링될 수 있다. 일부 양상들에서, 제1 무선 디바이스는 위협 엔티티의 추정된 로케이션을 결정하기 위해 제1 무선 디바이스가 위협 엔티티로부터 수신한 데이터 신호들과 함께 제3 무선 디바이스로부터의 보고에 제공된 정보를 활용할 수 있다. 일부 양상들에서, 제3 무선 디바이스로부터의 보고는 제3 무선 디바이스에 의해 결정된 위협 엔티티의 추정된 로케이션, 제3 무선 디바이스에 의해 측정된 위협 엔티티의 신호 강도 측정들, 또는 위협 엔티티의 다른 특성들을 포함할 수 있다. 일부 양상들에서, 제3 무선 디바이스로부터의 보고는 제3 무선 디바이스의 특성들, 이를테면 로케이션, 속력, 진로 및 타임스탬프(그러나 이에 제한되지 않음)를 포함할 수 있다. 제1 무선 디바이스는 하나 초과의 제3 무선 디바이스로부터 검출된 위협 엔티티와 관련된 보고를 수신하고, 위협 엔티티의 추정된 로케이션을 결정하기 위해 이러한 정보를 조합할 수 있다.

[0125] [0152] 2308에서, 제1 무선 디바이스는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 송신할 수 있다. 예를 들어, 2308은 장치(2402)의 메시지 컴포넌트(2446)에 의해 수행될 수 있다. 제1 무선 디바이스는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 적어도 하나의 제2 무선 디바이스에 송신할 수 있다. 검출된 위협 엔티티가 새로운 클래스의 검출된 물체로 간주될 수 있어서, 위협 엔티티가 물리적 장애물과는 반대로 스펙트럼 또는 보안 문제인 것으로 인해, 위협 엔티티를 표시하는 메시지는 SDSM 또는 CPM으로서 인코딩될 수 있다. 메시지는 위협 구역 외부의 적어도 하나의 제2 무선 디바이스뿐만 아니라 제1 무선 디바이스 부근 내의 임의의 다른 무선 디바이스로 브로드캐스트될 수 있다. 메시지는 사이드링크 통신(예컨대, PC5)을 통해 적어도 하나의 제2 무선 디바이스에 브로드캐스트될 수 있다. 일부 양상들에서, 메시지는 Uu 인터페이스를 통해 네트워크 엔티티(예컨대, 기지국)에 송신될 수 있다. 이러한 경우들에서, 네트워크 엔티티(예컨대, 기지국)는 위협 구역 외부의 다른 무선 디바이스들에 메시지를 중계할 수 있어서, 다른 무선 디바이스들은 예방 조치들을 사전에 취할 수 있다. 메시지는 적어도 하나의 제3 무선 디바이스로부터 수신된 위협 엔티티의 보고들의 수, 위협 엔티티의 심각도, 위협 엔티티 및 제1 무선 디바이스를 분리하는 거리, 또는 적어도 하나의 제2 무선 디바이스가 위협 구역에 접근하는 시간, 또는 이들의 조합 중 적어도 하나에 기초하여 송신될 수 있다. 메시지(예컨대, SDSM)는 위협 엔티티와의 접촉을 회피 또는 완화시키기 위해 적어도 하나의 제2 무선 디바이스에서 완화 액션을 트리거링할 수 있다. 메시지는, 적어도 하나의 제2 무선 디바이스가 위협 엔티티를 물리적으로 감지하기 위해 위협 엔티티의 위협 구역 내에 있지 않을 수 있더라도, 적어도 하나의 제2 무선 디바이스가 위협 엔티티를 가상으로 감지할 수 있게 한다.

[0126] [0153] 메시지는 위협 엔티티의 특성들과 관련된 정보를 포함할 수 있다. 일부 양상들에서, 메시지는 위협 엔티티의 타입과 연관된 신뢰도 값을 포함할 수 있다. 메시지는 적어도 제1 무선 디바이스의 대역폭에 걸쳐 측정된 RSSI의 평균을 포함할 수 있다. 재밍은 일반적으로 광대역이며, 제1 무선 디바이스의 전체 대역폭에 걸쳐 측정된 RSSI의 평균은 위협 엔티티를 재밍 디바이스인 것으로 표시할 수 있다. 일부 양상들에서, 메시지는 RSSI 임계치를 초과하는 각각의 서브채널에 대해 측정된 RSSI의 평균을 포함할 수 있다. 각각의 서브채널에 대한 RSSI의 평균은 시간 윈도우에 걸쳐 측정될 수 있다. 각각의 서브채널에 대해 측정된 RSSI의 평균은 위협 엔티티를 OOB 엔티티 또는 협대역 재머로서 표시할 수 있다. 메시지는 위협 엔티티로부터 수신된 데이터 신호들의 듀티 사이클을 포함할 수 있다. 위협 엔티티로부터의 데이터 신호의 듀티 사이클 정보는 무선 디바이스들이 듀티 사이클 동안 수신된 데이터를 무시하도록 허용할 수 있다. 일부 양상들에서, 메시지는 위협 엔티티의 L2 어드레스를 포함할 수 있다. 일부 경우들, 예를 들어, DoS 공격 또는 오작동 무선 디바이스(예컨대, 오작동 차량)에서, RSSI 보고는 관련이 없을 수 있다. 따라서, 메시지는 적어도 하나의 제2 무선 디바이스가 모뎀 계층에서 수신된 DoS 패킷들을 사전-필터링하도록 허용하기 위해 위협 엔티티의 L2 어드레스를 포함할 수 있다. 메시지는 위협 엔티티에 대응하는 적어도 하나의 IE를 추가로 표시할 수 있다. 적어도 하나의 IE는 위협 엔티티의 검출된 특성들을 포함할 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 포지션, 속력, 또는 진로, 또는 이들의 조합 중 적어도 하나를 포함할 수 있다. 예를 들어, 위협 엔티티의 포지션, 속력 및/또는 진로가 DoS 공격에 포함될 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 위협 엔티티의 포지션 주위의 반경을 포함할 수 있다. 예를 들어, 재머 또는 간섭자에 대해, 포지션 주위의 반경과 관련된 정보가 제공될 수 있다. 일부 양상들에서, 제1 무선 디바이스는 그의 다른 센서들(예컨대, 카메라, 레이더, LIDAR)로부터의 정보 및/또는 동일한 위협 엔티티를 검출하는 다른 무선 디바이스들로부터 수신된 메시지들(예컨대, SDSM 또는 MAP)을 조합하여 위협 엔티티의 특성들을 결정할 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 위협 엔티티의 측정된 RSSI와 관련된 정보를 포함할 수 있다. 일부 양상들에서, 위협 엔티티의 검출된 특성들은 위협 엔티티와 연관된 하나 이상의 계층들과 관련된 정보, 인증서 다이제스트, 셀 식별자 또는 PLMN을 포함할 수 있다. 메시지는 위협 엔티티를 위협 엔티티의 데이터 신호들을 송신하는 물체로서 식별할 수 있다. 일부 양상들에서, 물체는 VRU, 검출된 차량 또는 무선 장애물 중 하나를 포함할 수 있다.

[0127] [0154] 검출된 위협 타입이 C-V2X 재머인 경우들에서, IE(예컨대, DetectedJammerData)는 제1 무선 디바이스의 전체 대역폭 및 RSSI 평균 윈도우 크기에 걸친 RSSI의 평균과 관련된 정보를 포함할 수 있다. 일부 양상들에서, IE(예컨대, DetectedobjectCommonData)는 위협 엔티티의 위협 구역의 반경과 관련된 정보 뿐만 아니라 제1 무선 디바이스의 다른 센서들(예컨대, 카메라, 레이더, LIDAR)에 대한 조합된 정보를 포함할 수 있다. 검출된 위협 타입이 OOB 간섭자인 경우들에서, IE(예컨대, DetectedInterfererData)는 각각의 서브채널 또는 대역에 대한 측정된 RSSI, RSSI 보고 임계치, RSSI 평균 윈도우 크기 또는 위협 엔티티의 듀티 사이클을 포함할 수 있다. 검출된 위협 타입이 오작동 차량인 경우들에서, IE(예컨대, MisbehavingVehicleData)는 L2 어드레스 또는 인증서 다이제스트를 포함할 수 있다. 검출된 위협 타입이 WAN 재머인 경우들에서, IE(예컨대, DetectedJammerData)는 EARFCN, 셀 식별자들 또는 PLMN과 관련된 정보를 포함할 수 있다. 검출된 위협 타입이

GNSS 재머인 경우들에서, IE(예컨대, DetectedJammerData)는 GNSS 대역, L1, L2 또는 L5와 관련된 정보를 포함할 수 있다.

[0128] [0155] 도 24는 장치(2402)에 대한 하드웨어 구현의 예를 예시하는 도면(2400)이다. 장치(2402)는 UE이고, 셀룰러 RF 트랜시버(2422) 및 하나 이상의 SIM(subscriber identity module) 카드들(2420)에 커플링된 셀룰러 기저대역 프로세서(2404)(또한 모뎀으로 지칭됨), SD(secure digital) 카드(2408) 및 스크린(2410)에 커플링된 애플리케이션 프로세서(2406), 블루투스 모듈(2412), WLAN(wireless local area network) 모듈(2414), GNSS 모듈(2416) 및 전력 공급 장치(2418)를 포함한다. GNSS 모듈(2416)은 다양한 위성 포지셔닝 시스템들을 포함할 수 있다. 예를 들어, GNSS 모듈은 GPS(Global Positioning System), GLONASS(Global Navigation Satellite System), Galileo, BDS(BeiDou Navigation Satellite System), WAAS(Wide Area Augmentation System), EGNOS(European Geostationary Navigation Overlay Service), GAGAN(GPS Aided GEO Augmented Navigation), MSAS(MTSAT(Multifunctional Transport Satellites) Satellite Augmentation System), QZSS(Quasi-Zenith Satellite System), 또는 NavIC(Navigation with Indian Constellation)에 대응할 수 있다. 셀룰러 기저대역 프로세서(2404)는 셀룰러 RF 트랜시버(2422)를 통해 UE(104) 및/또는 BS(102/180)와 통신한다. 셀룰러 기저대역 프로세서(2404)는 컴퓨터 판독가능 매체/메모리를 포함할 수 있다. 컴퓨터 판독가능 매체/메모리는 비일시적일 수 있다. 셀룰러 기저대역 프로세서(2404)는, 컴퓨터 판독가능 매체/메모리 상에 저장된 소프트웨어의 실행을 포함하는 일반적인 프로세싱을 담당한다. 소프트웨어는, 셀룰러 기저대역 프로세서(2404)에 의해 실행될 때, 셀룰러 기저대역 프로세서(2404)로 하여금, 위에서 설명된 다양한 기능들을 수행하게 한다. 컴퓨터 판독가능 매체/메모리는 또한, 소프트웨어를 실행하는 경우 셀룰러 기저대역 프로세서(2404)에 의해 조작되는 데이터를 저장하기 위해 사용될 수 있다. 셀룰러 기저대역 프로세서(2404)는 수신 컴포넌트(2430), 통신 관리자(2432) 및 송신 컴포넌트(2434)를 더 포함한다. 통신 관리자(2432)는 하나 이상의 예시된 컴포넌트들을 포함한다. 통신 관리자(2432) 내의 컴포넌트들은 컴퓨터 판독가능 매체/메모리에 저장되고 그리고/또는 셀룰러 기저대역 프로세서(2404) 내의 하드웨어로서 구성될 수 있다. 셀룰러 기저대역 프로세서(2404)는 UE(350)의 컴포넌트일 수 있고, 메모리(360) 및/또는 TX 프로세서(368), RX 프로세서(356) 및 제어기/프로세서(359) 중 적어도 하나를 포함할 수 있다. 일 구성에서, 장치(2402)는 모뎀 칩일 수 있고, 단지 기저대역 프로세서(2404)를 포함할 수 있고, 다른 구성에서, 장치(2402)는 전체 UE(예컨대, 도 3의 350 참조)일 수 있고, 장치(2402)의 앞서 논의된 추가적인 모듈들을 포함할 수 있다.

[0129] [0156] 통신 관리자(2432)는 예컨대, 도 22의 2202 또는 도 23의 2302와 관련하여 설명된 바와 같이, 위협 구역 내의 위협 엔티티를 검출하도록 구성되는 검출 컴포넌트(2440)를 포함한다. 통신 관리자(2432)는 예컨대, 도 23의 2304와 관련하여 설명된 바와 같이, 제1 무선 디바이스에 의해 획득된 다른 데이터와 함께 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 엔티티의 추정된 로케이션을 결정하도록 구성되는 결정 컴포넌트(2442)를 더 포함한다. 통신 관리자(2432)는 예컨대, 도 23의 2306과 관련하여 설명된 바와 같이, 제3 무선 디바이스로부터, 위협 엔티티를 표시하는 보고를 수신하도록 구성되는 보고 컴포넌트(2444)를 더 포함한다. 통신 관리자(2432)는 예컨대, 도 22의 2204 또는 도 23의 2308과 관련하여 설명된 바와 같이, 위협 구역 내의 위협 엔티티를 표시하는 메시지를 송신하도록 구성되는 메시지 컴포넌트(2446)를 더 포함한다.

[0130] [0157] 장치는 도 22 또는 도 23의 전술된 흐름도들에서의 알고리즘의 블록들 각각을 수행하는 추가적인 컴포넌트들을 포함할 수 있다. 따라서, 도 22 또는 도 23의 전술된 흐름도들에서의 각각의 블록은 컴포넌트에 의해 수행될 수 있고, 장치는 그러한 컴포넌트들 중 하나 이상을 포함할 수 있다. 컴포넌트들은, 언급된 프로세스들/알고리즘을 수행하도록 특정적으로 구성된 하나 이상의 하드웨어 컴포넌트들일 수 있거나, 언급된 프로세스들/알고리즘을 수행하도록 구성된 프로세서에 의해 구현될 수 있거나, 프로세서에 의한 구현을 위해 컴퓨터 판독가능 매체 내에 저장될 수 있거나, 이들의 일부 조합일 수 있다.

[0131] [0158] 일 구성에서, 장치(2402), 및 특히 셀룰러 기저대역 프로세서(2404)는 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 구역 내의 위협 엔티티를 검출하기 위한 수단을 포함한다. 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해한다. 장치는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 적어도 하나의 제2 무선 디바이스에 송신하기 위한 수단을 포함한다. 장치는 제1 무선 디바이스의 하나 이상의 센서들로부터 수신된 데이터와 조합하여 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 엔티티의 추정된 로케이션을 결정하기 위한 수단을 더 포함한다. 장치는 제3 무선 디바이스로부터, 위협 엔티티를 표시하는 보고를 수신하기 위한 수단을 더 포함한다. 위협 엔티티의 추정된 로케이션은 보고의 수신에 대한 응답으로 결정된다. 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 장치(2402)의 전술된 컴포넌트들 중 하나 이상일 수 있다. 위에서 설명된 바와 같이, 장치

(2402)는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)를 포함할 수 있다. 따라서, 일 구성에서, 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)일 수 있다.

[0132] [0159] 도 25는 무선 통신 방법의 흐름도(2500)이다. 방법은 UE 또는 UE의 컴포넌트에 의해 수행될 수 있다(예컨대, UE(104); 장치(2702); 메모리(360)를 포함할 수 있고 전체 UE(350) 또는 UE(350)의 컴포넌트, 이를테면 TX 프로세서(368), RX 프로세서(356) 및/또는 제어기/프로세서(359)일 수 있는 셀룰러 기저대역 프로세서(2704)). 예시된 동작들 중 하나 이상은 선택적이거나, 생략되거나, 전치되거나, 또는 동시적일 수 있다. 방법은, 제2 무선 디바이스가 제1 무선 디바이스에 의해 검출된 위협 엔티티를 가상으로 감지하는 것에 기초하여 완화 액션을 개시하도록 허용할 수 있다.

[0133] [0160] 2502에서, 제2 무선 디바이스는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신할 수 있다. 예를 들어, 2502는 장치(2702)의 메시지 컴포넌트(2740)에 의해 수행될 수 있다. 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해할 수 있다. 제2 무선 디바이스는 제1 무선 디바이스로부터 또는 네트워크 엔티티로부터 메시지를 수신할 수 있다. 예를 들어, 제1 무선 디바이스는 위협 엔티티의 위협 구역 내에 있을 수 있고 위협 엔티티를 물리적으로 검출한다. 제1 무선 디바이스로부터 수신된 메시지는 SDSM 또는 CPM을 포함할 수 있다. 제2 무선 디바이스가 제1 무선 디바이스로부터 위협 엔티티를 표시하는 메시지를 수신하는 것은, 제2 무선 디바이스가 위협 엔티티의 위협 구역을 넘어선 것으로 인해 제2 무선 디바이스가 검출할 수 없는 위협 엔티티를 제2 무선 디바이스가 가상으로 감지할 수 있게 한다. 일부 양상들에서, 예를 들어, SPS(semi-persistent scheduling)에서, 제2 무선 디바이스는 예비들을 하기 위해 감지 윈도우 동안 데이터를 반송하는 서브채널들의 RSRP 및/또는 RSSI를 측정할 수 있다. 제2 무선 디바이스는, 측정된 RSRP/RSSI가 임계치를 초과하면, 후보 서브채널들의 리스트로부터 서브채널들을 배제할 수 있다. 또한, 제1 무선 디바이스로부터의 위협 엔티티를 표시하는 메시지를 사용하는 제2 무선 디바이스는 제1 무선 디바이스로부터의 위협 엔티티를 표시하는 메시지에서 보고된 RSSI 측정들에 기초하여 재밍 또는 간섭된 서브채널들을 배제할 수 있다. 이러한 가상 감지는, 특히 제2 무선 디바이스가 연장된 시간 기간 동안 SPS 예비들에 매달릴 가능성이 있는 경우, 제2 무선 디바이스에 의해 송신되는 메시지들의 수신 확률을 개선할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 네트워크 엔티티(예컨대, 기지국)로부터 위협 엔티티를 표시하는 메시지를 수신할 수 있다. 이러한 경우들에서, 무선 디바이스(예컨대, 제1 무선 디바이스)는 위협 엔티티의 위협 구역 내에 있는 동안 위협 엔티티를 물리적으로 검출하였다. 무선 디바이스는, 위협 구역 외부에 있고 위협 엔티티를 검출한 무선 디바이스로부터의 송신 범위를 넘어선 무선 디바이스들에 네트워크 엔티티가 메시지를 중계하도록 허용하기 위해, 검출된 위협 엔티티를 보고하는 메시지를 네트워크 엔티티에 송신하였다. 메시지는 위협 엔티티의 데이터 신호들의 듀티 사이클을 포함할 수 있다. 위협 엔티티의 데이터 신호의 듀티 사이클의 정보는 제2 무선 디바이스가 송신 예비들/구성들을 할 때 위협 엔티티의 듀티 사이클을 고려하게 할 수 있다. 일부 양상들에서, 메시지는 위협 엔티티를 검출한 제1 무선 디바이스의 안테나 엘리먼트들 중에서 피크 RSSI 검출을 포함할 수 있다. 지향성 수신으로 구성된 제1 무선 디바이스는, 위협 엔티티의 로케이션의 결정을 향상시킬 수 있고 메시지에 포함된 위협 구역을 제한하는 것을 보조할 수 있다.

[0134] [0161] 2504에서, 제2 무선 디바이스는 메시지(예컨대, SDSM)를 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 예를 들어, 2504는 장치(2702)의 완화 컴포넌트(2744)에 의해 수행될 수 있다. 제2 무선 디바이스는 위협 엔티티와의 접촉을 회피 또는 완화하기 위해 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 일부 양상들에서, 완화 액션은 위협 엔티티를 회피하기 위한 대안적인 경로를 선택하는 것, 더 견고한 MCS를 활용하는 것, 또는 위협 엔티티의 가상 감지를 포함할 수 있다. 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 실질적으로 저하시킬 수 있다. 협력적 또는 자동화된 운전 결정들은 안전 목적들을 위해 높은 신뢰도를 요구할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 검출된 위협 엔티티 또는 임의의 위협 엔티티에 의해 영향을 가장 적게 받는 것으로 주행의 스케줄링된 루트 또는 경로를 변경하기로 결정할 수 있다. 제2 무선 디바이스는, 제2 무선 디바이스가 네트워크 엔티티(예컨대, 기지국)로부터 위협 엔티티를 표시하는 메시지를 수신하는 경우들에서 위협 엔티티와의 접촉을 회피 또는 완화할 수 있다. 제1 무선 디바이스로부터 이격된 제2 무선 디바이스는 PC5를 통해 제1 무선 디바이스로부터 직접 메시지를 수신하기 위한 범위 내에 있지 않을 수 있어서, 제2 무선 디바이스는 Uu 링크를 통해 네트워크 엔티티(예컨대, 기지국)로부터 중계된 메시지를 수신한다. 제1 무선 디바이스로부터 떨어져 있는 제2 무선 디바이스는, 위협 엔티티를 회피하기 위해 대안적인 경로를 취하거나, 더 견고한 MCS를 활용하거나, 또는 위협 엔티티의 가상 감지와 같은 완화 액션을 준비하기에 충분한 시간을 제2 무선 디바이스에 제공할 수 있다. 일부 양상들에서, 네트워크 엔티티는 거리 교차로들에 있는 액세스 포인트들과 같은 알려진 위협들(예컨대, 정적)의 상세한

RF 핑거프린트를 제공하고 제2 무선 디바이스에 송신될 수 있는 Uu를 통해 클라우드 엔드포인트에 송신하도록 구성될 수 있는 기지국 또는 MEC 시스템을 포함할 수 있다. MEC는 부분적으로 더 높은 컴퓨테이셔널 자원들 및/또는 감각 입력들을 갖는 MEC로 인해 제1 무선 디바이스보다 위협 엔티티의 개선된 로컬화를 획득할 수 있다. 또한, 기지국 또는 MEC는 위협 엔티티를 보고하는 메시지를 PC5 및/또는 Uu 인터페이스들을 통해 제2 무선 디바이스에 송신할 수 있다.

[0135] [0162] 도 26은 무선 통신 방법의 흐름도(2600)이다. 방법은 UE 또는 UE의 컴포넌트에 의해 수행될 수 있다(예컨대, UE(104); 장치(2702); 메모리(360)를 포함할 수 있고 전체 UE(350) 또는 UE(350)의 컴포넌트, 이를테면 TX 프로세서(368), RX 프로세서(356) 및/또는 제어기/프로세서(359)일 수 있는 셀룰러 기저대역 프로세서(2704)). 예시된 동작들 중 하나 이상은 선택적이거나, 생략되거나, 전치되거나, 또는 동시적일 수 있다. 방법은, 제2 무선 디바이스가 제1 무선 디바이스에 의해 검출된 위협 엔티티를 가상으로 감지하는 것에 기초하여 완화 액션을 개시하도록 허용할 수 있다.

[0136] [0163] 2602에서, 제2 무선 디바이스는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신할 수 있다. 예를 들어, 2602는 장치(2702)의 메시지 컴포넌트(2740)에 의해 수행될 수 있다. 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해할 수 있다. 제2 무선 디바이스는 제1 무선 디바이스로부터 또는 네트워크 엔티티로부터 메시지를 수신할 수 있다. 예를 들어, 제1 무선 디바이스는 위협 엔티티의 위협 구역 내에 있을 수 있고 위협 엔티티를 물리적으로 검출한다. 제1 무선 디바이스로부터 수신된 메시지는 SDSM 또는 CPM을 포함할 수 있다. 제2 무선 디바이스가 제1 무선 디바이스로부터 위협 엔티티를 표시하는 메시지를 수신하는 것은, 제2 무선 디바이스가 위협 엔티티의 위협 구역을 넘어선 것으로 인해 제2 무선 디바이스가 검출할 수 없는 위협 엔티티를 제2 무선 디바이스가 가상으로 감지할 수 있게 한다. 일부 양상들에서, 예를 들어, SPS(semi-persistent scheduling)에서, 제2 무선 디바이스는 예비들을 하기 위해 감지 윈도우 동안 데이터를 반송하는 서브채널들의 RSRP 및/또는 RSSI를 측정할 수 있다. 제2 무선 디바이스는, 측정된 RSRP/RSSI가 임계치를 초과하면, 후보 서브채널들의 리스트로부터 서브채널들을 배제할 수 있다. 또한, 제1 무선 디바이스로부터의 위협 엔티티를 표시하는 메시지를 사용하는 제2 무선 디바이스는 제1 무선 디바이스로부터의 위협 엔티티를 표시하는 메시지에서 보고된 RSSI 측정들에 기초하여 재밍 또는 간섭된 서브채널들을 배제할 수 있다. 이러한 가상 감지는, 특히 제2 무선 디바이스가 연장된 시간 기간 동안 SPS 예비들에 매달릴 가능성이 있는 경우, 제2 무선 디바이스에 의해 송신되는 메시지들의 수신 확률을 개선할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 네트워크 엔티티(예컨대, 기지국)로부터 위협 엔티티를 표시하는 메시지를 수신할 수 있다. 이러한 경우들에서, 무선 디바이스(예컨대, 제1 무선 디바이스)는 위협 엔티티의 위협 구역 내에 있는 동안 위협 엔티티를 물리적으로 검출하였다. 무선 디바이스는, 위협 구역 외부에 있고 위협 엔티티를 검출한 무선 디바이스로부터의 송신 범위를 넘어선 무선 디바이스들에 네트워크 엔티티가 메시지를 중계하도록 허용하기 위해, 검출된 위협 엔티티를 보고하는 메시지를 네트워크 엔티티에 송신하였다. 메시지는 위협 엔티티의 데이터 신호들의 듀티 사이클을 포함할 수 있다. 위협 엔티티의 데이터 신호의 듀티 사이클의 정보는 제2 무선 디바이스가 송신 예비들/구성들을 할 때 위협 엔티티의 듀티 사이클을 고려하게 할 수 있다. 일부 양상들에서, 메시지는 위협 엔티티를 검출한 제1 무선 디바이스의 안테나 엘리먼트들 중에서 피크 RSSI 검출을 포함할 수 있다. 지향성 수신으로 구성된 제1 무선 디바이스는, 위협 엔티티의 로케이션의 결정을 향상시킬 수 있고 메시지에 포함된 위협 구역을 제한하는 것을 보조할 수 있다.

[0137] [0164] 2604에서, 제2 무선 디바이스는 메시지의 수신에 대한 응답으로 송신 파라미터들을 조정할 수 있다. 예를 들어, 2602는 장치(2702)의 조정 컴포넌트(2742)에 의해 수행될 수 있다. 제2 무선 디바이스는 BSM을 송신하기 위해 메시지의 수신에 대한 응답으로 송신 파라미터들을 조정할 수 있다. 일부 양상들에서, 조정된 송신 파라미터들은 송신 전력의 증가 또는 더 견고한 MCS의 사용, 또는 이들의 조합 중 적어도 하나를 포함할 수 있다. 더 견고한 MCS를 사용하는 것은 더 낮은 MCS로 스위칭하는 것을 포함할 수 있다. 일부 양상들에서, 송신 파라미터들을 조정하는 것은 위협 엔티티의 영향을 완화시킬 수 있지만, 확장된 범위 및/또는 증가된 오버-디-에어 송신 시간으로 인해 다른 무선 디바이스들과의 패킷 충돌 확률을 증가시킬 수 있다. 이러한 경우들에서, MCS 인덱스 및 송신 전력은 무선 디바이스 밀도 및 위협 신호 강도에 기초하여 조정될 수 있다.

[0138] [0165] 2606에서, 제2 무선 디바이스는 메시지(예컨대, SDSM)를 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 예를 들어, 2606은 장치(2702)의 완화 컴포넌트(2744)에 의해 수행될 수 있다. 제2 무선 디바이스는 위협 엔티티와의 접촉을 회피 또는 완화하기 위해 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 일부 양상들에서, 완화 액션은 위협 엔티티를 회피하기 위한 대안적인 경로를 선택하는 것, 더 견고한 MCS를 활용하는 것, 또는 위협 엔티티의 가상 감지를 포함할 수 있다. 위협 엔티티는 협력적 또는 자동

화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 실질적으로 저하시킬 수 있다. 협력적 또는 자동화된 운전 결정들은 안전 목적들을 위해 높은 신뢰도를 요구할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 검출된 위협 엔티티 또는 임의의 위협 엔티티에 의해 영향을 가장 적게 받는 것으로 주행의 스케줄링된 루트 또는 경로를 변경하기로 결정할 수 있다. 제2 무선 디바이스는, 제2 무선 디바이스가 네트워크 엔티티(예컨대, 기지국)로부터 위협 엔티티를 표시하는 메시지를 수신하는 경우들에서 위협 엔티티와의 접촉을 회피 또는 완화할 수 있다. 제1 무선 디바이스로부터 이격된 제2 무선 디바이스는 PC5를 통해 제1 무선 디바이스로부터 직접 메시지를 수신하기 위한 범위 내에 있지 않을 수 있어서, 제2 무선 디바이스는 Uu 링크를 통해 네트워크 엔티티(예컨대, 기지국)로부터 중계된 메시지를 수신한다. 제1 무선 디바이스로부터 떨어져 있는 제2 무선 디바이스는, 위협 엔티티를 회피하기 위해 대안적인 경로를 취하거나, 더 견고한 MCS를 활용하거나, 또는 위협 엔티티의 가상 감지와 같은 완화 액션을 준비하기에 충분한 시간을 제2 무선 디바이스에 제공할 수 있다. 일부 양상들에서, 네트워크 엔티티는 거리 교차로들에 있는 액세스 포인트들과 같은 알려진 위협들(예컨대, 정적)의 상세한 RF 핑거프린트를 제공하고 제2 무선 디바이스에 송신될 수 있는 Uu를 통해 클라우드 엔드포인트에 송신하도록 구성될 수 있는 RSU 또는 MEC 시스템을 포함할 수 있다. RSU 또는 MEC는 부분적으로 더 높은 컴퓨테이셔널 자원들 및/또는 감각 입력들을 갖는 RSU 또는 MEC로 인해 제1 무선 디바이스보다 위협 엔티티의 개선된 로컬화를 획득할 수 있다. 또한, RSU 또는 MEC는 위협 엔티티를 보고하는 메시지를 PC5 및/또는 Uu 인터페이스들을 통해 제2 무선 디바이스에 송신할 수 있다.

[0139] [0166] 도 27은 장치(2702)에 대한 하드웨어 구현의 예를 예시하는 도면(2700)이다. 장치(2702)는 UE이고, 셀룰러 RF 트랜시버(2722) 및 하나 이상의 SIM(subscriber identity module) 카드들(2720)에 커플링된 셀룰러 기저대역 프로세서(2704)(또한 모뎀으로 지칭됨), SD(secure digital) 카드(2708) 및 스크린(2710)에 커플링된 애플리케이션 프로세서(2706), 블루투스 모듈(2712), WLAN(wireless local area network) 모듈(2714), GNSS 모듈(2716) 및 전력 공급 장치(2718)를 포함한다. GNSS 모듈(2716)은 다양한 위성 포지셔닝 시스템들을 포함할 수 있다. 예를 들어, GNSS 모듈은 GPS(Global Positioning System), GLONASS(Global Navigation Satellite System), Galileo, BDS(BeiDou Navigation Satellite System), WAAS(Wide Area Augmentation System), EGNOS(European Geostationary Navigation Overlay Service), GAGAN(GPS Aided GEO Augmented Navigation), MSAS(MTSAT(Multifunctional Transport Satellites) Satellite Augmentation System), QZSS(Quasi-Zenith Satellite System), 또는 NavIC(Navigation with Indian Constellation)에 대응할 수 있다. 셀룰러 기저대역 프로세서(2704)는 셀룰러 RF 트랜시버(2722)를 통해 UE(104) 및/또는 BS(102/180)와 통신한다. 셀룰러 기저대역 프로세서(2704)는 컴퓨터 판독가능 매체/메모리를 포함할 수 있다. 컴퓨터 판독가능 매체/메모리는 비일시적일 수 있다. 셀룰러 기저대역 프로세서(2704)는, 컴퓨터 판독가능 매체/메모리 상에 저장된 소프트웨어의 실행을 포함하는 일반적인 프로세싱을 담당한다. 소프트웨어는, 셀룰러 기저대역 프로세서(2704)에 의해 실행될 때, 셀룰러 기저대역 프로세서(2704)로 하여금, 위에서 설명된 다양한 기능들을 수행하게 한다. 컴퓨터 판독가능 매체/메모리는 또한, 소프트웨어를 실행하는 경우 셀룰러 기저대역 프로세서(2704)에 의해 조작되는 데이터를 저장하기 위해 사용될 수 있다. 셀룰러 기저대역 프로세서(2704)는 수신 컴포넌트(2730), 통신 관리자(2732) 및 송신 컴포넌트(2734)를 더 포함한다. 통신 관리자(2732)는 하나 이상의 예시된 컴포넌트들을 포함한다. 통신 관리자(2732) 내의 컴포넌트들은 컴퓨터 판독가능 매체/메모리에 저장되고 그리고/또는 셀룰러 기저대역 프로세서(2704) 내의 하드웨어로서 구성될 수 있다. 셀룰러 기저대역 프로세서(2704)는 UE(350)의 컴포넌트일 수 있고, 메모리(360) 및/또는 TX 프로세서(368), RX 프로세서(356) 및 제어기/프로세서(359) 중 적어도 하나를 포함할 수 있다. 일 구성에서, 장치(2702)는 모뎀 칩일 수 있고, 단지 기저대역 프로세서(2704)를 포함할 수 있고, 다른 구성에서, 장치(2702)는 전체 UE(예컨대, 도 3의 350 참조)일 수 있고, 장치(2702)의 앞서 논의된 추가적인 모듈들을 포함할 수 있다.

[0140] [0167] 통신 관리자(2732)는 예컨대, 도 25의 2502 또는 도 26의 2602와 관련하여 설명된 바와 같이, 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신하도록 구성되는 메시지 컴포넌트(2740)를 포함한다. 통신 관리자(2732)는, 예컨대, 도 26의 2604와 관련하여 설명된 바와 같이, 메시지의 수신에 대한 응답으로 송신 파라미터들을 조정하도록 구성되는 조정 컴포넌트(2742)를 더 포함한다. 통신 관리자(2732)는, 예컨대, 도 25의 2504 또는 도 26의 2606과 관련하여 설명된 바와 같이, 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시하도록 구성되는 완화 컴포넌트(2744)를 더 포함한다.

[0141] [0168] 장치는 도 25 또는 도 26의 전술된 흐름도들에서의 알고리즘의 블록들 각각을 수행하는 추가적인 컴포넌트들을 포함할 수 있다. 따라서, 도 25 또는 도 26의 전술된 흐름도들에서의 각각의 블록은 컴포넌트에 의해 수행될 수 있고, 장치는 그러한 컴포넌트들 중 하나 이상을 포함할 수 있다. 컴포넌트들은, 언급된 프로세스들/알고리즘을 수행하도록 특정적으로 구성된 하나 이상의 하드웨어 컴포넌트들일 수 있거나, 언급된 프로세스들/

알고리즘을 수행하도록 구성된 프로세서에 의해 구현될 수 있거나, 프로세서에 의한 구현을 위해 컴퓨터 판독가능 매체 내에 저장될 수 있거나, 이들의 일부 조합일 수 있다.

[0142] [0169] 일 구성에서, 장치(2702), 및 특히 셀룰러 기저대역 프로세서(2704)는 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신하기 위한 수단을 포함한다. 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해한다. 장치는 위협 엔티티와의 접촉을 회피 또는 완화하기 위해 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시하기 위한 수단을 포함한다. 장치는, 메시지의 수신에 대한 응답으로 송신 파라미터들을 조정하기 위한 수단을 더 포함한다. 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 장치(2702)의 전술된 컴포넌트들 중 하나 이상일 수 있다. 위에서 설명된 바와 같이, 장치(2702)는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)를 포함할 수 있다. 따라서, 일 구성에서, 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)일 수 있다.

[0143] [0170] 도 28은 제1 무선 디바이스(2802) 및 제2 무선 디바이스(2804) 사이의 예시적인 통신 흐름(2800)을 예시한다. 통신은 송신 디바이스로부터 수신 디바이스로의 직접적인 V2X, V2V 또는 D2D 기반 통신에 기초할 수 있다. 디바이스(2802, 2804)로부터 송신하는 통신은 도 4와 관련하여 설명된 바와 같이, 특정 송신 디바이스의 범위 내의 다수의 수신 디바이스들에 의해 브로드캐스트 및 수신될 수 있다. 제1 무선 디바이스(2802)는 제1 UE에 대응할 수 있고, 제2 무선 디바이스(2804)는 제2 UE에 대응할 수 있다. 예를 들어, 도 1의 상황에서, 제1 무선 디바이스(2802)는 적어도 UE(104)에 대응할 수 있고, 제2 무선 디바이스(2804)는 적어도 104'에 대응할 수 있다. 다른 예에서, 도 3의 상황에서, 제1 무선 디바이스(2802)는 디바이스(350)에 대응할 수 있고, 제2 무선 디바이스(2804)는 디바이스(310)에 대응할 수 있다.

[0144] [0171] 2806에 예시된 바와 같이, 제1 무선 디바이스(2802)는 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 검출할 수 있다. 일부 양상들에서, 하나 이상의 물체 데이터 신호들은 오작동 무선 디바이스에 대응할 수 있다. 오작동 무선 디바이스의 데이터는 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 잘못된 또는 타당하지 않은 데이터를 포함할 수 있다. 일부 양상들에서, 오작동 무선 디바이스는 오작동 차량을 포함할 수 있다. 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 잘못된 또는 타당하지 않은 데이터는 로케이션, 속력 또는 진로 또는 이들의 조합 중 적어도 하나를 포함할 수 있다. 예를 들어, 하나 이상의 물체 데이터 신호들은 무선 디바이스들에 대해 현실적이지 않거나 예상되지 않는 데이터를 포함할 수 있다. 하나 이상의 물체 데이터 신호들은 실제 속력을 훨씬 넘어서는 속력의 값, 무의미하거나 또는 제1 무선 디바이스의 부근 내에 있지 않은 포지션 정보를 표시할 수 있거나, 또는 제1 무선 디바이스를 오버로딩하는 많은 양의 데이터를 포함할 수 있다. 하나 이상의 물체 데이터 신호들은, 본 개시가 본원에 제공된 예들로 제한되는 것으로 의도되지 않도록 다른 타입들의 일관되지 않거나 부정확한 데이터를 포함할 수 있다. 하나 이상의 물체 데이터 신호들은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물에 대응할 수 있다. 일부 양상들에서, 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물 또는 위협 엔티티의 하나 이상의 물체 데이터 신호들은 RSSI 임계치보다 큰 RSSI를 갖고 송신될 수 있다. 일부 양상들에서, 하나 이상의 물체 데이터 신호들은 DoS 공격자, 재머, 오작동 차량, OOB 간섭자, WAN 재머 또는 GNSS 재머에 대응할 수 있다. 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 하나 이상의 물체 데이터 신호들은 안전 사용 사례들에 대한 위협들을 제기할 수 있다. 예를 들어, 협력적 또는 자동화된 운전 결정들은 안전 목적들을 위해 높은 신뢰도를 요구할 수 있다. 장애물 또는 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 실질적으로 저하시킬 수 있다. 도로 조건들 및/또는 도로 사용자들에 대한 정확한 지식은 자동화된 차량들(예컨대, 제1 또는 제2 무선 디바이스)이 안전하고 효율적인 운전 결정들에 도달하도록 보조할 수 있으며, 이는 개별적으로 이루어지거나 또는 차량간 협의된 협력적인 기동들의 일부로서 이루어진 결정들을 포함할 수 있다.

[0145] [0172] 2808에 예시된 바와 같이, 제1 무선 디바이스(2802)는 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 송신할 수 있다. 제1 무선 디바이스(2802)는 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 적어도 제2 무선 디바이스(2804)에 송신할 수 있다. 제2 무선 디바이스(2804)는 제1 무선 디바이스(2802)로부터 메시지를 수신할 수 있다. 장애물 또는 위협 엔티티가 물리적 장애물과 반대로 스펙트럼 또는 보안 문제이기 때문에, 메시지는 SDSM 또는 CPM으로서 인코딩될 수 있다. 메시지는 위협 구역 외부의 적어도 하나의 제2 무선 디바이스뿐만 아니라 제1 무선 디바이스 부근 내의 임의의 다른 무선 디바이스로 브로드캐스트될 수 있다. 메시지는 사이드링크 통신(예컨대, PC5)을 통해 적어도 하나의 제2 무선 디바

이스에 브로드캐스트될 수 있다. 일부 양상들에서, 메시지는 PC5 인터페이스를 통해 네트워크 엔티티(예컨대, RSU)에 송신될 수 있다. 그러한 경우들에서, 네트워크 엔티티(예컨대, RSU)는, 제1 무선 디바이스의 송신 범위 밖에 있고 사이드링크 통신을 통해 메시지를 수신할 수 없는 다른 무선 디바이스들에 메시지를 중계할 수 있어서, 다른 무선 디바이스들은 예방 조치들을 사전에 취할 수 있다. 일부 양상들에서, 메시지는 검출된 하나 이상의 물체 데이터 신호들에 대응하는 적어도 하나의 IE를 추가로 표시한다. 적어도 하나의 IE는 검출된 오작동 무선 디바이스, DoS 공격자, 검출된 재머 또는 검출된 OOB 간섭자, WAN 재머, GNSS 재머 또는 이들의 조합 중 적어도 하나의 검출된 특성들을 포함할 수 있다. 적어도 하나의 IE는 검출된 물체들의 클래스들을 포함할 수 있다. 검출된 물체들의 각각의 클래스는 검출된 오작동 무선 디바이스, DoS 공격자, 검출된 재머 및 검출된 간섭자 중 개개의 하나에 대한 검출된 특성들을 포함할 수 있다. 검출된 물체 타입이 오작동 차량인 경우들에서, 검출된 물체 IE(예컨대, MisbehavingVehicleData)는 L2 어드레스 또는 인증서 다이제스트를 포함할 수 있다. 검출된 물체 타입이 OOB 간섭자인 경우들에서, 검출된 장애물 IE(예컨대, InterfererData)는 각각의 서브채널 또는 대역에 대한 측정된 RSSI, RSSI 보고 임계치, RSSI 평균 윈도우 크기 또는 위협의 듀티 사이클을 포함할 수 있다. 검출된 물체 타입이 C-V2X 재머인 경우들에서, 검출된 장애물 IE(예컨대, JammerData)는 제1 무선 디바이스의 전체 대역폭 및 RSSI 평균 윈도우 크기에 걸친 RSSI의 평균과 관련된 정보를 포함할 수 있다. 검출된 물체 타입이 GNSS 재머인 경우들에서, 검출된 장애물 IE(예컨대, JammerData)는 GNSS 대역, L1, L2 또는 L5와 관련된 정보를 포함할 수 있다. 검출된 물체 타입이 WAN 재머인 경우들에서, 검출된 장애물 IE(예컨대, JammerData)는 EARFCN, 셀 식별자들 또는 PLMN과 관련된 정보를 포함할 수 있다.

[0146] [0173] 일부 양상들에서, 메시지는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 송신하고 있을 수 있는 물체를 식별할 수 있다. 예를 들어, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 물체 또는 장애물은 기존의 검출된 물체들에 기초하여 식별될 수 있다. 일부 양상들에서, 물체는 VRU, 검출된 차량 또는 무선 장애물 중 하나를 포함할 수 있다. 예를 들어, VRU는 재머, 간섭자 또는 오작동 차량에 대응하는 속성들을 포함할 수 있다. 일부 양상들에서, 검출된 차량은 재머, 간섭자 또는 오작동 차량에 대응하는 속성들을 포함할 수 있다. 일부 양상들에서, 장애물은 재머, 간섭자 또는 오작동 차량에 대응하는 속성들을 포함할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 무선 차량, RSU 또는 VRU 중 적어도 하나를 포함한다.

[0147] [0174] 2810에 예시된 바와 같이, 제2 무선 디바이스(2804)는 메시지(예컨대, SDSM)를 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 제2 무선 디바이스(2804)는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해, 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 일부 양상들에서, 메시지는 협력적 또는 자동화된 운전 결정들을 방해하는 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해 적어도 제2 무선 디바이스에서 완화 액션을 트리거링할 수 있다. 장애물은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해할 수 있다. 일부 양상들에서, 완화 액션은 위협 엔티티를 회피하기 위한 대안적인 경로를 선택하는 것, 더 견고한 MCS를 활용하는 것, 또는 위협 엔티티의 가상 감지를 포함할 수 있다. 장애물은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 실질적으로 저하시킬 수 있다. 협력적 또는 자동화된 운전 결정들은 안전 목적들을 위해 높은 신뢰도를 요구할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 검출된 장애물 또는 임의의 장애물에 의해 영향을 가장 적게 받는 것으로 주행의 스케줄링된 루트 또는 경로를 변경하기로 결정할 수 있다.

[0148] [0175] 도 29는 무선 통신 방법의 흐름도(2900)이다. 방법은 UE 또는 UE의 컴포넌트에 의해 수행될 수 있다(예컨대, UE(104); 장치(3002); 메모리(360)를 포함할 수 있고 전체 UE(350) 또는 UE(350)의 컴포넌트, 이를테면 TX 프로세서(368), RX 프로세서(356) 및/또는 제어기/프로세서(359)일 수 있는 셀룰러 기저대역 프로세서(3004)). 예시된 동작들 중 하나 이상은 선택적이거나, 생략되거나, 전치되거나, 또는 동시적일 수 있다. 방법은, 제1 무선 디바이스가 검출된 위협 엔티티와 관련된 정보를 다른 무선 디바이스들과 공유하게 허용할 수 있다.

[0149] [0176] 2902에서, 제1 무선 디바이스는 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 검출할 수 있다. 예를 들어, 2902는 장치(3002)의 검출 컴포넌트(3040)에 의해 수행될 수 있다. 일부 양상들에서, 하나 이상의 물체 데이터 신호들은 오작동 무선 디바이스에 대응할 수 있다. 오작동 무선 디바이스의 데이터는 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 잘못된 또는 타당하지 않은 데이터를 포함할 수 있다. 일부 양상들에서, 오작동 무선 디바이스는 오작동 차량을 포함할 수 있다. 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 잘못된 또는 타당하지 않은 데이터는 로케이션,

속력 또는 진로 또는 이들의 조합 중 적어도 하나를 포함할 수 있다. 예를 들어, 하나 이상의 물체 데이터 신호들은 무선 디바이스들에 대해 현실적이지 않거나 예상되지 않는 데이터를 포함할 수 있다. 하나 이상의 물체 데이터 신호들은 실제 속력을 훨씬 넘어서는 속력의 값, 무의미하거나 또는 제1 무선 디바이스의 부근 내에 있지 않은 포지션 정보를 표시할 수 있거나, 또는 제1 무선 디바이스를 오버로딩하는 많은 양의 데이터를 포함할 수 있다. 하나 이상의 물체 데이터 신호들은, 본 개시가 본원에 제공된 예들로 제한되는 것으로 의도되지 않도록 다른 타입들의 일관되지 않거나 부정확한 데이터를 포함할 수 있다. 하나 이상의 물체 데이터 신호들은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물에 대응할 수 있다. 일부 양상들에서, 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물 또는 위협 엔티티의 하나 이상의 물체 데이터 신호들은 RSSI 임계치보다 큰 RSSI를 갖고 송신될 수 있다. 일부 양상들에서, 하나 이상의 물체 데이터 신호들은 DoS 공격자, 재머, 오작동 차량, OOB 간섭자, WAN 재머 또는 GNSS 재머에 대응할 수 있다. 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 하나 이상의 물체 데이터 신호들은 안전 사용 사례들에 대한 위협들을 제기할 수 있다. 예를 들어, 협력적 또는 자동화된 운전 결정들은 안전 목적들을 위해 높은 신뢰도를 요구할 수 있다. 장애물 또는 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 실질적으로 저하시킬 수 있다. 도로 조건들 및/또는 도로 사용자들에 대한 정확한 지식은 자동화된 차량들(예컨대, 제1 또는 제2 무선 디바이스)이 안전하고 효율적인 운전 결정들에 도달하도록 보조할 수 있으며, 이는 개별적으로 이루어지거나 또는 차량간 협의된 협력적인 기동들의 일부로서 이루어진 결정들을 포함할 수 있다.

[0150] [0177] 2904에서, 제1 무선 디바이스는 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 송신할 수 있다. 예를 들어, 2904는 장치(3002)의 메시지 컴포넌트(3042)에 의해 수행될 수 있다. 제1 무선 디바이스는 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 적어도 제2 무선 디바이스에 송신할 수 있다. 장애물 또는 위협 엔티티가 물리적 장애물과 반대로 스펙트럼 또는 보안 문제이기 때문에, 메시지는 SDSM 또는 CPM으로서 인코딩될 수 있다. 메시지는 위협 구역 외부의 적어도 하나의 제2 무선 디바이스뿐만 아니라 제1 무선 디바이스 부근 내의 임의의 다른 무선 디바이스로 브로드캐스트될 수 있다. 메시지는 사이드링크 통신(예컨대, PC5)을 통해 적어도 하나의 제2 무선 디바이스에 브로드캐스트될 수 있다. 일부 양상들에서, 메시지는 PC5 인터페이스를 통해 네트워크 엔티티(예컨대, RSU)에 송신될 수 있다. 그러한 경우들에서, 네트워크 엔티티(예컨대, RSU)는, 제1 무선 디바이스의 송신 범위 밖에 있고 사이드링크 통신을 통해 메시지를 수신할 수 없는 다른 무선 디바이스들에 메시지를 중계할 수 있어서, 다른 무선 디바이스들은 예방 조치들을 사전에 취할 수 있다. 일부 양상들에서, 메시지는 검출된 하나 이상의 물체 데이터 신호들에 대응하는 적어도 하나의 IE를 추가로 표시한다. 적어도 하나의 IE는 검출된 오작동 무선 디바이스, DoS 공격자, 검출된 재머, 검출된 OOB 간섭자, WAN 재머, GNSS 재머 또는 이들의 조합 중 적어도 하나의 검출된 특성들을 포함할 수 있다. 적어도 하나의 IE는 검출된 물체들의 클래스들을 포함할 수 있다. 검출된 물체들의 각각의 클래스는 검출된 오작동 무선 디바이스, DoS 공격자, 검출된 재머 및 검출된 간섭자 중 개개의 하나에 대한 검출된 특성들을 포함할 수 있다. 검출된 물체 타입이 오작동 차량인 경우들에서, 검출된 물체 IE(예컨대, MisbehavingVehicleData)는 L2 어드레스 또는 인증서 다이제스트를 포함할 수 있다. 검출된 물체 타입이 OOB 간섭자인 경우들에서, 검출된 장애물 IE(예컨대, InterfererData)는 각각의 서브채널 또는 대역에 대한 측정된 RSSI, RSSI 보고 임계치, RSSI 평균 윈도우 크기 또는 위협의 듀티 사이클을 포함할 수 있다. 검출된 물체 타입이 C-V2X 재머인 경우들에서, 검출된 장애물 IE(예컨대, JammerData)는 제1 무선 디바이스의 전체 대역폭 및 RSSI 평균 윈도우 크기에 걸친 RSSI의 평균과 관련된 정보를 포함할 수 있다. 검출된 물체 타입이 GNSS 재머인 경우들에서, 검출된 장애물 IE(예컨대, JammerData)는 GNSS 대역, L1, L2 또는 L5와 관련된 정보를 포함할 수 있다. 검출된 물체 타입이 WAN 재머인 경우들에서, 검출된 장애물 IE(예컨대, JammerData)는 EARFCN, 셀 식별자들 또는 PLMN과 관련된 정보를 포함할 수 있다.

[0151] [0178] 일부 양상들에서, 메시지(예컨대, SDSM)는 협력적 또는 자동화된 운전 결정들을 방해하는 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해 적어도 제2 무선 디바이스에서 완화 액션을 트리거링할 수 있다. 제2 무선 디바이스로의 메시지의 송신은 장애물 또는 위협 엔티티의 조기 검출을 제2 무선 디바이스에 제공할 수 있어서, 제2 무선 디바이스는 메시지에 기초하여 회피 또는 완화 액션들을 개시하도록 트리거링될 수 있다. 일부 양상들에서, 메시지는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 송신하고 있을 수 있는 물체를 식별할 수 있다. 예를 들어, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 물체 또는 장애물은 기존의 검출된 물체들에 기초하여 식별될 수 있다. 일부 양상들에서, 물체는 VRU, 검출된 차량 또는 무선 장애물 중 하나를 포함할 수 있다. 예를

들어, VRU는 재머, 간섭자 또는 오작동 차량에 대응하는 속성들을 포함할 수 있다. 일부 양상들에서, 검출된 차량은 재머, 간섭자 또는 오작동 차량에 대응하는 속성들을 포함할 수 있다. 일부 양상들에서, 장애물은 재머, 간섭자 또는 오작동 차량에 대응하는 속성들을 포함할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 무선 차량, RSU 또는 VRU 중 적어도 하나를 포함한다.

[0152] [0179] 도 30은 장치(3002)에 대한 하드웨어 구현의 예를 예시하는 도면(3000)이다. 장치(3002)는 UE이고, 셀룰러 RF 트랜시버(3022) 및 하나 이상의 SIM(subscriber identity module) 카드들(3020)에 커플링된 셀룰러 기저대역 프로세서(3004)(또한 모뎀으로 지칭됨), SD(secure digital) 카드(3008) 및 스크린(3010)에 커플링된 애플리케이션 프로세서(3006), 블루투스 모듈(3012), WLAN(wireless local area network) 모듈(3014), GNSS 모듈(3016) 및 전력 공급 장치(3018)를 포함한다. GNSS 모듈(3016)은 다양한 위성 포지셔닝 시스템들을 포함할 수 있다. 예를 들어, GNSS 모듈은 GPS(Global Positioning System), GLONASS(Global Navigation Satellite System), Galileo, BDS(BeiDou Navigation Satellite System), WAAS(Wide Area Augmentation System), EGNOS(European Geostationary Navigation Overlay Service), GAGAN(GPS Aided GEO Augmented Navigation), MSAS(MTSAT(Multifunctional Transport Satellites) Satellite Augmentation System), QZSS(Quasi-Zenith Satellite System), 또는 NavIC(Navigation with Indian Constellation)에 대응할 수 있다. 셀룰러 기저대역 프로세서(3004)는 셀룰러 RF 트랜시버(3022)를 통해 UE(104) 및/또는 BS(102/180)와 통신한다. 셀룰러 기저대역 프로세서(3004)는 컴퓨터 판독가능 매체/메모리를 포함할 수 있다. 컴퓨터 판독가능 매체/메모리는 비일시적일 수 있다. 셀룰러 기저대역 프로세서(3004)는, 컴퓨터 판독가능 매체/메모리 상에 저장된 소프트웨어의 실행을 포함하는 일반적인 프로세싱을 담당한다. 소프트웨어는, 셀룰러 기저대역 프로세서(3004)에 의해 실행될 때, 셀룰러 기저대역 프로세서(3004)로 하여금, 위에서 설명된 다양한 기능들을 수행하게 한다. 컴퓨터 판독가능 매체/메모리는 또한, 소프트웨어를 실행하는 경우 셀룰러 기저대역 프로세서(3004)에 의해 조작되는 데이터를 저장하기 위해 사용될 수 있다. 셀룰러 기저대역 프로세서(3004)는 수신 컴포넌트(3030), 통신 관리자(3032) 및 송신 컴포넌트(3034)를 더 포함한다. 통신 관리자(3032)는 하나 이상의 예시된 컴포넌트들을 포함한다. 통신 관리자(3032) 내의 컴포넌트들은 컴퓨터 판독가능 매체/메모리에 저장되고 그리고/또는 셀룰러 기저대역 프로세서(3004) 내의 하드웨어로서 구성될 수 있다. 셀룰러 기저대역 프로세서(3004)는 UE(350)의 컴포넌트일 수 있고, 메모리(360) 및/또는 TX 프로세서(368), RX 프로세서(356) 및 제어기/프로세서(359) 중 적어도 하나를 포함할 수 있다. 일 구성에서, 장치(3002)는 모뎀 칩일 수 있고, 단지 기저대역 프로세서(3004)를 포함할 수 있고, 다른 구성에서, 장치(3002)는 전체 UE(예컨대, 도 3의 350 참조)일 수 있고, 장치(3002)의 앞서 논의된 추가적인 모듈들을 포함할 수 있다.

[0153] [0180] 통신 관리자(3032)는, 예컨대, 도 29의 2902와 관련하여 설명된 바와 같이, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 검출하도록 구성되는 검출 컴포넌트(3040)를 포함한다. 통신 관리자(3032)는 예컨대, 도 29의 2904와 관련하여 설명된 바와 같이, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 송신하도록 구성되는 메시지 컴포넌트(3042)를 더 포함한다.

[0154] [0181] 장치는 도 29의 전술된 흐름도에서의 알고리즘의 블록들 각각을 수행하는 추가적인 컴포넌트들을 포함할 수 있다. 따라서, 도 29의 전술된 흐름도에서의 각각의 블록은 컴포넌트에 의해 수행될 수 있고, 장치는 그러한 컴포넌트들 중 하나 이상을 포함할 수 있다. 컴포넌트들은, 언급된 프로세스들/알고리즘을 수행하도록 특정적으로 구성된 하나 이상의 하드웨어 컴포넌트들일 수 있거나, 언급된 프로세스들/알고리즘을 수행하도록 구성된 프로세서에 의해 구현될 수 있거나, 프로세서에 의한 구현을 위해 컴퓨터 판독가능 매체 내에 저장될 수 있거나, 이들의 일부 조합일 수 있다.

[0155] [0182] 일 구성에서, 장치(3002), 및 특히 셀룰러 기저대역 프로세서(3004)는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 검출하기 위한 수단을 포함한다. 장치는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 적어도 제2 무선 디바이스에 송신하기 위한 수단을 포함한다. 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 장치(3002)의 전술된 컴포넌트들 중 하나 이상일 수 있다. 위에서 설명된 바와 같이, 장치(3002)는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)를 포함할 수 있다. 따라서, 일 구성에서, 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)일 수 있다.

[0156] [0183] 도 31은 무선 통신 방법의 흐름도(3100)이다. 방법은 UE 또는 UE의 컴포넌트에 의해 수행될 수 있다(예컨대, UE(104); 장치(3202); 메모리(360)를 포함할 수 있고 전체 UE(350) 또는 UE(350)의 컴포넌트, 이를테면

TX 프로세서(368), RX 프로세서(356) 및/또는 제어기/프로세서(359)일 수 있는 셀룰러 기저대역 프로세서(3204)). 예시된 동작들 중 하나 이상은 선택적이거나, 생략되거나, 전치되거나, 또는 동시적일 수 있다. 방법은, 제2 무선 디바이스가 위협 장애물의 위협 구역을 넘어선 동안 제1 무선 디바이스에 의해 검출된 위협 장애물의 통지를 수신하는 것에 대한 응답으로 완화 액션을 개시하도록 허용할 수 있다.

[0157] [0184] 3102에서, 제2 무선 디바이스는 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 수신할 수 있다. 예를 들어, 3102는 장치(3202)의 메시지 컴포넌트(3240)에 의해 수행될 수 있다. 제2 무선 디바이스는 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 제1 무선 디바이스로부터 수신할 수 있다. 일부 양상들에서, 하나 이상의 물체 데이터 신호들은 오작동 무선 디바이스에 대응할 수 있다. 오작동 무선 디바이스의 데이터는 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 잘못된 또는 타당하지 않은 데이터를 포함할 수 있다. 일부 양상들에서, 오작동 무선 디바이스는 오작동 차량을 포함할 수 있다. 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 잘못된 또는 타당하지 않은 데이터는 로케이션, 속력 또는 진로 또는 이들의 조합 중 적어도 하나를 포함할 수 있다. 예를 들어, 하나 이상의 물체 데이터 신호들은 무선 디바이스들에 대해 현실적이지 않거나 예상되지 않는 데이터를 포함할 수 있다. 하나 이상의 물체 데이터 신호들은 실제 속력을 훨씬 넘어서는 속력의 값, 무의미하거나 또는 제1 무선 디바이스의 부근 내에 있지 않은 포지션 정보를 표시할 수 있거나, 또는 제1 무선 디바이스를 오버로딩하는 많은 양의 데이터를 포함할 수 있다. 하나 이상의 물체 데이터 신호들은, 본 개시가 본원에 제공된 예들로 제한되는 것으로 의도되지 않도록 다른 타입들의 일관되지 않거나 부정확한 데이터를 포함할 수 있다. 하나 이상의 물체 데이터 신호들은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물에 대응할 수 있다. 일부 양상들에서, 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물 또는 위협 엔티티의 하나 이상의 물체 데이터 신호들은 RSSI 임계치보다 큰 RSSI를 갖고 송신될 수 있다. 일부 양상들에서, 하나 이상의 물체 데이터 신호들은 DoS 공격자, 재머, 오작동 차량, OOB 간섭자, WAN 재머 또는 GNSS 재머에 대응할 수 있다. 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 하나 이상의 물체 데이터 신호들은 안전 사용 사례들에 대한 위협들을 제기할 수 있다. 예를 들어, 협력적 또는 자동화된 운전 결정들은 안전 목적들을 위해 높은 신뢰도를 요구할 수 있다. 장애물 또는 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 실질적으로 저하시킬 수 있다. 도로 조건들 및/또는 도로 사용자들에 대한 정확한 지식은 자동화된 차량들(예컨대, 제1 또는 제2 무선 디바이스)이 안전하고 효율적인 운전 결정들에 도달하도록 보조할 수 있으며, 이는 개별적으로 이루어지거나 또는 차량간 협의된 협력적인 기동들의 일부로서 이루어진 결정들을 포함할 수 있다.

[0158] [0185] 일부 양상들에서, 메시지는 검출된 하나 이상의 물체 데이터 신호들에 대응하는 적어도 하나의 IE를 추가로 표시한다. 적어도 하나의 IE는 검출된 오작동 무선 디바이스, DoS 공격자, 검출된 재머, 검출된 OOB 간섭자, WAN 재머, GNSS 재머 또는 이들의 조합 중 적어도 하나의 검출된 특성들을 포함할 수 있다. 적어도 하나의 IE는 검출된 물체들의 클래스들을 포함할 수 있다. 검출된 물체들의 각각의 클래스는 검출된 오작동 무선 디바이스, DoS 공격자, 검출된 재머 및 검출된 간섭자 중 개개의 하나에 대한 검출된 특성들을 포함할 수 있다. 검출된 물체 타입이 오작동 차량인 경우들에서, 검출된 물체 IE(예컨대, MisbehavingVehicleData)는 L2 어드레스 또는 인증서 다이제스트를 포함할 수 있다. 검출된 물체 타입이 OOB 간섭자인 경우들에서, 검출된 장애물 IE(예컨대, InterfererData)는 각각의 서브채널 또는 대역에 대한 측정된 RSSI, RSSI 보고 임계치, RSSI 평균 윈도우 크기 또는 위협의 듀티 사이클을 포함할 수 있다. 검출된 물체 타입이 C-V2X 재머인 경우들에서, 검출된 장애물 IE(예컨대, JammerData)는 제1 무선 디바이스의 전체 대역폭 및 RSSI 평균 윈도우 크기에 걸친 RSSI의 평균과 관련된 정보를 포함할 수 있다. 검출된 물체 타입이 GNSS 재머인 경우들에서, 검출된 장애물 IE(예컨대, JammerData)는 GNSS 대역, L1, L2 또는 L5와 관련된 정보를 포함할 수 있다. 검출된 물체 타입이 WAN 재머인 경우들에서, 검출된 장애물 IE(예컨대, JammerData)는 EARFCN, 셀 식별자들 또는 PLMN과 관련된 정보를 포함할 수 있다.

[0159] [0186] 일부 양상들에서, 메시지는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 송신하고 있을 수 있는 물체를 식별할 수 있다. 예를 들어, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 물체 또는 장애물은 기존의 검출된 물체들에 기초하여 식별될 수 있다. 일부 양상들에서, 물체는 VRU, 검출된 차량 또는 무선 장애물 중 하나를 포함할 수 있다. 예를 들어, VRU는 재머, 간섭자 또는 오작동 차량에 대응하는 속성들을 포함할 수 있다. 일부 양상들에서, 검출된 차량은 재머, 간섭자 또는 오작동 차량에 대응하는 속성들을 포함할 수 있다. 일부 양상들에서, 장애물은 재머, 간섭자 또는 오작동 차량에 대응하는 속성들을 포함할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 무선 차량,

RSU 또는 VRU 중 적어도 하나를 포함한다.

[0160] [0187] 3104에서, 제2 무선 디바이스는 메시지(예컨대, SDSM)를 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 예를 들어, 3104는 장치(3202)의 완화 컴포넌트(3242)에 의해 수행될 수 있다. 제2 무선 디바이스는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해, 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시할 수 있다. 일부 양상들에서, 메시지는 협력적 또는 자동화된 운전 결정들을 방해하는 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해 적어도 제2 무선 디바이스에서 완화 액션을 트리거링할 수 있다. 장애물은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해할 수 있다. 일부 양상들에서, 완화 액션은 위협 엔티티를 회피하기 위한 대안적인 경로를 선택하는 것, 더 견고한 MCS를 활용하는 것, 또는 위협 엔티티의 가상 감지를 포함할 수 있다. 장애물은 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 실질적으로 저하시킬 수 있다. 협력적 또는 자동화된 운전 결정들은 안전 목적들을 위해 높은 신뢰도를 요구할 수 있다. 일부 양상들에서, 제2 무선 디바이스는 검출된 장애물 또는 임의의 장애물에 의해 영향을 가장 적게 받는 것으로 주행의 스케줄링된 루트 또는 경로를 변경하기로 결정할 수 있다.

[0161] [0188] 도 32는 장치(3202)에 대한 하드웨어 구현의 예를 예시하는 도면(3200)이다. 장치(3202)는 UE이고, 셀룰러 RF 트랜시버(3222) 및 하나 이상의 SIM(subscriber identity module) 카드들(3220)에 커플링된 셀룰러 기저대역 프로세서(3204)(또한 모뎀으로 지칭됨), SD(secure digital) 카드(3208) 및 스크린(3210)에 커플링된 애플리케이션 프로세서(3206), 블루투스 모듈(3212), WLAN(wireless local area network) 모듈(3214), GNSS 모듈(3216) 및 전력 공급 장치(3218)를 포함한다. GNSS 모듈(3216)은 다양한 위성 포지셔닝 시스템들을 포함할 수 있다. 예를 들어, GNSS 모듈은 GPS(Global Positioning System), GLONASS(Global Navigation Satellite System), Galileo, BDS(BeiDou Navigation Satellite System), WAAS(Wide Area Augmentation System), EGNOS(European Geostationary Navigation Overlay Service), GAGAN(GPS Aided GEO Augmented Navigation), MSAS(MTSAT(Multifunctional Transport Satellites) Satellite Augmentation System), QZSS(Quasi-Zenith Satellite System), 또는 NavIC(Navigation with Indian Constellation)에 대응할 수 있다. 셀룰러 기저대역 프로세서(3204)는 셀룰러 RF 트랜시버(3222)를 통해 UE(104) 및/또는 BS(102/180)와 통신한다. 셀룰러 기저대역 프로세서(3204)는 컴퓨터 판독가능 매체/메모리를 포함할 수 있다. 컴퓨터 판독가능 매체/메모리는 비일시적일 수 있다. 셀룰러 기저대역 프로세서(3204)는, 컴퓨터 판독가능 매체/메모리 상에 저장된 소프트웨어의 실행을 포함하는 일반적인 프로세싱을 담당한다. 소프트웨어는, 셀룰러 기저대역 프로세서(3204)에 의해 실행될 때, 셀룰러 기저대역 프로세서(3204)로 하여금, 위에서 설명된 다양한 기능들을 수행하게 한다. 컴퓨터 판독가능 매체/메모리는 또한, 소프트웨어를 실행하는 경우 셀룰러 기저대역 프로세서(3204)에 의해 조작되는 데이터를 저장하기 위해 사용될 수 있다. 셀룰러 기저대역 프로세서(3204)는 수신 컴포넌트(3230), 통신 관리자(3232) 및 송신 컴포넌트(3234)를 더 포함한다. 통신 관리자(3232)는 하나 이상의 예시된 컴포넌트들을 포함한다. 통신 관리자(3232) 내의 컴포넌트들은 컴퓨터 판독가능 매체/메모리에 저장되고 그리고/또는 셀룰러 기저대역 프로세서(3204) 내의 하드웨어로서 구성될 수 있다. 셀룰러 기저대역 프로세서(3204)는 UE(350)의 컴포넌트일 수 있고, 메모리(360) 및/또는 TX 프로세서(368), RX 프로세서(356) 및 제어기/프로세서(359) 중 적어도 하나를 포함할 수 있다. 일 구성에서, 장치(3202)는 모뎀 칩일 수 있고, 단지 기저대역 프로세서(3204)를 포함할 수 있고, 다른 구성에서, 장치(3202)는 전체 UE(예컨대, 도 3의 350 참조)일 수 있고, 장치(3202)의 앞서 논의된 추가적인 모듈들을 포함할 수 있다.

[0162] [0189] 통신 관리자(3232)는 예컨대, 도 31의 3102와 관련하여 설명된 바와 같이, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 수신하도록 구성되는 메시지 컴포넌트(3240)를 포함한다. 통신 관리자(3232)는, 예컨대, 도 31의 3104와 관련하여 설명된 바와 같이, 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시하도록 구성되는 완화 컴포넌트(3242)를 더 포함한다.

[0163] [0190] 장치는 도 31의 전술된 흐름도에서의 알고리즘의 블록들 각각을 수행하는 추가적인 컴포넌트들을 포함할 수 있다. 따라서, 도 31의 전술된 흐름도에서의 각각의 블록은 컴포넌트에 의해 수행될 수 있고, 장치는 그러한 컴포넌트들 중 하나 이상을 포함할 수 있다. 컴포넌트들은, 언급된 프로세스들/알고리즘을 수행하도록 특정적으로 구성된 하나 이상의 하드웨어 컴포넌트들일 수 있거나, 언급된 프로세스들/알고리즘을 수행하도록 구성된 프로세서에 의해 구현될 수 있거나, 프로세서에 의한 구현을 위해 컴퓨터 판독가능 매체 내에 저장될 수 있거나, 이들의 일부 조합일 수 있다.

[0164] [0191] 일 구성에서, 장치(3202), 및 특히 셀룰러 기저대역 프로세서(3204)는, 제1 무선 디바이스로부터, 자동

화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 수신하기 위한 수단을 포함한다. 장치는, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해, 메시지(예컨대, SDSM)를 수신하는 것에 대한 응답으로 완화 액션을 개시하기 위한 수단을 포함한다. 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 장치(3202)의 전술된 컴포넌트들 중 하나 이상일 수 있다. 위에서 설명된 바와 같이, 장치(3202)는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)를 포함할 수 있다. 따라서, 일 구성에서, 전술된 수단은, 전술된 수단에 의해 인용된 기능들을 수행하도록 구성되는 TX 프로세서(368), RX 프로세서(356), 및 제어기/프로세서(359)일 수 있다.

[0165] [0192] 개시된 프로세스들/흐름도들의 블록들의 특정 순서 또는 계층구조는 예시적인 접근법들의 예시임이 이해된다. 설계 선호도들에 기초하여, 프로세스들/흐름도들의 블록들의 특정 순서 또는 계층구조는 재배열될 수 있음이 이해된다. 추가로, 일부 블록들은 결합되거나 생략될 수 있다. 첨부된 방법 청구항들은 다양한 블록들의 엘리먼트들을 예시적 순서로 제시하고, 제시된 특정 순서 또는 계층구조로 제한되도록 의도되지 않는다.

[0166] [0193] 다음의 예들은 단지 예시적이며, 제한 없이, 본원에서 설명된 다른 실시예들 또는 교시들의 양상들과 조합될 수 있다.

[0167] [0194] 양상 1은 제1 무선 디바이스에서의 무선 통신 방법이고, BSM들의 송신을 간섭하는 데이터를 송신하는 위협 엔티티를 검출하는 단계; 및 위협 엔티티의 타입과 관련된 정보를 표시하는 메시지를 제2 무선 디바이스에 송신하는 단계를 포함한다.

[0168] [0195] 양상 2에서, 양상 1의 방법은, 서브채널들의 서브세트에 대한 또는 서브채널들의 서브세트 내의 각각의 서브채널에 대한 RSSI의 평균이 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 것에 기초하여 메시지 내의 정보가 RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트를 포함하는 것을 더 포함한다.

[0169] [0196] 양상 3에서, 양상 1 또는 양상 2의 방법은, 메시지 내의 정보가 서브채널들의 서브세트에 대한 평균 RSSI, 서브채널들의 서브세트 내의 각각의 서브채널에 대한 평균 RSSI, RSSI 임계치, RSSI 윈도우 시간 길이, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 또는 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 또는 이들의 조합 중 적어도 하나를 더 표시하는 것을 더 포함한다.

[0170] [0197] 양상 4에서, 양상 1 내지 양상 3 중 어느 하나의 방법은, 송신된 메시지가 SDSM, I2V 메시지 또는 CPM인 것을 더 포함한다.

[0171] [0198] 양상 5에서, 양상 1 내지 양상 4 중 어느 하나의 방법은, 위협 엔티티가 재머, OOB 간섭자, WAN 재머 또는 GNSS 재머를 포함하는 것을 더 포함한다.

[0172] [0199] 양상 6은, 하나 이상의 트랜시버들, 하나 이상의 프로세서들, 및 하나 이상의 트랜시버들 및 하나 이상의 프로세서들과 전자 통신하는 하나 이상의 메모리들을 포함하는 디바이스이고, 메모리들은 디바이스로 하여금 양상 1 내지 양상 5 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장한다.

[0173] [0200] 양상 7은, 양상 1 내지 양상 5 중 어느 하나에서와 같은 방법을 구현하거나 장치를 실현하기 위한 수단을 포함하는 시스템 또는 장치이다.

[0174] [0201] 양상 8은 하나 이상의 프로세서들로 하여금 양상 1 내지 양상 5 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장하는 비일시적 컴퓨터 판독가능 저장 매체이다.

[0175] [0202] 양상 9는 제2 무선 디바이스에서의 무선 통신 방법이고, 제1 무선 디바이스로부터 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신하는 단계 – 위협 엔티티는 BSM들의 송신을 간섭하는 데이터를 송신함 –; 제1 무선 디바이스로부터 위협 엔티티와 관련된 정보를 표시하는 메시지에 적어도 부분적으로 기초하여 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정하는 단계; 및 결정된 후보 자원 상에서 BSM을 적어도 제3 무선 디바이스에 송신하는 단계를 포함한다.

[0176] [0203] 양상 10에서, 양상 9의 방법은, 서브채널들의 서브세트에 대한 또는 서브채널들의 서브세트 내의 각각의 서브채널에 대한 RSSI의 평균이 적어도 RSSI 윈도우 시간 길이에 대해 RSSI 임계치보다 큰 것에 기초하여 메시

지 내의 정보가 RSSI 임계치보다 큰 RSSI를 갖는 서브채널들의 서브세트를 포함하는 것을 더 포함한다.

[0177] [0204] 양상 11에서, 양상 9 또는 양상 10의 방법은, 메시지 내의 정보가 서브채널들의 서브세트에 대한 평균 RSSI, 서브채널들의 서브세트 내의 각각의 서브채널에 대한 평균 RSSI, RSSI 임계치, RSSI 윈도우 시간 길이, 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 또는 서브채널들의 서브세트 중 적어도 하나에서 RSSI에 영향을 미치는 위협 엔티티와 연관된 로케이션 신뢰도 반경, 또는 이들의 조합 중 적어도 하나를 더 표시하는 것을 더 포함한다.

[0178] [0205] 양상 12에서, 양상 9 내지 양상 11 중 어느 하나의 방법은, 수신된 메시지가 SDSM, I2V 메시지 또는 CPM인 것을 더 포함한다.

[0179] [0206] 양상 13에서, 양상 9 내지 양상 12 중 어느 하나의 방법은, 위협 엔티티가 재머, OOB 간섭자, WAN 재머 또는 GNSS 재머를 포함하는 것을 더 포함한다.

[0180] [0207] 양상 14에서, 양상 9 내지 양상 13 중 어느 하나의 방법은, 후보 자원이 CSR을 포함하고, 후보 자원들의 세트가 CSR들의 세트를 포함하는 것을 더 포함한다.

[0181] [0208] 양상 15에서, 양상 9 내지 양상 14 중 어느 하나의 방법은, 후보 자원들의 세트 중 후보 자원을 결정하는 것이, 후보 자원들의 제1 서브세트를 결정하기 위해 후보 자원들의 세트에서 각각의 후보 자원에 대한 투사된 RSRP가 RSRP 임계치를 초과하는 것에 기초하여 후보 자원들의 세트에서 하나 이상의 후보 자원들을 배제하는 것; 가장 낮은 가중된 RSSI를 갖는 후보 자원들의 제2 서브세트를 획득하기 위해 가중된 RSSI 랭킹에 기초하여 후보 자원들의 제1 서브세트를 랭킹하는 것 - 제2 서브세트의 후보 자원들은 후보 자원들의 제1 서브세트의 일부임 -; 및 후보 자원들의 제2 서브세트로부터 후보 자원을 선택하는 것을 더 포함하는 것을 더 포함한다.

[0182] [0209] 양상 16에서, 양상 9 내지 양상 15 중 어느 하나의 방법은, 가중된 RSSI가 물리적으로 감지된 후보 자원들 및 하나 이상의 가상으로 감지된 후보 자원들을 포함하는 것을 더 포함한다.

[0183] [0210] 양상 17에서, 양상 9 내지 양상 16 중 어느 하나의 방법은, 물리적으로 감지된 후보 자원들이 감지 윈도우 내에서 제2 무선 디바이스에 의해 측정된 후보 자원들을 포함하는 것을 더 포함한다.

[0184] [0211] 양상 18에서, 양상 9 내지 양상 17 중 어느 하나의 방법은, 하나 이상의 가상으로 감지된 후보 자원들이 제1 무선 디바이스에 의해 측정되고 제1 무선 디바이스로부터 제2 무선 디바이스에 의해 수신된 메시지 내에 표시된 후보 자원들을 포함하는 것을 더 포함한다.

[0185] [0212] 양상 19에서, 양상 9 내지 양상 18 중 어느 하나의 방법은, 하나 이상의 가상으로 감지된 후보 자원들이 후보 자원들의 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 위협 엔티티와 연관된 로케이션 신뢰도 반경, 제1 무선 디바이스로부터 수신된 메시지와 연관된 타임스탬프, 제2 무선 디바이스의 속도, 제2 무선 디바이스의 가속도, 위협 엔티티의 로케이션과 관련된 제2 무선 디바이스의 주행 방향, 도로 기하구조와 관련된 정보, 또는 BSM과 연관된 송신 요건들, 또는 이들의 조합 중 적어도 하나에 기초하는 것을 더 포함한다.

[0186] [0213] 양상 20에서, 양상 9 내지 양상 19 중 어느 하나의 방법은, 후보 자원들의 세트 중 후보 자원을 결정하는 것이, 사전-필터 임계치를 초과하지 않는 후보 자원들의 필터링된 서브세트를 획득하기 위해, 사전-필터 임계치를 초과하는 RSSI를 갖는 후보 자원들의 세트에서 하나 이상의 가상으로 감지된 후보 자원들을 배제하는 것; RSRP 임계치를 초과하지 않는 후보 자원들의 제2 서브세트를 획득하기 위해, RSRP 임계치를 초과하는 사전-필터 임계치를 초과하지 않는, 후보 자원들의 필터링된 서브세트 내의 후보 자원들을 배제하는 것; 및 후보 자원들의 제2 서브세트로부터 후보 자원을 선택하는 것을 더 포함하는 것을 더 포함한다.

[0187] [0214] 양상 21에서, 양상 9 내지 양상 20 중 어느 하나의 방법은, 하나 이상의 가상으로 감지된 후보 자원들이 제1 무선 디바이스에 의해 측정되고 제1 무선 디바이스로부터 제2 무선 디바이스에 의해 수신된 메시지 내에 표시되는 것을 더 포함한다.

[0188] [0215] 양상 22에서, 양상 9 내지 양상 21 중 어느 하나의 방법은, 후보 자원들의 제2 서브세트가, 사전-필터 임계치를 초과하지 않는, 선택 풀 내의 총 후보 자원들의 미리 구성된 비율을 포함하는 것을 더 포함한다.

[0189] [0216] 양상 23에서, 양상 9 내지 양상 22 중 어느 하나의 방법은, 사전-필터 임계치가, 후보 자원들의 제2 서브세트가 선택 풀 내의 총 후보 자원들의 미리 구성된 비율 미만의 후보 자원들의 양을 포함하면 조정되는 것을 더 포함한다.

[0190] [0217] 양상 24에서, 양상 9 내지 양상 23 중 어느 하나의 방법은, 사전-필터 임계치가, 후보 자원들의 제2 서

브세트가 선택 풀 내의 총 후보 자원들의 미리 구성된 비율을 포함할 때까지 추가로 조정되는 것을 더 포함한다.

[0191] [0218] 양상 25에서, 양상 9 내지 양상 24 중 어느 하나의 방법은, 가상으로 감지된 후보 자원들이 후보 자원들의 RSSI에 영향을 미치는 위협 엔티티의 로케이션, 위협 엔티티와 연관된 로케이션 신뢰도 반경, 제1 무선 디바이스로부터 수신된 메시지와 연관된 타임스탬프, 제2 무선 디바이스의 속도, 제2 무선 디바이스의 가속도, 위협 엔티티의 로케이션과 관련된 제2 무선 디바이스의 주행 방향, 도로 기하구조와 관련된 정보, 또는 BSM과 연관된 송신 요건들, 또는 이들의 조합 중 적어도 하나에 기초하는 것을 더 포함한다.

[0192] [0219] 양상 26에서, 양상 9 내지 양상 25 중 어느 하나의 방법은, 후보 자원들의 세트 중 후보 자원의 결정이, 위협 구역 내의 위협 엔티티를 표시하는 추가적인 메시지들이 다른 무선 디바이스들로부터 수신되는지 여부에 기초하는 것을 더 포함한다.

[0193] [0220] 양상 27은, 하나 이상의 트랜시버들, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들과 전자 통신하는 하나 이상의 메모리들을 포함하는 디바이스이고, 메모리들은 디바이스로 하여금 양상 9 내지 양상 26 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장한다.

[0194] [0221] 양상 28은, 양상 9 내지 양상 26 중 어느 하나에서와 같은 방법을 구현하거나 장치를 실현하기 위한 수단을 포함하는 시스템 또는 장치이다.

[0195] [0222] 양상 29는 하나 이상의 프로세서들로 하여금 양상 9 내지 양상 26 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장하는 비일시적 컴퓨터 판독가능 저장 매체이다.

[0196] [0223] 양상 30은 제1 무선 디바이스에서의 무선 통신 방법이고, 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 구역 내의 위협 엔티티를 검출하는 단계 - 위협 엔티티는 협력적 또는 자동 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해함 -; 및 위협 구역 내의 위협 엔티티를 표시하는 메시지를 적어도 하나의 제2 무선 디바이스에 송신하는 단계를 포함한다.

[0197] [0224] 양상 31에서, 양상 30의 방법은, 위협 엔티티로부터 수신된 데이터 신호들이 무선 디바이스들에 대한 투사된 데이터와 일치하지 않는 데이터를 포함하는 것을 더 포함한다.

[0198] [0225] 양상 32에서, 양상 30 또는 양상 31의 방법은, 데이터 신호들이 오작동 무선 디바이스의 데이터를 포함하고, 오작동 무선 디바이스의 데이터가 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 타당하지 않은 데이터를 포함하는 것을 더 포함한다.

[0199] [0226] 양상 33에서, 양상 30 내지 양상 32 중 어느 하나의 방법은, 위협 엔티티의 타입이 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 결정되고, 위협 엔티티의 타입이 DoS 공격자, 재머, 오작동 차량, OOB 간섭자 또는 GNSS 재머를 포함하는 것을 더 포함한다.

[0200] [0227] 양상 34에서, 양상 30 내지 양상 33 중 어느 하나의 방법은, 메시지가 위협 엔티티의 타입과 연관된 신뢰도 값을 포함하는 것을 더 포함한다.

[0201] [0228] 양상 35에서, 양상 30 내지 양상 34 중 어느 하나의 방법은, 메시지가 적어도 제1 무선 디바이스의 대역폭에 걸쳐 측정된 평균 RSSI를 포함하는 것을 더 포함한다.

[0202] [0229] 양상 36에서, 양상 30 내지 양상 35 중 어느 하나의 방법은, 메시지가 RSSI 임계치를 초과하는 각각의 서브채널에 대해 측정된 평균 RSSI를 포함하고, 각각의 서브채널에 대한 평균 RSSI가 시간 윈도우에 걸쳐 측정되는 것을 더 포함한다.

[0203] [0230] 양상 37에서, 양상 30 내지 양상 36 중 어느 하나의 방법은, 메시지가 위협 엔티티의 L2 어드레스를 포함하는 것을 더 포함한다.

[0204] [0231] 양상 38에서, 양상 30 내지 양상 37 중 어느 하나의 방법은, 제1 무선 디바이스의 하나 이상의 센서들로부터 수신된 데이터와 조합하여 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 엔티티의 추정된 로케이션을 결정하는 단계를 더 포함한다.

[0205] [0232] 양상 39에서, 양상 30 내지 양상 38 중 어느 하나의 방법은, 제3 무선 디바이스로부터, 위협 엔티티를 표시하는 보고를 수신하는 단계를 더 포함하고, 위협 엔티티의 추정된 로케이션은 보고의 수신에 대한 응답으로

결정된다.

[0206] [0233] 양상 40에서, 양상 30 내지 양상 39 중 어느 하나의 방법은, 메시지가 위협 엔티티의 추정된 로케이션 및 위협 엔티티의 추정된 로케이션과 연관된 신뢰도 값을 포함하는 것을 더 포함한다.

[0207] [0234] 양상 41에서, 양상 30 내지 양상 40 중 어느 하나의 방법은, 메시지가 위협 엔티티에 대응하는 적어도 하나의 IE를 추가로 표시하고, 적어도 하나의 IE가 위협 엔티티의 검출된 특성들을 포함하는 것을 더 포함한다.

[0208] [0235] 양상 42에서, 양상 30 내지 양상 41 중 어느 하나의 방법은, 위협 엔티티의 검출된 특성들이 포지션, 속력, 또는 진로, 또는 이들의 조합 중 적어도 하나를 포함하는 것을 더 포함한다.

[0209] [0236] 양상 43에서, 양상 30 내지 양상 42 중 어느 하나의 방법은, 위협 엔티티의 검출된 특성들이 위협 엔티티의 포지션 주위의 반경을 포함하는 것을 더 포함한다.

[0210] [0237] 양상 44에서, 양상 30 내지 양상 43 중 어느 하나의 방법은, 위협 엔티티의 검출된 특성들이 위협 엔티티의 측정된 RSSI와 관련된 정보를 포함하는 것을 더 포함한다.

[0211] [0238] 양상 45에서, 양상 30 내지 양상 44 중 어느 하나의 방법은, 위협 엔티티의 검출된 특성들이 위협 엔티티와 연관된 하나 이상의 계층들과 관련된 정보, 인증서 다이제스트, 셀 식별자 또는 PLMN을 포함하는 것을 더 포함한다.

[0212] [0239] 양상 46에서, 양상 30 내지 양상 45 중 어느 하나의 방법은, 메시지가 위협 엔티티를 위협 엔티티의 데이터 신호들을 송신하는 물체로서 식별하는 것을 더 포함한다.

[0213] [0240] 양상 47에서, 양상 30 내지 양상 46 중 어느 하나의 방법은, 물체가 VRU, 검출된 차량 또는 무선 장애물 중 하나를 포함할 수 있는 것을 더 포함한다.

[0214] [0241] 양상 48에서, 양상 30 내지 양상 47 중 어느 하나의 방법은, 메시지기 적어도 하나의 제3 무선 디바이스로부터 수신된 위협 엔티티의 보고들의 수, 위협 엔티티의 심각도, 위협 엔티티 및 제1 무선 디바이스를 분리하는 거리, 또는 적어도 하나의 제2 무선 디바이스가 위협 구역에 접근하는 시간, 또는 이들의 조합 중 적어도 하나에 기초하여 송신되는 것을 더 포함한다.

[0215] [0242] 양상 49에서, 양상 30 내지 양상 48 중 어느 하나의 방법은, 메시지가 위협 엔티티와의 접촉을 회피 또는 완화시키기 위해 적어도 하나의 제2 무선 디바이스에서 완화 액션을 트리거링하는 것을 더 포함한다.

[0216] [0243] 양상 50에서, 양상 30 내지 양상 49 중 어느 하나의 방법은, 메시지가 위협 엔티티로부터 수신된 데이터 신호들의 듀티 사이클을 포함하는 것을 더 포함한다.

[0217] [0244] 양상 51은, 하나 이상의 트랜시버들, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들과 전자 통신하는 하나 이상의 메모리들을 포함하는 디바이스이고, 메모리들은 디바이스로 하여금 양상 30 내지 양상 50 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장한다.

[0218] [0245] 양상 52는, 양상 30 내지 양상 50 중 어느 하나에서와 같은 방법을 구현하거나 장치를 실현하기 위한 수단을 포함하는 시스템 또는 장치이다.

[0219] [0246] 양상 53은 하나 이상의 프로세서들로 하여금 양상 30 내지 양상 50 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장하는 비일시적 컴퓨터 판독가능 저장 매체이다.

[0220] [0247] 양상 54는 제2 무선 디바이스에서의 무선 통신 방법이고, 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신하는 단계 - 위협 엔티티는 협력적 또는 자동 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해함 -; 및 위협 엔티티와의 접촉을 회피 또는 완화하기 위해 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시하는 단계를 포함한다.

[0221] [0248] 양상 55에서, 양상 54의 방법은, 메시지의 수신에 대한 응답으로 송신 파라미터들을 조정하는 단계를 더 포함한다.

[0222] [0249] 양상 56에서, 양상 54 또는 양상 55의 방법은, 조정된 송신 파라미터들이 송신 전력의 증가 또는 더 견고한 MCS의 사용, 또는 이들의 조합 중 적어도 하나를 포함하는 것을 더 포함한다.

[0223] [0250] 양상 57에서, 양상 54 내지 양상 56 중 어느 하나의 방법은, 완화 액션이 위협 엔티티를 회피하기 위한

대안적인 경로의 선택을 포함하는 것을 더 포함한다.

[0224] [0251] 양상 58에서, 양상 54 내지 양상 57 중 어느 하나의 방법은, 메시지가 제1 무선 디바이스로부터 또는 네트워크 엔티티로부터 수신되는 것을 더 포함한다.

[0225] [0252] 양상 59는, 하나 이상의 트랜시버들, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들과 전자 통신하는 하나 이상의 메모리들을 포함하는 디바이스이고, 메모리들은 디바이스로 하여금 양상 54 내지 양상 58 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장한다.

[0226] [0253] 양상 60은, 양상 54 내지 양상 58 중 어느 하나에서와 같은 방법을 구현하거나 장치를 실현하기 위한 수단을 포함하는 시스템 또는 장치이다.

[0227] [0254] 양상 61은 하나 이상의 프로세서들로 하여금 양상 54 내지 양상 58 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장하는 비일시적 컴퓨터 판독가능 저장 매체이다.

[0228] [0255] 양상 62는 제1 무선 디바이스에서의 무선 통신 방법이고, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 검출하는 단계; 및 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 적어도 제2 무선 디바이스에 송신하는 단계를 포함한다.

[0229] [0256] 양상 63에서, 양상 62의 방법은, 하나 이상의 물체 데이터 신호들이 오작동 무선 디바이스에 대응하고, 오작동 무선 디바이스의 데이터가 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 타당하지 않은 데이터를 포함하는 것을 더 포함한다.

[0230] [0257] 양상 64에서, 양상 62 또는 양상 63의 방법은, 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 타당하지 않은 데이터가 로케이션, 속력 또는 진로 또는 이들의 조합 중 적어도 하나를 포함하는 것을 더 포함한다.

[0231] [0258] 양상 65에서, 양상 62 내지 양상 64 중 어느 하나의 방법은, 오작동 무선 디바이스가 오작동 차량을 포함하는 것을 더 포함한다.

[0232] [0259] 양상 66에서, 양상 62 내지 양상 65 중 어느 하나의 방법은, 하나 이상의 물체 데이터 신호들이 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물에 대응하는 것을 더 포함한다.

[0233] [0260] 양상 67에서, 양상 62 내지 양상 66 중 어느 하나의 방법은, 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물의 하나 이상의 물체 데이터 신호들이 RSSI 임계치보다 큰 RSSI를 갖고 송신되는 것을 더 포함한다.

[0234] [0261] 양상 68에서, 양상 62 내지 양상 67 중 어느 하나의 방법은, 하나 이상의 물체 데이터 신호들이 DoS 공격자, 재머, 또는 OBB 간섭자를 포함하는 것을 더 포함한다.

[0235] [0262] 양상 69에서, 양상 62 내지 양상 68 중 어느 하나의 방법은, 메시지가 검출된 하나 이상의 물체 데이터 신호들에 대응하는 적어도 하나의 IE를 추가로 표시하고, 적어도 하나의 IE가 검출된 오작동 무선 디바이스, DoS 공격자, 검출된 재머 또는 검출된 OOB 간섭자 또는 이들의 조합 중 적어도 하나의 검출된 특성들을 포함하는 것을 더 포함한다.

[0236] [0263] 양상 70에서, 양상 62 내지 양상 69 중 어느 하나의 방법은, 적어도 하나의 IE가 검출된 물체들의 클래스들을 포함하고, 검출된 물체들의 각각의 클래스가 검출된 오작동 무선 디바이스, DoS 공격자, 검출된 재머 및 검출된 간섭자 중 개개의 하나에 대한 검출된 특성들을 포함하는 것을 더 포함한다.

[0237] [0264] 양상 71에서, 양상 62 내지 양상 70 중 어느 하나의 방법은, 메시지가 협력적 또는 자동화된 운전 결정들을 방해하는 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해 적어도 제2 무선 디바이스에서 완화 액션을 트리거링하는 것을 더 포함한다.

[0238] [0265] 양상 72에서, 양상 62 내지 양상 71 중 어느 하나의 방법은, 메시지가, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 송신하고 있는 물체를 식별하는 것을 더 포함한다.

[0239] [0266] 양상 73에서, 양상 62 내지 양상 72 중 어느 하나의 방법은, 물체가 VRU, 검출된 차량 또는 무선 장애물 중 하나를 포함하는 것을 더 포함한다.

[0240] [0267] 양상 74에서, 양상 62 내지 양상 73 중 어느 하나의 방법은, 제2 무선 디바이스가 무선 차량, RSU 또는 VRU 중 적어도 하나를 포함하는 것을 더 포함한다.

[0241] [0268] 양상 75는, 하나 이상의 트랜시버들, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들과 전자 통신하는 하나 이상의 메모리들을 포함하는 디바이스이고, 메모리들은 디바이스로 하여금 양상 62 내지 양상 74 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장한다.

[0242] [0269] 양상 76은, 양상 62 내지 양상 74 중 어느 하나에서와 같은 방법을 구현하거나 장치를 실현하기 위한 수단을 포함하는 시스템 또는 장치이다.

[0243] [0270] 양상 77은 하나 이상의 프로세서들로 하여금 양상 62 내지 양상 74 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장하는 비일시적 컴퓨터 판독가능 저장 매체이다.

[0244] [0271] 양상 78은 제2 무선 디바이스에서의 무선 통신 방법이고, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 수신하는 단계; 및 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해, 메시지를 수신하는 것에 대한 응답으로 완화 액션을 개시하는 단계를 포함한다.

[0245] [0272] 양상 79에서, 양상 78의 방법은, 하나 이상의 물체 데이터 신호들이 오작동 무선 디바이스에 대응하고, 오작동 무선 디바이스의 데이터가 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 타당하지 않은 데이터를 포함하는 것을 더 포함한다.

[0246] [0273] 양상 80에서, 양상 78 또는 양상 79의 방법은, 오작동 무선 디바이스의 적어도 하나의 특성과 관련된 타당하지 않은 데이터가 로케이션, 속력 또는 진로 또는 이들의 조합 중 적어도 하나를 포함하는 것을 더 포함한다.

[0247] [0274] 양상 81에서, 양상 78 내지 양상 80 중 어느 하나의 방법은, 오작동 무선 디바이스가 오작동 차량을 포함하는 것을 더 포함한다.

[0248] [0275] 양상 82에서, 양상 78 내지 양상 81 중 어느 하나의 방법은, 하나 이상의 물체 데이터 신호들이 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물에 대응하는 것을 더 포함한다.

[0249] [0276] 양상 83에서, 양상 78 내지 양상 82 중 어느 하나의 방법은, 무선 스펙트럼 또는 자원들을 간섭하거나 방해하는 장애물의 하나 이상의 물체 데이터 신호들이 RSSI 임계치보다 큰 RSSI를 갖고 송신되는 것을 더 포함한다.

[0250] [0277] 양상 84에서, 양상 78 내지 양상 83 중 어느 하나의 방법은, 하나 이상의 물체 데이터 신호들이 DoS 공격자, 재머, 또는 OBB 간섭자를 포함하는 것을 더 포함한다.

[0251] [0278] 양상 85에서, 양상 78 내지 양상 84 중 어느 하나의 방법은, 메시지가 검출된 하나 이상의 물체 데이터 신호들에 대응하는 적어도 하나의 IE를 추가로 표시하고, 적어도 하나의 IE가 검출된 오작동 무선 디바이스, DoS 공격자, 검출된 재머 또는 검출된 OOB 간섭자 또는 이들의 조합 중 적어도 하나의 검출된 특성들을 포함하는 것을 더 포함한다.

[0252] [0279] 양상 86에서, 양상 78 내지 양상 85 중 어느 하나의 방법은, 적어도 하나의 IE가 검출된 물체들의 클래스들을 포함하고, 검출된 물체들의 각각의 클래스가 검출된 오작동 무선 디바이스, DoS 공격자, 검출된 재머 및 검출된 간섭자 중 개개의 하나에 대한 검출된 특성들을 포함하는 것을 더 포함한다.

[0253] [0280] 양상 87에서, 양상 78 내지 양상 86 중 어느 하나의 방법은, 메시지가 협력적 또는 자동화된 운전 결정들을 방해하는 하나 이상의 물체 데이터 신호들과의 접촉을 회피 또는 완화하기 위해 적어도 제2 무선 디바이스에서 완화 액션을 트리거링하는 것을 더 포함한다.

[0254] [0281] 양상 88에서, 양상 78 내지 양상 87 중 어느 하나의 방법은, 메시지가, 자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 송신하고 있는 물체를 식별하는

것을 더 포함한다.

[0255] [0282] 양상 89에서, 양상 78 내지 양상 88 중 어느 하나의 방법은, 물체가 VRU, 검출된 차량 또는 무선 장애물 중 하나를 포함하는 것을 더 포함한다.

[0256] [0283] 양상 90에서, 양상 78 내지 양상 89 중 어느 하나의 방법은, 제2 무선 디바이스가 무선 차량, RSU 또는 VRU 중 적어도 하나를 포함하는 것을 더 포함한다.

[0257] [0284] 양상 91에서, 양상 78 내지 양상 90 중 어느 하나의 방법은, 메시지가 제1 무선 디바이스로부터 또는 RSU로부터 수신되는 것을 더 포함한다.

[0258] [0285] 양상 92는, 하나 이상의 트랜시버들, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들과 전자 통신하는 하나 이상의 메모리들을 포함하는 디바이스이고, 메모리들은 디바이스로 하여금 양상 78 내지 양상 91 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장한다.

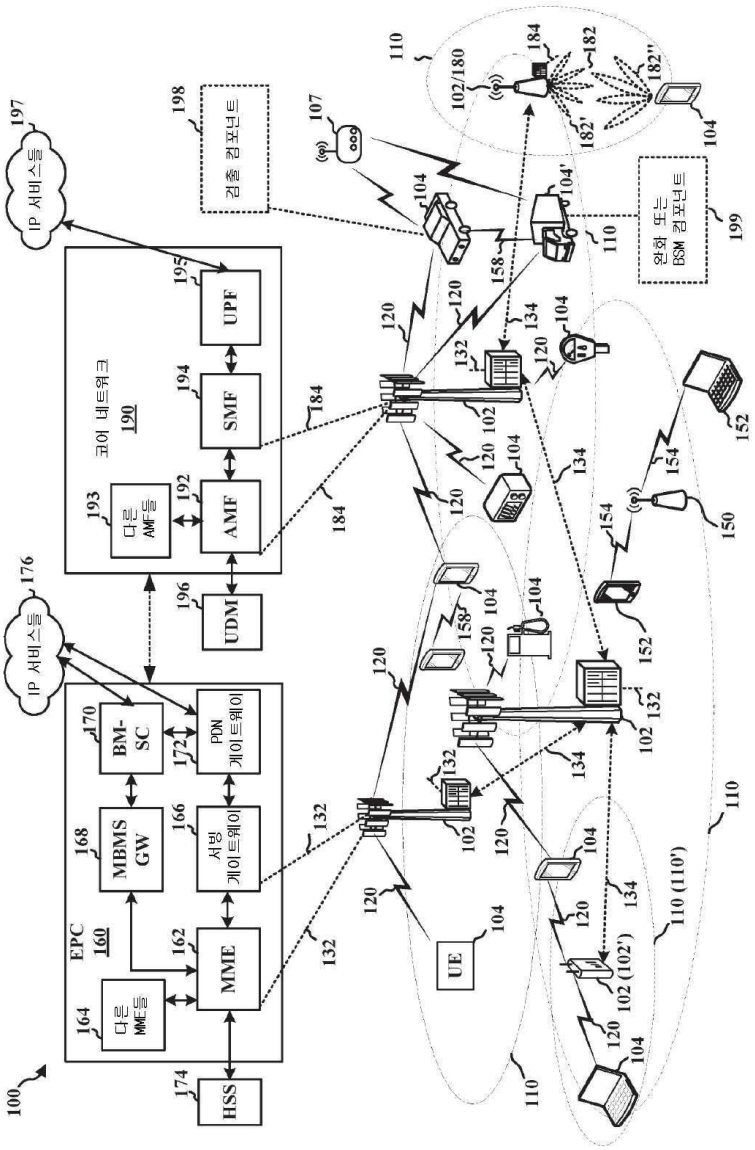
[0259] [0286] 양상 93은, 양상 78 내지 양상 91 중 어느 하나에서와 같은 방법을 구현하거나 장치를 실현하기 위한 수단을 포함하는 시스템 또는 장치이다.

[0260] [0287] 양상 94는 하나 이상의 프로세서들로 하여금 양상 78 내지 양상 91 중 어느 하나에서와 같은 방법을 구현하게 하도록 하나 이상의 프로세서들에 의해 실행가능한 명령들을 저장하는 비일시적 컴퓨터 판독가능 저장 매체이다.

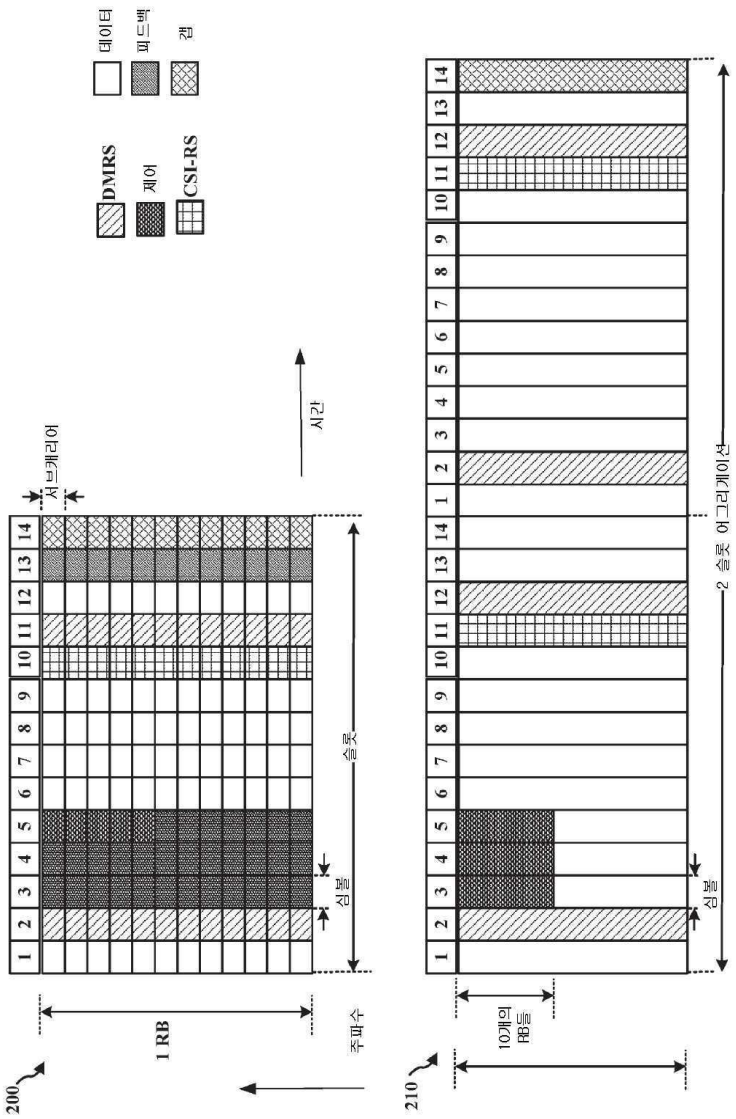
[0261] [0288] 상기의 설명은 임의의 당업자가 본원에 설명된 다양한 양상들을 실시할 수 있게 하도록 제공된다. 이러한 양상들에 대한 다양한 변형들이 당업자들에게 쉽게 명백할 것이며, 본 명세서에 정의된 일반적 원리들은 다른 양상들에 적용될 수 있다. 따라서, 청구항들은 본원에 나타난 양상들로 제한되는 것으로 의도되는 것이 아니라 청구항 문언과 일치하는 전체 범위에 따르며, 단수형 엘리먼트에 대한 참조는, "하나 및 오직 하나"로 구체적으로 언급되지 않는 한 그렇게 의도되는 것이 아니라 "하나 이상"으로 의도된다. "예시적인"이라는 단어는, "예, 예증 또는 예시로서 기능하는" 것을 의미하도록 본 명세서에서 사용된다. 본 명세서에서 "예시적인" 것으로 설명되는 임의의 양상은 반드시 다른 양상들에 비해 선호되거나 유리한 것으로 해석될 필요는 없다. 구체적으로 달리 언급되지 않으면, 용어 "일부"는 하나 이상을 나타낸다. "A, B 또는 C 중 적어도 하나", "A, B 또는 C 중 하나 이상", "A, B 및 C 중 적어도 하나", "A, B 및 C 중 하나 이상" 및 "A, B, C 또는 이들의 임의의 조합"과 같은 조합들은 A, B 및/또는 C의 임의의 조합을 포함하고, 다수의 A, 다수의 B 또는 다수의 C를 포함할 수 있다. 구체적으로, "A, B 또는 C 중 적어도 하나", "A, B 또는 C 중 하나 이상", "A, B 및 C 중 적어도 하나", "A, B 및 C 중 하나 이상" 및 "A, B, C 또는 이들의 임의의 조합"과 같은 조합들은 오직 A, 오직 B, 오직 C, A 및 B, A 및 C, B 및 C 또는 A 및 B 및 C일 수 있고, 임의의 이러한 조합들은 A, B 또는 C의 하나 이상의 멤버 또는 멤버들을 포함할 수 있다. 본 기술분야의 통상의 기술자들에게 공지되거나 추후 공지될 본 개시 전반에 걸쳐 설명되는 다양한 양상들의 엘리먼트들에 대한 모든 구조적 및 기능적 균등물들은 본원에 참조로 명백하게 통합되어 있고 청구항들에 의해 포함되는 것으로 의도된다. 또한, 본원에 개시된 어떠한 것도, 이러한 개시가 청구항들에 명시적으로 인용되었는지 여부와 무관하게 대중에게 제공되도록 의도되지 않는다. 용어들 "모듈", "메커니즘", "엘리먼트", "디바이스" 등은 용어 "수단"에 대한 대용물이 아닐 수 있다. 따라서, 엘리먼트가 "수단"이라는 어구를 사용하여 명시적으로 인용되지 않으면, 어떠한 청구항 엘리먼트도 수단 플러스 기능으로 해석되어서는 안된다.

도면

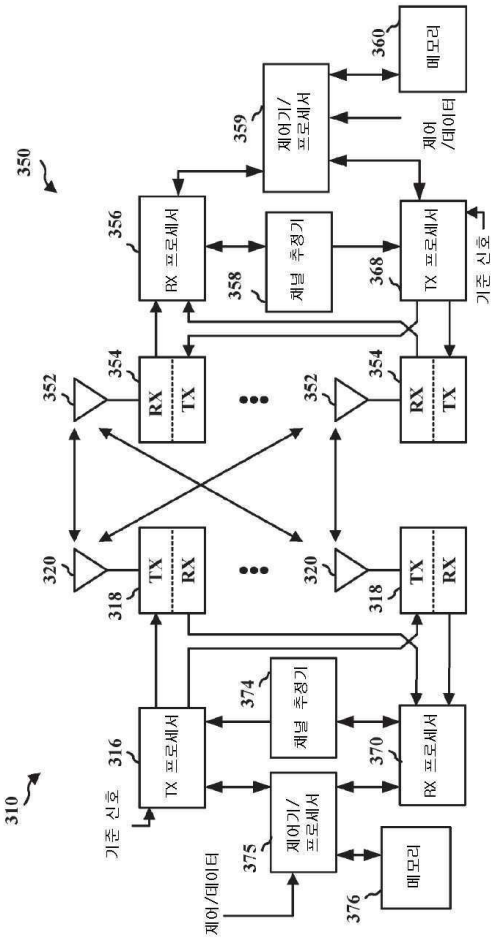
도면1


IP 서비스들
197
검출 컴포넌트
198
코어 네트워크
190
UPF
195
SMF
194
AMF
192
다른 AMF들
193
UDM
196
IP 서비스들
176
BM-SC
170
PDN 게이트웨이
172
MBMS GW
168
서빙 게이트웨이
166
MME
162
다른 MME들
164
EPC
160
HSS
174
100
110
102/180
184
182
182'
104
107
158
104'
110
위치 또는 BSM 컴포넌트
199
120
132
134
102
152
154
150
UE
110 (110')
102 (102')

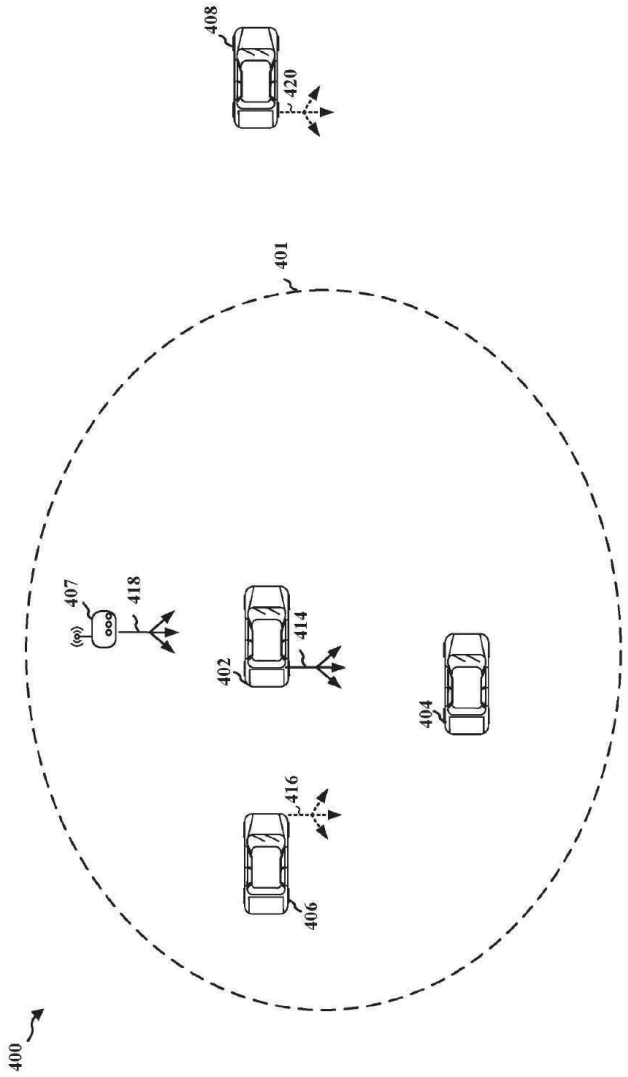
도면2


데이터
피드백
갭
DMRS
제어
CSI-RS
서브캐리어
시간
슬롯
심볼
1 RB
주파수
200
2 슬롯 어그리게이션
10개의 RBs들
210

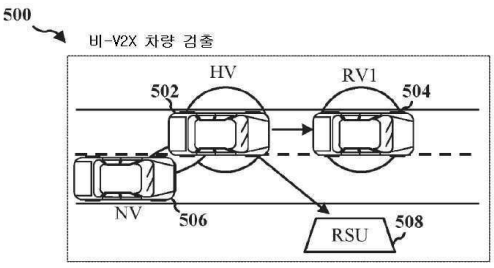
도면3


350
310
356
RX 프로세서
358
채널 추정기
359
제어기/프로세서
360
메모리
368
TX 프로세서
기준 신호
제어/데이터
352
354
RX
TX
320
318
TX
RX
316
TX 프로세서
374
채널 추정기
375
제어기/프로세서
376
메모리
370
RX 프로세서
기준 신호
제어/데이터

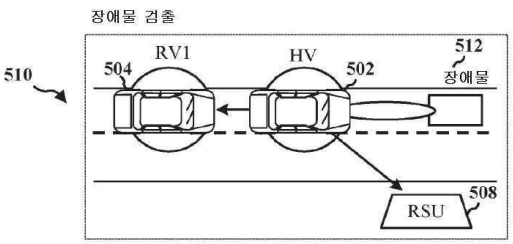
도면4



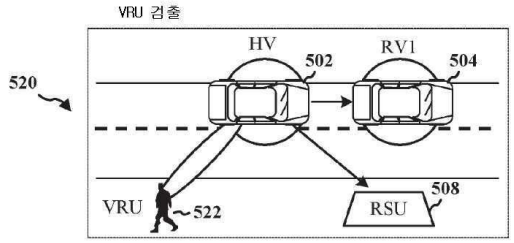
도면5a



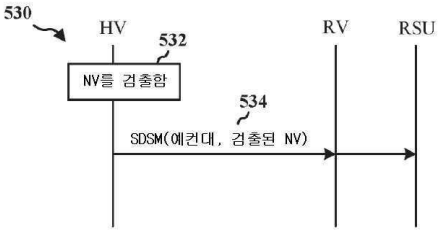
도면5b



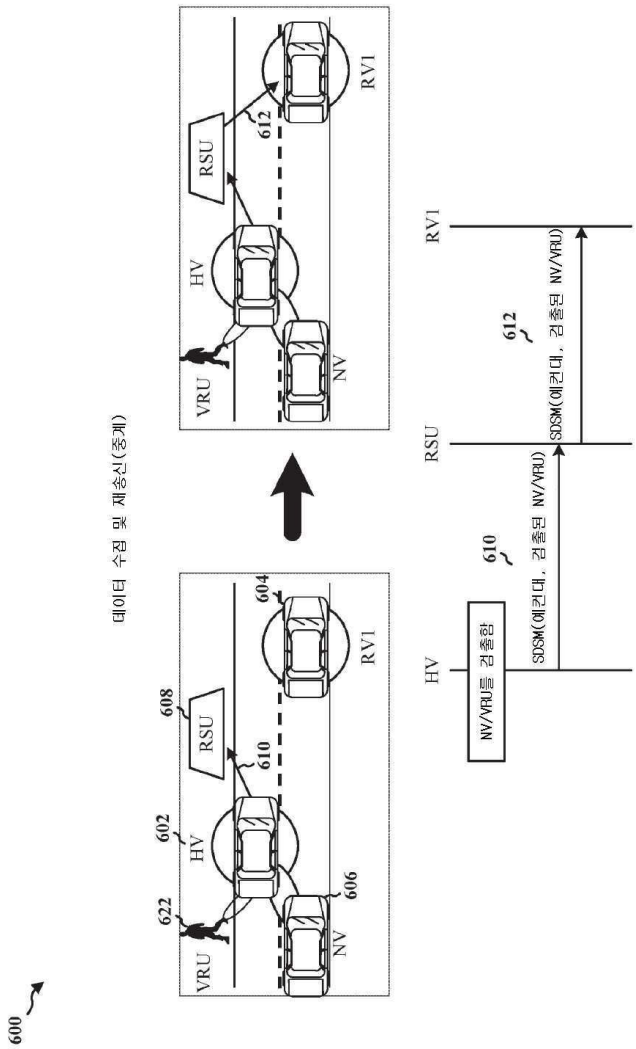
도면5c



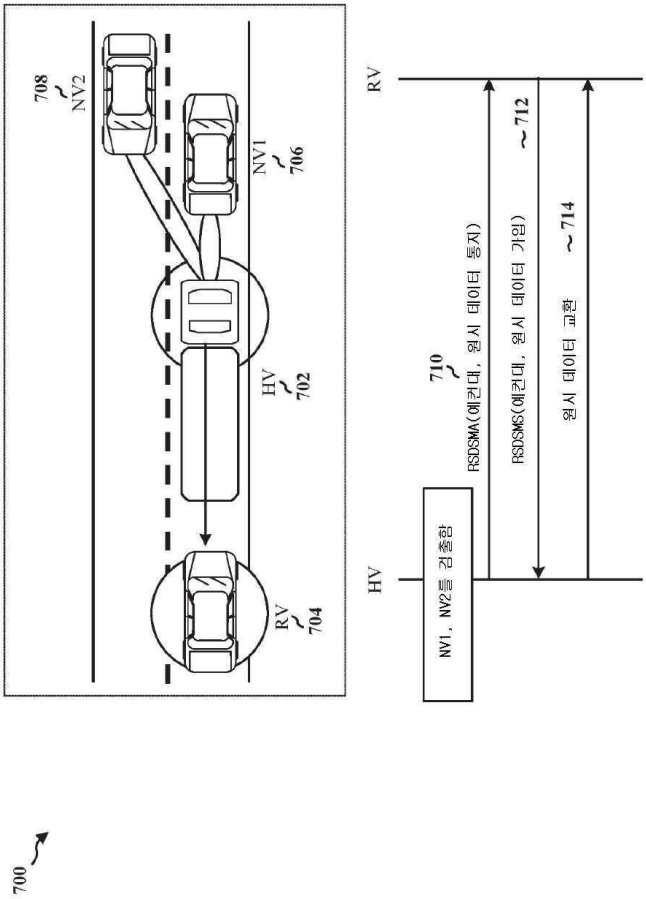
도면5d



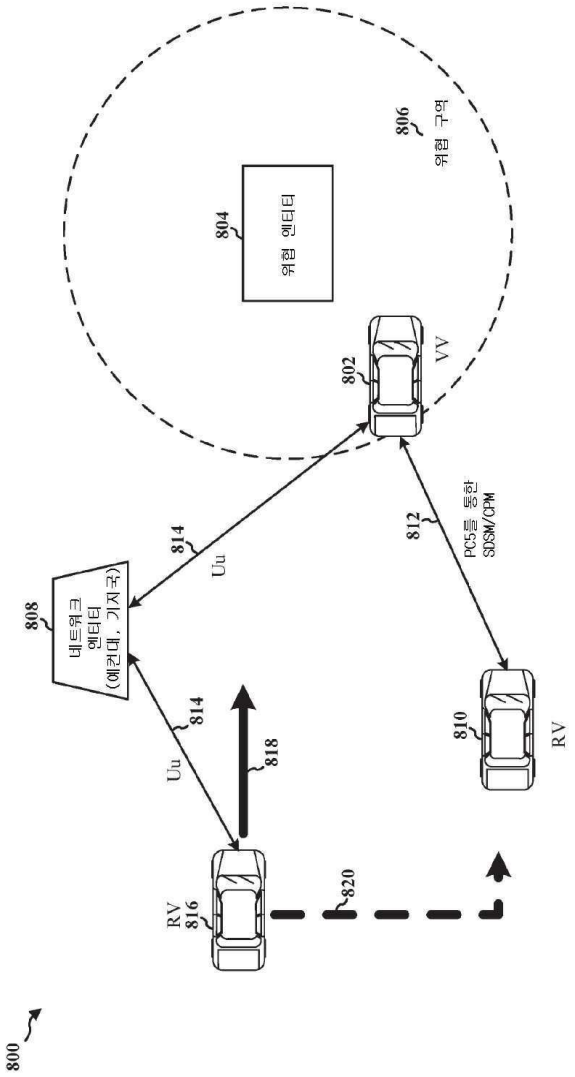
도면6



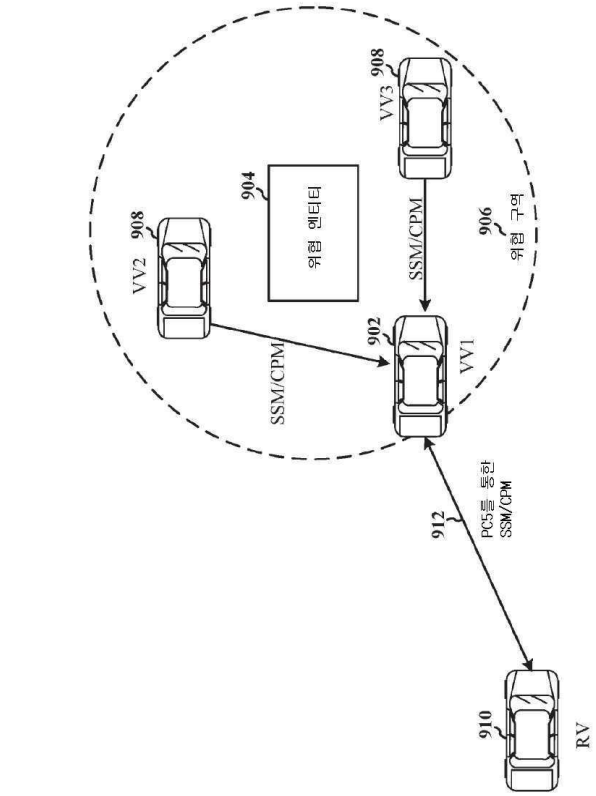
도면7


700
708
NV2
NV1
706
HV
702
RV
704
RV
HV
710
RSDSMA(에러대, 원시 데이터 통지)
RSDSMS(에러대, 원시 데이터 가입)
712
원시 데이터 교환
714
NV1, NV2를 검출함

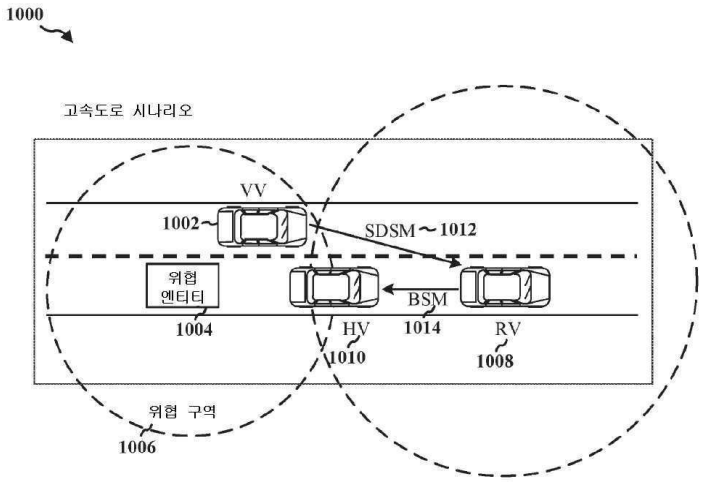
도면8


800
806
위험 구역
804
위험 엔터티
802
VV
812
PC5를 통한
SDSM/CPM
814
Uu
808
네트워크
엔터티
(예컨대, 기지국)
814
Uu
818
810
RV
RV
816
820

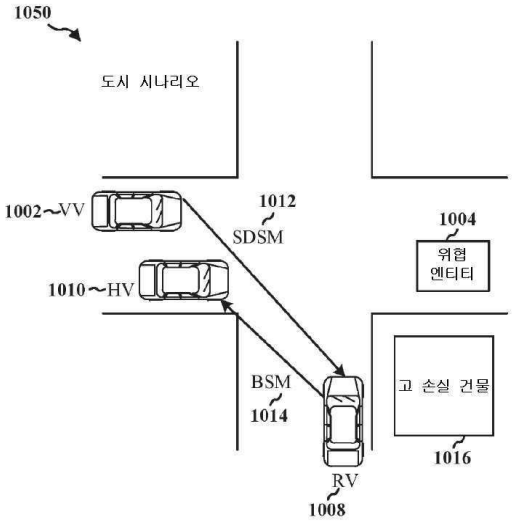
도면9


908
VV3
904
위협 엔티티
906
위협 구역
908
VV2
SSM/CPM
902
VV1
SSM/CPM
912
PC5를 통한
SSM/CPM
910
RV
900

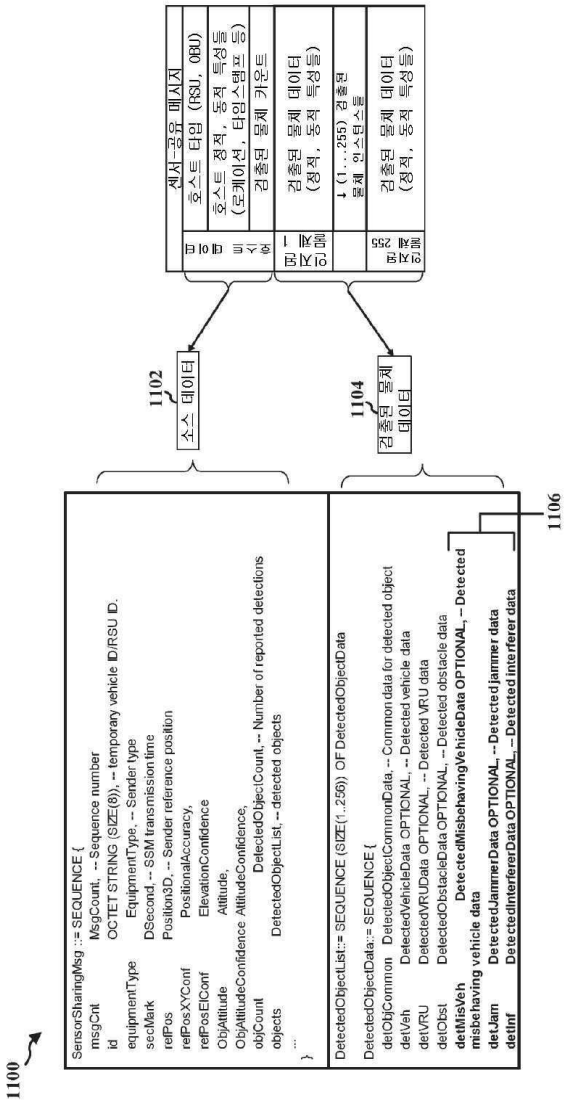
도면10a


1000
고속도로 시나리오
VV
1002
SDSM
1012
위협
엔티티
1004
BSM
1014
HV
1010
RV
1008
위협 구역
1006

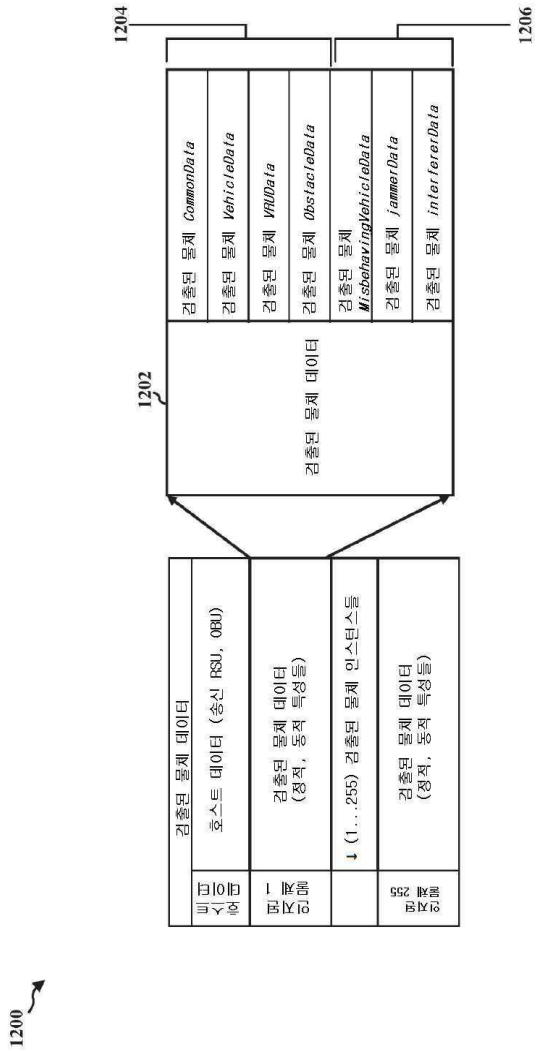
도면10b


1050
도시 시나리오
1002~VV
1012
SDSM
1004
위협
엔티티
1010~HV
BSM
1014
고 손실 건물
1016
RV
1008

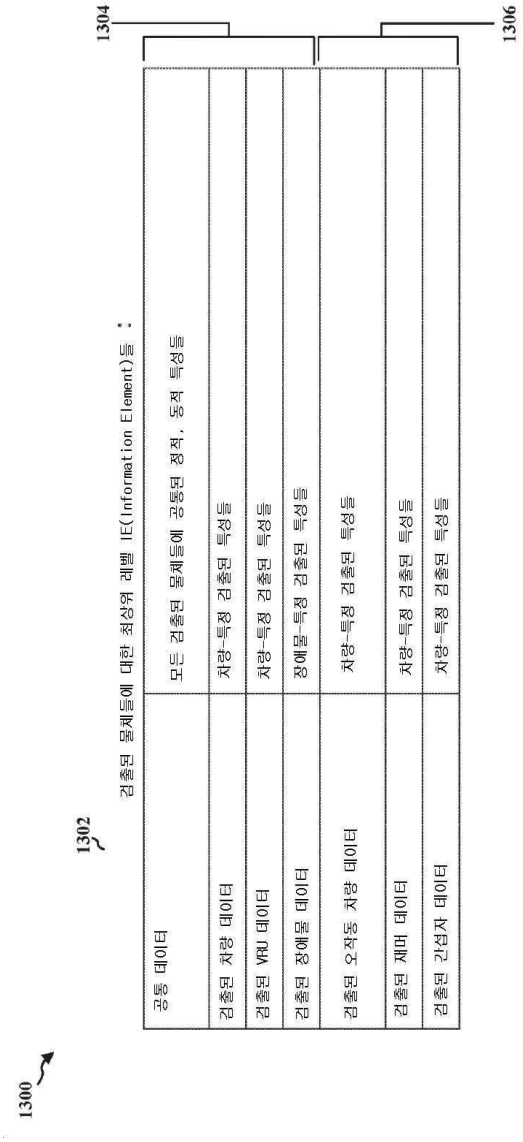
도면11


1100
SensorSharingMsg ::= SEQUENCE {
msgCnt MsgCount, -- Sequence number
id OCTET STRING (SIZE(8)), -- temporary vehicle ID/RSU ID.
equipmentType EquipmentType, -- Sender type
secMark DSecond, -- SSM transmission time
refPos Position3D, -- Sender reference position
refPosXYConf PositionalAccuracy,
refPosElConf ElevationConfidence
ObjAttitude Attitude,
ObjAttitudeConfidence AttitudeConfidence,
objCount DetectedObjectCount, -- Number of reported detections
objects DetectedObjectList, -- detected objects
...
}
DetectedObjectList::= SEQUENCE (SIZE(1..256)) OF DetectedObjectData
DetectedObjectData::= SEQUENCE {
detObjCommon DetectedObjectCommonData, -- Common data for detected object
detVeh DetectedVehicleData OPTIONAL, -- Detected vehicle data
detVRU DetectedVRUData OPTIONAL, -- Detected VRU data
detObst DetectedObstacleData OPTIONAL, -- Detected obstacle data
detMisVeh DetectedMisbehavingVehicleData OPTIONAL, -- Detected misbehaving vehicle data
detJam DetectedJammerData OPTIONAL, -- Detected jammer data
detIntf DetectedInterferer Data OPTIONAL, -- Detected interferer data
1102
소스 데이터
1104
검출된 물체 데이터
1106
센서 공유 메시지
헤더
소스 타입 (RSU, OBU)
호스트 정적, 동적 특성들 (로케이션, 타임스탬프 등)
검출된 물체 카운트
메시지 페이로드
검출된 물체 데이터 (정적, 동적 특성들)
1 (1...255) 검출된 물체 인스턴스들
검출된 물체 데이터 (정적, 동적 특성들)

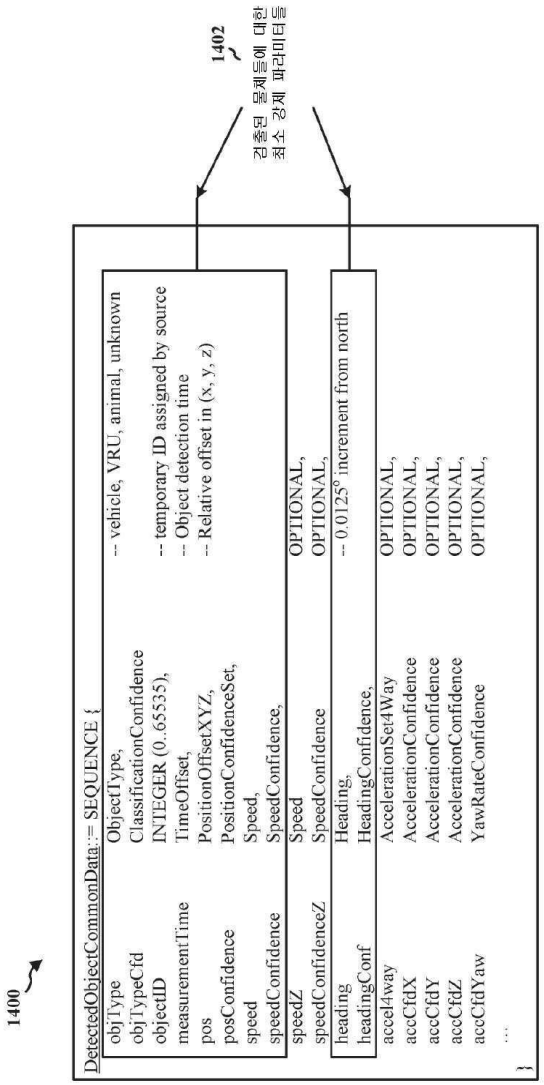
도면12


1200
검출된 물체 데이터
호스트 데이터 (송신 RSU, OBU)
검출된 물체 데이터 (정적, 동적 특성들)
↓ (1...255) 검출된 물체 인스턴스들
검출된 물체 데이터 (정적, 동적 특성들)
인지된 물체 1
인지된 물체 255
1202
검출된 물체 데이터
1204
검출된 물체 CommonData
검출된 물체 VehicleData
검출된 물체 VRUData
검출된 물체 ObstacleData
1206
검출된 물체 MisbehavingVehicleData
검출된 물체 jammerData
검출된 물체 intererData

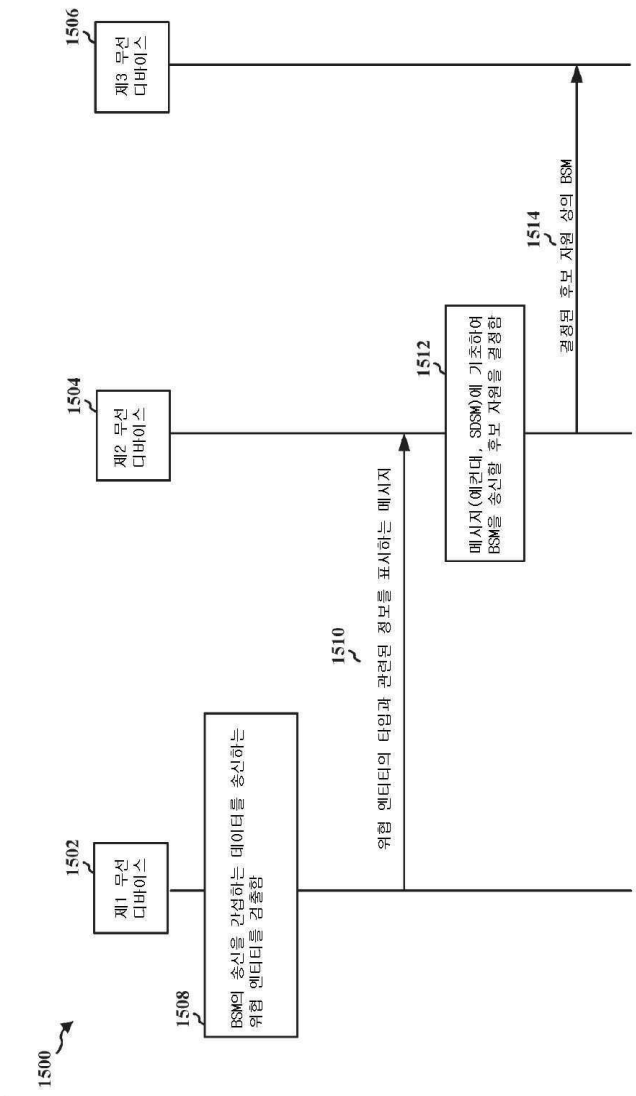
도면13


1300
1302
검출된 물체들에 대한 최상위 레벨 IE(Information Element)들 :
1304
1306
공통 데이터
모든 검출된 물체들에 공통된 정적, 동적 특성들
검출된 차량 데이터
차량-특정 검출된 특성들
검출된 VRU 데이터
차량-특정 검출된 특성들
검출된 장애물 데이터
장애물-특정 검출된 특성들
검출된 오작동 차량 데이터
차량-특정 검출된 특성들
검출된 제머 데이터
차량-특정 검출된 특성들
검출된 긴섬자 데이터
차량-특정 검출된 특성들

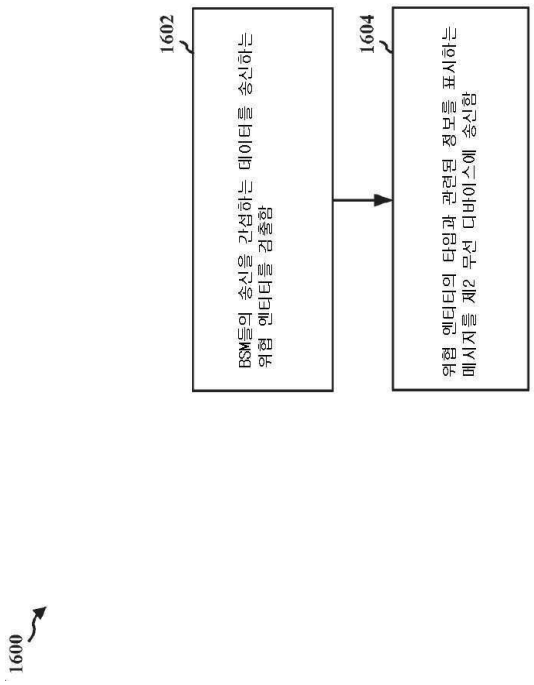
도면14


1400
1402
검출된 물체들에 대한 최소 강제 파라미터들
DetectedObjectCommonData ::= SEQUENCE {
objType ObjectType, -- vehicle, VRU, animal, unknown
objTypeCfd ClassificationConfidence
objectID INTEGER (0..65535), -- temporary ID assigned by source
measurementTime TimeOffset, -- Object detection time
pos PositionOffsetXYZ, -- Relative offset in (x, y, z)
posConfidence PositionConfidenceSet,
speed Speed,
speedConfidence SpeedConfidence,
speedZ Speed OPTIONAL,
speedConfidenceZ SpeedConfidence OPTIONAL,
heading Heading, -- 0.0125° increment from north
headingConf HeadingConfidence,
accel4way AccelerationSet4Way OPTIONAL,
accCfdX AccelerationConfidence OPTIONAL,
accCfdY AccelerationConfidence OPTIONAL,
accCfdZ AccelerationConfidence OPTIONAL,
accCfdYaw YawRateConfidence OPTIONAL,
...
}

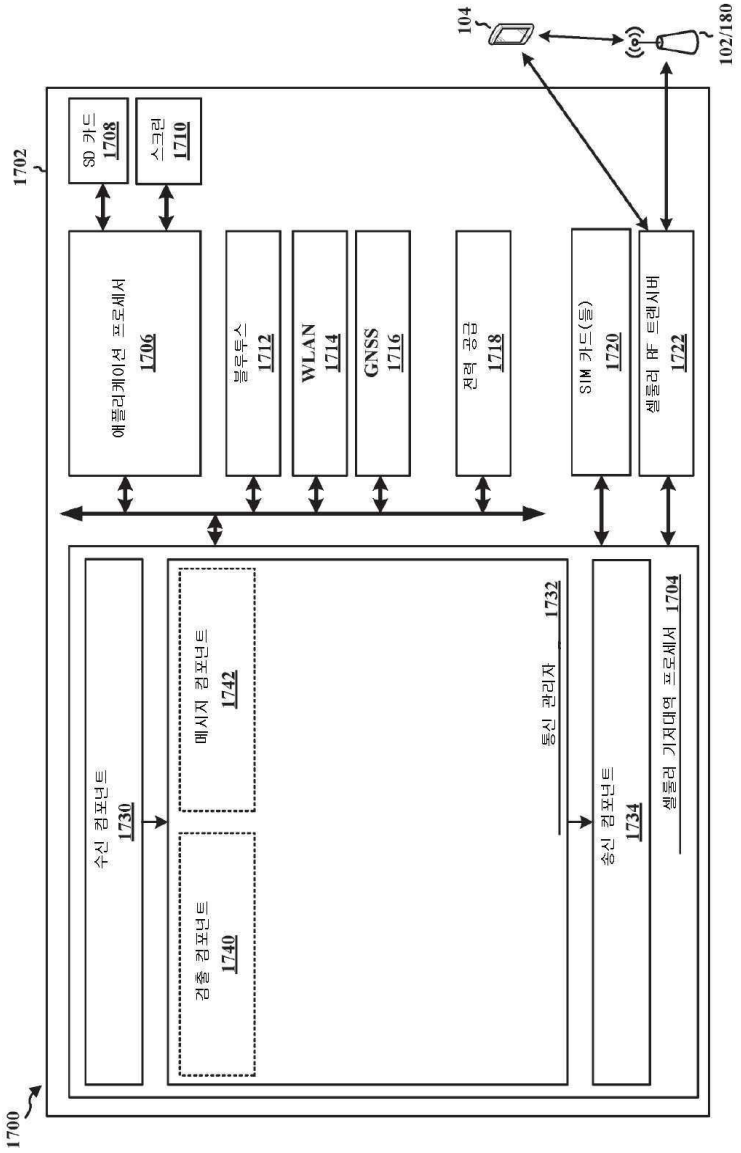
도면15


1500
1502
제1 무선 디바이스
1504
제2 무선 디바이스
1506
제3 무선 디바이스
1508
BSM의 송신을 감삽하는 데이터를 송신하는 위협 엔티티를 검출함
1510
위협 엔티티의 타입과 관련된 정보를 표시하는 메시지
1512
메시지(예컨대, SDSM)에 기초하여 BSM을 송신할 후보 자원을 결정함
1514
결정된 후보 자원 상의 BSM

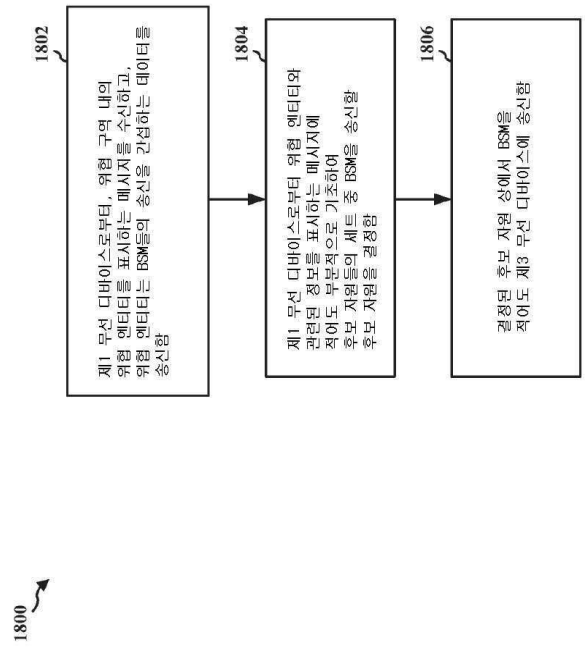
도면16


1600
1602
BSM들의 송신을 간섭하는 데이터를 송신하는
워험 엔티티를 검출함
1604
워험 엔티티의 타임과 관련된 정보를 표시하는
메시지를 제2 무선 디바이스에 송신함

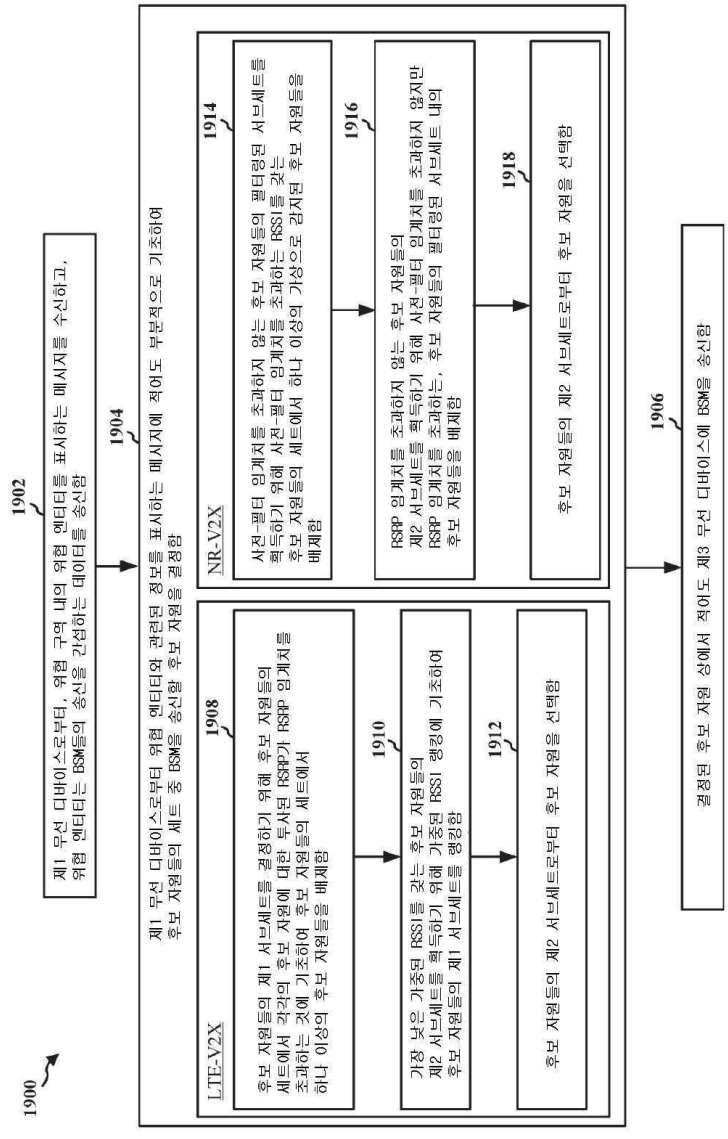
도면17


104
102/180
1702
SD 카드 1708
스크린 1710
애플리케이션 프로세서 1706
블루투스 1712
WLAN 1714
GNSS 1716
전력 공급 1718
SIM 카드(들) 1720
셀룰러 RF 트랜시버 1722
수신 컴포넌트 1730
메시지 컴포넌트 1742
검출 컴포넌트 1740
통신 관리자 1732
송신 컴포넌트 1734
셀룰러 기저대역 프로세서 1704
1700

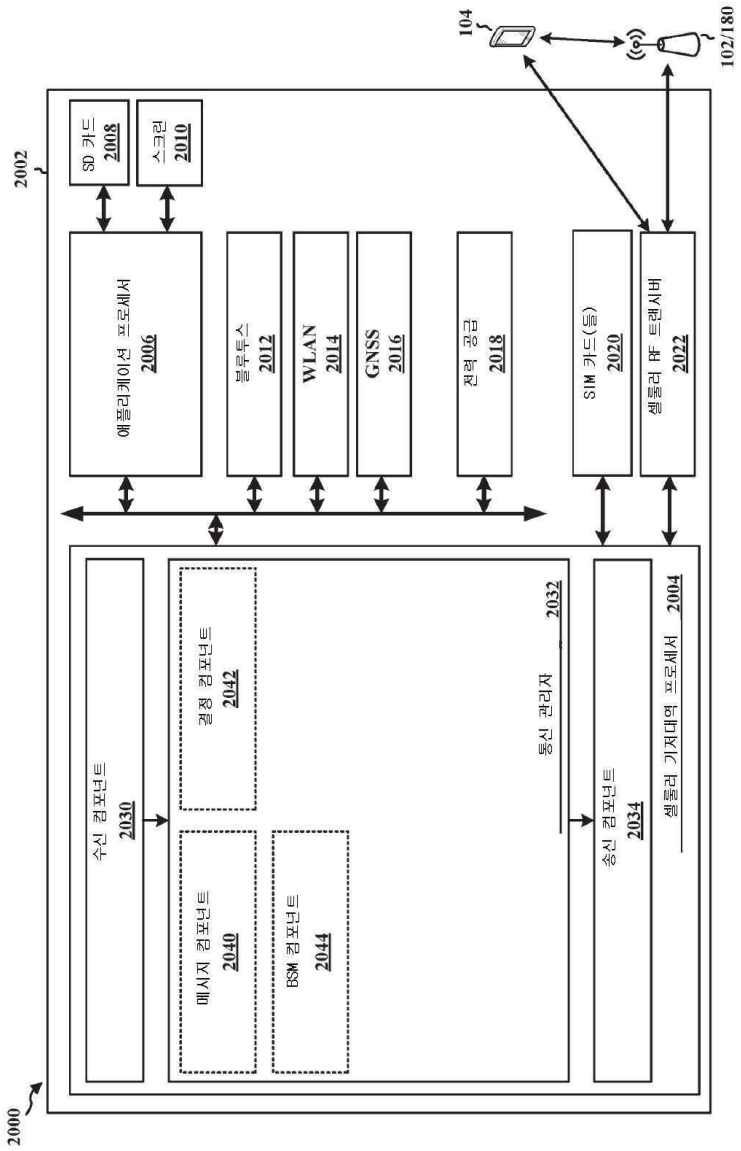
도면18


1800
1802
제1 무선 디바이스로부터, 위험 구역 내의 위협 엔티티를 표시하는 메시지를 수신하고, 위협 엔티티는 BSM들의 송신을 간섭하는 데이터를 송신함
1804
제1 무선 디바이스로부터 위협 엔티티와 관련된 정보를 표시하는 메시지에 적어도 부분적으로 기초하여 후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정함
1806
결정된 후보 자원 상에서 BSM을 적어도 제3 무선 디바이스에 송신함

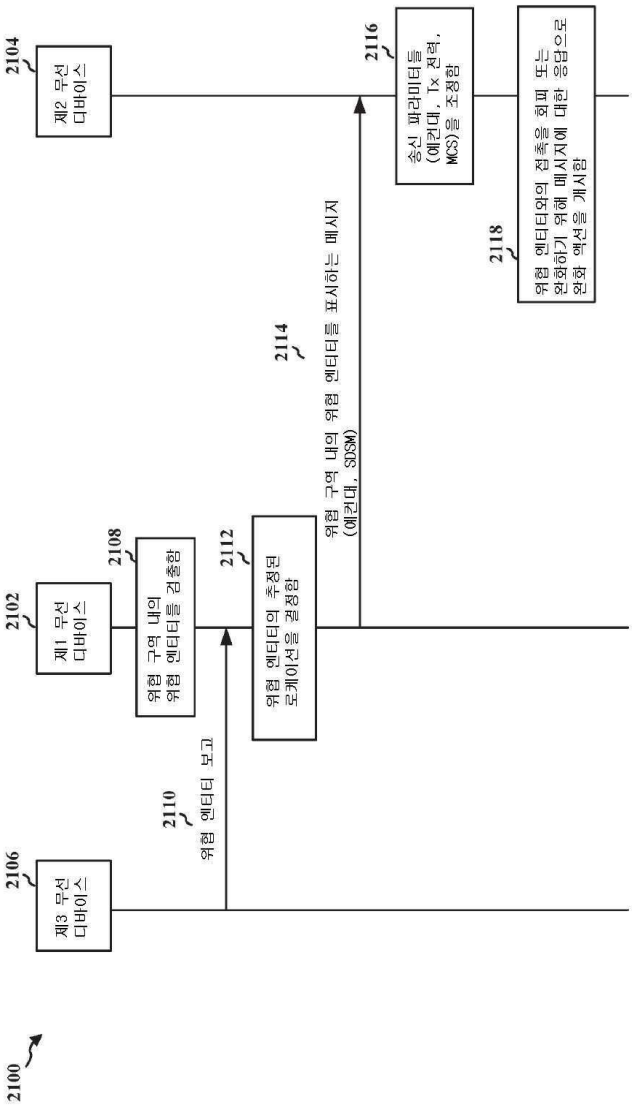
도면19


1900
1902
제1 무선 디바이스로부터, 위협 구역 내의 위협 엔티티를 표시하는 메시지를 수신하고,
위협 엔티티는 BSM들의 송신을 간섭하는 데이터를 송신함
1904
제1 무선 디바이스로부터 위협 엔티티와 관련된 정보를 표시하는 메시지에 적어도 부분적으로 기초하여
후보 자원들의 세트 중 BSM을 송신할 후보 자원을 결정함
LTE-V2X
1908
후보 자원들의 제1 서브세트를 결정하기 위해 후보 자원들의
세트에서 각각의 후보 자원에 대한 투사된 RSPP가 RSPP 임계치를
초과하는 것에 기초하여 후보 자원들의 세트에서
하나 이상의 후보 자원들을 배제함
1910
가장 낮은 가중된 RSSI를 갖는 후보 자원들의
제2 서브세트를 획득하기 위해 가중된 RSSI 랭킹에 기초하여
후보 자원들의 제1 서브세트를 랭킹함
1912
후보 자원들의 제2 서브세트로부터 후보 자원을 선택함
NR-V2X
1914
사전-필터 임계치를 초과하지 않는 후보 자원들의 필터링된 서브세트를
획득하기 위해 사전-필터 임계치를 초과하는 RSSI를 갖는
후보 자원들의 세트에서 하나 이상의 가상으로 감지된 후보 자원들을
배제함
1916
RSPP 임계치를 초과하지 않는 후보 자원들의
제2 서브세트를 획득하기 위해 사전-필터 임계치를 초과하지 않지만
RSPP 임계치를 초과하는, 후보 자원들의 필터링된 서브세트 내의
후보 자원들을 배제함
1918
후보 자원들의 제2 서브세트로부터 후보 자원을 선택함
1906
결정된 후보 자원 상에서 적어도 제3 무선 디바이스에 BSM을 송신함

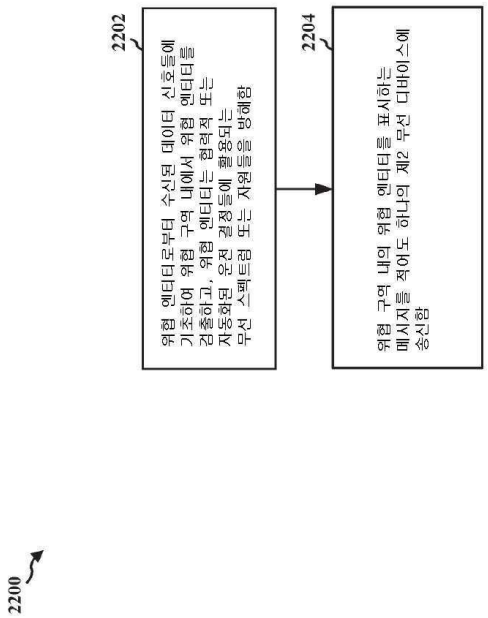
도면20


104
102/180
2002
SD 카드 2008
스크린 2010
애플리케이션 프로세서 2006
블루투스 2012
WLAN 2014
GNSS 2016
전력 공급 2018
SIM 카드(들) 2020
셀룰러 RF 트랜시버 2022
수신 컴포넌트 2030
결정 컴포넌트 2042
메시지 컴포넌트 2040
BSM 컴포넌트 2044
통신 관리자 2032
송신 컴포넌트 2034
셀룰러 기저대역 프로세서 2004
2000

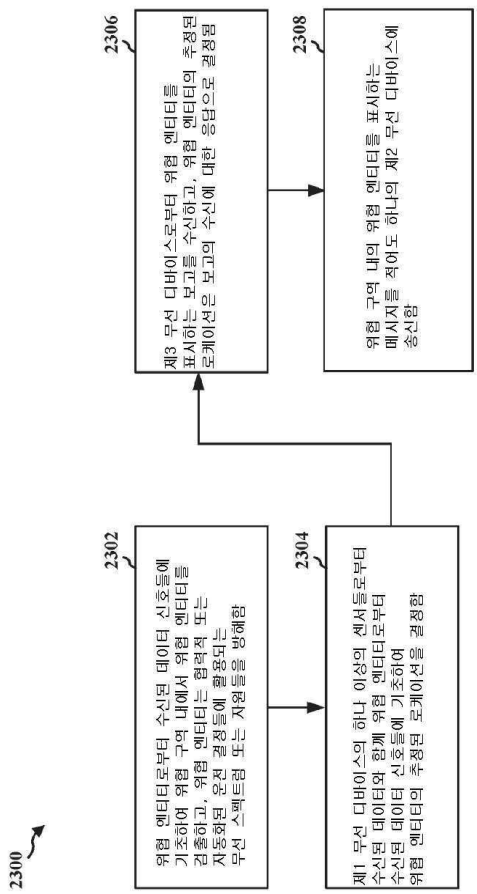
도면21


2100
제3 무선 디바이스
2106
제1 무선 디바이스
2102
제2 무선 디바이스
2104
2110
위험 엔티티 보고
위험 구역 내의 위험 엔티티를 검출함
2108
위험 엔티티의 추정된 로케이션을 결정함
2112
2114
위험 구역 내의 위험 엔티티를 표시하는 메시지 (예컨대, SDSM)
송신 파라미터들 (예컨대, Tx 전력, MCS)을 조정함
2116
위험 엔티티와의 접촉을 회피 또는 완화하기 위해 메시지에 대한 응답으로 완화 액션을 개시함
2118

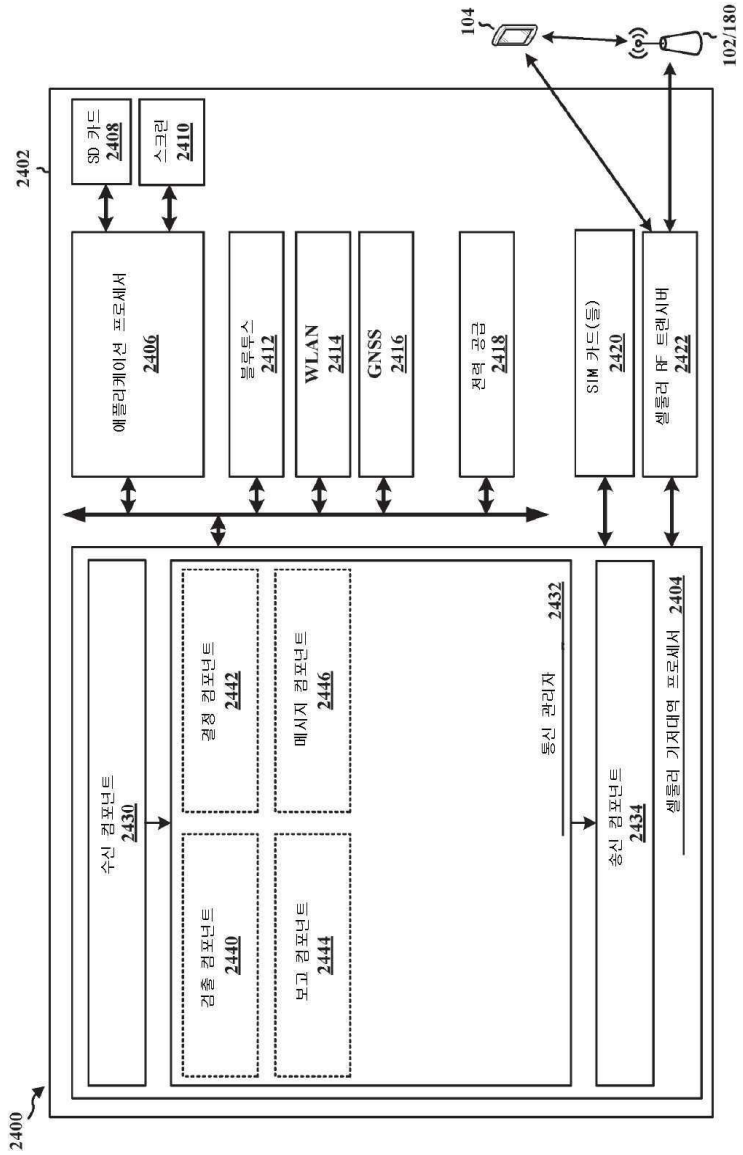
도면22


2200
2202
위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 구역 내에서 위협 엔티티를 검출하고, 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해함
2204
위협 구역 내의 위협 엔티티를 표시하는 메시지를 적어도 하나의 제2 무선 디바이스에 송신함

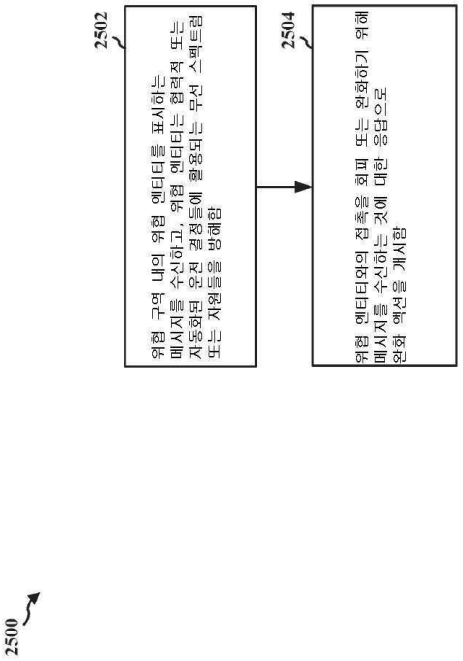
도면23


2300
2302
위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 구역 내에서 위협 엔티티를 검출하고, 위협 엔티티는 협력적 또는 자동화된 운전 결정들에 활용되는 무선 스펙트럼 또는 자원들을 방해함
2304
제1 무선 디바이스의 하나 이상의 센서들로부터 수신된 데이터와 함께 위협 엔티티로부터 수신된 데이터 신호들에 기초하여 위협 엔티티의 추정된 로케이션을 결정함
2306
제3 무선 디바이스로부터 위협 엔티티를 표시하는 보고를 수신하고, 위협 엔티티의 추정된 로케이션은 보고의 수신에 대한 응답으로 결정됨
2308
위협 구역 내의 위협 엔티티를 표시하는 메시지를 적어도 하나의 제2 무선 디바이스에 송신함

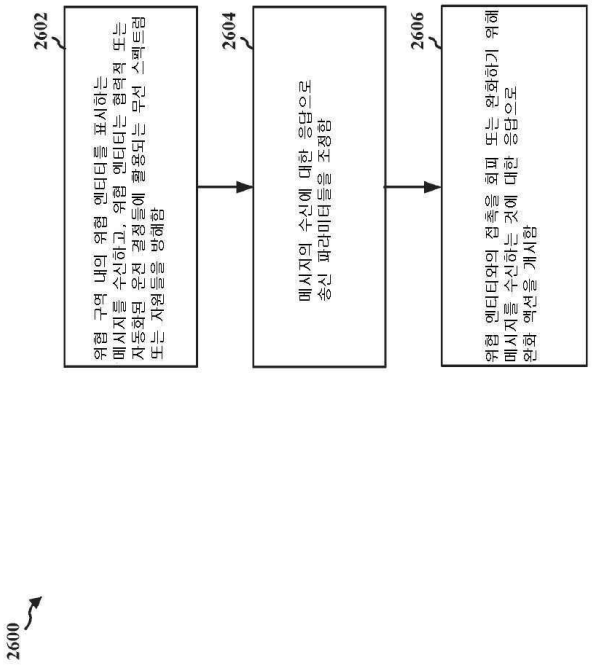
도면24


104
102/180
2402
SD 카드 2408
스크린 2410
애플리케이션 프로세서 2406
블루투스 2412
WLAN 2414
GNSS 2416
전력 공급 2418
SIM 카드(들) 2420
셀룰러 RF 트랜시버 2422
수신 컴포넌트 2430
결정 컴포넌트 2442
메시지 컴포넌트 2446
검출 컴포넌트 2440
보고 컴포넌트 2444
통신 관리자 2432
송신 컴포넌트 2434
셀룰러 기저대역 프로세서 2404
2400

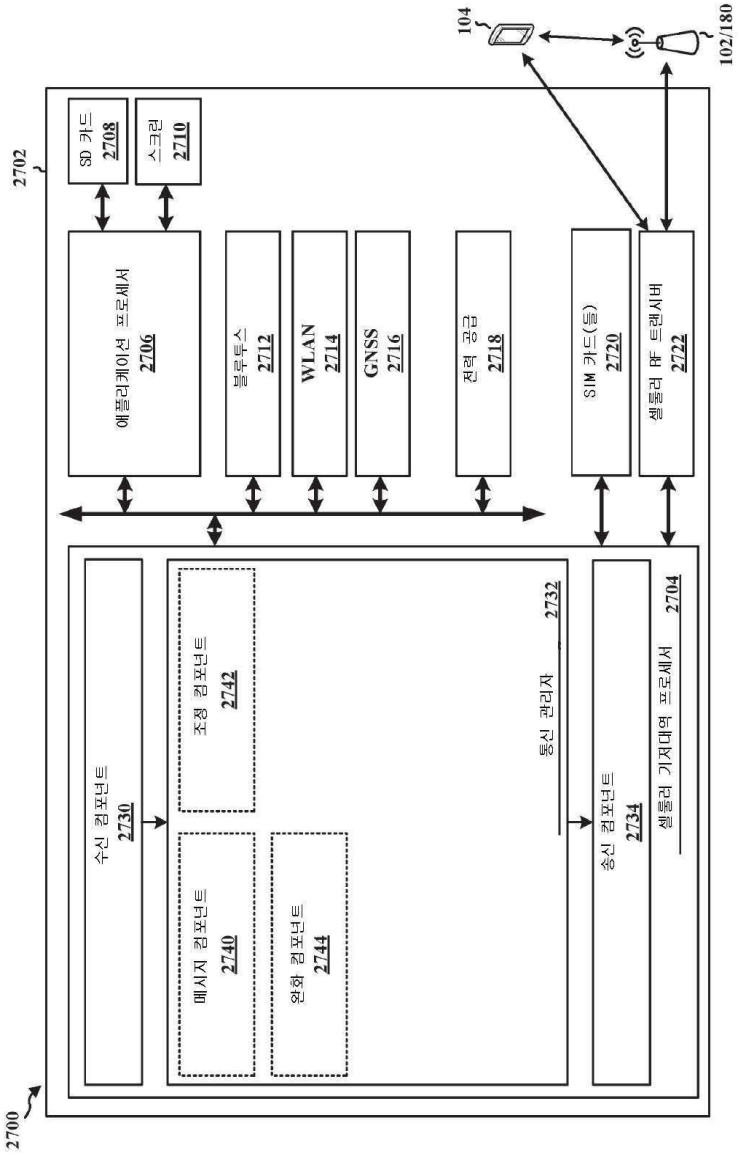
도면25


2500
2502
위협 구역 내의 위협 엔티티를 표시하는
메시지를 수신하고, 위협 엔티티는 협력적 또는
자동화된 운전 결정들에 활용되는 무선 스펙트럼
또는 자원들을 방해함
2504
위협 엔티티와의 접촉을 회피 또는 완화하기 위해
메시지를 수신하는 것에 대한 응답으로
완화 액션을 개시함

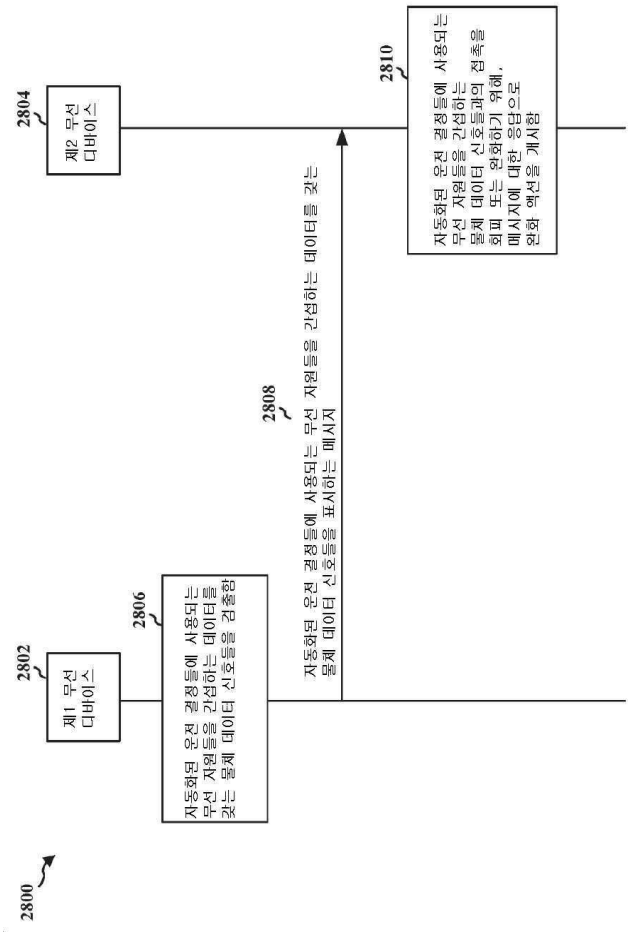
도면26


2600
2602
위협 구역 내의 위협 엔티티를 표시하는
메시지를 수신하고, 위협 엔티티는 협력적 또는
자동화된 운전 결정들에 활용되는 무선 스펙트럼
또는 자원들을 방해함
2604
메시지의 수신에 대한 응답으로
송신 파라미터들을 조정함
2606
위협 엔티티와의 접촉을 회피 또는 완화하기 위해
메시지를 수신하는 것에 대한 응답으로
완화 액션을 개시함

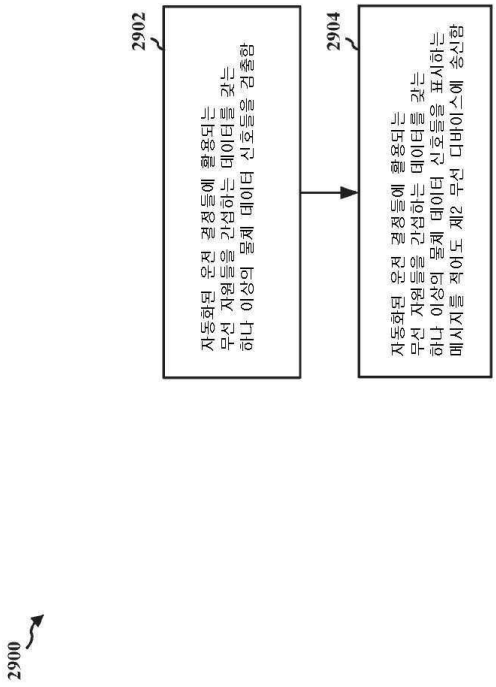
도면27


104
102/180
2702
SD 카드 2708
스크린 2710
애플리케이션 프로세서 2706
블루투스 2712
WLAN 2714
GNSS 2716
전력 공급 2718
SIM 카드(들) 2720
셀룰러 RF 트랜시버 2722
수신 컴포넌트 2730
조정 컴포넌트 2742
메시지 컴포넌트 2740
원화 컴포넌트 2744
통신 관리자 2732
송신 컴포넌트 2734
셀룰러 기저대역 프로세서 2704
2700

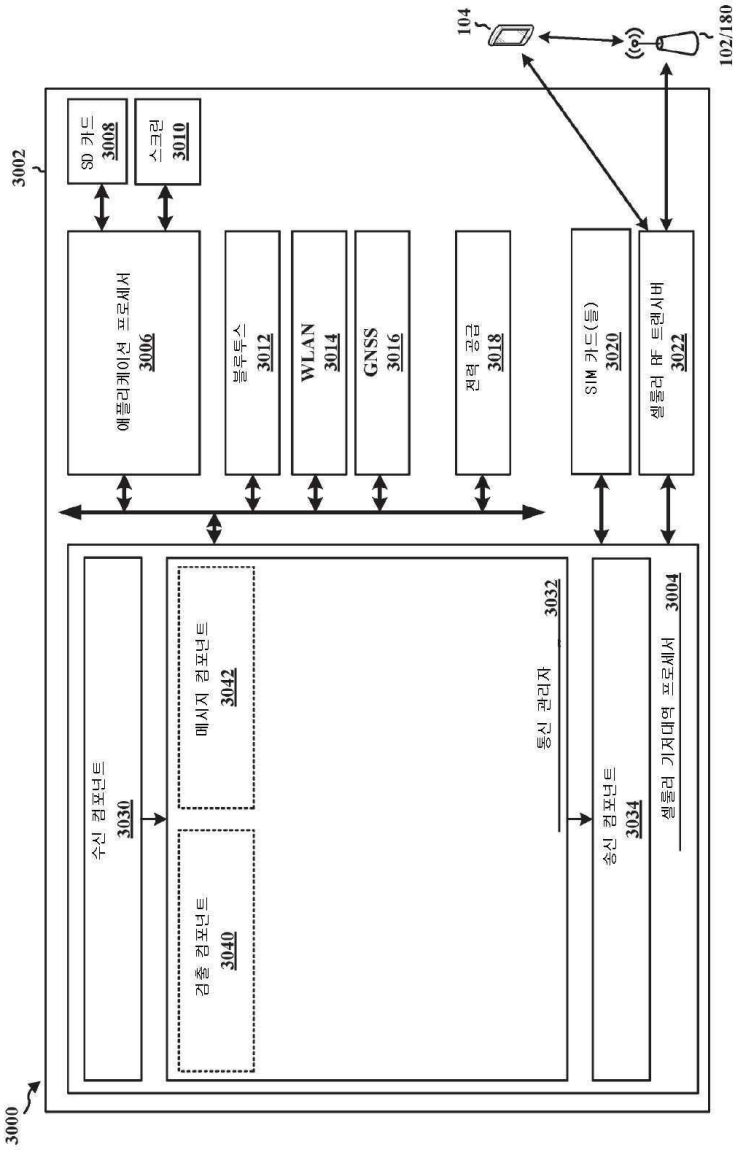
도면28


2800
2802
제1 무선 디바이스
2804
제2 무선 디바이스
2806
자동화된 운전 결정들에 사용되는 무선 자원들을 간섭하는 데이터를 갖는 물체 데이터 신호들을 검출함
2808
자동화된 운전 결정들에 사용되는 무선 자원들을 간섭하는 데이터를 갖는 물체 데이터 신호들을 표시하는 메시지
2810
자동화된 운전 결정들에 사용되는 무선 자원들을 간섭하는 물체 데이터 신호들의 접촉을 회피 또는 완화하기 위해, 메시지에 대한 응답으로 완화 액션을 개시함

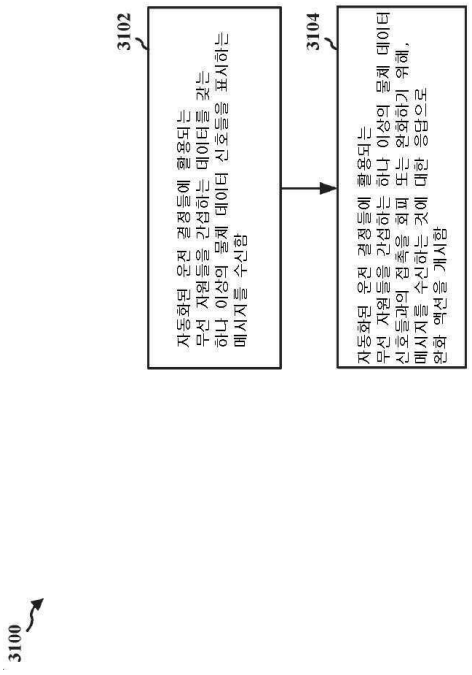
도면29


2900
2902
자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 검출함
2904
자동화된 운전 결정들에 활용되는 무선 자원들을 간섭하는 데이터를 갖는 하나 이상의 물체 데이터 신호들을 표시하는 메시지를 적어도 제2 무선 디바이스에 송신함

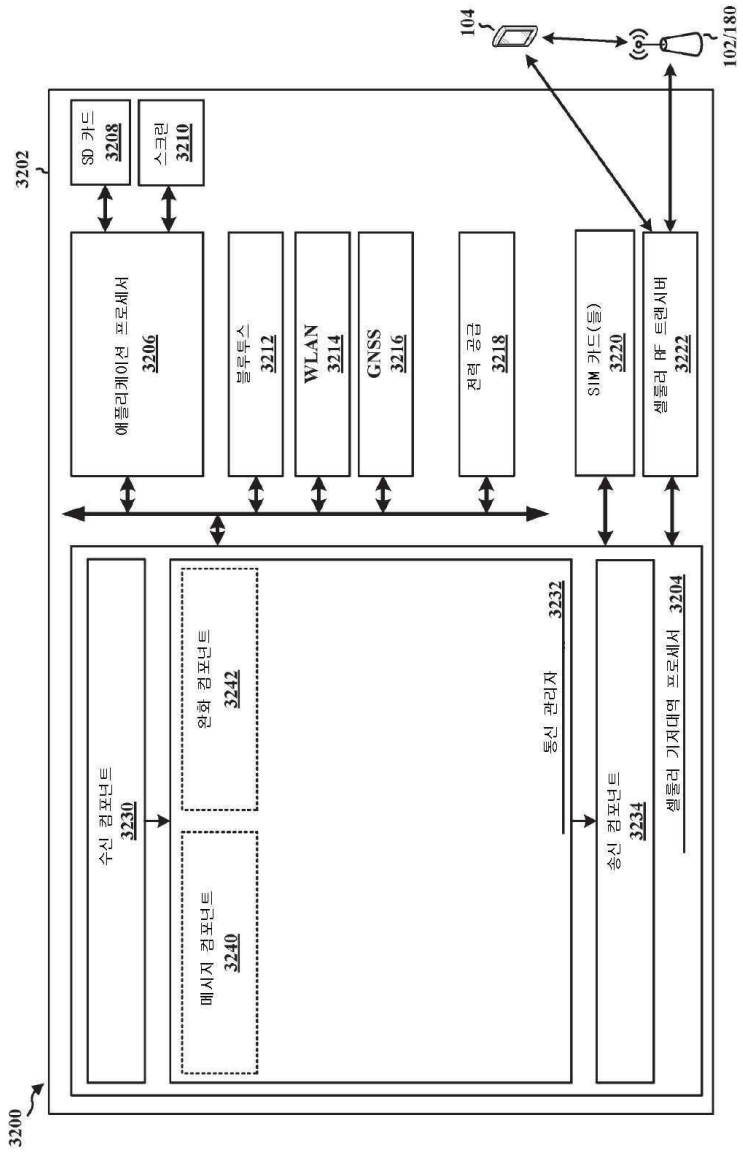
도면30


104
102/180
3002
SD 카드 3008
스크린 3010
애플리케이션 프로세서 3006
블루투스 3012
WLAN 3014
GNSS 3016
전력 공급 3018
SIM 카드(들) 3020
셀룰러 RF 트랜시버 3022
수신 컴포넌트 3030
메시지 컴포넌트 3042
검출 컴포넌트 3040
통신 관리자 3032
송신 컴포넌트 3034
셀룰러 기저대역 프로세서 3004
3000

도면31


3100
3102
자동화된 운전 결정들에 활용되는
무선 자원들을 간섭하는 데이터를 갖는
하나 이상의 물체 데이터 신호들을 표시하는
메시지를 수신함
3104
자동화된 운전 결정들에 활용되는
무선 자원들을 간섭하는 하나 이상의 물체 데이터
신호들과의 접촉을 회피 또는 완화하기 위해,
메시지를 수신하는 것에 대한 응답으로
완화 액션을 개시함

도면32


104
102/180
3202
SD 카드 3208
스크린 3210
애플리케이션 프로세서 3206
블루투스 3212
WLAN 3214
GNSS 3216
전력 공급 3218
SIM 카드(들) 3220
셀룰러 RF 트랜시버 3222
수신 컴포넌트 3230
완화 컴포넌트 3242
메시지 컴포넌트 3240
통신 관리자 3232
송신 컴포넌트 3234
셀룰러 기저대역 프로세서 3204
3200