(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0092751
(43) 공개일자 2015년08월13일

(51) 국제특허분류(Int. Cl.)
G06F 21/12 (2013.01) *G06F 21/33* (2013.01)
H04L 29/06 (2006.01) *H04W 12/06* (2009.01)
H04W 12/10 (2009.01) *H04W 12/12* (2009.01)
H04W 76/02 (2009.01)
(52) CPC특허분류
G06F 21/12 (2013.01)
G06F 21/33 (2013.01)
(21) 출원번호 10-2015-7017321
(22) 출원일자(국제) 2013년12월06일
심사청구일자 없음
(85) 번역문제출일자 2015년06월29일
(86) 국제출원번호 PCT/US2013/073522
(87) 국제공개번호 WO 2014/089403
국제공개일자 2014년06월12일
(30) 우선권주장
13/706,849 2012년12월06일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
반더빈, 미카엘라
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
파크, 빈센트 디.
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
트시르트시스, 게오르기오스
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

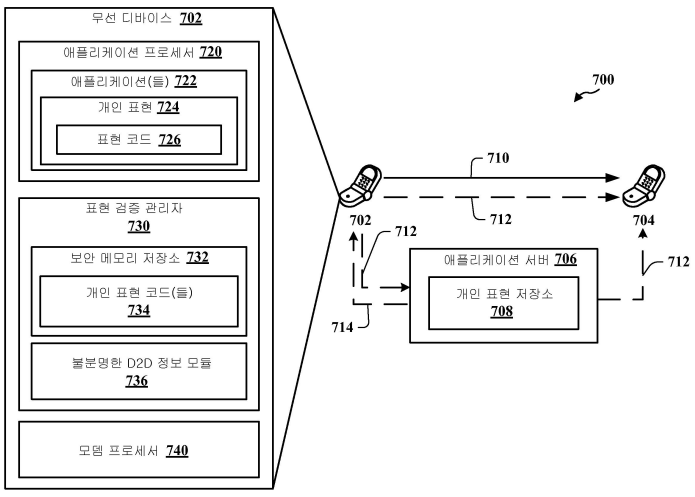
전체 청구항 수 : 총 52 항

(54) 발명의 명칭 **위장 위험들에 대비하여 개인 표현 보호를 제공하기 위한 방법들 및 장치**

(57) 요 약

무선 통신 네트워크에서의 개인 표현 보호의 제공과 관련하여 무선 통신을 위한 방법, 장치 및 컴퓨터 프로그램 물건이 제공된다. 일례로, UE는 개인 표현 및/또는 적어도, 개인 표현과 연관된 표현 코드에 대한 참조를 표명하라는 요청을 (예를 들어, UE 상에서 작동하는 애플리케이션으로부터) 내부적으로 수신하고, 표현 코드에 대한 참조 및/또는 표현 코드가 표현 코드의 저장된 인스턴스와 일치하는지 여부를 결정할 능력이 있다. 한 양상에서, UE는 표현 코드의 저장된 인스턴스가 요청과 함께 수신된 표현 코드에 대응하는 경우에 개인 표현 또는 표현 코드 중 적어도 하나를 표명할 능력이 있을 수도 있다. 다른 양상에서, UE는 저장된 표현 코드가 요청과 함께 수신된 표현 코드에 대응하지 않는 경우에 개인 표현과 연관된 임의의 정보의 표명을 금지할 능력이 있을 수도 있다.

대 표 도 - 도7



(52) CPC특허분류
H04L 63/12 (2013.01)
H04L 63/1466 (2013.01)
H04W 12/06 (2013.01)
H04W 12/10 (2013.01)
H04W 12/12 (2013.01)
H04W 76/023 (2013.01)

명 세 서

청구범위

청구항 1

통신 방법으로서,

개인 표현을 표명하라는 요청을 수신하는 단계 - 상기 요청은 적어도, 상기 개인 표현과 연관된 표현 코드에 대한 참조를 포함함 -;

적어도, 상기 표현 코드에 대한 참조가 상기 표현 코드의 이전에 획득되어 저장된 인스턴스에 대응하는지 여부를 표현 검증 관리자(EVM: expression verification manager)에 의해 결정하는 단계; 및

상기 표현 코드가 상기 표현 코드의 상기 저장된 인스턴스에 대응한다는 결정시 상기 개인 표현 또는 상기 표현 코드 중 적어도 하나를 표명하는 단계; 또는

상기 표현 코드가 상기 표현 코드의 상기 저장된 인스턴스에 대응하지 않는다는 결정시 상기 개인 표현과 연관된 정보의 표명을 금지하는 단계를 포함하는,

통신 방법.

청구항 2

제 1 항에 있어서,

상기 요청은 애플리케이션으로부터 수신되며,

상기 방법은,

상기 애플리케이션에 대한 구성 프로세스의 일부로서 상기 표현 코드의 인스턴스를 획득하는 단계; 및

상기 표현 코드의 인스턴스를 보안 메모리 저장소에 저장하는 단계를 더 포함하는,

통신 방법.

청구항 3

제 2 항에 있어서,

상기 보안 메모리 저장소는 UE와 연관된 비휘발성 메모리(NVM: non-volatile memory)인,

통신 방법.

청구항 4

제 2 항에 있어서,

상기 표현 코드와 연관된 불분명한 디바이스 투 디바이스(D2D: device to device) 정보를 전송하는 단계를 더 포함하는,

통신 방법.

청구항 5

제 4 항에 있어서,

상기 불분명한 D2D 정보는 하나 또는 그보다 많은 인가된(authorized) 디바이스들에 안전하게 전송되는,

통신 방법.

청구항 6

제 4 항에 있어서,

상기 불분명한 D2D 정보는 상기 애플리케이션과 연관된 애플리케이션 서버에 전송되는,

통신 방법.

청구항 7

제 4 항에 있어서,

상기 불분명한 D2D 정보는,

상기 개인 표현, 상기 표현 코드, 상기 애플리케이션의 명칭, 카운터, 생성 시간, 이전에 생성된 표현 코드, 만료일, 또는 표명하는 UE의 인증서 중 적어도 하나를 포함하는,

통신 방법.

청구항 8

제 4 항에 있어서,

상기 불분명한 D2D 정보의 진정성을 표시하는 디지털 서명을 생성하는 단계를 더 포함하며,

상기 불분명한 D2D 정보는 생성된 디지털 서명과 함께 전송되는,

통신 방법.

청구항 9

제 8 항에 있어서,

상기 디지털 서명은 또한,

운영자 서명 키, 임시 디바이스 식별자, 또는 생존 시간(TTL: time to live) 값 중 적어도 하나를 포함할 수 있는,

통신 방법.

청구항 10

제 1 항에 있어서,

신뢰 서버로부터 상기 표현 코드의 인스턴스를 안전하게 획득하는 단계; 및

상기 표현 코드의 인스턴스를 보안 메모리 저장소에 저장하는 단계를 더 포함하는,

통신 방법.

청구항 11

제 1 항에 있어서,

상기 EVM은 UE의 모뎀과 연관되는,

통신 방법.

청구항 12

제 1 항에 있어서,

상기 EVM은 상기 UE의 애플리케이션 인터페이스와 모뎀 인터페이스 간의 매개 계층으로서 구성되는,

통신 방법.

청구항 13

제 12 항에 있어서,

상기 EVM의 제 1 부분은 UE의 모뎀과 연관되고,

상기 EVM의 제 2 부분은 상기 UE의 애플리케이션 인터페이스와 모뎀 인터페이스 간의 매개 계층으로서 구성되는,

통신 방법.

청구항 14

무선 통신을 위한 장치로서,

개인 표현을 표명하라는 요청을 수신하기 위한 수단 - 상기 요청은 적어도, 상기 개인 표현과 연관된 표현 코드에 대한 참조를 포함함 -;

적어도, 상기 표현 코드에 대한 참조가 상기 표현 코드의 이전에 획득되어 저장된 인스턴스에 대응하는지 여부를 표현 검증 관리자(EVM)에 의해 결정하기 위한 수단; 및

상기 표현 코드가 상기 표현 코드의 상기 저장된 인스턴스에 대응한다는 결정시 상기 개인 표현 또는 상기 표현 코드 중 적어도 하나를 표명하기 위한 수단; 또는

상기 표현 코드가 상기 표현 코드의 상기 저장된 인스턴스에 대응하지 않는다는 결정시 상기 개인 표현과 연관된 정보의 표명을 금지하기 위한 수단을 포함하는,

무선 통신을 위한 장치.

청구항 15

제 14 항에 있어서,

상기 요청은 애플리케이션으로부터 수신되며,

상기 결정하기 위한 수단은,

상기 애플리케이션에 대한 구성 프로세스의 일부로서 상기 표현 코드의 인스턴스를 획득하도록 추가로 구성되고,

상기 장치는,

상기 표현 코드의 인스턴스를 보안 메모리 저장소에 저장하기 위한 수단을 더 포함하는,

무선 통신을 위한 장치.

청구항 16

제 15 항에 있어서,

상기 보안 메모리 저장소는 UE와 연관된 비휘발성 메모리(NVM)인,

무선 통신을 위한 장치.

청구항 17

제 15 항에 있어서,

상기 표명하기 위한 수단은,

상기 표현 코드와 연관된 불분명한 디바이스 투 디바이스(D2D) 정보를 전송하도록 구성되는,

무선 통신을 위한 장치.

청구항 18

제 17 항에 있어서,

상기 불분명한 D2D 정보는 하나 또는 그보다 많은 인가된 디바이스들에 안전하게 전송되는,

무선 통신을 위한 장치.

청구항 19

제 17 항에 있어서,

상기 불분명한 D2D 정보는 상기 애플리케이션과 연관된 애플리케이션 서버에 전송되는,

무선 통신을 위한 장치.

청구항 20

제 17 항에 있어서,

상기 불분명한 D2D 정보는,

상기 개인 표현, 상기 표현 코드, 상기 애플리케이션의 명칭, 카운터, 생성 시간, 이전에 생성된 표현 코드, 만료일, 또는 표명하는 UE의 인증서 중 적어도 하나를 포함하는,

무선 통신을 위한 장치.

청구항 21

제 17 항에 있어서,

상기 결정하기 위한 수단은,

상기 불분명한 D2D 정보의 진정성을 표시하는 디지털 서명을 생성하도록 추가로 구성되며,

상기 불분명한 D2D 정보는 생성된 디지털 서명과 함께 전송되는,

무선 통신을 위한 장치.

청구항 22

제 21 항에 있어서,

상기 디지털 서명은 또한,

운영자 서명 키, 임시 디바이스 식별자, 또는 생존 시간(TTL) 값 중 적어도 하나를 포함할 수 있는,

무선 통신을 위한 장치.

청구항 23

제 14 항에 있어서,

신뢰 서버로부터 상기 표현 코드의 인스턴스를 안전하게 획득하기 위한 수단; 및

상기 표현 코드의 인스턴스를 보안 메모리 저장소에 저장하기 위한 수단을 더 포함하는,

무선 통신을 위한 장치.

청구항 24

제 14 항에 있어서,

상기 EVM은 UE의 모뎀과 연관되는,

무선 통신을 위한 장치.

청구항 25

제 14 항에 있어서,

상기 EVM은 상기 UE의 애플리케이션 인터페이스와 모뎀 인터페이스 간의 매개 계층으로서 구성되는,

무선 통신을 위한 장치.

청구항 26

제 25 항에 있어서,

상기 EVM의 제 1 부분은 UE의 모뎀과 연관되고,

상기 EVM의 제 2 부분은 상기 UE의 애플리케이션 인터페이스와 모뎀 인터페이스 간의 매개 계층으로서 구성되는,

무선 통신을 위한 장치.

청구항 27

무선 통신을 위한 장치로서,

개인 표현을 표명하라는 요청을 수신하고 - 상기 요청은 적어도, 상기 개인 표현과 연관된 표현 코드에 대한 참조를 포함함 -;

적어도, 상기 표현 코드에 대한 참조가 상기 표현 코드의 이전에 획득되어 저장된 인스턴스에 대응하는지 여부를 표현 검증 관리자(EVM)에 의해 결정하고; 그리고

상기 표현 코드가 상기 표현 코드의 상기 저장된 인스턴스에 대응한다는 결정시 상기 개인 표현 또는 상기 표현 코드 중 적어도 하나를 표명하고; 또는

상기 표현 코드가 상기 표현 코드의 상기 저장된 인스턴스에 대응하지 않는다는 결정시 상기 개인 표현과 연관된 정보의 표명을 금지하도록 구성된 처리 시스템을 포함하는,

무선 통신을 위한 장치.

청구항 28

제 27 항에 있어서,

상기 요청은 애플리케이션으로부터 수신되며,

상기 처리 시스템은,

상기 애플리케이션에 대한 구성 프로세스의 일부로서 상기 표현 코드의 인스턴스를 획득하고; 그리고

상기 표현 코드의 인스턴스를 보안 메모리 저장소에 저장하도록 추가로 구성되는,

무선 통신을 위한 장치.

청구항 29

제 28 항에 있어서,

상기 보안 메모리 저장소는 UE와 연관된 비휘발성 메모리(NVM)인,

무선 통신을 위한 장치.

청구항 30

제 28 항에 있어서,

상기 처리 시스템은,

상기 표현 코드와 연관된 불분명한 디바이스 투 디바이스(D2D) 정보를 전송하도록 추가로 구성되는,

무선 통신을 위한 장치.

청구항 31

제 30 항에 있어서,

상기 불분명한 D2D 정보는 하나 또는 그보다 많은 인가된 디바이스들에 안전하게 전송되는,

무선 통신을 위한 장치.

청구항 32

제 30 항에 있어서,

상기 불분명한 D2D 정보는 상기 애플리케이션과 연관된 애플리케이션 서버에 전송되는,

무선 통신을 위한 장치.

청구항 33

제 30 항에 있어서,

상기 불분명한 D2D 정보는,

상기 개인 표현, 상기 표현 코드, 상기 애플리케이션의 명칭, 카운터, 생성 시간, 이전에 생성된 표현 코드, 만료일, 또는 표명하는 UE의 인증서 중 적어도 하나를 포함하는,

무선 통신을 위한 장치.

청구항 34

제 30 항에 있어서,

상기 처리 시스템은,

상기 불분명한 D2D 정보의 진정성을 표시하는 디지털 서명을 생성하도록 추가로 구성되며,

상기 불분명한 D2D 정보는 생성된 디지털 서명과 함께 전송되는,

무선 통신을 위한 장치.

청구항 35

제 34 항에 있어서,

상기 디지털 서명은 또한,

운영자 서명 키, 임시 디바이스 식별자, 또는 생존 시간(TTL) 값 중 적어도 하나를 포함할 수 있는,

무선 통신을 위한 장치.

청구항 36

제 27 항에 있어서,

상기 처리 시스템은,

신뢰 서버로부터 상기 표현 코드의 인스턴스를 안전하게 획득하고; 그리고

상기 표현 코드의 인스턴스를 보안 메모리 저장소에 저장하도록 추가로 구성되는,

무선 통신을 위한 장치.

청구항 37

제 27 항에 있어서,

상기 EVM은 UE의 모뎀과 연관되는,

무선 통신을 위한 장치.

청구항 38

제 27 항에 있어서,

상기 EVM은 상기 UE의 애플리케이션 인터페이스와 모뎀 인터페이스 간의 매개 계층으로서 구성되는,

무선 통신을 위한 장치.

청구항 39

제 38 항에 있어서,

상기 EVM의 제 1 부분은 UE의 모뎀과 연관되고,

상기 EVM의 제 2 부분은 상기 UE의 애플리케이션 인터페이스와 모뎀 인터페이스 간의 매개 계층으로서 구성되는,

무선 통신을 위한 장치.

청구항 40

컴퓨터 프로그램 물건으로서,

개인 표현을 표명하라는 요청을 수신하기 위한 코드 - 상기 요청은 적어도, 상기 개인 표현과 연관된 표현 코드에 대한 참조를 포함함 -;

적어도, 상기 표현 코드에 대한 참조가 상기 표현 코드의 이전에 획득되어 저장된 인스턴스에 대응하는지 여부를 표현 검증 관리자(EVM)에 의해 결정하기 위한 코드; 및

상기 표현 코드가 상기 표현 코드의 상기 저장된 인스턴스에 대응한다는 결정시 상기 개인 표현 또는 상기 표현 코드 중 적어도 하나를 표명하기 위한 코드; 또는

상기 표현 코드가 상기 표현 코드의 상기 저장된 인스턴스에 대응하지 않는다는 결정시 상기 개인 표현과 연관된 정보의 표명을 금지하기 위한 코드를 포함하는,

컴퓨터 판독 가능 매체를 포함하는,

컴퓨터 프로그램 물건.

청구항 41

제 40 항에 있어서,

상기 요청은 애플리케이션으로부터 수신되며,

상기 컴퓨터 프로그램 물건은,

상기 애플리케이션에 대한 구성 프로세스의 일부로서 상기 표현 코드의 인스턴스를 획득하기 위한 코드; 및

상기 표현 코드의 인스턴스를 보안 메모리 저장소에 저장하기 위한 코드를 더 포함하는,

컴퓨터 프로그램 물건.

청구항 42

제 41 항에 있어서,

상기 보안 메모리 저장소는 UE와 연관된 비휘발성 메모리(NVM)인,

컴퓨터 프로그램 물건.

청구항 43

제 41 항에 있어서,

상기 표현 코드와 연관된 불분명한 디바이스 투 디바이스(D2D) 정보를 전송하기 위한 코드를 더 포함하는,

컴퓨터 프로그램 물건.

청구항 44

제 43 항에 있어서,

상기 불분명한 D2D 정보는 하나 또는 그보다 많은 인가된 디바이스들에 안전하게 전송되는,

컴퓨터 프로그램 물건.

청구항 45

제 43 항에 있어서,

상기 불분명한 D2D 정보는 상기 애플리케이션과 연관된 애플리케이션 서버에 전송되는,

컴퓨터 프로그램 물건.

청구항 46

제 43 항에 있어서,

상기 불분명한 D2D 정보는,

상기 개인 표현, 상기 표현 코드, 상기 애플리케이션의 명칭, 카운터, 생성 시간, 이전에 생성된 표현 코드, 만료일, 또는 표명하는 UE의 인증서 중 적어도 하나를 포함하는,

컴퓨터 프로그램 물건.

청구항 47

제 43 항에 있어서,

상기 불분명한 D2D 정보의 진정성을 표시하는 디지털 서명을 생성하기 위한 코드를 더 포함하며,

상기 불분명한 D2D 정보는 생성된 디지털 서명과 함께 전송되는,

컴퓨터 프로그램 물건.

청구항 48

제 47 항에 있어서,

상기 디지털 서명은 또한,

운영자 서명 키, 임시 디바이스 식별자, 또는 생존 시간(TTL) 값 중 적어도 하나를 포함할 수 있는,

컴퓨터 프로그램 물건.

청구항 49

제 40 항에 있어서,

신뢰 서버로부터 상기 표현 코드의 인스턴스를 안전하게 획득하기 위한 코드; 및

상기 표현 코드의 인스턴스를 보안 메모리 저장소에 저장하기 위한 코드를 더 포함하는,

컴퓨터 프로그램 물건.

청구항 50

제 40 항에 있어서,

상기 EVM은 UE의 모뎀과 연관되는,

컴퓨터 프로그램 물건.

청구항 51

제 40 항에 있어서,

상기 EVM은 상기 UE의 애플리케이션 인터페이스와 모뎀 인터페이스 간의 매개 계층으로서 구성되는,

컴퓨터 프로그램 물건.

청구항 52

제 51 항에 있어서,

상기 EVM의 제 1 부분은 UE의 모뎀과 연관되고,

상기 EVM의 제 2 부분은 상기 UE의 애플리케이션 인터페이스와 모뎀 인터페이스 간의 매개 계층으로서 구성되는,

컴퓨터 프로그램 물건.

발명의 설명

기 술 분 야

[0001] [0001] 본 개시는 일반적으로 통신 시스템들에 관한 것으로, 보다 구체적으로는 무선 통신 기반 네트워크에서 디바이스 투 디바이스(D2D: device-to-device) 통신들에서의 개인 표현들의 사용에 관한 것이다.

배 경 기 술

[0002] [0002] 무선 통신 시스템들은 텔레포니, 비디오, 데이터, 메시징 및 브로드캐스트들과 같은 다양한 전기 통신 서비스들을 제공하도록 폭넓게 전개된다. 일반적인 무선 통신 시스템들은 이용 가능한 시스템 자원들(예를 들어, 대역폭, 송신 전력)을 공유함으로써 다수의 사용자들과의 통신을 지원할 수 있는 다중 액세스 기술들을 이용할 수 있다. 이러한 다중 액세스 기술들의 예들은 코드 분할 다중 액세스(CDMA: code division multiple access) 시스템들, 시분할 다중 액세스(TDMA: time division multiple access) 시스템들, 주파수 분할 다중 액세스(FDMA: frequency division multiple access) 시스템들, 직교 주파수 분할 다중 액세스(OFDMA: orthogonal frequency division multiple access) 시스템들, 단일 반송파 주파수 분할 다중 액세스(SC-FDMA: single-carrier frequency division multiple access) 시스템들, 및 시분할 동기식 코드 분할 다중 액세스(TD-SCDMA: time division synchronous code division multiple access) 시스템들을 포함한다.

[0003] [0003] 이러한 다중 액세스 기술들은 도시, 국가, 지방 그리고 심지어 전세계 레벨로 서로 다른 무선 디바이스들이 통신할 수 있게 하는 공통 프로토콜을 제공하도록 다양한 전기 통신 표준들에 채택되어 왔다. 전기 통신 표준의 일례는 롱 텀 에볼루션(LTE: long term evolution)이다. LTE는 3세대 파트너십 프로젝트(3GPP: Third Generation Partnership Project)에 의해 반포된 범용 모바일 전기 통신 시스템(UMTS: Universal Mobile Telecommunications System) 모바일 표준에 대한 확장(enhancement)들의 세트이다. LTE는 스펙트럼 효율을 개선함으로써 모바일 광대역 인터넷 액세스를 더욱 잘 지원하고, 비용들을 낮추며, 서비스들을 개선하고, 새로운 스펙트럼을 이용하며, 다운링크(DL: downlink) 상에서 OFDMA를, 업링크(UL: uplink) 상에서 SC-FDMA를, 그리고 다중 입력 다중 출력(MIMO: multiple-input multiple-output) 안테나 기술을 사용하여 다른 개방형 표준들과 더욱 잘 통합하도록 설계된다. LTE는, 직접 디바이스 투 디바이스(피어 투 피어) 통신을 지원할 수 있다.

[0004] [0004] 현재, 많은 디바이스들(예를 들어, 사용자 장비(UE: user equipment)들)이 셀룰러 네트워크에서 동작 가능하다. D2D LTE 프로토콜들이 직접 통신 범위 내에 있는 UE들 간의 통신들을 제공할 수 있다. UE들은 근접도 인식 애플리케이션들에 의해 구동되는 다양한 속성들(사용자 또는 서비스 아이덴티티들, 애플리케이션 특징들, 위치 등)을 표명하기 위한 표현들을 사용할 수 있다. 표현들은, 표명하는 UE의 범위 내에 있는 임의의 UE들에게 표현들이 액세스 가능한 경우에는 공개적일 수 있고, 아니면 사전에 인가된(authorized) 특정 UE만으로 액세스가 제한되는 경우에는 개인적일 수 있다. 개인 표현들을 사용할 때, 표명하는 UE는 근처에 있을 때 표명된 표현을 액세스/디코딩할 허가를 받은 하나 또는 그보다 많은 모니터링하고 있는 UE들에, 대응하는 표현 코드를 (예를 들어, 오프라인 프로세스를 통해) 제공했을 수도 있다.

[0005] [0005] 그러나 개인 표현 위장 위험들로부터 사용자 보안상의 결함들이 발생할 수도 있다. 예를 들어, 제 1 사용자가 제 2 사용자와 연관된 표현 코드를 알고 있는 경우, 제 1 사용자의 디바이스가 제 2 사용자의 표현 코드와 함께 개인 표현을 표명하라는 요청을 생성하기 위한 애플리케이션을 사용함으로써 제 1 사용자가 제 2 사용

자로 가장할 수 있다. 따라서 다른 사용자들이 제 2 사용자가 존재한다고 생각하도록 속임을 당할 수도 있다.

[0006] [0006] D2D 통신에 대한 요구가 증가함에 따라, 무선 통신 기반 네트워크들에서 개인 표현 식별자들을 보호하기 위한 방법들/장치들에 대한 필요성이 존재한다.

발명의 내용

[0007] [0007] 다음은 하나 또는 그보다 많은 양상들의 기본적인 이해를 제공하도록 이러한 양상들의 간단한 요약을 제시한다. 이 요약은 고려되는 모든 양상들의 포괄적인 개요가 아니며, 모든 양상들의 주요 또는 핵심 엘리먼트들을 식별하지도, 임의의 또는 모든 양상들의 범위를 기술하지도 않는 것으로 의도된다. 그 유일한 목적은 하나 또는 그보다 많은 양상들의 일부 개념들을 뒤에 제시되는 보다 상세한 설명에 대한 서론으로서 간단한 형태로 제시하는 것이다.

[0008] [0008] 하나 또는 그보다 많은 양상들 및 그에 대응하는 개시에 따르면, LTE 기반 WWAN에서의 개인 표현 보호의 제공과 관련하여 다양한 양상들이 설명된다. 일례로, UE는 개인 표현 및/또는 적어도, 개인 표현과 연관된 표현 코드에 대한 참조를 표명하라는 요청을 (예를 들어, UE 상에서 작동하는 애플리케이션으로부터) 내부적으로 수신하고, 표현 코드에 대한 참조 및/또는 표현 코드가 표현 코드의 저장된 인스턴스와 일치하는지 여부를 결정할 능력이 있다. 한 양상에서, UE는 표현 코드의 저장된 인스턴스가 요청과 함께 수신된 표현 코드에 대응하는 경우에 개인 표현 또는 표현 코드 중 적어도 하나를 표명할 능력이 있을 수도 있다. 다른 양상에서, UE는 저장된 표현 코드가 요청과 함께 수신된 표현 코드에 대응하지 않는 경우에 개인 표현과 연관된 임의의 정보의 표명을 금지할 능력이 있을 수도 있다.

[0009] [0009] 관련 양상들에 따르면, 무선 통신 네트워크에서 개인 표현 보호를 제공하기 위한 방법이 제공된다. 상기 방법은 적어도, 개인 표현을 표명하라는 요청에 대한 참조를 수신하는 단계를 포함할 수 있다. 한 양상에서, 상기 요청은 상기 개인 표현과 연관된 표현 코드를 포함할 수도 있다. 또한, 상기 방법은 적어도, 상기 표현 코드에 대한 참조가 상기 표현 코드의 이전에 획득되어 저장된 인스턴스에 대응하는지 여부를 표현 검증 관리자(EVM: expression verification manager)에 의해 결정하는 단계를 포함할 수 있다. 한 양상에서, 상기 방법은 상기 표현 코드가 상기 표현 코드의 저장된 인스턴스에 대응한다는 결정시 상기 개인 표현 또는 상기 표현 코드 중 적어도 하나를 표명하는 단계를 포함할 수 있다. 추가로 또는 대안으로, 한 양상에서, 상기 방법은 상기 표현 코드가 상기 표현 코드의 저장된 인스턴스에 대응하지 않는다는 결정시 상기 개인 표현과 연관된 정보의 표명을 금지하는 단계를 포함할 수 있다.

[0010] [0010] 다른 양상은 LTE 기반 무선 통신 네트워크에서 개인 표현 보호를 제공하도록 구성된 통신 장치에 관한 것이다. 이 통신 장치는 적어도, 개인 표현에 대한 참조를 표명하라는 요청을 수신하기 위한 수단을 포함할 수 있다. 한 양상에서, 상기 요청은 개인 표현과 연관된 표현 코드를 포함할 수도 있다. 또한, 상기 통신 장치는 적어도, 상기 표현 코드에 대한 참조가 상기 표현 코드의 이전에 획득되어 저장된 인스턴스에 대응하는지 여부를 표현 검증 관리자(EVM)에 의해 결정하기 위한 수단을 포함할 수 있다. 한 양상에서, 상기 통신 장치는 상기 표현 코드가 상기 표현 코드의 저장된 인스턴스에 대응한다는 결정시 상기 개인 표현 또는 상기 표현 코드 중 적어도 하나를 표명하기 위한 수단을 포함할 수 있다. 추가로 또는 대안으로, 한 양상에서, 상기 통신 장치는 상기 표현 코드가 상기 표현 코드의 저장된 인스턴스에 대응하지 않는다는 결정시 상기 개인 표현과 연관된 정보의 표명을 금지하기 위한 수단을 포함할 수 있다.

[0011] [0011] 다른 양상은 통신 장치에 관한 것이다. 상기 장치는 개인 표현을 표명하라는 요청을 수신하도록 구성된 처리 시스템을 포함할 수 있다. 한 양상에서, 상기 요청은 적어도, 상기 개인 표현과 연관된 표현 코드에 대한 참조를 포함할 수도 있다. 또한, 상기 처리 시스템은 적어도, 상기 표현 코드에 대한 참조가 상기 표현 코드의 이전에 획득되어 저장된 인스턴스에 대응하는지 여부를 표현 검증 관리자(EVM)에 의해 결정하도록 구성될 수 있다. 한 양상에서, 상기 처리 시스템은 상기 표현 코드가 상기 표현 코드의 저장된 인스턴스에 대응한다는 결정시 상기 개인 표현 또는 상기 표현 코드 중 적어도 하나를 표명하도록 추가로 구성될 수 있다. 추가로 또는 대안으로, 한 양상에서, 상기 처리 시스템은 상기 표현 코드가 상기 표현 코드의 저장된 인스턴스에 대응하지 않는다는 결정시 상기 개인 표현과 연관된 정보의 표명을 금지하도록 추가로 구성될 수 있다.

[0012] [0012] 또 다른 양상은 컴퓨터 프로그램 물건에 관한 것으로, 이는 개인 표현을 표명하라는 요청을 수신하기 위한 코드를 포함하는 컴퓨터 판독 가능 매체를 가질 수 있다. 한 양상에서, 상기 요청은 적어도, 상기 개인 표현과 연관된 표현 코드에 대한 참조를 포함할 수 있다. 또한, 상기 컴퓨터 판독 가능 매체는 적어도, 상기 표현 코드에 대한 참조가 상기 표현 코드의 이전에 획득되어 저장된 인스턴스에 대응하는지 여부를 표현 검증 관

리자(EVM)에 의해 결정하기 위한 코드를 포함할 수 있다. 한 양상에서, 상기 컴퓨터 판독 가능 매체는 상기 표현 코드가 상기 표현 코드의 저장된 인스턴스에 대응한다는 결정시 상기 개인 표현 또는 상기 표현 코드 중 적어도 하나를 표명하기 위한 코드를 포함할 수 있다. 추가로 또는 대안으로, 한 양상에서, 상기 컴퓨터 판독 가능 매체는 상기 표현 코드가 상기 표현 코드의 저장된 인스턴스에 대응하지 않는다는 결정시 상기 개인 표현과 연관된 정보의 표명을 금지하기 위한 코드를 포함할 수 있다.

[0013] [0013] 앞서 언급된 그리고 관련된 목적들의 이행을 위해, 하나 또는 그보다 많은 양상들은, 이후에 충분히 설명되며 청구항들에서 특별히 지적되는 특징들을 포함한다. 다음 설명 및 첨부 도면들은 하나 또는 그보다 많은 양상들의 특정 예시적인 특징들을 상세히 설명한다. 그러나 이러한 특징들은 다양한 양상들의 원리들이 채용될 수 있는 다양한 방식들 중 몇몇을 나타낼 뿐이며, 이러한 설명은 이러한 모든 양상들 및 그 등가물들을 포함하는 것으로 의도된다.

도면의 간단한 설명

[0014] [0014] 도 1은 네트워크 아키텍처의 일례를 나타내는 도면이다.

[0015] 도 2는 액세스 네트워크의 일례를 나타내는 도면이다.

[0016] 도 3은 LTE에서의 DL 프레임 구조의 일례를 나타내는 도면이다.

[0017] 도 4는 LTE에서의 UL 프레임 구조의 일례를 나타내는 도면이다.

[0018] 도 5는 사용자 평면 및 제어 평면에 대한 무선 프로토콜 아키텍처의 일례를 나타내는 도면이다.

[0019] 도 6은 액세스 네트워크에서 진화형(evolved) 노드 B와 사용자 장비의 일례를 나타내는 도면이다.

[0020] 도 7은 디바이스 투 디바이스 통신 네트워크를 나타내는 도면이다.

[0021] 도 8은 무선 통신 방법의 흐름도이다.

[0022] 도 9는 예시적인 장치에서 서로 다른 모듈들/수단들/컴포넌트들 사이의 데이터 흐름을 나타내는 개념적인 데이터 흐름도이다.

[0023] 도 10은 처리 시스템을 이용하는 장치에 대한 하드웨어 구현의 일례를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0015] [0024] 첨부 도면들과 관련하여 아래에 제시되는 상세한 설명은 다양한 구성들의 설명으로 의도되며 본 명세서에서 설명되는 개념들이 실시될 수 있는 유일한 구성들만을 나타내는 것으로 의도되는 것은 아니다. 상세한 설명은 다양한 개념들의 완전한 이해를 제공할 목적으로 특정 세부사항들을 포함한다. 그러나 이러한 개념들은 이러한 특정 세부사항들 없이 실시될 수도 있음이 해당 기술분야에서 통상의 지식을 가진 자들에게 명백할 것이다. 어떤 경우들에는, 이러한 개념들을 불명료하게 하는 것을 피하기 위해, 잘 알려진 구조들 및 컴포넌트들은 블록도 형태로 도시된다.

[0016] [0025] 이제 전기 통신 시스템들의 여러 양상들이 다양한 장치 및 방법들에 관하여 제시될 것이다. 이러한 장치 및 방법들은 다음의 상세한 설명에서 설명될 것이며 첨부 도면들에서 (통칭하여 "엘리먼트들"로 지칭되는) 다양한 블록들, 모듈들, 컴포넌트들, 회로들, 단계들, 프로세스들, 알고리즘들 등으로 예시될 것이다. 이러한 엘리먼트들은 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이들의 임의의 결합을 사용하여 구현될 수 있다. 이러한 엘리먼트들이 하드웨어로 구현되는지 아니면 소프트웨어로 구현되는지는 전체 시스템에 부과된 설계 제약들 및 특정 애플리케이션에 좌우된다.

[0017] [0026] 예로서, 엘리먼트나 엘리먼트의 임의의 부분 또는 엘리먼트들의 임의의 결합은 하나 또는 그보다 많은 프로세서들을 포함하는 "처리 시스템"으로 구현될 수 있다. 프로세서들의 예들은 마이크로프로세서들, 마이크로컨트롤러들, 디지털 신호 프로세서(DSP: digital signal processor)들, 필드 프로그래밍 가능한 게이트 어레이(FPGA: field programmable gate array)들, 프로그래밍 가능한 로직 디바이스(PLD: programmable logic device)들, 상태 머신들, 게이티드(gated) 로직, 이산 하드웨어 회로들, 및 본 개시 전반에 걸쳐 설명되는 다양한 기능을 수행하도록 구성된 다른 적당한 하드웨어를 포함한다. 처리 시스템의 하나 또는 그보다 많은 프로세서들은 소프트웨어를 실행할 수 있다. 소프트웨어는, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 하드웨어 기술 언어 또는 다른 식으로 지칭되든지 간에, 명령들, 명령 세트들, 코드, 코드 세그먼트들, 프로그램 코드,

프로그램들, 서브프로그램들, 소프트웨어 모듈들, 애플리케이션들, 소프트웨어 애플리케이션들, 소프트웨어 패키지들, 루틴들, 서브루틴들, 객체들, 실행 파일(executable)들, 실행 스레드들, 프로시저들, 함수들 등을 의미하는 것으로 광범위하게 해석될 것이다.

[0018] [0027] 따라서 하나 또는 그보다 많은 예시적인 실시예들에서, 설명되는 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 이들의 임의의 결합으로 구현될 수 있다. 소프트웨어로 구현된다면, 이 기능들은 컴퓨터 판독 가능 매체에 하나 또는 그보다 많은 명령들 또는 코드로서 저장되거나 인코딩될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체를 포함한다. 저장 매체는 컴퓨터에 의해 액세스 가능한 임의의 이용 가능한 매체일 수 있다. 한정이 아닌 예로서, 이러한 컴퓨터 판독 가능 매체는 RAM, ROM, EEPROM, CD-ROM이나 다른 광 디스크 저장소, 자기 디스크 저장소 또는 다른 자기 저장 디바이스들, 또는 명령들이나 데이터 구조들의 형태로 원하는 프로그램 코드를 전달 또는 저장하는데 사용될 수 있으며 컴퓨터에 의해 액세스 가능한 임의의 다른 매체를 포함할 수 있다. 본 명세서에서 사용되는 것과 같은 디스크(disk 및 disc)는 콤팩트 디스크(CD: compact disc), 레이저 디스크(laser disc), 광 디스크(optical disc), 디지털 다기능 디스크(DVD: digital versatile disc), 플로피 디스크(floppy disk) 및 블루레이 디스크(Blu-ray disc)를 포함하며, 여기서 디스크(disk)들은 보통 데이터를 자기적으로 재생하는 한편, 디스크(disc)들은 데이터를 레이저들에 의해 광학적으로 재생한다. 상기의 결합들 또한 컴퓨터 판독 가능 매체의 범위 내에 포함되어야 한다.

[0019] [0028] 도 1은 LTE 네트워크 아키텍처(100)를 나타내는 도면이다. LTE 네트워크 아키텍처(100)는 진화형 패킷 시스템(EPS: Evolved Packet System)(100)으로 지칭될 수도 있다. EPS(100)는 하나 또는 그보다 많은 사용자 장비(UE)(102), 진화형 UMTS 지상 무선 액세스 네트워크(E-UTRAN: Evolved UMTS Terrestrial Radio Access Network)(104), 진화형 패킷 코어(EPC: Evolved Packet Core)(110), 홈 가입자 서버(HSS: Home Subscriber Server)(120) 및 운영자의 IP 서비스들(122)을 포함할 수 있다. EPS는 다른 액세스 네트워크들과 상호 접속할 수 있지만, 단순하게 하기 위해 이러한 엔티티들/인터페이스들은 도시되지 않는다. 도시된 바와 같이, EPS는 패킷 교환 서비스들을 제공하지만, 해당 기술분야에서 통상의 지식을 가진 자들이 쉽게 인식하는 바와 같이, 본 개시 전반에 걸쳐 제시되는 다양한 개념들은 회선 교환 서비스들을 제공하는 네트워크들로 확장될 수 있다.

[0020] [0029] E-UTRAN은 진화형 노드 B(eNB: evolved Node B)(106) 및 다른 eNB들(108)을 포함한다. eNB(106)는 UE(102) 쪽으로 사용자 평면 및 제어 평면 프로토콜 종단들을 제공한다. eNB(106)는 백홀(예를 들어, X2 인터페이스)을 통해 다른 eNB들(108)에 접속될 수 있다. eNB(106)는 또한 기지국, 기지국 트랜시버, 무선 기지국, 무선 트랜시버, 트랜시버 기능, 기본 서비스 세트(BSS: basic service set), 확장 서비스 세트(ESS: extended service set) 또는 다른 어떤 적당한 전문용어로 지칭될 수도 있다. eNB(106)는 UE(102)에 EPC(110)에 대한 액세스 포인트를 제공한다. UE들(102)의 예들은 셀룰러폰, 스마트폰, 세션 개시 프로토콜(SIP: session initiation protocol) 전화, 랩톱, 개인용 디지털 보조 기기(PDA: personal digital assistant), 위성 라디오, 글로벌 포지셔닝 시스템, 멀티미디어 디바이스, 비디오 디바이스, 디지털 오디오 플레이어(예를 들어, MP3 플레이어), 카메라, 게임 콘솔, 또는 임의의 다른 유사한 기능의 디바이스를 포함한다. UE(102)는 또한 해당 기술분야에서 통상의 지식을 가진 자들에 의해 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 수도 있다.

[0021] [0030] eNB(106)는 S1 인터페이스에 의해 EPC(110)에 접속된다. EPC(110)는 이동성 관리 엔티티(MME: Mobility Management Entity)(112), 다른 MME들(114), 서빙 게이트웨이(116) 및 패킷 데이터 네트워크(PDN: Packet Data Network) 게이트웨이(118)를 포함한다. MME(112)는 UE(102)와 EPC(110) 사이의 시그널링을 처리하는 제어 노드이다. 일반적으로, MME(112)는 베어러 및 접속 관리를 제공한다. 모든 사용자 IP 패킷들은 서빙 게이트웨이(116)를 통해 전송되며, 서빙 게이트웨이(116) 그 자체는 PDN 게이트웨이(118)에 접속된다. PDN 게이트웨이(118)는 UE IP 어드레스 할당뿐 아니라 다른 기능들도 제공한다. PDN 게이트웨이(118)는 운영자의 IP 서비스들(122)에 접속된다. 운영자의 IP 서비스들(122)은 인터넷, 인트라넷, IP 멀티미디어 서브시스템(IMS: IP Multimedia Subsystem) 및 PS 스트리밍 서비스(PSS: PS Streaming Service)를 포함할 수 있다.

[0022] [0031] 도 2는 LTE 네트워크 아키텍처에서 액세스 네트워크(200)의 일례를 나타내는 도면이다. 이 예시에서, 액세스 네트워크(200)는 다수의 셀룰러 영역들(셀들)(202)로 분할된다. 하나 또는 그보다 많은 더 낮은 전력 등급의 eNB들(208)은 셀들(202) 중 하나 또는 그보다 많은 셀과 중첩하는 셀룰러 영역들(210)을 가질 수 있다. 더 낮은 전력 등급의 eNB(208)는 펨토 셀(예를 들어, 홈 eNB(HeNB: home eNB)), 피코 셀, 마이크로 셀 또는 원격 무선 헤드(RRH: remote radio head)일 수도 있다. 매크로 eNB들(204)이 각각의 셀(202)에 각각 할당되며

셀들(202) 내의 모든 UE들(206, 212)에 EPC(110)에 대한 액세스 포인트를 제공하도록 구성된다. UE들(212) 중 일부는 디바이스 투 디바이스 통신 중일 수도 있다. 액세스 네트워크(200)의 이러한 예시에는 중앙 집중형 제어기가 존재하지 않지만, 대안적인 구성들에서는 중앙 집중형 제어기가 사용될 수도 있다. eNB들(204)은 무선 베어러 제어, 승인 제어, 이동성 제어, 스케줄링, 보안, 및 서빙 게이트웨이(116)에 대한 접속성을 포함하는 모든 무선 관련 기능들을 담당한다.

[0023] [0032] 액세스 네트워크(200)에 의해 이용되는 변조 및 다중 액세스 방식은 전개되는 특정 전기 통신 표준에 따라 달라질 수 있다. LTE 애플리케이션들에서, DL에는 OFDM이 사용되고 UL에는 SC-FDMA가 사용되어 주파수 분할 듀플렉싱(FDD: frequency division duplexing)과 시분할 듀플렉싱(TDD: time division duplexing)을 모두 지원한다. 해당 기술분야에서 통상의 지식을 가진 자들이 다음의 상세한 설명으로부터 쉽게 인식하는 바와 같이, 본 명세서에서 제시되는 다양한 개념들은 LTE 애플리케이션들에 잘 맞는다. 그러나 이러한 개념들은 다른 변조 및 다중 액세스 기술들을 이용하는 다른 전기 통신 표준들로 쉽게 확장될 수 있다. 예로서, 이러한 개념들은 최적화된 에볼루션 데이터(EV-DO: Evolution-Data Optimized) 또는 울트라 모바일 브로드밴드(UMB: Ultra Mobile Broadband)로 확장될 수 있다. EV-DO 및 UMB는 CDMA2000 표준군의 일부로서 3세대 파트너십 프로젝트 2(3GPP2)에 의해 반포된 에어 인터페이스 표준들이며, CDMA를 이용하여 이동국들에 광대역 인터넷 액세스를 제공한다. 이러한 개념들은 또한 광대역-CDMA(W-CDMA) 및 CDMA의 다른 변형들, 예컨대 TD-SCDMA를 이용하는 범용 지상 무선 액세스(UTRA: Universal Terrestrial Radio Access); TDMA를 이용하는 글로벌 모바일 통신 시스템(GSM: Global System for Mobile Communications); 및 진화형 UTRA(E-UTRA), IEEE 802.11(Wi-Fi), IEEE 802.16(WiMAX), IEEE 802.20, 및 OFDMA를 이용하는 플래시-OFDM으로 확장될 수도 있다. UTRA, E-UTRA, UMTS, LTE 및 GSM은 3GPP 조직으로부터의 문서들에 기술되어 있다. CDMA2000 및 UMB는 3GPP2 조직으로부터의 문서들에 기술되어 있다. 실제 무선 통신 표준 및 이용되는 다중 액세스 기술은 특정 애플리케이션 및 시스템에 부과된 전체 설계 제약들에 좌우될 것이다.

[0024] [0033] 도 3은 LTE에서의 DL 프레임 구조의 일례를 나타내는 도면(300)이다. 프레임(10ms)은 동일한 크기의 10개의 서브프레임들로 분할될 수 있다. 각각의 서브프레임은 2개의 연속한 타임 슬롯들을 포함할 수 있다. 자원 블록을 각각 포함하는 2개의 타임 슬롯들을 나타내기 위해 자원 그리드가 사용될 수 있다. 자원 그리드는 다수의 자원 엘리먼트들로 분할된다. LTE에서, 자원 블록은 주파수 도메인에서 12개의 연속한 부반송파들을, 그리고 각각의 OFDM 심벌의 정규 주기적 프리픽스의 경우에는 시간 도메인에서 7개의 연속한 OFDM 심벌들을, 또는 84개의 자원 엘리먼트들을 포함한다. 확장된 주기적 프리픽스의 경우에, 자원 블록은 시간 도메인에서 6개의 연속한 OFDM 심벌들을 포함하며, 72개의 자원 엘리먼트들을 갖는다. 물리적 DL 제어 채널(PDCCH: physical DL control channel), 물리적 DL 공유 채널(PDSCH: physical DL shared channel), 및 다른 채널들이 자원 엘리먼트들에 맵핑될 수 있다.

[0025] [0034] 도 4는 LTE에서의 UL 프레임 구조의 일례를 나타내는 도면(400)이다. UL에 대한 이용 가능한 자원 블록들은 데이터 섹션과 제어 섹션으로 나뉠 수 있다. 제어 섹션은 시스템 대역폭의 2개의 에지들에 형성될 수 있으며 구성 가능한 크기를 가질 수 있다. 제어 섹션의 자원 블록들은 제어 정보의 전송을 위해 UE들에 할당될 수 있다. 데이터 섹션은 제어 섹션에 포함되지 않는 모든 자원 블록들을 포함할 수 있다. UL 프레임 구조는 인접한 부반송파들을 포함하는 데이터 섹션을 발생시키며, 이는 단일 UE에 데이터 섹션의 인접한 부반송파들 전부가 할당되게 할 수도 있다.

[0026] [0035] eNB에 제어 정보를 전송하도록 UE에 제어 섹션의 자원 블록들(410a, 410b)이 할당될 수 있다. eNB에 데이터를 전송하도록 UE에 또한 데이터 섹션의 자원 블록들(420a, 420b)이 할당될 수도 있다. UE는 제어 섹션의 할당된 자원 블록들 상의 물리적 UL 제어 채널(PUCCH: physical UL control channel)에서 제어 정보를 전송할 수 있다. UE는 데이터 섹션의 할당된 자원 블록들 상의 물리적 UL 공유 채널(PUSCH: physical UL shared channel)에서 데이터만 또는 데이터와 제어 정보 모두를 전송할 수 있다. UL 전송은 서브프레임의 두 슬롯들 모두에 걸칠 수 있으며 주파수에 걸쳐 호핑할 수도 있다.

[0027] [0036] 초기 시스템 액세스를 수행하고 물리적 랜덤 액세스 채널(PRACH: physical random access channel)(430)에서 UL 동기화를 달성하기 위해 한 세트의 자원 블록들이 사용될 수 있다. PRACH(430)는 랜덤 시퀀스를 전달하며 어떠한 UL 데이터/시그널링도 전달하지 못할 수 있다. 각각의 랜덤 액세스 프리앰블은 6개의 연속한 자원 블록들에 대응하는 대역폭을 점유한다. 시작 주파수는 네트워크에 의해 지정된다. 즉, 랜덤 액세스 프리앰블의 송신은 특정 시간 및 주파수 자원들로 제한된다. PRACH에 대한 주파수 호핑은 존재하지 않는다. PRACH 시도는 단일 서브프레임(1ms)에서 또는 몇 개의 인접한 서브프레임들의 시퀀스에서 전달되고, UE

는 프레임(10ms)별 단일 PRACH 시도만을 수행할 수 있다.

[0028] [0037] 도 5는 LTE에서의 사용자 평면 및 제어 평면에 대한 무선 프로토콜 아키텍처의 일례를 나타내는 도면(500)이다. 502의 UE 및 eNB에 대한 무선 프로토콜 아키텍처가 3개의 계층들: 계층 1, 계층 2 및 계층 3으로 도시된다. 3개의 계층들에 걸쳐 UE와 eNB 사이에서 데이터/시그널링의 통신이 발생할 수 있다. 계층 1(L1 계층)은 최하위 계층이며 다양한 물리 계층 신호 처리 기능들을 구현한다. L1 계층은 본 명세서에서 물리 계층(506)으로 지칭될 것이다. 계층 2(L2 계층)(508)는 물리 계층(506)보다 위에 있고 물리 계층(506) 위에서 UE와 eNB 사이의 링크를 담당한다.

[0029] [0038] 사용자 평면에서, L2 계층(508)은 매체 액세스 제어(MAC: media access control) 하위 계층(510), 무선 링크 제어(RLC: radio link control) 하위 계층(512) 및 패킷 데이터 컨버전스 프로토콜(PDCP: packet data convergence protocol) 하위 계층(514)을 포함하며, 이들은 네트워크 측의 eNB에서 종결된다. 도시되지 않았지만, UE는 네트워크 측의 PDN 게이트웨이(118)에서 종결되는 네트워크 계층(예를 들어, IP 계층), 및 접속의 다른 종단(예를 들어, 원단(far end) UE, 서버 등)에서 종결되는 애플리케이션 계층을 비롯하여, L2 계층(508) 위의 여러 상위 계층들을 가질 수 있다.

[0030] [0039] PDCP 하위 계층(514)은 서로 다른 무선 베어러들과 로직 채널들 사이의 다중화를 제공한다. PDCP 하위 계층(514)은 또한, 무선 송신 오버헤드를 감소시키기 위한 상위 계층 데이터 패킷들에 대한 헤더 압축, 데이터 패킷들의 암호화에 의한 보안, 및 eNB들 사이의 UE들에 대한 핸드오버 지원을 제공한다. RLC 하위 계층(512)은 상위 계층 데이터 패킷들의 분할 및 리어셈블리, 유실된 데이터 패킷들의 재전송, 및 하이브리드 자동 재전송 요청(HARQ: hybrid automatic repeat request)으로 인해 비순차적(out-of-order) 수신을 보상하기 위한 데이터 패킷들의 재정렬을 제공한다. MAC 하위 계층(510)은 로직 채널과 전송 채널 사이의 다중화를 제공한다. MAC 하위 계층(510)은 또한 하나의 셀에서의 다양한 무선 자원들(예를 들어, 자원 블록들)을 UE들 사이에 할당하는 것을 담당한다. MAC 하위 계층(510)은 또한 HARQ 동작들을 담당한다.

[0031] [0040] 제어 평면에서, UE 및 eNB에 대한 무선 프로토콜 아키텍처는 제어 평면에 대한 헤더 압축 기능이 존재하지 않는다는 점을 제외하고는 물리 계층(506) 및 L2 계층(508)에 대해 실질적으로 동일하다. 제어 평면은 또한 계층 3(L3 계층)에서의 무선 자원 제어(RRC: radio resource control) 하위 계층(516)을 포함한다. RRC 하위 계층(516)은 무선 자원들(즉, 무선 베어러들)의 획득 및 eNB와 UE 사이의 RRC 시그널링을 이용한 하위 계층들의 구성을 담당한다. 사용자 평면은 또한 인터넷 프로토콜(IP: internet protocol) 하위 계층(518) 및 애플리케이션 하위 계층(520)을 포함한다. IP 하위 계층(518)과 애플리케이션 하위 계층(520)은 eNB와 UE 사이의 애플리케이션 데이터의 통신 지원을 담당한다.

[0032] [0041] 도 6은 액세스 네트워크에서 UE(650)와 통신하는 WAN 엔티티(예를 들어, eNB, MME 등)(610)의 블록도이다. DL에서, 코어 네트워크로부터의 상위 계층 패킷들이 제어기/프로세서(675)에 제공된다. 제어기/프로세서(675)는 L2 계층의 기능을 구현한다. DL에서, 제어기/프로세서(675)는 헤더 압축, 암호화, 패킷 분할 및 재정렬, 로직 채널과 전송 채널 사이의 다중화, 및 다양한 우선순위 메트릭들에 기반한 UE(650)로의 무선 자원 할당들을 제공한다. 제어기/프로세서(675)는 또한 HARQ 동작들, 유실된 패킷들의 재전송, 및 UE(650)로의 시그널링을 담당한다.

[0033] [0042] 송신(TX) 프로세서(616)는 L1 계층(즉, 물리 계층)에 대한 다양한 신호 처리 기능들을 구현한다. 신호 처리 기능들은 UE(650)에서의 순방향 에러 정정(FEC: forward error correction)을 가능하게 하기 위한 코딩 및 인터리빙, 그리고 다양한 변조 방식들(예를 들어, 이진 위상 시프트 키잉(BPSK: binary phase-shift keying), 직교 위상 시프트 키잉(QPSK: quadrature phase-shift keying), M-위상 시프트 키잉(M-PSK: M-phase-shift keying), M-직교 진폭 변조(M-QAM: M-quadrature amplitude modulation))에 기반한 신호 성상도(constellation)들로의 맵핑을 포함한다. 그 후에, 코딩 및 변조된 심벌들은 병렬 스트림들로 분할된다. 그 후에, 각각의 스트림은 OFDM 부반송파에 맵핑되고, 시간 및/또는 주파수 도메인에서 기준 신호(예를 들어, 파일럿)와 다중화된 다음, 고속 푸리에 역변환(IFFT: Inverse Fast Fourier Transform)을 이용하여 함께 결합되어, 시간 도메인 OFDM 심벌 스트림을 전달하는 물리 채널을 생성한다. OFDM 스트림은 공간적으로 프리코딩되어 다수의 공간 스트림들을 생성한다. 채널 추정기(674)로부터의 채널 추정치들은 공간 처리에 대해서뿐만 아니라 코딩 및 변조 방식의 결정에도 사용될 수 있다. 채널 추정치는 UE(650)에 의해 전송되는 기준 신호 및/또는 채널 상태 피드백으로부터 도출될 수 있다. 그 후에, 각각의 공간 스트림은 개별 송신기(618)(TX)를 통해 서로 다른 안테나(620)에 제공된다. 각각의 송신기(618)(TX)는 송신을 위해 각각의 공간 스트림으로 RF 반송파를 변조한다.

[0034] [0043] UE(650)에서, 각각의 수신기(654)(RX)는 그 각자의 안테나(652)를 통해 신호를 수신한다. 각각의 수신기(654)(RX)는 RF 반송파 상에 변조된 정보를 복원하고 그 정보를 수신(RX) 프로세서(656)에 제공한다. RX 프로세서(656)는 L1 계층의 다양한 신호 처리 기능들을 구현한다. RX 프로세서(656)는 정보에 대한 공간 처리를 수행하여 UE(650)에 예정된 임의의 공간 스트림들을 복원한다. UE(650)에 다수의 공간 스트림들이 예정된다면, 이 공간 스트림들은 RX 프로세서(656)에 의해 단일 OFDM 심벌 스트림으로 결합될 수 있다. 그 후에, RX 프로세서(656)는 고속 푸리에 변환(FFT)을 사용하여 OFDM 심벌 스트림을 시간 도메인에서 주파수 도메인으로 변환한다. 주파수 도메인 신호는 OFDM 신호의 각각의 부반송파에 대한 개개의 OFDM 심벌 스트림을 포함한다. 각각의 부반송파 상의 심벌들, 그리고 기준 신호는 WAN 엔티티(610)에 의해 전송되는 가장 가능성 있는 신호 성상도 포인트들을 결정함으로써 복원 및 복조된다. 이러한 소프트 결정들은 채널 추정기(658)에 의해 계산되는 채널 추정치들을 기초로 할 수 있다. 그 다음, 소프트 결정들은 물리 채널을 통해 WAN 엔티티(610)에 의해 원래 전송되었던 데이터 및 제어 신호들을 복원하기 위해 디코딩 및 디인터리빙된다. 그 후에, 데이터 및 제어 신호들은 제어기/프로세서(659)에 제공된다.

[0035] [0044] 제어기/프로세서(659)는 L2 계층을 구현한다. 제어기/프로세서(659)는 프로그램 코드들과 데이터를 저장하는 메모리(660)와 연관될 수 있다. 메모리(660)는 컴퓨터 판독 가능 매체로 지칭될 수도 있다. UL에서, 제어기/프로세서(659)는 코어 네트워크로부터의 상위 계층 패킷들을 복원하기 위해 전송 채널과 로직 채널 사이의 역다중화, 패킷 리어셈블리, 암호 해독, 헤더 압축해제, 제어 신호 처리를 제공한다. 그 후에, 상위 계층 패킷들은 데이터 싱크(662)에 제공되는데, 데이터 싱크(662)는 L2 계층 상위의 모든 프로토콜 계층들을 나타낸다. 다양한 제어 신호들이 또한 L3 처리를 위해 데이터 싱크(662)에 제공될 수 있다. 제어기/프로세서(659)는 또한 HARQ 동작들을 지원하기 위해 확인 응답(ACK) 및/또는 부정 응답(NACK) 프로토콜을 이용한 에러 검출을 담당한다.

[0036] [0045] UL에서는, 제어기/프로세서(659)에 상위 계층 패킷들을 제공하기 위해 데이터 소스(667)가 사용된다. 데이터 소스(667)는 L2 계층 상위의 모든 프로토콜 계층들을 나타낸다. WAN 엔티티(610)에 의한 DL 송신과 관련하여 설명된 기능과 유사하게, 제어기/프로세서(659)는 헤더 압축, 암호화, 패킷 분할 및 재정렬, 그리고 WAN 엔티티(610)에 의한 무선 자원 할당들에 기반한 로직 채널과 전송 채널 사이의 다중화를 제공함으로써 사용자 평면 및 제어 평면에 대한 L2 계층을 구현한다. 제어기/프로세서(659)는 또한 HARQ 동작들, 유실된 패킷들의 재전송 및 WAN 엔티티(610)로의 시그널링을 담당한다.

[0037] [0046] WAN 엔티티(610)에 의해 전송된 기준 신호 또는 피드백으로부터 채널 추정기(658)에 의해 도출되는 채널 추정치들은 적절한 코딩 및 변조 방식들을 선택하고 공간 처리를 가능하게 하기 위해 TX 프로세서(668)에 의해 사용될 수 있다. TX 프로세서(668)에 의해 생성되는 공간 스트림들이 개개의 송신기들(654)(TX)을 통해 서로 다른 안테나(652)에 제공된다. 각각의 송신기(654)(TX)는 송신을 위해 각각의 공간 스트림으로 RF 반송파를 변조한다.

[0038] [0047] UE(650)에서의 수신기 기능과 관련하여 설명된 것과 유사한 방식으로 WAN 엔티티(610)에서 UL 송신이 처리된다. 각각의 수신기(618)(RX)는 그 각자의 안테나(620)를 통해 신호를 수신한다. 각각의 수신기(618)(RX)는 RF 반송파 상에 변조된 정보를 복원하고 그 정보를 RX 프로세서(670)에 제공한다. RX 프로세서(670)는 L1 계층을 구현할 수 있다.

[0039] [0048] 제어기/프로세서(675)는 L2 계층을 구현한다. 제어기/프로세서(675)는 프로그램 코드들과 데이터를 저장하는 메모리(676)와 연관될 수 있다. 메모리(676)는 컴퓨터 판독 가능 매체로 지칭될 수도 있다. UL에서, 제어기/프로세서(675)는 UE(650)로부터의 상위 계층 패킷들을 복원하기 위해 전송 채널과 로직 채널 사이의 역다중화, 패킷 리어셈블리, 암호 해독, 헤더 압축해제 및 제어 신호 처리를 제공한다. 제어기/프로세서(675)로부터의 상위 계층 패킷들은 코어 네트워크에 제공될 수 있다. 제어기/프로세서(675)는 또한 HARQ 동작들을 지원하기 위해 ACK 및/또는 NACK 프로토콜을 이용한 에러 검출을 담당한다.

[0040] [0049] 도 7은 디바이스 투 디바이스 통신 시스템(700)의 도면이다. 디바이스 투 디바이스 통신 시스템(700)은 복수의 무선 디바이스들(702, 704)을 포함한다. 선택적인 양상에서, 디바이스 투 디바이스 통신 시스템(700)은 또한 무선 디바이스들(702, 704) 중 하나 또는 그보다 많은 무선 디바이스와 통신하도록 동작 가능한 애플리케이션 서버(706)를 포함할 수도 있다.

[0041] [0050] 디바이스 투 디바이스 통신 시스템(700)은 예를 들어, 무선 광역 네트워크(WWAN: wireless wide area network)와 같은 셀룰러 통신 시스템과 중첩할 수 있다. 무선 디바이스들(702, 704) 중 일부는 DL/UL WWAN 스펙트럼 및/또는 비면허 스펙트럼(예를 들어, WiFi)을 사용하여 디바이스 투 디바이스 통신으로 함께 통신할 수

있고, 일부는 기지국과 통신할 수 있으며, 일부는 두 가지 모두를 수행할 수 있다. 다른 양상에서, WWAN은 하나 또는 그보다 많은 네트워크 엔티티들(예를 들어, MME들 등)을 통해 제공되는 접속을 통해 조정된 통신 환경을 제공할 수 있는 다수의 기지국들을 포함할 수 있다.

[0042] [0051] 무선 디바이스(702)는 다른 컴포넌트들 중에서도, 애플리케이션 프로세서(720), 표현 검증 관리자(730) 및 모뎀 프로세서(740)를 포함할 수 있다. 한 양상에서, 애플리케이션 프로세서(720)는 하나 또는 그보다 많은 애플리케이션들(722)을 인에이블하도록 구성될 수 있다. 이러한 양상에서, 애플리케이션(722)은 하나 또는 그보다 많은 다른 인가된 피어 디바이스들(예를 들어, 무선 디바이스(704))에 표명하기 위한 개인 표현(724)을 포함할 수 있다. 도 7에 도시된 바와 같이, 각각의 개인 표현은 연관된 표현 코드(726)를 가질 수 있다. 표현 코드(726)는 수신하는 무선 디바이스에 의해 인터셉트되어 개인 표현(724)에 액세스하는 것을 돕는데 사용될 수 있다. 또한, 표현 코드(726)는 (예를 들어, 요청하는 애플리케이션(722)이 디바이스- 이 디바이스로부터 표현 코드가 생성/저장됨 -와 연관됨을 확인하는) 개인 표현(724) 자체 인증을 돕는데 사용될 수도 있다.

[0043] [0052] 표현 검증 관리자(730)는 보안 메모리 저장소(732)(예를 들어, 보안 비휘발성 메모리)를 포함할 수도 있다. 한 양상에서, 표현 검증 관리자(730)는 애플리케이션(722) 구성/재구성 프로세스들의 일부로서 개인 표현 코드들을 생성할 수 있다. 예를 들어, 애플리케이션(722)의 설치의 일부로서, 표현 검증 관리자(730)가 개인 표현 코드들을 생성할 수도 있다. 일례로, 표현 검증 관리자(730)는 애플리케이션(722)이 (예를 들어, 피어 디바이스들(704)이 개인 표현에 액세스하도록 허용된) 개인 표현과 연관된 액세스 특징들을 변경하도록 재구성될 때 업데이트된 개인 표현 코드들을 생성할 수 있다. 한 양상에서, 표현 검증 관리자(730)는 각각의 애플리케이션(722)과 연관된 다수의 개인 표현 코드들을 생성할 수 있다. 다른 양상에서, 보안 메모리 저장소(732)는 생성된 개인 표현 코드들을 안전하게 저장할 수 있다. 도 7은 표현 검증 관리자(730)를 애플리케이션 프로세서(720) 및 모뎀 프로세서(740)와는 별개의 모듈로서 도시하지만, 표현 검증 관리자(730)는 애플리케이션 프로세서(720)에, 모뎀 프로세서(740)에, 또는 이들의 임의의 결합에 상주할 수도 있다. 또한, 한 양상에서, 표현 검증 관리자(730)는 애플리케이션 프로세서(720)와 모뎀 프로세서(740) 간의 인터페이스 역할을 할 수도 있다. 다른 양상에서, 표현 검증 관리자(730)의 제 1 부분은 모뎀 프로세서(740)와 연관될 수 있고, 표현 검증 관리자(730)의 제 2 부분은 애플리케이션 프로세서(720)와 모뎀 프로세서(740) 간의 매개 계층으로서 구성될 수 있다. 다른 양상에서, 보안 메모리 저장소(732)는 다른 디바이스들(704)로부터의 정보(예를 들어, 불분명한 D2D 정보(712))를 저장할 수 있다. 이러한 양상에서, 수신된 정보는 생존 시간(TTL: time to live) 값을 가질 수 있다. 다른 양상에서, TTL 값은 로컬하게 생성될 수도 있다. 모뎀 프로세서(740)는 하나 또는 그보다 많은 무선 액세스 기술(RAT: radio access technology)들을 사용하여 정보를 수신 및 전송하도록 구성될 수 있다.

[0044] [0053] 애플리케이션 서버(706)는 정보 개인 표현과 연관된 통신을 저장하도록 구성될 수 있다. 한 양상에서는, 개인 표현 코드들(726)을 무선 디바이스들(예를 들어, 702, 704) 상의 애플리케이션들(722)에 배포할 때 애플리케이션 서버(706)가 사용자 선택 관계들에 부착될 수 있다. 한 양상에서, 신뢰되는 애플리케이션 서버(706)가 보안 메모리 저장소(732)에 저장될 표현 코드(734)를 생성할 수 있다.

[0045] [0054] 동작 양상에서, 애플리케이션(722) 구성/재구성 프로세스의 일부로서, 불분명한 D2D 정보 모듈(736)이 무선 디바이스(702)가 불분명한 D2D 정보(712)를 생성하도록 도울 수 있다. 한 양상에서, 불분명한 D2D 정보(712)는 인가된 무선 디바이스(704)에 직접 전송될 수 있다. 다른 양상에서, 불분명한 D2D 정보(712)는 개인 표현 저장소(708)로의 저장 및 하나 또는 그보다 많은 인가된 무선 디바이스들(704)로의 전달을 위해 애플리케이션 서버(706)로 전달될 수도 있다. 한 양상에서, 불분명한 D2D 정보(712)는 개인 표현(724), 표현 코드(726), 애플리케이션(722) 명칭, 카운터, 생성 시간, 이전에 생성된 표현 코드, 만료일, 표명하는 무선 디바이스(702)의 인증서 등을 포함할 수 있다. 다른 양상에서, 불분명한 D2D 정보(712)는 불분명한 D2D 정보(712)의 진정성을 표시하는 디지털 서명으로 서명될 수 있다. 이러한 양상에서, 디지털 서명은 운영자 서명 키, 임시 디바이스 식별자, TTL 값 등을 포함할 수 있다.

[0046] [0055] 다른 동작 양상에서는, 무선 디바이스(702)와 연관된 애플리케이션(722)이 개인 표현(724)이 표명될 것을 요청할 수도 있다. 이러한 양상에서, 애플리케이션(722)은 개인 표현(724) 및 연관된 표현 코드(726)와 함께 요청을 표현 검증 관리자(730)에 전송할 수 있다. 표현 검증 관리자(730)는 수신된 표현 코드(726)를 보안 메모리 저장소(732)에 저장된 개인 표현 코드(734)와 비교하도록 구성될 수 있다. 표현 코드(726)가 저장된 개인 표현 코드(734)와 일치한다면, 표현 검증 관리자(730)는 모뎀 프로세서(740)가 개인 표현(724)을 표명(710)하게 한다. 반면, 표현 코드(726)가 저장된 개인 표현 코드(734)와 일치하지 않는다면, 표현 검증 관리자(730)는 모뎀 프로세서(740)가 개인 표현(724)을 표명(710)하는 것을 금지한다.

[0047] [0056] 무선 디바이스는 대안으로 해당 기술분야에서 통상의 지식을 가진 자들에 의해, 사용자 장비(UE), 이동국, 가입자국, 모바일 유닛, 가입자 유닛, 무선 유닛, 무선 노드, 원격 유닛, 모바일 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 수도 있다.

[0048] [0057] 아래에서 논의되는 예시적인 방법들과 장치들은 예를 들어, IEEE 802.11 표준을 기반으로 하는 와이파이(Wi-Fi)나, FlashLinQ, WiMedia, 블루투스(Bluetooth), 지그비(ZigBee)를 기반으로 하는 무선 디바이스 투 디바이스 통신 시스템과 같은 다양한 무선 디바이스 투 디바이스 통신 시스템들 중 임의의 시스템에 적용 가능하다. 논의를 단순히 하기 위해, 예시적인 방법들 및 장치는 LTE의 맥락 안에서 논의된다. 그러나 해당 기술분야에서 통상의 지식을 가진 자는 예시적인 방법들 및 장치들이 다양한 다른 무선 디바이스 투 디바이스 통신 시스템들에 더 일반적으로 적용될 수 있다고 이해할 것이다.

[0049] [0058] 도 8은 제시된 대상의 다양한 양상들에 따른 다양한 방법들을 나타낸다. 설명의 단순화를 위해, 방법들은 일련의 동작들 또는 시퀀스 단계들로서 도시 및 설명되지만, 일부 동작들은 본 명세서에서 도시 및 설명되는 것과 다른 순서들로 그리고/또는 다른 동작들과 동시에 일어날 수 있으므로, 청구 대상은 동작들의 순서로 한정되지는 않는다고 이해 및 인식되어야 한다. 예를 들어, 해당 기술분야에서 통상의 지식을 가진 자들은 방법이 대안으로, 상태도에서와 같이 일련의 상호 관련 상태들이나 이벤트들로서 표현될 수 있다고 이해 및 인식할 것이다. 더욱이, 청구 대상에 따른 방법을 구현하기 위해, 예시되는 모든 동작들이 필요한 것은 아닐 수도 있다. 추가로, 이후에 그리고 본 명세서 전반에 개시된 방법들은 이러한 방법들을 컴퓨터들로 전송 및 전달하는 것을 가능하게 하기 위한 제조품에 저장될 수 있다고 또한 인식되어야 한다. 본 명세서에서 사용되는 제조품이라는 용어는 임의의 컴퓨터 판독 가능 디바이스, 반송파 또는 매체로부터 액세스 가능한 컴퓨터 프로그램을 포괄하는 것으로 의도된다.

[0050] [0059] 도 8은 제 2 무선 통신 방법의 흐름도(800)이다. 이 방법은 UE에 의해 수행될 수 있다.

[0051] [0060] 선택적인 양상에서, 블록(802)에서, UE는 애플리케이션 및 연관된 개인 표현에 대한 구성 프로세스의 일부로서 표현 코드를 생성할 수 있다. 한 양상에서, 표현 코드는 액세스 제어에, 예를 들어 대응하는 개인 표현에 대한 액세스가 허용되는 것들을 필터링하는데 사용될 수 있다. 예를 들어, 먼저 D2D 가능 애플리케이션이 설치되면(그리고/또는 친구 추가 해제(de-friending)가 예를 들어, 개인 표현 액세스 인가의 철회를 발생시키면), UE는 개인 표현 및 개인 표현과 연관된 표현 코드를 모두 생성할 수 있다. 한 양상에서, 표현 코드가 방송에 의해(over the air) 사용되는 경우에는, UE가 개인 표현을 생성하지 않고 표현 코드를 재생성할 수도 있다.

[0052] [0061] 추가로 또는 대안으로 선택적인 양상에서는, 블록(814)에서, UE가 신뢰 서버로부터 표현 코드를 안전하게 수신할 수 있다.

[0053] [0062] 한 양상에서는, 블록(804)에서 UE가 생성된 표현 코드를 저장할 수 있다. 한 양상에서, 표현 코드는 키 저장소에 저장될 수 있다. 이러한 양상에서, 키 저장소는 데이터 및 코드를 위해 보호되는 비휘발성 물리적 메모리를 포함할 수 있다. 키 저장소는 표명된 개인 표현들에 대한 로컬 키들(예를 들어, 코드들)을 유지할 수 있다. 다른 선택적인 양상에서, 키 저장소는 모니터링되는 개인 표현들에 대한 원격 키들을 유지하고 선택적으로 검증한다. 이러한 양상에서, 원격 키들의 검증은 원격 UE가 예를 들어, 서명 검증을 이용함으로써 이 UE가 해당 표현을 모니터링하도록 인가되었음을 체크하는 것을 포함한다.

[0054] [0063] 선택적인 양상에서, UE는 또한 표현 코드와 연관된 불분명한 D2D 정보를 전송할 수도 있다. 이러한 양상에서, 불분명한 D2D 정보는 다른 UE 및/또는 신뢰되는 애플리케이션 서버에 전송될 수 있다. 또한, 이러한 양상에서, 불분명한 D2D 정보는 개인 표현, 표현 코드, 애플리케이션의 명칭, 카운터, 생성 시간, 이전에 생성된 표현 코드, 만료일, 표명하는 UE의 인증서 등을 포함할 수 있다. 다른 양상에서, 불분명한 D2D 정보는 불분명한 D2D 정보의 진정성을 표시하는 디지털 서명으로 서명될 수 있다. 이러한 양상에서, 디지털 서명은 운영자 서명 키, 임시 디바이스 식별자, 생존 시간(TTL) 값 등을 포함할 수 있다.

[0055] [0064] 블록(808)에서, UE는 표현 코드(및/또는 표현 코드에 대한 참조)를 포함하며 연관된 개인 표현의 표명을 요청하는, 애플리케이션으로부터의 요청을 수신할 수 있다.

[0056] [0065] 블록(810)에서, UE는 표명 요청에 포함된 표현 코드가 요청하는 애플리케이션에 대한 저장된 표현 코드와 일치하는지 여부를 결정할 수 있다. 한 양상에서, UE와 연관된 표현 검증 관리자(EVM)가 이러한 결정을 수행할 수 있다. 이러한 양상에서, EVM은 UE 애플리케이션 프로세서에(이것이 고레벨 운영 시스템(HLOS: high

level operating system) "서비스"의 일부일 때), 모뎀 프로세서에, 또는 이들의 임의의 결합에 상주하는 신뢰되는 엔티티일 수 있다. 또한, 한 양상에서, EVM은 애플리케이션과 UE의 모뎀 프로세서 간의 인터페이스 역할을 할 수도 있다. 다른 양상에서, EVM의 제 1 부분은 UE의 모뎀과 연관될 수 있고, EVM의 제 2 부분은 애플리케이션 계층과 UE의 모뎀 간의 매개 계층으로서 구성될 수 있다.

[0057] [0066] 블록(810)에서, UE가 표명 요청에 포함된 표현 코드가 요청하는 애플리케이션에 대한 저장된 표현 코드와 일치한다고 결정한다면, 블록(812)에서 UE는 개인 표현을 표명할 수 있다.

[0058] [0067] 반면, 블록(810)에서, UE가 표명 요청에 포함된 표현 코드가 요청하는 애플리케이션에 대한 저장된 표현 코드와 일치하지 않는다고 결정한다면, 블록(816)에서 UE는 개인 표현의 표명을 금지할 수 있다.

[0059] [0068] 도 9는 예시적인 장치(902)에서 서로 다른 모듈들/수단들/컴포넌트들 사이의 데이터 흐름을 나타내는 개념적인 데이터 흐름도(900)이다. 이 장치는 UE일 수 있다.

[0060] [0069] 장치(902)는 개인 표현(922)을 표명하라는 애플리케이션으로부터의 요청(920)을 수신할 수 있는 애플리케이션 처리 모듈(910)을 포함한다. 한 양상에서, 요청(920)은 표현 코드(916) 및/또는 표현 코드(916)에 대한 참조를 포함할 수 있다. 한 양상에서, 표현 코드(916)는 애플리케이션 구성 모듈(906)에 의해 생성되어 보안 메모리 모듈(908)에 저장될 수 있다. 선택적인 양상에서, 표현 코드(916)는 수신 모듈(904)을 사용하여 신뢰되는 애플리케이션 서버(706)로부터 수신될 수 있다. 장치(902)는 요청(920)과 함께 수신된 표현 코드(916) 및/또는 표현 코드(916)에 대한 참조를 보안 메모리 모듈(908)에 저장된 표현 코드(916)와 비교하도록 구성될 수 있는 개인 표현 검증 모듈(912)을 더 포함할 수 있다. 한 양상에서, 개인 표현 검증 모듈(912)은 표현 검증 관리자(730)에 관해 설명한 바와 같이 구현될 수 있다. 표현 코드들(916)이 일치하는 경우, 개인 표현 검증 모듈(912)은 송신 모듈(914)이 개인 표현(922)을 표명하게 한다. 반면, 표현 코드들(916)이 일치하지 않는 경우, 개인 표현 검증 모듈(912)은 송신 모듈(914)이 개인 표현(922)을 표명하는 것을 금지한다. 다른 양상에서, 애플리케이션 구성 모듈(906)은 송신 모듈(914)을 사용한 송신을 위해 표현 코드와 연관된 불분명한 D2D 정보(918)를 생성할 수 있다. 이러한 양상에서, 불분명한 D2D 정보(918)는 다른 UE (예를 들어, UE(704)) 및/또는 신뢰되는 애플리케이션 서버(706)에 전송될 수 있다. 또한, 이러한 양상에서, 불분명한 D2D 정보(918)는 개인 표현, 표현 코드, 애플리케이션의 명칭, 카운터, 생성 시간, 이전에 생성된 표현 코드, 만료일, 표명하는 UE의 인증서 등을 포함할 수 있다. 다른 양상에서, 불분명한 D2D 정보(918)는 불분명한 D2D 정보의 진정성을 표시하는 디지털 서명으로 서명될 수 있다.

[0061] [0070] 이 장치는 도 8의 앞서 언급한 흐름도에서 알고리즘의 단계들 각각을 수행하는 추가 모듈들을 포함할 수 있다. 이에 따라, 도 8의 앞서 언급한 흐름도의 각각의 단계는, 모듈에 의해 수행될 수 있고, 장치는 그러한 모듈들 중 하나 또는 그보다 많은 모듈을 포함할 수 있다. 모듈들은 구체적으로, 언급된 프로세스들/알고리즘을 실행하도록 구성되거나, 언급된 프로세스들/알고리즘을 수행하도록 구성된 프로세서에 의해 구현되거나, 프로세서에 의한 구현을 위해 컴퓨터 판독 가능 매체 내에 저장되거나, 또는 이들의 어떤 결합에 의한, 하나 또는 그보다 많은 하드웨어 컴포넌트들일 수 있다.

[0062] [0071] 도 10은 처리 시스템(1014)을 이용하는 장치(902')에 대한 하드웨어 구현의 일례를 나타내는 도면(1000)이다. 처리 시스템(1014)은 일반적으로 버스(1024)로 제시된 버스 아키텍처로 구현될 수 있다. 버스(1024)는 처리 시스템(1014)의 특정 애플리케이션 및 전체 설계 제약들에 따라 많은 수의 상호 접속 버스들 및 브리지들을 포함할 수 있다. 버스(1024)는 프로세서(1004), 모듈들(904, 906, 908, 910, 912, 914) 및 컴퓨터 판독 가능 매체(1006)로 제시된 하나 또는 그보다 많은 프로세서들 및/또는 하드웨어 모듈들을 포함하는 다양한 회로들을 서로 링크한다. 버스(1024)는 또한, 해당 기술분야에 잘 알려져 있고 이에 따라 더 이상 설명되지 않을, 타이밍 소스들, 주변 장치들, 전압 조정기들 및 전력 관리 회로들과 같은 다양한 다른 회로들을 링크할 수도 있다.

[0063] [0072] 처리 시스템(1014)은 트랜시버(1010)에 연결될 수 있다. 트랜시버(1010)는 하나 또는 그보다 많은 안테나들(1020)에 연결된다. 트랜시버(1010)는 전송 매체를 통해 다양한 다른 장치와 통신하기 위한 수단을 제공한다. 처리 시스템(1014)은 컴퓨터 판독 가능 매체(1006)에 연결된 프로세서(1004)를 포함한다. 프로세서(1004)는 컴퓨터 판독 가능 매체(1006) 상에 저장된 소프트웨어의 실행을 포함하여, 일반적인 처리를 담당한다. 소프트웨어는 프로세서(1004)에 의해 실행될 때, 처리 시스템(1014)으로 하여금 임의의 특정 장치에 대해 앞서 설명한 다양한 기능들을 수행하게 한다. 컴퓨터 판독 가능 매체(1006)는 또한 소프트웨어 실행시 프로세서(1004)에 의해 조작되는 데이터를 저장하기 위해 사용될 수도 있다. 처리 시스템은 모듈들(904, 906, 908, 910, 912, 914) 중 적어도 하나를 더 포함한다. 모듈들은 컴퓨터 판독 가능 매체(1006)에 상주/저장되어 프로세서

(1004)에서 구동하는 소프트웨어 모듈들, 프로세서(1004)에 연결된 하나 또는 그보다 많은 하드웨어 모듈들, 또는 이들의 어떤 결합일 수 있다. 처리 시스템(1014)은 UE(650)의 컴포넌트일 수도 있고, 메모리(660) 및/또는 TX 프로세서(668), RX 프로세서(656) 및 제어기/프로세서(659) 중 적어도 하나를 포함할 수도 있다.

[0064] [0073] 한 구성에서, 무선 통신을 위한 장치(902/902')는 개인 표현과 연관된 표현 코드를 포함하며 개인 표현을 표명하라는 요청을 수신하기 위한 수단, 표현 코드가 표현 코드의 이전에 획득되어 저장된 인스턴스에 대응하는지 여부를 표현 검증 관리자(EVM)에 의해 결정하기 위한 수단, 표현 코드가 이 표현 코드의 저장된 인스턴스에 대응한다는 결정시 개인 표현 또는 표현 코드 중 적어도 하나를 표명하기 위한 수단, 및/또는 표현 코드가 표현 코드의 저장된 인스턴스에 대응하지 않는다는 결정시 개인 표현과 연관된 정보의 표명을 금지하기 위한 수단을 포함한다. 다른 양상에서, 장치(902/902')는 애플리케이션에 대한 구성 프로세스의 일부로서 표현 코드의 인스턴스를 획득하기 위한 수단을 포함할 수도 있다. 이러한 양상에서, 장치(902/902')는 표현 코드의 인스턴스를 보안 메모리 저장소에 저장하기 위한 수단을 포함할 수도 있다. 다른 양상에서, 장치(902/902')는 표현 코드와 연관된 불분명한 D2D 정보를 전송하기 위한 수단을 포함할 수도 있다. 다른 양상에서, 장치(902/902')는 불분명한 D2D 정보의 진정성을 표시하는 디지털 서명을 생성하도록 추가로 구성될 수도 있으며, 여기서 불분명한 D2D 정보는 생성된 디지털 서명과 함께 전송된다. 한 양상에서, 장치(902/902')는 신뢰 서버로부터 표현 코드의 인스턴스를 안전하게 획득하기 위한 수단을 포함할 수 있다. 이러한 양상에서, 장치(902/902')는 표현 코드의 인스턴스를 보안 메모리 저장소에 저장하기 위한 수단을 포함할 수도 있다. 앞서 언급한 수단들은, 앞서 언급한 수단들에 의해 기술된 기능들을 수행하도록 구성된 장치(902')의 처리 시스템(1014) 및/또는 장치(902)의 앞서 언급한 모듈들 중 하나 또는 그보다 많은 것일 수도 있다. 앞서 설명한 바와 같이, 처리 시스템(1014)은 TX 프로세서(668), RX 프로세서(656) 및 제어기/프로세서(659)를 포함할 수 있다. 따라서 한 구성에서, 앞서 언급한 수단은, 앞서 언급한 수단에 의해 기술된 기능들을 수행하도록 구성된 TX 프로세서(668), RX 프로세서(656) 및 제어기/프로세서(659)일 수 있다.

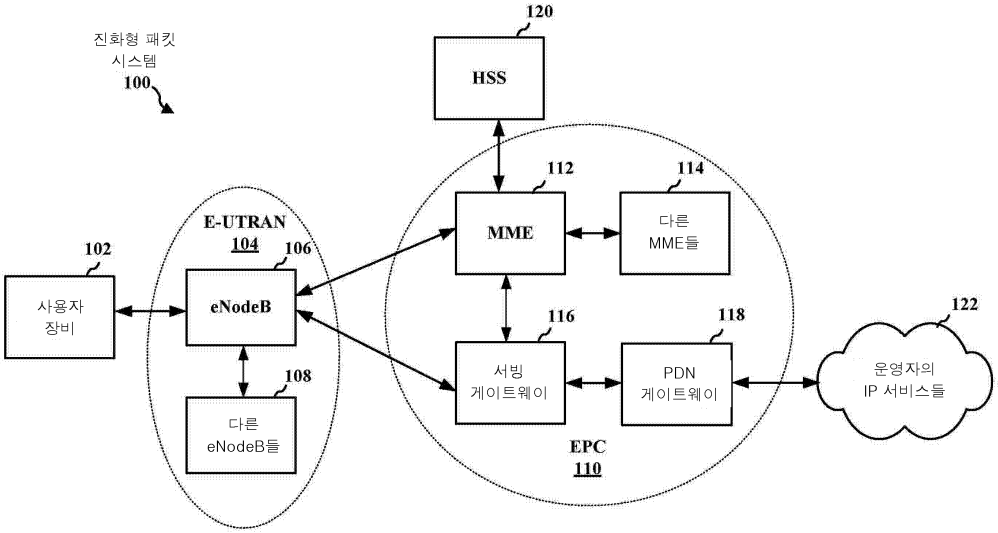
[0065] [0074] 개시된 프로세스들의 단계들의 특정 순서 또는 계층 구조는 예시적인 접근 방식들의 실례인 것으로 이해된다. 설계 선호들을 기초로, 프로세스들의 단계들의 특정 순서 또는 계층 구조는 재배열될 수도 있다고 이해된다. 추가로, 일부 단계들은 결합되거나 생략될 수도 있다. 첨부한 방법 청구항들은 다양한 단계들의 엘리먼트들을 예시적인 순서로 제시하며, 제시된 특정 순서 또는 계층 구조로 한정되는 것으로 여겨지는 것은 아니다.

[0066] [0075] 본 명세서에서 "예시적인"이라는 단어는 일례, 실례 또는 예시로서의 역할을 의미하는데 사용된다. 본 명세서에 "예시적인"으로서 설명된 어떠한 양상 또는 설계도 반드시 다른 양상들 또는 설계들에 비해 선호되거나 유리한 것으로 해석되는 것은 아니다. 추가로, 본 명세서에서 사용된 바와 같이, 항목들의 리스트 "중 적어도 하나" 및/또는 "중 하나 또는 그보다 많은 것"을 의미하는 문구는 단일 멤버들을 비롯하여 그러한 항목들의 임의의 결합을 의미한다. 일례로, "*a*, *b* 또는 *c* 중 적어도 하나"는 *a*, *b*, *c*, *a-b*, *a-c*, *b-c* 그리고 *a-b-c*를 커버하는 것으로 의도된다.

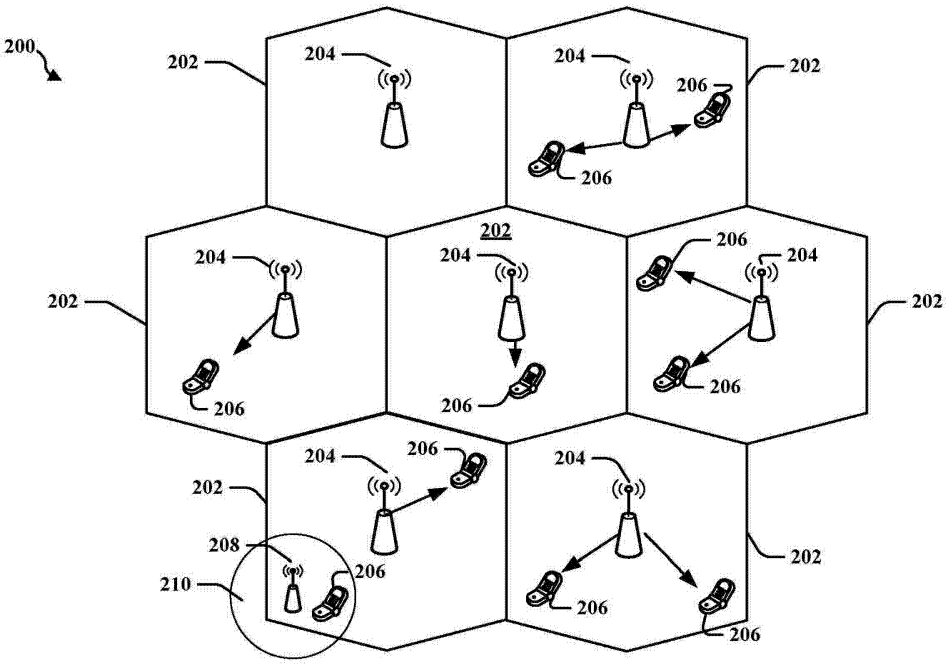
[0067] [0076] 상기 설명은 해당 기술분야에서 통상의 지식을 가진 임의의 자가 본 명세서에서 설명된 다양한 양상들을 실시할 수 있게 하도록 제공된다. 이러한 양상들에 대한 다양한 변형들이 해당 기술분야에서 통상의 지식을 가진 자들에게 쉽게 명백할 것이며, 본 명세서에 정의된 일반 원리들은 다른 양상들에 적용될 수도 있다. 따라서 청구항들은 본 명세서에 도시된 양상들로 한정되는 것으로 의도되는 것이 아니라 청구항 문언과 일치하는 전체 범위에 따르는 것이며, 여기서 엘리먼트에 대한 단수 언급은 구체적으로 그렇게 언급하지 않는 한 "하나 및 단 하나"를 의미하는 것으로 의도되는 것이 아니라, 그보다는 "하나 또는 그보다 많은"을 의미하는 것이다. 구체적으로 달리 언급되지 않는 한, "일부"라는 용어는 하나 또는 그보다 많은 것을 의미한다. 해당 기술분야에서 통상의 지식을 가진 자들에게 알려진 또는 나중에 알려지게 될 본 개시 전반에 걸쳐 설명된 다양한 양상들의 엘리먼트들에 대한 모든 구조적 그리고 기능적 등가물들은 인용에 의해 본 명세서에 명백히 포함되며, 청구항들에 의해 포괄되는 것으로 의도된다. 더욱이, 본 명세서에 개시된 내용은, 청구항들에 이러한 개시 내용이 명시적으로 기재되어 있는지 여부에 관계없이, 공중이 사용하도록 의도되는 것은 아니다. 청구항 엘리먼트가 명백히 "~을 위한 수단"이라는 문구를 사용하여 언급되지 않는 한, 어떠한 청구항 엘리먼트도 수단 + 기능으로서 해석되어야 하는 것은 아니다.

도면

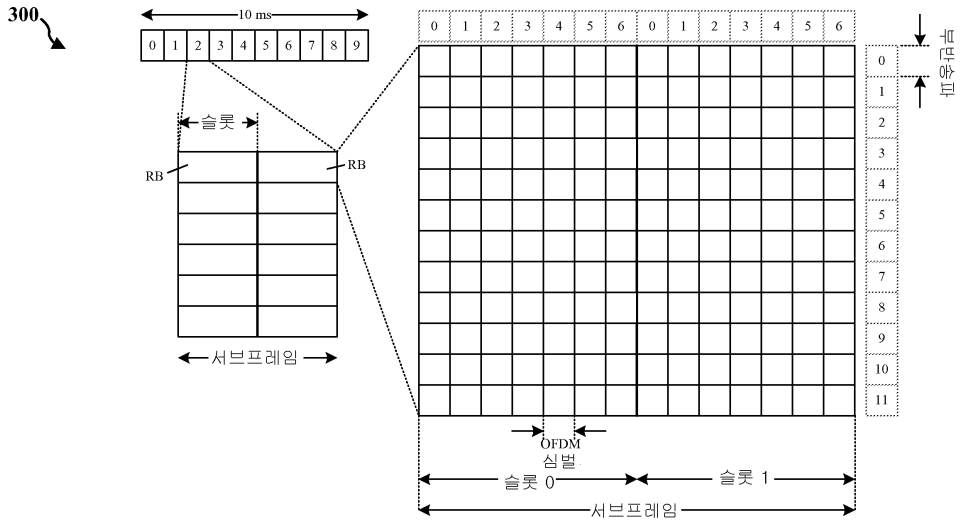
도면1


진화형 패킷
시스템
100
120
HSS
112
114
MME
다른
MME들
E-UTRAN
104
106
102
사용자
장비
eNodeB
116
118
122
서빙
게이트웨이
PDN
게이트웨이
운영자의
IP 서비스들
108
다른
eNodeB들
EPC
110

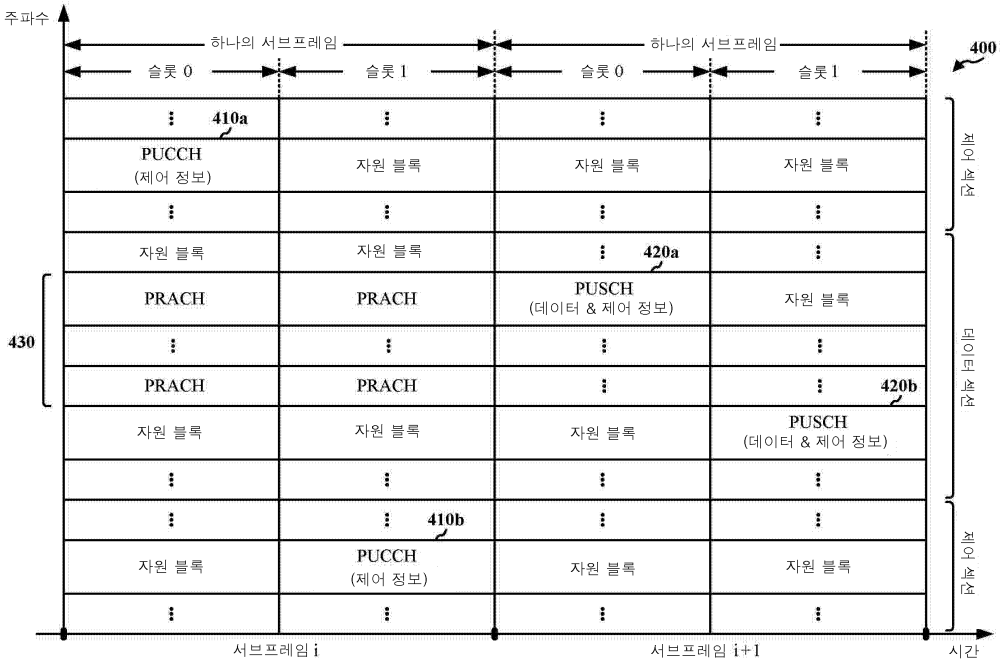
도면2


200
202
204
206
208
210

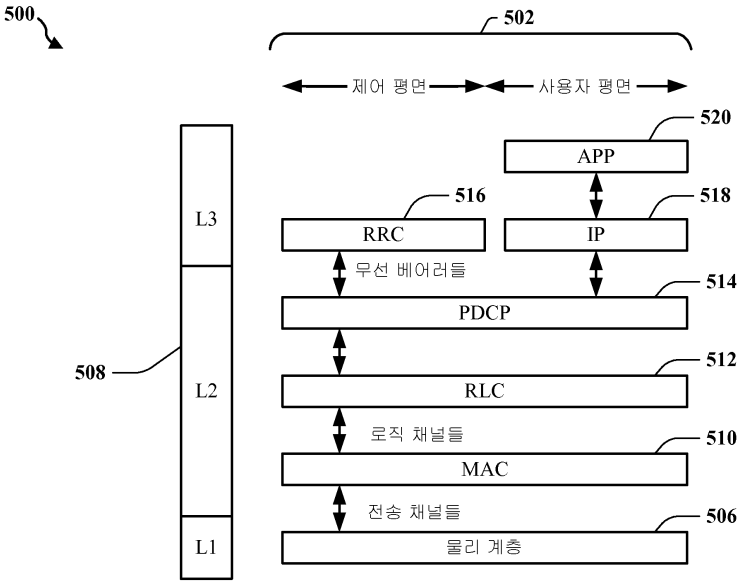
도면3


300
10 ms
0 1 2 3 4 5 6 7 8 9
슬롯
RB
RB
서브프레임
0 1 2 3 4 5 6 0 1 2 3 4 5 6
0 1 2 3 4 5 6 7 8 9 10 11
부반송파
OFDM 심벌
슬롯 0
슬롯 1
서브프레임

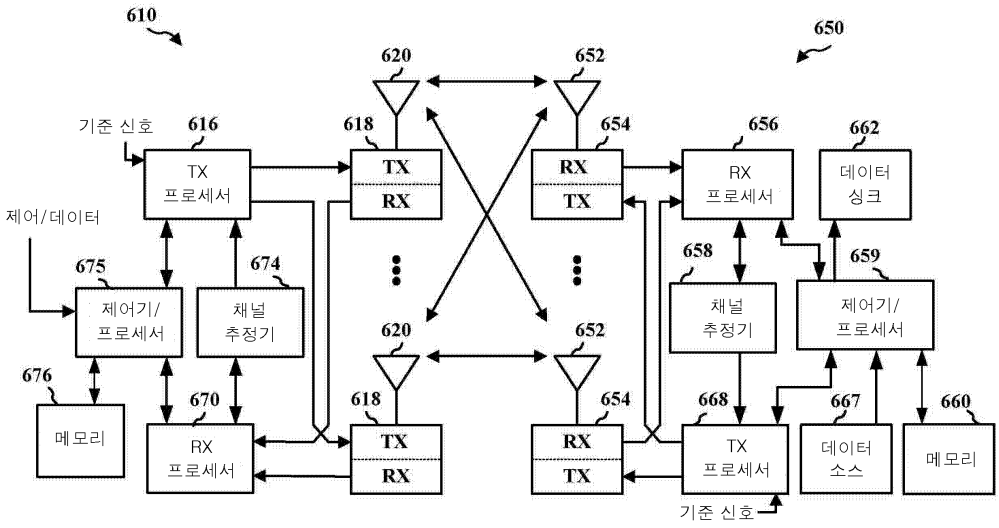
도면4


주파수
하나의 서브프레임
하나의 서브프레임
400
슬롯 0
슬롯 1
슬롯 0
슬롯 1
410a
PUCCH
(제어 정보)
자원 블록
자원 블록
자원 블록
제어 섹션
자원 블록
자원 블록
420a
PRACH
PRACH
PUSCH
(데이터 & 제어 정보)
자원 블록
430
PRACH
PRACH
420b
자원 블록
자원 블록
자원 블록
PUSCH
(데이터 & 제어 정보)
데이터 섹션
410b
자원 블록
PUCCH
(제어 정보)
자원 블록
자원 블록
제어 섹션
서브프레임 i
서브프레임 i+1
시간

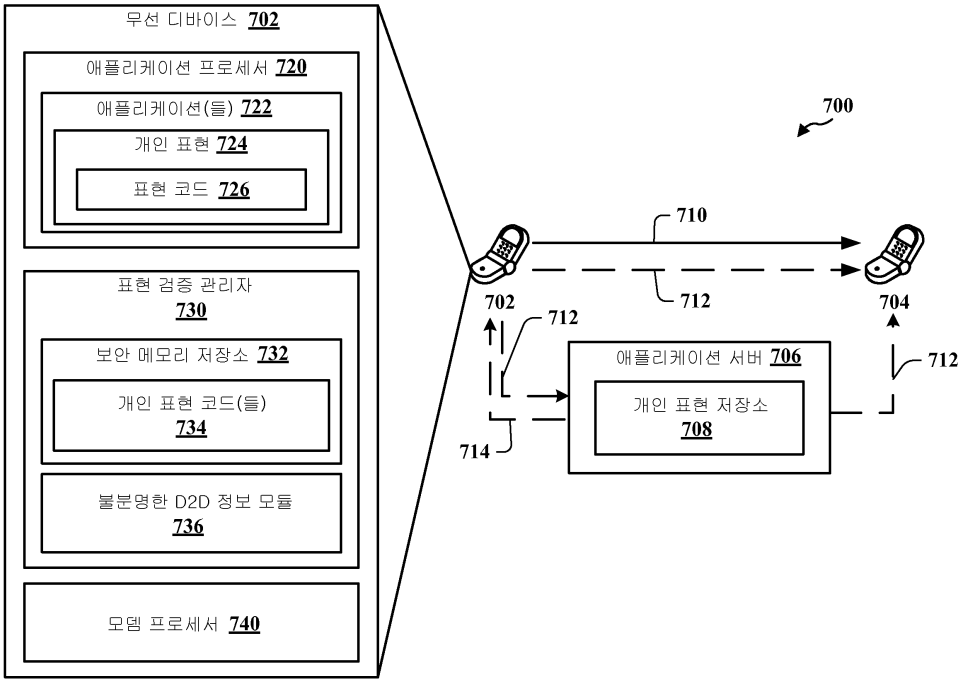
도면5


500
502
제어 평면
사용자 평면
520
APP
516
518
RRC
IP
L3
무선 베어러들
514
PDCP
508
L2
512
RLC
로직 채널들
510
MAC
전송 채널들
506
L1
물리 계층

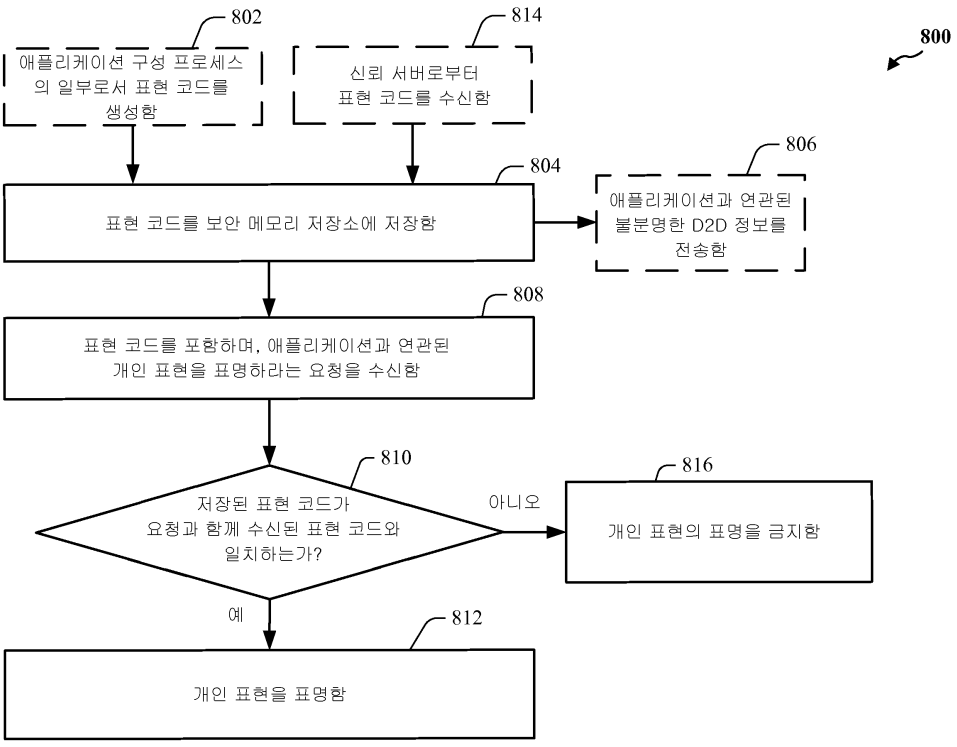
도면6


610
650
620
652
기준 신호
616
618
654
656
662
TX
프로세서
TX
RX
RX
TX
RX
프로세서
데이터
싱크
제어/데이터
675
674
658
659
제어기/
프로세서
채널
추정기
채널
추정기
제어기/
프로세서
620
652
676
670
618
654
668
667
660
메모리
RX
프로세서
TX
RX
RX
TX
TX
프로세서
데이터
소스
메모리
기준 신호

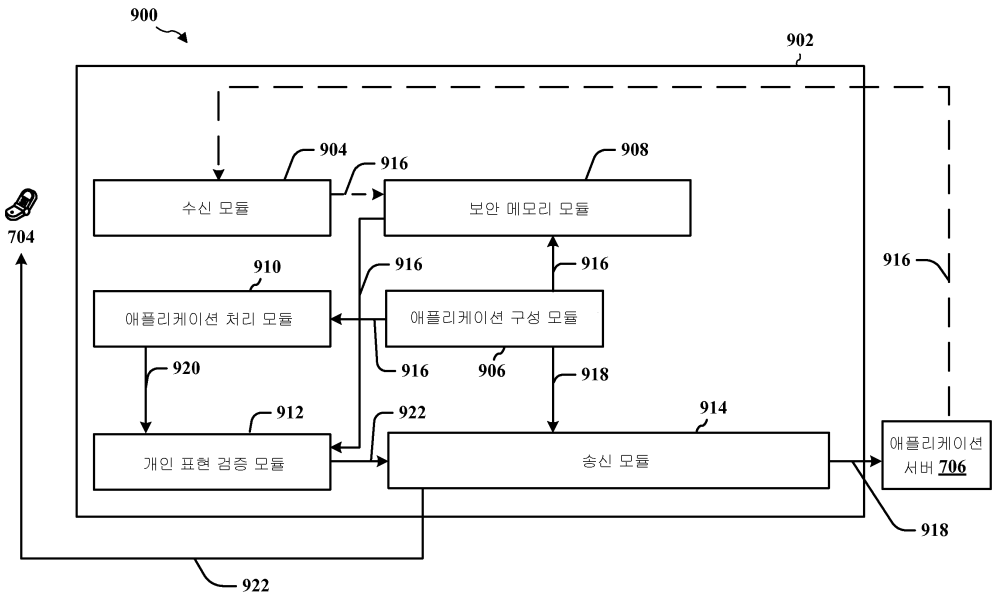
도면7


무선 디바이스 702
애플리케이션 프로세서 720
애플리케이션(들) 722
개인 표현 724
표현 코드 726
표현 검증 관리자 730
보안 메모리 저장소 732
개인 표현 코드(들) 734
불분명한 D2D 정보 모듈 736
모뎀 프로세서 740
700
710
712
702
704
712
712
714
애플리케이션 서버 706
개인 표현 저장소 708

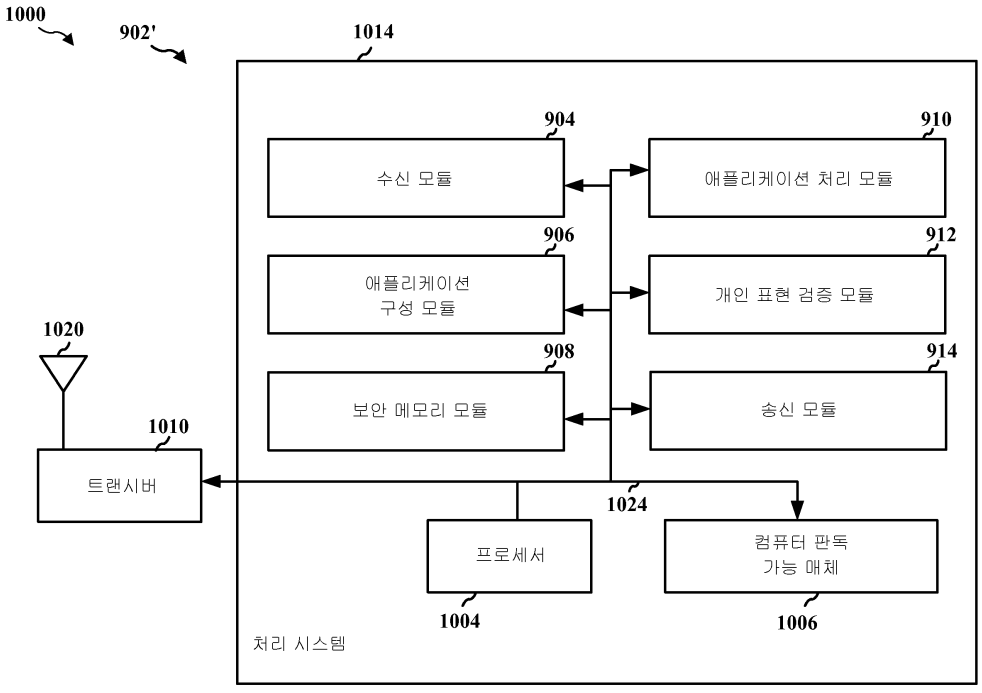
도면8


800
802
애플리케이션 구성 프로세스의 일부로서 표현 코드를 생성함
814
신뢰 서버로부터 표현 코드를 수신함
804
표현 코드를 보안 메모리 저장소에 저장함
806
애플리케이션과 연관된 불분명한 D2D 정보를 전송함
808
표현 코드를 포함하며, 애플리케이션과 연관된 개인 표현을 표명하라는 요청을 수신함
810
저장된 표현 코드가 요청과 함께 수신된 표현 코드와 일치하는가?
아니오
816
개인 표현의 표명을 금지함
예
812
개인 표현을 표명함

도면9


900
902
904
916
908
수신 모듈
보안 메모리 모듈
704
910
916
916
916
애플리케이션 처리 모듈
애플리케이션 구성 모듈
920
916
906
918
912
922
914
개인 표현 검증 모듈
송신 모듈
애플리케이션
서버 706
918
922

도면10


1000
902'
1014
904
910
수신 모듈
애플리케이션 처리 모듈
906
912
애플리케이션
구성 모듈
개인 표현 검증 모듈
1020
908
914
보안 메모리 모듈
송신 모듈
1010
트랜시버
1024
프로세서
컴퓨터 판독
가능 매체
1004
1006
처리 시스템