(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년09월13일
(11) 등록번호 10-2443184
(24) 등록일자 2022년09월07일

(51) 국제특허분류(Int. Cl.)
H04W 12/033 (2021.01) *H04W 12/04* (2021.01)
H04W 12/06 (2021.01) *H04W 76/12* (2018.01)
(52) CPC특허분류
H04W 12/033 (2021.01)
H04L 63/205 (2013.01)
(21) 출원번호 10-2022-7002358(분할)
(22) 출원일자(국제) 2015년09월23일
심사청구일자 2022년01월21일
(85) 번역문제출일자 2022년01월21일
(65) 공개번호 10-2022-0016297
(43) 공개일자 2022년02월08일
(62) 원출원 특허 10-2017-7007646
원출원일자(국제) 2015년09월23일
심사청구일자 2020년09월09일
(86) 국제출원번호 PCT/US2015/051622
(87) 국제공개번호 WO 2016/049125
국제공개일자 2016년03월31일
(30) 우선권주장
62/054,271 2014년09월23일 미국(US)
14/862,124 2015년09월22일 미국(US)
(56) 선행기술조사문헌
EP02387283 A2
US20130201957 A1
US20130301611 A1
WO2014094835 A1

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
그리엇, 미구엘
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
수, 하오
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
바자페얌, 마드하반 스리니바산
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤남

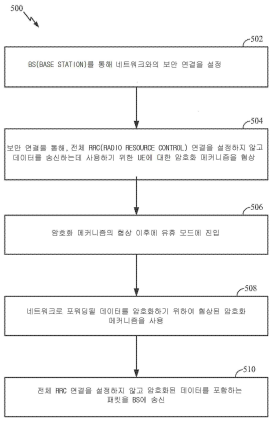
전체 청구항 수 : 총 67 항 심사관 : 이준석

(54) 발명의 명칭 **보안 비연결형 업링크 소형 데이터 송신을 위한 방법들 및 장치**

(57) 요 약

본 개시물의 특정 양상들은 일반적으로 무선 디바이스에 의한 보안 비연결형 업링크 송신들을 위한 기법들에 관한 것이다. 이러한 기법들은 비연결형 송신들 및 후속하는 보안 비연결형 업링크 송신들에 대한 셋업의 일부로서 암호화 메커니즘의 협상을 제공할 수 있다.

대 표 도 - 도5



(52) CPC특허분류
H04W 12/04 (2021.01)
H04W 12/06 (2021.01)
H04W 76/12 (2018.02)

명 세 서

청구범위

청구항 1

UE(user equipment)에 의한 무선 통신을 위한 방법으로서,

BS(base station)를 통해 네트워크와의 보안 연결을 설정하는 단계 - 상기 보안 연결을 설정하는 것은 TAU(tracking area update) 또는 부착 프로시저(attach procedure) 중 적어도 하나를 포함함 -;

상기 보안 연결을 통해, 상기 UE가 상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용하기 위한 암호화 메커니즘을 협상하는 단계;

상기 암호화 메커니즘의 협상 이후에 유휴 모드에 진입하는 단계;

상기 유휴 모드로부터 전이한 후에 상기 네트워크에 송신될 데이터를 암호화하기 위하여 상기 협상된 암호화 메커니즘을 사용하는 단계; 및

상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 상기 암호화된 데이터를 포함하는 패킷을 상기 BS에 송신하는 단계를 포함하는, UE에 의한 무선 통신을 위한 방법.

청구항 2

제 1 항에 있어서,

상기 암호화 메커니즘을 협상하는 단계는,

비연결형 셋업에 대한 요청을 송신하는 단계 - 상기 요청은 상기 UE에 의해 지원되는 하나 또는 그 초과의 암호화 메커니즘들을 표시함 - ; 및

상기 지원되는 암호화 메커니즘들 중 적어도 하나를 표시하는 응답을 수신하는 단계를 포함하는, UE에 의한 무선 통신을 위한 방법.

청구항 3

제 1 항에 있어서,

상기 암호화된 데이터를 포함하는 패킷을 송신하기 위한 자원들에 대한 요청을 상기 BS에 송신하는 단계를 더 포함하는, UE에 의한 무선 통신을 위한 방법.

청구항 4

제 1 항에 있어서,

상기 패킷은 상기 네트워크가 상기 UE를 인증하기 위한 메커니즘을 더 포함하는, UE에 의한 무선 통신을 위한 방법.

청구항 5

제 1 항에 있어서,

상기 패킷의 송신 이후에, 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제하였음을 확인응답하는 메시지를 수신하는 단계를 더 포함하는, UE에 의한 무선 통신을 위한 방법.

청구항 6

제 5 항에 있어서,

상기 메시지는 페이징 메시지를 포함하는, UE에 의한 무선 통신을 위한 방법.

청구항 7

제 6 항에 있어서,

상기 페이징 메시지의 송신은 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제하였다는 확인응답을 표시하는, UE에 의한 무선 통신을 위한 방법.

청구항 8

제 5 항에 있어서,

상기 메시지는 상기 UE가 상기 네트워크를 인증하기 위한 메커니즘을 포함하는, UE에 의한 무선 통신을 위한 방법.

청구항 9

제 1 항에 있어서,

상기 패킷의 송신 이후에:

상기 UE가 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제하였다는 ACK(acknowledgement)를 수신하지 않았음을 결정하는 단계; 및

상기 결정에 대한 응답으로 상기 패킷을 재송신하는 단계를 더 포함하는, UE에 의한 무선 통신을 위한 방법.

청구항 10

무선 통신을 위한 장치로서,

적어도 하나의 프로세서; 및

상기 적어도 하나의 프로세서에 커플링된 메모리를 포함하며,

상기 메모리는 상기 장치로 하여금,

BS(base station)를 통해 네트워크와의 보안 연결을 설정하게 하고 - 상기 보안 연결을 설정하는 것은 TAU(tracking area update) 또는 부착 프로시저(attach procedure) 중 적어도 하나를 포함함 -;

상기 보안 연결을 통해, 상기 장치가 상기 장치와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용하기 위한 암호화 메커니즘을 협상하게 하고;

상기 암호화 메커니즘의 협상 이후에 유휴 모드에 진입하게 하고;

상기 유휴 모드로부터 전이한 후에 상기 네트워크에 송신될 데이터를 암호화하기 위하여 상기 협상된 암호화 메커니즘을 사용하게 하고; 그리고

상기 장치와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 상기 암호화된 데이터를 포함하는 패킷을 상기 BS에 송신하게 하도록,

상기 적어도 하나의 프로세서에 의해 실행될 수 있는 명령들을 포함하는, 무선 통신을 위한 장치.

청구항 11

제 10 항에 있어서,

비연결형 셋업에 대한 요청을 송신하고 - 상기 요청은 상기 장치에 의해 지원되는 하나 또는 그 초과의 암호화 메커니즘들을 표시함 - ; 그리고

상기 지원되는 암호화 메커니즘들 중 적어도 하나를 표시하는 응답을 수신함으로써,

상기 명령들은 상기 장치로 하여금 암호화 메커니즘을 협상하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 무선 통신을 위한 장치.

청구항 12

제 10 항에 있어서,

상기 명령들은 상기 장치로 하여금 상기 암호화된 데이터를 포함하는 패킷을 송신하기 위한 자원들에 대한 요청을 상기 BS에 송신하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 무선 통신을 위한 장치.

청구항 13

제 10 항에 있어서,

상기 패킷은 상기 네트워크가 상기 장치를 인증하기 위한 메커니즘을 더 포함하는, 무선 통신을 위한 장치.

청구항 14

제10 항에 있어서,

상기 명령들은 상기 장치로 하여금 상기 패킷의 송신 이후에, 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제하였음을 확인응답하는 메시지를 수신하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 무선 통신을 위한 장치.

청구항 15

제 14 항에 있어서,

상기 메시지는 페이징 메시지를 포함하는, 무선 통신을 위한 장치.

청구항 16

제 15 항에 있어서,

상기 페이징 메시지의 송신은 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제하였다는 확인응답을 표시하는, 무선 통신을 위한 장치.

청구항 17

제 14 항에 있어서,

상기 메시지는 상기 장치가 상기 네트워크를 인증하기 위한 메커니즘을 포함하는, 무선 통신을 위한 장치.

청구항 18

제 10 항에 있어서,

상기 명령들은 상기 장치로 하여금 상기 패킷의 송신 이후에:

상기 장치가 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제하였다는 ACK(acknowledgement)를 수신하지 않았음을 결정하게 하고; 그리고

상기 결정에 대한 응답으로 상기 패킷을 재송신하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 무선 통신을 위한 장치.

청구항 19

무선 통신을 위한 장치로서,

BS(base station)를 통해 네트워크와의 보안 연결을 설정하기 위한 수단 - 상기 보안 연결을 설정하는 것은 TAU(tracking area update) 또는 부착 프로시저(attach procedure) 중 적어도 하나를 포함함 -;

상기 보안 연결을 통해, 상기 장치가 상기 장치와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용하기 위한 암호화 메커니즘을 협상하기 위한 수단;

상기 암호화 메커니즘의 협상 이후에 유휴 모드에 진입하기 위한 수단;

상기 유휴 모드로부터 전이한 후에 상기 네트워크에 송신될 데이터를 암호화하기 위하여 상기 협상된 암호화 메

커니즘을 사용하기 위한 수단; 및

상기 장치와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 상기 암호화된 데이터를 포함하는 패킷을 상기 BS에 송신하기 위한 수단을 포함하는, 무선 통신을 위한 장치.

청구항 20

제 19 항에 있어서,

상기 암호화 메커니즘을 협상하기 위한 수단은,

비연결형 셋업에 대한 요청을 송신하기 위한 수단 - 상기 요청은 상기 장치에 의해 지원되는 하나 또는 그 초과의 암호화 메커니즘들을 표시함 - ; 및

상기 지원되는 암호화 메커니즘들 중 적어도 하나를 표시하는 응답을 수신하기 위한 수단을 포함하는, 무선 통신을 위한 장치.

청구항 21

제 19 항에 있어서,

상기 암호화된 데이터를 포함하는 패킷을 송신하기 위한 자원들에 대한 요청을 상기 BS에 송신하기 위한 수단을 더 포함하는, 무선 통신을 위한 장치.

청구항 22

제 19 항에 있어서,

상기 패킷은 상기 네트워크가 상기 장치를 인증하기 위한 메커니즘을 더 포함하는, 무선 통신을 위한 장치.

청구항 23

제 19 항에 있어서,

상기 패킷의 송신 이후에, 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제하였음을 확인응답하는 메시지를 수신하기 위한 수단을 더 포함하는, 무선 통신을 위한 장치.

청구항 24

제 23 항에 있어서,

상기 메시지는 페이징 메시지를 포함하는, 무선 통신을 위한 장치.

청구항 25

제 24 항에 있어서,

상기 페이징 메시지의 송신은 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제하였다는 확인응답을 표시하는, 무선 통신을 위한 장치.

청구항 26

제 23 항에 있어서,

상기 메시지는 상기 장치가 상기 네트워크를 인증하기 위한 메커니즘을 포함하는, 무선 통신을 위한 장치.

청구항 27

제 19 항에 있어서,

상기 패킷의 송신 이후에, 상기 장치가 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제하였다는 ACK(acknowledgement)를 수신하지 않았음을 결정하기 위한 수단; 및

상기 패킷의 송신 이후에, 상기 결정에 대한 응답으로 상기 패킷을 재송신하기 위한 수단을 더 포함하는, 무선

통신을 위한 장치.

청구항 28

컴퓨터 실행가능한 코드가 저장된 비-일시적 컴퓨터 판독가능한 저장 매체로서,

상기 컴퓨터 실행가능한 코드는 하나 이상의 프로세서에 의해 실행되는 경우에 UE(user equipment)로 하여금,

BS(base station)를 통해 네트워크와의 보안 연결을 설정하게 하고 - 상기 보안 연결을 설정하는 것은 TAU(tracking area update) 또는 부착 프로시저(attach procedure) 중 적어도 하나를 포함함 -;

상기 보안 연결을 통해, 상기 UE가 상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용하기 위한 암호화 메커니즘을 협상하게 하고;

상기 암호화 메커니즘의 협상 이후에 유휴 모드에 진입하게 하고;

상기 유휴 모드로부터 전이한 후에 상기 네트워크에 송신될 데이터를 암호화하기 위하여 상기 협상된 암호화 메커니즘을 사용하게 하고; 그리고

상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 상기 암호화된 데이터를 포함하는 패킷을 상기 BS에 송신하게 하는, 비-일시적 컴퓨터 판독가능한 저장 매체.

청구항 29

BS(base station)에 의한 네트워크에서의 무선 통신을 위한 방법으로서,

암호화된 데이터를 포함하는 패킷을 UE(user equipment)와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 상기 UE로부터 수신하는 단계 - 상기 패킷은 상기 네트워크가 상기 UE를 인증하기 위한 메커니즘을 포함함 -;

상기 UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신하는 단계 - 상기 통신하는 것은 상기 메커니즘을 상기 네트워크 엔티티에 제공하는 것을 포함함 -;

상기 네트워크 엔티티가 상기 UE를 인증한 이후에 상기 암호화된 데이터를 암호화해제하기 위한 암호화해제 정보를 상기 네트워크 엔티티로부터 수신하는 단계; 및

상기 암호화된 데이터를 암호화해제하기 위하여 상기 암호화해제 정보를 사용하는 단계를 포함하는, BS에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 30

제 29 항에 있어서,

상기 암호화된 데이터를 성공적으로 암호화해제한 후에, 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제했음을 확인응답하는 메시지를 상기 UE로 송신하는 단계를 더 포함하는, BS에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 31

제 30 항에 있어서,

상기 메시지는 페이징 메시지를 포함하는, BS에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 32

제 31 항에 있어서,

상기 페이징 메시지의 송신은 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제했다는 확인응답을 표시하는, BS에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 33

제 30 항에 있어서,

상기 메시지는 상기 UE가 상기 네트워크를 인증하기 위한 메커니즘을 포함하는, BS에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 34

네트워크에서의 무선 통신을 위한 장치로서,

적어도 하나의 프로세서; 및

상기 적어도 하나의 프로세서에 커플링된 메모리를 포함하며,

상기 메모리는 상기 장치로 하여금,

암호화된 데이터를 포함하는 패킷을 UE(user equipment)와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 상기 UE로부터 수신하게 하고 - 상기 패킷은 상기 네트워크가 상기 UE를 인증하기 위한 메커니즘을 포함함 -;

상기 UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신하게 하고 - 상기 통신하는 것은 상기 메커니즘을 상기 네트워크 엔티티에 제공하는 것을 포함함 -;

상기 네트워크 엔티티가 상기 UE를 인증한 이후에 상기 암호화된 데이터를 암호화해제하기 위한 암호화해제 정보를 상기 네트워크 엔티티로부터 수신하게 하고; 그리고

상기 암호화된 데이터를 암호화해제하기 위하여 상기 암호화해제 정보를 사용하게 하도록,

상기 적어도 하나의 프로세서에 의해 실행될 수 있는 명령들을 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 35

제 34 항에 있어서,

상기 명령들은 상기 장치로 하여금, 상기 암호화된 데이터를 성공적으로 암호화해제 후에, BS가 상기 암호화된 데이터를 성공적으로 암호화해제했음을 확인응답하는 메시지를 상기 UE로 송신하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 네트워크에서의 무선 통신을 위한 장치.

청구항 36

제 35 항에 있어서,

상기 메시지는 페이징 메시지를 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 37

제 36 항에 있어서,

상기 페이징 메시지의 송신은 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제했다는 확인응답을 표시하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 38

제 35 항에 있어서,

상기 메시지는 상기 UE가 상기 네트워크를 인증하기 위한 메커니즘을 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 39

네트워크에서의 무선 통신을 위한 장치로서,

암호화된 데이터를 포함하는 패킷을 UE(user equipment)와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 상기 UE로부터 수신하기 위한 수단 - 상기 패킷은 상기 네트워크가 상기 UE를 인증하기 위한 메커니즘을 포함함 -;

상기 UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신하기 위한 수단 - 상기 통신하는 것은 상기 메커니즘을 상기 네트워크 엔티티에 제공하는 것을 포함함 -;

상기 네트워크 엔티티가 상기 UE를 인증한 이후에 상기 암호화된 데이터를 암호화해제하기 위한 암호화해제 정보를 상기 네트워크 엔티티로부터 수신하기 위한 수단; 및

상기 암호화된 데이터를 암호화해제하기 위하여 상기 암호화해제 정보를 사용하기 위한 수단을 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 40

제 39 항에 있어서,

상기 암호화된 데이터를 성공적으로 암호화해제한 후에, 상기 장치가 상기 암호화된 데이터를 성공적으로 암호화해제했음을 확인응답하는 메시지를 상기 UE로 송신하기 위한 수단을 더 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 41

제 40 항에 있어서,

상기 메시지는 페이징 메시지를 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 42

제 41 항에 있어서,

상기 페이징 메시지의 송신은 상기 장치가 상기 암호화된 데이터를 성공적으로 암호화해제했다는 확인응답을 표시하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 43

제 40 항에 있어서,

상기 메시지는 상기 UE가 상기 네트워크를 인증하기 위한 메커니즘을 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 44

컴퓨터 실행가능한 코드가 저장된 비-일시적 컴퓨터 판독가능한 저장 매체로서,

상기 컴퓨터 실행가능한 코드는 하나 이상의 프로세서에 의해 실행되는 경우에 네트워크의 BS(base station)로 하여금,

암호화된 데이터를 포함하는 패킷을 UE(user equipment)와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 상기 UE로부터 수신하게 하고 - 상기 패킷은 상기 네트워크가 상기 UE를 인증하기 위한 메커니즘을 포함함 -;

상기 UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신하게 하고 - 상기 통신하는 것은 상기 메커니즘을 상기 네트워크 엔티티에 제공하는 것을 포함함 -;

상기 네트워크 엔티티가 상기 UE를 인증한 이후에 상기 암호화된 데이터를 암호화해제하기 위한 암호화해제 정보를 상기 네트워크 엔티티로부터 수신하게 하고; 그리고

상기 암호화된 데이터를 암호화해제하기 위하여 상기 암호화해제 정보를 사용하게 하는, 비-일시적 컴퓨터 판독가능한 저장 매체.

청구항 45

네트워크 엔티티에 의한 네트워크에서의 무선 통신을 위한 방법으로서,

BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하는 단계;

상기 보안 연결을 통해, 상기 UE가 상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용할 암호화 메커니즘을 협상하는 단계;

상기 UE의 인증을 수행하기 위하여 상기 BS와 통신하는 단계 - 암호화된 데이터는 상기 UE로부터 상기 BS에 의해 패킷에서 수신됨 - ; 및

상기 UE의 인증 후에,

상기 UE가 상기 네트워크를 인증하기 위한 적어도 하나의 메커니즘을 상기 BS에 제공하는 단계;

상기 암호화된 데이터를 암호화해제하기 위한 암호화해제 정보를 상기 BS로 제공하는 단계; 및

상기 암호화해제 정보를 사용하여 암호화해제된 데이터를 상기 BS로부터 수신하는 단계를 포함하는, 네트워크 엔티티에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 46

제 45 항에 있어서,

상기 협상하는 단계는,

비연결형 셋업에 대한 요청을 상기 UE로부터 수신하는 단계 - 상기 요청은 상기 UE에 의해 지원되는 하나 또는 그 초과의 암호화 메커니즘들을 표시함 - ; 및

상기 지원되는 암호화 메커니즘들 중 적어도 하나를 표시하는 응답을 송신하는 단계를 포함하는, 네트워크 엔티티에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 47

제 45 항에 있어서,

상기 네트워크가 상기 UE를 인증하기 위한 적어도 하나의 메커니즘을 상기 패킷에서 상기 BS로부터 수신하는 단계; 및

상기 UE를 인증하기 위해서 상기 적어도 하나의 메커니즘을 사용하는 단계를 더 포함하는, 네트워크 엔티티에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 48

네트워크에서의 무선 통신을 위한 장치로서,

적어도 하나의 프로세서; 및

상기 적어도 하나의 프로세서에 커플링된 메모리를 포함하며,

상기 메모리는 상기 장치로 하여금,

BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하게 하고;

상기 보안 연결을 통해, 상기 UE가 상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용할 암호화 메커니즘을 협상하게 하고;

상기 UE의 인증을 수행하기 위하여 상기 BS와 통신하게 하고 - 암호화된 데이터는 상기 UE로부터 상기 BS에 의해 패킷에서 수신됨 - ; 그리고

상기 UE의 인증 후에,

상기 UE가 상기 네트워크를 인증하기 위한 적어도 하나의 메커니즘을 상기 BS에 제공하게 하고;

상기 암호화된 데이터를 암호화해제하기 위한 암호화해제 정보를 상기 BS로 제공하게 하고; 그리고

상기 암호화해제 정보를 사용하여 암호화해제된 데이터를 상기 BS로부터 수신하게 하도록,

상기 적어도 하나의 프로세서에 의해 실행될 수 있는 명령들을 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 49

제 48 항에 있어서,

비연결형 셋업에 대한 요청을 상기 UE로부터 수신하고- 상기 요청은 상기 UE에 의해 지원되는 하나 또는 그 초과의 암호화 메커니즘들을 표시함 - ; 그리고

상기 지원되는 암호화 메커니즘들 중 적어도 하나를 표시하는 응답을 송신함으로써,

상기 명령들은 상기 장치로 하여금 암호화 메커니즘을 협상하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 네트워크에서의 무선 통신을 위한 장치.

청구항 50

제 48 항에 있어서,

상기 명령들은 상기 장치로 하여금

상기 네트워크가 상기 UE를 인증하기 위한 적어도 하나의 메커니즘을 상기 패킷에서 상기 BS로부터 수신하게 하고; 그리고

상기 UE를 인증하기 위해서 상기 적어도 하나의 메커니즘을 사용하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 네트워크에서의 무선 통신을 위한 장치.

청구항 51

네트워크에서의 무선 통신을 위한 장치로서,

BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하기 위한 수단;

상기 보안 연결을 통해, 상기 UE가 상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용할 암호화 메커니즘을 협상하기 위한 수단;

상기 UE의 인증을 수행하기 위하여 상기 BS와 통신하기 위한 수단 - 암호화된 데이터는 상기 UE로부터 상기 BS에 의해 패킷에서 수신됨 - ; 및

상기 UE의 인증 후에,

상기 UE가 상기 네트워크를 인증하기 위한 적어도 하나의 메커니즘을 상기 BS에 제공하기 위한 수단;

상기 암호화된 데이터를 암호화해제하기 위한 암호화해제 정보를 상기 BS로 제공하기 위한 수단; 및

상기 암호화해제 정보를 사용하여 암호화해제된 데이터를 상기 BS로부터 수신하기 위한 수단을 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 52

제 51 항에 있어서,

상기 협상하기 위한 수단은,

비연결형 셋업에 대한 요청을 상기 UE로부터 수신하기 위한 수단 - 상기 요청은 상기 UE에 의해 지원되는 하나 또는 그 초과의 암호화 메커니즘들을 표시함 - ; 및

상기 지원되는 암호화 메커니즘들 중 적어도 하나를 표시하는 응답을 송신하기 위한 수단을 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 53

제 51 항에 있어서,

상기 네트워크가 상기 UE를 인증하기 위한 적어도 하나의 메커니즘을 상기 패킷에서 상기 BS로부터 수신하기 위한 수단; 및

상기 UE를 인증하기 위해서 상기 적어도 하나의 메커니즘을 사용하기 위한 수단을 더 포함하는, 네트워크에서의

무선 통신을 위한 장치.

청구항 54

컴퓨터 실행가능한 코드가 저장된 비-일시적 컴퓨터 판독가능한 저장 매체로서,

상기 컴퓨터 실행가능한 코드는 하나 이상의 프로세서에 의해 실행되는 경우에 네트워크의 네트워크 엔티티로 하여금,

BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하게 하고;

상기 보안 연결을 통해, 상기 UE가 상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용할 암호화 메커니즘을 협상하게 하고;

상기 UE의 인증을 수행하기 위하여 상기 BS와 통신하게 하고 - 암호화된 데이터는 상기 UE로부터 상기 BS에 의해 패킷에서 수신됨 - ; 및

상기 UE의 인증 후에,

상기 UE가 상기 네트워크를 인증하기 위한 적어도 하나의 메커니즘을 상기 BS에 제공하게 하고;

상기 암호화된 데이터를 암호화해제하기 위한 암호화해제 정보를 상기 BS로 제공하게 하고; 그리고

상기 암호화해제 정보를 사용하여 암호화해제된 데이터를 상기 BS로부터 수신하게 하는, 비-일시적 컴퓨터 판독가능한 저장 매체.

청구항 55

네트워크 엔티티에 의한 네트워크에서의 무선 통신을 위한 방법으로서,

BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하는 단계 - 상기 보안 연결을 설정하는 것은 TAU(tracking area update) 또는 부착 프로시저(attach procedure) 중 적어도 하나를 포함함 -;

상기 보안 연결을 통해, 상기 UE가 상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용할 암호화 메커니즘을 협상하는 단계;

상기 UE의 인증을 수행하기 위하여 상기 BS와 통신하는 단계 - 암호화된 데이터는 상기 UE로부터 상기 BS에 의해 패킷에서 수신됨 - ;

상기 BS로부터 상기 암호화된 데이터를 수신하는 단계; 및

상기 암호화된 데이터를 암호화해제하기 위해서 암호화해제 정보를 사용하는 단계를 포함하는, 네트워크 엔티티에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 56

제 55 항에 있어서,

상기 암호화 메커니즘을 협상하는 단계는,

비연결형 셋업에 대한 요청을 상기 UE로부터 수신하는 단계 - 상기 요청은 상기 UE에 의해 지원되는 하나 또는 그 초과의 암호화 메커니즘들을 표시함 - ; 및

상기 지원되는 암호화 메커니즘들 중 적어도 하나를 표시하는 응답을 송신하는 단계를 포함하는, 네트워크 엔티티에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 57

제 55 항에 있어서,

상기 네트워크가 상기 UE를 인증하기 위한 적어도 하나의 메커니즘을 상기 패킷에서 상기 BS로부터 수신하는 단계; 및

상기 UE를 인증하기 위해서 상기 적어도 하나의 메커니즘을 사용하는 단계를 더 포함하는, 네트워크 엔티티에

의한 네트워크에서의 무선 통신을 위한 방법.

청구항 58

제 55 항에 있어서,

상기 UE의 인증 후에, 상기 UE가 상기 네트워크를 인증하기 위한 적어도 하나의 메커니즘을 상기 BS에 제공하는 단계를 더 포함하는, 네트워크 엔티티에 의한 네트워크에서의 무선 통신을 위한 방법.

청구항 59

네트워크에서의 무선 통신을 위한 장치로서,

적어도 하나의 프로세서; 및

상기 적어도 하나의 프로세서에 커플링된 메모리를 포함하며,

상기 메모리는 상기 장치로 하여금,

BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하게 하고 - 상기 보안 연결을 설정하는 것은 TAU(tracking area update) 또는 부착 프로시저(attach procedure) 중 적어도 하나를 포함함 -;

상기 보안 연결을 통해, 상기 UE가 상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용할 암호화 메커니즘을 협상하게 하고;

상기 UE의 인증을 수행하기 위하여 상기 BS와 통신하게 하고 - 암호화된 데이터는 상기 UE로부터 상기 BS에 의해 패킷에서 수신됨 - ;

상기 BS로부터 상기 암호화된 데이터를 수신하게 하고; 그리고

상기 암호화된 데이터를 암호화해제하기 위해서 암호화해제 정보를 사용하게 하도록,

상기 적어도 하나의 프로세서에 의해 실행될 수 있는 명령들을 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 60

제 59 항에 있어서,

비연결형 셋업에 대한 요청을 상기 UE로부터 수신하고 - 상기 요청은 상기 UE에 의해 지원되는 하나 또는 그 초과의 암호화 메커니즘들을 표시함 - ; 및

상기 지원되는 암호화 메커니즘들 중 적어도 하나를 표시하는 응답을 송신함으로써,

상기 명령들은 상기 장치로 하여금 암호화 메커니즘을 협상하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 네트워크에서의 무선 통신을 위한 장치.

청구항 61

제 59 항에 있어서,

상기 명령들은 상기 장치로 하여금

상기 네트워크가 상기 UE를 인증하기 위한 적어도 하나의 메커니즘을 상기 패킷에서 상기 BS로부터 수신하게 하고; 그리고

상기 UE를 인증하기 위해서 상기 적어도 하나의 메커니즘을 사용하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 네트워크에서의 무선 통신을 위한 장치.

청구항 62

제 61 항에 있어서,

상기 명령들은 상기 장치로 하여금 상기 UE의 인증 후에, 상기 UE가 상기 네트워크를 인증하기 위한 적어도 하나의 메커니즘을 상기 BS에 제공하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 네트

워크에서의 무선 통신을 위한 장치.

청구항 63

네트워크에서의 무선 통신을 위한 장치로서,

BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하기 위한 수단 – 상기 보안 연결을 설정하는 것은 TAU(tracking area update) 또는 부착 프로시저(attach procedure) 중 적어도 하나를 포함함 –;

상기 보안 연결을 통해, 상기 UE가 상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용할 암호화 메커니즘을 협상하기 위한 수단;

상기 UE의 인증을 수행하기 위하여 상기 BS와 통신하기 위한 수단 – 암호화된 데이터는 상기 UE로부터 상기 BS에 의해 패킷에서 수신됨 – ;

상기 BS로부터 상기 암호화된 데이터를 수신하기 위한 수단; 및

상기 암호화된 데이터를 암호화해제하기 위해서 암호화해제 정보를 사용하기 위한 수단을 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 64

제 63 항에 있어서,

상기 암호화 메커니즘을 협상하기 위한 수단은,

비연결형 셋업에 대한 요청을 상기 UE로부터 수신하기 위한 수단 – 상기 요청은 상기 UE에 의해 지원되는 하나 또는 그 초과의 암호화 메커니즘들을 표시함 – ; 및

상기 지원되는 암호화 메커니즘들 중 적어도 하나를 표시하는 응답을 송신하기 위한 수단을 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 65

제 63 항에 있어서,

상기 네트워크가 상기 UE를 인증하기 위한 적어도 하나의 메커니즘을 상기 패킷에서 상기 BS로부터 수신하기 위한 수단; 및

상기 UE를 인증하기 위해서 상기 적어도 하나의 메커니즘을 사용하기 위한 수단을 더 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 66

제 65 항에 있어서,

상기 UE의 인증 후에, 상기 UE가 상기 네트워크를 인증하기 위한 적어도 하나의 메커니즘을 상기 BS에 제공하기 위한 수단을 더 포함하는, 네트워크에서의 무선 통신을 위한 장치.

청구항 67

컴퓨터 실행가능한 코드가 저장된 비-일시적 컴퓨터 판독가능한 저장 매체로서,

상기 컴퓨터 실행가능한 코드는 하나 이상의 프로세서에 의해 실행되는 경우에 네트워크의 네트워크 엔티티로 하여금,

BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하게 하고 – 상기 보안 연결을 설정하는 것은 TAU(tracking area update) 또는 부착 프로시저(attach procedure) 중 적어도 하나를 포함함 –;

상기 보안 연결을 통해, 상기 UE가 상기 UE와 상기 네트워크 사이의 설정된 데이터 라디오 베어러 없이 데이터를 송신하는데 사용할 암호화 메커니즘을 협상하게 하고;

상기 UE의 인증을 수행하기 위하여 상기 BS와 통신하게 하고 – 암호화된 데이터는 상기 UE로부터 상기 BS에 의해 패킷에서 수신됨 – ;

상기 BS로부터 상기 암호화된 데이터를 수신하게 하고; 그리고

상기 암호화된 데이터를 암호화해제하기 위해서 암호화해제 정보를 사용하게 하는, 비-일시적 컴퓨터 판독가능한 저장 매체.

발명의 설명

기 술 분 야

[0001] 관련 출원(들)에 대한 상호-참조

[0002] [0001] 본 출원은 2014년 9월 23일자로 출원된 미국 가출원 일련 번호 제62/054,271호 및 2015년 9월 22일자로 출원된 미국 출원 일련 번호 제14/862,124호의 이익을 주장하고, 그에 의해 상기 출원들 둘 다는 그 전체 내용이 인용에 의해 명백하게 포함된다.

[0003] [0002] 본 개시물의 특정 양상들은 일반적으로, 감소된 시그널링 오버헤드를 가지는 UE(user equipment)로부터의 보안 업링크 데이터 송신들을 수행하기 위한 방법들 및 장치에 관한 것이다.

배 경 기 술

[0004] [0003] 무선 통신 시스템들은 음성, 데이터 등과 같은 다양한 타입들의 통신 컨텐츠를 제공하기 위하여 폭넓게 전개된다. 이 시스템들은 이용가능한 시스템 자원들(예컨대, 대역폭 및 송신 전력)을 공유함으로써 다수의 사용자들과의 통신을 지원할 수 있는 다중-액세스(multiple-access) 시스템들일 수 있다. 이러한 다중-액세스 시스템들의 예들은 CDMA(Code Division Multiple Access) 시스템들, TDMA(Time Division Multiple Access) 시스템들, FDMA(Frequency Division Multiple Access) 시스템들, 3GPP(3^{rd} Generation Partnership Project) LTE(Long Term Evolution) 시스템들, LTE-A(Long Term Evolution Advanced) 시스템들 및 OFDMA(Orthogonal Frequency Division Multiple Access) 시스템들을 포함한다.

[0005] [0004] 일반적으로, 무선 다중-액세스 통신 시스템은 다수의 무선 단말들에 대한 통신을 동시에 지원할 수 있다. 각각의 단말은 순방향 및 역방향 링크들 상에서의 송신들을 통해 하나 또는 그 초과의 기지국들과 통신한다. 순방향 링크(또는 다운링크)는 기지국들로부터 단말들로의 통신 링크를 지칭하고, 역방향 링크(또는 업링크)는 단말들로부터 기지국들로의 통신 링크를 지칭한다. 이 통신 링크는 단일-입력 단일-출력, 다중-입력 단일-출력 또는 MIMO(multiple-input multiple-output) 시스템을 통해 설정될 수 있다.

[0006] [0005] MTC(machine-type communications) 디바이스들과 같은 특정 타입들의 디바이스들은 단지 전송할 작은 양의 데이터를 가질 수 있으며, 그 데이터를 비교적 드물게 전송할 수 있다. 이러한 경우들에서, 네트워크 연결을 설정하는데 필요한 오버헤드의 양은 연결 동안 전송되는 실제 데이터에 비해 아주 높을 수 있다.

발명의 내용

[0007] [0006] 본 개시물의 특정 양상들은 UE(user equipment)에 의한 무선 통신을 위한 방법을 제공한다. 방법은 일반적으로, BS(base station)를 통해 네트워크와의 보안 연결을 설정하는 단계, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하는 단계, 암호화 메커니즘의 협상 이후에 유휴 모드에 진입하는 단계, 네트워크에 포워딩될 데이터를 암호화하기 위하여 협상된 암호화 메커니즘을 사용하는 단계, 및 전체 RRC 연결을 설정하지 않고 암호화된 데이터를 포함하는 패킷을 BS에 송신하는 단계를 포함한다.

[0008] [0007] 본 개시물의 특정 양상들은 UE(user equipment)에 의한 무선 통신을 위한 장치를 제공한다. 장치는 일반적으로, BS(base station)를 통해 네트워크와의 보안 연결을 설정하고, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하고, 암호화 메커니즘의 협상 이후에 유휴 모드에 진입하고, 네트워크에 송신될 데이터를 암호화하기 위하여 협상된 암호화 메커니즘을 사용하고, 그리고 전체 RRC 연결을 설정하지 않고 암호화된 데이터를 포함하는 패킷을 BS에 송신하도록 구성되는 적어도 하나의 프로세서, 및 적어도 하나의 프로세서에 커플링된 메모리를 포함한다.

[0009] [0008] 본 개시물의 특정 양상들은 UE(user equipment)에 의한 무선 통신을 위한 장치를 제공한다. 장치는 일반적으로, BS(base station)를 통해 네트워크와의 보안 연결을 설정하기 위한 수단, 보안 연결을 통해, 전체

RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하기 위한 수단, 암호화 메커니즘의 협상 이후에 유휴 모드에 진입하기 위한 수단, 네트워크에 포워딩될 데이터를 암호화하기 위하여 협상된 암호화 메커니즘을 사용하기 위한 수단, 및 전체 RRC 연결을 설정하지 않고 암호화된 데이터를 포함하는 패킷을 BS에 송신하기 위한 수단을 포함한다.

[0010] [0009] 본 개시물의 특정 양상들은 UE(user equipment)에 의한 무선 통신을 위한 컴퓨터 판독가능한 매체를 제공한다. 컴퓨터 판독가능한 매체는 일반적으로, 적어도 하나의 프로세서에 의해 실행되는 경우 UE로 하여금: BS(base station)를 통해 네트워크와의 보안 연결을 설정하게 하고, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하게 하고, 암호화 메커니즘의 협상 이후에 유휴 모드에 진입하게 하고, 네트워크에 송신될 데이터를 암호화하기 위하여 협상된 암호화 메커니즘을 사용하게 하고, 그리고 전체 RRC 연결을 설정하지 않고 암호화된 데이터를 포함하는 패킷을 BS에 송신하게 하는 코드를 포함한다.

[0011] [0010] 본 개시물의 특정 양상들은 BS(base station)에 의한 무선 통신을 위한 방법을 제공한다. 방법은 일반적으로, 암호화된 데이터를 포함하는 패킷을 전체 RRC(radio resource control) 연결을 설정하지 않은 UE(user equipment)로부터 수신하는 단계, UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신하는 단계, 네트워크 엔티티가 UE를 인증한 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 네트워크 엔티티로부터 수신하는 단계, 및 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용하는 단계를 포함한다.

[0012] [0011] 본 개시물의 특정 양상들은 BS(base station)에 의한 무선 통신을 위한 장치를 제공한다. 장치는 일반적으로, 암호화된 데이터를 포함하는 패킷을 전체 RRC(radio resource control) 연결을 설정하지 않은 UE(user equipment)로부터 수신하고, UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신하고, 네트워크 엔티티가 UE를 인증한 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 네트워크 엔티티로부터 수신하고, 그리고 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용하도록 구성되는 적어도 하나의 프로세서, 및 적어도 하나의 프로세서에 커플링된 메모리를 포함한다.

[0013] [0012] 본 개시물의 특정 양상들은 BS(base station)에 의한 무선 통신을 위한 장치를 제공한다. 장치는 일반적으로, 암호화된 데이터를 포함하는 패킷을 전체 RRC(radio resource control) 연결을 설정하지 않은 UE(user equipment)로부터 수신하기 위한 수단, UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신하기 위한 수단, 네트워크 엔티티가 UE를 인증한 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 네트워크 엔티티로부터 수신하기 위한 수단, 및 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용하기 위한 수단을 포함한다.

[0014] [0013] 본 개시물의 특정 양상들은 BS(base station)에 의한 무선 통신을 위한 컴퓨터 판독가능한 매체를 제공한다. 컴퓨터 판독가능한 매체는 일반적으로, 적어도 하나의 프로세서에 의해 실행되는 경우 BS로 하여금: 암호화된 데이터를 포함하는 패킷을 전체 RRC(radio resource control) 연결을 설정하지 않은 UE(user equipment)로부터 수신하게 하고, UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신하게 하고, 네트워크 엔티티가 UE를 인증한 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 네트워크 엔티티로부터 수신하게 하고, 그리고 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용하게 하는 코드를 포함한다.

[0015] [0014] 본 개시물의 특정 양상들은 네트워크 엔티티에 의한 무선 통신을 위한 방법을 제공한다. 방법은 일반적으로, BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하는 단계, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하는 단계, UE의 인증을 수행하기 위하여 BS와 통신하는 단계 - 암호화된 데이터는 UE로부터 BS에 의해 패킷에서 수신됨 - , 암호화된 데이터를 BS로부터 수신하는 단계, 및 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용하는 단계를 포함한다.

[0016] [0015] 본 개시물의 특정 양상들은 네트워크 엔티티에 의한 무선 통신을 위한 장치를 제공한다. 장치는 일반적으로, BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하고, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하고, UE의 인증을 수행하기 위하여 BS와 통신하고 - 암호화된 데이터는 UE로부터 BS에 의해 패킷에서 수신됨 - , 암호화된 데이터를 BS로부터 수신하고, 그리고 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용하도록 구성되는 적어도 하나의 프로세서, 및 적어도 하나의 프로세서에 커플링된 메모리를 포함한다.

[0017] [0016] 본 개시물의 특정 양상들은 네트워크 엔티티에 의한 무선 통신을 위한 장치를 제공한다. 장치는 일반적으로, BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하기 위한 수단, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하기 위한 수단, UE의 인증을 수행하기 위하여 BS와 통신하기 위한 수단 – 암호화된 데이터는 UE로부터 BS에 의해 패킷에서 수신됨 – , 암호화된 데이터를 BS로부터 수신하기 위한 수단, 및 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용하기 위한 수단을 포함한다.

[0018] [0017] 본 개시물의 특정 양상들은 네트워크 엔티티에 의한 무선 통신을 위한 컴퓨터 판독가능한 매체를 제공한다. 컴퓨터 판독가능한 매체는 일반적으로, 적어도 하나의 프로세서에 의해 실행되는 경우 네트워크 엔티티로 하여금: BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하게 하고, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하게 하고, UE의 인증을 수행하기 위하여 BS와 통신하게 하고 – 암호화된 데이터는 UE로부터 BS에 의해 패킷에서 수신됨 – , 암호화된 데이터를 BS로부터 수신하게 하고 그리고 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용하게 하는 코드를 포함한다.

[0019] [0018] 본 개시물의 특정 양상들은 네트워크 엔티티에 의한 무선 통신을 위한 방법을 제공한다. 방법은 일반적으로, BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하는 단계, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하는 단계, UE의 인증을 수행하기 위하여 암호화된 데이터를 포함하는 패킷을 UE로부터 수신한 BS와 통신하는 단계, UE의 인증 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 BS에 제공하는 단계, 및 암호화해제 정보를 사용하여 암호화해제된 데이터를 BS로부터 수신하는 단계를 포함한다.

[0020] [0019] 본 개시물의 특정 양상들은 네트워크 엔티티에 의한 무선 통신을 위한 장치를 제공한다. 장치는 일반적으로, BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하고, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하고, UE의 인증을 수행하기 위하여 BS와 통신하고 – 암호화된 데이터는 UE로부터 BS에 의해 패킷에서 수신됨 – , UE의 인증 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 BS에 제공하고, 그리고 암호화해제 정보를 사용하여 암호화해제된 데이터를 BS로부터 수신하도록 구성되는 적어도 하나의 프로세서, 및 적어도 하나의 프로세서에 커플링된 메모리를 포함한다.

[0021] [0020] 본 개시물의 특정 양상들은 네트워크 엔티티에 의한 무선 통신을 위한 장치를 제공한다. 장치는 일반적으로, BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하기 위한 수단, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하기 위한 수단, UE의 인증을 수행하기 위하여 BS와 통신하기 위한 수단 – 암호화된 데이터는 UE로부터 BS에 의해 패킷에서 수신됨 – , UE의 인증 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 BS에 제공하기 위한 수단, 및 암호화해제 정보를 사용하여 암호화해제된 데이터를 BS로부터 수신하기 위한 수단을 포함한다.

[0022] [0021] 본 개시물의 특정 양상들은 네트워크 엔티티에 의한 무선 통신을 위한 컴퓨터 판독가능한 매체를 제공한다. 컴퓨터 판독가능한 매체는 일반적으로, 적어도 하나의 프로세서에 의해 실행되는 경우 네트워크 엔티티로 하여금: BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정하게 하고, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하게 하고, UE의 인증을 수행하기 위하여 BS와 통신하게 하고 – 암호화된 데이터는 UE로부터 BS에 의해 패킷에서 수신됨 – , UE의 인증 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 BS에 제공하게 하고, 그리고 암호화해제 정보를 사용하여 암호화해제된 데이터를 BS로부터 수신하게 하는 코드를 포함한다.

[0023] [0022] 다른 실시예들은, 제한없이, 적어도 하나의 프로세서에 의해 실행되는 경우 본원에서 개시되는 하나 또는 그 초과의 양상들을 수행하는 코드를 포함하는 컴퓨터 판독가능한 매체뿐만 아니라, 본원에서 개시되는 양상들 중 하나 또는 그 초과의 양상들을 구현하도록 구성되는 프로세서 및 메모리를 가지는 장치를 포함한다.

도면의 간단한 설명

[0025] [0023] 개시물의 양상들 및 실시예들은 유사한 참조 부호들이 전체에서 대응하게 식별하는 도면들과 함께 취해지는 경우 아래에서 기술되는 상세한 설명으로부터 더 명백해질 것이다.

[0024] 도 1은 본 개시물의 특정 양상들에 따른 예시적 다중 액세스 무선 통신 시스템을 예시한다.

[0025] 도 2는 본 개시물의 특정 양상들에 따른 액세스 포인트 및 사용자 단말의 블록도를 예시한다.

[0026] 도 3은 본 개시물의 특정 양상들에 따른, 무선 디바이스에서 활용될 수 있는 다양한 컴포넌트들을 예시한다.

[0027] 도 4는 본 개시물의 특정 양상들에 따른, LTE RACH 경합-기반 프로시저에 대한 메시지 흐름을 예시한다.

[0028] 도 5는 본 개시물의 특정 양상들에 따른, UE에 의해 수행될 수 있는 예시적 동작들을 예시한다.

[0029] 도 6은 본 개시물의 특정 양상들에 따른, BS(base station)에 의해 수행될 수 있는 예시적 동작들을 예시한다.

[0030] 도 7은 본 개시물의 특정 양상들에 따른, 네트워크 엔티티에 의해 수행될 수 있는 예시적 동작들을 예시한다.

[0031] 도 8은 본 개시물의 특정 양상들에 따른, 암호화 메커니즘의 협상 및 비연결형 송신의 셋업에 대한 예시적 호 흐름을 예시한다.

[0032] 도 9는 본 개시물의 특정 양상들에 따른, 보안 비연결형 업링크 데이터 송신(들)에 대한 예시적 호 흐름을 예시한다.

발명을 실시하기 위한 구체적인 내용

[0026] [0033] 본 개시물의 양상들은 특정 디바이스들(예컨대, MTC(machine-type communications) 디바이스들, eMTC(enhanced MTC) 디바이스들 등)이 데이터의 송신 이전에 보안 연결을 설정할 필요성 없이 데이터를 송신하게 허용할 수 있는 기법들을 제공한다. 아래에서 더 상세하게 설명될 바와 같이, 이 기법들은 비연결형 송신 및 후속하는 보안 비연결형 업링크 송신들에 대한 셋업의 부분으로서 암호화 메커니즘의 협상을 수반할 수 있다.

[0027] [0034] 본 개시물의 다양한 양상들은 첨부한 도면들을 참조하여 이하에서 더 완전하게 설명된다. 그러나, 본 개시물은 많은 상이한 형태들로 구현될 수 있으며, 본 개시물의 전반에 걸쳐 제시되는 임의의 특정 구조 또는 기능으로 제한되는 것으로 해석되지 않아야 한다. 오히려, 이 양상들은, 본 개시물이 철저하고 완전할 것이며, 개시물의 범위를 당해 기술 분야의 당업자들에게 완전히 전달하도록 제공된다. 본원에서의 교시 사항들에 기초하여, 당해 기술 분야의 당업자는 개시물의 범위가 개시물의 임의의 다른 양상과 독립적으로 구현되든 또는 임의의 다른 양상과 결합하여 구현되든 간에, 본원에서 개시되는 개시물의 임의의 양상을 커버하는 것으로 의도된다는 것을 인식하여야 한다. 예컨대, 본원에서 기술되는 많은 양상들을 사용하여 장치가 구현될 수 있거나 또는 방법이 실시될 수 있다. 또한, 개시물의 범위는 본원에서 기술되는 개시물의 다양한 양상들과 더불어 또는 그 이외에, 다른 구조, 기능, 또는 구조 및 기능을 사용하여 실시되는 이러한 장치 또는 방법을 커버하는 것으로 의도된다. 본원에서 개시되는 개시물의 임의의 양상은 청구항의 하나 또는 그 초과의 엘리먼트들에 의해 구현될 수 있다는 것이 이해되어야 한다.

[0028] [0035] "예시적"이라는 단어는 본원에서 "예, 예시 또는 예증으로서 제공되는"의 의미로 사용된다. "예시적"으로서 본원에서 설명된 임의의 양상은 다른 양상들에 비해 바람직하거나 유익한 것으로 반드시 해석되어야 하는 것은 아니다.

[0029] [0036] 특정 양상들이 본원에서 설명되지만, 이 양상들의 많은 변형들 및 치환들은 개시의 범위 내에 속한다. 바람직한 양상들의 일부 이익들 및 이점들이 언급되지만, 개시물의 범위는 특정 이익들, 용도들, 또는 목적들에 제한되는 것으로 의도되지 않는다. 오히려, 개시물의 양상들은 상이한 무선 기술들, 시스템 구성들, 네트워크들 및 송신 프로토콜들에 광범위하게 적용가능한 것으로 의도되며, 이들 중 일부는 바람직한 양상들의 도면들 및 다음의 설명에서 예로서 예시된다. 상세한 설명 및 도면들은 제한하는 것이 아니라 단지 개시물의 예시에 불과하고, 개시물의 범위는 첨부되는 청구항들 및 그 등가물들에 의해 정의된다.

[0030] [0037] 본원에서 설명되는 기법들은 다양한 무선 통신 네트워크들, 이를테면, CDMA(Code Division Multiple Access) 네트워크들, TDMA(Time Division Multiple Access) 네트워크들, FDMA(Frequency Division Multiple Access) 네트워크들, OFDMA(Orthogonal FDMA) 네트워크들 및 SC-FDMA(Single-Carrier FDMA) 네트워크들 등에

대해 사용될 수 있다. "네트워크들" 및 "시스템들"이라는 용어들은 종종 상호교환가능하게 사용된다. CDMA 네트워크는 UTRA(Universal Terrestrial Radio Access), CDMA 2000 등과 같은 라디오 기술을 구현할 수 있다. UTRA 는 W-CDMA(Wideband-CDMA) 및 LCR(Low Chip Rate)을 포함한다. CDMA2000은 IS-2000, IS-95, 및 IS-856 표준들을 커버한다. TDMA 네트워크는 GSM(Global System for Mobile Communications)과 같은 라디오 기술을 구현할 수 있다. OFDMA 네트워크는 라디오 기술, 이를테면, E-UTRA(Evolved UTRA), IEEE 802.11, IEEE 802.16, IEEE 802.20, 플래시-OFDM® 등을 구현할 수 있다. UTRA, E-UTRA, 및 GSM은 UMTS(Universal Mobile Telecommunication System)의 부분이다. LTE(Long Term Evolution) 및 LTE-A(LTE-Advanced)는 E-UTRA를 사용하는 UMTS의 최신 릴리스들이다. UTRA, E-UTRA, GSM, UMTS, 및 LTE는 3GPP("3rd Generation Partnership Project")라고 명명되는 기구로부터의 문서들에서 설명된다. CDMA2000은 3GPP2("3rd Generation Partnership Project 2")라고 명명되는 기구로부터의 문서들에서 설명된다. 간략함을 위하여, "LTE"는 LTE 및 LTE-A를 지칭한다.

[0031] [0038] SC-FDMA(single carrier frequency division multiple access)는 송신기 측에서 단일 캐리어 변조를 그리고 수신기 측에서 주파수 도메인 등화를 활용하는 송신 기법이다. SC-FDMA는 OFDMA 시스템의 것들과 유사한 성능 및 본질적으로 동일한 전반적 복잡도를 가진다. 그러나, SC-FDMA 신호는 그것의 고유한 단일 캐리어 구조로 인한 더 낮은 PAPR(peak-to-average power ratio)을 가진다. SC-FDMA는, 특히, 더 낮은 PAPR이 송신 전력 효율성에 관해 모바일 단말에 크게 유익한 업링크 통신들에서 큰 관심을 끈다. 그것은 3GPP LTE 및 이볼브드 UTRA에서 업링크 다중 액세스 방식에 대해 현재 작용하는 가정이다.

[0032] [0039] AP(access point)는 Node B, RNC(Radio Network Controller), eNodeB(eNB), BSC(Base Station Controller), BTS(Base Transceiver Station), BS(Base Station), TF(Transceiver Function), 라디오 라우터, 라디오 트랜시버, BSS(Basic Service Set), ESS(Extended Service Set), RBS(Radio Base Station) 또는 일부 다른 용어를 포함하거나, 이들로 구현되거나, 또는 이들로 알려져 있을 수 있다.

[0033] [0040] AT(access terminal)는, 액세스 단말, 가입자 스테이션, 가입자 유닛, 이동국, 원격국, 원격 단말, 원격 디바이스, 무선 디바이스, 디바이스, 사용자 단말, 사용자 에이전트, 사용자 디바이스, UE(user equipment), 사용자 스테이션, MTC(machine-type communications) 디바이스 또는 일부 다른 용어를 포함하거나, 이들로 구현되거나, 또는 이들로 알려져 있을 수 있다. MTC 디바이스들의 예들은 단일 배터리 충전에 대해 수년 동안 동작(가능하게는 실행되지 않음(unattended))하도록 예상될 수 있는 로봇들, 드론들, 다양한 무선 센서들, 모니터들, 검출기들, 미터들 또는 다른 타입 데이터 모니터링, 생성 또는 중계 디바이스들을 포함한다.

[0034] [0041] 일부 구현들에서, 액세스 단말은 셀룰러 전화, 스마트 폰, 코드리스 전화(cordless telephone), SIP(Session Initiation Protocol) 폰, WLL(wireless local loop) 스테이션, PDA(personal digital assistant), 태블릿, 넷북, 스마트북, 울트라북, 무선 연결 능력을 가지는 핸드헬드 디바이스, STA(Station) 또는 무선 모뎀에 연결되는 일부 다른 적합한 프로세싱 디바이스를 포함할 수 있다. 따라서, 본원에서 교시되는 하나 또는 그 초과의 양상들은 폰(예컨대, 셀룰러 폰, 스마트 폰), 컴퓨터(예컨대, 데스크탑), 휴대용 통신 디바이스, 휴대용 컴퓨팅 디바이스(예컨대, 랩탑, 개인용 데이터 보조기, 태블릿, 넷북, 스마트북, 울트라북), 엔터테인먼트 디바이스(예컨대, 음악 또는 비디오 디바이스, 게이밍 디바이스, 위성 라디오), 포지셔닝 시스템 디바이스(예컨대, GPS, Beidou, GLONASS, Galileo), 웨어러블 디바이스(예컨대, 스마트 워치, 스마트 손목밴드, 스마트 의류, 스마트 안경, 스마트 반지, 스마트 팔찌), 또는 무선 또는 유선 매체를 통해 통신하도록 구성되는 임의의 다른 적합한 디바이스에 통합될 수 있다. 일부 양상들에서, 노드는 무선 노드이다. 이러한 무선 노드는, 예컨대, 유선 또는 무선 통신 링크를 통해 네트워크(예컨대, 인터넷과 같은 WAN(wide area network) 또는 셀룰러 네트워크)에 대한 또는 이 네트워크로의 연결성을 제공할 수 있다.

[0035] [0042] 도 1은 본 개시물의 양상들이 실시될 수 있는, LTE 네트워크일 수 있는 다중 액세스 무선 통신 시스템을 도시한다.

[0036] [0043] 예시되는 바와 같이, AP(access point)(100)는 다수의 안테나 그룹들을 포함할 수 있는데, 하나의 그룹은 안테나들(104 및 106)을 포함하고, 또 다른 그룹은 안테나들(108 및 110)을 포함하며, 추가 그룹은 안테나들(112 및 114)을 포함한다. 도 1에서, 각각의 안테나 그룹에 대해 단지 두개의 안테나들만이 도시되지만, 더 많거나 또는 더 적은 안테나들이 각각의 안테나 그룹에 대해 활용될 수 있다. AT(access terminal)(116)는 안테나들(112 및 114)과 통신할 수 있으며, 여기서, 안테나들(112 및 114)은 순방향 링크(120) 상에서 AT(116)로 정보를 송신하며, 역방향 링크(118) 상에서 AT(116)로부터 정보를 수신한다. AT(122)는 안테나들(104 및 106)과 통신할 수 있으며, 여기서, 안테나들(104 및 106)은 순방향 링크(126) 상에서 AT(122)로 정보를 송신하며, 역방

향 링크(124) 상에서 AT(122)로부터 정보를 수신한다. FDD(Frequency Division Duplex) 시스템에서, 통신 링크들(118, 120, 124 및 126)은 통신을 위하여 상이한 주파수들을 사용할 수 있다. 예컨대, 순방향 링크(120)는 역방향 링크(118)에 의해 사용되는 것과는 상이한 주파수를 사용할 수 있다.

[0037] [0044] 각각의 그룹의 안테나들 및/또는 이들이 통신하도록 설계된 영역은 종종 AP의 섹터로 지칭된다. 본 개시물의 하나의 양상에서, 각각의 안테나 그룹은 AP(100)에 의해 커버되는 영역들의 섹터 내의 AT들로 통신하도록 설계될 수 있다.

[0038] [0045] AT(130)는 AP(100)와 통신할 수 있으며, 여기서, AP(100)로부터의 안테나들은 순방향 링크(132) 상에서 AT(130)로 정보를 송신하며, 역방향 링크(134) 상에서 AT(130)로부터 정보를 수신한다. AT들(116, 122 및 130)은 MTC 디바이스들일 수 있다.

[0039] [0046] 순방향 링크들(120 및 126) 상에서의 통신에서, AP(100)의 송신 안테나들은 상이한 AT들(116 및 122)에 대한 순방향 링크들의 신호-대-잡음비를 개선하기 위하여 빔포밍을 활용할 수 있다. 또한, 자신의 커버리지 전반에 랜덤하게 산재되어 있는 AT들에 송신하기 위하여 빔포밍을 사용하는 AP는 단일 안테나를 통해 자신의 모든 AT들에 송신하는 AP보다 이웃 셀들의 AT들에 더 적은 간섭을 야기한다.

[0040] [0047] 양상에 따라, 하나 또는 그 초과의 AT들(116, 122, 130) 및 AP(들)(100)는 코어 네트워크(도시되지 않음)와 통신할 수 있다. AP(100)는 S1 인터페이스에 의해 코어 네트워크(도시되지 않음)에 연결될 수 있다. 코어 네트워크는 MME(Mobility Management Entity)(예컨대, 도 8-9에 예시되는 바와 같음), HSS(Home Subscriber Server)(도시되지 않음), S-GW(Serving Gateway)(예컨대, 도 9에 예시되는 바와 같음) 및 P-GW(Packet Data Network) 게이트웨이(예컨대, 도 9에 예시되는 바와 같음)를 포함할 수 있다. MME는 AT와 코어 네트워크 사이의 시그널링을 프로세싱하는 제어 노드이다. MME는 또한 이동성 관리, 베어러 관리, 페이징 메시지들의 분배, 보안 제어, 인증, 게이트웨이 선택 등과 같은 다양한 기능들을 수행할 수 있다. HSS는 MME에 연결되고, AT의 인증 및 허가와 같은 다양한 기능들을 수행할 수 있으며, 위치 및 IP 정보를 MME에 제공할 수 있다. S-GW는 사용자 IP 패킷들을 P-GW에 전달할 수 있으며, 패킷 라우팅 및 포워딩, 이동성 앵커링, 패킷 버퍼링, 네트워크-트리거링된 서비스들의 개시 등과 같은 다양한 기능들을 수행할 수 있다. P-GW는 운영자의 IP 서비스들(이제 도시됨)에 연결되며, UE IP 어드레스 할당뿐만 아니라 다른 기능들을 제공할 수 있다. 운영자의 IP 서비스들은 인터넷(Internet), 인트라넷(Intranet), IMS(IP Multimedia Subsystem) 및 PSS(PS Streaming Service)를 포함할 수 있다.

[0041] [0048] 본원에서 제시되는 특정 양상들에 따라, 아래에서 더 상세하게 설명될 바와 같이, AT들(예컨대, 도 1에 예시됨)은 데이터의 송신 이전에 AP를 통해 네트워크(예컨대, 도 8-9에 예시되는 MME, S-GW, P-GW 등)로의 보안 연결을 설정할 필요성 없이 데이터를 송신할 수 있다.

[0042] [0049] 도 2는 본 개시물의 양상들에 따른, MIMO(multiple-input multiple-output) 시스템(200) 내의 송신기 시스템(210)(예컨대, AP로 또한 알려져 있음) 및 수신기 시스템(250)(예컨대, AT로 또한 알려져 있음)의 양상의 블록도를 예시한다. 송신기 시스템(210)은 도 6을 참조하여 아래에서 설명되는 BS-측 동작들을 수행하도록 구성될 수 있는 반면, 수신기 시스템(250)은 도 5를 참조하여 아래에서 설명되는 UE-측 동작들을 수행하도록 구성될 수 있다.

[0043] [0050] 시스템(210) 및 시스템(250) 각각은 송신 및 수신 둘 다에 대한 능력들을 가진다. 시스템(210) 또는 시스템(250)이 송신하고 있는지, 수신하고 있는지 아니면 동시에 송신 및 수신하고 있는지는 애플리케이션에 종속된다. 송신기 시스템(210)에서, 다수의 데이터 스트림들에 대한 트래픽 데이터는 데이터 소스(212)로부터 송신(TX)데이터 프로세서(214)로 제공된다.

[0044] [0051] 본 개시물의 하나의 양상에서, 각각의 데이터 스트림은 각각의 송신 안테나 상에서 송신될 수 있다. TX 데이터 프로세서(214)는 각각의 데이터 스트림에 대해 선택된 특정 코딩 방식에 기초하여 각각의 데이터 스트림에 대한 트래픽 데이터를 포맷, 코딩, 및 인터리빙하여, 코딩된 데이터를 제공한다.

[0045] [0052] 각각의 데이터 스트림에 대한 코딩된 데이터는 OFDM 기법들을 사용하여 파일럿 데이터로 멀티플렉싱될 수 있다. 파일럿 데이터는 전형적으로, 알려진 방식으로 프로세싱되는 알려진 데이터 패턴이며, 채널 응답을 추정하기 위하여 수신기 시스템에서 사용될 수 있다. 그 다음, 각각의 데이터 스트림에 대한 멀티플렉싱된 파일럿 및 코딩된 데이터는 변조 심볼들을 제공하기 위하여 그 데이터 스트림에 대해 선택된 특정 변조 방식(예컨대, BPSK, QPSK, M-PSK 또는 M-QAM)에 기초하여 변조(예컨대, 심볼 맵핑)된다. 각각의 데이터 스트림에 대한 데이터 레이트, 코딩, 및 변조는 제어기/프로세서(230)에 의해 수행되는 명령들에 의해 결정될 수 있다. 메모

리(232)는 송신 시스템(210)에 대한 데이터 및 소프트웨어/펌웨어를 저장할 수 있다.

[0046] [0053] 그 다음, 모든 데이터 스트림들에 대한 변조 심볼들이 TX MIMO 프로세서(220)에 제공되며, TX MIMO 프로세서(220)는 (예컨대, OFDM을 위하여) 변조 심볼들을 추가로 프로세싱할 수 있다. 그 다음, TX MIMO 프로세서(220)는 N_T개의 변조 심볼 스트림들을 N_T개의 송신기들(TMTR)(222a 내지 222t)에 제공한다. 본 개시물의 특정 양상들에서, TX MIMO 프로세서(220)는 데이터 스트림들의 심볼들, 및 그 심볼들을 송신하고 있는 안테나에 빔포밍 가중치들을 적용한다.

[0047] [0054] 각각의 송신기(222)는 하나 또는 그 초과의 아날로그 신호들을 제공하기 위하여 각각의 심볼 스트림을 수신 및 프로세싱하고, MIMO 채널 상에서의 송신에 적합한 변조된 신호를 제공하기 위하여 아날로그 신호들을 추가로 컨디셔닝(condition)(예컨대, 증폭, 필터링 및 상향변환)한다. 그 다음, 송신기들(222a 내지 222t)로부터의 N_T개의 변조된 신호들은 N_T개의 안테나들(224a 내지 224t)로부터 각각 송신된다.

[0048] [0055] 수신기 시스템(250)에서, 송신된 변조된 신호들은 N_R개의 안테나들(252a 내지 252r)에 의해 수신될 수 있고, 각각의 안테나(252)로부터 수신된 신호는 각각의 수신기(RCVR)(254a 내지 254r)로 제공될 수 있다. 각각의 수신기(254)는 각각의 수신된 신호를 컨디셔닝(예컨대, 필터링, 증폭 및 하향변환)하고, 컨디셔닝된 신호를 디지털화하여 샘플들을 제공하고, 그 샘플들을 추가로 프로세싱하여 대응하는 "수신된" 심볼 스트림을 제공할 수 있다.

[0049] [0056] 그 다음, 수신(RX) 데이터 프로세서(260)는 N_T개의 "검출된" 심볼 스트림들을 제공하기 위하여 특정 수신기 프로세싱 기법에 기초하여 N_R개의 수신기들(254)로부터의 N_R개의 수신된 심볼 스트림들을 수신 및 프로세싱한다. 그 다음, RX 데이터 프로세서(260)는 데이터 스트림에 대한 트래픽 데이터를 복원하기 위하여 각각의 검출된 심볼 스트림을 복조, 디인터리빙(deinterleave) 및 디코딩한다. RX 데이터 프로세서(260)에 의한 프로세싱은 송신기 시스템(210)에서 TX MIMO 프로세서(220) 및 TX 데이터 프로세서(214)에 의해 수행된 것과 상보적일 수 있다.

[0050] [0057] 제어기/프로세서(270)는 어떤 프리-코딩 행렬을 사용할 것인지를 주기적으로 결정한다. 제어기/프로세서(270)는 행렬 인덱스 부분 및 랭크(rank) 값 부분을 포함하는 역방향 링크 메시지를 공식화(formulate)한다. 메모리(272)는 수신기 시스템(250)에 대한 데이터 및 소프트웨어/펌웨어를 저장할 수 있다. 역방향 링크 메시지는 통신 링크 및/또는 수신된 데이터 스트림에 관한 다양한 타입들의 정보를 포함할 수 있다. 그 다음, 역방향 링크 메시지는, 데이터 소스(236)로부터 다수의 데이터 스트림들에 대한 트래픽 데이터를 또한 수신하는 TX 데이터 프로세서(238)에 의해 프로세싱되고, 변조기(280)에 의해 변조되고, 송신기들(254a 내지 254r)에 의해 컨디셔닝되고, 송신기 시스템(210)으로 다시 송신된다.

[0051] [0058] 송신기 시스템(210)에서, 수신기 시스템(250)으로부터의 변조된 신호들은 안테나들(224)에 의해 수신되고, 수신기들(222)에 의해 컨디셔닝되고, 복조기(240)에 의해 복조되고, RX 데이터 프로세서(242)에 의해 프로세싱되어 수신기 시스템(250)에 의해 송신된 역방향 링크 메시지를 추출한다. 그 다음, 제어기/프로세서(230)는 빔포밍 가중치들을 결정하기 위하여 어떤 프리-코딩 행렬을 사용할 것인지를 결정하며, 그 다음, 추출된 메시지를 프로세싱한다.

[0052] [0059] 특정 양상들에 따라, 제어기들/프로세서들(230 및 270)은 각각 송신기 시스템(210) 및 수신기 시스템(250)에서의 동작을 지시할 수 있다. 예컨대, 제어기/프로세서(270), TX 데이터 프로세서(238), RX 데이터 프로세서(260) 및/또는 수신기 시스템(250)에서의 다른 제어기들, 프로세서들 및 모듈들은 도 5를 참조하여 아래에서 설명되는 동작들 및/또는 본원에서 설명되는 기법들에 대한 다른 동작들을 수행 또는 지시하도록 구성될 수 있다. 또 다른 양상에 따라, 제어기/프로세서(230), TX 데이터 프로세서(214), RX 데이터 프로세서(242) 및/또는 수신기 시스템(210)에서의 다른 제어기들, 프로세서들 및 모듈들은 도 6을 참조하여 아래에서 설명되는 동작들 및/또는 본원에서 설명되는 기법들에 대한 다른 동작들을 수행 또는 지시하도록 구성될 수 있다.

[0053] [0060] 도 3은 도 1에 예시되는 무선 통신 시스템 내에서 채용될 수 있는 무선 디바이스(302)에서 활용될 수 있는 다양한 컴포넌트들을 예시한다. 무선 디바이스(302)는 본원에서 설명되는 다양한 방법들을 구현하도록 구성될 수 있는 디바이스의 예이다. 무선 디바이스(302)는 액세스 포인트(예컨대, 도 1에 예시되는 AP(100)), 액세스 단말들(예컨대, 도 1에 예시되는 AT들(116, 122 및 130)) 중 임의의 액세스 단말, 또는 네트워크 엔티티(예컨대, 도 8-9에 예시되는 MME)일 수 있다.

[0054] [0061] 무선 디바이스(302)는 무선 디바이스(302)의 동작을 제어하는 제어기/프로세서(304)를 포함할 수 있다.

제어기/프로세서(304)는 또한, 예컨대, CPU(central processing unit)로 지칭될 수 있다. ROM(read-only memory), RAM(random access memory), 플래시 메모리, PCM(phase change memory)을 포함할 수 있는 메모리(306)는 명령들 및 데이터를 제어기/프로세서(304)에 제공한다. 메모리(306)의 일부분은 또한, NVRAM(non-volatile random access memory)을 포함할 수 있다. 제어기/프로세서(304)는 전형적으로, 메모리(306) 내에 저장된 프로그램 명령들에 기초하여 논리적 그리고 산술적 동작들을 수행한다. 메모리(306) 내의 명령들은, 예컨대, UE가 업링크 비연결형 송신 동안 데이터를 보안적으로 송신하게 하기 위하여 본원에서 설명되는 방법들을 구현하도록 실행가능할 수 있다.

[0055] [0062] 무선 디바이스(302)는 또한, 무선 디바이스(302)와 원격 위치 사이에서의 데이터의 송신 및 수신을 허용하기 위한 송신기(310) 및 수신기(312)를 포함할 수 있는 하우징(308)을 포함할 수 있다. 송신기(310) 및 수신기(312)는 트랜시버(314)로 결합될 수 있다. 단일 또는 복수의 송신 안테나들(316)은 하우징(308)에 부착되며, 트랜시버(314)에 전기적으로 커플링될 수 있다. 무선 디바이스(302)는 또한, (도시되지 않은) 다수의 송신기들, 다수의 수신기들 및 다수의 트랜시버들을 포함할 수 있다.

[0056] [0063] 무선 디바이스(302)는 또한, 트랜시버(314)에 의해 수신된 신호들의 레벨을 검출 및 정량화하기 위한 노력으로 사용될 수 있는 신호 검출기(318)를 포함할 수 있다. 신호 검출기(318)는 총 에너지, 심볼당 서브캐리어당 에너지, 전력 스펙트럼 밀도 및 다른 신호들과 같은 이러한 신호들을 검출할 수 있다. 무선 디바이스(302)는 또한 신호들의 프로세싱 시 사용하기 위한 DSP(digital signal processor)(320)를 포함할 수 있다.

[0057] [0064] 무선 디바이스(302)의 다양한 컴포넌트들은, 데이터 버스와 더불어, 전력 버스, 제어 신호 버스 및 상태 신호 버스를 포함할 수 있는 버스 시스템(322)에 의해 함께 커플링될 수 있다. 제어기/프로세서(304)는 아래에서 논의되는 본 개시물의 특정 양상들에 따라, 보안 비연결형 업링크 데이터 송신에 대한 프로시저들을 수행하기 위하여 메모리(306) 내에 저장된 명령들에 액세스하도록 구성될 수 있다.

[0058] [0065] 도 4는 본 개시물의 특정 양상들에 따른, 예시적 LTE RACH 경합-기반 프로시저에 대한 메시지 흐름(400)을 예시한다. 402에서, UE는 FDD를 위하여 0의 초기 타이밍 어드밴스(Timing Advance)를 가정하는 프리앰블(MSG1)을 전송할 수 있다. 전형적으로, 프리앰블은 셀 상에서 할당되는 한 세트의 프리앰블들 사이에서 UE에 의해 랜덤하게 선택되며, MSG 3에 대해 요청되는 사이즈로 링크될 수 있다. 404에서, eNB는 RAR(random access response) 또는 MSG2를 전송할 수 있다. MSG 2는 또한 MSG 3에 대한 승인을 표시할 수 있다. 406에서, UE는 승인을 사용하여 MSG 3을 전송할 수 있다. 408에서, eNB는 MSG 3을 디코딩할 수 있고, RRC(Radio Resource Control) 시그널링 메시지를 에코 백(echo back)하거나 또는 C-RNTI(cell radio network temporary identifier)로 스크램블링된 UL 승인(예컨대, DCI 0)을 전송할 수 있다.

[0059] [0066] 위에서 서술된 바와 같이, MTC(machine-type communications) 디바이스들 및 eMTC(enhanced MTC) 디바이스들 등과 같은 특정 타입들의 디바이스들은 대부분의 시간 동안 저전력 상태(예컨대, 유휴 상태)에 있는 것으로 예상될 수 있다. 그러나, 일반적으로, MT(mobile terminated) 또는 MO(mobile originated) 데이터 연결이 요구되는 때마다, 디바이스는 유휴 상태로부터 연결 상태로 변환(transition)한다.

[0060] [0067] 이 변환은 전형적으로 몇몇 단계들을 수반한다: 랜덤 액세스 및 경합 해결, RRC(radio resource control) 연결 셋업, 서비스 요청, 보안 활성화, DRB(data radio bearer) 설정 및 실제 데이터 송신 및 수신. 특정 디바이스들(예컨대, MTC 디바이스들 등)에 있어서, 일반적으로 위의 시그널링 오버헤드는 종종 교환되는 데이터량보다 훨씬 크다. 더욱이, 특정 양상들에서, 디바이스는 데이터가 송신 및 수신될 때까지 유휴 상태로 다시 변환되지 않을 수 있다. 예컨대, 특정 상황들에서, 디바이스는 유휴 상태로의 변환 이전에 ACK(acknowledgement)를 기다려야 할 수 있는데, 이는 전력 효율적이지 않다.

[0061] [0068] 따라서, 데이터를 송신 및/또는 수신하기 위하여 유휴 모드로부터 변환하는 경우 시그널링 오버헤드를 감소시키는 것은 전력 소비량을 감소시킬 수 있다. 본원에서 제시되는 특정 양상들에 따라, UE(예컨대, MTC 디바이스, 도 1에 예시되는 AT(들) 등)는 UE가 RRC 연결 모드에의 진입과 연관된 오버헤드없이 데이터를 송신할 수 있도록 비연결형 액세스 송신을 수행할 수 있다. 특정 양상들에 따라, 비연결형 액세스 모드는 전체 RRC 연결 셋업을 요구하지 않는 신속한 변환들을 허용할 수 있다. 또 다른 양상에 따라, RACH 프로시저(예컨대, 도 4에 예시됨)는 비연결형 액세스를 제공하도록 수정될 수 있다.

[0062] [0069] 위에서 설명된 바와 같이, 특정 양상들에 따라, 데이터 송신과 연관된 시그널링 오버헤드량을 감소시키기 위하여, UE는 연결(본원에서 비연결형 액세스 송신으로 지칭됨)을 먼저 설정하는 오버헤드없이 데이터를 송신할 수 있고, 이는 전력 소비를 감소시킬 수 있다. 그러나, 일부 경우들에서, 비연결형 송신은 보안적이지 않

을 수 있다. 예컨대, 특정 양상들에 따라, (예컨대, 비연결형 액세스 송신을 사용하여) UE가 메시지를 송신하는 경우, UE 및/또는 네트워크는 아직 인증되지 않을 수 있다.

[0063] [0070] 그러나, 본 개시물의 양상들은 UE가 비연결형 송신을 전송하기 이전에 암호화 메커니즘을 협상하게 한다. 예컨대, 비연결형 송신은 단지 성공적 협상 이후에 사용된다. 그 다음, UE는 비연결형 송신에서 전송된 데이터를 암호화하기 위하여 이 암호화 메커니즘을 사용할 수 있다. 그 다음, 기지국(예컨대, eNB)은 네트워크(예컨대, MME(mobility management entity))를 통해 UE를 인증하고, 그것이 그 다음 암호화된 데이터를 암호화 해제하는데 사용할 수 있는 정보(예컨대, 키, 시퀀스 번호 등)를 수신하기 위하여 단계들을 취할 수 있다.

[0064] [0071] 따라서, 본 개시물의 양상들은 데이터의 송신 이전에 (예컨대, 네트워크를 통해) 보안 연결을 설정할 필요성 없이 데이터의 보안 송신을 허용할 수 있다.

[0065] [0072] 도 5, 6 및 7은 보안 비연결형 송신에서 수반되는 상이한 엔티티들에 의해 수행될 수 있는 예시적 동작들을 예시한다.

[0066] [0073] 예컨대, 도 5는, 예컨대, UE(예컨대, MTC 디바이스, 도 1의 AT(116), 도 2의 수신기 시스템(250) 또는 도 3의 무선 디바이스(302) 등)에 의해 수행될 수 있는 보안 비연결형 데이터 송신을 위한 예시적 동작들(500)을 예시한다.

[0067] [0074] 502에서, UE는 BS(base station)를 통해 네트워크와의 보안 연결을 설정한다. 504에서, UE는 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상한다. 506에서, UE는 암호화 메커니즘의 협상 이후에 유휴 모드에 진입한다. 508에서, UE는 네트워크에 포워딩될 데이터를 암호화하기 위하여 협상된 암호화 메커니즘을 사용한다. 510에서, UE는 전체 RRC 연결을 설정하지 않고 암호화된 데이터를 포함하는 패킷을 BS에 송신한다.

[0068] [0075] 도 6은 (예컨대, UE에 의한 보안 비연결형 데이터 송신을 제공하기 위하여) 예컨대, BS에 의해 수행될 수 있는 예시적 동작들(600)을 예시한다. 특정 양상들에 따라, BS는 도 1의 AP(100), 도 2의 송신기 시스템(210), 도 3의 무선 디바이스(302) 등일 수 있다.

[0069] [0076] 602에서, BS는 암호화된 데이터를 포함하는 패킷을 전체 RRC(radio resource control) 연결을 설정하지 않은 UE(user equipment)로부터 수신한다. 604에서, BS는 UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신한다. 606에서, BS는 네트워크 엔티티가 UE를 인증한 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 네트워크 엔티티로부터 수신한다. 608에서, BS는 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용한다.

[0070] [0077] 도 7은 UE에 의한 보안 비연결형 데이터 송신을 제공하기 위하여, 예컨대, 네트워크 엔티티에 의해 수행될 수 있는 예시적 동작들(700)을 예시한다. 특정 양상들에 따라, 네트워크 엔티티는 MME(예컨대, 도 8-9에 예시됨)일 수 있다.

[0071] [0078] 702에서, MME는 BS(base station)를 통해 UE(user equipment)와의 보안 연결을 설정한다. 704에서, MME는 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상한다. 706에서, MME는 UE의 인증을 수행하기 위하여, 암호화된 데이터를 포함하는 패킷을 UE로부터 수신한 BS와 통신한다. 708에서, MME는 UE의 인증 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 BS에 제공한다. 710에서, MME는 암호화해제 정보를 사용하여 암호화해제된 데이터를 BS로부터 수신한다. 도 10을 참조하여 아래에서 더 상세하게 설명될 바와 같이, 일부 경우들에서, MME 및 S-GW는 단일 네트워크 엔티티일 수 있고, 엔티티는, 암호화해제 정보를 BS에 제공하기 보다는, 암호화된 데이터를 BS로부터 수신하고 암호화해제 정보를 사용하여 그것을 암호화해제할 수 있다.

[0072] [0079] 위에서 언급된 바와 같이, 특정 양상들에 따라, UE가 보안 비연결형 데이터 송신을 송신하기 이전에, UE는 먼저, 비연결형 송신에 대한 셋업의 일부로서 암호화 메커니즘의 협상을 위하여 (예컨대, BS를 통해) MME와 협상할 수 있다. 특정 양상들에 따라, 비연결형 업링크 데이터 송신은 단지 비연결형 송신의 성공적 협상 및/또는 셋업 이후에 시도될 수 있다.

[0073] [0080] 도 8은 본 개시물의 양상들에 따른, 비연결형 송신에 대한 셋업의 일부로서 암호화 메커니즘의 협상을 위하여 UE(802), BS(804) 및 MME(806)(예컨대, 네트워크 엔티티) 사이의 메시지들의 교환을 도시하는 예시적 호 흐름도(800)를 예시한다. UE(802)는 MTC 디바이스, 도 1의 AT(116), 도 2의 수신기 시스템(250) 또는 도 3의 무선 디바이스(302) 등 중 임의의 것일 수 있다. BS(804)는 도 1의 AP(100), 도 2의 송신기 시스템(210), 도

3의 무선 디바이스(302) 등일 수 있다.

[0074] [0081] 특정 양상들에 따라, 도 8의 단계 1에 도시되는 바와 같이, UE(802) 및 MME(806)(예컨대, 네트워크 엔티티)는, 예컨대, eNodeB(eNB)(804)를 통해 보안 연결을 설정할 수 있다. 특정 양상들에서, 보안 연결은 (예컨대, 3GPP LTE 등에 대해) 기존 표준들에 따라 구현되는 RRC 연결 및/또는 보안 NAS(non-access stratum) 연결로 구성될 수 있다. 예컨대, 보안 연결은 TAU(tracking area update) 메커니즘 및/또는 부착 프로시저 중 적어도 하나를 포함할 수 있다. 또 다른 양상에서, 보안 연결은 새로운 프로시저(예컨대, 현재 표준들에 의해 정의되지 않음)를 활용하여 구현될 수 있다.

[0075] [0082] 도 8의 단계들 2 및 3에 도시되고 도 5 및 도 7에 대해 위에서 설명된 바와 같이, UE(802) 및 MME(806)는, 보안 연결을 통해, 전체 RRC 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상할 수 있다. 예컨대, 도 8의 단계 2에 예시되는 바와 같이, UE(802)는 비연결형 송신을 위하여 UE(802)에 의해 지원되는 하나 또는 그 초과의 암호화 메커니즘들의 리스트를 포함하는 비연결형 셋업 요청을 MME(806)에 송신할 수 있다. 일단 MME(806)가 비연결형 셋업 요청을 수신하면, MME(806)는 (예컨대, 도 8의 단계 3에 도시되는 바와 같이) 비연결형 송신을 위하여 사용될 암호화 메커니즘의 표시를 적어도 포함하는 연결 셋업 응답을 송신할 수 있다. 표시된 암호화 메커니즘은 UE(802)에 의해 지원되고 요청(예컨대, 초기 시퀀스 번호, 키들 등)에서 리스팅되는 암호화 메커니즘들 중 하나와 관련된 정보일 수 있다. 그러나, 일부 경우들에서, 비연결형 셋업 응답은 요청에서 UE에 의해 리스팅되는 것 이외의 암호화 메커니즘을 표시할 수 있다.

[0076] [0083] 특정 양상들에 따라, 도 8의 단계 4에 도시되는 바와 같이, MME(806) 및 UE(802)가 비연결형 송신에 대한 셋업의 일부로서 암호화 메커니즘에 대해 성공적으로 협상되면(예컨대, MME가 비연결형 셋업 요청을 수락(accept)하였음), 연결이 릴리스될 수 있고, UE(802)는 유휴 모드에 진입할 수 있다. UE(802)는 (예컨대, 일부 기간의 시간 동안 또는 달리 표시될 때까지) 성공적 협상 이후에 비연결형 송신을 사용하려고 시도할 수 있다. UE(802)는 UE(802)와 MME(806) 사이의 전체 RRC 연결을 설정하지 않고 데이터를 송신하기 위하여 비연결형 송신을 사용할 수 있다. 예컨대, 하나의 실시예에서, UE(802)는 RRC 연결 모드에 진입하지 않고 비연결형 송신을 사용하여 데이터를 송신할 수 있다. 하나의 실시예에서, UE(802)는 UE(802)와 MME(806) 사이의 적어도 하나의 데이터 라디오 베어러를 설정하지 않고 비연결형 송신을 사용하여 데이터를 송신할 수 있다. 대안적으로, MME(806)가 UE(802)로부터의 요청을 거절 또는 무시하였다면, UE(802)는 비연결형 송신을 사용하려고 시도하지 않을 수 있다. 단계들 3 및 4는 독립형 메시지들 또는 기존 메시지들 상으로 피기-백되는 메시지들을 포함할 수 있다.

[0077] [0084] 본원에서 제공되는 양상들에 따라, 비연결형 셋업 요청 메시지 및 비연결형 셋업 응답 메시지는 기존 NAS 메시지들의 일부로서 제공될 수 있거나 또는 새로운 메시지들을 통해 제공될 수 있다. 또 다른 양상에 따라, 암호화 메커니즘의 성공적 협상 및/또는 비연결형 송신에 대한 셋업 은 일부 기간의 시간 동안 유효할 수 있다. 예컨대, 성공적 협상은 만료 시간(예컨대, 24 시간, 48 시간 등)의 만료 시 만료될 수 있거나, 일단 UE가 eNB 및/또는 네트워크로부터 지정된 영역 외부로 나가면 만료될 수 있거나, 또는 일부 다른 기준들이 적용될 수 있다(예컨대, 네트워크는 임의의 시간에 협상된 암호화 메커니즘을 리보크(revoke)할 수 있음).

[0078] [0085] 도 9는 (예컨대, 도 8에 도시되는 동작들이 수행되었다고 가정하면) 보안 비연결형 UL 데이터 송신을 위한 예시적 호 흐름도(900)를 예시한다. (예컨대, 도 8에 대해) 위에서 설명된 바와 같이, 하나의 양상에서, UE(802)는 비연결형 송신에 대한 셋업의 일부로서 암호화 메커니즘의 성공적 협상 이후까지 보안 비연결형 UL 데이터 송신을 시도하지 않을 수 있다. 도 9의 동작들은 도 8에서와 같이 초기 협상없이 다수회 발생할 수 있다.

[0079] [0086] 특정 양상들에 따라, 위에서 설명된 바와 같이, 암호화 메커니즘의 성공적 협상 이후에, UE(802)는 (예컨대, eNB를 통해) 네트워크로 포워딩될 데이터를 암호화하기 위하여 협상된 암호화 메커니즘을 사용할 수 있다. 양상에서, UE(802)는 그 다음, 암호화된 데이터를 포함하는 패킷을 송신하기 위하여 eNB(804)로부터의 자원들을 요청할 수 있다. 따라서, 도 9의 단계 1에 도시되는 바와 같이, eNB(804)가 요청된 자원들을 UE(802)에 제공하면, UE(802)는 그 다음 비연결형 송신을 사용하여 암호화된 데이터를 포함하는 패킷을 eNB(804)에 송신할 수 있다. 양상에 따라, UE(802)는 전체 RRC 연결을 설정하지 않고(예컨대, UE와 MME(806) 사이의 임의의 데이터 라디오 베어러들을 설정하지 않고, RRC 연결 모드에 진입하지 않고 등) 패킷을 송신함으로써 비연결형 송신을 사용할 수 있다. 또 다른 양상에 따라, 패킷은 서비스 요청의 일부로서 송신될 수 있다.

[0080] [0087] 일부 경우들에서, 암호화된 데이터를 포함하는 송신된 패킷은 네트워크가 UE(802)를 인증하기 위한 메커니즘 또는 수단을 포함할 수 있다. 예컨대, 메커니즘 또는 수단은 UE(802)의 MAC(medium access control)

또는 쇼트 MAC 어드레스 중 적어도 하나를 포함할 수 있다.

[0081] [0088] 도 9의 단계 2에 도시되는 바와 같이, 암호화된 데이터를 포함하는 패킷을 RRC 연결 모드에 있지 않은 UE(802)로부터 수신한 이후에, eNB(804)는 그 다음, UE(802)의 인증을 수행하기 위하여 MME(806)(예컨대, 네트워크 엔티티)와 통신할 수 있다. 예컨대, 도 9에 도시되는 바와 같이, eNB(804)는 UE(802)로부터 수신된 인증 정보(예컨대, UE의 MAC 또는 쇼트 MAC 어드레스)를 가지는 메시지를 MME(806)에 송신할 수 있다. 양상에서, eNB(804)는 또한, 자신의 어드레스(예컨대, eNB 어드레스) 및/또는 사용자 평면 송신에 대한 터널링 정보(예컨대, S1 TEID(들)(DL)(터널 엔드포인트 식별자들(다운링크))를 포함할 수 있다.

[0082] [0089] 도 9의 단계 3에 도시되는 바와 같이, 일단 MME(806)가 UE(802)를 인증하는데 필요한 정보(예컨대, UE의 MAC 또는 쇼트 MAC 어드레스)를 포함하는 메시지를 eNB(804)로부터 수신하면, MME(806)는, 예컨대, UE의 MAC 또는 쇼트 MAC 어드레스를 활용하여 UE를 인증할 수 있다.

[0083] [0090] 도 9의 단계 4에 도시되는 바와 같이, MME(806)는 그 다음, 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 eNB(804)에 제공할 수 있다. 예컨대, 도 9에 도시되는 바와 같이, MME(806)는 암호화해제 정보(예컨대, 보안 컨텍스트)를 eNB(804)에 제공할 수 있다. 또 다른 실시예에서, 암호화해제 정보를 eNB(804)에 제공하는 것과 더불어, 또는 대안적으로, MME(806)는 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용할 수 있다. 양상에서, MME(806)는 또한, 서빙 게이트웨이(S-GW) 정보(예컨대, S-GW 어드레스) 및/또는 터널링 정보(예컨대, S1 TEID(들)(UL)(터널 엔드포인트 식별자들(업링크))를 eNB에 제공할 수 있다. 또 다른 양상에서, MME(806)는 네트워크를 인증하기 위하여 UE(802)에 대한 MAC 또는 쇼트 MAC 어드레스를 (eNB(804)에) 제공할 수 있다. 도 9의 단계 5에 도시되는 바와 같이, eNB(804)는 UE(802)에 의해 송신된 패킷 내의 암호화된 데이터(예컨대, 소형 데이터 패킷 등)를 암호화해제하기 위하여 MME(806)로부터 수신된 암호화해제 정보를 사용할 수 있다.

[0084] [0091] 도 9의 단계 6에 도시되는 바와 같이, 암호화된 데이터를 성공적으로 암호화해제한 이후에, eNB(804)는 eNB(804)가 암호화된 데이터를 성공적으로 암호화해제하였음을 확인응답하는 메시지(예컨대, ACK(acknowledgement))를 UE(802)에 전송할 수 있다. 특정 양상들에서, 이 ACK는 그것이 메시지를 올바른 네트워크에 전송하였음을 알기 위한 UE(802)에 대한 인증된 ACK일 수 있다. 이 보안 ACK는 ACK에 MME 제공 MAC 또는 쇼트 MAC를 포함하여 eNB(804)에 의해 수행될 수 있다. 특정 양상들에서, 메시지는 페이징 메시지를 포함할 수 있다(따라서, UE가 유휴하도록 리턴하고, 확인응답을 표시하는 페이징 메시지들을 체크하기 위하여 웨이크업하게 함). 양상에서, ACK는 페이징 메시지, 또 다른 메시지 및/또는 페이징 메시지 이후의 별개의 자원 내에 포함될 수 있다. 또 다른 양상에서, 페이징 메시지 그 자체의 단순한 송신은 eNB(804)가 암호화된 데이터를 성공적으로 암호화해제하였다는 확인응답을 표시할 수 있다. 예컨대, 페이징 메시지는 UE(802)가 연결이 여전히 활성적임(다시 말해서, 예컨대, 도 8의 프로시저를 사용하는 어떠한 재설정도 필요하지 않음)을 알게 한다. 또 다른 양상에서, 메시지는 네트워크를 인증하기 위한 UE(802)에 대한 메커니즘 또는 수단을 포함할 수 있다. 예컨대, 메커니즘 또는 수단은 MAC 또는 쇼트 MAC 어드레스 중 적어도 하나를 포함할 수 있다. 추가로, 또 다른 양상에 따라, UE(802)는 여전히 유휴 모드에 있으면서 메시지를 수신할 수 있다.

[0085] [0092] 특정 양상들에 따라, UE는 패킷의 송신 이후에, UE가 eNB(804)가 암호화된 데이터를 성공적으로 암호화해제하였다는 ACK(acknowledgment)를 수신하지 않았음(또는 명시적 네거티브 확인응답-NAK를 수신함)을 결정할 수 있다. 어느 경우든, UE(802)는 결정에 대한 응답으로, 패킷을 재송신할 수 있다.

[0086] [0093] 특정 양상들에 따라, 서비스 요청의 수신 및 UE(802)의 인증 이후에, MME(806), S-GW(902) 및 P-GW(904)는 (예컨대, 도 9의 단계들 7-10에 도시되는 바와 같이) 송신된 데이터 패킷을 포워딩하기 위하여 베어러들을 수정 및/또는 업데이트하도록 조정할 수 있다.

[0087] [0094] 도 9에 예시되는 호 흐름이 보안 비연결형 송신에서 수반되는 상이한 엔티티들의 단지 하나의 예를 예시한다는 점이 주목된다. 예컨대, 일부 경우들에서, MME(806) 및 S-GW(902)는 공통 네트워크 엔티티일 수 있다. 이 경우, MME(806)가 암호화해제 정보를 eNB에 전송하기 보다는, eNB가 암호화된 데이터를 전송할 수 있고, MME/S-GW가 암호화해제 정보를 사용하여 데이터를 디코딩 및 암호화해제할 수 있다. 도 10은 이러한 엔티티가 수행할 수 있는 예시적 동작들(1000)을 예시한다. 예시되는 바와 같이, 동작들(1002-1006)은 위에서 설명된 도 7의 동작들(702-706)과 동일할 수 있다. 그러나, UE의 인증 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 BS에 제공하고(708에 따라), 암호화해제 정보를 사용하여 암호화해제된 데이터를 BS로부터 수신하기(710에 따라) 보다는, 엔티티는 (1008에서) 암호화된 데이터를 BS로부터 수신하고, (1010에서) 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용할 수 있다.

[0088] [0095] 위에서 설명된 방법들의 다양한 동작들은 대응하는 기능들 또는 동작들을 수행할 수 있는 임의의 적합한 수단에 의해 수행될 수 있다. 수단은, 회로, ASIC(application specific integrated circuit) 또는 프로세서를 포함하는(그러나, 이들로 제한되는 것은 아님) 다양한 하드웨어 및/또는 소프트웨어/펌웨어 컴포넌트(들) 및/또는 모듈(들)을 포함할 수 있다. 일반적으로, 도면들에서 예시되는 동작들이 존재하는 경우, 그 동작들은 동작들을 수행할 수 있는 대응하는 기능적 수단에 의해 수행될 수 있다. 하나의 구성에서, UE(802)는, BS(base station)를 통해 네트워크와의 보안 연결을 설정하기 위한 수단, 보안 연결을 통해, 전체 RRC(radio resource control) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상하기 위한 수단, 암호화 메커니즘의 협상 이후에 유휴 모드에 진입하기 위한 수단, 네트워크에 포워딩될 데이터를 암호화하기 위하여 협상된 암호화 메커니즘을 사용하기 위한 수단, 및 전체 RRC 연결을 설정하지 않고 암호화된 데이터를 포함하는 패킷을 BS에 송신하기 위한 수단을 포함한다. 하나의 양상에서, 전술된 수단은 전술된 수단에 의해 기술되는 기능들을 수행하도록 구성되는 안테나들(252), 트랜시버들(254), 제어기/프로세서(270), 메모리(272), 송신 데이터 프로세서(238), 수신 데이터 프로세서(260), 변조기(280) 또는 이들의 조합들일 수 있다. 하나의 구성에서, eNB(804)는, 암호화된 데이터를 포함하는 패킷을 전체 RRC(radio resource control) 연결을 설정하지 않은 UE(user equipment)로부터 수신하기 위한 수단, UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신하기 위한 수단, 네트워크 엔티티가 UE를 인증한 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 네트워크 엔티티로부터 수신하기 위한 수단, 및 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용하기 위한 수단을 포함한다. 하나의 양상에서, 전술된 수단은 전술된 수단에 의해 기술되는 기능들을 수행하도록 구성되는 안테나들(224), 트랜시버들(222), 제어기/프로세서(230), 메모리(232), 송신 데이터 프로세서(214), 송신 MIMO 프로세서(220), 수신 데이터 프로세서(242), 복조기(240) 또는 이들의 조합들일 수 있다.

[0089] [0096] 본원에서 사용되는 바와 같이, "결정하는"이라는 용어는 아주 다양한 동작들을 포함한다. 예컨대, "결정하는"은 계산하는, 컴퓨팅하는, 프로세싱하는, 유도하는, 조사하는, 룩업(look up)(예컨대, 표, 데이터 베이스 또는 또 다른 데이터 구조에서 룩업)하는, 확인하는 등을 포함할 수 있다. 또한, "결정하는"은 수신하는(예컨대, 정보를 수신하는), 액세스하는(예컨대, 메모리 내의 데이터에 액세스하는) 등을 포함할 수 있다. 또한, "결정하는"은 해결하는, 선정하는, 선택하는, 설정하는 등을 포함할 수 있다.

[0090] [0097] 본원에서 사용되는 바와 같이, 항목들의 리스트 "중 적어도 하나"를 지칭하는 문구는 단일 부재들 및 중복 부재들을 포함하는 그러한 항목들의 임의의 조합을 지칭한다. 예로서, "a, b 또는 c 중 적어도 하나"는 a, b, c, a-b, a-c, b-c, a-b-c, aa, abb, abccc 등을 커버하는 것으로 의도된다.

[0091] [0098] 본 개시물과 관련하여 설명되는 다양한 예시적 논리적 블록들, 모듈들, 및 회로들은, 범용 프로세서, DSP(digital signal processor), ASIC(application specific integrated circuit), FPGA(field programmable gate array signal) 또는 다른 PLD(programmable logic device), 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들 또는 본원에서 설명되는 기능들을 수행하도록 설계되는 이들의 임의의 조합으로 구현 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로, 프로세서는 임의의 상업적으로 이용가능한 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합, 예컨대, DSP와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 또는 그 초과의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

[0092] [0099] 본 개시물과 관련하여 설명되는 알고리즘 또는 방법의 단계들은 직접 하드웨어로 구현되거나, 프로세서에 의해 실행되는 소프트웨어/펌웨어 모듈로 구현되거나, 또는 이 둘의 조합으로 구현될 수 있다. 소프트웨어/펌웨어 모듈은 당해 기술 분야에 알려진 임의의 형태의 저장 매체에 상주할 수 있다. 사용될 수 있는 저장 매체들의 일부 예들은 RAM(random access memory), ROM(read only memory), 플래시 메모리, EPROM 메모리, EEPROM 메모리, PCM(phase change memory), 레지스터들, 하드디스크, 분리가능한(removable) 디스크, CD-ROM 등을 포함한다. 소프트웨어/펌웨어 모듈은 단일 명령 또는 다수의 명령들을 포함할 수 있으며, 몇몇 상이한 코드 세그먼트들을 통해, 상이한 프로그램들 사이에, 그리고 다수의 저장 매체들에 걸쳐 분산될 수 있다. 저장 매체는 프로세서가 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기록할 수 있도록 프로세서에 커플링될 수 있다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다.

[0093] [00100] 본원에서 개시되는 방법들은 설명되는 방법을 달성하기 위한 하나 또는 그 초과의 단계들 또는 동작들을 포함한다. 방법 단계들 및/또는 동작들은 청구항들의 범위를 벗어나지 않으면서 서로 상호교환될 수 있다. 다시 말해서, 단계들 또는 동작들의 특정 순서가 특정되지 않는 한, 특정 단계들 및/또는 동작들의 순서 및/또

는 사용은 청구항들의 범위를 벗어나지 않으면서 수정될 수 있다.

[0094] [00101] 설명되는 기능들은 하드웨어, 소프트웨어/펌웨어 또는 이들의 조합으로 구현될 수 있다. 소프트웨어/펌웨어로 구현되는 경우, 기능들은 컴퓨터 판독가능한 매체 상에 하나 또는 그 초과의 명령들로서 저장될 수 있다. 저장 매체들은 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체들일 수 있다. 제한이 아닌 예로서, 이러한 컴퓨터 판독가능한 매체들은, RAM, ROM, PCM(phase change memory), EEPROM, CD-ROM 또는 다른 광학 디스크 저장, 자기 디스크 저장 또는 다른 자기 저장 디바이스들, 또는 원하는 프로그램 코드를 명령들 또는 데이터 구조들의 형태로 반송 또는 저장하는데 사용될 수 있고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 본원에서 사용되는 바와 같은 디스크(disk 및 disc)는 CD(compact disc), 레이저 디스크(disc), 광 디스크(disc), DVD(digital versatile disc), 플로피 디스크(disk) 및 블루-레이® 디스크(disc)를 포함하며, 여기서 디스크(disk)들은 통상적으로 데이터를 자기적으로 재생하는 반면, 디스크(disc)들은 레이저들을 이용하여 데이터를 광학적으로 재생한다.

[0095] [00102] 따라서, 특정 양상들은 본원에서 제시되는 동작들을 수행하기 위한 컴퓨터 프로그램 제품을 포함할 수 있다. 예컨대, 이러한 컴퓨터 프로그램 제품은 명령들이 저장된(그리고/또는 인코딩된) 컴퓨터 판독가능한 매체를 포함할 수 있으며, 명령들은 본원에서 설명되는 동작들을 수행하기 위하여 하나 또는 그 초과의 프로세서들에 의해 실행가능하다. 특정 양상들에서, 컴퓨터 프로그램 제품은 패키징 재료(packaging material)를 포함할 수 있다.

[0096] [00103] 소프트웨어/펌웨어 또는 명령들은 또한 송신 매체 상에서 송신될 수 있다. 예컨대, 소프트웨어/펌웨어가 웹사이트, 서버, 또는 다른 원격 소스로부터 동축 케이블, 광섬유 케이블, 트위스티드 페어(twisted pair), DSL(digital subscriber line), 또는 (적외선, 라디오 및 마이크로파와 같은) 무선 기술들을 사용하여 송신되는 경우, 동축 케이블, 광섬유 케이블, 트위스티드 페어, DSL, 또는 (적외선, 라디오 및 마이크로파와 같은) 무선 기술들이 송신 매체의 정의 내에 포함된다.

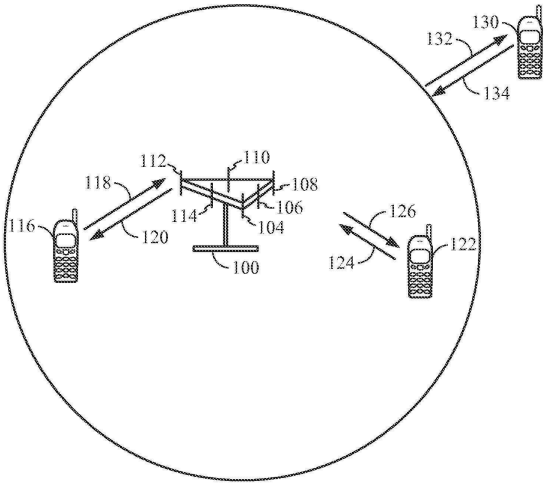
[0097] [00104] 추가로, 본원에서 설명되는 방법들 및 기법들을 수행하기 위한 모듈들 및/또는 다른 적절한 수단은 적용가능한 경우, 사용자 단말 및/또는 기지국에 의해 다운로드되고 그리고/또는 다른 방식으로 획득될 수 있다는 것이 인식되어야 한다. 예컨대, 이러한 디바이스는 본원에서 설명되는 방법들을 수행하기 위한 수단의 전달을 가능하게 하기 위하여 서버에 커플링될 수 있다. 대안적으로, 본원에서 설명되는 다양한 방법들은 저장 수단(예컨대, RAM, ROM, (CD(compact disc) 또는 플로피 디스크와 같은) 물리적 저장 매체 등)을 통해 제공될 수 있어서, 사용자 단말 및/또는 기지국은 저장 수단을 디바이스에 커플링시키거나 또는 제공할 시, 다양한 방법들을 획득할 수 있다. 더욱이, 본원에서 설명되는 방법들 및 기법들을 디바이스에 제공하기 위한 임의의 다른 적합한 기법이 활용될 수 있다.

[0098] [00105] 청구항들은 위에서 예시된 정밀한 구성 및 컴포넌트들에 제한되지 않는다는 것이 이해될 것이다. 청구항들의 범위를 벗어나지 않으면서 위에서 설명된 방법들 및 장치의 배열, 동작 및 세부사항들에서 다양한 수정들, 변화들 및 변형들이 이루어질 수 있다.

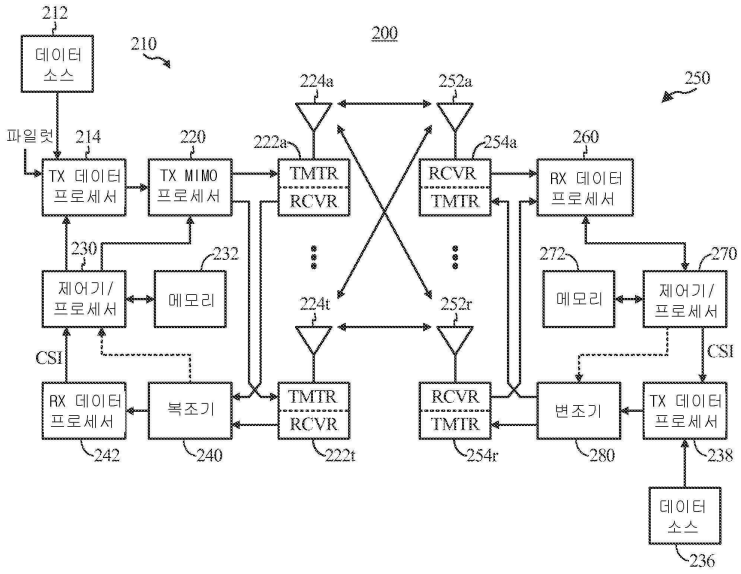
[0099] [00106] 위의 설명은 본 개시물의 양상들에 관련되지만, 개시물의 기본 범위로부터 벗어나지 않으면서 개시물의 다른 그리고 추가 양상들이 고안될 수 있으며, 개시물의 범위는 다음의 청구항들에 의해 결정된다.

도면

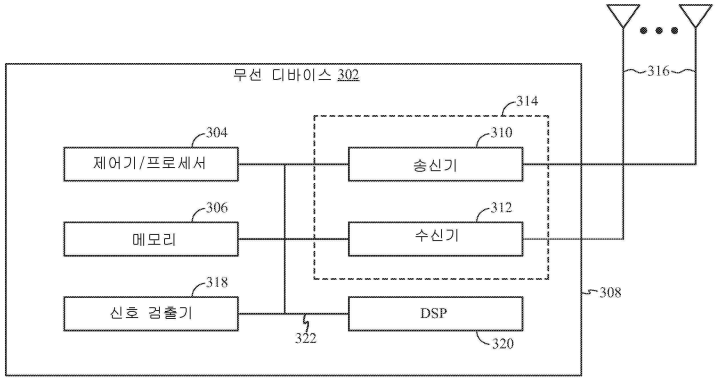
도면1



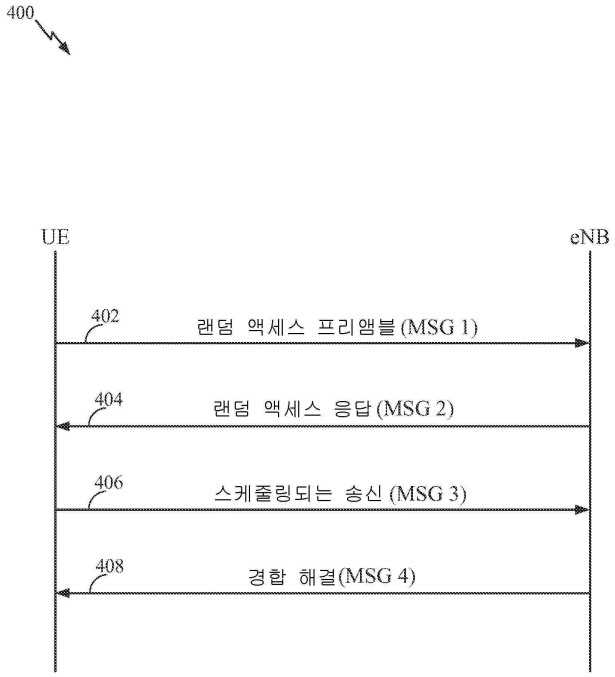
도면2



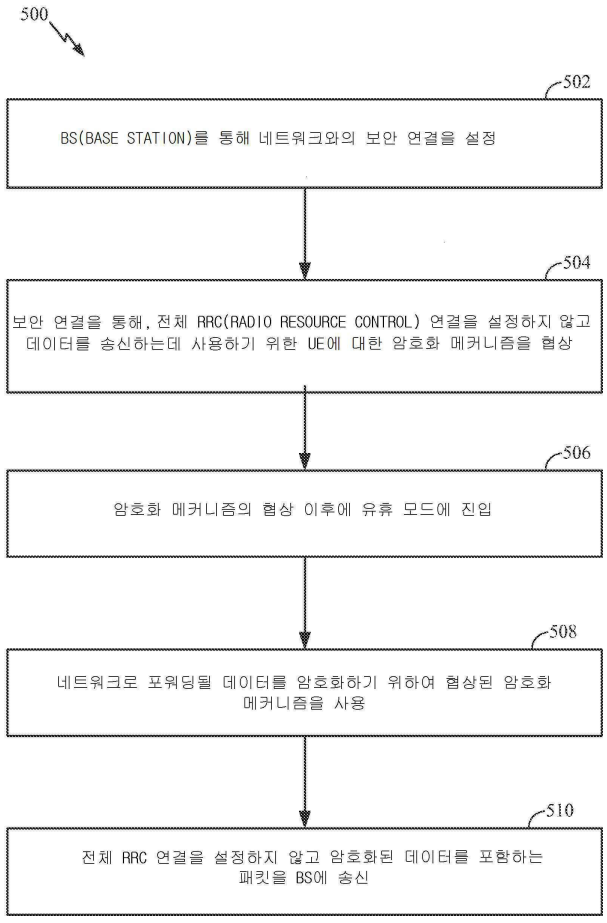
도면3



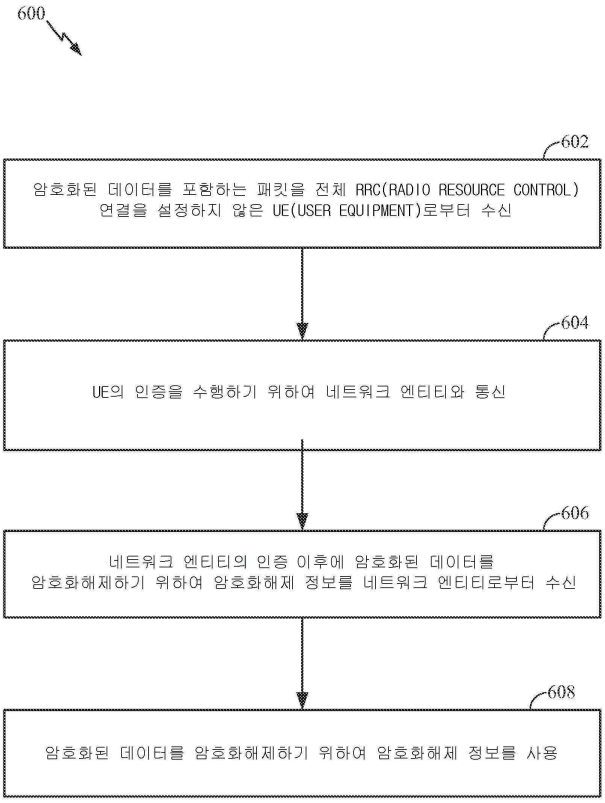
도면4


400
UE
eNB
402
랜덤 액세스 프리앰블 (MSG 1)
404
랜덤 액세스 응답 (MSG 2)
406
스케줄링되는 송신 (MSG 3)
408
경합 해결(MSG 4)

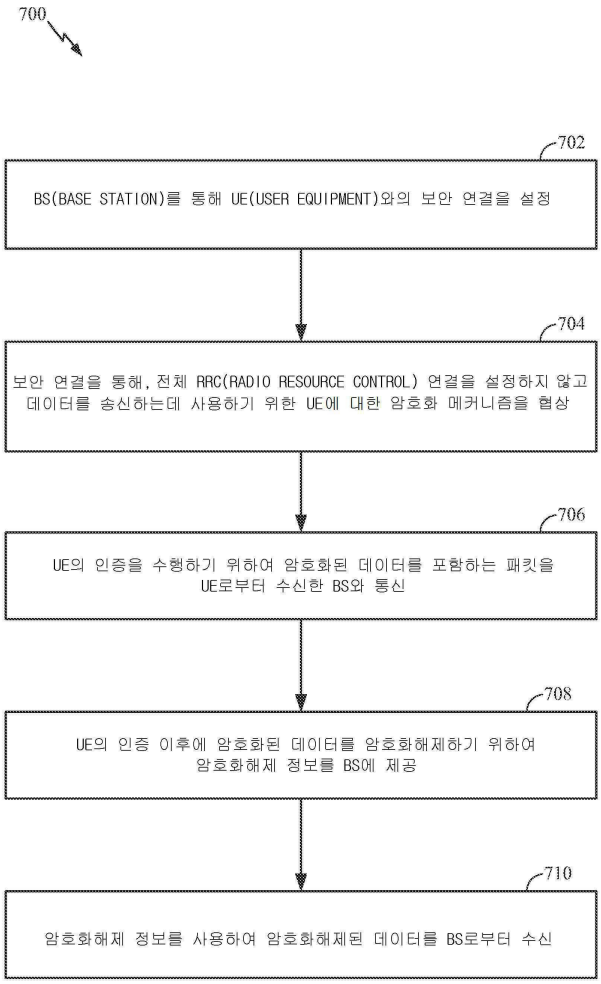
도면5


500
502
BS(BASE STATION)를 통해 네트워크와의 보안 연결을 설정
504
보안 연결을 통해, 전체 RRC(RADIO RESOURCE CONTROL) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상
506
암호화 메커니즘의 협상 이후에 유휴 모드에 진입
508
네트워크로 포워딩될 데이터를 암호화하기 위하여 협상된 암호화 메커니즘을 사용
510
전체 RRC 연결을 설정하지 않고 암호화된 데이터를 포함하는 패킷을 BS에 송신

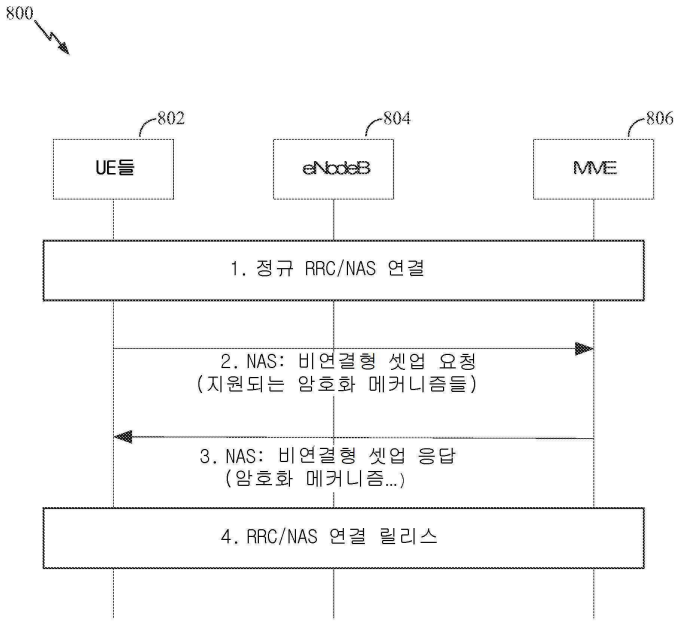
도면6


600
602
암호화된 데이터를 포함하는 패킷을 전체 RRC(RADIO RESOURCE CONTROL) 연결을 설정하지 않은 UE(USER EQUIPMENT)로부터 수신
604
UE의 인증을 수행하기 위하여 네트워크 엔티티와 통신
606
네트워크 엔티티의 인증 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 네트워크 엔티티로부터 수신
608
암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용

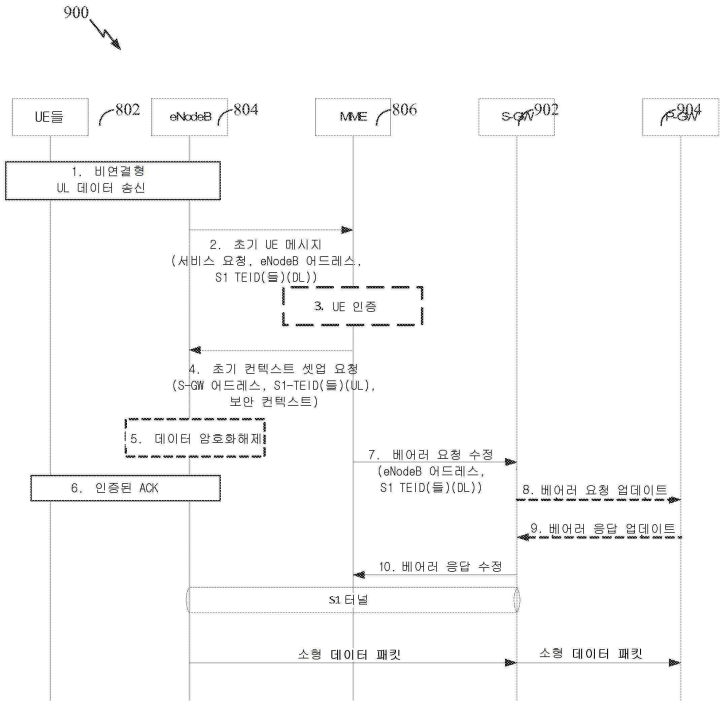
도면7


700
702
BS(BASE STATION)를 통해 UE(USER EQUIPMENT)와의 보안 연결을 설정
704
보안 연결을 통해, 전체 RRC(RADIO RESOURCE CONTROL) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상
706
UE의 인증을 수행하기 위하여 암호화된 데이터를 포함하는 패킷을 UE로부터 수신한 BS와 통신
708
UE의 인증 이후에 암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 BS에 제공
710
암호화해제 정보를 사용하여 암호화해제된 데이터를 BS로부터 수신

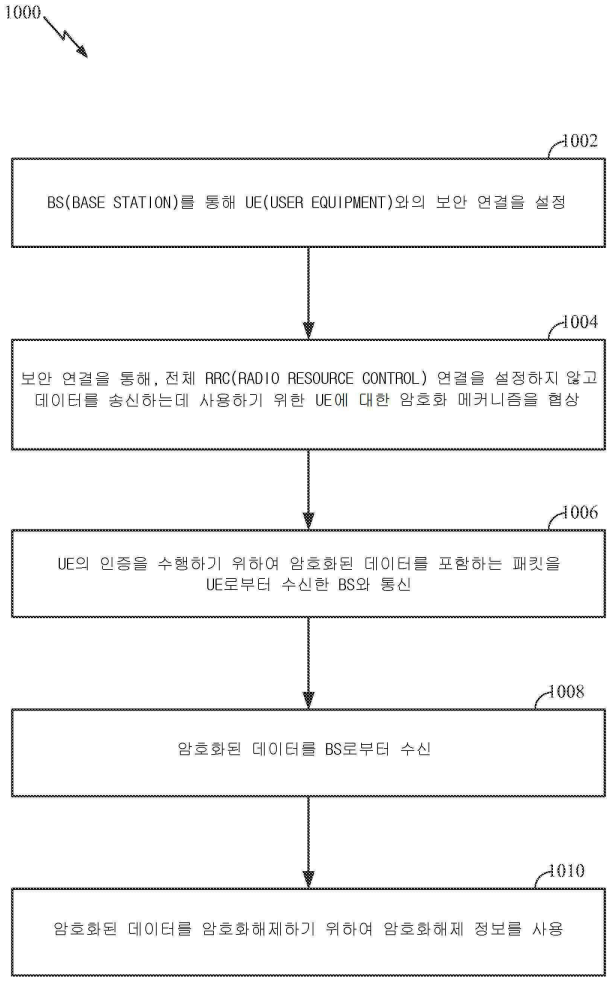
도면8


800
802
804
806
UE들
eNodeB
MME
1. 정규 RRC/NAS 연결
2. NAS: 비연결형 셋업 요청
(지원되는 암호화 메커니즘들)
3. NAS: 비연결형 셋업 응답
(암호화 메커니즘...)
4. RRC/NAS 연결 릴리스

도면9


900
UE들
802
eNodeB
804
MME
806
S-GW
902
P-GW
904
1. 비연결형 UL 데이터 송신
2. 초기 UE 메시지 (서비스 요청, eNodeB 어드레스, S1 TEID(들)(DL))
3. UE 인증
4. 초기 컨텍스트 셋업 요청 (S-GW 어드레스, S1-TEID(들)(UL), 보안 컨텍스트)
5. 데이터 암호화해제
6. 인증된 ACK
7. 베어러 요청 수정 (eNodeB 어드레스, S1 TEID(들)(DL))
8. 베어러 요청 업데이트
9. 베어러 응답 업데이트
10. 베어러 응답 수정
S1 터널
소형 데이터 패킷
소형 데이터 패킷

도면10


1000
1002
BS(BASE STATION)를 통해 UE(USER EQUIPMENT)와의 보안 연결을 설정
1004
보안 연결을 통해, 전체 RRC(RADIO RESOURCE CONTROL) 연결을 설정하지 않고 데이터를 송신하는데 사용하기 위한 UE에 대한 암호화 메커니즘을 협상
1006
UE의 인증을 수행하기 위하여 암호화된 데이터를 포함하는 패킷을 UE로부터 수신한 BS와 통신
1008
암호화된 데이터를 BS로부터 수신
1010
암호화된 데이터를 암호화해제하기 위하여 암호화해제 정보를 사용

【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 35

【변경전】

제 34 항에 있어서,

상기 명령들은 상기 장치로 하여금, 상기 암호화된 데이터를 성공적으로 암호화해제 후에, 상기 BS가 상기 암호화된 데이터를 성공적으로 암호화해제했음을 확인응답하는 메시지를 상기 UE로 송신하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 네트워크에서의 무선 통신을 위한 장치.

【변경후】

제 34 항에 있어서,

상기 명령들은 상기 장치로 하여금, 상기 암호화된 데이터를 성공적으로 암호화해제 후에, BS가 상기 암호화된 데이터를 성공적으로 암호화해제했음을 확인응답하는 메시지를 상기 UE로 송신하게 하도록 상기 적어도 하나의 프로세서에 의해 추가로 실행될 수 있는, 네트워크에서의 무선 통신을 위한 장치.