(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년01월27일
(11) 등록번호 10-2357094
(24) 등록일자 2022년01월25일

(51) 국제특허분류(Int. Cl.)
H04W 12/04 (2021.01) *H04W 12/06* (2021.01)
(52) CPC특허분류
H04W 12/04 (2021.01)
H04W 12/06 (2021.01)
(21) 출원번호 10-2017-7011984
(22) 출원일자(국제) 2015년10월23일
심사청구일자 2020년10월07일
(85) 번역문제출일자 2017년05월01일
(65) 공개번호 10-2017-0080591
(43) 공개일자 2017년07월10일
(86) 국제출원번호 PCT/US2015/057232
(87) 국제공개번호 WO 2016/073229
국제공개일자 2016년05월12일
(30) 우선권주장
62/074,513 2014년11월03일 미국(US)
14/919,397 2015년10월21일 미국(US)
(56) 선행기술조사문헌
KR1020090004896 A*
US20120155324 A1*
US20140004824 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
이 수범
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
호른 개빈 버나드
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
팔라니고운데르 아난드
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인코리아나

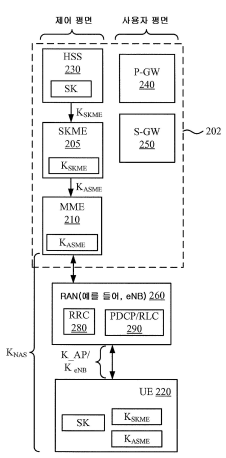
전체 청구항 수 : 총 60 항 심사관 : 이준석

(54) 발명의 명칭 **무선 통신을 위한 장치들 및 방법들**

(57) 요 약

인증 및 키 일치가 디바이스와 수행되고 디바이스와 연관된 인증 정보가 획득되며, 인증 정보는 인증 세션 키를 포함한다. 세션 키 관리 엔티티 (SKME) 는 인증 세션 키에 기초하여 이동성 세션 키를 생성하고 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 이동성 세션 키를 송신한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 2463/061 (2013.01)

명 세 서

청구범위

청구항 1

네트워크 디바이스에서 동작하는 방법으로서,

디바이스와 인증 및 키 일치를 수행하는 단계;

상기 네트워크 디바이스에서, 상기 디바이스와 연관된 인증 정보를 획득하는 단계로서, 상기 인증 정보는 적어도 인증 세션 키를 포함하는, 상기 인증 정보를 획득하는 단계;

상기 네트워크 디바이스에서, 상기 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 를 식별하는 MME 식별 값 및 상기 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하는 단계; 및

상기 디바이스를 서빙하는 상기 MME 에 상기 이동성 세션 키를 송신하는 단계를 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 2

제 1 항에 있어서,

상기 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하는 단계를 더 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 3

제 1 항에 있어서,

상기 인증 정보를 획득하는 단계는,

상기 디바이스와 연관된 인증 정보는 상기 네트워크 디바이스에 저장되지 않는 것을 결정하는 단계;

인증 정보 요청을 홈 가입자 서버에 송신하는 단계; 및

상기 인증 정보 요청을 송신하는 것에 응답하여 상기 홈 가입자 서버로부터 상기 디바이스와 연관된 상기 인증 정보를 수신하는 단계를 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 4

제 1 항에 있어서,

상기 인증 정보를 획득하는 단계는

상기 디바이스와 연관된 인증 정보가 상기 네트워크 디바이스에 저장되는 것을 결정하는 단계; 및

상기 네트워크 디바이스에서의 메모리 회로로부터 상기 인증 정보를 취출하는 단계를 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 5

제 4 항에 있어서,

상기 디바이스로부터 키 설정 식별자를 수신하는 단계; 및

상기 디바이스와 연관된 상기 인증 정보가 수신된 상기 키 설정 식별자에 기초하여 상기 네트워크 디바이스에 저장되는 것을 결정하는 단계를 더 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 6

제 1 항에 있어서,

상기 디바이스와 인증 및 키 일치를 수행하기 전에, 상기 디바이스로부터 발신하는 비액세스 계층 (NAS) 메시지를, 상기 MME 로부터 수신하는 단계를 더 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 7

제 1 항에 있어서,

상기 MME 식별 값은 글로벌 고유 MME 식별자 (globally unique MME identifier; GUMMEI) 인, 네트워크 디바이스에서 동작하는 방법.

청구항 8

제 1 항에 있어서, .

상기 MME 식별 값은 MME 그룹 식별자 (MMEGI) 인, 네트워크 디바이스에서 동작하는 방법.

청구항 9

제 1 항에 있어서,

상기 디바이스를 서빙하는 각각의 MME 에 대해 상이한 이동성 관리 키를 생성하는 단계를 더 포함하고,

상기 상이한 이동성 관리 키들의 각각은 각각의 MME 와 연관된 상이한 MME 식별 값 및 상기 인증 세션 키에 부분적으로 기초하는, 네트워크 디바이스에서 동작하는 방법.

청구항 10

제 1 항에 있어서,

MME 재위치와 관련하여, 제 2 MME 가 상기 디바이스를 서빙하려고 시도하고 있는 것을 결정하는 단계;

상기 제 2 MME 와 연관된 제 2 MME 식별 값 및 상기 인증 세션 키에 부분적으로 기초하여 제 2 이동성 관리 키를 생성하는 단계; 및

MME 재위치를 용이하게 하기 위해 상기 제 2 MME 에 상기 제 2 이동성 관리 키를 송신하는 단계를 더 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 11

제 1 항에 있어서,

카운터 값 키 카운트를 유지하는 단계; 및

추가로 카운터 값 키 카운트에 부분적으로 기초하여 상기 이동성 세션 키를 생성하는 단계를 더 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 12

제 1 항에 있어서,

상기 이동성 세션 키를 생성하는 단계는, 입력(들) 으로서 상기 인증 세션 키, 상기 MME 를 고유하게 식별하는 상기 MME 식별 값, 및 카운터 값 키 카운트 중 적어도 하나를 갖는 키 도출 함수를 사용하여 상기 이동성 세션 키를 도출하는 단계를 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 13

네트워크 디바이스로서,

데이터를 전송 및 수신하도록 구성된 통신 인터페이스; 및

상기 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

디바이스와 인증 및 키 일치를 수행하고;

상기 네트워크 디바이스에서, 상기 디바이스와 연관된 인증 정보를 획득하는 것으로서, 상기 인증 정보는 적어도 인증 세션 키를 포함하는, 상기 인증 정보를 획득하고;

상기 네트워크 디바이스에서, 상기 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 를 식별하는 MME 식별 값 및 상기 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하며, 그리고

상기 디바이스를 서빙하는 상기 MME 에 상기 이동성 세션 키를 송신하도록 구성되는, 네트워크 디바이스.

청구항 14

제 13 항에 있어서,

상기 프로세싱 회로는 또한,

상기 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하도록 구성되는, 네트워크 디바이스.

청구항 15

제 13 항에 있어서,

상기 인증 정보를 획득하도록 구성된 상기 프로세싱 회로는,

상기 디바이스와 연관된 인증 정보는 상기 네트워크 디바이스에 저장되지 않는 것을 결정하는 것;

인증 정보 요청을 홈 가입자 서버에 송신하는 것; 및

상기 인증 정보 요청을 송신하는 것에 응답하여 상기 홈 가입자 서버로부터 상기 디바이스와 연관된 상기 인증 정보를 수신하는 것을 포함하는, 네트워크 디바이스.

청구항 16

제 13 항에 있어서,

상기 프로세싱 회로는 또한,

상기 디바이스와 인증 및 키 일치를 수행하기 전에, 상기 디바이스로부터 발신하는 비액세스 계층 (NAS) 메시지를, 상기 MME 로부터 수신하도록 구성되는, 네트워크 디바이스.

청구항 17

제 16 항에 있어서,

수신된 상기 NAS 메시지는 상기 디바이스를 서빙하는 상기 MME 를 식별하는 상기 MME 식별 값 및 상기 디바이스를 식별하는 디바이스 식별자를 포함하는, 네트워크 디바이스.

청구항 18

네트워크 디바이스로서,

디바이스와 인증 및 키 일치를 수행하는 수단;

상기 네트워크 디바이스에서, 상기 디바이스와 연관된 인증 정보를 획득하는 수단으로서, 상기 인증 정보는 적어도 인증 세션 키를 포함하는, 상기 인증 정보를 획득하는 수단;

상기 네트워크 디바이스에서, 상기 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 를 식별하는 MME 식별 값 및 상기 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하는 수단; 및

상기 디바이스를 서빙하는 상기 MME 에 상기 이동성 세션 키를 송신하는 수단을 포함하는, 네트워크 디바이스.

청구항 19

제 18 항에 있어서,

상기 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하는 수단을 더 포함하는, 네트워크 디바이스.

청구항 20

네트워크 디바이스에서 동작하는 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 명령들은 적어도 하나의 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

디바이스와 인증 및 키 일치를 수행하게 하고;

상기 네트워크 디바이스에서, 상기 디바이스와 연관된 인증 정보를 획득하게 하는 것으로서, 상기 인증 정보는 적어도 인증 세션 키를 포함하는, 상기 인증 정보를 획득하게 하고;

상기 네트워크 디바이스에서, 상기 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 를 식별하는 MME 식별 값 및 상기 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하게 하고; 그리고

상기 디바이스를 서빙하는 상기 MME 에 상기 이동성 세션 키를 송신하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 21

제 20 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때 추가로 상기 프로세서로 하여금,

상기 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 22

네트워크 디바이스에서 동작하는 방법으로서,

디바이스로부터 비액세스 계층 (NAS) 메시지를 수신하는 단계;

상기 디바이스를 서빙하는 상기 네트워크 디바이스를 식별하는 네트워크 디바이스 식별 값과 함께 상기 NAS 메시지를 세션 키 관리 엔티티 (SKME) 디바이스에 포워딩하는 단계;

상기 SKME 디바이스로부터 이동성 세션 키를 수신하는 단계로서, 상기 이동성 세션 키는 상기 디바이스와 무선 통신 네트워크 사이에서 공유되는 키로부터 도출되었던 인증 세션 키 및 상기 네트워크 디바이스 식별 값에 부분적으로 기초하는, 상기 이동성 세션 키를 수신하는 단계; 및

상기 디바이스에 키 도출 데이터를 송신하는 단계로서, 상기 키 도출 데이터는 상기 디바이스가 상기 이동성 세션 키를 도출하는 것을 가능하게 하는, 상기 키 도출 데이터를 송신하는 단계를 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 23

제 22 항에 있어서,

상기 네트워크 디바이스 식별 값은 글로벌 고유 이동성 관리 엔티티 식별자 (GUMMEI) 인, 네트워크 디바이스에서 동작하는 방법.

청구항 24

제 22 항에 있어서,

상기 네트워크 디바이스 식별 값은 이동성 관리 엔티티 그룹 식별자 (MMEGI) 인, 네트워크 디바이스에서 동작하는 방법.

청구항 25

제 22 항에 있어서, .

상기 SKME 디바이스로부터 수신된 상기 이동성 세션 키는 추가로 상기 SKME 디바이스에서 유지되는 카운터 값 키 카운트에 부분적으로 기초하는, 네트워크 디바이스에서 동작하는 방법.

청구항 26

제 22 항에 있어서,

상기 키 도출 데이터는 상기 디바이스에 송신된 NAS 보안 모드 커맨드 메시지에 포함되는, 네트워크 디바이스에서 동작하는 방법.

청구항 27

제 22 항에 있어서,

상기 키 도출 데이터는 상기 네트워크 디바이스 식별 값을 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 28

제 22 항에 있어서,

상기 키 도출 데이터는 상기 SKME 디바이스에서 유지되는 카운터 값 키 카운트를 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 29

제 22 항에 있어서,

제 2 네트워크 디바이스가 상기 디바이스를 서빙할 필요가 있다는 것을 결정하는 단계;

상기 제 2 네트워크 디바이스가 상기 네트워크 디바이스와 공통 그룹 식별자를 공유하는 것을 결정하는 단계; 및

상기 이동성 세션 키를 상기 제 2 네트워크 디바이스에 송신하는 단계를 더 포함하는, 네트워크 디바이스에서 동작하는 방법.

청구항 30

제 29 항에 있어서,

상기 네트워크 디바이스 및 상기 제 2 네트워크 디바이스는 이동성 관리 엔티티들 (MME들) 이고 상기 공통 그룹 식별자는 공통 MME 그룹 식별자인, 네트워크 디바이스에서 동작하는 방법.

청구항 31

네트워크 디바이스로서,

데이터를 전송 및 수신하도록 구성된 통신 인터페이스; 및

상기 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

디바이스로부터 비액세스 계층 (NAS) 메시지를 수신하고;

상기 디바이스를 서빙하는 상기 네트워크 디바이스를 식별하는 네트워크 디바이스 식별 값과 함께 상기 NAS 메시지를 세션 키 관리 엔티티 (SKME) 디바이스에 포워딩하고;

상기 SKME 디바이스로부터 이동성 세션 키를 수신하는 것으로서, 상기 이동성 세션 키는 상기 디바이스와 무선 통신 네트워크 사이에서 공유되는 키로부터 도출되었던 인증 세션 키 및 상기 네트워크 디바이스 식별 값에 부분적으로 기초하는, 상기 이동성 세션 키를 수신하고; 그리고

상기 디바이스에 키 도출 데이터를 송신하는 것으로서, 상기 키 도출 데이터는 상기 디바이스가 상기 이동성 세션 키를 도출하는 것을 가능하게 하는, 상기 키 도출 데이터를 송신하도록 구성되는, 네트워크 디바이스.

청구항 32

제 31 항에 있어서,

상기 네트워크 디바이스 식별 값은 글로벌 고유 이동성 관리 엔티티 식별자 (GUMMEI) 인, 네트워크 디바이스.

청구항 33

제 31 항에 있어서, .

상기 SKME 디바이스로부터 수신된 상기 이동성 세션 키는 추가로 상기 SKME 디바이스에서 유지되는 카운터 값 키 카운트에 부분적으로 기초하는, 네트워크 디바이스.

청구항 34

제 31 항에 있어서,

상기 키 도출 데이터는 상기 네트워크 디바이스 식별 값을 포함하는, 네트워크 디바이스.

청구항 35

제 31 항에 있어서,

상기 프로세싱 회로는 또한,

제 2 네트워크 디바이스가 상기 디바이스를 서빙할 필요가 있다는 것을 결정하고;

상기 제 2 네트워크 디바이스가 상기 네트워크 디바이스와 공통 그룹 식별자를 공유하는 것을 결정하며; 그리고

상기 이동성 세션 키를 상기 제 2 네트워크 디바이스에 송신하도록 구성되는, 네트워크 디바이스.

청구항 36

네트워크 디바이스로서,

디바이스로부터 비액세스 계층 (NAS) 메시지를 수신하는 수단;

상기 디바이스를 서빙하는 상기 네트워크 디바이스를 식별하는 네트워크 디바이스 식별 값과 함께 상기 NAS 메시지를 세션 키 관리 엔티티 (SKME) 디바이스에 포워딩하는 수단;

상기 SKME 디바이스로부터 이동성 세션 키를 수신하는 수단으로서, 상기 이동성 세션 키는 상기 디바이스와 무선 통신 네트워크 사이에서 공유되는 키로부터 도출되었던 인증 세션 키 및 상기 네트워크 디바이스 식별 값에 부분적으로 기초하는, 상기 이동성 세션 키를 수신하는 수단; 및

상기 디바이스에 키 도출 데이터를 송신하는 수단으로서, 상기 키 도출 데이터는 상기 디바이스가 상기 이동성 세션 키를 도출하는 것을 가능하게 하는, 상기 키 도출 데이터를 송신하는 수단을 포함하는, 네트워크 디바이스.

청구항 37

제 36 항에 있어서,

제 2 네트워크 디바이스가 상기 디바이스를 서빙할 필요가 있다는 것을 결정하는 수단;

상기 제 2 네트워크 디바이스가 상기 네트워크 디바이스와 공통 그룹 식별자를 공유하는 것을 결정하는 수단; 및

상기 이동성 세션 키를 상기 제 2 네트워크 디바이스에 송신하는 수단을 더 포함하는, 네트워크 디바이스.

청구항 38

네트워크 디바이스에서 동작하는 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 명령들은 적어도 하나의 프로세서에 의해 실행될 때 상기 프로세서로 하여금,

디바이스로부터 비액세스 계층 (NAS) 메시지를 수신하게 하고;

상기 디바이스를 서빙하는 상기 네트워크 디바이스를 식별하는 네트워크 디바이스 식별 값과 함께 상기 NAS 메시지를 세션 키 관리 엔티티 (SKME) 디바이스에 포워딩하게 하고;

상기 SKME 디바이스로부터 이동성 세션 키를 수신하게 하는 것으로서, 상기 이동성 세션 키는 상기 디바이스와 무선 통신 네트워크 사이에서 공유되는 키로부터 도출되었던 인증 세션 키 및 상기 네트워크 디바이스 식별 값에 부분적으로 기초하는, 상기 이동성 세션 키를 수신하게 하며; 그리고

상기 디바이스에 키 도출 데이터를 송신하게 하는 것으로서, 상기 키 도출 데이터는 상기 디바이스가 상기 이동성 세션 키를 도출하는 것을 가능하게 하는, 상기 키 도출 데이터를 송신하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 39

제 38 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때 추가로 상기 프로세서로 하여금

제 2 네트워크 디바이스가 상기 디바이스를 서빙할 필요가 있다는 것을 결정하게 하고;

상기 제 2 네트워크 디바이스가 상기 네트워크 디바이스와 공통 그룹 식별자를 공유하는 것을 결정하게 하며; 그리고

상기 이동성 세션 키를 상기 제 2 네트워크 디바이스에 송신하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 40

디바이스에서 동작하는 방법으로서,

세션 키 관리 엔티티 (SKME) 디바이스와 인증 및 키 일치를 수행하는 단계;

홈 가입자 서버 (HSS) 와 공유된 비밀 키에 부분적으로 기초하여 인증 세션 키를 생성하는 단계로서, 상기 인증 세션 키는 상기 SKME 디바이스에 알려져 있는, 상기 인증 세션 키를 생성하는 단계;

상기 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 를 식별하는 MME 식별 값 및 상기 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하는 단계로서, 상기 이동성 세션 키는 상기 디바이스를 서빙하는 상기 MME 에 알려져 있는, 상기 이동성 세션 키를 생성하는 단계; 및

상기 이동성 세션 키를 사용하여 상기 디바이스로부터 무선 통신 네트워크에 전송된 데이터를 암호로 보안하는 단계를 포함하는, 디바이스에서 동작하는 방법.

청구항 41

제 40 항에 있어서,

상기 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하는 단계를 더 포함하는, 디바이스에서 동작하는 방법.

청구항 42

제 40 항에 있어서,

상기 SKME 디바이스로 성공적으로 인증된 후 상기 MME 로부터 키 도출 데이터를 수신하는 단계를 더 포함하고,

상기 키 도출 데이터는 상기 디바이스가 상기 이동성 세션 키를 도출하는 것을 가능하게 하는, 디바이스에서 동작하는 방법.

청구항 43

제 42 항에 있어서,

상기 키 도출 데이터는 상기 디바이스를 서빙하는 상기 MME 를 식별하는 상기 MME 식별 값을 포함하는, 디바이

스에서 동작하는 방법.

청구항 44

제 40 항에 있어서,

상기 MME 식별 값은 글로벌 고유 MME 식별자 (GUMMEI) 인, 디바이스에서 동작하는 방법.

청구항 45

제 40 항에 있어서,

상기 MME 식별 값은 MME 그룹 식별자 (MMEGI) 인, 디바이스에서 동작하는 방법.

청구항 46

제 42 항에 있어서,

상기 키 도출 데이터는 상기 SKME 디바이스에서 유지되는 카운터 값 키 카운트를 포함하는, 디바이스에서 동작하는 방법.

청구항 47

제 42 항에 있어서,

상기 키 도출 데이터는 상기 MME 로부터 수신된 보안 모드 커맨드 메시지에 포함되는, 디바이스에서 동작하는 방법.

청구항 48

제 40 항에 있어서,

상기 이동성 세션 키를 생성하는 단계는, 입력(들) 로서 상기 인증 세션 키, 상기 MME 를 고유하게 식별하는 상기 MME 식별 값, 및 카운터 값 키 카운트 중 적어도 하나를 갖는 키 도출 함수를 사용하여 상기 이동성 세션 키를 도출하는 단계를 포함하는, 디바이스에서 동작하는 방법.

청구항 49

제 40 항에 있어서,

상기 디바이스를 서빙하려고 시도하는 제 2 MME 를 고유하게 식별하는 제 2 MME 식별자를 포함하는 MME 재위치의 통지를 수신하는 단계;

상기 제 2 MME 를 고유하게 식별하는 상기 제 2 MME 식별자 및 상기 인증 세션 키에 부분적으로 기초하여 제 2 이동성 세션 키를 생성하는 단계를 더 포함하는, 디바이스에서 동작하는 방법.

청구항 50

제 40 항에 있어서,

상기 이동성 세션 키에 부분적으로 기초하여 노드 B 키 K_{eNB} 를 도출하는 단계; 및

상기 노드 B 키 K_{eNB} 를 사용하여 상기 디바이스를 서빙하는 무선 액세스 노드에 송신된 데이터를 암호화하는 단계를 더 포함하는, 디바이스에서 동작하는 방법.

청구항 51

디바이스로서,

무선 통신 네트워크로 데이터를 전송하고 상기 무선 통신 네트워크로부터 데이터를 수신하도록 구성된 무선 통신 인터페이스; 및

상기 무선 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

세션 키 관리 엔티티 (SKME) 디바이스와 인증 및 키 일치를 수행하고;

홈 가입자 서버 (HSS) 와 공유된 비밀 키에 부분적으로 기초하여 인증 세션 키를 생성하는 것으로서, 상기 인증 세션 키는 상기 SKME 디바이스에 알려져 있는, 상기 인증 세션 키를 생성하고;

상기 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 를 식별하는 MME 식별 값 및 상기 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하는 것으로서, 상기 이동성 세션 키는 상기 디바이스를 서빙하는 상기 MME 에 알려져 있는, 상기 이동성 세션 키를 생성하며; 그리고

상기 이동성 세션 키를 사용하여 상기 디바이스로부터 상기 무선 통신 네트워크에 전송된 데이터를 암호로 보안하도록 구성되는, 디바이스.

청구항 52

제 51 항에 있어서,

상기 프로세싱 회로는 또한,

상기 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하도록 구성되는, 디바이스.

청구항 53

제 51 항에 있어서,

상기 프로세싱 회로는 또한,

상기 SKME 디바이스로 성공적으로 인증된 후 상기 MME 로부터 키 도출 데이터를 수신하도록 구성되고,

상기 키 도출 데이터는 상기 디바이스가 상기 이동성 세션 키를 도출하는 것을 가능하게 하는, 디바이스.

청구항 54

제 53 항에 있어서,

상기 키 도출 데이터는 상기 디바이스를 서빙하는 상기 MME 를 식별하는 상기 MME 식별 값을 포함하는, 디바이스.

청구항 55

제 51 항에 있어서,

상기 이동성 세션 키를 생성하는 것은, 입력(들) 로서 상기 인증 세션 키, 상기 MME 를 고유하게 식별하는 상기 MME 식별 값, 및 카운터 값 키 카운트 중 적어도 하나를 갖는 키 도출 함수를 사용하여 상기 이동성 세션 키를 도출하는 것을 포함하는, 디바이스.

청구항 56

제 51 항에 있어서,

상기 프로세싱 회로는 또한,

상기 디바이스를 서빙하려고 시도하는 제 2 MME 를 고유하게 식별하는 제 2 MME 식별자를 포함하는 MME 재위치의 통지를 수신하고;

상기 제 2 MME 를 고유하게 식별하는 상기 제 2 MME 식별자 및 상기 인증 세션 키에 부분적으로 기초하여 제 2 이동성 세션 키를 생성하도록 구성되는, 디바이스.

청구항 57

디바이스로서,

세션 키 관리 엔티티 (SKME) 디바이스와 인증 및 키 일치를 수행하는 수단;

홈 가입자 서버 (HSS) 와 공유된 비밀 키에 부분적으로 기초하여 인증 세션 키를 생성하는 수단으로서, 상기 인증 세션 키는 상기 SKME 디바이스에 알려져 있는, 상기 인증 세션 키를 생성하는 수단;

상기 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 를 식별하는 MME 식별 값 및 상기 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하는 수단으로서, 상기 이동성 세션 키는 상기 디바이스를 서빙하는 상기 MME 에 알려져 있는, 상기 이동성 세션 키를 생성하는 수단; 및

상기 이동성 세션 키를 사용하여 상기 디바이스로부터 무선 통신 네트워크에 전송된 데이터를 암호로 보안하는 수단을 포함하는, 디바이스.

청구항 58

제 57 항에 있어서,

상기 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하는 수단을 더 포함하는, 디바이스.

청구항 59

디바이스에서 동작하는 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 명령들은 적어도 하나의 프로세서에 의해 실행될 때 상기 프로세서로 하여금,

세션 키 관리 엔티티 (SKME) 디바이스와 인증 및 키 일치를 수행하게 하고;

홈 가입자 서버 (HSS) 와 공유된 비밀 키에 부분적으로 기초하여 인증 세션 키를 생성하게 하는 것으로서, 상기 인증 세션 키는 상기 SKME 디바이스에 알려져 있는, 상기 인증 세션 키를 생성하게 하고;

상기 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 를 식별하는 MME 식별 값 및 상기 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하게 하는 것으로서, 상기 이동성 세션 키는 상기 디바이스를 서빙하는 상기 MME 에 알려져 있는, 상기 이동성 세션 키를 생성하게 하며; 그리고

상기 이동성 세션 키를 사용하여 상기 디바이스로부터 무선 통신 네트워크에 전송된 데이터를 암호로 보안하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 60

제 59 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때 추가로 상기 프로세서로 하여금,

상기 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 61

삭제

청구항 62

삭제

청구항 63

삭제

청구항 64

삭제

발명의 설명

기 술 분 야

[0001] 관련 출원들에 대한 상호 참조

[0002] 이 출원은 2014 년 11 월 3 일에 미국특허청 (USPTO) 에 출원되고 명칭이 "Apparatus and Method Having an Improved Cellular Network Key Hierarchy" 인 가출원 제 62/074,513 호 및 2015 년 10 월 21 일에 미국특허청에 출원되고 명칭이 "Apparatuses and Methods for Wireless Communication" 인 정규출원 제 14/919,397 호에 대한 우선권 및 이익을 주장하며, 그 전체 개시물들은 본 명세서에 참조로서 명백히 통합된다.

[0003] 분야

[0004] 본 개시물은 일반적으로 셀룰러 네트워크에 대한 개선된 키 계층구성 (hierarchy) 에 관련된다.

배 경 기 술

[0005] 도 1 에 나타낸 현재 셀룰러 네트워크 아키텍처 (100) 는, 사용자 장비 (120) 에 의해 셀룰러 네트워크로의 액세스를 제어하기 위한 절차들을 구현하기 위해 이동성 관리 엔티티 (MME)(110) 를 사용한다. 통상적으로, MME (110) 는 코어 네트워크 (102) 엘리먼트로서 네트워크 서비스 제공자에 의해 소유되고 동작되며, 네트워크 서비스 제공자에 의해 제어되는 보안 위치에 위치된다. 코어 네트워크 (102) 는 홈 가입자 서버 (HSS)(130) 및 MME (110) 를 포함한 제어 평면, 및 패킷 데이터 네트워크 (P-DN) 게이트웨이 (PGW)(140) 및 서빙 게이트웨이 (S-GW)(150) 를 포함한 사용자 평면을 갖는다. MME (110) 는 무선 액세스 노드 (160)(예를 들어, 진화된 노드 B (eNB)) 에 접속된다. RAN (160) 은 UE (120) 에 무선 인터페이스들 (예를 들어, 무선 리소스 제어 (RRC)(180) 및 패킷 데이터 수렴 프로토콜 (PDCP)/무선 링크 제어 (RLC)(190)) 를 제공한다.

[0006] 향후 셀룰러 네트워크 아키텍처들에서, MME들 (110) 또는 MME들 (110) 의 많은 기능들을 수행하는 네트워크 컴포넌트들은, 이들이 물리적으로 더 액세스가능하고 및/또는 다른 네트워크 오퍼레이터들로부터 격리되지 않기 때문에 덜 안전한, 네트워크 에지 쪽으로 밀리게 될 것이라는 것이 구상된다. 네트워크 기능들이, 예를 들어 클라우드 (예를 들어, 인터넷) 로 이동될 때, 이들은 물리적 격리의 더 낮은 레벨을 갖거나 물리적 격리를 갖지 않을 수도 있기 때문에 이들이 안전하다고 상정되지 않을 수도 있다. 또한, 네트워크 장비는 단일 네트워크 서비스 제공자에 의해 소유되지 않을 수도 있다. 일 예로서, 다중 MME 인스턴스들이 단일의 물리적 하드웨어 디바이스 내에 호스팅될 수도 있다. 그 결과, MME들로 전송된 키들은 보다 빈번하게 리프레싱을 필요로 할 수도 있고 이로써 MME들로 인증 벡터들 (AV들) 을 포워딩하는 것이 바람직하지 않을 수도 있다.

[0007] MME 기능들이 네트워크 에지에 근접하여 수행되는 향후의 셀룰러 네트워크 아키텍처들에 대한 부가 보안을 제공하는 개선된 장치들 및 방법들에 대한 필요성이 있다.

발명의 내용

과제의 해결 수단

[0008] 일 피처는 네트워크 디바이스에서 동작하는 방법을 제공하며, 방법은 디바이스와 인증 및 키 일치를 수행하는 단계, 디바이스와 연관된 인증 정보를 획득하는 단계로서, 인증 정보는 적어도 인증 세션 키를 포함하는, 인증 정보를 획득하는 단계, 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하는 단계, 및 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 이동성 세션 키를 송신하는 단계를 포함한다. 일 양태에 따라, 방법은 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하는 단계를 더 포함한다.
다른 양태에 따라, 인증 정보를 획득하는 단계는, 디바이스와 연관된 인증 정보는 네트워크 디바이스에 저장되지 않는 것을 결정하는 단계, 인증 정보 요청을 홈 가입자 서버에 송신하는 단계, 및 인증 정보 요청을 송신하는 것에 응답하여 홈 가입자 서버로부터 디바이스와 연관된 인증 정보를 수신하는 단계를 포함한다.

[0009] 일 양태에 따라, 인증 정보를 획득하는 단계는, 디바이스와 연관된 인증 정보가 네트워크 디바이스에 저장되는 것을 결정하는 단계, 및 네트워크 디바이스에서의 메모리 회로로부터 인증 정보를 취출하는 단계를 포함한다.
다른 양태에 따라, 방법은 디바이스로부터 키 설정 식별자를 수신하는 단계, 및 디바이스와 연관된 인증 정보가 수신된 키 설정 식별자에 기초하여 네트워크에 저장되는 것을 결정하는 단계를 더 포함한다. 또 다른 양태에 따라, 방법은 디바이스와 인증 및 키 일치를 수행하기 전에, 디바이스로부터 발신하는 비액세스 계층 (NAS) 메시지를 MME 로부터 수신하는 단계를 더 포함한다.

[0010] 일 양태에 따라, 방법은 MME 를 식별하는 MME 식별 값에 부분적으로 기초하여 이동성 세션 키를 생성하는 단계

를 더 포함한다. 다른 양태에 따라, MME 식별 값은 글로벌 고유 MME 식별자 (globally unique MME identifier; GUMMEI) 이다. 또 다른 양태에 따라, MME 식별 값은 MME 그룹 식별자 (MMEGI) 이다.

[0011] 일 양태에 따라, 방법은 디바이스를 서빙하는 각각의 MME 에 대해 상이한 이동성 관리 키를 생성하는 단계를 더 포함하고, 상이한 이동성 관리 키들의 각각은 각각의 MME 와 연관된 상이한 MME 식별 값 및 인증 세션 키에 부분적으로 기초한다. 다른 양태에 따라, 방법은 MME 재위치와 관련하여, 제 2 MME 가 디바이스를 서빙하려고 시도하고 있는 것을 결정하고, 제 2 MME 와 연관된 MME 식별 값 및 인증 세션 키에 부분적으로 기초하여 제 2 이동성 관리 키를 생성하며, 그리고 MME 재위치를 용이하게 하기 위해 제 2 MME 에 제 2 이동성 관리 키를 송신하는 단계를 더 포함한다. 또 다른 양태에 따라, 방법은 카운터 값 키 카운트 (Key Count) 를 유지하는 단계, 및 추가로 카운터 값 키 카운트에 부분적으로 기초하여 이동성 세션 키를 생성하는 단계를 더 포함한다. 다른 양태에 따라, 이동성 세션 키를 생성하는 단계는, 입력(들) 으로서 인증 세션 키, MME 를 고유하게 식별하는 MME 식별 값, 및/또는 카운터 값 키 카운트 중 적어도 하나를 갖는 키 도출 함수를 사용하여 이동성 세션 키를 도출하는 단계를 포함한다.

[0012] 다른 피처는, 데이터를 전송 및 수신하도록 구성된 통신 인터페이스, 및 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하는 네트워크 디바이스를 제공하며, 프로세싱 회로는, 디바이스와 인증 및 키 일치를 수행하고, 디바이스와 연관된 인증 정보를 획득하는 것으로서, 인증 정보는 적어도 인증 세션 키를 포함하는, 상기 인증 정보를 획득하고, 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하며, 그리고 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 이동성 세션 키를 송신하도록 구성된다. 일 양태에 따라, 프로세싱 회로는 또한, 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하도록 구성된다. 다른 양태에 따라, 인증 정보를 획득하도록 구성된 프로세싱 회로는, 디바이스와 연관된 인증 정보는 네트워크 디바이스에 저장되지 않는 것을 결정하는 것, 인증 정보 요청을 홈 가입자 서버에 송신하는 것, 및 인증 정보 요청을 송신하는 것에 응답하여 홈 가입자 서버로부터 디바이스와 연관된 인증 정보를 수신하는 것을 포함한다.

[0013] 일 양태에 따라, 프로세싱 회로는 또한, 추가로 MME 를 식별하는 MME 식별 값에 부분적으로 기초하여 이동성 세션 키를 생성하도록 구성된다. 다른 양태에 따라, 프로세싱 회로는 또한, 디바이스와 인증 및 키 일치를 수행하기 전에, 디바이스로부터 발신하는 비액세스 계층 (NAS) 메시지를, MME 로부터 수신하도록 구성된다. 또 다른 양태에 따라, 수신된 NAS 메시지는 MME 를 식별하는 MME 식별 값 및 디바이스를 식별하는 디바이스 식별자를 포함한다.

[0014] 또 다른 피처는, 디바이스와 인증 및 키 일치를 수행하는 수단, 디바이스와 연관된 인증 정보를 획득하는 수단으로서, 인증 정보는 적어도 인증 세션 키를 포함하는, 인증 정보를 획득하는 수단, 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하는 수단, 및 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 이동성 세션 키를 송신하는 수단을 포함하는, 네트워크 디바이스를 제공한다. 일 양태에 따라, 네트워크 디바이스는 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하는 수단을 더 포함한다.

[0015] 다른 피처는, 네트워크 디바이스에서 동작하는 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체를 제공하며, 명령들은 적어도 하나의 프로세서에 의해 실행될 때, 프로세서로 하여금, 디바이스와 인증 및 키 일치를 수행하게 하고, 디바이스와 연관된 인증 정보를 획득하게 하는 것으로서, 인증 정보는 적어도 인증 세션 키를 포함하는, 인증 정보를 획득하게 하고, 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하게 하며, 그리고 이동성 세션 키를 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 송신하게 한다. 일 양태에 따라, 명령들은 프로세서에 의해 실행될 때 추가로 프로세서로 하여금, 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하게 한다.

[0016] 다른 피처는, 네트워크 디바이스에서 동작하는 방법을 제공하며, 방법은 디바이스로부터 비액세스 계층 (NAS) 메시지를 수신하는 단계, 네트워크 디바이스를 식별하는 네트워크 디바이스 식별 값과 함께 NAS 메시지를 세션 키 관리 엔티티 (SKME) 디바이스에 포워딩하는 단계, SKME 디바이스로부터 이동성 세션 키를 수신하는 단계로서, 이동성 세션 키는 디바이스와 무선 통신 네트워크 사이에서 공유되는 키로부터 도출되었던 인증 세션 키에 부분적으로 기초하는, 이동성 세션 키를 수신하는 단계, 및 디바이스로 키 도출 데이터를 송신하는 단계로서, 키 도출 데이터는 디바이스가 이동성 세션 키를 도출하는 것을 가능하게 하는, 상기 키 도출 데이터를 송신하는 단계를 포함한다. 일 양태에 따라, SKME 디바이스로부터 수신된 이동성 세션 키는 추가로 네트워크 디바이스 식별 값에 부분적으로 기초한다. 다른 양태에 따라, SKME 디바이스로부터 수신된 이동성 세션 키는 추가로 네트워크 디바이스 식별 값에 부분적으로 기초한다. 다른 양태에 따라, 네트워크 디바이스 식별 값

은 글로벌 고유 이동성 관리 엔티티 식별자 (GUMMEI) 이다.

[0017] 일 양태에 따라, 네트워크 디바이스 식별 값은 이동성 관리 엔티티 그룹 식별자 (MMEGI) 이다. 다른 양태에 따라, SKME 디바이스로부터 수신된 이동성 세션 키는 추가로 SKME 디바이스에서 유지되는 카운터 값 키 카운트에 부분적으로 기초한다. 또 다른 양태에 따라, 키 도출 데이터는 디바이스에 송신된 NAS 보안 모드 커맨드 메시지에 포함된다.

[0018] 일 양태에 따라, 키 도출 데이터는 네트워크 디바이스 식별 값을 포함한다. 다른 양태에 따라, 키 도출 데이터는 SKME 디바이스에서 유지되는 카운터 값 키 카운트를 포함한다. 또 다른 양태에 따라, 방법은 제 2 네트워크 디바이스가 디바이스를 서빙할 필요가 있다는 것을 결정하는 단계, 제 2 네트워크 디바이스가 네트워크 디바이스와 공통 그룹 식별자를 공유하는 것을 식별하는 단계, 및 이동성 세션 키를 제 2 네트워크 디바이스에 송신하는 단계를 더 포함한다. 또 다른 양태에 따라, 네트워크 디바이스 및 제 2 네트워크 디바이스는 이동성 관리 엔티티들 (MME들) 이고 공통 그룹 식별자는 공통 MME 그룹 식별자이다.

[0019] 다른 피처는, 데이터를 전송 및 수신하도록 구성된 통신 인터페이스, 및 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하는 네트워크 디바이스를 제공하며, 프로세싱 회로는, 디바이스로부터 비액세스 계층 (NAS) 메시지를 수신하고, 네트워크 디바이스를 식별하는 네트워크 디바이스 식별 값과 함께 NAS 메시지를 세션 키 관리 엔티티 (SKME) 디바이스에 포워딩하고, SKME 디바이스로부터 이동성 세션 키를 수신하는 것으로서, 이동성 세션 키는 디바이스와 무선 통신 네트워크 사이에서 공유되는 키로부터 도출되었던 인증 세션 키에 부분적으로 기초하는, 상기 이동성 세션 키를 수신하고, 그리고 디바이스에 키 도출 데이터를 송신하는 것으로서, 키 도출 데이터는 디바이스가 이동성 세션 키를 도출하는 것을 가능하게 하는, 상기 키 도출 데이터를 송신하도록 구성된다. 일 양태에 따라, 프로세싱 회로는 또한, 제 2 네트워크 디바이스가 디바이스를 서빙할 필요가 있다는 것을 결정하고, 제 2 네트워크 디바이스가 네트워크 디바이스와 공통 그룹 식별자를 공유하는 것을 식별하며, 그리고 이동성 세션 키를 제 2 네트워크 디바이스에 송신하도록 구성된다.

[0020] 다른 피처는, 디바이스로부터 비액세스 계층 (NAS) 메시지를 수신하는 수단, 네트워크 디바이스를 식별하는 네트워크 디바이스 식별 값과 함께 NAS 메시지를 세션 키 관리 엔티티 (SKME) 디바이스에 포워딩하는 수단, SKME 디바이스로부터 이동성 세션 키를 수신하는 수단으로서, 이동성 세션 키는 디바이스와 무선 통신 네트워크 사이에서 공유되는 키로부터 도출되었던 인증 세션 키에 부분적으로 기초하는, 상기 이동성 세션 키를 수신하는 수단, 및 디바이스에 키 도출 데이터를 송신하는 수단으로서, 키 도출 데이터는 상기 디바이스가 상기 이동성 세션 키를 도출하는 것을 가능하게 하는, 상기 키 도출 데이터를 송신하는 수단을 포함하는, 네트워크 디바이스를 제공한다. 일 양태에 따라, 제 2 네트워크 디바이스가 디바이스를 서빙할 필요가 있다는 것을 결정하는 수단, 제 2 네트워크 디바이스가 네트워크 디바이스와 공통 그룹 식별자를 공유하는 것을 결정하는 수단, 및 이동성 세션 키를 제 2 네트워크 디바이스에 송신하는 수단을 더 포함한다.

[0021] 다른 피처는, 네트워크 디바이스에서 동작하는 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체를 제공하며, 명령들은 적어도 하나의 프로세서에 의해 실행될 때 프로세서로 하여금, 디바이스로부터 비액세스 계층 (NAS) 메시지를 수신하게 하고, 네트워크 디바이스를 식별하는 네트워크 디바이스 식별 값과 함께 NAS 메시지를 세션 키 관리 엔티티 (SKME) 디바이스에 포워딩하게 하고, SKME 디바이스로부터 이동성 세션 키를 수신하게 하는 것으로서, 이동성 세션 키는 디바이스와 무선 통신 네트워크 사이에서 공유되는 키로부터 도출되었던 인증 세션 키에 부분적으로 기초하는, 상기 이동성 세션 키를 수신하게 하며, 그리고 디바이스에 키 도출 데이터를 송신하게 하는 것으로서, 키 도출 데이터는 디바이스가 이동성 세션 키를 도출하는 것을 가능하게 하는, 키 도출 데이터를 송신하게 한다. 일 양태에 따라, 명령들은 프로세서에 의해 실행될 때 추가로 프로세서로 하여금, 제 2 네트워크 디바이스가 디바이스를 서빙할 필요가 있다는 것을 결정하게 하고, 제 2 네트워크 디바이스가 네트워크 디바이스와 공통 그룹 식별자를 공유하는 것을 결정하게 하며, 그리고 이동성 세션 키를 제 2 네트워크 디바이스에 송신하게 한다.

[0022] 다른 피처는, 디바이스에서 동작하는 방법을 제공하며, 방법은 세션 키 관리 엔티티 (SKME) 디바이스와 인증 및 키 일치를 수행하는 단계, 홈 가입자 서버 (HSS) 와 공유된 비밀 키에 부분적으로 기초하여 인증 세션 키를 생성하는 단계로서, 인증 세션 키는 SKME 디바이스에 알려져 있는, 상기 인증 세션 키를 생성하는 단계, 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하는 단계로서, 이동성 세션 키는 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 알려져 있는, 상기 이동성 세션 키를 생성하는 단계, 및 이동성 세션 키를 사용하여 디바이스로부터 무선 통신 네트워크에 전송된 데이터를 암호로 보안하는 단계를 포함한다. 일 양태에 따라, 방법은 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하는 단계를 더

포함한다. 다른 양태에 따라, SKME 디바이스로 성공적으로 인증된 후 MME 로부터 키 도출 데이터를 수신하는 단계를 더 포함하고, 키 도출 데이터는 디바이스가 이동성 세션 키를 도출하는 것을 가능하게 한다.

[0023] 일 양태에 따라, 키 도출 데이터는 디바이스를 서빙하는 MME 를 식별하는 MME 식별 값을 포함하고, 방법은, 추가로 MME 식별 값에 부분적으로 기초하여 이동성 세션 키를 생성하는 단계를 더 포함한다. 다른 양태에 따라, 키 도출 데이터는 SKME 디바이스에서 유지되는 카운터 값 키 카운트를 포함한다. 다른 양태에 따라, 키 도출 데이터는 MME 로부터 수신된 보안 모드 커맨드 메시지에 포함된다.

[0024] 일 양태에 따라, 이동성 세션 키를 생성하는 단계는, 입력(들) 로서 인증 세션 키, MME 를 고유하게 식별하는 MME 식별 값, 및/또는 카운터 값 키 카운트 중 적어도 하나를 갖는 키 도출 함수를 사용하여 상기 이동성 세션 키를 도출하는 단계를 포함한다. 다른 양태에 따라, 방법은 디바이스를 서빙하려고 시도하는 제 2 MME 를 고유하게 식별하는 MME 식별자를 포함하는 MME 재위치의 통지를 수신하는 단계, 제 2 MME 를 고유하게 식별하는 MME 식별자 및 인증 세션 키에 부분적으로 기초하여 제 2 이동성 세션 키를 생성하는 단계를 더 포함한다. 또 다른 양태에 따라, 방법은 이동성 세션 키에 부분적으로 기초하여 노드 B 키 K_{eNB} 를 도출하는 단계, 및 노드 B 키 K_{eNB} 를 사용하여 디바이스를 서빙하는 무선 액세스 노드에 송신된 데이터를 암호화하는 단계를 더 포함한다.

[0025] 다른 피처는 무선 통신 네트워크로 데이터를 전송하고 상기 무선 통신 네트워크로부터 데이터를 수신하도록 구성된 무선 통신 인터페이스, 및 무선 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하는, 디바이스를 제공하며, 프로세싱 회로는, 세션 키 관리 엔티티 (SKME) 디바이스와 인증 및 키 일치를 수행하고, 홈 가입자 서버 (HSS) 와 공유된 비밀 키에 부분적으로 기초하여 인증 세션 키를 생성하는 것으로서, 인증 세션 키는 SKME 디바이스에 알려져 있는, 상기 인증 세션 키를 생성하고, 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하는 것으로서, 이동성 세션 키는 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 알려져 있는, 이동성 세션 키를 생성하며, 그리고 이동성 세션 키를 사용하여 디바이스로부터 무선 통신 네트워크에 전송된 데이터를 암호로 보안하도록 구성된다. 일 양태에 따라, 프로세싱 회로는 또한, 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하도록 구성된다. 다른 양태에 따라, 프로세싱 회로는 또한, SKME 디바이스로 성공적으로 인증된 후 MME 로부터 키 도출 데이터를 수신하도록 구성되고, 키 도출 데이터는 디바이스가 이동성 세션 키를 도출하는 것을 가능하게 한다. 또 다른 양태에 따라, 키 도출 데이터는 디바이스를 서빙하는 MME 를 식별하는 MME 식별 값을 포함하고, 프로세싱 회로는 또한, 추가로 MME 식별 값에 부분적으로 기초하여 이동성 세션 키를 생성하도록 구성된다.

[0026] 일 양태에 따라, 이동성 세션 키를 생성하는 것은, 입력(들) 로서 인증 세션 키, MME 를 고유하게 식별하는 MME 식별 값, 및/또는 카운터 값 키 카운트 중 적어도 하나를 갖는 키 도출 함수를 사용하여 이동성 세션 키를 도출하는 것을 포함한다. 다른 양태에 따라, 프로세싱 회로는 또한, 디바이스를 서빙하려고 시도하는 제 2 MME 를 고유하게 식별하는 MME 식별자를 포함하는 MME 재위치의 통지를 수신하고, 제 2 MME 를 고유하게 식별하는 MME 식별자 및 인증 세션 키에 부분적으로 기초하여 제 2 이동성 세션 키를 생성하도록 구성된다.

[0027] 다른 피처는, 세션 키 관리 엔티티 (SKME) 디바이스와 인증 및 키 일치를 수행하는 수단, 홈 가입자 서버 (HSS) 와 공유된 비밀 키에 부분적으로 기초하여 인증 세션 키를 생성하는 수단으로서, 인증 세션 키는 SKME 디바이스에 알려져 있는, 상기 인증 세션 키를 생성하는 수단, 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하는 수단으로서, 이동성 세션 키는 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 알려져 있는, 이동성 세션 키를 생성하는 수단, 및 이동성 세션 키를 사용하여 디바이스로부터 무선 통신 네트워크에 전송된 데이터를 암호로 보안하는 수단을 포함하는, 디바이스를 제공한다. 일 양태에 따라, 디바이스는 인증 세션 키에 기초하여 상이한 MME들에 대해 상이한 이동성 세션 키들을 생성하는 수단을 더 포함한다.

[0028] 다른 피처는, 디바이스에서 동작하는 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체를 제공하며, 명령들은 적어도 하나의 프로세서에 의해 실행될 때 프로세서로 하여금, 세션 키 관리 엔티티 (SKME) 디바이스와 인증 및 키 일치를 수행하게 하고, 홈 가입자 서버 (HSS) 와 공유된 비밀 키에 부분적으로 기초하여 인증 세션 키를 생성하게 하는 것으로서, 인증 세션 키는 SKME 디바이스에 알려져 있는, 상기 인증 세션 키를 생성하게 하고, 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하게 하는 것으로서, 이동성 세션 키는 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 알려져 있는, 상기 이동성 세션 키를 생성하게 하며, 그리고 이동성 세션 키를 사용하여 디바이스로부터 무선 통신 네트워크에 전송된 데이터를 암호로 보안한다. 일 양태에 따라, 명령들은 프로세서에 의해 실행될 때 추가로 프로세서 하여금, 인증 세션 키에 기초하여 상이한 MME들에

대해 상이한 이동성 세션 키들을 생성하게 한다.

도면의 간단한 설명

[0029] 도 1 은 종래 기술에서 발견된 무선 통신 시스템의 일 예의 블록 다이어그램이다.

도 2 는 무선 통신 네트워크를 도시한다.

도 3a 및 도 3b 는 무선 통신 네트워크에서 동작하는 프로세스 플로우 다이어그램을 도시한다.

도 4 및 도 5 는 사용자 장비가 로밍하고 이에 따라 홈 네트워크의 외부의 방문 네트워크에 있는 시나리오들을 도시한다.

도 6 은 무선 통신 네트워크에 대한 키 계층구성의 개략적 다이어그램을 도시한다.

도 7 은 무선 통신 네트워크에 접속하는 UE 에 대한 어태치 절차 및 초기 데이터 전송의 플로우 다이어그램을 도시한다.

도 8 은 S1-핸드오버 절차의 플로우 다이어그램을 도시한다.

도 9a 및 도 9b 는 MME 재위치를 필요로 하는 새로운 위치로 UE 가 이동한 후의 추적 영역 업데이트 절차의 플로우 다이어그램을 도시한다.

도 10 은 디바이스의 개략적 블록 다이어그램을 도시한다.

도 11 은 디바이스 프로세싱 회로의 개략적 블록 다이어그램을 도시한다.

도 12 는 디바이스에서 동작하는 방법을 도시한다.

도 13 은 네트워크 디바이스의 개략적 블록 다이어그램을 도시한다.

도 14 는 네트워크 디바이스 프로세싱 회로의 제 1 예시적인 개략적 블록 다이어그램을 도시한다.

도 15 는 네트워크 디바이스 프로세싱 회로의 제 2 예시적인 개략적 블록 다이어그램을 도시한다.

도 16 은 네트워크 디바이스에서 동작하는 제 1 예시적인 방법을 도시한다.

도 17 은 네트워크 디바이스에서 동작하는 제 2 예시적인 방법을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0030] 본 명세서에서 단어 "예시적인" 은 "예, 예증 또는 예시로서 작용하는" 을 의미하도록 사용된다. "예시적인" 으로서 본 명세서에 기재된 임의의 실시형태는 반드시 다른 실시형태들 보다 선호되거나 이로운 것으로 해석되지 않는다.

[0031] 도 2 는 개시물의 일 양태에 따른 무선 통신 네트워크 (200) 를 도시한다. 무선 통신 네트워크 (200) 는 코어 네트워크 (202), 무선 액세스 노드 (예를 들어, eNB)(260), 및 무선 통신 디바이스 (예를 들어, UE)(220) 를 포함한다. 코어 네트워크는, 특히 세션 키 관리 엔티티 (SKME) 디바이스 (205)(본 명세서에서 "인증 세션 키 앵커 기능 디바이스" 로서 지칭될 수도 있음), MME (210), HSS (230), P-GW (240), 및 S-GW (250) 을 포함한다. SKME 디바이스 (205), MME (210), 및 HSS (230) 은 제어 평면을 포함하는 한편, P-GW (240) 및 S-GW (250) 은 사용자 평면을 포함한다. 이러한 무선 통신 네트워크 (200) 의 아키텍처는 제 5 세대 (5G) 셀룰러 네트워크에서 사용될 수도 있다.

[0032] 무선 액세스 노드 (260) 는, 예를 들어 진화된 노드 B (eNB) 일 수도 있고 MME (210) 및 UE (220) 와 통신할 수도 있다. RAN (260) 은 UE (220) 에 무선 인터페이스들 (예를 들어, 무선 리소스 제어 (RRC)(280) 및 패킷 데이터 수렴 프로토콜 (PDCP)/무선 링크 제어 (RLC)(290)) 을 제공한다.

[0033] SKME (205) 는 무선 통신 네트워크 (200) 내부에 깊게 위치된 신뢰 앵커 또는 키 앵커일 수도 있다. SKME (205) 는 그것이 서빙하는 각각의 MME (210) 에 대해 이동성 세션 키들 (예를 들어, 키 K_{ASME}) 를 도출한다 (도 2 는 단지 하나 (1) 의 MME (210) 를 도시하지만, SKME (205) 는 복수의 MME들과 통신하고 및/또는 복수의 MME들을 서빙할 수도 있다). 따라서, MME들 (210) 및/또는 MME들의 기능들을 수행하는 네트워크 디바이스들이 네트워크의 에지로 밀려날 때 (즉, RAN 에 근접하거나 RAN 과 병치), SKME (205) 는 외부 엔티티들로부터의 물리적 액세스가 금지되는 네트워크 (200) 내부에 깊게 머무른다. 이러한 방식으로 SKME (205) 는 MME (210)

와 HSS (230) 사이에서 중개자로서 작용한다.

[0034] HSS (230) 은 UE (220) 와 무선 통신 네트워크의 인증 센터 (AuC)(도 2 에 나타내지 않음) 사이에 공유되는 하나 이상의 비밀 키들 (SK) 에 기초하여 인증 세션 키 (예를 들어, 키 K_{SKME}) 를 생성한다. 하나 이상의 비밀 키들은, 예를 들어 루트 키일 수도 있고 및/또는 루트 키로부터 도출된 칩퍼 키 (CK) 및 무결성 키 (IK) 일 수도 있다. 인증 세션 키 (K_{SKME}) 는 SKME (205) 로 전송되며, 이는 결국 인증 세션 키 (K_{SKME}) 에 부분적으로 기초하여 이동성 세션 키 (K_{ASME})를 생성한다. 그 후 SKME (205) 는 그것이 생성되었던 MME (210) 로 이동성 세션 키 (K_{ASME}) 를 전송한다. eNB 키 (K_{eNB}) 와 같은 다른 키들은 이동성 세션 키 (K_{ASME}) 로부터 도출되고 RAN (260) 과 UE (220) 사이의 통신을 보안하기 위해 사용될 수도 있다.

[0035] 도 3a 및 도 3b 는 개시물의 일 양태에 따른 무선 통신 네트워크 (200) 의 프로세스 플로우 다이어그램 (300) 을 도시한다. 네트워크 (200) 의 일부 컴포넌트들 (예를 들어, RAN (260), P-GW (240), S-GW (250)) 은 명료함을 위해 도 3 으로부터 생략되었다.

[0036] 도 3a 를 참조하면, 프로세스는 UE (220) 가 비액세스 계층 (NAS) 메시지를 MME (210) 에 (예를 들어, 도 3a 에 도시되지 않은 RAN (260) 을 통해) 송신하는 것으로 시작할 수도 있다. 특히, NAS 메시지는, 예를 들어 어태치 요청, 후속 서비스 요청, 또는 추적 영역 업데이트 요청일 수도 있다. 일부 경우들에서, NAS 메시지는 UE (220) 와 연관된 키 설정 식별자 (KSI) 및/또는 UE (220) 를 식별하는 디바이스 식별자 (예를 들어, 국제 모바일 가입자 아이덴티티 (IMSI)) 를 포함할 수도 있다. MME (210) 은 그 후 NAS 메시지 및 KSI (포함되는 경우) 를 SKME (205) 로 포워드 (304) 할 수도 있다. SKME (205) 는 다음으로 UE (220) 에 대한 인증 정보가 SKME (205) 에 이미 저장되어 있는지 여부를 결정 (306) 할 수도 있다. 그렇다면, SKME (205) 는 UE (220) 와 인증 및 키 일치 (AKA) 를 수행 (312) 하기 위해 UE (220) 에 대해 저장된 인증 정보 (예를 들어, 인증 벡터) 를 사용한다. 그렇지 않다면, SKME (205) 는 UE (220) 와 연관된 인증 정보를 요청하는 인증 정보 요청을 HSS (230) 에 송신 (308) 할 수도 있다. 이에 대응하여, HSS (230) 는 SKME (205) 에 하나 이상의 인증 벡터들 (예를 들어, 인증 정보) 를 제공 (310) 할 수도 있다. 제공된 인증 벡터들 중 적어도 하나는 UE (220) 와 연관되고 UE (200) 와 AKA 를 수행 (312) 하기 위해 사용될 수 있다. 인증 벡터는 예상된 응답 (XRES), 인증 값 (AUTN), 난수 (RAND) 를 포함할 수도 있고, 인증 세션 키 (K_{SKME}) 는 "제 1 인증 세션 키 (K_{SKME})", "제 2 인증 세션 키 (K_{SKME})" 등으로 본 명세서에서 지칭될 수도 있다. AUTN 은 UE (220) 가 HSS (230) 와 공유하는 비밀 키 및 시퀀스 수에 기초할 수도 있다.

[0037] 인증 세션 키 (K_{SKME}) 는 네트워크의 AuC 와 UE 사이에 공유되는 하나 이상의 비밀 키들에 부분적으로 기초하여 HSS 에서 생성될 수도 있다. 이들 비밀 키들은 루트 키 및/또는 루트 키로부터 도출된 칩퍼 키 (CK) 및 무결성 키 (IK) 를 포함할 수도 있다. AKA 를 추가로 수행하기 위해, SKME (205) 는 인증 응답 (RES) 을 요청하는 인증 요청 메시지 (예를 들어, AUTN 및 RAND 를 포함) 를 UE (220) 에 송신할 수도 있다. SKME (205) 는 그 후 UE (220) 와의 인증이 성공적인지 여부를 결정하도록 매치를 위해 RES 를 XRES 와 비교할 수도 있다.

[0038] AKA (312) 의 성공적인 완료 후, SKME (205) 는 UE (220) 에 의해 제공된 KSI (있다면) 에 기초하여 UE (220) 에 대해 적절한 인증 세션 키 (K_{SKME}) 를 식별 (314) 할 수도 있다. 이것은 SKME (205) 가 HSS (230) 로부터 복수의 인증 세션 키들 (K_{SKME}) 를 갖는 복수의 인증 벡터들을 수신하는 경우 행해질 수도 있다. SKME (205) 는 그 후 이동성 관리 키 (K_{ASME})(예를 들어, "제 1 이동성 관리 키 (K_{ASME})", "제 2 이동성 관리 키 (K_{ASME})", "제 3 이동성 관리 키 (K_{ASME})" 등) 를 도출/생성 (316) 할 수도 있다. 이동성 관리 키 (K_{ASME}) 는 인증 세션 키 (K_{SKME}), MME 식별 값 (예를 들어, 글로벌 고유 MME 식별자 (GUMMI), MME 식별자 (MMEI), MME 그룹 식별자 (MMEGI), 공중 육상 모바일 네트워크 식별자 (PLMN ID), MME 코드 (MMEC) 등), 및/또는 카운터 값 (예를 들어, 키 카운트) 에 기초할 수도 있다. 따라서, K_{ASME} 는 K_{ASME} = KDF(K_{SKME}, MME 식별 값 | 키 카운트) 로서 도출될 수도 있으며, 여기서 KDF 는 키 도출 함수이다. 카운터 값 키 카운트는 MME (210) 로의 역 재위치가 발생할 때마다 SKME (205) 가 동일한 MME (210) 에 대해 프레시 (fresh) K_{ASME} 키를 도출하는 것을 가능하게 하기 위해 SKME (205) 에 의해 증가될 수도 있는 카운터 값이다. 일 양태에 따라, 한번 사용된 수 (임시값 (nonce)) 는 카운터 값 키 카운트 대신 사용될 수도 있다. 다른 양태에 따라, MME 식별 값 (예를 들어, GUMMEI, MMEGI, MMEI, MMEC, PLMN ID 등) 은 그것이 특정 MME 아이덴티티를 인증하기 위해 사용되지 않는 경우 생략될

수도 있다. 예를 들어, SKME (205) 은 그것이 K_{ASME} 를 제공하는 MME들 (210) 과 항상 동일한 네트워크에 있으면, 키 도출에 MME 식별 값을 포함시키는 것이 불필요할 수도 있다. 따라서, 다른 예에 따라, K_{ASME} 는 K_{ASME} = KDF(K_{SKME}, 임시값) 또는 K_{ASME} = KDF(K_{SKME}, 키 카운트) 로서 도출될 수도 있다. MME 식별 값은 네트워크 디바이스 식별 값의 일 예일 수도 있다.

[0039] 다음, SKME (205) 는 그것이 생성되었던 MME (210) 에 이동성 세션 키 (K_{ASME}) 를 전송 (318) 할 수도 있다. MME (210) 는 UE (220) 가 이동성 세션 키 (K_{ASME}) 를 생성하는 것을 돕기 위해 UE (220) 에 키 도출 데이터 (KDD) 를 전송 (320) 할 수도 있다. 일 예에 따라, 키 도출 데이터는 비액세스 계층 (NAS) 보안 모드 커맨드 (SMC) 에 포함될 수도 있다. 키 도출 데이터는 MME 식별 값 (예를 들어, GUMMEI, MMEGI, MMEI, MMEC, PLMN ID 등) 을 포함할 수도 있고, 카운터 값 키 카운트 및/또는 키 (K_{ASME}) 를 생성하는데 사용되었던 임시값을 포함할 수도 있다. 이 데이터로, UE (220) 는 그 후 키 (K_{ASME}) 를 생성/도출 (322) 하고 그것을 그 자체와 무선 통신 네트워크/서빙 네트워크 (예를 들어, MME (210), SKME (205) 등) 사이에서, 데이터 트래픽과 같은 통신을 보안하기 위해 사용한다. MME (210) 와 UE (220) 는 또한 이동성 관리 키 (K_{ASME}) 에 기초하여 후속 키들 (예를 들어, K_{eNB}, K_{NASenc}, K_{NASint}, NK 등) 을 생성/도출 (324) 하고 이들을 UE (220), MME (210), 및/또는 UE (220)를 서빙하는 RAN (예를 들어, eNB)(260) 사이의 통신들을 보안하기 위해 사용한다.

[0040] 일 양태에 따라, 인증 세션 키 (K_{SKME}) 는 입력들로서 비밀 키 (예를 들어, CK, IK 등) 및 서빙 네트워크 아이덴티티 (SN_id) 를 갖는 제 1 키 도출 함수를 사용하여 도출될 수도 있다. 이동성 세션 키 (K_{ASME}) 는 제 2 키 도출 함수를 사용하여 도출될 수도 있다. 제 1 및 제 2 키 도출 함수들은, 예를 들어 키-해시 메시지 인증 코드 (key-hashed message authentication code; HMAC) HMAC-256, HMAC-SHA-256, HMAC-SHA-3 등에 기초할 수도 있다. 인증 및 키 일치는 확장가능 인증 프로토콜 (EAP), 또는 특정 NAS 시그널링을 사용하여 수행될 수도 있다. 이동성 세션 키 (K_{ASME}) 는 AKA 절차 (UE 와 현재 어태치된 UME 에 대해) 동안, 또는 MME 재위치를 수반하는 핸드오버 동안 도출될 수도 있다. 세션은 SKME (205) 에 의해 현재 어태치된 MME 에 대해 정의될 수도 있다. MME 재위치는 MMEGI 를 공유하는 MME 들의 그룹 내에서 수행될 수도 있다. 대안으로, MME 재위치는 상이한 MMEGI 를 갖는 다른 MME 로 수행될 수도 있다. 일 양태에 따라, GUMMEI 는 MMEGI 및 MME 코드의 조합에 기초할 수도 있다.

[0041] 개시물의 일 양태에 따라, MME 는 보안 보호되는 통신 채널을 통해 SKME (300) 로부터 이동성 세션 키 (K_{ASME}) 를 수신할 수도 있다. 다른 양태에 따라, MME 재위치 동안 타겟 MME 는, 2 개의 MME들이 동일한 MME 그룹에 속하는 경우 (예를 들어 양자가 동일한 MME 그룹 식별자 (MMEGI) 를 가짐), 다른 MME 에 의해 사용된 키 K_{ASME} 를 수신할 수도 있다.

[0042] 도 4 및 도 5 는 도 2 에 나타낸 UE (220) 가 로밍하고 있고 이로써 홈 네트워크 (202) 의 외부에서 방문 네트워크 (400) 에 있는 시나리오들을 도시한다. 그러한 경우, 방문 네트워크의 SKME (405) 는 로컬 키 앵커가 되고 또한 UE (220) 와 상호 인증 (예를 들어, AKA) 을 수행하며, 일반적으로 도 3 에 관하여 상술한 프로세스에 후속한다. 유사하게, 방문 네트워크 내에서 MME 재위치 (예를 들어, 핸드오버 또는 추적 영역 업데이트) 동안, 방문 네트워크 (400) 의 로컬 SKME (405) 는 신규 K_{ASME} 를 도출하고 그것을 타겟/신규 MME 에 제공한다.

키 K_{eNB} 는 신규 K_{ASME} 로부터 도출될 수도 있다. 도 2, 도 4 및 도 5 에서, 키 K_{NAS} 는 UE (220) 와 MME (210) 사이에서 제어 메시지들을 보안하는데 사용된다.

[0043] 도 6 은 상술한 무선 통신 네트워크 (200) 에 대한 키 계층구성의 개략적 다이어그램을 도시한다. UE 의 유니버셜 가입자 아이덴티티 모듈 (USIM) 및 네트워크의 인증 센터 (AuC) 는 루트 키를 저장할 수도 있다. 루트 키로부터, 무결성 키 (IK) 및 칩퍼 키 (CK) 가 도출되고 HSS 에 제공된다. 루트 키, CK 및 IK 는 UE 와 네트워크 사이에 공유된 공유 비밀 키들로 고려될 수도 있다.

[0044] HSS 는 결국 인증 세션 키 (K_{SKME}) 를 생성하고 그것을 SKME 에 제공할 수도 있다. 세션 키 K_{SKME} 는 전체 인증 세션 동안 유효하다. SKME 는 K_{SKME} 를 활용하여 이동성 세션 키 (K_{ASME}) 를 생성하고 그 키를 UE 를 서빙하는 MME 에 제공할 수도 있다. 일 양태에서, 이동성 세션 키 (K_{ASME}) 는 특정 MME 에 대해서만 유효할 수도 있다. 다른 양태들에서, 이동성 세션 키 (K_{ASME}) 는 동일한 그룹 (예를 들어, 동일한 MMEGI 를 가짐) 의 MME

들 사이에서 공유될 수도 있다. UE 를 서빙하는 MME 는 결국 K_{ASME} 에 기초하여 다른 키들 (K_{NASenc}, K_{NASint}, K_{eNB}/NH 등) 을 생성할 수도 있다.

[0045] **어태치, 핸드오버 및 추적 영역 업데이트 (TAU) 프로세스들**

[0046] 네트워크로의 초기 어태치 동안, UE 는 세션 키 관리 엔티티 (SKME) 와 인증 및 키 일치 (AKA) 를 수행한다. 인증이 성공적이면, SKME 는 UE 가 어태치되는 MME 에 대해 키 (예를 들어, K_{ASME}) 를 도출하고 그 키를 MME 에 제공한다.

[0047] MME 재위치를 수반하는 추적 영역 업데이트 (TAU) 가 UE 에 의해 요청될 때, 그 TAU 요청을 수신하는 신규 MME 는 SKME 로부터 신규 키 (K_{ASME}) 를 수신하고 NAS SMC 절차를 수행하는 것에 의해 UE 와 보안 연관성을 확립한다. 유사하게, MME 재위치를 수반하는 핸드오버가 발생할 때, 타겟 MME 는 또한 SKME 로부터 신규 키 (K_{ASME}) 를 얻고 UE 와 보안 연관성을 확립한다.

[0048] 2 개의 추적 영역들을 지원하는 MME 는 UE 가 추적 영역들 사이에서 이동할 때 이동성 세션 키 (KS_{ASME}) 의 변화를 초기화한다. 이것은 UE 로부터 네트워크 구성을 은닉한다. 예를 들어, UE들은 추적 영역들만 보고 MME들은 보지 않을 수도 있다. 이것은 추적 영역들을 변화시키는 핸드오버 또는 TAU 양자에 응답하여 발생할 수도 있다.

[0049] 도 7 은 개시물의 일 양태에 따라 무선 통신 네트워크 (예를 들어, 무선 셀룰러 네트워크) 에 접속하는 UE 에 대한 어태치 절차 및 초기 데이터 전송의 플로우 다이어그램을 도시한다. 먼저, UE (220) 는 어태치 요청 (702) 을 RAN (260) 에 송신하고, 이는 결국 요청을 MME (210) 에 포워드하며, 이는 결국 요청을 (가능하다면 KSI 정보와 함께) SKME (205) 에 포워드한다. SKME (205) 는 그 후 인증 정보 요청 (704) 을 HSS (230) 에 송신할 수도 있고 이에 대응하여 그것은 예상된 응답 (XRES), 인증값 (AUTN), 난수 (RAND), 및 인증 세션 키 (K_{SKME}) 을 포함할 수도 있는 하나 이상의 인증 벡터들 (706) 을 HSS (230) 로부터 수신한다. AUTN 은 UE (220) 가 HSS (230) 와 공유하는 비밀 키 및 시퀀스 수에 기초할 수도 있다.

[0050] 일단 SKME (205) 가 UE (220) 와 연관된 인증 벡터를 가지면, UE (220) 및 SKME (205) 는 AKA (708) 를 수행할 수도 있다. AKA 가 일단 성공적이면, SKME (205) 는 인증 세션 키 (K_{SKME}), MME 식별값 (예를 들어, GUMMEI, MMEI, MMEGI 등), 및/또는 카운터 값 (예를 들어, 키 카운트) 에 기초하여 이동성 세션 키 (K_{ASME}) 를 도출할 수도 있다. 따라서, K_{ASME} 는 K_{ASME} = KDF(K_{SKME}, MME 식별 값 | 키 카운트) 로서 도출될 수도 있고, 여기서 KDF 는 키 도출 함수이다. 카운터 값 키 카운트는 MME (210) 로의 역 핸드오버가 발생할 때마다 SKME (205) 가 동일한 MME (210) 에 대해 프레시 K_{ASME} 키를 도출하는 것을 가능하게 하기 위해 SKME (205) 에 의해 증가될 수도 있는 카운터 값이다. 일 양태에 따라, 한번 사용된 수 (임시값) 가 카운터 값 대신 사용될 수도 있다. 다른 양태에 따라, GUMMEI 는 특정 MME 아이덴티티를 인증하기 위해 사용되지 않는 경우 생략될 수도 있다. 예를 들어, SKME (205) 는 그것이 K_{ASME} 를 제공하는 MME들과 항상 동일한 네트워크에 있으면, 키 도출에 GUMMEI 를 포함하는 것이 불필요할 수도 있다. 따라서, 다른 예에 따라, K_{ASME} 는 K_{ASME} = KDF(K_{SKME}, 임시값) 로서 도출될 수도 있다. 그 후 이동성 세션 키 (K_{ASME}) 는 MME (210) 에 전송 (710) 된다. MME (210) 는 그 후 UE (220) 로 NAS SMC 절차를 수행 (712) 하기 위해 이동성 세션 키 (K_{ASME}) 를 사용할 수도 있다. NAS SMC 절차 동안, MME (210) 는 그것의 GUMMEI 및/또는 키 카운트를 UE (220) 에 제공할 수도 있어서 UE (220) 가 또한 K_{ASME} 를 도출할 수 있다. 도 7 에 나타낸 나머지 단계들 (714-828) 은 4G LTE 셀룰러 통신 프로토콜들에서 발견된 것들과 유사할 수도 있다.

[0051] 도 8 은 개시물의 일 양태에 따른 S1-핸드오버 절차의 플로우 다이어그램을 도시한다. 먼저, 소스 eNB (260a)(즉, 현재 eNB) 는 핸드오버 (HO) 요구 메시지 (802) 를 소스 MME (210a)(즉, 현재 MME) 에 송신한다. 다음, 소스 MME (210a) 는 HO 요구 메시지에 기초하여 타겟 MME (210b)(즉, 신규 MME) 에 재위치 요청 (804) 을 송신/포워드한다. 타겟 MME (210b) 는 세션 요청 (806) 을 생성하고 타겟 서빙 게이트웨이 (S-GW)(250b) 에 송신하며 타겟 S-GW (250b) 로부터 세션 응답 (808) 을 수신할 수도 있다. 타겟 MME (210b) 는 또한 이동성 세션 키 K_{ASME} 에 대한 키 요청 (810) 을 SKME (205) 에 송신할 수도 있다. 그렇게 하는데 있어서, 타겟 MME (210b) 는 그 MME 식별 값 (예를 들어, GUMMEI) 을 SKME (205) 에 제공할 수도 있다.

SKME (205) 는 결국 MME 의 GUMMEI, HSS (230)(위에 기재됨) 로부터 이전에 수신된 인증 세션 키 (K_{SKME}), 및 키 카운트를 사용하여 이동성 세션 키 (K_{ASME}) 를 생성할 수도 있다. 일 양태에 따라, 한번 사용된 수 (임시값) 는 키 카운트 대신 사용될 수도 있다. 다른 양태에 따라, 특정 MME 아이덴티티를 인증하는 것이 바람직하지 않은 경우, GMMEI 는 생략될 수도 있다. SKME (205) 는 타겟 MME (210b) 에 K_{ASME} (812) 를 송신한다. 일 양태에 따라, 타겟 MME (210b) 는 세션 요청 (806) 을 타겟 S-GW (250b) 에 송신하고 대략 동일한 시간에 키 요청 (810) 을 송신할 수도 있다. 따라서, 단계들 (806 및 810) 은 단계들 (808 및 812) 과 동시에 수행될 수도 있다.

[0052] 타겟 MME (210b) 는 그 후 핸드오버 요청 (814) 을 타겟 eNB (260b)(즉, 잠재적 신규 eNB) 에 송신할 수도 있고 이에 대응하여 타겟 eNB (260b) 는 핸드오버 응답 (816) 을 역 전송한다. 핸드오버 요청 (814) 은 K_{ASME} 를 사용하여 타겟 MME (210b) 에 의해 도출된 키 K_{eNB} 를 포함할 수도 있다. 핸드오버 응답 (816) 은 타겟 eNB (260b) 가 핸드오버를 허용하는 것에 동의하는지 여부를 표시한다. 타겟 eNB (260b) 가 핸드오버를 허용하는 것에 동의하면 타겟 MME (210b) 는 키 (즉, K_{ASME}) 확인응답 메시지 (818) 를 SKME (205) 에 전송한다.

키 확인응답 메시지를 수신할 시, SKME (205) 는 그 후 키 카운트 카운터 값을 증가시킬 수도 있다. 키 확인응답 메시지 (818) 를 전송하는 단계는 핸드오버 요청 확인응답 (816) 이 수신될 때까지 지연되는데 이는 핸드오버 요청이 타겟 eNB (260b) 에 의해 거절될 수도 있기 때문이다. 그러한 경우, 신규 K_{ASME} 는 UE (220) 에 의해 도출될 필요가 없고 이 경우 SKME (205) 는 키 카운트를 증가할 필요가 없을 수도 있다. 타겟 MME (210b) 가 소스 MME (210a) 에 재위치 응답 (820) 을 전송한 후, 소스 MME (210a) 는 UE (220) 에 포워드되는 (824) 소스 eNB (260a) 에 핸드오버 커맨드 (822) 를 전송한다. 핸드오버 커맨드 (822, 824) 는, UE (220) 가 타겟 eNB (260b) 에 대한 신규 K_{eNB} 및 신규 K_{ASME} 을 도출할 수 있도록 키 카운트 및 타겟 MME (210b) 의 GUMMEI 를 포함할 수도 있다. UE (220) 는 타겟 eNB (260b) 에 핸드오버 확인 메시지 (826) 로 응답한다. 핸드오버 확인 메시지 (826) 는 무결성 보호되고 칩퍼될 수도 있다.

[0053] 도 9a 및 도 9b 는 개시물의 일 양태에 따른 MME 재위치를 요구하는 신규 위치로 UE (220) 를 이동한 후의 추적 영역 업데이트 절차의 플로우 다이어그램을 도시한다. 도 9a 를 참조하면, 먼저, UE (220) 는 추적 영역 업데이트 요청을 생성하고 RAN (260)(예를 들어, eNB) 에 송신한다. eNB (260) 는 결국 추적 영역 업데이트 요청을 UE (220) 와 연관되고 및/또는 UE (220) 를 서빙하는 타겟 MME (210b)(예를 들어, "신규 MME") 에 포워드한다 (904). eNB (260) 는 어느 신규 MME (210b) 가 UE (220) 의 위치를 포함한 다양한 기준에 기초하여 추적 영역 업데이트 요청을 전송할지를 결정한다. 추적 영역 업데이트 요청은, UE (220) 와 현재 연관된 MME 인, 소스 MME (210a)(예를 들어, "구 MME") 의 GUMMEI 를 포함하는 글로벌 고유 임시 식별자 (GUTI) 를 포함할 수도 있다. 타겟 MME (210b) 는 그 후 UE 콘택스트 요청 메시지를 소스 MME (210a) 에 송신하기 (906) 위해 그것이 수신하는 추적 영역 업데이트 요청에서 GUMMEI 를 사용할 수도 있다. 소스 MME (210a) 는 그 후 UE 콘택스트 응답 메시지에서 UE 콘택스트 정보로 응답한다 (908). 확인응답은, 이 응답이 일단 수신되면 타겟 MME (210b) 로부터 소스 MME (210a) 로 전송될 수도 있다.

[0054] 타겟 MME (210b) 는 그 후 위치 업데이트 및 키 요청 (즉, K_{ASME} 키 요청) 을 SKME (205) 에 전송할 수도 있다.

위치 업데이트는 그 후 위치 소거 메시지를 소스 MME (210a) 에 전송하는 HSS (230) 에 포워드된다. 이에 대응하여, 소스 MME (210a) 는 위치 소거 확인응답 메시지를 HSS (230) 에 역 송신할 수도 있다 (916). SKME (205) 는 이전에 기재된 바와 같이 키 카운트 카운터 값 및/또는 타겟 MME (210b) 의 GMMEI 에 기초하여 타겟 MME (210b) 의 신규 K_{ASME} 를 생성할 수도 있다. 일 양태에 따라, 한번 사용된 수 (임시값) 가 키 카운트 대신 사용될 수도 있다. 다른 양태에 따라, GUMMEI 는 그것이 특정 MME 아이덴티티를 인증하기를 원치 않는 경우 생략될 수도 있다. 신규 K_{ASME} 는 타겟 MME (210b) 로 송신된다. SKME (205) 로부터 K_{ASME} 를 수신할 시, 타겟 MME (210b) 는 SKME (205) 에 키 확인응답 메시지로 회신 (920) 한다. 일 양태에 따라, 타겟 MME (210b) 는 그것이 위치 업데이트 및 키 요청을 SKME (205) 에 송신 (912) 하는 대략 동일한 시간에 소스 MME (210a) 에 UE 콘택스트 요청 메시지를 송신 (906) 할 수도 있다. 따라서, 단계들 (906, 908, 및 910) 은 단계들 (912, 914, 916, 918, 920) 과 동시에 수행될 수도 있다.

[0055] 도 9b 를 참조하면, 타겟 MME (210b) 가 일단 SKME (205) 로부터 K_{ASME} 를 수신하면, 타겟 MME (210b) 는 그 후 UE (220) 로 비액세스 계층 보안 모드 커맨드 절차를 수행 (922, 924) 한다. 보안 모드 커맨드 절차 동안, UE (220) 는 타겟 MME (210b) 에 의해 사용된 키 (K_{ASME}) 를 도출하는데 이는 타겟 MME (210b) 가 UE (220) 에

그 GUMMEI 를 제공하기 때문이다. 또한 UE (220) 가 일단 타겟 MME (210b) 와 동일한 K_{ASME} 를 가지면, UE (220) 및 타겟 MME (210b) 는 K_{ASME} 키에 기초하여 보안 통신들에 관여할 수도 있다. 예를 들어, 타겟 MME (210b) 는 K_{ASME} 또는 K_{ASME} 로부터 도출된 다른 키들 (예를 들어, NAS 암호화 및 무결성 보호 키들) 에 의해 통신들이 암호화되는 UE (220) 와 추적 영역 업데이트 교환에 관여 (926, 928) 할 수도 있다. 이러한 교환은 타겟 MME 의 GUMMEI 에 기초하여 신규 GUTI 를 포함하는, 타겟 MME (210b) 으로부터 UE (220) 에 전송된 메시지를 포함할 수도 있다. 그러한 메시지는 다시 K_{ASME} 또는 K_{ASME} 로부터 도출된 다른 키에 의해 암호화된다.

[0056] 도 9b 에 나타내고 위에 기재된 바와 같이, NAS SMC (922, 924) 다음 추적 영역 업데이트 프로세스 (926, 928) 가 후속한다. 개시물의 일부 양태들에서, NAS SMC (922, 924) 및 추적 영역 업데이트 프로세스 (926, 928) 는 결합될 수도 있다. 예를 들어, 타겟 MME (210b) 로부터 UE (220) 로 전송된 NAS SMC 메시지 (922) 는 추적 영역 업데이트 메시지 (926) 와 결합될 수도 있다. 그렇게 하는데 있어서, 결합된 메시지의 일 부분 (예를 들어, 추적 영역 업데이트와 연관된 부분) 만이 암호화될 수도 있는 한편, UE 가 K_{ASME} 를 도출하는 것을 돕는 메시지의 부분은 암호화되지 않고 남겨진다. MME 에 의해 배정되는, GUTI 의 부분인, 신규 임시 모바일 가입자 아이덴티티 (TMSI) 는 암호화될 수도 있다.

[0057] **키 도출**

[0058] 위에 논의된 바와 같이, AKA 는 UE 와 SKME 사이에서 실행된다. 키 K_{SKME} 는 HSS 에 의해 도출되고 SKME 로 전송된다. HSS 의 관점으로부터, 인증 벡터들은 4G LTE 와 동일한 방식으로 구성되고 MME 대신 SKME 에 전송된다. 따라서, HSS 는 임의의 수정 없이 SKME 에 접속될 수도 있다.

[0059] SKME 는 주어진 MME 에 대한 이동성 세션 키 (K_{ASME}) 를 도출하고 이로써 MME 의 GUMMEI 는 K_{ASME} 키 도출 프로세스에 사용될 수도 있다. NAS 카운트 값은 신규 K_{ASME} 에 대해 제로 (0) 으로 초기화될 수도 있다. 일 예에서, 구 NAS 카운트 값들은 추적 영역 업데이트(들) 이 완성되지 않는다면 폐기되지 않는다. 키 (K_{ASME}) 의 프레시성 (freshness) 에 대하여, UE 및 SKME 는 키 카운트 카운터 값을 유지하고 그것을 K_{ASME} 도출을 위해 사용할 수도 있다. 이것은 UE 가 다시 MME 로 역 이동하는 경우들에서 동일한 K_{ASME} 를 도출하는 것을 회피하기 위해 행해질 수도 있다. 키 카운트 카운터 값은 초기 AKA 가 성공적으로 수행될 때 제로 (0) 또는 일부 다른 미리 결정된 값으로 초기화될 수도 있다. 일부 양태들에서, 임시값은 키 카운트 카운터 값 대신 사용될 수도 있다. 다른 양태에서, GUMMEI 는 키 도출로부터 생략될 수도 있다.

[0060] 키들 (K_{SKME}, K_{ASME}, K_{eNB}, 다음 홉 (NH) 등) 을 생성하기 위해 사용된 키 도출 함수 (KDF) 는 HMAC-SHA-256, HMAC-SHA-3 등을 활용할 수도 있다. 입력 스트링 (S) 은 n + 1 입력 파라미터들로부터 구성될 수도 있다. 예를 들어, $S = [FC \,||\, P_0 \,||\, L_0 \,||\, P_1 \,||\, L_1 \,||\, P_2 \,||\, L_2 \,||\, \cdots \,||\, P_N \,||\, L_N]$. 필드 코드 (FC) 는 알고리즘의 상이한 인스턴스들 사이를 구별하기 위해 사용된 단일 옥텟 (octet) 일 수도 있고 0x50 - 0x5F 범위의 값을 사용할 수도 있다. 입력 파라미터들 (P_0 내지 P_N) 은 n + 1 입력 파라미터 인코딩들이다. P_0 는 정적 ASCII-인코딩된 스트링일 수도 있다. 값들 (L_0 내지 L_N) 은 대응 입력 파라미터들 (P_0 내지 P_N) 의 길이의 2 개의 옥텟 표현들이다.

[0061] K_{SKME} 도출

[0062] $K_{SKME} = KDF(K_{CK/IK}, S)$. 입력 (S) 는 $[FC \,||\, P_0 \,||\, L_0 \,||\, P_1 \,||\, L_1]$ 와 동일할 수도 있으며, 여기서 FC = 0x50, P_0 = SN id, L_0 = SN id 의 길이 (즉, L_0 = 0x00 0x03), P_1 = SQN XOR AK, 그리고 L_1 = P_1 의 길이 (즉, L_1 = 0x00 0x06). SQN 은 시퀀스 수이고 AK 는 익명 키이며, XOR 는 배타적 OR 연산이다. 값 SQN XOR AK 은 인증 토큰 (AUTN) 의 부분으로서 UE 에 전송된다. AK 가 사용되지 않으면 AK 는 TS 33.102 (즉, 000 …0) 에 따라 처리될 수도 있다. 입력 키 $K_{CK/IK}$ 는 칩퍼 키 (CK) 및 무결성 키 (IK) 의 연결 (concatenation), 즉 $K_{CK/IK}$ = CK || IK 이다.

[0063] K_{ASME} 도출

[0064] $K_{ASME} = KDF(K_{SKME}, S)$. 입력 S 는 $[FC \,||\, P_0 \,||\, L_0 \,||\, P_1 \,||\, L_1]$ 와 동일할 수도 있으며, 여기서 FC = 0x51,

P_0 = GUMMEI, L_0 = 48 비트 GUMMEI 의 길이 (즉, L_0 = 0x00 0x06), P_1 = 키 카운트, 그리고 L_1 은 P_1 의 길이와 동일할 수도 있다 (예를 들어, L_1 = 0x00 0x08). 이것은 단지 K_{ASME} 가 어떻게 도출될 수 있는지의 일 예이다. 다른 양태들에서, GUMMEI 는 생략될 수도 있고 한번 사용된 난수 (예를 들어, 임시값) 는 키 카운트 카운터 값 대신 사용될 수도 있다.

[0065] NH 도출

[0066] $NH = KDF(K_{ASME}, S)$. 입력 S 는 [FC || P_0 || L_0] 와 동일할 수도 있고, 여기서 FC = 0x52, P_0 = Sync-입력, L_0 = Sync-입력의 길이 (즉, L_0 = 0x00 0x20). Sync-입력 파라미터는 초기 NH 도출에 대해 신규 도출된 K_{eNB}, 그리고 모든 후속 도출들에 대한 이전 NH 일 수도 있다. 이것은 NH 체인을 초래하며, 여기서 다음 NH 는 항상 새로우며 이전 NH 로부터 도출된다.

[0067] K_{eNB} 도출

[0068] $K'_{eNB} = KDF(K_X, S)$. 핸드오버 목적들에 대한 조항 7.2.8 에 명시된 바와 같이 eNB 및 UE 에서 타겟 물리 셀 식별자 및 프레시 NH 로부터 또는 현재 K_{eNB} 로부터 K'_{eNB} 를 도출할 때, 입력 (S) 는 [FC || P_0 || L_0 || P_1 || L_1] 와 동일할 수도 있으며, 여기서 FC = 0x53, P_0 = 타겟 물리 셀 식별자 (PCI), L_0 = PCI 의 길이 (예를 들어, L_0 = 0x00 0x02), P_1 = EARFCN-DL (타겟 물리 셀 다운링크 주파수), 그리고 L_1 = P_1 의 길이 (예를 들어, L_1 = 0x00 0x02). 입력 키 (K_X) 는, 핸드오버에서의 인덱스가 증가하거나 그렇지 않으면 현재 256 비트 K_{eNB} 가 사용될 때 256 비트 다음 홉 (HN) 키 일 수도 있다.

[0069] 위에 나타내고 기재된 도 7 내지 도 9 는 MME들이 소스로부터 타겟 MME 로 변화하는 것을 가정한다. 하지만, 단일 MME 가 2 개의 MME들 (소스 MME 및 타겟 MME) 의 역할을 가정하고 2 개의 MME들 사이에 실제 간섭이 없을 때 동일한 프로세스 플로우 다이어그램이 사용될 수도 있다.

[0070] 도 10 은 개시물의 일 양태에 따른 디바이스 (1000)(예를 들어, "사용자 디바이스", "사용자 장비", "무선 통신 디바이스") 의 개략적 블록 다이어그램을 도시한다. 디바이스 (1000) 는 집적 회로, 복수의 집적 회로들, 또는 하나 이상의 집적 회로들을 통합하는 전자 디바이스일 수도 있다. 디바이스 (1000) 는 또한 무선 통신 디바이스, 예컨대 모바일 폰, 스마트 폰, 랩탑, 개인용 디지털 보조기 (PDA), 테블릿, 컴퓨터, 스마트워치, 및 헤드 장착형 웨어러블 컴퓨터 (예를 들어, Google Glass®) 일 수도 있지만, 이에 제한되지 않는다. 디바이스 (1000) 는 서로 통신가능하게 커플링될 수도 있는, 적어도 하나 이상의 무선 통신 인터페이스들 (1002), 하나 이상의 메모리 회로들 (1004), 하나 이상의 입력 및/또는 출력 (I/O) 디바이스들/회로들 (1006), 및/또는 하나 이상의 프로세싱 회로들 (1008) 을 포함할 수도 있다. 예를 들어, 인터페이스 (1002), 메모리 회로 (1004), I/O 디바이스들 (1006), 및 프로세싱 회로 (1008) 는 버스 (1010) 를 통해 서로 통신가능하게 커플링될 수도 있다. 무선 통신 인터페이스 (1002) 는 디바이스 (1000) 가 무선 통신 네트워크 (104) 와 무선으로 통신하는 것을 허용한다. 따라서, 인터페이스 (1002) 는 디바이스 (1000) 가 무선 광역 네트워크들 (WWAN), 예컨대 모바일 통신 셀룰러 네트워크들 뿐만 아니라 짧은 범위, 무선 로컬 영역 네트워크들 (예를 들어, WiFi®, Zigbee®, Bluetooth® 등) 과 무선으로 통신하는 것을 허용한다.

[0071] 메모리 회로 (1004) 는 하나 이상의 휘발성 메모리 회로들 및/또는 비휘발성 메모리 회로들을 포함할 수도 있다. 따라서, 메모리 회로 (1004) 는 동적 랜덤 액세스 메모리 (DRAM), 정적 랜덤 액세스 메모리 (SRAM), 자기저항 랜덤 액세스 메모리 (MRAM), 전기적 소거가능 프로그램가능 리드 온니 메모리 (EEPROM), 플래시 메모리 등을 포함할 수도 있다. 메모리 회로 (1004) 는 하나 이상의 암호 키들을 저장할 수도 있다. 메모리 회로 (1004) 는 또한 프로세싱 회로 (1008) 에 의해 실행될 수도 있는 명령들을 저장할 수도 있다. I/O 디바이스들/회로들 (1006) 은 하나 이상의 키보드들, 마우스들, 디스플레이들, 터치스크린 디스플레이들, 프린터들, 지문 스캐너들, 및 임의의 다른 입력 및/또는 출력 디바이스들을 포함할 수도 있다.

[0072] 프로세싱 회로 (1008)(예를 들어, 프로세서, 중앙 프로세싱 유닛 (CPU), 어플리케이션 프로세싱 유닛 (APU) 등) 은 메모리 회로 (1006) 에 저장된 명령들 및/또는 사용자 디바이스 (1000) 에 통신가능하게 커플링된 다른 컴퓨터 판독가능 저장 매체 (예를 들어, 하드 디스크 드라이브, 광학 디스크 드라이버, 고체 상태 드라이브 등) 에 저장된 명령들을 실행할 수도 있다. 프로세싱 회로 (1008) 는 도 3a, 도 3b, 도 6, 도 7, 도 8, 도 9a, 도 9b 및/또는 도 12 를 참조하여 논의된 것들을 포함한 본 명세서에 기재된 디바이스 (1000) 의 단계들 및/또는

프로세스들 중 어느 하나를 수행할 수도 있다. 일 양태에 따라, 프로세싱 회로 (1008) 는 범용 프로세서일 수도 있다. 다른 양태에 따라, 프로세싱 회로는 도 3a, 도 3b, 도 6, 도 7, 도 8, 도 9a, 도 9b 및/또는 도 12 를 참조하여 논의된 것들을 포함한 본 명세서에 기재된 UE (220) 의 단계들 및/또는 프로세스들을 수행하기 위해 하드 와이어링될 수도 있다 (예를 들어, 주문형 집적 회로 (ASIC) 일 수도 있다).

[0073] 도 11 은 일 양태에 따른 디바이스 프로세싱 회로 (1008) 의 개략적 블록 다이어그램을 도시한다. 프로세싱 회로 (1008) 는 인증 및 키 일치 (AKA) 수행 회로 (1102), 인증 세션 키 생성 회로 (1104), 이동성 세션 키 생성 회로 (1106), 및/또는 데이터 보안 회로 (1108) 를 포함할 수도 있다. 일 양태에 따라, 이들 회로들 (1102, 1104, 1106, 1108) 은 ASIC들일 수도 있고 하드 와이어링되어 그 개별 프로세스들을 수행한다.

[0074] AKA 수행 회로 (1102) 는 SKME 디바이스와 인증 및 키 일치를 수행하기 위한 하나의 비한정 예일 수도 있다. 인증 세션 키 생성 회로 (1104) 는 홈 가입자 서버와 공유된 보안 키에 부분적으로 기초하여 인증 세션 키를 생성하기 위한 수단의 하나의 비한정 예일 수도 있다. 이동성 세션 키 생성 회로 (1106) 는 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하기 위한 수단의 하나의 비한정 예일 수도 있다. 데이터 보안 회로 (1108) 는 이동성 세션 키를 사용하여 디바이스로부터 무선 통신 네트워크에 전송된 데이터를 암호로 보안하기 위한 수단의 하나의 비한정 예일 수도 있다.

[0075] 도 12 는 디바이스 (1000) 에서 동작하는 방법 (1200) 을 도시한다. 먼저, 세션 키 관리 엔티티 (SKME) 와 인증 및 키 일치가 수행된다 (1202), 다음, 인증 세션 키가 홈 가입자 서버 (HSS) 와 공유된 보안 키에 적어도 기초하여 생성되며 (1204), 인증 세션 키는 SKME 디바이스에 알려져 있다. 그 후, 이동성 세션 키가 인증 세션 키에 부분적으로 기초하여 생성되고 (1206), 이동성 세션 키는 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 알려져 있다. 다음, 디바이스로부터 무선 통신 네트워크에 전송된 데이터는 이동성 세션 키를 사용하여 암호로 보안된다 (1208).

[0076] 도 13 은 개시물의 일 양태에 따른 네트워크 디바이스 (1300) 의 개략적 블록 다이어그램을 도시한다. 네트워크 디바이스 (1300) 는, 다른 네트워크 컴포넌트들 중에서, SKME, MME, RAN, S-GW, 및/또는 P-GW 일 수도 있다. 네트워크 디바이스 (1300) 는 서로 통신가능하게 커플링될 수도 있는, 적어도 하나 이상의 무선 통신 인터페이스들 (1302), 하나 이상의 메모리 회로들 (1304), 하나 이상의 입력 및/또는 출력 (I/O) 디바이스들/회로들 (1306), 및/또는 하나 이상의 프로세싱 회로들 (1308) 을 포함할 수도 있다. 예를 들어, 인터페이스 (1302), 메모리 회로 (1304), I/O 디바이스들 (1306), 및 프로세싱 회로 (1308) 는 버스 (1310) 를 통해 서로 통신가능하게 커플링될 수도 있다. 무선 통신 인터페이스 (1302) 는 네트워크 디바이스 (1300) 가 사용자 디바이스 (102) 와 무선으로 통신하는 것을 허용한다. 따라서, 인터페이스 (1302) 는 디바이스 (1300) 가 무선 광역 네트워크들 (WWAN), 예컨대 모바일 통신 셀룰러 네트워크들 뿐만 아니라 짧은 범위, 무선 로컬 영역 네트워크들 (예를 들어, WiFi®, Zigbee®, Bluetooth® 등) 과 무선으로 통신하는 것을 허용한다.

[0077] 메모리 회로 (1304) 는 하나 이상의 휘발성 메모리 회로들 및/또는 비휘발성 메모리 회로들을 포함할 수도 있다. 따라서, 메모리 회로 (1304) 는 동적 랜덤 액세스 메모리 (DRAM), 정적 랜덤 액세스 메모리 (SRAM), 자기저항 랜덤 액세스 메모리 (MRAM), 전기적 소거가능 프로그램가능 리드 온니 메모리 (EEPROM), 플래시 메모리 등을 포함할 수도 있다. 메모리 회로 (1304) 는 하나 이상의 암호 키들을 저장할 수도 있다. 메모리 회로 (1304) 는 또한 프로세싱 회로 (1308) 에 의해 실행될 수도 있는 명령들을 저장할 수도 있다. I/O 디바이스들/회로들 (1306) 은 하나 이상의 키보드들, 마우스들, 디스플레이들, 터치스크린 디스플레이들, 프린터들, 지문 스캐너들, 및 임의의 다른 입력 및/또는 출력 디바이스들을 포함할 수도 있다.

[0078] 프로세싱 회로 (1308)(예를 들어, 프로세서, 중앙 프로세싱 유닛 (CPU), 어플리케이션 프로세싱 유닛 (APU) 등) 은 메모리 회로 (1306) 에 저장된 명령들 및/또는 사용자 디바이스 (1300) 에 통신가능하게 커플링된 다른 컴퓨터 판독가능 저장 매체 (예를 들어, 하드 디스크 드라이브, 광학 디스크 드라이버, 고체 상태 드라이브 등) 에 저장된 명령들을 실행할 수도 있다. 프로세싱 회로 (1308) 는 도 3a, 도 3b, 도 6, 도 7, 도 8, 도 9a, 도 9b, 도 16 및/또는 도 17 을 참조하여 논의된 것들을 포함한 본 명세서에 기재된 네트워크 디바이스들의 단계들 및/또는 프로세스들 중 어느 하나를 수행할 수도 있다. 일 양태에 따라, 프로세싱 회로 (1308) 는 범용 프로세서일 수도 있다. 다른 양태에 따라, 프로세싱 회로 (1308) 는 도 3a, 도 3b, 도 6, 도 7, 도 8, 도 9a, 도 9b, 도 16 및/또는 도 17 를 참조하여 논의된 것들을 포함한 본 명세서에 기재된 SKME (205) 및/또는 MME (210, 210a, 210b) 의 단계들 및/또는 프로세스들을 수행하기 위해 하드 와이어링될 수도 있다 (예를 들어, 주문형 집적 회로 (ASIC) 일 수도 있다).

[0079] 도 14 는 일 양태에 따른 디바이스 프로세싱 회로 (1008) 의 개략적 블록 다이어그램을 도시한다. 프로세싱

회로 (1308) 는 인증 및 키 일치 (AKA) 수행 회로 (1402), 인증 정보 획득 회로 (1404), 이동성 세션 키 생성 회로 (1406), 및/또는 이동성 세션 키 송신 회로 (1408) 를 포함할 수도 있다. 일 양태에 따라, 이들 회로들 (1402, 1404, 1406, 1408) 은 ASIC들일 수도 있고 하드 와이어링되어 그 개별 프로세스들을 수행한다.

[0080] AKA 수행 회로 (1402) 는 디바이스와 인증 및 키 일치를 수행하기 위한 수단의 하나의 비한정 예일 수도 있다.

인증 정보 획득 회로 (1404) 는 디바이스와 연관된 인증 정보를 획득하기 위한 수단의 하나의 비한정 예일 수도 있고, 인증 정보는 적어도 인증 세션 키를 포함한다. 이동성 세션 키 생성 회로 (1406) 는 인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성하기 위한 수단의 하나의 비한정 예일 수도 있다. 이동성 세션 키 송신 회로 (1408) 는 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 이동성 세션 키를 송신하기 위한 수단의 하나의 비한정 예일 수도 있다.

[0081] 도 15 는 다른 양태에 따른 네트워크 디바이스 프로세싱 회로 (1308) 의 개략적 블록 다이어그램을 도시한다.

프로세싱 회로 (1308) 는 NAS 메시지 수신 회로 (1502), NAS 메시지 포워딩 회로 (1504), 이동성 세션 키 수신 회로 (1506), 및/또는 키 도출 데이터 송신 회로 (1508) 을 포함할 수도 있다. 일 양태에서, 이들 회로들 (1502, 1504, 1506, 1508) 은 ASIC들일 수도 있고 그 개별 프로세스들을 수행하기 위해 하드 와이어링된다.

[0082] NAS 메시지 수신 회로 (1502) 는 디바이스로부터 비액세스 계층 (NAS) 메시지를 수신하기 위한 수단의 하나의 비한정 예일 수도 있다. NAS 메시지 포워딩 회로 (1504) 는 세션 키 관리 엔티티 (SKME) 디바이스에 네트워크 디바이스를 식별하는 네트워크 디바이스 식별 값과 함께 NAS 메시지를 포워딩하기 위한 수단의 하나의 비한정 예일 수도 있다. 이동성 세션 키 수신 회로 (1506) 는 SKME 디바이스로부터 이동성 세션 키를 수신하기 위한 수단의 하나의 비한정 예일 수도 있으며, 이동성 세션 키는 디바이스와 무선 통신 네트워크 사이에 공유된 키로부터 도출되었던 인증 세션 키에 부분적으로 기초한다. 키 도출 데이터 송신 회로 (1508) 는 디바이스에 키 도출 데이터를 송신하기 위한 수단의 하나의 비한정 예일 수도 있고, 키 도출 데이터는 디바이스가 이동성 세션키를 도출하는 것을 가능하게 한다.

[0083] 도 16 은 네트워크 디바이스 (1300) 에서 동작하는 방법 (1600) 을 도시한다. 먼저, 디바이스와 인증 및 키 일치가 수행된다 (1602). 다음, 디바이스와 연관된 인증 정보가 획득되며 (1604), 인증 정보는 적어도 인증 세션키를 포함한다. 그 후, 인증 세션 키에 부분적으로 기초하는 이동성 세션 키가 생성된다 (1606). 다음, 이동성 세션 키가 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 송신된다 (1608).

[0084] 도 17 은 네트워크 디바이스 (1300) 에서 동작하는 방법 (1700) 을 도시한다. 먼저, 비액세스 계층 (NAS) 메시지가 디바이스로부터 수신된다 (1702). 다음, 네트워크 디바이스를 식별하는 네트워크 디바이스 식별값과 함께 NAS 메시지가 세션 키 관리 엔티티 (SKME) 디바이스에 포워딩된다 (1704). 그 후, SKME 디바이스로부터 이동성 세션 키가 수신되고 (1706), 이동성 세션 키는 디바이스와 무선 통신 네트워크 사이에 공유된 키로부터 도출되었던 인증 세션 키에 부분적으로 기초한다. 다음, 키 도출 데이터가 디바이스에 송신되며 (1708), 키 도출 데이터는 디바이스가 이동성 세션 키를 도출하는 것을 가능하게 한다.

[0085] 도 2, 도 3a, 도 3b, 도 4, 도 5, 도 6, 도 7, 도 8, 도 9a, 도 9b, 도 10, 도 11, 도 13, 도 14, 도 15, 도 16, 및/또는 도 17 에 도시된 컴포넌트들, 단계들, 피처들, 및/또는 기능들의 하나 이상은 단일 컴포넌트, 단계, 피처 또는 기능으로 재배열되고 및/결합되거나 수 개의 컴포넌트들, 단계들, 또는 기능들에서 구현될 수도 있다. 부가 엘리먼트들, 컴포넌트들, 단계들, 및/또는 피처들이 또한 발명을 벗어나지 않으면서 부가될 수도 있다. 도 2, 도 3a, 도 3b, 도 4, 도 5, 도 6, 도 7, 도 8, 도 9a, 도 9b, 도 10, 도 11, 도 12, 도 13, 도 14, 및/또는 도 15 에 도시된 장치, 디바이스들, 및/또는 컴포넌트들은 도 2, 도 3a, 도 3b, 도 6, 도 7, 도 8, 도 9a, 도 9b, 도 12, 도 16, 및/또는 도 17 에 기재된 방법들, 피처들, 또는 단계들 중 하나 이상을 수행하도록 구성될 수도 있다. 본 명세서에 기재된 알고리즘은 또한 효율적으로 소프트웨어에서 구현되고 및/또는 하드웨어에 임베딩될 수도 있다.

[0086] 또한, 본 개시물의 양태들은, 플로우챠트, 플로우 다이어그램, 구조 다이어그램, 또는 블록 다이어그램으로서 도시되는 프로세스로서 기재될 수도 있다는 것을 유의한다. 플로우챠트가 순차적 프로세스로서 동작들을 기재할 수도 있지만, 동작들을 병렬로 또는 동시에 수행될 수도 있다. 부가적으로, 동작들의 순서는 재배열될 수도 있다. 프로세스는 그 동작들이 완료될 때 종료된다. 프로세스는 방법, 기능, 절차, 서브루틴, 서브프로그램 등에 대응할 수도 있다. 프로세스가 기능에 대응할 때, 그 종료는 콜링 기능 또는 메인 기능으로의 기능의 리턴에 대응한다.

[0087] 게다가, 저장 매체는 리드 온니 메모리 (ROM), 랜덤 액세스 메모리 (RAM), 자기 디스크 저장 매체들, 광학 저장 매체들, 플래시 메모리 디바이스들, 및/또는 다른 머신 판독가능 매체들을 포함한, 데이터를 저장하기 위한 하나 이상의 디바이스들, 및 정보를 저장하기 위한 프로세서 판독가능 매체들, 및/또는 컴퓨터 판독가능 매체들을 나타낼 수도 있다. 용어들 "머신 판독가능 매체", "컴퓨터 판독가능 매체", 및/또는 "프로세서 판독가능 매체" 는, 비일시적 매체들, 예컨대 포터블 또는 고정 저장 디바이스들, 광학 저장 디바이스들, 및 명령(들) 및/또는 데이터를 저장하거나 포함할 수 있는 다양한 다른 매체들을 포함할 수도 있지만 이에 제한되지 않는다. 따라서, 본 명세서에 기재된 다양한 방법들은, "머신 판독가능 매체", "컴퓨터 판독가능 매체", 및/또는 "프로세서 판독가능 매체" 에 저장되고 하나 이상의 프로세서들, 머신들, 및/또는 디바이스들에 의해 실행될 수도 있는 명령들 및/또는 데이터에 의해 전부 또는 부분적으로 구현될 수도 있다.

[0088] 게다가, 개시물의 양태들은 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 또는 그 임의의 조합에 의해 구현될 수도 있다. 소프트웨어, 펌웨어, 미들웨어, 또는 마이크로코드에서 구현될 때, 필요한 태스크들을 수행하기 위한 프로그램 코드 또는 코드 세그먼트들은 머신 판독가능 매체, 예컨대 저장 매체 또는 다른 스토리지(들) 에 저장될 수도 있다. 프로세서는 필요한 태스크들을 수행할 수도 있다. 코드 세그먼트는 절차, 기능, 서브프로그램, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스, 또는 명령들, 데이터 구조들 또는 프로그램 세그먼트들의 임의의 조합을 나타낼 수도 있다. 코드 세그먼트는 정보, 데이터, 인수(argument)들, 파라미터들, 또는 데이터 콘텐츠를 전달 및/또는 수신하는 것에 의해 하드웨어 회로 또는 다른 코드 세그먼트에 커플링될 수도 있다. 정보, 인수들, 파라미터들, 데이터 등은, 메모리 공유, 메시지 전달, 토큰 전달, 네트워크 송신 등을 포함한 임의의 적절한 수단에 의해 전달되고, 포워드되고, 또는 송신될 수도 있다.

[0089] 본 명세서에 개시된 예들과 관련하여 기재된 다양한 예시적인 논리 블록들, 모듈들, 회로들, 엘리먼트들, 및/또는 컴포넌트들은, 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적 회로 (ASIC), 필드 프로그램가능 게이트 어레이 (FPGA), 또는 다른 프로그램가능 로직 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본 명세서에 기재된 기능들을 수행하도록 설계된 그 임의의 조합으로 구현되거나 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안으로, 프로세서는 임의의 종래 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수도 있다. 프로세서는 또한 컴퓨팅 컴포넌트들의 조합, 예를 들어 DSP 및 마이크로프로세서의 조합, 다수의 마이크로프로세서들, DSP 코어와 협력하는 하나 이상의 마이크로프로세서들, 또는 임의의 다른 그러한 구성으로서 구현될 수도 있다.

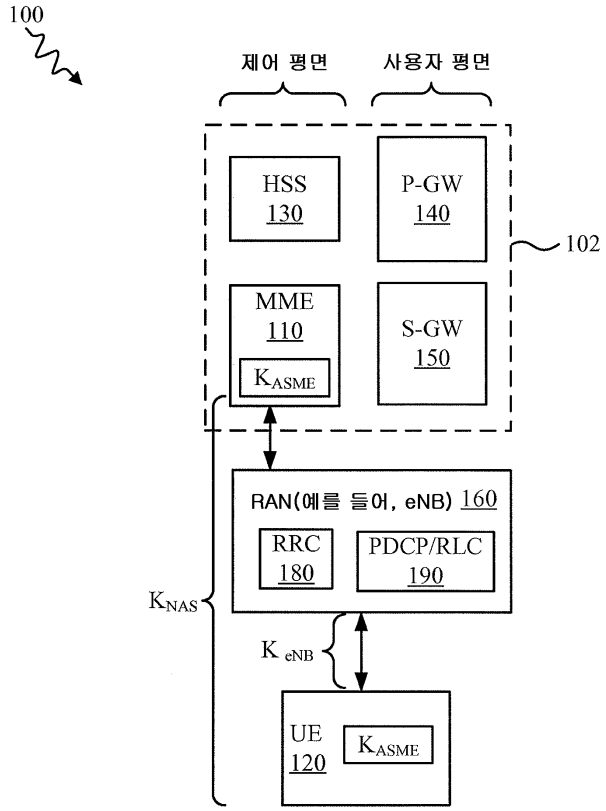
[0090] 본 명세서에 개시된 예들과 관련하여 기재된 방법들 또는 알고리즘은, 하드웨어에서 직접, 프로세서에 의해 실행가능한 소프트웨어 모듈에서, 또는 양자의 조합에서, 프로세싱 유닛, 프로그래밍 명령들, 또는 다른 디렉션들의 형태로 구현될 수도 있고, 단일 디바이스에 포함되거나 다중 디바이스들에 걸쳐 분산될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, 레지스터들, 하드 디스크, 탈착가능 디스크, CD-ROM, 또는 종래에 알려진 저장 매체의 임의의 다른 형태에 상주할 수도 있다. 저장 매체는 프로세서가 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기입할 수 있도록 프로세서에 커플링될 수도 있다. 대안으로, 저장 매체는 프로세서에 통합될 수도 있다.

[0091] 당업자는 또한, 본 명세서에 개시된 양태들과 관련하여 기재된 다양한 예시적인 논리 블록들, 모듈들, 회로들 및 알고리즘 단계들은 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양자의 조합으로서 구현될 수도 있다는 것을 이해하게 된다. 이러한 하드웨어 및 소프트웨어의 상호교환성을 명백히 예시하기 위해서, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 그 기능에 관하여 일반적으로 위에 기재되었다. 그러한 기능이 하드웨어로서 구현되는지 또는 소프트웨어로서 구현되는지는 전체 시스템에 부과된 특정 어플리케이션 및 설계 제약들에 의존한다.

[0092] 본 명세서에 기재된 발명의 다양한 피처들은 발명으로부터 벗어나지 않으면서 상이한 시스템들에서 구현될 수 있다. 개시물의 상기 양태들은 단지 예시들일 뿐이고 발명을 제한하는 것으로 해석되지 않아야 함을 유의해야 한다. 본 개시물의 양태들의 기재는 예시적인 것을 의도되고 청구항들의 범위를 제한하는 것으로 의도되지 않는다. 이로써, 본 기법들은 장치들의 다른 타입들에 쉽게 적용될 수 있고 많은 대안들, 수정들, 및 변형들이 당업자에게 자명할 것이다.

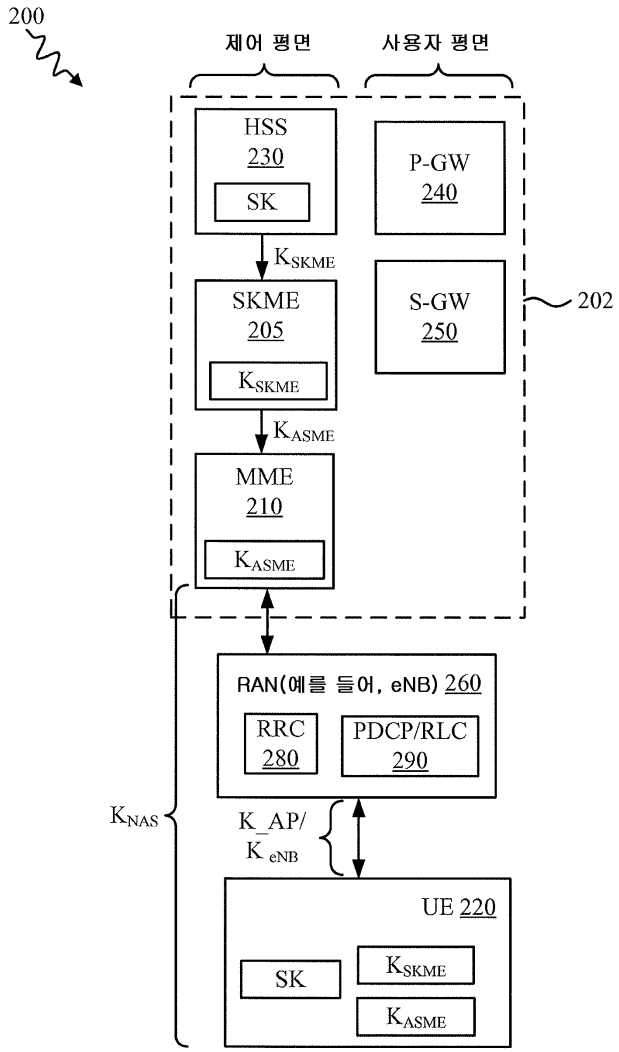
도면

도면1

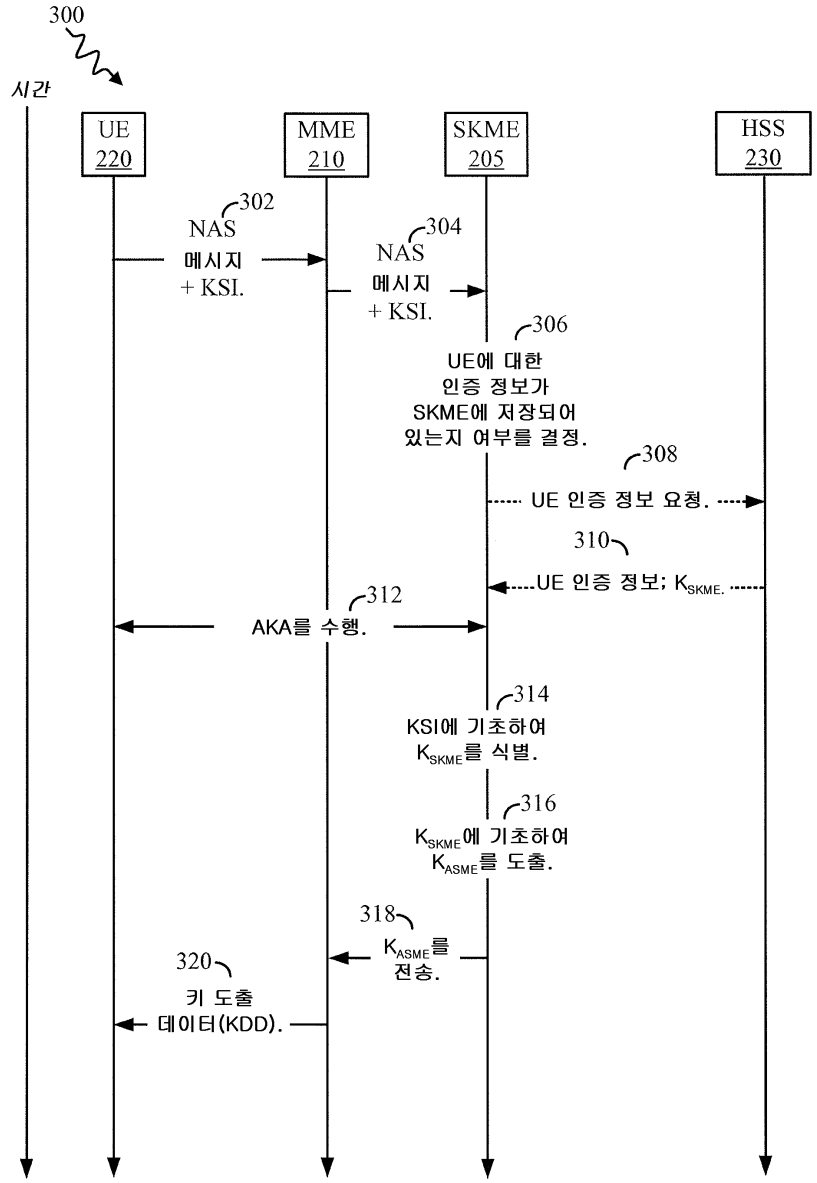

100
제어 평면
사용자 평면
HSS
130
P-GW
140
102
MME
110
K_{ASME}
S-GW
150
RAN(예를 들어, eNB) 160
RRC
180
PDCP/RLC
190
K_{NAS}
K_{eNB}
UE
120
K_{ASME}

(종래 기술)

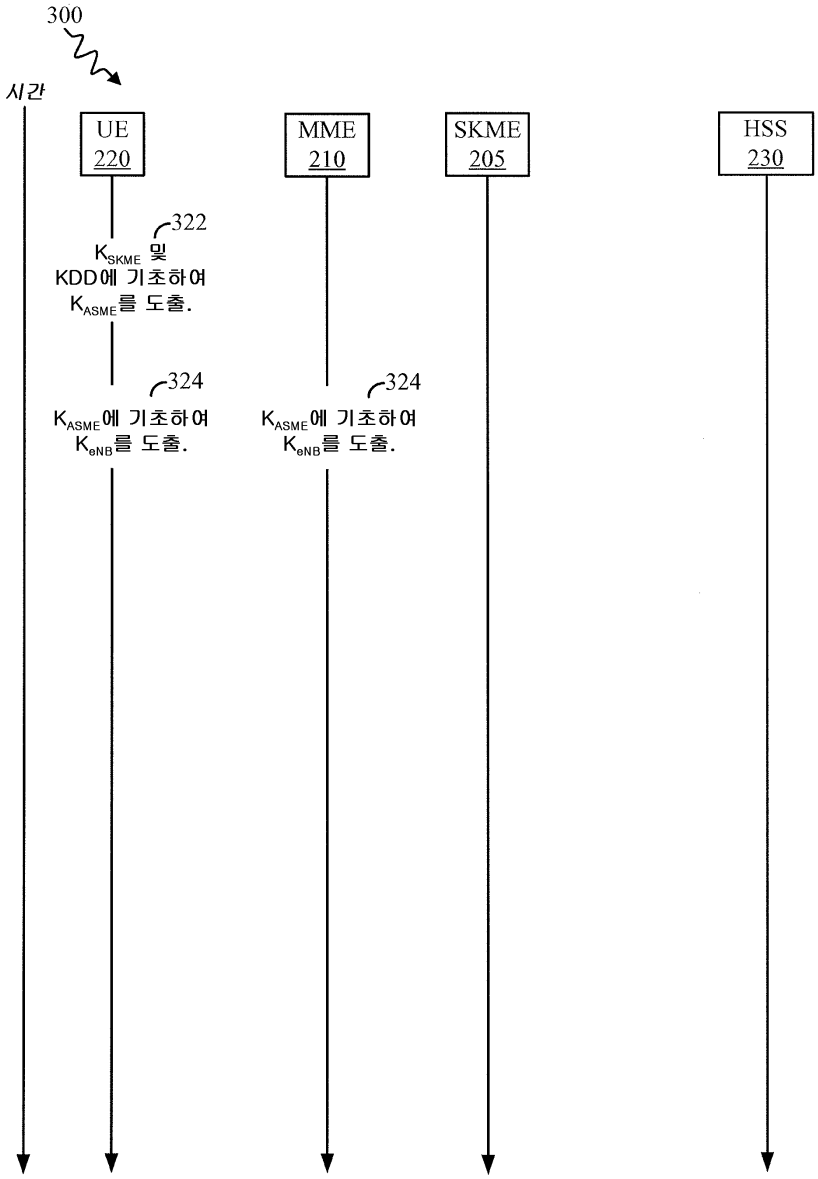
도면2


200
제어 평면
사용자 평면
HSS
230
SK
P-GW
240
K_{SKME}
SKME
205
K_{SKME}
S-GW
250
202
K_{ASME}
MME
210
K_{ASME}
RAN(예를 들어, eNB) 260
RRC
280
PDCP/RLC
290
K_{NAS}
K_AP/
K_{eNB}
UE 220
SK
K_{SKME}
K_{ASME}

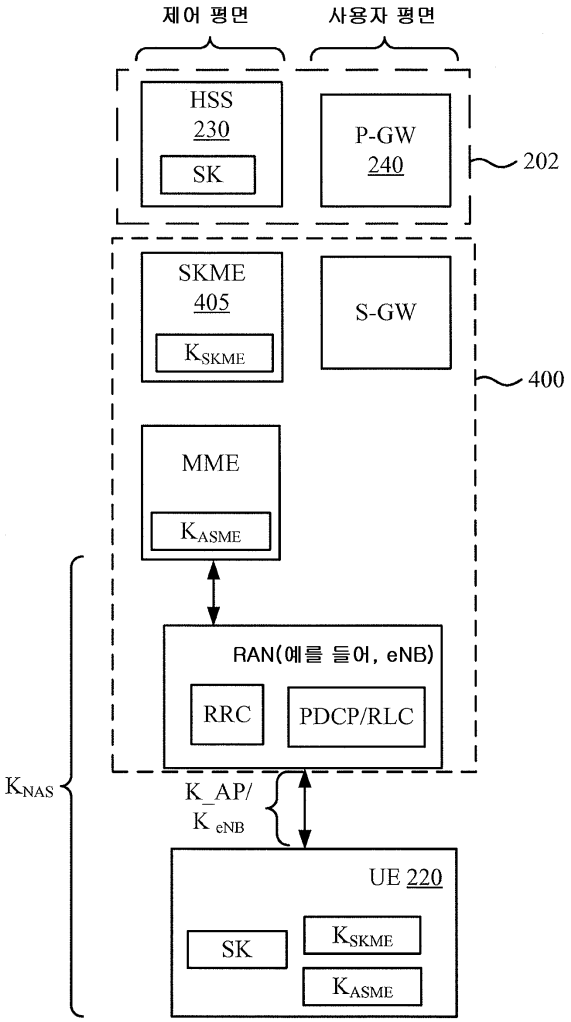
도면3a


300
시간
UE 220
MME 210
SKME 205
HSS 230
302
NAS 메시지 + KSI.
304
NAS 메시지 + KSI.
306
UE에 대한 인증 정보가 SKME에 저장되어 있는지 여부를 결정.
308
UE 인증 정보 요청.
310
UE 인증 정보; K_{SKME}.
312
AKA를 수행.
314
KSI에 기초하여 K_{SKME}를 식별.
316
K_{SKME}에 기초하여 K_{ASME}를 도출.
318
K_{ASME}를 전송.
320
키 도출 데이터(KDD).

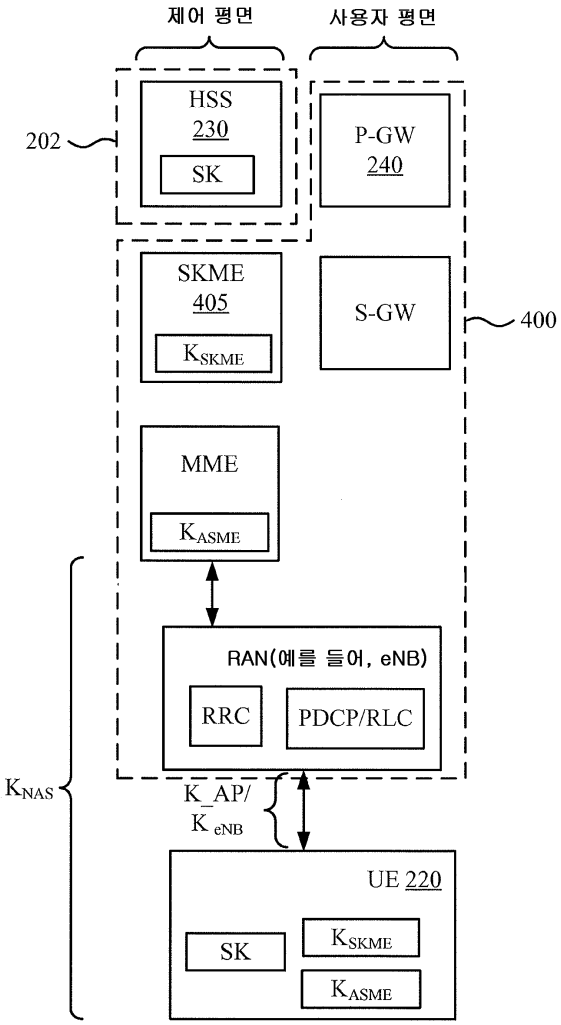
도면3b


300
시간
UE
220
MME
210
SKME
205
HSS
230
322
K_{SKME} 및
KDD에 기초하여
K_{ASME}를 도출.
324
K_{ASME}에 기초하여
K_{eNB}를 도출.
324
K_{ASME}에 기초하여
K_{eNB}를 도출.

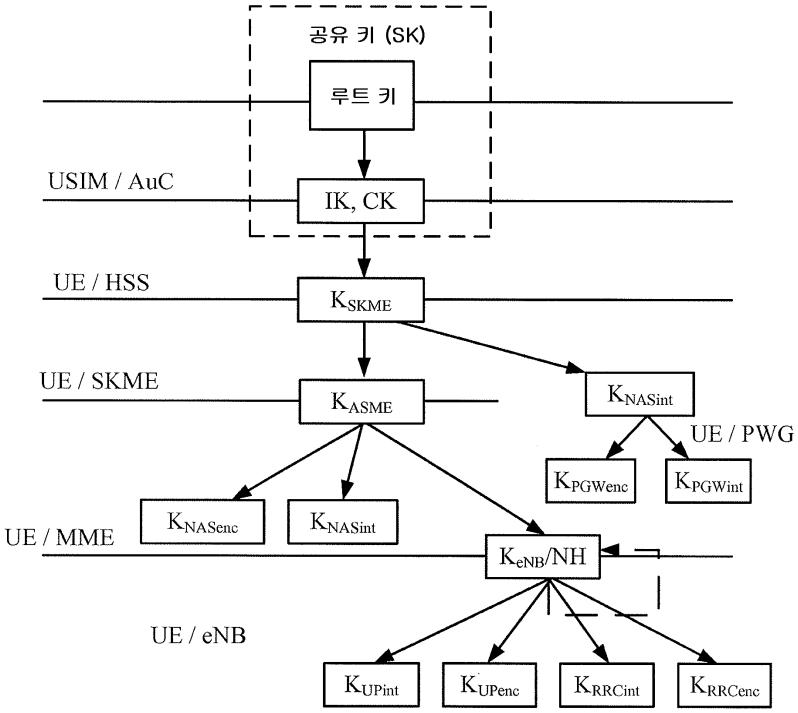
도면4


제어 평면
사용자 평면
HSS
230
SK
P-GW
240
202
SKME
405
K_{SKME}
S-GW
400
MME
K_{ASME}
RAN(예를 들어, eNB)
RRC
PDCP/RLC
K_{NAS}
K_AP/
K_{eNB}
UE 220
SK
K_{SKME}
K_{ASME}

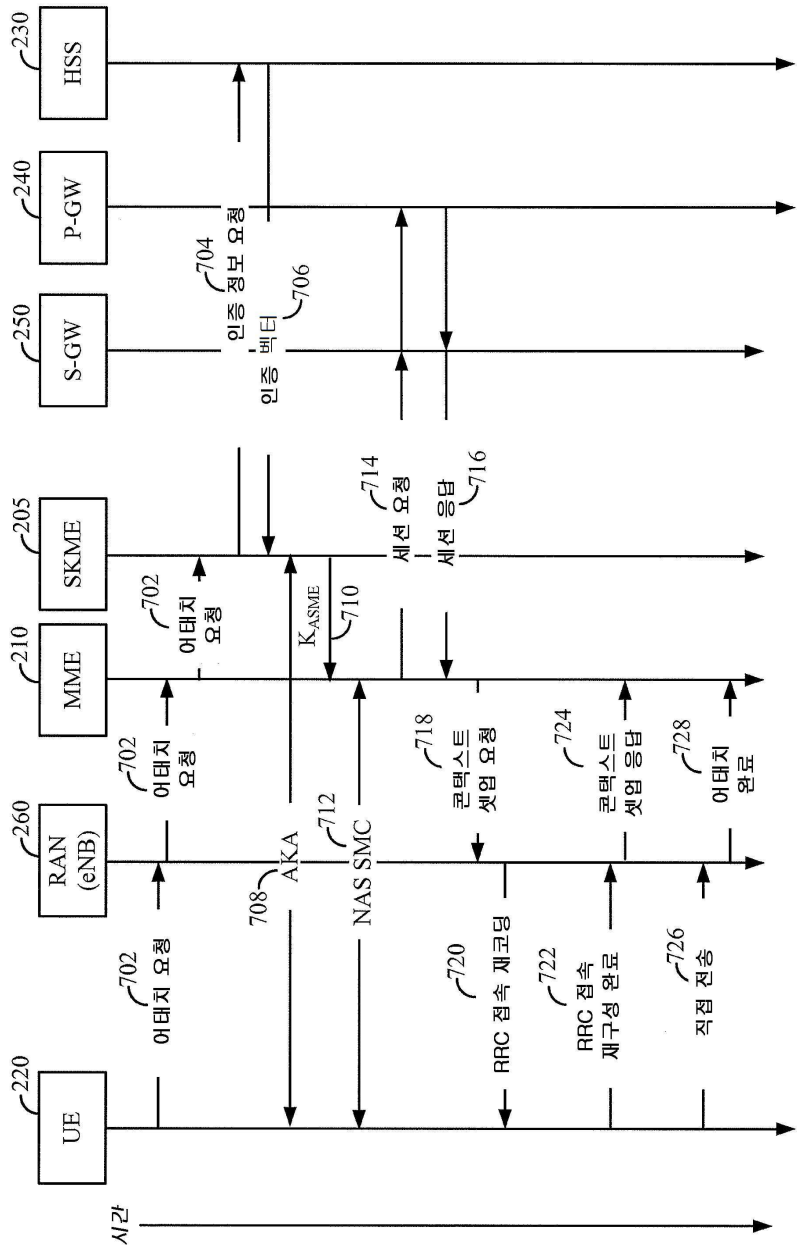
도면5


제어 평면
사용자 평면
HSS
230
SK
202
P-GW
240
SKME
405
K_{SKME}
S-GW
400
MME
K_{ASME}
RAN(예를 들어, eNB)
RRC
PDCP/RLC
K_{NAS}
K_AP/
K_{eNB}
UE 220
SK
K_{SKME}
K_{ASME}

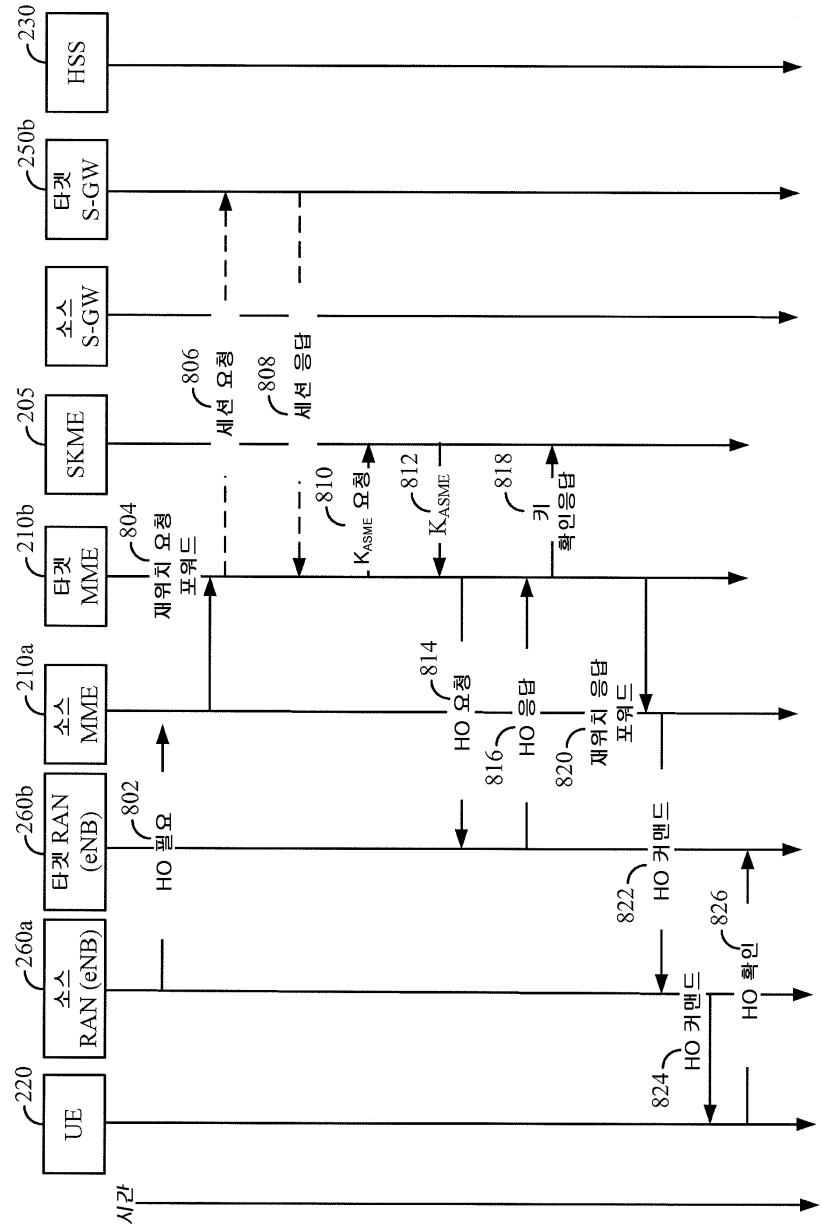
도면6


공유 키 (SK)
루트 키
USIM / AuC
IK, CK
UE / HSS
K_{SKME}
UE / SKME
K_{ASME}
K_{NASint}
UE / PWG
K_{PGWenc}
K_{PGWint}
K_{NASenc}
K_{NASint}
UE / MME
K_{eNB}/NH
UE / eNB
K_{UPint}
K_{UPenc}
K_{RRCint}
K_{RRCenc}

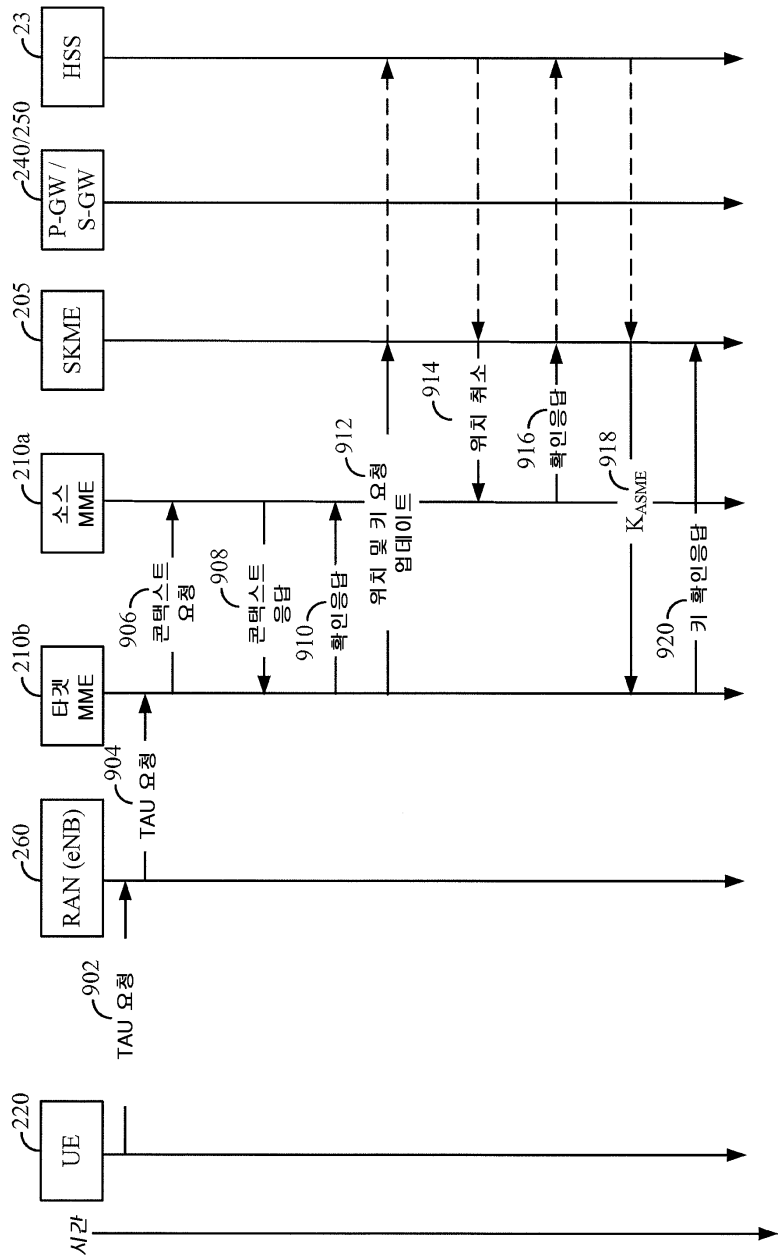
도면7


230
HSS
240
P-GW
250
S-GW
205
SKME
210
MME
260
RAN (eNB)
220
UE
시간
702 어태치 요청
704 인증 정보 요청
706 인증 벡터
708 AKA
710 K_{ASME}
712 NAS SMC
714 세션 요청
716 세션 응답
718 콘텍스트 셋업 요청
720 RRC 접속 재코딩
722 RRC 접속 재구성 완료
724 콘텍스트 셋업 응답
726 직접 전송
728 어태치 완료

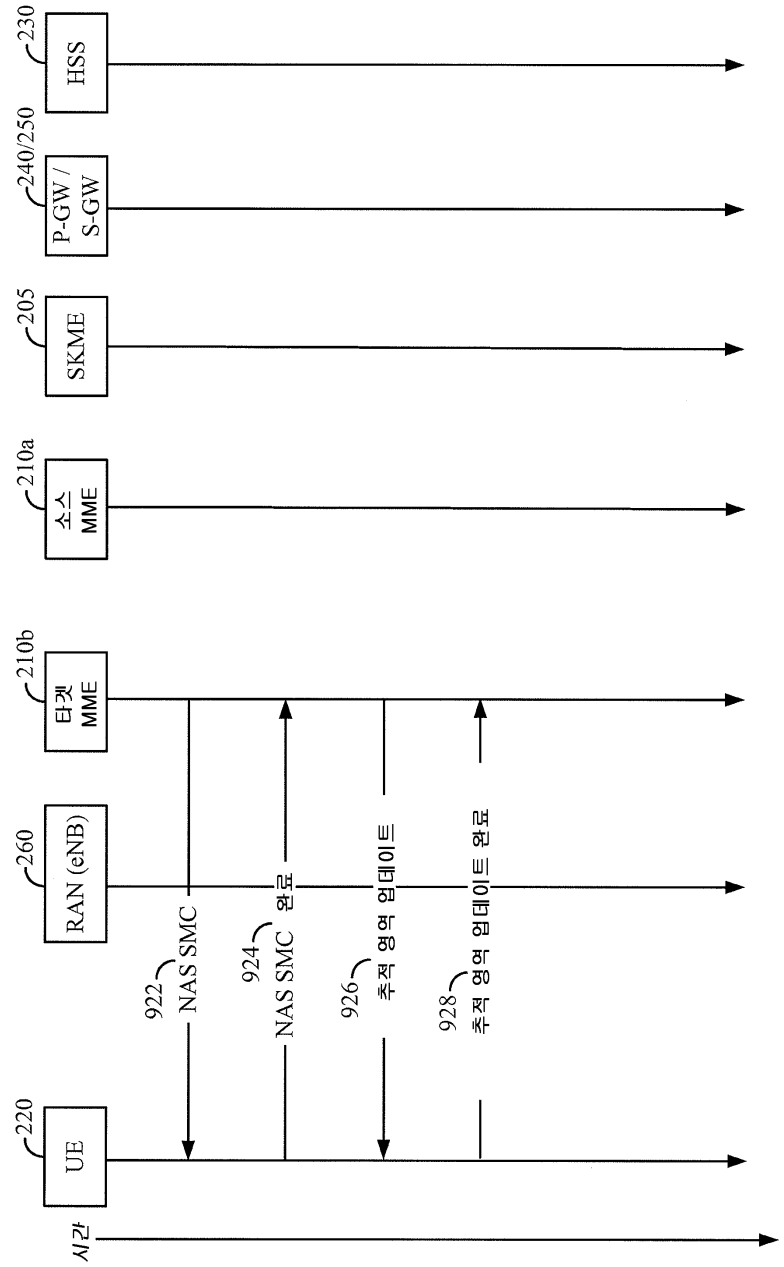
도면8


220
UE
260a
소스 RAN (eNB)
260b
타겟 RAN (eNB)
210a
소스 MME
210b
타겟 MME
205
SKME
250b
타겟 S-GW
소스 S-GW
230
HSS
802
HO 필요
804
재위치 요청 포워드
806
세션 요청
808
세션 응답
810
K_{ASME} 요청
812
K_{ASME}
814
HO 요청
816
HO 응답
818
키 확인응답
820
재위치 응답 포워드
822
HO 커맨드
824
HO 커맨드
826
HO 확인
시간

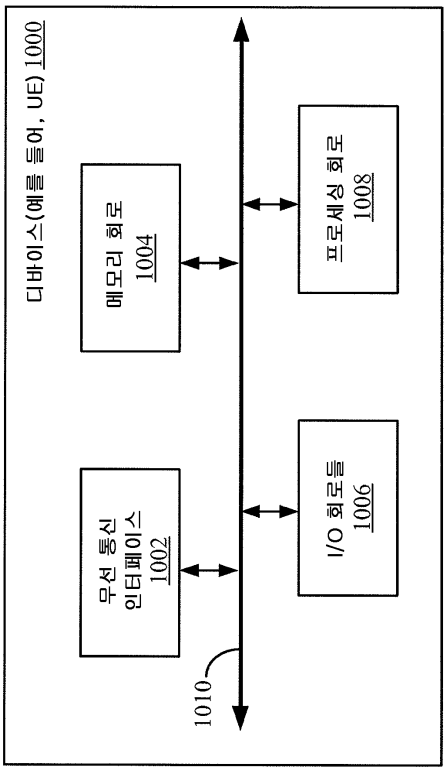
도면9a


UE
220
RAN (eNB)
260
타겟 MME
210b
소스 MME
210a
SKME
205
P-GW / S-GW
240/250
HSS
23
시간
902 TAU 요청
904 TAU 요청
906 콘텍스트 요청
908 콘텍스트 응답
910 확인응답
912 위치 및 키 요청 업데이트
914 위치 취소
916 확인응답
918 K_{ASME}
920 키 확인응답

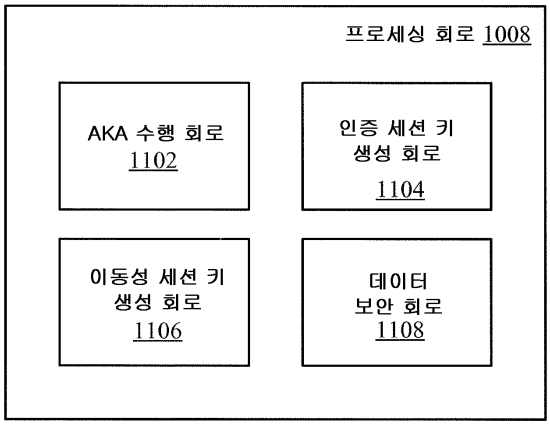
도면9b


230
HSS
240/250
P-GW / S-GW
205
SKME
210a
소스 MME
210b
타겟 MME
260
RAN (eNB)
220
UE
922
NAS SMC
924
NAS SMC 완료
926
추적 영역 업데이트
928
추적 영역 업데이트 완료
시간

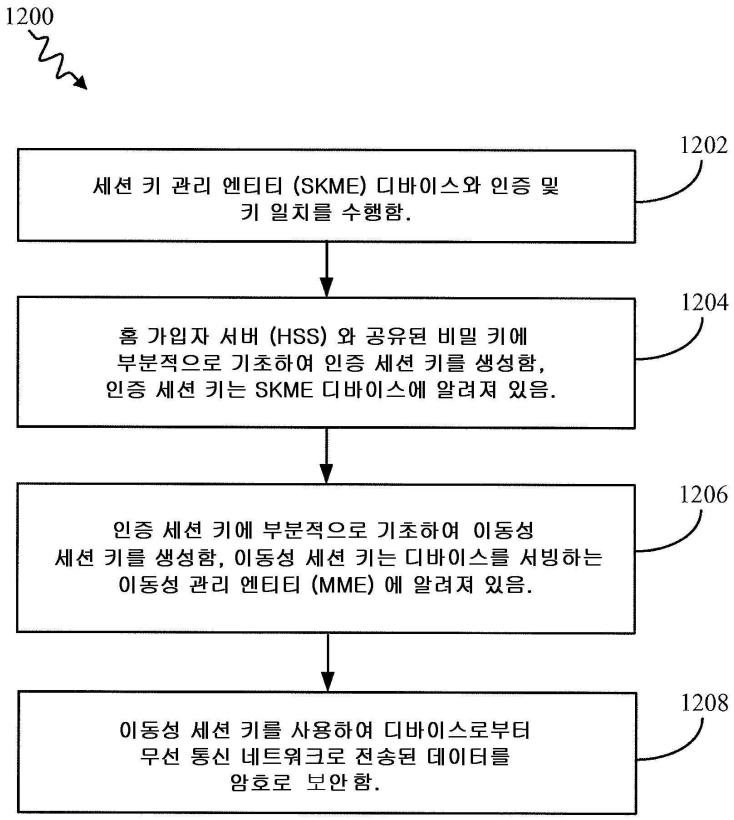
도면10


디바이스(예를 들어, UE) 1000
메모리 회로 1004
프로세싱 회로 1008
무선 통신 인터페이스 1002
I/O 회로들 1006
1010

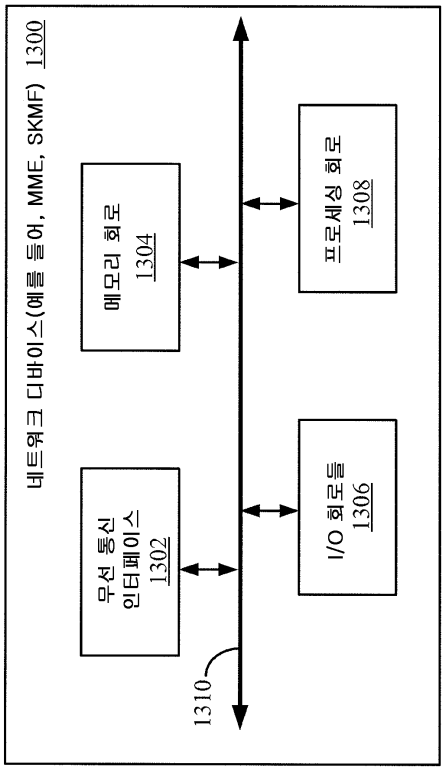
도면11


프로세싱 회로 1008
AKA 수행 회로 1102
인증 세션 키 생성 회로 1104
이동성 세션 키 생성 회로 1106
데이터 보안 회로 1108

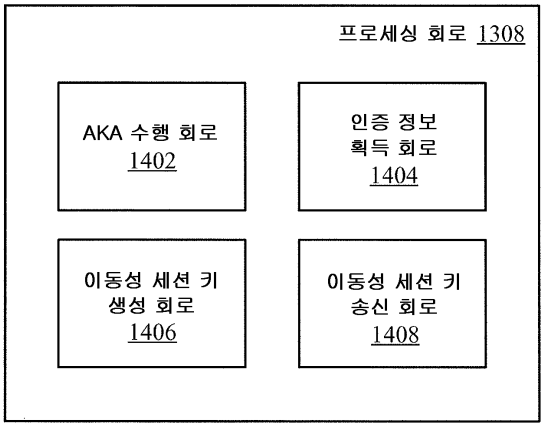
도면12


1200
세션 키 관리 엔티티 (SKME) 디바이스와 인증 및 키 일치를 수행함.
1202
홈 가입자 서버 (HSS) 와 공유된 비밀 키에 부분적으로 기초하여 인증 세션 키를 생성함, 인증 세션 키는 SKME 디바이스에 알려져 있음.
1204
인증 세션 키에 부분적으로 기초하여 이동성 세션 키를 생성함, 이동성 세션 키는 디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에 알려져 있음.
1206
이동성 세션 키를 사용하여 디바이스로부터 무선 통신 네트워크로 전송된 데이터를 암호로 보안함.
1208

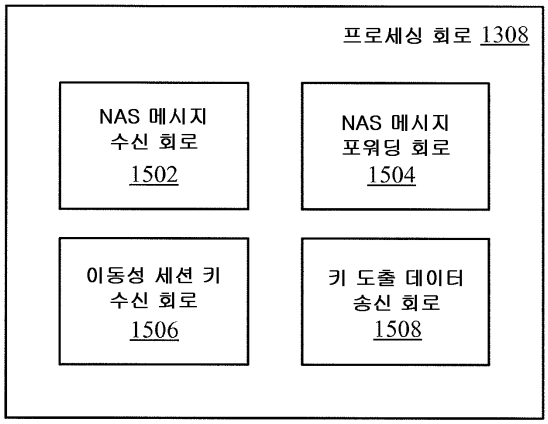
도면13


네트워크 디바이스(예를 들어, MME, SKMF) 1300
메모리 회로 1304
프로세싱 회로 1308
무선 통신 인터페이스 1302
I/O 회로들 1306
1310

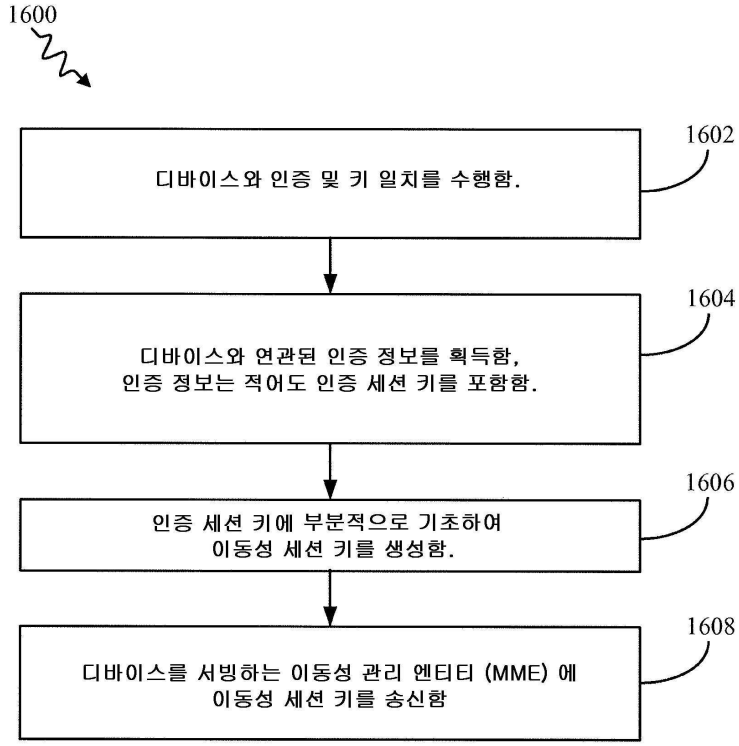
도면14


프로세싱 회로 1308
AKA 수행 회로
1402
인증 정보
획득 회로
1404
이동성 세션 키
생성 회로
1406
이동성 세션 키
송신 회로
1408

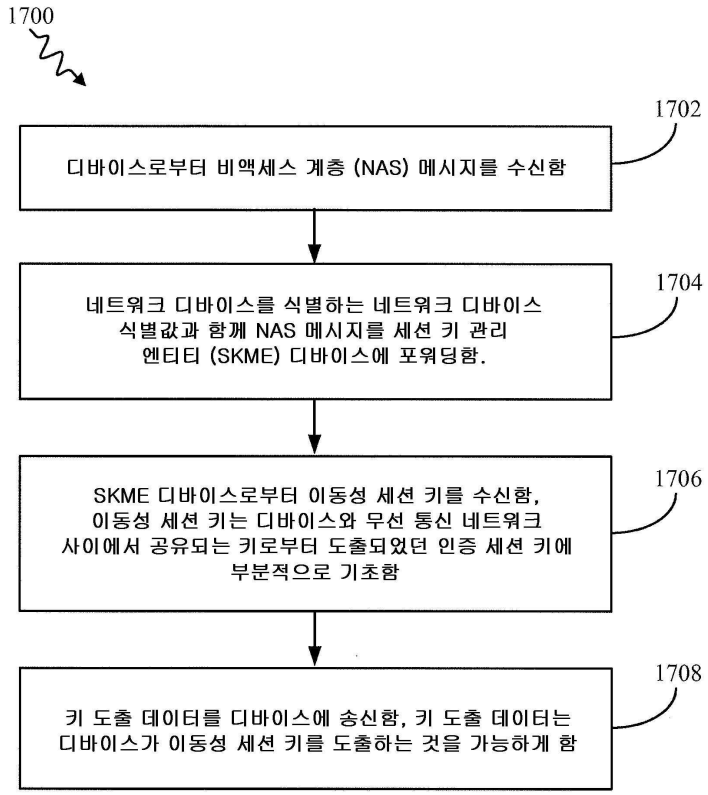
도면15


프로세싱 회로 1308
NAS 메시지
수신 회로
1502
NAS 메시지
포워딩 회로
1504
이동성 세션 키
수신 회로
1506
키 도출 데이터
송신 회로
1508

도면16


1600
1602
디바이스와 인증 및 키 일치를 수행함.
1604
디바이스와 연관된 인증 정보를 획득함,
인증 정보는 적어도 인증 세션 키를 포함함.
1606
인증 세션 키에 부분적으로 기초하여
이동성 세션 키를 생성함.
1608
디바이스를 서빙하는 이동성 관리 엔티티 (MME) 에
이동성 세션 키를 송신함

도면17


1700
1702
디바이스로부터 비액세스 계층 (NAS) 메시지를 수신함
1704
네트워크 디바이스를 식별하는 네트워크 디바이스
식별값과 함께 NAS 메시지를 세션 키 관리
엔티티 (SKME) 디바이스에 포워딩함.
1706
SKME 디바이스로부터 이동성 세션 키를 수신함,
이동성 세션 키는 디바이스와 무선 통신 네트워크
사이에서 공유되는 키로부터 도출되었던 인증 세션 키에
부분적으로 기초함
1708
키 도출 데이터를 디바이스에 송신함, 키 도출 데이터는
디바이스가 이동성 세션 키를 도출하는 것을 가능하게 함