(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년11월07일
(11) 등록번호 10-2042327
(24) 등록일자 2019년11월01일

(51) 국제특허분류(Int. Cl.)
H04W 12/02 (2009.01) *H04L 29/12* (2006.01)
H04W 12/06 (2009.01) *H04W 8/04* (2009.01)
H04W 8/18 (2009.01)
(52) CPC특허분류
H04W 12/02 (2019.01)
H04L 61/6054 (2013.01)
(21) 출원번호 10-2017-7024377
(22) 출원일자(국제) 2016년02월22일
심사청구일자 2019년04월08일
(85) 번역문제출일자 2017년08월30일
(65) 공개번호 10-2017-0125831
(43) 공개일자 2017년11월15일
(86) 국제출원번호 PCT/US2016/018860
(87) 국제공개번호 WO 2016/140823
국제공개일자 2016년09월09일
(30) 우선권주장
62/128,724 2015년03월05일 미국(US)
14/808,862 2015년07월24일 미국(US)
(56) 선행기술조사문헌
US20060154646 A1
US20090024848 A1
Hiten Choudhury et al., Enhancing User Identity Privacy in LTE, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012

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

전체 청구항 수 : 총 48 항 심사관 : 이준석

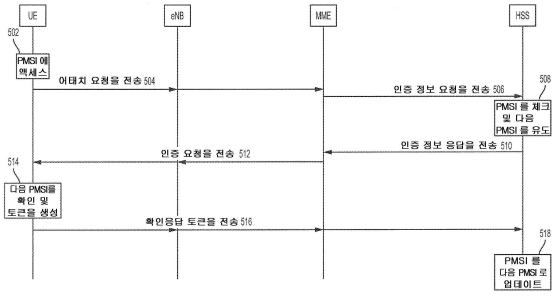
(54) 발명의 명칭 **무선 네트워크들에서의 아이덴티티 프라이버시**

(57) 요 약

시스템들 및 기법들은 프라이버시 모바일 가입자 아이덴티티를 대신 제공함으로써 사용자 장비의 국제 모바일 가입자 아이덴티티를 보호하기 위해 개시된다. 서빙 네트워크에 대한 어태치 시도에서, UE 는 IMSI 대신에 PMSI 를 제공하여, IMSI 를 노출로부터 보호한다. PMSI 는, 서빙 네트워크에서의 중간의 노드 엘리먼트들이

(뒷면에 계속)

대 표 도



PMSI 와 IMSI 사이의 관계의 지식을 갖지 않도록 홈 네트워크 서버와 UE 사이에서 결정된다. 어태치 요청에서의 PMSI 의 수신 시에, 서버는 후속 어태치 요청에서 이용될 다음 PMSI 를 생성하고 다음 PMSI 를 확인을 위해 UE 로 전송한다. UE 는 UE 와 서버 사이에 동기화하기 위해 다음 PMSI 를 확인하고 서버로 확인응답 토큰을 전송한다. UE 및 서버는 그 후 각각 현재 및 다음 PMSI 값들의 로컬 카피들을 업데이트한다.

(52) CPC특허분류
H04W 12/06 (2019.01)
H04W 8/04 (2013.01)
H04W 8/183 (2013.01)

(72) 발명자
에스콧 애드리안 에드워드
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775
호른 개빈 버나드
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775

명 세 서

청구범위

청구항 1

사용자 장비 (UE) 에 의한 네트워크 액세스를 위한 방법으로서,

초기 어태치 메시지를 사용하여 상기 UE 를 식별하기 위해, 국제 모바일 가입자 아이덴티티 (IMSI) 에 대한 직접 대체물로서 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 상기 UE 로부터 서빙 네트워크로 전송하는 단계;

상기 서빙 네트워크와 통신하는 서버로부터, 다음 PMSI 및 추적 인덱스를 포함하는 인증 요청을 수신하는 단계;

상기 UE 에 의해, 상기 PMSI 및 추적 인덱스로부터 UE-기반 다음 PMSI 를 유도하는 단계;

상기 UE 에 의해, 상기 UE-기반 다음 PMSI 와 상기 다음 PMSI 가 매칭하는 것에 응답하여 수신의 확인응답을 생성하는 단계; 및

상기 UE 로부터, 상기 서버로 상기 다음 PMSI 의 상기 수신의 확인응답을 전송하는 단계

를 포함하는, UE 에 의한 네트워크 액세스를 위한 방법.

청구항 2

제 1 항에 있어서,

상기 UE 에 의해, 초기 PMSI 에 기초하여 네트워크 액세스를 위한 상기 PMSI 를 결정하는 단계를 더 포함하는, UE 에 의한 네트워크 액세스를 위한 방법.

청구항 3

제 2 항에 있어서,

상기 서버에의 상기 UE 의 가입자 등록 동안 상기 초기 PMSI 를 수신하는 단계를 더 포함하는, UE 에 의한 네트워크 액세스를 위한 방법.

청구항 4

제 2 항에 있어서,

상기 서버와의 공중 경유 (over-the-air) 통신을 통한 가입자 등록 후에 상기 초기 PMSI 를 프로비저닝하는 단계를 더 포함하는, UE 에 의한 네트워크 액세스를 위한 방법.

청구항 5

제 4 항에 있어서,

복수의 값들이 난수 또는 의사-난수를 포함하고,

상기 UE 에서 생성된 상기 난수 또는 상기 의사-난수를 포함하는 수로부터 상기 UE 에 의해, 제안된 PMSI 를 생성하는 단계;

상기 UE 에 의해, 서버 공개 키를 이용하여 생성된 상기 PMSI 를 암호화하는 단계로서, 상기 서버는 대응하는 서버 개인 키를 유지하는, 상기 PMSI 를 암호화하는 단계;

상기 암호화 후에 상기 UE 로부터, 생성된 상기 PMSI 를 상기 서버로 전송하는 단계; 및

상기 UE 에서, 상기 초기 PMSI 로서 생성된 상기 PMSI 를 이용하기 위해 상기 서버로부터 확인응답을 수신하는 단계

를 더 포함하는, UE 에 의한 네트워크 액세스를 위한 방법.

청구항 6

제 1 항에 있어서,

상기 생성 이전에, 매치가 있는지를 결정하기 위해 상기 인증 요청의 일부로서 수신된 상기 다음 PMSI 와 상기 UE-기반 다음 PMSI 를 비교하는 단계

를 더 포함하는, UE 에 의한 네트워크 액세스를 위한 방법.

청구항 7

제 1 항에 있어서,

다음 어태치 메시지에서의 이용을 위해 상기 UE 에 확인된 상기 다음 PMSI 를 저장하는 단계

를 더 포함하는, UE 에 의한 네트워크 액세스를 위한 방법.

청구항 8

제 1 항에 있어서,

상기 인증 요청을 수신하는 단계는,

익명 키를 이용하여 상기 인증 요청에서의 상기 다음 PMSI 를 해독하는 단계를 더 포함하며,

상기 익명 키는 상기 UE 와 상기 서버 사이에 공유된 비밀 키로부터 유도되는, UE 에 의한 네트워크 액세스를 위한 방법.

청구항 9

제 1 항에 있어서,

상기 다음 PMSI 는, PMSI 생성 키와 함께, 상기 PMSI 에 결부된, 상기 추적 인덱스의 해시를 포함하는, UE 에 의한 네트워크 액세스를 위한 방법.

청구항 10

사용자 장비 (UE) 로서,

프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 저장하도록 구성된 메모리;

트랜시버로서,

초기 어태치 메시지를 사용하여 상기 UE 를 식별하기 위해, 국제 모바일 가입자 아이덴티티 (IMSI) 에 대한 직접 대체물로서 상기 PMSI 를 서빙 네트워크로 전송하고; 그리고

상기 서빙 네트워크와 통신하는 서버로부터, 다음 PMSI 및 추적 인덱스를 포함하는 인증 요청을 수신하도록

구성된, 상기 트랜시버; 및

프로세서로서,

상기 PMSI 및 상기 추적 인덱스로부터 UE-기반 다음 PMSI 를 유도하고; 그리고

상기 UE-기반 다음 PMSI 와 상기 다음 PMSI 가 매칭하는 것에 응답하여 수신의 확인응답을 생성하도록

구성된, 상기 프로세서를 포함하고,

상기 트랜시버는 상기 서버로 상기 수신의 확인응답을 전송하도록 추가로 구성되는, 사용자 장비.

청구항 11

제 10 항에 있어서,

상기 프로세서는,

상기 메모리에 저장된 초기 PMSI 에 기초하여 네트워크 액세스를 위한 상기 PMSI 를 결정하도록 추가로 구성되는, 사용자 장비.

청구항 12

제 11 항에 있어서,

상기 사용자 장비는 상기 서버에의 상기 UE 의 가입자 등록 동안 상기 초기 PMSI 를 수신하는, 사용자 장비.

청구항 13

제 11 항에 있어서,

상기 사용자 장비는 상기 서버와의 공중 경유 통신을 통한 가입자 등록 후에 상기 초기 PMSI 를 프로비저닝하도록 구성되는, 사용자 장비.

청구항 14

제 13 항에 있어서,

복수의 값들이 상기 UE 에서 생성된 난수 또는 의사-난수를 포함하고;

상기 프로세서는, 상기 UE 에서 생성된 상기 난수 또는 의사-난수를 포함하는 수로부터, 제안된 초기 PMSI 를 생성하고 그리고 서버 공개 키를 이용하여 생성된 상기 PMSI 를 암호화하도록 추가로 구성되고, 상기 서빙 네트워크 상의 상기 서버는 대응하는 서버 개인 키를 유지하고; 그리고

상기 트랜시버는 상기 서버에 암호화 후에 생성된 상기 PMSI 를 송신하고 그리고 상기 초기 PMSI 로서 생성된 상기 PMSI 를 이용하기 위해 상기 서버로부터 확인응답을 수신하도록 추가로 구성되는, 사용자 장비.

청구항 15

제 10 항에 있어서,

상기 프로세서는,

매치가 있는지를 결정하기 위해 상기 인증 요청의 일부로서 수신된 상기 다음 PMSI 와 상기 UE-기반 다음 PMSI 를 비교하도록 추가로 구성되는, 사용자 장비.

청구항 16

제 15 항에 있어서,

상기 메모리는 다음 어태치 메시지에서의 이용을 위해 상기 다음 PMSI 를 저장하도록 추가로 구성되는, 사용자 장비.

청구항 17

제 10 항에 있어서,

상기 프로세서는 익명 키를 이용하여 상기 인증 요청에서의 상기 다음 PMSI 를 해독하도록 추가로 구성되며,

상기 익명 키는 상기 UE 와 상기 서버 사이에 공유된 비밀 키로부터 유도되는, 사용자 장비.

청구항 18

네트워크 상의 서버와의 네트워크 액세스를 셋업하기 위한 방법으로서,

개재하는 서빙 네트워크에서의 하나 이상의 네트워크 엘리먼트들을 통해 사용자 장비 (UE) 로부터, 초기 어태치 메시지로부터 상기 UE 를 식별하기 위해, 국제 모바일 가입자 아이덴티티 (IMSI) 에 대한 직접 대체물로서 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 수신하는 단계;

상기 서버에 의해, 상기 PMSI 에 기초하여 다음 PMSI 를 결정하는 단계;

상기 서버로부터, 인증의 일부로서, 상기 다음 PMSI 및 추적 인덱스를 포함하는 인증 정보를 상기 서빙 네트워

크에 송신하는 단계; 및

상기 서빙 네트워크를 통해 상기 UE 로부터, 상기 다음 PMSI 에 매칭하는, 상기 PMSI 및 상기 추적 인덱스로부터 상기 UE 에 의해 유도된, UE-기반 다음 PMSI 에 응답하여 생성된 확인응답 토큰을 가진, 상기 다음 PMSI 의 확인을 포함하는 수신의 확인응답을 수신하는 단계

를 포함하는, 네트워크 상의 서버와의 네트워크 액세스를 셋업하기 위한 방법.

청구항 19

제 18 항에 있어서,

상기 서버에 의해, 초기 PMSI 에 기초하여 네트워크 액세스를 위한 상기 PMSI 를 결정하는 단계를 더 포함하는, 네트워크 상의 서버와의 네트워크 액세스를 셋업하기 위한 방법.

청구항 20

제 19 항에 있어서,

상기 서버에서, 상기 서버에의 상기 UE 의 가입자 등록 동안 상기 초기 PMSI 를 수신하는 단계를 더 포함하는, 네트워크 상의 서버와의 네트워크 액세스를 셋업하기 위한 방법.

청구항 21

제 19 항에 있어서,

상기 UE 로부터, 제안된 초기 PMSI 를 수신하는 단계;

상기 서버에 의해, 대응하는 서버 공개 키에 의해 상기 UE 에서 암호화된 상기 제안된 초기 PMSI 를 서버 개인 키를 이용하여 해독하는 단계;

상기 서버에 의해, 상기 UE 와 연관된 상기 초기 PMSI 로서 상기 제안된 초기 PMSI 를 저장하는 단계; 및

상기 UE 에, 상기 초기 PMSI 로서 상기 제안된 초기 PMSI 의 확인응답을 송신하는 단계

를 더 포함하는, 네트워크 상의 서버와의 네트워크 액세스를 셋업하기 위한 방법.

청구항 22

제 18 항에 있어서,

상기 서버와 상기 UE 사이에 공유된 비밀 키로부터 익명 키를 유도하는 단계;

유도된 상기 익명 키를 이용하여 상기 인증 정보에서의 상기 다음 PMSI 를 암호화하는 단계; 및

상기 UE 로부터의 후속 초기 어태치 메시지에 응답하는데 이용하기 위해 상기 서버에 상기 PMSI 대신에 상기 다음 PMSI 를 저장하는 단계

를 더 포함하는, 네트워크 상의 서버와의 네트워크 액세스를 셋업하기 위한 방법.

청구항 23

제 18 항에 있어서,

상기 결정하는 단계는,

상기 다음 PMSI 와 상이한 UE 와 연관된 다른 기존 PMSI 사이의 충돌을 검출하는 단계; 및

상기 추적 인덱스를 증분시키고 그리고 상기 다음 PMSI 및 증분된 상기 추적 인덱스에 기초하여 새로운 다음 PMSI 를 결정하는 단계

를 더 포함하는, 네트워크 상의 서버와의 네트워크 액세스를 셋업하기 위한 방법.

청구항 24

제 18 항에 있어서,

상기 서버가 위에 있는 홈 네트워크와는 별개인 상기 서빙 네트워크 상의 이동성 관리 엔티티 (MME) 로부터, 상기 UE 의 상기 IMSI 에 대한 요청을 수신하는 단계; 및

상기 요청에 응답하여, 상기 UE 의 상기 IMSI 대신에 상기 초기 어태치 메시지에서 이용되는 상기 UE 의 상기 PMSI 를 전송하는 단계

를 더 포함하는, 네트워크 상의 서버와의 네트워크 액세스를 셋업하기 위한 방법.

청구항 25

제 18 항에 있어서,

상기 초기 어태치 메시지에 포함된 상기 PMSI 에 대한 매치를 위해 하나 이상의 데이터베이스들을 탐색하는 단계; 및

매치를 로케이팅하지 않는 것에 응답하여, 상기 UE 에서의 업데이트된 PMSI 의 생성을 위해 상기 UE 에 유지된 PMSI 인덱스를 변경하기 위한 상기 UE 에 대한 통지를 전송하는 단계

를 더 포함하는, 네트워크 상의 서버와의 네트워크 액세스를 셋업하기 위한 방법.

청구항 26

서버로서,

사용자 장비 (UE) 의 복수의 프라이버시 모바일 가입자 아이덴티티들 (PMSI) 을 저장하도록 구성된 데이터베이스;

UE 로부터 개재하는 서빙 네트워크에서의 하나 이상의 네트워크 엘리먼트들을 통해, 초기 어태치 메시지로부터 상기 UE 를 식별하기 위해, 국제 모바일 가입자 아이덴티티 (IMSI) 에 대한 직접 대체물로서 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 수신하도록 구성된 트랜시버; 및

상기 PMSI 에 기초하여 상기 UE 에 대한 다음 PMSI 를 결정하도록 구성된 프로세서

를 포함하고;

상기 트랜시버는, 인증의 일부로서, 상기 다음 PMSI 및 추적 인덱스를 포함하는 인증 정보를 상기 서빙 네트워크에 송신하고, 그리고 상기 서빙 네트워크를 통해 상기 UE 로부터, 상기 다음 PMSI 에 매칭하는 상기 PMSI 및 상기 추적 인덱스로부터 유도된 UE-기반 다음 PMSI 에 응답하여 생성된 확인응답 토큰을 가진, 상기 다음 PMSI 의 확인을 포함하는 수신의 확인응답을 수신하도록 추가로 구성되는, 서버.

청구항 27

제 26 항에 있어서,

상기 프로세서는 초기 PMSI 에 기초하여 네트워크 액세스를 위한 상기 PMSI 를 결정하도록 추가로 구성되는, 서버.

청구항 28

제 27 항에 있어서,

상기 트랜시버는 상기 서버에의 상기 UE 의 가입자 등록 동안 상기 초기 PMSI 를 수신하도록 추가로 구성되는, 서버.

청구항 29

제 27 항에 있어서,

상기 트랜시버는 상기 UE 로부터, 제안된 초기 PMSI 를 수신하도록 추가로 구성되고;

상기 프로세서는, 대응하는 서버 공개 키에 의해 상기 UE 에서 암호화된 상기 제안된 초기 PMSI 를 서버 개인 키를 이용하여 해독하고 그리고 상기 UE 와 연관된 상기 초기 PMSI 로서 상기 제안된 초기 PMSI 를 저장하도록 추가로 구성되고; 그리고

상기 트랜시버는 상기 UE 에, 상기 초기 PMSI 로서 상기 제안된 초기 PMSI 의 확인응답을 송신하도록 추가로 구성되는, 서버.

청구항 30

제 26 항에 있어서,

상기 프로세서는, 상기 서버와 상기 UE 사이에 공유된 비밀 키로부터 익명 키를 유도하고 그리고 유도된 상기 익명 키를 이용하여 상기 인증 정보에서의 상기 다음 PMSI 를 암호화하도록 추가로 구성되고; 그리고

상기 데이터베이스는 상기 UE 로부터의 후속 초기 어태치 메시지에 응답하는데 이용하기 위해 상기 PMSI 대신에 상기 다음 PMSI 를 저장하도록 추가로 구성되는, 서버.

청구항 31

제 26 항에 있어서,

상기 프로세서는, 상기 결정하는 것의 일부로서,

상기 다음 PMSI 와 상기 데이터베이스에서의 상이한 UE 와 연관된 다른 기존 PMSI 사이의 충돌을 검출하고; 그리고

상기 추적 인덱스를 증분시키고 그리고 상기 다음 PMSI 및 증분된 상기 추적 인덱스에 기초하여 새로운 다음 PMSI 를 결정하도록

추가로 구성되는, 서버.

청구항 32

제 26 항에 있어서,

상기 트랜시버는,

상기 서버가 위에 있는 홈 네트워크와는 별개인 상기 서빙 네트워크 상의 이동성 관리 엔티티 (MME) 로부터, 상기 UE 의 상기 IMSI 에 대한 요청을 수신하고; 그리고

상기 요청에 응답하여, 상기 UE 의 상기 IMSI 대신에 상기 초기 어태치 메시지에서 이용되는 상기 UE 의 상기 PMSI 를 전송하도록

추가로 구성되는, 서버.

청구항 33

제 26 항에 있어서,

상기 프로세서는 상기 초기 어태치 메시지에 포함된 상기 PMSI 에 대한 매치를 위해 상기 데이터베이스를 탐색하도록 추가로 구성되고; 그리고

상기 트랜시버는 매치를 로케이팅하지 않는 것에 응답하여, 상기 UE 에서의 업데이트된 PMSI 의 생성을 위해 상기 UE 에 유지된 PMSI 인덱스를 변경하기 위한 상기 UE 에 대한 통지를 전송하도록 추가로 구성되는, 서버.

청구항 34

프로그램 코드를 기록하고 있는 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 프로그램 코드는,

사용자 장비 (UE) 로 하여금, 초기 어태치 메시지를 사용하여 상기 UE 를 식별하기 위해, 국제 모바일 가입자 아이덴티티 (IMSI) 에 대한 직접 대체물로서 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 서빙 네트워크로 전송하게 하기 위한 코드;

상기 UE 로 하여금, 상기 서빙 네트워크와 통신하는 서버로부터, 다음 PMSI 및 추적 인덱스를 포함하는 인증 요청을 수신하게 하기 위한 코드;

상기 UE 로 하여금, 상기 PMSI 및 상기 추적 인덱스로부터 UE-기반 다음 PMSI 를 유도하게 하기 위한 코드;

상기 UE 로 하여금, 상기 UE 와 상기 서버 사이에 PMSI 동기화의 매치가 있는지를 결정하기 위해 상기 인증 요청의 일부로서 수신된 상기 다음 PMSI 와 상기 UE-기반 다음 PMSI 를 비교하게 하기 위한 코드;

상기 UE 로 하여금, 상기 매치를 결정하는 것에 응답하여, 상기 UE-기반 다음 PMSI 와 상기 다음 PMSI 가 매칭하는 것에 응답하여 수신의 확인응답을 생성하게 하기 위한 코드; 및

상기 UE 로 하여금, 상기 서버로 상기 다음 PMSI 의 상기 수신의 확인응답을 전송하게 하기 위한 코드

를 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 35

제 34 항에 있어서,

상기 UE 로 하여금, 초기 PMSI 에 기초하여 네트워크 액세스를 위한 상기 PMSI 를 결정하게 하기 위한 코드를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 36

제 35 항에 있어서,

상기 UE 로 하여금, 상기 서버에의 상기 UE 의 가입자 등록 동안 상기 초기 PMSI 를 수신하게 하기 위한 코드를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 37

제 35 항에 있어서,

상기 UE 로 하여금, 상기 서버와의 공중 경유 통신을 통한 가입자 등록 후에 상기 초기 PMSI 를 프로비저닝하게 하기 위한 코드를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 38

제 37 항에 있어서,

상기 UE 로 하여금, 제안된 PMSI 를 생성하게 하기 위한 코드;

상기 UE 로 하여금, 서버 공개 키를 이용하여 생성된 상기 PMSI 를 암호화하게 하기 위한 코드로서, 상기 서버는 대응하는 서버 개인 키를 유지하는, 상기 PMSI 를 암호화하게 하기 위한 코드;

상기 UE 로 하여금, 상기 암호화 후에, 상기 서버로 생성된 상기 PMSI 를 전송하게 하기 위한 코드; 및

상기 UE 로 하여금, 상기 초기 PMSI 로서 생성된 상기 PMSI 를 이용하기 위해 상기 서버로부터 확인응답을 수신하게 하기 위한 코드

를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 39

제 34 항에 있어서,

상기 UE 로 하여금, 다음 어태치 메시지에서의 이용을 위해 상기 UE 에 확인된 상기 다음 PMSI 를 저장하게 하기 위한 코드를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 40

제 34 항에 있어서,

상기 UE 로 하여금, 익명 키를 이용하여 상기 인증 요청에서의 상기 다음 PMSI 를 해독하게 하기 위한 코드를 더 포함하며,

상기 익명 키는 상기 UE 와 상기 서버 사이에 공유된 비밀 키로부터 유도되는, 비일시적 컴퓨터 판독가능 저장

매체.

청구항 41

프로그램 코드를 기록하고 있는 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 프로그램 코드는,

서버로 하여금, 개재하는 서빙 네트워크에서의 하나 이상의 네트워크 엘리먼트들을 통해 사용자 장비 (UE) 로부터, 초기 어태치 메시지로부터 상기 UE 를 식별하기 위해, 국제 모바일 가입자 아이덴티티 (IMSI) 에 대한 직접 대체물로서 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 수신하게 하기 위한 코드;

상기 서버로 하여금, 상기 PMSI 에 기초하여 다음 PMSI 를 결정하게 하기 위한 코드;

상기 서버로 하여금, 인증의 일부로서, 상기 다음 PMSI 및 추적 인덱스를 포함하는 인증 정보를 상기 서빙 네트워크에 송신하게 하기 위한 코드; 및

상기 서버로 하여금, 상기 서빙 네트워크를 통해 상기 UE 로부터, 상기 다음 PMSI 에 매칭하는, 상기 PMSI 및 상기 추적 인덱스로부터 상기 UE 에 의해 유도된, UE-기반 다음 PMSI 에 응답하여 생성된 확인응답 토큰을 가진, 상기 다음 PMSI 의 확인을 포함하는 수신의 확인응답을 수신하게 하기 위한 코드

를 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 42

제 41 항에 있어서,

상기 서버로 하여금, 초기 PMSI 에 기초하여 네트워크 액세스를 위한 상기 PMSI 를 결정하게 하기 위한 코드를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 43

제 42 항에 있어서,

상기 서버로 하여금, 상기 서버에의 상기 UE 의 가입자 등록 동안 상기 초기 PMSI 를 수신하게 하기 위한 코드를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 44

제 42 항에 있어서,

상기 서버로 하여금, 상기 UE 로부터, 제안된 초기 PMSI 를 수신하게 하기 위한 코드;

상기 서버로 하여금, 대응하는 서버 공개 키에 의해 상기 UE 에서 암호화된 상기 제안된 초기 PMSI 를 서버 개인 키를 이용하여 해독하게 하기 위한 코드; 및

상기 서버로 하여금, 상기 UE 에, 상기 초기 PMSI 로서 상기 제안된 초기 PMSI 의 확인응답을 송신하게 하기 위한 코드

를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 45

제 41 항에 있어서,

상기 서버로 하여금, 상기 서버와 상기 UE 사이에 공유된 비밀 키로부터 익명 키를 유도하게 하기 위한 코드;

상기 서버로 하여금, 유도된 상기 익명 키를 이용하여 상기 인증 정보에서의 상기 다음 PMSI 를 암호화하게 하기 위한 코드; 및

상기 서버로 하여금, 상기 UE 로부터의 후속 초기 어태치 메시지에 응답하는데 이용하기 위해 상기 서버에 상기 PMSI 대신에 상기 다음 PMSI 를 저장하게 하기 위한 코드

를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 46

제 41 항에 있어서,

상기 서버로 하여금, 상기 다음 PMSI 를 결정하게 하기 위한 코드는,

상기 서버로 하여금, 상기 다음 PMSI 와 상이한 UE 와 연관된 다른 기존 PMSI 사이의 충돌을 검출하게 하기 위한 코드; 및

상기 서버로 하여금, 상기 추적 인덱스를 증분시키고 그리고 상기 다음 PMSI 및 증분된 상기 추적 인덱스에 기초하여 새로운 다음 PMSI 를 결정하게 하기 위한 코드

를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 47

제 41 항에 있어서,

상기 서버로 하여금, 상기 서버가 위에 있는 홈 네트워크와는 별개인 상기 서빙 네트워크 상의 이동성 관리 엔티티 (MME) 로부터, 상기 UE 의 상기 IMSI 에 대한 요청을 수신하게 하기 위한 코드; 및

상기 서버로 하여금, 상기 요청에 응답하여, 상기 UE 의 상기 IMSI 대신에 상기 초기 어태치 메시지에서 이용되는 상기 UE 의 상기 PMSI 를 전송하게 하기 위한 코드

를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 48

제 41 항에 있어서,

상기 서버로 하여금, 상기 초기 어태치 메시지에 포함된 상기 PMSI 에 대한 매치를 위해 하나 이상의 데이터베이스들을 탐색하게 하기 위한 코드; 및

상기 서버로 하여금, 매치를 로케이팅하지 않는 것에 응답하여, 상기 UE 에서의 업데이트된 PMSI 의 생성을 위해 상기 UE 에 유지된 PMSI 인덱스를 변경하기 위한 상기 UE 에 대한 통지를 전송하게 하기 위한 코드

를 더 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 49

삭제

발명의 설명

기 술 분 야

[0001] **관련 출원들에 대한 상호-참조**

[0002] 본 출원은, "Identity Privacy in Wireless Networks" 를 발명의 명칭으로 하여 2015년 3월 5일자로 출원된 미국 가특허출원 제62/128,724호의 이익을 주장하는 2015년 7월 24일자로 출원된 미국 정규특허출원 제14/808,862호의 이익을 주장하고, 이들 양자 모두의 개시는 전부 본 명세서에 참조로 통합된다.

[0003] **기술분야**

[0004] 본 출원은 무선 통신 시스템들에 관한 것으로, 특히 무선 통신 동안 가입자 아이덴티티들의 프라이버시를 증가시키는 것에 관한 것이다.

배 경 기 술

[0005] 네트워크로부터 서비스들을 수신하기 위해, 알려지지 않은 사용자 장비 (UE) 는 네트워크에 등록해야 하거나 또는 다르게는 네트워크에 알려져야 한다. 이것은 네트워크 어태치 프로시저 (network attach procedure) 를 이용하여 달성된다. 그 어태치 프로시저의 일부로서, UE 는 그의 국제 모바일 가입자 아이덴티티 (international mobile subscriber identity; IMSI) 번호를 전송한다. IMSI 는 UE 가 통신하는 (또는 그

대신 통신하는) 모든 네트워크들에 대해 그 UE 가 이용하는 고유 식별 (unique identification) 이다. UE 는 이동성 관리 엔티티 (mobility management entity; MME) 에서 수신되는 어태치 요청를 사용하여 IMSI 를 전송한다.

[0006] 도청자들 및 추적하는 것으로부터 IMSI 를 보호하려는 시도로, 임시 모바일 가입자 아이덴티티 (temporary mobile subscriber identity; TMSI) 가 UE 를 초기에 인증한 후에 이용될 수 있다. TMSI 는 특정 영역에 대해 로컬적이고 따라서 각각의 영역에서 재배정되어야 한다. 게다가, TMSI 는, (TMSI 의 배정이 UE 의 실제의 아이덴티티와 연관될 수 있도록 그리고) 초기 인증을 위해 UE 가 IMSI 를 제공한 후에 우선 배정된다. 때때로 글로벌 고유 임시 UE 아이덴티티 (globally unique temporary UE identity; GUTI) 가 IMSI 대신에 초기 어태치 요청에서 제공된다. UE 가 그의 IMSI 대신에 GUTI 를 전송하는 경우, MME 는 UE 와 이전에 상호작용했을 수도 있는 다른 네트워크 엘리먼트들로부터 식별을 요청한다. UE 가 다른 네트워크 엘리먼트들에 알려져 있다면, 그 다른 네트워크 엘리먼트들은 IMSI 로 응답한다. UE 가 알려져 있지 않다면, MME 는 그 후 로케이션 레지스터에 의한 업데이트 프로시저들을 위해 추후에 이용되는 식별을 위한 그의 IMSI 를 제공할 것을 UE 에게 요청한다.

[0007] 상기 접근법들 중 임의의 접근법 하에서, IMSI 는 여전히 취약하다. IMSI 는 초기 어태치 요청에 포함되거나 또는 인증되도록 하기 위하여 추후에 제공되어야 하거나 둘 중 어느 하나이다. 따라서, IMSI 는 공중 경유 (over-the-air) 트래픽을 통해 수동적으로 모니터링되고 사용자 아이덴티티를 결정하는데 이용될 수도 있다. 종종 어태치 요청에서의 IMSI 는 플레인텍스트로 있어, IMSI 를 모니터링에 훨씬 더 취약한 상태가 되게 한다. UE 가 IMSI 를 전송하지 않는 시나리오들에서도, MME 는 다른 네트워크 엘리먼트들로부터 실제 IMSI 를 여전히 획득하고, 여러 상이한 네트워크 엘리먼트들은 실제 IMSI 를 저장할 수도 있다 (예를 들어, MME, 서빙 게이트웨이 (S-GW), 및/또는 PDN 게이트웨이 (P-GW)). 이것은 IMSI 를 취약하고 서빙 네트워크의 신뢰성에 의존하는 상태가 되게 한다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0008] 본 개시의 하나의 양태에서, 사용자 장비 (UE) 에 의한 네트워크 액세스를 위한 방법은, UE 로부터, 네트워크 상의 서버로 초기 어태치 메시지를 사용하여 UE 를 식별하기 위한 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 국제 모바일 가입자 아이덴티티 (IMSI) 대신에 전송하는 단계, 서버로부터, 다음 PMSI 를 포함하는 인증 요청을 수신하는 단계로서, 다음 PMSI 는 PMSI 로부터 유도된 상이한 값인, 상기 인증 요청을 수신하는 단계, 및 UE 로부터, 서버로 다음 PMSI 의 수신의 확인응답을 전송하는 단계를 포함한다.

[0009] 본 개시의 추가적인 양태에서, 사용자 장비는, 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 저장하도록 구성된 메모리, 네트워크 상의 서버로 초기 어태치 메시지를 사용하여 UE 를 식별하기 위한 PMSI 를 국제 모바일 가입자 아이덴티티 (IMSI) 대신에 전송하고 그리고 서버로부터, 다음 PMSI 를 포함하는 인증 요청을 수신하는 것으로서, 다음 PMSI 는 PMSI 로부터 유도된 상이한 값인, 상기 인증 요청을 수신하도록 구성된 트랜시버, 및 수신의 확인응답을 생성하도록 구성된 프로세서로서, 트랜시버는 서버로 수신의 확인응답을 전송하도록 추가로 구성되는, 상기 프로세서를 포함한다.

[0010] 본 개시의 추가적인 양태에서, 프로그램 코드를 기록하고 있는 컴퓨터 판독가능 매체는, 사용자 장비 (UE) 로 하여금, 네트워크 상의 서버로 초기 어태치 메시지를 사용하여 UE 를 식별하기 위한 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 국제 모바일 가입자 아이덴티티 (IMSI) 대신에 전송하게 하기 위한 코드, UE 로 하여금, 서버로부터, 다음 PMSI 를 포함하는 인증 요청을 수신하게 하기 위한 코드로서, 다음 PMSI 는 PMSI 로부터 유도된 상이한 값인, 상기 인증 요청을 수신하게 하기 위한 코드, 및 UE 로 하여금, 서버로 다음 PMSI 의 수신의 확인응답을 전송하게 하기 위한 코드를 포함한다.

[0011] 본 개시의 추가적인 양태에서, 네트워크 상의 서버로 네트워크 액세스를 셋업하기 위한 방법은, 개재하는 서빙 네트워크에서의 하나 이상의 네트워크 엘리먼트들을 통해 사용자 장비 (UE) 로부터, 초기 어태치 메시지로부터 UE 를 식별하기 위한 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 국제 모바일 가입자 아이덴티티 (IMSI) 대신에 수신하는 단계, 서버에 의해, PMSI 에 기초하여 다음 PMSI 를 결정하는 단계, 서버로부터, 다음 PMSI 를

포함하는 인증 요청을 송신하는 단계, 및 UE 로부터, 다음 PMSI 의 확인을 포함하는 수신의 확인응답을 수신하는 단계를 포함한다.

[0012] 본 개시의 추가적인 양태에서, 서버는, 사용자 장비 (UE) 의 복수의 프라이버시 모바일 가입자 아이덴티티들 (PMSI) 을 저장하도록 구성된 데이터베이스, UE 로부터 개재하는 서빙 네트워크에서의 하나 이상의 네트워크 엘리먼트들을 통해, 초기 어태치 메시지로부터 UE 를 식별하기 위한 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 국제 모바일 가입자 아이덴티티 (IMSI) 대신에 수신하도록 구성된 트랜시버, 및 PMSI 에 기초하여 UE 에 대한 다음 PMSI 를 결정하도록 구성된 프로세서로서, 트랜시버는 다음 PMSI 를 포함하는 인증 요청을 송신하고 그리고 다음 PMSI 의 확인을 포함하는 수신의 확인응답을 수신하도록 추가로 구성되는, 상기 프로세서를 포함한다.

[0013] 본 개시의 추가적인 양태에서, 프로그램 코드를 기록하고 있는 컴퓨터 판독가능 매체는, 서버로 하여금, 개재하는 서빙 네트워크에서의 하나 이상의 네트워크 엘리먼트들을 통해 사용자 장비 (UE) 로부터, 초기 어태치 메시지로부터 UE 를 식별하기 위한 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 국제 모바일 가입자 아이덴티티 (IMSI) 대신에 수신하게 하기 위한 코드, 서버로 하여금, PMSI 에 기초하여 다음 PMSI 를 결정하게 하기 위한 코드, 서버로 하여금, 다음 PMSI 를 포함하는 인증 요청을 송신하게 하기 위한 코드, 및 서버로 하여금, UE 로부터, 다음 PMSI 의 확인을 포함하는 수신의 확인응답을 수신하게 하기 위한 코드를 포함한다.

도면의 간단한 설명

[0014] 도 1 은 본 개시의 다양한 양태들에 따른 무선 통신 네트워크를 예시한다.

도 2 는 본 개시의 실시형태들에 따른 예시적인 UE 의 블록 다이어그램이다.

도 3 은 본 개시의 실시형태들에 따른 예시적인 서버의 블록 다이어그램이다.

도 4 는 본 개시의 다양한 양태들에 따른 예시적인 송신기 시스템을 예시하는 블록 다이어그램이다.

도 5 는 본 개시의 다양한 양태들에 따라 무선 네트워크들에서 아이덴티티 프라이버시를 지원하기 위한 UE, 서빙 네트워크, 및 홈 네트워크 사이의 일부 시그널링 양태들을 예시하는 프로토콜 다이어그램이다.

도 6a 는 본 개시의 다양한 양태들에 따른 어태치 프로세스를 개시하는 UE 에 대한 예시적인 방법을 예시하는 플로우차트이다.

도 6b 는 본 개시의 다양한 양태들에 따른 어태치 프로세스에서 기능하는 서버에 대한 예시적인 방법을 예시하는 플로우차트이다.

도 7a 는 본 개시의 다양한 양태들에 따른 UE 에 대한 PMSI 초기화를 위한 예시적인 방법을 예시하는 플로우차트이다.

도 7b 는 본 개시의 다양한 양태들에 따른 서버에 대한 PMSI 초기화를 위한 예시적인 방법을 예시하는 플로우차트이다.

발명을 실시하기 위한 구체적인 내용

[0015] 아래에 기재된 상세한 설명은, 첨부된 도면들과 관련하여, 다양한 구성들의 설명으로서 의도되고 본 명세서에서 설명된 개념들이 실시될 수도 있는 유일한 구성들을 표현하도록 의도되지 않는다. 상세한 설명은 다양한 개념들의 철저한 이해를 제공하는 목적을 위해 특정 상세들을 포함한다. 그러나, 이들 개념들은 이들 특정 상세들 없이 실시될 수도 있다는 것이 당업자들에게 명백할 것이다. 일부 인스턴스들에서, 잘 알려진 구조들 및 컴포넌트들은 이러한 개념들을 모호하게 하는 것을 회피하기 위하여 블록 다이어그램 형태로 도시된다.

[0016] 본 명세서에서 설명된 기법들은 CDMA, TDMA, FDMA, OFDMA, SC-FDMA 및 다른 네트워크들과 같은 다양한 무선 통신 네트워크들을 위해 이용될 수도 있다. 용어들 "네트워크" 및 "시스템" 은 종종 상호교환가능하게 사용된다. CDMA 네트워크는 범용 지상 무선 액세스 (Universal Terrestrial Radio Access; UTRA), cdma2000 등과 같은 무선 기술을 구현할 수도 있다. UTRA 는 광대역 CDMA (WCDMA) 및 CDMA 의 다른 변형들을 포함한다. cdma2000 은 IS-2000, IS-95 및 IS-856 표준들을 커버한다. TDMA 네트워크는 GSM (Global System for Mobile Communications) 과 같은 무선 기술을 구현할 수도 있다. OFDMA 네트워크는 진화된 UTRA (E-UTRA), UMB (Ultra Mobile Broadband), IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, Flash-OFDMA 등과 같은 무선 기술을 구현할 수도 있다. UTRA 및 E-UTRA 는 범용 모바일 전기통신 시스템 (Universal Mobile

Telecommunication System; UMTS) 의 일부이다. 3GPP 롱 텀 에볼루션 (Long Term Evolution; LTE) 및 LTE-어드밴스드 (LTE-A) 는 E-UTRA 를 이용하는 UMTS 의 새로운 릴리즈들이다. UTRA, E-UTRA, UMTS, LTE, LTE-A 및 GSM 은 "제 3 세대 파트너십 프로젝트" (3GPP) 로 명명된 기관으로부터의 문서들에 설명되어 있다. CDMA2000 및 UMB 는 "제 3 세대 파트너십 프로젝트 2" (3GPP2) 로 명명된 기관으로부터의 문서들에 설명되어 있다. 본 명세서에서 설명된 기법들은 상기 언급된 무선 네트워크들 및 무선 기술들 뿐만 아니라 다른 무선 네트워크들 및 무선 기술들, 이를 테면 차세대 (예를 들어, 제 5 세대 (5G)) 네트워크를 위해 이용될 수도 있다. 본 개시의 실시형태들은 상기 열거된 네트워크들 및/또는 아직 개발되지 않은 것들 중 임의의 하나 이상 상에서 이용될 수도 있는 임의의 타입의 변조 스킴에 관련된다.

[0017] 본 개시의 실시형태들은 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 대신 제공함으로써 사용자 장비의 국제 모바일 가입자 아이덴티티를 보호하기 위한 시스템들 및 기법들을 도입한다. 실시형태에서, UE 는 서빙 네트워크에 어태치 요청을 개시한다. IMSI 또는 서빙 네트워크 상의 일부 엘리먼트가 IMSI 에 액세스하기 위해 여전히 이용할 수 있는 연관된 정보를 제공하는 대신에, UE 는 PMSI 를 어태치 요청과 함께 제공한다. PMSI 는 그 후, IMSI 가 UE 와 서버 사이에서 요구되지 않도록, 프로세스 전반에 걸쳐 이용된다. 실시형태에서, (각각의 UE 에 대한 그리고 또한 특정 UE 에 대한 상이한 반복 (iteration) 들에 대한) 각각의 PMSI 는 다른 것들로부터 고유하다. 이것은 도청하는 것으로부터 그리고 서빙 네트워크에서의 임의의 잠재적으로 악의적인 엘리먼트들로부터 IMSI 를 보호한다. 이 예를 계속하면, 서빙 네트워크의 엘리먼트들은 인증 정보 요청의 일부로서 PMSI 를 (예를 들어, 홈 가입자 서버 (HSS) 와 같은) UE 의 홈 네트워크 상의 서버로 전달한다. HSS 는 대응하는 UE 를 식별하기 위해 PMSI 를 로케이팅하고 인증 정보 응답을 네트워크 엘리먼트에 제공한다. 응답의 일부로서, HSS 는 또한 UE 가 후속 어태치 요청을 위해 이용할 다음 PMSI 를 유도하고, PMSI 충돌들에 대해 체크하고, 그리고 다음 PMSI 및 PMSI 추적 인덱스를 UE 로 함께 전달하기 위해 서빙 네트워크에서의 네트워크 엘리먼트들에 제공한다.

[0018] 다음 PMSI 및 PMSI 추적 인덱스는 암호화된 형태로 제공될 수 있다. 암호화된 형태에서, 다음 PMSI 및 PMSI 추적 인덱스는 서빙 네트워크에서의 잠재적으로 악의적인 네트워크 엘리먼트들로부터 그리고 도청하는 것으로부터 보호되는 상태로 있다. UE 는 암호화된 다음 PMSI 및 PMSI 추적 인덱스를 수신하고 그들을 해독할 수 있다. UE 는 UE 및 HSS 가 동기화되는 것을 확인하기 위해 다음 PMSI 의 그 자신의 카피를 유도한다. 다음 PMSI 가 UE 와 HSS 사이에서 동기화된다고 확인한 후에, UE 는 서버로 확인응답 토큰을 전송한다. UE 및 서버는 그 후 각각 현재 및 다음 PMSI 값들의 로컬 카피들을 업데이트한다. HSS 는 UE 에 대한 PMSI 의 모든 반복을 저장할 필요는 없다. 그 대신에, HSS 는 초기 PMSI 값 및 원하는 PMSI 추적 인덱스 값에 기초하여 PMSI 의 임의의 반복에 도달할 수 있다.

[0019] 추가의 실시형태에서, 초기 PMSI 는 UE 와 HSS 사이에 합의될 수도 있다. 실시형태에서, 초기 PMSI 는, 초기 PMSI 가 UE 의 SIM 카드에 프로비저닝되고 HSS 에 등록되도록, 가입자 등록에서 합의된다. 다른 실시형태에서, UE 는 가입자 등록에서 PMSI 가 프로비저닝되지 않고 오히려 HSS 와 공중 경유 등록을 개시한다. UE 는 초기 PMSI 값을 생성하고, 그리고 HSS 의 공개 키 (public key) (또는 UE 와 HSS 사이의 다른 공유 키) 를 이용하여 초기 PMSI 값을 암호화한 후에, HSS 로 제안된 초기 PMSI 를 전송할 수도 있다. HSS 는 대응하는 개인 키 (private key) 로 UE 로부터의 초기 PMSI 를 해독하고 PMSI 가 HSS 에 등록된 임의의 다른 기존 PMSI 값들과 충돌하는지 여부를 결정할 수도 있다. 어떤 충돌들도 없다는 것을 확인 시에, HSS 는 UE 에 초기 PMSI 를 확인응답하고 그리고 그것을, UE 가 추후에 그의 첫번째 어태치 요청을 개시할 때의 이용을 위해 저장할 수도 있다.

[0020] 도 1 은 본 개시의 다양한 양태들에 따른 무선 통신 네트워크 (100) 를 예시한다. 무선 통신 네트워크 (100) 는 다수의 UE들 (102), 뿐만 아니라 다수의 기지국들 (104) 을 포함할 수도 있다. 단일의 UE (102) 및 단일의 기지국 (104) 이 단지 예시 및 설명의 단순성을 위해 도 1 에 도시되어 있다. 기지국 (104) 은 진화된 노드 B (eNodeB) 를 포함할 수도 있다. 기지국은 또한 기지국 트랜시버 또는 액세스 포인트로 지칭될 수도 있다.

[0021] 기지국 (104) 은 도시한 바와 같이 UE (102) 와 통신한다. UE (102) 는 업링크 및 다운링크를 통해 기지국 (104) 과 통신할 수도 있다. 다운링크 (또는 순방향 링크) 는 기지국 (104) 으로부터 UE (102) 로의 통신 링크를 지칭한다. 업링크 (또는 역방향 링크) 는 UE (102) 로부터 기지국 (104) 으로의 통신 링크를 지칭한다.

[0022] UE들 (102) 은 무선 네트워크 (100) 전반에 걸쳐 산재될 수도 있고, 각각의 UE (102) 는 정지식 또는 이동식일

수도 있다. UE (102) 는 또한 단말기, 이동국, 가입자 유닛 등으로 지칭될 수도 있다. UE (102) 는 셀룰러 폰, 스마트폰, 개인 휴대 정보 단말기, 무선 모뎀, 랩톱 컴퓨터, 태블릿 컴퓨터 등일 수도 있다. 무선 통신 네트워크 (100) 는 본 개시의 다양한 양태들이 적용되는 네트워크의 하나의 예이다.

[0023] 도 1 에는 또한, 이동성 관리 엔티티 (MME) (106) 가 예시되어 있다. MME (106) 는 세션 관리 및 가입자들 (예를 들어, UE (102)) 에 관련된 제어 평면 기능들을 담당하고 있을 수도 있다. 예를 들어, MME (106) 는 이동성 세션 관리, 뿐만 아니라 다른 네트워크들로의 핸드오버들, 로밍, 및 가입자 인증에 대한 지원을 제공할 수도 있다. MME (106) 는, 몇 가지만 예로 들면, UE (102) 의 초기 어태치 동안의 S-GW 의 선택, NAS (non-access stratum) 시그널링, NAS 시그널링 보안, P-GW 선택, 전용 베어러 확립을 포함한 베어러 관리 기능들, 시그널링 트래픽의 합법적 도청, 및 다른 기능들을 도울 수도 있다. MME (106) 및 기지국 (104) 은 동일한 서빙 네트워크 (108) (예를 들어, 진화된 패킷 코어 (EPC) 의 일부) 에 있을 수도 있다. 인지될 바와 같이, 서빙 네트워크 (108) 는 본 개시의 양태들의 논의의 단순성을 위해 도 1 에 도시되지 않은 많은 다른 네트워크 엘리먼트들을 포함한다.

[0024] MME (106) 는 홈 네트워크 (114) 에서의 서버 (112) 와 통신한다. 실시형태에서, 서버 (112) 는, 다른 것들 중에서 사용자 가입 정보를 유지하는 하나 이상의 데이터베이스들을 저장 및 업데이트하는 것을 담당하고 있는 홈 로케이션 레지스터 (home location register; HLR) 를 유지하는 홈 가입자 서버 (HSS) 이다. 다른 것들 중에서, 홈 네트워크 (114) 에서의 서버 (112) 는 UE (102) 에 대한 IMSI (사용자 식별/어드레싱) 의 카피를 갖는다. 서버 (112) 는 또한 서비스 가입 상태들 및/또는 서비스 품질 (QoS) 정보 (예를 들어, 최대 허용된 비트 레이트, 허용된 트래픽 클래스, 등) 를 식별하는 사용자 프로파일 정보를 유지할 수도 있다. 서버 (112) 는 또한, 인증 기능들, 이를 테면 사용자 아이덴티티 키들로부터의 보안 정보 생성을 관리하는 것 및 보안 정보의 HLR (및 다른 네트워크 엔티티들) 에의 프로비전을 포함할 수도 있다. 보안 정보에 의해, 네트워크-UE 인증이 수행될 수도 있다. 하나의 서버 (112) 가 예시 및 설명의 단순성의 목적들을 위해 도 1 에 예시된다. 홈 네트워크 (114) 는 다수의 HSS 를 포함할 수도 있다. 예를 들어, HSS 의 수는 모바일 가입자들의 수, 장비 용량, 및 네트워크 조직화에 의존할 수도 있다. MME (106) 는 인지될 바와 같이 다양한 타입들의 직접 또는 간접 접속일 수도 있는 네트워크 (110) 를 통해 서버 (112) 와 통신할 수도 있다.

[0025] 무선 네트워크들에서 아이덴티티 프라이버시를 지원하기 위한 UE, 서빙 네트워크, 및 홈 네트워크 (및 연관된 서버) 사이의 일부 시그널링 양태들을 예시하는 프로토콜 다이어그램을 포함하는 후속 도면들에 대하여 아래에 더 상세히 설명될 바와 같이, UE (102) 는 IMSI 를 제외하고 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 이용하여 서빙 네트워크 (108) 및 홈 네트워크 (114) 와 통신할 수도 있다. PMSI 는 UE (102) 와 특별히 연관되고 UE (102) 와 서버 (112) 양자 모두에 의해 유지되는 고유 번호일 수도 있다. 본 개시의 실시형태들에서, PMSI 는 UE (102) 와 서버 (112) 양자 모두에서 합의되고 유지되는 초기 PMSI 를 포함할 수도 있다. UE (102) 의 PMSI 에 대한 특정한 값이 한번 이용될 수도 있어, UE (102) 가 어태치 요청을 개시하는 각각의 후속 시간에 새로운 PMSI 값이 요청의 일부로서 제공된다. UE (102) 및 서버 (112) 는 단지 합의되는 초기 PMSI 및 인덱스를 저장할 수도 있다. 그 결과, PMSI 값은 (예를 들어, UE (102) 및 서버 (112) 가 주어진 세션을 위해 이용되는 특정한 PMSI 에 대해 계속 합의 상태에 있도록) UE (102) 와 서버 (112) 양자 모두에서 특정 PMSI 에 도달하기 위해 얼마나 많은 유도 반복들이 수행되어야 하는지를 설명하기 위해 초기 PMSI 및 특정 인덱스 값의 공유된 지식에 기초하여 후속하여 유도될 수도 있다.

[0026] 예에서, UE (102) 는, 기지국 (104) 으로 그의 초기 어태치 요청의 일부로서, 그의 PMSI 를 IMSI 대신에 전송할 수도 있다. 기지국 (104) 은 그 후 UE 의 PMSI 를 가진 어태치 요청을 MME (106) 로 포워딩한다. MME (106) 는 홈 네트워크 (114) 에서의 서버 (112) 로의 인증 정보 요청에 PMSI 를 포함한다. 서버 (112) 는 IMSI 가 서빙 네트워크 (108) 에 제공될 필요가 없도록, MME (106) 로부터의 초기 어태치 요청/인증 정보 요청에서 제공된 PMSI 에 기초하여 UE (102) 를 식별할 수 있다. 서버 (112) 로부터 다시 UE (102) 로의 통신도 물론 IMSI 대신에 PMSI 에 또한 기초/포함할 것이다. 통신 경로에서의 이들 스테이지들 전부에서의 IMSI 를 대신한 PMSI 의 이용은, PMSI 가 IMSI 대신에 저장될 것이기 때문에, UE (102) 와 기지국 (104) 사이의 공중 경유 도청의 위험을 감소시키고 서빙 네트워크 (108) 에서의 임의의 네트워크 엘리먼트들로부터 UE (102) 의 IMSI 의 이용가능성을 제거한다.

[0027] 도 2 는 본 개시의 실시형태들에 따른 예시적인 UE (102) 의 블록 다이어그램이다. UE (102) 는 상기 설명된 많은 구성들 중 임의의 하나를 가질 수도 있다. UE (102) 는 프로세서 (202), 메모리 (204), PMSI 모듈 (208), 트랜시버 (210), 및 안테나 (216) 를 포함할 수도 있다. 이들 엘리먼트들은 예를 들어, 하나 이상의

버스들을 통해, 서로 직접 또는 간접 통신하고 있을 수도 있다.

[0028] 프로세서 (202) 는 중앙 프로세싱 유닛 (CPU), 디지털 신호 프로세서 (DSP), 애플리케이션-특정 집적 회로 (ASIC), 제어기, 필드 프로그래밍가능 게이트 어레이 (FPGA) 디바이스, 다른 하드웨어 디바이스, 펌웨어 디바이스, 또는 도 1 에 대하여 상기 도입된 UE (102) 를 참조하여 본 명세서에서 설명되고 아래에 더 상세히 논의된 동작들을 수행하도록 구성된 그 임의의 조합을 포함할 수도 있다. 프로세서 (202) 는 또한 컴퓨팅 디바이스들의 조합, 예를 들어, DSP 와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 이상의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수도 있다.

[0029] 메모리 (204) 는 캐시 메모리 (예를 들어, 프로세서 (202) 의 캐시 메모리), 랜덤 액세스 메모리 (RAM), 자기저항식 RAM (MRAM), 판독-전용 메모리 (ROM), 프로그래밍가능 판독-전용 메모리 (PROM), 소거가능한 프로그래밍가능 판독 전용 메모리 (EPROM), 전기적으로 소거가능한 프로그래밍가능 판독 전용 메모리 (EEPROM), 플래시 메모리, 솔리드 스테이트 메모리 디바이스, 하드 디스크 드라이브들, 다른 형태들의 휘발성 및 비휘발성 메모리, 또는 상이한 타입들의 메모리의 조합을 포함할 수도 있다. 실시형태에서, 메모리 (204) 는 비일시적 컴퓨터 판독가능 매체를 포함한다. 메모리 (204) 는 명령들 (206) 을 저장할 수도 있다. 명령들 (206) 은, 프로세서 (202) 에 의해 실행될 때, 프로세서 (202) 로 하여금, 본 개시의 실시형태들과 관련하여 UE (102) 를 참조하여 본 명세서에서 설명된 동작들을 수행하게 하는 명령들을 포함할 수도 있다. 명령들 (206) 은 코드로 또한 지칭될 수도 있다. 용어들 "명령들" 및 "코드" 는 임의의 타입의 컴퓨터 판독가능 스테이트먼트(들)를 포함하는 것으로 폭넓게 해석되어야 한다. 예를 들어, 용어들 "명령들" 및 "코드" 는 하나 이상의 프로그램들, 루틴들, 서브-루틴들, 함수들, 프로시저들, 등을 지칭할 수도 있다. "명령들" 및 "코드" 는 단일의 컴퓨터 판독가능 스테이트먼트 또는 다수의 컴퓨터 판독가능 스테이트먼트들을 포함할 수도 있다.

[0030] PMSI 모듈 (208) 은 본 개시의 다양한 양태들을 위해 이용될 수도 있다. 예를 들어, PMSI 모듈 (208) 은 특정 UE (102) 에 대한 PMSI 의 초기 프로비저닝에 관계될 수도 있다. 실시형태에서, PMSI 는 UE (102) 에 대한 IMSI 와 동시에 UE (102) 에 프로비저닝된다. 예를 들어, 일부 인스턴스들에서, PMSI 는 도 1 의 서버 (112) 와 같은 HSS 에의 가입자 등록 동안 IMSI 와 함께 프로비저닝된다. 이 프로비저닝은 제조 시에 UE (102) 상의 SIM 카드에서 일어날 수도 있다. 다른 실시형태에서, IMSI 는 PMSI 가 UE (102) 와 서버 (112) 사이에 합의되기 전에 프로비저닝될 수도 있다. 예를 들어, UE (102) 및 서버 (112) 는 IMSI 가 UE (102) 에 대해 이미 프로비저닝된 후에 공중 경유로 제 1 (초기) PMSI 에 합의할 수도 있다. PMSI 가 공중 경유로 합의될 때, UE (102) 는 (아래에 도 7a 에 대하여 더 상세히 논의될 바와 같이) 제안된 초기 PMSI 를 생성하고 제안된 초기 PMSI 를 서버 (112) 에 의해 제공된 공개 키로 암호화할 수도 있다. 이렇게 하여, UE (102) 에 의해 송신된 제안된 초기 PMSI 는 도청하는 것 및 서빙 네트워크 (108) 에서의 잠재적으로 타협된 네트워크 엘리먼트들로부터 보호될 수도 있다. 서버 (112) 는 대응하는 개인 키를 유지하고 제안된 초기 PMSI 를 해독할 수 있다. 서버 (112) 는 서버 (112) 에 의해 또는 다르게는 홈 네트워크 (114) 내에 유지된 임의의 다른 UE 의 PMSI 와의 충돌들이 없다는 것을 입증하기 위해 하나 이상의 데이터베이스들에 대해 제안된 초기 PMSI 를 체크할 수도 있다.

[0031] PMSI 모듈 (208) 은 추가적으로 PMSI 확인응답에 관계될 수도 있다. 상기 언급한 바와 같이, 특정한 PMSI 값 (초기 PMSI 에 기초함) 은 상이한 PMSI 값이 후속 어태치 요청들을 위해 제공되도록 미리결정된 수의 어태치 요청들 (예를 들어, 1, 2, 3, 또는 그 이상) 을 위해서만 이용될 수도 있다. UE (102) 로부터의 어태치 요청에 응답하여, 서버 (112) 는 "다음 PMSI" - 후속 세션에서 이용될 다음 PMSI 값 - 를 생성하고 초기 어태치 요청에 응답하여 인증 요청의 일부로서 다음 PMSI 를 UE (102) 와 공유할 수도 있다. UE (102) 의 PMSI 모듈 (208) 은 저장된 초기 PMSI 및 증분된 인덱스 (아래에 추가로 논의함) 에 기초하여 그 자신의 다음 PMSI 값을 계산하고 로컬 계산된 다음 PMSI 를 서버 (112) 로부터 수신된 다음 PMSI 와 비교할 수도 있다. 매치 (match) 가 있다면, PMSI 모듈 (208) 은, UE (102) 로 하여금, 서버 (112) 에 다음 PMSI 를 확인응답하는 응답을 생성하게 할 수도 있다. 매치가 없다면, PMSI 모듈 (208) 은, 재컴퓨테이션 후에 값들이 매치하도록 다음 PMSI 를 사용하여 서버 (112) 로부터 수신된 인덱스로 그의 로컬 인덱스를 업데이트할 수도 있다.

[0032] 트랜시버 (210) 는 모뎀 서브시스템 (212) 및 무선 주파수 (RF) 유닛 (214) 을 포함할 수도 있다. 트랜시버 (210) 는 기지국들 (104) 과 같은 다른 디바이스들과 양방향으로 통신하도록 구성된다. 모뎀 서브시스템 (212) 은 변조 및 코딩 스킴 (MCS), 예를 들어, 저밀도 패리티 체크 (low-density parity check; LDPC) 코딩 스킴, 터보 코딩 스킴, 콘볼루션 코딩 스킴, 등에 따라 PMSI 모듈 (208) 로부터 데이터를 변조 및/또는 인코딩하도록 구성될 수도 있다. RF 유닛 (214) 은 (아웃바운드 송신들에 대한) 모뎀 서브시스템 (212) 으로부터의 또는 기지국 (104) 과 같은 다른 소스에서 비롯되는 송신들의 변조된/인코딩된 데이터를 프로세싱 (예를 들

어, 아날로그 투 디지털 컨버전 또는 디지털 투 아날로그 컨버전 등을 수행) 하도록 구성될 수도 있다. 트랜시버 (210) 에 함께 통합된 것으로서 도시되지만, 모뎀 서브시스템 (212) 및 RF 유닛 (214) 은 UE (102) 가 다른 디바이스들과 통신하는 것을 가능하게 하기 위해 UE (102) 에서 함께 커플링되는 별개의 디바이스들일 수도 있다.

[0033] RF 유닛 (214) 은 하나 이상의 다른 디바이스들로의 송신을 위해 안테나 (216) 에 변조된 및/또는 프로세싱된 데이터, 예를 들어, 데이터 패킷들 (또는, 더 일반적으로는, 하나 이상의 데이터 패킷들 및 PMSI 값들을 포함한 다른 정보를 포함할 수도 있는 데이터 메시지들) 을 제공할 수도 있다. 이것은, 예를 들어, 본 개시의 실시형태들에 따른 기지국 (104) 으로의 데이터 메시지들의 송신을 포함할 수도 있다. 안테나 (216) 는 또한, 기지국 (104) 으로부터 송신된 데이터 메시지들을 수신하고 수신된 데이터 메시지들을 트랜시버 (210) 에서의 프로세싱 및/또는 복조를 위해 제공할 수도 있다. 도 2 는 단일의 안테나로서 안테나 (216) 를 예시하지만, 안테나 (216) 는 다수의 송신 링크들을 유지하기 위하여 유사한 또는 상이한 설계들의 다수의 안테나들을 포함할 수도 있다.

[0034] 도 3 은 본 개시의 실시형태들에 따른 예시적인 서버 (112) 의 블록 다이어그램이다. 서버 (112) 는 프로세서 (302), 메모리 (304), PMSI 모듈 (308), 데이터베이스 (310), 및 트랜시버 (312) 를 포함할 수도 있다. 이들 엘리먼트들은 예를 들어, 하나 이상의 버스들을 통해, 서로 직접 또는 간접 통신하고 있을 수도 있다. 도 1 에 대하여 상기 언급한 바와 같이, 서버 (112) 는 단지 2 개만 예로 들면, 홈 로케이션 레지스터 및 인증 기능성을 제공하는 HSS 일 수도 있다.

[0035] 프로세서 (302) 는 CPU, DSP, ASIC, 제어기, FPGA 디바이스, 다른 하드웨어 디바이스, 펌웨어 디바이스, 또는 상기 도 1 에서 도입된 서버 (112) 를 참조하여 본 명세서에서 설명된 동작들을 수행하도록 구성된 그 임의의 조합을 포함할 수도 있다. 프로세서 (302) 는 또한, 컴퓨팅 디바이스들의 조합, 예를 들어, DSP 와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 이상의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수도 있다.

[0036] 메모리 (304) 는 캐시 메모리 (예를 들어, 프로세서 (302) 의 캐시 메모리), RAM, MRAM, ROM, PROM, EPROM, EEPROM, 플래시 메모리, 솔리드 스테이트 메모리 디바이스, 하나 이상의 하드 디스크 드라이브들, 다른 형태들의 휘발성 및 비휘발성 메모리, 또는 상이한 타입들의 메모리의 조합을 포함할 수도 있다. 실시형태에서, 메모리 (304) 는 비일시적 컴퓨터 판독가능 매체를 포함한다. 메모리 (304) 는 명령들 (306) 을 저장할 수도 있다. 명령들 (306) 은, 프로세서 (302) 에 의해 실행될 때, 프로세서 (302) 로 하여금, 본 개시의 실시형태들과 관련하여 서버 (112) 를 참조하여 본 명세서에서 설명된 동작들을 수행하게 하는 명령들을 포함할 수도 있다. 명령들 (306) 은 또한, 도 2 에 대하여 상기 논의한 바와 같은 임의의 타입의 컴퓨터 판독가능 스테이트먼트(들)를 포함하는 것으로 폭넓게 해석될 수도 있는 코드로 지칭될 수도 있다.

[0037] PMSI 모듈 (308) 은 본 개시의 다양한 양태들을 위해 이용될 수도 있다. 예를 들어, PMSI 모듈 (308) 은 특정 UE (102) 에 대한 PMSI 의 초기 프로비저닝에 관계될 수도 있다. 실시형태에서, PMSI 는 예를 들어, 가입자 등록 동안, UE (102) 에 대한 IMSI 와 동시에 데이터베이스 (310) 에 프로비저닝 및 저장된다. 다른 실시형태에서, IMSI 는 PMSI 가 서버 (112) 와 UE (102) 사이에 합의되기 전에 프로비저닝될 수도 있다. 예를 들어, 서버 (112) 는 IMSI 가 UE (102) 에 대해 이미 프로비저닝된 후에 UE (102) 로부터 공중 경유로 제 1 (초기) PMSI 에 합의할 수도 있다. 공중 경유로 합의할 때, 서버 (112) 는 (아래에 도 7b 에 대하여 더 상세히 논의될 바와 같이) UE (102) 에 의해 생성되고 UE (102) 로부터 수신된 제안된 초기 PMSI 를 수신할 수도 있다. 제안된 초기 PMSI 는 서버 (112) 에 의해 UE (102) 에 제공된 공개 키로 암호화되었을 수도 있다. 그 결과, 서버 (112) 는 대응하는 개인 키를 이용하여 제안된 초기 PMSI 를 해독할 수도 있다. 이렇게 하여, PMSI 는 도청하는 것 및 서빙 네트워크 (108) 에서의 잠재적으로 타협된 네트워크 엘리먼트들로부터 보호될 수도 있다. 서버 (112) 는 서버 (112) 에 의해 또는 다르게는 홈 네트워크 (114) 내에 유지된 임의의 다른 UE 의 PMSI 와의 충돌들이 없다는 것을 입증하기 위해 데이터베이스 (310) 에서의 PMSI 값들에 대해 제안된 초기 PMSI 를 체크할 수도 있다.

[0038] PMSI 모듈 (308) 은 추가적으로 UE (102) 와의 초기 어태치 프로시저에 관계될 수도 있다. 서버 (112) 는 UE 로부터 초기 어태치 요청에 의해 제공된 PMSI 를 수신하고 PMSI 를 데이터베이스 (310) 에 저장된 PMSI 값들에 대해 체크할 수도 있다. UE (102) 로부터의 어태치 요청에 응답하여, 서버 (112) 는 다음 PMSI 를 생성하고 다음 PMSI 를 초기 어태치 요청에 대한 인증 요청 응답의 일부로서 UE (102) 에 송신할 수도 있다. UE (102) 로부터 다음 PMSI 를 확인응답하는 응답을 수신하는 것에 응답하여, PMSI 모듈 (308) 은 데이터베이스

(310) 에 저장된 PMSI 값들을 업데이트한다. 예를 들어, 현재 PMSI 값은 이전 PMSI 값이 되고 다음 PMSI 값은 UE (102) 로부터의 후속 어태치 요청과 같은 후속 반복을 위해 활용되는 현재 PMSI 값이 된다.

[0039] 논의의 목적들을 위해, 본 명세서에서는 4 개의 PMSI 값들이 참조된다: (1) 후속 PMSI 값들을 유도하기 위해 UE (102) 및 서버 (112) 가 이용하는 초기 합의된 PMSI 값인 초기 PMSI; (2) 현재 어태치 요청 프로시저에서 이용되는 PMSI 값인 현재 PMSI (예를 들어, UE (102) 가 초기 어태치 요청을 전송하는 처음에 현재 PMSI 는 초기 PMSI 와 동일할 수도 있는 한편, 다른 실시형태들에서, PMSI 는 초기 어태치 요청 동안에도 초기 PMSI 가 보다 안전하게 유지되도록 1 회 이상 반복될 수도 있다); (3) 현재 PMSI 에 선행하는 PMSI 인 사전 또는 이전 PMSI (예를 들어, 이전 어태치 요청에서 이용되는 PMSI 및/또는 현재 PMSI 에 도달하는데 이용되는 PMSI); 및 (4) 현재 PMSI 에 후속하는 PMSI 인 다음 PMSI (예를 들어, UE (102) 가 임의의 주어진 서빙 네트워크 (108) 와 개시하는 다음 어태치 프로시저를 위한 PMSI 가 무엇이어야 하는지에 대한 합의를 위해 UE (102) 와 서버 (112) 양자 모두에 의해 유도된 PMSI).

[0040] 데이터베이스 (310) 는 서버 (112), 예를 들어, 도 1 에 대하여 상기 언급된 HLR 에 의해 유지된 하나 이상의 데이터베이스들을 포함할 수도 있다. 데이터베이스 (310) 는 가입자 정보, 이를 테면 사용자 식별 및 어드레싱 (예를 들어, IMSI, PMSI (초기 PMSI, 현재 PMSI, 이전 PMSI, 및/또는 다음 PMSI 를 포함함) PMSI 추적 인덱스, 및 가입자들 모두의 또는 서브세트의 모바일 전화기 번호를 포함함), 프로파일 정보 (예를 들어, 서비스 가입 상태들), 뿐만 아니라 각각의 가입자와 연관된 보안 정보 (예를 들어, 보안 키들) 를 추적할 수도 있다.

[0041] 트랜시버 (312) 는, 서버 (112) 로 하여금, 외부 소스들, 이를 테면 홈 네트워크 (114) 또는 서빙 네트워크 (108) 내의 다른 네트워크 엘리먼트들로부터 데이터를 송신 및 수신하기 위해 통신하는 것을 가능하게 한다. 트랜시버 (312) 는 무선 및/또는 유선 통신들을 가능하게 할 수도 있다. 트랜시버 (312) 는 인지될 바와 같이, 예를 들어, 이더넷 접속, WiFi 접속, 또는 다른 타입들의 모뎀 및/또는 RF 서브시스템들을 포함할 수도 있다.

[0042] 도 4 는 본 개시의 소정의 양태들에 따른 MIMO 시스템 (400) 에서의 예시적인 송신기 시스템 (410) (예를 들어, 기지국 (104)) 및 수신기 시스템 (450) (예를 들어, UE (102)) 을 예시하는 블록 다이어그램이다. 송신기 시스템 (410) 에서, 다수의 데이터 스트림들에 대한 트래픽 데이터는 데이터 소스 (412) 로부터 송신 (TX) 데이터 프로세서 (414) 에 제공된다. 트래픽 데이터는 본 개시의 양태들에 따른 하나 이상의 MME 엔티티들로부터의 인증 요청들을 포함하여, 온갖 종류의 트래픽을 포함할 수도 있다.

[0043] 예를 들어, 다운링크 송신에서, 각각의 데이터 스트림은 개별의 송신 안테나를 통해 송신된다. TX 데이터 프로세서 (414) 는 코딩된 데이터를 제공하기 위해 그 데이터 스트림에 대해 선택된 특정한 코딩 스킴에 기초하여 각각의 데이터 스트림에 대한 트래픽 데이터를 포매팅, 코딩, 및 인터리빙한다.

[0044] 각각의 데이터 스트림에 대한 코딩된 데이터는 OFDM 기법들을 이용하여 파일럿 데이터와 멀티플렉싱될 수도 있다. 파일럿 데이터, 예를 들어, 파일럿 시퀀스는, 통상적으로 알려진 방식으로 프로세싱되는 알려진 데이터 패턴이고 채널 응답 또는 다른 채널 파라미터들을 추정하기 위해 수신기 시스템에서 이용될 수도 있다. 파일럿 데이터는 파일럿 심볼들로 포매팅될 수도 있다. OFDM 심볼 내의 파일럿 심볼들의 수 및 파일럿 심볼들의 배치는 프로세서 (430) 에 의해 수행된 명령들에 의해 결정될 수도 있다.

[0045] 각각의 데이터 스트림에 대한 멀티플렉싱된 파일럿 및 코딩된 데이터는 그 후 변조 심볼들을 제공하기 위해 그 데이터 스트림에 대해 선택된 특정한 변조 스킴 (예를 들어, BPSK, QSPK, M-PSK, 또는 M-QAM) 에 기초하여 변조된다 (즉, 심볼 맵핑된다). 각각의 데이터 스트림에 대한 데이터 레이트, 코딩, 및 변조는 프로세서 (430) 에 의해 수행된 명령들에 의해 결정될 수도 있다. 각각의 프레임에서의 파일럿 심볼들의 수 및 파일럿 심볼들의 배치는 또한, 예를 들어, 도 2 또는 도 3 에 대하여 상기 설명한 바와 같이, 프로세서 (430) 에 의해 수행된 명령들에 의해 결정될 수도 있다. 송신기 시스템 (410) 은 물론 예를 들어, 도 2 또는 도 3 에 대하여 상기 설명한 바와 같이, 메모리 (432) 를 더 포함한다.

[0046] 모든 데이터 스트림들에 대한 변조 심볼들은 그 후 (예를 들어, OFDM 을 위해) 변조 심볼들을 추가로 프로세싱할 수도 있는 TX MIMO 프로세서 (420) 에 제공된다. TX MIMO 프로세서 (420) 는 그 후 N_T 개의 변조 심볼 스트림들을 N_T 개의 송신기들 (TMTR) (422_a 내지 422_t) 에 제공한다. 일부 실시형태들에서, TX MIMO 프로세서 (420) 는 빔포밍 가중치들을 데이터 스트림들의 심볼들에 그리고 심볼이 송신되고 있는 안테나에 적용한다. 송신기 시스템 (410) 은 단 하나의 안테나를 갖거나 또는 다수의 안테나들을 갖는 실시형태들을 포함한다.

[0047] 각각의 송신기 (422) 는 하나 이상의 아날로그 신호들을 제공하기 위해 개별의 심볼 스트림을 수신 및 프로세싱하고, MIMO 채널을 통한 송신에 적합한 변조된 신호를 제공하기 위해 아날로그 신호들을 추가로 컨디셔닝 (예를 들어, 증폭, 필터링, 및 업컨버팅) 한다. 송신기들 (422_a 내지 422_t) 로부터의 N_T 개의 변조된 신호들은 그 후 각각 N_T 개의 안테나들 (424_a 내지 424_t) 로부터 송신된다. 본 명세서에서 설명된 기법들은 또한 단 하나의 송신 안테나를 가진 시스템들에 적용된다. 하나의 안테나를 이용한 송신은 멀티-안테나 시나리오보다 더 단순하다. 예를 들어, 단일의 안테나 시나리오에서는 TX MIMO 프로세서 (420) 에 대한 필요성이 없을 수도 있다.

[0048] 수신기 시스템 (450) 에서, 송신된 변조된 신호들은 N_R 개의 안테나들 (452_a 내지 452_r) 에 의해 수신되고, 각각의 안테나 (452) 로부터의 수신된 신호는 개별의 수신기 (RCVR) (454_a 내지 454_r) 에 제공된다. 각각의 수신기 (454) 는 개별의 수신된 신호를 컨디셔닝 (예를 들어, 필터링, 증폭, 및 다운컨버팅) 하고, 컨디셔닝된 신호를 디지털화하여 샘플들을 제공하고, 샘플들을 추가로 프로세싱하여 대응하는 "수신된" 심볼 스트림을 제공한다. 본 명세서에서 설명된 기법들은 또한 단 하나의 안테나 (452) 를 갖는 수신기 시스템 (450) 의 실시형태들에 적용된다.

[0049] RX 데이터 프로세서 (460) 는 그 후 N_T 개의 검출된 심볼 스트림들을 제공하기 위해 특정한 수신기 프로세싱 기법에 기초하여 수신기들 (454_a 내지 454_r) 로부터 N_R 개의 수신된 심볼 스트림들을 수신 및 프로세싱한다. RX 데이터 프로세서 (460) 는 그 후 데이터 스트림에 대한 트래픽 데이터를 복구하기 위해 각각의 검출된 심볼 스트림을 필요에 따라 복조, 디인터리빙, 및 디코딩한다. 복구된 트래픽은 예를 들어, 본 개시의 양태들에 따라 MME 로부터의 인증 정보 요청에서의 정보를 포함할 수도 있다. RX 데이터 프로세서 (460) 에 의한 프로세싱은 송신기 시스템 (410) 에서 TX MIMO 프로세서 (420) 및 TX 데이터 프로세서 (414) 에 의해 수행한 것과 상보적일 수 있다.

[0050] RX 데이터 프로세서 (460) 에 의해 제공된 정보는 프로세서 (470) 가 TX 데이터 프로세서 (438) 에 제공할 채널 상태 정보 (CSI) 및 다른 정보와 같은 레포트들을 생성하는 것을 허용한다. 프로세서 (470) 는 송신기 시스템에 송신할 CSI 및/또는 파일럿 요청을 포함하는 역방향 링크 메시지를 공식화 (formulating) 한다.

[0051] 프로세서 (470) 는 예를 들어 도 2 또는 도 3 에서 설명된 프로세서들에 대하여 상기 설명한 바와 같이 구현될 수도 있다. 역방향 링크 메시지들에 더하여, 수신기 시스템 (450) 은 어태치 요청들, 확인응답 토큰들, 및 통신 세션 뿐만 아니라 통신 세션 중의 데이터를 확립하기 위한 다른 정보를 포함하는 다른 다양한 타입들의 정보를 송신할 수도 있다. 메시지는 TX 데이터 프로세서 (438) 에 의해 프로세싱되고, TX MIMO 프로세서 (480) 에 의해 변조되고, 송신기들 (454_a 내지 454_r) 에 의해 컨디셔닝되고, 그리고 다시 송신기 시스템 (410) 에 송신될 수 있다. 도시한 바와 같이, TX 데이터 프로세서 (438) 는 데이터 소스 (436) 로부터 다수의 데이터 스트림들에 대한 트래픽 데이터를 또한 수신할 수도 있다.

[0052] 송신기 시스템 (410) 에서, 수신기 시스템 (450) 으로부터의 변조된 신호들은 안테나들 (424) 에 의해 수신되고, 수신기들 (422) 에 의해 컨디셔닝되고, 복조기 (440) 에 의해 복조되고, 그리고 RX 데이터 프로세서 (442) 에 의해 프로세싱되어 수신기 시스템 (450) 에 의해 송신된 역방향 링크 메시지를 추출한다. 그 결과, 데이터는 송신기 시스템 (410) 과 수신기 시스템 (450) 사이에서 전송 및 수신될 수도 있다. 송신기 시스템 (410) 은 또한, 인지될 바와 같이, 그것이 수신기 시스템 (450) 으로부터 수신하는 정보를 그의 서빙 네트워크 내의 다른 네트워크 엘리먼트들에 송신하고 그리고 서빙 네트워크에서의 하나 이상의 다른 네트워크 엘리먼트들로부터 정보를 수신하는데 이용될 수도 있다. 도 4 에 예시된 실시형태는 단지 예시적이고, 본 개시의 실시형태들은 도 4 에 예시되지 않은 다른 송신기/수신기 시스템들에 적용가능하다.

[0053] 도 5 는 본 개시의 다양한 양태들에 따라 무선 네트워크들에서 아이덴티티 프라이버시를 지원하기 위한 UE, 서빙 네트워크, 및 홈 네트워크 (및 서버) 사이의 일부 시그널링 양태들을 예시하는 프로토콜 다이어그램이다. 논의의 단순성을 위해, 도 5 의 프로토콜 다이어그램에서의 액션들을 설명하는데 있어서 도 1 에 도시된 엘리먼트들 (예를 들어, UE (102), eNB 같은 기지국 (104), MME (106), 및 HSS 같은 서버 (112)) 을 참조하게 될 것이다. 게다가 단순성을 위해, 논의는 어태치 프로시저의 모든 양태들 대신에 본 개시의 실시형태들의 양태들을 설명하는 프로토콜 플로우의 그 양태들에 초점을 맞출 것이다 (예를 들어, 논의는 다른 어태치 프로시저들, 또는 TS 23.401 5.3.2.1 에서 확인된 바와 같은 일부 오버랩을 가진 3GPP 표준에 더하여, 또는 그것과는 상이한 양태들에 초점을 맞출 것이다).

[0054] 액션 (502) 에서, UE (102) 는 UE (102) 에 저장된 현재 PMSI 에 액세스한다. UE (102) 가 서빙 네트워크 (108) 에 어태치하려고 시도하고 있는 것이 처음인 경우, 현재 PMSI 는 (예를 들어, PMSI 가 UE (102) 의 IMSI 와 동시에 프로비저닝되는 경우, 또는 PMSI 가 추후에 그러나 어태치 요청 전에 합의된 경우) 초기 PMSI 에 대응할 수도 있다. 사전 어태치 프로시저들이 일어났거나, 또는 서버 (112) 에서의 PMSI 충돌들에 의해 필요해진 실시형태들에서, UE (102) 에 저장된 현재 PMSI 는 사전 어태치 프로시저 동안 서버 (112) 와 UE 사이에 합의된 다음 PMSI 이다. UE (102) 는 초기 PMSI, 현재 PMSI, 이전 PMSI, 및/또는 다음 PMSI 를 포함하여, 하나 이상의 PMSI 값들을 저장할 수도 있다. 일부 인스턴스들에서, 현재 PMSI 는 사전 PMSI 값(들)과는 완전히 다른 값으로서 저장된다.

[0055] 일부 실시형태들에서, UE (102) 는 이전 PMSI 및 PMSI 추적 인덱스로부터 현재 PMSI 를 유도한다. 예를 들어, PMSI 추적 인덱스는 초기 PMSI 로 0 에서 초기화될 수도 있고, UE (102) 및 서버 (112) 가 어태치 프로시저를 성공적으로 완료할 때마다, PMSI 추적 인덱스는 UE (102) 와 서버 (112) 양자 모두에서 고정 값 (예를 들어, 1) 만큼 증분될 수도 있다. 따라서, UE (102) 및 서버 (112) 의 각각은 현재 이용중인 PMSI 의 임의의 반복에 도달하는데 이용될 수 있는 [초기 PMSI, PMSI 추적 인덱스] 를 저장할 수도 있다. 각각은 또한 [현재 PMSI, PMSI 추적 인덱스] 를 저장하고 (예를 들어, 인덱스 값들이 UE (102) 와 서버 (112) 사이에 매치하지 않는 경우) 초기 PMSI 를 대신 참조하게 될 필요가 있는지 여부를 결정하기 위해 PMSI 추적 인덱스에 의존할 수도 있다.

[0056] 액션 (504) 에서, UE (102) 는, 예를 들어, 후에 MME (106) 로 포워딩하는 기지국 (104) 에 초기 어태치 요청을 송신함으로써, 서빙 네트워크 (108) 로 초기 어태치 요청을 전송한다. 초기 어태치 요청은 IMSI 대신에 현재 PMSI (또는 서빙 네트워크 (108) 내의 하나 이상의 엘리먼트들이 UE (102) 의 IMSI 와 연관시키기 위해 이용할 수 있는 임의의 다른 값) 를 포함한다.

[0057] 액션 (504) 동안 MME (106) 가 초기 어태치 요청을 수신한 후에, 액션 (506) 에서, MME (106) 는 초기 어태치 요청에서의 정보를 취하고 서버 (112) 로 인증 정보 요청을 전송한다. 인증 정보 요청은 현재 PMSI 및 서빙 네트워크 (108) 가 UE (102) 에 의해 액세스되는 것과 관련 있는 시퀀스 번호를 포함할 수도 있다.

[0058] 액션 (508) 에서, 액션 (506) 동안 서버 (112) 가 인증 정보 요청을 수신한 후에, 서버 (112) 는 인증 정보 요청에 포함된 PMSI 를 체크하고 (다른 것들 중에서) 하나 이상의 데이터베이스들에 대해 PMSI 를 체크한다. 액션 (508) 의 일부로서, 서버 (112) 는 PMSI 를 (PMSI 가 암호화된 경우) 해독한다. 예를 들어, 서버 (112) 는 PMSI 를 암호화는데 활용된 공개 키와 연관된 개인 키를 이용하여 PMSI 를 해독할 수도 있다. 서버 (112) 는 예를 들어, 상기 도 3 에서 설명된 데이터베이스 (310) 에 저장된 값들과 PMSI 를 비교한다. 서버 (112) 가 PMSI 값들 사이에 매치를 발견하면, 서버 (112) 는 또한 UE (102) 로부터 수신된 현재 PMSI 에 대응하는 IMSI 에 대해 체크할 수도 있다.

[0059] PMSI 값들의 매치가 있는 경우, 액션 (508) 의 일부로서 서버 (112) (예를 들어, PMSI 모듈 (308)) 는 MME (106) 에 대한 인증 응답에의 포함을 위해 다음 PMSI 를 유도할 수 있다. 실시형태에서, 다음 PMSI 는 다음과 같이 유도된다. PMSI 추적 인덱스는 예를 들어, 고정량, 1 만큼 증분되고, 데이터베이스 (310) 에 저장된 (그리고 MME (106) 로부터의 인증 정보 요청에서 식별한 바와 같은) 현재 PMSI 값에 결합 (concatenating) 된다. 이 값은 K_{PMSI} 값과 함께, 다른 유도 함수로의 입력으로서 포함된다. K_{PMSI} 는 PMSI 생성 키이다.

예를 들어, K_{PMSI} 는 오리지널 키 (K) (예를 들어, EPS 마스터 키) 및 PMSI 유도 콘텍스트 CTX 를 입력들로서 갖는 키 유도 함수 (KDF) 를 이용함으로써 생성될 수도 있다 (예를 들어, K_{PMSI} = KDF(K, CTX)). CTX 는 콘텍스트, 예를 들어, "PMSI 생성" 과 같은 스트링일 수도 있다 - 키 생성에서 콘텍스트를 이용함으로써, 동일한 키 (K) 는 상이한 키 생성 결과들을 초래하기 위해 상이한 콘텍스트들을 통합하는 것에 의해서와 같이, 상이한 키들을 생성하는데 이용될 수도 있다.

[0060] K_{PMSI} 값 및 인덱스와 결합된 PMSI 는 함수에서 함께 해싱된다 (예를 들어, (결과 = HMAC(K_{PMSI}, PMSI | 인덱스), 여기서 | 는 결합 연산자이다)). 함수의 결과는 HMAC 함수의 출력 (키잉-해시 메시지 인증 코드) 이 고정 수의 디지트들 (예를 들어, 9 내지 10 디지트들) 에 제한되도록 절단될 수도 있다. 절단된 결과는 그 후 MNC (mobile network code) 및 MCC (mobile country code) 와 결합될 수도 있고 결과의 값은 다음 PMSI 가 된다. 이 값은, 절단의 결과로서, 실시형태에서 15 디지트들 길이일 수도 있지만, (더 긴 및 더 짧은 양자 모두의) 다른 길이들이 본 개시의 범위로부터 벗어남 없이 가능하다는 것이 인지될 것이다. 전체 동작은 실시형태에서 다음과 같이 설명될 수도 있다:

[0061] 다음 PMSI = MCC | MNC | Truncate(HMAC(K_{PMSI}, PMSI | 인덱스)). (식 1)

[0062] 대체로, 서버 (112) 는 PMSI 추적 인덱스와 함께 PMSI (예를 들어, 초기 및/또는 현재 PMSI) 를 저장할 수도 있다. PMSI 추적 인덱스는 서버 (112) 로 하여금, 초기 PMSI 를 x 횟수 반복적으로 해싱함으로써 초기 PMSI 로부터 현재 PMSI 를 컴퓨팅하는 것을 가능하게 하며, 여기서 x 는 PMSI 추적 인덱스 값과 동일하다. PMSI 추적 인덱스는 또한 어카운팅 뿐만 아니라 충돌 회피에 유용하다. 예를 들어, 서버 (112) 는 임의의 다른 UE 의 PMSI 와의 충돌들이 없다는 것을 입증하기 위해 다른 알려진 PMSI 값들에 대해 생성된 다음 PMSI 를 체크할 수도 있다. 충돌이 있는 경우, 서버 (112) 는 인덱스를 (예를 들어, 1 만큼) 증분시키고 새로운 PMSI-결합된-인덱스 값으로 식 (1) 을 반복할 수도 있다.

[0063] 액션 (510) 에서, 서버 (112) 는 생성된 정보를 취하고 그것을 MME (106) 로 전송될 인증 정보 응답에 통합한다. 다음 PMSI 는 인증 정보 응답에서의 추가된 보안을 위해, 예를 들어, MME (106) 가 UE (102) 와 서버 (112) 사이의 다음 PMSI 를 알아차릴 수 없도록 암호화될 수도 있다. 예를 들어, 다음 PMSI 는 K_{PMSI} 및 난수 (RAND) 로부터 유도되는 익명 키 (anonymity key) (예를 들어, 익명 키 = 함수(K_{PMSI}, RAND)) 로 암호화될 수도 있다.

[0064] 익명 키는 K_{PMSI} 및 난수 (RAND) 를 입력들로서 키 유도 함수에 배치함으로써 유도된다. 키 유도 함수는 3GPP 표준 (또는 장래의 등가의/유사한 표준), 예를 들어, f5* 에 부합하는 임의의 유도 함수일 수도 있다. 실시형태에서, 키 유도 함수는 HMAC 함수일 수도 있다. 따라서, 실시형태에서, 익명 키는 HMAC(K_{PMSI}, RAND) 에 의해 유도될 수도 있다. 대안의 실시형태에서, 익명 키는 초기 서빙 네트워크 (108) 인증이 가능해지는 키 암호화 키 (key encryption key; KEK) 일 수도 있다.

[0065] 액션 (510) 의 일부로서, 서버 (112) 는 MME (106) 로 인증 정보 응답을 전송할 수 있다. 인증 정보 응답은, 다른 것들 중에서, 인증 벡터 및 다음 PMSI/PMSI 추적 인덱스를 (유도가 상기 설명되는 익명 함수에 의해 암호화되는 바와 같이) 암호화된 형태로 포함할 수도 있다. 실시형태에서, 인증 벡터 그 자체는 인증 토큰, 예상 응답, 난수, 및 로컬 마스터 키 K_{ASME} 를 포함할 수도 있다. 따라서, 인증 벡터를 위해 전통적으로 포함될 수도 있는 것에 더하여, 본 개시의 실시형태들은 또한 UE (102) 와의 동기화를 위해 다음 PMSI 및 PMSI 추적 인덱스를 포함한다. MME (106) 는 인증 벡터를 저장할 수도 있지만, 일부 실시형태들에서, 암호화된 PMSI/PMSI 추적 인덱스를 저장하지 않는다.

[0066] 액션 (512) 에서, MME (106) 는 UE (102) 로 인증 요청을 전송함으로써 UE (102) 와의 상호 인증에 참여한다. 인증 요청은 액션 (510) 의 인증 정보 응답으로부터 획득된 정보를 취한다. 예를 들어, MME (106) 는 예상 응답을 인증의 일부로서 유지할 수도 있고 인증 토큰, 난수, eKSI (eUTRAN key set identifier), 뿐만 아니라 암호화된 다음 PMSI 및 PMSI 추적 인덱스를 전달한다.

[0067] 액션 (514) 에서, UE (102) 는 (MME (106) 와의 전통의 상호 인증 프로시저들에 더하여) 다음 PMSI 를 확인하고 서버 (112) 로의 리턴을 위해 확인응답 토큰을 생성한다. 이것과 관련하여, UE (102) 는 액션 (512) 에서 수신된 인증 요청으로부터 암호화된 다음 PMSI 및 PMSI 추적 인덱스 값들을 해독한다. UE (102) 는 UE (102) 가 서버 (112) (그러나 MME (106) 는 아님) 가 또한 갖는 공유된 비밀 키 (secret key) CTX (PMSI 유도 키) 를 갖기 때문에 다음 PMSI 및 PMSI 추적 인덱스 값들을 해독할 수 있다.

[0068] UE (102) 는 그들이 동기화되는 것을 확인하기 위해 서버 (112) 에 의해 생성된 다음 PMSI 에 대해 비교하기 위하여 저절로 다음 PMSI 를 유도한다. UE (102) 는 현재 PMSI 를 다음 PMSI 추적 인덱스와 해싱함으로써 다음 PMSI 를 유도할 수도 있다. 대안적으로, UE (102) 는 초기 PMSI 를 x 횟수 반복적으로 해싱함으로써 다음 PMSI 를 유도할 수도 있고, 여기서 x 는 PMSI 추적 인덱스 값과 동일하다 (UE (102) 로 로컬로 저장되는 바와 같거나 또는 서버 (112) 로부터 해독되는 것과 같음). UE (102) 는 그 후 로컬로 유도된 다음 PMSI 를 서버 (112) 로부터 수신된 다음 PMSI 와 비교한다. 값들이 매치하면, UE (102) 는 확인응답 토큰을 생성하는 것을 진행할 수도 있다.

[0069] 2 개의 다음 PMSI 값들이 매치하지 않으면 (예를 들어, UE (102) 가 그 자신의 버전의 PMSI 추적 인덱스를 이용한 경우), UE (102) 및 서버 (112) 는 동기화되지 않는다. 이것은, 예를 들어, UE (102) 로부터의 또는 UE (102) 로의 메시지가 수송중에 드롭된 상황들에서 일어날 수도 있다. 이 시나리오에서, UE (102) 는 서버 (112) 로부터 수신 및 해독된 PMSI 추적 인덱스에 대응하도록 그의 PMSI 추적 인덱스를 업데이트할 수도 있다. UE (102) 는 그 후 다음 PMSI 를 재-유도하고 다시 서버 (112) 로부터 수신 및 해독된 다음 PMSI 와 비교할

수도 있다.

[0070] 후속 어태치 프로시저를 위한 현재 PMSI 값으로서 이용될 다음 PMSI 가 확인되면, UE (102) 는 확인응답 토큰을 생성하는 것을 진행할 수도 있다. 확인응답 토큰은 암호화된 시퀀스 번호 (동기화를 위해 이용됨) 및 MAC-A 값을 결합함으로써 생성될 수도 있다. 암호화 양태는 UE (102) 와 서버 (112) 사이에 공유되는 시퀀스 번호를 암호화하는 것을 수반한다. 암호화는, 실시형태에서, 액션 (510) 에서 상기 설명된 익명 키 (예를 들어, 익명 키는 여기서 3GPP 표준 또는 다른 표준과 부합하는 상이한 함수를 이용하여 유도된다) 와는 상이한 다른 익명 키에 의해 수행될 수도 있다. 예를 들어, 시퀀스 번호를 암호화하는데 이용되는 익명 키 그 자체는, 입력들로서, 상기 설명된 K_{PMSI} 및 난수를 취하는 다양한 키 유도 함수들 중 임의의 것에 의해 생성될 수도 있다.

[0071] 암호화된 시퀀스 번호에 결합된 MAC-A 값은, 다른 익명 키 (예를 들어, 상기 설명된 다른 익명 키들 중 임의의 것과는 상이함), 난수와 결합된 시퀀스 번호 및 인증 관리 필드 (Authentication Management Field; AMF) 값을 입력들로서 취하는 메시지 인증 함수 (예를 들어, f1*) 로부터 생성된다. 메시지 인증 함수에서 입력으로서 이용되는 익명 키는 K_{PMSI} 및 난수를 입력들로서 취하는 다른 키 유도 함수에 의해 생성될 수도 있다. 이들 함수들 및 특정 입력들은 논의의 단순성을 위해 설명된다. 인지될 바와 같이, 다른 함수들 및 그 함수들에 대한 입력들이 본 개시의 범위로부터 벗어남 없이 이용될 수도 있다.

[0072] 액션 (516) 에서, UE (102) 는 액션 (514) 에서 생성된 확인응답 토큰을 PMSI 확인응답 메시지로서 다시 MME (106) 및 서버 (112) 로 전송한다. PMSI 확인응답 메시지는 액션 (514) 에 대하여 생성 및 상술된 인증 토큰, 뿐만 아니라 난수 (예를 들어, 상기 키 유도 함수(들)에서 이용되는 동일한 난수) 를 포함할 수도 있다. 실시형태에서, PMSI 확인응답 메시지는 여기에 상세히 설명되지 않은 UE (102) 로부터 MME (106) 로의 어태치 프로시저의 다른 양태들 (예를 들어, 암호로 쓰여진 옵션들 응답 메시지) 과 함께 피기백될 수도 있다. MME (106) 에서, PMSI 확인응답 메시지는 MME (106) 로부터 서버 (112) 로, 서버 (112) 로 전송된 다른 메시지 (예를 들어, 업데이트 로케이션 요청) 와 함께 피기백될 수도 있다.

[0073] 액션 (518) 에서, 확인응답 토큰의 수신 시에 서버 (112) 는 이전 PMSI 를 현재 PMSI 값으로 업데이트하고 현재 PMSI 를 (UE (102) 에 의해 확인되었고 따라서 동기화되는) 다음 PMSI 값으로 업데이트한다. 이것은 UE (102) 의 로케이션이 UE (102) 의 IMSI 를 노출시키지 않고 서버 (112) 에 의해 적절히 업데이트될 수도 있도록 확립된 세션 동안, 예를 들어, 다른 MME들로의 핸드오프 동안 어태치 프로시저에서 이용되는 PMSI 값이 서버 (112), 서빙 네트워크 (108), 및 UE (102) 사이에서 여전히 이용될 수도 있도록 유용하다. 어태치 프로시저는 그 후 전통적으로 수행되는 다른 양태들을 계속 포함할 수도 있지만, IMSI 의 임의의 이용은 본 개시에 따라 PMSI 의 이용으로 대체된다.

[0074] 예를 들어, 도 5 에 대하여 상기 설명한 바와 같이, UE (102) 의 성공적인 인증 후에, 서버 (112) 는 일부 관할권에서의 법률에 의해, 도 1 에 예시된 서빙 네트워크 (108) 와 같은 요청하는 서빙 네트워크에 UE (102) 에 대한 IMSI 를 노출시키도록 요구될 수도 있다. 본 개시의 양태들에 따르면, 서버 (112) 는 이들 환경들에서 악의적인 MME (106) 와 같은 하나 이상의 악의적인 네트워크 엘리먼트들의 가능성에 대해 보호하기 위해 IMSI 대신에 PMSI 를 여전히 공급할 수도 있다.

[0075] 이러한 요청은 다음과 같이 보이게 될 수도 있다 (도 5 에는 예시되지 않음). MME (106) 는 서버 (112) 로 UE (102) 의 IMSI 요청을 전송할 수도 있다. 본 개시의 실시형태들에 따르면, UE (102) 의 IMSI 는 어태치 프로시저 (또는 핸드오버) 동안 MME (106) 에 의해 수신되지 않고 오히려 PMSI 가 수신되었기 때문에, MME (106) 는 K_{IMSI} 암호화 키와 함께 UE (102) 와 연관된 수신된 PMSI 를 포함한다. K_{IMSI} 암호화 키는, 입력들로서 K_{ASNE} (Access Security Management Entity) 및 IMSI 취출 키를 갖는 HMAC 함수와 같은 함수로부터의 결과로서 생성될 수도 있다. K_{ASME} 는 MME (106) 와 서버 (112) 양자 모두에 알려진 MME (106) 베이스 키이다.

[0076] IMSI 요청에 응답하여, 서버 (112) 는 IMSI 응답을 제공한다. 실시형태에서, 서버 (112) 는 MME (106) 가 IMSI 에 도달하는 다른 능력 없이도 PMSI 를 전송한다. 이것은, 예를 들어, 서버 (112) 가 IMSI 요청의 대상인 UE (102) 에 대한 IMSI 와 PMSI 사이의 연관성을 여전히 유지하기 때문에 가능할 수도 있고, 따라서 모든 의도들을 위해 PMSI 는 서버 (112) 가 IMSI 를 이용하는 것과 동일한 정보를 PMSI 를 이용하여 액세스할 수 있을 것이기 때문에 요청된 검증 (validation) 을 제공한다. 다른 실시형태에서, 서버 (112) 는 PMSI 뿐만 아니라 IMSI 의 암호화된 버전으로 응답한다. 예를 들어, 서버 (112) 는 PMSI 와 IMSI 양자 모두를 취하고 그들을 K_{IMSI} 를 이용하여 암호화할 수도 있다. 그 결과, IMSI 는 K_{ASME} 를 정당하게 소유하는 MME (116) 에 의

해서만 정확하게 해독될 수도 있다.

[0077] 이제 도 6a 로 돌아가면, 플로우차트는 본 개시의 다양한 양태들에 따른 PMSI 를 이용하여 어태치 프로세스를 개시하는 UE 에 대한 예시적인 방법 (600) 을 예시한다. 방법 (600) 은 서빙 네트워크 (108) (예를 들어, 서빙 네트워크 (108) 의 단지 2 개의 네트워크 엘리먼트들만을 예시하기 위해 기지국 (104) 및 MME (106)) 와 통신하고 있는 UE (102) 에서 구현될 수도 있다. 방법 (600) 은 논의의 단순성을 위해 특정 UE (102) 에 대하여 설명될 것이지만, 본 명세서에서 설명된 양태들은 복수의 UE들 (102) 에 적용가능할 수도 있다는 것이 인지될 것이다. 추가적인 단계들이 방법 (600) 의 단계들 전에, 동안, 그리고 후에 제공될 수 있고, 설명된 단계들의 일부가 방법 (600) 의 다른 실시형태들을 위해 대체 또는 제거될 수 있는 것으로 이해된다.

[0078] 단계 (602) 에서, UE (102) 는 단계 (604) 에서의 초기 어태치 요청을 위해 이용될 현재 PMSI 에 액세스한다. 도 5 에 대하여 상기 논의한 바와 같이, 현재 PMSI 는 그것이 UE (102) 에 대한 첫번째 어태치 시도라면 UE (102) 에 (예를 들어, 메모리 (204) 내에) 에 저장된 초기 PMSI 일 수도 있다. 사전 어태치 프로시저들이 일어난 다른 실시형태들에서, 현재 PMSI 는 사전 어태치 프로시저 동안 서버 (112) 와 UE (102) 사이에서 확인된 다음 PMSI 이다.

[0079] 단계 (604) 에서, 일단 현재 PMSI 가 취출되면 UE (102) 는 현재 서빙 네트워크 (예를 들어, 도 1 에 예시한 바와 같은 108) 로 초기 어태치 요청을 전송한다. 초기 어태치 요청은 다른 정보 뿐만 아니라, IMSI 또는 UE (102) 의 IMSI 를 복원하는데 이용될 수 있는 다른 값 대신에 취출된 현재 PMSI 를 포함한다. 초기 어태치 요청은 MME (106) 로 요청을 포워딩하는 기지국 (104) 에 의해 수신될 수도 있다. MME (106) 가 초기 어태치 요청을 수신한 후에, MME (106) 는 초기 어태치 요청에서의 정보를 취하고 서버 (112) 로 IMSI 대신에 PMSI 를 사용하여 인증 정보 요청을 전송한다.

[0080] 단계 (606) 에서, UE (102) 는 (예를 들어, 도 5 의 액션 (512) 에서 상기 설명한 바와 같이) 서빙 네트워크 (108) 에서 (예를 들어, 기지국 (104) 을 통해) MME (106) 로부터 인증 요청을 수신한다. 인증 요청은, MME (106) 가 해독할 적절한 키를 갖지 않기 때문에 액세스할 수 없을 수도 있는, 서버 (112) 로부터의 암호화된 다음 PMSI 및 PMSI 추적 인덱스를 포함할 수 있다.

[0081] 단계 (608) 에서, UE (102) 는 MME (106) 로부터의 인증 요청의 일부로서 수신된 다음 PMSI 및 PMSI 추적 인덱스 값들을 해독한다. UE (102) 는, 도 5 의 액션들 (508 및 514) 에 대하여 상기 설명한 바와 같이, 서버 (112) 가 값들을 암호화하는데 이용된 익명 키를 생성하는데 있어서 이용한 공유된 비밀 키를 UE (102) 가 갖기 때문에 다음 PMSI 및 PMSI 추적 인덱스 값들을 해독할 수 있다.

[0082] 단계 (610) 에서, UE (102) 는 저절로 (즉, 단계 (608) 에서 수신된 다음 PMSI 및 PMSI 추적 인덱스에 의존하지 않고) 다음 PMSI 값을 유도한다. 실시형태에서, UE (102) 는 UE (102) 에 (예를 들어, 메모리 (204) 내에) 저장된 이전 PMSI 값 및 PMSI 추적 인덱스 값에 기초하여 다음 PMSI 값을 유도한다. 다른 실시형태에서, UE (102) 는 UE (102) 로 저장된 초기 PMSI 값 및 PMSI 추적 인덱스의 현재 값에 기초하여 (예를 들어, PMSI 값을 PMSI 추적 인덱스의 현재 값과 동일한 횟수 해싱하여) 다음 PMSI 값을 유도한다.

[0083] 단계 (612) 에서, UE (102) (예를 들어, PMSI 모듈 (208) 과 협력한 프로세서 (202)) 는 로컬로 유도된 다음 PMSI 값을 수신된 및 해독된 다음 PMSI 값과 비교한다.

[0084] 판정 단계 (614) 에서, 로컬로 유도된 다음 PMSI 값과 수신된 및 해독된 다음 PMSI 값이 매치하지 않으면, 방법 (600) 은, UE (102) 가 그의 로컬 버전의 PMSI 추적 인덱스를 서버 (112) 로부터의 수신된 및 해독된 PMSI 추적 인덱스의 값과 동일하게 업데이트하는 단계 (616) 로 진행한다. 방법 (600) 은 그 후, 단계 (616) 로부터, 다시, 프로세스가 상기 설명한 바와 같이 계속되는 단계 (610) 로 진행한다.

[0085] 판정 단계 (614) 로 리턴하여, 로컬로 유도된 다음 PMSI 값과 수신된 및 해독된 다음 PMSI 값이 매치하면, 방법 (600) 은 단계 (618) 로 진행한다.

[0086] 단계 (618) 에서, UE (102) (예를 들어, PMSI 모듈 (208) 과 협력한 프로세서 (202)) 는, 예를 들어, 도 5 의 액션 (514) 에 대하여 상기 설명한 바와 같이, 서버 (112) 로 전송될 확인응답 토큰을 생성한다.

[0087] 단계 (620) 에서, UE (102) 는 예를 들어, 서빙 네트워크 (108) 의 하나 이상의 네트워크 엘리먼트들을 통해, 생성된 확인응답 토큰을 서버 (112) 로 전송한다. UE (102) 는 또한, 그의 로컬 PMSI 값들을, 예를 들어, 현재 PMSI 값을 반영하기 위한 이전 PMSI (현재 어태치 프로시저에서 이용되는 PMSI) 및 동기화된 다음 PMSI 값을 반영하기 위한 현재 PMSI 를 업데이트함으로써 업데이트한다. UE (102) 및 서빙 네트워크 (108) 는 인지

될 바와 같이 통신 세션을 확립하는 것을 계속할 수도 있다.

[0088] 도 6b 는 본 개시의 다양한 양태들에 따른 PMSI 를 이용하는 어태치 프로세스에서의 서버에 대한 예시적인 방법 (630) 을 예시하는 플로우차트이다. 방법 (630) 은 서빙 네트워크 (108) (예를 들어, 서빙 네트워크 (108) 의 단지 하나의 네트워크 엘리먼트 예를 예시하기 위해 MME (106)) 와 통신하고 있는 서버 (112) 에서 구현될 수도 있다. 방법 (630) 은 논의의 단순성을 위해 서버 (112) 에 대하여 설명될 것이지만, 본 명세서에서 설명된 양태들은 복수의 서버들 (112) 에 적용가능할 수도 있다는 것이 인지될 것이다. 추가적인 단계들은 방법 (630) 의 단계들 전에, 동안, 및 후에 제공될 수 있고, 설명된 단계들의 일부는 방법 (630) 의 다른 실시형태들을 위해 대체 또는 제거될 수 있는 것으로 이해된다.

[0089] 단계 (632) 에서, 서버 (112) 는 그의 IMSI 대신에 UE (102) 에 의해 MME (106) 에 제공된 현재 PMSI 를 포함하는 인증 정보 요청을 서빙 네트워크 (108), 예를 들어, MME (106) 로부터 수신한다. 액션 (506) 에 대하여 상기 설명한 바와 같이, MME (106) 는 MME (106) 가 UE (102) 로부터 수신한 초기 어태치 요청에 기초하여 인증 정보 요청을 전송한다.

[0090] 단계 (634) 에서, 서버 (112) (예를 들어, PMSI 모듈 (308) 및 데이터베이스 (310) 와 협력한 프로세서 (302)) 는 예를 들어, 도 5 의 액션 (508) 에 대하여 상기 설명한 바와 같이, 수신된 PMSI 에 대응하는 특정 UE (102) 를 식별하기 위해 서버 (112) 에 이미 유지된 (또는 다른 경우에 서버 (112) 에 의해 액세스가능한) PMSI 값들에 대해 수신된 PMSI 를 체크한다.

[0091] 단계 (636) 에서, 매치를 발견한 후에 서버 (112) 는 데이터베이스 (310) 에 로케이팅된 (또는 다른 경우에 서버 (112) 에 의해 액세스가능한) 수신된 PMSI 와 연관된 PMSI 추적 인덱스를 증분시킨다. PMSI 추적 인덱스는 서버 (112) 에 의해 유지되고 UE 의 PMSI 레코드와 연관된 상태로 유지된다. PMSI 추적 인덱스는, 상기 설명한 바와 같이, 서버 (112) 로 하여금, UE (102) 와 서버 (112) 사이에 합의된 초기 PMSI 에 기초하여 UE (102) 의 PMSI 의 임의의 반복을 컴퓨팅하는 것을 가능하게 한다. PMSI 값의 임의의 반복에 도달하는 이 능력은 또한 서버 (112) 로 하여금, 다양한 어카운팅 및 차징 목적들을 달성하는 것을 가능하게 한다. 서버 (112) 는 또한, 충돌들이 서버 (112) 에 의해 유도된 가능한 다음 PMSI 값과 다른 UE (102) 에 대한 서버 (112) 에 이미 유지된 다른 PMSI 값 사이에 일어나는 상황들을 어드레싱하기 위해 PMSI 추적 인덱스를 이용한다. 실시형태에서, PMSI 추적 인덱스는 일 예로 1 의 값만큼 증분될 수도 있다.

[0092] 단계 (638) 에서, 서버 (112) (예를 들어, PMSI 모듈 (308) 과 협력한 프로세스 (302)) 는 다음 PMSI 를 유도한다. 서버 (112) 는, 예를 들어 도 5 의 액션 (508) 에 대하여 상기 설명한 바와 같이, 단계 (632) 에서의 인증 정보 요청에서 수신된 현재 PMSI 뿐만 아니라 단계 (636) 로부터의 증분된 PMSI 추적 인덱스에 기초하여 다음 PMSI 를 유도할 수도 있다. 유사하게, 서버는 초기 PMSI 및 PMSI 추적 인덱스 값에 기초하여 다음 PMSI 를 유도할 수도 있다.

[0093] 판정 단계 (640) 에서, 서버 (112) 는 임의의 다른 UE 의 PMSI 와의 충돌이 없다는 것을 입증하기 위해 다른 알려진 PMSI 값들에 대해 단계 (638) 에서 유도된 다음 PMSI 를 체크한다. 충돌이 있다면, 방법 (630) 은, 다시 PMSI 추적 인덱스가 증분되는 단계 (636) 로 다시 진행하고, 그 후 다음 PMSI 가 단계 (638) 에서 새로운 PMSI 추적 인덱스 값으로 유도된다.

[0094] 판정 단계 (640) 로 리턴하여, 충돌들이 없다면, 방법 (630) 은 단계 (642) 로 진행한다. 단계 (642) 에서, 서버 (112) 는 예를 들어, 도 5 의 액션 (508) 에 대하여 상기 설명한 바와 같이, 다음 PMSI 및 증분된 PMSI 추적 값들을 암호화한다. 도 5 에서 논의한 바와 같이, 암호화된 다음 PMSI 및 PMSI 추적 인덱스 값들은 인증 벡터와 함께 인증 정보 응답에 포함될 수도 있다.

[0095] 단계 (644) 에서, 서버 (112) 는 MME (106) 에 암호화된 다음 PMSI 및 PMSI 추적 인덱스 값들을 포함하는 인증 정보 응답을 송신한다. MME (106) 는 그 후 UE (102) 와의 상호 인증에 참여할 수 있다. 그 상호 인증의 일부로서, MME (106) 는 MME (106) 에서 정보를 해독하지 않고 암호화된 다음 PMSI 및 PMSI 추적 인덱스 값들을 송신할 수 있다.

[0096] 예를 들어, 도 6a 의 단계들 (608 내지 616) 중 하나 이상에 따라, UE (102) 가 다음 PMSI 값을 확인한 후에, 방법 (600) 은 단계 (646) 로 진행한다. 단계 (646) 에서, 일단 UE (102) 가 다음 PMSI 값을 확인했거나 또는 다르게는 (예를 들어, 새로운 제안된 다음 PMSI 값을 전송하거나, 새로운 다음 PMSI 값을 요청하거나, 또는 수신된 및 해독된 PMSI 추적 인덱스의 값을 반영하기 위해 그의 로컬 PMSI 추적 인덱스를 조정함으로써) 동기화를 완료했다면, 서버 (112) 는 MME (106) 를 통해 UE (102) 로부터 인증 토큰을 수신한다. 응답으로,

서버 (112) 는 그 후 그의 PMSI 정보를 업데이트한다 (예를 들어, 서버 (112) 는 현재 PMSI 값을 반영하기 위한 이전 PMSI (현재 어태치 프로시저에서 이용되는 PMSI) 및 동기화된 다음 PMSI 값을 반영하기 위한 현재 PMSI 를 업데이트한다). UE (102) 및 서빙 네트워크 (108) 는 인지될 바와 같이 통신 세션을 확립하는 것을 계속할 수도 있다.

[0097] 이제 도 7a 로 돌아가면, 플로우차트는 본 개시의 다양한 양태들에 따른 UE 에 대한 PMSI 초기화를 위한 예시적인 방법 (700) 을 예시한다. 방법 (700) 은 기지국 (104) 및 MME (106) 와 통신하고 있는 UE (102) 에서 구현될 수도 있다. 방법 (700) 은 논의의 단순성을 위해 단일의 UE (102) 에 대하여 설명될 것이지만, 본 명세서에서 설명된 양태들은 복수의 UE들 (102) 에 적용가능할 수도 있다는 것이 인지될 것이다. 추가적인 단계들이 방법 (700) 의 단계들 전에, 동안, 및 후에 제공될 수 있고, 설명된 단계들의 일부가 방법 (700) 의 다른 실시형태들을 위해 대체 또는 제거될 수 있는 것으로 이해된다.

[0098] 단계 (702) 에서, UE (102) 는 초기화 프로세스를 시작한다. 이것은 (예를 들어, 본 개시의 양태들에 따라 UE (102) 의 SIM 카드를 IMSI 및 PMSI 값들로 프로그래밍하는) UE (102) 의 프로비저닝 시에 또는 추후에 일어날 수도 있다.

[0099] 판정 단계 (704) 에서, UE (102) 는 그것이 프로비저닝 시에 초기화된 PMSI 를 이미 갖는지 여부를 결정한다. 이것은, 예를 들어, 프로세서 (202), 메모리 (204), 및 PMSI 모듈 (208) 간에 협력하여 행해질 수도 있다. PMSI 가 이미 초기화되었다면, 방법 (700) 은, 초기 PMSI 가 저장되고 PMSI 초기화 방법 (700) 이 종료하는 단계 (716) 로 진행한다. PMSI 가 아직 초기화되지 않았다면, 방법 (700) 은 단계 (706) 로 진행한다.

[0100] 단계 (706) 에서, 프로세서 (202) 및 PMSI 모듈 (208) 은 함께 협력하여 제안된 초기 PMSI 를 생성한다. 제안된 초기 PMSI 는 임의의 다양한 팩터들에 기초할 수도 있다. 실시형태에서, 제안된 초기 PMSI 는 UE (102) 의 IMSI 에 기초, 예를 들어, 난수 또는 의사-난수와 결합된 하나 이상의 해싱 함수들 및/또는 반복들에 기초할 수도 있다. 다른 실시형태에서, PMSI 는 UE (102) 의 IMSI 에 기초하지 않고 오히려 몇 가지만 예로 들면, 난수 또는 의사-난수에 기초하여, 어떤 도청자들도 PMSI 로부터 IMSI 를 유도할 수 없을 것이다.

[0101] 단계 (708) 에서, 프로세서 (202) 및 PMSI 모듈 (208) 은 함께 협력하여 단계 (706) 에서 생성된 제안된 초기 PMSI 를 암호화한다. 실시형태에서, PMSI 는 서버 (112) 가 이전에 언젠가 UE (102) 와 공유한 공개 키를 이용하여 암호화된다. 서버 (112) 는 수신 시에 PMSI 를 해독하기 위한 대응하는 개인 키를 갖는다.

[0102] 단계 (710) 에서, UE (102) 는, 트랜시버 (210) 를 통해, 암호화된 PMSI 를 서버 (112) 에, 예를 들어, 기지국 (104) 및/또는 MME (106) 를 경유하여 송신한다.

[0103] 단계 (712) 에서, UE (102) 는 (트랜시버 (210) 를 통해) 제안된 초기 PMSI 의 수신을 확인응답하는 응답을 서버 (112) 로부터 수신한다.

[0104] 판정 단계 (714) 에서, 프로세서 (202) 및 PMSI 모듈 (208) 은 함께 협력하여 서버 (112) 가 제안된 초기 PMSI 를 수락했다는 것을 서버 (112) 로부터 수신된 응답이 표시하는지 여부를 결정한다. 응답이 서버 (112) 가 제안된 초기 PMSI 를 수락했다는 것을 표시한다면, 방법 (700) 은, 초기 PMSI 가 저장되고 방법 (700) 이 종료하는 단계 (716) 로 진행한다. 응답이 서버 (112) 가 제안된 초기 PMSI 를 수락하지 않았다는 것을 표시하면, 방법 (700) 은 방금 거절된 것과는 상이한 새로운 제안된 초기 PMSI 를 생성하기 위해 단계 (706) 로 리턴한다. 제안된 초기 PMSI 는, 예를 들어, PMSI 와, 예를 들어, 서버 (112) 의 데이터베이스 (310) 에 이미 저장된 다른 연관된 UE 의 임의의 다른 PMSI 사이에 충돌이 있는 경우에 거절될 수도 있다.

[0105] 방법 (700) 은 UE (102) 와 서버 (112) 양자 모두에 합의가능한 PMSI 가 도달될 때까지 반복할 수도 있다. 대안의 실시형태에서, 판정 단계 (714) 에서, 서버 (112) 가 제안된 초기 PMSI 를 수락하지 않았다고 UE (102) 가 결정하면, UE (102) 는 또한, 서버 (112) 가 UE (102) 에 대한 그 자신의 제안된 초기 PMSI 를 전송했는지 여부를 식별하기 위해 서버 (112) 로부터의 응답 (단계 (712) 에서와 동일한 또는 상이한 응답) 을 검토할 수도 있다. 이 실시형태에서, UE (102) 는 UE (102) 에 수락가능한지 또는 아닌지를 결정하기 위해 서버 (112) 로부터 제안된 초기 PMSI 를 체크할 수도 있다. 어떤 이슈들도 없다면, UE (102) 는 서버 (112) 로부터 제안된 초기 PMSI 를 수락하고 서버 (112) 에 수락을 통지할 수도 있다. 일단 초기 PMSI 가 합의되면, 초기 PMSI 는 후속 이용을 위해 UE (102) 에 저장되고 방법 (700) 은 단계 (716) 에서 종료한다.

[0106] 도 7b 는 본 개시의 다양한 양태들에 따른 서버에 대한 PMSI 를 이용하는 어태치 프로세스를 위한 예시적인 방법 (720) 을 예시하는 플로우차트이다. 방법 (720) 은 논의의 단순성을 위해 단일의 서버 (112) 및 단일의 UE (102) 에 대하여 설명될 것이지만, 본 명세서에서 설명된 양태들은 임의의 수의 서버들 (112) 및/또는 UE들

(102) 에 적용가능할 수도 있다는 것이 인지될 것이다. 추가적인 단계들은 방법 (720) 의 단계들 전에, 동안, 및 후에 제공될 수 있고, 설명된 단계들의 일부는 방법 (720) 의 다른 실시형태들을 위해 대체 또는 제거될 수 있는 것으로 이해된다.

[0107] 단계 (722) 에서, 서버 (112) 는 예를 들어, 트랜시버 (312) 를 통해 UE (102) 로부터 암호화된, 제안된 초기 PMSI 를 수신한다.

[0108] 단계 (724) 에서, 서버 (112) 는 예를 들어, 프로세서 (302), 메모리 (304), 및 PMSI 모듈 (308) 에 의해 협력하여 수신된 PMSI 를 해독한다. 실시형태에서, 수신된 PMSI 는 서버 (112) 에서 또는 서버 (112) 에 대해 유지된 개인 키에 대응하는 공개 키로 UE (102) 에서 암호화되었다.

[0109] 단계 (726) 에서, 서버 (112) 는 데이터베이스 (310) 에 (또는 서버 (112) 에서의 임의의 다른 데이터베이스 내에 또는 복수의 UE들에 대한 정보를 유지하고 서버 (112) 에 의해 액세스가능한 다른 곳에) 다른 UE들에 대해 이미 존재하는 다른 PMSI 값들과 수신된, 해독된 PMSI 를 비교한다.

[0110] 단계 (728) 에서, 서버 (112) 는 수신된, 제안된 초기 PMSI 와, 서버 (112) 에 저장되거나 또는 다르게는 서버 (112) 에 의해 액세스가능한 임의의 다른 PMSI 값들 사이에 어떤 충돌들이 있는지를 결정한다.

[0111] 판정 단계 (730) 에서, 서버 (112) 는 단계 (728) 에서의 결정에 기초하여, 제안된 초기 PMSI 를 수락하는지 안하는지를 판정한다. 서버 (112) 가 제안된 초기 PMSI 를 수락하면, 방법 (720) 은, 서버 (112) 가 UE (102) 로 초기 PMSI 의 수락의 확인응답을 전송하는 단계 (734) 로 진행하고, 초기 PMSI 를, (예를 들어, 서버 (112) 가 UE (102) 에 대해 유지하는 레코드의 일부로서) 그것이 UE (102) 와 연관되도록 서버 (112) 에서 데이터베이스 (310) 내에 저장한다.

[0112] 판정 단계 (730) 에서, 서버 (112) 가 제안된 초기 PMSI 를 수락하지 않는다고 결정하면, 방법 (720) 은, 서버 (112) 가 그 서버 (112) 가 UE (102) 에 송신하는 UE (102) 로부터의 새로운 PMSI 를 요청하고 응답을 대기하는 단계 (732) 로 진행한다. 대안의 실시형태에서, 서버 (112) 는 그 대신 저절로 제안된 초기 PMSI 를 (판정 단계 (730) 에 응답하여) 생성하고 그것을 부정하면서 UE (102) 에 송신할 수도 있다.

[0113] 정보 및 신호들은 다양한 상이한 기술들 및 기법들 중 임의의 것을 이용하여 표현될 수도 있다. 예를 들어, 상기 설명 전반에 걸쳐 참조될 수도 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심볼들, 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 입자들, 광학장들 또는 입자들, 또는 그 임의의 조합으로 표현될 수도 있다.

[0114] 본 명세서의 개시와 관련하여 설명된 다양한 예시적인 블록들 및 모듈들은 범용 프로세서, DSP, ASIC, FPGA 또는 다른 프로그래밍가능 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본 명세서에서 설명된 기능들을 수행하도록 설계된 그 임의의 조합으로 구현 또는 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안으로, 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수도 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합 (예를 들어, DSP 와 마이크로프로세서의 조합, 다수의 마이크로프로세서들, DSP 코어와 결합된 하나 이상의 마이크로프로세서들, 또는 임의의 다른 이러한 구성) 으로서 구현될 수도 있다.

[0115] 본 명세서에서 설명된 기능들은 하드웨어, 프로세서에 의해 실행된 소프트웨어, 펌웨어, 또는 그 임의의 조합에서 구현될 수도 있다. 프로세서에 의해 실행된 소프트웨어에서 구현되면, 기능들은 컴퓨터 판독가능 매체 상에 하나 이상의 명령들 또는 코드로서 저장 또는 이를 통해 송신될 수도 있다. 다른 예들 및 구현들은 본 개시 및 첨부된 청구항들의 범위 내에 있다. 예를 들어, 소프트웨어의 본성으로 인해, 상기 설명된 기능들은 프로세서에 의해 실행된 소프트웨어, 하드웨어, 펌웨어, 하드와이어링, 또는 이들 중 임의의 것의 조합들을 이용하여 구현될 수 있다. 기능들을 구현하는 피처들은 또한, 기능들의 부분들이 상이한 물리적 로케이션들에서 구현되도록 분포되는 것을 포함하여, 다양한 포지션들에 물리적으로 로케이팅될 수도 있다. 또한, 청구항들을 포함하여 본 명세서에서 사용한 바와 같이, 아이템들의 리스트 (예를 들어, "중 적어도 하나" 또는 "중 하나 이상" 과 같은 어구가 앞에 오는 아이템들의 리스트) 에서 사용한 바와 같은 "또는" 은, 예를 들어, [A, B, 또는 C 중 적어도 하나] 의 리스트가 A 또는 B 또는 C 또는 AB 또는 AC 또는 BC 또는 ABC (즉, A 및 B 및 C) 를 의미하도록 포괄적 리스트를 표시한다.

[0116] 본 개시의 실시형태들은, 서빙 네트워크로 초기 어태치 메시지를 사용하여 UE 를 식별하기 위한 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 국제 모바일 가입자 아이덴티티 (IMSI) 대신에 전송하기 위한 수단; 서빙 네트워크로부터, 서빙 네트워크와 통신하는 서버에 의해 결정된 다음 PMSI 를 포함하는 인증 요청을 수신하기 위

한 수단으로서, 다음 PMSI 는 PMSI 로부터 유도되는, 상기 인증 요청을 수신하기 위한 수단; 및 서빙 네트워크를 통해 서버로 다음 PMSI 의 수신의 확인응답을 전송하기 위한 수단을 포함하는 사용자 장비 (UE) 를 포함한다.

[0117] UE 는 이전 PMSI 로부터 PMSI 를 유도하기 위한 수단을 더 포함하고, 이전 PMSI 는 초기 PMSI 를 포함한다. UE 는 이전 PMSI 로부터 PMSI 를 유도하기 위한 수단을 더 포함하고, 이전 PMSI 는 초기 PMSI 로부터 유도된 PMSI 값을 포함한다. UE 는, UE 에 의해, 초기 PMSI 에 기초하여 네트워크 액세스를 위한 PMSI 를 결정하기 위한 수단을 더 포함한다. UE 는 서버에의 UE 의 가입자 등록 동안 초기 PMSI 를 수신하기 위한 수단을 더 포함한다. UE 는 서버와의 공중 경유 통신을 통한 가입자 등록 후에 초기 PMSI 를 프로비저닝하기 위한 수단을 더 포함한다. UE 는 제안된 PMSI 를 생성하기 위한 수단; 서버 공개 키를 이용하여 생성된 PMSI 를 암호화하기 위한 수단으로서, 서버는 대응하는 서버 개인 키를 유지하는, 상기 PMSI 를 암호화하기 위한 수단; 및 초기 PMSI 로서 생성된 PMSI 를 이용하기 위해 서버로부터 확인응답을 수신하기 위한 수단을 더 포함한다. UE 는 UE-기반 다음 PMSI 를 결정하기 위한 수단; 및 매치가 있는지를 결정하기 위해 인증 요청의 일부로서 수신된 다음 PMSI 와 UE-기반 다음 PMSI 를 비교하기 위한 수단을 더 포함한다. UE 는 매치가 있다고 결정하는 것에 응답하여 확인응답 토큰을 생성하기 위한 수단으로서, 수신의 확인응답은 확인응답 토큰을 포함하는, 상기 확인응답 토큰을 생성하기 위한 수단; 및 다음 어태치 메시지에서의 이용을 위해 UE 에 확인된 다음 PMSI 를 저장하기 위한 수단을 더 포함한다. UE 는 익명 키를 이용하여 인증 요청에서의 다음 PMSI 를 해독하기 위한 수단을 더 포함하며, 익명 키는 UE 와 서버 사이에 공유된 비밀 키로부터 유도된다.

[0118] 본 개시의 실시형태들은, 개재하는 서빙 네트워크에서의 하나 이상의 네트워크 엘리먼트들을 통해 사용자 장비 (UE) 로부터, 초기 어태치 메시지로부터 UE 를 식별하기 위한 프라이버시 모바일 가입자 아이덴티티 (PMSI) 를 국제 모바일 가입자 아이덴티티 (IMSI) 대신에 수신하기 위한 수단; 서버에 의해, PMSI 에 기초하여 다음 PMSI 를 결정하기 위한 수단; 서버로부터, 인증의 일부로서 서빙 네트워크에 의해 UE 에 중계되는 다음 PMSI 를 포함하는 인증 정보를 서빙 네트워크에 송신하기 위한 수단; 및 서빙 네트워크를 통해 UE 로부터, 다음 PMSI 의 확인을 포함하는 수신의 확인응답을 수신하기 위한 수단을 포함하는 서버를 더 포함한다.

[0119] 서버는 이전 PMSI 로부터 다음 PMSI 를 유도하기 위한 수단을 더 포함하고, 이전 PMSI 는 초기 PMSI 를 포함한다. 서버는 이전 PMSI 로부터 다음 PMSI 를 유도하기 위한 수단을 더 포함하고, 이전 PMSI 는 초기 PMSI 로부터 유도된 PMSI 값을 포함한다. 서버는, 서버에 의해, 초기 PMSI 에 기초하여 네트워크 액세스를 위한 PMSI 를 결정하기 위한 수단을 더 포함한다. 서버는, 서버에서, 서버에의 UE 의 가입자 등록 동안 초기 PMSI 를 수신하기 위한 수단을 더 포함한다. 서버는, UE 로부터, 제안된 초기 PMSI 를 수신하기 위한 수단; 서버에 의해, 대응하는 서버 공개 키에 의해 UE 에서 암호화된 제안된 초기 PMSI 를 서버 개인 키를 이용하여 해독하기 위한 수단; 및 UE 에, 초기 PMSI 로서 제안된 초기 PMSI 의 확인응답을 송신하기 위한 수단을 더 포함한다. 서버는, 서버와 UE 사이에 공유된 비밀 키로부터 익명 키를 유도하기 위한 수단; 유도된 익명 키를 이용하여 인증 정보에서의 다음 PMSI 를 암호화하기 위한 수단; 확인응답의 일부로서, 다음 PMSI 를 확인응답하는 확인응답 토큰을 수신하기 위한 수단; 및 UE 로부터의 후속 초기 어태치 메시지에 응답하는데 이용하기 위해 서버에 PMSI 대신에 다음 PMSI 를 저장하기 위한 수단을 더 포함한다. 서버는 다음 PMSI 와 상이한 UE 와 연관된 다른 기존 PMSI 사이의 충돌을 검출하기 위한 수단; 및 PMSI 인덱스를 증분시키고 그리고 다음 PMSI 및 증분된 PMSI 인덱스에 기초하여 새로운 다음 PMSI 를 결정하기 위한 수단을 더 포함한다. 서버는, 서버가 위에 있는 홈 네트워크와는 별개인 서빙 네트워크 상의 이동성 관리 엔티티 (MME) 로부터, UE 의 IMSI 에 대한 요청을 수신하기 위한 수단; 및 요청에 응답하여, UE 의 IMSI 대신에 초기 어태치 메시지에서 이용되는 UE 의 PMSI 를 전송하기 위한 수단을 더 포함한다. 서버는, 초기 어태치 메시지에 포함된 PMSI 에 대한 매치를 위해 하나 이상의 데이터베이스들을 탐색하기 위한 수단; 및 매치를 로케이팅하지 않는 것에 응답하여, UE 에서의 업데이트된 PMSI 의 생성을 위해 UE 에 유지된 PMSI 인덱스를 변경하기 위한 UE 에 대한 통지를 전송하기 위한 수단을 더 포함한다.

[0120] 본 개시의 실시형태들은, 사용자 장비 (UE) 에 의한 네트워크 액세스를 위한 방법을 더 포함하고, 그 방법은, UE 에 의해, 서빙 네트워크에 어태치하기로 결정하는 단계; 및 UE 로부터, 서빙 네트워크로 UE 에 대한 영구 식별자 (ID) 대신에 임시 ID 를 포함하는 초기 어태치 메시지를 전송하는 단계로서, 서빙 네트워크의 인증 서버 (HSS) 에 의한 보안 콘텍스트는 임시 ID 에 기초하여 확립되는, 상기 초기 어태치 메시지를 전송하는 단계를 포함한다.

[0121] 방법은, 서빙 네트워크의 HSS 로부터, HSS 에 의해 결정된 다음 임시 ID 를 포함하는 인증 요청을 수신하는 단계를 더 포함하고, 다음 임시 ID 는 초기 어태치 메시지에 포함된 임시 ID 로부터 유도된다. 방법은, UE 로

부터, 서빙 네트워크를 통해 HSS 로 다음 임시 ID 의 수신의 확인응답을 전송하는 단계를 더 포함한다.

[0122] 본 개시의 실시형태들은, 임시 식별자 (ID) 를 저장하도록 구성된 메모리; 서빙 네트워크에 어태치하기로 결정하도록 구성된 프로세서; 및 서빙 네트워크로 UE 에 대한 영구 ID 대신에 임시 ID 를 포함하는 초기 어태치 메시지를 전송하도록 구성된 트랜시버로서, 서빙 네트워크의 인증 서버 (HSS) 에 의한 보안 콘텍스트는 임시 ID 에 기초하여 확립되는, 상기 트랜시버를 더 포함한다.

[0123] UE 는, 트랜시버가 서빙 네트워크의 HSS 로부터, HSS 에 의해 결정된 다음 임시 ID 를 포함하는 인증 요청을 수신하는 것으로서, 다음 임시 ID 는 초기 어태치 메시지에 포함된 임시 ID 로부터 유도되는, 상기 인증 요청을 수신하도록 추가로 구성되는 것을 더 포함한다. UE 는, 프로세서가 수신의 확인응답을 생성하도록 추가로 구성되고, 트랜시버가 서빙 네트워크를 통해 HSS 로 수신의 확인응답을 전송하도록 추가로 구성되는 것을 더 포함한다.

[0124] 본 개시의 실시형태들은, 네트워크 상의 서버로 네트워크 액세스를 셋업하기 위한 방법을 더 포함하고, 그 방법은, 서빙 네트워크를 통해 사용자 장비 (UE) 로부터, UE 에 대한 영구 식별자 (ID) 대신에 임시 ID 를 포함하는 초기 어태치 메시지를 수신하는 단계; 및 임시 ID 에 기초하여 보안 콘텍스트를 확립하는 단계를 포함한다.

[0125] 방법은 초기 어태치 메시지에 포함된 임시 ID 에 기초하여 다음 임시 ID 를 결정하는 단계를 더 포함한다. 방법은, 서버로부터, 인증의 일부로서 서빙 네트워크를 통해 UE 에 다음 임시 ID 를 포함하는 인증 정보를 송신하는 단계를 더 포함한다. 방법은, 서빙 네트워크를 통해 UE 로부터, 다음 임시 ID 의 확인을 포함하는 수신의 확인응답을 수신하는 단계를 더 포함한다.

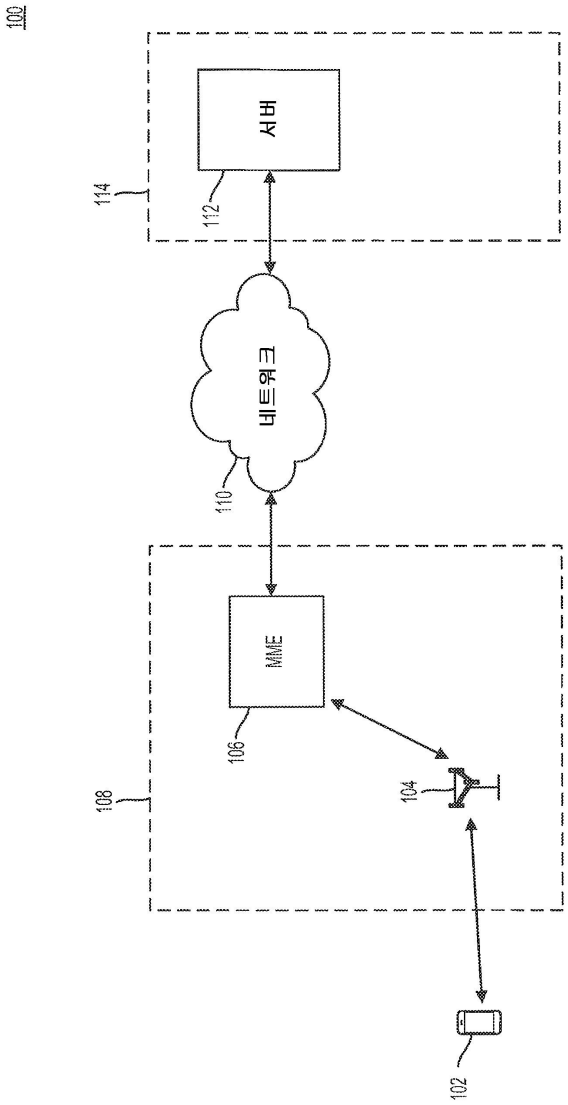
[0126] 본 개시의 실시형태들은, 서빙 네트워크를 통해 사용자 장비 (UE) 로부터, UE 에 대한 영구 식별자 (ID) 대신에 임시 ID 를 포함하는 초기 어태치 메시지를 수신하도록 구성된 트랜시버; 및 임시 ID 에 기초하여 보안 콘텍스트를 확립하도록 구성된 프로세서를 포함하는 서버를 더 포함한다.

[0127] 서버는, 프로세서가 초기 어태치 메시지에 포함된 임시 ID 에 기초하여 다음 임시 ID 를 결정하도록 추가로 구성되는 것을 더 포함한다. 서버는, 트랜시버가 인증의 일부로서 서빙 네트워크를 통해 UE 에 다음 임시 ID 를 포함하는 인증 정보를 송신하도록 추가로 구성되는 것을 더 포함한다. 서버는, 서빙 네트워크를 통해 UE 로부터, 다음 임시 ID 의 확인을 포함하는 수신의 확인응답을 수신하도록 추가로 구성되는 것을 더 포함한다.

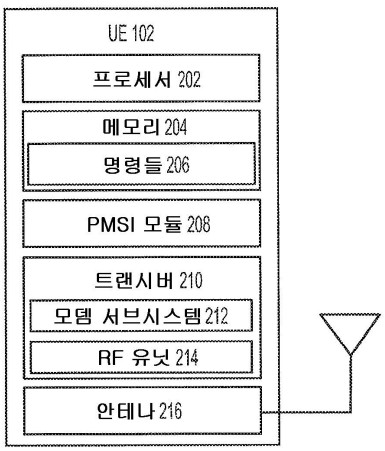
[0128] 당업자들이 이미 인식할 바와 같이 및 장래에 특정한 애플리케이션에 의존하여, 많은 변경들, 치환들 및 변동들이 본 개시의 사상 및 범위로부터 벗어남 없이 본 개시의 디바이스들의 이용의 방법들, 재료들, 장치, 및 구성들에서 그리고 이들에 대해 이루어질 수 있다. 이것을 고려하여, 본 개시의 범위는 그들이 단지 그의 일부 예들을 예로 들 뿐이기 때문에 본 명세서에서 예시 및 설명된 특정한 실시형태들의 범위에 제한되어서는 안되고, 오히려, 이후에 첨부된 청구항들 및 그들의 기능적 등가물들의 것과 완전히 상응해야 한다.

도면

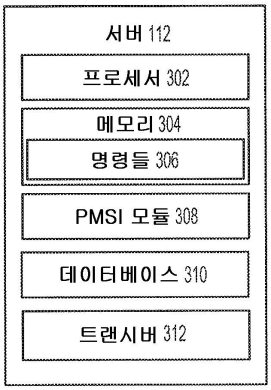
도면1


100
서버
112
114
네트워크
110
MME
106
104
108
102

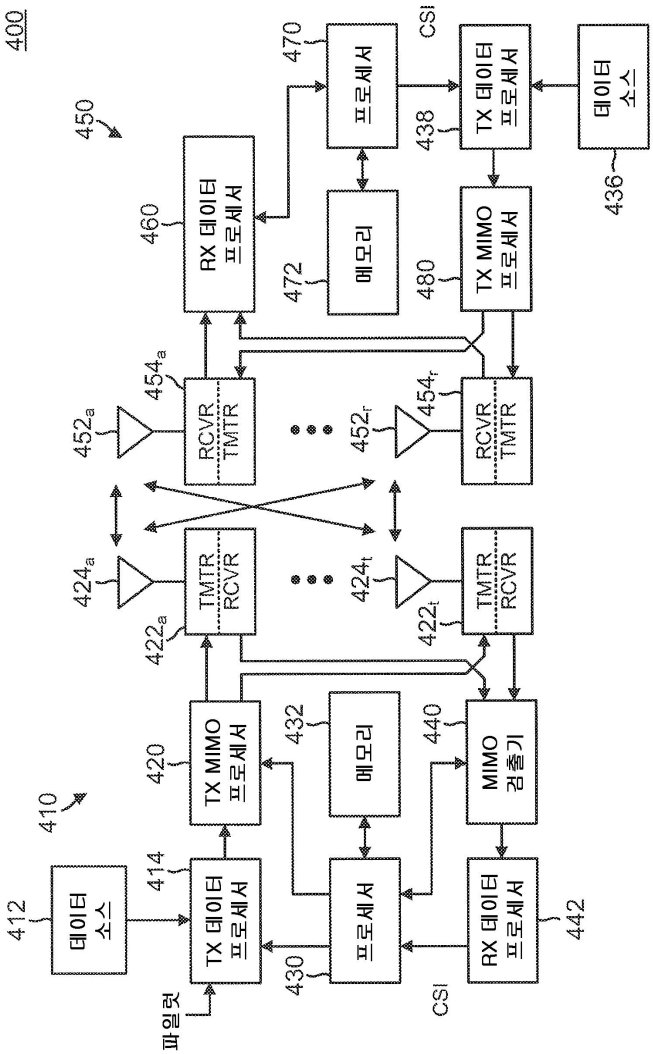
도면2


UE 102
프로세서 202
메모리 204
명령들 206
PMSI 모듈 208
트랜시버 210
모뎀 서브시스템 212
RF 유닛 214
안테나 216

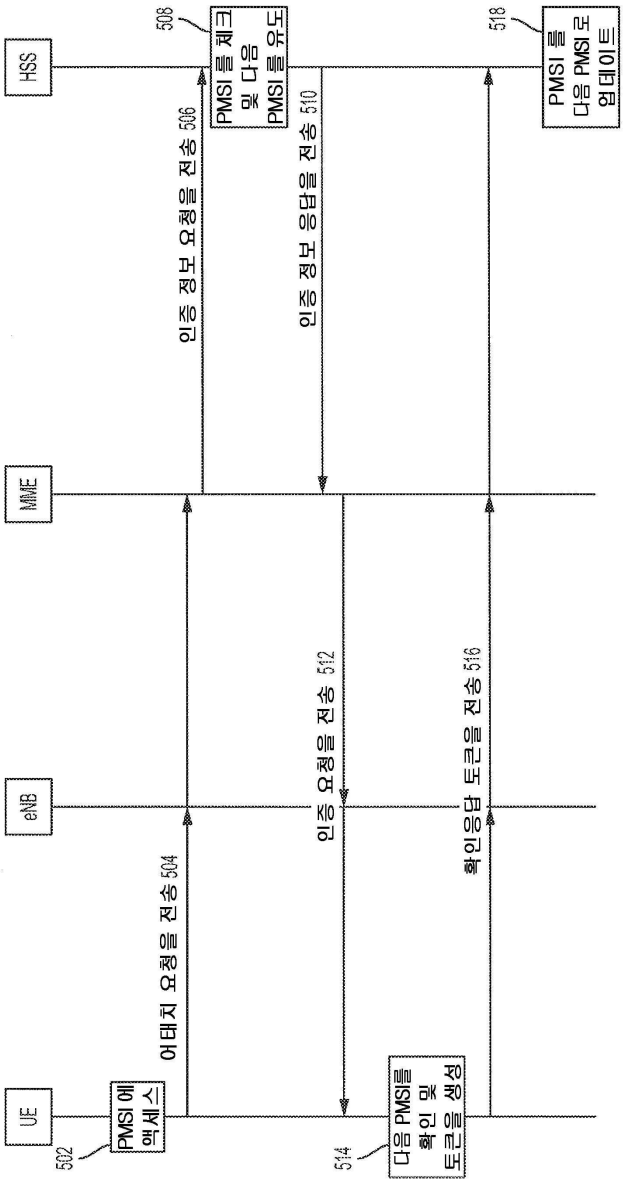
도면3


서버 112
프로세서 302
메모리 304
명령들 306
PMSI 모듈 308
데이터베이스 310
트랜시버 312

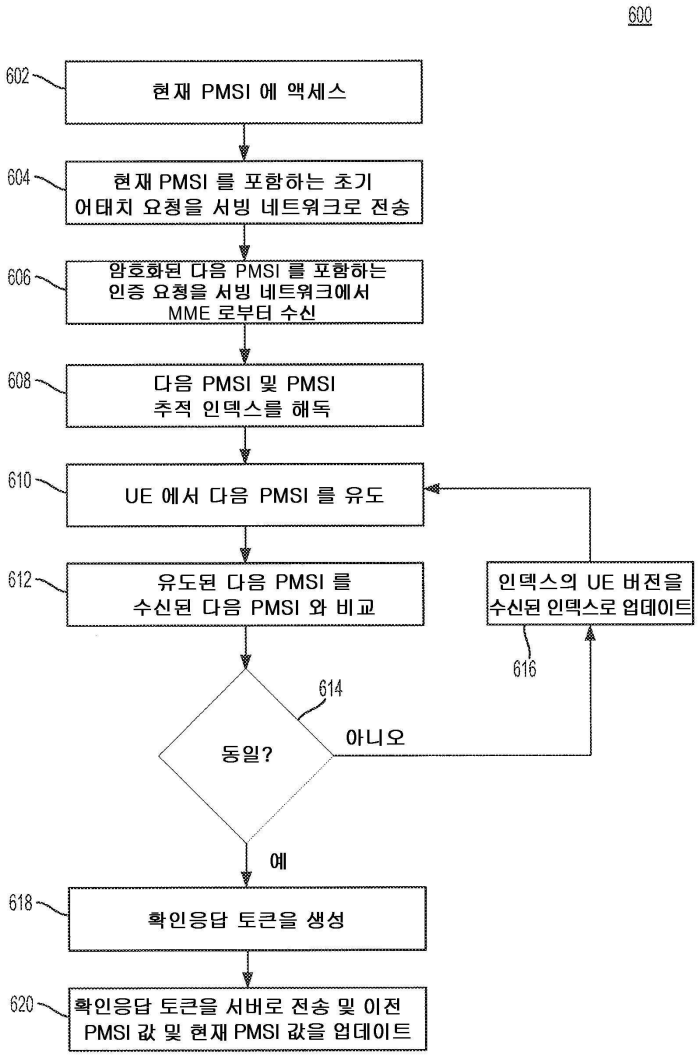
도면4


400
450
460
RX 데이터 프로세서
470
프로세서
CSI
438
TX 데이터 프로세서
데이터 소스
436
472
메모리
480
TX MIMO 프로세서
454a
452a
RCVR TMTR
452f
454f
424a
TMTR RCVR
424t
422a
422t
410
420
TX MIMO 프로세서
432
메모리
440
MIMO 검출기
412
데이터 소스
414
TX 데이터 프로세서
430
프로세서
442
RX 데이터 프로세서
파일럿
CSI

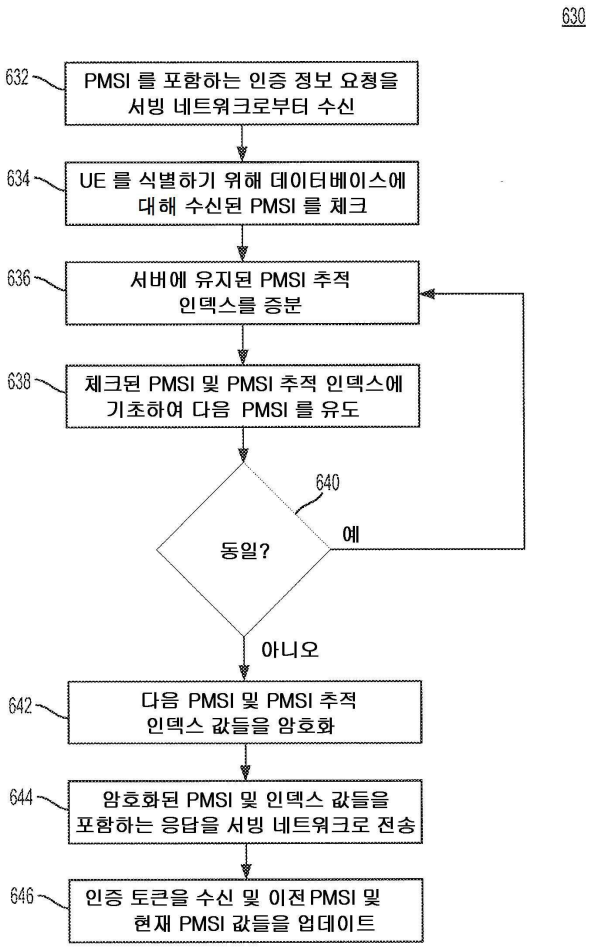
도면5


UE
eNB
MME
HSS
PMSI 에 액세스
502
어태치 요청을 전송 504
인증 정보 요청을 전송 506
PMSI 를 체크 및 다음 PMSI 를 유도
508
인증 정보 응답을 전송 510
인증 요청을 전송 512
다음 PMSI를 확인 및 토큰을 생성
514
확인응답 토큰을 전송 516
PMSI 를 다음 PMSI 로 업데이트
518

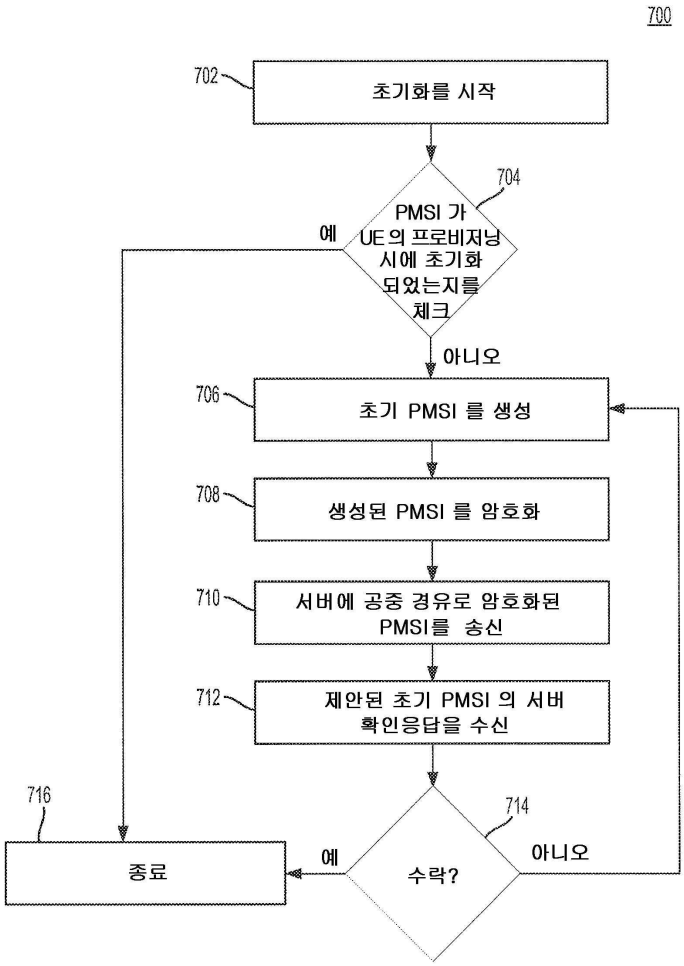
도면6a


600
602
현재 PMSI 에 액세스
604
현재 PMSI 를 포함하는 초기 어태치 요청을 서빙 네트워크로 전송
606
암호화된 다음 PMSI 를 포함하는 인증 요청을 서빙 네트워크에서 MME 로부터 수신
608
다음 PMSI 및 PMSI 추적 인덱스를 해독
610
UE 에서 다음 PMSI 를 유도
612
유도된 다음 PMSI 를 수신된 다음 PMSI 와 비교
614
동일?
아니오
예
616
인덱스의 UE 버전을 수신된 인덱스로 업데이트
618
확인응답 토큰을 생성
620
확인응답 토큰을 서버로 전송 및 이전 PMSI 값 및 현재 PMSI 값을 업데이트

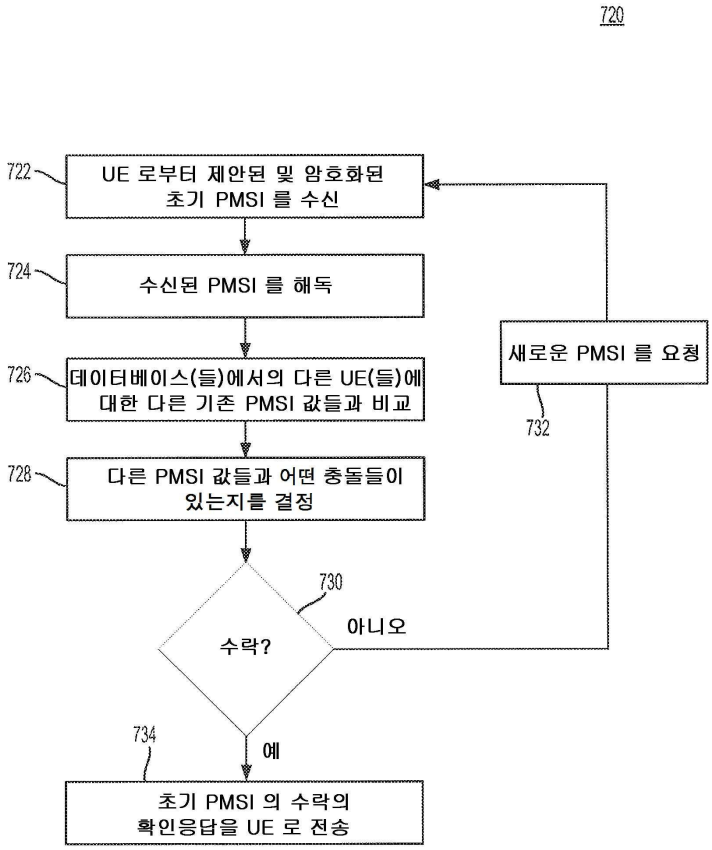
도면6b


630
632
PMSI 를 포함하는 인증 정보 요청을 서빙 네트워크로부터 수신
634
UE 를 식별하기 위해 데이터베이스에 대해 수신된 PMSI 를 체크
636
서버에 유지된 PMSI 추적 인덱스를 증분
638
체크된 PMSI 및 PMSI 추적 인덱스에 기초하여 다음 PMSI 를 유도
640
동일?
예
아니오
642
다음 PMSI 및 PMSI 추적 인덱스 값들을 암호화
644
암호화된 PMSI 및 인덱스 값들을 포함하는 응답을 서빙 네트워크로 전송
646
인증 토큰을 수신 및 이전 PMSI 및 현재 PMSI 값들을 업데이트

도면7a


700
702
초기화를 시작
704
PMSI 가 UE의 프로비저닝 시에 초기화 되었는지를 체크
예
아니오
706
초기 PMSI 를 생성
708
생성된 PMSI 를 암호화
710
서버에 공중 경유로 암호화된 PMSI를 송신
712
제안된 초기 PMSI 의 서버 확인응답을 수신
714
수락?
예
아니오
716
종료

도면7b


720
722
UE 로부터 제안된 및 암호화된 초기 PMSI 를 수신
724
수신된 PMSI 를 해독
726
데이터베이스(들)에서의 다른 UE(들)에 대한 다른 기존 PMSI 값들과 비교
728
다른 PMSI 값들과 어떤 충돌들이 있는지를 결정
730
수락?
아니오
732
새로운 PMSI 를 요청
734
예
초기 PMSI 의 수락의 확인응답을 UE 로 전송