(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년07월13일
(11) 등록번호 10-1159441
(24) 등록일자 2012년06월18일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) *H04W 12/10* (2009.01)
(21) 출원번호 10-2010-7011417
(22) 출원일자(국제) 2008년10월22일
심사청구일자 2010년05월27일
(85) 번역문제출일자 2010년05월25일
(65) 공개번호 10-2010-0085135
(43) 공개일자 2010년07월28일
(86) 국제출원번호 PCT/US2008/080694
(87) 국제공개번호 WO 2009/055414
국제공개일자 2009년04월30일
(30) 우선권주장
60/982,698 2007년10월25일 미국(US)
(56) 선행기술조사문헌
EP01248487 A2*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인터디지탈 패튼 홀딩스, 인크
미국 델라웨어 19810 윌밍턴 실버사이드 로드 3411 콩코드 플라자 스위트 105 해글리 빌딩
(72) 발명자
소마선다람 산카르
영국 런던 엔더블유1 6에이피 클라렌스 게이트 가든스 플랫 150
무커지 라자트 피.
미국 캘리포니아주 94133-2094 샌 프란시스코 스톡톤 스트리트 넘버 디-304 2133
(74) 대리인
신정건, 김태홍

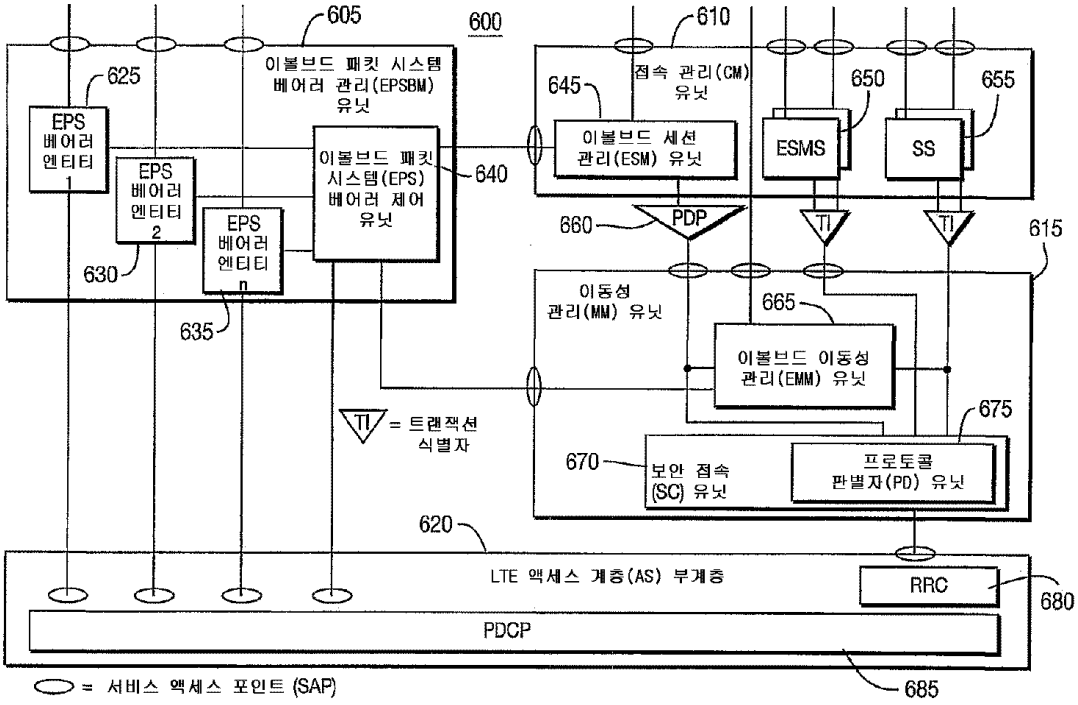
전체 청구항 수 : 총 15 항 심사관 : 이선택

(54) 발명의 명칭 **ＬＴＥ 모바일 유닛에서의 비접속 계층(ＮＡＳ) 보안을 가능하게 하는 방법 및 장치**

(57) 요 약

본 방법 및 장치는 LTE WTRU들에서의 NAS 계층(계층 3)의 처리를 수행하며, 이는 NAS 프로토콜 계층이 계층 3 메시지를 정확한 NAS 엔티티에 라우팅하고 새로운 NAS 메시지 유형 및 정보 요소를 인코딩하는 것을 허용받는다. NAS 보안을 가능하게 하는 새로운 아키텍처가 제공된다. NAS 메시지가 발생할 때, NAS 메시지의 프로토콜 판별자(PD), NAS 메시지의 헤더에서의 표시자 필드, NAS 메시지의 유형, NAS 보안 상태 변수, 및 RRC 프로토콜에 의한 표시 중 적어도 하나에 기초하여 NAS 메시지를 암호화, 암호해독 및/또는 무결성 검사할지 여부에 대한 판정이 행해진다. NAS 보안 상태 변수는 NAS 보안이 현재 활성 상태인지 여부를 표시하며, 1 비트를 포함할 수 있다.

대 표 도


605
600
610
625
645
650
655
이볼브드 패킷 시스템 베어러 관리(EPSBM) 유닛
접속 관리(CM) 유닛
EPS 베어러 엔티티 1
EPS 베어러 엔티티 2
EPS 베어러 엔티티 n
이볼브드 패킷 시스템(EPS) 베어러 제어 유닛
640
이볼브드 세션 관리(ESM) 유닛
ESMS
SS
660
PDP
TI
615
630
635
이동성 관리(MM) 유닛
665
이볼브드 이동성 관리(EMM) 유닛
675
TI = 트랜잭션 식별자
670
보안 접속(SC) 유닛
프로토콜 판별자(PD) 유닛
620
LTE 액세스 계층(AS) 부계층
RRC
680
PDCP
685
= 서비스 액세스 포인트 (SAP)

특허청구의 범위

청구항 1

비접속 계층(NAS; non-access stratum) 메시지를 처리하는 방법에 있어서,

NAS 메시지를 발생시키고,

NAS 보안 상태 변수에 기초하여 상기 NAS 메시지를 암호화할지 여부를 결정하는 것

을 포함하고,

상기 NAS 보안 상태 변수는, 상기 NAS 보안 상태 변수가 제1 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 현재 활성 상태임을 표시하고, 상기 NAS 보안 상태 변수가 제2 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 활성 상태가 아님을 표시하는 것인 NAS 메시지 처리 방법.

청구항 2

제1항에 있어서, 상기 NAS 보안 상태 변수는 1 비트를 포함하는 것인 NAS 메시지 처리 방법.

청구항 3

제1항에 있어서, 상기 NAS 보안 상태 변수는, 암호화가 시작했음을 표시하는데 이용되는 NAS 프로토콜 데이터 유닛(PDU; protocol data unit)을 포함하는 것인 NAS 메시지 처리 방법.

청구항 4

비접속 계층(NAS; non-access stratum) 메시지를 처리하는 방법에 있어서,

NAS 메시지를 발생시키고,

NAS 보안 상태 변수에 기초하여 상기 NAS 메시지에 대한 무결성 검사를 수행할지 여부를 결정하는 것

을 포함하고,

상기 NAS 보안 상태 변수는, 상기 NAS 보안 상태 변수가 제1 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 현재 활성 상태임을 표시하고, 상기 NAS 보안 상태 변수가 제2 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 활성 상태가 아님을 표시하는 것인 NAS 메시지 처리 방법.

청구항 5

제4항에 있어서, 상기 NAS 보안 상태 변수는 1 비트를 포함하는 것인 NAS 메시지 처리 방법.

청구항 6

무선 송수신 유닛(WTRU; wireless transmit/receive unit)에 있어서,

비접속 계층(NAS; non-access stratum) 메시지를 발생시키도록 구성된 이볼브드 세션 관리(ESM; evolved session management) 유닛과,

NAS 보안 상태 변수에 기초하여 상기 NAS 메시지를 암호화할지 여부를 결정하도록 구성된 보안 접속(SC; secure connectivity) 유닛

을 포함하고,

상기 NAS 보안 상태 변수는, 상기 NAS 보안 상태 변수가 제1 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 현재 활성 상태임을 표시하고, 상기 NAS 보안 상태 변수가 제2 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 활성 상태가 아님을 표시하는 것인 무선 송수신 유닛.

청구항 7

제6항에 있어서, 상기 NAS 보안 상태 변수는 1 비트를 포함하는 것인 무선 송수신 유닛.

청구항 8

제6항에 있어서, 상기 NAS 보안 상태 변수는, 암호화가 시작했음을 표시하는데 이용되는 NAS 프로토콜 데이터 유닛(PDU; protocol data unit)을 포함하는 것인 무선 송수신 유닛.

청구항 9

제6항에 있어서, 상기 SC 유닛은 프로토콜 판별자(PD; protocol discriminator) 유닛을 포함하는 것인 무선 송수신 유닛.

청구항 10

무선 송수신 유닛(WTRU; wireless transmit/receive unit)에 있어서,

비접속 계층(NAS; non-access stratum) 메시지를 발생시키도록 구성된 이볼브드 세션 관리(ESM; evolved session management) 유닛과,

NAS 보안 상태 변수에 기초하여 상기 NAS 메시지를 암호해독할지 여부를 결정하도록 구성된 보안 접속(SC; secure connectivity) 유닛

을 포함하고,

상기 NAS 보안 상태 변수는, 상기 NAS 보안 상태 변수가 제1 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 현재 활성 상태임을 표시하고, 상기 NAS 보안 상태 변수가 제2 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 활성 상태가 아님을 표시하는 것인 무선 송수신 유닛.

청구항 11

제10항에 있어서, 상기 NAS 보안 상태 변수는 1 비트를 포함하는 것인 무선 송수신 유닛.

청구항 12

제10항에 있어서, 상기 SC 유닛은 프로토콜 판별자(PD; protocol discriminator) 유닛을 포함하는 것인 무선 송수신 유닛.

청구항 13

무선 송수신 유닛(WTRU; wireless transmit/receive unit)에 있어서,

비접속 계층(NAS; non-access stratum) 메시지를 발생시키도록 구성된 이볼브드 세션 관리(ESM; evolved session management) 유닛과,

NAS 보안 상태 변수에 기초하여 상기 NAS 메시지에 대한 무결성 검사를 수행할지 여부를 결정하도록 구성된 보안 접속(SC; secure connectivity) 유닛

을 포함하고,

상기 NAS 보안 상태 변수는, 상기 NAS 보안 상태 변수가 제1 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 현재 활성 상태임을 표시하고, 상기 NAS 보안 상태 변수가 제2 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 활성 상태가 아님을 표시하는 것인 무선 송수신 유닛.

청구항 14

무선 송수신 유닛(WTRU; wireless transmit/receive unit)에 있어서,

비접속 계층(NAS; non-access stratum) 메시지를 발생시키도록 구성된 이볼브드 이동성 관리(EMM; evolved mobility management) 유닛과,

NAS 보안 상태 변수에 기초하여 상기 NAS 메시지를 암호화할지 여부를 결정하도록 구성된 보안 접속(SC; secure connectivity) 유닛

을 포함하고,

상기 NAS 보안 상태 변수는, 상기 NAS 보안 상태 변수가 제1 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대

해 현재 활성 상태임을 표시하고, 상기 NAS 보안 상태 변수가 제2 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 활성 상태가 아님을 표시하는 것인 무선 송수신 유닛.

청구항 15

무선 송수신 유닛(WTRU; wireless transmit/receive unit)에 있어서,

비접속 계층(NAS; non-access stratum) 메시지를 발생시키도록 구성된 이볼브드 이동성 관리(EMM; evolved mobility management) 유닛과,

NAS 보안 상태 변수에 기초하여 상기 NAS 메시지에 대한 무결성 검사를 수행할지 여부를 결정하도록 구성된 보안 접속(SC; secure connectivity) 유닛

을 포함하고,

상기 NAS 보안 상태 변수는, 상기 NAS 보안 상태 변수가 제1 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 현재 활성 상태임을 표시하고, 상기 NAS 보안 상태 변수가 제2 값을 가질 때 NAS 보안이 상기 NAS 메시지에 대해 활성 상태가 아님을 표시하는 것인 무선 송수신 유닛.

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

명 세 서

기 술 분 야

[0001] 본 출원은 무선 통신에 관한 것이다.

배 경 기 술

[0002] 3세대 파트너쉽 프로젝트(3GPP; third generation partnership project) 롱텀 이볼루션(LTE; long term evolution) 프로그램에 대한 현재의 노력은 개선된 스펙트럼 효율, 감소된 레이턴시, 보다 나은 무선 자원 이용도를 제공하여 보다 적은 비용으로 보다 빠른 사용자 경험과 보다 풍부한 애플리케이션 및 서비스를 가져오기 위해 LTE 설정 및 구성에 대한 새로운 기술, 새로운 아키텍처 및 새로운 방법을 가져오는 것이다.

[0003] LTE 계층 3(L3) 아키텍처는 일반 패킷 무선 서비스(GPRS; general packet radio service)가 가능한 WTRU(wireless transmit/receive unit)(즉, 이동국)를 위한 기존의 L3 아키텍처에 대한 이볼루션으로서 고려될 수 있다. LTE는 새로운 이동성 관리(MM; mobility management) 개념(예를 들어, 라우팅 영역을 대체한 추적 영역의 개념) 및 새로운 MM 절차(예를 들어, 추적 영역 업데이트 절차에 복수의 추적 영역이 할당될 수 있음)를 정의한다. 이들 새로운 절차는 LTE 비접속 계층(NAS; non-access stratum)의 일부분인 새로운 L3 프로토콜(예를 들어, 이볼브드 이동성 관리(EMM; evolved mobility management) 및 이볼브드 세션 관리(ESM; evolved session management))에 의해 보다 자세하게 기술될 것이다. 이들 새로운 프로토콜 엔티티는 GPRS 이

동성 관리(GPRS mobility management; GMM), 세션 관리(SM; session management) 등의 LTE 등가물이다.

[0004] 추가로, 이볼루션 프로세스의 부분으로서, 3GPP는 UMTS(universal mobile telecommunications system) 및 GSM(global system for mobile communications)에 이용되는 것과 다른 LTE에서의 보안 아키텍처를 이용할 것이다. 비교를 위하여, (패킷 교환(PS) 도메인에서의) UMTS 인증 및 키 동의(AKA; authentication and key agreement) 절차가 새로운 LTE 절차에 대한 베이스라인이 되는 것으로서 고려될 수 있다. 이하, 현재의 UMTS AKA 절차 및 새로운 LTE 보안 절차의 간략한 설명을 설명할 것이다.

[0005] UMTS AKA 및 암호화 절차는 복수의 프로토콜 계층들을 통해 확산(spread)되며 NAS와 무선 자원 제어(RRC; radio resource control) 시그널링 양쪽 모두를 이용하여 자신들의 목표를 달성한다. 간단히, WTRU의 식별 및 인증은 NAS 시그널링을 통하여 이루어진다. NAS 레벨에서의 인증이 이루어지면, 네트워크는 RRC 메시지인 보안 모드 코맨드를 이용하여 암호화 및/또는 무결성 보호(integrity protection)를 활성화한다. 보안 모드 코맨드를 이용하여 보안을 활성화하면, WTRU에서의 NAS 계층은 먼저 (GMM와 AS 사이에 정의된) GMMAS 서비스 액세스 포인트(SAP; service access point)를 통하여 GMMAS-SECURITY-RESPONSE 프리미티브(primitive)를 이용하여 암호 키(CK; ciphering key) 및 무결성 키(IK; integrity key)를 액세스 계층(AS; access stratum)에 전달한다. RRC는 이들 키를 수신하고 (RRC와 RLC 사이의 C-SAP를 통하여) CRLC-CONFIG 프리미티브 및 (RRC와 MAC 사이의 C-SAP를 통하여) CMAC-CONFIG 프리미티브를 이용하여 무선 링크 제어(RLC; radio link control) 및 매체 액세스 제어(MAC; medium access control)에 이들 키를 전달한다. C-SAP는 RRC와 하위계층들 사이의 C-평면(C-plane) 시그널링을 위한 서비스 액세스 포인트이다. 실제 암호화 및 무결성 보호는 통상 RLC에서 수행되지만 투명(transparent) RLC 모드 트래픽의 경우에 MAC에서 수행된다. 하위계층(즉, MAC/RLC)은 상위 계층을 향해 예정된 메시지들(예를 들어, L3 NAS 메시지들)이 정확하게 무결성 보호 및/또는 암호화되었음을 보장할 책임이 있다. 그렇지 못하면, 하위계층은 메시지를 무시/누락(drop)시킨다.

[0006] LTE에서, 보안을 위하여 근본적으로 다른 아키텍처가 제안되었다. 주요 차이점은 (즉, MAC/RLC에서) 단일의 보안 계층 대신에, 두개의 보안 레벨 - NAS 보안 및 AS 보안 - 이 있다는 점이다. NAS 보안은 이동성 관리 엔티티(MME; mobility management entity)(즉, 코어 네트워크)에서 터미네이션하고, AS 보안은 기지국(즉, eNode-B)에서 터미네이션한다. 간단히, AKA 절차는 NAS에서 완료되고, NAS 보안 키가 먼저 유도되고 완료시 AS 보안 파라미터는 암호적으로 별도의 방식으로 NAS 키로부터 유도된다(즉, AS 키의 인지는 침입자가 NAS 키를 결정하는 것을 허용하지 않는다). 이 결정에 대한 주요 원리는 LTE에서는 취약한 위치(예를 들어, 홈 Node-B)에 있는 기지국을 갖는다는 것이였으며, RRC(및 그에 따라 보안)가 기지국에서 터미네이션되기 때문에 이는 보안 리스크인 것으로 고려되었다. 따라서, 두개의 보안 레벨이 요구된다.

[0007] 도 1은 통상적인 LTE L3 헤더(100)의 구조를 나타낸다. LTE L3 헤더(100)의 첫번째 옥텟은 트랜잭션 식별자 또는 스킵 표시자 필드(105)와 프로토콜 판별자(PD; protocol discriminator) 필드(110)를 포함한다. LTE L3 헤더(100)의 두번째 옥텟은 메시지 유형 필드(115)를 포함한다. LTE L3 헤더(100)의 추가적인 옥텟은 필요에 따라 다른 정보 요소(120)를 포함할 수 있다. 이전에 설명된 바와 같이, 새로운 L3 프로토콜 엔티티가 제안되었다(예를 들어, EMM 및 ESM). 그러나, 현재의 LTE L3 헤더(100)는 이들 새로운 프로토콜을 지원하지 않는다. 구체적으로, 도 1의 LTE L3 헤더(100)에서의 PD 필드(110)는 옵션으로서 이들 새로운 프로토콜을 구별하도록 강화된다.

[0008] 도 2는 도 1의 LTE L3 헤더(100)의 PD 필드(110)를 나타낸다. 도 1 및 도 2를 참조하여 보면, LTE L3 헤더(100)에서의 첫번째 옥텟의 마지막 4개의 비트(4321)는 PD 필드(110)를 형성하며, 이는 LTE L3 헤더(100)를 포함하는 L3 메시지를 적절한 NAS 엔티티(예를 들어, 현재 MM/GMM/SM)에 라우팅하기 위해 NAS의 MM 부계층(sub-layer)에서의 라우팅 엔티티에 의해 이용되어진다.

[0009] PS-전용 UMTS WTRU의 통상적인 NAS 아키텍처(300)가 도 3에 도시되어 있다. NAS 아키텍처(300)는 무선 액세스 베어러 관리(RABM; radio access bearer management) 유닛(305), 접속 관리(CM; connection management) 유닛(310), MM 유닛(315) 및 AS 부계층(320)을 포함한다. RABM 유닛(305)은 복수의 무선 액세스 베어러(RAB; radio access bearer) 엔티티(325, 330 및 335) 및 RAB 제어 유닛(340)을 포함한다. CM 유닛(310)은 SM 유닛(345), GPRS 짧은 메시지 서비스(GSMS; GPRS short message service) 엔티티(350) 및 보조 서비스(SS; supplemental service) 엔티티(355)를 포함한다. 패킷 데이터 프로토콜(PDP; packet data protocol; 360)은 CM 유닛(310)과 MM 유닛(315) 사이의 인터페이스로서 이용된다. MM 유닛(315)은 GPRS MM(GMM) 유닛(365) 및 PD 유닛(370)을 포함한다. MM 유닛(315)과 RABM 유닛(305) 양쪽 모두는 AS 부계층(320)과 인터페이스하는데, 이는 무선 자원 제어기(RRC; radio resource controller; 375), 브로드캐스트 멀티캐스트 제어기(BMC; broadcast multicast controller; 380) 및 패킷 데이터 변환 프로토콜(PDCP; packet data conversion

protocol; 385)을 포함한다. AS 부계층(320)은 MM 유닛(315)과 RABM 유닛(305)에 서비스를 제공한다. MM 유닛(315)은 CM 유닛(310)의 엔티티들에 서비스를 제공한다.

[0010] RAB 제어 유닛(340)은 RAB 엔티티(325, 330 및 335)를 추가, 변경, 삭제, 및/또는 재구성한다. PD 유닛(370)은 NAS 메시지 정보 요소(IE; information element)를 여러 NAS 엔티티에 라우팅하는데 이용된다. SM 유닛(345)은 RABM 유닛(305)에 서비스들을 제공하고 MM 유닛(315)의 서비스들을 이용한다. GSMS 엔티티가 GMM 유닛(365)으로부터의 서비스들을 이용한다는 점을 제외하면, GSMS 엔티티(350)는 GSM에서의 GPRS 서비스들에 대한 SMS 엔티티와 일치한다. SS 엔티티가 PS 시그널링 접속으로부터의 서비스를 이용한다는 점을 제외하면, SS 엔티티(355)는 비GPRS 서비스에 대한 SS 엔티티와 일치한다. PDP 콘텍스트가 활성화 상태에 있는 동안 RABM 유닛(305)은 활성화/해제될 수 있는 RAB의 개념들을 숨긴다. 단말에서의 업링크(UL) 데이터를 해제되었던 RAB 상에서 전송하려 하면(NSAPI(network service access point identifier)), RABM 유닛(305)은 GMM 유닛(365) 내의 서비스 요청 절차를 트리거할 것이다.

[0011] 통상적으로, NAS 메시지 IE는 TLV(type/length/value) 포맷으로 인코딩된다. 도 4에 도시된 바와 같이, NAS 메시지 IE는 5개 유형의 IE(405, 410, 415, 420 및 425) 중 하나에 속한다. 도 4에 도시된 바와 같이, IE(405)는 유형(T) 단독 포맷을 가지며, IE(410)는 값(V) 단독 포맷을 가지며, IE(415)는 값 및 유형(TV) 포맷을 가지며, IE(420)는 길이 및 값(LV) 포맷을 가지며, IE(425)는 유형, 길이 및 값(TLV) 포맷을 갖는다. 도 4에 나타낸 바와 같이, IE 표시자(유형)는 IE들(405, 415 및 425)에 존재하지만 IE들(410 및 420)에는 존재하지 않는다. 길이 표시자는 IE들(420 및 425)에 존재하지만, IE들(405, 410 및 415)에는 존재하지 않는다. 값 표시자는 IE들(410, 415, 420 및 425)에는 존재하지만 IE(405)에는 존재하지 않는다.

[0012] 도 3의 NAS 아키텍처(300)를 이용하는 일부 문제는 제안된 새로운 NAS 메시지들이 식별되기 위하여 정의된 어떠한 메시지 유형들도 갖지 않는다는 점이다. 또한 예상된 새로운 NAS IE들의 일부는 그들의 인코딩을 위해 정의된 포맷을 갖지 않는다. 또한, 도 3에 도시된 NAS 엔티티는 보안을 지원하지 않는다(즉, 현재의 NAS 아키텍처를 이용하여 LTE NAS에서 보안을 구현하는 것이 어렵다).

[0013] 추가로, NAS 아키테처(300)에서, LTE에 대해 제안된 암호화 알고리즘은 블록 암호이다, 즉, 이들은 키스트림 블록을 발생시키도록 암호화될 프로토콜 데이터 유닛(PDU; protocol data unit)의 길이 표시 - 암호화되지 않는 PDU의 길이와 동일한 길이를 가짐 - 및 CK를 이용하여 작업한다. 그 후, 이 키스트림 블록을 암호화되지 않은 PDU에 비트단위(bitwise)로 추가(일반적으로)하여, 암호화된 PDU를 발생시킨다. 또한, 암호해독을 위하여 동일한 키스트림 블록을 발생시키기 위해 이 절차를 수신기에서 이용한다. 그 다음에, 이 키스트림 블록은 수신되어진 암호화된 PDU에 비트단위로 추가된다.

[0014] LTE에서는, NAS 메시지의 암호화가 동의되어 왔다. 따라서, NAS 계층은 암호화될 L3 NAS PDU의 길이를 암호화 알고리즘에 표시해야 한다. 현재, NAS가 이렇게 행하기 위한 기능은 존재하지 않는다.

[0015] 마지막으로, MME의 재할당이 허용되면, 핸드오버 동안에 MME 재할당이 발생할 수 있는 것이 가능하다. MME의 재할당을 수행하는데 이용된 핸드오버 절차의 일례가 도 5에 도시되어 있다. 현재, 무선 링크 장애와 MME간 핸드오버(inter-MME handover)시 NAS 시퀀스 번호(SN; sequence number) 및 하이퍼 프레임 번호(hyper frame number; HFN)의 처리를 위해 정의된 절차가 존재하지 않는다.

발명의 내용

해결하려는 과제

[0016] 본 발명은 LTE에서 NAS 보안을 가능하게 하는 새로운 아키텍처를 제공하는 것이다.

과제의 해결 수단

[0017] 본 출원은 LTE WTRU들에서의 NAS 계층(L3)의 특징을 설명하며, 이 특징에 의해 NAS 프로토콜 계층이 계층 3 메시지를 정확한 NAS 엔티티에 라우팅하고 새로운 NAS 메시지 유형 및 정보 요소를 인코딩하는 것을 허용받는다. NAS 보안을 가능하게 하는 새로운 아키텍처가 제공된다. NAS 메시지가 발생할 때, NAS 메시지의 프로토콜 판별자(PD; protocol discriminator), NAS 메시지의 헤더에서의 표시자 필드, NAS 메시지의 유형, NAS 보안 상태 변수, 및 RRC 프로토콜에 의한 표시 중 적어도 하나에 기초하여 NAS 메시지를 암호화, 암호해독 및/또는 무결성 검사할지 여부에 대한 판정이 행해진다. NAS 보안 상태 변수는 NAS 보안이 현재 활성 상태인지 여부를 표시하며, 1 비트를 포함할 수 있다.

[0018] NAS 프로토콜 계층은 L3 메시지를 정확한 LTE NAS 엔티티(예를 들어, EMM 및 ESM)에 라우팅하는 것을 허용받는다. 새로운 NAS 메시지 유형 및 새로운 NAS IE들의 인코딩이 허용된다. NAS 보안을 가능하게 하고, 동일한 길이의 암호 키스트림의 발생을 위한 NAS PDU의 길이의 결정을 허용하는 새로운 NAS 아키텍처가 제공된다. 또한, NAS 계층은 무선 링크 장애 및 핸드오버시 SN 및 HFN을 처리하도록 허용된다.

발명의 효과

[0019] 본 발명의 구성에 따르면, NAS 보안을 가능하게 하고, 동일한 길이의 암호 키스트림의 발생을 위한 NAS PDU의 길이의 결정을 허용하는 새로운 NAS 아키텍처를 제공할 수 있다.

도면의 간단한 설명

[0020] 첨부된 도면과 결합하여 이해되고 예를 들어 주어진 다음 설명으로부터 본 발명의 보다 자세한 이해가 이루어질 수 있다.

도 1은 통상적인 LTE L3 헤더의 구조를 나타낸다.

도 2는 도 1의 LTE L3 헤더의 PD 필드를 나타낸다.

도 3은 PS-전용 UMTS WTRU의 통상적인 NAS 아키텍처를 나타낸다.

도 4는 NAS 메시지 IE의 유형/길이/값(TLV)의 인코딩 포맷을 나타낸다.

도 5는 통상적인 MME간 핸드오버 절차의 일례를 나타낸다.

도 6은 새로운 NAS 아키텍처의 일례를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0021] 이하에 언급할 때, 이하에서 언급될 때, 용어, "WTRU"는 사용자 기기(UE), 이동국, 고정 또는 이동 가입자 유닛, 페이저, 셀룰라 전화기, 개인 휴대 정보 단말기(PDA), 컴퓨터 또는 무선 환경에서 동작가능한 임의의 기타 유형의 사용자 디바이스를 포함하지만 이들에 한정되는 것은 아니다. 이하에서 언급될 때, 용어 "기지국"은 노드-B, 사이트 컨트롤러, 액세스 포인트(AP) 또는 무선 환경에서 동작가능한 임의의 기타 유형의 인터페이싱 디바이스를 포함하지만 이들에 한정되는 것은 아니다.

[0022] 계층 3 PD 필드에 대한 강화

[0023] 도 1을 참조하여 보면, LTE L3 헤더(100)에서의 L3 PD 필드(110)가 강화될 수 있고, 이에 의해 L3 PD 필드(110)의 비트들의 특정한 조합은 LTE LE 헤더(100)를 뒤따르는 L3 메시지가 상위 계층 LTE L3 메시지(예를 들어, EMM, ESM)임을 표시한다.

[0024] 용어, EMM 및 ESM은 LTE MM 및 SM 엔티티 및 프로토콜 및 이들의 관련 기능들을 기술하는데 이용된다. 임의의 추가적인 엔티티/프로토콜이 LTE에 대한 NAS 계층에서 정의/변경된다면, 이들 각각의 프로토콜이 또한 L3 PD 필드에 추가될 수 있다. 그러나, 도 2에 도시된 바와 같이, 이렇게 행하기 위해서는 매우 적은 비트 조합이 이용가능하다. 따라서, 다음 옵션이 구현될 수 있다.

[0025] 1) (임의의 순서로) EMM 및 ESM 프로토콜을 표시하기 위해 예비 PD 값('0111' 및 '1101')을 정의한다.

[0026] 2) PD 필드가 하나의 옥텟(또는 그 이상)이도록 확장하고 EMM 및 ESM 프로토콜에 (이 증가된 PD 필드가 취할 수 있는 이용가능한 값들 중에서) 두개의 값들을 매핑한다.

[0027] 3) EMM 및 ESM 프로토콜을 표시하기 위해 일부 기존의 PD 값들(예를 들어, GMM 메시지에 대해 1000)을 재사용한다.

[0028] 메시지 유형 기술에 대한 강화

[0029] 도 1을 참조하여 보면, LTE L3 헤더(100)의 두번째 옥텟은 메시지 유형 필드(115)를 포함한다. 이 옥텟의 다른 값들이 프로토콜 판별자 필드(110)에 의해 식별된 프로토콜 계층의 다른 메시지들에 매핑한다.

[0030] LTE에 대해 예상되는 새로운 L3 NAS 메시지를 정의하기 위해, 메시지 유형 필드(115)에서의 추가적인 값들이 다음을 위해 할당된다.

[0031] 1) 추적 영역 업데이트 요청;

[0032] 2) 추적 영역 업데이트 수락(Accept);

[0033] 3) 추적 영역 업데이트 완료;

[0034] 4)추적 영역 업데이트 거절;

[0035] 5) NAS 보안 모드 코맨드

[0036] 6) NAS 보안 모드 코맨드 완료; 및

[0037] 7) NAS 보안 모드 코맨드 실패.

[0038] NAS 메시지에서의 새로운 IC 정보 요소

[0039] NAS 메시지를 무결성 검사하기 위해, 새로운 NAS IC IE를 각각의 NAS 메시지에 첨부할 수 있다. 수신기는 이 수신된 IE의 값과 자신들의 계산값을 비교한다. (이것이 알려진 알고리즘의 출력일 때) IC 비트의 길이는 고정되어 있기 쉽기 때문에, 값 부분의 길이가 고정될 때 IC IE는 유형 3 NAS 메시지 IE(유형 및 값(TV) 단독)로서 인코딩될 수 있다. 대안으로서, 이는 유형 2 또는 일부 다른 유형으로서 인코딩될 수 있다. 새로운 IE 식별자는 NAS IC IE를 식별하기 위해 정의될 수 있다.

[0040] NAS 계층을 보안하는 새로운 아키텍처

[0041] NAS 계층을 보안하기 위한 다음의 다른 아키텍처들이 기술된다.

[0042] 보안을 위한 새로운 NAS 엔티티/프로토콜

[0043] 도 6은 WTRU(즉, 이동국) 내에 상주할 수 있는 새로운 NAS L3 아키텍처(600)의 일례를 나타낸다. NAS L3 아키텍처(600)는 이볼브드 패킷 시스템 베어러 관리(EPSBM; evolved packet system bearer management) 유닛(605), CM 유닛(610), MM 유닛(615) 및 LTE AS 부계층(620)을 포함한다. EPSBM 유닛(605)은 복수의 이볼브드 패킷 시스템(EPS; evolved packet system) 베어러 엔티티(625, 630 및 635), 및 EPS 제어 유닛(640)을 포함한다. CM 유닛(610)은 이볼브드 세션 관리(ESM; evolved session management) 유닛(645), 이볼브드 짧은 메시지 서비스(ESMS; evolved short message service) 엔티티(650), 및 보조 서비스(SS; supplemental service) 엔티티(655)를 포함한다. PDP(660)는 CM 유닛(610) 및 MM 유닛(615) 사이의 인터페이스로서 이용된다. MM 유닛(615)은 이볼브드 이동성 관리(EMM; evolved mobility management) 유닛(665) 및 보안 접속(SC; secure connectivity) 유닛(370)을 포함한다. SC 유닛(370)은 PD 유닛(375)을 포함한다. MM 유닛(615)과 EPSBM 유닛(605) 양쪽 모두는 RRC(680) 및 PDCP(685)을 포함하는 LTE AS 부계층(620)과 인터페이스한다.

[0044] EPS 베어러 엔티티(625, 630 및 635)는 WTRU와 패킷 데이터 노드(PDN; packet data node) 게이트웨이 사이에서 실행하며 무선 베어러(RB; radio bearer) 및 EPS 액세스 베어러의 조합으로 구성된다. EPSBM 유닛(605)은 EPS 베어러의 변경 및 구성을 제어한다. LTE AS 부계층(620)은 MM 유닛(615) 및 EPSBM 유닛(605)에 서비스를 제공한다. ESM 유닛(645)은 EPSBM 유닛(605)에 서비스들을 제공하고 MM 유닛(615)의 서비스들을 이용한다. ESMS 엔티티(650)는 EMM 유닛(665)으로부터의 서비스를 이용한다는 점을 제외하면 GSM에서의 GPRS 서비스에 대한 SMS 엔티티와 일치한다. SS 엔티티(655)는 PS 시그널링 접속으로부터의 서비스를 이용한다는 점을 제외하면 비-GPRS 서비스에 대한 것과 일치한다.

[0045] EMM 유닛(665) 및 ESM 유닛(645)으로부터의 모든 메시지들이 SC 유닛(670)을 통하여 LTE AS 부계층(620)에 전달되도록 SC 유닛(670)이 이용된다. SC 유닛(670)은 도 6에 도시된 바와 같이 MM 유닛(615)의 서브엔티티로서 보여질 수 있거나 또는 MM 유닛(615)과 별도의 L3 엔티티로서 보여질 수 있다. SC 유닛(670)의 기능이 또한 하위 계층들(예를 들어, RRC(680))에 상주할 수 있고, 및 이 기능은 또한 자신의 프로토콜을 갖도록 정의될 수 있다.

[0046] 기능적으로, 다음의 것의 임의의 조합이 구현될 수 있다.

[0047] 1) EMM, ESM 및 다른 엔티티(예를 들어, SMS)가 SC 유닛(670)에 메시지를 전송할 수 있다.

[0048] 2) SAP 및 관련 프리미티브가 EMM 유닛(665) 및 SC 유닛(670)과, ESM 유닛(645) 및 SC 유닛(670)에 대해 정의될 수 있다.

[0049] 3) SC 유닛(670)(또는 보다 일반적으로는 NAS)이 NAS 보안이 현재 활성상태에 있는지 여부를 표시하는 NAS 보안 상태 변수(예를 들어, 1 비트)를 정의할 수 있다. 암호화와 무결성 보호 간을 구별하기 위해 이러한 두개

의 변수들을 갖는 것이 가능하다. 암호화의 존재 및 부재를 표시하기 위해 1 비트 NAS 보안 상태 변수를 대신하여 프리마티브가 NAS와 RRC 사이에 교환될 수 있음을 주지한다. 또한, 1 비트가 암호화가 시작했음을 표시하는데 이용되는 별도의 PDU로서 고려될 수 있다(예를 들어, 별도의 NAS 메시지가 이러한 목적을 위해 이용될 수 있다). 대안으로서, 이 1 비트는 모든 NAS PDU 내에 포함될 수 있다.

[0050] 4) SC 유닛(670)은 투명 모드 또는 비투명 모드에서 동작할 수 있다. 투명 모드에서, SC 유닛(670)은 특정한 NAS 메시지를 암호/암호해독 및/또는 무결성 검사를 행하지 않을 것이다. 이 결정은 다음의 인자들: 메시지의 프로토콜 판별자, (특정한 PDU에 대한 암호화 및/또는 무결성 보호의 요건을 표시하는) L3 프로토콜 헤더의 표시자 필드, 메시지 유형, NAS 보안 상태 변수, 상위 계층 프로토콜에 의한 표시(예를 들어, 이 메시지를 암호화/무결성 검사하지 않도록 하는 EMM 유닛(665) 및/또는 ESM 유닛(645)으로부터 SC 유닛(670)으로의 표시)의 임의의 조합에 기초할 수 있다.

[0051] 5) 비투명 모드에서, SC 유닛(670)은 관련 NAS PDU를 암호화/암호해독 및/또는 무결성 검사할 수 있다. 이 결정은 또한 다음의 인자들: 메시지의 프로토콜 판별자, (특정 PDU에 대한 암호화 및/또는 무결성 보호의 요건을 표시하는) L3 프로토콜 헤더에서의 표시자 필드, 메시지 유형, NAS 보안 상태 변수, 상위 계층 프로토콜에 의한 표시(예를 들어, 이 메시지를 암호화/무결성 검사하지 않도록 하는 EMM 유닛(665) 및/또는 ESM 유닛(645)으로부터 SC 유닛(670)으로의 표시)의 임의의 조합에 기초할 수 있다.

[0052] 6) 수신 측에서, SC 유닛(670)은 하위 계층으로부터 NAS PDU를 수신할 수 있고, 투명 모드에서 동작중이라면, 자신의 프로토콜 판별자에 기초하여 정확한 상위 계층 엔티티(예를 들어, EMM/ESM)에 NAS PDU를 라우팅할 수 있다. 수신중인 SC 유닛(670)이 비투명 모드에 있다면, SC 유닛(670)은 NAS PDU를 암호화 및/또는 무결성 검사하고, 자신의 NAS SN 및/또는 NAS HFN를 증분시킨 다음, NAS 헤더의 PD 필드에 기초하여 메시지를 라우팅할 수 있다. 수신 측은 메시지의 암호해독 후 무결성 검사를 행할 수 있거나 또는 송신측에서의 이들 동작의 순서에 따라 역으로 행할 수 있다.

[0053] 이전에 설명된 바와 같이, SC 유닛(670)에 대한 별도의 프로토콜을 갖는 것이 가능할 수 있다. 이러한 프로토콜은 L3 헤더 내의 자신의 프로토콜 판별자를 가짐으로써 구별될 수 있다. 이 프로토콜에 속하는 이 메시지 유형은 무엇보다도 암호화, 인증, 식별 및 키 동의에 관련된 것일 수 있다. 예들은 다음의 것을 포함한다.

[0054] 1) 아이덴티티 요청;

[0055] 2) 아이덴티티 응답;

[0056] 3) 인증 요청;

[0057] 4) 인증 응답;

[0058] 5) 인증 실패;

[0059] 6) 인증 거부;

[0060] 7) NAS 보안 모드 코맨드;

[0061] 8) NAS 보안 모드 코맨드 완료; 및

[0062] 9) NAS 보안 모드 코맨드 실패.

[0063] 또한, 이 엔티티에 대한 상태 머신을 정의하는 것이 가능할 수 있다. 일례로서, 다음은 가능한 상태를 기술한다(이들 상태 및 다른 상태에 대한 다른 명칭이 가능할 수 있음).

[0064] a) SECURITY INACTIVE: 이 상태에서는, WTRU가 네트워크에 대해 인증받지 못하고 보안 콘텍스트가 WTRU 내에 또는 네트워크 내에 존재하지 않는다. 이 상태의 서브상태로서(또는 별도의 상태로서) 진행중인 AKA 세션, NAS 보안 모드 코맨드 교환 및 RRC 보안 모드 코맨드 교환을 표시하는 상태들을 가질 수 있다.

[0065] b) SECURITY ACTIVE: 이 상태에서는, WTRU가 네트워크에 대해 인증되며, 보안 콘텍스트가 WTRU 내에 및 네트워크 내에 존재한다. WTRU는 일부 키(예를 들어, K_{asme}) 또는 모든 키를 가질 수 있다.

[0066] 또한, 보다 복잡하지만 다른 방식으로 이 동일한 SCE를 구현하는 것이 가능할 수 있다. 예를 들어, 전송측에서, NAS PDU를 구성했던 (EMM 유닛(655) 또는 ESM 유닛(645)과 같은) 상위 계층 콜링 엔티티가 NAS PDU를 NAS SC 유닛(670)에 전송할 수 있다. 그 다음, NAS SC 유닛(670)은 PDU를 암호화 및/또는 무결성 검사를 행한 다음 및 PDU를 콜링 엔티티에 반환할 수 있다. 그 다음, 콜링 엔티티는 안전한 NAS PDU를 하위 계층(즉, RRC)에

전송할 수 있다. 이 방법은 MM 유닛(615)과 LTE AS 부계층(620) 사이에 기존의 SAP를 라우팅하는 이점을 갖는다. 그러나, 수신 측에서 는, 메시지를 정확한 상위 계층 프로토콜 엔티티에 라우팅할 수 있기 전에, 메시지를 암호해독 및 무결성 검사한다. 이 기능은 모든 수신한 NAS PDU들을 SC 유닛(670)에 라우팅하고 그 후 SC 유닛(670)이 라우팅 결정을 행함으로써 달성될 수 있다.

[0067] 다른 옵션은 각각의 NAS 계층이 자신의 프로토콜 내의 메시지들의 암호화/무결성 보호를 행하는 것이다. 따라서, EMM 유닛(665)은 EMM 메시지를 암호화/무결성 보호/암호해독할 수 있고 ESM 유닛(645)은 ESM 메시지를 암호화/무결성 보호/암호해독할 수 있으며 이하 동일하게 이루어진다. 이 경우에 SC 유닛(670)의 역할은 이용되고 있는 일련 번호(SN)의 충돌이 없도록 EMM 및 ESM 계층 (및 임의의 다른 계층들)에 SN을 제공하는 것으로 제한될 수 있다. 이 문제는 NAS PDU 마다 기초하는 대신에 프로토콜 PDU 마다 기초하여 증분하도록 SN을 정의함으로써 없어질 수 있다. 이 경우, 각각의 NAS 부계층(예를 들어, EMM/ESM)은 이 프로토콜에 속하는 모든 NAS PDU마다 증분되는 자신의 SN/HFN을 가질 수 있다. 이 버전에서, 수신측에서는 (수신받은 NAS PDU가 암호화되지 않은 것으로 가정하면) NAS 계층의 라우팅 엔티티가 NAS 헤더의 프로토콜 판별자 필드에 기초하여 수신받은 NAS PDU를 정확한 NAS 엔티티에 라우팅할 수 있고, 그 다음, 각각의 프로토콜 엔티티가 메시지를 암호해독 및/또는 무결성 검사를 행할 수 있다.

[0068] NAS PDU 길이의 결정

[0069] NAS 계층은 (암호해독된) NAS PDU의 일부분의 길이를 암호화 엔진에 제공할 수 있다. 다음은 이 길이를 결정하기 위한 여러가지 옵션들이다.

[0070] 1) 전송 NAS 엔티티는 L3 메시지에서(예를 들어, 프로토콜 헤더에서)의 길이의 표시를 포함할 수 있다. 이 길이는 전체 메시지의 길이거나 또는 암호화된 메시지 부분의 길이거나 또는 NAS 엔티티가 발생되는 것이 필요한 키스트림 블록의 길이를 결정하는 것을 허용하는 일부 다른 값의 길이일 수 있다.

[0071] 2) 전송 NAS 엔티티는 전송을 위한 L3 메시지를 전달할 때 RRC에의 L3 메시지의 길이의 표시를 포함할 수 있다. 이 길이 표시는 수신기의 RRC 계층에 의해 수신되고 수신기 NAS 엔티티 상에 전달되며, 여기서, 발생된 키스트림 블록의 길이를 결정하는데 이용된다.

[0072] 3) 현재, NAS 계층은 NAS 계층에서 재세그먼테이션을 수행함이 없이 완전한 NAS PDU를 예상한다. 그 결과, NAS PDU를 수신할 때, 수신중인 엔티티는 NAS PDU가 완전한 것임을 확산할 수 있다(엔티티가 예상값을 손실한 메시지를 수신한다면 그 거동은 현재 메시지를 폐기하는 것이다). 따라서, NAS PDU의 길이 결정을 구현에 이르기 까지 남겨놓는 것이 가능하다.

[0073] 수신기에서의 예시적인 구현이 아래 주어진다.

[0074] 1) NAS PDU가 수신된다;

[0075] 2) NAS PDU가 메모리/버퍼 또는 그 등가물 내에 저장된다;

[0076] 3) 메시지 크기가 결정된다(예를 들어, 점유된 메모리/버퍼 공간);

[0077] 4) 메시지의 크기로부터 암호화되지 않은 메시지 부분의 길이를 감산함으로써 메시지의 암호화된 부분의 길이가 결정된다. 암호화되지 않은 메시지 부분의 길이는 고정될 수 있거나 또는 (예를 들어, 메시지 유형/프로토콜에 따라) 알려진 패턴으로 변할 수 있거나 또는 수신중인 NAS 엔티티에서의 전송 NAS 엔티티에 의해 구성될 수 있다; 및

[0078] 5) 암호해독을 위해 이용될 키스트림을 결정하기 위해 암호화된 부분의 길이는 암호화 알고리즘에 전달된다.

[0079] 무선 링크 장애 및 핸드오버시 NAS SN 및 HFN의 처리

[0080] 이들 절차의 부분으로서, 현재의 NAS SN 및 HFN 번호를 네트워크에서 처리하는 방법을 결정할 필요가 있다.

[0081] 핸드오버 동안에, 다음 중 임의의 것이 WTRU 및 소스 MME에서 현재 NAS SN 및 HFN으로 수행될 수 있다.

[0082] 1) 이들은 양쪽 모두가 디폴트 값으로 리세트될 수 있다.

[0083] 2) NAS HFN은 리세트될 수 없지만 NAS SN는 리세트될 수 있다. 소스 MME가 HO(Handover) 요청의 일부로서 NAS HFN을 타겟에 전달한다.

[0084] 3) NAS SN은 리세트될 수 없지만, NAS HFN이 리세트될 수 있다. 소스 MME가 HO 요청의 일부로서 NAS SN을 타

겟에 전달한다.

[0085] 4) NAS HFN와 NAS SN가 모두 리세트될 수 없다. 소스 MME가 NAS HFN와 NAS SN 양쪽 모두를 HO 요청의 일부로서 타겟에 전달한다.

[0086] 응답될 필요가 있는 다른 질문은 임의의 파라미터들(NAS SN 및/또는 HFN)이 리세트되고 있다면, 이 리세트가 트리거될 때와 어떻게 새로운 NAS/ASME 키가 WTRU에 전달되는지이다.

[0087] 따라서, MME간 핸드오버 동안, NAS 메시지는 소스 MME로부터, 새로운 NAS 및 ASME 키를 유도하는데 필요한 파라미터들을 제공하는 WTRU에 트리거된다. 대안으로서, 소스 MME는 (기존의 암호화/무결성 보호를 이용하여) 안전한 방식으로 WTRU에 새로운 NAS 및 ASME 키를 제공한다. 일례로서, 이 메시지는 NAS 보안 모드 코맨드/재구성일 수 있다. 이 NAS 메시지는 핸드오버 코맨드 이전에 (예를 들어, 별도의 다운링크 직접 전송 메시지에서) 또는 핸드오버 코맨드 내의 L3 메시지로서 전송될 수 있다. 다른 대안으로서, 이 정보는 RRC 메시지에서 직접 전송될 수 있다.

[0088] NAS SN 및/또는 HFN의 리세트가 핸드오버의 하위 계층 표시에 의해 즉각적으로 (예를 들어, RRC가 핸드오버 코맨드를 수신할 때) 또는 상기 별도의 NAS 메시지의 수신에 의해 트리거될 수 있다.

[0089] 무선 링크 장애 및 eNodeB간 핸드오버 시 NAS SN 및 HFN의 처리

[0090] 업링크(UL) 및 다운링크(DL)에서 무선 링크(RL) 장애 및 eNodeB간 핸드오버에 대해서, NAS SN 및/또는 HFN은 리세트될 수 있다. 이는 메시지(예를 들어, RRC 메시지)의 전송 또는 수신에 의해 트리거될 수 있다.

[0091] NAS에서의 재전송의 처리

[0092] 재전송의 경우, NAS 계층은 다시 전송된 패킷이 중복의 PDU(이미 수신된 PDU) 또는 새로운 PDU인지 여부를 검출할 수 있다. 중복 검출 엔티티는 EMM 또는 ESM 아래에 위치한 공통 엔티티일 수 있고 들어오는 패킷이 이전에 전송되었던 것인지 여부를 모니터링할 수 있다. 전송된 NAS PDU에 대한 확인응답이 수신되지 않았을 경우, 하위 계층들은 NAS 계층에 이 표시를 제공할 수 있다. NAS 계층은 동일한 SN을 이용하여 PDU를 재전송(또는 새로운 PDU를 전송)하기 위해 이 표시를 이용할 수 있다.

[0093] 중복 검출이 허용되지 않는 경우, 새로운 시퀀스 번호를 이용하여 데이터를 전송하는 것과는 반대로, 실패된 전송의 경우에 동일한 시퀀스 번호를 이용하여 데이터를 전송할 수 있다.

[0094] 대안으로서, 또는 추가적으로, NAS가 NAS 트랜잭션 식별자를 이용하여 중복의 메시지를 검출할 수 있다. 이는 NAS 헤더의 일부인 NAS 트랜잭션 ID를 필요로 할 수 있다. 따라서, WTRU는 임의의 수신된 중복 메시지를 폐기할 수 있다.

[0095] [실시예]

[0096] 1. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, NAS 메시지의 헤더에서의 표시자 필드에 기초하여 NAS 메시지를 암호화할지 여부를 결정하는 것을 포함하는 방법.

[0097] 2. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, NAS 메시지의 PD에 기초하여 NAS 메시지를 암호화할지 여부를 결정하는 것을 포함하는 방법.

[0098] 3. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, NAS 메시지의 유형에 기초하여 NAS 메시지를 암호화할지 여부를 결정하는 것을 포함하는 방법.

[0099] 4. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, NAS 보안 상태 변수에 기초하여 NAS 메시지를 암호화할지 여부를 결정하는 것을 포함하는 방법.

[0100] 5. 실시예 4에 있어서, NAS 보안 상태 변수는 NAS 보안이 현재 활성 상태인지 여부를 표시하는 것인 방법.

[0101] 6. 실시예 4에 있어서, NAS 보안 상태 변수는 1 비트를 포함하는 것인 방법.

[0102] 7. 실시예 4에 있어서, NAS 보안 상태 변수는 암호화가 시작했음을 표시하는데 이용되는 NAS PDU를 포함하는 것인 방법.

[0103] 8. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, RRC 프로토콜에 의한 표시에 기초하여 NAS 메시지를 암호화할지 여부를 결정하는 것을 포함하는 방법.

[0104] 9. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, NAS 메시지의 헤더에서의 표시

자 필드에 기초하여 NAS 메시지에 대한 무결성 검사를 수행할지 여부를 결정하는 것을 포함하는 방법.

[0105] 10. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, NAS 메시지의 PD에 기초하여 NAS 메시지에 대한 무결성 검사를 수행할지 여부를 결정하는 것을 포함하는 방법.

[0106] 11. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, NAS 메시지의 유형에 기초하여 NAS 메시지에 대한 무결성 검사를 수행할지 여부를 결정하는 것을 포함하는 방법.

[0107] 12. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, NAS 보안 상태 변수에 기초하여 NAS 메시지에 대한 무결성 검사를 수행할지 여부를 결정하는 것을 포함하는 방법.

[0108] 13. 실시예 12에 있어서, NAS 보안 상태 변수는 NAS 보안이 현재 활성 상태인지 여부를 표시하는 것인 방법.

[0109] 14. 실시예 13에 있어서, NAS 보안 상태 변수는 1 비트를 포함하는 것인 방법.

[0110] 15. 실시예 13에 있어서, NAS 보안 상태 변수는 암호화가 시작했음을 표시하는데 이용되는 NAS PDU를 포함하는 것인 방법.

[0111] 16. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, RRC 프로토콜에 의한 표시에 기초하여 NAS 메시지에 대한 무결성 검사를 수행할지 여부를 결정하는 것을 포함하는 방법.

[0112] 17. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, 프로토콜 판별자(PD) 필드를 포함하는 NAS PDU를 하위 계층으로부터 수신하고, NAS PDU를 암호화하고, NAS PDU와 관련된 NAS SN 및 HFN 중 적어도 하나를 증분시키고, PD 필드에 기초하여 NAS PDU를 상위 계층 엔티티에 라우팅하는 것을 포함하는 NAS 메시지 처리 방법.

[0113] 18. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, 프로토콜 판별자(PD) 필드를 포함하는 NAS PDU를 하위 계층으로부터 수신하고, NAS PDU에 대한 무결성 검사를 수행하고, NAS PDU와 관련된 NAS SN 및 HFN 중 적어도 하나를 증분시키고, PD 필드에 기초하여 NAS PDU를 상위 계층 엔티티에 라우팅하는 것을 포함하는 NAS 메시지 처리 방법.

[0114] 19. WTRU에 있어서, NAS 메시지를 발생시키도록 구성된 ESM 유닛과, NAS 메시지의 PD, NAS 메시지의 헤더에서의 표시자 필드, NAS 메시지의 유형, NAS 보안 상태 변수, 및 RRC 프로토콜에 의한 표시 중 적어도 하나에 기초하여 NAS 메시지를 암호화할지 여부를 결정하도록 구성된 SC 유닛을 포함하는 WTRU.

[0115] 20. 실시예 19에 있어서, NAS 보안 상태 변수는 NAS 보안이 현재 활성 상태인지 여부를 표시하는 것인 WTRU.

[0116] 21. 실시예 20에 있어서, NAS 보안 상태 변수는 1 비트를 포함하는 것인 WTRU.

[0117] 22. 실시예 20에 있어서, NAS 보안 상태 변수는 암호화가 시작했음을 표시하는데 이용되는 NAS PDU를 포함하는 것인 WTRU.

[0118] 23. 실시예 19에 있어서, SC 유닛은 PD 유닛을 포함하는 것인 WTRU.

[0119] 24. WTRU에 있어서, NAS 메시지를 발생시키도록 구성된 ESM 유닛과, NAS 메시지의 PD, NAS 메시지의 헤더에서의 표시자 필드, NAS 메시지의 유형, NAS 보안 상태 변수, 및 RRC 프로토콜에 의한 표시 중 적어도 하나에 기초하여 NAS 메시지를 암호해독할지 여부를 결정하도록 구성된 SC 유닛을 포함하는 WTRU.

[0120] 25. 실시예 24에 있어서, NAS 보안 상태 변수는 NAS 보안이 현재 활성 상태인지 여부를 표시하는 것인 WTRU.

[0121] 26. 실시예 25에 있어서, NAS 보안 상태 변수는 1 비트를 포함하는 것인 WTRU.

[0122] 27. 실시예 25에 있어서, SC 유닛은 PD 유닛을 포함하는 것인 WTRU.

[0123] 28. WTRU에 있어서, NAS 메시지를 발생시키도록 구성된 ESM 유닛과, NAS 메시지의 PD, NAS 메시지의 헤더에서의 표시자 필드, NAS 메시지의 유형, NAS 보안 상태 변수, 및 RRC 프로토콜에 의한 표시 중 적어도 하나에 기초하여 NAS 메시지에 대한 무결성 검사를 수행할지 여부를 결정하도록 구성된 SC 유닛을 포함하는 WTRU.

[0124] 29. 실시예 28에 있어서, NAS 보안 상태 변수는 NAS 보안이 현재 활성 상태인지 여부를 표시하는 것인 WTRU.

[0125] 30. 실시예 29에 있어서, NAS 보안 상태 변수는 1 비트를 포함하는 것인 WTRU.

[0126] 31. 실시예 28에 있어서, SC 유닛은 PD 유닛을 포함하는 것인 WTRU.

[0127] 32. WTRU에 있어서, NAS 메시지를 발생시키도록 구성된 EMM 유닛과, NAS 메시지의 PD, NAS 메시지의 헤더에서의 표시자 필드, NAS 메시지의 유형, NAS 보안 상태 변수, 및 RRC 프로토콜에 의한 표시 중 적어도 하나에 기

초하여 NAS 메시지를 암호화할지 여부를 결정하도록 구성된 SC 유닛을 포함하는 WTRU.

[0128] 33. 실시예 32에 있어서, NAS 보안 상태 변수는 NAS 보안이 현재 활성 상태인지 여부를 표시하는 것인 WTRU.

[0129] 34. 실시예 33에 있어서, NAS 보안 상태 변수는 1 비트를 포함하는 것인 WTRU.

[0130] 35. 실시예 33에 있어서, NAS 보안 상태 변수는, 암호화가 시작했음을 표시하는데 이용되는 NAS PDU를 포함하는 것인 WTRU.

[0131] 36. 실시예 32에 있어서, SC 유닛은 PD 유닛을 포함하는 것인 WTRU.

[0132] 37. WTRU에 있어서, NAS 메시지를 발생시키도록 구성된 EMM 유닛과, NAS 메시지의 PD, NAS 메시지의 헤더에서의 표시자 필드, NAS 메시지의 유형, NAS 보안 상태 변수, 및 RRC 프로토콜에 의한 표시 중 적어도 하나에 기초하여 NAS 메시지에 대한 무결성 검사를 수행할지 여부를 결정하도록 구성된 SC 유닛을 포함하는 WTRU.

[0133] 38. 실시예 37에 있어서, NAS 보안 상태 변수는 NAS 보안이 현재 활성 상태인지 여부를 표시하는 것인 WTRU.

[0134] 39. 실시예 38에 있어서, NAS 보안 상태 변수는 1 비트를 포함하는 것인 WTRU.

[0135] 40. 실시예 37에 있어서, SC 유닛은 PD 유닛을 포함하는 것인 WTRU.

[0136] 41. WTRU에서 NAS 메시지를 처리하는 방법에 있어서, NAS 메시지를 발생시키고, NAS 메시지의 표시에 기초하여 발생될 필요가 있는 키스트림 블록의 길이를 결정하는 것을 포함하는 방법.

[0137] 42. 실시예 41에 있어서, 표시는 NAS 메시지의 전체 길이를 전달하는 것인 방법.

[0138] 43. 실시예 41에 있어서, 표시는 수신중인 NAS 엔티티가 발생될 키스트림 블록의 길이를 결정하는 것을 허용하는 값을 전달하는 것인 방법.

[0139] 44. WTRU에 있어서, NAS 메시지를 발생시키도록 구성된 EMM 유닛과, NAS 메시지의 표시에 기초하여 발생될 필요가 있는 키스트림 블록의 길이를 결정하도록 구성된 SC 유닛을 포함하는 WTRU.

[0140] 45. 실시예 44에 있어서, 표시는 NAS 메시지의 전체 길이를 전달하는 것인 WTRU.

[0141] 46. 실시예 44에 있어서, 표시는 수신중인 NAS 엔티티가 발생될 키스트림 블록의 길이를 결정하는 것을 허용하는 값을 전달하는 것인 WTRU.

[0142] 특징들 및 요소들이 실시예들에서 특정 조합으로 설명되어 있지만, 각각의 특징 또는 요소는 실시예들의 다른 특징들 및 요소들 없이 단독으로, 또는 다른 특징들 및 요소들을 갖고 또는 갖지 않고 여러 조합들로 이용될 수 있다. 여기에 제공된 방법들 또는 흐름도들은 범용 컴퓨터 또는 프로세서에 의한 실행을 위해 컴퓨터 판독가능 저장 매체에서 실체적으로 구현되는 컴퓨터 프로그램, 소프트웨어, 또는 펌웨어로 실행될 수 있다. 컴퓨터 판독가능 저장 매체들의 예들은 판독 전용 메모리(ROM), 무작위 액세스 메모리(RAM), 레지스터, 캐시 메모리, 반도체 메모리 디바이스, 내부 하드 디스크 및 착탈 가능 디스크와 같은 자기 매체, 자기 광학 매체, 및 CD-ROM 디스크 및 디지털 다기능 디스크(DVD)와 같은 광학 매체를 포함한다.

[0143] 적절한 프로세서들은 예를 들어, 범용 프로세서, 특수 목적 프로세서, 통상적인 프로세서, 디지털 신호 프로세서(DSP), 복수의 마이크로프로세서, DSP 코어와 관련된 1 이상의 마이크로프로세서, 컨트롤러, 마이크로컨트롤러, 응용 주문형 직접 회로(ASIC), 필드 프로그래밍가능 게이트 어레이(FPGA) 회로, 임의의 기타 유형의 집적 회로(IC), 및/또는 상태 머신을 포함한다.

[0144] 소프트웨어와 관련된 프로세서는 WTRU, UE, 단말기, 기지국, 무선 네트워크 컨트롤러(RNC) 또는 임의의 호스트 컴퓨터에 이용하기 위한 무선 주파수 트랜시버를 구현하는데 이용될 수 있다. WTRU는 카메라, 비디오 카메라 모듈, 비디오폰, 스피커폰, 바이블레이션 디바이스, 스피커, 마이크로폰, 텔레비젼 트랜시버, 핸드 프리 헤드셋, 키보드, 블루투스®

모듈, 주파수 변조(FM) 무선 유닛, 액정 디스플레이(LCD) 표시 유닛, 유기 발광 다이오드 (OLED) 표시 유닛, 디지털 뮤직 플레이어, 미디어 플레이어, 비디오 게임 플레이어 모듈, 인터넷 브라우저, 및/또는 임의의 무선 근거리 통신 네트워크(WLAN) 모듈 또는 초광대역(UWB) 모듈과 같이, 하드웨어 및/또는 소프트웨어로 구현되는 모듈과 결합하여 이용될 수 있다.

부호의 설명

[0145] 605: EPSBM 유닛

610: CM 유닛

615: MM 유닛

620: LTE AS 부계층

625, 630, 635: EPS 베어러 엔티티 1

640: EPS 베어러 제어 유닛

645: ESM 유닛

650: ESMS 엔티티

655: SS 엔티티

660: PDP 유닛

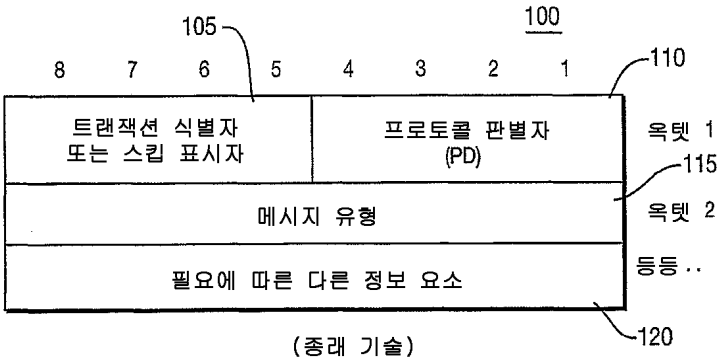
665: EMM 유닛

670: SC 유닛

675: PD 유닛

도면

도면1



(종래 기술)

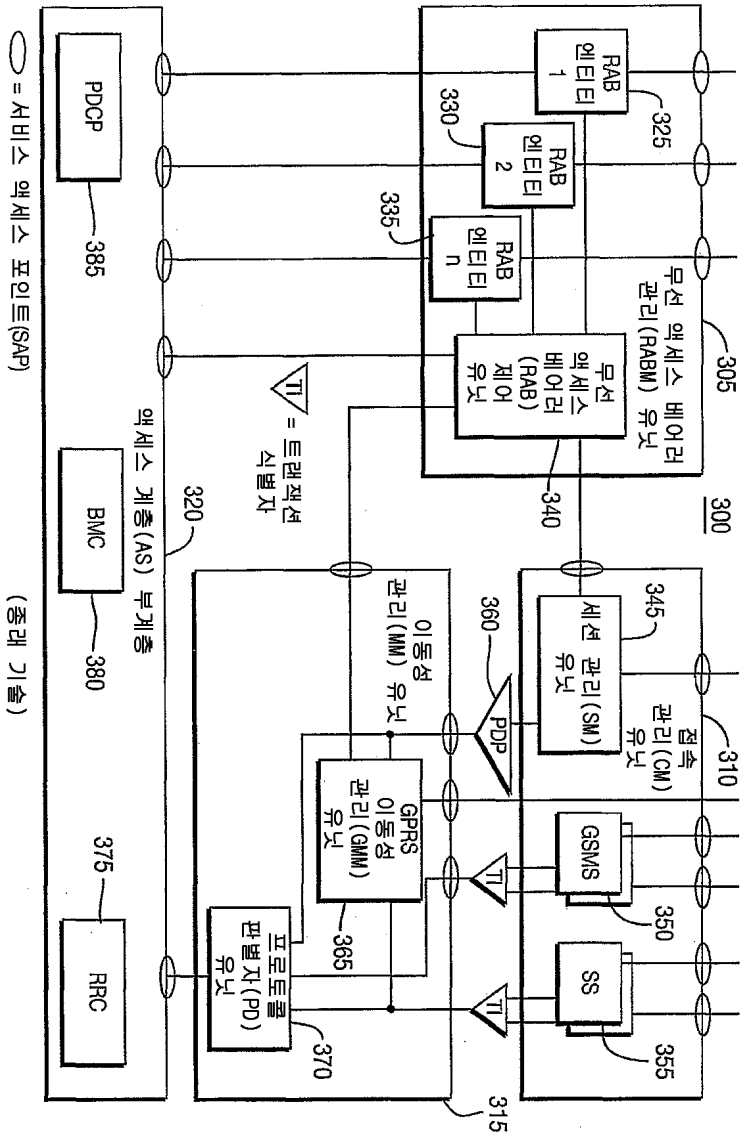
도면2

110

BITS 4321	
0000	그룹 콜 제어
0001	브로드캐스트 콜 제어
0010	예약됨: 프로토콜의 초기 단계에 할당되었음
0011	콜 제어; 콜 관련 SS 메시지
0100	GPRS 투명 전송 프로토콜(GTTP)
0101	이동성 관리 메시지
0110	무선 자원 관리 메시지
1000	GPRS 이동성 관리 메시지
1001	SMS 메시지
1010	GPRS 세션 관리 메시지
1011	콜과 관련되지 않은 SS 메시지
1100	위치 서비스
1110	PD를 하나의 옥텟 길이로 확장하기 위해 예약됨
1111	테스트 절차를 위해 예약됨

(종래 기술)

도면3

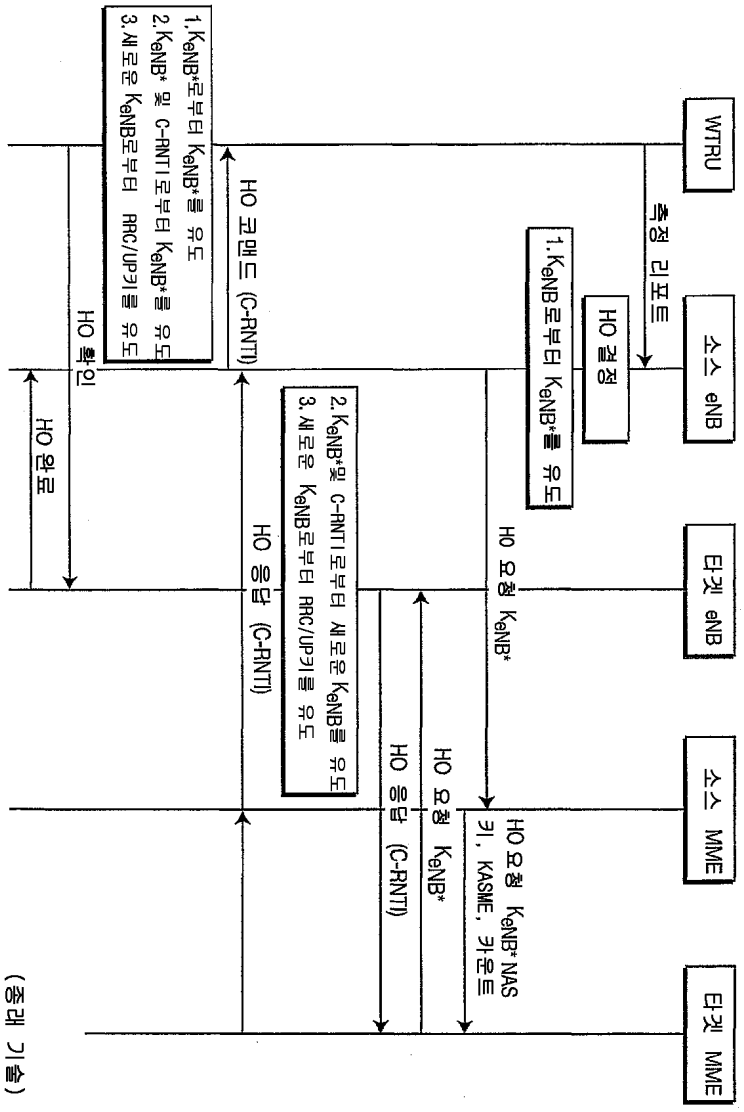


도면4

	포맷	의미	IE 표시자 (유형) 제공	길이 표시자 제공	값 표시자 제공
405	T	유형 단독	예	아니오	아니오
410	V	값 단독	아니오	아니오	예
415	TV	유형 및 값	예	아니오	예
420	LV	길이 및 값	아니오	예	예
425	TLV	유형,길이 및 값	예	예	예

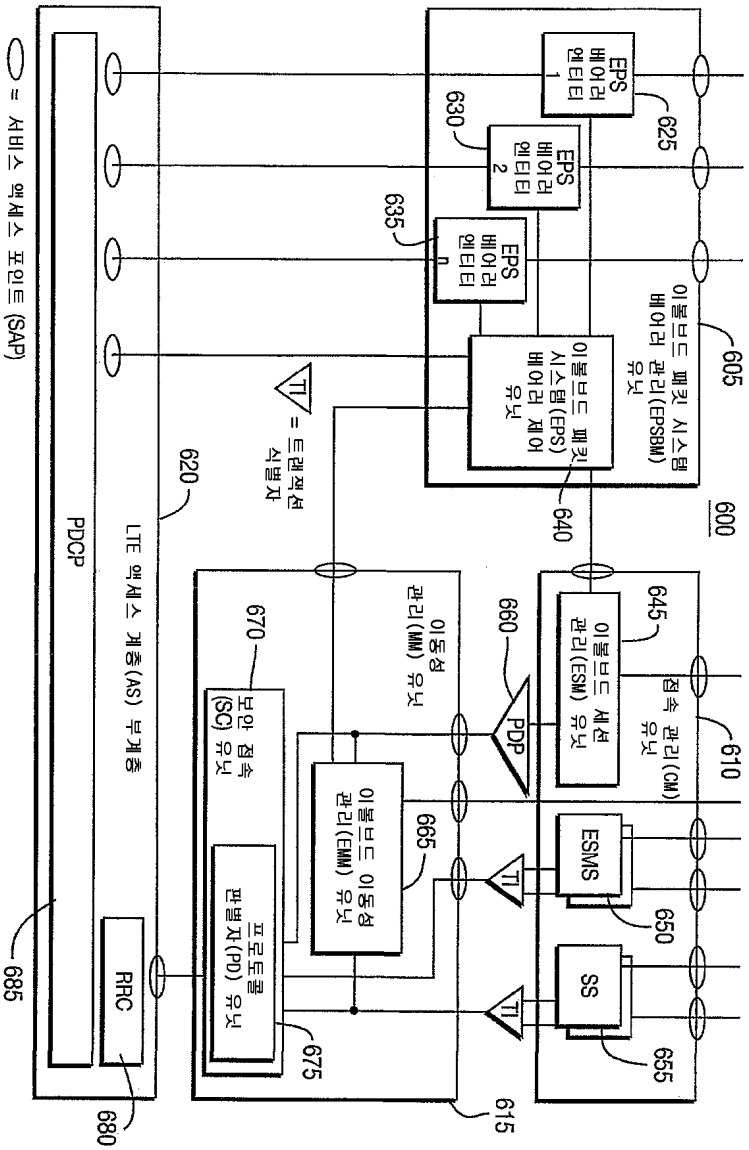
(종래 기술)

도면5


WTRU
소스 eNB
타겟 eNB
소스 MME
타겟 MME
측정 리포트
HO 결정
1. KeNB로부터 KeNB*를 유도
HO 요청 KeNB*
HO 요청 KeNB* NAS 키, KASME, 카운트
HO 요청 KeNB*
HO 응답 (C-RNTI)
2. KeNB*및 C-RNTI로부터 새로운 KeNB를 유도
3. 새로운 KeNB로부터 RRC/UP키를 유도
HO 응답 (C-RNTI)
HO 코맨드 (C-RNTI)
1. KeNB*로부터 KeNB*를 유도
2. KeNB* 및 C-RNTI로부터 KeNB*를 유도
3. 새로운 KeNB로부터 RRC/UP키를 유도
HO 확인
HO 완료

(종래 기술)

도면6


= 서비스 액세스 포인트 (SAP)
PDCP
RRC
LTE 액세스 계층(AS) 부계층
685
680
620
= 트랜잭션 식별자
보안 접속(SC) 유닛
프로토콜 판별자(PD) 유닛
675
670
이동성 관리(MM) 유닛
이볼브드 이동성 관리(EMM) 유닛
665
660
PDP
TI
TI
TI
ESMS
SS
650
655
615
이볼브드 세션 관리(ESM) 유닛
645
접속 관리(CM) 유닛
610
이볼브드 패킷 시스템 베어러 관리(EPSBM) 유닛
605
600
이볼브드 패킷 시스템(EPS) 베어러 제어 유닛
640
EPS 베어러 엔티티 n
635
EPS 베어러 엔티티 2
630
EPS 베어러 엔티티
625