

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012년 10월 4일 (04.10.2012)



(10) 국제공개번호
WO 2012/134218 A2

- (51) 국제특허분류:
H04B 7/26 (2006.01) H04W 12/08 (2009.01)
- (21) 국제출원번호: PCT/KR2012/002377
- (22) 국제출원일: 2012년 3월 30일 (30.03.2012)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
61/469,823 2011년 3월 31일 (31.03.2011) US
- (71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): 엘지전자 주식회사 (LG ELECTRONICS INC.) [KR/KR]; 서울 영등포구 여의도동 20, 150-721 Seoul (KR).
- (72) 발명자: 겸
- (75) 발명자/출원인 (US 에 한하여): 이영대 (LEE, Young-dae) [KR/KR]; 경기도 안양시 동안구 호계 1동 533번지 엘지전자 특허센터, 431-080 Gyeonggi-do (KR). 이송준 (YI, Seungjune) [KR/KR]; 경기도 안양시 동안구 호계 1동 533번지 엘지전자 특허센터, 431-080 Gyeonggi-do (KR). 천성덕 (CHUN, Sungduck) [KR/KR]; 경기도 안양시 동안구 호계 1동 533번지 엘지전자 특허센터

터, 431-080 Gyeonggi-do (KR). 박성준 (PARK, Sungjun) [KR/KR]; 경기도 안양시 동안구 호계 1동 533번지 엘지전자 특허센터, 431-080 Gyeonggi-do (KR). 정성훈 (JUNG, Sunghoon) [KR/KR]; 경기도 안양시 동안구 호계 1동 533번지 엘지전자 특허센터, 431-080 Gyeonggi-do (KR).

(74) 대리인: 김용인 (KIM, Yong In) 등; 서울 송파구 잠실동 175-9 현대빌딩 7층 KBK 특허법률사무소, 138-861 Seoul (KR).

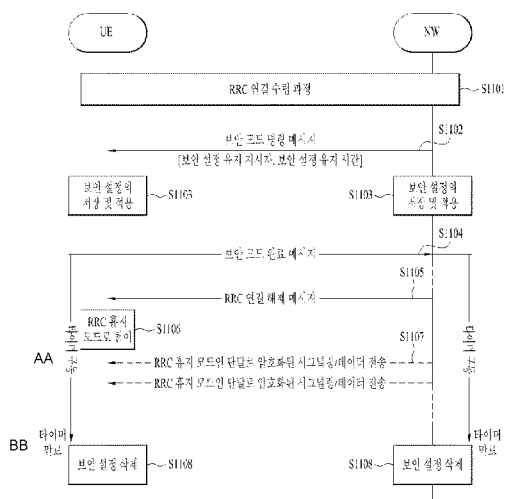
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[다음 쪽 계속]

(54) Title: METHOD FOR USER EQUIPMENT SETTING SECURITY WITH NETWORK IN WIRELESS COMMUNICATION SYSTEM AND APPARATUS FOR SAME

(54) 발명의 명칭: 무선 통신 시스템에서 단말이 네트워크와의 보안 설정 방법 및 이를 위한 장치

[Fig. 11]



- AA ... Timer actuation
BB ... Timer expiration
S1101 ... RRC connection establishment process
S1102 ... Security mode command message [indicator for maintaining security setting, time for maintaining security setting]
S1103 ... Save and apply security setting
S1104 ... Security mode completion message
S1105 ... RRC disconnection message
S1106 ... Shift to RRC resting mode
S1107 ... Transmit encoded data/signal to user equipment in RRC resting mode
S1108 ... Delete security setting

(57) Abstract: In the present invention, a method for a user equipment transmitting/receiving a signal with a network in a wireless communication system is disclosed. More particularly, the method comprises the following steps: receiving security setting information from the network; transmitting or receiving data with the network based on the security setting information; receiving a disconnection message from the network; releasing connection from the network; and actuating a timer when an indicator for maintaining the security setting is received from the network, wherein the security setting information is maintained while the timer is actuated.

(57) 요약서: 본 출원에서는 무선 통신 시스템에서 단말이 네트워크와 신호를 송수신하는 방법이 개시된다. 구체적으로, 상기 네트워크로부터 보안 설정 정보를 수신하는 단계; 상기 보안 설정 정보에 기반하여 상기 네트워크와 데이터를 송신 또는 수신하는 단계; 상기 네트워크로부터 연결 해제 메시지를 수신하는 단계; 상기 네트워크와의 연결을 해제하는 단계; 및 상기 네트워크로부터 보안 설정 유지 지시자를 수신한 경우, 타이머를 구동하는 단계를 포함하고, 상기 타이머가 구동하는 동안 상기 보안 설정 정보를 유지하는 것을 특징으로 한다.

WO 2012/134218 A2



(84) **지정국** (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

- 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

명세서

발명의 명칭: 무선 통신 시스템에서 단말이 네트워크와의 보안 설정 방법 및 이를 위한 장치

기술분야

- [1] 본 발명은 무선 통신 시스템에 관한 것으로서, 보다 상세하게는, 무선 통신 시스템에서 단말이 네트워크와의 보안 설정 방법 및 이를 위한 장치에 관한 것이다.

배경기술

- [2] 본 발명이 적용될 수 있는 무선 통신 시스템의 일례로서 3GPP LTE (3rd Generation Partnership Project Long Term Evolution; 이하 "LTE"라 함) 통신 시스템에 대해 개략적으로 설명한다.
- [3] 도 1은 무선 통신 시스템의 일례로서 E-UMTS 망구조를 개략적으로 도시한 도면이다. E-UMTS(Evolved Universal Mobile Telecommunications System) 시스템은 기존 UMTS(Universal Mobile Telecommunications System)에서 진화한 시스템으로서, 현재 3GPP에서 기초적인 표준화 작업을 진행하고 있다. 일반적으로 E-UMTS는 LTE(Long Term Evolution) 시스템이라고 할 수도 있다. UMTS 및 E-UMTS의 기술 규격(technical specification)의 상세한 내용은 각각 "3rd Generation Partnership Project; Technical Specification Group Radio Access Network"의 Release 7과 Release 8을 참조할 수 있다.
- [4] 도 1을 참조하면, E-UMTS는 단말(User Equipment; UE)과 기지국(eNode B; Enb), 네트워크(E-UTRAN)의 종단에 위치하여 외부 네트워크와 연결되는 접속 게이트웨이(Access Gateway; AG)를 포함한다. 기지국은 브로드캐스트 서비스, 멀티캐스트 서비스 및/또는 유니캐스트 서비스를 위해 다중 데이터 스트림을 동시에 전송할 수 있다.
- [5] 한 기지국에는 하나 이상의 셀이 존재한다. 셀은 1.25, 2.5, 5, 10, 15, 20Mhz 등의 대역폭 중 하나로 설정돼 여러 단말에게 하향 또는 상향 전송 서비스를 제공한다. 서로 다른 셀은 서로 다른 대역폭을 제공하도록 설정될 수 있다. 기지국은 다수의 단말에 대한 데이터 송수신을 제어한다. 하향 링크(Downlink; DL) 데이터에 대해 기지국은 하향 링크 스케줄링 정보를 전송하여 해당 단말에게 데이터가 전송될 시간/주파수 영역, 부호화, 데이터 크기, HARQ(Hybrid Automatic Repeat and reQuest) 관련 정보 등을 알려준다. 또한, 상향 링크(Uplink; UL) 데이터에 대해 기지국은 상향 링크 스케줄링 정보를 해당 단말에게 전송하여 해당 단말이 사용할 수 있는 시간/주파수 영역, 부호화, 데이터 크기, HARQ 관련 정보 등을 알려준다. 기지국간에는 사용자 트래픽 또는 제어 트래픽 전송을 위한 인터페이스가 사용될 수 있다. 핵심망(Core Network; CN)은 AG와 단말의 사용자 등록 등을 위한 네트워크 노드 등으로 구성될 수

있다. AG는 복수의 셀들로 구성되는 TA(Tracking Area) 단위로 단말의 이동성을 관리한다.

- [6] 무선 통신 기술은 WCDMA를 기반으로 LTE까지 개발되어 왔지만, 사용자와 사업자의 요구와 기대는 지속적으로 증가하고 있다. 또한, 다른 무선 접속 기술이 계속 개발되고 있으므로 향후 경쟁력을 가지기 위해서는 새로운 기술 진화가 요구된다. 비트당 비용 감소, 서비스 가용성 증대, 융통성 있는 주파수 밴드의 사용, 단순구조와 개방형 인터페이스, 단말의 적절한 파워 소모 등이 요구된다.

발명의 상세한 설명

기술적 과제

- [7] 상술한 바와 같은 논의를 바탕으로 이하에서는 무선 통신 시스템에서 단말이 네트워크와의 보안 설정 방법 및 이를 위한 장치를 제안하고자 한다.

과제 해결 수단

- [8] 본 발명의 일 실시예인 무선 통신 시스템에서 단말이 네트워크와 신호를 송수신하는 방법은, 상기 네트워크로부터 보안 설정 정보를 수신하는 단계; 상기 보안 설정 정보에 기반하여 상기 네트워크와 데이터를 송신 또는 수신하는 단계; 상기 네트워크로부터 연결 해제 메시지를 수신하는 단계; 상기 네트워크와의 연결을 해제하는 단계; 및 상기 네트워크로부터 보안 설정 유지 지시자를 수신한 경우, 타이머를 구동하는 단계를 포함하고, 상기 타이머가 구동하는 동안 상기 보안 설정 정보를 유지하는 것을 특징으로 한다.
- [9] 여기서, 상기 보안 설정 유지 지시자는 상기 보안 설정 정보 또는 상기 연결 해제 메시지에 포함될 수 있고, 상기 보안 설정 정보 또는 상기 연결 해제 메시지는 보안 유지 시간에 관한 정보를 포함하는 것을 특징으로 한다.
- [10] 나아가, 상기 방법은 상기 네트워크와의 연결을 해제 시 상기 보안 설정 정보를 비활성화하는 단계; 및 보안 설정 활성화 지시자를 포함하는 연결 요청 메시지를 상기 네트워크로 송신하는 단계를 더 포함하는 것을 특징으로 한다. 이 경우, 상기 연결 요청 메시지 송신 시 또는 상기 연결 요청 메시지에 대한 긍정 응답 수신 시, 상기 보안 설정 정보를 활성화하는 것을 특징으로 한다. 여기서, 상기 타이머가 만료되기 전에, 상기 보안 설정 정보를 활성화하는 경우, 상기 타이머를 다시 시작할 수 있다.
- [11] 바람직하게는, 상기 타이머가 만료되거나 또는 상기 네트워크로부터 보안 설정 삭제 지시자를 수신 시, 상기 보안 설정 정보를 삭제하는 단계를 더 포함하는 것을 특징으로 한다.
- [12] 한편, 본 발명의 다른 실시예인 무선 통신 시스템에서 네트워크가 단말과 신호를 송수신하는 방법은, 상기 단말로 보안 설정 정보를 송신하는 단계; 상기 보안 설정 정보에 기반하여 상기 단말과 데이터를 송신 또는 수신하는 단계; 및 상기 단말로 연결 해제 메시지를 송신하는 단계를 포함하고, 상기 보안 설정

정보 또는 상기 연결 해제 메시지에 보안 설정 유지 지시자를 포함하는 것을 특징으로 한다. 또한, 상기 단말과의 연결을 해제하는 단계; 및 타이머를 구동하는 단계를 더 포함하고, 상기 타이머가 구동하는 동안 상기 보안 설정 정보를 유지하는 것을 특징으로 할 수 있다.

- [13] 또한, 상기 방법은, 상기 단말과의 연결을 해제 시 상기 보안 설정 정보를 비활성화하는 단계; 및 보안 설정 활성화 지시자를 포함하는 연결 요청 메시지를 상기 단말로부터 수신하는 단계를 더 포함할 수 있다. 여기서, 상기 연결 요청 메시지 수신 시 또는 상기 연결 요청 메시지에 대한 긍정 응답 송신 시, 상기 보안 설정 정보를 활성화할 수 있다. 또한, 상기 타이머가 만료되기 전에, 상기 보안 설정 정보를 활성화하는 경우, 상기 타이머를 다시 시작하는 것을 특징으로 한다.

- [14] 바람직하게는, 상기 타이머가 만료되거나 또는 상기 단말로 보안 설정 삭제 지시자를 송신 시, 상기 보안 설정 정보를 삭제하는 단계를 더 포함할 수 있다.

발명의 효과

- [15] 본 발명의 실시예에 따르면 무선 통신 시스템에서 단말과 네트워크와의 보안 설정을 위한 시그널링 오버헤드는 효과적으로 감소할 수 있다.
- [16] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [17] 도 1은 무선 통신 시스템의 일례로서 E-UMTS 망구조를 개략적으로 도시한 도면.
- [18] 도 2는 E-UTRAN(Evolved Universal Terrestrial Radio Access Network)의 네트워크 구조를 개념적으로 도시하는 도면.
- [19] 도 3은 3GPP 무선 접속망 규격을 기반으로 한 단말과 E-UTRAN 사이의 무선 인터페이스 프로토콜(Radio Interface Protocol)의 제어평면(Control Plane) 및 사용자평면(User Plane) 구조를 나타내는 도면.
- [20] 도 4는 3GPP 시스템에 이용되는 물리 채널들 및 이들을 이용한 일반적인 신호 전송 방법을 설명하기 위한 도면.
- [21] 도 5는 LTE 시스템에서 사용되는 무선 프레임의 구조를 예시하는 도면.
- [22] 도 6은 호출 메시지를 이용한 일반적인 송수신 방법을 설명하기 위한 도면.
- [23] 도 7은 일반적인 보안 키 생성 과정을 예시하는 도면이다.
- [24] 도 8은 보안 활성화 과정이 성공한 경우를 예시하는 도면이다.
- [25] 도 9는 보안 활성화 과정이 실패한 경우를 예시하는 도면이다.
- [26] 도 10은 MTC(Machine type communication)의 구조를 설명하기 위한 도면.
- [27] 도 11은 본 발명의 제 1 실시예에 따른 신호 송수신 방법을 예시하는 도면이다.
- [28] 도 12는 본 발명의 제 2 실시예에 따른 신호 송수신 방법을 예시하는 도면이다.

- [29] 도 13은 본 발명의 제 3 실시예에 따른 신호 송수신 방법을 예시하는 도면이다.
- [30] 도 14는 본 발명의 제 4 실시예에 따른 신호 송수신 방법을 예시하는 도면이다.
- [31] 도 15는 본 발명의 실시예에 따른 통신 장치의 블록 구성도를 예시한다.

발명의 실시를 위한 형태

- [32] 이하에서 첨부된 도면을 참조하여 설명된 본 발명의 실시예들에 의해 본 발명의 구성, 작용 및 다른 특징들이 용이하게 이해될 수 있을 것이다. 이하에서 설명되는 실시예들은 본 발명의 기술적 특징들이 3GPP 시스템에 적용된 예들이다.
- [33] 본 명세서는 LTE 시스템 및 LTE-A 시스템을 사용하여 본 발명의 실시예를 설명하지만, 이는 예시로서 본 발명의 실시예는 상기 정의에 해당되는 어떤 통신 시스템에도 적용될 수 있다.
- [34] 도 2는 E-UTRAN(Evolved Universal Terrestrial Radio Access Network)의 네트워크 구조를 개념적으로 도시하는 도면이다. 특히 E-UTRAN시스템은 기존 UTRAN시스템에서 진화한 시스템이다. E-UTRAN은 셀(eNB)들로 구성되며, 셀들은 X2 인터페이스를 통해 연결된다. 셀은 무선 인터페이스를 통해 단말과 연결되며, S1 인터페이스를 통해 EPC(Evolved Packet Core)에 연결된다.
- [35] EPC에는 MME(Mobility Management Entity), S-GW(Serving-Gateway) 및 PDN-GW(Packet Data Network-Gateway)로 구성된다. MME는 단말의 접속 정보나 단말의 능력에 관한 정보를 가지고 있으며, 이러한 정보는 단말의 이동성 관리에 주로 사용된다. S-GW는 E-UTRAN을 종단점으로 갖는 게이트웨이이며, PDN-GW는 PDN(Packet Data Network)을 종단점으로 갖는 게이트웨이이다.
- [36] 도 3은 3GPP 무선 접속망 규격을 기반으로 한 단말과 E-UTRAN 사이의 무선 인터페이스 프로토콜(Radio Interface Protocol)의 제어평면(Control Plane) 및 사용자평면(User Plane) 구조를 나타내는 도면이다. 제어평면은 단말(User Equipment; UE)과 네트워크가 호를 관리하기 위해서 이용하는 제어 메시지들이 전송되는 통로를 의미한다. 사용자평면은 애플리케이션 계층에서 생성된 데이터, 예를 들어, 음성 데이터 또는 인터넷 패킷 데이터 등이 전송되는 통로를 의미한다.
- [37] 제 1 계층인 물리계층은 물리채널(Physical Channel)을 이용하여 상위 계층에게 정보 전송 서비스(Information Transfer Service)를 제공한다. 물리계층은 상위에서 매체접속제어(Medium Access Control) 계층과는 전송채널(Transport Channel)을 통해 연결되어 있다. 상기 전송채널을 통해 매체접속제어 계층과 물리계층 사이에 데이터가 이동한다. 송신측과 수신측의 물리계층 사이는 물리채널을 통해 데이터가 이동한다. 상기 물리채널은 시간과 주파수를 무선 자원으로 활용한다. 구체적으로, 물리채널은 하향 링크에서 OFDMA(Orthogonal Frequency Division Multiple Access) 방식으로 변조되고, 상향 링크에서 SC-FDMA(Single Carrier Frequency Division Multiple Access) 방식으로 변조된다.

- [38] 제 2 계층에는 매체접속제어 (Medium Access Control; MAC) 계층, 무선링크제어 (Radio Link Control; RLC) 계층 및 패킷 데이터 수렴 프로토콜(Packet Data Convergence Protocol; PDCP) 계층이 존재한다. 제 2 계층의 MAC 계층은 다양한 논리채널 (Logical Channel)을 다양한 전송채널에 매핑시키는 역할을 하며, 또한 여러 논리채널을 하나의 전송채널에 매핑시키는 논리채널 다중화 (Multiplexing)의 역할을 수행한다. MAC 계층은 상위 계층인 RLC 계층과는 논리채널 (Logical Channel)로 연결되어 있으며, 논리채널은 크게 전송되는 정보의 종류에 따라 제어 평면의 정보를 전송하는 제어채널 (Control Channel)과 사용자 평면의 정보를 전송하는 트래픽채널 (Traffic Channel)로 구분된다.
- [39] 또한, 제 2 계층의 RLC 계층은 상위 계층으로부터 수신한 데이터를 분할 (Segmentation) 및 연결 (Concatenation)하여 하위 계층이 무선 구간으로 데이터를 전송하기에 적합하도록 데이터 크기를 조절하는 역할을 수행한다. 또한, 각각의 무선 베어러 (Radio Bearer; RB)가 요구하는 다양한 QoS(Quality of Service)를 보장할 수 있도록 하기 위해 투명 모드(Transparent Mode, TM), 무응답 모드 (Un-acknowledged Mode, UM), 및 응답 모드 (Acknowledged Mode, AM)의 세가지 동작 모드를 제공하고 있다. 특히, AM RLC는 신뢰성 있는 데이터 전송을 위해 자동 반복 및 요청 (Automatic Repeat and Request; ARQ) 기능을 통한 재전송 기능을 수행하고 있다.
- [40] 마지막으로, 제 2 계층의 PDCP 계층은 IPv4나 IPv6와 같은 IP 패킷 전송 시에 대역폭이 작은 무선 구간에서 효율적으로 전송하기 위하여 상대적으로 크기가 크고 불필요한 제어정보를 담고 있는 IP 패킷 헤더 사이즈를 줄여주는 헤더압축 (Header Compression) 기능을 수행한다. 이는 데이터의 헤더(Header) 부분에서 반드시 필요한 정보만을 전송하도록 하여, 무선 구간의 전송효율을 증가시키는 역할을 한다. 또한, LTE 시스템에서는 PDCP 계층이 보안 (Security) 기능도 수행하는데, 이는 제 3 자의 데이터 감청을 방지하는 암호화(Ciphering)와 제 3 자의 데이터 조작을 방지하는 무결성 보호(Integrity protection)로 구성된다.
- [41] PDCP 계층에서 수행하는 기능은 상술한 바와 같이 헤더 압축, 암호화, 무결성 보호, PDCP 일련번호(Sequence Number) 유지 등 여러 가지가 존재하며, 이들은 RB의 종류에 따라 선택적으로 수행된다.
- [42] 제 3 계층의 무선 자원제어(Radio Resource Control; RRC) 계층은 제어 평면에서만 정의된다. RRC 계층은 무선 베어러(Radio Bearer; RB)들의 설정(Configuration), 재설정(Re-configuration) 및 해제(Release)와 관련되어 논리채널, 전송채널 및 물리채널들의 제어를 담당한다. RB는 단말과 네트워크 간의 데이터 전달을 위해 제2계층에 의해 제공되는 서비스를 의미한다. 이를 위해, 단말과 네트워크의 RRC 계층은 서로 RRC 메시지를 교환한다.
- [43] 무선 베어러 (Radio Bearer; RB)는 제어 평면에서 RRC 메시지를 전송하는데 사용되는 SRB (Signaling Radio Bearer)와 사용자 평면에서 사용자 데이터를

전송하는데 사용되는 DRB (Data Radio Bearer) 두 가지로 크게 구분할 수 있으며, 이 중 DRB는 사용하는 RLC의 동작 방식에 따라 UM RLC를 사용하는 UM DRB와 AM RLC를 사용하는 AM DRB로 구분될 수 있다.

- [44] 이하 단말의 RRC 상태와 RRC 연결 방법에 대해 설명한다. RRC 상태란 단말의 RRC가 E-UTRAN의 RRC와 논리적 연결(logical connection)이 되어 있는지 여부를 말하며, 연결되어 있는 경우는 RRC 연결 상태(RRC_CONNECTED), 연결되어 있지 않은 경우는 RRC 휴지 상태(RRC_IDLE)라고 부른다.
- [45] E-UTRAN은 RRC 연결 상태의 단말의 존재를 셀 단위에서 파악할 수 있기 때문에 단말을 효과적으로 제어할 수 있다. 반면에 E-UTRAN은 RRC 휴지 상태의 단말을 셀 단위에서 파악할 수 없으며, 셀 보다 더 큰 지역 단위인 TA 단위로 CN이 관리한다. 즉, RRC 휴지 상태의 단말이 셀로부터 음성이나 데이터와 같은 서비스를 받기 위해서는 RRC 연결 상태로 상태 천이하여야 한다.
- [46] 특히 사용자가 단말의 전원을 맨 처음 켜었을 때, 단말은 먼저 적절한 셀을 탐색한 후 해당 셀에서 RRC 휴지 상태에 머무른다. RRC 휴지 상태에 머물러 있던 단말은 RRC 연결을 맺을 필요가 있는 경우에만 비로소 E-UTRAN의 RRC와 RRC 연결 설정 (RRC connection establishment) 과정을 수행하여 RRC 연결 상태로 천이한다. 여기서 RRC 연결을 맺을 필요가 있는 경우란 사용자의 통화 시도 등의 이유로 상향 데이터 전송이 필요하다거나, E-UTRAN으로부터 페이지징 메시지를 수신한 경우 이에 대한 응답 메시지를 전송해야 하는 경우 등을 들 수 있다.
- [47] 한편, RRC 계층의 상위에 있는 NAS(Non-Access Stratum) 계층은 세션 관리(Session Management)와 이동성 관리(Mobility Management) 등의 기능을 수행한다. NAS 계층에서는 단말의 이동성 관리를 위하여 EMM(EPS Mobility Management) 등록 상태(EMM-REGISTERED) 및 EMM 미등록 상태(EMM-UNREGISTERED) 두 가지 상태가 정의되어 있으며, 이 두 상태는 단말과 MME에 적용된다. 초기 단말은 EMM 미등록 상태이며, 이 단말이 네트워크에 접속하기 위해서 초기 접속(Initial Attach) 절차를 통해서 해당 네트워크에 등록하는 과정을 수행한다. 접속 절차가 성공적으로 수행되면 단말 및 MME는 EMM 등록 상태가 된다.
- [48] 또한 NAS 계층에서는 단말과 EPC 간 시그널링 연결(signaling connection)을 관리하기 위하여 ECM(EPS Connection Management) 휴지 상태(ECM_IDLE) 및 ECM 연결 상태(ECM_CONNECTED) 두 가지가 정의되어 있으며, 이 두 상태는 단말 및 MME에게 적용된다. ECM 휴지 상태의 단말이 E-UTRAN과 RRC 연결을 맺으면 해당 단말은 ECM 연결 상태가 된다. ECM 휴지 상태에 있는 MME는 E-UTRAN과 S1 연결을 맺으면 ECM 연결 상태가 된다.
- [49] 단말이 ECM 휴지 상태에 있을 때에는 E-UTRAN은 단말의 정보(context)를 가지고 있지 않다. 따라서 ECM 휴지 상태의 단말은 네트워크의 명령을 받을 필요 없이 셀 선택 또는 셀 재선택 절차와 같은 단말 기반의 이동성 관련 절차를

수행한다. 반면 단말이 ECM 연결 상태에 있을 때에는 단말의 이동성은 네트워크의 명령에 의해서 관리된다. ECM 휴지 상태에서 단말의 위치가 네트워크가 알고 있는 위치와 달라질 경우 단말은 TA 갱신(Tracking Area Update) 절차를 통해 네트워크에 단말의 해당 위치를 알린다.

- [50] LTE 시스템에서 기지국(eNB)을 구성하는 하나의 셀은 1.25, 2.5, 5, 10, 15, 20Mhz 등의 대역폭 중 하나로 설정되어 여러 단말에게 하향 또는 상향 전송 서비스를 제공한다. 서로 다른 셀은 서로 다른 대역폭을 제공하도록 설정될 수 있다.
- [51] 네트워크에서 단말로 데이터를 전송하는 하향 전송채널은 시스템 정보를 전송하는 BCH(Broadcast Channel), 페이징 메시지를 전송하는 PCH(Paging Channel), 사용자 트래픽이나 제어 메시지를 전송하는 하향 SCH(Shared Channel) 등이 있다. 하향 멀티캐스트 또는 방송 서비스의 트래픽 또는 제어 메시지의 경우 하향 SCH를 통해 전송될 수도 있고, 또는 별도의 하향 MCH(Multicast Channel)을 통해 전송될 수도 있다.
- [52] 한편, 단말에서 네트워크로 데이터를 전송하는 상향 전송채널로는 초기 제어 메시지를 전송하는 RACH(Random Access Channel), 사용자 트래픽이나 제어 메시지를 전송하는 상향 SCH(Shared Channel)가 있다. 전송채널의 상위에 있으며, 전송채널에 매핑되는 논리채널(Logical Channel)로는 BCCH(Broadcast Control Channel), PCCH(Paging Control Channel), CCCH(Common Control Channel), MCCH(Multicast Control Channel), MTCH(Multicast Traffic Channel) 등이 있다.
- [53] 도 4는 3GPP 시스템에 이용되는 물리 채널들 및 이들을 이용한 일반적인 신호 전송 방법을 설명하기 위한 도면이다.
- [54] 단말은 전원이 켜지거나 새로이 셀에 진입한 경우 기지국과 동기를 맞추는 등의 초기 셀 탐색(Initial cell search) 작업을 수행한다(S401). 이를 위해, 단말은 기지국으로부터 주 동기 채널(Primary Synchronization Channel; P-SCH) 및 부 동기 채널(Secondary Synchronization Channel; S-SCH)을 수신하여 기지국과 동기를 맞추고, 셀 ID 등의 정보를 획득할 수 있다. 그 후, 단말은 기지국으로부터 물리 방송 채널(Physical Broadcast Channel)을 수신하여 셀 내 방송 정보를 획득할 수 있다. 한편, 단말은 초기 셀 탐색 단계에서 하향 링크 참조 신호(Downlink Reference Signal; DL RS)를 수신하여 하향 링크 채널 상태를 확인할 수 있다.
- [55] 초기 셀 탐색을 마친 단말은 물리 하향 링크 제어 채널(Physical Downlink Control Channel; PDCCH) 및 상기 PDCCH에 실린 정보에 따라 물리 하향 링크 공유 채널(Physical Downlink Control Channel; PDSCH)을 수신함으로써 좀더 구체적인 시스템 정보를 획득할 수 있다(S402).
- [56] 한편, 기지국에 최초로 접속하거나 신호 전송을 위한 무선 자원이 없는 경우 단말은 기지국에 대해 임의 접속 과정(Random Access Procedure; RACH)을 수행할 수 있다(단계 S403 내지 단계 S406). 이를 위해, 단말은 물리 임의 접속

- 채널(Physical Random Access Channel; PRACH)을 통해 특정 시퀀스를 프리앰블로 전송하고(S403), PDCCH 및 대응하는 PDSCH를 통해 프리앰블에 대한 응답 메시지를 수신할 수 있다(S404). 경쟁 기반 RACH의 경우, 추가적으로 충돌 해결 절차(Contention Resolution Procedure)를 수행할 수 있다.
- [57] 상술한 바와 같은 절차를 수행한 단말은 이후 일반적인 상/하향 링크 신호 전송 절차로서 PDCCH/PDSCH 수신(S407) 및 물리 상향 링크 공유 채널(Physical Uplink Shared Channel; PUSCH)/물리 상향 링크 제어 채널(Physical Uplink Control Channel; PUCCH) 전송(S408)을 수행할 수 있다. 특히 단말은 PDCCH를 통하여 하향링크 제어 정보(Downlink Control Information; DCI)를 수신한다. 여기서 DCI는 단말에 대한 자원 할당 정보와 같은 제어 정보를 포함하며, 그 사용 목적에 따라 포맷이 서로 다르다.
- [58] 한편, 단말이 상향 링크를 통해 기지국에 전송하는 또는 단말이 기지국으로부터 수신하는 제어 정보는 하향 링크/상향 링크 ACK/NACK 신호, CQI(Channel Quality Indicator), PMI(Precoding Matrix Index), RI(Rank Indicator) 등을 포함한다. 3GPP LTE 시스템의 경우, 단말은 상술한 CQI/PMI/RI 등의 제어 정보를 PUSCH 및/또는 PUCCH를 통해 전송할 수 있다.
- [59] 도 5는 LTE 시스템에서 사용되는 무선 프레임의 구조를 예시하는 도면이다.
- [60] 도 5를 참조하면, 무선 프레임(radio frame)은 10ms($327200 \times T_s$)의 길이를 가지며 10개의 균등한 크기의 서브프레임(subframe)으로 구성되어 있다. 각각의 서브프레임은 1ms의 길이를 가지며 2개의 슬롯(slot)으로 구성되어 있다. 각각의 슬롯은 0.5ms($15360 \times T_s$)의 길이를 가진다. 여기에서, T_s 는 샘플링 시간을 나타내고, $T_s = 1/(15\text{kHz} \times 2048) = 3.2552 \times 10^{-8}$ (약 33ns)로 표시된다. 슬롯은 시간 영역에서 복수의 OFDM 심볼을 포함하고, 주파수 영역에서 복수의 자원블록(Resource Block; RB)을 포함한다. LTE 시스템에서 하나의 자원블록은 12개의 부반송파 $\times$ 7(6)개의 OFDM 심볼을 포함한다. 데이터가 전송되는 단위시간인 TTI(Transmission Time Interval)는 하나 이상의 서브프레임 단위로 정해질 수 있다. 상술한 무선 프레임의 구조는 예시에 불과하고, 무선 프레임에 포함되는 서브프레임의 수 또는 서브프레임에 포함되는 슬롯의 수, 슬롯에 포함되는 OFDM 심볼의 수는 다양하게 변경될 수 있다.
- [61] 도 6은 호출 메시지를 이용한 일반적인 송수신 방법을 설명하기 위한 도면이다.
- [62] 도 6을 참조하여 설명하면, 호출 메시지는 호출 이유(Paging Cause)와 단말 식별자(UE Identity) 등으로 구성된 호출 기록(Paging record)을 포함한다. 상기 호출 메시지를 수신할 때, 단말은 전력소비 감소를 목적으로 불연속 수신 주기(Discontinuous Reception; DRX)를 수행할 수 있다.
- [63] 구체적으로, 망은 호출 주기(Paging DRX Cycle)라 불리는 시간 주기마다 여러 개의 호출 기회 시간(Paging Occasion; PO)을 구성하고, 특정 단말은 특정 호출 기회 시간만을 수신하여 호출 메시지를 획득할 수 있도록 한다. 상기 단말은 상기 특정 호출 기회 시간 이외의 시간에는 호출 채널을 수신하지 않으며 전력

소비를 줄이기 위해 수면 상태에 있을 수 있다. 하나의 호출 기회 시간은 하나의 TTI에 해당된다.

- [64] 기지국과 단말은 호출 메시지의 전송을 알리는 특정 값으로 호출 지시자(Paging Indicator; PI)를 사용한다. 기지국은 PI의 용도로 특정 식별자(예, Paging - Radio Network Temporary Identity; P-RNTI)를 정의하여 단말에게 호출 정보 전송을 알릴 수 있다. 일 예로, 단말은 DRX 주기마다 깨어나서 호출 메시지의 출현 여부를 알기 위해 하나의 서브 프레임을 수신한다. 단말은 수신한 서브 프레임의 L1/L2 제어채널(PDCCH)에 P-RNTI가 있다면, 해당 서브 프레임의 PDSCH에 호출 메시지가 있다는 것을 알 수 있다. 또한, 호출 메시지에 자신의 단말식별자(예, IMSI)가 있다면 단말은 기지국에 응답(예를 들어, RRC 연결 또는 시스템 정보 수신)하여 서비스를 받게 된다.
- [65] 다음은, 시스템 정보(System Information)에 관한 설명이다. 시스템 정보는 단말이 기지국에 접속하기 위해서 알아야 하는 필수 정보를 포함한다. 따라서 단말은 기지국에 접속하기 전에 시스템 정보를 모두 수신하고 있어야 하고, 또한 항상 최신의 시스템 정보를 가지고 있어야 한다. 그리고 시스템 정보는 한 셀 내의 모든 단말이 알고 있어야 하는 정보이므로, 기지국은 주기적으로 시스템 정보를 전송한다.
- [66] 시스템 정보는 MIB(Master Information Block), SB(Scheduling Block) 및 SIB(System Information Block)로 구분될 수 있다. MIB는 단말이 해당 셀의 물리적 구성, 예를 들어 대역폭을 알 수 있도록 한다. SB는 SIB들의 전송정보, 예를 들어, 전송 주기 등을 알려준다. SIB는 서로 관련 있는 시스템 정보의 집합체이다. 예를 들어, 특정 SIB는 주변의 셀의 정보만을 포함하고, 다른 SIB는 단말이 사용하는 상향 무선 채널의 정보만을 포함한다.
- [67] 기지국은 단말에게 시스템 정보의 변경 여부를 알려주기 위해서, 호출 메시지를 전송한다. 이 경우, 호출메시지는 시스템 정보 변경 지시자를 포함한다. 단말은 호출 주기에 따라 호출 메시지를 수신하여, 만일 호출 메시지가 상기 시스템 정보 변경 지시자를 포함할 경우, 논리채널인 BCCH를 통해 전송되는 시스템 정보를 수신한다.
- [68] 이하 셀 선택 및 셀 재선택 과정에 대해 설명한다.
- [69] 단말의 전원이 켜지면 단말은 적절한 품질의 셀을 선택하여 서비스를 받기 위한 준비 절차들을 수행해야 한다. RRC 휴지 상태에 있는 단말은 항상 적절한 품질의 셀을 선택하여 이 셀을 통해 서비스를 제공받기 위한 준비를 하고 있어야 한다. 예를 들어, 전원이 막 켜진 단말은 네트워크에 등록을 하기 위해 적절한 품질의 셀을 선택해야 한다. RRC 연결 상태에 있던 단말이 RRC 휴지 상태에 진입하면, 이 단말은 RRC 휴지 상태에서 머무를 셀을 선택해야 한다. 이와 같이, 단말이 RRC 휴지 상태와 같은 서비스 대기 상태로 머물고 있기 위해서 특정 조건을 만족하는 셀을 고르는 과정을 셀 선택 (Cell Selection)이라고 한다. 중요한 점은, 셀 선택은 단말이 RRC 휴지 상태로 머물러 있을 셀을 현재 결정하지 못한

상태에서 수행하는 것이므로, 가능한 신속하게 셀을 선택하는 것이 무엇보다 중요하다. 따라서 일정 기준 이상의 무선 신호 품질을 제공하는 셀이라면, 비록 이 셀이 단말에게 가장 좋은 무선 신호 품질을 제공하는 셀이 아니라고 하더라도, 단말의 셀 선택 과정에서 선택될 수 있다.

[70] 셀 선택 기준을 만족하는 셀을 단말이 고르면, 단말은 해당 셀의 시스템 정보로부터 해당 셀에서 단말의 RRC 휴지 상태에서의 동작에 필요한 정보를 수신한다. 단말이 RRC 휴지 상태에서의 동작에 필요한 모든 정보를 수신한 후, 망으로 서비스를 요청하거나 망으로부터 서비스를 받기 위하여 RRC 휴지 상태에서 대기한다.

[71] 단말이 일단 셀 선택 과정을 통해 어떤 셀을 선택한 이후, 단말의 이동성 또는 무선 환경의 변화 등으로 단말과 기지국간의 신호의 세기나 품질이 바뀔 수 있다. 따라서 만약 선택한 셀의 품질이 저하되는 경우, 단말은 더 좋은 품질을 제공하는 다른 셀을 선택할 수 있다. 이렇게 셀을 다시 선택하는 경우, 일반적으로 현재 선택된 셀보다 더 좋은 신호 품질을 제공하는 셀을 선택한다. 이런 과정을 셀 재선택(Cell Reselection)이라고 한다. 셀 재선택 과정은, 무선 신호의 품질 관점에서, 일반적으로 단말에게 가장 좋은 품질을 제공하는 셀을 선택하는데 기본적인 목적이 있다. 무선 신호의 품질 관점 이외에, 네트워크는 주파수 별로 우선 순위를 결정하여 단말에게 알릴 수 있다. 이러한 우선 순위를 수신한 단말은, 셀 재선택 과정에서 이 우선 순위를 무선 신호 품질 기준보다 우선적으로 고려하게 된다.

[72] 이하, RRC 연결 과정에 관하여 보다 상세히 설명한다.

[73] RRC 연결 수립(connection establishment) 과정은 SRB1의 수립을 포함한다. E-UTRAN은 S1 연결 수립 완료에 앞서, 즉 EPC로부터 UE 컨텍스트 정보 수신에 앞서, RRC 연결 수립 과정을 완료한다. 결과적으로, RRC 연결의 초기 단계에서는 AS 계층 보안이 활성화되지 않는다. RRC 연결의 초기 단계에서 E-UTRAN은 단말로 하여금 측정 보고를 수행하도록 설정할 뿐이며, 단말은 보안 활성화가 이루어진 후에야 비로소 핸드오버 메시지를 송수신할 수 있다.

[74] EPC로부터 UE 컨텍스트 정보 수신한 후, E-UTRAN은 초기 보안 설정 활성화 과정을 통하여 암호화(ciphering) 및 무결성 검사(integrity protection)를 위한 보안 설정을 활성화한다. 보안 설정을 활성화하기 위한 RRC 메시지는 무결성 검사의 대상 일뿐, 암호화는 상기 보안 설정 활성화 과정 완료 후에야 적용될 수 있다. 즉, 보안 활성화에 대한 응답 메시지는 무결성 검사만 적용되고, 이후 SRB2 및 DRB 수립을 위한 메시지들은 암호화와 무결성 검사 모두가 적용된다.

[75] 초기 보안 설정 활성화 과정 완료 후, E-UTRAN은 SRB2 및 DRB 수립을 위한 과정을 개시한다. 즉, E-UTRAN은 단말로부터 초기 보안 활성화에 대한 확인 메시지를 수신하기 이전에 SRB2 및 DRB 수립을 위한 과정을 수행한다. 이와 같은 경우, E-UTRAN은 SRB2 및 DRB 수립을 위한 RRC 연결 재설정 메시지에 암호화와 무결성 검사 모두를 적용한다. 한편, E-UTRAN은 초기 보안 활성화가

실패하거나 RB 수립이 실패한 경우, RRC 연결을 해제한다. 다시 말해, E-UTRAN은 보안 활성화 이전에 SRB2 및 DRB를 수립하지 않는다.

[76] 이하, 보안(Security)에 관하여 설명한다. 도 7은 일반적인 보안 키 생성 과정을 예시하는 도면이다.

[77] 도 7을 참조하면, MME는 HE(Home environment)에게 인증 벡터(authentication vectors)를 요청함으로써 AKA(Authentication and Key Agreement) 과정을 개시한다. HE는 기본 키(base-key) K_{ASME} 를 포함하는 인증 벡터를 상기 MME로 응답한다. 따라서, AKA 과정의 결과, EPC와 UE, 즉 단말은 K_{ASME} 를 공유할 수 있다. K_{ASME} 로부터 NAS 키들과 K_{eNB} 및 NH(Next Hop) 등의 파라미터들이 생성된다. K_{ASME} 는 EPC 외부의 엔티티로 전달되지 않지만, 단말이 ECM-CONNECTED 모드로 천이하는 경우 K_{eNB} 및 NH는 EPC로부터 eNB로 전달될 수 있다. eNB와 UE는 K_{eNB} 로부터 UP(User Plain) 키들 및 RRC 키들을 생성할 수 있다. UP(User Plain) 키들 및 RRC 키들은 핸드오버 시 갱신될 수 있다.

[78] K_{eNB} *는 타겟 PCI(Physical Cell ID), 타겟 주파수 및 K_{eNB} , 또는 타겟 PCI, 타겟 주파수 및 NH 중 하나의 조합으로부터 UE와 소스 eNB에 의하여 생성될 수 있다. 이후, K_{eNB} *는 타겟 셀에서 RRC 및 UP 트래픽을 위하여 사용되는 새로운 K_{eNB} 를 지칭한다. 단말이 ECM-IDLE 모드로 천이한 경우, 모든 키들은 eNB로부터 삭제된다.

[79] AS 계층의 보안은 SRB에서의 RRC 시그널링에 대한 무결성 검사와 함께 SRB에서의 RRC 시그널링 및 DRB에서의 사용자 데이터에 대한 암호화를 포함한다. RRC 계층은 AS 설정의 일부인 보안 설정을 제어한다. 여기서, 보안 설정은, 무결성 검사 알고리즘, 암호화 알고리즘과 함께, 'keyChangeIndicator' 및 'nextHopChainingCount'와 같은 2개의 파라미터를 포함한다. 상기 보안 설정은 단말이 핸드오버 및/또는 RRC 연결 재수립 과정에서 AS 계층 보안 키를 결정 시 사용된다. 한편, 무결성 검사 알고리즘은 SRB1 및 SRB2에 공통되며, 암호화 알고리즘은 모든 RB, 즉 SRB1, SRB2 및 DRB 모두에 공통된다.

[80] 보다 구체적으로, AS 계층은 3개의 서로 다른 보안 키, 즉 RRC 시그널링의 무결성 검사를 위한 키 K_{RRCint} , RRC 시그널링의 암호화를 위한 키 K_{RRCenc} 및 사용자 데이터의 암호화를 위한 키 K_{UPenc} 를 적용한다. 상기 3개의 보안 키 모두 K_{eNB} 로부터 생성된다. RRC 연결이 수립되면 K_{eNB} 로부터 새로운 AS 계층 보안 키들이 생성되기 때문에, 상기 키 생성을 위한 새로운 인자는 불필요하다.

[81] 핸드오버 수행을 위한 RRC 메시지의 무결성 검사 및 암호화는 핸드오버 수행 이전에 사용 중인 보안 설정에 기반하여 소스 eNB에 의하여 수행된다. 무결성 검사 알고리즘 및 암호화 알고리즘은 핸드오버 수행 이후에만 변경될 수 있으며, 상기 4개의 AS 계층 보안 키, 즉 K_{eNB} , K_{RRCint} , K_{RRCenc} 및 K_{UPenc} 는 핸드오버 및 RRC 연결 재수립 시 마다 변경된다.

[82] 상기 'keyChangeIndicator'는 핸드오버 시 사용되며, 단말이 가장 최근의 가용 K_{ASME} 키와 관련된 보안 키들을 사용하는지 여부를 지시한다. 또한,

‘nextHopChainingCount’는 핸드오버 및 RRC 연결 재수립 시 단말에 의하여 새로운 K_{eNB} 생성 시 사용된다. 인트라 셀 핸드오버 과정은 RRC 연결 모드에서 상기 보안 키들을 변경하기 위하여 사용될 수 있다.

[83] 한편, RRC 연결 모드에서 RRC 휴지 모드로 천이하는 경우, eNB는 RRC 휴지 모드인 단말의 보안 키들을 삭제하고, 단지 MME에만 저장하게 된다. 즉, eNB와 UE는 NH , K_{eNB} , $K_{RRCCenc}$, K_{RRCint} 및 K_{UPenc} 등을 삭제하지만, MME와 UE는 K_{ASME} , K_{NASint} 및 K_{NASenc} 를 저장한다.

[84] 이하, 초기 보안 활성화 과정에 관하여 구체적으로 설명한다.

[85] 도 8은 보안 활성화 과정이 성공한 경우를 예시하는 도면이고, 도 9는 보안 활성화 과정이 실패한 경우를 예시하는 도면이다.

[86] 도 8 및 도 9를 참조하면, E-UTRAN은 단계 801 및 단계 901과 같이 RRC 연결 모드에 있는 단말에게 보안 모드 명령(security mode command) 메시지를 송신함으로써 보안 활성화 과정을 개시한다. 상술한 바와 같이, 이 과정은 SRB1만이 수립된 경우로서 SRB2 및 DRB 수립 이전의 과정이다.

[87] 단계 801 및 단계 901과 같이 보안 모드 명령(security mode command) 메시지를 수신하면, 상기 단말은 K_{eNB} 키를 생성한다. 또한, 상기 보안 모드 명령 메시지가 지시하는 무결성 검사 알고리즘과 연관된 K_{RRCint} 키를 생성한다.

[88] 이후, 하위 계층으로 상기 무결성 검사 알고리즘과 K_{RRCint} 키를 이용한 상기 보안 모드 명령 메시지의 무결성 검사를 지시한다. 만약, 상기 보안 모드 명령 메시지의 무결성 검사가 성공한 경우, 상기 보안 모드 명령 메시지가 지시하는 암호화 알고리즘과 연관된 $K_{RRCCenc}$ 키 및 K_{UPenc} 키를 생성한다.

[89] 이후, 하위 계층으로 하여금 보안 모드 완료 메시지를 포함한 이후의 RRC 메시지들에 대하여 상기 무결성 검사 알고리즘과 K_{RRCint} 키를 이용한 무결성 검사를 수행하도록 지시하며, 동시에 암호화 알고리즘과 $K_{RRCCenc}$ 키 및 K_{UPenc} 키를 이용한 암호화 과정을 적용하도록 설정한다.

[90] 이와 같은 과정이 완료된 후, 상기 AS 계층 보안이 활성화된 것으로 간주하며, 단계 802와 같이 네트워크로 보안 모드 완료 메시지를 송신하여 보안 활성화 과정을 종료한다.

[91] 반면에, 상기 보안 모드 명령 메시지의 무결성 검사가 실패한 경우, 보안 모드 명령 메시지 수신 이전에 사용되는 설정을 이용하게 된다. 또한, 단계 902와 같이 네트워크로 보안 모드 실패 메시지를 송신하여 보안 활성화 과정을 종료한다.

[92] 이하 MTC(Machine type communication)에 대해 설명한다.

[93] MTC란 사람의 개입 없이 기계(Machine)와 기계 사이에 통신이 이루어지는 것을 의미하며, MTC에 사용되는 단말이 MTC 기기(MTC device)이다. MTC는 다른 말로 M2M(Machine to Machine)으로도 불린다. MTC를 통해 제공되는 서비스는 기존의 사람이 개입하는 통신에서의 서비스와는 차별성을 가지며, 다음과 같은 다양한 범주의 서비스가 존재한다. 예를 들면, 추적(Tracking), 계량(Metering), 지불 시스템(Payment), 의료 분야 서비스, 원격 조정 등의

서비스가 MTC에서 제공된다.

- [94] 도 10은 MTC(Machine type communication)의 구조를 설명하기 위한 도면이다.
- [95] MTC 기기는 다른 MTC 기기나 MTC 서버와 이동 통신망을 통해서 통신을 한다. 상기 MTC 서버는 도 10과 같이 MTC 기기를 통해서 제공되는 서비스인 계량, 도로 정보, 사용자 전자 장치 조정 등을 MTC 사용자(User)에게 제공할 수 있다.
- [96] 상기 MTC 서비스를 효율적으로 지원하기 위해서, MTC 기기의 적은 움직임(low mobility), 지연 내성(Delay tolerant), 짧은 데이터 전송(Short data transmission)등과 같은 특성을 고려해 볼 수 있다. 이와 같은 이유로, 상기 MTC 기기는 지연 내성 접속(Delay tolerant access) 지원 단말이라고 지칭할 수도 있다. 또한, 수많은 MTC 기기들이 하나의 셀 내에 존재할 수 있다는 것을 가정할 수 있다.
- [97] 종래 기술에 따르면, RRC 연결 모드에서 RRC 휴지 모드로 천이하는 경우, eNB는 저장하고 있던 보안 키(security key)들을 삭제한다. 따라서, RRC 휴지 모드의 단말을 위한 정보들은 오직 MME에서만 유지될 수 있다. 즉, eNB는 단말의 상태 정보를 더 이상 저장하지 않고 메모리에 저장된 현재 보안 키들을 삭제하는 것으로 가정할 수 있다. 특히, RRC 휴지 모드로 천이하는 경우, eNB와 단말은 NH, KeNB, KRRCenc, KRRCint 및 KUPenc를 삭제하며, MME와 단말은 KASME, KNASint and KNASenc만을 저장하게 된다.
- [98] 반면에, 단말이 전용 채널 상에서 데이터를 송수신하기 위하여 RRC 연결 모드로 들어가고, 데이터 송수신 완료 이후 RRC 휴지 모드로 다시 천이할 수 있다. 이와 같은 경우, MTC 단말의 경우와 같이 짧은 데이터를 순간적으로 전송하는 경우에는, 보안 과정은 데이터 송수신을 위하여 활성화되기 때문에, 단말은 RRC 연결 수립 과정 이후 또 다시 보안 설정을 수행하여야 한다. 따라서, MTC 단말의 경우 데이터 전송 시마다 매번 보안 설정을 수행하여야 하는 오버헤드가 발생할 수 있다. 즉, MTC 기기와 같이, 아주 가끔 짧은 데이터만을 전송하는 단말에게 있어서는, 데이터 양에 비해 보안 활성화로 인한 시그널링 오버헤드가 훨씬 큰 문제점이 발생한다.
- [99] 따라서, RRC 연결 시 보안 활성화로 인하여 시그널링 오버헤드를 줄이기 위해서, 본 발명은, 단말은 네트워크와 RRC 연결을 설정하며, 네트워크로부터 수신한 보안 설정 메시지를 기반으로 보안 설정을 수행한다. 이후, 단말이 네트워크와의 RRC 연결을 해제하고 RRC 휴지 모드로 천이한 경우, 일정 시간 동안 상기 보안 설정을 유지하는 것을 제안한다.
- [100] 또한, RRC 휴지 모드에 있는 단말은 보안 활성화 지시자를 포함하는 RRC 연결 요청 메시지나 RRC 연결 셋업 완료 메시지를 송신하여, 별도의 보안 설정 메시지 없이, 상기 유지하고 있는 보안 설정을 이용하여 다른 RRC 연결을 수립할 수 있다.
- [101] 바람직하게는, 단말은 네트워크로부터 보안 설정 유지 지시자를 수신할 수

있다. 여기서, 상기 보안 설정 유지 지시자는 RRC 연결 셋업 메시지 또는 RRC 연결 해제 메시지에 포함될 수 있다. 즉, 네트워크, 즉 eNB은 RRC 연결 셋업 메시지 또는 다른 하향링크 RRC 메시지를 통해 상기 단말과 설정한 보안 설정을 계속 저장할 것인지, 또는 사용할 것인지, 또는 활성화할 것인지 여부를 알려준다.

- [102] 한편, 단말은 보안 모드 명령(Security Mode Command) 메시지 또는 RRC 연결 재설정(connection reconfiguration) 메시지 중 적어도 하나를 통하여 상기 보안 설정 메시지를 수신할 수 있다. 네트워크로부터 상기 보안 설정 메시지를 수신할 때, 단말은 상기 보안 설정 정보를 RRC 휴지 모드에서 저장해야 하는지 여부에 관한 정보 및 보안 설정 유지 시간에 관한 정보도 함께 수신할 수 있다.
- [103] 만약, 단말이 RRC 휴지 모드로 천이한 경우, eNB와 단말은 보안 설정 유지 시간 동안 상기 보안 설정을 저장할 수 있다. 즉, 보안 설정 유지 시간에 관한 정보를 수신한 단말은, 보안 설정 정보를 수신할 때 또는 RRC 연결을 해제할 때 상기 보안 설정 유지 시간을 위한 타이머를 시작하고, RRC 연결 해제 후에도 상기 타이머가 구동하는 동안에는 보안 설정을 유지하며, 타이머가 만료되면 저장한 보안 설정을 제거한다.
- [104] 물론, RRC 연결 모드 또는 RRC 휴지 모드 단말 모두에 있어, 단말은 하나의 셀로부터 상기 보안설정 정보를 수신하여 저장하고, 다른 셀로 이동한 경우 타이머 만료 여부와 무관하게 저장한 보안설정 정보를 제거할 수 있다.
- [105] 한편, 보안 설정은 네트워크로부터 수신한 상기 보안 설정 메시지를 이용하여 (AS 계층에서 사용하는) 암호화 알고리즘을 획득하고 암호화 키를 생성하는 과정을 포함할 수 있다. 결과적으로, 하나 이상의 RB에 대하여 암호화(또는 무결성 검사) 등을 적용할 수 있다.
- [106] 물론, 네트워크로부터 상기 보안 설정의 삭제를 지시받은 경우에는, 타이머 만료 여부와 무관하게, 단말은 유지하고 있는 보안 설정을 삭제할 수 있다.
- [107] 도 11은 본 발명의 제 1 실시예에 따른 신호 송수신 방법을 예시하는 도면이다.
- [108] 도 11을 참조하면, RRC 휴지 모드인 단말과 네트워크는 단계 1101과 같이 RRC 연결 수립(RRC Connection Establishment) 과정을 수행하여, RRC 연결 모드로 들어간다.
- [109] 이후, 단말은 네트워크로부터 단계 1102와 같이 보안 모드 명령 메시지를 수신할 수 있다. 상기 보안 모드 명령 메시지는 보안 설정 유지 지시자 및 보안 설정 유지 시간에 관한 정보를 포함할 수 있다. 특히, 보안 설정 유지 지시자는 단말이 RRC 휴지 모드로 천이한 후 현재의 보안 설정의 저장 및 유지 여부를 지시할 수 있다.
- [110] 상기 보안 모드 명령 메시지를 수신한 단말은, 상기 보안 모드 명령 메시지에 포함된 보안 설정 정보를 저장한다. 이후, 상기 보안 설정 정보가 지시하는 암호화 알고리즘을 이용하여 하나 이상의 보안 키를 생성할 수 있다. 따라서, 단말은 단계 1103과 같이 DCCH를 위한 SRB 및 DTCH를 위한 DRB에 대하여

상기 보안 키를 이용한 암호화 및 보안 설정을 적용한다.

- [111] 또한, 단말은 보안 설정 유지 시간에 대응하는 타이머를 개시할 수 있다. 상기 타이머가 구동하는 동안, 단말은 상기 보안 설정 및 보안 키를 저장하고 유지할 수 있다. 물론, 네트워크도 보안 설정 유지 시간에 대응하는 타이머를 개시하며, 상기 타이머가 구동하는 동안, 네트워크 또한 C-RNTI, IMSI, TMSI 등을 단말 식별자와 같이 상기 보안 설정 및 보안 키를 저장하고 유지할 수 있다. 보안 활성화를 성공한 경우, 단말은 단계 1104에서 네트워크로 보안 모드 완료 메시지를 송신한다.
- [112] 계속하여, 단말이 네트워크로부터 단계 1105와 같이 RRC 연결 해제 메시지를 수신하면, 단말은 단계 1106와 같이 바로 RRC 휴지 모드로 천이한다. 그러나, 본 발명에 따르면 단말은 타이머가 만료하기 까지 상기 보안 설정과 보안 키 등을 저장하고 유지할 수 있다. 한편, 단말과 네트워크는 RRC 연결 해제 메시지 수신 시, 상기 타이머를 재시작하는 것으로 구현할 수도 있다.
- [113] 이후, 단말은 단계 1107과 같이 네트워크로부터 암호화된 시그널링 또는 암호화된 데이터를 수신하게 된다. 여기서 암호화된 시그널링 또는 암호화된 데이터는 방송 채널이나 DTCH나 DCCH를 전달하는 공통 채널을 통하여 수신할 수 있다. 따라서, 단말은 저장하고 있는 보안 설정 및 보안 키 등을 이용하여 수신한 시그널링 또는 데이터의 복호할 수 있다.
- [114] 만약, 타이머가 만료한 경우, 상기 단말이 RRC 연결 모드인지 또는 RRC 휴지 모드인지와 무관하게, 단말과 네트워크는 단계 1108과 같이 보안 설정을 삭제할 수 있다.
- [115] 도 12는 본 발명의 제 2 실시예에 따른 신호 송수신 방법을 예시하는 도면이다. 특히, 도 12는 단말과 네트워크가 RRC 연결 요청 메시지를 송수신한 후 바로 SRB 및 DRB에 대하여 암호화를 적용하는 것을 예시한다.
- [116] 도 12를 참조하면, RRC 휴지 모드인 단말과 네트워크는 단계 1201과 같이 RRC 연결 수립(RRC Connection Establishment) 과정을 수행하여, RRC 연결 모드로 들어간다.
- [117] 또한, 단말은 네트워크로부터 단계 1202와 같이 보안 모드 명령 메시지를 수신하고, 단계 1203과 같이 보안 모드 완료 메시지를 송신할 수 있다. 이 과정에서, 상기 보안 모드 명령 메시지를 수신한 단말은 상기 보안 모드 명령 메시지에 포함된 보안 설정 정보를 저장한다. 이후, 상기 보안 설정 정보가 지시하는 암호화 알고리즘을 이용하여 하나 이상의 보안 키를 생성할 수 있다. 따라서, 단말은 단계 1204과 같이 DCCH를 위한 SRB 및 DTCH를 위한 DRB에 대하여 상기 보안 키를 이용한 암호화 및 보안 설정을 적용하고 저장한다.
- [118] 이후, 네트워크는 단계 1205에서 RRC 연결 해제 메시지를 단말로 송신할 수 있다. 상기 RRC 연결 해제 메시지는 보안 설정 유지 지시자 및 보안 설정 유지 시간에 관한 정보를 포함할 수 있다. 특히, 보안 설정 유지 지시자는 단말이 RRC 휴지 모드로 천이한 후 현재의 보안 설정의 저장 및 유지 여부를 지시할 수 있다.

즉, RRC 연결 해제 메시지를 수신한 단말은 RRC 연결을 해제하고, 현재의 보안 설정 및 보안 키를 저장한다. 다만, 단말과 네트워크는 현재의 보안 설정을 비활성화시킨다.

- [119] 또한, 단말은 보안 설정 유지 시간에 대응하는 타이머를 개시할 수 있다. 상기 타이머가 구동하는 동안, 단말은 상기 보안 설정 및 보안 키를 저장하고 유지할 수 있다. 물론, 네트워크도 보안 설정 유지 시간에 대응하는 타이머를 개시하며, 상기 타이머가 구동하는 동안, 네트워크 또한 C-RNTI, IMSI, TMSI 등을 단말 식별자와 같이 상기 보안 설정 및 보안 키를 저장하고 유지할 수 있다.
- [120] 이후, 단계 1206과 같이 단말이 CCCH 상에서 RRC 연결 요청 메시지를 송신하는 경우를 고려할 수 있다. 상기 RRC 연결 요청 메시지는 암호화되지 않은 메시지인 것이 바람직하다. 여기서 RRC 연결 요청 메시지는 단말 식별자와 함께 저장된 보안 설정을 활성화시키기 위한 보안 활성화 지시자를 포함할 수 있다. 이러한 RRC 연결 요청 메시지를 송신한 단말은 저장된 보안 설정을 이용하여 보안 모드를 활성화시킬 수 있다.
- [121] 상기 RRC 연결 요청 메시지를 수신한 네트워크는, 상기 보안 활성화 및/또는 지시자를 이용하여 상기 단말에 저장된 보안 설정이 어떠한 것인지 인지할 수 있다. 따라서, 네트워크는 단계 1207에서 상기 단말로 RRC 연결 셋업 메시지를 송신한다. 여기서 RRC 연결 셋업 메시지는 상기 활성화된 보안 모드에 따라 암호화되어 DCCH/SRB1 상에서 송신된다. 반면에 보안 활성화가 이루어지지 않은 경우라면, 상기 RRC 연결 셋업 메시지는 CCCH/SRB0 상에서 암호화가 이루어지지 않은 상태로 송신된다.
- [122] 단말이 SRB1의 설정 (즉, 디폴트 설정) 또는 SIB 상에서 방송되는 설정과 함께 보안 설정 역시 저장하고 있는 경우라면, 단말은 상기 암호화된 RRC 연결 셋업 메시지를 복호할 수 있다.
- [123] 반면에, RRC 연결 과정이 실패한 경우라면, 네트워크는 단말로 페이징 이유를 보안 실패로 설정한 페이징 메시지를 송신하고, 이에 대한 응답으로 단말은 연결 이유를 보안 실패로 설정한 RRC 연결 요청 메시지를 네트워크로 송신한다.
- [124] 한편, 암호화된 RRC 연결 셋업 메시지를 수신하고 이를 복호한 단말은 단계 1208에서 상기 저장된 보안 설정 및 보안 키를 이용하여 암호화한 RRC 연결 셋업 완료 메시지를 DCCH/SRB1 상에서 네트워크로 송신한다. RRC 연결 요청 메시지의 송신, 암호화된 RRC 연결 셋업 메시지의 복호, 암호화된 RRC 연결 셋업 메시지의 송신, 암호화된 RRC 연결 셋업 메시지에 대한 ACK 응답 수신 중 하나의 경우, 상기 단말과 네트워크는 타이머 구동을 중지한다. 또한, 암호화된 RRC 연결 셋업 메시지의 복호 또는 암호화된 RRC 연결 셋업 메시지의 송신 중 하나의 경우에서, 상기 단말은 저장된 보안 설정을 적용, 즉 활성화 한다.
- [125] 이후, 단말은 네트워크로부터 단계 1209와 같이 암호화된 시그널링과 데이터를 수신할 수 있다.
- [126] 한편, 네트워크는 단계 1210에서 다시 RRC 연결 해제 메시지를 단말로 송신할

수 있다. 상기 RRC 연결 해제 메시지는 보안 설정 유지 지시자 및 보안 설정 유지 시간에 관한 정보를 포함할 수 있다. 특히, 보안 설정 유지 지시자는 단말이 RRC 휴지 모드로 천이한 후 현재의 보안 설정의 저장 및 유지 여부를 지시할 수 있다. 즉, RRC 연결 해제 메시지를 수신한 단말은 RRC 연결을 해제하고, 현재의 보안 설정 및 보안 키를 저장한다. 다만, 단말과 네트워크는 현재의 보안 설정을 비활성화시킨다.

[127] 도 13은 본 발명의 제 3 실시예에 따른 신호 송수신 방법을 예시하는 도면이다. 도 12와 달리, 도 13은 보안 활성화 지시자를 포함하는 RRC 연결 셋업 완료 메시지를 송신한 후에, 보안 설정을 활성화하고 암호화를 적용하는 경우를 예시한다. 물론, RRC 연결 셋업 완료 메시지에 대한 ACK 응답 수신 후에, 보안 설정을 활성화하고 암호화를 적용하는 경우 역시 본 실시예에 적용되는 사항임은 자명하다.

[128] 도 13을 참조하면, 단말과 네트워크는 RRC 연결 수립 과정이 완료되어 RRC 연결 상태임에도 타이머 구동을 정지하지 않는 것을 알 수 있다.

[129] 또한, 도 12와 달리, 단계 1311과 같이 보안 설정 삭제 지시자를 포함하는 RRC 연결 해제 메시지를 수신하면, 단말과 네트워크는 단계 1312에서 타이머 구동을 중지하고 저장된 보안 설정을 삭제한다. 만약, 보안 설정이 활성화되어 있다면, 보안 설정을 비활성화시킨다.

[130] 물론, 보안 설정 삭제 지시자를 포함하지 않는 RRC 연결 해제 메시지를 수신하면, 단말과 네트워크는 타이머 구동을 유지하며, 현재 저장된 보안 설정을 유지한다.

[131] 도 14는 본 발명의 제 4 실시예에 따른 신호 송수신 방법을 예시하는 도면이다.

[132] 도 14를 참조하면, 단말이 보안 설정을 저장하고 있는 경우, 네트워크는 단말의 메모리에서 보안 설정을 삭제하기 위하여, 네트워크는 단계 1406과 같이 보안 설정 삭제 지시자를 포함하는 페이징 메시지와 같은 하향링크 시그널링을 송신할 수 있다.

[133] 상기 보안 설정 삭제 지시자를 포함하는 페이징 메시지를 수신한 단말은 메모리에서 보안 설정을 삭제하고 타이머 구동을 중지한다. 물론, 보안 설정이 활성화되어 있다면, 비활성화 시킨다.

[134] 도 15는 본 발명의 실시예에 따른 통신 장치의 블록 구성도를 예시한다.

[135] 도 15를 참조하면, 통신 장치(1500)는 프로세서(1510), 메모리(1520), RF 모듈(1530), 디스플레이 모듈(1540) 및 사용자 인터페이스 모듈(1550)을 포함한다.

[136] 통신 장치(1500)는 설명의 편의를 위해 도시된 것으로서 일부 모듈은 생략될 수 있다. 또한, 통신 장치(1500)는 필요한 모듈을 더 포함할 수 있다. 또한, 통신 장치(1500)에서 일부 모듈은 보다 세분화된 모듈로 구분될 수 있다. 프로세서(1510)는 도면을 참조하여 예시한 본 발명의 실시예에 따른 동작을 수행하도록 구성된다. 구체적으로, 프로세서(1510)의 자세한 동작은 도 1 내지 도

10에 기재된 내용을 참조할 수 있다.

- [137] 메모리(1520)는 프로세서(1510)에 연결되며 오퍼레이팅 시스템, 어플리케이션, 프로그램 코드, 데이터 등을 저장한다. RF 모듈(1530)은 프로세서(1510)에 연결되며 기저대역 신호를 무선 신호를 변환하거나 무선신호를 기저대역 신호로 변환하는 기능을 수행한다. 이를 위해, RF 모듈(1530)은 아날로그 변환, 증폭, 필터링 및 주파수 상향 변환 또는 이들의 역과정을 수행한다. 디스플레이 모듈(1540)은 프로세서(1510)에 연결되며 다양한 정보를 디스플레이한다. 디스플레이 모듈(1540)은 이로 제한되는 것은 아니지만 LCD(Liquid Crystal Display), LED(Light Emitting Diode), OLED(Organic Light Emitting Diode)와 같은 잘 알려진 요소를 사용할 수 있다. 사용자 인터페이스 모듈(1550)은 프로세서(1510)와 연결되며 키패드, 터치 스크린 등과 같은 잘 알려진 사용자 인터페이스의 조합으로 구성될 수 있다.
- [138] 이상에서 설명된 실시예들은 본 발명의 구성요소들과 특징들이 소정 형태로 결합된 것들이다. 각 구성요소 또는 특징은 별도의 명시적 언급이 없는 한 선택적인 것으로 고려되어야 한다. 각 구성요소 또는 특징은 다른 구성요소나 특징과 결합되지 않은 형태로 실시될 수 있다. 또한, 일부 구성요소들 및/또는 특징들을 결합하여 본 발명의 실시예를 구성하는 것도 가능하다. 본 발명의 실시예들에서 설명되는 동작들의 순서는 변경될 수 있다. 어느 실시예의 일부 구성이나 특징은 다른 실시예에 포함될 수 있고, 또는 다른 실시예의 대응하는 구성 또는 특징과 교체될 수 있다. 특허청구범위에서 명시적인 인용 관계가 있지 않은 청구항들을 결합하여 실시예를 구성하거나 출원 후의 보정에 의해 새로운 청구항으로 포함시킬 수 있음은 자명하다.
- [139] 본 문서에서 본 발명의 실시예들은 주로 단말과 기지국 간의 데이터 송수신 관계를 중심으로 설명되었다. 본 문서에서 기지국에 의해 수행된다고 설명된 특정 동작은 경우에 따라서는 그 상위 노드(upper node)에 의해 수행될 수 있다. 즉, 기지국을 포함하는 복수의 네트워크 노드들(network nodes)로 이루어지는 네트워크에서 단말과의 통신을 위해 수행되는 다양한 동작들은 기지국 또는 기지국 이외의 다른 네트워크 노드들에 의해 수행될 수 있음은 자명하다. 기지국은 고정국(fixed station), Node B, eNode B(eNB), 액세스 포인트(access point) 등의 용어에 의해 대체될 수 있다.
- [140] 본 발명에 따른 실시예는 다양한 수단, 예를 들어, 하드웨어, 펌웨어(firmware), 소프트웨어 또는 그것들의 결합 등에 의해 구현될 수 있다. 하드웨어에 의한 구현의 경우, 본 발명의 일 실시예는 하나 또는 그 이상의 ASICs(application specific integrated circuits), DSPs(digital signal processors), DSPDs(digital signal processing devices), PLDs(programmable logic devices), FPGAs(field programmable gate arrays), 프로세서, 콘트롤러, 마이크로 콘트롤러, 마이크로 프로세서 등에 의해 구현될 수 있다.
- [141] 펌웨어나 소프트웨어에 의한 구현의 경우, 본 발명의 일 실시예는 이상에서

설명된 기능 또는 동작들을 수행하는 모듈, 절차, 함수 등의 형태로 구현될 수 있다. 소프트웨어 코드는 메모리 유닛에 저장되어 프로세서에 의해 구동될 수 있다. 상기 메모리 유닛은 상기 프로세서 내부 또는 외부에 위치하여, 이미 공지된 다양한 수단에 의해 상기 프로세서와 데이터를 주고 받을 수 있다.

- [142] 본 발명은 본 발명의 특징을 벗어나지 않는 범위에서 다른 특정한 형태로 구체화될 수 있음은 당업자에게 자명하다. 따라서, 상기의 상세한 설명은 모든 면에서 제한적으로 해석되어서는 아니되고 예시적인 것으로 고려되어야 한다. 본 발명의 범위는 첨부된 청구항의 합리적 해석에 의해 결정되어야 하고, 본 발명의 등가적 범위 내에서의 모든 변경은 본 발명의 범위에 포함된다.

산업상 이용가능성

- [143] 상술한 바와 같은 무선 통신 시스템에서 단말이 네트워크와의 보안 설정 방법 및 이를 위한 장치는 3GPP LTE 시스템에 적용되는 예를 중심으로 설명하였으나, 3GPP LTE 시스템 이외에도 다양한 무선 통신 시스템에 적용하는 것이 가능하다.

청구범위

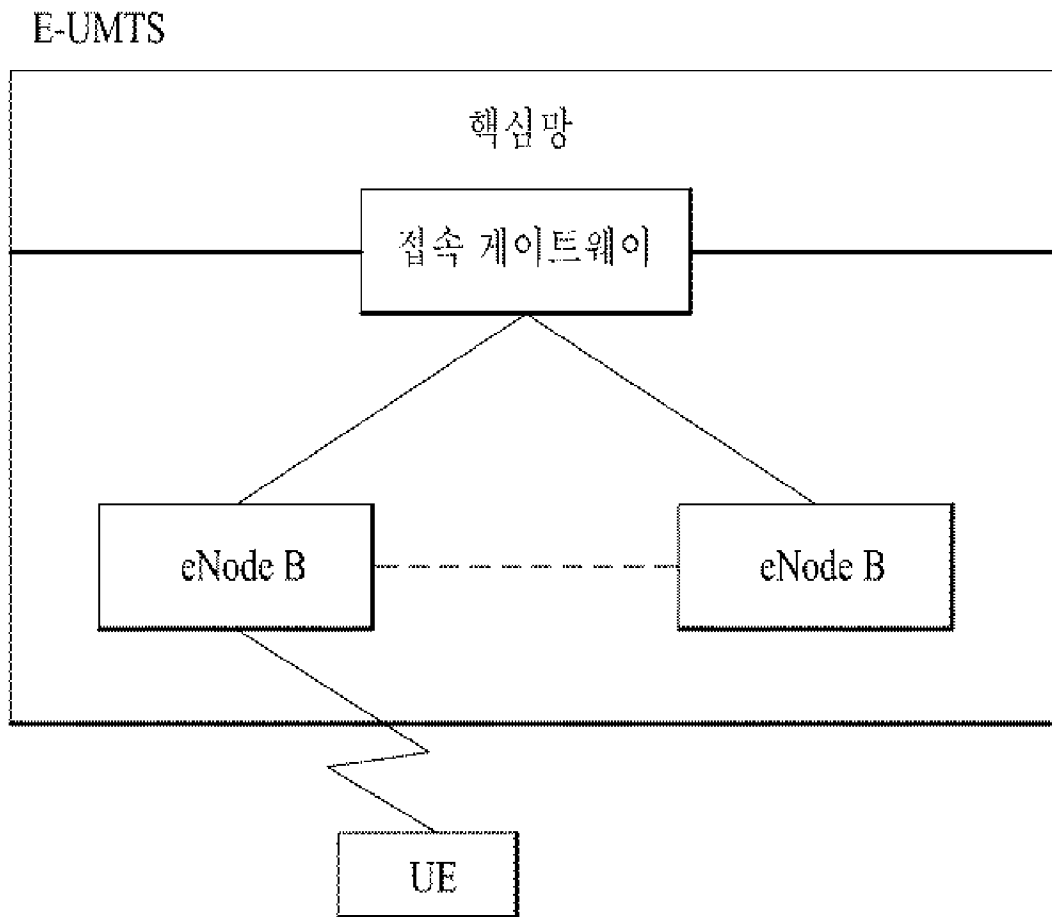
- [청구항 1] 무선 통신 시스템에서 단말이 네트워크와 신호를 송수신하는 방법에 있어서,
 상기 네트워크로부터 보안 설정 정보를 수신하는 단계;
 상기 보안 설정 정보에 기반하여 상기 네트워크와 데이터를 송신 또는 수신하는 단계;
 상기 네트워크로부터 연결 해제 메시지를 수신하는 단계;
 상기 네트워크와의 연결을 해제하는 단계; 및
 상기 네트워크로부터 보안 설정 유지 지시자를 수신한 경우, 타이머를 구동하는 단계를 포함하고,
 상기 타이머가 구동하는 동안 상기 보안 설정 정보를 유지하는 것을 특징으로 하는,
 신호 송수신 방법.
- [청구항 2] 제 1 항에 있어서,
 상기 보안 설정 유지 지시자는,
 상기 보안 설정 정보 또는 상기 연결 해제 메시지에 포함되는 것을 특징으로 하는,
 신호 송수신 방법.
- [청구항 3] 제 1 항에 있어서,
 상기 보안 설정 정보 또는 상기 연결 해제 메시지는,
 보안 유지 시간에 관한 정보를 포함하는 것을 특징으로 하는,
 신호 송수신 방법.
- [청구항 4] 제 1 항에 있어서,
 상기 네트워크와의 연결을 해제 시 상기 보안 설정 정보를 비활성화하는 단계; 및
 보안 설정 활성화 지시자를 포함하는 연결 요청 메시지를 상기 네트워크로 송신하는 단계를 더 포함하는 것을 특징으로 하는,
 신호 송수신 방법.
- [청구항 5] 제 4 항에 있어서,
 상기 연결 요청 메시지 송신 시 또는 상기 연결 요청 메시지에 대한 긍정 응답 수신 시, 상기 보안 설정 정보를 활성화하는 것을 특징으로 하는,
 신호 송수신 방법.
- [청구항 6] 제 5 항에 있어서,
 상기 타이머가 만료되기 전에, 상기 보안 설정 정보를 활성화하는 경우, 상기 타이머를 다시 시작하는 것을 특징으로 하는,
 신호 송수신 방법.

- [청구항 7] 제 1 항에 있어서,
상기 타이머가 만료되거나 또는 상기 네트워크로부터 보안 설정 삭제 지시자를 수신 시, 상기 보안 설정 정보를 삭제하는 단계를 더 포함하는 것을 특징으로 하는,
신호 송수신 방법.
- [청구항 8] 무선 통신 시스템에서 네트워크가 단말과 신호를 송수신하는 방법에 있어서,
상기 단말로 보안 설정 정보를 송신하는 단계;
상기 보안 설정 정보에 기반하여 상기 단말과 데이터를 송신 또는 수신하는 단계; 및
상기 단말로 연결 해제 메시지를 송신하는 단계를 포함하고, 상기 보안 설정 정보 또는 상기 연결 해제 메시지에 보안 설정 유지 지시자를 포함하는 것을 특징으로 하는,
신호 송수신 방법.
- [청구항 9] 제 8 항에 있어서,
상기 단말과의 연결을 해제하는 단계; 및
타이머를 구동하는 단계를 더 포함하고, 상기 타이머가 구동하는 동안 상기 보안 설정 정보를 유지하는 것을 특징으로 하는,
신호 송수신 방법.
- [청구항 10] 제 8 항에 있어서,
상기 보안 설정 정보 또는 상기 연결 해제 메시지는,
보안 유지 시간에 관한 정보를 포함하는 것을 특징으로 하는,
신호 송수신 방법.
- [청구항 11] 제 9 항에 있어서,
상기 단말과의 연결을 해제 시 상기 보안 설정 정보를 비활성화하는 단계; 및
보안 설정 활성화 지시자를 포함하는 연결 요청 메시지를 상기 단말로부터 수신하는 단계를 더 포함하는 것을 특징으로 하는,
신호 송수신 방법.
- [청구항 12] 제 11 항에 있어서,
상기 연결 요청 메시지 수신 시 또는 상기 연결 요청 메시지에 대한 긍정 응답 송신 시, 상기 보안 설정 정보를 활성화하는 것을 특징으로 하는,
신호 송수신 방법.
- [청구항 13] 제 12 항에 있어서,
상기 타이머가 만료되기 전에, 상기 보안 설정 정보를 활성화하는 경우, 상기 타이머를 다시 시작하는 것을 특징으로 하는,
신호 송수신 방법.

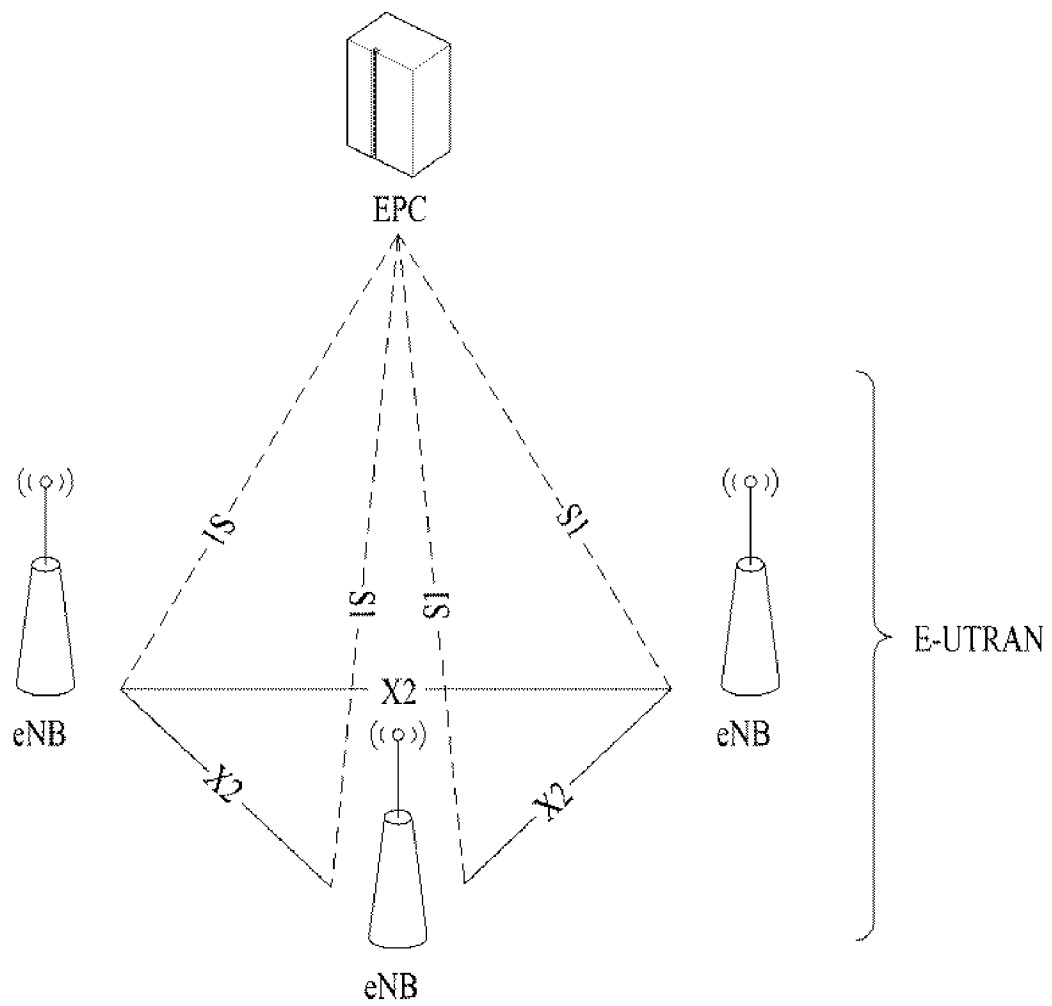
[청구항 14]

제 9 항에 있어서,
상기 타이머가 만료되거나 또는 상기 단말로 보안 설정 삭제
지시자를 송신 시, 상기 보안 설정 정보를 삭제하는 단계를 더
포함하는 것을 특징으로 하는,
신호 송수신 방법.

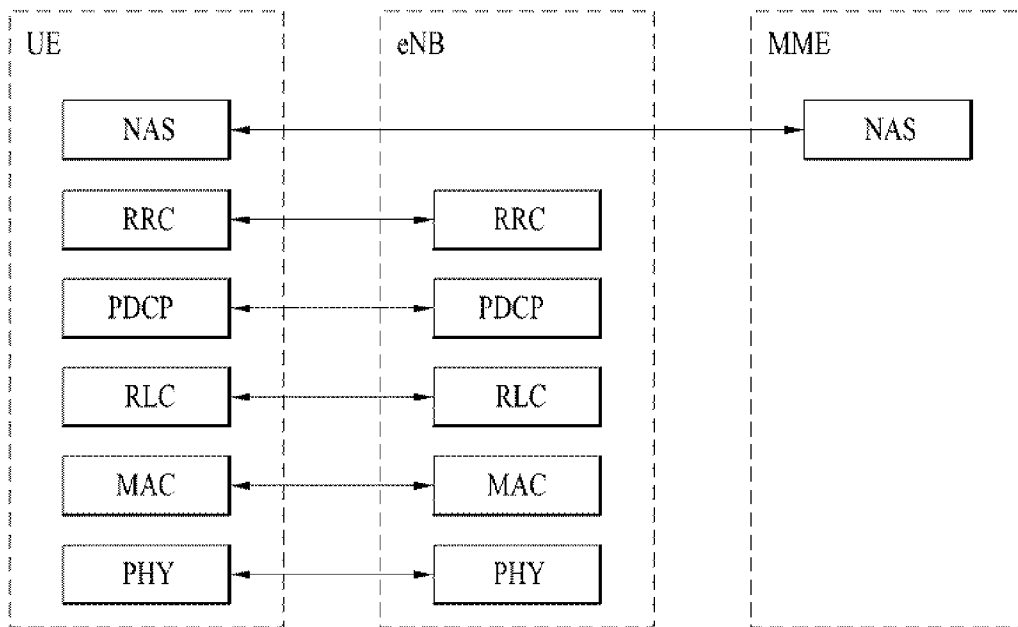
[Fig. 1]



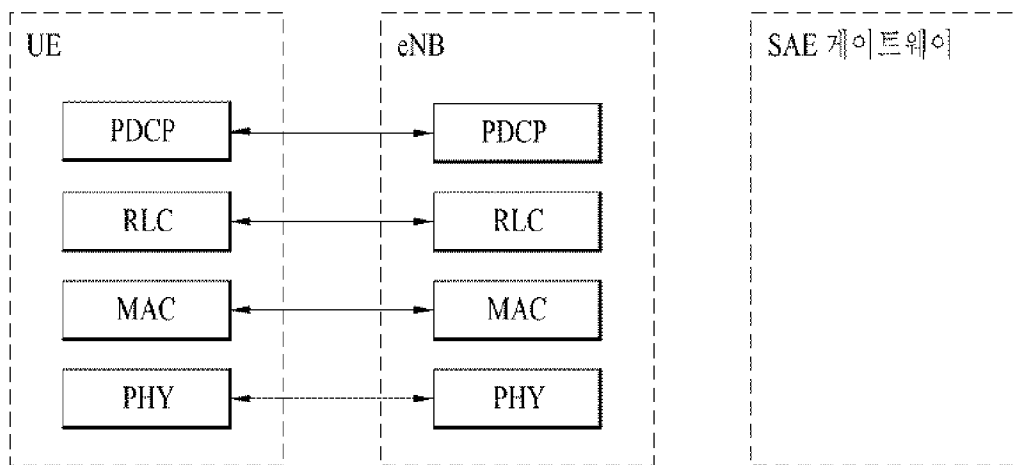
[Fig. 2]



[Fig. 3]

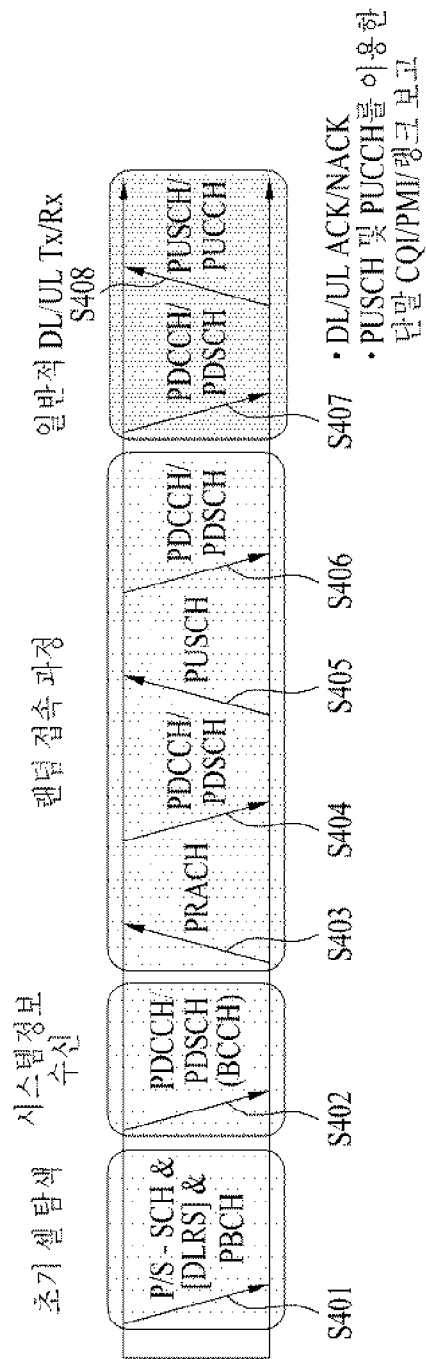


(a) 제어-평면 프로토콜 스택

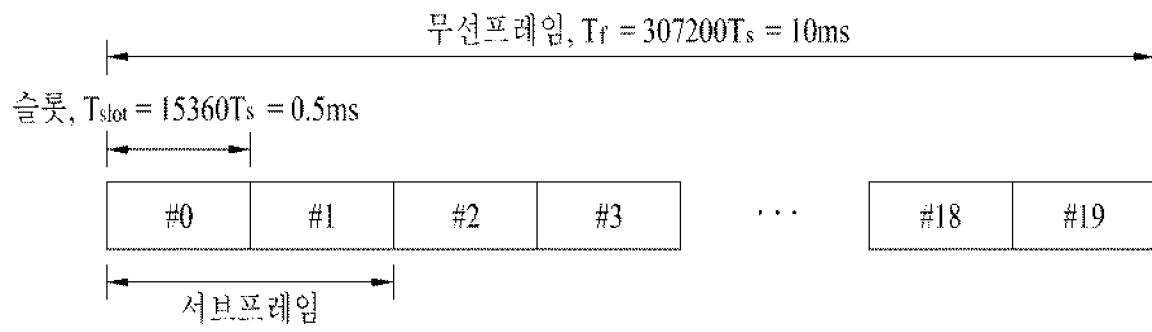


(b) 사용자-평면 프로토콜 스택

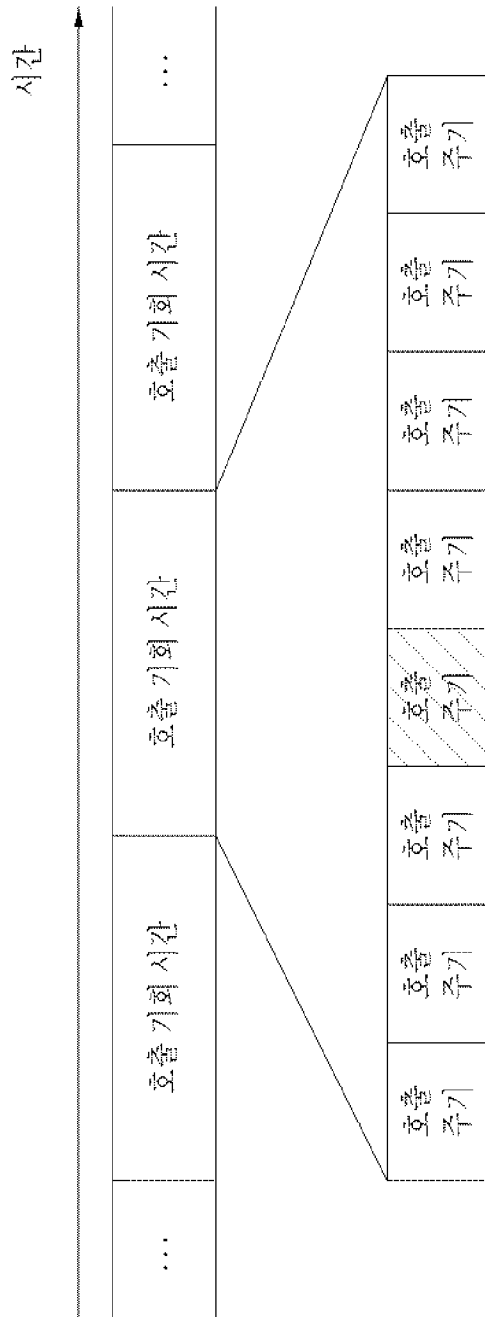
[Fig. 4]



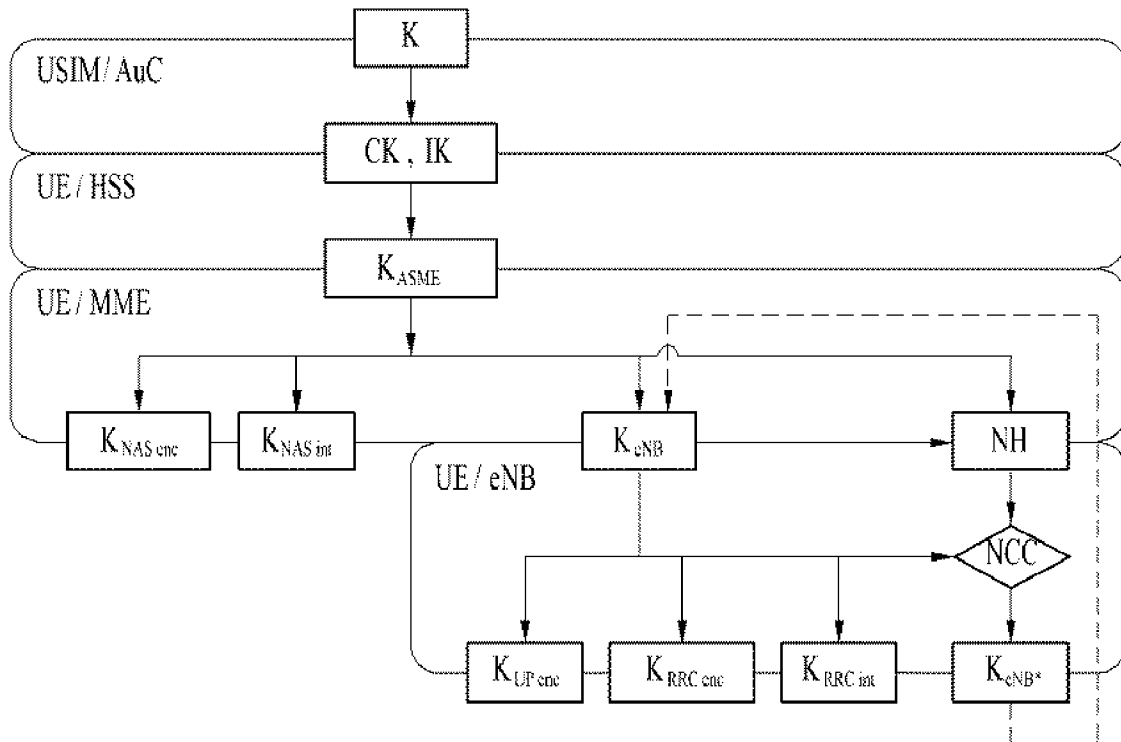
[Fig. 5]



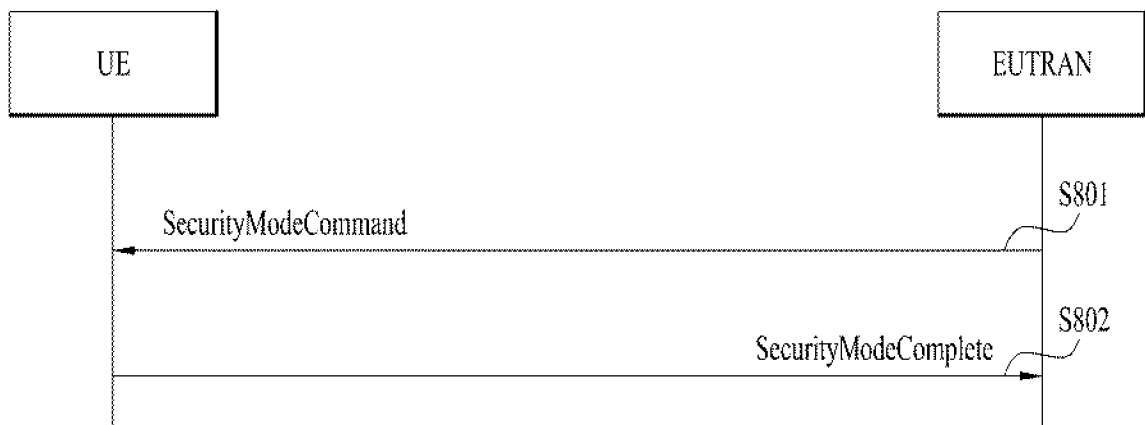
[Fig. 6]



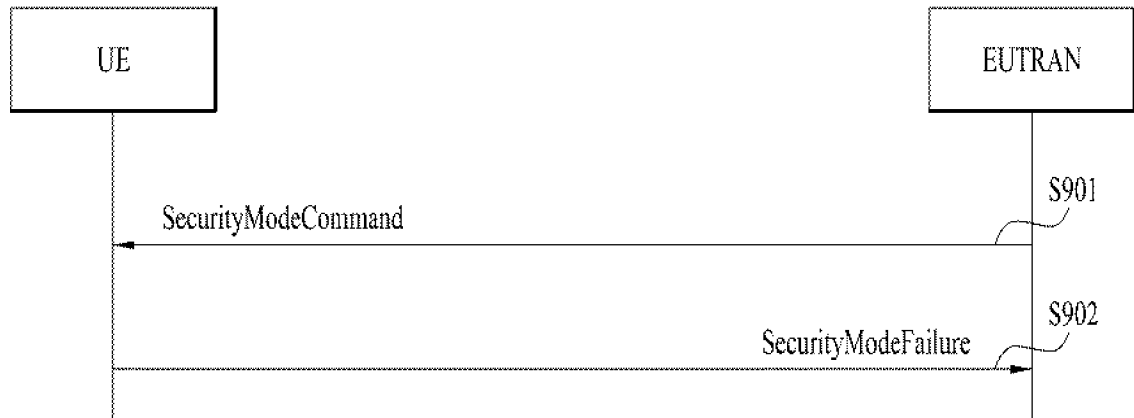
[Fig. 7]



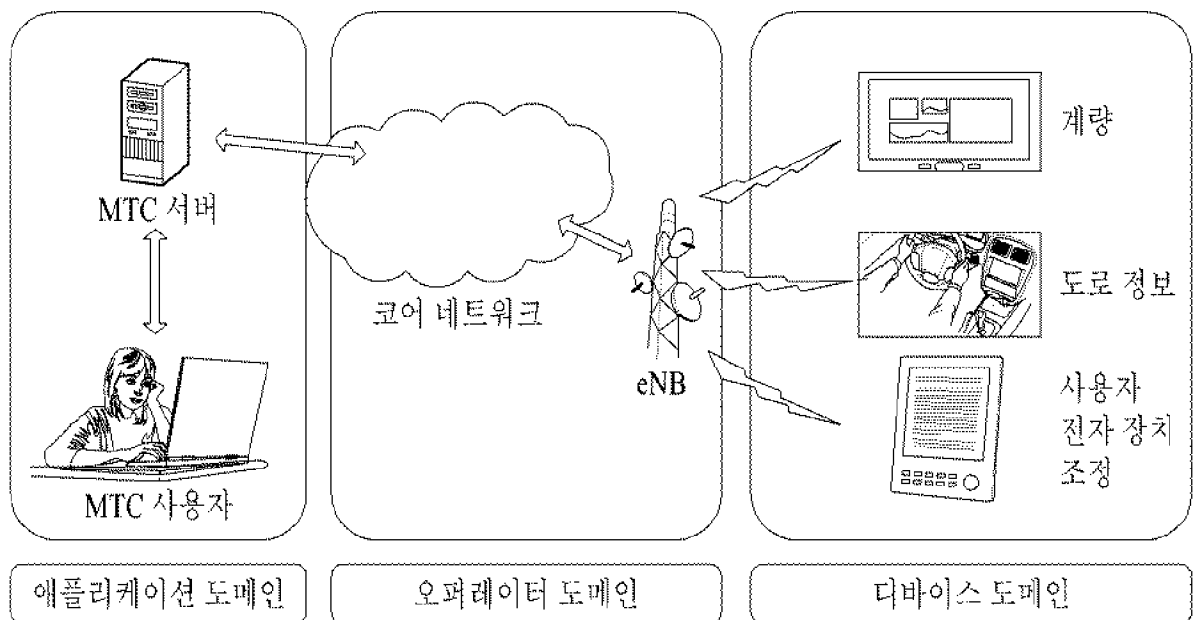
[Fig. 8]



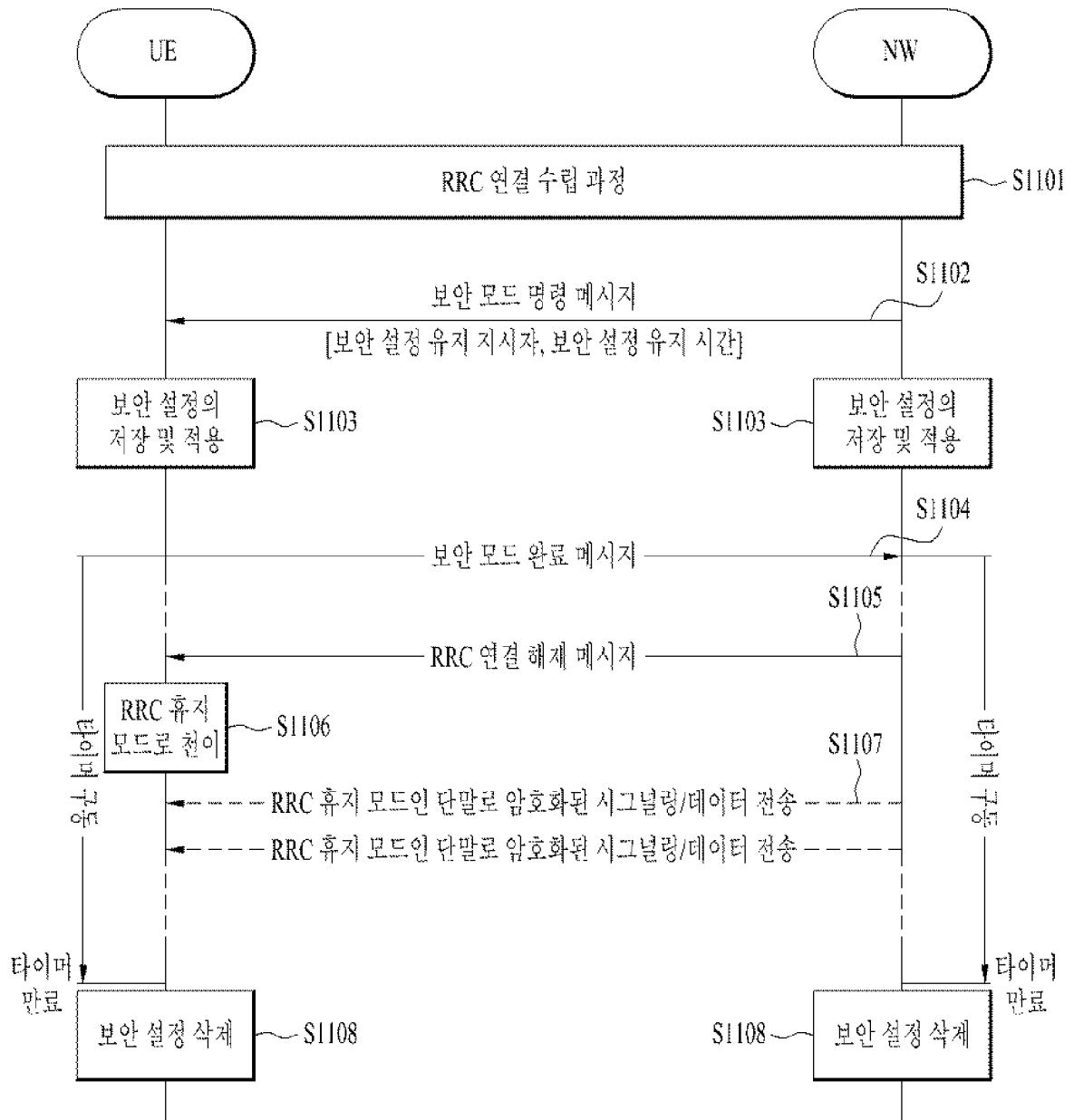
[Fig. 9]



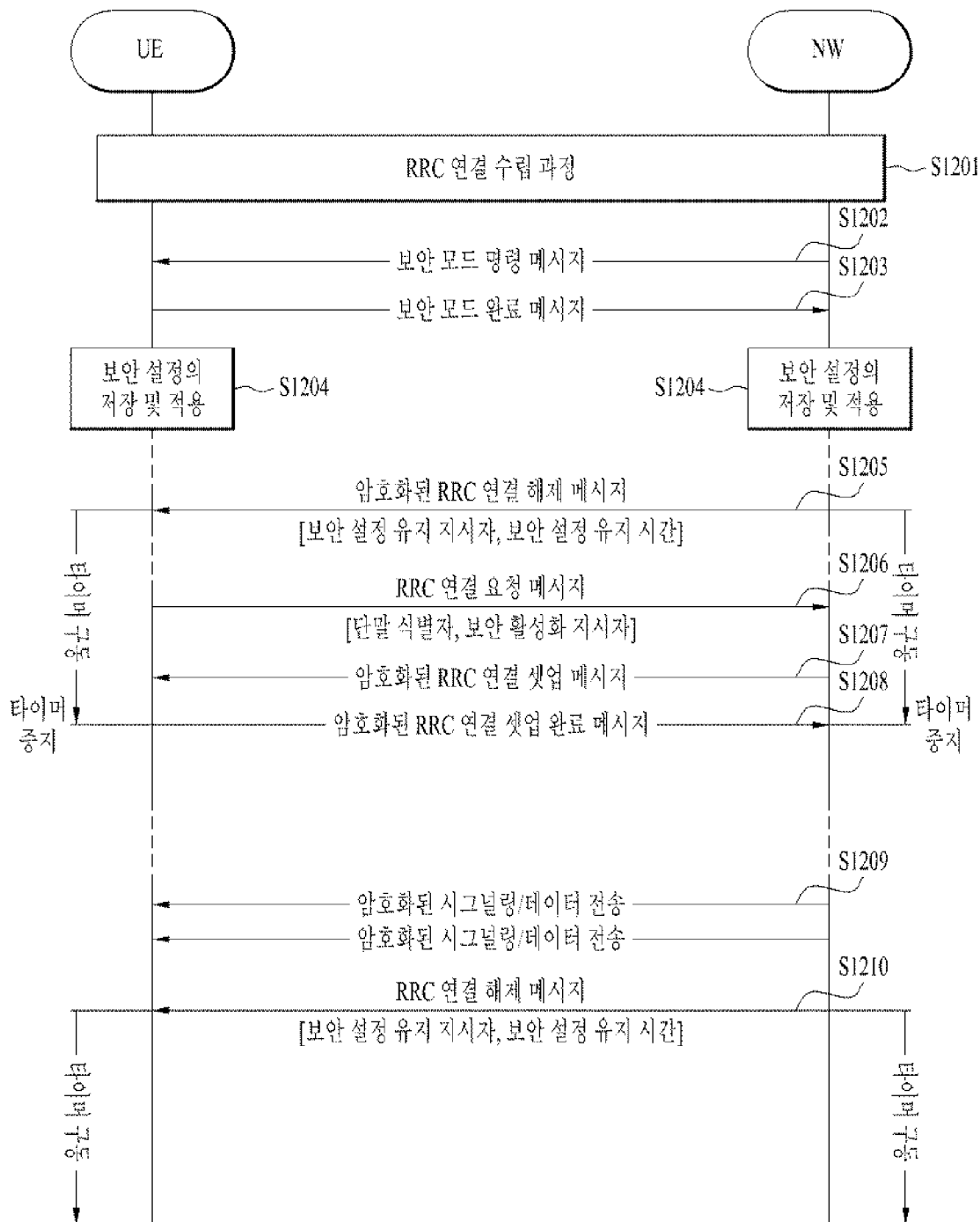
[Fig. 10]



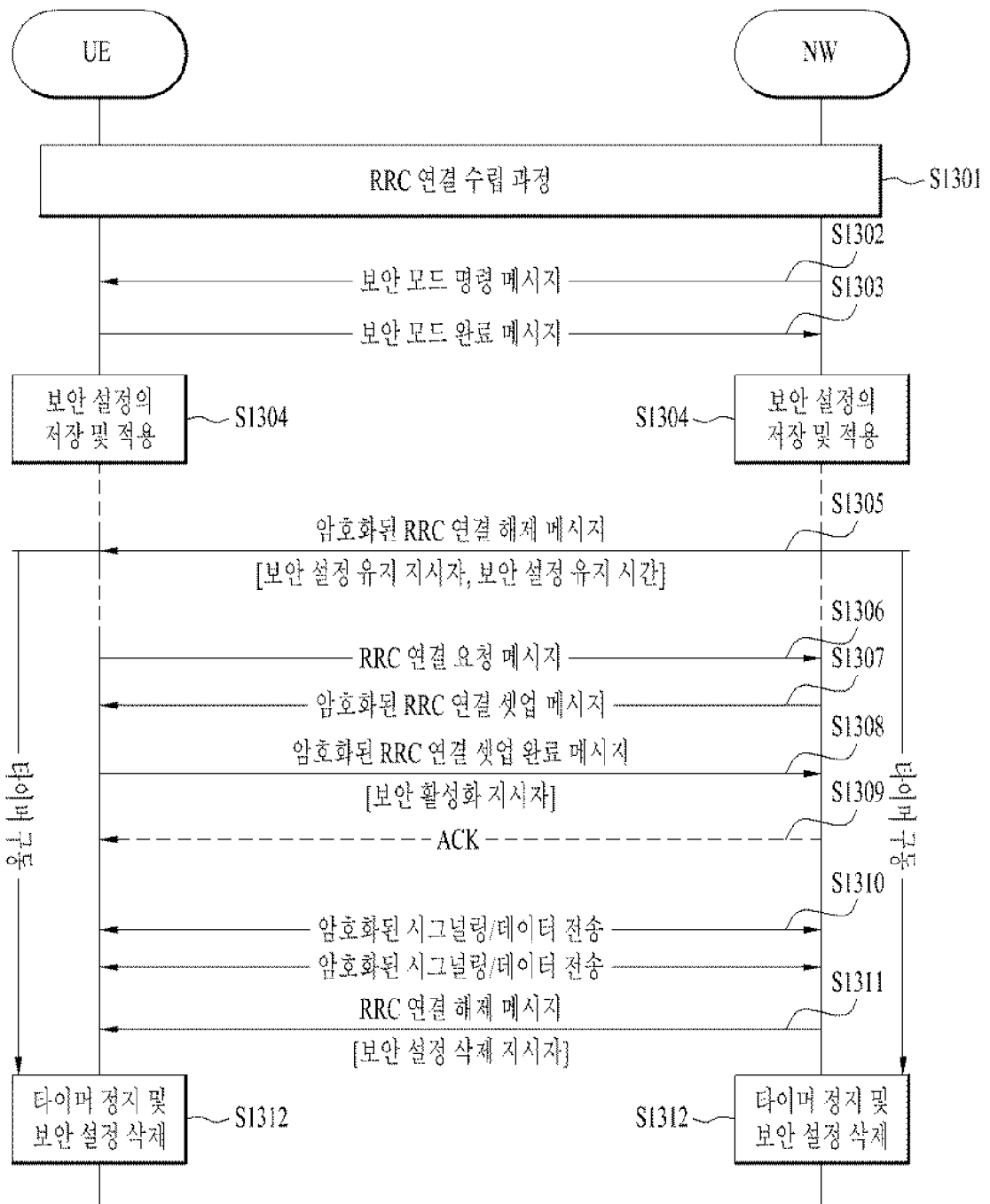
[Fig. 11]



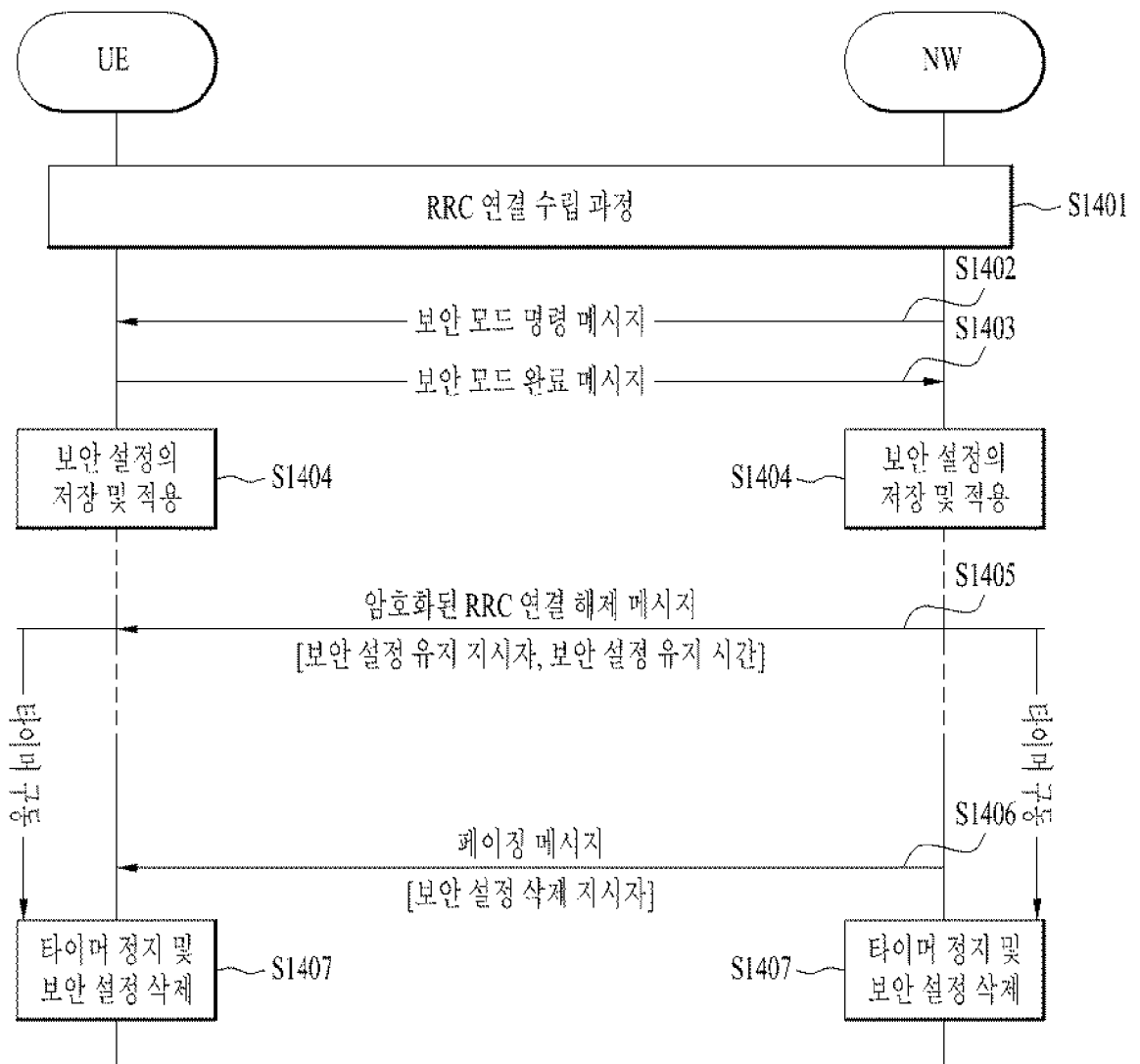
[Fig. 12]



[Fig. 13]



[Fig. 14]



[Fig. 15]

