



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0000890
(43) 공개일자 2019년01월03일

<p>(51) 국제특허분류(Int. Cl.) H04W 48/16 (2009.01) H04W 48/02 (2009.01)</p> <p>(52) CPC특허분류 H04W 48/16 (2013.01) H04W 48/02 (2013.01)</p> <p>(21) 출원번호 10-2018-7034938</p> <p>(22) 출원일자(국제) 2018년06월25일 심사청구일자 2018년11월30일</p> <p>(85) 번역문제출일자 2018년11월30일</p> <p>(86) 국제출원번호 PCT/KR2018/007142</p> <p>(87) 국제공개번호 WO 2018/236196 국제공개일자 2018년12월27일</p> <p>(30) 우선권주장 62/523,786 2017년06월23일 미국(US) 62/523,799 2017년06월23일 미국(US)</p>	<p>(71) 출원인 엘지전자 주식회사 서울특별시 영등포구 여의대로 128 (여의도동)</p> <p>(72) 발명자 이영대 서울시 서초구 양재대로11길 19 LG전자 특허센터 최현정 서울시 서초구 양재대로11길 19 LG전자 특허센터</p> <p>(74) 대리인 인비전 특허법인</p>
---	---

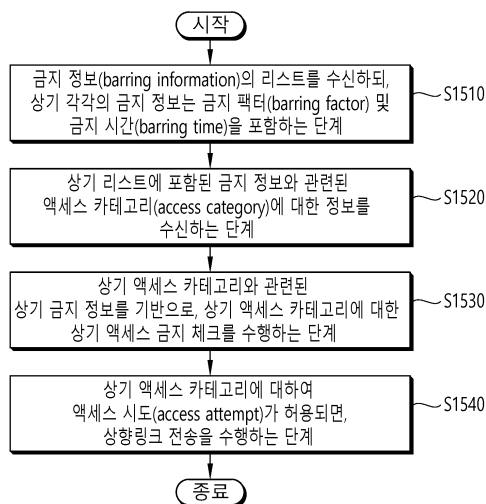
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 액세스 금지 체크를 수행하는 방법 및 장치

(57) 요약

무선 통신 시스템에서 단말이 액세스 금지 체크(access barring check)를 수행하는 방법 및 이를 지원하는 장치가 제공된다. 상기 방법은, 금지 정보(barring information)의 리스트를 수신하되, 상기 각각의 금지 정보는 금지 팩터(barring factor) 및 금지 시간(barring time)을 포함하는 단계; 상기 리스트에 포함된 금지 정보와 관련된 액세스 카테고리(access category)에 대한 정보를 수신하는 단계; 상기 액세스 카테고리와 관련된 상기 금지 정보를 기반으로, 상기 액세스 카테고리에 대한 상기 액세스 금지 체크를 수행하는 단계; 및 상기 액세스 카테고리에 대하여 액세스 시도(access attempt)가 허용되면, 상향링크 전송을 수행하는 단계;를 포함할 수 있다.

대표도 - 도15



명세서

청구범위

청구항 1

무선 통신 시스템에서 단말이 액세스 금지 체크(access barring check)를 수행하는 방법에 있어서,

금지 정보(barring information)의 리스트를 수신하되, 상기 각각의 금지 정보는 금지 팩터(barring factor) 및 금지 시간(barring time)을 포함하는 단계;

상기 리스트에 포함된 금지 정보와 관련된 액세스 카테고리(access category)에 대한 정보를 수신하는 단계;

상기 액세스 카테고리 및 관련된 상기 금지 정보를 기반으로, 상기 액세스 카테고리에 대한 상기 액세스 금지 체크를 수행하는 단계; 및

상기 액세스 카테고리에 대하여 액세스 시도(access attempt)가 허용되면, 상향링크 전송을 수행하는 단계;를 포함하는 것을 특징으로 하는 방법.

청구항 2

제 1 항에 있어서,

상기 금지 정보의 리스트는 네트워크로부터 수신되는 것을 특징으로 하는 방법.

청구항 3

제 2 항에 있어서,

상기 금지 정보의 리스트는 시스템 정보를 통해 수신되는 것을 특징으로 하는 방법.

청구항 4

제 1 항에 있어서,

상기 리스트에 포함된 상기 각각의 금지 정보는 하나 이상의 액세스 카테고리 및 관련되는 것을 특징으로 하는 방법.

청구항 5

제 4 항에 있어서,

상기 액세스 카테고리가 상기 하나 이상의 액세스 카테고리에 포함되면, 상기 액세스 카테고리에 대한 상기 액세스 금지 체크는 상기 액세스 카테고리 및 관련된 상기 금지 정보를 기반으로 수행되는 것을 특징으로 하는 방법.

청구항 6

제 1 항에 있어서,

상기 액세스 카테고리는 상기 단말의 NAS 계층(non-access stratum layer)으로부터 상기 단말의 RRC 계층(radio resource control layer)으로 전송되는 것을 특징으로 하는 방법.

청구항 7

제 6 항에 있어서,

상기 액세스 카테고리가 상기 단말의 NAS 계층으로부터 상기 단말의 RRC 계층으로 전송되면, 상기 액세스 카테고리에 대한 상기 액세스 금지 체크는 상기 액세스 카테고리 및 관련된 상기 금지 정보를 기반으로 수행되는 것을 특징으로 하는 방법.

청구항 8

제 1 항에 있어서,

상기 금지 정보와 관련된 상기 액세스 카테고리에 대한 정보는 네트워크로부터 수신되는 것을 특징으로 하는 방법.

청구항 9

제 1 항에 있어서,

상기 액세스 시도가 상기 액세스 카테고리에 대하여 금지되면, 상기 액세스 카테고리에 대한 타이머를 개시하는 단계;를 더 포함하는 것을 특징으로 하는 방법.

청구항 10

제 1 항에 있어서,

상기 상향링크 전송은 RRC 연결 요청 메시지의 전송을 포함하는 것을 특징으로 하는 방법.

청구항 11

무선 통신 시스템에서 액세스 금지 체크(access barring check)를 수행하는 단말에 있어서, 상기 단말은

메모리; 송수신기; 및

상기 메모리 및 상기 송수신기와 연결된 프로세서를 포함하되, 상기 프로세서는

상기 송수신기가 금지 정보(barring information)의 리스트를 수신하도록 제어하되, 상기 각각의 금지 정보는 금지 팩터(barring factor) 및 금지 시간(barring time)을 포함하고;

상기 송수신기가 상기 리스트에 포함된 금지 정보와 관련된 액세스 카테고리(access category)에 대한 정보를 수신하도록 제어하고;

상기 액세스 카테고리과 관련된 상기 금지 정보를 기반으로, 상기 액세스 카테고리에 대한 상기 액세스 금지 체크를 수행하고; 및

상기 액세스 카테고리에 대하여 액세스 시도(access attempt)가 허용되면, 상향링크 전송을 수행하는 것을 특징으로 하는 단말.

청구항 12

제 11 항에 있어서,

상기 금지 정보의 리스트는 네트워크로부터 수신되는 것을 특징으로 하는 단말.

청구항 13

제 12 항에 있어서,

상기 금지 정보의 리스트는 시스템 정보를 통해 수신되는 것을 특징으로 하는 단말.

청구항 14

제 11 항에 있어서,

상기 리스트에 포함된 상기 각각의 금지 정보는 하나 이상의 액세스 카테고리과 관련되는 것을 특징으로 하는 단말.

청구항 15

제 14 항에 있어서,

상기 액세스 카테고리가 상기 하나 이상의 액세스 카테고리에 포함되면, 상기 액세스 카테고리에 대한 상기 액세스 금지 체크는 상기 액세스 카테고리과 관련된 상기 금지 정보를 기반으로 수행되는 것을 특징으로 하는 단

말.

발명의 설명

기술 분야

[0001] 본 발명은 무선 통신 시스템에 관한 것으로서, 더 구체적으로는, 단말이 액세스 금지 체크를 수행하는 방법 및 이를 지원하는 장치에 관한 것이다.

배경 기술

[0002] 4G(4th-Generation) 통신 시스템 상용화 이후 증가 추세에 있는 무선 데이터 트래픽 수요를 충족시키기 위해, 개선된 5G(5th-Generation) 통신 시스템 또는 pre-5G 통신 시스템을 개발하기 위한 노력이 이루어지고 있다. 이러한 이유로, 5G 통신 시스템 또는 pre-5G 통신 시스템은 4G 네트워크 이후 (beyond 4G network) 통신 시스템 또는 LTE(long term evolution) 시스템 이후(post LTE) 이후의 시스템이라 불리고 있다.

발명의 내용

해결하려는 과제

[0003] 한편, 액세스 카테고리들은 서비스 유형 속성을 포함하므로, 특정 서비스에 속하는 액세스들은 다른 액세스들보다 우선 순위가 높은 것으로 처리되어야 한다. 예를 들어, 응급 서비스에 대한 액세스는 일반 서비스의 우선 순위보다 높거나, 또는 정상적인 서비스에 대한 액세스들은 IOT (Internet of Things) 데이터 전송의 액세스들보다 우선 순위가 높을 수 있다. 한편, NR에서는 64 개의 액세스 카테고리들이 정의되며, 액세스 금지 체크(access barring check)는 63 개의 액세스 카테고리에 적용될 수 있다. 액세스 금지 파라미터들이 각각의 액세스 카테고리들에 대해 정의되면, 액세스 금지 파라미터들의 전송을 위한 네트워크의 시그널링이 증가할 수 있다. 따라서 액세스 금지 정보 집합에 기반한 액세스 금지 체크 메커니즘이 제안될 필요가 있다.

과제의 해결 수단

[0004] 일 실시 예에 있어서, 무선 통신 시스템에서 단말이 액세스 금지 체크(access barring check)를 수행하는 방법이 제공된다. 상기 방법은, 금지 정보(barring information)의 리스트를 수신하되, 상기 각각의 금지 정보는 금지 팩터(barring factor) 및 금지 시간(barring time)을 포함하는 단계; 상기 리스트에 포함된 금지 정보와 관련된 액세스 카테고리(access category)에 대한 정보를 수신하는 단계; 상기 액세스 카테고리들과 관련된 상기 금지 정보를 기반으로, 상기 액세스 카테고리에 대한 상기 액세스 금지 체크를 수행하는 단계; 및 상기 액세스 카테고리에 대하여 액세스 시도(access attempt)가 허용되면, 상향링크 전송을 수행하는 단계;를 포함할 수 있다.

[0005] 다른 실시 예에 있어서, 무선 통신 시스템에서 액세스 금지 체크(access barring check)를 수행하는 단말이 제공된다. 상기 단말은 메모리; 송수신기; 및 상기 메모리 및 상기 송수신기와 연결된 프로세서를 포함하되, 상기 프로세서는 상기 송수신기가 금지 정보(barring information)의 리스트를 수신하도록 제어하되, 상기 각각의 금지 정보는 금지 팩터(barring factor) 및 금지 시간(barring time)을 포함하고; 상기 송수신기가 상기 리스트에 포함된 금지 정보와 관련된 액세스 카테고리(access category)에 대한 정보를 수신하도록 제어하고; 상기 액세스 카테고리들과 관련된 상기 금지 정보를 기반으로, 상기 액세스 카테고리에 대한 상기 액세스 금지 체크를 수행하고; 및 상기 액세스 카테고리에 대하여 액세스 시도(access attempt)가 허용되면, 상향링크 전송을 수행할 수 있다.

발명의 효과

[0006] 금지 정보의 전송을 위한 네트워크의 시그널링이 감소될 수 있다.

도면의 간단한 설명

[0007] 도 1은 LTE 시스템의 구조를 나타낸다.
 도 2는 제어 평면에 대한 LTE 시스템의 무선 인터페이스 프로토콜을 나타낸다.
 도 3은 사용자 평면에 대한 LTE 시스템의 무선 인터페이스 프로토콜을 나타낸다.

도 4는 5G 시스템 아키텍처를 나타낸다.

도 5는 NG-RAN과 5GC 간의 기능적 분리를 나타낸다.

도 6은 액세스 금지 체크의 예를 나타낸다.

도 7은 데이터 통신을 위한 어플리케이션 특정 혼잡 제어(ACDC)에 대한 액세스 금지 체크의 예를 나타낸다.

도 8은 본 발명의 일 실시 예에 따른, 액세스 카테고리에 매핑된 액세스 금지 정보에 따른 액세스 제어 절차를 나타낸다.

도 9는 본 발명의 일 실시 예에 따른, 적어도 하나의 액세스 카테고리와의 금지 정보 간의 매핑 관계의 예를 나타낸다.

도 10은 본 발명의 일 실시 예에 따른, 액세스 카테고리에 매핑된 액세스 금지 정보에 기반한 액세스 제어 절차를 나타낸다.

도 11은 본 발명의 일 실시 예에 따른, 네트워크 슬라이스 그룹의 예를 나타낸다.

도 12는 본 발명의 일 실시 예에 따른, 액세스 금지 구성에 기반하는 슬라이스 그룹의 예를 나타낸다.

도 13은 본 발명의 일 실시 예에 따른, 공통 액세스 금지 구성의 예를 나타낸다.

도 14는 본 발명의 일 실시 예에 따른, 네트워크 슬라이스 그룹에 기반하는 액세스 금지 메커니즘을 나타낸다.

도 15는 본 발명의 일 실시 예에 따른, UE가 액세스 금지 체크를 수행하는 방법을 도시한 블록도이다.

도 16은 본 발명의 실시 예가 구현되는 무선 통신 시스템의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0008] 이하의 기술은 CDMA(code division multiple access), FDMA(frequency division multiple access), TDMA(time division multiple access), OFDMA(orthogonal frequency division multiple access), SC-FDMA(single carrier frequency division multiple access) 등과 같은 다양한 무선 통신 시스템에 사용될 수 있다. CDMA는 UTRA(universal terrestrial radio access)나 CDMA2000과 같은 무선 기술로 구현될 수 있다. TDMA는 GSM(global system for mobile communications)/GPRS(general packet radio service)/EDGE(enhanced data rates for GSM evolution)와 같은 무선 기술로 구현될 수 있다. OFDMA는 IEEE(institute of electrical and electronics engineers) 802.11(Wi-Fi), IEEE 802.16(WiMAX), IEEE 802-20, E-UTRA(evolved UTRA) 등과 같은 무선 기술로 구현될 수 있다. IEEE 802.16m은 IEEE 802.16e의 진화로, IEEE 802.16e에 기반한 시스템과의 하위 호환성(backward compatibility)를 제공한다. UTRA는 UMTS(universal mobile telecommunications system)의 일부이다. 3GPP(3rd generation partnership project) LTE(long term evolution)은 E-UTRA(evolved-UMTS terrestrial radio access)를 사용하는 E-UMTS(evolved UMTS)의 일부로써, 하향링크에서 OFDMA를 채용하고 상향링크에서 SC-FDMA를 채용한다. LTE-A(advanced)는 3GPP LTE의 진화이다. 5G 통신 시스템은 LTE-A의 진화이다.

[0009] 설명을 명확하게 하기 위해, LTE-A/5G를 위주로 기술하지만 본 발명의 기술적 사상이 이에 제한되는 것은 아니다.

[0010] 도 1은 LTE 시스템의 구조를 나타낸다. 통신 네트워크는 IMS 및 패킷 데이터를 통한 인터넷 전화(Voice over internet protocol: VoIP)와 같은 다양한 통신 서비스들을 제공하기 위하여 넓게 설치된다.

[0011] 도 1을 참조하면, LTE 시스템 구조는 하나 이상의 단말(UE; 10), E-UTRAN(evolved-UMTS terrestrial radio access network) 및 EPC(evolved packet core)를 포함한다. 단말(10)은 사용자에 의해 움직이는 통신 장치이다. 단말(10)은 고정되거나 이동성을 가질 수 있으며, MS(mobile station), UT(user terminal), SS(subscriber station), 무선기기(wireless device) 등 다른 용어로 불릴 수 있다.

[0012] E-UTRAN은 하나 이상의 eNB(evolved node-B; 20)를 포함할 수 있고, 하나의 셀에 복수의 단말이 존재할 수 있다. eNB(20)는 제어 평면(control plane)과 사용자 평면(user plane)의 끝 지점을 단말에게 제공한다. eNB(20)는 일반적으로 단말(10)과 통신하는 고정된 지점(fixed station)을 말하며, BS(base station), BTS(base transceiver system), 액세스 포인트(access point) 등 다른 용어로 불릴 수 있다. 하나의 eNB(20)는 셀마다 배치될 수 있다. eNB(20)의 커버리지 내에 하나 이상의 셀이 존재할 수 있다. 하나의 셀은 1.25, 2.5,

5, 10 및 20 MHz 등의 대역폭 중 하나를 가지도록 설정되어 여러 단말에게 하향링크(DL; downlink) 또는 상향링크(UL; uplink) 전송 서비스를 제공할 수 있다. 이때 서로 다른 셀은 서로 다른 대역폭을 제공하도록 설정될 수 있다.

- [0013] 이하에서, DL은 eNB(20)에서 단말(10)로의 통신을 의미하며, UL은 단말(10)에서 eNB(20)으로의 통신을 의미한다. DL에서 송신기는 eNB(20)의 일부이고, 수신기는 단말(10)의 일부일 수 있다. UL에서 송신기는 단말(10)의 일부이고, 수신기는 eNB(20)의 일부일 수 있다.
- [0014] EPC는 제어 평면의 기능을 담당하는 MME(mobility management entity), 사용자 평면의 기능을 담당하는 S-GW(system architecture evolution (SAE) gateway)를 포함할 수 있다. MME/S-GW(30)은 네트워크의 끝에 위치할 수 있으며, 외부 네트워크와 연결된다. MME는 단말의 접속 정보나 단말의 능력에 관한 정보를 가지며, 이러한 정보는 주로 단말의 이동성 관리에 사용될 수 있다. S-GW는 E-UTRAN을 종단점으로 갖는 게이트웨이이다. MME/S-GW(30)은 세션의 종단점과 이동성 관리 기능을 단말(10)에 제공한다. EPC는 PDN(packet data network)-GW(gateway)를 더 포함할 수 있다. PDN-GW는 PDN을 종단점으로 갖는 게이트웨이이다.
- [0015] MME는 eNB(20)로의 NAS(non-access stratum) 시그널링, NAS 시그널링 보안, AS(access stratum) 보안 제어, 3GPP 액세스 네트워크 간의 이동성을 위한 inter CN(core network) 노드 시그널링, 아이들 모드 단말 도달 가능성(페이징 재전송의 제어 및 실행 포함), 트래킹 영역 리스트 관리(아이들 모드 및 활성화 모드인 단말을 위해), P-GW 및 S-GW 선택, MME 변경과 함께 핸드오버를 위한 MME 선택, 2G 또는 3G 3GPP 액세스 네트워크로의 핸드오버를 위한 SGSN(serving GPRS support node) 선택, 로밍, 인증, 전용 베어러 설정을 포함한 베어러 관리 기능, PWS(public warning system: 지진/쓰나미 경보 시스템(ETWS) 및 상용 모바일 경보 시스템(CMAS) 포함) 메시지 전송 지원 등의 다양한 기능을 제공한다. S-GW 호스트는 사용자 별 기반 패킷 필터링(예를 들면, 심층 패킷 검사를 통해), 합법적 차단, 단말 IP(internet protocol) 주소 할당, DL에서 전송 레벨 패킷 마킹, UL/DL 서비스 레벨 과금, 게이팅 및 등급 강제, APN-AMBR에 기반한 DL 등급 강제의 갖가지 기능을 제공한다. 명확성을 위해 MME/S-GW(30)은 "게이트웨이"로 단순히 표현하며, 이는 MME 및 S-GW를 모두 포함할 수 있다.
- [0016] 사용자 트래픽 전송 또는 제어 트래픽 전송을 위한 인터페이스가 사용될 수 있다. 단말(10) 및 eNB(20)은 Uu 인터페이스에 의해 연결될 수 있다. eNB(20)들은 X2 인터페이스에 의해 상호간 연결될 수 있다. 이웃한 eNB(20)들은 X2 인터페이스에 의한 망형 네트워크 구조를 가질 수 있다. eNB(20)들은 S1 인터페이스에 의해 EPC와 연결될 수 있다. eNB(20)들은 S1-MME 인터페이스에 의해 EPC와 연결될 수 있으며, S1-U 인터페이스에 의해 S-GW와 연결될 수 있다. S1 인터페이스는 eNB(20)와 MME/S-GW(30) 간에 다수-대-다수 관계(many-to-many-relation)를 지원한다.
- [0017] eNB(20)은 게이트웨이(30)에 대한 선택, RRC(radio resource control) 활성화(activation) 동안 게이트웨이(30)로의 라우팅(routing), 페이징 메시지의 스케줄링 및 전송, BCH(broadcast channel) 정보의 스케줄링 및 전송, UL 및 DL에서 단말(10)들로의 자원의 동적 할당, eNB 측정의 설정(configuration) 및 제공(provisioning), 무선 베어러 제어, RAC(radio admission control) 및 LTE 활성화 상태에서 연결 이동성 제어 기능을 수행할 수 있다. 상기 언급처럼 게이트웨이(30)는 EPC에서 페이징 개시, LTE 아이들 상태 관리, 사용자 평면의 암호화, SAE 베어러 제어 및 NAS 시그널링의 암호화와 무결성 보호 기능을 수행할 수 있다.
- [0018] 도 2는 제어 평면에 대한 LTE 시스템의 무선 인터페이스 프로토콜을 나타낸다. 도 3은 사용자 평면에 대한 LTE 시스템의 무선 인터페이스 프로토콜을 나타낸다.
- [0019] 단말과 E-UTRAN 간의 무선 인터페이스 프로토콜의 계층은 통신 시스템에서 널리 알려진 OSI(open system interconnection) 모델의 하위 3개 계층을 바탕으로 L1(제1 계층), L2(제2 계층) 및 L3(제3 계층)으로 구분된다. 단말과 E-UTRAN 간의 무선 인터페이스 프로토콜은 수평적으로 물리 계층, 데이터 링크 계층(data link layer) 및 네트워크 계층(network layer)으로 구분될 수 있고, 수직적으로는 제어 신호 전송을 위한 프로토콜 스택(protocol stack)인 제어 평면(control plane)과 데이터 정보 전송을 위한 프로토콜 스택인 사용자 평면(user plane)으로 구분될 수 있다. 무선 인터페이스 프로토콜의 계층은 단말과 E-UTRAN에서 쌍(pair)으로 존재할 수 있고, 이는 Uu 인터페이스의 데이터 전송을 담당할 수 있다.
- [0020] 물리 계층(PHY; physical layer)은 L1에 속한다. 물리 계층은 물리 채널을 통해 상위 계층에 정보 전송 서비스를 제공한다. 물리 계층은 상위 계층인 MAC(media access control) 계층과 전송 채널(transport channel)을 통해 연결된다. 물리 채널은 전송 채널에 맵핑 된다. 전송 채널을 통해 MAC 계층과 물리 계층 사이로 데이터가 전송될 수 있다. 서로 다른 물리 계층 사이, 즉 송신기의 물리 계층과 수신기의 물리 계층 간에 데이터는 물리 채널

널을 통해 무선 자원을 이용하여 전송될 수 있다. 물리 계층은 OFDM(orthogonal frequency division multiplexing) 방식을 이용하여 변조될 수 있고, 시간과 주파수를 무선 자원으로 활용한다.

[0021] 물리 계층은 몇몇의 물리 제어 채널(physical control channel)을 사용한다. PDCCH(physical downlink control channel)은 PCH(paging channel) 및 DL-SCH(downlink shared channel)의 자원 할당, DL-SCH와 관련되는 HARQ(hybrid automatic repeat request) 정보에 대하여 단말에 보고한다. PDCCH는 상향링크 전송의 자원 할당에 관하여 단말에 보고하기 위해 상향링크 그래프트를 나눌 수 있다. PCFICH(physical control format indicator channel)은 PDCCH를 위해 사용되는 OFDM 심벌의 개수를 단말에 알려주며, 모든 서브프레임마다 전송된다. PHICH(physical hybrid ARQ indicator channel)은 UL-SCH 전송에 대한 HARQ ACK(acknowledgement)/NACK(non-acknowledgement) 신호를 나른다. PUCCH(physical uplink control channel)은 하향링크 전송을 위한 HARQ ACK/NACK, 스케줄링 요청 및 CQI와 같은 UL 제어 정보를 나른다. PUSCH(physical uplink shared channel)은 UL-SCH(uplink shared channel)를 나른다.

[0022] 물리 채널은 시간 영역에서 복수의 서브프레임(subframe)들과 주파수 영역에서 복수의 부반송파(subcarrier)들로 구성된다. 하나의 서브프레임은 시간 영역에서 복수의 심벌들로 구성된다. 하나의 서브프레임은 복수의 자원 블록(RB; resource block)들로 구성된다. 하나의 자원 블록은 복수의 심벌들과 복수의 부반송파들로 구성된다. 또한, 각 서브프레임은 PDCCH를 위하여 해당 서브프레임의 특정 심벌들의 특정 부반송파들을 이용할 수 있다. 예를 들어, 서브프레임의 첫 번째 심벌이 PDCCH를 위하여 사용될 수 있다. PDCCH는 PRB(physical resource block) 및 MCS(modulation and coding schemes)와 같이 동적으로 할당된 자원을 나눌 수 있다. 데이터가 전송되는 단위 시간인 TTI(transmission time interval)는 1개의 서브프레임의 길이와 동일할 수 있다. 서브프레임 하나의 길이는 1ms일 수 있다.

[0023] 전송채널은 채널이 공유되는지 아닌지에 따라 공통 전송 채널 및 전용 전송 채널로 분류된다. 네트워크에서 단말로 데이터를 전송하는 DL 전송 채널(DL transport channel)은 시스템 정보를 전송하는 BCH(broadcast channel), 페이징 메시지를 전송하는 PCH(paging channel), 사용자 트래픽 또는 제어 신호를 전송하는 DL-SCH 등을 포함한다. DL-SCH는 HARQ, 변조, 코딩 및 전송 전력의 변화에 의한 동적 링크 적응 및 동적/반정적 자원 할당을 지원한다. 또한, DL-SCH는 셀 전체에 브로드캐스트 및 빔포밍의 사용을 가능하게 할 수 있다. 시스템 정보는 하나 이상의 시스템 정보 블록들을 나른다. 모든 시스템 정보 블록들은 같은 주기로 전송될 수 있다. MBMS(multimedia broadcast/multicast service)의 트래픽 또는 제어 신호는 MCH(multicast channel)를 통해 전송된다.

[0024] 단말에서 네트워크로 데이터를 전송하는 UL 전송 채널은 초기 제어 메시지(initial control message)를 전송하는 RACH(random access channel), 사용자 트래픽 또는 제어 신호를 전송하는 UL-SCH 등을 포함한다. UL-SCH는 HARQ 및 전송 전력 및 잠재적인 변조 및 코딩의 변화에 의한 동적 링크 적응을 지원할 수 있다. 또한, UL-SCH는 빔포밍의 사용을 가능하게 할 수 있다. RACH는 일반적으로 셀로의 초기 접속에 사용된다.

[0025] L2에 속하는 MAC 계층은 논리 채널(logical channel)을 통해 상위 계층인 RLC(radio link control) 계층에게 서비스를 제공한다. MAC 계층은 복수의 논리 채널에서 복수의 전송 채널로의 맵핑 기능을 제공한다. 또한, MAC 계층은 복수의 논리 채널에서 단수의 전송 채널로의 맵핑에 의한 논리 채널 다중화 기능을 제공한다. MAC 부 계층은 논리 채널상의 데이터 전송 서비스를 제공한다.

[0026] 논리 채널은 전송되는 정보의 종류에 따라, 제어 평면의 정보 전달을 위한 제어 채널과 사용자 평면의 정보 전달을 위한 트래픽 채널로 나눌 수 있다. 즉, 논리 채널 타입의 집합은 MAC 계층에 의해 제공되는 다른 데이터 전송 서비스를 위해 정의된다. 논리채널은 전송 채널의 상위에 위치하고 전송채널에 맵핑 된다.

[0027] 제어 채널은 제어 평면의 정보 전달만을 위해 사용된다. MAC 계층에 의하여 제공되는 제어 채널은 BCCH(broadcast control channel), PCCH(paging control channel), CCCH(common control channel), MCCH(multicast control channel) 및 DCCH(dedicated control channel)을 포함한다. BCCH는 시스템 제어 정보를 방송하기 위한 하향링크 채널이다. PCCH는 페이징 정보의 전송 및 셀 단위의 위치가 네트워크에 알려지지 않은 단말을 페이징 하기 위해 사용되는 하향링크 채널이다. CCCH는 네트워크와 RRC 연결을 갖지 않을 때 단말에 의해 사용된다. MCCH는 네트워크로부터 단말에게 MBMS 제어 정보를 전송하는데 사용되는 일대다 하향링크 채널이다. DCCH는 RRC 연결 상태에서 단말과 네트워크간에 전용 제어 정보 전송을 위해 단말에 의해 사용되는 일대일 양방향 채널이다.

[0028] 트래픽 채널은 사용자 평면의 정보 전달만을 위해 사용된다. MAC 계층에 의하여 제공되는 트래픽 채널은

DTCH(dedicated traffic channel) 및 MTCH(multicast traffic channel)을 포함한다. DTCH는 일대일 채널로 하나의 단말의 사용자 정보의 전송을 위해 사용되며, 상향링크 및 하향링크 모두에 존재할 수 있다. MTCH는 네트워크로부터 단말에게 트래픽 데이터를 전송하기 위한 일대다 하향링크 채널이다.

[0029] 논리 채널과 전송 채널간의 상향링크 연결은 UL-SCH에 맵핑 될 수 있는 DCCH, UL-SCH에 맵핑 될 수 있는 DTCH 및 UL-SCH에 맵핑 될 수 있는 CCCH를 포함한다. 논리 채널과 전송 채널간의 하향링크 연결은 BCH 또는 DL-SCH에 맵핑 될 수 있는 BCCH, PCH에 맵핑 될 수 있는 PCCH, DL-SCH에 맵핑 될 수 있는 DCCH, DL-SCH에 맵핑 될 수 있는 DTCH, MCH에 맵핑 될 수 있는 MCCH 및 MCH에 맵핑 될 수 있는 MTCH를 포함한다.

[0030] RLC 계층은 L2에 속한다. RLC 계층의 기능은 하위 계층이 데이터를 전송하기에 적합하도록 무선 섹션에서 상위 계층으로부터 수신된 데이터의 분할/연접에 의한 데이터의 크기 조정을 포함한다. 무선 베어러(RB; radio bearer)가 요구하는 다양한 QoS를 보장하기 위해, RLC 계층은 투명 모드(TM; transparent mode), 비 확인 모드(UM; unacknowledged mode) 및 확인 모드(AM; acknowledged mode)의 세 가지의 동작 모드를 제공한다. AM RLC는 신뢰성 있는 데이터 전송을 위해 ARQ(automatic repeat request)를 통해 재전송 기능을 제공한다. 한편, RLC 계층의 기능은 MAC 계층 내부의 기능 블록으로 구현될 수 있으며, 이때 RLC 계층은 존재하지 않을 수도 있다.

[0031] PDCP(packet data convergence protocol) 계층은 L2에 속한다. PDCP 계층은 상대적으로 대역폭이 작은 무선 인터페이스 상에서 IPv4 또는 IPv6와 같은 IP 패킷을 도입하여 전송되는 데이터가 효율적으로 전송되도록 불필요한 제어 정보를 줄이는 헤더 압축 기능을 제공한다. 헤더 압축은 데이터의 헤더에 필요한 정보만을 전송함으로써 무선 섹션에서 전송 효율을 높인다. 게다가, PDCP 계층은 보안 기능을 제공한다. 보안기능은 제3자의 검사를 방지하는 암호화 및 제3자의 데이터 조작을 방지하는 무결성 보호를 포함한다.

[0032] RRC(radio resource control) 계층은 L3에 속한다. L3의 가장 하단 부분에 위치하는 RRC 계층은 오직 제어 평면에서만 정의된다. RRC 계층은 단말과 네트워크 간의 무선 자원을 제어하는 역할을 수행한다. 이를 위해 단말과 네트워크는 RRC 계층을 통해 RRC 메시지를 교환한다. RRC 계층은 RB들의 구성(configuration), 재구성(re-configuration) 및 해제(release)와 관련되어 논리 채널, 전송 채널 및 물리 채널들의 제어를 담당한다. RB는 단말과 네트워크 간의 데이터 전달을 위해 L1 및 L2에 의해 제공되는 논리적 경로이다. 즉, RB는 단말과 E-UTRAN 간의 데이터 전송을 위해 L2에 의해 제공되는 서비스를 의미한다. RB가 설정된다는 것은 특정 서비스를 제공하기 위해 무선 프로토콜 계층 및 채널의 특성을 규정하고, 각각의 구체적인 파라미터 및 동작 방법을 결정함을 의미한다. RB는 SRB(signaling RB)와 DRB(data RB) 두 가지로 구분될 수 있다. SRB는 제어 평면에서 RRC 메시지를 전송하는 통로로 사용되며, DRB는 사용자 평면에서 사용자 데이터를 전송하는 통로로 사용된다.

[0033] 도 2를 참조하면, RLC 및 MAC 계층(네트워크 측에서 eNB에서 종료)은 스케줄링, ARQ 및 HARQ와 같은 기능을 수행할 수 있다. RRC 계층(네트워크 측에서 eNB에서 종료)은 방송, 페이징, RRC 연결 관리, RB 제어, 이동성 기능 및 단말 측정 보고/제어와 같은 기능을 수행할 수 있다. NAS 제어 프로토콜(네트워크 측에서 게이트웨이의 MME에서 종료)은 SAE 베어러 관리, 인증, LTE_IDLE 이동성 핸들링, LTE_IDLE에서 페이징 개시 및 단말과 게이트웨이 간의 시그널링을 위한 보안 제어와 같은 기능을 수행할 수 있다.

[0034] 도 3을 참조하면, RLC 및 MAC 계층(네트워크 측에서 eNB에서 종료)은 제어 평면에서의 기능과 동일한 기능을 수행할 수 있다. PDCP 계층(네트워크 측에서 eNB에서 종료)은 헤더 압축, 무결성 보호 및 암호화와 같은 사용자 평면 기능을 수행할 수 있다.

[0035] 도 4는 5G 시스템 아키텍처를 나타낸다.

[0036] 도 4를 참조하면, 차세대 무선 액세스 네트워크 (NG-RAN) 노드는 UE에 대하여 NR 무선 액세스 (NR) 사용자 평면 및 제어 평면 프로토콜 종단들을 제공하는 gNB일 수도 있고, 또는 UE에 대하여 진화된 유니버설 지상 무선 접속 (E-UTRA) 사용자 평면 및 제어 평면 프로토콜 종단들을 제공하는 ng-eNB일 수도 있다. gNB들 및 ng-eNB들은 Xn 인터페이스를 통해 서로 상호 연결될 수 있다. gNB들 및 ng-eNB들은 또한 NG 인터페이스를 통해 5G 코어 네트워크 (5GC)에 연결될 수 있고, 보다 구체적으로는 NG-C 인터페이스를 통해 AMF (액세스 및 이동성 관리 기능)에 연결될 수 있고, NG-U 인터페이스를 통해 UPF (사용자 평면 기능)에 연결될 수 있다. NG-C는 NG-RAN과 5GC 간의 제어 평면 인터페이스에 의할 수 있고, NG-U는 NG-RAN과 5GC 간의 사용자 평면 인터페이스에 의할 수 있다.

[0037] 도 5는 NG-RAN과 5GC 간의 기능적 분리를 나타낸다.

- [0038] 도 5를 참조하면, gNB 및 ng-eNB는 다음 기능을 호스트할 수 있다.
- [0039] - 무선 자원 관리를 위한 기능들: 무선 베어러 제어, 무선 허가 제어, 연결 이동성 제어, 상향링크 및 하향링크 (스케줄링) 모두에서 UE들에 대한 자원들의 동적 할당;
- [0040] - 데이터의 IP 헤더 압축, 암호화 및 무결성 보호;
- [0041] - AMF 로의 라우팅이 UE에 의해 제공된 정보로부터 결정될 수 없는 경우, UE 어태치(attach) 시 AMF의 선택;
- [0042] - 사용자 평면 데이터를 UPF (들)로 라우팅;
- [0043] - AMF를 향한 제어 평면 정보의 라우팅;
- [0044] - 연결 설정 및 해제;
- [0045] - 페이징 메시지의 스케줄링 및 전송;
- [0046] - (AMF 또는 O M으로부터 발생하는) 시스템 방송 정보의 스케줄링 및 전송;
- [0047] - 이동성 및 스케줄링을 위한 측정 및 측정 보고 구성'
- [0048] - 상향링크에서의 전송 레벨 패킷 마킹;
- [0049] - 세션 관리;
- [0050] - 네트워크 슬라이싱의 지원;
- [0051] - QoS 플로우 관리 및 데이터 무선 베어러로의 매핑;
- [0052] - RRC_INACTIVE 상태에 있는 UE들의 지원;
- [0053] - NAS 메시지들의 배포 기능;
- [0054] - 무선 액세스 네트워크 공유;
- [0055] - 이중 연결성;
- [0056] - NR과 E-UTRA 간의 긴밀한 연동(interworking).
- [0057] AMF (Access and Mobility Management Function)는 다음 주요 기능들을 호스팅할 수 있다.
- [0058] - NAS 시그널링 중단
- [0059] - NAS 시그널링 보안;
- [0060] - AS 보안 제어;
- [0061] - 3GPP 액세스 네트워크들 간의 이동성을 위한 인터 CN 노드 시그널링;
- [0062] - 유휴(idle) 모드 UE 도달 가능성 (페이징 재전송의 제어 및 실행 포함);
- [0063] - 등록 영역 관리;
- [0064] - 인트라-시스템 및 인터-시스템 이동성의 지원;
- [0065] - 액세스 인증;
- [0066] - 로밍 권한들의 체크를 포함하는 액세스 인증;
- [0067] - 이동성 관리 제어 (가입 및 정책들);
- [0068] - 네트워크 슬라이싱의 지원;
- [0069] - SMF 선택.
- [0070] UPF (User Plane Function)는 다음 주요 기능들을 호스트할 수 있다.
- [0071] - 인트라 / 인터-RAT 이동성을 위한 앵커 포인트 (적용 가능한 경우);
- [0072] - 데이터 네트워크에 대한 상호 연결의 외부 PDU 세션 포인트;

- [0073] - 패킷 라우팅 및 포워딩;
- [0074] - 패킷 검사(inspection) 및 정책 규칙 적용(enforcement)의 사용자 평면 부분;
- [0075] - 트래픽 사용보고;
- [0076] - 데이터 네트워크로 트래픽 플로우들을 라우팅하는 것을 지원하는 상향링크 분류자;
- [0077] - 멀티-홈 PDU 세션을 지원하는 분기 포인트(branching point);
- [0078] - 사용자 평면에 대한 QoS 취급, 예컨대 패킷 필터링, 게이팅, UL / DL 요금 집행(rate enforcement);
- [0079] - 상향링크 트래픽 검증 (QoS 플로우 매핑에 대한 SDF);
- [0080] - 하향링크 패킷 버퍼링 및 하향링크 데이터 통지 트리거링;
- [0081] 세션 관리 기능 (SMF)은 다음 주요 기능들을 호스트할 수 있다.
- [0082] - 세션 관리;
- [0083] - UE IP 주소 할당 및 관리;
- [0084] - UP 기능들의 선택 및 제어;
- [0085] - 트래픽을 적절한 목적지(destination)로 라우팅하기 위해 UPF에서 트래픽 조정(steering)을 구성한다;
- [0086] - 정책 집행 및 QoS의 제어 부분;
- [0087] - 하향링크 데이터 통지.
- [0088] 도 6은 액세스 금지 체크(access barring check)의 예를 나타낸다.
- [0089] 도 6을 참조하면, 네트워크 또는 기지국의 과부하(overload) 또는 혼잡 상태에서, 기지국은 시스템 정보를 통해 ACB (Access Class Barring)-관련 정보를 방송할 수 있다. 시스템 정보는 시스템 정보 블록 (SIB) 타입 2일 수 있다.
- [0090] SIB 유형 1은 다음 표와 같은 ACB-관련 정보를 포함할 수 있다.

표 1

필드(Field)	설명(Description)
ac-BarringFactor	UE에 의해 생성되는 랜덤 값이 ac-BarringFactor의 값보다 더 작은 경우, 액세스가 허용된다. 그렇지 않으면, 액세스가 금지된다.
ac-BarringForCSFB	회선 전환(CS) 폴백에 대한 ACB. CS 폴백은 VoLTE 호를 이전 3G 호로 변환한다.
ac-BarringForEmergency	응급 서비스에 대한 ACB
ac-BarringForMO-Data	모바일 발신 데이터에 대한 ACB
ac-BarringForMO-Signalling	모바일 발신 제어 신호에 대한 ACB
ac-BarringForSpecialAC	특정 액세스 클래스들에 대한 ACB, 즉 11 내지 15.
ac-BarringTime	액세스가 금지되는 경우의 시간을 나타낸다.
ssac-BarringForMMTEL-Video	MMTEL 비디오의 모바일 발생에 대한 각각의 서비스에 대한 ACB.
ssac-BarringForMMTEL-Voice	MMTEL 음성의 모바일 발생에 대한 각각의 서비스에 대한 ACB.

- [0092] 한편, UE1은 IMS 서비스, 예를 들어 VoLTE에 의한 호(call)의 모바일 발생(mobile orienting)을 결정하고 서비스 요청 메시지를 생성할 수 있다. 유사하게, UE2는 일반 데이터의 모바일 발생을 결정하고 서비스 요청 메시지를 생성할 수 있다.
- [0093] 이어서, UE1은 RRC 연결 요청 메시지를 생성할 수 있다. 마찬가지로, UE2는 RRC 연결 요청 메시지를 생성할 수 있다.
- [0094] 한편, UE1은 액세스 금지 체크 (즉, ACB가 적용되는지 여부)를 수행할 수 있다. 유사하게, UE2는 액세스 금지 체크 (즉, ACB가 적용되는지 여부)를 수행할 수 있다.
- [0095] ACB가 적용되지 않으면 UE1과 UE2는 RRC 연결 요청 메시지를 각각 전송할 수 있다. 그러나, ACB가 적용되는 경

우, UE1 및 UE2 모두 RRC 연결 요청 메시지를 각각 전송하지 않을 수 있다.

- [0096] 액세스 금지 체크는 다음과 같이 상세하게 설명될 것이다. 일반적으로, 10 개의 액세스 등급들 (예를 들어, AC0, AC1, ... 및 AC9) 중 적어도 하나가 UE에 랜덤하게 할당될 수 있다. 예외적으로, 응급한 응급 액세스의 경우 AC10이 할당된다. 이와 같이, 랜덤하게 할당 된 액세스 등급의 값은 UE1 및 UE2의 각각의 USIM에 저장될 수 있다. 이후, UE1과 UE2는 저장된 액세스 등급에 기반하여, 수신된 ACB-관련 정보에 포함된 금지 팩터를 이용하여 액세스 등급이 적용되었는지 여부를 검증할 수 있다. 액세스 금지 체크는 각 액세스 계층 (AS: Access Stratum) 계층, 즉 UE1과 UE2의 RRC 계층 (radio resource control layer)에서 수행될 수 있다.
- [0097] 액세스 금지 체크는 다음과 같이 더 상세하게 설명될 것이다.
- [0098] ac-BarringPerPLMN-List는 UE1 및 UE2 각각이 수신한 SIB 유형 2에 포함될 수 있으며, 상위 계층에서 선택된 PLMN에 대응하는 plmn-identityIndex와 매칭되는 AC-BarringPerPLMN 엔트리가 ac-BarringPerPLMN-List에 포함되면, 상위 계층에 의해 선택된 PLMN에 대응하는 plmn-identityIndex와 매칭되는 AC-BarringPerPLMN 엔트리가 선택된다.
- [0099] 다음으로, UE1 및 UE2가 RRC 연결 요청을 수행하는 경우, T303을 Tbarring으로 사용하고 ac-BarringForMO-Data를 금지 파라미터들로 사용하여 액세스 금지 체크를 수행할 수 있다.
- [0100] 금지가 결정되면, UE1 및 UE2의 각각의 AS (RRC) 계층은 RRC 연결 설정의 실패를 상위 계층에 통지할 수 있다.
- [0101] 이어서, 이와 같이, 액세스가 금지되는 경우, 각 AS (RRC) 계층은 T302 타이머 또는 Tbarring 타이머가 실행 중인지 여부를 결정할 수 있다. 타이머가 실행 중이 아니면, T302 타이머 또는 Tbarring 타이머가 실행될 수 있다.
- [0102] 한편 T302 타이머 또는 Tbarring 타이머가 실행되는 동안 AS (RRC) 계층은 해당 셀에 대한 모든 액세스가 금지된 것으로 간주한다.
- [0103] 전술한 바와 같이, 네트워크 과부하 및 혼잡 상황에서, 기지국은 ACB-관련 정보를 UE에 제공할 수 있다. 그런 다음, UE는 USIM에 저장된 액세스 클래스에 기반하여 수신된 ACB 정보에 포함된 금지 팩터를 사용하여 셀에 대한 액세스가 금지되는지를 체크할 수 있다. 액세스 금지 체크를 통해, 최종적으로, 액세스 시도(access attempt)가 수행되지 않는다. 즉, 액세스 금지 체크를 통해 해당 셀에 대한 액세스가 금지된 경우, UE는 액세스를 시도하지 않고, 해당 셀에 대한 액세스가 금지되지 않은 경우, UE는 액세스를 시도한다. 액세스 금지 체크는 AS 계층에서 수행된다. 여기서, 액세스 시도는 UE의 AS (RRC) 계층이 RRC 연결 요청 메시지를 기지국으로 전송하는 것을 의미한다.
- [0104] 한편, 액세스 금지 체크는 예를 들어 발신 호, 발신 데이터, 발신 IMS 음성 및 발신 IMS 비디오와 같은 UE의 일반적인 모바일 발신 (MO: mobile originating) 서비스를 수행할 수 있다. 즉, ACB는 모든 응용 프로그램들의 액세스에 적용될 수 있고, (하지만, 응급 서비스 또는 페이징에 대한 응답은 제외).
- [0105] 발신 호, 발신 데이터, 발신 IMS 음성 및 발신 IMS 비디오와 같은 일반적인 모바일 발신 (MO) 서비스를 차별화하는 방법으로, 데이터 통신을 위한 어플리케이션 특정 혼잡 제어 (ACDC: application specific congestion control)가 제안된다.
- [0106] 도 7은 데이터 통신을 위한 어플리케이션 특정 혼잡 제어(ACDC)에 대한 액세스 금지 체크의 예를 나타낸다.
- [0107] 도 7을 참조하면, 먼저 기지국은 SIB를 통해 UE에게 ACDC 금지 정보 (barring information)를 제공할 수 있다.
- [0108] 한편, 특정 어플리케이션이 UE에서 실행되고 데이터 통신 서비스가 특정 응용 어플리케이션에 의해 필요한 경우, 특정 응용 프로그램의 실행을 제어하기 위한 응용 계층은 응용 속성 관련 정보를 NAS 계층 (non-access stratum layer)에 제공할 수 있다.
- [0109] 그런 다음, 응용 계층으로부터 수신된 응용 속성 관련 정보에 기반하여, UE의 NAS 계층은 ACDC에 대한 응용 카테고리 결정할 수 있다.
- [0110] 이어서, 서비스 연결 (서비스 요청 메시지의 전송 또는 확장 서비스 요청 메시지의 전송)을 위한 서비스 요청 절차를 시작하는 경우, UE의 NAS 계층은 AS 계층 (즉, RRC 층)에 응용 카테고리에 관한 정보를 전달(deliver)할 수 있다.

- [0111] NAS 계층의 서비스 요청 절차 (서비스 요청 메시지의 전송 또는 확장 서비스 요청 메시지의 전송)를 수행하기 전에, 네트워크로부터 수신한 응용 카테고리 및 ACDC 금지 정보에 기반하여, AS 계층 (예컨대, RRC 계층)은 ACDC 금지 체크 (barring check)를 수행하여 서비스 요청 절차를 허용할지 여부를 결정할 수 있다.
- [0112] ACDC 금지 체크의 결과로 금지 대상이 아니고 허용되는 것이라고 판단되면, UE의 AS 계층 (즉, RRC 계층)은 RRC 연결 요청 메시지를 기지국으로 전송할 수 있다.
- [0113] 전술한 바와 같이, ACDC를 통해 UE에서 현재 실행 중인 어플리케이션이 요구하는 서비스 요청은 구별을 통해 허용 또는 금지될 수 있다.
- [0114] 한편, NG-RAN은 RACH 백 오프, RRC 연결 거부, RRC 연결 해제 및 UE 기반 액세스 금지 메커니즘과 같은 과부하 및 액세스 제어 기능을 지원할 수 있다. 하나의 통합된 액세스 제어 프레임워크가 NR에 적용될 수 있다. 각각의 식별된 액세스 시도에 대해 하나의 액세스 카테고리 (access category) 및 하나 이상의 액세스 신원들 (Identities)이 선택될 수 있다. NG-RAN은 액세스 카테고리 및 액세스 신원들과 연관된 금지 제어 정보를 방송할 수 있고, UE는 방송된 금지 정보 및 선택된 액세스 카테고리 및 액세스 신원들에 기반하여, 식별된 액세스 시도가 허가되는지 여부를 결정할 수 있다. 동일한 NG-RAN을 공유하는 다수의 코어 네트워크들의 경우에, NG-RAN은 각 PLMN에 대한 방송 제어 정보를 개별적으로 제공한다. 통합 액세스 제어 프레임 워크는 모든 UE 상태에 적용 가능할 수 있다. UE 상태들은 RRC_IDLE, RRC_INACTIVE 또는 RRC_CONNECTED 상태를 포함할 수 있다. RRC_IDLE에서, UE NAS는 액세스 카테고리를 RRC에 통지하고, 연결 요청은 gNB가 요청을 거절할지 여부를 결정할 수 있게 하는 일부 정보를 포함한다.
- [0115] 운영자의 정책에 기반하여, 5G 시스템은 액세스 신원들 및 액세스 카테고리에 따라 달라지는 관련 금지 파라미터들을 사용하여 UE가 네트워크에 액세스하는 것을 방지(prevent)할 수 있어야 한다. 액세스 신원들은 표 2에 나열된 바와 같이 UE에서 구성된다. 이러한 액세스 신원들은 언제든지 금지될 수 있다.

표 2

액세스 신원 넘버(Access Identity number)	UE 구성 (UE configuration)
0	UE는 이 표에서의 임의의 파라미터로 구성되지 않음
1 (NOTE 1)	UE는 멀티미디어 우선순위 서비스(MPS)로 구성됨.
2 (NOTE 2)	UE는 미션 임계 서비스(MCS)로 구성됨.
3-10	향후 사용을 위해 예약됨
11 (NOTE 3)	액세스 클래스 11이 UE에 구성됨.
12 (NOTE 3)	액세스 클래스 12가 UE에 구성됨.
13 (NOTE 3)	액세스 클래스 13이 UE에 구성됨.
14 (NOTE 3)	액세스 클래스 14가 UE에 구성됨.
15 (NOTE 3)	액세스 클래스 15가 UE에 구성됨.
<p>NOTE 1: 액세스 신원 1은 MPS에 대해 구성된 UE들에 의해 구성이 유효한 PLMN에서 사용된다. 구성이 유효한 PLMN은 HPLMN, HPLMN과 등가인 PLMN들, 본국(home country)의 방문 PLMN들, 및 본국 외부의 구성된 방문 PLMN이다.</p> <p>NOTE 2: 액세스 신원 2는 MCS에 대해 구성된 UE들에 의해, 구성이 유효한 PLMN에서 사용된다. 구성이 유효한 PLMN은 HPLMN 또는 HPLMN과 등가인 PLMN들이다.</p> <p>NOTE 3: 액세스 신원들 11 및 15는 EHPLMN 리스트가 없거나 또는 임의의 EHPLMN에 없는 경우에만, 홈 PLMN에서 유효하다. 액세스 신원들 12, 13 및 14는 홈 PLMN 및 본국의 방문 PLMN들에서만 유효하다. 이러한 목적을 위해 본국은 IMSI의 MCC 부분의 국가로 정의된다.</p>	

- [0117] 액세스 카테고리들은 표 3에 나열된 바와 같이 액세스 시도의 유형 및 UE와 관련된 조건들의 조합으로 정의된다. 액세스 카테고리 0은 액세스 신원들과 관계없이, 금지되지 않는다. 네트워크는 페이지징을 보낼지 여부를 제어하여 액세스 카테고리 0에 관련된 액세스 시도들의 양을 제어할 수 있다.

표 3

액세스 카테고리 넘버(Access Category number)	UE에 관련된 조건들(Conditions related to UE)	액세스 시도의 유형(Type of access attempt)
0	전부(All)	페이지징에서 발생하는 MO 시그널링

1 (NOTE 1)	UE가 지연 허용 서비스에 대해 구성되고, UE의 HPLMN 및 선택된 PLMN에 기반하여 판단된, 액세스 카테고리 1에 대한 액세스 제어의 대상이 됨.	응급을 제외하고 전부
2	전부	응급
3	액세스 카테고리 1의 조건들을 제외하고 전부.	페이징이 아닌 것에서 발생하는 MO 시그널링
4	액세스 카테고리 1의 조건들을 제외하고 전부.	MMTE 음성 (NOTE 3)
5	액세스 카테고리 1의 조건들을 제외하고 전부.	MMTE 비디오
6	액세스 카테고리 1의 조건들을 제외하고 전부.	SMS
7	액세스 카테고리 1의 조건들을 제외하고 전부.	임의의 다른 액세스 카테고리들에 속하지 않는 MO 데이터
8-31		예약된 표준화된 액세스 카테고리들
32-63 (NOTE 2)	전부	운영자 분류에 기반하여
<p>NOTE 1: 액세스 카테고리 1에 대한 금지 파라미터는 액세스 카테고리가 다음 카테고리들 중 하나에 속하는 UE에 적용되는지 여부를 정의하는 정보를 수반한다: 지연 허용 서비스를 위해 구성된 UE들; 지연 허용 서비스를 위해 구성되고 해당 HPLMN이나 이에 등가인 PLMN에 있지 않는 UE들; 지연 허용 서비스를 위해 구성되고, SIM/USIM상에서의 운영자-정의 PLMN 선택자 리스트에서 UE가 로밍 중인 국가의 가장 선호하는 PLMN으로 나열되지 않거나 또는 그들의 HPLMN에 있지 않거나 또는 그들의 HPLMN에 등가인 PLMN에 있지 않는 UE들.</p> <p>NOTE 2: 운영자 분류 및 표준화된 액세스 카테고리에 기반하는 액세스 카테고리가 있고 액세스 시도가 이들 모두에 카테고리화될 수 있고, 표준화된 액세스 카테고리가 0도 2도 아닌 경우, UE는 운영자 분류에 기반하여 액세스 카테고리를 적용한다. 운영자 분류 및 표준화된 액세스 카테고리에 기반하는 액세스 카테고리가 있고 액세스 시도가 이들 모두에 카테고리화될 수 있고, 표준화된 액세스 카테고리가 0 또는 2 인 경우, UE는 표준화된 액세스 카테고리를 적용한다.</p> <p>NOTE 3: 실-시간 텍스트 (RTT)를 포함한다.</p> <p>NOTE 4: IMS 메시징을 포함한다.</p>		

[0119] 하나 이상의 액세스 신원들과 하나의 액세스 카테고리만 선택되어 액세스 시도를 위해 테스트된다. 5G 네트워크는 RAN의 하나 이상의 영역들에서 금지 제어 정보 (즉, 액세스 신원 및 액세스 카테고리 및 연관된 금지 파라미터들의 리스트)를 방송할 수 있어야 한다. UE의 구성 및 방송 금지 제어 정보(broadcast barring control information)로부터 UE가 수신하는 금지 파라미터에 기반하여 UE는 특정 신규 액세스 시도가 허용되는지 여부를 결정할 수 있어야 한다. 동일한 RAN을 공유하는 다중 코어 네트워크들의 경우, RAN은 서로 다른 코어 네트워크들에 대해 개별적으로 액세스 제어를 적용할 수 있어야 한다. 통합 액세스 제어 프레임워크는 E-UTRA를 사용하는 5G CN에 액세스하는 UE들 및 NR을 사용하여 5G CN에 액세스하는 UE 모두에 적용 가능해야 한다.

[0120] 액세스 카테고리들은 서비스 유형 속성을 포함하므로 특정 서비스에 속한 액세스들은 다른 액세스보다 우선 순위가 높은 것으로 처리된다. 예를 들어, 응급 서비스에 대한 액세스는 일반 서비스의 액세스 보다 우선 순위보다 높거나 정상적인 서비스에 대한 액세스가 IOT (Internet of Things) 데이터 전송의 액세스 보다 우선 순위가 높을 수 있다. 한편, NR에서는 64 개의 액세스 카테고리가 정의되며 액세스 금지 체크는 63 개의 액세스 카테고리들에 적용될 수 있다. 액세스 금지 파라미터들이 각각의 액세스 카테고리들에 대해 정의되면, 액세스 금지 파라미터들의 전송을 위한 네트워크의 시그널링이 증가할 수 있다. 따라서 액세스 금지 정보 집합에 기반한 액세스 금지 체크 메커니즘이 제안될 필요가 있다. 이하, 본 발명의 실시 예에 따른 액세스 금지 정보 집합에 기반하여 UE가 액세스 금지를 수행하는 방법 및 이를 지원하는 장치가 상세히 설명된다.

[0121] 본 발명의 일 실시 예에 따르면, 하나 이상의 액세스 카테고리가 특정 액세스 우선 순위에 매핑될 수 있고, 그 다음에 UE는 액세스 우선 순위에 기반하여 액세스 금지 메커니즘을 수행할 수 있다. 본 발명에서, 액세스 우선 순위는 우선 순위, 액세스 금지 정보, 금지 정보, 액세스 금지 구성 또는 금지 구성으로 지칭될 수 있다.

[0122] 도 8은 본 발명의 일 실시 예에 따른, 액세스 카테고리에 매핑된 액세스 금지 정보에 따른 액세스 제어 절차를 나타낸다.

[0123] 도 8을 참조하면, 단계 S810에서, UE는 네트워크로부터 금지 정보의 리스트를 수신할 수 있다. 금지 정보의 리

스트는 시스템 정보를 통해 기지국으로부터 수신될 수 있다. 예를 들어, 시스템 정보는 시스템 정보 블록 1 또는 2 일 수 있다. 금지 정보에는 특정 금지 팩터 (barring factor) 및 특정 금지 시간 (barring time)이 포함될 수 있다. 표 4는 금지 정보 리스트의 예를 나타낸다.

표 4

[0124]

	금지 팩터(Barring Factor)	금지 시간(Barring Time)
금지 정보 #0	p05	s16
금지 정보 #1	p20	s32
금지 정보 #2	p55	s64
금지 정보 #3	P85	s128

[0125]

표 4를 참조하면, 금지 정보 리스트는 금지 정보 # 0 내지 금지 정보 # 3을 포함할 수 있으며, 금지 정보 각각은 특정 금지 팩터 및 특정 금지 시간을 포함할 수 있다.

[0126]

표 5는 금지 정보의 리스트의 예를 나타낸다. 표 5에서 금지 정보의 리스트는 BarringPerPriority로 참조될 수 있다.

표 5

[0127]

```

BarringPerPriority ::= SEQUENCE (SIZE (1..maxPriority)) OF BarringPerPriority

BarringPerPriority ::= SEQUENCE {
barringPriority#1  AC-BarringConfig  OPTIONAL,  -- Need OP,
barringPriority#2  AC-BarringConfig  OPTIONAL,  -- Need OP,
}                OPTIONAL  -- Need OP
}

AC-BarringConfig ::= SEQUENCE {
ac-BarringFactor  ENUMERATED {p00, p05, p10, p15, p20, p25, p30, p40, p50, p60, p70, p75,
p80, p85, p90, p95},
ac-BarringTime    ENUMERATED {s4, s8, s16, s32, s64, s128, s256, s512},
ac-BarringForSpecialAC  BIT STRING (SIZE(5))
}
    
```

[0128]

표 5를 참조하면, BarringPerPriority는 barringPriority # 1 및 barringPriority # 2를 포함할 수 있고, barringPriority 각각은 특정 ac-BarringFactor 및 특정 ac-BarringTime을 포함할 수 있다.

[0129]

표 6은 금지 정보 리스트의 또 다른 예를 나타낸다. 표 6에서, 금지 정보 리스트는 UAC-BarringInfoSetList로 지칭될 수 있고, 금지 정보는 UAC-BarringInfoSet로 참조될 수 있다.

표 6

[0130]

```

UAC-BarringPerCatList ::= SEQUENCE (SIZE (1..maxAccessCat-1)) OF UAC-BarringPerCat

UAC-BarringPerCat ::= SEQUENCE {
AccessCategory    INTEGER (1..maxAccessCat-1),
uac-barringInfoSetIndex    INTEGER (1.. maxBarringInfoSet)
}

UAC-BarringInfoSetList ::= SEQUENCE (maxBarringInfoSet) OF UAC-BarringInfoSet

UAC-BarringInfoSet ::= SEQUENCE {
uac-BarringFactor    ENUMERATED {p00, p05, p10, p15, p20, p25, p30, p40, p50, p60, p70, p75,
p80, p85, p90, p95},
uac-BarringTime    ENUMERATED {s4, s8, s16, s32, s64, s128, s256, s512},
uac-BarringForAccessIdentity    BIT STRING (SIZE(7))
}
    
```

[0131] 표 6을 참조하면, UAC-BarringInfoSetList는 하나 이상의 UAC-BarringInfoSet을 포함할 수 있고, UAC-BarringInfoSet 각각은 uac-BarringFactor 및 uac-BarringTime을 포함할 수 있다.

[0132] 단계 S820에서, UE는 리스트에 포함된 특정 금지 정보와 액세스 카테고리 간의 매핑 정보를 수신할 수 있다. 표 6을 참조하면, UAC-BarringPerCat은 AccessCategory 및 uac-barringInfoSetIndex를 포함할 수 있고, uac-barringInfoSetIndex는 uac-BarringInfoSetList 필드의 엔트리의 인덱스이다. 예를 들어, 값 1은 uac-BarringInfoSetList의 첫 번째 엔트리에 해당하고 값 2는 이 리스트의 두 번째 엔트리에 해당하고, 이와 같은 식으로 계속된다. 즉, uac-barringInfoSetIndex는 금지 정보의 리스트 중, Access-Category에 매핑된 특정 금지 정보를 지시할 수 있다.

[0133] 액세스 카테고리 와 금지 정보 간의 매핑 관계는 도 9를 참조하여 상세히 설명될 것이다.

[0134] 도 9는 본 발명의 일 실시 예에 따른, 적어도 하나의 액세스 카테고리 와 금지 정보 간의 매핑 관계의 예를 나타낸다.

[0135] 도 9를 참조하면, 금지 정보 # 0은 액세스 카테고리 # 1, 액세스 카테고리 # 2 및 액세스 카테고리 # 3에 매핑될 수 있다. 금지 정보 # 1은 액세스 카테고리 # 4 및 액세스 카테고리 # 5에 매핑될 수 있다. 금지 정보 # 2는 액세스 카테고리 # 6, 액세스 카테고리 # 7 및 액세스 카테고리 # 8에 매핑될 수 있다. 금지 정보 # 3은 액세스 카테고리 # 9에 매핑될 수 있다. 즉, 하나의 금지 정보는 적어도 하나의 액세스 카테고리에 매핑될 수 있다.

[0136] 표 7은 적어도 하나의 액세스 카테고리 와 우선 순위 (즉, 금지 정보) 간의 매핑 관계의 다른 예를 나타낸다.

표 7

[0137]

우선순위(Priority)	액세스 카테고리 (Access category)
0	AC#1, AC#2 (예컨대, 응급 서비스, 운영자 서비스들)
1	...
...	...
디폴트(Default)	다른 우선순위들로 구성된 것들을 제외한 모든 AC들
P	AC#N (예컨대, 지연 허용 서비스들)

[0138] 다시 도 8을 참조하면, 단계 S820에서, 네트워크는 적어도 하나의 액세스 카테고리 와 금지 정보 간의 매핑 관계의 일부를 UE에 제공할 수 있다. 네트워크는 UE에 특정 액세스 카테고리를 제공할 수 있고, 또한 네트워크는 어떤 금지 정보가 특정 액세스 카테고리에 매핑 되는지를 UE에 통지할 수 있다. 예를 들어, 네트워크는 UE에게 액세스 카테고리 # 3 및 금지 정보 # 0을 지시하는 지시를 제공할 수 있다.

[0139] 대안적으로, 단계 S820에서, 네트워크는 적어도 하나의 액세스 카테고리 와 금지 정보 간의 모든 매핑 관계를 UE에 제공할 수 있다.

- [0140] 단계 S830에서, UE는 특정 액세스 카테고리에 매핑된 특정 금지 정보에 기반하여, 특정 액세스 카테고리에 대한 액세스 금지 체크를 수행할 수 있다. 이를 위해, UE는 특정 액세스 카테고리에 대응하는 특정 금지 정보를 선택하고, 그 다음에 선택된 특정 금지 정보에 기반하여 셀에 대한 액세스가 금지되는지 여부를 결정할 수 있다. 특정 액세스 카테고리는 UE의 비-액세스 계층 (NAS) 계층으로부터 UE의 무선 자원 제어 (RRC) 계층으로 전송될 수 있다. UE RRC가 특정 액세스 카테고리를 UE RRC로 전송하고, UE RRC가 특정 액세스 카테고리에 매핑된 특정 금지 정보를 갖는 경우, UE RRC는 특정 액세스 카테고리에 매핑된 특정 금지 정보에 기반하여, 특정 액세스 카테고리에 대한 액세스 금지 체크를 수행할 수 있다.
- [0141] 단계 S840에서, UE는 액세스 카테고리에 대한 액세스 시도가 허용되면, 그 셀로의 상향링크 전송을 수행할 수 있다. 그렇지 않으면, 액세스 카테고리에 대한 액세스 시도가 금지되면, UE는 타이머를 시작할 수 있다.
- [0142] 본 발명의 일 실시 예에 따르면, 하나 이상의 액세스 카테고리들이 특정 금지 정보에 매핑될 수 있고, UE는 적어도 하나의 액세스 카테고리에 매핑된 금지 정보에 기반하여 액세스 금지 메커니즘을 수행할 수 있다. 따라서, 액세스 금지 파라미터가 각각의 액세스 카테고리들에 대해 정의되는 경우와 비교하여, 액세스 금지 파라미터들의 전송을 위한 네트워크의 시그널링이 감소될 수 있다.
- [0143] 도 10은 본 발명의 일 실시 예에 따른, 액세스 카테고리에 매핑된 액세스 금지 정보에 기반한 액세스 제어 절차를 나타낸다.
- [0144] UE들은 액세스 우선 순위들에 기반하여 액세스 금지 체크를 수행할 수 있다. 우선 순위를 위한 액세스 금지 팩터들을 포함하는 방송 지시를 수신한 후, UE는 우선 순위 기반 액세스 금지 정보에 기반하여 셀로의 액세스가 허용되는지 여부를 결정한다.
- [0145] 도 10을 참조하면, 단계 S1010에서, UE는 각 우선 순위에 대한 금지 정보 요소를 수신할 수 있다. 금지 정보 요소들의 리스트는 시스템 정보를 통해 수신된다. 예를 들어, 시스템 정보는 SIB1 또는 SIB2 일 수 있다. 그런 다음, UE는 특정 액세스 카테고리에 대응하는 우선 순위를 위한 금지 정보를 선택할 수 있다. 우선 순위 및 액세스 카테고리는 UE의 NAS 계층에 의해 지시된다. 대안적으로, 우선 순위는 네트워크에 의해 통지되고, 액세스 카테고리는 UE의 NAS 계층에 의해 지시된다.
- [0146] 하나 이상의 액세스 카테고리들은 도 10에 도시된 바와 같이 액세스 우선 순위를 구성할 수 있다. 우선 순위 정의는 네트워크에 의해 사전-구성되거나 통지될 수 있다. 예를 들어 등록 동안에 우선 순위 정의가 통지될 수 있다. 초기 등록을 위해, 운영자가 사전-구성된 액세스 우선 순위 정보, 예컨대 범용 집적 회로 카드 (UICC)를 제공하지 않으면, UE는 액세스 우선 순위를 알지 못할 수 있다. UE는 등록 수락(Registration Accept)의 수신 시 액세스 우선 순위 정보를 수신할 것이다. UE NAS 계층은 요청을 제출하는 경우 정보를 유지하여 UE RRC 계층으로 전달할 수 있다.
- [0147] 표 7을 참조하면 액세스 우선 순위는 표준화된 우선 순위와 운영자-구성 우선 순위들로 구성될 수 있다. 또한, 임의의 우선 순위가 지정되지 않은 액세스에 대해 디폴트 액세스 우선 순위(Default access priority)가 정의될 수 있다. 일부 액세스들이 지연 허용 서비스(delay tolerant services)에 대해 정의되고 우선 순위는 가장 낮아야 하므로, 디폴트 우선 순위는 가장 낮은 우선 순위로 설정하지 않아도 된다.
- [0148] 단계 S1020에서, UE는 선택된 금지 정보에 기반하여 셀에 대한 액세스가 금지되는지 여부를 결정할 수 있다. 예를 들어, UE RRC 계층은 NAS 요청에 포함된 우선 순위 및 네트워크로부터 방송된 액세스 금지 정보에 기반하여 셀에 대한 액세스가 허용되는지 여부를 결정할 수 있다.
- [0149] 단계 S1030에서, UE는 액세스 카테고리에 대한 액세스 시도가 허용되면 그 셀로의 상향링크 전송을 수행할 수 있다. 그렇지 않으면, 액세스 카테고리에 대한 액세스 시도가 금지되면, UE는 타이머를 시작할 수 있다.
- [0150] 한편, 5G에서 네트워크 기능 최적화를 위해 네트워크 슬라이싱이 지원된다. 네트워크 운영자는 서로 다른 서비스 그룹들에 대해 서로 다른 네트워크 슬라이스 인스턴스들을 배치(deploy)할 수 있다. 각 PDU 세션은 특정 네트워크 슬라이스에 전용될 수 있다. 이를 기반으로, 네트워크는 고객들에게 차별화된 서비스를 제공할 수 있다. 특정 서비스를 지원하려면, 네트워크 운영자가 여러 네트워크 슬라이스들을 할당해야 할 수 있다. 예를 들어, 일반적인 IMS 서비스는 4G에서 3 개의 EPS 베어러들을 사용하기 때문에 3개의 네트워크 슬라이스들에 매핑하여 약 3개의 PDU 세션들을 필요로 할 수 있다; 하나는 시그널링 전송 용이고 다른 하나는 음성 통화 용이고 다른 하나는 화상 통화 용이다. 즉, 세 개의 네트워크 슬라이스들이 IMS 서비스에 할당된다. 따라서 네트워크가 특정 서비스의 트래픽을 정확하게 제어하기 위해서는, 해당 서비스에 할당된 여러 네트워크 슬라이스에 제어가 적용

되어야 한다. 5G 시스템에서 액세스 금지 메커니즘은 액세스 카테고리들을 기반으로 수행된다. 액세스 카테고리들은 정의에서 서비스 유형을 포함하기 때문에, 네트워크 슬라이싱 및 액세스 카테고리들에는 이들 간의 관계가 있다. 즉, 액세스 금지는 네트워크 슬라이스들을 기반으로 수행될 수 있다.

[0151] 본 발명의 일 실시 예에 따르면, UE는 네트워크 슬라이스 그룹 기반 금지 구성을 사용하여 액세스 금지 체크를 수행할 수 있다. 금지 구성은 네트워크 슬라이스 그룹 및 액세스 카테고리들의 매핑을 기반으로 할 수 있다. 각 네트워크 슬라이스 그룹은 하나 이상의 액세스 카테고리들에 매핑될 수 있다. 매핑은 UE 자체에 의해 결정되거나 또는 네트워크 운영자에 의해 제공될 수 있다.

[0152] 네트워크 슬라이스 그룹은 도 11에 도시된 바와 같이 정의될 수 있다. 하나 이상의 네트워크 슬라이스들이 네트워크 슬라이스 그룹을 구성할 수 있다. 각 슬라이스 그룹은 액세스 금지 팩터가 각 액세스 카테고리에 할당될 수 있는 하나 이상의 액세스 카테고리들에 매핑될 수 있다. UE가 등록된 PLMN이 네트워크 슬라이싱을 지원하고 UE가 사전-구성된 슬라이싱 정보를 갖는다면, UE는 구성된 그룹 정보를 사용할 수 있다. 또는, 정보는 등록 수락 메시지(Registration Accept message)를 통해 전달될 수 있다.

[0153] 초기 등록 동안, UE는 네트워크 슬라이스 그룹 정보를 알지 못할 수 있다. 네트워크는 등록 수락을 UE에 전송하는 경우 그룹 정보를 통지할 것이다. 그룹 정보는 UE NAS 계층에서 유지될 수 있고 UE가 연결 설정을 요청하는 경우 UE RRC 계층으로 전달될 수 있다. 네트워크 슬라이스 그룹 정보는 도 12에 제시된 바와 같은 디폴트 슬라이스 그룹(Default Slice Group)을 포함할 수 있다. 슬라이스 그룹이 UE에 적용될 수 없는 경우, UE는 디폴트 슬라이스 그룹을 사용할 것이다. gNB는 슬라이스 그룹들에 기반으로 액세스 금지 정보를 전송할 수 있다. 심지어 디폴트 슬라이스 그룹이 이용 가능하지 않은 경우, UE는 도 13에 제시된 바와 같이 액세스 카테고리들만을 기반으로 공통 금지 체크를 수행할 수 있다. 네트워크 슬라이싱은 선택적인 특성이기 때문에, 네트워크 슬라이싱을 지원하지 않는 PLMN들에 등록된 UE들은 물론 공통 금지 체크를 수행할 수 있다.

[0154] 도 14는 본 발명의 일 실시 예에 따른, 네트워크 슬라이스 그룹에 따른 액세스 금지 메커니즘을 나타낸다.

[0155] 도 14를 참조하면, 초기 등록 절차는 단계 S1400 내지 단계 S1420을 포함하고, 성공적인 등록 이후 절차는 단계 S1430 내지 단계 S1450을 포함한다.

[0156] 단계 S1400에서, UE는 gNB로부터 방송 지시 (예컨대, SystemInformationBlock1 또는 2)를 통해 액세스 금지 정보를 수신할 수 있다. PLMN이 액세스 제어를 위한 디폴트 슬라이스 그룹을 정의하는 경우, 방송 지시는 그룹에 대한 금지 정보를 포함할 수 있다. 대안적으로, PLMN이 디폴트 슬라이스 그룹을 정의하지 않거나 또는 네트워크 슬라이싱을 지원하지 않으면, 방송 지시는 공통 액세스 금지 정보를 포함할 수 있다. 방송 지시 메시지 (예를 들어, SystemInformationBlock1 또는 2)는 표 8과 같은 슬라이스 그룹들에 기반하여 금지 정보를 제공할 수 있다.

표 8

[0157]

```
SystemInformationBlockType2 ::= SEQUENCE {
ac-BarringInfoSliceGroup#1 SEQUENCE {
ac-BarringForAccessCategory#1 BOOLEAN,
ac-BarringForAccessCategory#2 AC-BarringConfig OPTIONAL, -- Need OP
}
ac-BarringInfoSliceGroup#2 SEQUENCE {
ac-BarringForAccessCategory#5 AC-BarringConfig OPTIONAL, -- Need OP
}
ac-BarringInfoDefaultSliceGroup SEQUENCE {
ac-BarringForAccessCategory#3 AC-BarringConfig OPTIONAL, -- Need OP
ac-BarringForAccessCategory#4 AC-BarringConfig OPTIONAL, -- Need OP
}
}
```

[0158] UE가 등록(Registration)을 요청하면, UE NAS 계층은 UE RRC 계층으로의 연결 설정을 위해 필요한 정보를 통지할 수 있다. UE가 디폴트 슬라이스 그룹을 사전-구성한 경우, UE NAS 계층은 이용 가능하다면, 슬라이스를 통지하고, 선택적으로 UE RRC 계층에 카테고리 정보 (예컨대, sliceGroupId, accessCategoryId)를 액세스할 수 있다. 대안적으로, UE가 슬라이스 정보를 갖지 않으면, UE NAS 계층은 UE RRC 계층에 액세스 카테고리를 통지할

수 있다.

- [0159] UE RRC 계층은 금지 정보를 선택하고 셀에 대한 액세스가 금지되는지 여부를 결정할 수 있다.
- [0160] 단계 S1410에서, 금지되지 않으면, UE는 등록 요청(Registration Request)을 전송할 수 있다.
- [0161] 단계 S1420에서, UE는 슬라이스 그룹 정보로 등록 수락을 수신하고 등록된 PLMN에 대한 그룹 정보를 업데이트할 수 있다. 슬라이스 그룹 정보는 슬라이스 그룹 식별자 (예컨대, sliceGroupId) 및 연관된 액세스 카테고리 리스트들을 포함할 수 있다.
- [0162] 단계 S1430에서, UE는 방송 지시 (예를 들어, SystemInformationBlock1 또는 2)를 통해 네트워크 슬라이스 그룹에 기반하여 액세스 금지 정보를 수신할 수 있다. 방송 지시 메시지 (예를 들어, SystemInformationBlock1 또는 2)는 표 8과 같은 슬라이스 그룹들에 기반하여 금지 정보를 제공할 수 있다. 그런 다음, UE는 PLMN에 대한 액세스 금지 정보를 업데이트할 수 있다. RRC 연결 설정 동안, UE RRC 계층은 특정 액세스 카테고리에 대응하는 네트워크 슬라이스 그룹에 대한 금지 정보를 선택할 수 있다.
- [0163] 그런 다음, 단계 S1440에서, UE는 셀에 대한 액세스가 금지되는지 여부를 결정할 수 있다.
- [0164] 단계 S1450에서, UE는 액세스 카테고리에 대한 액세스 시도가 허용되면 RRC 연결 요청을 네트워크에 전송한다. 그렇지 않으면, 액세스 카테고리에 대한 액세스 시도가 금지되면, UE는 타이머를 시작할 수 있다.
- [0165] 본 발명의 일 실시 예에 따르면, UE는 각 네트워크 슬라이스 그룹에 대한 금지 정보 팩터 수신할 수 있다. 금지 정보 요소의 리스트는 시스템 정보를 통해 수신된다. 그런 다음, UE는 특정 액세스 카테고리에 대응하는 네트워크 슬라이스 그룹에 대한 금지 정보를 선택할 수 있다. 슬라이스 그룹은 UE의 NAS 계층에 의해 지시될 수 있다. 그런 다음, UE는 선택된 금지 정보에 기반하여 셀에 대한 액세스가 금지되는지 여부를 결정할 수 있다.
- [0166] 도 15는 본 발명의 일 실시 예에 따른, UE가 액세스 금지 체크를 수행하는 방법을 도시한 블록도이다.
- [0167] 도 15를 참조하면, 단계 S1510에서 UE는 금지 정보의 리스트를 수신할 수 있다. 각 금지 정보는 특정 금지 팩터 및 특정 금지 시간을 포함할 수 있다.
- [0168] 금지 정보의 리스트는 네트워크로부터 수신할 수 있다. 금지 정보의 리스트는 시스템 정보를 통해 수신될 수 있다.
- [0169] 단계 S1520에서, UE는 리스트에 포함된 특정 금지 정보와 관련된 액세스 카테고리에 관한 정보를 수신할 수 있다. 예를 들어, 상기 정보는 리스트에 포함된 특정 금지 정보와 액세스 카테고리 간의 매핑 정보일 수 있다. 리스트에 포함된 특정 금지 정보는 하나 이상의 액세스 카테고리들과 관련될 수 있다. 매핑 정보는 네트워크로부터 수신될 수 있다.
- [0170] 단계 S1530에서, UE는 액세스 카테고리에 관한 특정 금지 정보에 기반하여 액세스 카테고리에 대한 액세스 금지 체크를 수행할 수 있다.
- [0171] 액세스 카테고리가 하나 이상의 액세스 카테고리들에 포함되는 경우, 액세스 카테고리에 대한 액세스 금지 체크는 액세스 카테고리 및 관련된 특정 금지 정보에 기반하여 수행될 수 있다.
- [0172] 액세스 카테고리는 UE의 비-액세스 계층 (NAS) 계층으로부터 UE의 무선 자원 제어 (RRC) 계층으로 전송될 수 있다. 액세스 카테고리가 UE의 NAS 계층으로부터 UE의 RRC 계층으로 전송되는 경우, 액세스 카테고리에 관한 특정 금지 정보에 기반하여 액세스 카테고리에 대한 액세스 금지 체크가 수행될 수 있다.
- [0173] 단계 S1540에서, UE는 액세스 카테고리에 대한 액세스 시도가 허용되면, 상향링크 전송을 수행할 수 있다. 상향링크 전송은 무선 자원 제어 (RRC: Radio Resource Control) 연결 요청 메시지의 전송을 포함한다. 대안적으로, 액세스 카테고리에 대한 액세스 시도가 금지되면, UE는 액세스 카테고리에 대한 타이머를 시작할 수 있다.
- [0174] 본 발명의 일 실시 예에 따르면, 하나 이상의 액세스 카테고리들이 특정 금지 정보에 매핑될 수 있고, 그런 다음 UE는 적어도 하나의 액세스 카테고리에 매핑된 금지 정보에 기반하여 액세스 금지 메커니즘들을 수행할 수 있다. 따라서, 각 액세스 카테고리에 대해 금지 정보가 정의되는 경우와 비교하여, 금지 정보의 전송을 위한 네트워크의 시그널링이 감소될 수 있다.
- [0175] 도 16은 본 발명의 실시 예가 구현되는 무선 통신 시스템의 블록도이다.
- [0176] 기지국(1600)은 프로세서(processor, 1601), 메모리(memory, 1602) 및 송수신기(transceiver, 1603)를 포함한다

다. 메모리(1602)는 프로세서(1601)와 연결되어, 프로세서(1601)를 구동하기 위한 다양한 정보를 저장한다. 송수신기(1603)는 프로세서(1601)와 연결되어, 무선 신호를 송신 및/또는 수신한다. 프로세서(1601)는 제안된 기능, 과정 및/또는 방법을 구현한다. 전술한 실시 예에서 기지국의 동작은 프로세서(1601)에 의해 구현될 수 있다.

[0177] 단말(1610)은 프로세서(1611), 메모리(1612) 및 송수신기(1613)를 포함한다. 메모리(1612)는 프로세서(1611)와 연결되어, 프로세서(1611)를 구동하기 위한 다양한 정보를 저장한다. 송수신기(1613)는 프로세서(1611)와 연결되어, 무선 신호를 송신 및/또는 수신한다. 프로세서(1611)는 제안된 기능, 과정 및/또는 방법을 구현한다. 전술한 실시 예에서 단말의 동작은 프로세서(1611)에 의해 구현될 수 있다.

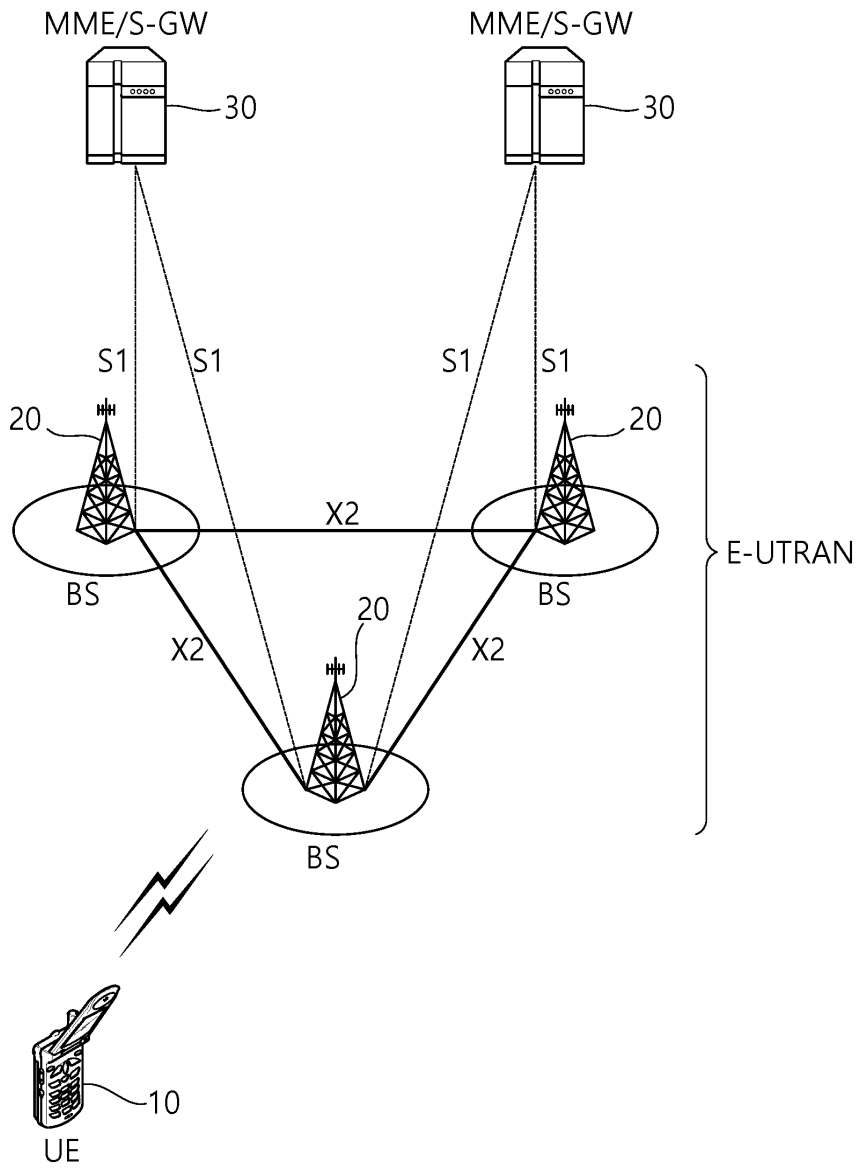
[0178] 프로세서는 ASIC(application-specific integrated circuit), 다른 칩셋, 논리 회로 및/또는 데이터 처리 장치를 포함할 수 있다. 메모리는 ROM(read-only memory), RAM(random access memory), 플래시 메모리, 메모리 카드, 저장 매체 및/또는 다른 저장 장치를 포함할 수 있다. 송수신기는 무선 신호를 처리하기 위한 베이스밴드 회로를 포함할 수 있다. 실시 예가 소프트웨어로 구현될 때, 상술한 기법은 상술한 기능을 수행하는 모듈(과정, 기능 등)로 구현될 수 있다. 모듈은 메모리에 저장되고, 프로세서에 의해 실행될 수 있다. 메모리는 프로세서 내부 또는 외부에 있을 수 있고, 잘 알려진 다양한 수단으로 프로세서와 연결될 수 있다.

[0179] 상술한 일례들에 기초하여 본 명세서에 따른 다양한 기법들이 도면과 도면 부호를 통해 설명되었다. 설명의 편의를 위해, 각 기법들은 특정한 순서에 따라 다수의 단계나 블록들을 설명하였으나, 이러한 단계나 블록의 구체적인 순서는 청구항에 기재된 발명을 제한하는 것이 아니며, 각 단계나 블록은 다른 순서로 구현되거나, 또 다른 단계나 블록들과 동시에 수행되는 것이 가능하다. 또한, 통상의 기술자라면 간 단계나 블록이 한정적으로 기술된 것이나 아니며, 발명의 보호 범위에 영향을 주지 않는 범위 내에서 적어도 하나의 다른 단계들이 추가되거나 삭제되는 것이 가능하다는 것을 알 수 있을 것이다.

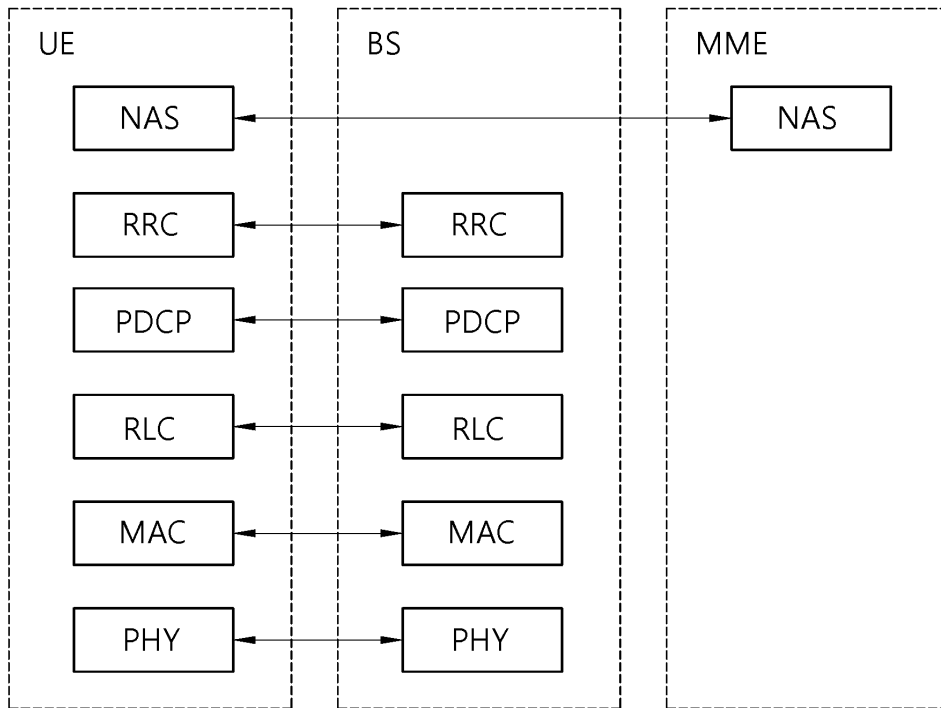
[0180] 상술한 실시 예는 다양한 일례를 포함한다. 통상의 기술자라면 발명의 모든 가능한 일례의 조합이 설명될 수 없다는 점을 알 것이고, 또한 본 명세서의 기술로부터 다양한 조합이 파생될 수 있다는 점을 알 것이다. 따라서 발명의 보호범위는, 이하 청구항에 기재된 범위를 벗어나지 않는 범위 내에서, 상세한 설명에 기재된 다양한 일례를 조합하여 판단해야 할 것이다.

도면

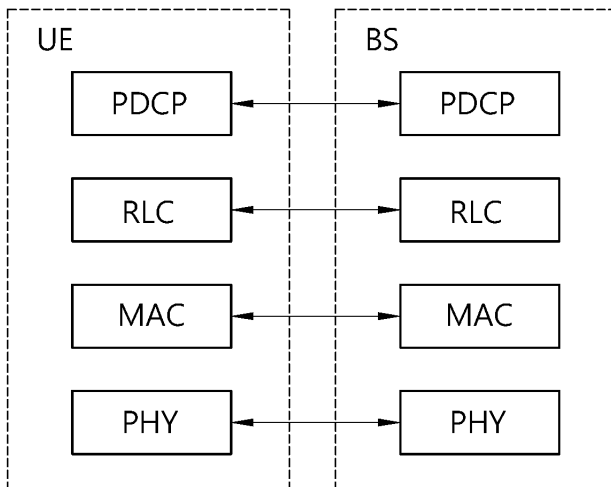
도면1



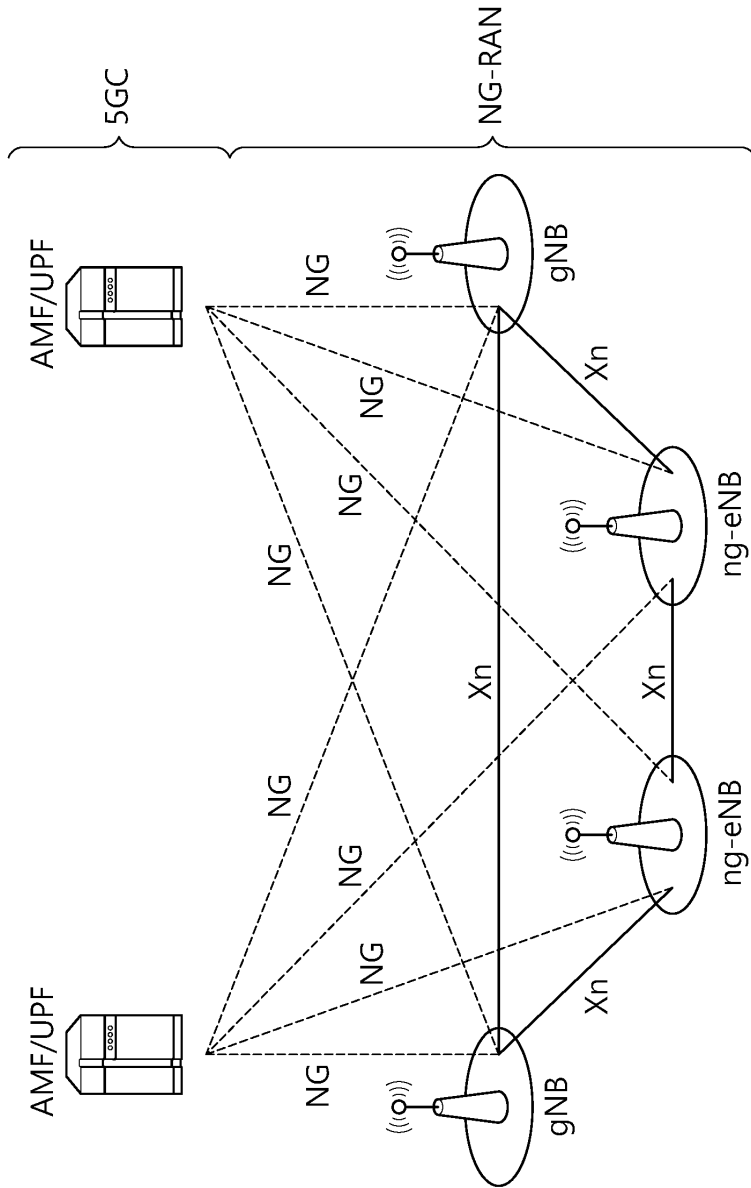
도면2



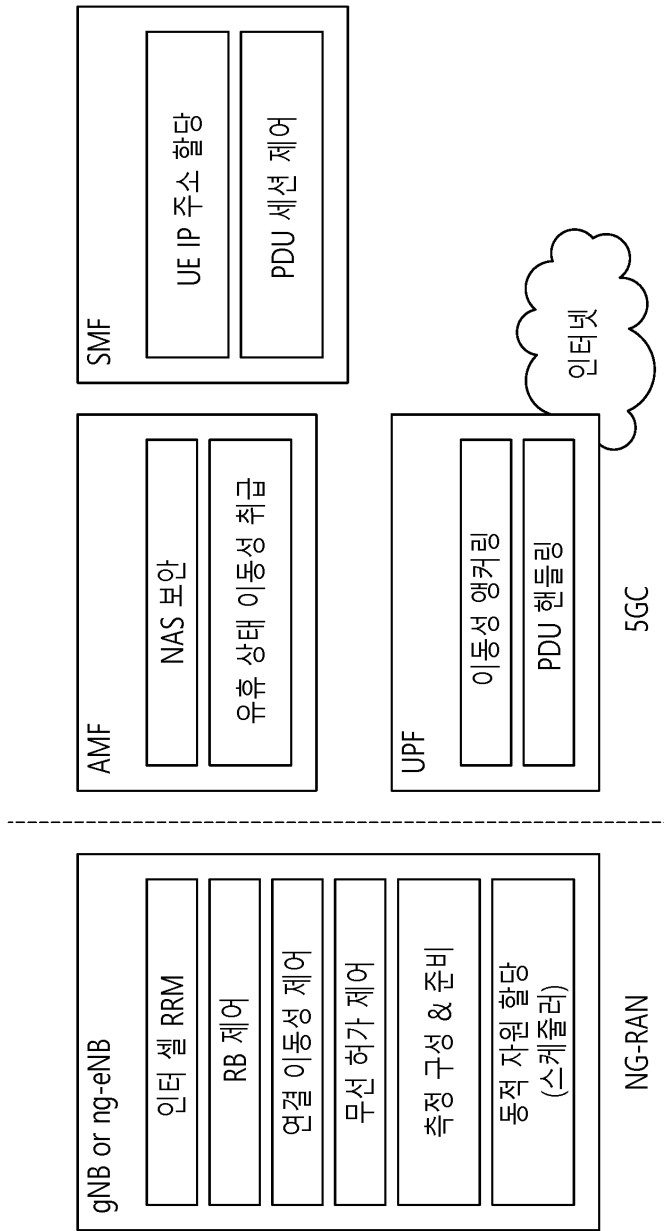
도면3



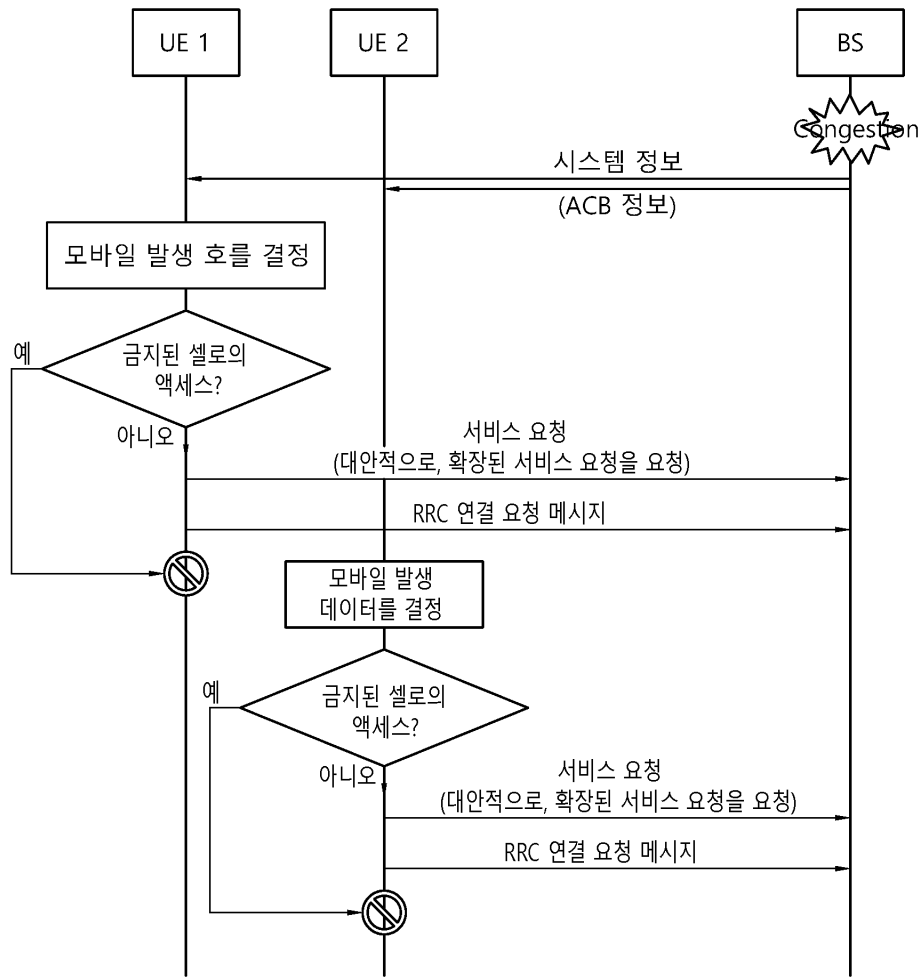
도면4



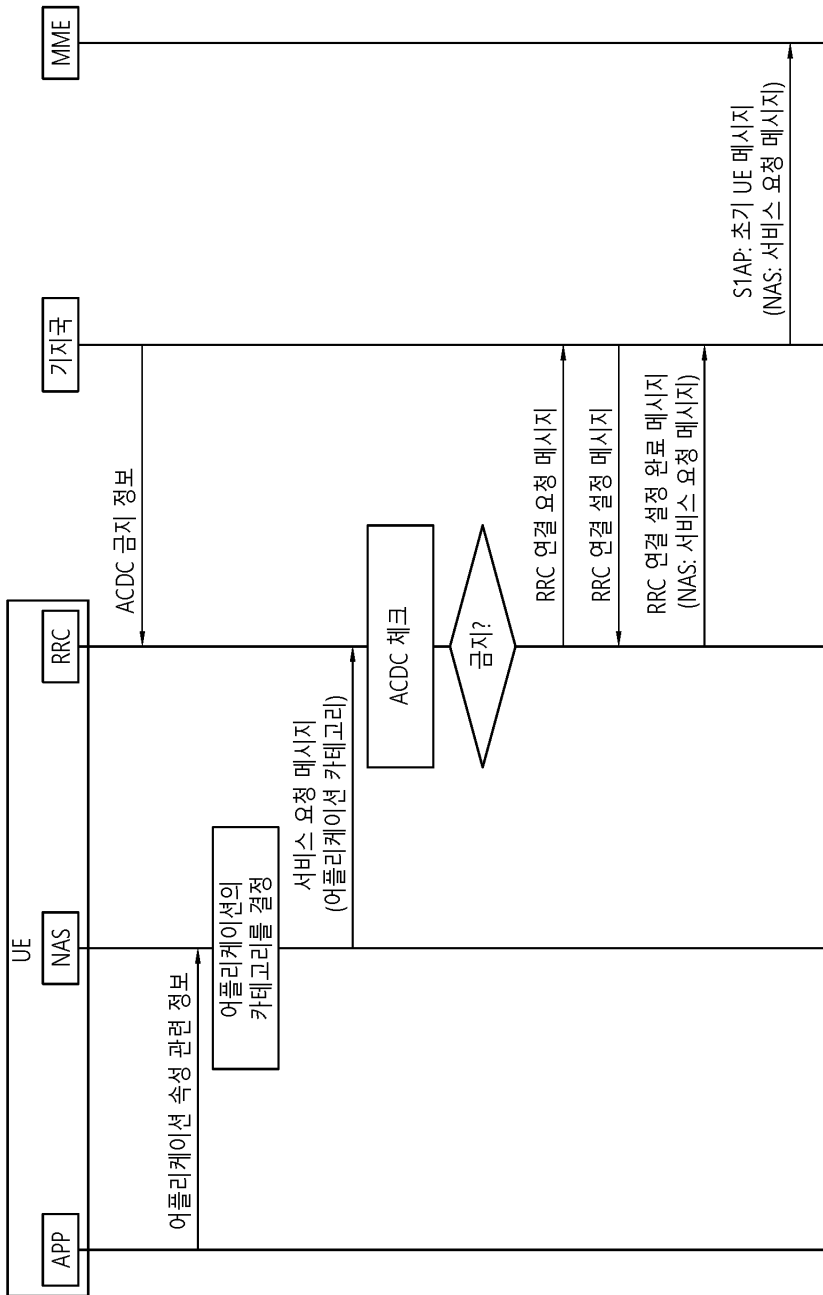
도면5



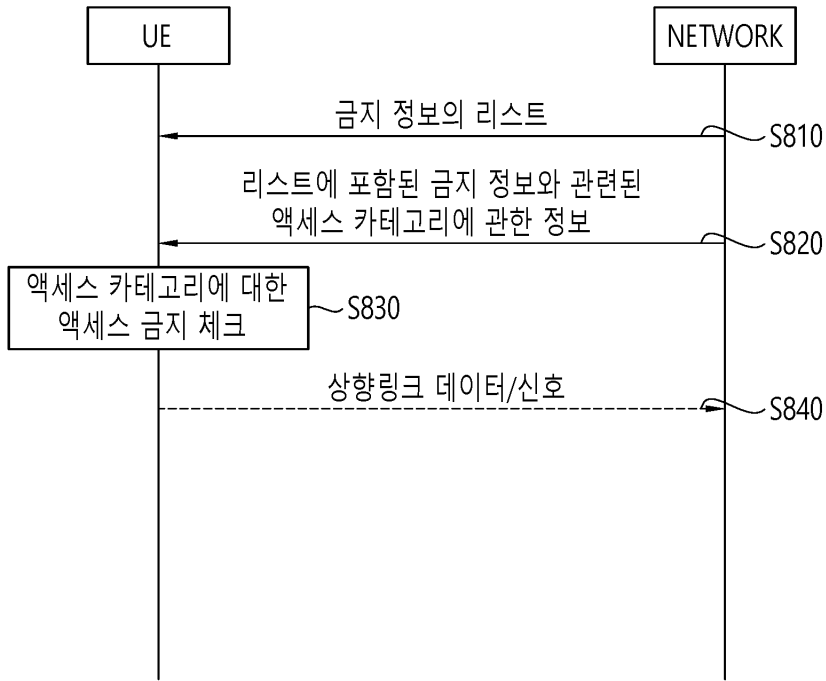
도면6



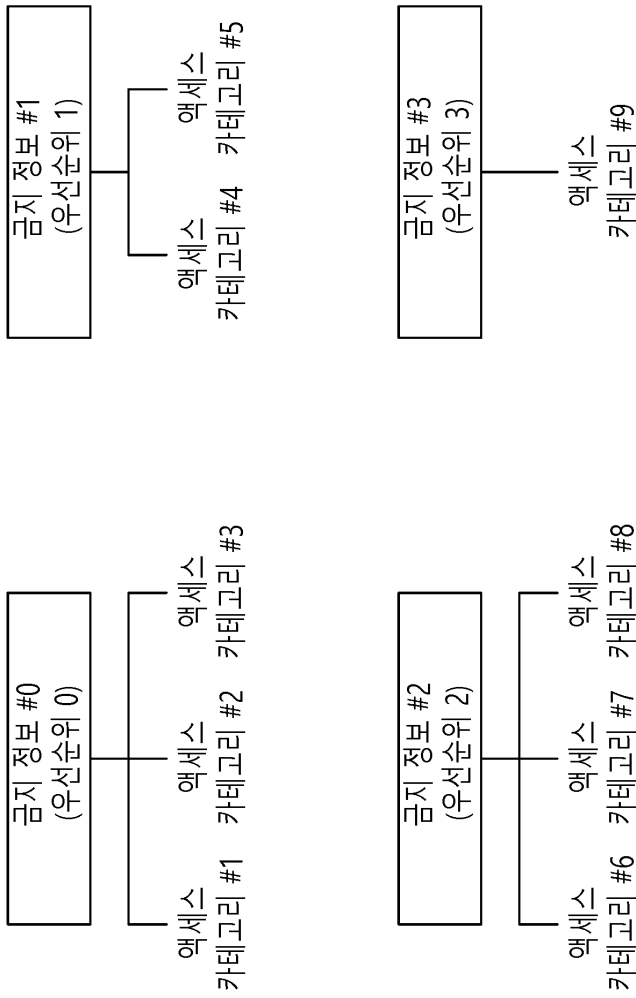
도면7



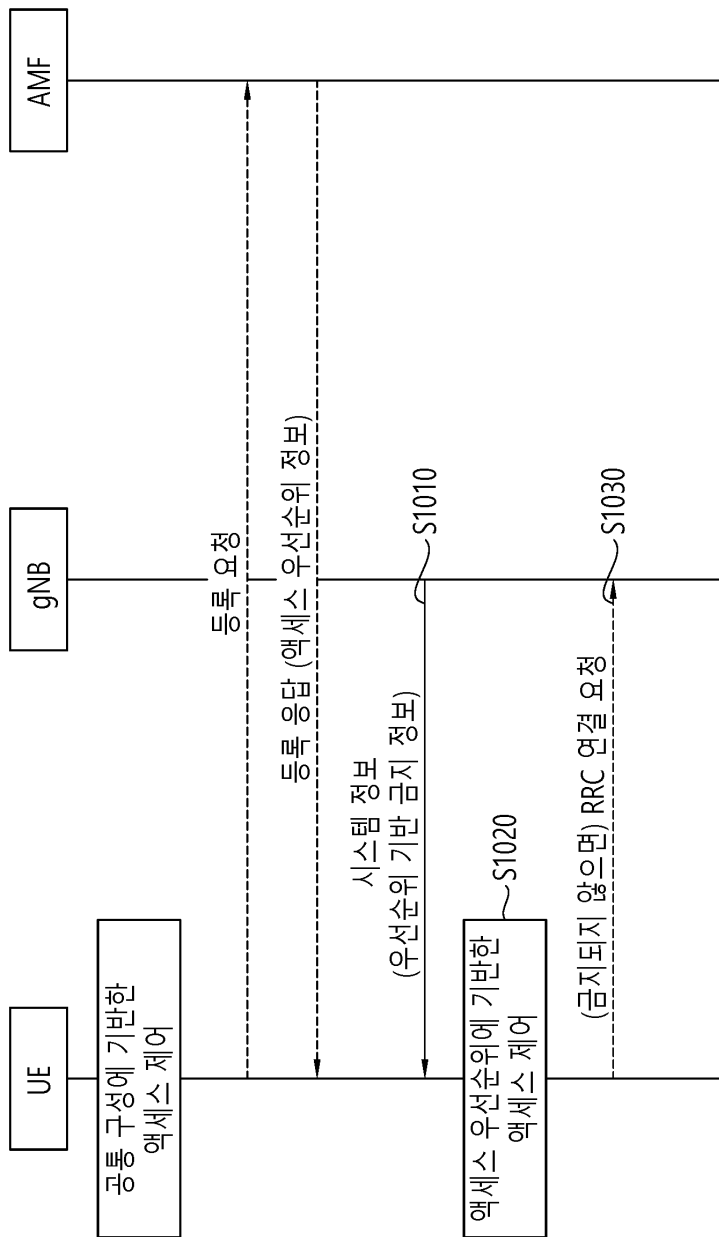
도면8



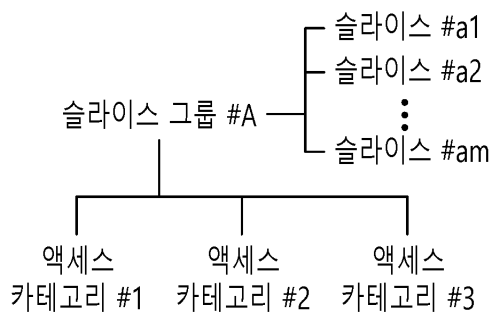
도면9



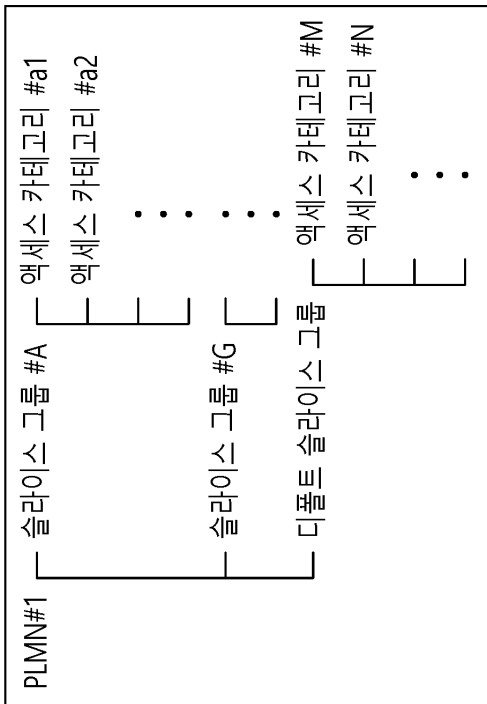
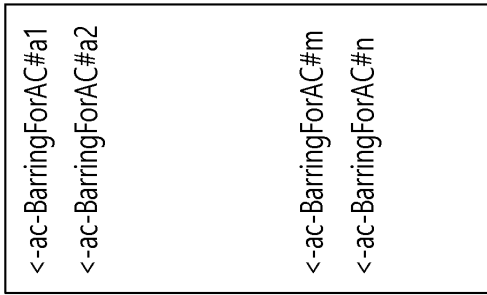
도면10



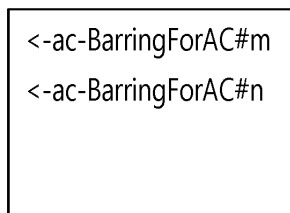
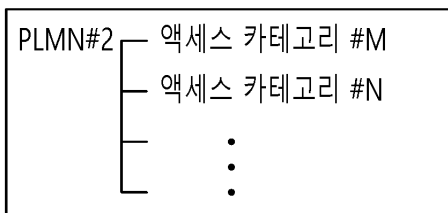
도면11



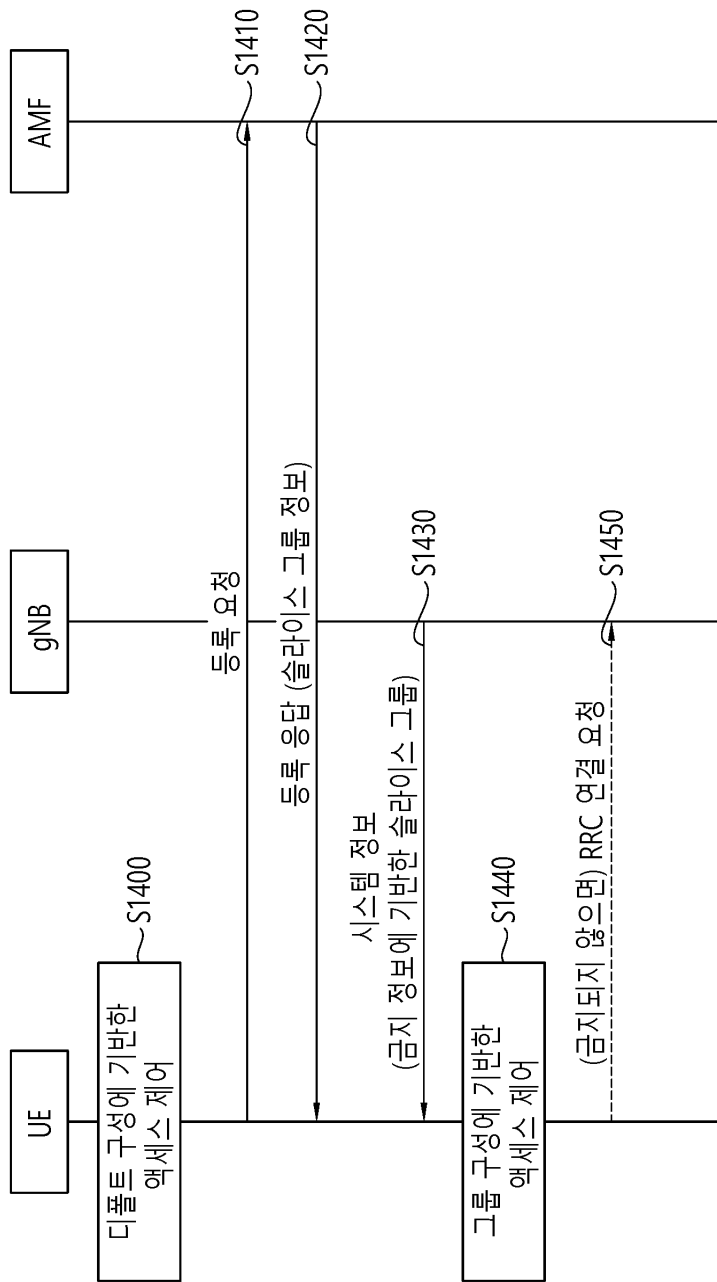
도면12



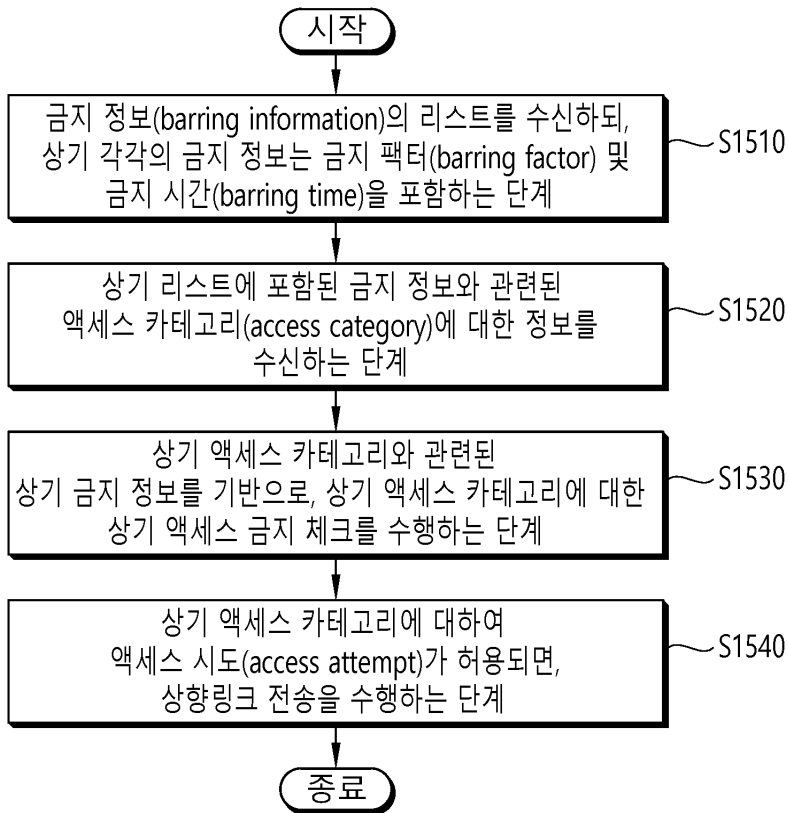
도면13



도면14



도면15



도면16

