(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년05월20일
(11) 등록번호 10-0959047
(24) 등록일자 2010년05월13일

(51) Int. Cl.
H04L 9/14 (2006.01)
(21) 출원번호 10-2004-7006888
(22) 출원일자(국제출원일자) 2002년10월31일
심사청구일자 2007년10월31일
(85) 번역문제출일자 2004년05월06일
(65) 공개번호 10-2004-0053282
(43) 공개일자 2004년06월23일
(86) 국제출원번호 PCT/US2002/035297
(87) 국제공개번호 WO 2003/041442
국제공개일자 2003년05월05일
(30) 우선권주장
10/011,964 2001년11월05일 미국(US)
(56) 선행기술조사문헌
WO2001049058 A1*
WO2001063954 A1*
KR100864077 B1
KR1020010102406 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
퀵로이프랭클린주니어
미국92107캘리포니아주샌디에고바르셀로나드라이브1150
호사이이우덩컨
미국92122캘리포니아주샌디에고피오레테라스5225넘버디117
(74) 대리인
특허법인코리아나

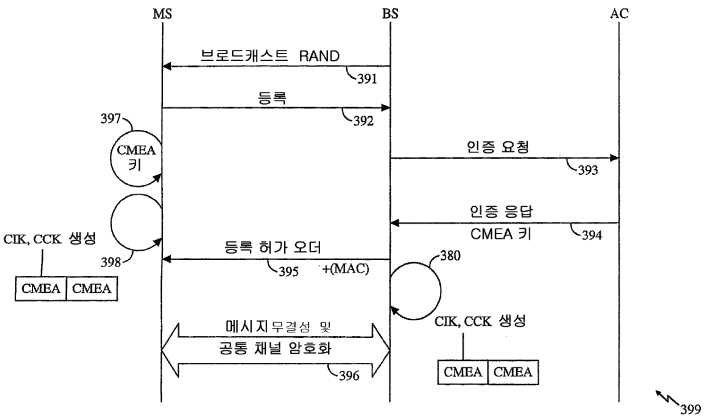
전체 청구항 수 : 총 13 항 심사관 : 조영제

(54) CDMA 통신 시스템에서의 메시지 무결성을 위한 방법 및 장치

(57) 요 약

통신 시스템 (100) 에서, 인증 센터 (198), 또는 인증 센터 (198) 와 이동 스위칭 센터 (199) 사이의 인터페이스 (197) 의 동작 버전에 관계없이 메시지 무결성을 위한 방법 및 장치를 제공한다. 이 방법 및 장치는 CMEA (cellular message encryption algorithm) 키를 생성하는 것과, 이동국과 기지국 사이의 메시지 보존을 위한 CMEA 키를 기초하여 CIK (CMEA-key-derived integrity key) 를 생성하는 것을 포함하다. 이동국은 등록 메시지를 기지국으로 송신하고, 이동국이 기지국으로부터 등록 허가 오더 또는 인증 벡터의 일부 엘리먼트들을 수신하는지 여부에 기초하여 기지국과 통신하는 인증 센터 (198) 의 동작 버전을 결정한다. 만일 이동국이 기지국으로부터 유효한 등록 허가 오더를 수신하면, CIK 가 CMEA 키에 기초하여 생성된다.

대 표 도



특허청구의 범위

청구항 1

기지국, 이동국, 및 상기 이동국에 관련된 인증 정보를 관리하기 위한 인증 센터를 포함하는 통신 시스템에서 메시지 무결성 (integrity) 을 위한 방법으로서,

상기 이동국으로부터 상기 기지국으로 등록 메시지를 송신하는 단계;

CMEA (cellular message encryption algorithm) 키를 생성하는 단계; 및

상기 이동국이 상기 기지국으로부터 등록 허가 오더를 수신하는 경우, 상기 이동국과 상기 기지국 사이의 메시지 무결성을 위해 상기 CMEA 키에 기초하여 상기 이동국에서 국부적으로 CIK (CMEA-key-derived integrity key) 를 생성하는 단계를 포함하는, 메시지 무결성을 위한 방법.

청구항 2

제 1 항에 있어서,

상기 CIK 를 생성하는 단계는 상기 CMEA 키를 2 회 반복하여 상기 CIK 를 생성하는 단계를 포함하는, 메시지 무결성을 위한 방법.

청구항 3

제 1 항에 있어서,

상기 이동국과 상기 기지국은 각각 상기 통신 시스템의 역방향 통신 및 순방향 통신에 대하여 상기 CMEA 키에 기초하여 상기 CIK 를 생성하는 단계를 국부적으로 수행하는, 메시지 무결성을 위한 방법.

청구항 4

기지국, 이동국, 및 상기 이동국에 관련된 인증 정보를 관리하기 위한 인증 센터를 포함하는 통신 시스템에서 메시지 무결성 (integrity) 을 위한 장치로서,

상기 이동국으로부터 상기 기지국으로 등록 메시지를 송신하는 수단;

CMEA (cellular message encryption algorithm) 키를 생성하는 수단; 및

상기 이동국이 상기 기지국으로부터 등록 허가 오더를 수신하는 경우, 상기 이동국과 상기 기지국 사이의 메시지 무결성을 위해 상기 CMEA 키에 기초하여 상기 이동국에서 국부적으로 CIK (CMEA-key-derived integrity key) 를 생성하는 수단을 구비하는, 메시지 무결성을 위한 장치.

청구항 5

제 4 항에 있어서,

상기 CIK 를 생성하는 수단은 상기 CMEA 키를 2 회 반복하여 상기 CIK 를 생성하는 수단을 구비하는, 메시지 무결성을 위한 장치.

청구항 6

제 4 항에 있어서,

상기 이동국과 상기 기지국은 각각 역방향 통신 및 순방향 통신에 대하여 상기 CMEA 키에 기초하여 상기 CIK 를 생성하는 것을 국부적으로 수행하는 수단을 구비하는, 메시지 무결성을 위한 장치.

청구항 7

기지국, 이동국, 및 상기 이동국에 관련된 인증 정보를 관리하기 위한 인증 센터를 포함하는 통신 시스템에서 메시지 무결성 (integrity) 을 위한 프로세서로서,

상기 이동국으로부터 상기 기지국으로 등록 메시지를 송신하는 수단;

CMEA (cellular message encryption algorithm) 키를 생성하는 수단; 및

상기 이동국이 상기 기지국으로부터 등록 허가 오더를 수신하는 경우, 상기 이동국과 상기 기지국 사이의 메시지 무결성을 위해 상기 CMEA 키에 기초하여 상기 이동국에서 국부적으로 CIK (CMEA-key-derived integrity key) 를 생성하는 수단을 구비하는, 메시지 무결성을 위한 프로세서.

청구항 8

제 7 항에 있어서,

상기 CIK 를 생성하는 수단은 상기 CMEA 키를 2 회 반복하여 상기 CIK를 생성하는 수단을 구비하는, 메시지 무결성을 위한 프로세서.

청구항 9

이동국에서 메시지 무결성 (integrity) 을 위한 방법으로서,

등록 메시지를 기지국에 송신하는 단계; 및

상기 이동국이 상기 기지국으로부터 등록 허가 오더 또는 인증 벡터의 엘리먼트들을 수신하는지 여부에 기초하여 상기 기지국과 통신하는 인증 센터의 동작 버전을 결정하는 단계를 포함하는, 메시지 무결성을 위한 방법.

청구항 10

제 9 항에 있어서,

CMEA (cellular message encryption algorithm) 키를 생성하는 단계; 및

상기 이동국이 상기 기지국으로부터 상기 등록 허가 오더를 수신하는 경우, 상기 이동국과 기지국 사이의 메시지 무결성을 위해 상기 CMEA 키에 기초하여 CIK (CMEA-key-derived integrity key) 를 생성하는 단계를 더 포함하는, 메시지 무결성을 위한 방법.

청구항 11

제 10 항에 있어서,

상기 CIK 를 생성하는 단계는 상기 CMEA 키를 2 회 반복하여 상기 CIK 를 생성하는 단계를 포함하는, 메시지 무결성을 위한 방법.

청구항 12

제 10 항에 있어서,

상기 이동국과 상기 기지국은 각각 상기 통신 시스템의 역방향 통신 및 순방향 통신에 대하여 상기 CMEA 키에 기초하여 상기 CIK 를 생성하는 단계를 국부적으로 수행하는, 메시지 무결성을 위한 방법.

청구항 13

제 10 항에 있어서,

상기 CIK 에 기초하여 MAC (message authentication code) 를 생성하는 단계; 및

상기 이동국에 대한 상기 등록 허가 오더의 통신을 위해 상기 MAC 를 이용하여 상기 기지국의 합법성을 검증하는 단계를 더 포함하는, 메시지 무결성을 위한 방법.

명 세 서

[0001] **분야**

[0002] 본 발명은 일반적으로 통신 분야에 관한 것으로, 더욱 상세하게는 셀룰라 통신 시스템의 통신에 관한 것이다.

[0003] **배경**

[0004] CDMA (code division multiple access) 통신 시스템들은 초기 세대로부터 더욱 더 진보된 세대까지 발전되고 있다. 시스템 업데이트시에, 시스템의 다양한 동작들과 연관되는 하나 이상의 파라미터가 변화할 수도 있다. 또한, 이러한 새로운 파라미터들내에서 더욱 진보된 시스템의 이동국들이 동작하도록 업데이트되고 있다. 초기 세대의 시스템들 중 하나는 본 명세서에 참고로 포함된 TIA/EIA-95A/B 표준에 정의되는 파라미터들에 따라 동작한다. 더욱 더 진보된 시스템들 중 하나는 본 명세서에 참고로 포함된 TIA/EIA-IS-2000-A 표준에 따라 동작한다. 이 특허 출원시에는, TIA/EIA-IS-2000-A 표준의 새로운 버전은 개발단계에 있고 여기서 참조되는 TIA/EIA-IS-2000-B 표준으로 릴리즈되어 있다. 표준들의 카피는 어드레스 : http://www.3gpp2.org 에서 월드 와이드 웹에 액세스하거나 또는 TIA, Standards and Technology Department, 2500 Wilson Boulevard, Arlington, VA 22201, United States of America 에 가입함으로써 획득될 수도 있다.

[0005] 통신 시스템은 많은 서로 다른 구성요소들을 갖는다. 각 구성요소의 동작 파라미터들은 대응하는 표준에 의해 정의된다. 시스템은 대응하는 표준의 새로운 버전에 따라 동작하도록 어떤 구성요소들을 변경함으로써 부분적으로 업데이트될 수도 있다. 제안된 TIA/EIA-IS-2000-B 표준의 필수적이고 본질적인 특징들 중 하나는 이동국과 기지국 사이에 통신의 메시지 무결성을 제공하는 것이다. 메시지 무결성은 메시지의 전송자의 합법성을 보증한다. 메시지 무결성을 달성하기 위하여, AKA (Authentication and Key Agreement) 과정이 표준의 관련 부분들에서 개발되어 정의되어 있다. AC (Authentication Center) 는 시스템에서 동작하는 이동국들과 관련된 인증 정보를 관리하는 구성요소이다. MSC (mobile switching center) 와 AC 사이의 인터페이스의 동작 파라미터들은 AKA 과정을 수행하는 초기의 버전으로부터 업그레이드될 필요가 있다. MSC-AC 인터페이스 업그레이드 없이, AKA 과정을 수행할 수 있는 업그레이드된 이동국들 및 기지국들은, MSC-AC 인터페이스를 통하여 AKA 정보를 운반하기 위한 시스템의 부족으로 인하여 실제로 AKA 과정을 수행할 수 없다. 그 결과, 메시지 무결성이 수행될 수 없게 된다. 이러한 상태는, 기지국들과 이동국들이 MSC-AC 인터페이스들을 업그레이드시키기 이전에 제안된 TIA/EIA-IS-2000-B 표준에 따라 동작하도록 업그레이드되는 경우에는 중요한 배치 문제점을 갖는다.

[0006] 이 목적 뿐만 아니라 그 밖의 목적을 위하여, 더욱 진보된 세대의 이동국들 및 기지국들이 메시지 무결성을 수행할 수 있는 방법 및 장치가 요구되고 있다.

[0007] **개요**

[0008] 통신 시스템에서, 방법 및 장치는 인증 센터 또는 그 인증 센터와 이동 스위칭 센터 사이의 인터페이스의 동작 버전에 관계없이 메시지 무결성을 제공한다. 이 방법 및 장치는 CMEA (cellular message encryption algorithm) 키를 생성하는 것, 및 이동국과 기지국 사이의 메시지 무결성을 위한 CMEA 키에 기초하여 CIK (CMEA-key-derived integrity key) 를 생성하는 것을 포함한다. 이동국은 등록 메시지를 기지국에 송신하고, 이동국이 기지국으로부터 등록 허가 오더 또는 인증 벡터의 엘리먼트를 수신하는지 여부에 기초하여 기지국과의 통신시에 인증 센터의 동작 버전을 결정한다. 만일 이동국이 기지국으로부터 유효한 등록 허가 오더를 수신한다면, CIK 는 CMEA 키에 기초하여 생성된다. CIK 는 CMEA 키를 2 회 반복함으로써 생성된다. 이동국과 기지국은 각각 통신 시스템의 역방향 통신 및 순방향 통신에 대하여 CMEA 키에 기초하여 CIK 를 국부적으로 생성한다.

[0009] **도면의 간단한 설명**

[0010] 본 발명의 특징, 목적, 및 이점은 도면들을 참조하여 설명된 상세한 설명부로부터 명확하게 되고, 동일한 참조 부호들은 도면 전반에 걸쳐서 동일하게 식별된다.

[0011] 도 1 은 본 발명의 다양한 실시형태들에 따라 동작할 수 있는 통신 시스템을 나타낸다.

[0012] 도 2 는 본 발명의 다양한 양태들에 따른 데이터 레이트로 수신된 데이터를 수신 및 디코딩하는 통신 시스템 수신기를 나타낸다.

[0013] 도 3 은 본 발명의 다양한 양태들에 따른 스케줄링된 데이터 레이트로 데이터 패킷들을 송신하는 통신 시스템 송신기를 나타낸다.

[0014] 도 4 는 본 발명의 다양한 양태에 따른 인증 절차 및 키 셋-업 절차를 나타낸다.

[0015] 도 5 는 TIA/EIA-IS-2000-B 표준에 따른 인증 절차 및 키 셋-업 절차를 나타낸다.

[0016] 도 6 은 본 발명의 다양한 양태들에 따른 통신 시스템에서 이동국이 메시지 무결성을 수행하는 프로세스 흐름을

나타낸다.

[0017] **상세한 설명**

[0018] 본 발명의 다양한 실시형태들은 TIA (Telecommunication Industry Association) 및 다른 표준화 기구에 의해 공표된 다양한 표준들에 개시되고 설명되었던 CDMA (code division multiple access) 기술에 따라 동작하는 무선 통신 시스템에 포함될 수도 있다. 도 1 은 본 발명의 다양한 실시형태들을 포함하면서 어떤 CDMA 통신 시스템 표준들에 따라 동작할 수 있는 통신 시스템 (100) 의 일반적인 블록도를 나타낸다. 통신 시스템 (100) 은 음성, 데이터 또는 양자의 통신을 위한 것일 수도 있다. 일반적으로, 통신 시스템 (100) 은 이동국들 (102 내지 104) 과 같은 다수의 이동국들 사이에, 그리고 이동국들 (102 내지 104) 과 공중 스위치 전화 및 데이터 네트워크 (105) 사이에 통신 링크들을 제공하는 기지국 (101) 을 포함한다. 본 발명의 주요 범위 및 다양한 이점들을 벗어나지 않고 도 1 의 이동국들은 데이터 액세스 단말이라 하며 기지국은 데이터 액세스 네트워크라 할 수 있다. 기지국 (101) 은 기지국 제어기 및 베이스 트랜시버 시스템과 같은 다수의 구성요소들을 포함할 수도 있다. 간략함을 위하여, 이러한 구성요소들을 나타내지는 않는다. 또한, 기지국 (101) 은 다른 기지국들 예를 들어 기지국 (160) 과 통신할 수도 있다. 기지국들 (101, 160) 에 연결된 MSC (199) 는 통신 시스템 (100) 의 다양한 동작 양태들을 제어할 수도 있다. AC (198) 은 시스템 (100) 내에 제공된 인증 서비스들을 관리하기 위하여 MSC (199) 와 통신할 수도 있다. AC (198) 와 MSC (199) 사이의 인터페이스 (197) 는 인증 프로세스와 관련된 관련 정보를 통신하기 위한 통신 매체를 제공한다.

[0019] 기지국 (101) 은 기지국 (101) 으로부터 송신된 순방향 링크 신호를 통하여 그 커버리지 영역에 있는 각 이동국과 통신한다. 이동국들 (102 내지 104) 로 목표된 순방향 링크 신호들은 합산되어 순방향 링크 신호 (106) 를 형성할 수도 있다. 순방향 링크 신호 (106) 를 수신하는 각 이동국 (102 내지 104) 은 순방향 링크 신호 (106) 를 디코딩하여 그 사용자에 대하여 목표화된 정보를 추출한다. 또한, 기지국 (160) 은 순방향 링크 신호를 통하여 그 커버리지 영역내에 있는 이동국들과 통신할 수도 있다. 이동국들 (102 내지 104) 은 대응하는 역방향 링크들을 통하여 기지국들 (101 및 160) 과 통신한다. 각 역방향 링크는 각 이동국 (102 내지 104) 의 역방향 링크 신호들 (107 내지 109) 과 같은 역방향 링크 신호에 의해 유지된다.

[0020] 도 2 는 수신된 CDMA 신호를 프로세싱 및 복조하는데 사용되는 수신기 (200) 의 블록도를 나타낸다. 수신기 (200) 는 역방향 및 순방향 링크 신호들의 정보를 디코딩하는데 사용될 수도 있다. 수신 (RX) 샘플들은 RAM (204) 에 기억될 수도 있다. 수신 샘플들은 RF/IF (radio frequency/intermediate frequency) 시스템 (290) 및 안테나 시스템 (292) 에 의해 생성된다. RF/IF 시스템 (290) 및 안테나 시스템 (292) 은 다수의 신호들을 수신하고 그 수신된 신호들을 RF/IF 프로세싱하여 다이버시티 이득을 수신하는 하나 이상의 구성요소를 포함할 수도 있다. 다수의 수신 신호들은 서로 다른 전파 경로들을 통하여 전파되는 공통 소스로부터의 신호일 수도 있다. 안테나 시스템 (292) 은 RF 신호들을 수신하고, 그 RF 신호들을 RF/IF 시스템 (290) 으로 전송한다. RF/IF 시스템 (290) 은 어떤 종래의 RF/IF 수신기일 수도 있다. 그 수신된 RF 신호들을 필터링하고, 다운-컨버트하고, 디지털화하여 베이스 밴드 주파수들에서 RX 샘플들을 형성한다. 그 샘플들을 디멀티플렉서(demux)(202) 로 공급한다. 디멀티플렉서 (202) 의 출력을 탐색기 유닛 (206) 및 핑거 엘리먼트 (208) 들로 공급한다. 제어 유닛 (210) 은 거기에 연결되어 있다. 결합기 (212) 는 디코더 (214) 를 핑거 엘리먼트 (208) 들에 연결한다. 제어 유닛 (210) 은 소프트웨어에 의해 제어되는 마이크로프로세서일 수 있고, 동일한 집적 회로 또는 별도의 집적 회로상에 위치될 수도 있다. 디코더 (214) 의 디코딩 기능은 터보 디코더 또는 어떤 다른 적절한 알고리즘들에 따라 수행될 수도 있다.

[0021] 동작 동안에, 수신 샘플들은 디멀티플렉서 (202) 로 공급된다. 디멀티플렉서 (202) 는 탐색기 유닛 (206) 과 핑거 엘리먼트 (208) 들에 샘플들을 공급한다. 제어 유닛 (210) 은 탐색기 유닛 (206) 으로부터의 탐색 결과들에 기초하여 상이한 시간 오프셋들에서 수신 신호의 복조 및 역확산을 수행하도록 핑거 엘리먼트 (208) 들을 구성한다. 복조의 결과들은 결합되어 디코더 (214) 로 전송된다. 디코더 (214) 는 데이터를 디코딩하고 그 디코딩된 데이터를 출력한다. 디코딩 프로세스는 수신된 데이터를 역암호화하는 프로세스를 포함할 수도 있다. 채널들의 역확산은 단일 타이밍 가정에서 수신된 샘플들을 PN 시퀀스 및 할당된 월시 함수의 복소 컨주게이트와 곱하고, 적분 및 덤프 누산기 회로 (미도시) 를 종종 이용하여 그 결과 샘플들을 디지털 필터링함으로써 수행된다. 이러한 기술은 일반적으로 당해 분야에 공지되어 있다.

[0022] 도 3 은 역방향 및 순방향 링크 신호들을 송신하는 송신기 (300) 의 블록도를 나타낸다. 송신용 트래픽 채널 데이터는 변조기 (301) 로 입력되어 변조된다. 변조는 QAM, PSK 또는 BPSK 와 같은 어떤 일반적으로 공지된 변조 기술들에 따라 수행될 수도 있다. 데이터는 변조기 (301) 에서 데이터 레이트로 인코딩된다.

변조기 (301) 로 입력된 데이터는 메시지 무결성을 수행하는 데이터를 포함할 수도 있다. 데이터 레이트는 데이터 레이트/전력 레벨 선택기 (303) 에 의해 선택될 수도 있다. 역방향 링크 신호들에 있어서, 데이터 레이트 선택은 수신 기지국으로부터의 피드백 정보에 기초할 수도 있다. 그에 따라서 데이터 레이트/전력 레벨 선택기 (303) 는 변조기 (301) 에서 데이터 레이트를 선택한다. 변조기 (301) 의 출력은 안테나 (304) 로부터 송신하기 위하여 블록 (302) 에서 신호 확산 동작을 통하여 통과하여 증폭된다. 또한, 파일럿 신호는 블록 (307) 에서 생성된다. 파일럿 신호는 블록 (307) 에서 적절한 레벨로 증폭된다. 파일럿 신호 전력 레벨은 수신 기지국에서의 채널 상태에 따라 이루어질 수도 있다. 파일럿 신호는 결합기 (308) 에서 트래픽 채널 신호와 결합된다. 그 결합된 신호는 증폭기 (309) 에서 증폭되어 안테나 (304) 로부터 송신될 수도 있다. 안테나 (304) 는 안테나 어레이들 및 다중 입력 다중 출력 구성들을 포함한 임의의 수의 조합일 수도 있다. 또한, 데이터 레이트/전력 레벨 선택기 (303) 는 송신된 신호의 증폭 레벨에 대한 전력 레벨을 피드백 정보에 따라 선택한다. 선택된 데이터 레이트와 전력 레벨의 결합에 의해 송신된 데이터를 수신 기지국에서 적절하게 디코딩할 수 있다.

[0023] 이동국 (102) 은 기지국 (101) 의 커버리지 영역으로부터 기지국 (160) 의 커버리지 영역으로 로밍할 수도 있다. 이동국은 기지국들 (101 및 160) 에 대하여 소프트 핸드오프 프로세스를 통과할 수도 있다. 핸드오프 프로세스는 일반적으로 공지되어 있다. 이동국 (102) 은 기지국 (160) 으로부터 순방향 링크 신호 (161) 를 수신하고 역방향 링크 신호 (117) 를 송신함으로써 통신 서비스를 계속 이용한다. AC (198) 는 이동국과 일부 기지국들 (101 및 160) 사이의 보안 통신을 위하여 암호 키들을 인증 및 제공하는데 사용된다.

[0024] 도 4 에 나타낸 메시지 흐름 (399) 을 참조하여, 인증 및 암호화를 위한 메시지 흐름을 본 발명의 다양한 양태들에 따라 나타낸다. 메시지 흐름 (399) 에 관계된 기지국과 이동국은 제안된 TIA/EIA-IS-2000-B 표준에 따라 동작한다. 이 경우, AC (198) 은 제안된 TIA/EIA-IS-2000-B 표준의 관련 표준 섹션에 따라 동작하도록 업데이트되어 있지 않다. AC (198) 와 MSC (199) 사이의 인터페이스는, TIA/EIA-IS-2000-B 에서 약술한 바와 같이 메시지 무결성 및 암호화의 동작들에 관련되고, 본 명세서에 참고로 포함된 ANSI-41 표준에 일치하여 동작하도록 업데이트되어 있지 않다. 기지국은 RAND (random access number) 메시지 (391) 를 모든 이동국에 브로드캐스트한다. 이동국은 RAND 를 이용하여 등록 메시지 (392) 를 생성한다. 기지국은 MSC-AC 인터페이스 (197) 를 통하여, 등록 메시지에 의해 AC (198) 로 운반되는 인증 정보를 인증 요청 메시지 (393) 에 의해 통신한다. AC (198) 는 내부적으로 인증 요청 메시지내의 인증 정보를 예상된 값과 비교하고, 이동국의 인증을 확인하고, CMEA (cellular message encryption algorithm) 키 (394) 를 운반하는 인증 응답 메시지를 생성한다. CMEA 키의 생성에 의해 이동국과 기지국 사이에 암호화된 통신을 행할 수 있다. 이동국에서, 동일한 CMEA 키가 또한 내부 메시지 (397) 에 의해 생성된다. 이동국은 국부적으로 생성된 CMEA 키에 기초하여 내부 메시지 (398) 에 의해 CCK (CMEA-key-derived cipher key) 를 국부적으로 생성한다. CCK 는 암호화에 사용된다. 또한, 이동국은, 본 발명의 실시형태에 따라, 기지국에 대하여 메시지 무결성을 수행하는 CIK (CMEA-key-derived integrity key) 를 생성한다. CIK 는 CMEA 키에 기초할 수도 있다. 본 발명의 실시형태에 따라 CMEA 키를 2 회 반복하여 CIK 를 생성한다. 또한, 기지국은 내부 메시지 (380) 에 의해 국부적으로 CCK 를 생성한다. 또한, 기지국은 이동국에 대하여 메시지 무결성을 위한 CMEA 키에 기초하여 동일한 CIK 를 생성한다. 기지국은 인증 응답 메시지 (394) 에 기초하여 등록 허가 오더 (395) 를 이동국에 송신한다. 등록 허가 오더 (395) 는 MAC (message authentication code) 를 포함할 수도 있다. MAC 의 값들은 기지국에서 생성된 CIK 에 기초할 수도 있다. 생성된 CIK 는 사전정의된 함수에 따라 MAC 를 생성하도록 프로세서에 대한 입력으로 사용될 수도 있다. 이와 같이, 기지국 자체에서 생성된 CIK 에 기초한 이동국은 등록 허가 오더 (395) 를 송신하여 기지국의 합법성 (legitimacy) 을 검증할 수 있다. 이 시점 이후에, 이동국과 기지국 사이의 공통 통신 (396) 은 공지된 암호화 알고리즘에 따라 CCK 를 통하여 암호화될 수도 있다. 또한, 기지국과 이동국 사이의 공통 통신 (396) 들은 기지국과 이동국에서 생성된 CIK 에 기초하여 메시지 무결성 체크를 포함할 수도 있다. 따라서, 메시지 무결성 특징은 AC (198) 가 TIA/EIA-IS-2000A 표준들에 정의된 동작들과는 상이하게 동작하도록 요구하지 않고 이동국과 기지국 사이의 통신들에 제공된다.

[0025] 도 5 에 나타낸 메시지 흐름 (400) 을 참조하여, 인증 및 암호를 위한 메시지 흐름을 나타낸다. 나타낸 기지국과 이동국은 제안된 TIA/EIA-IS-2000-B 표준에 따라 동작한다. AC (198) 는 TIA/EIA-IS-2000-B 표준에 정의되는 관련 표준에 따라 동작한다. MSC-AC 인터페이스 (197) 는 TIA/EIA-IS-2000-B 표준에 의해 정의된 바와 같이 인증 파라미터들의 통신을 허용하도록 표준 ANSI-41 의 관련 섹션들에 기초하여 업데이트된다. 메시지 흐름 (400) 은 이동국, 기지국과 AC (198) 사이에 사용될 수도 있다. 기지국은 RAND (random access number) 메시지 (421) 를 모든 이동국들로 브로드캐스트한다. 이동국은 RAND 를 이용하여 등록 메시

지 (401) 를 생성한다. 그 후, 기지국은 인증 요청 메시지 (408) 를 AC (198) 로 전송한다. 그 후, AC (198) 는 인증 응답 메시지 (402) 를 전송한다. 메시지 (402) 는 TIA/EIA-IS-2000-B 에 따라 AV (authentication vector) 의 세트를 운반한다. 각 AV 는 IK (integrity key) 와 CK (cipher key) 를 포함하는 인증에 사용되는 다수의 엘리먼트를 포함한다. 기지국은 인증 벡터들 중 하나를 선택하고 그 선택된 AV 의 일부 엘리먼트들을 인증 요청 메시지 (403) 에 의해 이동국으로 송신한다. AV 의 엘리먼트들은 AC (198) 에서 유지되는 루트 키에 기초하여 생성된다. 또한, 동일한 루트 키가 이동국에 저장된다. 이동국은 통신된 AV 엘리먼트들이 저장된 루트 키에 기초하여 생성되는 AV 엘리먼트와 일치하는지를 내부적으로 체크한다. 만일 일치하면, 이동국은 실제로 기지국을 인증한다. 루트 키 및 통신된 AV 엘리먼트들에 기초하여, 이동국은 내부 메시지 (405) 를 통하여 국부적으로 IK 및 CK 를 생성한다. 또한, 이동국은 통신된 AV 엘리먼트들에 기초하여 사용자 응답 (RES) 을 생성한다. 그 후, 이동국은 기지국에 인증 응답 (404) 의 RES 를 송신한다. 또한, 기지국은 국부적으로 내부 메시지 (406) 를 통하여 IK 및 DK 를 생성한다. 기지국은 수신된 RES 를 예상된 RES 와 비교한다. 만일 일치하면, 기지국은 실제로 이동국을 인증한다. 이때, 통신 (407) 들은 TIA/EIA-IS-2000-B 표준에 따라 메시지 무결성 및 암호화를 수행할 수도 있다.

[0026] 본 발명의 다양한 양태들에 의해 인증 프로세스에 기인하는 CMEA 키를 메시지 무결성을 수행하는 무결성 키로서 사용할 수 있다. 이동국은 제안된 TIA/EIA-IS-2000-B 표준 뿐만 아니라 AC (198) 또는 MSC-AC 인터페이스 (197) 의 상이한 버전들에 따라 동작하는 기지국들에 대한 시스템들로 로밍할 수 있으므로, 이동국은 AC (198) 또는 MSC-AC 인터페이스 (197) 중 어느 버전들이 시스템에 통합되었는지를 미리 알 수 없다. 더욱 상세하게는, 만일 제안된 TIA/EIA-IS-2000-B 표준에 따라 동작하는 이동국과 기지국이 통신 시스템 (100) 에서 통신하는 반면에 AC (198) 가 TIA/EIA-IS-95-B 또는 TIA/EIA-IS-2000-A 에 따라 동작하고 및/또는 MSC-AC 인터페이스 (197) 가 TIA/EIA-IS-95-B 또는 TIA/EIA-IS-2000-A 와 관련된 ANSI-41 에 따라 동작하는 경우, 이동국은 메시지 무결성 특징의 부족으로 인하여 기지국과의 어떤 통신을 거절할 수도 있다. 따라서, 이동국은, 부가되는 복잡성 없이, AC (198) 또는 MSC-AC 인터페이스 (197) 중 어느 버전들이 시스템에 통합되었는지를 식별하는 방법 및 장치를 요구한다.

[0027] 도 6 을 참조하여, 흐름도 (600) 는 AC (198) 또는 MSC-AC 인터페이스 (197) 의 버전에 관계없이 이동국으로 하여금 메시지 무결성 키를 구축하고 기지국에 대한 인증을 수행하도록 하는 알고리즘을 나타낸다. 단계 601 에서, 이동국은 인증되어 있거나 또는 인증되어 있지 않을 수 있다. 단계 602 에서, 이동국은, AC (198) 가 TIA/EIA-IS-95B 또는 TIA/EIA-IS-2000-A 따라 동작한다고 가정하면, 등록 메시지 (392) 를 기지국으로 전송하고 CMEA 키를 계산하고 내부 메시지들 (397 및 398) 을 통하여 CIK 및 CCK 를 생성한다. 이동국이 성공적인 인증 프로세스를 통과하면, 이동국은 이미 무결성 키, 및 인증의 스타일에 의존하는 CIK 또는 IK 중 어느 하나를 가진다. 그 경우에, 등록 메시지의 MAC (message authentication code) 는 등록 메시지에 포함된다. MAC 가 존재하면 기지국은 이동국과의 국부적 인증을 수행하며, 이는 네트워크내의 인증관련 트래픽을 감소시킨다. 이동국은 기지국으로부터 등록 허가 오더 (395) 를 수신할 것을 기대한다. 단계 603 에서, 이동국은 AC (198) 또는 MSC-AC 인터페이스 (197) 가 TIA/EIA-IS-95B 및 TIA/EIA-IS-2000-A 또는 TIA/EIA-IS-2000-B 에 따라 동작하는 지를 판정한다. TIA/EIA-IS-95B 및 TIA/EIA-IS-2000-A 에 따른 인증을 2G 인증이라 할 수도 있다. TIA/EIA-IS-2000-B 에 따른 인증을 3G 인증이라 할 수도 있다. 타이머는 이동국이 이러한 모드에 머무르는 시간량을 제한하는데 사용될 수도 있다. 타이머가 단계 604 에서 만료되는 경우, 프로세스는 단계 602 에서 개시하고, 만일 이동국이 이미 무결성 키를 갖고 있지 않으면, 이 경우에, 이동국은 단계 606 으로 직접 이동한다. 만일 이동국이 기지국으로부터 등록 허가 오더 (395) 를 수신하면, AC (198) 및 MSC-AC 인터페이스 (197) 는 2G 인증 절차에 따라 동작한다. 단계 605 의 프로세스는 단계 606 으로 진행한다. 단계 606 에서, 이동국은, 기지국과 공통 채널로 통신하기 위하여 메시지 무결성 및 암호화를 수행하는 내부 메시지들 (397 및 398) 을 통하여, 생성된 CMEA 키를 이용하여 CIK 및 CCK 를 유도한다. 만일 이동국이 기지국으로부터 인증 요청 메시지 (403) 를 수신하면, AC (198) 또는 MSC-AC 인터페이스 (197) 는 3G 인증 절차에 따라 동작한다. 이와 같이, 단계 605 의 프로세스 흐름은 단계 607 로 진행하여 생성된 CMEA 키 및 어떤 펜딩된 CIK 및 CCK 를 버리고, IK 및 CK 를 생성한다. 단계 607 의 프로세스는 하나 이상의 단계를 포함할 수도 있다. 단계 608 에서, IK 및 CK 는 내부 메시지 (405) 를 통하여 생성된다. 단계들 (609 및 610) 에서, 인증은 이동국이 긴 시간 동안 이러한 모드에 남아 있는 것을 방지하기 위하여 타이머의 이용에 따라 기지국에 의해 확인된다. 단계 611 에서, 이동국은 메시지 무결성 및 암호화를 위한 IK 및 CK 를 확립한다. 단계 612 에서, 이동국은 기지국에 대하여 메시지 무결성 및 암호화의 파라미터들의 정확한 세트를 유지한다. 이동국이 등록을 수행하도록 요청할 때 마다 프로세스가 반복될 수도 있다.

[0028] 또한, 당업자는 여기서 개시된 실시형태와 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들, 및

알고리즘 단계들을 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이들의 조합으로 구현할 수도 있음을 이해할 수 있다. 하드웨어와 소프트웨어의 이러한 대체 가능성을 분명히 설명하기 위하여, 다양한 예시적인 구성요소들, 블록들, 모듈들, 회로들 및 단계들을 주로 그들의 기능의 관점에서 상술하였다. 그러한 기능이 하드웨어로 구현될지 소프트웨어로 구현될지는 전체 시스템상에 부과된 특정한 애플리케이션 및 설계 제약조건들에 의존한다. 당업자는 설명된 기능을 각각의 특정한 애플리케이션에 대하여 다양한 방식으로 구현할 수 있지만, 그러한 구현 결정이 본 발명의 범위를 벗어나도록 하는 것으로 해석해서는 안된다.

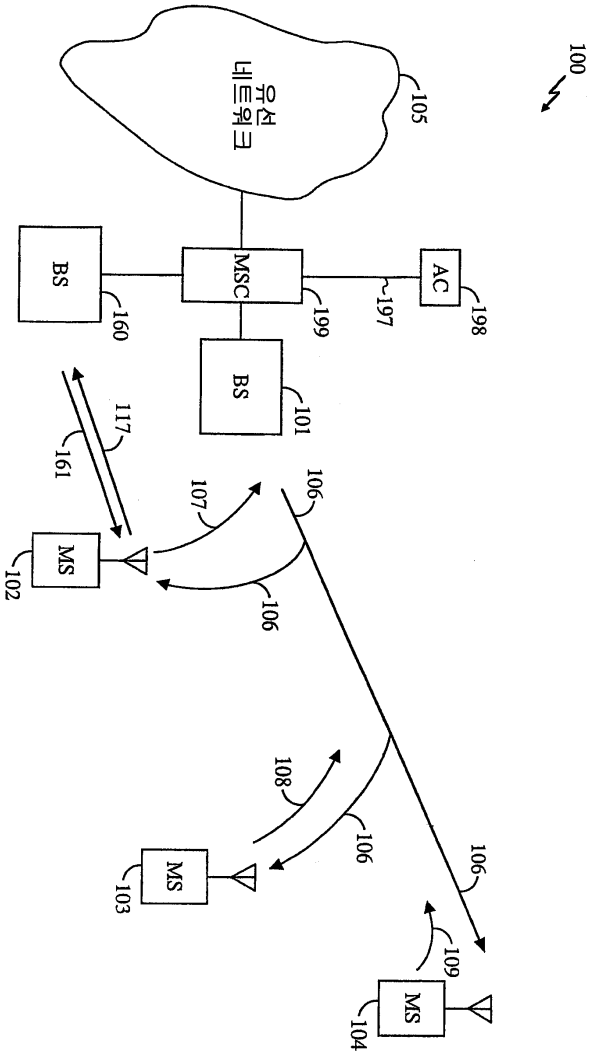
[0029] 여기서 개시된 실시형태들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들은 범용 프로세서, 디지털 신호 프로세서 (DSP), 응용 주문형 집적 회로 (ASIC), 필드 프로그래머블 게이트 어레이 (FPGA), 또는 기타 프로그래머블 논리 장치, 별도의 게이트 또는 트랜지스터 로직, 별도의 하드웨어 구성요소들, 또는 여기서 설명된 기능을 수행하도록 설계되는 이들의 조합으로 구현 또는 실행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 다른 방법으로, 그 프로세서는 종래의 프로세서, 콘트롤러, 마이크로콘트롤러, 또는 상태 머신일 수도 있다. 또한, 프로세서는 계산 장치들의 조합, 예를 들어, DSP 와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 이상의 마이크로프로세서들 또는 기타의 구성물로 구현될 수도 있다.

[0030] 여기서 개시된 실시형태들과 관련하여 설명된 방법 또는 알고리즘의 단계들은 프로세서에 의해 실행되는 하드웨어 및 소프트웨어 모듈, 또는 그 2 개의 조합으로 직접 구현될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래쉬 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터, 하드 디스크, 착탈식 디스크, CD-ROM, 또는 당업계에 알려진 기타 다른 형태의 저장 매체에 포함될 수 있다. 예시적인 저장 매체는 그 저장 매체로부터 정보를 판독할 수 있고 저장 매체에 정보를 기입할 수 있는 프로세서에 결합된다. 다른 방법으로, 저장 매체는 프로세서와 일체형일 수도 있다. 프로세서 및 저장 매체는 ASIC 에 포함될 수도 있다. ASIC 은 사용자 단말장치에 포함될 수도 있다. 다른 방법으로, 프로세서 및 저장 매체는 별도의 구성요소들로서 사용자 단말장치에 포함될 수도 있다.

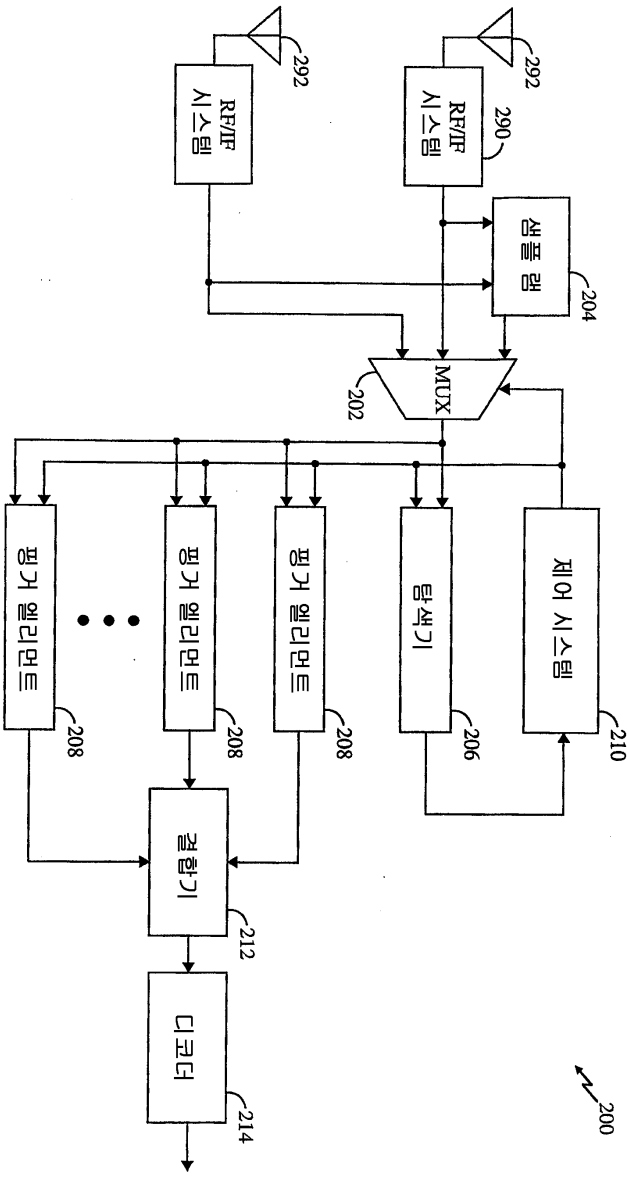
[0031] 개시된 실시형태들에 대한 상기의 설명은 당업자로 하여금 본 발명을 제조 또는 이용할 수 있도록 제공된다. 이들 실시형태에 대한 다양한 변형들은 당업자에게 명백하며, 여기서 정의된 일반적인 원리들은 본 발명의 창의력을 이용하지 않고도 다른 실시형태들에 적용할 수도 있다. 따라서, 본 발명은 여기서 나타낸 실시형태들로 한정하려는 것이 아니라, 여기서 개시되는 원리들 및 신규한 특징들과 부합하는 최광의 범위를 부여하려는 것이다.

도면

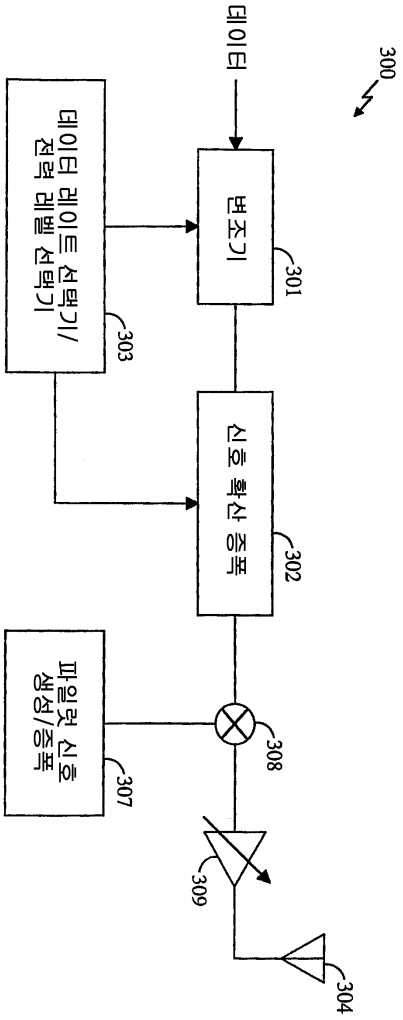
도면1


100
유선 네트워크
105
BS
160
MSC
199
197
AC
198
BS
101
117
161
MS
102
107
106
106
108
MS
103
106
109
MS
104

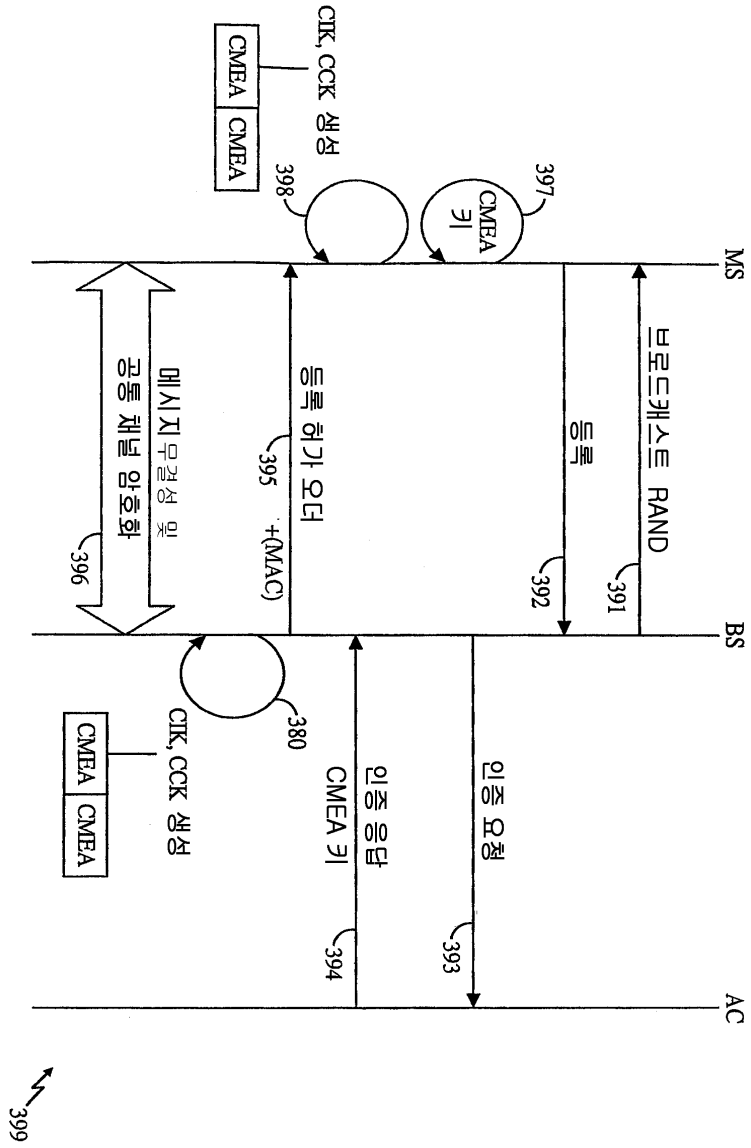
도면2


292
RF/IF 시스템
290
292
RF/IF 시스템
샘플 랩
204
MUX
202
핑거 엘리먼트
208
핑거 엘리먼트
208
핑거 엘리먼트
208
탐색기
206
제어 시스템
210
결합기
212
디코더
214
200

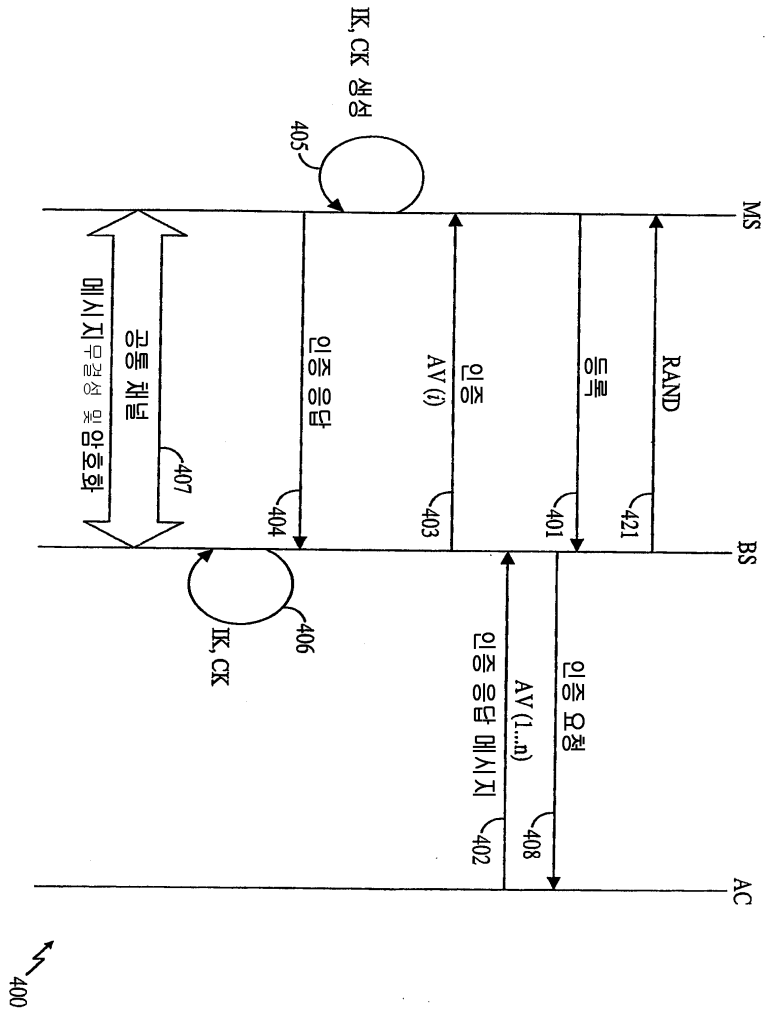
도면3


300
데이터
변조기
301
데이터 레이트 선택기/
전력 레벨 선택기
303
신호 확산 증폭
302
파일럿 신호
생성/증폭
307
308
309
304

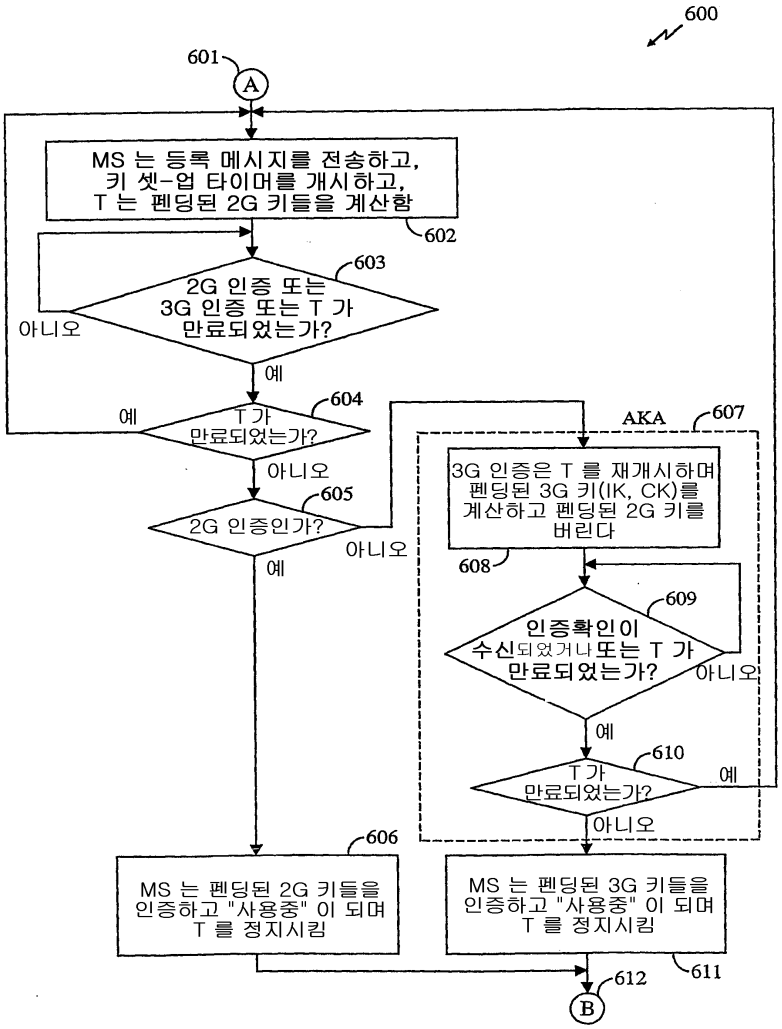
도면4


MS
BS
AC
CMEA 키
397
CIK, CCK 생성
CMEA
CMEA
398
브로드캐스트 RAND
391
등록
392
등록 허가 오더
395
+(MAC)
메시지 무결성 및
공통 채널 암호화
396
인증 요청
393
인증 응답
CMEA 키
394
CIK, CCK 생성
CMEA
CMEA
380
399

도면5


IK, CK 생성
405
MS
RAND
421
등록
401
인증
AV (i)
403
인증 응답
404
공통 채널
407
메시지 무결성 및 암호화
IK, CK
406
BS
인증 응답 메시지
402
AV (1...n)
인증 요청
408
AC
400

도면6


600
601
A
MS 는 등록 메시지를 전송하고,
키 셋-업 타이머를 개시하고,
T 는 펜딩된 2G 키들을 계산함
602
603
2G 인증 또는
3G 인증 또는 T 가
만료되었는가?
아니오
예
604
예
T 가
만료되었는가?
아니오
605
2G 인증인가?
아니오
예
AKA
607
3G 인증은 T 를 재개시하며
펜딩된 3G 키(IK, CK)를
계산하고 펜딩된 2G 키를
버린다
608
609
인증확인이
수신되었거나 또는 T 가
만료되었는가?
아니오
예
610
T 가
만료되었는가?
예
아니오
606
MS 는 펜딩된 2G 키들을
인증하고 "사용중" 이 되며
T 를 정지시킴
MS 는 펜딩된 3G 키들을
인증하고 "사용중" 이 되며
T 를 정지시킴
611
612
B