(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년07월11일
(11) 등록번호 10-1164682
(24) 등록일자 2012년07월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
H04L 9/08 (2006.01) *H04L 12/46* (2006.01)
(21) 출원번호 10-2005-7018891
(22) 출원일자(국제) 2004년04월02일
심사청구일자 2009년04월02일
(85) 번역문제출일자 2005년10월04일
(65) 공개번호 10-2006-0003338
(43) 공개일자 2006년01월10일
(86) 국제출원번호 PCT/US2004/010304
(87) 국제공개번호 WO 2004/091176
국제공개일자 2004년10월21일
(30) 우선권주장
60/460,257 2003년04월02일 미국(US)
(56) 선행기술조사문헌
KR1019990088046 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
콸콤 인코포레이티드
미국 캘리포니아 샌디에고 모어하우스 드라이브5775 (우 92121-1714)
(72) 발명자
자인, 니킬
미국 92130 캘리포니아 샌디에고 페더만 레인 4291
콜린스, 브루스
미국 92131 캘리포니아 샌디에고 앵겔리쿠에 스트리트 11730
나가라즈, 타디 엠.
미국 92131 캘리포니아 샌디에고 사이프레스 캐년 로드 11820-2
(74) 대리인
남상선

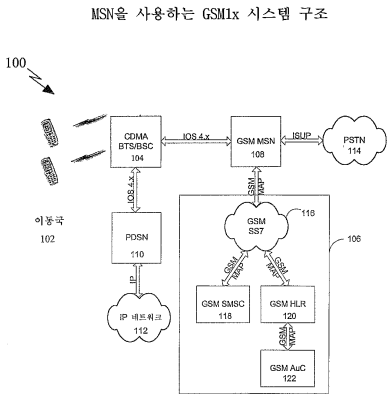
전체 청구항 수 : 총 17 항 심사관 : 양종필

(54) 발명의 명칭 **CDMA 네트워크 및 GSM 네트워크 사이에서의 암호화**

(57) 요 약

GSM 네트어크에 가입된 이동국이 CDMA 네트워크로 로밍되고 상기 CDMA 네트워크를 사용하도록 인증되고 CDMA 네트워크에의 가입 없이 메시지들을 암호화할 수 있도록 공유된 비밀 데이터가 CDMA 네트워크와 GSM 네트워크 사이에서 인증되고 암호화되도록 사용된다. GSM 인증 자격 증명(credential)을 사용하여 CDMA 네트워크에 있는 GSM 가입자 인증의 목적은 키 Kc를 SSD-A로서 대체함으로써 달성되고 메시지들은 CAVE 알고리즘을 사용하여 Kc를 SSD-B로서 대체하여 암호화된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

제 1 네트워크와 제 2 네트워크 사이에서 상기 제 1 네트워크에 가입된 이동국(MS)이 상기 제 2 네트워크를 사용하여 통신할 수 있도록 하기 위한 무선 통신 방법으로서,

상기 이동국의 아이덴티티(identity)를 저장하는 단계;

상기 이동국의 상기 아이덴티티에 기초하여 상기 제 1 네트워크로부터 인증 정보를 획득하는 단계 ? 상기 제 1 네트워크는 GSM 네트워크이고 상기 제 2 네트워크는 CDMA 네트워크임 ? ;

키를 생성하기 위해 상기 제 1 네트워크로부터의 상기 인증 정보를 사용하는 단계 ? 생성되는 키는 범용 글로벌 게이트웨이(GGG; General Global Gateway)에서 수신되고, 상기 범용 글로벌 게이트 웨이는 상기 생성되는 키를 상기 제 1 네트워크로부터 획득함 ? ;

상기 이동국을 인증하기 위해 상기 범용 글로벌 게이트웨이에서 제 1 알고리즘에서 사용되는 인증 키를 상기 키로 대체하는 단계; 및

상기 이동국과 상기 제 2 네트워크 사이에서 메시지들을 암호화하기 위해 제 2 알고리즘에서 사용되는 암호 키를 상기 키로 대체하는 단계

를 포함하고,

상기 범용 글로벌 게이트웨이는 상기 제 1 네트워크와 상기 제 2 네트워크 사이에서 상호작용(interwork)하는 상호작용 및 상호운용 기능부를 갖고, 상기 제 2 네트워크에 대한 방문자 위치 등록기(VLR; Visitor Location Register)로서 상기 이동국에 대해 기능하고 그리고 단문 메시지 서비스 센터(SMSC; Short Message Service Center)로서 기능하며, 그리고 상기 제 2 네트워크에서 인증 제어기(AC; Authentication Controller)로서 역할하는,

무선 통신 방법.

청구항 2

제1항에 있어서,

상기 제 1 알고리즘은 상기 제 2 네트워크에서 실행되는,

무선 통신 방법.

청구항 3

제1항에 있어서,

상기 인증 키는 SSD-A인,

무선 통신 방법.

청구항 4

제1항에 있어서,

상기 암호 키는 SSD-B인,

무선 통신 방법.

청구항 5

제1항에 있어서,

상기 제 1 알고리즘은 CAVE 알고리즘인,

무선 통신 방법.

청구항 6

제 1항에 있어서,

상기 제 2 알고리즘은 CAVE 알고리즘인,

무선 통신 방법.

청구항 7

제1항에 있어서,

상기 GSM 네트워크는 범용 패킷 무선 서비스(GPRS; General Packet Radio Services)인,

무선 통신 방법.

청구항 8

제1항에 있어서,

상기 GSM 네트워크는 유니버셜 이동 통신 시스템(UMTS; Universal Mobile Telecommunication System)인,

무선 통신 방법.

청구항 9

제1항에 있어서,

상기 GSM 네트워크는 광대역-CDMA(W-CDMA)인,

무선 통신 방법.

청구항 10

제1항에 있어서,

상기 CDMA 네트워크는 cdma2000-1x인,

무선 통신 방법.

청구항 11

제1항에 있어서,

상기 CDMA 네트워크는 cdma2000-1xEV-DO인,

무선 통신 방법.

청구항 12

제 1 네트워크와 제 2 네트워크 사이에서 상기 제 2 네트워크를 사용하여 통신하기 위한 이동국 ? 상기 이동국은 상기 제 1 네트워크에 가입됨 ? 으로서,

상기 이동국의 아이덴티티를 저장하기 위한 수단;

상기 이동국의 상기 아이덴티티에 기초하여 상기 제 1 네트워크로부터 인증 정보를 획득하기 위한 수단 ? 상기 제 1 네트워크는 GSM 네트워크이고 상기 제 2 네트워크는 CDMA 네트워크임 ? ;

키를 생성하기 위해 상기 제 1 네트워크로부터의 상기 인증 정보를 사용하기 위한 수단 ? 생성되는 키는 범용 글로벌 게이트웨이에서 수신되고, 상기 범용 글로벌 게이트 웨이는 상기 생성되는 키를 상기 제 1 네트워크로부터 획득함 ? ;

상기 이동국을 인증하기 위해 상기 범용 글로벌 게이트웨이에서 제 1 알고리즘에서 사용되는 인증 키를 상기 키로 대체하기 위한 수단; 및

상기 이동국과 상기 제 2 네트워크 사이에서 메시지들을 암호화하기 위해 제 2 알고리즘에서 사용되는 암호

키를 상기 키로 대체하기 위한 수단

을 포함하고,

상기 범용 글로벌 게이트웨이는 상기 제 1 네트워크와 상기 제 2 네트워크 사이에서 상호작용하는 상호작용 및 상호운용 기능부를 갖고, 상기 제 2 네트워크에 대한 방문자 위치 등록기(VLR)로서 상기 이동국에 대해 기능하고 그리고 단문 메시지 서비스 센터(SMSC)로서 기능하며, 그리고 상기 제 2 네트워크에서 인증 제어기(AC)로서 역할하는,

이동국.

청구항 13

제12항에 있어서,

상기 GSM 네트워크는 범용 패킷 무선 서비스(GPRS)인,

이동국.

청구항 14

제12항에 있어서,

상기 GSM 네트워크는 유니버셜 이동 통신 시스템(UMTS)인,

이동국.

청구항 15

제12항에 있어서,

상기 GSM 네트워크는 광대역-CDMA(W-CDMA)인,

이동국.

청구항 16

제12항에 있어서,

상기 CDMA 네트워크는 cdma2000-1x인,

이동국.

청구항 17

제12항에 있어서,

상기 CDMA 네트워크는 cdma2000-1xEV-DO인,

이동국.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 통신 시스템에 관한 것으로서, 특히 CDMA 네트워크 및 GSM 네트워크 사이에서의 암호화를 위한 시스템에 관한 것이다.

배 경 기 술

[0002] 관련 출원에 대한 교차 참조

본 출원은 출원 번호가 60/460,257이고 출원일이 2003년 4월 2일인 미국 가출원 특허의 우선권을 청구한다.

공동-계류중인 특허 출원에 대한 참조

본 특허 출원은 다음 공동 계류중인 미국 특허 출원들:

출원일이 2004년 3월 18일이고 출원 번호가 10/804,265인 "Internetworking Between A CDMA Network And A GSM Network", 출원일이 2004년 3월 18일이고 출원 번호가 10/804,301인 "Authenticating Between A CDMA Network And A GSM Network", 및 출원일이 2004년 3월 18일이고 출원 번호가 10/804,267인 "Using Shared Secret(SSD) To Authenticate Between A CDMA Network And A GSM Network"에 관련되며, 이들은 본 발명의 양수인에게 양도되고 본 명세서에 명시적으로 포함된다.

코드 분할 다중 접속(CDMA)은 상대적으로 큰 대역폭 용량을 가지는(즉, 다른 통신 기술들에 비해 주파수 밴드당 보다 많은 전화통화를 서비스하는) 디지털 무선 기술이다. 특히, CDMA의 확산 스펙트럼 원리들은 보안 통신을 가능하게 한다. 본 명세서에서 참조로써 통합되는 미국 특허 번호 4,901,307호는 음성 통화 및 비-음성 컴퓨터 데이터 모두를 전송하는데 사용될 수 있는 CDMA 시스템에 대해 상술하고 있다.

[0003] CDMA의 장점에도 불구하고, 다른 원리들을 사용하는 다른 무선 시스템들이 존재한다. 예를 들어, 전세계 도처에서 시분할 다중 접속 방식을 채용하는 GSM이 사용된다.

[0004] CDMA 원리들이 사용되든 또는 다른 무선 원리들이 사용되든지 간에, 무선 통신 시스템들은 2개의 주요 컴포넌트들, 즉 무선 라디오 접속 네트워크(RAN)와, 공중 교환 전화망(PSTN), 인터넷(특히 데이터 통화만을 위해 사용되지는 않음) 등과 같은 외부 시스템 및 RAN과 통신하는 코어 인프라를 가지는 것으로 간주될 수 있다. 다양한 무선 기술들과 관련되는 코어 인프라들은 하드웨어의 관점에서, 그리고 특정화된 전형적인 시스템-특정 통화 스위칭, 가입신청, 참여자 인증 및 호출 모니터링, 및 결제를 지원하기 위한 통신 프로토콜의 개발의 관점에서 매우 값비싸다. 결과적으로, 하나의 무선 시스템의 통신 프로토콜(GSM의 경우 GSM 프로토콜 및 cdma2000-1x과 같은 CDMA의 경우 IS-41 프로토콜)은 하나의 시스템 또는 다른 시스템의 코어 인프라에서의 값비싸고 허용되지 않는 변경들 없이는 다른 시스템의 프로토콜들과는 호환될 수 없다.

[0005] CDMA 네트워크 및 GSM 네트워크 사이의 상호 네트워킹하여 이에 의해 그 고유한 장점을 가진 CDMA 기반 RAN의 사용을 가능케 하고, 전세계에서 널리 사용되는 GSM 기반 코어 인프라의 사용을 가능케 하는 것이 바람직하다.

[0006] 따라서, 듀얼 모드 이동국은 예를 들어 유럽에서는 GSM 코어 인프라와 인터페이싱하고, 예를 들어 미국에서는 CDMA 인프라를 사용할 수 있도록 유리하게 인에이블될 수 있다.

발명의 상세한 설명

[0007] 본 발명의 일 양상에서, 제1 네트워크에 가입된 이동국(MS)이 제2 네트워크를 사용하여 통신하도록 하기 위해서 제1 네트워크 및 제2 네트워크 사이의 무선 통신 방법은 이동국 아이덴티티(identity)를 저장하는 단계, 이동국 아이덴티티에 기반하여 제1 네트워크로부터의 인증 정보를 획득하는 단계, 키를 발생시키기 위해서 제1 네트워크로부터 인증 정보를 사용하는 단계, 이동국을 인증하기 위해서 제1 알고리즘에서 사용되는 SSD-A를 상기 키로 대체하는 단계, 이동국 및 제2 네트워크 사이의 메시지들을 암호화하기 위해서 제2 알고리즘에서 사용되는 SSD-B를 상기 키로 대체하는 단계를 포함한다.

본 발명의 다른 양상에서, 제 1 네트워크와 제 2 네트워크 사이에서 상기 제 1 네트워크에 가입된 이동국(MS)이 상기 제 2 네트워크를 사용하여 통신할 수 있도록 하기 위한 무선 통신 방법은 상기 이동국의 아이덴티티(identity)를 저장하는 단계, 상기 이동국의 상기 아이덴티티에 기초하여 상기 제 1 네트워크로부터 인증 정보를 획득하는 단계 ? 상기 제 1 네트워크는 GSM 네트워크이고 상기 제 2 네트워크는 CDMA 네트워크임 ? , 키를 생성하기 위해 상기 제 1 네트워크로부터의 상기 인증 정보를 사용하는 단계 ? 생성되는 키는 범용 글로벌 게이트웨이(GGG; General Global Gateway)에서 수신되고, 상기 범용 글로벌 게이트 웨이는 상기 생성되는 키를 상기 제 1 네트워크로부터 획득함 ? , 상기 이동국을 인증하기 위해 상기 범용 글로벌 게이트웨이에서 제 1 알고리즘에서 사용되는 인증 키를 상기 키로 대체하는 단계, 및 상기 이동국과 상기 제 2 네트워크 사이에서 메시지들을 암호화하기 위해 제 2 알고리즘에서 사용되는 암호 키를 상기 키로 대체하는 단계를 포함하고, 상기 범용 글로벌 게이트웨이는 상기 제 1 네트워크와 상기 제 2 네트워크 사이에서 상호작용(interwork)하는 상호작용 및 상호운용 기능부를 갖고, 상기 제 2 네트워크에 대한 방문자 위치 등록기(VLR; Visitor Location Register)로서 상기 이동국에 대해 기능하고 그리고 단문 메시지 서비스 센터(SMSC; Short Message Service Center)로서 기능하며, 그리고 상기 제 2 네트워크에서 인증 제어기(AC; Authentication Controller)로서 역할한다.

본 발명의 또 다른 양상에서, 제 1 네트워크와 제 2 네트워크 사이에서 상기 제 2 네트워크를 사용하여 통신

하기 위한 이동국 ? 상기 이동국은 상기 제 1 네트워크에 가입됨 ? 은 상기 이동국의 아이덴티티를 저장하기 위한 수단, 상기 이동국의 상기 아이덴티티에 기초하여 상기 제 1 네트워크로부터 인증 정보를 획득하기 위한 수단 ? 상기 제 1 네트워크는 GSM 네트워크이고 상기 제 2 네트워크는 CDMA 네트워크임 ? , 키를 생성하기 위해 상기 제 1 네트워크로부터의 상기 인증 정보를 사용하기 위한 수단 ? 생성되는 키는 범용 글로벌 게이트웨이에서 수신되고, 상기 범용 글로벌 게이트 웨이는 상기 생성되는 키를 상기 제 1 네트워크로부터 획득함 ? , 상기 이동국을 인증하기 위해 상기 범용 글로벌 게이트웨이에서 제 1 알고리즘에서 사용되는 인증 키를 상기 키로 대체하기 위한 수단, 및 상기 이동국과 상기 제 2 네트워크 사이에서 메시지들을 암호화하기 위해 제 2 알고리즘에서 사용되는 암호 키를 상기 키로 대체하기 위한 수단을 포함하고, 상기 범용 글로벌 게이트웨이는 상기 제 1 네트워크와 상기 제 2 네트워크 사이에서 상호작용하는 상호작용 및 상호운용 기능부를 갖고, 상기 제 2 네트워크에 대한 방문자 위치 등록기(VLR)로서 상기 이동국에 대해 기능하고 그리고 단문 메시지 서비스 센터(SMSC)로서 기능하며, 그리고 상기 제 2 네트워크에서 인증 제어기(AC)로서 역할한다.

[0008] 본 발명의 다른 실시예들은 하기 설명으로부터 당업자에게 자명할 것임이 이해되며 본 발명의 다양한 실시예들이 제시되며, 예를 통해 기술되어 진다. 알 수 있는 바와 같이, 본 발명은 다른 상이한 실시예들을 포함하며, 본 발명의 몇몇 상세 항목들은 다양한 양상들에서의 다양한 변형들일 수 있고, 이 역시 본 발명의 영역에 속한다. 따라서, 하기 도면 및 실시예들은 예로써 간주되어야 할 뿐이고, 제한적으로 해석되어서는 안 된다.

실 시 예

[0023] 약어 정리

[0024] 3GPP2- 3세대 파트너쉽 프로젝트 2

[0025] Ack-확인 응답(Acknowledgement)

[0026] ACM-어드레스 완료 메시지

[0027] ANM-답신 메시지

[0028] Assign-할당

[0029] AuC-인증 센터

[0030] Auth-인증

[0031] AUTHR-인증 응답

[0032] BS-기지국

[0033] BSC-기지국 제어기

[0034] BTS-기지국 트랜시버 서브시스템

[0035] CAVE-셀룰러 인증 및 음성 암호화

[0036] CDMA-코드 분할 다중 접속

[0037] CDMA2000-3세대 CDMA

[0038] CH-채널

[0039] CM-셀룰러 메시지

[0040] CMEA-셀룰러 메시지 암호화 알고리즘

[0041] ECMEA-확장 CMEA

[0042] ESN-전자 일련 번호

[0043] GSM-이동 통신용 글로벌 시스템

[0044] GSM1x-CDMA2000 과 GSM-MAP의 컨버젼스

[0045] HLR-홈 위치 등록기

[0046] IAM-초기 어드레스 메시지

[0047] IMSI-국제 이동 가입자 아이덴티티

[0048] ISUP-ISDN 사용자 부

[0049] Info-정보

[0050] IOS-상호 운용 규격

[0051] IP-인터넷 프로토콜

[0052] Kc-암호화 키

[0053] Ki-개별 가입자 인증 키

[0054] MAP-모바일 애플리케이션 부

[0055] MIN-모바일 아이덴티티 번호

[0056] MO-이동국 발신

[0057] MS-이동국

[0058] MSN-이동 교환 노드

[0059] MT-이동국 착신

[0060] PDSN-패킷 데이터 서비스 노드

[0061] PLC-사설 롱(long) 코드

[0062] PLCM-PLC 마스크

[0063] Priv-프라이버시

[0064] PSTN-공중 교환 전화망

[0065] RAN-무선 접속 네트워크

[0066] RAND-랜덤 챌린지 데이터

[0067] Req-요구

[0068] Resp-응답

[0069] SIM-가입자 아이덴티티 모듈

[0070] SMS-단문 메시지 서비스

[0071] SMSC-단문 메시지 서비스 센터

[0072] SRES-서명된 응답

[0073] SSD-공유 비밀 데이터

[0074] SS7-시그널링 시스템 7

[0075] TCH-트래픽 채널

[0076] VP-음성 프라이버시

[0077] VPM-VP 마스크

[0078] 시스템 구조

[0079] 일 실시예에서, 시스템은 CDMA RAN을 GSM 코어 네트워크와 통합한다. 이는 GSM 가입 및 GSM 네트워크 엔티티를 구비한 이동국(MS)을 사용함으로써 달성된다. GSM 네트워크를 위한 2가지 옵션들은 다음과 같다.

[0080] (1) 이동 교환 노드(MSN); 및

[0081] (2) 상호 네트워킹 및 상호운용성 기능부(IF).

[0082] 이동 교환 노드(MSN)는 표준 IOS 호환 CDMA RAN 및 GSM 코어 네트워크 사이의 통신을 지원하는 네트워크 교환 엘리먼트이다. GSM MSN 은 HLR, AuC 및 SMSC와 같은 GSM 코어 네트워크 엔티티를 통해 동작한다. MSN을 사용하는 GSM 시스템 구조는 도1에 제시된다.

[0083] 범용 글로벌 게이트웨이(GGG)는 CDMA 및 GSM 코어 네트워크들 사이에서 상호작용하는 상호작용 및 상호운용 기능부(IIF)이다. 용어 "상호작용" 및 "상호운용"은 서로 혼용되어 사용될 수 있다. 일 실시예에서, GGG는 GSM1x 글로벌 게이트웨이로 지칭될 수 있다. GGG는 인증 및 SMS 기능성을 향상시키는 J-STD-038Ⅲ에 대한 발전된 형태(evolution)를 나타낸다. 이러한 GGG 솔루션은 CDMA RAN 뿐만 아니라 표준 CDMA MSC/VLR을 사용한다. GGG는 HLR, AuC, GMSC 및 SMSC와 같은 표준 GSM 네트워크 엘리먼트들 및 이러한 엘리먼트들 사이에서 상호작용한다. GGG를 사용하는 이러한 GSM 시스템 구조는 도2에 제시된다.

[0084] MSN 구조

[0085] 도1은 본 발명의 일 실시예에 따라 MSN을 사용하는 시스템 구조(100)에 대한 블록 다이어그램이다. 상기 시스템(100)은 이동국들(102), CDMA 네트워크(104), GSM 네트워크(106), MSN(108), PDSN(110), IP 네트워크(112) 및 PSTN(114)을 포함한다.

[0086] CDMA 네트워크(104)는 BTS 들 및 BSC 들을 포함한다. CDMA 네트워크(104)는 PDSN(110)과 인터페이스하고, PDSN(110)은 IP 네트워크(112)와 인터페이싱한다. 일 실시예에서, CDMA 네트워크(104) 및 PDSN(110) 사이의 인터페이스는 IOS4.x에 따른다. 일 실시예에서, PDSN(110) 및 IP 네트워크(112) 사이의 인터페이스는 IP를 사용한다.

[0087] CDMA 네트워크(104)는 GSM MSN(108)과 인터페이싱한다. 일 실시예에서, CDMA 네트워크(104) 및 GSM MSN(108) 사이의 인터페이스는 IOS4.x를 따른다.

[0088] GSM MSN(108)은 PSTN(114)과 인터페이싱한다. 일 실시예에서, GSM MSN(108) 및 PSTN(114) 사이의 인터페이스는 ISUP를 통해 이뤄진다.

[0089] GSM MSN(108)은 GSM 네트워크(14)와 인터페이싱한다. 일 실시예에서, GSM 네트워크(14)는 GSM SS7(116), GSM 단문 메시지 센터(GSM SMSC)(118), GSM 홈 위치 등록기(GSM HLR)(120) 및 GSM 인증 센터(GSM AuC)(122)를 포함한다.

[0090] GGG 아키텍쳐

[0091] 도 2는 일 실시예에 따른 CDMA 네트워크(12), GSM 네트워크(14), 범용 글로벌 게이트웨이(GGG)(16) 및 이동국들(18, 20, 22, 24)을 포함하는 무선 통신 시스템(10)의 블록 다이어그램을 도시한다. GSM 이동국(20)은 가입자 아이덴티티 모듈(SIM)(28)을 포함한다. CDMA 이동국(24)은 SIM(28)을 포함한다. SIM들(26, 28)은 기술적으로 공지된 원리들에 따라, 각각 이동국들(20, 24)에서 제거할 수 있도록 이동식으로 연결되어 있다. 일 실시예에서, GGG는 범용 글로벌 게이트웨이이다.

[0092] GGG(16)는 CDMA 네트워크(12)와 GSM 네트워크(14) 사이를 네트워킹한다. GGG는 CDMA 네트워크(12) 및 GSM 네트워크(14)로 메시지들을 전송하거나 이들로부터 메시지들을 수신하도록 허용하는 송수신기(미도시)를 포함한다.

[0093] 일 실시예에서, CDMA 네트워크는 ANSI-41 네트워크이다. CDMA 네트워크(12)가 cdma2000-1x 및 cdma2000-1xEV-DO를 포함하는 임의의 다양한 CDMA 네트워크들을 포함하되, 이들에 한정되지 않는다는 것은 당업자에게 명백한 사항이다. 또한, GSM 네트워크(14)가 범용 패킷 무선 서비스(GPRS), 유니버셜 이동 통신 시스템(UMTS) 및 광대역-CDMA(W-CDMA)를 포함하는 임의의 다양한 GSM 네트워크 또는 대체 네트워크를 포함하되, 이들에 한정되지 않는다는 것은 당업자에게 명백한 사항이다.

[0094] GSM 네트워크(14)는 GSM 코어(30) 및 GSM 무선 액세스 네트워크(32)를 포함한다. GSM 코어(30)는 GSM 홈 위치 등록기(GSM HLR)(34), GSM 인증 센터(GSM AuC)(36), GSM 단문 메시지 센터(GSM SMSC)(38) 및 GSM 게이트웨이 이동 스위칭 센터(GSM GMSC)(40)를 포함한다. CDMA 네트워크(12)는 CDMA 홈 위치 등록기(CDMA HLR)(42), CDMA 인증 센터(CDMA AuC)(44), CDMA MSC(46) 및 관련된 CDMA 무선 액세스 네트워크(CDMA RAN)(48)을 포함한

다.

[0095] CDMA 코어(20)에 가입된 GSM 이동국과 관련하여, GGG(16)는 방문자 위치 등록기(VLR)(50)로서 GSM 네트워크(14)에서 기능한다. GSM 코어(30)에 가입된 CDMA 이동국(24)과 관련하여, GGG(16)는 방문자 위치 등록기(Visitor LR)(52)로서 CDMA 네트워크(12)에서 기능한다.

[0096] 이동국들(18, 20, 22, 24)은 코어 인프라구조들(12, 14) 모두에 가입할 필요는 없으며 코어 인프라구조들(12, 14) 중 하나에만 가입할 수 있다.

[0097] CDMA 코어(20)에 가입된 GSM 이동국과 GSM 코어(24)에 가입된 CDMA 이동국 모두와 관련하여, GGG(16)는 단문 메시지 서비스 센터(SMSC)(54)로서 기능한다. GGG(16)는 SMSC(54)를 포함하거나 SMSC(54)와 통신할 수 있으며, 이는 당업자에게 명백한 사항이다.

[0098] 이동국들(18, 20)은 GSM 시그널링 프로토콜, GSM 인증 절차 및 GSM 단문 메시지 서비스를 지원한다. 마찬가지로, 이동국들(18, 20)은 CDMA 시그널링 프로토콜, CDMA 인증 절차 및 CDMA 단문 메시지 서비스를 지원한다.

[0099] GSM 코어(24)에 가입된 CDMA 이동국을 등록하는 동안에, GGG는 CDMA 네트워크에서 인증 제어기로서 동작하지만, GSM 인증 메커니즘을 이용하여 이동국(24)을 인증한다. 마찬가지로, CDMA 코어(20)에 가입된 GSM 이동국을 등록하는 동안에, GGG는 GSM 네트워크에서 인증 제어기로서 동작하지만, CDMA 인증 메커니즘을 이용하여 이동국(20)을 인증한다.

[0100] GGG는 단문 메시지 서비스 센터(54)를 통해 메시지 센터로서 동작한다. CDMA 네트워크에서, SMS 메시지들은 CDMA SMS 메커니즘을 이용하여 이동국(24)으로부터 그리고 이동국(24)으로 라우팅된다. 즉, CDMA 네트워크에서, GSM 메시지들은 CDMA SMS 메커니즘을 이용하여 이동국(24)으로부터 그리고 이동국(24)으로 터널링된다. GSM 메시지들은 CDMA SMS 메시지들 내에 캡슐화된다.

[0101] 마찬가지로, GSM 네트워크에서, SMS 메시지들은 GSM SMS 메커니즘을 이용하여 이동국(20)으로부터 그리고 이동국(20)으로 라우팅된다. 즉, GSM 네트워크에서, CDMA 메시지들은 GSM SMS 메커니즘을 이용하여 이동국(20)으로부터 그리고 이동국(20)으로 터널링된다. CDMA 메시지들은 GSM SMS 메시지들 내에 캡슐화된다.

[0102] 등록된 GSM 가입자(24)에 대한 인입 호출은 가입자의 홈 GSM 네트워크(14)에서 GSM 게이트웨이 MSC(GSM GMSC)(40)에 도달한다. GMSC(40)는 CDMA 네트워크(12)에 있는, 가입자(24)의 위치를 결정하기 위해 GSM LR(50)을 조회한다. GSM LR(50)의 관점으로부터의 GSM 가입자(24)의 위치는 GGG(16)에 있으며, GGG(16)는 GSM VLR로 나타난다. GSM LR(50)이 GGG(16)로부터의 라우팅 정보를 요구하면, GGG(16)는 서비스 CDMA LR(52)로부터의 라우팅 정보를 요구하고 그리하여 상기 호출은 CDMA MSC(46)로 라우팅된다.

[0103] 마찬가지로, 등록된 CDMA 가입자(20)에 대한 인입 호출은 가입자의 홈 CDMA 네트워크(12)에서 CDMA MSC(46)로 도달한다. CDMA MSC(46)는 GSM 네트워크(14)에 있는, 가입자(20)의 위치를 결정하기 위해 CDMA LR(52)을 조회한다. CDMA LR(52)의 예측에 의한 CDMA 가입자(20)의 위치는 GGG(16)에 있으며, GGG(16)는 CDMA VLR로 나타난다. CDMA LR(52)이 GGG(16)로부터의 라우팅 정보를 요구하면, GGG(16)는 서비스 GSM LR(50)로부터의 라우팅 정보를 요구하고 그리하여 상기 호출은 GSM GMSC(40)로 라우팅된다.

[0104] CDMA-기반 이동국들(22, 24)은 기술적으로 공지된 CDMA 원리들에 따라 CDMA 무선 액세스 네트워크(RAN)(48)를 사용하여 CDMA 이동 스위칭 센터(MSC)(46)와 통신한다. 일 실시예에서, CDMA MSC(46)는 IS-41 MSC이다.

[0105] 마찬가지로, GSM-기반 이동국들(18, 20)은 기술적으로 공지된 GSM 원리들에 따라 GSM RAN(32)을 사용하여 GSM 이동 스위칭 센터(GSM GMSC)(40)와 통신한다.

[0106] 기술적으로 공지된 CDMA 원리들에 따라, CDMA RAN(48)은 기지국들과 기지국 제어기들을 포함한다. 일 실시예에서, 도 2에 도시된 CDMA RAN(24)은 cdma2000을 이용하며, 구체적으로 cdma2000 1x, cdma2000 3x 또는 cdma2000 고속 데이터 레이트(HDR) 원리들을 이용한다.

[0107] 기술적으로 공지된 GSM 원리들에 따라, GSM RAN(32)은 기지국들과 기지국 제어기들을 포함한다. 일 실시예에서, GSM RAN(32)은 GSM, GPRS, EDGE, UMTS 또는 W-CDMA 원리들을 이용한다.

[0108] CDMA MSC(46)와 CDMA RAN(48)을 포함하는 CDMA 코어 인프라구조는 가입자 이동국(22)을 인증하고, 특정 CDMA 코어 인프라구조에 의해 요구되는 계정 및 빌링(billing) 정보를 수집하기 위해, 기술적으로 공지된 CDMA 원리들에 따라 CDMA 인증 센터(CDMA AuC)(44) 및 CDMA 홈 위치 등록기(CDMA HLR)(42)를 포함하거나 또는 액세스할 수 있다.

[0109] 마찬가지로, GSM 코어(30)는 가입자 이동국(18)을 인증하고, 특정 GSM 코어 인프라구조에 의해 요구되는 계정 및 빌링 정보를 수집하기 위해, 기술적으로 공지된 GSM 원리들에 따라 GSM 인증 센터(GSM AuC)(36) 및 GSM 홈 위치 등록기(GSM HLR)(34)를 포함하거나 또는 액세스할 수 있다.

[0110] CDMA MSC(46)는 GSM 네트워크(14)와 통신하기 위해 GGG(16)를 사용한다. GSM 네트워크(14)는 가입자 이동국(24)을 인증하고 특정 GSM 코어(30)에 의해 요구되는 계정 및 빌링 정보를 수집하기 위해, 기술적으로 공지된 GSM 원리들에 따라 GSM 인증 센터(36) 및 GSM 홈 위치 등록기(HLR)(34)를 포함하거나 또는 액세스할 수 있다.

[0111] 마찬가지로, GSM GMSC(40)는 CDMA 네트워크(12)와 통신하기 위해 GGG(16)를 사용한다. CDMA 네트워크(12)는 가입자 이동국(20)을 인증하고 특정 CDMA 네트워크(12)에 의해 요구되는 계정 및 빌링 정보를 수집하기 위해, 기술적으로 공지된 CDMA 원리들에 따라 CDMA 인증 센터(44) 및 CDMA 홈 위치 등록기(HLR)(42)를 포함하거나 또는 액세스할 수 있다.

[0112] GSM 코어(30)와 CDMA 코어 인프라구조 모두는 공중 전화 교환망(PSTN) 및/또는 인터넷 프로토콜(IP) 네트워크와 같은 네트워크와 통신할 수 있다.

[0113] GSM 코어(30)에 가입된 CDMA 이동국(24)과 관련하여, GGG(16)는 GSM 네트워크(14)에 대한 VLR(50)로서 기능한다. GGG는 VLR(50)을 위한 GSM 프로토콜 요구들을 충족시킨다. GGG(16)가 인입 호출들을 CDMA 네트워크(12)로 라우팅하는 것을 제외하고, GGG는 GSM 규격들에 따라 GSM HLR(34) 및 GSM SMSC(38)와 같은 GSM 코어 네트워크 엘리먼트들과 상호 작용한다. 상기 이동국이 CDMA 네트워크(12)에 등록하면, GSM LR(50)은 또한 GSM 네트워크(14)를 통해 위치 갱신을 수행한다. 이러한 측면에서, GGG는 전체 CDMA 네트워크(12)에 대한 VLR로서 동작한다.

[0114] CDMA 네트워크(12)에 가입된 GSM 이동국(20)과 관련하여 GGG(16)는 CDMA 네트워크(14)에 대한 VLR(52)로서 기능한다. GGG(16)는 VLR(52)을 위한 CDMA 프로토콜 요구들을 충족시킨다. GGG(16)가 인입 호출들을 CDMA 네트워크(12)로 라우팅하는 것을 제외하고, GGG는 CDMA 사양들에 따라 CDMA HLR(42) 및 CDMA MSC(46)와 같은 CDMA 코어 네트워크 엘리먼트들과 상호 작용한다. 상기 이동국이 GSM 네트워크(14)에 등록하면, CDMA LR(52)은 또한 CDMA 네트워크(12)를 통해 위치 갱신을 수행한다. 이러한 측면에서, GGG는 전체 GSM 네트워크에 대한 VLR로서 동작한다.

[0115] CDMA 네트워크(12)에 있는 이동국이 GSM 네트워크(14)로부터 호출을 받으면, 호출은 표준 규격들 마다 GGG(16)에 있는 CDMA LR(52)로 라우팅된다. GGG(16)는 상기 호출을 CDMA 네트워크(12)로 라우팅한다. CDMA 네트워크(12)는 결국 상기 호출을 상기 이동국을 서비스하는 CDMA MSC(46)로 라우팅한다. 유사하게, SMS가 GSM 네트워크(14)로부터 CDMA 네트워크(12)로 라우팅되면, GGG(16)는 CDMA 네트워크(12) 내에 있는 메시지 센터(미도시)로 메시지를 라우팅한다.

[0116] GSM 네트워크(14)에 있는 이동국이 CDMA 네트워크(12)로부터 호출을 받으면, 호출은 표준 사양들에 따라 GGG(16)에 있는 GSM LR(50)로 라우팅된다. GGG(16)는 상기 호출을 GSM 네트워크(14)로 라우팅한다. GSM 네트워크(14)는 결국 상기 호출을 상기 이동국을 서비스하는 GSM GMSC(40)로 라우팅한다. 유사하게, SMS가 CDMA 네트워크(12)로부터 GSM 네트워크(14)로 라우팅되면, GGG(16)는 GSM 네트워크(14) 내에 있는 GSM SMSC(38)로 메시지를 라우팅한다.

[0117] 이동국이 CDMA 네트워크(12)를 통해 등록하면, CDMA 네트워크(12)는 GSM 네트워크(14)로 위치 갱신 표시를 전송한다. 그 후에 GSM LR(50)은 표준 사양들에 따라 GSM 코어 네트워크(14)를 통해 위치 갱신을 수행한다.

[0118] 이동국이 GSM 네트워크(14)에 등록하면, GSM 네트워크(14)는 CDMA 네트워크(12)로 위치 갱신 표시를 전송한다. 그 후에 CDMA LR(52)은 표준 사양들에 따라 CDMA 네트워크(12)를 통해 위치 갱신을 수행한다.

[0119] GSM 코어(30)에 가입된 CDMA 이동국(24)과 관련하여, GGG(16)는 CDMA 네트워크(12)에서 HLR(52)로서 동작한다. CDMA LR(52)은 GSM에서 CDMA로의 로밍을 위한 HLR 프로토콜 요구들을 충족시켜야 한다. HLR(50)이 가지고 있는 정보 중 중요한 부분은 이동국(24)을 서비스하는 CDMA MSC(46)의 주소이다. GGG(16)에 있는 GSM LR(50)이 호출을 CDMA 측(12)으로 라우팅하면, CDMA LR(52)은 추가적으로 상기 호출을 서비스 MSC(46)로 라우팅할 것이다.

[0120] CDMA 네트워크(12)에 가입된 GSM 이동국(20)과 관련하여, GGG(16)는 GSM 네트워크(14)에서 HLR(50)로서 동작한다. GSM LR(50)은 CDMA에서 GSM로의 로밍을 위한 HLR 프로토콜 요구들을 충족시켜야 한다. HLR이 가지고 있는 정보 중 중요한 부분은 이동국(20)을 서비스하는 GSM GMSC(40)의 주소이다. GGG(16)에 있는 CDMA

LR(52)이 호출을 GSM 측(14)으로 라우팅하면, GSM LR(50)은 추가적으로 상기 호출을 서비스 MSC(40)로 라우팅할 것이다.

[0121] GGG는 GSM 가입자들(24)에 대하여 CDMA 네트워크에서 인증 제어기(AUC)로서 동작한다. CDMA 네트워크(12)에 있는 AUC(44)는 이동국의 인증과 네트워크 자원들에 대한 허용/거부를 담당한다. GGG에 있는 AUC 기능은 GGG 또는 MS에서 A-키 제공(provisioning)을 요구하지 않는다. 대신에 GGG는 이동국(24)을 인증하기 위해 GSM 인증서와 GSM 시그널링을 통한 GSM 인증 방법을 이용한다. GGG는 CDMA AUC(44)에 의해 수신될 수 있는 유효 메시지들에 응답한다.

[0122] GGG는 CDMA 가입자들(20)에 대하여 GSM 네트워크에 있는 인증 제어기(AUC)로서 동작한다. GSM 네트워크(14)에 있는 AUC(36)는 이동국의 인증과 네트워크 자원들에 대한 허용/거부를 담당한다. GGG에 있는 AUC 기능은 GGG 또는 MS에서 A-키 제공을 요구하지 않는다. 대신에 GGG는 이동국(20)을 인증하기 위해 CDMA 인증서와 CDMA 시그널링을 통한 CDMA 인증 방법을 이용한다. GGG는 GSM AUC(36)에 의해 수신될 수 있는 유효 메시지들에 응답한다.

[0123] GGG(16)는 CDMA 네트워크(12)에서 메시지 센터(MC)로서 동작하며 GSM SMS 메커니즘을 이용하여 CDMA 이동국(24)과 GSM GMSC(40) 사이에서 SMS 메시지들을 라우팅한다.

[0124] 마찬가지로, GGG(16)는 GSM 네트워크(14)에서 메시지 센터(MC)로서 동작하며 CDMA SMS 메커니즘을 이용하여 GSM 이동국(20)과 CDMA MSC(46) 사이에서 SMS 메시지들을 라우팅한다.

[0125] CDMA MS(24)는 CDMA 네트워크에 유효 아이덴티티를 가질 필요가 있다. 이 아이덴티티가 GSM 국제 이동 가입자 아이덴티티(IMSI)과 다르다면(즉, CDMA 네트워크가 정확한 IMSI를 사용하지 않는다면), GGG는 CDMA 아이덴티티와 GSM IMSI간 맵핑을 제공한다. 이동국(24)을 고유하게 식별하기 위해 당업계에 공지된 어떠한 기술/방법도 사용될 수 있음이 당업자들에게 명백하다.

[0126] GSM MS(20)는 GSM 네트워크에 유효 아이덴티티를 가지도록 요구된다. 실시예에서 이 아이덴티티는 GSM IMSI이다(즉, CDMA 네트워크가 정확한 IMSI를 사용하지 않는다면). GSM 네트워크 내 아이덴티티(identity)가 CDMA 네트워크 내 아이덴티티와 다르다면, GGG는 GSM 아이덴티티와 CDMA 아이덴티티 간 맵핑을 제공한다. 이동국(20)을 고유하게 식별하기 위해 당업계에 공지된 임의의 기술/방법이 사용될 수 있음이 당업자들에게 명백하다.

[0127] 제한적이지 않은 실시예에서, 이동국(18, 20)은 Kyocera, Samsung, 또는 GSM 원리 및 GSM OTA(over-the-air) 통신 무선 인터페이스를 이용하는 다른 제조사에 의해 제조된 이동 전화기이다. 제한적이지 않은 실시예에서, 이동국(22, 24)은 Kyocera, Samsung, 또는 CDMA 원리 및 CDMA OTA(over-the-air) 통신 무선 인터페이스를 이용하는 다른 제조사에 의해 제조된 이동 전화기이다. 그러나 본 발명은 랩탑 컴퓨터, 무선 핸드셋 또는 전화기, 데이터 트랜시버, 또는 페이징 및 위치 결정 수신기와 같은 다른 이동국에 적용된다. 이동국은 필요에 따라 (자동차, 트럭, 보트, 비행기, 기차를 포함하는) 차량 장착용으로 핸드-헬드 식이거나 휴대가능할 수 있다. 그러나 무선 통신 장치들은 일반적으로 이동성이 있는 것으로 간주되지만, 본 발명은 일부 실시예들에서는 "고정" 유닛에 적용될 수 있는 것으로 이해해야 한다. 또한, 본 발명은 디지털 비디오 정보를 포함하는 음성 및/또는 데이터 정보를 전달하는데 사용되는 데이터 모듈 또는 모뎀에 적용되며, 유선 또는 무선 링크를 이용하여 다른 장치들과 통신할 수도 있다. 또한, 모뎀이나 모듈을 미리 결정된 조화 또는 조합 방식으로 작동시켜 다수의 통신 채널로 정보를 전달하는 명령들이 사용될 수 있다. 무선 통신 장치들은 어떤 통신 시스템들에서 때때로 사용자 단말, 이동국, 이동 유닛, 가입자 유닛, 이동 라디오 또는 무선 전화, 무선 유닛이라고도 하며, 또는 간단히 "사용자" 및 "모바일"이라고도 한다.

[0128] <u>SSD를 사용하지 않는 인증</u>

[0129] 도 3a 및 3b는 SSD를 사용하지 않는 실시예에 따라 GSM 네트워크(14)의 가입에 대한 CDMA 이동국(24)을 인증하기 위한 흐름도를 나타낸다. 도 3a 및 3b는 도 6의 설명으로 알고 있는 바와 같이 설명된다.

[0130] 단계(202)에서 이동국(MS;24)은 CDMA 영역으로 로밍하고, 제어 흐름은 단계(204)로 진행한다. 단계(204)에서 이동국(24)은 CDMA RAN(48)을 통해 CDMA MSC(46)로의 등록 시스템 액세스를 초기화하고, 제어 흐름은 단계(206)로 진행한다.

[0131] 등록 시스템 액세스는 CDMA RAN(48)을 통한 CDMA MSC(46)로의 메시지이며, 상기 메시지는 이동국(24)의 아이

덴티티를 포함한다. 일 실시예에서, 이동국(24)의 아이덴티티는 SIM(28)에 의해 제공될 수 있다. 일 실시예에서, 이동국(24)의 아이덴티티는 IMSI이다. 일 실시예에서, 이동국(24)의 아이덴티티는 이동국 아이덴티티 번호(MIN)이다.

[0132] 단계(206)에서 CDMA MSC(46)는, 이동국 아이덴티티에 기반하며, 이동국(24)이 GSM 가입자인지의 여부를 결정한다. 일 실시예에서, 이동국(24)의 아이덴티티는 IMSI이고, IMSI가 다른 정보 중에서도 특히 이동국이 가입하고 있는 국가 및 네트워크를 나타내는 코드를 포함하기 때문에 MSC(46)가 이것을 결정할 수 있다.

[0133] CDMA 가입 이동국(22)이 시험중인 이동국인 경우에, 제어 흐름은 단계(208)로 진행한다. 단계(208)에서 이동국(22)은 CDMA HLR(42) 및 CDMA AUC(44)를 사용하는 CDMA 코어 인프라구조에 의한 CDMA 원리를 이용하여 인증된다.

[0134] GSM 네트워크(14)에 가입한 CDMA 이동국(24)이 시험중인 이동국인 경우에, 제어 흐름은 단계(210)로 진행한다. 단계(210)에서 CDMA MSC(46)는 GGG(16)에서 CDMA LR(52)에 인증 요구를 전송함으로써 GGG(16)에 액세스하고, 실시예에 따라 제어 흐름은 단계(212)로 진행한다. 다른 실시예에서, 제어 흐름은 단계(214)로 진행한다.

[0135] 일 실시예에서, 이동국(24)의 아이덴티티는 인증 요구의 일부분로서 CDMA LR(52)에 전송된다. 대안으로, 인증 요구 외에도 이동국(24)의 아이덴티티가 CDMA LR(52)로 전송된다.

[0136] 일 실시예에서, 인증 요구는 파라미터(MIN, ESN, COUNT)를 포함할 수 있다. ESN은 전자 일련 번호이다.

[0137] 일 실시예에서, 인증 요구는 파라미터(MIN, ESN, COUNT)를 포함할 수 있다. ESN은 전자 일련 번호이다. COUNT는 GGG(16)와 이동국(24)간의 상호 협의된 이벤트인 미리 결정된 이벤트의 카운트를 나타낸다. 일 실시예에서, GGG(16)는 GGG(16)와 상호 작용하는 노드와 COUNT의 업데이트를 공유한다. 다른 노드와의 업데이트 기능을 공유함으로써, GGG(16)와 다른 노드간 메시지 트래픽이 감소할 수 있다. 예를 들어, GGG(16)가 COUNT의 업데이트 기능을 CDMA MSC(46)와 공유한다면, GGG(16)와 CDMA MSC(46) 사이의 메시지 트래픽이 감소할 수 있다.

[0138] 일 실시예에서, COUNT는 이동국(24)이 GSM 네트워크(14)로의 액세스를 시도하는 회수를 나타낸다. 이동국(24)이 GSM 네트워크에 액세스할 때마다 GGG는 특정 이동국(24)에 대한 COUNT를 업데이트한다. 이동국(24)은 또한 자신이 GSM 네트워크(14)에 액세스하는 회수에 대해 자신의 COUNT를 업데이트한다. GGG(16)는 ESN의 값을 저장한다. 다른 실시예에서, COUNT는 이동국에 의한 인증 요구 수를 나타낸다. 카운트될 수 있는 많은 이벤트가 존재하며, 이동국(24) 및 GGG(16)가 이를 카운트할 수 있음이 당업자들에게 명백하다.

[0139] 단계(212)에서 GGG(16)는 COUNT 값과 GGG 데이터베이스의 카운트 값을 비교한다. COUNT 값이 GGG 데이터베이스의 카운트 값과 동일하다면, 제어 흐름은 단계(214)로 진행한다. COUNT 값이 GGG 데이터베이스의 카운트 값과 동일하지 않다면, 제어 흐름은 단계(216)로 진행한다. 어플리케이션에 따라, 인증 요구가 유효한지 여부를 결정하는데 다양한 기준이 적용될 수 있음이 당업자에게 명백하다.

[0140] 단계(214)에서 인증 요구 리턴 결과(ARRR)가 참(true)으로 설정되고, 제어 흐름은 단계(218)로 진행한다. 인증 요구 리턴 결과 메시지는 인증 요구 결과를 나타낸다.

[0141] 단계(216)에서 인증 요구 리턴 결과는 거짓(false)으로 설정되고, 제어 흐름은 단계(220)로 진행한다.

[0142] 참의 인증 요구 리턴 결과에 응답하여, GGG(16)는 GSM 네트워크(14)에 액세스하여 GSM HLR(34) 및 GSM AuC(36)로부터 필요한 인증 정보를 얻는다. 단계(218)에서 GGG(16)는 데이터베이스 내에서 MIN을 검색하여 대응하는 GSM IMSI를 얻고, 일 실시예에 따라 이동국(24)의 IMSI를 갖는 GSM HLR 인증 메시지를 GSM HLR/AuC(34, 36)에 전송함으로써 GSM 네트워크(14)에 액세스한다. 제어 흐름은 단계(220)로 진행한다.

[0143] 방법 단계들은 본 발명의 범위를 벗어나지 않으면서 교환될 수 있다. 따라서 단계(218)는 단계(220) 전에 수행될 필요는 없음이 당업자에게 명백하다.

[0144] 단계(220)에서 GGG(16)는 CDMA MSC(46)에 인증 요구 리턴 결과를 전송하고 제어 흐름은 단계(222)로 진행한다. 단계(222)에서 인증 요구 리턴 결과가 검사된다. 인증 요구 리턴 결과가 참이면, 단계(224)에서 GGG(16)는 타이머(T_{REG})를 시작하고 제어 흐름은 단계(226)로 진행한다.

[0145] 인증 요구 리턴 결과가 거짓이라면, 제어 흐름은 단계(228)로 진행한다. 단계(228)에서 CDMA MSC(46)는 인증되지 않은 이동국(24)을 지시하는 이동국(24)에 이동국 인증 메시지를 전송한다. 이동국은 응용에 따라 인증

을 재시도할 수 있음이 당업자에게 명백하다.

[0146] GGG는 프로그램 로직을 실행하기 위한 로직 유닛(미도시)을 포함한다. 로직 유닛은 범용 프로세서, 전용 프로세서 및/또는 펌웨어를 포함할 수 있음이 당업자들에게 명백하다.

[0147] 단계(226)에서 성공적인 인증을 표시하는 인증 요구 리턴 결과를 수신할 때 CDMA MSC(46)는 GGG(16)의 CDMA LR(52)에 등록 통보를 전송한다. 제어 흐름은 단계(230)로 진행한다.

[0148] 단계(230)에서 T_{REG} 종료 전에 GGG(16)가 등록 통보를 수신했는지 여부를 결정하기 위한 확인이 이루어진다. T_{REG} 종료 전에 GGG(16)가 등록 통보를 수신했다면, 제어 흐름은 단계(232)로 진행하고, 그렇지 않으면 제어 흐름은 단계(234)로 진행한다. 단계(232)에서 등록 통보 리턴 결과는 T_{REG}가 종료하지 않았음을 지시하도록 설정되고, 제어 흐름은 단계(236)로 진행한다. 단계(234)에서 등록 통보 리턴 결과는 T_{REG}가 종료했음을 지시하도록 설정되고, 제어 흐름은 단계(236)로 진행한다.

[0149] 단계(236)에서 GGG(16)는 T_{REG}가 종료했는지 여부를 지시하는 등록 통보 리턴 결과로 등록 통보에 응답한다. 등록 통보 리턴 결과는 GGG(16)에서 CDMA MSC(46)로 진행한다.

[0150] 일 실시예에서, GGG(16)는 SMS 전용 모드/상태를 지시하는 등록 통보 리턴 결과를 갖는 또는 상기 등록 통보 리턴 결과 내의 메시지를 전송한다. "SMS 전용"은 이동국(24)이 SMS 메시지만 송신 및 수신하고, 데이터 및/또는 음성 메시지는 송신 및 수신하지 않는 것을 의미한다. 제어 흐름은 단계(238)로 진행한다.

[0151] 단계(238)에서 CDMA MSC(46)는 등록 통보 리턴 결과 수신시 이동국(24)에 등록 수락 메시지를 전송한다. 등록 통보 리턴 결과와 같이, 등록 수락 메시지는 T_{REG}가 종료했는지 여부를 지시한다. 제어 흐름은 단계(240)로 진행한다.

[0152] 단계(240)에서 이동국(24)은 등록 수락 메시지가 수락된 등록을 지시하는지 여부, 즉 T_{REG}가 종료하지 않았는지 여부를 결정한다. T_{REG}가 종료했다면, 제어 흐름은 단계(242)로 진행하고, 그렇지 않으면 제어 흐름은 단계(244)로 진행한다.

[0153] 단계(242)에서 이동국(24)은 등록을 재시도할 수도 있고 재시도하지 않을 수도 있다. 이동국 어플리케이션에 따라, 이동국이 등록을 재시도할 수도 있고 재시도하지 않을 수도 있음이 당업자에게 명백하다.

[0154] 방법 단계들은 본 발명의 범위를 벗어나지 않으면서 교환될 수 있다. 따라서 단계(244)는 단계(242) 후에 수행될 필요가 없음이 당업자에게 명백하다.

[0155] 단계(244)는 GSM HLR 인증 메시지가 단계(218)의 GSM HLR/AuC(34, 36)에 전송될 후에만 실행되어야 한다. 단계(244)에서 GSM HLR/AuC(34, 36)는 인증 파라미터를 포함하는 GGG 인증 메시지를 GGG(16)에 전송하고 제어 흐름은 단계(246)로 진행한다.

[0156] GGG(16)가 CDMA MSC(46)에 등록 통보 리턴 결과를 성공적으로 전송하고 GSM HLR/AuC(34, 36)로부터 GGG 인증 메시지를 수신한 후, 단계(246)에서 GGG(16)는 CDMA MSC(46)에 GSM 인증 요구 메시지를 전송한다. 제어 흐름은 단계(248)로 진행한다. 단계(248)에서, CDMA MSC(46)는 이동국(24)에 GSM 인증 요구 메시지를 전달하고, 제어 흐름은 단계(250)로 진행한다.

[0157] 일 실시예에서, 단계(210)의 원래 인증 요구에 적용된 기준을 제외하고 응용은 이동국을 인증하기 위한 더 많은 기준을 가질 수도 있다. 따라서, 일 실시예에서, CDMA MSC(46)는 GGG(16)에 제 2 인증 요구(미도시)을 전송하고 GGG(16)는 제 2 인증 요구(미도시)에 응답한다.

[0158] 단계(250)에서 이동국(24)은 GSM 인증 방법을 이용하여 암호화 키와 같은 인증 파라미터를 결정하고 CDMA MSC(46)에 인증 파라미터를 포함하는 인증 응답을 전송함으로써 GSM 인증 요구 메시지에 응답한다. 일 실시예에서, 인증 응답은 IS-637 SMS 전송을 이용하여 전송된다. 제어 흐름은 단계(252)로 진행한다.

[0159] 단계(252)에서 CDMA MSC(46)는 GGG(16)에 인증 응답을 전달하고, GGG(16)는 단계(244)에서 인증 파라미터를 GSM HLR/AuC(34, 36)로부터 수신된 값들과 매치시킴으로써 인증 파라미터를 유효화한다. 제어 흐름은 단계(254)로 진행한다.

[0160] 단계(254)에서 GGG(16)는 GSM HLR(34)에 업데이트 위치 메시지를 전송하여 이동국(24)의 위치를 업데이트하고 제어 흐름은 단계(256)로 진행한다. 단계(256)에서 GSM HLR(34)은 이동국(24)의 GSM 가입자 프로파일 데이터

를 GGG(16)의 GSM LR(50)에 전송한다. 제어 흐름은 단계(258)로 진행한다.

[0161] 단계(258)에서, GGG(16)는 CDMA 가입자 프로파일로 GSM 가입자 프로파일 데이터를 맵핑하고 자격부여 지시(Qualification Directive)에 있는 CDMA 프로파일 데이터를 CDMA MSC(46)으로 전송하며, 제어 흐름은 단계(260)로 진행한다. 자격부여 지시는 이동국(24)이 자격을 부여받았을, 즉 GSM 네트워크(14)와 통신하도록 인가됨을 의미한다. 만일 이동국(24)이 자격을 부여받지 않았다면, 이동국(24)은 GSM 네트워크(14)(미도시)와 통신할 권한이 없다. 실시예에서, GGG(16)는 CDMA MSC(46) "풀 프로파일"을 나타내며, 이는 차례로 이동국으로 전달되어 이동국(24)이 SMS 메시지에 한정되지 않고 전송 및 수신할 수 있음을 나타낸다.

[0162] 단계(260)에서, CDMA MSC(46)은 자격부여 지시에 응답하고, 자격부여 지시 응답(Qualification Directive Response)을 CDMA LR(52)로 전송하고 제어 흐름은 단계(262)로 진행한다.

[0163] 단계(262)에서, GSM 가입자 프로파일 데이터를 수신하는 GSM LR(50)에 응답하여, GGG(16)은 GSM 가입자 프로파일 데이터 응답을 GSM HLR/AuC(34, 36)로 전송한다.

[0164] 단계(264)에서, 단계(254)에서의 GGG(16)으로부터의 업데이트 위치 메시지를 수신하는 GSM HLR(34)에 응답하여, GSM HLR(34)는 업데이트 위치 메시지에 응답하고 업데이트 위치 메시지 응답을 GSM LR(50)로 전송하는데, 업데이트 위치 메시지 응답은 이동국(24)의 위치가 GSM LR(50)에서 업데이트됨을 나타낸다.

[0165] 인증 키

[0166] GGG가 J-STD-038IIF와 대단히 상이한 부분은 인증의 영역에서이다. J-STD-038 IIF는 로밍 가입자가 이중 예약-하나는 ANSI-41이고 다른 하나는 GSM-을 갖기 때문에, 가입자를 ANSI-41 외래(foreign) 모드에서 인증하기 위해 표준 ANSI-41 기술을 사용한다. 대조적으로, GGG 솔루션은 ANSI-41 외래 모드 로밍자가 완전한 ANSI-41 가입을 갖는 것을 요구하지 않는다. 특히, MS 또는 GGG는 ANSI-41 A-키들이 제공될 필요가 있다. 이하에서는 우선 표준 ANSI-41 인증 메커니즘이 설명된다. 이어, ANSI-41 방법에 대한 변경이 설명된다.

[0167] 표준 ANSI-41 인증

[0168] 인증 키들을 생성하는 표준 ANSI-41 방식은 도4에 도시된다. A-키(이동국 및 인증 센터에만 알려진 비밀 데이터) 및 RANDSSD로 불리는 랜덤 번호가 비밀 공유 데이터(SSD)로 불리는 128비트 수를 생성하기 위해 CAVE 알고리즘을 사용하여 프로세싱된다. 이러한 연산은 이동국 및 인증 센터에서 수행된다. SSD는 인증을 위해 사용된 64-비트 SSD-A 키 및 암호화를 위해 사용된 64-비트 SSD B-키로 구성된다. 각각의 시스템 액세스에 대해, 이동국은 SSD-A, ESN, MIN, 인증 데이터(AUTH_DATA-IMSI_S 또는 시스템 액세스 타입에 의존하는 다이얼링된 디지트) 및 오버헤드 메시지에서 RAN에 의해 브로드캐스트되는 랜덤 수(RAND)를 프로세싱함으로써 인증 응답(AUTHR)을 생성한다. 프로세싱은 CAVE 알고리즘을 실행함으로써 다시 수행된다. 이동국은 시스템 액세스에서 AUTHR을 전송하고, 인증 센터(또는 선택적으로 MSC/VLR)가 독립적으로 동일한 계산을 하고 그 결과를 수신된 것과 비교할 때 인증된다.

[0169] SSD-A로서 Kc 사용

[0170] GSM 인증 자격 증명을 사용하는 ANSI-41 네트워크에서 GSM 가입자를 인증하는 목표는 SSD-A로서 Kc를 사용함으로써 달성될 수 있다. 실시예에 따라 SSD-A 키 및 AUTHR(402)을 생성하는 새로운 방법은 도 5에 도시된다. GSM 인증(404)이 이동국에서 그리고 GSM AuC에서 실행될 때, 비밀 키 Ki(가입자의 SIM 및 GSM AuC에만 알려짐) 및 랜덤 수(GSM_RAND)가 SRES 및 암호화 키(Kc)를 생성하기 위해 사용된다. Kc는 길이가 SSD-A와 마찬가지로 64비트이다. 따라서, Kc는 CAVE 알고리즘을 사용하는 AUTHR의 표준 ANSI-41 계산에서 SSD-A 값에 대해 대체될 수 있다.

[0171] GGG가 GSM AuC 및 RAND(418), AuthenticationRequest INVOKE에서의 ESN(420), MIN(422) 및 AUTH_DATA(424)로부터 GSM 인증 트리플렛(즉, GSM_RAND, SRES 및 Kc)을 얻기 때문에, GGG는 이동국이 GSM/RAND(408)를 사용하여 우선 인증된 후, ANSI-41 방법을 사용하여 이동국을 인증하기 위해 SSD-A 값으로서 Kc값을 사용할 수 있다. 다시 말해, 이동국이 GGG에서의 GSM_RAND(408)의 값을 사용하여 GSM 인증을 실행한 후, GGG 및 이동국이 Kc의 공통 값을 갖는다. 이러한 GSM 인증은 IS-637 SMS 전송을 통한 GSM 시그널링을 사용하여 ANSI-41/CDMA2000 네트워크에서 실행될 수 있다. 이동국 및 GGG가 일단 Kc의 동일한 값을 가지면, 이러한 값은 SSD-A로서 사용될 수 있으며, 표준 ANSI-41 방법이 이동국을 인증하기 위해 사용될 수 있다. ANSI-41 인증 기술을 사용하는 장점은 더욱 우수한 시그널링 효율성이다. 이러한 방식은 GSM 자격 증명(credential)을 사용하는 ANSI-41 네트워크에서 이동국을 인증하는 목표에 또한 부합한다.

[0172] SSD 공유를 사용한 인증

[0173] 도 3의 동작 개요의 경우, GGG에서 ANSI-41 AC는 인증 책임을 유지한다. 서빙 MSC/VLR은 GGG에서 ANSI-41 HLR/AC로의 AuthenticationRequest INVOKE를 사용하여 각각의 이동국 액세스 시도(예를 들어, 등록, 발신, 페이즈 응답 및 플래시)에 대해 응답하도록 가정된다. 이러한 방식이 최대 보안성을 제공하지만, ANSI-41 MSC/VLR 및 GGG 사이의 시그널링 트래픽이 가중된다.

[0174] MSC/VLR-HLR/AC 시그널링 트래픽을 감소시키기 위해, AC가 서빙 MSC/VLR을 사용하여 소정의 인증 응답을 분배하게 하는 방법이 이하에서 설명된다. Kc의 값이 도4를 참조하여 설명된 바와 같이, SSD-A를 위해 사용되면, SSD 공유는 GGG 기반 GSM1x 솔루션에 적용된다. 본 섹션의 나머지는 어떻게 SSD 공유가 실행되는 지를 설명한다.

[0175] SSD 업데이트

[0176] 도6은 GGG가 본 실시예에 따라 서빙 MSC/VLR과 공유한 SSD를 업데이트하는 연속적인 SSD 업데이트 절차에 대한 정보 흐름을 도시한다. 이러한 시나리오의 초기 조건은 GGG가 서빙 MSC/MVR과 공유한 SSD를 이미 가지고 있고, MSC/VLR이 시스템 액세스를 실행할 때 MS를 인증하는 것이다.

[0177] 이하의 절차는 이러한 정보 흐름을 개시한다.

[0178] 단계(501)에서, GGG는 MIN, ESN 및 NOSSD 파라미터를 사용하여 ANSI-41 MSC/VLR로의 인증 규격(IS41_AUTHDIR) 호출에 의해 SSD 업데이트를 시작한다.

[0179] 단계(502)에서, MSC/VLR은 특정 MS에 대해 가지고 있는 SSD를 폐지하고 GGG로의 인증 규격 리턴 요구를 호출함으로써 응답한다. MSC/VLR은 이러한 MS의 각각의 시스템 액세스에 대한 GGG에서 HLR/AC로의 AuthenticationRequest을 호출할 것이다.

[0180] 단계(503)에서, GGG는 MS에 대해 CallHistoryCount(COUNT)의 현재 값을 요구하기 위해 MSC/VLR로의 Count Request(IS41_COUNTREQ)를 호출한다.

[0181] 단계(504)에서, MSC/VLR은 요구된 COUNT 파라미터를 포함하는 Count Return Result(IS41_countreq)으로 응답한다.

[0182] 단계(505)에서, GGG가 MS에 대해 어떠한 추가의 GSM 인증 트리플렛을 갖지 않는다면, GGG는 GSM HLR로의 MAP_SEND_AUTHENTICATION_INFO를 호출한다. MS가 시스템을 액세스한 이후, 이하의 단계들이 발생한다.

[0183] 단계(506)에서, GSM HLR은 인증 트리플렛의 세트(적어도 하나)를 포함하는 MAP_send_authentication_info로 응답한다.

[0184] 단계(507)에서, MS가 시스템을 액세스한 이후, 다음 단계가 발생한다.

[0185] 단계(508)에서, SSD가 더 이상 공유되지 않기 때문에, MSC/VLR은 MS 시스템 액세스를 인증하기 위해 GGG로의 Authentication Request(IS41_AUTHREQ)를 호출한다.

[0186] 단계(509)에서, 이전 단계에서 파라미터가 수신되고, Kc(SSD-A)의 값이 MS에 대해 저장된 경우, GGG의 AC는 ANSI-41 인증을 실행한다. AC는 성공적인 ANSI-41 인증을 나타내기 위해 MSC-VLR로의 Authentication Request Return Result(IS41_authreq)를 호출한다.

[0187] 단계(510)에서, GGG는 IS41_SMDPP 전송을 사용하여 GSM1x Authentication Request를 호출함으로써 GSM1x 인증 프로세스를 시작한다.

[0188] 단계(511)에서, MSC는 이러한 SMS를 MS로 전달한다.

[0189] 단계(512)에서, MS는 GSM 인증 방법을 사용하여 SRES 및 Kc를 계산하고, IS-637 SMS 전송을 사용하여 응답(GSM1x Auth Rsp)을 전송함으로써 GSM1x 인증 요구에 응답한다.

[0190] 단계(513)에서, MSC는 SMS를 GGG로 전달하고, GGG는 GSM1x AuthRsp의 SRES가 GSM HLR/AuC로부터 수신된 값에 부합하는지를 확인한다. 이러한 단계는 MS로의 SSD 업데이트를 완료한다.

[0191] 단계(514)에서, MS에 의한 다음 시스템의 액세스시, MSC/VLR은 GGG에 대해 Authentication Request(IS_AUTHREQ)를 호출한다.

[0192] 단계(515)에서, GGG의 AC는 이전 단계에서 파라미터가 수신되고 Kc(SSD-A)의 값이 MS에 대해 저장된 경우,

ANSI-41 인증을 실행한다. 이후 AC는 성공적인 ANSI-41 인증을 나타내기 위해 MSC/VLR 쪽으로 Authentication Request Ruturn Result(IS41_authreq)를 호출한다. SSD 파라미터가 MSC/VLR과 SSD를 공유하기 위해 포함된다.

[0193] SSD 공유를 사용한 초기 등록

[0194] 도7은 본 실시예에 따른 SSD 공유에 대해 변경된 초기 등록 개요를 도시한다. 도7에 도시된 정보 흐름은 단계(619)까지 도3a 및 3b의 흐름도에 도시된 정보 흐름과 유사하다.

[0195] 단계(601)에서, 초기 등록 개요는 MS가 등록 시스템 액세스를 실행할 때 시작한다.

[0196] 단계(602)에서, ANSI-41 MSC/VLR은 GGG의 HLR(GSM1x MS에 대한 HLR)에 대해 Authentication Request(IS_AUTHREQ)를 호출한다. 이러한 AUTHREQ에서의 상대적인 파라미터는 MIN, ESN 및 COUNT이다. GGG는 ESN의 값을 저장하고 COUNT 값을 데이터 베이스에서의 값과 비교한다.

[0197] 단계(603)에서, GGG는 대응하는 GSM IMSI를 얻기 위해 데이터 베이스에서 MIN을 찾고 GSM HLR/AuC에 대해 MAP_SEND_AUTHENTICATION_INFO를 호출한다.

[0198] 단계(604)에서, GGG는 성공적인 인증을 나타내는 MSC/VLR에 대해 Authentication Request Return Result(IS41_autherq)를 호출하고 타이머(TREG)를 시작한다.

[0199] 단계(605)에서, 성공적인 인증을 나타내는 IS41_authreq를 수신할 때, MSC/VLR은 GGG의 HLR에 대해 Registration Notification(IS41_REGNOT)를 호출한다.

[0200] 단계(606)에서, (본 시나리오에서와 같이) TREG가 종료하기 전에 GGG가 IS41_REGNOT를 수신한 경우, 프로파일 매크로 인증 SMS만을 가진 Registration Notification Return Result(IS41_regnot)로 응답한다. SMS는 이하와 같이 특정된다.

[0201] SMS_Origination="모두 허락"

[0202] SMS_TerminationRestriction="모두 허락"

[0203] OriginationIndicator="단일 가입자 번호"(예를 들어, 안내를 실행)

[0204] 단계(607)에서, IS41_regnot를 수신한 때, MSC/VLR은 MS로 등록 접수를 전송한다.

[0205] 단계(608)에서, GGG는 하나 이상의 인증 트리플렛을 포함하는 GSM HLR/AuC로부터 MAP_send_authentication_info를 수신한다.

[0206] 단계(609)에서, GGG가 성공적으로 IS41_regnot를 MSC/VLR(6)으로 전송하고 GSM HLR/AuC(8)로부터 MAP_send_authentication_info를 수신한 후, IS41_SMDPP 전송을 사용하여 GSM1x 인증 요구(GSM1x Auth Req) 메시지를 전송한다.

[0207] 단계(610)에서, MSC는 이러한 SMS를 MS로 전달한다.

[0208] 단계(611)에서, MS는 GSM 인증 방법을 사용하여 SRES 및 Kc를 계산하고, IS-637 SMS 전송을 사용하여 응답(GSM1x Auth Rsp)를 전송함으로써 GSM1x 인증 요구에 응답한다.

[0209] 단계(612)에서, MSC는 GGG로 SMS를 전달하고, GGG는 GSM1x Auth Rsp가 GSM HLR/AuC로부터 수신된 값과 매치함을 확인한다.

[0210] 단계(613)에서, GGG는 MS의 위치를 업데이트 하기 위해 GSM HLR에 대해 MAP_UPDATE_LOC를 호출한다.

[0211] 단계(614)에서, GSM HLR은 가입자 프로파일을 전송하기 위해 GGG에서 GSM VLR에 대해 MAP_INSERT_SUB_DATA를 호출한다.

[0212] 단계(615)에서, GGG는 ANSI-41 가입자 프로파일에 대해 GSM 가입자 프로파일을 맵핑하고 자격부여 지시(Qualification Directive)(IS41_QUALDIR)를 호출함으로써 상기 ANSI-41 프로파일을 MSC/VLR로 전송한다.

[0213] 단계(616)에서, MSC/VLR은 단계(615)의 Qualification Directive에 응답한다.

[0214] 단계(617)에서, GGG는 단계(614)의 MAP_INSERT_SUB_DATA에 응답한다.

[0215] 단계(618)에서, GMS HLR은 단계(613)의 MAP_UPDATE_LOC에 응답한다.

[0216] 단계(619)에서, MS에 의한 다음 시스템 액세스시에, 다음과 같은 단계들이 실행된다.

[0217] 단계(620)에서, MSC/VLR VLR은 GGG쪽으로 인증 요구(IS41_AUTHREQ)을 호출한다.

[0218] 단계(621)에서, GGG의 AC는 이전 단계에서 수신된 파라미터들 및 상기 MS을 위하여 저장된 Kc(SSD-A)의 값이 주어질때 ANSI-41 인증을 실행한다. 그 다음에, AC는 성공적인 ANSI-41 인증을 지시하기 위하여 MSC/VLR쪽으로 인증 요구 리턴 결과(IS-41_authreq)를 호출한다. SSD 파라미터는 또한 SSD와 MSC/VLR을 공유하도록 포함된다.

[0219] SSD 공유시 새로운 MSC/VLR에서의 등록

[0220] 도 8은 SSD 공유가 실시예에 따라 허용될때 새로운 MSC/VLR으로의 성공적인 등록을 위한 정보 흐름을 도시한다.

[0221] 단계(715)에서, MS에 의한 다음 시스템 액세스시에, 다음과 같은 단계들이 수행된다.

[0222] 단계(716)에서, MSC/VLR VLR은 GGG쪽으로 인증 요구(IS41_AUTHREQ)를 호출한다.

[0223] 단계(717)에서, GGG의 AC는 이전 단계에서 수신되고 상기 MS를 위하여 저장된 Kc(SSD-A)의 값이 주어질 때 ANSI-41 인증을 실행한다. 그 다음에, AC는 성공적인 ANSI-41 인증을 지시할때 MSC/VLR쪽으로 인증 요구 리턴 결과(IS41_authreq)를 호출한다. SSD 파라미터는 또한 SSD와 MSC/VLR을 공유하도록 포함된다.

[0224] 암호화

[0225] GSM 암호화는 성공적인 GSM 인증에 기초한다. 인증을 위하여 MSN에 의하여 MS에 전송된 RAND 값은 GSM Kc의 생성시에 사용된다. RAND 값은 Kc 값을 생성하기 위하여 SIM에 전송된다. 일 실시예에서, 공지된 GSM(A8) 알고리즘이 Kc 값을 생성하기 위하여 사용된다. SIM은 GSM 네트워크에서 (A8을 사용하여) 벌크 암호화를 위하여 Kc를 MS에 리턴시킨다. A3 및 A8은 인증 및 키 생성 함수들이다.

[0226] 인증 절차의 개요

[0227] 도 9는 일 실시예에 따라 GSM 이동국에 대한 인증 절차에 대한 개요를 도시한다. 도 9는 GSM 이동국에 의하여 사용되는 인증절차의 개요이다.

[0228] MSN(902)은 랜덤수 RAND를 인증 요구(904)를 MS(906)에 전송한다. RAND는 MS(906)에 의하여 GSM SIM 카드(908)에 전송된다. 도 9의 RAND는 도 4에 도시된 GSM_RAND와 동일하다.

[0229] MS(906)은 GSM SIM 카드(908)와 인터페이싱한다. 일 실시예에서, GSM SIM 카드는 제거가능하다. 선택적으로, GSM 카드는 MS(906)에 통합된다. 일 실시예에서, GSM SIM(908)은 MSN(902)에 전송되는 SRES를 계산하기 위하여 GSM 인증 알고리즘을 사용한다.

[0230] 일 실시예에서, MS(906)는 GSM 인증 방법을 사용하여 SRES 및 Kc를 계산하고 SRES를 가진 인증 응답을 MSN(902)에 전송함으로서 인증 요구(904)에 응답한다.

[0231] MSN(902)은 GSM SIM(908)로부터 MSN(902)로 리턴된 SRES을 검증한다. MSN은 GSM SIM 카드(908)에 의하여 리턴된 SRES가 GSM AuC(도시안됨)에 의하여 MSN에 제공된 SRES와 매칭되는지를 검사한다.

[0232] 키 생성

[0233] 도 10은 GSM 네트워크에서 GSM MS를 사용한 GSM 키 생성을 기술한다. 도 11은 CDMA 네트워크에서 CDMA MS를 사용하는 CDMA 키 생성을 기술한다.

[0234] 일 실시예에 따르면, 시스템은 CDMA RNA과 GSM 코어 네트워크를 끊김없이 통합한다. 이는 CDMA RAN을 GMS 코어 네트워크에 연결하는 GSM MSN을 사용하여 달성된다. 암호화 설계는 GSM 및 CDMA 키 생성 알고리즘들을 결합한다. 일 실시예에서, 시스템은 음성 트래픽을 스크램블링 하기 위해 PLC와 같은 확산 스펙트럼을 사용한다. 일 실시예에서, GSM 키 생성은 A5/1, 즉 암호화 알고리즘을 사용한다. 일 실시예에서, GSM 키 생성은 A5/2를 사용한다.

[0235] 일 실시예에서, 시스템은 GSM 네트워크에 가입된 가진 이동국, 즉 GSM 네트워크로부터의 Ki로 액세스하는 이동국이 CDMA 네트워크에서 로밍될 수 있고 GSM 가입에 따라 인증되며, 이동국에 의하여 전송 및 수신된 메시지들은 암호화될 수 있도록 도 11의 CDMA 키 생성과 도 10의 GSM 키 생성을 결합시킨다. 따라서, GSM SIM을 가진 이동국은 CDMA 네트워크에 끊김없이 동작한다.

[0236] 일 실시예에 따르면, 도 10은 GSM 인증 및 프라이버시를 위하여 사용되는 GSM 키 생성 프로세스를 기술한다. 도 10은 GSM 환경에서 GSM 인증 및 암호화가 수행되는 방법을 한정한다.

[0237] RAND(1002) 및 Ki(1004)는 두 개의 알고리즘들, 즉 A3(1006) 및 A8(1008)에 입력된다. 이들 두개의 엘리먼트들은 두 개의 다른 엘리먼트들, SRES(1010) 및 Kc(1012)를 생성한다. SRES(1010)는 인증 파라미터이다. 인증 프로세스동안, 네트워크는 SRES를 가진 응답을 획득하고 SIM 또는 인증 중심으로 리턴한다. 네트워크는 SRES에 기초하여 이동국을 인증한다.

[0238] GSM 프라이버시는 음성 패킷들의 암호화를 의미한다. 음성 트래픽(1014)으로부터, 획득된 모든 음성 프레임은 다른 장치들이 음성 프레임들을 디코딩하는 것을 방지하도록 암호화된다. 다른 장치들은 그들이 Kc에 대하여 액세스하지 않기 때문에 음성 프레임들을 디코딩할 수 없다.

[0239] A8(1008)은 암호화 키인 Kc를 발생시킨다. Kc는 음성 암호화를 수행하기 위하여 사용된다. 음성 인코딩동안 다수의 비트들을 제공하는 Kc 및 음성 트래픽 엘리먼트(1014)는 알고리즘들 A5/1 또는 A5/2(1016)을 사용하여 함께 결합된다. A5/1 또는 A5/2 알고리즘들(1016)은 GSM 프라이버시에 대한 GSM 암호화를 인에이블한다.

[0240] 도 11은 본 발명에 따른 CDMA 키 생성을 나타낸다.

[0241] CDMA 인증 프로세스가 턴 오프된다. 그러나 GSM MSN 및 MS는 음성 프라이버시(VP)용 음성 프라이버시 마스크(VPM)를 생성하게 된다. GSM MS 및 MSN은 시그널링 프라이버시를 위한 강화된 셀룰러 메시지 암호화 알고리즘(ECMEA) 키를 생성하게 된다.

[0242] MSN 및 MS는 VP용 VPM 및 시그널링 프라이버시를 위한 ECMEA를 계산하기 위한 프로세스로 다음의 엘리먼트들을 대체하게 된다.

[0243] SSD-A는 Kc로 대체된다.

[0244] SSD-B는 Kc로 대체된다.

[0245] ESN은 IMSI로 대체된다.

[0246] 네트워크와 이동국 모두 A-키(1102)를 가지며, 네트워크로 결코 전송되지 않는다. ESN(1104), A-키(1102) 및 RAND(1106)는 CAVE 알고리즘(1108)에 입력된다. 도 11의 이 RAND(1106)는 도 4의 RAND와 동일하다. CAVE 알고리즘(1108)은 SSD(1110)를 생성한다. SSD(1110)은 128비트이며, 이는 두 부분, SSD-A(1112) 및 SSD-B(1114)로 분할된다. SSD-A(1112) 및 SSD-B(1114)는 CAVE 알고리즘(1116, 1118)의 2개의 다른 단계에 입력된다. 단계(1116)들 중 하나는 인증 정보 AUTHR(1120)를 계산하는데 사용된다. 인증 비트들은 액세스마다 전송되는 비트들의 시퀀스이므로, 네트워크는 공유된 비밀 데이터 SSD를 갖는 이동국을 제외하고 다른 장치들이 인증 AUTHR을 생성할 수 없었다고 판단할 수 있다. 이것이 네트워크가 이동국이 인증되는지 여부를 결정할 수 있는 방법이다. 마찬가지로, 네트워크는 항상 RAND를 전송하여, 이동국이 네트워크를 결정할 수 있게 한다. 인증의 중요성은 네트워크가 정확한 이동국과 확실히 통신할 수 있게 한다는 점이다.

[0247] SSD-B(1114)는 CAVE 알고리즘(1118)의 다른 인스턴트로 진행한다. CAVE 알고리즘(1118)에 대한 다른 입력은 ESN(1114), MIN이나 최종 다이얼 번호(1122)와 같은 인증 데이터, 및 SSD-A를 이용하여 실행된 CAVE 알고리즘(1116)의 출력을 포함한다. CAVE 알고리즘(1118)은 이러한 입력을 처리하여 VPMASK(1124) 및 CMEA 키(1126)를 생성한다. VPMASK 및 CMEA 키는 CDMA 패킷을 암호화하는데 사용된다. Kc로 제공된 GSM 키 생성 및 Kc를 이용하여 실행된 알고리즘 A5/1 및 A5/2와 같이, CDMA 키 생성은 SSD-B를 제공하고, CAVE 알고리즘은 SSD-B를 이용하여 실행된다. 두 경우 모두, 암호화를 위해 암호가 생성된다.

[0248] 일 실시예에서, 시스템은 도 10의 GSM 키 생성과 도 11의 CDMA 키 생성을 조합한다. 도 1에서와 같이 GSM SIM을 구비한 이동국에 랜덤 수가 전송되고 이동국은 Kc를 생성한다. 이후 Kc는 도 11의 CDMA 키 생성에서 SSD-A 및 SSD-B에 대체된다. 그리고 이동국은 도 11의 CDMA 키 생성에 나타낸 바와 같이 정확하게 수행한다.

[0249] 따라서 동작의 하이브리드 모드, 즉 CDMA 네트워크에서 로밍하는 GSM SIM을 구비한 이동국에서, 이동국은 랜덤 수를 이용하여 Kc 및 SRES를 생성한다. Kc가 생성되면, SSD-A 및 SSD-B에 대해 Kc가 치환되고, 이는 네트

워크와 이동국 모두 유효 인증 데이터 & 암호화를 갖게 한다.

[0250] 등록시 메시지 흐름

[0251] 도 12-14는 하이브리드 인증 모드, 즉 CDMA 네트워크에서 로밍하는 GSM SIM을 구비한 이동국에 대해 일 실시예에 따른 메시지 흐름을 나타낸다. MSN은 CDMA 네트워크에서 MSC와 동일한 레벨이다. 다른 실시예에서, GGG를 구비한 네트워크에서 동일한 처리가 이어진다. GGG 구조에서 네트워크는 MSN 대신 CDMA MSC를 구비하고 네트워크는 도 6-8에 나타낸 바와 같이 GGG를 포함한다.

[0252] 도 12는 실시예에 따른 등록시 메시지 흐름을 나타낸다. 도 12는 이동국이 인증되는 처음의 메시지 흐름을 설명한다.

[0253] 도 12는 이동국이 스위치 온 되었다고 가정한다. 이동국은 등록 메시지(1202)를 전송하며, 이 메시지는 위치 업데이트 요청(1204)의 일부로서 MSN에 전송된다. 등록 메시지는 BTS/BSC와 MSN 사이의 인터페이스의 위치 업데이트 요청으로 전환된다. BTS/BSC와 MSN 사이의 인터페이스는 A-인터페이스라 하며, 이는 CDMA2000 표준으로 정의된다.

[0254] MSN에 의해 위치 업데이트 요청이 수신된 후, MSN은 MAP_SEND_AUTHENTICATION Info(1206)를 GSM HLR/AuC(1206)에 전송한다. MSN은 MAP_SEND_AUTHENTICATION Info(1206)를 GSM HLR/AuC(1206)에 전송하여 이동국에 대한 인증 정보를 얻는다. MSN은 GSM HLR/AuC로부터의 MAP_SEND AUTHENTICATION 응답(1200)의 요청에 따라 SRES, 랜덤 수, Kc 및 다른 인증 파라미터들을 획득한다. 이어지는 인증을 위해, MSN은 다른 인증 파라미터들을 획득할 수 있다.

[0255] 3 세트(SRES, 랜덤 수 및 Kc)가 MSN에 저장된다. MSN은 BTS/BSC에 GSM 인증 요청(1210)을 전송한다. SMS는 상술한 바와 같이 랜덤 수를 캡슐화하는데 사용된다. 랜덤 수는 데이터 버스트 메시지 Auth Request DataBurst(1212)를 통해 이동국으로 전달된다. 이동국은 Auth Response DataBurst(1214)에 의해 Auth Request DataBurst(1212)에 응답한다.

[0256] 이동국에 의해 랜덤 수가 SIM에 전송된다. SIM은 SRES를 리턴하고 Kc를 계산한다. SRES는 인증 응답(1216)으로 MSN으로 다시 리턴된다. MSN은 AuC로부터 수신된 SRES를 이동국이 전송한 SRES와 비교할 수 있고, 두 SRES가 매치하면, MSN은 이동국이 인증된 것으로 판단하고 이동국이 인증된다.

[0257] MSN은 업데이트 위치 요청(1218)으로 GSM HLR을 업데이트한다. GSM HLR은 업데이트 위치 응답(1220)으로 업데이트 위치 요청(1218)에 응답한다. 업데이트 위치 응답(1220)을 수신한 후, MSN은 BTS/BSC에 위치 업데이트 수락(1222)을 전송한다. BTS/BSC는 이동국에 등록 수락 명령을 이동국에 전송하고 이동국에는 GSM 네트워크 사용이 허가된다.

[0258] 도 12의 메시지 흐름 마지막에, 이동국은 Kc를 갖고, 이 Kc는 AuC가 MSN에 전송한 Kc와 동일하다. MSN 및 이동국이 동일한 Kc를 가지면, 둘 다 암호화 준비가 된다. 도 13 및 14는 암호화를 가능하게 하는 호출 흐름이다.

[0259] 일 실시예에서, 최적 프라이버시를 제공하기 위한 등록 직후 GSM 인증이 수행된다. 일 실시예에서, MS가 GSM 인증 프로세스를 통과한 후 모바일 착신(MT) 호출에 대한 페이지 응답, 또는 모바일 발신(MO) 호출에 대한 발신 메시지로 음성 및 시그널링 프라이버시가 요청된다.

[0260] 다음 두가지 경우들은 전화기의 전원이 온되고 호출이 수행되거나 등록이 종료되기 전에 수신되는 경우에 존재한다.

[0261] 이동 발신된 호출 동안 메시지 흐름

[0262] 도 13은 일 실시예에 따른 MO 호출 동안 메시지 흐름을 도시한다. MSN은 ENCRYPTION_INFORMATION 필드의 PRIVACY_MODE_REQUEST 메시지에서의 호출 설정 동안 VPM 및 ECMEA KEY 키를 BTS에 전송할 수 있다.

[0263] 도 13은 두개의 부분들로 분할될 수 있다. 상기 부분에서 인증 절차는 CDMA 호출 설정이다. 이동국은 발신(1302)을 전송하고 BTS/BSC는 BTS/BSC가 발신 메시지를 수신하였는지를 표시하는 확인응답 명령(1304)을 전송한다. 확인응답 명령(1304)은 발신 메시지가 신뢰성있게 전송될 수 없는 경우에 필요하다.

[0264] BTS/BSC는 호출을 설정하기 위해 MSN(1306)에 CM_Service_Request를 전송한다. 상기 요구의 결과로서, 이동국에 할당된 채널을 획득하기 위해 BTS/BSC에 할당 요구(1308)을 전송한다. BTS/BSC는 이동국에 CH 할당(1310)을 전송한다.

[0265] 이동국은 트래픽 채널(TCH) 프리앰블(1312)을 BTS/BSC에 전송한다. TCH 프리앰블(1312)은 이동국이 잡음을 생성하는 것을 의미한다. BTS/BSC는 이동국을 청취하며, 이동국을 획득할 것을 시도한다. BTS/BSC가 이동국을 획득하자마자, BTS/BSC는 순방향(FW) Ack 명령(1314)을 이동국에 전송한다. FW Ack 명령(1314)은 BTS/BSC에 TCH 프리앰블(1312)을 수신할 것을 지시한다.

[0266] 서비스 접속(1316)은 BTS/BSC로부터 이동국으로 전송된다. BTS/BSC으로부터의 서비스 접속은 이동국에 이동국이 현재 서비스중이거나 서비스 준비중일 것을 지시한다. 이동국은 서비스 접속 종료(1318)를 사용하여 BTS/BSC에 서비스 접속을 확인응답하고, 그후에 BTS/BSC로부터 MSN으로 할당 종료(1320)를 전송한다. 상기 시점에서, MSN은 이동국으로의 트래픽 채널을 갖는다.

[0267] IAM(1322) 및 ACM(1324)은 PSTN과 다른측에 링크를 형성하여 전화기 네트워크에 SS7 시그널링한다. 이동국은 호출을 수행한다. IAM 메시지는 호출된 디바이스가 "벨을 울리도록"한다. ACM은 SS7 호출 설정의 종료이다.

[0268] 트래픽 채널이 형성된 후에, GSM 인증 절차가 선택적으로 수행될 수 있다. 선택적인 GSM 인증 절차는 오버헤드 채널들 또는 트래픽 채널들에서 계속될 수 있다. 이동국 발신 호출에 대하여, MSN은 인증 절차를 수행할 것인지에 대하여 선택적으로 결정할 수 있다. 그러나, MSN이 인증 절차를 수행하지 않는다 할지라도, 이동국이 생성한 최종 Kc는 MSN Kc와 동일한 Kc이다. Kc는 GSM 인증 절차가 수행될 때만 변경된다.

[0269] 사용자가 호출의 다른 종료에 응답할 때, PSTN은 ANM(1326)을 MSN으로 전송한다. ANM(1326)은 호출된 디바이스가 선택된 SS7 시그널링 마다의 응답 메시지이다. 사용자가 호출의 다른 종료에 응답한 후에, MSN은 프라이버시 모드(1328)로 돌아가도록 결정될 수 있고, 상기 프라이버시 모드(1328)는 BTS/BSC에 암호화를 시작할 것을 지시하고 프라이버시 모드 메시지에서 계산된 롱 코드 마스크임을 표시한다. MSN은 BTS가 VPM 마스크 및 CMREA 키를 사용하는 것을 표시하고 상기 키들을 프라이버시 모드 메시지내에서 전송한다.

[0270] VPM 마스크 및 CMEA 키는 CDMA2000 표준에서 설명되는 것과 같이 사용된다. 그들은 음성 패킷들을 암호화하기 위해 사용된다. 프라이버시 모드 메시지(1328)에서, MSN은 이동국에 암호화를 시작할 것을 지시하고 이동국은 요구 프라이버시 롱코드 전송 응답(1332)을 가지는 응답들을 확인한다.

[0271] BTS/BSC는 MS에 요구 프라이버시 롱코드 전송 명령(1330)을 전송하고, 이동국은 요구 프라이버시 롱코드 전송 응답(1332)으로 응답한다.

[0272] 요구 프라이버시 롱코드 전송 응답(1332)을 수신한 후에, BTS/BSC는 MSN에 프라이버시 모드 종료(1334)를 전송한다. 프라이버시 모드가 종료된 후에, 이동국들은 음성 프레임들이 암호화되는 것을 의미하는 스크램블된 통화 상태에 있다.

[0273] 이동 종료된 호출 동안 메시지 흐름

[0274] 도 14는 일 실시예에 따라 모바일 착신(MT) 호출 동안 메시지 흐름을 도시한다. MSN은 ENCRYPTION_INFORMATION 필드의 PRIVACY_MODE_REQUEST 메시지내의 호출 설정 동안 BTS에 VPM 및 ECMEA 키를 전송할 수 있다.

[0275] 도 14는 호출이 PSTN측에서 발신될 때 프라이버시 모드의 일 예이다. 호출은 상기 이동국을 호출하는 또다른 이동국을 수반할 수 있다. MSN 및 PSTN 사이의 메시지들은 PSTN에 발신 및 종료 메시지를 전송하기 위해 사용되는 SS7 메시지들로서 정의된다.

[0276] IAM(1402)은 호출이 이동국에서 초기화되는 것을 MSN에 지시하는 요구이다. IAM에 응답하여, MSN은 이동국을 페이징하는데, 이는 이동국이 도 12에 의해 정의된 것과 같이 이전에 등록되기 때문이다. MSN은 페이징 요구(1404)을 BTS/BSC에 전송한다. 상기 시점에서, 이동국은 이미 Kc를 갖고 있는데, 이는 이미 GSM 인증 절차를 사용하여 인증되었기 때문이다.

[0277] MSN으로부터 페이징 요구를 수신하면, BTS/BSC는 일반 메시지(1406)를 이동국에 전송한다. 이동국은 BTS/BSC로 전송된 페이지 응답(1408)으로써 페이지에 응답한다. BTS/BSC는 페이지 응답(1410)을 MSN에 전송한다. 페이지 응답(1410)이 MSN에 의해 수신되면, MSN은 이동국이 존재하며, 이미 호출을 수신하였을 인식한다. 이

후 MSN은 할당 요구(1412)을 BTS/BSC에 전송한다. 할당 요구(1412)는 BTS/BSC에 이동국에 대하여 채널을 설정할 것을 지시하고, BTS/BSC는 채널을 이동국에 할당하고, 채널 할당(1414)을 이동국에 전송한다.

[0278] 이동국은 TCH 프리앰블(1416)을 BTS/BSC에 전송한다. TCH 프리앰블(1416)은 이동국이 순방향 채널을 통해 몇몇 잡음을 형성하여 BTS/BSC가 이동국을 획득할 수 있음을 지시한다. BTS/BSC는 TCH 프리앰블을 수신한 후에 이동국에 FW Ack Order(1418)을 전송한다.

[0279] BTS/BSC가 이동국을 획득하면, 서비스 접속(1420) 및 서비스 접속 종료(1422)이 존재한다. BTS/BSC는 서비스 접속(1420)을 이동국에 전송하고, 이동국은 서비스 접속 종료(1422)를 사용하여 서비스 접속(1420)에 응답한다.

[0280] BTS/BSC는 이동국에 정보를 갖는 경보(1424)를 전송한다. 정보를 가지는 경보는 이동국이 벨을 울리는 것에 대한 요구이다. 이동국이 벨을 울리기 시작하면, 할당 종료(1426)는 BTS/BSC으로부터 MSN으로 전송된다. 할당 종료는 MSN에 이동국이 벨을 울리고 있으며, 채널이 이동국에 할당된다고 지시한다. ACM(1428)은 PSTN에 이동국이 벨을 울릴 것을 지시하도록 MSN으로부터 PSTN으로 전송된다.

[0281] 상기 시점에서, 사용자는 호출된 이동국을 픽업하고, 접속 명령(1430)은 이동국으로부터 BTS/BSC으로 전송된다. 그후에, BTS/BSC는 접속(1432)을 MSN으로 전송한다.

[0282] 접속이 형성되면, GSM 인증 절차는 선택적으로 수행될 수 있다. GSM 인증 절차를 수행하는 시점은 선택적이며, 따라서, 인증 정책은 예를 들어 매 5회의 호출들 또는 매 10호의 호출들 마다 수행되도록 지정될 수 있다. AuC는 인증 정책을 MSN에 표시하며, MSN은 상기 정책을 따를 수 있다.

[0283] 인증 절차가 수행되면, 새로운 Kc값들이 결정되며, 이는 이전에 설명된 것과 같이 동기화될 수 있다. 프라이버시 모드 요구(1434), 요구 프라이버시 롱 코드 트랜지션 명령(1436), 요구 프라이버시 롱 코드 전송 응답(1438), 프라이버시 모드 종료(1440), 및 ANM(1442)은 도 13에 도시된 것과 같이 동작한다. ANM(1442)이 MSN으로부터 PSTN으로 전송된 후에, MSN은 호출을 시작하며, 이는 스크램블 모드에서 수행된다. ANM은 이전과 같은 응답 메시지이다.

[0284] GSM 네트워크에서, 인증 센터는 GSM MSC가 인증을 수행해야할 때의 GSM MSC를 말한다. CDMA 네트워크에서, AuC가 MSC에 인증을 수행해야할 때를 표시하는 이러한 매핑은 존재하지 않는다. 그러나, 믹스된 이동국, 즉 CDMA 네트워크에서 GSM SIM 로밍을 수행하는 이동국에 대하여, GSM 인증 절차는 MSN이 상기 절차를 수행해야 할 때마다, 즉, MSN의 인증 정책들에 따라 수행될 수 있다. 따라서, MSN은 AuC에 의해 세팅된 정책들을 수행할 수 있다.

[0285] 여기에서 상세히 설명되고 도시된 것과 같은 CDMA 네트워크와 GSM 네트워크 사이의 특정 암호화는 본 발명의 전술된 목표들을 달성할 수 있지만, 이는 본 발명의 바람직한 실시예이며, 따라서 본발명에 의해 고려되는 주요 과제를 나타내고, 본 발명의 사상은 당업자에게 명백한 다른 실시들을 완전히 포함하며, 본 발명의 사상은 따라서 첨부된 청구항들이 아닌 다른 항들에 의해서는 제한되지 않는다. 단독의 엘리먼트에 대한 참조는 "하나 및 단 하나"를 의미하는 것이 아니라 "하나 이상"을 의미하도록 지정된다. 공지되었거나 이후에 당업자에게 공지될 상기 바람직한 실시예의 엘리먼트들에 대한 모든 구조적이고 기능적인 등가물들은 본 발명의 청구항들에 의해 포함되도록 지정된다. 또한, 본 발명에 의해 해결되는 것으로 고려되는 각각의 및 모든 문제를 처리하기 위한 방법 또는 디바이스는 본 발명의 청구항들에 의해 포함되어야할 필요는 없다. 따라서, 어떤 엘리먼트, 구성요소, 또는 방법 단계도 청구항에 언급된 엘리먼트, 구성요소, 또는 방법 단계들과 관련되지 않는 것으로 의도된다. 엘리먼트가 "수단"을 사용하여 언급되거나 방법 청구항의 경우에 엘리먼트가 "작용" 대신에 "단계"로서 언급되는 경우가 아니면, 여기에 개시된 어떤 청구항 엘리먼트도 35 U.S.C. §112, 6항의 조항에서 해석되지 않아야 한다.

[0286] 본 발명의 방법 단계들은 본 발명의 사상을 벗어나지 않고 상호교환될 수 있다.

도면의 간단한 설명

[0009] 도1은 본 발명의 실시예에 따른 이동 교환 노드(MSN)를 사용하는 시스템 구조에 대한 블록 다이어그램이다.

[0010] 도2는 본 발명의 실시예에 따른 CDMA 네트워크, GSM 네트워크, 범용 글로벌 게이트웨이(GGG), 및 이동국들을 포함하는 무선 통신 시스템의 블록 다이어그램이다.

[0011] 도3a 및 도3b는 비밀 공유 데이터(SSD)를 사용하지 않는 본 발명의 실시예에 따라, GSM 네트워크에의 가입을

통해 CDMA 이동국을 인증하기 위한 흐름도이다.

[0012] 도4는 인증을 발생시키는 표준 ANSI-41 방법을 보여주는 도이다.

[0013] 도5는 본 발명의 실시예에 따라 SSD-A로서 Kc를 사용함으로써 GSM 인증 적격을 사용하는 ANSI-41 네트워크에서 GSM 가입자를 인증하는 것을 보여주는 도이다.

[0014] 도6은 성공적인 SSD 갱신 과정에 대한 정보 흐름을 보여주는 도이며, 여기서 GGG는 본 발명의 실시예에 따라 서비스 MSC/VLR과 공유된 SSD를 갱신한다.

[0015] 도7은 본 발명의 실시예에 따라 SSD 공유를 위해 수정된 초기 등록 시나리오를 보여주는 도이다.

[0016] 도8은 본 발명의 실시예에 따라 SSD 공유가 허용되는 경우 새로운 MSC/VLR 을 통한 성공적인 등록을 위한 정보 흐름을 보여주는 도이다.

[0017] 도9는 본 발명의 실시예에 따라 GSM 이동국에 대한 인증 절차에 대한 개요를 보여주는 도이다.

[0018] 도10은 GSM 네트워크에서 GSM MS를 통한 GSM 키 발생을 보여주는 도이다.

[0019] 도11은 CDMA 네트워크에서 CDMA MS를 통한 CDMA 키 발생을 보여주는 도이다.

[0020] 도12는 본 발명의 실시예에 따른 등록 기간동안 메시지 흐름을 보여주는 도이다.

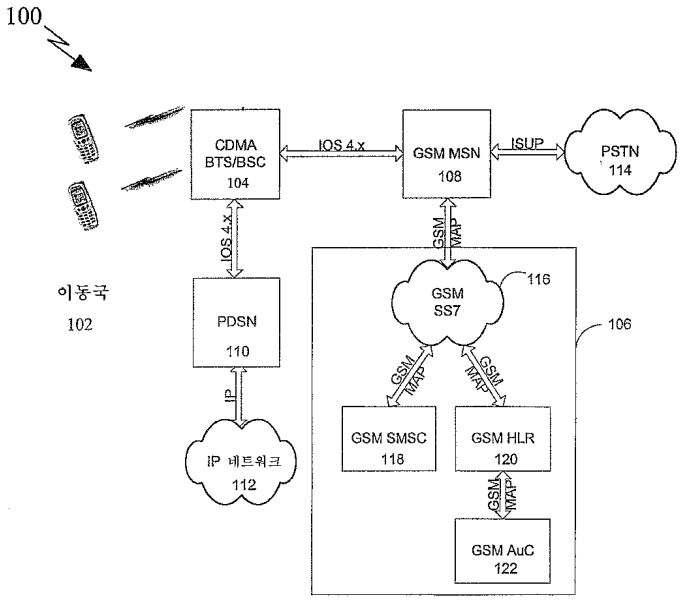
[0021] 도13은 본 발명의 실시예에 따른 이동국 발신(MO) 호출 기간동안의 메시지 흐름을 보여주는 도이다.

[0022] 도14는 본 발명의 실시예에 따른 이동국 착신(MT) 호출 기간동안의 메시지 흐름을 보여주는 도이다.

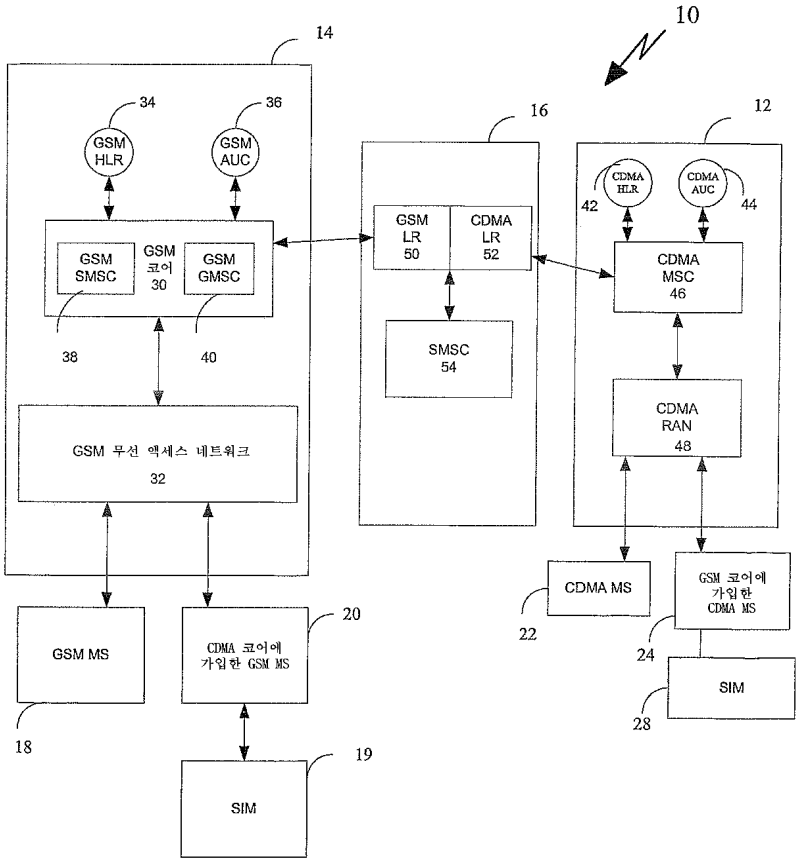
도면

도면1

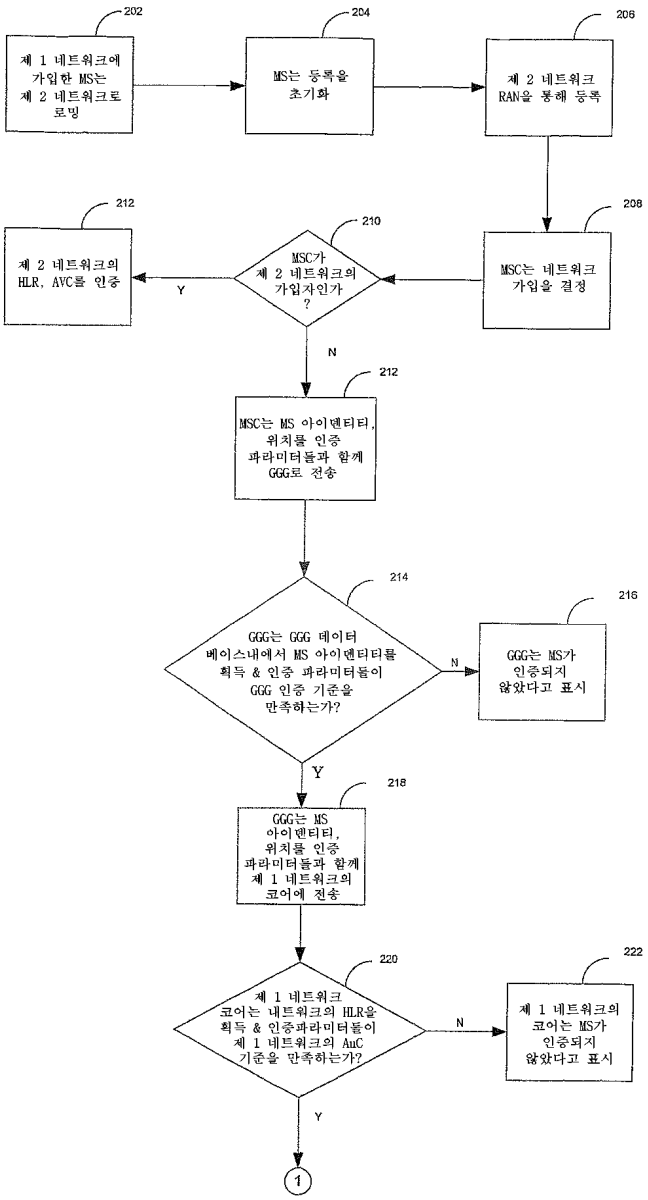
MSN을 사용하는 GSM1x 시스템 구조



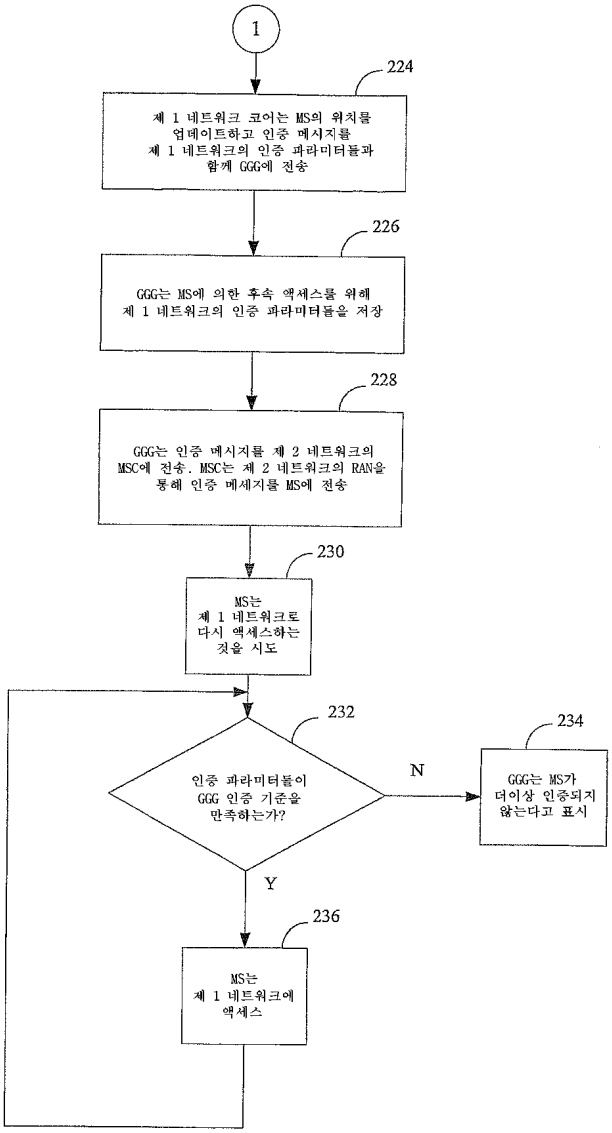
도면2


10
14
34
36
GSM HLR
GSM AUC
GSM SMSC
GSM 코어 30
GSM GMSC
38
40
GSM 무선 액세스 네트워크 32
GSM MS
18
CDMA 코어에 가입한 GSM MS
20
SIM
19
16
GSM LR 50
CDMA LR 52
SMSC 54
12
CDMA HLR
CDMA AUC
42
44
CDMA MSC 46
CDMA RAN 48
CDMA MS
22
GSM 코어에 가입한 CDMA MS
24
SIM
28

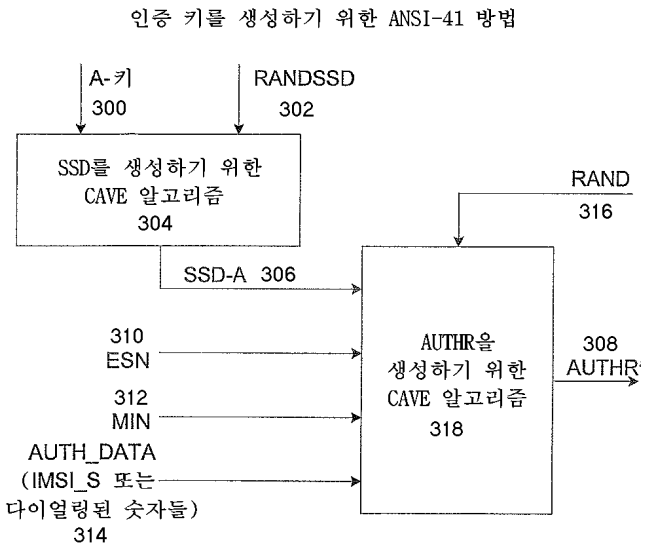
도면3a


202
제 1 네트워크에 가입한 MS는 제 2 네트워크로 로밍
204
MS는 등록을 초기화
206
제 2 네트워크 RAN을 통해 등록
208
MSC는 네트워크 가입을 결정
210
MSC가 제 2 네트워크의 가입자인가 ?
Y
212
제 2 네트워크의 HLR, AVC를 인증
N
212
MSC는 MS 아이덴티티, 위치를 인증 파라미터들과 함께 GGG로 전송
214
GGG는 GGG 데이터 베이스내에서 MS 아이덴티티를 획득 & 인증 파라미터들이 GGG 인증 기준을 만족하는가?
N
216
GGG는 MS가 인증되지 않았다고 표시
Y
218
GGG는 MS 아이덴티티, 위치를 인증 파라미터들과 함께 제 1 네트워크의 코어에 전송
220
제 1 네트워크 코어는 네트워크의 HLR을 획득 & 인증파라미터들이 제 1 네트워크의 AuC 기준을 만족하는가?
N
222
제 1 네트워크의 코어는 MS가 인증되지 않았다고 표시
Y
1

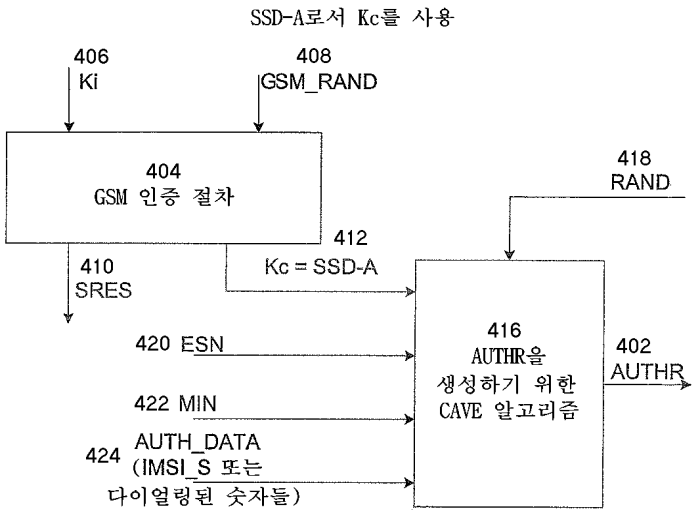
도면3b


1
224
제 1 네트워크 코어는 MS의 위치를 업데이트하고 인증 메시지를 제 1 네트워크의 인증 파라미터들과 함께 GGG에 전송
226
GGG는 MS에 의한 후속 액세스를 위해 제 1 네트워크의 인증 파라미터들을 저장
228
GGG는 인증 메시지를 제 2 네트워크의 MSC에 전송. MSC는 제 2 네트워크의 RAN을 통해 인증 메세지를 MS에 전송
230
MS는 제 1 네트워크로 다시 액세스하는 것을 시도
232
인증 파라미터들이 GGG 인증 기준을 만족하는가?
N
234
GGG는 MS가 더이상 인증되지 않는다고 표시
Y
236
MS는 제 1 네트워크에 액세스

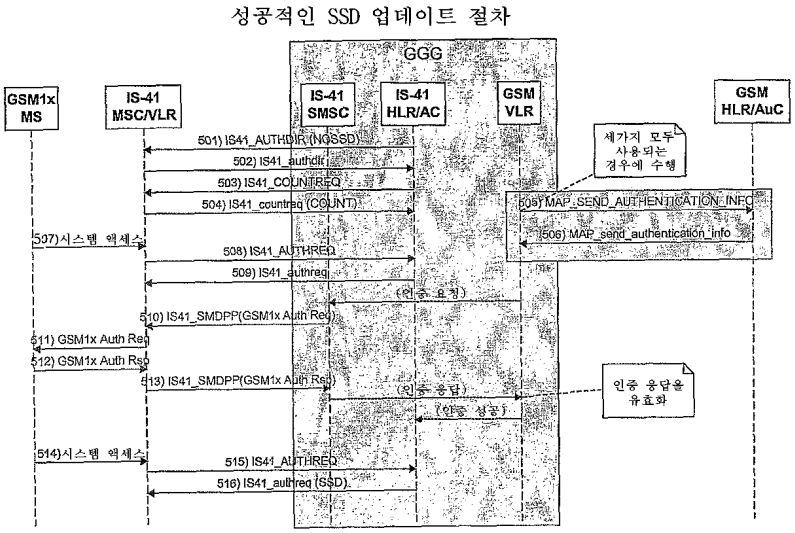
도면4


인증 키를 생성하기 위한 ANSI-41 방법
A-키
300
RANDSSD
302
SSD를 생성하기 위한
CAVE 알고리즘
304
RAND
316
SSD-A 306
310
ESN
312
MIN
AUTH_DATA
(IMSI_S 또는
다이얼링된 숫자들)
314
AUTHR을
생성하기 위한
CAVE 알고리즘
318
308
AUTHR

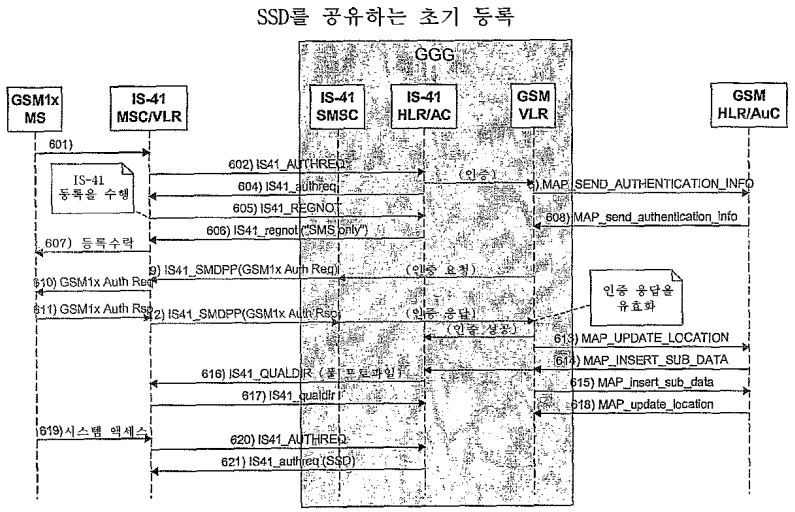
도면5


SSD-A로서 Kc를 사용
406
Ki
408
GSM_RAND
404
GSM 인증 절차
418
RAND
412
Kc = SSD-A
410
SRES
420 ESN
422 MIN
424
AUTH_DATA
(IMSI_S 또는
다이얼링된 숫자들)
416
AUTHR을
생성하기 위한
CAVE 알고리즘
402
AUTHR

도면6

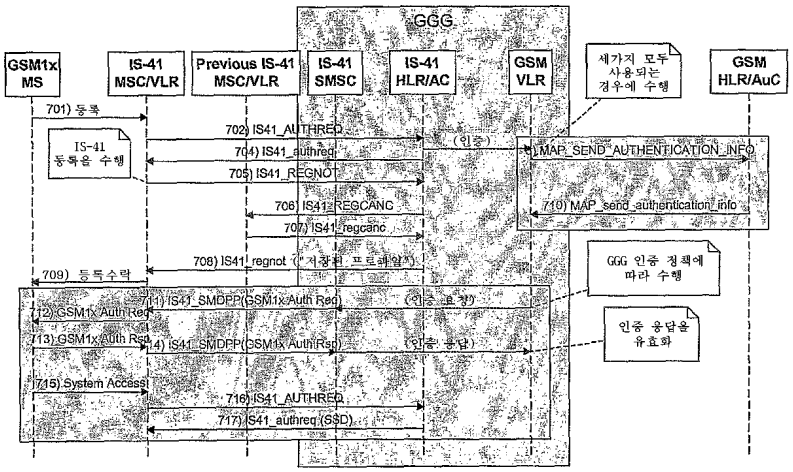

성공적인 SSD 업데이트 절차
GGG
GSM1x MS
IS-41 MSC/VLR
IS-41 SMSC
IS-41 HLR/AC
GSM VLR
GSM HLR/AuC
세가지 모두 사용되는 경우에 수행
501) IS41_AUTHDIR (NGSSD)
502) IS41_authdir
503) IS41_COUNTREQ
504) IS41_countreq (COUNT)
505) MAP_SEND_AUTHENTICATION_INFO
506) MAP_send_authentication_info
507)시스템 액세스
508) IS41_AUTHREQ
509) IS41_authreq
(인증 요청)
510) IS41_SMDPP(GSM1x Auth Req)
511) GSM1x Auth Req
512) GSM1x Auth Rsp
513) IS41_SMDPP(GSM1x Auth Rsp)
(인증 응답)
인증 응답을 유효화
(인증 성공)
514)시스템 액세스
515) IS41_AUTHREQ
516) IS41_authreq (SSD)

도면7


SSD를 공유하는 초기 등록
GGG
GSM1x MS
IS-41 MSC/VLR
IS-41 SMSC
IS-41 HLR/AC
GSM VLR
GSM HLR/AuC
601)
602) IS41_AUTHREQ
(인증)
IS-41 등록을 수행
604) IS41_authreq
MAP_SEND_AUTHENTICATION_INFO
605) IS41_REGNOT
606) MAP_send_authentication_info
606) IS41_regnot ("SMS only")
607) 등록수락
609) IS41_SMDPP(GSM1x Auth Req)
(인증 요청)
610) GSM1x Auth Req
611) GSM1x Auth Rsp
612) IS41_SMDPP(GSM1x Auth Rsp)
(인증 응답)
인증 응답을 유효화
(인증 성공)
613) MAP_UPDATE_LOCATION
614) MAP_INSERT_SUB_DATA
615) MAP_insert_sub_data
616) IS41_QUALDIR (불 프로파일)
617) IS41_qualdir
618) MAP_update_location
619)시스템 액세스
620) IS41_AUTHREQ
621) IS41_authreq (SSD)

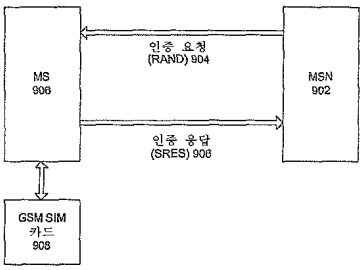
도면8

SSD를 공유하여 새로운 MSC/VLR을 성공적으로 등록

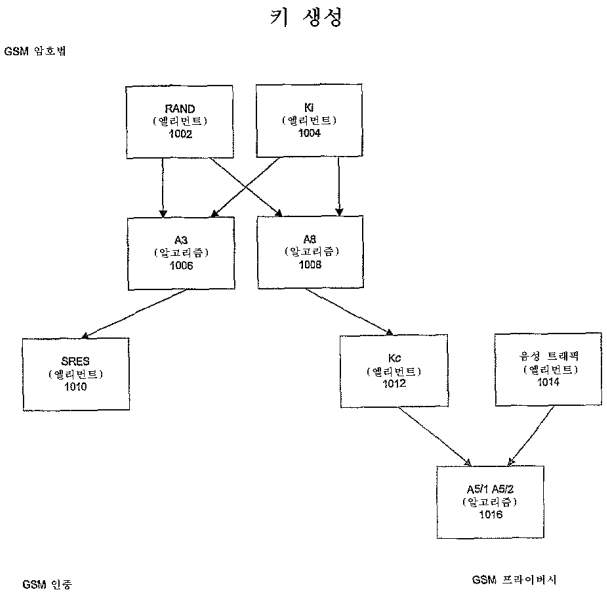


도면9

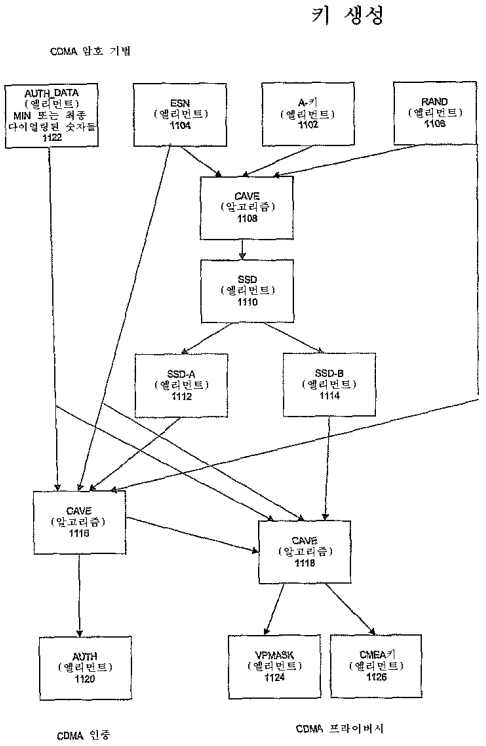
인증 절차의 개요



도면10

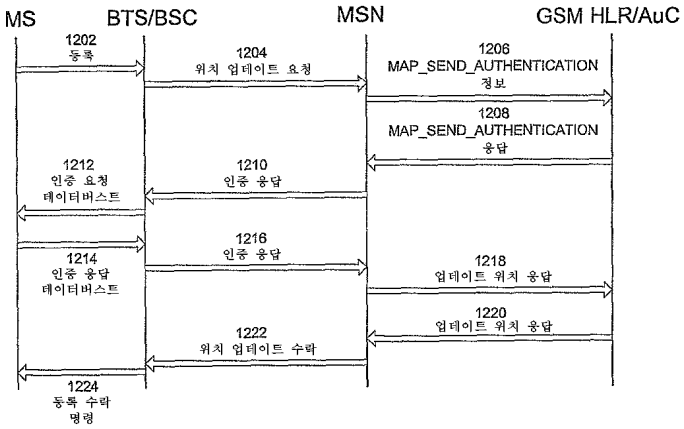

키 생성
GSM 암호법
RAND
(엘리먼트)
1002
Ki
(엘리먼트)
1004
A3
(알고리즘)
1006
A8
(알고리즘)
1008
SRES
(엘리먼트)
1010
Kc
(엘리먼트)
1012
음성 트래픽
(엘리먼트)
1014
A5/1 A5/2
(알고리즘)
1016
GSM 인증
GSM 프라이버시

도면11


키 생성
CDMA 암호 기법
AUTH_DATA
(엘리먼트)
MIN 또는 최종
다이얼링된 숫자들
1122
ESN
(엘리먼트)
1104
A-키
(엘리먼트)
1102
RAND
(엘리먼트)
1106
CAVE
(알고리즘)
1108
SSD
(엘리먼트)
1110
SSD-A
(엘리먼트)
1112
SSD-B
(엘리먼트)
1114
CAVE
(알고리즘)
1116
CAVE
(알고리즘)
1118
AUTH
(엘리먼트)
1120
VPMASK
(엘리먼트)
1124
CMEA키
(엘리먼트)
1126
CDMA 인증
CDMA 프라이버시

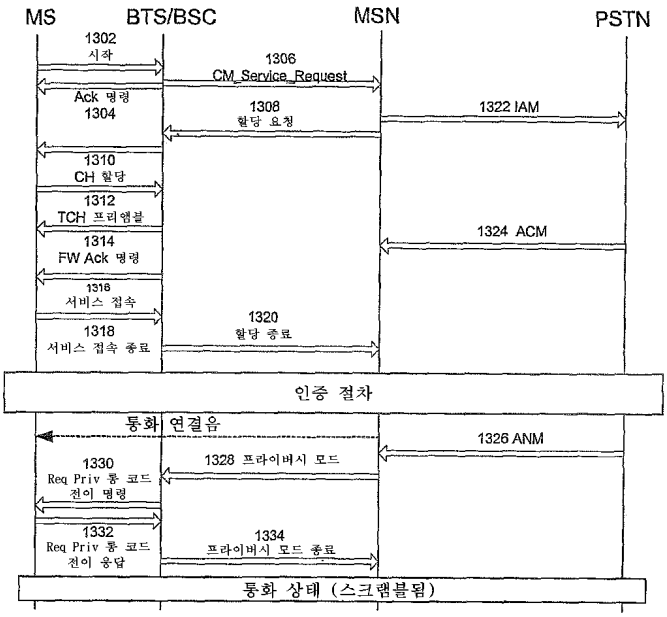
도면12

등록 동안 메세지 흐름

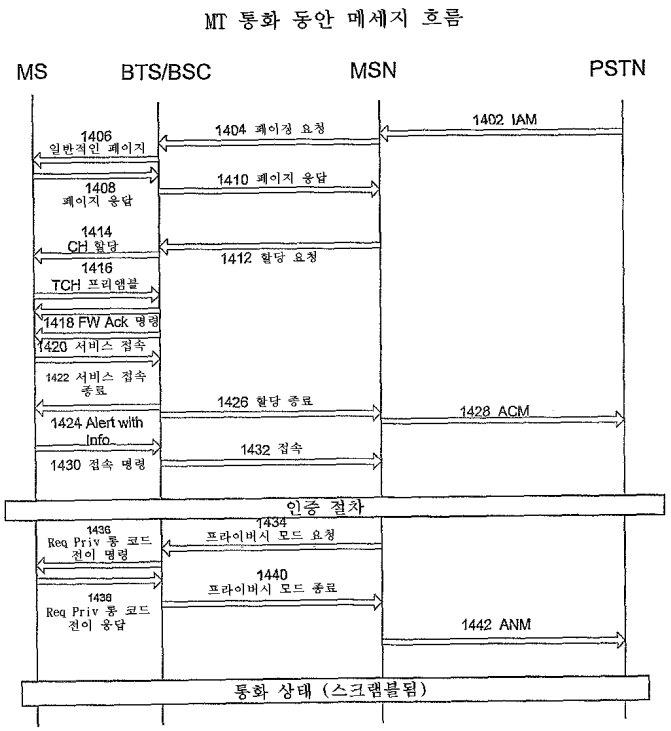


도면13

MO 통화 동안 메세지 흐름



도면14


MT 통화 동안 메세지 흐름
MS
BTS/BSC
MSN
PSTN
1406
일반적인 페이지
1404 페이징 요청
1402 IAM
1408
페이지 응답
1410 페이지 응답
1414
CH 할당
1412 할당 요청
1416
TCH 프리앰블
1418 FW Ack 명령
1420 서비스 접속
1422 서비스 접속 종료
1426 할당 종료
1428 ACM
1424 Alert with Info
1430 접속 명령
1432 접속
인증 절차
1434
프라이버시 모드 요청
1436
Req Priv 통 코드 전이 명령
1440
프라이버시 모드 종료
1438
Req Priv 통 코드 전이 응답
1442 ANM
통화 상태 (스크램블됨)