(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0116401
(43) 공개일자 2009년11월11일

(51) Int. Cl.
H04B 7/26 (2006.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2008-0042308
(22) 출원일자 2008년05월07일
심사청구일자 2009년04월30일

(71) 출원인
주식회사 케이티
경기 성남시 분당구 정자동 206
(72) 발명자
최종윤
서울 송파구 신천동 7-18
강유진
서울 강남구 일원동 718번지 샘터마을아파트 107동 1301호
(74) 대리인
유미특허법인

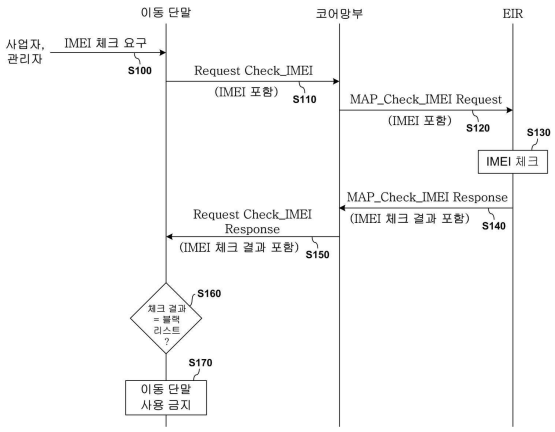
전체 청구항 수 : 총 18 항

(54) 이동 단말 인증 방법과, 그 방법을 수행하는 이동 단말 및코어망 장치

(57) 요 약

본 발명은 이동 단말 인증 방법과, 그 방법을 수행하는 이동 단말 및 코어망 장치에 관한 것이다. 이동 단말이 외부로부터 IMEI 체크를 통한 인증 요구를 받으면, 코어망 장치로 IMEI 체크를 수행하는 인증 요청을 송신한다. 코어망 장치는 IMEI 체크를 수행하는 인증 요청을 수신하여 EIR로 요구하고, EIR로부터 IMEI 체크 결과를 수신한다. IMEI 체크의 결과는 화이트, 블랙, 그레이 중 어느 하나의 정보이다. 코어망 장치는 EIR로부터 수신한 IMEI 체크 결과를 이동 단말로 송신한다. 이동 단말은 코어망 장치로부터 수신된 IMEI 체크 결과에 따라 이동 단말의 사용을 제한한다. IMEI 체크 결과가 블랙인 경우, 이동 단말의 사용을 제한한다. 본 발명에 따르면, 이동 단말이 능동적으로 코어망 장치에 이동 단말의 사용 가능 여부의 판단을 요청함으로써, 이동 통신망의 부하가 줄어 망 전체의 안정성이 높아진다. 또한, 망 자원이 절약되어 이동 통신망에 대한 투자비가 감소된다.

대 표 도 - 도4



특허청구의 범위

청구항 1

이동 단말에서 식별번호를 이용하여 이동 단말을 인증하는 방법에 있어서,

a) 식별번호-여기서 식별번호는 상기 이동 단말을 식별하기 위한 상기 이동 단말에 고유한 식별번호임-를 이용한 인증 요구를 수신하는 단계;

b) 상기 인증 요구에 따라 상기 식별번호를 포함하는 인증 요청을 이동 통신 시스템의 코어망으로 송신하는 단계; 및

c) 상기 코어망으로부터 상기 인증 요청에 대한 결과를 수신하고, 상기 결과에 따라 상기 이동 단말의 사용을 제한하는 단계

를 포함하는 인증 방법.

청구항 2

제1항에 있어서,

상기 a) 단계에서,

상기 인증 요구가 페이징, 문자 메시지 또는 OTA(Over The Air) 데이터 중 하나를 통해 수신되는 인증 방법.

청구항 3

제1항에 있어서,

상기 c) 단계에서,

상기 인증 요청에 대한 결과에는 상기 이동 단말의 식별번호가 불법 단말인 지의 여부를 알 수 있는 정보가 포함되는 인증 방법.

청구항 4

제3항에 있어서,

상기 인증 요청에 대한 결과는 화이트, 블랙 또는 그레이 중 어느 하나인 인증 방법.

청구항 5

제4항에 있어서,

상기 c) 단계에서,

상기 이동 단말은 상기 인증 요청에 대한 결과가 블랙인 경우, 상기 이동 단말의 사용을 제한하는 인증 방법.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서,

상기 a) 단계에서,

상기 인증 요구는 상기 이동 단말에서 망설정시에 기존에 설정된 이동 통신망이 아닌 다른 이동 통신망으로 설정되는 것으로 판단되는 경우에 수신되는 인증 방법.

청구항 7

제1항 내지 제5항 중 어느 한 항에 있어서,

상기 이동 단말의 식별번호는 IMEI(International Mobile station Equipment Identity) 또는 IMEISV(IMEI and Software Version number)인 인증 방법.

청구항 8

이동 단말에 대한 이동 통신 서비스를 제공하는 이동 통신 시스템의 코어망에서 상기 이동 단말을 인증하는 방법에 있어서,

a) 상기 이동 단말로부터 상기 이동 단말의 식별번호-여기서 식별번호는 상기 이동 단말을 식별하기 위한 상기 이동 단말에 고유한 식별번호임-를 이용한 인증 요청을 수신하는 단계;

b) 상기 인증 요구에 따라 상기 식별번호를 포함하는 인증 요청을 EIR(Equipment Identity Register)로 송신하는 단계; 및

c) 상기 EIR로부터 상기 인증 요청에 대한 결과를 수신하고, 상기 결과를 상기 a) 단계에서 수신된 인증 요청에 대한 응답으로 상기 이동 단말로 송신하는 단계

를 포함하는 인증 방법.

청구항 9

제8항에 있어서,

상기 b) 단계에서,

상기 EIR로 송신되는 인증 요청은 MAP(Mobile Application Part) 프로토콜 메시지를 통해 수행되는 인증 방법.

청구항 10

제8항에 있어서,

상기 c) 단계에서,

상기 인증 요청에 대한 결과는 화이트, 블랙 또는 그레이 중 어느 하나인 인증 방법.

청구항 11

식별번호를 이용하여 인증을 수행하는 이동 단말에 있어서,

상기 이동 단말에 고유한 식별번호를 이용한 인증 요구가 수신되는지를 검출하는 검출부;

상기 검출부에 의해 인증 요구가 검출되는 경우, 이동 통신 시스템의 코어망을 통해 상기 식별번호를 이용한 인증을 수행하는 인증부; 및

상기 인증부에 의해 수행된 인증의 결과에 따라 상기 이동 단말의 사용 제한을 제어하는 제어부

를 포함하는 이동 단말.

청구항 12

제11항에 있어서,

상기 검출부는 외부로부터 수신되는 페이징, 문자 메시지 또는 OTA 데이터를 분석하여 상기 인증 요구가 수신되는지를 검출하는 이동 단말.

청구항 13

제11항에 있어서,

상기 제어부는 상기 인증부에 의해 수행된 인증의 결과가 블랙인 것으로 확인되는 경우, 상기 이동 단말의 사용을 제한하는 이동 단말.

청구항 14

제11항에 있어서,

상기 인증부는 상기 인증의 결과가 그레이인 것으로 확인되면, 일정 시간이 지난 후 상기 코어망을 통한 인증을 재시도하는 이동 단말.

청구항 15

이동 단말에 대한 인증을 수행하는 이동 통신 시스템의 코어망 장치에 있어서,

상기 이동 단말로부터 식별번호를 이용한 인증 요청이 수신되는지를 검출하는 검출부; 및

상기 검출부에 의해 인증 요청이 검출되는 경우, EIR을 통해 상기 이동 단말의 식별번호를 이용한 인증을 수행하고, 수행된 상기 인증의 결과를 상기 이동 단말로 송신하는 인증 처리부

를 포함하는 코어망 장치.

청구항 16

제15항에 있어서,

상기 인증 처리부는 상기 이동 단말의 식별번호를 이용한 인증을 수행하기 위해 MAP 프로토콜 메시지를 통해 상기 EIR과 메시지를 송수신하는 코어망 장치.

청구항 17

제15항에 있어서,

상기 인증의 결과는 화이트, 블랙 또는 그레이 중 어느 하나인 코어망 장치.

청구항 18

제15항 내지 제17항 중 어느 한 항에 있어서,

상기 코어망 장치는 MSV(Mobile Switching center serVer) 또는 SGSN(Serving GPRS Supporting Node)인 코어망 장치.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 이동 단말 인증 방법에 관한 것으로, 특히 도난 단말과 같은 불법 단말의 사용을 금지시키기 위한 이동 단말 인증 방법과, 그 방법을 수행하는 이동 단말 및 코어망 장치에 관한 것이다.

배 경 기 술

<2> 최근 이동 통신망의 사용 환경은 유무선 그리고 음성 또는 데이터 통신에 상관없이 사용자들에게 신뢰성이 있는 서비스를 제공하는 것뿐만 아니라 통신을 수행하는 당사자들간에 보안 서비스를 제공하는 것을 요구하고 있다.

<3> 이러한 요구의 일환으로 이동 통신망 환경에서는 도난 단말, 복제 단말 등과 같은 불법 단말의 부적당한 사용을 방지하기 위해 이동 단말의 식별번호(International Mobile station Equipment Identity, 이하 "IMEI"라고 함)를 이용하여 이동 단말의 인증을 수행하고 있다.

<4> 일예로, 이동 통신망에서 이동 단말에 대한 정보, 특히 불법 단말 여부 정보를 관리하는 노드인 기기 식별번호 레지스터(Equipment Identity Register, 이하 "EIR"이라고 함)가 코어망의 MSC(Mobile Switching Center) 서버(이하 "MSV"라고 함)나 SGSN(Serving GPRS Supporting Node)으로부터 이동 단말의 IMEI를 받아서 해당 IMEI의 불법 단말 여부를 판단하여 전달함으로써, 코어망의 MSV나 SGSN이 불법 단말에 대한 이동 통신 서비스를 제공하지 않음으로써 불법 단말을 사용하지 못하도록 하고 있다. 이를 위해, EIR은 이동 단말의 IMEI를 서비스 등급별로 여러 리스트로 분류하여 상태 정보 및 관련 정보를 관리하며, 이러한 리스트로는 기본적으로 화이트(White) 리스트, 블랙(Black) 리스트, 그레이(Gray) 리스트를 포함한다. 여기서, 화이트 리스트는 망 내에서 서비스 이용을 인증받은 IMEI로 구성되고, 블랙 리스트는 망 내에서 서비스 이용을 인증받지 못한 IMEI나 불법 단말의 IMEI로 구성되며, 그레이 리스트는 망 운용자의 운용상의 이유 등으로 관리가 필요한 IMEI로 구성된다. 따라서, EIR을 통해 블랙 리스트에 속하는 것으로 확인되는 IMEI에 대해 코어망에서 해당 이동 단말의 사용을 금지시키게 된다.

<5> 그러나, 상기한 종래 방식에 따르면, 도난 단말 등의 불법 단말의 사용을 막기 위해 코어망에서 이동 단말이 매

번 호 시도를 할 때마다 EIR을 통한 인증을 받게 하여 불법 단말 여부를 블랙 리스트에서 확인하여야 하므로, 모든 호 시도시에 코어망을 포함한 이동 통신 네트워크에 추가로 트래픽이 발생하여 결과적으로 과도한 부하가 발생하게 되는 문제점이 있다. 이러한 부하의 증가는 이동 통신망 전체의 안정성을 저해할 수 있는 잠재적인 요소에 해당하므로 망 부하를 크게 증가시키지 않으면서 불법 단말의 사용을 금지하기 위한 다른 방안이 요구된다.

발명의 내용

해결 하고자하는 과제

<6> 본 발명이 이루고자 하는 기술적 과제는, 이동 단말이 능동적으로 코어망에 이동 단말의 사용 가능 여부의 판단을 요청함으로써 이동 통신망의 부하를 줄일 수 있는 이동 단말 인증 방법과, 그 방법을 수행하는 이동 단말 및 코어망 장치를 제공하는 것이다.

과제 해결수단

<7> 이러한 기술적 과제를 달성하기 위한 본 발명의 하나의 특징에 따른 인증 방법은,

<8> 이동 단말에서 식별번호를 이용하여 이동 단말을 인증하는 방법으로서,

<9> a) 식별번호-여기서 식별번호는 상기 이동 단말을 식별하기 위한 상기 이동 단말에 고유한 식별번호임-를 이용한 인증 요구를 수신하는 단계; b) 상기 인증 요구에 따라 상기 식별번호를 포함하는 인증 요청을 이동 통신 시스템의 코어망으로 송신하는 단계; 및 c) 상기 코어망으로부터 상기 인증 요청에 대한 결과를 수신하고, 상기 결과에 따라 상기 이동 단말의 사용을 제한하는 단계를 포함한다.

<10> 본 발명의 다른 특징에 따른 인증 방법은,

<11> 이동 단말에 대한 이동 통신 서비스를 제공하는 이동 통신 시스템의 코어망에서 상기 이동 단말을 인증하는 방법으로서,

<12> a) 상기 이동 단말로부터 상기 이동 단말의 식별번호-여기서 식별번호는 상기 이동 단말을 식별하기 위한 상기 이동 단말에 고유한 식별번호임-를 이용한 인증 요청을 수신하는 단계; b) 상기 인증 요구에 따라 상기 식별번호를 포함하는 인증 요청을 EIR(Equipment Identity Register)로 송신하는 단계; 및 c) 상기 EIR로부터 상기 인증 요청에 대한 결과를 수신하고, 상기 결과를 상기 a) 단계에서 수신된 인증 요청에 대한 응답으로 상기 이동 단말로 송신하는 단계를 포함한다.

<13> 본 발명의 또 다른 특징에 따른 이동 단말은,

<14> 식별번호를 이용하여 인증을 수행하는 이동 단말로서,

<15> 상기 이동 단말에 고유한 식별번호를 이용한 인증 요구가 수신되는지를 검출하는 검출부; 상기 검출부에 의해 인증 요구가 검출되는 경우, 이동 통신 시스템의 코어망을 통해 상기 식별번호를 이용한 인증을 수행하는 인증부; 및 상기 인증부에 의해 수행된 인증의 결과에 따라 상기 이동 단말의 사용 제한을 제어하는 제어부를 포함한다.

<16> 본 발명의 또 다른 특징에 따른 코어망 장치는,

<17> 이동 단말에 대한 인증을 수행하는 이동 통신 시스템의 코어망 장치로서,

<18> 상기 이동 단말로부터 식별번호를 이용한 인증 요청이 수신되는지를 검출하는 검출부; 및 상기 검출부에 의해 인증 요청이 검출되는 경우, EIR을 통해 상기 이동 단말의 식별번호를 이용한 인증을 수행하고, 수행된 상기 인증의 결과를 상기 이동 단말로 송신하는 인증 처리부를 포함한다.

효 과

<19> 이동 통신망의 부하가 줄어 망 전체의 안정성이 높아진다.

<20> 또한, 망 자원이 절약되어 이동 통신망에 대한 투자비가 감소된다.

발명의 실시를 위한 구체적인 내용

<21> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

<22> 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현할 수 있다.

<23> 본 명세서에서 이동 단말(Mobile Terminal, MT)은 이동국(Mobile Station, MS), 가입자국(Subscriber Station, SS), 휴대 가입자국(Portable Subscriber Station, PSS), 사용자 장치(User Equipment, UE), 접근 단말(Access Terminal, AT) 등을 지칭할 수도 있고, 이동국, 가입자국, 휴대 가입자 국, 사용자 장치 등의 전부 또는 일부의 기능을 포함할 수도 있다.

<24> 본 명세서에서 기지국(Base Station, BS)은 접근점(Access Point, AP), 무선 접근국(Radio Access Station, RAS), 노드B(Node B), 송수신 기지국(Base Transceiver Station, BTS), MMR(Mobile Multihop Relay)-BS 등을 지칭할 수도 있고, 접근점, 무선 접근국, 노드B, 송수신 기지국, MMR-BS 등의 전부 또는 일부의 기능을 포함할 수도 있다.

<25> 이제 본 발명의 실시예에 따른 이동 단말 인증 방법과, 그 방법을 수행하는 이동 단말 및 코어망 장치에 대하여 도면을 참고로 하여 상세하게 설명한다.

<26> 설명하기 전에 본 발명의 실시예에서는 도난 단말이나 복제 단말 등과 같은 불법 단말에 대한 신고가 이동 통신망의 사업자에게 접수되어 해당 불법 단말의 IMEI가 이미 EIR의 블랙 리스트에 등록되어 관리되고 있는 것으로 가정한다.

<27> 도 1은 본 발명의 실시예에 따른 이동 단말 인증 방법이 적용되는 이동 통신 시스템을 개략적으로 도시한 도면이다.

<28> 도 1에 도시된 바와 같이, 본 발명의 실시예가 적용되는 이동 통신 시스템은 코어망부(100) 및 EIR(200)을 포함한다.

<29> 코어망부(100)는 이동 단말(300)에 대한 각종의 이동 통신 서비스를 제공하며, 이동 통신망 전체에 대한 주요 제어 기능을 담당하는 부분으로서, 이동 통신의 기본 서비스 제공에 있어서 필수적인 시스템 구성요소로 구성된다. 이러한 코어망부(100)는 이동 단말(300)로부터의 통신 호에 대한 서비스를 제공하는 MSV 또는 이동 단말(300)에 대해 데이터 등 패킷 호에 대한 서비스를 제공하는 SGSN을 포함한다. 물론, 코어망부(100)가 이동 통신 서비스를 제공하기 위한 다른 구성요소를 포함하지만, 여기에서는 설명을 간결하게 하기 위해 본 발명의 실시예와 관련된 내용을 설명하는데 필요한 구성요소에 대해서만 설명한다.

<30> 코어망부(100)는 외부, 즉 코어망부(100)를 관리하는 사업자로부터 도난 단말 등의 불법 단말의 신고가 접수되면, 이동 단말(100)로 자신의 IMEI의 사용 가능 여부를 체크하게 하는 IMEI 체크(check_IMEI)를 수행할 것을 요구한다. 즉, 이동 단말(100)의 IMEI를 이용한 이동 단말의 인증을 수행하도록 요구한다. 이러한 IMEI 체크 수행의 요구는 이동 단말(300)에 다양한 방식으로 전달될 수 있다. 예를 들어, 타입을 Check_IMEI로 하는 페이징(Paging), SMS(Short Message Service) 등의 문자 메시지, OTA(Over The Air) 기술 등을 사용하여 이동 단말(300)에게 IMEI 체크 수행을 요구하는 명령을 전달할 수 있다. 이러한 IMEI 체크 수행을 요구하는 명령은 이동 통신망의 관리자, 사업자 등의 시스템으로부터 이동 단말(300)로 전달될 수 있으나, 이러한 명령이 모두 코어망부(100)를 통해 전달되므로, 본 발명의 실시예에서는 코어망부(100)로부터 이동 단말(300)로 IMEI 체크 수행의 요구가 전달되는 것으로 나타내었다.

<31> 코어망부(100)가 이동 단말(300)로부터 IMEI 체크를 요청받으면, EIR(200)을 통해 이동 단말(300)의 IMEI가 속하는 리스트의 종류, 즉 화이트, 블랙 리스트, 그레이 리스트 중 하나의 리스트 정보를 제공받아서 이동 단말(300)로 전달한다.

<32> EIR(200)은 코어망부(100)에 접속이 허가된 이동 단말을 식별하기 위해 이동 단말의 IMEI를 저장하여 관리한다. 특히, EIR(200)은 각 이동 단말의 IMEI를 화이트 리스트, 블랙 리스트 및 그레이 리스트로 분류하여 관리한다.

이 때, 불법 단말의 IMEI는 블랙 리스트로 분류되어 관리된다.

<33> EIR(200)은 코어망부(100)로부터 IMEI 체크를 요청받으면 화이트, 블랙, 그레이 중 이동 단말(300)의 IMEI가 속하는 리스트의 종류 정보를 코어망부(100)로 전달한다.

<34> 한편, 이동 단말(300)은 코어망부(100)의 IMEI 체크의 요구를 수신하여 코어망부(100)로 IMEI 체크를 요청하고, 코어망부(100)로부터 IMEI 체크의 결과, 즉 이동 단말(300)의 IMEI가 속하는 리스트의 종류 정보를 전달받는다. 만일 코어망부(100)로부터 전달받은 리스트의 종류 정보가 블랙이면, 이동 단말(300)이 불법 단말이므로 이미 잘 알려져 있는 여러 가지 방법을 사용하여 사용자가 이동 단말(300) 자신을 사용할 수 없도록 제어한다. 이하에서, IMEI 체크의 결과가 블랙이라서 이동 단말(300)의 사용을 제어하는 것은 호 시도할 때뿐만 아니라 이동 단말(300)의 재시작으로 인한 위치 등록을 수행하지 않는 것을 의미한다.

<35> 그러나, IMEI 체크 결과가 화이트나 그레이이면 이동 단말(300)은 불법 단말이 아니므로 사용자가 계속 사용할 수 있도록 그대로 현 상태를 유지한다.

<36> 도 2는 도 1에 도시된 이동 단말(300)의 상세 블록도이다.

<37> 도 2에 도시된 바와 같이, 이동 단말(300)은 신호 송수신부(310), 인증 요구 검출부(320), 단말 인증부(330) 및 단말 사용 제어부(340)를 포함한다.

<38> 신호 송수신부(310)는 코어망부(100)를 통해 이동 단말(300)이 이동 통신 서비스를 제공받을 수 있는 각종의 신호를 송수신한다. 신호 송수신부(310)와 코어망부(100)가 기지국(미도시) 등을 통해 무선 신호를 송수신하는 것에 대해서는 이미 잘 알려져 있으므로, 여기에서는 기지국(미도시)을 통한 신호 송수신에 대해서는 구체적인 설명을 생략한다.

<39> 인증 요구 검출부(320)는 신호 송수신부(310)를 통해 수신되는 신호를 분석하여 이동 단말(300)의 인증, 즉, 이동 단말(300)의 IMEI 체크 수행을 요구하는 페이징, 문자 메시지, OTA 데이터 등의 요구가 수신되는지를 검출한다.

<40> 단말 인증부(330)는 인증 요구 검출부(320)로부터 이동 단말(300)의 인증을 수행하라는 요구가 검출되면, 코어망부(100)를 통한 IMEI 체크를 수행한다. 즉, 단말 인증부(330)는 신호 송수신부(310)를 통해 코어망부(100)로 IMEI 체크를 요청하고, 코어망부(100)로부터 EIR(200)를 통한 IMEI 체크 결과를 수신하여 이동 단말(300)의 IMEI 체크를 통한 인증을 수행한다. 단말 인증부(330)는 코어망부(100)로부터 전달받은 IMEI 체크 결과가 블랙인 것으로 확인되면 단말 인증이 실패한 것으로 판단하고, 화이트나 그레이인 것으로 확인되면 단말 인증이 성공한 것으로 판단한다.

<41> 여기서, 단말 인증부(330)는 단말 인증을 위해 IMEI 체크를 수행하기 위해 코어망부(100)로 IMEI 체크 요청 메시지(Request Check_IMEI)를 송신하고, 코어망부(100)로부터 IMEI 체크 결과가 포함된 IMEI 체크 요청 응답 메시지(Request Check_IMEI Response)를 수신한다.

<42> 단말 사용 제어부(340)는 단말 인증부(330)에 의해 수행된 단말 인증 결과 실패한 것으로 판단되면 이동 단말(300)의 사용을 금지시키기 위한 제어를 수행한다.

<43> 도 3은 도 1에 도시된 코어망부(200)의 상세 블록도이다.

<44> 도 3에 도시된 바와 같이, 코어망부(200)는 단말측 신호 송수신부(110), EIR측 신호 송수신부(120), 인증 요청 검출부(130) 및 인증 처리부(140)를 포함한다.

<45> 단말측 신호 송수신부(110)는 이동 단말(300)에 대한 이동 통신 서비스를 제공하기 위해 이동 단말(300)과의 신호 송수신을 담당한다.

<46> EIR측 신호 송수신부(120)는 이동 단말의 IMEI를 이용하여 단말 인증을 수행하기 EIR(200)과의 신호 송수신을 담당한다.

<47> 인증 요청 검출부(130)는 단말측 신호 송수신부(110)를 통해 수신되는 신호를 분석하여 이동 단말(300)의 인증, 즉, 이동 단말(300)의 IMEI 체크를 수행하는 요청 메시지가 수신되는지를 검출한다.

<48> 인증 처리부(140)는 인증 요청 검출부(130)로부터 이동 단말(300)에 대한 IMEI 체크 요청이 검출되면, EIR(200)을 통한 IMEI 체크를 수행한다. 즉, 인증 처리부(140)는 EIR측 신호 송수신부(120)를 통해 EIR(200)로 IMEI 체크를 요청하고, EIR(200)로부터 IMEI 체크 결과를 수신하여 단말측 신호 송수신부(110)를 통해 이동 단말

(300)로 IMEI 체크 결과를 전달한다. 이러한 EIR(200)을 통한 IMEI 체크는 MAP(Mobile Application Part) 프로토콜 메시지를 통해 이루어진다. 여기서, 인증 처리부(140)는 IMEI 체크를 수행하기 위해 EIR(200)로 IMEI 체크를 위한 MAP 메시지(MAP_Check_IMEI Request)를 송신하고, EIR(200)로부터 IMEI 체크 결과가 포함된 IMEI 체크 응답을 위한 MAP 메시지(MAP_Check_IMEI Response)를 수신한다. 그리고, 인증 처리부(140)는 EIR(200)로부터 전달받은 체크 결과가 포함된 IMEI 체크 요청 응답 메시지(Request Check_IMEI response)를 이동 단말(300)로 전달한다.

<49> 이하, 도 4를 참조하여 본 발명의 실시예에 따른 이동 단말 인증 방법에 대해 설명한다.

<50> 상세한 설명 전에 본 발명의 실시예에서는 도난 단말이나 복제 단말 등과 같은 불법 단말에 대한 신고가 이동 통신망의 사업자에게 접수되면, 전산 등을 통하여 해당 불법 단말의 IMEI가 EIR(200)의 블랙 리스트에 업데이트 되어 관리되고 있는 것으로 가정한다.

<51> 이와 같이, 불법 단말에 대한 신고가 접수되면, 이동 단말(300)은 이동 통신망의 관리자, 사업자 등으로부터 단말 인증, 즉 IMEI 체크를 수행할 것을 요구하는 명령을 수신한다(S100). 이러한 명령은 상기에서 기재한 바와 같이, 페이징, 문자 메시지, OTA 데이터 등을 통해 이동 단말(300)로 수신된다. 즉, 이동 단말(300)의 신호 송수신부(310)를 통해 수신된 신호를 인증 요구 검출부(320)가 검출하여 단말 인증 요구라는 것이 판명된다. 여기서, 페이징, 문자 메시지, OTA 데이터 등이 이동 통신망의 관리자나 사업자로부터 송신되어 코어망부(100)를 통해 이동 단말(300)로 수신되지만, IMEI 체크의 발신이 코어망부(100)가 아닌 다른 곳에서 이루어지는 것을 구분하여 나타내기 위해 도 4에서와 같이 나타내었다.

<52> 다음, 이동 단말(300)은 단말 인증을 수행하기 위해 IMEI 체크 요청 메시지(Request Check_IMEI)를 코어망부(100)로 송신한다(S110). 이 때 IMEI 체크 요청 메시지에는 이동 단말(300)의 IMEI가 포함되어야 한다. 즉, 이동 단말(300)의 단말 인증부(330)가 신호 송수신부(310)를 통해 IMEI 체크 요청 메시지를 코어망부(100)로 송신한다.

<53> 그 후, 코어망부(100)는 이동 단말(300)로부터의 IMEI 체크 요청을 수신하였으므로, IMEI 체크를 위해 MAP 메시지(MAP_Check_IMEI Request)를 EIR(200)로 송신한다(S120). 이 때, IMEI 체크를 위한 MAP 메시지에는 이동 단말(300)의 IMEI가 포함되어 있다. 즉, 코어망부(100)의 인증 요청 검출부(130)가 단말측 신호 송수신부(110)로부터 수신된 신호를 인증 요청 검출부(130)가 검출하여 IMEI 체크 요청이라는 것을 판단한 후, 인증 처리부(140)가 MAP 메시지를 EIR측 신호 송수신부(120)를 통해 EIR(200)로 송신한다.

<54> 한편, EIR(200)은 코어망부(100)로부터 IMEI 체크를 위한 MAP 메시지를 수신하면, 수신된 MAP 메시지에 포함되어 있는 IMEI가 화이트 리스트, 블랙 리스트, 그레이 리스트 중에서 어느 리스트에 속해 있는지를 검사하고(S130), 검사 결과를 IMEI 체크 결과로써 포함하는 IMEI 체크 결과 MAP 메시지(MAP_Check_IMEI Response)를 코어망부(100)로 송신한다(S140). 즉, IMEI 체크 결과 MAP 메시지에는 이동 단말(300)의 IMEI가 속하는 리스트의 종류 정보가 포함된다.

<55> 계속해서, 코어망부(100)는 EIR(200)로부터 송신된 IMEI 체크 결과 MAP 메시지를 수신한 후, IMEI 체크 결과를 상기 단계(S110)에서 수신한 IMEI 체크 요청 메시지에 대한 응답 메시지(Request Check_IMEI Response)에 포함시켜 이동 단말(300)로 송신한다(S150). 즉, 코어망부(100)의 인증 처리부(140)가 EIR측 신호 송수신부(120)를 통해 EIR(200)로부터 수신한 MAP 메시지에 포함된 IMEI 체크 결과를 응답 메시지에 포함시켜서 단말측 신호 송수신부(110)를 통해 이동 단말(300)로 송신한다.

<56> 다음, 이동 단말(300)은 코어망부(100)로부터 송신되는 IMEI 체크 결과가 포함된 응답 메시지(Request Check_IMEI Response)를 수신한 후, IMEI 체크 결과가 블랙인 지의 여부를 판단한다(S160). 만약 IMEI 체크 결과가 블랙이면, 이동 단말(300)이 불법 단말에 해당하므로, 이동 단말(300)은 사용자가 자신을 사용하여 이동 통신 서비스를 제공받을 수 없도록 제어한다(S170). 즉, 이동 단말(300)의 단말 인증부(330)가 IMEI 체크 결과 블랙이면, 단말 사용 제어부(340)를 통해 이동 단말(300)의 사용을 금지시키기 위한 제어를 수행한다.

<57> 그러나, IMEI 체크 결과가 블랙이 아니고 화이트이면 이동 단말(300)은 정상 단말로써 사용 가능하므로 후속 처리 없이 현 상태를 유지시킨다.

<58> 한편, IMEI 체크 결과가 그레이이면, 여러 가지 처리 방안이 존재하지만, 그 중 하나의 예로써 이동 단말(300)의 정상 사용이 가능하도록 함과 동시에 일정 시간이 지나면 이동 단말(300)의 IMEI 체크 동작(S110 내지 S160)을 재시도하도록 특별 처리할 수 있다. 다른 예로, IMEI 체크 결과가 그레이이면, 종래의 가입자 인증, 예를 들어 AuC(Authentication Center)나 HLR(Home Location Register)을 통한 인증을 수행하여 성공하면 화이트인

것으로 처리할 수 있다. 이 경우, 상기 단계(S140)에서 코어망부(100)가 EIR(200)로부터 IMEI 체크 결과를 받은 후, IMEI 체크 결과가 그레이이면 가입자 인증을 수행하고, 그 결과 인증이 성공하면 IMEI 체크 결과가 화이트인 것으로 설정하여 상기 단계(S150)에서 이동 단말(300)로 송신되는 응답 메시지를 송신하도록 하는 것이다.

<59> 한편, 이동 단말(300)은 코어망부(100)를 경유하여 EIR(200)에서 수행된 인증 결과, 즉 화이트, 블랙, 그레이 중 하나의 결과를 수신하면, 이동 단말(300)의 재시작과 관계없이 이동 단말(300)은 해당 인증 결과를 비휘발적으로 저장하여 관리하고, 상기 단계(S100)에서 IMEI 체크 요구에 의해 인증이 수행되거나 또는 인증 결과가 그레이라서 재시도에 의해 인증이 수행되어 EIR(200)로부터 새로운 인증 결과가 수신되면 이동 단말(300)은 이전에 저장하여 관리하는 인증 결과를 갱신하여 관리한다.

<60> 다음, 도 5를 참조하여 본 발명의 실시예에 따른 인증 방법을 수행하기 위한 이동 단말(300)에서의 동작 방법에 대해 설명한다.

<61> 이동 단말(300)의 인증 요구 검출부(320)는 신호 송수신부(310)를 통해 페이징, 문자 메시지, OTA 데이터 등이 수신되면(S200) 이들을 분석하여 이동 통신망의 관리자, 사업자 등으로부터 요구되는 단말 인증, 즉 IMEI 체크의 수행을 요구하는 명령이 수신되는 지의 여부를 판단한다(S210).

<62> 만일 수신되는 페이징, 문자 메시지, OTA 데이터를 분석한 결과 단말 인증을 요구하는 명령인 것으로 검출되면 해당 사실을 단말 인증부(330)로 전달하고, 단말 인증부(330)는 신호 송수신부(310)를 통해 이동 단말(300)의 IMEI를 포함한 IMEI 체크 요청 메시지(Request Check_IMEI)를 코어망부(100)로 송신하여 IMEI 체크를 요청한다(S220).

<63> 그 후, 코어망부(100)를 통해 EIR(200)에서 수행된 IMEI 체크 결과가 응답 메시지(Request Check_IMEI Response)를 통해 송신되면, 이동 단말(300)의 단말 인증부(330)가 신호 송수신부(310)를 통해 응답 메시지를 수신하여 결과적으로 IMEI 체크 결과를 수신한다(S230).

<64> 다음, 단말 인증부(330)는 상기 단계(S230)에서 수신된 IMEI 체크 결과가 어느 리스트에 속하는지를 확인하기 위해 먼저 블랙인지를 판단한다(S240).

<65> 만약 IMEI 체크 결과가 블랙이면, 이동 단말(300)이 불법 단말에 해당하므로, 단말 인증부(330)는 단말 사용 제어부(340)를 통해 이동 단말(300)의 사용을 금지시키기 위한 제어를 수행한다(S250). 즉, 사용자가 이동 단말(300)을 사용하여 이동 통신 서비스를 제공받을 수 없도록 제어한다.

<66> 한편, 상기 단계(S240)에서 IMEI 체크 결과가 블랙이 아니면 그레이인지를 판단한다(S260).

<67> 만약 그레이이면, 단말 인증부(330)는 일정 시간을 카운트하여 경과하면 EIR(200)을 통한 IMEI 체크를 재시도하기 위해 상기 단계(S220)부터 반복 수행한다.

<68> 한편, 상기 단계(S260)에서 IMEI 체크 결과가 그레이가 아니면 IMEI 체크 결과가 화이트이어서 이동 단말(300)이 정상 단말이므로, 단말 인증부(330)는 어떠한 조치 없이 단말 인증을 종료한다.

<69> 상기한 바와 같이, 본 발명의 실시예에서는 코어망부(100)가 이동 단말(300)이 호를 접속할 때마다 단말 인증을 수행하지 않고, 필요시에 이동 단말(300)이 능동적으로 코어망부(100)를 통해 EIR(200)에 의한 IMEI 체크를 수행하여 단말 인증을 수행함으로써 이동 통신망을 부하가 매우 감소되고, 이로 인해 이동 통신망 전체의 안정성이 높아질 수 있다.

<70> 한편, 상기에서는 이동 통신망의 관리자나 사업자 등에게 불법 단말에 대한 신고가 접수된 경우, 불법 단말이 능동적으로 자신의 IMEI의 블랙 리스트 여부를 판단하여 사용 금지를 수행하는 것에 대해 기재하였으나, 국내의 이동 통신망의 관리자나 사업자에게 불법 단말에 대한 신고가 어려운 이동 단말, 예를 들어 외국 제품의 이동 단말의 경우에는 상기한 방법으로 단말 인증을 처리할 시기를 잡기가 어렵다. 특히, 국내 이동 통신 사업자가 외국의 이동 통신 사업자와 협력하여 상호 계약에 의해 외국 제품의 이동 단말을 국내에 들여와 사용하는 경우 상기한 방법을 적용하기가 어렵다.

<71> 이를 위해, 본 발명의 실시예에서는 도 4를 참조하여 설명한 상기 단계(S110)에서 이동 단말(300)이 IMEI 체크를 시작하는 시기를 제공하는 상기 단계(S100) 대신에, 이동 단말(300)의 전원이 켜져서 이동 단말(300)이 위치한 이동 통신망에 대하여 위치 등록을 통한 망설정시에 이동 단말(300)이 기존에 설정되어 있던 망과 다른 망인가를 판단하여 다른 망인 경우에 IMEI 체크를 수행하는 상기 단계(S110)의 처리 시기를 제공하도록 한다. 이러한 IMEI 체크 처리 시기를 제공하는 것은 상기 단계(S100)와 함께 사용될 수도 있다.

<72> 또한, 상기에서는 불법 단말을 인증하기 위해 이동 단말의 IMEI를 사용하여 인증하는 것으로만 설명하였지만, 본 발명의 기술적 범위는 여기에 한정되지 않고, 휴대용 단말, 예를 들어 PDA나 스마트폰 등도 포함하여 불법 단말을 인증하기 위해 IMEISV(IMEI and Software Version number)를 사용하여 인증하는 것도 가능하다. 이러한 인증은 상기에서 설명한 IMEI 대신에 EIR(200)이 IMEISV를 저장하여 관리하고, 이동 단말, PDA, 스마트폰 등이 IMEI 체크시 코어망부(100)를 통해 IMEISV를 EIR(200)로 전달함으로써 EIR(200)에서 IMEISV에 기초한 불법 단말의 인증이 이루어지고, 그 결과가 코어망부(100)를 통해 단말로 전달됨으로써 IMEISV를 이용한 단말의 인증이 수행될 수 있다.

<73> 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면의 간단한 설명

<74> 도 1은 본 발명의 실시예에 따른 이동 단말 인증 방법이 적용되는 이동 통신 시스템을 개략적으로 도시한 도면이다.

<75> 도 2는 도 1에 도시된 이동 단말의 상세 블록도이다.

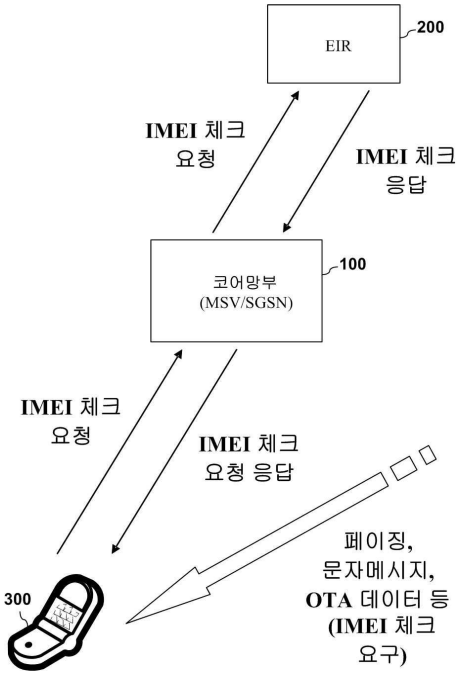
<76> 도 3은 도 1에 도시된 코어망부의 상세 블록도이다.

<77> 도 4는 본 발명의 실시예에 따른 이동 단말 인증 방법의 흐름도이다.

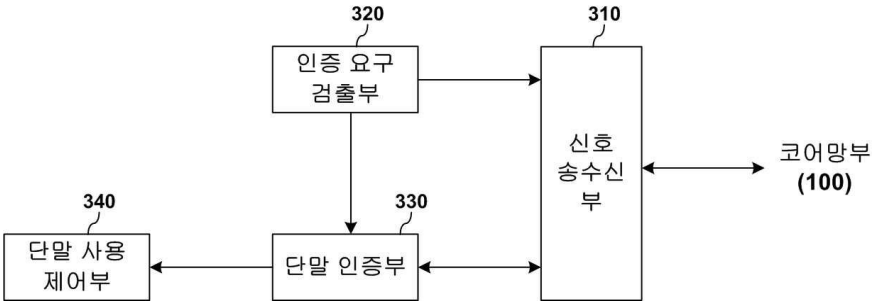
<78> 도 5는 본 발명의 실시예에 따른 인증 방법을 수행하기 위한 이동 단말에서의 동작 방법의 흐름도이다.

도면

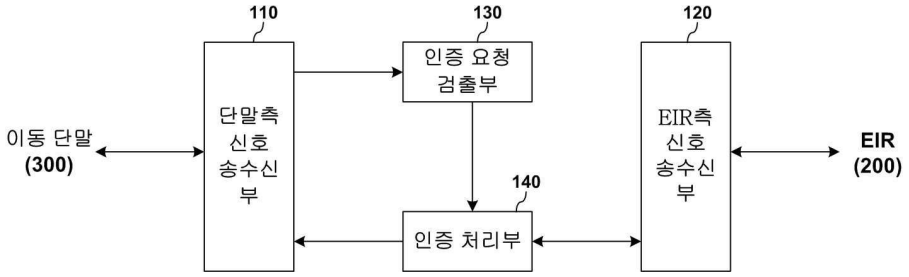
도면1



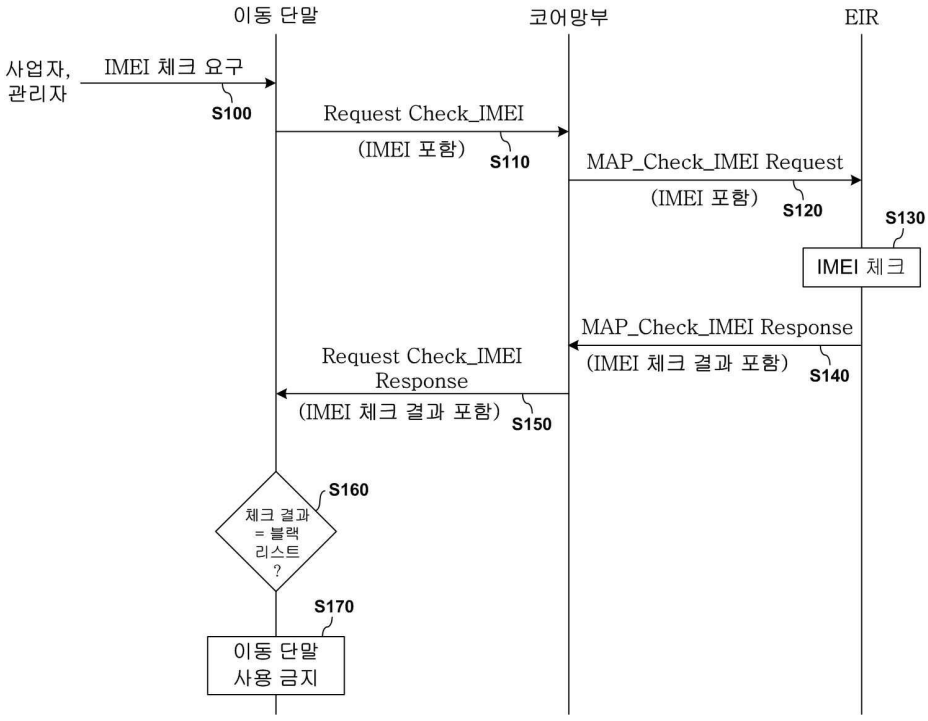
도면2


320
인증 요구
검출부
310
신호
송수신
부
코어망부
(100)
340
단말 사용
제어부
330
단말 인증부

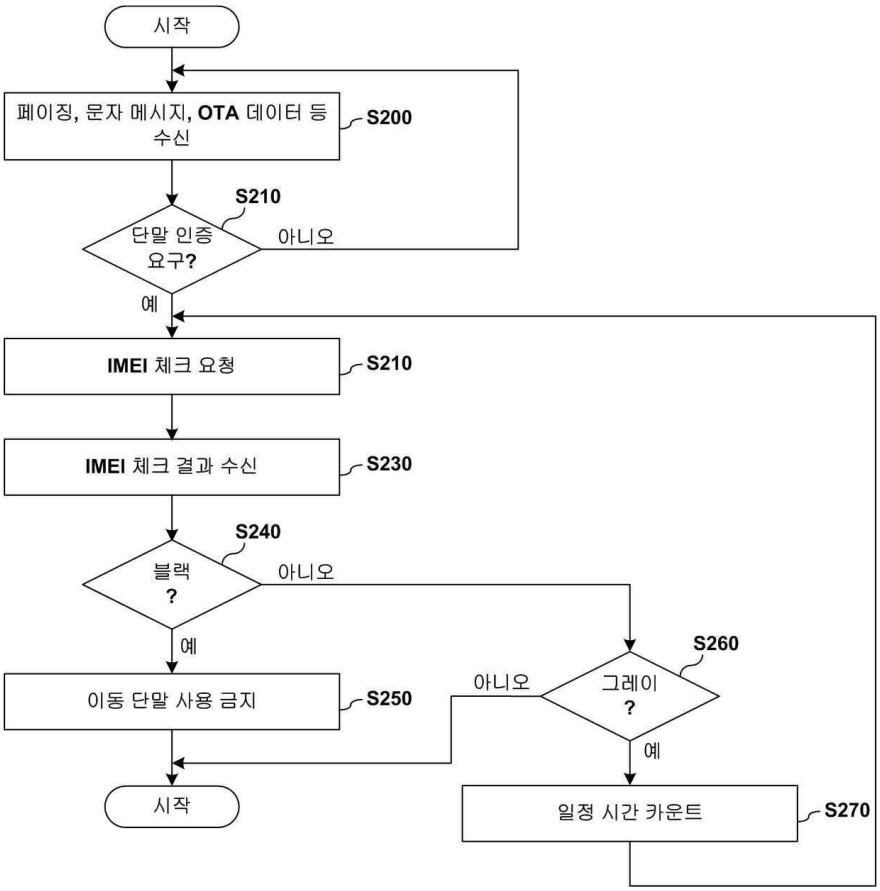
도면3


110
130
120
이동 단말
(300)
단말측
신호
송수신
부
인증 요청
검출부
EIR측
신호
송수신
부
EIR
(200)
140
인증 처리부

도면4


이동 단말
코어망부
EIR
사업자,
관리자
IMEI 체크 요구
S100
Request Check_IMEI
(IMEI 포함)
S110
MAP_Check_IMEI Request
(IMEI 포함)
S120
S130
IMEI 체크
MAP_Check_IMEI Response
(IMEI 체크 결과 포함)
S140
Request Check_IMEI
Response
(IMEI 체크 결과 포함)
S150
S160
체크 결과
= 블랙
리스트
?
S170
이동 단말
사용 금지

도면5


시작
페이징, 문자 메시지, OTA 데이터 등 수신
S200
S210
단말 인증 요구?
아니오
예
IMEI 체크 요청
S210
IMEI 체크 결과 수신
S230
S240
블랙 ?
아니오
예
S260
그레이 ?
아니오
예
이동 단말 사용 금지
S250
시작
일정 시간 카운트
S270