(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0029199
(43) 공개일자 2009년03월20일

(51) Int. Cl.
H04B 1/40 (2006.01) *G06F 21/00* (2006.01)
G06F 21/22 (2006.01)
(21) 출원번호 10-2008-7029839
(22) 출원일자 2008년12월05일
심사청구일자 없음
번역문제출일자 2008년12월05일
(86) 국제출원번호 PCT/IB2007/001105
국제출원일자 2007년06월08일
(87) 국제공개번호 WO 2007/141607
국제공개일자 2007년12월13일
(30) 우선권주장
60/804,221 2006년06월08일 미국(US)

(71) 출원인
브래들리, 키애런
아일랜드 더블린 13 서튼 발도일 로드 2
(72) 발명자
브래들리, 키애런
아일랜드 더블린 13 서튼 발도일 로드 2
(74) 대리인
김학수, 문경진

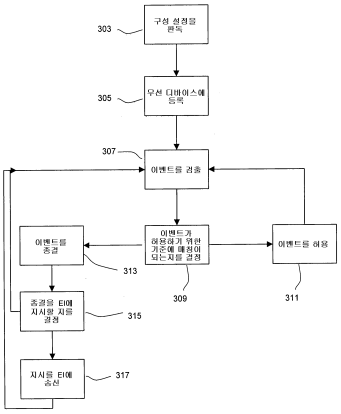
전체 청구항 수 : 총 60 항

(54) S I M-기반 방화벽을 위한 방법 및 장치

(57) 요 약

무선 디바이스 또는 SIM 카드에서 발생할 수 있는 이벤트를 필터하고 조절하기 위해 SIM-기반 방화벽을 사용하기 위한 방법은: 구성 설정을 읽는 단계; 무선 디바이스를 등록하고 타이머를 시작하는 단계; 이벤트를 검출하는 단계; 이벤트가 허용 기준과 매칭되는 지를 결정하는 단계; 및 만약 이벤트가 매칭된다면 이벤트를 허용하는 단계를 포함할 수 있다. 만약 이벤트가 허용되지 않으면, 이 방법은 이벤트를 종결하는 단계; 외부 인터페이스에게 통지할지를 결정하는 단계; 및 표시를 외부 인터페이스에게 가능하게 전송하는 단계를 포함할 수 있다. 이벤트가 검출되었고/되었다는 차단되었다는 표시는 원격 시스템에 또한 전송될 수 있다.

대 표 도 - 도3



특허청구의 범위

청구항 1

모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법으로서,

(a) SIM을 포함하는 모바일 디바이스에 대해 발생하는 이벤트의 표시를 상기 SIM에 의해 수신하는 단계;

(b) 상기 이벤트가 적어도 하나의 조건을 만족하는지를 SIM에 의해 결정하는 단계와;

(c) 상기 이벤트를 상기 SIM에 의해 차단하는 단계를

포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 2

제1항에 있어서, 상기 이벤트는 유출(outgoing) 콜을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 3

제1항에 있어서, 상기 이벤트는 유입 콜을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 4

제1항에 있어서, 상기 이벤트는 유입 문자 메시지를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 5

제1항에 있어서, 상기 이벤트는 유출 문자 메시지를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 6

제1항에 있어서, 상기 이벤트는 MMS 메시지, SMS 메시지, 또는 USSD 메시지 중 하나를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 7

제1항에 있어서, 상기 이벤트는 비디오 콜, 푸시 투 토크(Push To Talk) 콜, VOIP 콜, 이메일, 셀 방송, 즉석 메시징 메시지, GRPS, 블루투스, 네트워크 통신, 또는 데이터 연결 개시 중 적어도 하나를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 8

제1항에 있어서, 상기 적어도 하나의 조건은 상기 이벤트 소스의 전화 번호를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 9

제1항이 있어서, 상기 적어도 하나의 조건은 상기 이벤트 소스의 전화 번호의 부분을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 10

제1항에 있어서, 상기 적어도 하나의 조건은 상기 이벤트 소스의 지리적 영역을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 11

제1항에 있어서, 상기 적어도 하나의 조건은 상기 이벤트가 발생하는 시간을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 12

제1항에 있어서, 상기 적어도 하나의 조건은 상기 이벤트가 발생하는 날짜를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 13

제1항에 있어서, 상기 적어도 하나의 조건은 주어진 시간 기간 동안 상기 모바일 디바이스를 통해 이전에 취급된 콜의 전체 분량을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 14

제1항에 있어서, 상기 적어도 하나의 조건은 주어진 시간 기간 동안 상기 모바일 디바이스를 통해 이전에 취급된 문자 메시지의 전체 분량을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 15

제1항에 있어서, 상기 적어도 하나의 조건은 주어진 시간 기간 동안 상기 모바일 디바이스를 통해 이전에 취급된 MMS 메시지의 전체 분량을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 16

제1항에 있어서, 상기 적어도 하나의 조건은 주어진 시간 기간 동안 상기 모바일 디바이스를 통해 이전에 취급된 데이터의 전체 분량을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 17

제1항에 있어서, 상기 적어도 하나의 조건은 주어진 시간 기간 동안 상기 모바일 디바이스를 통해 이전에 취급된 이벤트의 전체 분량을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 18

제1항에 있어서, 상기 적어도 하나의 조건은 상기 이벤트의 소스 주소의 특성을 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 19

제18항에 있어서, 상기 소스 주소는 IP 주소, URL, SS 서비스 코드, 또는 USSD 서비스 코드 중 하나인, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 20

제1항에 있어서, 단계 (c)는 상기 모바일 디바이스의 사용자 인터페이스를 통해 이벤트가 표시되는 것을 상기 SIM이 방해하는 단계를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 21

제1항에 있어서, 단계 (c)는 상기 이벤트에 관련된 정보를 상기 모바일 디바이스가 송신하는 것을 상기 SIM이 방해하는 단계를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 22

제1항에 있어서, 미리 결정된 이벤트 세트의 표시를 수신하기 위해 상기 SIM에 의해 등록하는 단계를 더 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 23

제1항에 있어서, 원격 소스로부터 상기 적어도 하나의 조건을 상기 모바일 디바이스가 수신하는 단계를 더 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 24

제23항에 있어서, 차단하기 위한 상기 적어도 하나의 조건을 웹사이트를 통해 수신하는 단계와; 상기 적어도 하나의 조건을 상기 모바일 디바이스에게 송신하는 단계를 더 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 25

제1항에 있어서, 음성 인식 또는 자동화된 전화 응답 시스템 중 하나를 통해, 차단하기 위한 상기 적어도 하나의 조건을 수신하는 단계와; 상기 모바일 디바이스에 상기 적어도 하나의 조건을 송신하는 단계를 더 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 26

제1항에 있어서, 대화형 TV 또는 인터넷 프로토콜 TV(IPTV)를 통해, 차단하기 위한 상기 적어도 하나의 조건을 수신하는 단계와; 상기 모바일 디바이스에 상기 적어도 하나의 조건을 송신하는 단계를 더 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 27

제1항에 있어서, 모바일 인터넷 사이트를 통해, 차단하기 위한 상기 적어도 하나의 조건을 수신하는 단계와; 상기 모바일 디바이스에 상기 적어도 하나의 조건을 송신하는 단계를 더 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 28

제1항에 있어서, 제2 모바일 디바이스를 통해, 차단하기 위한 상기 적어도 하나의 조건을 수신하는 단계와; 상기 모바일 디바이스에 상기 적어도 하나의 조건을 송신하는 단계를 더 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 29

제1항에 있어서, 상기 이벤트가 검출되었다는 표시를 원격시스템에 송신하는 단계를 더 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 30

제29항에 있어서, 상기 이벤트가 차단되었다는 표시를 상기 원격 시스템에 송신하는 단계를 더 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 31

모바일 디바이스에서 방화벽으로 사용하기 위한 SIM으로서,

SIM을 포함하는 모바일 디바이스에 대해 발생하는 이벤트의 지시를 상기 SIM에 의해 수신하기 위한 수단;

상기 이벤트가 적어도 하나의 조건을 만족하는지를 SIM에 의해 결정하기 위한 수단과;

상기 이벤트를 상기 SIM에 의해 차단하기 위한 수단을

포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 32

제31항에 있어서, 상기 이벤트는 유출 콜을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 33

제31항에 있어서, 상기 이벤트는 유입 콜을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 34

제31항에 있어서, 상기 이벤트는 유입 문자 메시지를 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 35

제31항에 있어서, 상기 이벤트는 유출 문자 메시지를 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 36

제31항에 있어서, 상기 이벤트는 MMS 메시지, SMS 메시지, 또는 USSD 메시지 중 하나를 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 37

제31항에 있어서, 상기 이벤트는 비디오 콜, 푸시 투 토크(Push To Talk) 콜, VOIP 콜, 이메일, 셀 방송, 즉석 메시징 메시지, GRPS, 블루투스, 네트워크 통신, 또는 데이터 연결 개시 중 적어도 하나를 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 38

제31항에 있어서, 상기 적어도 하나의 조건은 상기 이벤트 소스의 전화 번호를 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 39

제31항이 있어서, 상기 적어도 하나의 조건은 상기 이벤트 소스의 전화 번호의 부분을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 40

제31항에 있어서, 상기 적어도 하나의 조건은 상기 이벤트 소스의 지리적 영역을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 41

제31항에 있어서, 상기 적어도 하나의 조건은 상기 이벤트가 발생하는 시간을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 42

제31항에 있어서, 상기 적어도 하나의 조건은 상기 이벤트가 발생하는 날짜를 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 43

제31항에 있어서, 상기 적어도 하나의 조건은 주어진 시간 기간 동안 상기 모바일 디바이스를 통해 이전에 취급된 콜의 전체 분량을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 44

제31항에 있어서, 상기 적어도 하나의 조건은 주어진 시간 기간 동안 상기 모바일 디바이스를 통해 이전에 취급된 문자 메시지의 전체 분량을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 45

제31항에 있어서, 상기 적어도 하나의 조건은 주어진 시간 기간 동안 상기 모바일 디바이스를 통해 이전에 취급된 MMS 메시지의 전체 분량을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 46

제31항에 있어서, 상기 적어도 하나의 조건은 주어진 시간 기간 동안 상기 모바일 디바이스를 통해 이전에 취급된 데이터의 전체 분량을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 47

제31항에 있어서, 상기 적어도 하나의 조건은 주어진 시간 기간 동안 상기 모바일 디바이스를 통해 이전에 취급된 이벤트의 전체 분량을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 48

제31항에 있어서, 상기 적어도 하나의 조건은 상기 이벤트의 소스 주소의 특성을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 49

제48항에 있어서, 상기 소스 주소는 IP 주소, URL, SS 서비스 코드, 또는 USSD 서비스 코드 중 하나인, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 50

제31항에 있어서, 상기 SIM은 상기 모바일 디바이스의 사용자 인터페이스를 통해 이벤트가 지시되는 것을 방해하기 위한 수단을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 51

제31항에 있어서, 상기 SIM은 상기 이벤트에 관련된 정보를 상기 모바일 디바이스가 송신하는 것을 방해하기 위한 수단을 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 52

제31항에 있어서, 미리 결정된 이벤트 세트의 표시를 수신하기 위해 상기 SIM에 의해 등록하기 위한 수단을 더 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 53

제31항에 있어서, 원격 소스로부터 상기 적어도 하나의 조건을 상기 SIM에 의해 수신하기 위한 수단을 더 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 54

제31항에 있어서, 웹사이트, 음성 인식 또는 자동화된 전화 응답 시스템, 대화형 TV, 인터넷 프로토콜 TV(IPTV), 모바일 인터넷 사이트, 또는 제2 모바일 디바이스 중 적어도 하나를 통해 입력된 데이터로부터 상기 적어도 하나의 조건을 상기 SIM에 의해 수신하기 위한 수단을 더 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 55

제31항에 있어서, 상기 이벤트가 검출되었다는 표시를 상기 원격 시스템에 송신하기 위한 수단을 더 포함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 56

제55항에 있어서, 상기 이벤트가 차단되었다는 표시를 상기 원격 시스템에 송신하기 위한 수단을 더 포

함하는, 모바일 디바이스에서 방화벽으로 사용하기 위한 SIM.

청구항 57

모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법으로서,

(a) 모바일 디바이스 내의 SIM에 의해 상기 SIM의 메모리의 부분의 수정을 검출하는 단계;

(b) 상기 모바일 디바이스에 대해 발생하는 이벤트의 표시를 상기 SIM에 의해 수신하는 단계;

(c) 상기 수정의 검출에 적어도 부분적으로 기초하여 상기 이벤트를 상기 SIM에 의해 차단하는 단계를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 58

제57항에 있어서, 단계 (a)는 상기 SIM의 메모리의 부분이 수정되었다는 표시를 상기 모바일 디바이스의 운영 체제로부터 수신하는 단계를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 59

제57항에 있어서, 단계 (a)는 상기 SIM의 메모리의 부분이 수정되었다는 지시를 상기 SIM의 운영 체제로부터 수신하는 단계를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

청구항 60

제57항에 있어서, 단계 (a)는 상기 메모리의 부분의 콘텐츠는 이전 시간의 메모리의 부분의 콘텐츠와는 다르다고 결정하는 단계를 포함하는, 모바일 디바이스에서 SIM 기반 방화벽을 동작시키기 위한 방법.

명 세 서

기 술 분 야

<1> 관련된 출원들

<2> 본 출원은 "SIM-기반 방화벽을 위한 방법 및 장치"라는 명칭의 2006년 6월 8일에 출원된 미합중국 가특허 출원 일련 번호 60/804,221로의 우선권을 주장한다.

<3> 본 발명은 가입자 식별 모듈을 이용하기 위한 무선 디바이스와, 이러한 디바이스 상에서 유입(incoming) 및 유출(outgoing) 통신, 데이터와 이벤트를 필터링하고 조절하기 위한 수단에 대한 것이다.

배 경 기 술

<4> 무선 디바이스 상에서 유입 및 유출 이벤트를 효과적으로 필터링하기 위한 능력이 요구되는 많은 상황들이 존재한다. 하지만, 종래 기술은 무선 전화 네트워크에서 현대의 무선 디바이스에 의해 송신되고 수신될 수 있는 복수의 데이터와 통신을 세밀하게(fine-grained) 제어하는 것을 허용하기에는 적절하지 않을 수 있다.

<5> 예를 들면, 모바일 통신을 위한 글로벌 시스템(GSM)과 유니버설 모바일 통신 시스템(UMTS)의 고정된 다이얼링 번호(fixed daialing number: FDN) 서비스는 유출 콜과 베어러(bearer) 서비스 및 텔레서비스가 제한되는 것을 허용할 수 있지만, 현대의 무선 서비스에 의해 송신되고 수신될 수 있는 복수의 데이터와 통신을 제어하지 않는다. GSM과 UMTS의 금지된 다이얼링 번호(BDN) 서비스는 한정된 전화 번호로의 유출 콜을 막으나, 유입 콜을 제어하지 않으며, 현대의 무선 디바이스에 의해 송신되고 수신될 수 있는 복수의 데이터와 통신을 제어하지 않는다.

<6> 모바일 네트워크 향상된 로직(CAMEL)을 위한 맞춤형(Customized) 애플리케이션을 사용하는 지능형 네트워크(intelligent network: IN) 또는 무선 전화 네트워크에 배치된 무선 지능형 네트워크(WIN) 기술은 무선 전화 네트워크내의 현대의 무선 디바이스에 의해 송신되고 수신될 수 있는 데이터와 통신에 대한 어느 정도의 제어를 제공할 수 있지만, 이러한 네트워크들은 배치시키기가 복잡하고, 비용이 많이 들고, 시간 소모적이다.

<7> 따라서, 무선 전화 네트워크에서 무선 디바이스에 의해 송신되고 수신될 수 있는 복수의 데이터, 통신 및 이벤트를 효과적인 세밀한 제어를 제공하는 해결책에 대한 필요가 존재한다.

발명의 상세한 설명

<8> 본 발명은 네트워크 내에서 무선 디바이스에 의해 송신되고 수신될 수 있는 복수의 데이터, 통신 및 이벤트의 세밀한 제어를 제공하기 위한 시스템과 방법에 대한 것이다.

<9> 일 양상에서, 본 발명은 무선 디바이스 또는 SIM 카드에서 발생할 수 있는 이벤트를 필터링하고 조절하기 위해 SIM-기반 방화벽을 사용하기 위한 방법이다. 간단히 개괄해서, 이 방법은: 구성 설정을 읽는 단계; 무선 디바이스를 등록하고 타이머를 시작하는 단계; 이벤트를 검출하는 단계; 이벤트가 허용 기준과 매칭되는지를 결정하는 단계; 및 만약 이벤트가 매칭된다면 이벤트를 허용하는 단계를 포함할 수 있다. 만약 이벤트가 허용되지 않으면, 이 방법은 이벤트를 종결하는 단계; 외부 인터페이스에게 통지할지를 결정하는 단계; 및 표시를 외부 인터페이스에게 가능하게 전송하는 단계를 포함할 수 있다. 이 방법은 이벤트가 검출되었고/되었거나 차단되었는지에 대한 표시를 원격 시스템에 전송하는 단계를 또한 포함할 수 있다.

<10> 다른 하나의 양상에서 본 발명은 SIM 기반 방화벽을 원격으로 관리하기 위한 방법이다. 간단한 개요에서, 이 방법은: 네트워크로부터 원격 관리 이벤트를 수신하는 단계를 포함한다. 원격 관리 이벤트는: SIM 기반 방화벽이 멈추도록 표시하는 단계; SIM 기반 방화벽이 다시 시작하도록 표시하는 단계; SIM 기반 방화벽의 구성 설정을 수정하는 단계; SIM 기반 방화벽의 수정된 구성 설정을 저장하는 단계; SIM 기반 방화벽의 실행 파일과 라이브러리를 수정하는 단계; 및 SIM 기반 방화벽의 수정된 실행 파일과 라이브러리를 저장하는 단계 중 하나 이상을 포함할 수 있다.

<11> 다른 하나의 양상에서, 본 발명은 위에서 설명된 방법 중 임의의 하나의 발명을 수행하기 위한 디지털 전자 시스템 또는 시스템들이다.

<12> 본 발명의 전술된 그리고 다른 목적, 양상, 특징과 이점은 첨부된 도면과 연계되어 다음 설명을 참조함으로써 더 잘 이해될 수 있고 보다 명백하게 될 것이다.

실 시 예

<18> 이제 도 1a를 참조하면, 네트워크에 연결된 SIM 기반 방화벽을 통합하는 무선 디바이스의 일 실시예를 묘사하는 블록도가 도시된다. 간단한 개요에서, 무선 디바이스(101)는 중앙 처리 장치(CPU)(103), 가입자 식별 모듈(Subscriber Identity Module: SIM)(107), SIM 기반 방화벽(109), 무선 트랜시버(115)와 외부 인터페이스(EI)(111)를 포함한다. 무선 디바이스는 하나 이상의 네트워크(105)와 통신할 수 있고, 하나 이상의 송신기/수신기 국(113)과 통신할 수 있다.

<19> 여전히 도 1a를 참조하면, 이제 더 상세히, 무선 디바이스(101)가 도시된다. 여기서, 용어 무선 디바이스는 무선, 케이블 또는 다른 실체적인 전송 매체를 이용하지 않고 네트워크에 및 네트워크로부터 음성 및/또는 데이터(비음성) 정보를 송수신할 수 있는 임의의 디바이스를 참조한다. 일 실시예에서, 무선 디바이스(101)는 모바일 폰을 포함할 수 있다. 다른 실시예들에서, 무선 디바이스(101)는 셀룰러 폰, 스마트 폰, 고정된-모바일 컨버전스(convergence) 폰, 위성 폰, 무선 데이터 카드, 무선 개인 디지털 어시트턴트(PDA), 무선 모뎀 또는 컴퓨터, 그리고 무선으로 통신하는 전자 시스템을 포함할 수 있다.

<20> 도시된 실시예에서, 무선 디바이스(101)는 SIM(107)을 포함한다. SIM(107)은 CPU, 암호화 프로세서, 판독 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 전기적으로 소거가능한 프로그래밍 가능 판독-전용 메모리(EEPROM)와 입출력 회로 중 하나 이상을 포함할 수 있다.

<21> SIM(107)은 SIM(107)의 소유자, SIM(107)이 연결하기 위한 허가를 가진 네트워크, SIM(107)이 네트워크상에서 액세스할 수 있는 서비스, 그리고 전화 번호부에 대한 고유의 가입 및 인증 정보를 저장하기 위해 사용될 수 있다. SIM(107)은 하나의 이상의 가치가 부가된 애플리케이션을 포함할 수 있다. 이러한 애플리케이션은: 은행 업무, 바이오메트릭, 의료, 보안, 생산성, 신원 관리, 디지털 서명, 공중키 기반구조(PKI), 멀티미디어, 티켓 발행, 디지털 권리 관리, 게임, 및 충성도(loyality) 애플리케이션을 포함할 수 있다. SIM 애플리케이션은 SIM 애플리케이션 툴키트(SAT) 기술 또는 다른 스마트 카드 애플리케이션 기술을 이용할 수 있다.

<22> 다른 실시예에서, 무선 디바이스는 SIM 대신에 유니버설 집적 회로 카드(UICC)를 포함할 수 있다. UICC는: GSM 가입자 식별 모듈(SIM), UMTS 인터넷 프로토콜 멀티미디어 서비스 식별 모듈(ISIM), CDMA 제거가능한 사용자 식별 모듈(R-UIM), 그리고 가치 부가된 애플리케이션 중 하나 이상을 포함할 수 있다. UICC 애플리케이션은: USAT(Universal SIM Application Toolkit), CCAT(CDMA Card Application Toolkit), CAT(Card Application

Toolkit), UATK(UIM application Toolkit) 또는 다른 스마트 카드 기술 중 하나 이상을 사용할 수 있다. 이런 상황에서, SIM(107)은 SIM 카드와 USIM을 구비한 UICC 둘 다, 또는 다른 IM, UICC상에 상주하는 애플리케이션을 나타내기 위해 일반적으로 사용된다.

<23> 도시된 실시예에서, SIM(107)은 SIM 방화벽(109)으로 여기서 참조되는 SIM 기반 방화벽 애플리케이션(109)을 포함할 수 있다. SIM 방화벽(109)은 네트워크(105), 무선 디바이스(101), SIM(107)과 외부 인터페이스(111)간의 양쪽 방향으로 통과하는 데이터, 통신, 및 이벤트를 검출하고, 필터링하고 조절하는 프로그래밍 가능한 로직을 포함할 수 있다. SIM 방화벽(109)은 하나 이상의 구성 가능한 기준에 대해서 데이터, 통신 및 이벤트를 평가할 수 있다. 만약 데이터, 통신 및 이벤트가 규정된 기준에 매칭된다면, 이것들은 네트워크(105), 무선 디바이스(101), SIM(107)과 무선 디바이스의 외부 인터페이스(111) 사이에서 양쪽 방향으로 계속하는 것이 거절되거나 허용될 수 있다.

<24> 일 실시예에서, SIM 방화벽(109)은 SMS 또는 셀 방송(CB) 메시지를 가진 무선(Over The Air: OTA) 관리를 사용해서, 베어러 독립 프로토콜(BIP)을 사용해서, 자바 원격 메소드 호출(RMI)을 사용해서, J2ME를 위한 보안과 신뢰 서비스 API(SATSA) 규격을 지원하는 자바 2 마이크로 에디션(J2ME) 미들렛(midlet)을 사용해서, 무선 디바이스의 운영 체제를 사용해서, 무선 디바이스상의 애플리케이션을 사용해서, SIM에 물리적으로 연결되는 카드 승인 디바이스(CAD) 또는 다른 스마트 카드 판독기를 사용해서, 단거리 무선 주파수 기술에 의해 SIM과 통신할 수 있는 비접촉 스마트 카드 기술을 사용해서 SIM(107)의 제조 과정의 일부로서 SIM으로 전송되어 설치될 수 있다.

<25> 도시된 실시예에서, SIM 방화벽(109)은 SMS 메시지, 셀 방송 메시지, BIP, 자바 RMI, SATSA 규격 또는 다른 원격 관리 기술을 지원하는 J2ME 미들렛, 무선 디바이스의 운영 체제, 무선 디바이스 상의 애플리케이션 중 하나 이상을 사용해서 네트워크 상에서 원격으로 관리될 수 있다. 실시예는 SIM(107)에 물리적으로 연결되지 않으면서 SIM 방화벽(109)을 개인이 관리하게 할 수 있다.

<26> 일 실시예에서, SIM 방화벽(109)은 카드 승인 디바이스(CAD) 또는 SIM에 물리적으로 연결된 다른 스마트 카드 판독기를 사용해서; 단거리 주파수 기술에 의해 SIM과 통신할 수 있는 비접촉 스마트 카드 기술을 사용해서 국부적으로 관리될 수 있다.

<27> 도시된 실시예에서, SIM 방화벽은 모바일 디바이스가 전원이 켜질 때 자동으로 시작할 수 있고, 모바일 디바이스가 전원이 꺼질 때 정지할 수 있다. SIM 방화벽은 또한 여기서 설명된 국부적 및 원격 관리 기술 중 임의의 하나 또는 전부에 의해 정지되고 시작될 수 있다.

<28> 도시된 실시예에서, 무선 디바이스(101)는 외부 인터페이스(EI)(111)를 포함할 수 있다. 외부 인터페이스는 인간-기계간의 인터페이스(MMI)와 기계간의 인터페이스(M2M) 중 하나 이상을 포함할 수 있다. MMI는 제한이 없이, 스크린, 카메라, 지문 판독기, 키보드, 키패드, 마이크로폰, 광 센서, 오디오 센서, 움직임 센서, 스피커를 포함하는 무선 디바이스와 개인이 상호작용하거나 동작시키게 하는 임의의 디바이스를 포함할 수 있다. M2M은 제한이 없이, RS-232 직렬 통신 데이터 포트, 제조자의 독점적인(proprietary) 통신 데이터 포트, 유니버설 직렬 버스(USB) 데이터 포트, 블루투스 트랜시버 데이터 포트, 초광대역(UWB) 트랜시버 데이터 포트, 적외선 데이터 포트, 다른 단거리 무선 주파수 기술 데이터 포트, 또는 무선 디바이스가 다른 디바이스와 통신할 수 있게 하는 다른 데이터 포트를 포함하는, 무선 디바이스와 다른 디바이스가 데이터를 교환하게 하거나 이러한 무선 디바이스를 작동시키게 하는 임의의 디바이스를 포함할 수 있다.

<29> 도시된 실시예에서, 무선 디바이스(101)는 네트워크(105)와 통신할 수 있다. 네트워크(105)는 무선 송신물을 수신할 수 있는 임의의 알려진 네트워크를 포함할 수 있다.

<30> 이제 도 1b를 참조하면, 예시적인 네트워크(105)가 도시된다. 네트워크(105)는 다음 중 임의의 하나 또는 전부를 포함할 수 있다: 해당 기술에서 모바일 국(MS)으로 설명되는 무선 디바이스(101); 베이스 트랜시버 국(BTS)(113), 기지국 제어기(BSC)(147), 모바일 스위칭 센터(MSC)(117), 홈 위치 등록기(HLR)(119), 인증 센터(AuC)(121), 방문자 위치 등록기(VLR)(123), 게이트웨이 모바일 스위칭 센터(GMSC)(125), 공중 스위칭 전화통신 네트워크(PSTN)(127), 짧은 메시지 서비스 센터(SMSC)(129), 장비 식별 등록기(EIR)(131), 구조화되지 않은 보조 서비스 데이터(USSDGW) 게이트웨이(133), 인터넷 애플리케이션 서버(IAS)(135), 게이트웨이 일반 패킷 무선 서비스(GPRS) 지원 노드(GGSN)(137), 서빙 GPRS 지원 노드(SGSN)(139), 패킷 데이터 네트워크(PDN)(141), SIM OTA 서버(OTA)(143), 및 SMS 게이트웨이 MSCs(SMS GMSC)(145). 네트워크(105)의 구성 요소는 임의의 상호 연결 기술을 사용해서 임의의 토폴로지에서 연결될 수 있다.

<31> 여기서 설명된 네트워크(105)는 일반화된 GSM/GPRS 네트워크를 포함할 수 있지만, 당업자는 본 발명이 다른 베

어러(bearer), 프로토콜, 기술, 아키텍처와 토폴로지를 이용하는 대안적인 네트워크에서 배치될 수 있다는 것을 인식할 것이다. 다른 실시예에서, 네트워크(105)는 다음 중 하나 이상을 이용할 수 있다: 유니버설 모바일 전화 통신 서비스(UMTS), 코드 분할 다중 액세스(CDMA2000 1x, CDMA2000 1xEV-DO, CDMA2000 1xEV-DV, CDMA TIA/EIA/ANSI-95A/B를 포함하는 CDMA), GPRS, GSM 발전을 위한 향상된 데이터 속도(EDGE), 광대역 코드 분할 다중 액세스(W-CDMA), 개인용 디지털 셀룰러(PDC), 통합된 디지털 향상된 네트워크(iDEN), 고속 업링크 패킷 액세스(HSUPA) UMTS, 고속 다운링크 패킷 액세스(HSDPA) UMTS, 모바일 멀티미디어 액세스의 자유(FOMA), 시분할-동기 코드 분할 다중 액세스(TD-SCDMA), 시분할-코드 분할 다중 액세스(TD-CDMA), UMTS-시분할 듀플렉싱(UMTS-TDD), UMTS 장기간 발전(LTE), 주파수 분할 다중화(FDM), 주파수 분할 듀플렉싱(FDD), 직접 시퀀스 초광대역(DS-UWB), 인터넷 프로토콜 멀티미디어 서브시스템(IMS), 세션 개시 프로토콜(SIP), 직교 주파수 분할 배수(OFDM), 직교 주파수 분할 다중 액세스(OFDMA), 소프트웨어-정의된 무선(SDR), 개인용 통신 서비스(PCS), 고속 회로-스위칭된 데이터(HSCSD), 초광대역(UWB), 광대역 통합된 급송 향상된 네트워크(WiDEN), 인가되지 않은 모바일 액세스(UMA), WiMax IEE 802.16, WiFi IEE 802.11, 무선 로컬 영역 네트워크(WLAN), 회로 스위칭된 데이터(CSD), 무선 광역 네트워크(WWAN), 인터넷 프로토콜상의 음성(VOIP), 시간 분할 다중 액세스(TDMA), 무선 광대역(WiBro), 시간 분할 CDMA(TD-CDMA), WLAN상의 음성(VoWLAN), 다중-입력 다중-출력(MIMO), 가변-확산-인수 확산 직교 주파수 분할 다중화, 푸시-투-토크(PTT), 신호 시스템 7(SS7), IP 상의 SS7, 메시지 전송 부분-레벨 2 피어-투-피어 적응 층(M2PA), 메시지 전송 부분-레벨 3 사용자 적응 층(M3UA), 공통 채널 신호 시스템 7(CCS7), 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP), 하이퍼 텍스트 전송 프로토콜(HTTP), 하이퍼 텍스트 전송 프로토콜 보안(HTTPS), 사용자 데이터그램 프로토콜(UDP).

<32> 이제 도 2a를 참조하면, SIM 기반 방화벽에 의해 처리되는 이벤트의 일 실시예를 묘사하는 흐름도가 도시된다. 간단한 개요에서, 네트워크(105)는 무선 디바이스에 의해 수신된 이벤트를 개시한다(단계 201). 무선 디바이스(101) 내에서 동작하는 SIM 기반 방화벽(109)은 이벤트를 검출하고(단계 203), 이벤트를 평가한다(단계 205). SIM 기반 방화벽은 이벤트를 허용하고(단계 207), 그리고 나서 이 이벤트는 자신이 EI(111)로 전달된 지점에서 계속 진행한다(단계 209). 그리고 나서 이벤트는 EI(111)으로부터 무선 디바이스로의 전송에 의해 종결될 수 있는데(단계 211), 그리고 나서 이 이벤트는 네트워크에 전달된다(단계 213).

<33> 여전히 도 2a를 참조하면서 이제 더 상세히, 도시된 실시예에서, 네트워크(105)는 무선 디바이스에 의해 수신된 이벤트를 개시한다(단계 201). 이벤트는 다음 중 하나 이상을 포함할 수 있다: 음성 콜, 비디오 콜, PTT 콜, 셀 방송 메시지, SMS 메시지, 즉석 메시징 메시지, 무선 애플리케이션 프로토콜(WAP) 푸시 메시지, 멀티미디어 메시징 서비스(MMS) 통지, SIM 갱신 메시지, 향상된 메시징 서비스(EMS) 메시지, 전자 메일 통지, 전자 메일 메시지, 유입 암호화된/해독된 데이터 연결 통지, 유입 암호화된/해독된 데이터 연결, 모바일 TV 데이터, 무선 디바이스의 페이징/폴링, 유입 라디오, 비디오 또는 다른 멀티미디어 콘텐츠, 무선 디바이스 운영 체제 갱신, 무선 디바이스 애플리케이션 갱신, 무선 디바이스 펌웨어 갱신, 새로운 무선 디바이스 애플리케이션의 설치.

<34> 도시된 실시예에서, 그 후 이벤트는 무선 디바이스에서 SIM상에서 실행되고 있는 SIM 기반의 방화벽 애플리케이션에 의해 검출될 수 있다(단계 203). 특정 실시예에서, SIM 방화벽은 무선 디바이스 또는 무선 디바이스 운영 체제에 이전에 등록되어서, 네트워크로부터 수신될 수 있는 하나 이상의 이벤트를 통지 받을 수 있다. 일 실시예에서, 이벤트가 무선 디바이스에 의해 수신된 후에, 이벤트에 대한 정보 및 유입 이벤트에 대한 제어는 무선 디바이스로부터 SIM 방화벽으로 전달될 수 있다. 다른 실시예에서, SIM은 하나 이상의 이벤트를 능동적으로 검출할 수 있다.

<35> 도시된 일 실시예에서, 그리고 나서 이벤트는 SIM 또는 무선 디바이스 상에 저장될 수 있는 구성 가능한 기준에 대해 SIM 방화벽에 의해 평가될 수 있다(단계 205). 기준은 다음 중 하나 이상을 포함할 수 있다: 이벤트 유형, 유입 및 유출 이벤트, 데이터 유형, 데이터 콘텐츠, 애플리케이션 유형, 프로토콜, 베어러, 소스 주소, 목적지 주소, 시간, 날짜, 이전 이용 분량, 및 이전 이벤트의 개수.

<36> 일 실시예에서, SIM 방화벽은 부분적 및/또는 완전 매칭에 의해 소스 및 목적지 주소를 평가할 수 있다. SIM 방화벽은 다음 중 하나 이상을 포함할 수 있는 주소 지정 방식을 평가할 수 있다: 인터넷 프로토콜(IPv4 및/또는 IPv6) 주소 및/또는 포트 번호들, 고유 자원 로케이터 주소, 이메일 주소, GPRS APN(Access Point Name)들, MSISDN(Mobile Station Integrated Services Digital Network) 번호, USSD 서비스 코드, 셀 ID, IMEI(Internal Mobile Equipment Identity)、IMSI(International Mobile Subscriber Identity), SMS 포트 번호, 무선 디바이스 포트 번호, 그리고 무선 디바이스에 의해 지원되는 다른 주소지정 방식.

<37> 다른 실시예에서, SIM 방화벽은 하나 이상의 시간 구성요소의 임의의 조합에 의해 이벤트를 평가할 수 있다. 예

를 들면, 부모는 자녀가 학교에서 공부하는 동안에는 친구에게 전화를 걸거나 받기 위해 모바일 폰을 사용할 수 없게 지정할 수 있다. 또는, 예를 들면, 회사의 관리자는 회사의 모바일 폰이 작업 시간 또는 평일에만 사용될 수 있게 지정할 수 있다. SIM 방화벽은 또한 구성 가능하게 예정된 기초 위에서(예, SIM 방화벽은 매 10초마다 조건을 평가할 수 있다) 이벤트를 평가할 수 있다.

<38> 도시된 실시예에서, 만약 이벤트가 구성된 기준에 의해 금지되지 않는다면, SIM 기반 방화벽은 이벤트가 진행되게 할 수 있으며(단계 207), 이벤트의 제어는 SIM으로부터 무선 디바이스로 전달되고, 그리고 나서 무선 디바이스의 외부 인터페이스에 전달된다(단계 209).

<39> 도시된 실시예에서, 그리고 나서 무선 디바이스의 외부 인터페이스는 이벤트를 처리할 수 있다(단계 209). 이벤트는 외부 인터페이스의 M2M 또는 MMI 인터페이스에 의해 처리될 수 있다.

<40> 도시된 실시예에서, 이벤트는 외부 인터페이스(111)로부터 무선 디바이스로의 전송에 의해 종결될 수 있으며(단계 211), 그리고 나서 이벤트는 네트워크에 전달된다(단계 213).

<41> 비록 도시된 실시예에서, SIM 기반 방화벽이 이벤트가 진행되는 것을 허용한 후에(단계 207), 이벤트의 제어는 SIM으로부터 무선 디바이스에 전달되고, 그리고 나서 무선 디바이스의 외부 인터페이스에 전달되지만(단계 209), 다른 실시예에서 이벤트의 제어는 처리를 위해 다음 중 하나의 엔티티(entity)에 전달될 수 있다: 무선 디바이스, 무선 디바이스상의 애플리케이션, 무선 디바이스의 운영 체제, 무선 디바이스의 펌웨어, SIM, SIM상의 애플리케이션. 이벤트는 수신 엔티티로부터 전송에 의해 종결될 수 있으며, 그리고 나서 이벤트는 네트워크에 전달될 수 있다(단계 213).

<42> 도 2b를 이제 참조하면, SIM 기반 방화벽에 의해 처리되는 이벤트의 다른 하나의 실시예를 묘사하는 흐름도가 도시된다. 간단한 개요에서, 네트워크(105)는 무선 디바이스에 의해 수신된 이벤트를 개시한다(단계 201). 무선 디바이스(101) 내에서 작동하는 SIM 기반 방화벽(109)은 이벤트를 검출하고(단계 203), 이벤트를 평가한다(단계 205). SIM 기반 방화벽은 이벤트를 금표시키고, 이벤트는 종결된다(단계 219). 그리고 나서 이벤트는 무선 디바이스로부터 네트워크로의 전송에 의해 종결될 수 있다(단계 221).

<43> 여전히 도 2b를 참조하면, 이제 더 상세히, 도시된 실시예에서 네트워크(105)는 무선 디바이스에 의해 수신된 이벤트를 개시한다(단계 201). 이 단계는 도 2a와 연계되어 설명되는 바와 같이 수행될 수 있다.

<44> 도시된 실시예에서, 그리고 나서 이벤트는 SIM상에서 실행되는 SIM 기반 방화벽 애플리케이션에 의해 검출될 수 있다(단계 203). 이 단계는 도 2a와 연계되어 설명되는 바와 같이 수행될 수 있다.

<45> 도시된 실시예에서, 그리고 나서 이벤트는 SIM 또는 무선 디바이스 상에 저장될 수 있는 구성 가능한 기준에 대해 SIM 기반의 방화벽 애플리케이션에 의해 평가될 수 있다(단계 205). 이 단계는 여기서 설명된 실시예들 중 임의의 하나에 따라 수행될 수 있다. 도시된 실시예에서, 이벤트는 구성된 기준에 의해 금지되고, SIM 방화벽은 이벤트가 계속되는 것을 방해한다.

<46> 그리고 나서 이벤트는 종결되고(단계 219) 제어는 무선 디바이스에 전달된다. 특정 실시예에서, 이벤트의 종결은 무선 디바이스로부터 네트워크로의 송신에 의해 종결될 수 있다(단계 221).

<47> 비록 도 2a와 도 2b에서 도시된 실시예들에서, 이벤트가 네트워크에 의해 개시되지만(단계 201), 다른 실시예에서 SIM 기반 방화벽은 무선 디바이스(101), SIM(107), SIM상의 애플리케이션, 무선 디바이스의 외부 인터페이스(111)에 개시될 수 있는 다른 이벤트, 또는 SIM 기반 방화벽(109)에 의해 추론될 수 있는 이벤트를 검출하고 평가할 수 있다.

<48> 무선 디바이스에 의해 개시된 이벤트는 타이머에 의해 생성된 이벤트, 외부 또는 내부 카드 판독기에 의해 생성된 이벤트, 무선 디바이스의 파일 시스템 또는 메모리에 액세스하거나 이것들을 수정하는 것과 관련된 이벤트, SD(Secure Digital) 플래시, MMC(Multi Media Card) 플래시, 컴팩트 플래시 저장 디바이스, 메모리 스틱, 플래시 램/롬, EPROM(소거가능한 프로그래밍 가능 판독 전용 메모리), EEPROM(전기적으로 소거가능한 프로그래밍 가능 판독 전용 메모리), 고체 메모리, 하드 드라이브, 낸드 플래시 저장 디바이스와 같은 외부 저장 기술에 액세스하고 이를 수정하는 것과 관련된 이벤트, 또는 무선 디바이스 상에서 실행되는 애플리케이션 또는 서비스를 시작하거나 종결하는 것과 관련된 이벤트, 무선 디바이스의 운영 체제에 의해 생성된 이벤트, 무선 디바이스상의 데이터 세션을 시작하거나 종결하는 것과 관련된 이벤트, 다른 디바이스로부터 블루투스 통신을 수신하는 것과 관련된 이벤트, 다른 디바이스로부터 적외선 통신을 수신하는 것과 관련된 이벤트, 그리고 단거리 무선 기술을 사용해서 다른 디바이스로부터 통신을 수신하는 것과 관련된 이벤트를 제한 없이 포함할 수 있다.

<49> 무선 디바이스의 외부 인터페이스에 의해 개시된 이벤트는 무선 디바이스상의 버튼을 사용자가 다루는 것과 관련된 이벤트, 무선 디바이스상의 조이스틱을 사용자가 다루는 것과 관련된 이벤트, 무선 디바이스의 음성 제어를 포함하는 사용자 입력 매커니즘을 사용자 다루는 것과 관련된 이벤트, SMS 메시지를 사용자가 송신하는 것과 관련된 이벤트, MMS 메시지를 사용자가 송신하는 것과 관련된 이벤트, USSD 메시지와 관련된 이벤트, 즉석 메시지를 사용자가 송신하는 것과 관련된 이벤트, 음성 콜을 사용자가 시작하거나 종결하는 것과 관련된 이벤트, 비디오 콜을 사용자가 시작하거나 종결하는 것과 관련된 이벤트, VOIP 콜을 사용자가 시작하거나 종결하는 것과 관련된 이벤트, PTT 콜을 사용자가 시작하거나 종결하는 것과 관련된 이벤트, 블루투스 데이터 세션을 사용자가 시작하거나 종결하는 것과 관련된 이벤트, 적외선 데이터 세션을 사용자가 시작하거나 종결하는 것과 관련된 이벤트, 데이터 세션을 사용자가 시작하거나 종결하는 것과 관련된 이벤트, 무선 디바이스 또는 SIM상의 서비스를 시작하거나 종결하는 것과 관련된 이벤트, 및 무선 디바이스 또는 SIM상의 애플리케이션을 사용자가 시작하거나 종결하는 것과 관련된 이벤트, M2M을 통해 무선 디바이스에 송신된 AT 명령어, M2M을 통해 SIM에 송신된 AT 명령어, M2M을 통해 SIM 또는 무선 디바이스에 송신된 다른 프로그램 명령어를 포함할 수 있다.

<50> SIM에 의해 개시된 이벤트는 SIM상의 애플리케이션에 의해 생성된 이벤트, SIM의 파일 시스템 또는 메모리에 액세스하거나 이를 수정하는 것과 관련된 이벤트, SIM의 암호화되거나 이와 다르게 보호된 파일 또는 메모리에 액세스하거나 이를 수정하는 것과 관련된 이벤트, 및 SIM의 파일 또는 메모리에 적용된 암호화 동작과 관련된 이벤트를 포함할 수 있다.

<51> 도 3을 참조하면, 이벤트를 필터링하기 위해 SIM 방화벽에 의해 수행된 방법의 일 실시예를 묘사하는 흐름도가 도시된다. 간단한 소개에서, 본 방법은: 구성 설정을 판독하는 단계(단계 303); 무선 디바이스에 등록하는 단계(단계 305); 이벤트를 검출하는 단계(단계 307); 이벤트가 허용 기준에 매칭되는 지를 결정하는 단계(단계 309); 및 만약 이벤트가 매칭이 된다면, 이벤트를 허용하는 단계(단계 311)를 포함한다. 만약 이벤트가 허용되지 않는다면, 본 방법은 그리고 나서 이벤트를 종결시키는 단계(단계 313); EI에게 통지할지를 결정하는 단계(단계 315); 및 EI에게 표시를 잠재적으로 송신하는 단계(단계 317)를 포함할 수 있다.

<52> 여전히 도 3을 참조하면, 이제 더 상세히, 도시된 실시예에서, SIM 방화벽은 구성 설정을 판독한다(단계 303). 일 실시예에서, 방화벽은 SIM상에 저장된 파일로부터 구성 설정을 판독한다. 다른 실시예에서, 방화벽은 SIM의 메모리로부터 구성 설정을 판독한다. 또 다른 실시예에서, 방화벽은 모바일 디바이스 상에서 이와는 다르게 저장된 파일로부터 구성 설정을 판독한다.

<53> 일 실시예에서, 구성 설정은 무선 디바이스 또는 SIM상의 파일 또는 메모리 구역을 포함한다. 파일 또는 메모리 구역은 소스 주소, 목적지 주소, 프로토콜, 베어러, 이벤트 유형, 유입 또는 유출 방향, 데이터 유형, 데이터 콘텐츠, 애플리케이션, 자원, 이벤트가 허용되거나 금지될 수 있는 시간, 이벤트가 금지되는 경우 외부 인터페이스에게 통지되어야 하는가에 대한 여부, 그리고 하나 이상의 이러한 기준에 매칭되는 이벤트가 허용되거나 금지되어야 하는가에 대한 여부 중 하나 이상을 포함할 수 있다.

<54> SIM 기반 방화벽이 구성 설정을 판독한 후에(단계 303), 그리고 나서 이 방화벽은 무선 디바이스에 등록할 수 있고, 임의의 요구된 타이머를 시작할 수 있다(단계 305). SIM 방화벽은 무선 디바이스에 의해 통지되어야 할 구성 설정 내에 지정된 임의의 이벤트를 무선 디바이스에 등록한다.

<55> 일 실시예에서 SIM 방화벽은 구성 설정 내에 지정된 시간에 종료되기 위해 하나 이상의 타이머를 시작할 수 있다. 다른 실시예에서 SIM 방화벽은 구성 설정 내에 정해진 간격을 두고 종료되기 위해 하나 이상의 타이머를 시작할 것을 무선 디바이스에게 요청할 수 있다. 타이머가 종료되면, SIM 방화벽은 무선 디바이스에 의해 이벤트를 통지 받는다.

<56> 도시된 일 실시예에서, SIM 방화벽은 이벤트를 검출하고(단계 307), SIM 방화벽은 이벤트가 허용 기준에 매칭되는 지를 결정한다(단계 309). 만약 이벤트가 허용 기준에 매칭이 되면, 이 이벤트가 허용되고(단계 311), 이에 따라 SIM 방화벽이 다른 하나의 이벤트를 검출하기 위해 준비가 된다(단계 307). 상기 결정은 여기서 설명된 임의의 기준과 정보를 사용해서 수행될 수 있다. 다른 실시예에서, SIM 방화벽은 이벤트가 거절 기준에 매칭이 되는지를 결정할 수 있다. 여전히 다른 실시예에서, SIM 방화벽은 허용 기준과 거절 기준 양쪽 모두에 기초해서 이벤트를 허용할지를 결정할 수 있다. 일 실시예에서, SIM 방화벽은 기준의 계층 구조를 포함할 수 있다. 예를 들면, SIM 방화벽은 주어진 지역 코드로의 모든 유출 콜을 거절하기 위한 기준을 포함할 수 있지만, 상기 지역 코드 내의 특정 번호로부터의 콜을 허용한다.

<57> 만약 이벤트가 허용 기준에 매칭이 되지 않는다면, 이벤트는 종결될 수 있으며(단계 313) 이에 따라 SIM 방화벽

은 다른 하나의 이벤트를 검출하기 위해 준비된다(단계 307). 특정 실시예에서, SIM 방화벽은 금지된 이벤트가 종결되었다는 것을 외부 인터페이스가 통지 받아야 하는지를 결정하기 위해 구성 설정을 액세스하고(단계 315), 이에 따라 SIM 방화벽은 다른 하나의 이벤트를 검출할 준비가 된다(단계 307).

<58> 다른 실시예에서, SIM 방화벽은 이벤트가 종결되었거나(단계 313) 허용되었는지에(단계 311) 대한 표시를 네트워크에 송신할 수 있다. 송신은 SMS 메시지, USSD, BIP, HTTP/HTTPS, GPRS, TCP/IP, UDP 또는 다른 통신 기술 중 하나 이상을 사용할 수 있다.

<59> 특정 실시예에서, 그 후 네트워크 또는 무선 디바이스는 개인, 무선 디바이스, 컴퓨터, 서버, 또는 이벤트가 검출되었고/되었거나 종결된 임의의 다른 전자 시스템에 통지를 송신할 수 있다. 네트워크 또는 무선 디바이스는 전자 메일, SMS, EMS, MMS, 즉석 메시지, 음성 콜, 비디오 콜, VOIP 콜, PTT 콜 또는 대화식 음성 응답(IVR)을 사용하는 음성 콜, 음성 확장성 마크업 언어(VXML)와 문자 대 음성(TTS) 기술, HTTP/S, TCP/IP, UDP, 확장성 마크업 언어(XML) 또는 다른 통신 기술을 사용하여 통지를 송신할 수 있다. 예를 들면, 네트워크는 주어진 전화 번호로부터의 콜이 자녀의 전화에 도달되는 것으로부터 차단되었다는 것을 부모의 이메일 주소에 이메일 통지를 송신할 수 있다. 또는, 예를 들면, 무선 디바이스는 디바이스의 사용자가 주어진 지역 코드로 전화를 거는 것으로부터 차단되었다는 것을 회사의 회계 관리자에 의해 액세스될 수 있는 로그에 통지를 송신할 수 있다. 또는 예를 들면, 무선 디바이스는 주어진 인터넷 사이트 또는 IP 주소가 자녀의 모바일 전화에 의해 액세스되고 있다는 것을 부모의 모바일 디바이스에 문자 메시지로 송신할 수 있다.

<60> 이제 도 4를 참조하면, 원격 관리 이벤트를 처리하기 위한 SIM 방화벽에 의해 수행되는 방법의 일 실시예를 묘사하는 흐름도가 도시된다. 간단한 개요에서, 이 방법은 네트워크로부터 원격 관리 이벤트를 수신하는 단계(407)를 포함한다. 원격 관리 이벤트는 SIM 방화벽에게 중지하라고 지시하는 단계(단계 409); SIM 방화벽에게 재시작할 것을 지시하는 단계; SIM 방화벽의 구성 설정을 수정하는 단계(단계 411); SIM 방화벽의 수정된 구성 설정을 저장하는 단계(413); SIM 방화벽의 실행가능 파일과 라이브러리(415)를 수정하는 단계; SIM 방화벽의 수정된 실행가능 파일과 라이브러리(417)를 저장하는 단계; 및 SIM 방화벽을 재시작하는 단계(419) 중 하나 이상을 포함할 수 있다.

<61> 다른 실시예에서 SIM 방화벽은 로컬 관리 이벤트를 처리하기 위한 위에서 설명된 방법을 수행할 수 있다. 이 방법은 여기서 설명된 실시예들 중 임의의 하나에 따라 수행될 수 있다. 여전히 다른 실시예에서, 원격 관리 이벤트는, 무선 디바이스상의 애플리케이션, 또는 무선 디바이스의 운영 체제에 의해 수신되고 그리고 일부 경우에 수정되어 SIM 방화벽 또는 SIM에 전송될 수 있다.

<62> 여전히 도 4를 참조하면, 이제 더 상세히, 도시된 실시예에서 SIM 방화벽은 네트워크로부터 원격 관리 이벤트를 수신한다(단계 407). 이 단계는 여기서 설명된 실시예들 중 임의의 하나에 따라 수행될 수 있다.

<63> 도시된 실시예에서, SIM 방화벽은 SIM 방화벽이 실행되는 것을 중지시키기 위한 지령을 포함하는 원격 관리 이벤트를 수신할 수 있다(단계 409). 실행을 중지시키는 지령은 실행을 영구적으로 중지시키기 위한 지령; SIM 방화벽이 재시작할 시점에서 무선 디바이스가 전원이 켜질 때까지 실행을 중지시키기 위한 지령, 또는 다시 시작하라고 지시될 때까지 실행하는 것을 중지시키기 위한 지령을 포함할 수 있다. 상기 지령을 수신하면, SIM 방화벽은 이에 따라서 실행하는 것을 중지한다.

<64> 도시된 실시예에서, SIM 방화벽, 또는 SIM 운영 체제는 구성 설정을 수정하기 위한 지령을 포함하는 원격 관리 이벤트를 수신할 수 있다(단계 411). 구성 설정을 수정하기 위한 지령은 새로운 구성 설정을 가지고 기존의 구성 설정을 겹쳐 쓰거나 기존 구성 설정을 삭제하고 이것을 새로운 구성 설정 데이터로 대체시키기 위한 지령과 데이터를 포함할 수 있다.

<65> 도시된 실시예에서, SIM 방화벽, 또는 SIM 운영 체제는 그리고 나서 SIM, 또는 무선 디바이스 상의 영속(persistent) 저장 디바이스에 새로운 구성 설정을 저장한다(단계 413). SIM 방화벽은 즉시로 새로운 구성 설정을 사용할 수 있거나, 재시작하고(단계 419) 구성 설정을 판독한다.

<66> 도시된 실시예에서, SIM 방화벽, 또는 SIM 운영 체제는 SIM 방화벽 애플리케이션의 라이브러리와 파일을 수정하기 위한 지령을 포함하는 원격 관리 이벤트를 수신할 수 있다(단계 415). SIM 방화벽의 라이브러리와 파일을 수정하기 위한 지령은 라이브러리와 파일을 삭제하고, 이것을 새로운 라이브러리와 파일로 대체시키거나 라이브러리와 파일을 새로운 라이브러리와 파일로 겹쳐 쓰기 위해 필요한 지령과 데이터를 포함할 수 있다. 다른 실시예에서 SIM 파일의 라이브러리와 파일을 수정하기 위한 지령은 네트워크상의 위치로부터 새로운 라이브러리와 파일을 다운로딩하기 위한 지령을 포함할 수 있다.

<67> SIM 방화벽, 또는 SIM 운영 체제는 그리고 나서 SIM 또는 무선 디바이스상의 영속 저장 디바이스에 파일과 라이브러리를 저장한다(단계 417). SIM 방화벽은 그리고 나서 즉시로 새로운 라이브러리와 파일을 사용하거나 새로운 라이브러리와 파일을 사용하기 위해 재시작할 수 있다(단계 419).

<68> 특정 실시예에서, 개인, 무선 디바이스, 컴퓨터 또는 전자 시스템은 SIM 방화벽의 구성 설정을 원격으로 설정하기 위해 설명된 방법을 사용할 수 있다. 일 실시예에서, 인터넷 웹 브라우저를 사용하는 개인은 인가된 사용자가 SIM 방화벽의 구성 설정을 수정하도록 허용하는 웹사이트에 연결된다. 웹사이트는 그리고 나서 네트워크에 연결되고, 구성 설정을 SIM 방화벽에 송신한다. 네트워크는 그리고 나서 이벤트가 종결되었거나 허용되었다는 통지를 웹사이트, 또는 무선 디바이스 또는 전자 시스템에 송신한다. 다른 실시예에서, 개인은 SMS, MMS, EMS, 즉석 메시징, 무선 애플리케이션 프로토콜(WAP), i-모드, IVR, 또는 다른 통신 기술을 사용해서 구성 설정을 원격으로 설정할 수 있다. 특정 실시예에서, 구성 설정은 IPTV, 대화식 TV, 모바일 웹사이트, 음성 인식 시스템, 또는 음성 자동화 시스템 중 하나 이상을 사용해서 사용자에 의해 원격으로 설정될 수 있다. 특정 실시예에서, 구성 설정은 제2 모바일 디바이스를 사용해서 사용자에 의해 원격으로 설정될 수 있다. 이러한 실시예들 중 하나에서, 구성 설정은 제2 모바일 디바이스로부터 예를 들면 블루투스 연결에 의해 구성될 디바이스로 직접적으로 송신될 수 있다.

<69> 예를 들면, 자녀를 위해 모바일 폰을 최근에 구입한 부모는 이 전화기가 전화를 걸 수 있거나 콜을 수신할 수 있는 번호와 임의의 다른 방화벽 설정을 부모가 지정하는 것을 허용하는 웹사이트로 로그인할 수 있다. 그리고 나서 이 웹사이트는 구성된 설정을 자녀의 전화기에 송신할 수 있으며, 이 전화기에서 이 설정이 활성화될 것이다. 또는, 예를 들면, 회사는 회사 고용인들에 분배된 복수의 디바이스를 구성하기 위해 웹사이트를 사용할 수 있다. 관리자는 디바이스에 의해 사용될 수 있는 최대 분 길이(number of minutes)를 설정하기 위해 웹사이트를 액세스할 수 있다. 그리고 나서 웹사이트는 이 회사에 의해 지정된 모든 디바이스에 구성된 설정을 송신할 수 있다.

<70>

산업상 이용 가능성

<71> 본 발명은 가입자 식별 모듈을 이용하기 위한 무선 디바이스와, 이러한 디바이스 상에서 유입 및 유출 통신, 데이터와 이벤트를 필터링하고 조절하기 위한 수단에 이용가능하다.

도면의 간단한 설명

<13> 도 1a는 네트워크에 연결된 SIM 기반 방화벽을 통합하는 무선 디바이스의 일 실시예를 묘사하는 블록도.

<14> 도 1b는 네트워크의 일 실시예를 묘사하는 블록도.

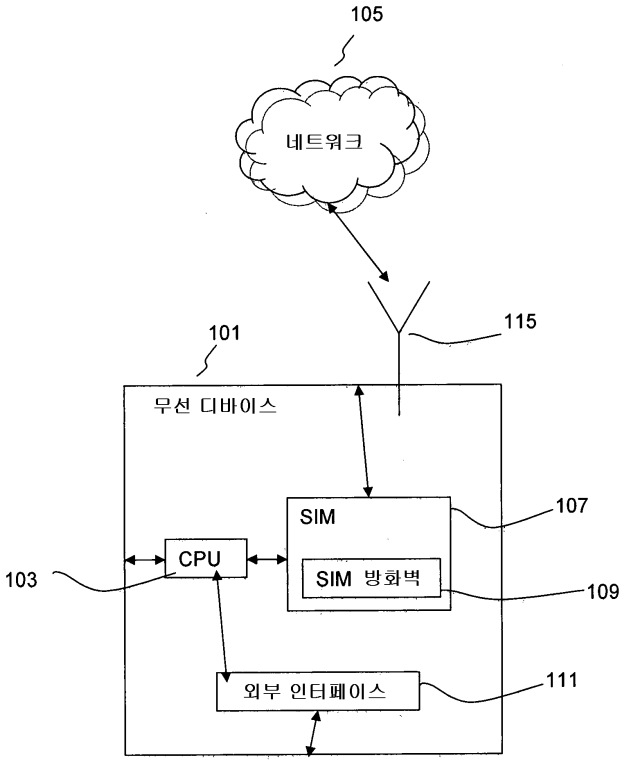
<15> 도 2a와 도 2b는 SIM 기반 방화벽에 의해 처리되는 이벤트의 다양한 실시예를 묘사하는 흐름도.

<16> 도 3은 이벤트를 필터링하기 위한 SIM 기반 방화벽에 의해 수행되는 방법의 일 실시예를 묘사하는 흐름도.

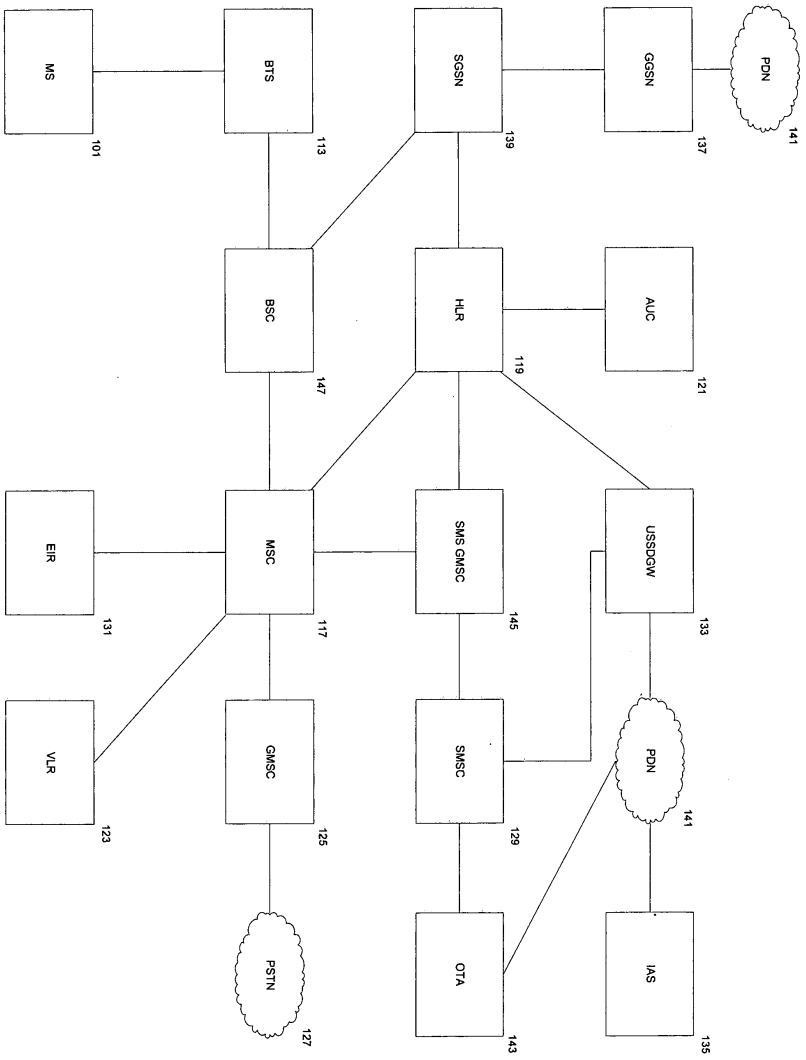
<17> 도 4는 SIM 기반 방화벽을 원격으로 관리하기 위한 일 실시예를 묘사하는 흐름도.

도면

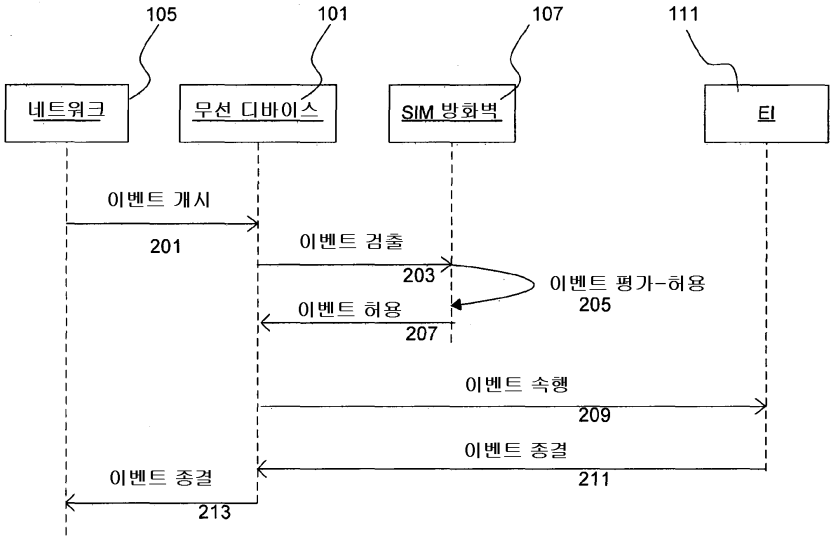
도면1a


105
네트워크
115
101
무선 디바이스
SIM
107
CPU
103
SIM 방화벽
109
외부 인터페이스
111

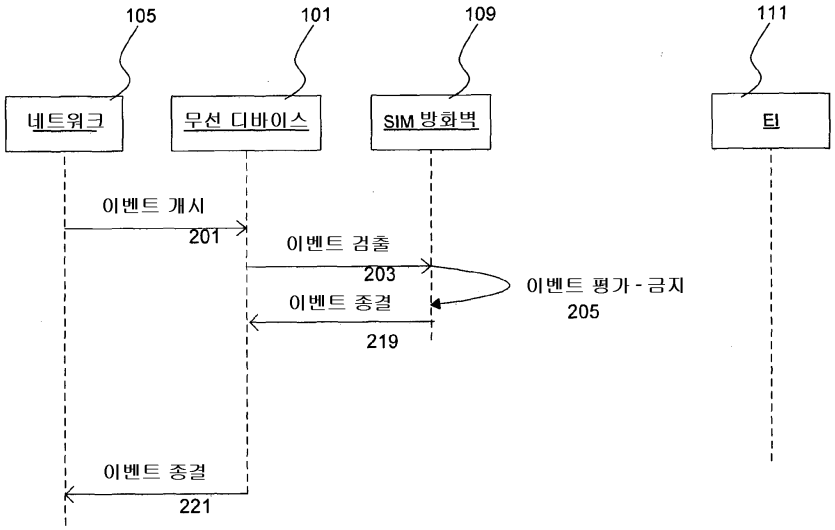
도면1b


MS
101
BTS
113
SGSN
139
GGSN
137
PDN
141
BSC
147
HLR
119
AUC
121
EIR
131
MSC
117
SMS GMSC
145
USSDGW
133
VLR
123
GMSC
125
SMSC
129
PDN
141
PSTN
127
OTA
143
IAS
135

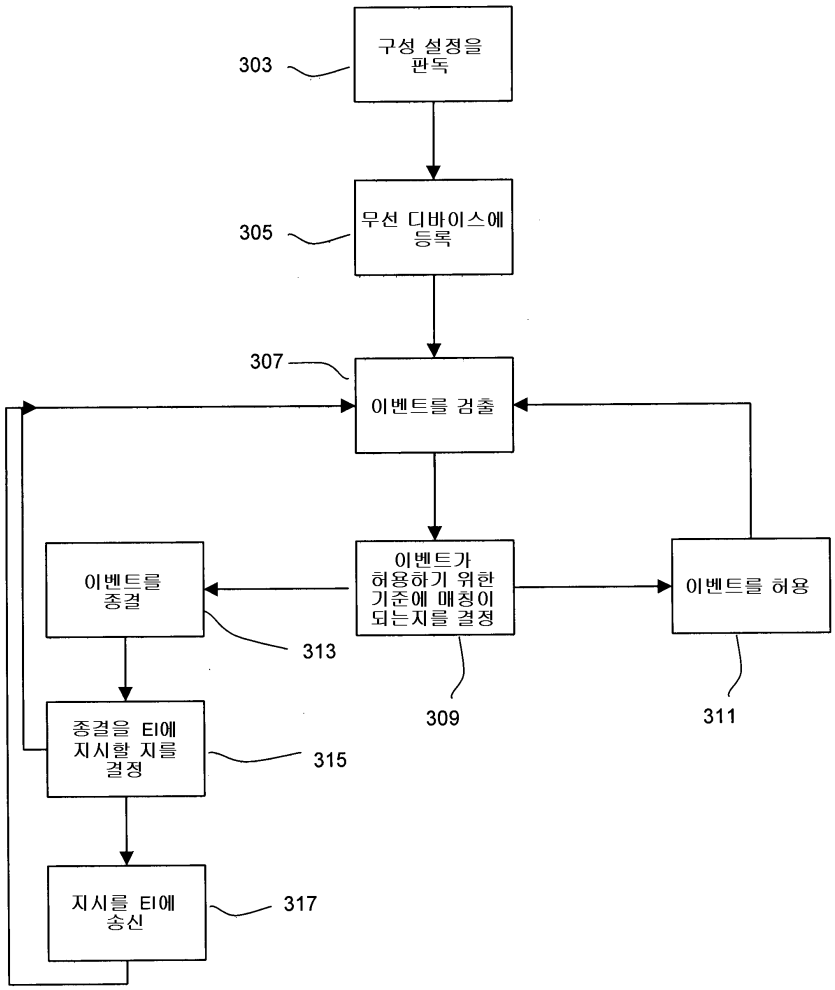
도면2a


105
101
107
111
네트워크
무선 디바이스
SIM 방화벽
EI
이벤트 개시
201
이벤트 검출
203
이벤트 평가-허용
205
이벤트 허용
207
이벤트 속행
209
이벤트 종결
211
이벤트 종결
213

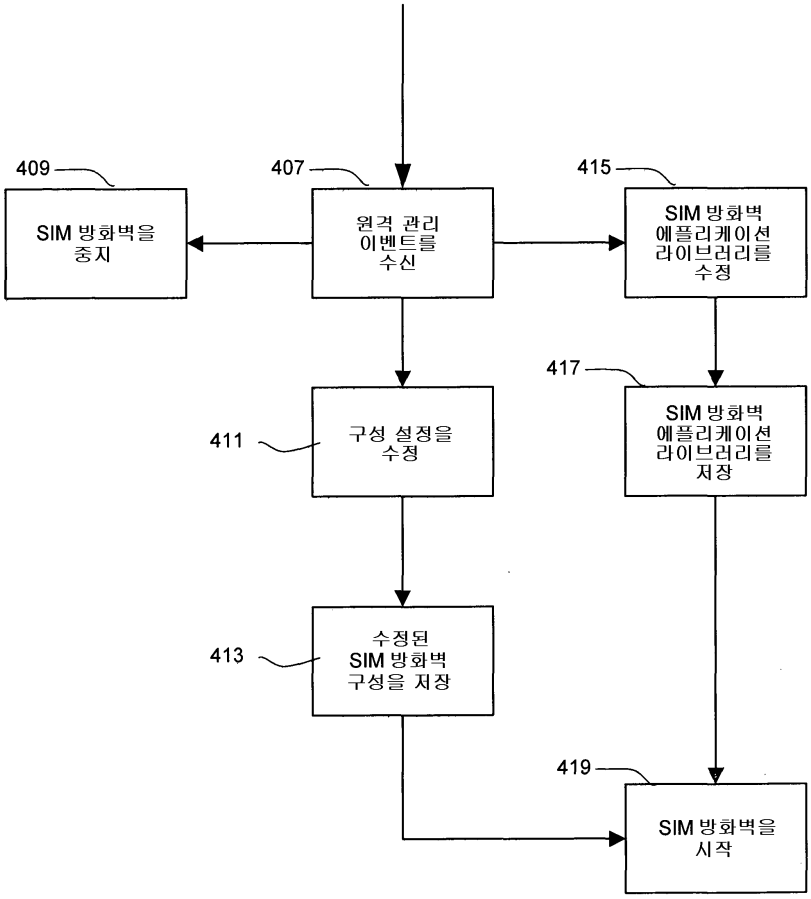
도면2b


105
101
109
111
네트워크
무선 디바이스
SIM 방화벽
EI
이벤트 개시
201
이벤트 검출
203
이벤트 평가 - 금지
205
이벤트 종결
219
이벤트 종결
221

도면3


구성 설정을 판독
303
무선 디바이스에 등록
305
307
이벤트를 검출
이벤트를 종결
313
이벤트가 허용하기 위한 기준에 매칭이 되는지를 결정
309
이벤트를 허용
311
종결을 티에 지시할 지를 결정
315
지시를 티에 송신
317

도면4


409
SIM 방화벽을 중지
407
원격 관리 이벤트를 수신
415
SIM 방화벽 에플리케이션 라이브러리를 수정
417
SIM 방화벽 에플리케이션 라이브러리를 저장
411
구성 설정을 수정
413
수정된 SIM 방화벽 구성을 저장
419
SIM 방화벽을 시작