(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 712 700**

(51) Int. CI.:

H04W 12/12 (2009.01)
H04L 29/06 (2006.01)
H04W 52/04 (2009.01)
H04W 88/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.06.2007 E 07110159 (6)**

(97) Fecha y número de publicación de la concesión europea: **28.11.2018 EP 2003818**

(54) Título: **Un detector de hombre-en-el-medio y un método que lo usa**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.05.2019

(73) Titular/es:

EXFO OY (100.0%)
Elektroniikkatie 2
90570 Oulu, FI

(72) Inventor/es:

LOTVONEN, JUKKA;
KUMPULA, JUHA;
AHOKONGAS, MARKUS y
PAUNA, JANNE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Un detector de hombre-en-el-medio y un método que lo usa

Campo de la invención

La invención se relaciona con un método de detección de ataques de intrusión de un atacante fraudulento. La invención se relaciona también con un aparato detector y software de hombre-en-el-medio (man-in-the-middle) que es utilizado en el método.

Antecedentes de la invención

Estaciones base (BS) fraudulentas pueden ser usadas en redes inalámbricas para capturar identidades de terminales móviles, para ubicar terminales móviles y espiar comunicaciones de los terminales móviles. En redes GSM (Sistema Global para comunicaciones Móviles) realizar ataques de hombre-en-el-medio (man-in-the-middle) es posible porque las estaciones base de la red GSM no se autentican a sí mismas a través de los terminales móviles a los que sirven. Este fenómeno proporciona una posibilidad para que una estación base fraudulenta tome el control de uno o más terminales móviles. Cuando un terminal móvil ha aceptado una BS fraudulenta como su estación base servidora la estación base fraudulenta puede por ejemplo ordenar al terminal móvil engañado desactivar su cifrado GSM. Cuando el terminal móvil hace una llamada, la estación base fraudulenta puede reenrutar la llamada a una estación base de la red autentica y transportar la voz/datos del terminal móvil a la red móvil auténtica. Por lo tanto el terminal móvil no descubre que la estación base fraudulenta le está engañando.

La publicación de EE.UU. 2006/0197702 sugiere una solución al problema del hombre-en-el-medio (man-in-the-middle) en un caso donde un terminal móvil es estacionario. Según la publicación en ese caso no existe la necesidad de hacer traspasos. Sin embargo, si la estación base fraudulenta causa un traspaso el terminal móvil puede detectar que la potencia que recibe aumenta y/o la dirección de la transmisión cambia. Estos cambios son usados como una máscara de un ataque de hombre-en-el-medio (man-in-the-middle). Sin embargo esta solución solo es usable en un caso estacionario.

El caso de una estación móvil que se mueve es más complicado. Porque el terminal móvil está en movimiento, la potencia que recibe y/o dirección de transmisión de la estación base servidora cambia. Por lo tanto la solución sugerida en el documento de EE.UU 2006/0197702 puede dar alertas incorrectas.

Varias otras publicaciones describen cómo las estaciones base fraudulentas pueden ser detectadas en redes WLAN. La publicación de EE.UU 2004/0023640 describe un sistema donde mediciones de terminales móviles o puntos de acceso pueden ser usados en un punto de acceso especial para detectar un punto de acceso o estación base fraudulenta. Sin embargo la estación móvil no puede por sí misma detectar que un punto de acceso, que ha sido medido, es ilegal.

En el documento de EE.UU. 2003/02325989 se describe cómo un servidor maestro en una red WLAN puede determinar si el punto de acceso en la red WLAN está ubicado en una ubicación geográfica desconocida. En las mediciones el servidor maestro usa mediciones de intensidad de la señal de estaciones pertenecientes a la WLAN. Si la ubicación determinada no es correcta el servidor maestro define ese punto de acceso ilegal.

En el documento EP 1763178 un terminal móvil envía sus resultados de mediciones acerca de puntos de acceso en recepción a un controlador en la red central móvil. El controlador determina si algún punto de acceso es un punto de acceso permitido o ilegal.

En el documento de EE.UU. 2005/0060576 es descrito un sistema que incluye un gestor de seguridad especial. El gestor de seguridad inspecciona el tráfico de la red y puede detectar direcciones de red ilegales que pueden pertenecer a puntos de acceso fraudulentos o dispositivos de clientes no autorizados.

En el documento WO 2007/054834 una estación móvil reporta a un punto de acceso servidor la intensidad de señal recibida de todos los puntos de acceso en el área por la que viaja. El punto de acceso servidor puede detectar un punto de acceso fraudulento en base a las inconsistencias en los reportes de intensidad de señal durante un traspaso.

En el documento de EE.UU. 2006/0276173 es descrito un sistema de seguridad a ser usado en una red de acceso por radio (RAN). En el sistema de seguridad descrito tanto un controlador de estación base como una radio móvil pueden incluir medios para monitorizar y notificar procesos internos detectados anormalmente específicos para detectar una o más anormalidades en la radio móvil tal como un incremento del uso de la CPU, almacenamiento de memoria, lectura-escritura de memoria, mensajes de entrada o salida maliciosos, y nombres de archivos de viruses. La RAN puede después de detectar la anormalidad denegar el acceso por radio móvil, dar un acceso condicional o acceso limitado en base a la anormalidad específica detectada. El sistema descrito protege el sistema de la RAN central y puede evitar que abonados móviles (MS) infectados sobrecarguen los recursos del sistema de la RAN mediante la monitorización del comportamiento y búsqueda de patrones específicos de la radio móvil.

Las estaciones base fraudulentas usan características del procedimiento de reselección de red para hacer que los terminales móviles campen en la estación base fraudulenta. En terminales móviles de redes GSM son medidas de manera periódica la calidad de recepción de estaciones base vecinas y la estación base servidora. Cuando la calidad de recepción de una estación base vecina excede la calidad de la estación base servidora, la estación base vecina es seleccionada como una estación base servidora según el procedimiento de reselección de red. Una estación base fraudulenta se hace pasar por una célula vecina, y mediante el uso de alta potencia de transmisión y la modificación de parámetros de selección de red difundidos en los mensajes de información del sistema la estación base fraudulenta se vuelve un destino tentador para la reselección de célula. Después de eso, los terminales móviles en el área de la célula fraudulenta seleccionarán la estación base fraudulenta como una célula servidora.

Un grupo de células de la red celular pueden ser agrupadas en un área de ubicación. Todas las células de la misma ubicación son enviadas en el canal de difusión uno y el mismo código de área de ubicación (código LAC). Normalmente una estación base fraudulenta usa un código LAC diferente de el de la célula servidora para iniciar a los terminales móviles el procedimiento de actualización de ubicación. Si los terminales móviles intentan reseleccionar la estación base fraudulenta, puede capturar identidades de terminales móviles cercanos.

Un terminal móvil de un sistema de radio celular siempre intenta seleccionar una cierta estación base y acampar dentro de su área de cobertura. Tradicionalmente la reselección de célula está basada en mediciones de intensidad de la señal de radio recibida, bien en la estación base o en el terminal móvil. Por ejemplo, en el sistema GSM cada estación base transmite una señal en la así llamada frecuencia baliza que es diferente para estaciones base vecinas. En el sistema GSM una estación base transmite en el así llamado canal BCCH (Canal de Control de Difusión) los parámetros p1 y p2 hacia el terminal móvil, por lo cual esos parámetros son usados para calcular los así llamados valores C. Por ejemplo, el valor C1 comúnmente usado en la red GSM celular es calculado a partir de la ecuación a continuación:

$$C1 := (A - \text{Max.}(B, 0)),$$

donde

- A:= nivel promedio de la señal recibida – p1 (dB)

- B:= p2 – potencia de transmisión máxima del terminal (dB)

- p1:= valor mínimo permitido para la señal recibida

- p2 := potencia de transmisión máxima permitida para un terminal

Los terminales deben medir los niveles de recepción en las señales de difusión de todas las estaciones base que pueden recibir para que puedan ser capaces de calcular el valor C1 de cada célula recibida. La célula que tenga el valor C1 calculado más alto es la más ventajosa al respecto de la conexión de radio. Para optimizar la reselección de célula la red puede también transmitir parámetros adicionales que permitan el uso de los así llamados valores C2. Una descripción más detallada es presentada por ejemplo en el documento ETSI 05.08 versión 6.4.0. Una estación base fraudulenta intenta usar este fenómeno de reselección de célula.

Las estaciones base transmiten a los terminales móviles información sobre las frecuencias del BCCH usadas por las células vecinas, para que los terminales sepan en qué frecuencias deben escuchar para encontrar las transmisiones del BCCH de las células vecinas.

La Fig. 1 muestra un ejemplo de un ataque contra un terminal 150 móvil que es posible en los sistemas celulares de la técnica anterior. Hay tres células servidoras auténticas en la red 10: célula A 110, célula B 120 y célula C 130. Todas pueden pertenecer a la misma área de ubicación y por lo tanto envían el mismo código LAC en los canales de difusión. El terminal 150 móvil recibe las señales 111, 121 y 131 de difusión desde estas células en consecuencia. En el ejemplo descrito de la Fig. 1 la célula A 110 es la célula servidora al terminal 150 móvil.

Una estación 101 base fraudulenta intenta reclutar al terminal 150 móvil. Usa alta potencia de transmisión en sus transmisiones 102 del BCCH comparada con la transmisión de las estaciones base de las células auténticas. La estación base fraudulenta más probablemente usa un código LAC en su transmisión que difiere de los códigos LAC de las estaciones base cercanas auténticas de la red 10 celular. La estación base puede establecer una o más conexiones 103 por ejemplo con la estación base auténtica de la célula A 110. La estación base de la célula A 110 ve la estación 101 base fraudulenta como un terminal o terminales móviles normales. Por lo tanto la estación A 110 base auténtica no excluye la estación 101 base fraudulenta en su operación.

Por lo tanto, existe una necesidad de un método y aparato mediante los cuales un hombre-en-el-medio (man-in-the-middle) puede ser detectado en casos estacionarios o en movimiento de un terminal móvil.

Compendio

Un objeto de la presente invención es proporcionar un nuevo método y un aparato que use el método para detectar una estación base fraudulenta en una red celular.

Los objetos de la invención se logran mediante un método y un aparato móvil que pueden detectar anomalías tanto en transmisiones que se originan desde la estación base fraudulenta como la ubicación de la estación base fraudulenta.

Más desarrollos de la invención son materia de las reivindicaciones dependientes.

Una ventaja de la invención es que aumenta la seguridad de un sistema de comunicación móvil.

Otra ventaja de la invención es que puede ser integrada como una parte de un terminal móvil.

Otra ventaja más de la invención es que la estación base fraudulenta puede ser encontrada aun si el terminal móvil está en movimiento.

La idea de la presente invención es básicamente como sigue: Hay un terminal móvil al que se le proporciona software que tiene un acceso a los parámetros de mediciones de la red recibidos. El terminal móvil comprende software mediante el cual todos los tipos de anomalías en las transmisiones de señalización de las estaciones base cercanas pueden ser analizadas y detectadas. Las anomalías pueden ser por ejemplo anomalías en transmisiones del BCCH como que un código LAC de una estación base difiera substancialmente del código LAC de otras células, potencia de transmisión sorprendentemente alta, id de célula desconocido, diferentes frecuencias de actualización de ubicación periódica, diferentes valores de C1 o C2 y anomalías en mensajes de señalización como horas de red erróneas, diferente código de causa en terminaciones de actualizaciones de ubicación, mensaje de aviso incorrecto, mensaje de aviso con IMSI (Identidad de Abonado Móvil Internacional) o alguna combinación de los anteriores. Una anomalía puede también ser una ubicación geográfica de la estación base fraudulenta que no está incluida en una lista de posibles ubicaciones de las estaciones base pertenecientes a la red celular servidora.

En una realización ventajosa los parámetros de red usados en estaciones base de red auténticas son configurados y guardados en una memoria del aparato de medición anterior antes de la detección anómala. Estos parámetros pueden también incluir posiciones y áreas de cobertura de las estaciones base auténticas. Estos parámetros son ventajosamente grabados y pueden ser visualizados mediante el uso de una pantalla de mapa o importados de un sistema GIS (Sistema de Información Gráfica). Cualquier anomalía puede entonces ser detectada mediante la comparación de los parámetros recibidos de las estaciones base con los parámetros de la estación base de referencia configurada.

En otra solución los parámetros de red de las estaciones base son almacenados por adelantado en una base de datos con información de posición. Los parámetros de red grabados pueden ser usados más tarde para hacer detección de anomalías sin una necesidad de escanear todas las estaciones base. Los parámetros de red grabados pueden ser también usados para detectar nuevas células que usan parámetros de red normales o uso de un nivel de potencia más alto que antes.

Las anomalías encontradas pueden de manera ventajosa ser usadas para dar una alerta al usuario del terminal móvil. El usuario puede de manera opcional bien acampar o quedarse fuera de la estación base fraudulenta. En ambos casos el terminal móvil según la invención puede tomar una portadora para ubicar la estación base fraudulenta.

Breve descripción de los dibujos

Más alcance de aplicabilidad de la presente invención será aparente a partir de la descripción detallada dada en adelante. Sin embargo, se debería comprender que la descripción detallada y ejemplos específicos, mientras que indican realizaciones ventajosas de la invención, se dan solo a modo de ilustración, dado que varios cambios y modificaciones dentro del espíritu y alcance de la invención serán aparentes para los expertos en la técnica a partir de esta descripción detallada. Las referencias se hacen a los dibujos que acompaña en los cuales:

La Fig. 1 muestra un ejemplo de una red de telecomunicación de una técnica anterior donde una estación base fraudulenta está transmitiendo;

la Fig. 2a muestra como un ejemplo una realización del aparato de medición del hombre-en-el-medio (man-in-the-middle) según la invención;

la Fig. 2b muestra como un ejemplo bloques funcionales principales de una implementación en software del detector del hombre-en-el-medio (man-in-the-middle) según la invención;

la Fig. 3a muestra como un ejemplar un diagrama de flujo una realización ventajosa del método según la invención;

la Fig. 3b muestra como un ejemplar un diagrama de flujo una segunda realización ventajosa del método según la invención; y

la Fig. 3c muestra como un ejemplar un diagrama de flujo una tercera realización ventajosa del método según la invención.

Descripción detallada

La Fig. 1 fue discutida en conjunto con la descripción de la técnica anterior.

La Fig. 2a ilustra un ejemplo de un aparato 20 de medición según la invención. El aparato 20 de medición puede usarse en un sistema de medición que puede ser usado para encontrar una estación 101 base fraudulenta. El aparato 20 de medición comprende ventajosamente una unidad de procesamiento que puede ser por ejemplo un PC 203. El aparato 20 de medición además comprende un terminal 202 móvil y de manera opcional también un dispositivo 201 de ubicación de GPS. El dispositivo 201 de ubicación de GSPS puede ser usado en mediciones de ubicación del aparato de medición. El aparato de medición puede también comprender un sistema 204 de antena direccional que puede ser usado cuando se toma una portadora de la estación 101 base fraudulenta.

El terminal 202 móvil incluido en el aparato 20 de medición comprende ventajosamente una unidad de procesador, memoria, transmisor y receptor mediante el cual es capaz de transmitir y recibir mensajes en una célula servidora. El terminal 202 móvil puede recibir transmisiones de señalización de células servidoras y vecinas. La transmisión recibida puede ser por ejemplo una transmisión del BCCH, mensajes de aviso con IMSI (Identidad de Abonado Móvil Internacional) o mensajes de rechazo de actualización de ubicación. La dirección de la estación base fraudulenta puede ser encontrada sin acampar en la estación base fraudulenta mediante el uso de las mediciones de células vecinas disponibles.

En una solución ventajosa el software de medición según la invención se ejecuta en el PC 203 del aparato 20 de medición. El software busca anomalías de las transmisiones recibidas de las células servidora y vecinas. Las anomalías buscadas pueden comprender por ejemplo anomalías en las transmisiones del BCCH como un código LAC de una célula que difiera substancialmente del código LAC de las otras células, potencia de transmisión alta, id de célula desconocido, diferentes frecuencias de actualización de ubicación periódica, diferentes valores de C1 o C2 y anomalías en secuencias de comunicación como horas de red erróneas, diferente código de causa en terminaciones de actualizaciones de ubicación, mensaje de aviso incorrecto, mensaje de aviso con IMSI o alguna combinación de las anteriores.

El PC 203 comprende ventajosamente también un elemento de presentación y un altavoz para dar una alerta cuando una estación 101 base fraudulenta ha sido detectada. La alerta puede ser dada por ejemplo mediante la reproducción de un sonido de alerta, vibración, luces que parpadean o presentando alerta en una pantalla del aparato 20 de medición.

La antena 204 direccional puede de manera ventajosa conectarse a la estación 202 móvil del aparato 20 de medición. Cuando una estación 101 base fraudulenta es detectada una portadora de la transmisión 210 puede ser tomada mediante el giro de la antena 204 direccional. La estación 101 base fraudulenta está en una dirección desde donde la estación 202 móvil del aparato 20 de medición recibe un nivel de recepción máximo. Cuando la portadora de la estación 101 base fraudulenta ha sido tomada una estimación de su distancia desde el aparato 20 de medición puede ser calculada mediante el uso del avance de tiempo que la estación 101 base fraudulenta usa en su transmisión. Si el PC 203 está en una posición para recuperar una aplicación de mapa electrónico puede mostrar un lugar estimado de la estación 101 base fraudulenta en el mapa.

En otra realización ventajosa el software de medición según la invención se ejecuta en un terminal móvil convencional de una red celular. El terminal móvil puede también de manera opcional comprender una unidad de GPS para encontrar ubicaciones. Un sistema de antena direccional auxiliar puede conectarse al terminal móvil para tomar una portadora a una estación base fraudulenta. Cuando se sospecha de la estación base fraudulenta, el software según la invención da una alerta por ejemplo mediante la reproducción de un sonido de alerta, vibración, luces que parpadean o presentando alerta en la pantalla del terminal móvil.

Tras la detección de la estación base fraudulenta el terminal móvil puede enviar una alerta vía mensaje SMS (Servicio de Mensajes Cortos) u otros medios de comunicación a un sistema de información definido de antemano. El sistema de información puede de manera ventajosa enviar de vuelta un mapa de los alrededores a la estación móvil. El terminal móvil puede entonces mostrar en su elemento de presentación su posición actual y una ubicación estimada de la estación base fraudulenta detectada.

Las mediciones de ubicaciones del terminal móvil en la red celular servidora pueden ser en base también a medidas triangulares conocidas en la técnica. En las redes GSM avances de tiempo de las estaciones base pueden ser utilizados en las mediciones triangulares. La medición triangular puede por lo tanto reemplazar el uso de una unidad de GPS cuando encuentra una ubicación del terminal móvil.

La Fig. 2b ilustra un ejemplo de bloques funcionales principales de software 22 de medición según la invención. Un bloque 221 de medición de red del software es usado para recibir transmisiones de señalización desde la estación base servidora y estaciones base en el vecindario. Las transmisiones recibidas pueden comprender por ejemplo transmisiones del BCCH, mensajes de aviso o mensajes de rechazo de la actualización de la ubicación.

Un bloque 225 de posicionamiento opcional del software usa datos del receptor GPS o datos del receptor de posicionamiento por satélite equivalente para encontrar la ubicación actual del terminal móvil. La ubicación puede ser calculada de manera alternativa mediante el uso de mediciones triangulares en la red celular servidora.

Un bloque 223 de base de datos del software contiene una base de datos donde los parámetros de la estación base de referencia pueden ser almacenados de antemano. Por ejemplo códigos LAC de células, identificadores de células, valores C2 y códigos de causa usados en los mensajes de rechazo de actualizaciones de ubicación y los mismos recibidos desde las estaciones base reales pueden ser almacenados en ella. También la posición actual del aparato de medición puede ser almacenada en la base de datos.

Un bloque 224 de mapa del software es usado para presentar parámetros de la estación base de referencia y resultados de mediciones reales en una presentación en mapa.

El bloque 222 de detección implementa detección de la estación base fraudulenta. En el primer paso de detección todas las células escuchadas por el aparato de medición son escaneadas. Durante el escaneo el terminal de medición puede hacer una actualización de ubicación en las células para encontrar parámetros intercambiados durante el procedimiento de actualización de ubicación. En el siguiente paso de detección posibles anomalías en los parámetros grabados o en otros mensajes relativos a la movilidad son detectados mediante la comparación de parámetros y mensajes grabados de una estación base fraudulenta con parámetros grabados de otras estaciones base auténticas. Las posibles anomalías a ser buscadas pueden ser por ejemplo código LAC de una célula que difiera substancialmente del código LAC de las otras células, potencia de transmisión alta, id de célula desconocido, diferentes frecuencias de actualización de ubicación periódica, diferentes valores de C1 o C2 y anomalías en secuencias de comunicación como horas de red erróneas, diferente código de causa en terminaciones de actualizaciones de ubicación, mensaje de aviso incorrecto, mensaje de aviso con IMSI o alguna combinación de las anteriores.

En una realización ventajosa de la invención el bloque 222 de detección usa resultados del bloque 225 de posicionamiento para encontrar su ubicación actual. Después de eso puede recuperar parámetros de red dependientes de la ubicación del bloque 223 de base de datos y comparar datos de medición reales del bloque 221 de medición de red contra los datos de referencia recuperados. En un caso donde un cambio de los parámetros de la red pueda ser encontrados el bloque 222 de detección de manera ventajosa genera una alerta.

Un bloque 224 de mapa opcional del software puede recuperar y presentar en un mapa la ubicación actual del terminal móvil. Puede conectar información de la red de referencia con la ubicación medida. El bloque 224 de mapa puede también recuperar resultados de mediciones del BCCH de la base de datos 223 y visualizar esos resultados en el mapa.

Las Figuras 3a, 3b y 3c representan los pasos principales de realizaciones ventajosas del método de detección según la invención.

La Fig. 3a representa un ejemplo donde la transmisión de señalización de las células servidora y vecinas son usadas. La transmisión puede comprender por ejemplo mensajes del BCCH, mensajes de aviso y mensajes de rechazo de actualizaciones de ubicación. Los mensajes recibidos se pueden usar tanto solos como una combinación para detectar una estación base fraudulenta. Puede no existir la necesidad de guardar los parámetros de red por adelantado. En el paso 300 el aparato de medición o un terminal móvil capaz de detectar una estación base fraudulenta inicia una medición según la invención.

En el paso 310 el aparato de medición recibe transmisiones de señalización de la célula servidora y todas las células vecinas. Durante el paso el aparato de medición puede hacer una actualización de ubicación en una célula para encontrar parámetros intercambiados durante el procedimiento de actualización de ubicación. El aparato de medición puede interpretar los mensajes de señalización recibidos.

En el paso 311 el bloque de detección del software busca anomalías entre las transmisiones de diferentes células. Las anomalías buscadas pueden ser por ejemplo un código LAC que difiera substancialmente del código LAC de las otras células, potencia de transmisión alta, id de célula desconocido, diferentes frecuencias de actualización de ubicación periódica, diferentes valores de C1 o C2 y anomalías en secuencias de comunicación como horas de red erróneas, diferente código de causa en terminaciones de actualizaciones de ubicación, mensaje de aviso incorrecto, mensaje de aviso con IMSI o alguna combinación de las anteriores.

En el paso 312 se decide si una anomalía ha sido detectada o no. Si no se encuentran anomalías, entonces en el paso 313 se decide si la búsqueda de anomalías debería continuar o no. Si se decide que la búsqueda continuará, el proceso vuelve al paso 310 donde nuevas transmisiones de las células son recibidas. Si se decide que la búsqueda de estaciones base fraudulentas no necesita continuar, el proceso termina en el paso 317. En esa etapa el software de detección según la invención establece un estado no activo.

Si en el paso 312 una o más anomalías son encontradas entonces en el paso 314 el software de detección levanta una alerta sobre una estación base fraudulenta. La alerta puede ser por ejemplo dar un sonido de alerta, vibración, luces que parpadean o presentando alerta en la pantalla del terminal móvil o aparato de medición.

En el paso 315 se decide si existe una necesidad de ubicar de manera precisa donde está la estación base fraudulenta. Si la ubicación precisa no es necesaria el proceso de detección termina en el paso 317.

Si en el paso 315 se decide ubicar la estación base fraudulenta, entonces en el paso 316 el aparato de detección o terminal móvil toma una portadora a la estación base fraudulenta. Eso puede lograrse mediante el uso de una antena direccional que puede estar conectada al terminal móvil. Tras encontrar la dirección de la transmisión, mediante el uso por ejemplo de un avance de tiempo usado por la estación base fraudulenta una estimación de una distancia a la estación base fraudulenta puede ser calculada. Otro método para estimar la distancia es usar la potencia de transmisión de la estación base fraudulenta.

Después de la operación de ubicación el proceso termina en el paso 317 donde el terminal móvil de manera ventajosa continúa acampando en la estación base fraudulenta para no dar ninguna pista de que la estación base fraudulenta ha sido detectada. De manera alternativa, la estación móvil hace una nueva reselección en una estación base real de la red celular.

La Fig. 3b representa otro ejemplo ventajoso donde transmisión de señalización recibida realmente, por ejemplo mensajes del BCCH de estaciones base y parámetros de red conocidos, son usados para detectar una estación base fraudulenta. Los parámetros de la red reales han sido guardados por adelantado en la memoria del terminal móvil o aparato de medición.

En el paso 300 el aparato de medición o un terminal móvil capaz de detectar una estación base fraudulenta inicia una medición según la invención.

En el paso 302 los parámetros de la red guardados por adelantado son recuperados de la memoria del terminal móvil o aparato de medición.

Después de eso en el paso 320 el aparato de medición recibe transmisiones de señalización de las células, por ejemplo difusiones del BCCH de la célula servidora y todas las células vecinas. Durante el paso el aparato de medición puede hacer una actualización de ubicación en una célula para encontrar parámetros intercambiados durante el procedimiento de actualización de ubicación. El aparato de medición puede interpretar los mensajes de señalización recibidos.

En el paso 321 el bloque de detección del software busca anomalías por ejemplo entre difusiones del BCCH de células diferentes y parámetros de red guardados por adelantado. Las anomalías buscadas pueden ser por ejemplo un código LAC que difiera substancialmente del código LAC de las otras células, potencia de transmisión alta, id de célula desconocido, diferentes frecuencias de actualización de ubicación periódica, diferentes valores de C1 o C2 y anomalías en secuencias de comunicación como horas de red erróneas, diferente código de causa en terminaciones de actualizaciones de ubicación, mensaje de aviso incorrecto, mensaje de aviso con IMSI o alguna combinación de las anteriores.

En el paso 322 se decide si una anomalía ha sido detectada o no. Si no se encuentran anomalías entonces en el paso 323 se decide si la búsqueda de una estación base fraudulenta debería continuar o no. Si se decide que la búsqueda continuará el proceso vuelve al paso 320 donde nuevas difusiones del BCCH son recibidas. Si se decide que la búsqueda de estaciones base fraudulentas no necesita continuar, el proceso termina en el paso 327. En esa etapa el software de detección según la invención establece un estado no activo.

Si en el paso 322 una o más anomalías son encontradas entonces en el paso 324 el software de detección levanta una alerta sobre una estación base fraudulenta. La alerta puede ser por ejemplo dar un sonido de alerta, vibración, luces que parpadean o presentando alerta en la pantalla del terminal móvil o aparato de medición.

En el paso 325 se decide si existe una necesidad de ubicar de manera precisa donde está la estación base fraudulenta. Si la ubicación precisa no es necesaria el proceso de detección termina en el paso 327.

Si en el paso 325 se decide ubicar la estación base fraudulenta, entonces en el paso 326 el aparato de detección o terminal móvil toma una portadora a la estación base fraudulenta. Eso puede lograrse mediante el uso de una antena direccional que puede estar conectada al terminal móvil. Tras encontrar la dirección de la transmisión, mediante el uso por ejemplo de un avance de tiempo usado por la estación base fraudulenta una estimación de una distancia a la estación base fraudulenta puede ser calculada. Otro método para estimar la distancia es usar la potencia de transmisión de la estación base fraudulenta.

Después de la operación de ubicación el proceso termina en el paso 327 donde el terminal móvil de manera ventajosa continúa acampando en la estación base fraudulenta para no dar ninguna pista de que la estación base fraudulenta ha sido detectada. De manera alternativa, la estación móvil hace una nueva reselección en una estación base real de la red celular.

La Fig. 3c representa otro ejemplo ventajoso donde transmisión de señalización recibida de la estación base servidora, por ejemplo mensajes del BCCH, parámetros de red guardados con antelación e información de posición de las estaciones base, son usados para detectar una estación base fraudulenta. Los parámetros de la red e

información de posición de las estaciones base pertenecientes a la red han sido guardados por adelantado en la memoria del terminal móvil o aparato de medición.

En el paso 300 el aparato de medición o un terminal móvil capaz de detectar una estación base fraudulenta inicia una medición según la invención.

En el paso 303 los parámetros de la red guardados por adelantado e información de posición son recuperados de la memoria del terminal móvil o aparato de medición.

Después de eso, en el paso 330 el aparato de medición recibe por ejemplo difusiones del BCCH de la célula servidora y todas las células vecinas. Durante el paso el aparato de medición puede hacer una actualización de ubicación en una célula para encontrar parámetros intercambiados durante el procedimiento de actualización de ubicación. El aparato de medición puede interpretar los mensajes de señalización recibidos.

En el paso 331 el bloque de detección del software busca anomalías entre difusiones del BCCH de células, parámetros de red guardados por adelantado e información de posición. Las anomalías buscadas pueden ser por ejemplo un código LAC que difiera substancialmente del código LAC de las otras células, potencia de transmisión alta, id de célula desconocido, diferentes frecuencias de actualización de ubicación periódica, diferentes valores de C1 o C2 y anomalías en secuencias de comunicación como horas de red erróneas, diferente código de causa en terminaciones de actualizaciones de ubicación, mensaje de aviso incorrecto, mensaje de aviso con IMSI o alguna combinación de las anteriores.

Mediante el uso de su propia medición de ubicación de GPS el terminal móvil puede decidir mediante el uso de la potencia de transmisión o avance de tiempo de la célula servidora y su propia información de ubicación si la célula servidora está ubicada en un lugar geográfico predeterminado, esto es, si es una de las células definidas con antelación.

En el paso 332 se decide si una anomalía ha sido detectada o no. Si no se encuentran anomalías entonces en el paso 333 se decide si la búsqueda de una estación base fraudulenta debería continuar o no. Si se decide por alguna razón que la búsqueda continuará, el proceso vuelve al paso 330 donde nuevas difusiones del BCCH son recibidas. Si se decide que la búsqueda de estaciones base fraudulentas no necesita continuar, el proceso termina en el paso 337. En esa etapa el software de detección según la invención establece un estado no activo.

En el paso 332 se decide si una anomalía ha sido detectada o no. Si en el paso 332 una anomalía es detectada entonces en el paso 334 el software de detección levanta una alerta sobre una estación base fraudulenta. La alerta puede ser por ejemplo dar un sonido de alerta, vibración, luces que parpadean o presentando alerta en una pantalla del aparato de medición. Después de eso un mapa puede ser presentado donde las ubicaciones del terminal móvil y estaciones base reales están posicionadas.

En el paso 335 se decide si existe una necesidad de ubicar de manera más precisa donde está la estación base fraudulenta. Si la ubicación precisa no es necesaria el proceso de detección termina en el paso 337.

Si en el paso 335 se decide ubicar de manera precisa la estación base fraudulenta, entonces en el paso 336 el aparato de detección o terminal móvil toma una portadora a la estación base fraudulenta. Eso puede lograrse mediante el uso de una antena direccional que puede estar conectada al terminal móvil. Tras encontrar la dirección de la transmisión, mediante el uso por ejemplo de un avance de tiempo usado por la estación base fraudulenta una estimación de una distancia a la estación base fraudulenta puede ser calculada. Otro método para estimar la distancia es usar la potencia de transmisión de la estación base fraudulenta. Después de eso un lugar estimado de la estación base fraudulenta puede ser presentado en una presentación de mapa.

Después de la operación de ubicación el proceso termina en el paso 337 donde el terminal móvil de manera ventajosa continúa acampando en la estación base fraudulenta para no dar ninguna pista de que la estación base fraudulenta ha sido detectada. De manera alternativa, la estación móvil hace una nueva reselección en una estación base real de la red celular.

Los bloques funcionales del software de detección representados en la Fig. 2a y pasos del método representados en las figuras 3a-3c pueden ser implementados mediante el uso de un lenguaje de programación adecuado conocido en la técnica. El software de detección es guardado de manera ventajosa en una memoria del terminal móvil, aparato de medición u ordenador personal. Las instrucciones comprendidas en el software de detección son ejecutadas de manera ventajosa en un procesador adecuado incluido en un terminal móvil o aparato de medición. Los resultados de la detección pueden ser presentados en una unidad de presentación incluida en el terminal móvil o aparato de medición.

Algunas realizaciones ventajosas según la invención fueron descritas anteriormente. Sin embargo la invención no se limita a los ejemplos de GSM ventajosos descritos. Varias realizaciones de la invención pueden ser usadas en un número de sistemas celulares diferentes. La idea inventiva puede ser aplicada en numerosas formas dentro del alcance definido por las reivindicaciones adjuntas a este documento.

REIVINDICACIONES

1. Un método para detectar una estación base fraudulenta de una red (10) de telefonía celular, el método que comprende

- un terminal (150, 202) móvil de la red de telefonía celular que recibe mensajes (310, 320, 330) de señalización al menos desde una estación base de una célula (110, 120, 130) de la red (10) de telefonía celular

- el terminal móvil interpreta un mensaje (310, 320, 330) de señalización recibido que se recibe desde una estación (101) base fraudulenta,

- el terminal móvil busca una anomalía (311, 321, 331) mediante la comparación de al menos un parámetro de señalización del mensaje de señalización recibido desde la estación (101) base fraudulenta con un parámetro de señalización de comparación conocido de la red (10) de telefonía celular,

caracterizado en que, el parámetro de señalización de comparación conocido está incluido en el mensaje (310, 320, 330) de señalización recibido desde al menos una de las estaciones base de las células (110, 120, 130) de la red (10) de telefonía celular, y

- el terminal (150, 202) que da una alerta (312, 314, 322, 324, 332, 334) si la comparación da un resultado desigual acerca de al menos un parámetro de señalización.

2. El método según la reivindicación 1, caracterizado en que el parámetro de señalización de comparación ha sido guardado en una memoria del terminal por adelantado de un mensaje de señalización recibido desde al menos una de las estaciones base de las células (110, 120, 130) de la red (10) de telefonía celular.

3. El método según la reivindicación 1 o 2, caracterizado en que un parámetro de señalización usado en la comparación es incluido en un mensaje del canal de control de difusión.

4. El método según la reivindicación 1 o 2, caracterizado en que un parámetro de señalización usado en la comparación es incluido en un mensaje de aviso.

5. El método según la reivindicación 1 o 2, caracterizado en que un parámetro de señalización usado en la comparación es incluido en un mensaje de rechazo de actualización de ubicación.

6. El método según cualquiera de las reivindicaciones 1 a 5, caracterizado en que un parámetro usado en la comparación (311, 321, 331) es uno de los siguientes: un código de área de ubicación, valor C1, valor C2, id de célula, hora de la red, potencia de transmisión, frecuencia de actualización de ubicación periódica, código de causa en la terminación de la actualización de ubicación e identidad de abonado móvil internacional.

7. El método según la reivindicación 1, caracterizado en que tras una alerta dada una portadora es tomada (316, 326, 336) a la estación base fraudulenta para ubicar su posición geográfica.

8. El método según la reivindicación 1, caracterizado en que la red (10) celular es una red GSM.

9. Un terminal (202, 150) de una red (10) de telefonía celular que comprende

- medios para recibir un mensaje (221) de señalización al menos desde una estación base de una célula (110, 120, 130) de una red (10) de telefonía celular,

- medios para interpretar (221) el mensaje de señalización recibido que es recibido desde una estación (101) base fraudulenta, y

- medios para guardar (223) parámetros de señal interpretados, y

- medios para buscar una anomalía (222) en un mensaje de señalización recibido mediante la comparación de al menos un parámetro de señalización del mensaje de señalización recibido desde la estación (101) base fraudulenta con un parámetro de comparación conocido de la red (10) de telefonía celular,

caracterizado en que,

- los medios para interpretar (221) el mensaje de señalización recibido están configurados para usar como el parámetro de señalización de comparación conocido un parámetro que está incluido en el mensaje (310, 320, 330) de señalización recibido desde una de las estaciones base de las células (110, 120, 130) de la red (10) de telefonía celular, y que el terminal (202, 150) además comprende medios para dar una alerta sobre una estación base fraudulenta si la comparación da un resultado desigual acerca de al menos un parámetro de señalización.

10. El terminal (202, 150) móvil según la reivindicación 9, caracterizado en que los medios para buscar una anomalía están configurados para interpretar un parámetro de señalización incluido en un mensaje del canal de control de difusión contra un parámetro de señalización de comparación.

11. El terminal (202, 150) móvil según la reivindicación 9, caracterizado en que los medios para buscar una anomalía están configurados para interpretar un parámetro de señalización incluido en un mensaje de aviso contra un parámetro de señalización de comparación.

12. El terminal (202, 150) móvil según la reivindicación 9, caracterizado en que los medios para buscar una anomalía están configurados para interpretar un parámetro de señalización incluido en un mensaje de rechazo de actualización de ubicación contra un parámetro de señalización de comparación.

13. El terminal (202, 150) móvil según cualquiera de las reivindicaciones 9 a 12, caracterizado en que caracterizado en que un parámetro usado en la comparación es uno de los siguientes: un código de área de ubicación, valor C1, valor C2, id de célula, hora de la red, potencia de transmisión, frecuencia de actualización de ubicación periódica, código de causa en la terminación de la actualización de ubicación e identidad de abonado móvil internacional.

14. El terminal (202, 150) móvil según la reivindicación 9, caracterizado en que el terminal móvil además comprende medios para hacer mediciones (201) de ubicación los resultados de las cuales son configuradas para ser usadas como un parámetro de comparación adicional en la búsqueda de anomalías.

15. El terminal (202, 150) móvil según la reivindicación 14, caracterizado en que el terminal móvil además comprende medios para recuperar y mostrar una ubicación del aparato (202, 150) móvil y estaciones base de la red (10) celular servidora en una presentación de mapa.

16. El terminal (202, 150) móvil según cualquiera de las reivindicaciones 9 a 15 caracterizado en que el terminal móvil además comprende medios para tomar una portadora (204) hacia una estación (101) base fraudulenta detectada.

17. El terminal (202, 150) móvil según la reivindicación 16, caracterizado en que el terminal móvil además comprende medios para estimar una distancia (204) a la estación (101) base fraudulenta bien mediante el uso de un avance de tiempo o de la potencia de transmisión de la estación base fraudulenta.

18. El terminal (202, 150) móvil según la reivindicación 17, caracterizado en que es un terminal (202, 150) de una red (10) GSM.

19. El terminal (202, 150) móvil según cualquiera de las reivindicaciones 9-18, caracterizado en que el terminal (202, 150) móvil está incrustado en un aparato (20) de detección móvil que está configurado para dar una alerta sobre la estación (101) base fraudulenta detectada.

20. Un producto (22) de programa informático que comprende medios de código de programa almacenados en un medio legible por un ordenador, los medios de código de programa están adaptados para realizar cualquiera de los pasos de las reivindicaciones 1 a 6 cuando el programa es ejecutado en un procesador (203).

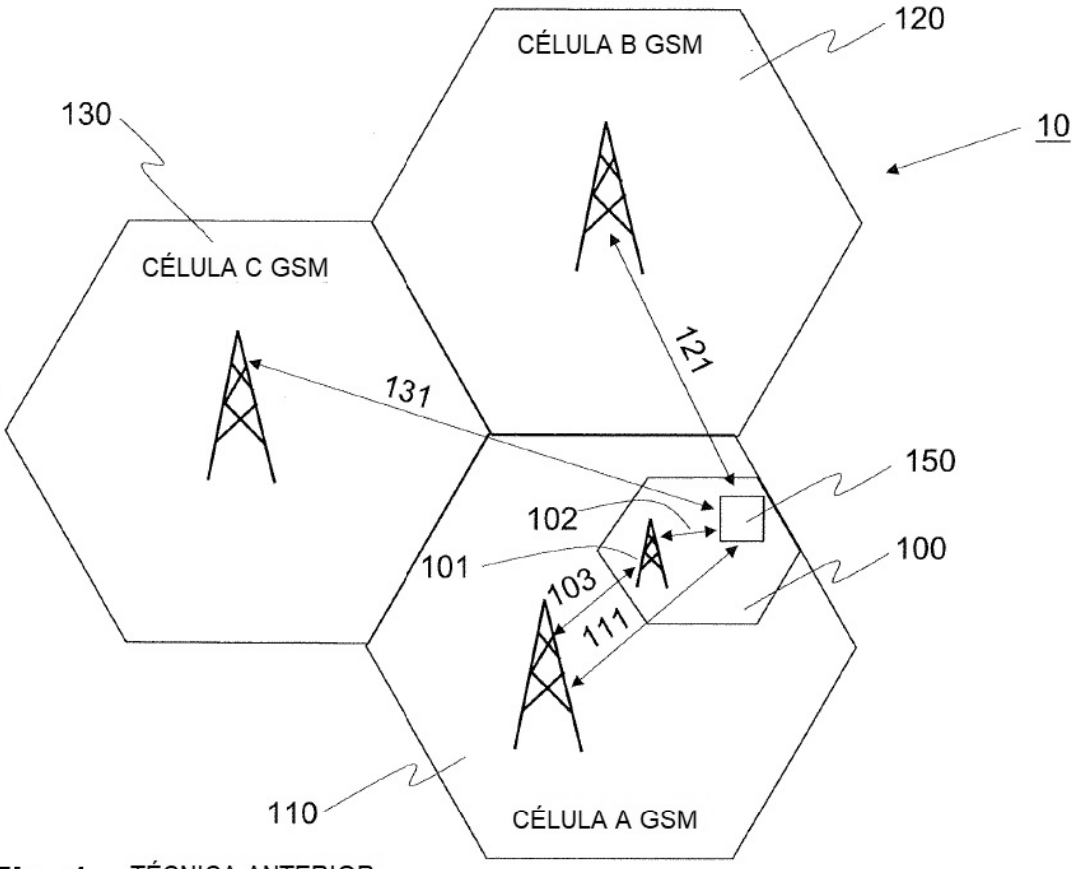

Fig. 1a TÉCNICA ANTERIOR

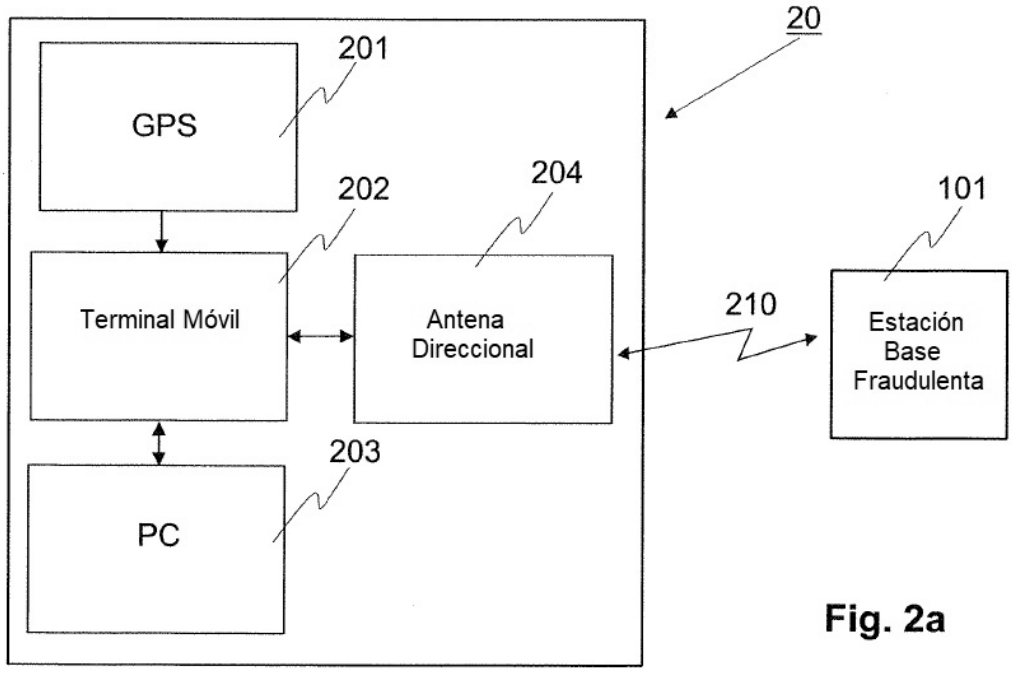

Fig. 2a

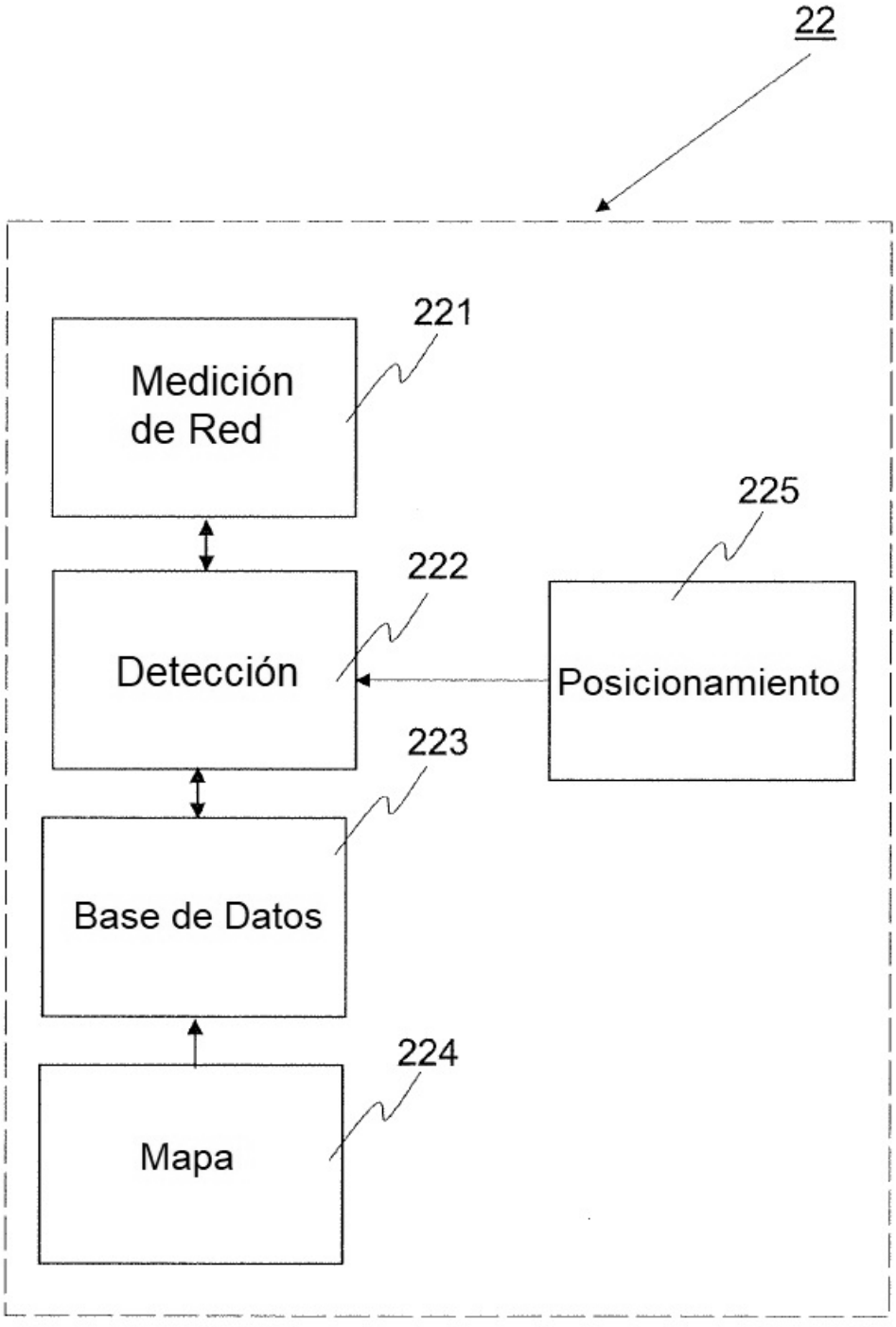
22
221
Medición de Red
225
222
Detección
Posicionamiento
223
Base de Datos
224
Mapa

Fig. 2b

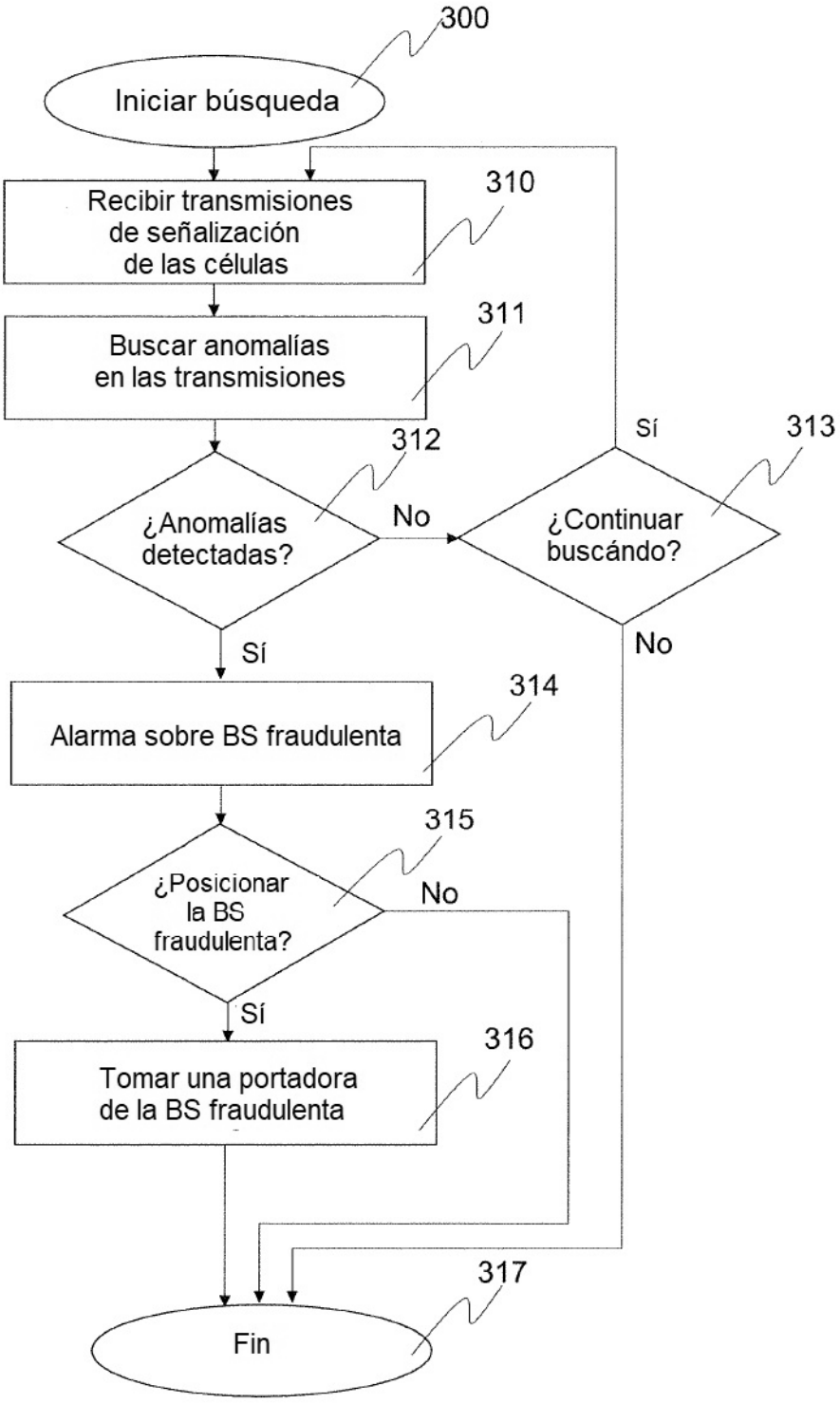
300
Iniciar búsqueda
310
Recibir transmisiones de señalización de las células
311
Buscar anomalías en las transmisiones
312
¿Anomalías detectadas?
No
313
¿Continuar buscándo?
Sí
No
Sí
314
Alarma sobre BS fraudulenta
315
¿Posicionar la BS fraudulenta?
No
Sí
316
Tomar una portadora de la BS fraudulenta
317
Fin

Fig. 3a

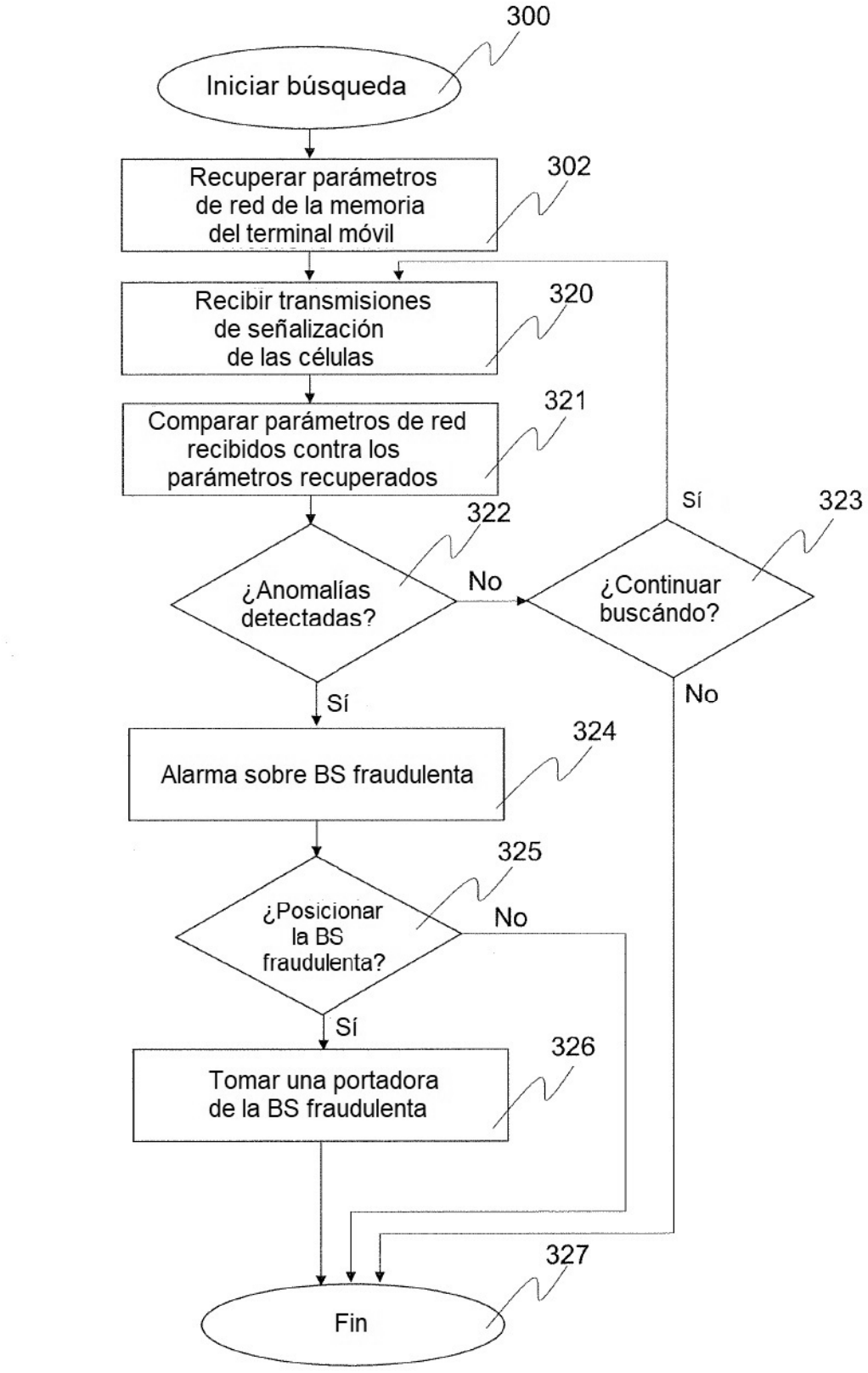
300
Iniciar búsqueda
302
Recuperar parámetros de red de la memoria del terminal móvil
320
Recibir transmisiones de señalización de las células
321
Comparar parámetros de red recibidos contra los parámetros recuperados
322
¿Anomalías detectadas?
No
Sí
323
¿Continuar buscándo?
Sí
No
324
Alarma sobre BS fraudulenta
325
¿Posicionar la BS fraudulenta?
No
Sí
326
Tomar una portadora de la BS fraudulenta
327
Fin

Fig. 3b

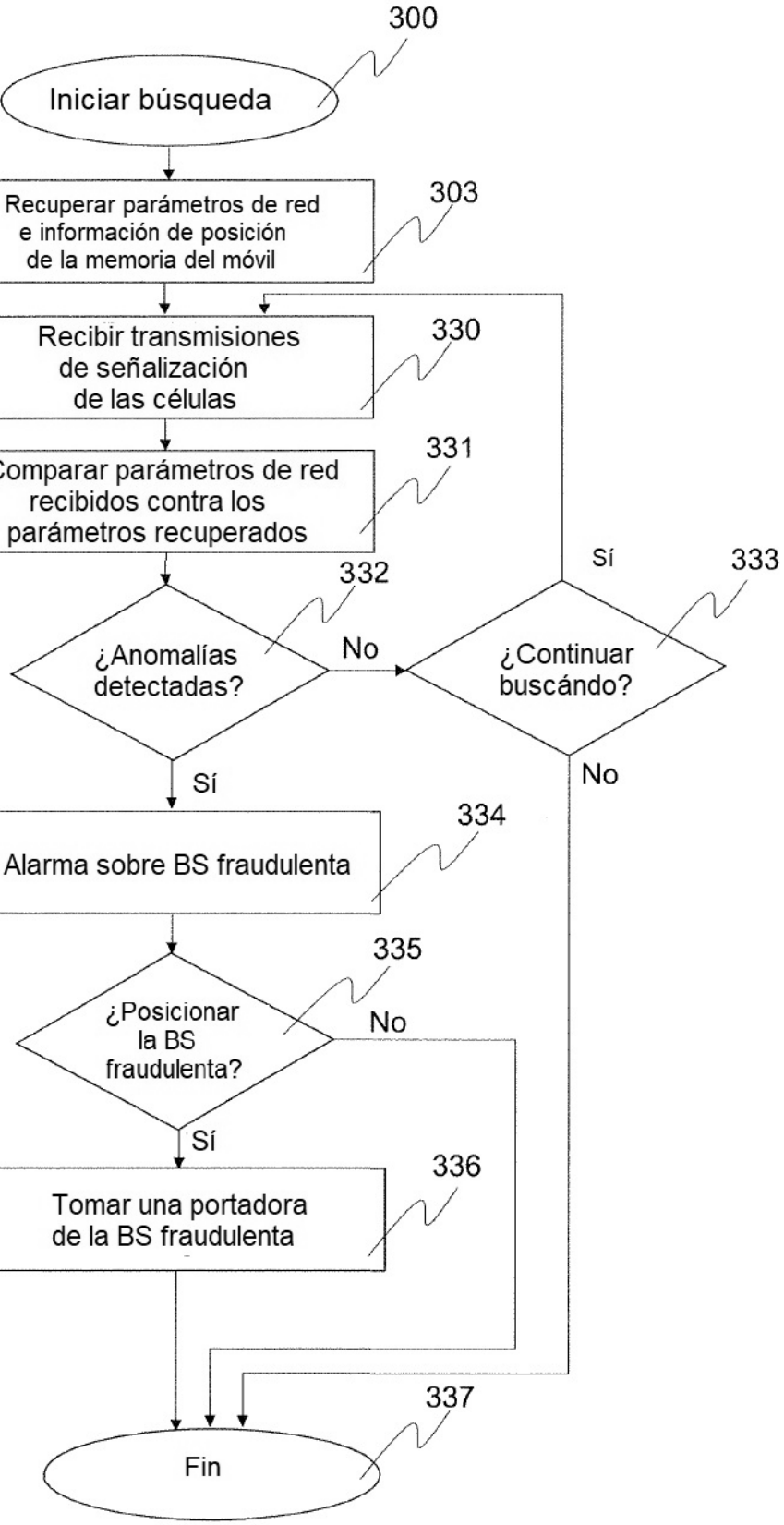
300
Iniciar búsqueda
303
Recuperar parámetros de red e información de posición de la memoria del móvil
330
Recibir transmisiones de señalización de las células
331
Comparar parámetros de red recibidos contra los parámetros recuperados
332
¿Anomalías detectadas?
No
Sí
333
¿Continuar buscándo?
Sí
No
334
Alarma sobre BS fraudulenta
335
¿Posicionar la BS fraudulenta?
No
Sí
336
Tomar una portadora de la BS fraudulenta
337
Fin

Fig. 3c