

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 378 842**

21 Número de solicitud: 200900376

51 Int. Cl.:

**H04W 24/08** (2009.01)

12

PATENTE DE INVENCION

B1

22 Fecha de presentación:

11.02.2009

43 Fecha de publicación de la solicitud:

18.04.2012

Fecha de la concesión:

07.03.2013

45 Fecha de publicación de la concesión:

20.03.2013

73 Titular/es:

**UNIVERSIDAD DE SEVILLA  
OTRI-PABELLÓN DE BRASIL, PASEO DE LAS  
DELICIAS S/N  
41013 SEVILLA (Sevilla) ES**

72 Inventor/es:

**MARTÍNEZ OLMOS, Pablo;  
MURILLO FUENTES, Juan José y  
REYES GUERRERO, José Carlos**

54 Título: **MÉTODO DE DETECCIÓN REMOTA DE INTERFERENCIA EN EL ENLACE DESCENDENTE DE SISTEMAS INALÁMBRICOS CELULARES DE TELECOMUNICACIÓN.**

57 Resumen:

La interferencia está típicamente causada por un inhibidor de frecuencia (103). En el referido sistema celular los terminales conectan con una estación base (101). El método incluye al menos un terminal móvil modificado (105) y un dispositivo de seguimiento (102). A dicho terminal (105), correctamente sincronizado y registrado en la red, se le añade una aplicación para detectar una interferencia, mientras que el dispositivo de seguimiento (102) se encarga de leer y monitorizar el tráfico en los canales comunes de señalización; detectándose un mal funcionamiento del DL al analizar un anormal tráfico en los canales comunes de señalización del DL; consistiendo esa anomalía en un inusual número de respuestas a repetidos mensajes de petición de canal dedicado.

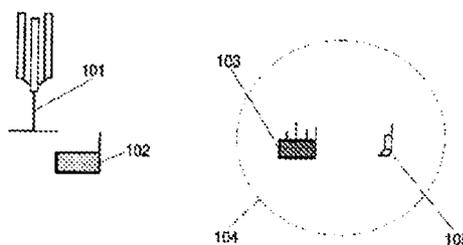


FIG. 1

ES 2 378 842 B1

## DESCRIPCIÓN

Método de detección remota de interferencia en el enlace descendente de sistemas inalámbricos celulares de tele-  
comunicación.

5

### Objeto de la invención

La presente invención, tal y como se expresa en el enunciado de esta memoria descriptiva, se refiere a un método  
de detección remota de interferencia en el enlace descendente de sistemas inalámbricos celulares de telecomunicación,  
cuya finalidad consiste en aportar una solución tecnológica para algunos problemas que se plantean en una red celular  
de telecomunicaciones inalámbrica. La invención es un método diseñado para detectar elementos interferentes en las  
comunicaciones de un sistema celular. En particular, dicho método permite la detección de un fallo en el enlace que  
comunica una estación central con un terminal. Esto es el enlace conocido como descendente. La principal aplicación  
de la invención es mejorar la seguridad contra inhibidores de frecuencia en una red celular de telecomunicación  
inalámbrica. Tiene así un impacto importante en los sistemas de seguridad basados en terminales inalámbricos para  
transmitir una alarma a una estación central. En estos sistemas, personas no autorizadas pueden impedir la transmisión  
de la alarma mediante el uso de un inhibidor de frecuencia de enlace descendente de corto alcance.

La invención se centra en la detección de un inhibidor sobre el enlace descendente (DL), o un mal funcionamiento  
en el DL. Por tanto, el dispositivo de detección presentado puede ser utilizado, además de para la detección de inhi-  
bidores de sistemas de alarmas con conexión inalámbrica, para procedimientos de optimización de red. Básicamente,  
un terminal inhibido en el DL retransmitirá sistemáticamente sus mensajes de petición de canal dedicado puesto que  
es incapaz de leer las respuestas de red en los canales de señalización común del enlace descendente. Para una rápida  
detección, se programará en el terminal una simple funcionalidad: cuando éste detecta una nula calidad en la portado-  
ra de señalización, éste inicia un procedimiento de establecimiento de conexión, enviando un mensaje de petición de  
canal dedicado en el canal de acceso aleatorio del enlace ascendente (UL). Utilizando un dispositivo, implementado  
en la propia estación base o externamente, que se sincronice a la portadora de señalización en el DL (ó UL) se detectan  
repeticiones sistemáticas de respuestas de red a mensajes de petición de canal dedicado como prueba de la existencia  
de un inhibidor. Para evitar falsas alarmas y localizar los terminales inhibidos, se realiza un intento de conexión con  
los terminales que potencialmente puedan estar inhibidos para comprobar su disponibilidad.

La invención propone un método sencillo y no intrusivo para detectar remotamente un inhibidor de frecuencia  
basado en el estudio del tráfico en los canales de señalización del DL. Este método no requiere la modificación  
del protocolo ni en la estación base ni en el terminal y puede ser implementado en cualquier celda de cualquier  
operador de telefonía móvil, puesto que todos ellos utilizan similares procedimientos de asignación de canal dedicado  
de señalización.

### Antecedentes de la invención

Cuando se utiliza un terminal inalámbrico como parte de un sistema de seguridad remoto, la existencia de un  
inhibidor de frecuencia impide la transmisión de las señales de alarma. La detección y señalización de un inhibidor  
de frecuencia, o cualquier otra fuente de interferencia, en sistemas celulares inalámbricos es un problema abierto. Los  
inhibidores de frecuencia típicamente inhiben el enlace descendente (DL) con el fin de no ser detectados.

Los inhibidores de frecuencia son dispositivos diseñados para evitar cualquier comunicación inalámbrica por irra-  
diación de ruido en una porción del espectro. Pueden ser utilizados eventualmente por razones de seguridad, por  
ejemplo, para evitar la activación de cualquier artefacto explosivo. Este tipo de inhibidores generalmente irradian rui-  
do de alta potencia y banda ancha. Por lo tanto, inhiben cualquier sistema inalámbrico en el entorno, ocultando tanto  
el enlace que comunica estación base y terminal como el enlace entre el terminal y la estación base; denominados  
enlaces ascendente y descendente respectivamente. En este escenario la detección de un inhibidor es relativamente  
inmediata.

Por otro lado, los inhibidores de frecuencia pueden ser diseñados específicamente para evitar la comunicación en  
un sistema en concreto; por ejemplo para inhibir un sistema de alarma inalámbrica, que suelen operar sobre redes  
móviles celulares 2G, 2G+, /3G,... Con el fin de que el inhibidor de frecuencia no sea detectado, éstos no suelen radiar  
en la banda correspondiente al enlace de subida o up-link (UL). Si el inhibidor radiase suficiente potencia en el UL  
como para alcanzar la estación base con una potencia similar a la emitida por los terminales, la presencia del inhibidor  
sería fácilmente detectable sin más que monitorizar el tráfico interrumpido y los niveles de potencia recibidos en la  
estación base. En este sentido, los inhibidores de frecuencia más sofisticados están diseñados de forma que únicamente  
radien en el enlace descendente o down-link (DL). En este caso, el terminal es capaz de comunicarse con la estación  
base pero no puede recibir ningún mensaje de ésta. En redes celulares, esto implica que el terminal es incapaz de leer  
la señalización necesaria en redes 2G y 3G para iniciar la comunicación con la estación base. Dicha señalización es  
transmitida por parte de la estación base a través de los canales comunes de control (CCCHs).

El proceso para detectar un inhibidor de frecuencia consta de dos problemas diferenciados. Primero, el terminal de-  
be detectar la presencia del inhibidor analizando la señal recibida (detección). Segundo, debe señalar dicha situación  
a la red (señalización). Con respecto a la detección, en la invención se propone un método muy sencillo comparado  
con los propuestos en las referencias [1], [2] y [3] que aparecen al final de este apartado. Respecto a la señalización,

son escasas las referencias o soluciones propuestas a día de hoy, por lo que es un problema abierto. En la referencia bibliográfica [2], se propone un método de señalización para un terminal GSM. Éste señala a la estación base su condición de inhibido en un mensaje de petición de canal dedicado o Channel Request Message, modificado con respecto al canal de acceso aleatorio RACH en el UL descrito en el estándar 3GPP TS 144018 V7.13 (2008-07). Obviamente, este mensaje debe ser comprendido por la estación base. Esta invención, a pesar de su simplicidad, plantea un gran problema en su implementación, puesto que ésta podría requerir la modificación del protocolo GSM/GPRS tanto en el terminal como en la estación base. Especialmente para esta última, el coste asociado es muy grande al tener que modificar el software implementado en ésta.

No conocemos en el estado actual de la técnica soluciones en las que no sea imperativa la modificación de la estación base, en tanto que la presente invención permite la no modificación de dicha estación base. Así, según la invención, para una rápida y eficiente detección, se requiere una simple funcionalidad añadida al terminal potencialmente inhibido: cuando no pueda decodificar los canales de control, éste comenzará la señalización correspondiente al establecimiento de una conexión, lo que no implica modificación alguna de su protocolo, sino tan solo la inclusión de algún programa adicional en el terminal. Por otro lado, la señalización emitida por el terminal inhibido puede ser detectada tanto en la estación base como en un terminal externo. Por tanto, el invento puede ser implementado en una estación base, pero también para evitar el coste asociado puede ser implementado en un escáner de frecuencia sintonizado a la portadora del DL en la celda. Plataformas SDRs (software defined radios), que implican un menor coste y son dispositivos fácilmente programables, son una solución muy adecuada para implementar el escáner de frecuencia debido a la dificultad para encontrar en el mercado escáneres con acceso completo a los canales de control.

## Referencias

[1] **Robert C. Hendrickson**, Jamming detection in a Wireless security system, Patente US number: 5950110, Sep 7, 1999. International Classification: H04K 300;H04B 1700.

[2] **Moscovitz Y., Depernini F., Locatellin M.**, Method and user equipment for jamming detection and signalling, International Patente Classification: H044 3/00, International Publication Number: WO 2005/112321 A1, Nov. 24, 2005.

[3] **Wenyuan Xu, Ke Ma, Trappe, W., Yanyong Zhang**, Jamming sensor networks: attack and defense strategies, IEEE Network Volume 20, Issue 3, May-June 2006 Page(s):41-47.

## Descripción de la invención

Para lograr los objetivos y evitar los inconvenientes indicados en anteriores apartados, la invención consiste en un método de detección remota de interferencia en el enlace descendente de sistemas inalámbricos celulares de telecomunicación, estando esta interferencia típicamente causada por un inhibidor de frecuencia que actúa sobre un terminal móvil, y siendo el sistema considerado un sistema celular en el cual los terminales se conectan a una estación base.

Novedosamente, según la invención, el referido método incluye al menos un terminal móvil modificado y un dispositivo de seguimiento, de manera que a este terminal, correctamente sincronizado y registrado en la red, se le añade una aplicación para detectar una interferencia; en tanto que el dispositivo de seguimiento se encarga de leer y monitorizar el tráfico en los canales comunes de señalización del enlace descendente (DL) o ascendente (UL); detectándose un mal funcionamiento de DL analizando un anormal tráfico en los canales comunes de señalización; consistiendo dicha anomalía en un inusual número de mensajes repetidos de petición de canal dedicado (siendo dicha petición un procedimiento inicial previo al establecimiento de cualquier comunicación en estándares de telefonía celular) o de respuestas a estos mensajes.

Según la realización preferente de la invención, el método de la misma incluye los siguientes procesos en el terminal móvil modificado:

- a) medida continua de la calidad en la portadora de señalización;
  - b) en caso de una pobre calidad, se inicia un proceso de señalización, correspondiente al establecimiento de una conexión; iniciándose este proceso de señalización enviando un mensaje de petición de canal de señalización dedicado a través del canal de acceso aleatorio del correspondiente enlace ascendente (UL);
  - c) en caso de alta interferencia de acuerdo a los estándares de comunicaciones móviles celulares, el móvil retransmite la petición después de un determinado tiempo; y cuando se ha alcanzado un número máximo de retransmisiones, el móvil retorna al estado a);
- en tanto que el método implica los siguientes procesos en el dispositivo de seguimiento:
- d) sincronización con la portadora de señalización del enlace descendente (DL) ó ascendente (UL);
  - e) análisis de las peticiones de canal dedicado o respuestas de red a estas peticiones; de manera que alcanzado un número de peticiones suficiente en un determinado período de tiempo, se considera la existencia de un

inhibidor de frecuencia; estando los distintos mensajes de petición o respuesta espaciados un tiempo no mayor que el establecido en el estándar entre dos retransmisiones de petición de canal por parte del móvil;

- f) el dispositivo de seguimiento utiliza una estrategia de polling o interrogación para intentar establecer una conexión y comprobar así el estado de los terminales una vez se ha considerado probable la existencia de un inhibidor.

Además, según las realizaciones preferentes de la invención, el referido sistema celular puede ser una red celular 2G, 3G UMTS, u otra.

Según las realizaciones preferentes de la invención, en el método de la misma, el dispositivo de seguimiento se dispone en proximidad de la estación base al objeto de presentar las máximas posibilidades de quedar fuera del área de cobertura del posible inhibidor, el cual se tendría que situar en proximidad del terminal móvil a inhibir para efectuar su función.

Así, según se ha descrito, la presente invención aporta un método para detectar cuando un terminal inalámbrico móvil se encuentra afectado por una alta interferencia, normalmente debido a la presencia de un inhibidor, en el sentido descendente (DL) de la celda y comunicar dicha situación a algún dispositivo o sistema externo. Asumiendo que un terminal en un sistema de comunicación inalámbrico puede detectar altas interferencias en el DL, éste solo debería comunicar esta situación a la estación base utilizando el sentido ascendente (UL) sin embargo, por diseño en la mayor parte de sistemas celulares, previamente a cualquier comunicación, la estación base y el terminal deben establecer un canal de señalización dedicado. Una fuerte interferencia en el DL, que puede estar causada por un inhibidor de frecuencia cercano al terminal, oculta la transmisión de información a través de los canales de control del sentido descendente. Como resultado, el canal de señalización dedicado comentado anteriormente no se puede establecer, y el terminal es incapaz de enviar información alguna a la estación base, ni siquiera su identidad. En un sistema de seguridad en el cual la conexión a la central se realiza a través de un sistema celular, un inhibidor de frecuencia sobre el DL impediría cualquier transmisión de señal de alarma.

El método que se describe en la presente invención puede ser implementado tanto en un dispositivo remoto como en la estación base del sistema inalámbrico. Sea cual sea el dispositivo utilizado, la clave está en monitorizar el canal de control común para encontrar continuas repeticiones de peticiones, o sus respuestas, de establecimiento de canal, a las que el terminal inhibidor nunca contestará pues nunca las recibirá. Si la estación base o un dispositivo externo detecta este comportamiento en el tráfico de señalización, se iniciará un proceso de polling o comprobación mediante interrogación a aquellos terminales que estén siendo protegidos frente a inhibidores en la celda.

Las ventajas que el presente invento aporta con respecto a métodos anteriores son varias. Primero, no requiere una modificación del protocolo en la estación base (BS) o terminal móvil (MS), puesto que se basa en como la señalización en los canales comunes (CCCHs) se ve degradada cuando un terminal móvil se encuentra dentro del alcance de un inhibidor de frecuencia sobre el DL. Asimismo, varios dispositivos pueden ser monitorizados frente a inhibidores simultáneamente con un único dispositivo de seguimiento o tracking en cada celda. Si dicho dispositivo de seguimiento se implementa en una plataforma SDR, en lugar de ser programado en la propia estación base, el invento se hace independiente del operador móvil, lo que incrementa enormemente su potencial explotación comercial.

A continuación, para facilitar una mejor comprensión de esta memoria descriptiva y formando parte integrante de la misma, se acompañan unas figuras en las que con carácter ilustrativo y no limitativo se ha representado el objeto de la invención.

### Breve descripción de las figuras

Figura 1.- Representa esquemáticamente un diagrama de bloques funcionales que muestran un escenario propuesto para la aplicación de un método de detección remota de referencia realizado según la presente invención.

Figura 2.- Representa un diagrama de flujo del terminal potencialmente inhibido de la anterior figura 1 según el referido método de la invención.

Figura 3.- Representa un diagrama de flujo del dispositivo de seguimiento de la anterior figura 1 según el método de la presente invención, para el DL.

Figura 4.- Representa esquemáticamente el flujo de mensajes en el proceso de señalización de inhibición en el método referido en las anteriores figuras.

Figura 5.- Muestra la tabla 1 referida en el texto de esta memoria y correspondiente a valores para el parámetro S según el estándar 3GPP TS144018 V7.13 (2008-07).

Figura 6.- Muestra la tabla 2 referida en el texto de esta memoria correspondiente a slots de acceso del canal RACH y la relación con el canal de adquisición (AICH) del DL PRACH ( $\tau_{p-a} = 7680$  chips) según el estándar 3GPP TS 25.214 V7.9.0 (2008-07).

Figura 7.- Muestra la tabla 3 referida en el texto de esta memoria correspondiente a slots de acceso de los distintos subcanales RACH según el estándar 3GPP TS 25.214 V7.9.0 (2008-07).

### Descripción de un ejemplo de realización de la invención

5 Seguidamente se realiza una descripción de un ejemplo de la invención haciendo referencia a la numeración adoptada en las figuras.

Así, según puede verse en la figura 1, el método de la invención cuenta con dos elementos encargados de la  
 10 detección y señalización de interferencia o inhibición. El terminal potencialmente inhibido 105, también denominado estación móvil (MS), y el dispositivo de monitorización o seguimiento 102. Supondremos interferido únicamente el enlace descendente por un inhibidor de frecuencia 103 que actúa en un área de cobertura 104, con lo que el enlace ascendente puede ser utilizado por el terminal para enviar información a la estación base 101 (BTS), pero no así en el sentido contrario. El terminal 105 está correctamente registrado a la red móvil, esto es correctamente sincronizado y  
 15 sintonizado a la configuración radio de la red. Además, en él se ha programado una simple funcionalidad añadida con respecto a un terminal estándar. Dicha funcionalidad se describe en el diagrama de flujo de la figura 2. Inicialmente, el terminal 105 monitoriza la calidad y potencia de la señal recibida en la portadora de señalización (203). En el momento en que se encuentre una calidad pobre y dichos canales no puedan ser decodificados (204) se inicia el proceso de señalización de una posible situación de inhibición (205), intentando establecer una conexión con la estación base  
 20 101. Si un inhibidor 103, o cualquier otro dispositivo, está interfiriendo los canales del DL, el terminal 105 no puede completar el proceso de señalización por el mismo, puesto que el proceso de establecimiento del canal de señalización dedicado no puede ser completado. Típicamente éste involucra los siguientes pasos:

1°) El terminal envía un mensaje de petición de canal dedicado en el canal de acceso aleatorio (RACH) del sentido  
 25 ascendente (UL). Puede mandar o no, dependiendo del estándar y su implementación, un código aleatorio que le será devuelto en la respuesta a esa petición.

2°) El contador de peticiones de canal dedicado se incrementa en una unidad (206). Existe un máximo en el número  
 30 de repeticiones del mensaje de petición anterior, que denotaremos por  $N_{\max}$ . El valor del parámetro  $N_{\max}$  depende del estándar de comunicación inalámbrica en cuestión.

3°) El terminal espera respuesta en el correspondiente canal de control del DL hasta un máximo de  $T_0$  (207), donde  
 35  $T_0$  depende del estándar de comunicación inalámbrica considerado. Si se recibe respuesta (positiva o negativa) de la red, se concluye que no existe presencia significativa de interferencia y el proceso de establecimiento de conexión es cancelado (208). En caso contrario, se envía otro mensaje de petición de canal dedicado a través del RACH siempre que no se haya superado el máximo número de repeticiones permitidas. Dependiendo de la configuración de la red, en cada retransmisión el terminal puede repetir la referencia aleatoria de la petición o cambiarla. Nótese que en este proceso no se transmite información sobre la identidad del móvil.

4°) Cuando el contador de peticiones de canal alcanza el valor  $N_{\max}$ , el terminal no comienza un nuevo proceso  
 40 completo (202) de petición de canal dedicado hasta que un temporizador haya expirado (210). De nuevo este temporizador depende del estándar en cuestión.

45 Los procesos dentro de la línea discontinua 211 constituyen la funcionalidad adicional que debe ser programada en el terminal. El resto de pasos son típicos de cualquier estándar de comunicación inalámbrico, y por lo tanto ya están programadas en el terminal.

50 Las referencias 201 y 209 de la figura 2 corresponden respectivamente a las funciones de inicio y contador de peticiones de canal.

El dispositivo de seguimiento 102 analiza el tráfico en los canales de control en el DL, ó el UL, con el fin de  
 55 detectar situaciones sospechosas. Esta funcionalidad puede ser implementada en la estación base, pero también en un elemento externo. En la figura 3 se describe el funcionamiento de este dispositivo para el DL. Para el UL sería similar pero monitorizando las peticiones directamente y no las respuestas a las peticiones. Una vez éste se ha sintonizado y sincronizado a la portadora de señalización (302), comienza la monitorización de los canales CCCHS en el DL (304). Cuando detecta la primera respuesta de la red a una petición de canal de señalización de canal dedicado (305), un contador, que denominaremos contador de respuestas de red, se incrementa (306). Como ya se ha comentado anteriormente, un terminal inhibidor repetirá sistemáticamente la petición de canal varias veces al no recibir respuesta  
 60 de la red. Tras la lectura de cada respuesta de la red, el dispositivo de seguimiento comprueba que no hay un nuevo mensaje de respuesta en los siguientes  $T_0$  (307). En caso negativo, no ha habido repetición y se asume que la respuesta de la red llegó a su destino y que el móvil que solicitó el canal dedicado no está interferido en el enlace descendente. En este caso, se resetea el contador de respuestas de red (303). En caso contrario, si se detecta una nueva respuesta de red para un canal dedicado en un tiempo menor de  $T_0$  segundos, se incrementa el contador (308). Cuando dicho contador alcanza el umbral  $N_{\max}^{\text{JAM}}$  (309), la situación se concluye determinando que el terminal está inhibido y se activa la  
 65 condición de alarma. Si el terminal móvil inhibido repite la referencia aleatoria en todas sus peticiones, el dispositivo de seguimiento únicamente debe llevar la cuenta de las respuestas de red con igual referencia. En este escenario, el riesgo de falsa alarma se minimiza, dado que respuestas de red con distintas referencias aleatorias son asignadas a diferentes

terminales. Por el contrario, si dicha referencia es potencialmente distinta en cada retransmisión, el dispositivo debe contar y considerar conjuntamente todas las respuestas de red detectadas, lo que incrementa el riesgo de falsa alarma.  $N_{\max}^{\text{JAM}}$  puede ser fijado a  $N_{\max}$  o a cualquier otro valor. Si tomamos  $N_{\max}^{\text{JAM}} > N_{\max}$ , cuando el contador alcance  $N_{\max}$  el dispositivo debe esperar la siguiente respuesta de red no un tiempo  $T_0$  sino  $T_0 + \text{Temp}$  segundos, donde Temp es la duración del temporizador en 210. En este caso, la condición en 309 es modificada para asegurar dicha situación. Fijar  $N_{\max}^{\text{JAM}} > N_{\max}$  es una buena opción para minimizar el riesgo de falsa alarma, especialmente cuando el teléfono móvil no repite la misma referencia aleatoria entre peticiones de canal dedicado.

El siguiente paso es comprobar si realmente el terminal está inhibido. Esto puede lograrse con una simple interrogación o polling, esto es mediante un simple intento de conexión. El propio escáner, o cualquier otro dispositivo, manda un mensaje al conjunto de los terminales supervisados en la celda y espera asentimiento. Este es el intento de establecimiento de conexión en 310. En el caso de que no haya respuesta de alguno de los terminales, se considerará que éste está bajo la influencia de una fuerte interferencia, potencialmente causada por un inhibidor.

Las referencias 301, 311 y 312 de la figura 3 corresponden respectivamente a las funciones de inicio, interrogación de disponibilidad y situación de terminal móvil inhibido.

En la figura 4 se muestra un diagrama que ilustra los mensajes intercambiados por el terminal 105 y la red una vez que el primero ha detectado una posible situación de inhibición. También se estiman los tiempos de respuesta y latencia involucrados. El primer mensaje de petición de canal (Channel request message) (401) llega a la estación base 101 con un determinado retardo de propagación, que podemos estimar en el orden de  $10^{-5}$  segundos, lo denotaremos por  $O(10^{-5})$ . Tras un determinado tiempo de procesamiento, la estación base manda un mensaje de respuesta (405) a dicha petición a través de los canales comunes del DL. Dicho mensaje no se recibe en el terminal en caso de fuerte interferencia en el enlace descendente, pero si se detecta en el dispositivo de seguimiento (404). Éste se colocará siempre cerca de la estación base, si no se programase en la propia estación base. En todo caso, lejos de la influencia del posible inhibidor de frecuencia. Cada  $T_0$  segundos (406), tiempo que se establece de forma que sea mayor que la suma de los retardos de propagación y de procesamiento de la estación base, se envía un nuevo mensaje de petición de canal (407), siendo de nuevo detectado en el dispositivo de seguimiento (409) y enviándose un nuevo mensaje de respuesta (410) desde la estación base. Después de que el equipo de seguimiento detecte  $N_{\max}^{\text{JAM}}$  retransmisiones (412), tras una última petición de canal (411) se realiza un intento de conexión o polling con el terminal (413). Por tanto, el proceso completo de detección de un inhibidor implica un retardo máximo de  $N_{\max}^{\text{JAM}} \times T_0$  segundos si  $N_{\max}^{\text{JAM}} \leq N_{\max}$  o  $N_{\max}^{\text{JAM}} \times T_0 + \text{Temp}$  cuando  $N_{\max}^{\text{JAM}} > N_{\max}$ . En ambos casos, es de orden  $O(10^{-2})$ . Por tanto, podemos detectar remotamente la presencia de un inhibidor en un tiempo aproximadamente de 0,1 segundos.

Cuando el tráfico de una celda es significativo, el riesgo de falsa alarma, es decir, el riesgo de hacer pollings innecesarios, aumenta. Sin embargo, esta posibilidad es mínima ya que en general será muy difícil encontrar  $N_{\max}^{\text{JAM}} \geq N_{\max}$  respuestas de red a peticiones de canal separadas un tiempo menor que  $T_0$  segundos. El riesgo de falsa alarma se reduce aun más si el terminal repite la referencia aleatoria en los distintos mensajes de petición de canal.

Las referencias 402, 403 y 408 de la figura 4 corresponden respectivamente a retardo de propagación, retardo de procesamiento en la estación base y tiempo entre mensajes de respuesta.

El método de detección propuesto puede implementarse también en una celda únicamente con un dispositivo de seguimiento sin añadir nuevas funcionalidades a los terminales móviles. En este caso, el proceso de detección de un inhibidor será mucho más lento, puesto que éste se iniciará cuando el terminal móvil envíe, eventualmente, un mensaje de petición de canal; por ejemplo para tareas de actualización de posición. Con la funcionalidad descrita para el terminal en la figura 1, se refuerza la transmisión del mensaje de petición de canal en el momento en que se detecta una posible inhibición.

El método de detección y señalización de un inhibidor de frecuencia que se ha descrito puede ser aplicado directamente a temas de seguridad. En el mercado existen distintos modelos de alarmas que se conectan de forma inalámbrica con las agencias de seguridad a través de las redes de telefonía móvil celular. Estos dispositivos, por tanto, pueden verse anulados con la presencia de un inhibidor de frecuencia. Si la agencia de seguridad utiliza un dispositivo de seguimiento y añade la funcionalidad descrita en la figura 2 al terminal de alarma, la presencia de un inhibidor se detectaría en menos de un segundo.

El método propuesto para la detección de un inhibidor de frecuencia puede ser implementado tanto en redes celulares GSM/GPRS como en redes 3GUMTS. Aunque en ambas tecnologías el acceso radio es distinto, los procedimientos de señalización referidos a la asignación de un canal dedicado son similares.

Seguidamente se describe una implementación en una red GSM/GPRS:

En una red GSM/GPRS, el método de detección y señalización se implementa utilizando los siguientes parámetros del correspondiente estándar de comunicación inalámbrica [3GPP TS 144018 V7.13 (2008-07)]:

- El terminal GSM/GPRS envía una petición de canal en el canal del acceso aleatorio RACH del enlace ascendente o UL.

- El máximo número de retransmisiones de una petición de canal ( $N_{\max}$ ) está dado por el parámetro Max\_retrans, fijado por la red en el canal BCCH del DL.
- Entre dos retransmisiones consecutivas del mensaje de petición de canal, el terminal espera un tiempo máximo de  $S+T-1$  slots, donde  $T$  es un parámetro difundido en el canal BCCH y se calcula a partir de la tabla 1 que se muestra en la figura 5. El número  $S+T-1$  multiplicado por el tiempo de slots es  $T_0$ , correspondiente al que aparece en las referencias 207 y 307 de las figuras 2 y 3 respectivamente.
- El dispositivo de seguimiento monitoriza el canal de concesión de canal o Access Granted Channel (AG-CH) y el canal de búsqueda o Paging Access Channel (PACH), buscando mensajes de respuesta de red a peticiones de canal. En GSM/GPRS dichos mensajes se denominan en caso positivo de acceso inmediato o Immediate Assignment (IA) o en caso negativo mensajes de negación de acceso inmediato o Immediate Assignment Reject (IAR).

Es importante notar que muchos de los parámetros involucrados en el proceso de detección y señalización propuesto dependen únicamente de información difundida por la red en el canal BCCH de cada celda. Sin embargo, pueden tomarse valores fijos. En este caso, una opción sería tomar los máximos valores contemplados en el protocolo:

- $N_{\max}^{\text{IAM}} = N_{\max} = \text{Max\_retrans} = 7$ .
- $T_0 = 50$  slots.

Asimismo, podemos seguir una estrategia más conservadora y fijar el parámetro Max\_retrans a un valor mayor, por ejemplo veinte retransmisiones. Esto minimizará la probabilidad de falsa alarma, pero debemos tener en cuenta que cada siete retransmisiones leídas en el dispositivo de seguimiento (igual al número de retransmisiones permitido por el estándar en cada intento de conexión), el dispositivo debe esperar otra repetición de petición de canal un tiempo de  $T_0 + \text{Temp}$ , donde Temp es la duración del temporizador en 210, que en el estándar GSM/GPRS es denominado T316.

Seguidamente se describe una implementación en una red 3G UMTS:

En una red 3G UMTS, la detección y señalización de un terminal inhibido se implementa utilizando los siguientes parámetros y procedimientos, según los estándares de comunicación inalámbrica 3GPP TS 25.211 V7.6.0 (2008-07) y 3GPP TS 25.214 V7.9.0 (2008-07):

- El terminal UMTS potencialmente inhibido envía un mensaje de petición de canal dedicado en el canal de acceso aleatorio (RACH).
- Dicho mensaje consta de un conjunto de preámbulos (4096 chips) escogidos aleatoriamente a partir de un conjunto de dieciséis posibles firmas, hasta que recibe respuesta de la red en el canal de adquisición o Acquisition Indicator Channel del DL.
- El número máximo de retransmisiones del preámbulo ( $N_{\max}$ ) está dado por el parámetro Preamble\_retrans\_max, difundido en el canal BCCH del DL. Por tanto, el parámetro  $N_{\max}$  en la figura 2, (209) es igual a Preamble\_retrans\_max. De nuevo, se puede fijar  $N_{\max}^{\text{IAM}}$  a un valor superior. En este caso, cada Preamble\_retrans\_max respuestas de red detectadas en el dispositivo de seguimiento, éste deberá esperar  $T_0 + \text{Temp}$  segundos para la siguiente respuesta de red en lugar de los  $T_0$  segundos usuales, donde Temp es la duración del temporizador en 210. En sistemas UMTS, Temp es siempre menor que  $\text{NB01}_{\max} \times 10$  ms, donde  $\text{NB01}_{\max}$  se proporciona en los canales de señalización común.
- La red difunde las firmas disponibles en cada momento y los subcanales RACH para cada servicio o Access Service class (ASC). El terminal inhibido transmite un preámbulo en el primer slot disponible en el subcanal RACH. El reparto de slots para los distintos subcanales RACH se muestran en la tabla 3 de la figura 7. Como podemos observar, cada trama del canal RACH consta de quince slots de acceso y cada subcanal RACH consta de unos siete u ocho slots. En celdas con alto tráfico, en cada subcanal RACH puede haber un número grande de slots no disponibles y el tiempo entre retransmisiones de un preámbulo puede ser relativamente extenso, pero no es probable que éste sea mayor al tiempo de trama RACH (esto significaría que todos los slots de acceso están ocupados simultáneamente). Podemos por tanto fijar el parámetro  $T_0$ , el que aparece en las referencias 207 y 307 de las figuras 2 y 3, como el tiempo de una trama RACH, esto es, quince veces el tiempo de slots (150 ms aproximadamente).
- El dispositivo de seguimiento monitoriza el canal de adquisición del DL (AICH), leyendo los indicadores de adquisición para cada petición, que están asociados a la misma asignatura, según la tabla 2 que se muestra en la figura 6.

Respecto a otros aspectos en la implementación de la invención, cabe decir que la implementación del terminal móvil con la funcionalidad requerida es extremadamente sencilla puesto que no es más que un terminal móvil usual o similar que ejecuta un programa sencillo y que para nada afecta al protocolo del terminal: en el momento en que detecte una calidad nula en los canales de control comunes del DL (CCCH), comienza la señalización correspondiente a una llamada de voz. Esta pequeña aplicación es muy sencilla de desarrollar utilizando los paquetes de desarrollo o software development kits (SDKs) que los fabricantes usualmente proporcionan de forma gratuita. Por tanto, modificar el terminal de usuario no es en modo alguno costoso.

El dispositivo de seguimiento debe leer continuamente los canales de control del DL. Por tanto, necesitamos un dispositivo capaz de sincronizarse con la portadora de señalización de la red celular y monitorizar la información difundida en los distintos canales. La solución más sencilla y flexible para la implementación del dispositivo es utilizar una plataforma de radio programable (SDR), ya que modificar una estación base es extremadamente caro. Puesto que un solo dispositivo de seguimiento puede monitorizar y trabajar con varios terminales que implementen la funcionalidad indicada anteriormente, su coste está justificado. Asimismo, utilizar una plataforma programable hace que la solución propuesta en este trabajo sea independiente del operador de red y por tanto, una solución no intrusiva.

20

25

30

35

40

45

50

55

60

65

## REIVINDICACIONES

1. Método de detección remota de interferencia en el enlace descendente de sistemas inalámbricos celulares de telecomunicación, estando esta interferencia típicamente causada por un inhibidor de frecuencia (103) y siendo el sistema considerado un sistema celular en el cual los terminales se conectan a una estación base (101); **caracterizado** porque dicho método incluye al menos un terminal móvil modificado (105) y un dispositivo de seguimiento (102), de manera que a ese terminal modificado (105), correctamente sincronizado y registrado en la red, se le añade una aplicación para detectar una interferencia; en tanto que el dispositivo de seguimiento (102) se encarga de leer y monitorizar el tráfico en los canales comunes de señalización del enlace descendente (DL) o ascendente (UL); detectándose un mal funcionamiento del DL analizando un anormal tráfico en los canales comunes de señalización; consistiendo dicha anomalía en un inusual número de mensajes de peticiones, o sus respuestas, de canal dedicado (siendo dicha petición un procedimiento inicial previo al establecimiento de cualquier comunicación en estándares de telefonía celular).

Se **caracteriza** porque incluye los siguientes procesos en el terminal móvil modificado (105):

- a) medida continua de la calidad en la portadora de señalización;
- b) en caso de una pobre calidad, se inicia un proceso de señalización, correspondiente al establecimiento de una conexión; iniciándose este proceso de señalización enviando un mensaje de petición de canal de señalización dedicado a través del canal de acceso aleatorio del correspondiente enlace ascendente (UL);
- c) en caso de alta interferencia de acuerdo a los estándares de comunicaciones móviles celulares, el móvil retransmite la petición después de un determinado tiempo; y cuando se ha alcanzado un número máximo de retransmisiones, el móvil retorna al estado a);

y en tanto que el método implica los siguientes procesos en el dispositivo de seguimiento (102):

- d) sincronización con la portadora de señalización del enlace descendente (DL);
- e) análisis de las respuestas de red a peticiones de canal dedicado; de manera que alcanzado un número de peticiones suficiente en un determinado período de tiempo, se considera la existencia de un inhibidor de frecuencia; estando los distintos mensajes de respuestas espaciados un tiempo no mayor que el establecido en el estándar entre dos retransmisiones de petición de canal por parte del móvil;
- f) el dispositivo de seguimiento (102) utiliza una estrategia de polling o interrogación para intentar establecer una conexión y comprobar así el estado de los terminales una vez se ha considerado probable la existencia de un inhibidor (103).

2. Método de detección remota de interferencia en el enlace descendente de sistemas inalámbricos celulares de telecomunicación, según la reivindicación 1 ó 2, **caracterizado** porque dicho sistema celular es bien una red celular 2G, 3G UMTS, u otra.

3. Método de detección remota de interferencia en el enlace descendente de sistemas inalámbricos celulares de telecomunicación, según una cualquiera de las reivindicaciones anteriores, **caracterizado** porque el dispositivo de seguimiento (102) puede estar en la propia estación base o fuera, en cuyo caso se dispone en proximidad a la estación base (101) al objeto de presentar las máximas posibilidades de quedar fuera del área de cobertura (104) del posible inhibidor (103), el cual se tendría que situar en proximidad del terminal móvil a inhibir (105) para tratar de efectuar su función.

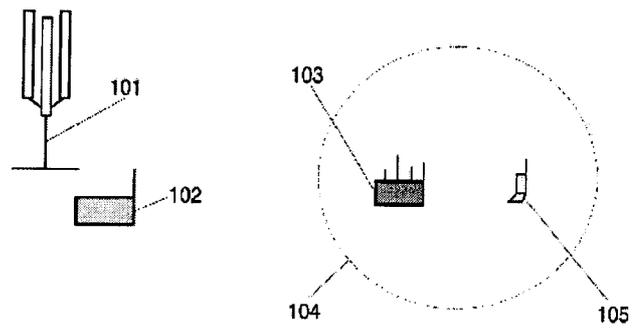


FIG. 1

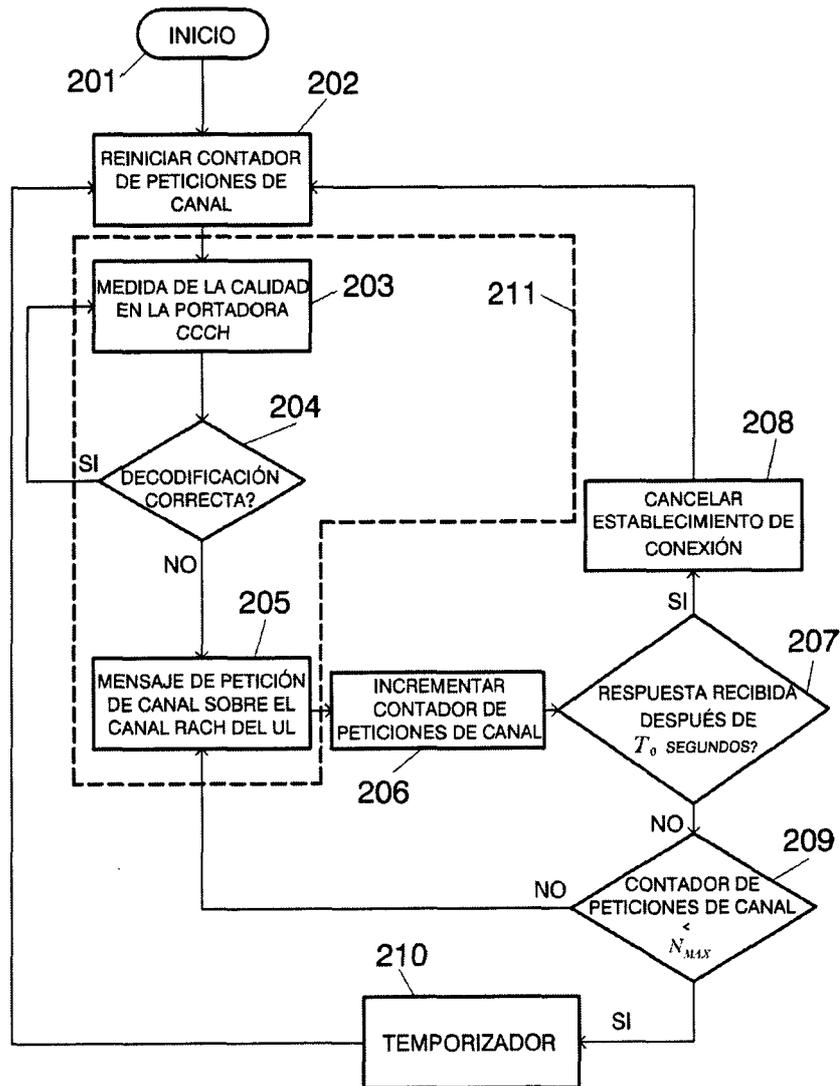


FIG. 2

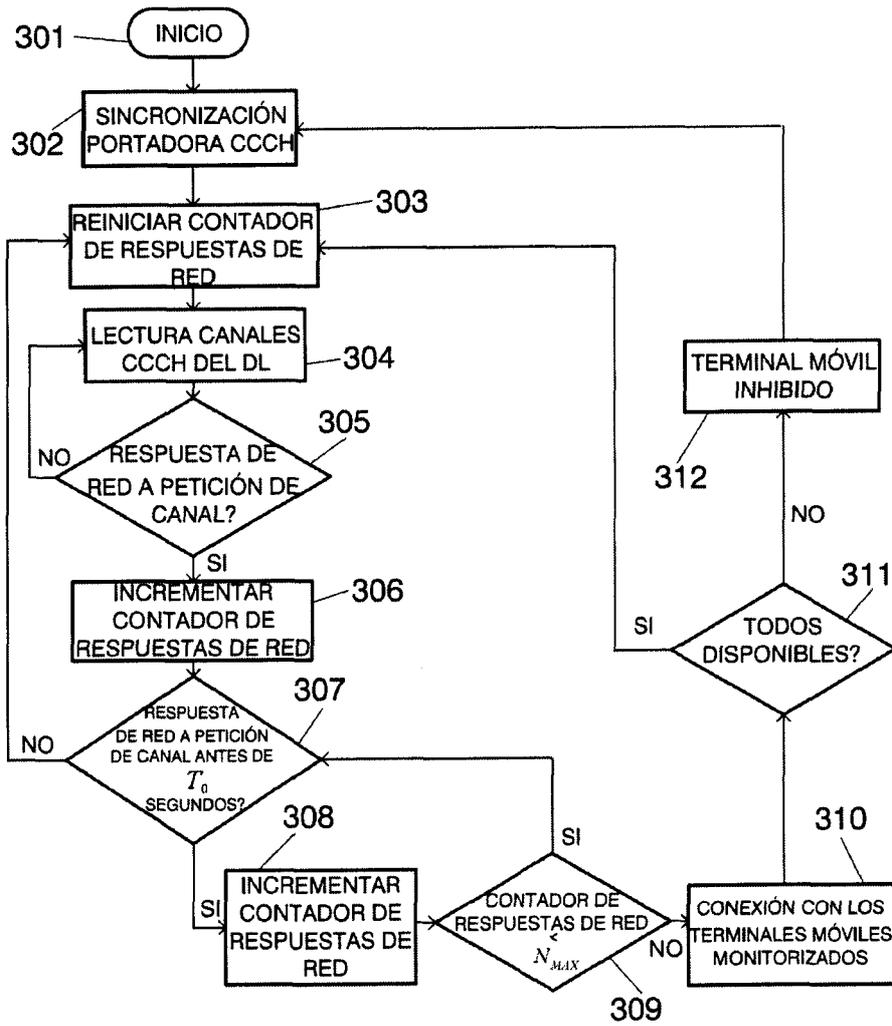


FIG. 3

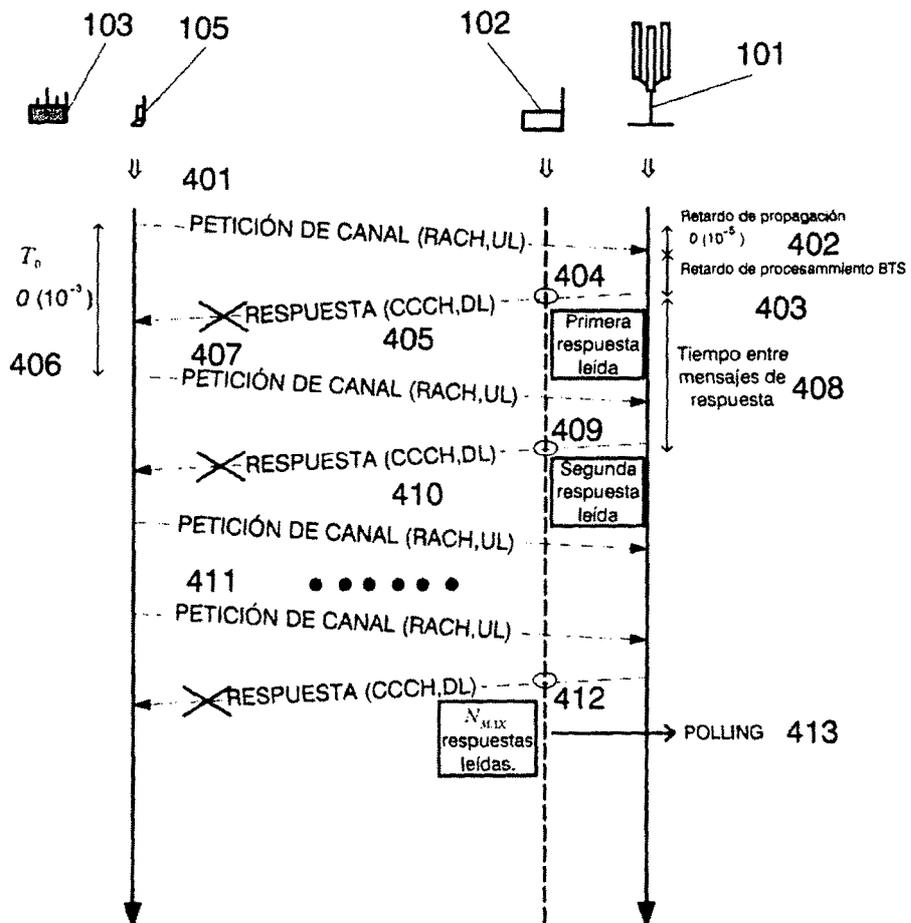


FIG. 4

$T$	CCCH no combinado	CCH/SDCCH combinado
3,8,15,50	55	41
4,9,16	76	52
5,10,20	109	58
6,11,25	163	86
7,12,32	217	115

Tabla 1. Valores para el parámetro S.

FIG. 5

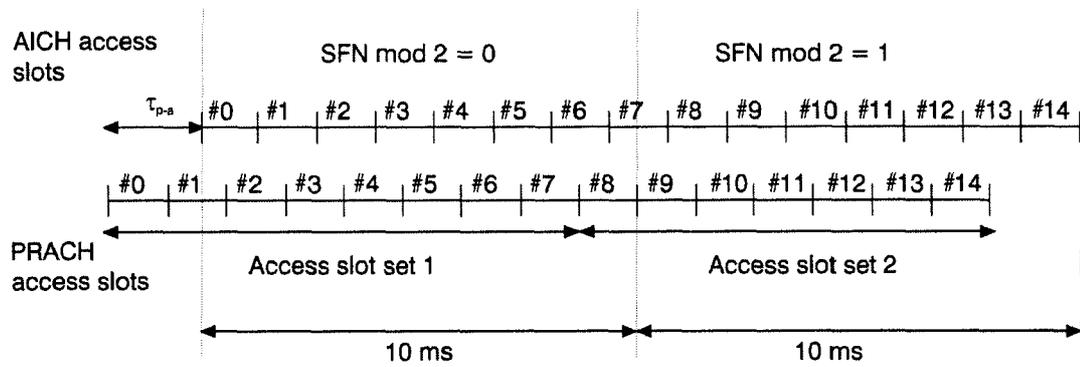


Tabla 2 Slots de Acceso del canal RACHA y la relación con el canal de adquisición (AICH) del DL PRACH ( $\tau_{p-a} = 7680$  chips).

FIG. 6

SFN modulo 8 of corresponding P- CCPCH frame	Sub-channel number											
	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7				
1	12	13	14						8	9	10	11
2				0	1	2	3	4	5	6	7	
3	9	10	11	12	13	14						8
4	6	7					0	1	2	3	4	5
5			8	9	10	11	12	13	14			
6	3	4	5	6	7					0	1	2
7						8	9	10	11	12	13	14

Tabla 3. Slots de acceso de los distintos sub-canales RACH.

**FIG. 7**



OFICINA ESPAÑOLA  
DE PATENTES Y MARCAS

ESPAÑA

②<sup>1</sup> N.º solicitud: 200900376

②<sup>2</sup> Fecha de presentación de la solicitud: 11.02.2009

③<sup>2</sup> Fecha de prioridad:

### INFORME SOBRE EL ESTADO DE LA TÉCNICA

⑤<sup>1</sup> Int. Cl.: **H04W24/08** (2009.01)

### DOCUMENTOS RELEVANTES

Categoría	⑥ <sup>1</sup> Documentos citados	Reivindicaciones afectadas
X	GB 2435987 A (MOTOROLA INC) 12.09.2007, página 4, líneas 27-31; página 10, líneas 22-31; página 14, líneas 1-5; página 18, líneas 20-23.	1-3

Categoría de los documentos citados

X: de particular relevancia

Y: de particular relevancia combinado con otro/s de la misma categoría

A: refleja el estado de la técnica

O: referido a divulgación no escrita

P: publicado entre la fecha de prioridad y la de presentación de la solicitud

E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

**El presente informe ha sido realizado**

para todas las reivindicaciones

para las reivindicaciones nº:

Fecha de realización del informe  
02.04.2012

Examinador  
M. Muñoz Sanchez

Página  
1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04W

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 02.04.2012

**Declaración**

<b>Novedad (Art. 6.1 LP 11/1986)</b>	Reivindicaciones 1-3	<b>SI</b>
	Reivindicaciones	<b>NO</b>
<b>Actividad inventiva (Art. 8.1 LP11/1986)</b>	Reivindicaciones	<b>SI</b>
	Reivindicaciones 1-3	<b>NO</b>

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

**Base de la Opinión.-**

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

**1. Documentos considerados.-**

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	GB 2435987 A (MOTOROLA INC)	12.09.2007

**2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración****Reivindicaciones independientes**

Reivindicación 1: Siguiendo la redacción de la reivindicación 1 el documento D01 divulga un método de detección de interferencia (jamming) en un sistema celular en el que existe un terminal móvil capaz de detectar jamming (pág 10 líneas 22-31). Por otro lado se realiza una monitorización por parte de la estación base (BS) que da servicio al terminal móvil de los mensajes recibidos de este y otros terminales y cuando el número de mensajes supera un cierto umbral además de producirse dichos mensajes con una cierta asiduidad el jamming se confirma (pág 14 líneas 1-5).

El documento D01 divulga también la forma en la que el mensaje de señalización es transmitido (a través del canal de acceso aleatorio, pág 18 líneas 20-23), el uso de estándares de comunicaciones móviles celulares y la estrategia de polling para comprobar que efectivamente existe jamming producido por un inhibidor (pág 4 líneas 27-31) siendo las diferencias con el documento de la solicitud los valores de los parámetros en la aplicación de los estándares. Por tanto D01 afecta a la actividad inventiva de la reivindicación 1 según el artículo 8.1 de la Ley de Patentes.

**Reivindicaciones dependientes**

Reivindicaciones 2, 3: Las reivindicaciones 2 (tipo de red) y 3 (localización del dispositivo de seguimiento) presentan opciones de diseño evidentes para el experto en la materia y por tanto D01 afecta a la actividad inventiva de las reivindicaciones 2 y 3 según el artículo 8.1 de la Ley de Patentes.