Capítulo 2

Sistema de detección de inhibidores de enlace descendente

2.1 Arquitectura

Debido al elevado coste que supone la modificación de software del terminal, y especialmente, de la estación base de un sistema de comunicaciones móviles celular, en [1] y [2] se diseñó un método no intrusivo para la detección remota de un inhibidor de frecuencia, que no requiere modificar la estación base, puesto que este puede ser implementado en un dispositivo externo. Este dispositivo podría ser integrado en la estación base pero a un mayor coste económico. La solución propuesta es independiente del operador móvil, lo que incrementa enormemente su potencial explotación comercial.

En este capítulo se explicará la solución, y como desarrollar un demostrador de la misma.

2.2 Terminal móvil inhibido

A continuación se describen los pasos realizados en la primera fase, la de detección.

2.2.1 Fase de detección

En esta sección se describe la fase de detección del inhibidor de frecuencia. En la siguiente figura se muestra el esquema de la aplicación instalable en el terminal para que se pueda localizar la presencia de un inhibidor y luego se describe el funcionamiento de esta.

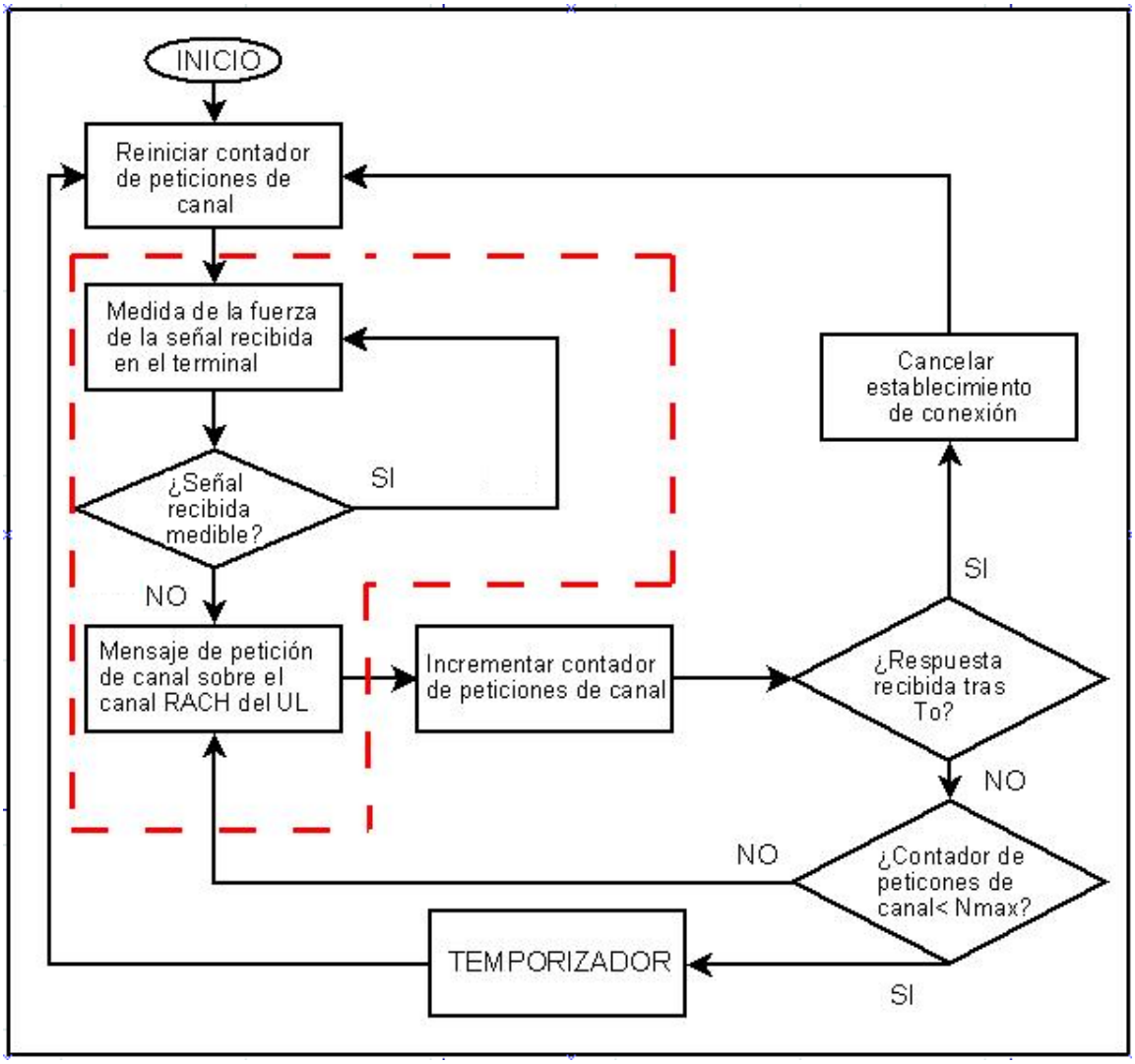

Figura 4. Diagrama de flujo del terminal inhibido.

Dentro de la línea discontinua, se pueden ver los pasos que constituyen la funcionalidad adicional que se ha programado en el terminal. El resto de etapas ya están programadas en el teléfono, y son realizadas en la mayoría de estándares de comunicación inalámbrica.

Primero, el terminal monitoriza la potencia de la señal recibida en la portadora de señalización. En el momento en que el terminal no reciba la señal adecuadamente, se inicia el proceso de señalización de una posible situación de inhibición, intentando establecer conexiones con la estación base. Si un inhibidor o cualquier otro dispositivo están interfiriendo los canales del DL, el terminal no puede realizar el proceso de señalización completo, puesto que el establecimiento del canal de señalización dedicado no puede ser realizado. El proceso se desarrolla en los siguientes pasos:

- El terminal envía una petición de canal dedicado en el canal de acceso aleatorio (RACH) del enlace ascendente.

- Al existir un número máximo de repeticiones de la petición anterior, que se va a denominar N_{max}, el contador de peticiones de canal es incrementado en una unidad. El valor del parámetro N_{max} depende del estándar de comunicación inalámbrica.

- El terminal espera respuesta en el correspondiente canal de control común descendente hasta un máximo de T_0 segundos, donde T_0 depende del estándar de comunicación inalámbrica considerado. Si se recibe respuesta (positiva o negativa) de la red, no existe presencia significativa de interferencia y el proceso de establecimiento de conexión será cancelado. 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.

- Cuando el contador de peticiones de canal alcanza el valor N_{max}, el terminal comienza de nuevo el proceso, monitorizando el valor de la señal y reiniciando el valor del contador de peticiones de canal. Aunque como se ve en la figura, antes deberá de esperar a que un temporizador haya expirado. Este temporizador va a depender del estándar GSM.

2.3 Dispositivo de seguimiento

Este dispositivo ha sido diseñado externamente a la estación base, por lo que es independiente al operador móvil y su objetivo es, monitorizar el canal de control común descendente.

Se ha programado mediante una plataforma SDR (Software Defined Radio) para implementar un escáner de frecuencia sintonizado a la portadora del enlace descendente. Con este se desea monitorizar el canal de control común en el sentido descendente y encontrar continuas repeticiones de respuestas a peticiones de establecimiento de canal, que el terminal inhibido nunca recibirá, con lo que continuará retransmitiendo dichas peticiones, como se explica en la sección anterior. Al detectarse este comportamiento en el tráfico de señalización, se inicia un control de estado de los terminales que están siendo protegidos frente a inhibición.

El concepto fundamental de la tecnología SDR es acercar el procesamiento software tanto como sea posible a la antena. Es decir, el diseño de sistemas de radiocomunicaciones definidos en software se basa en la utilización de dispositivos que convierten las ondas de radio a la entrada de la antena en señales digitales procesables en una computadora de forma transparente desde el punto de vista del software.

En la elección del receptor se ha seleccionado, como plataforma SDR, el software GNU Radio [4], y el dispositivo hardware USRP (Universal Software Radio Peripheral), desarrollado por Ettus Research LLC [5]. El USRP se utiliza para digitalizar las señales analógicas recibidas en las frecuencias de radio para que puedan ser procesadas en un ordenador de propósito general.

Figura 5. Receptor USRP.

Una ventaja adicional referente al empleo específico de estos elementos, radica en que además de que GNU Radio y el USRP están basados en software y hardware libre respectivamente, el esquemático del USRP está disponible públicamente. Esto hace que las posibilidades en cuanto a soporte y desarrollo del sistema sean elevadas.

2.3.1 Descripción del USRP y de sus componentes

El USRP se emplea para realizar la conexión entre el dominio de RF (Radio Frequency) y la computadora. Este dispositivo toma a su entrada las señales de radio provenientes de la antena, que se pasan a frecuencia intermedia en el front-end, luego se digitalizan y se pasan a banda base. Por último se podrán obtener en el ordenador a través del puerto USB. Será deseable que el USRP realice el mínimo procesamiento para que el sistema sea lo más independiente del hardware como sea posible.

Para entender el funcionamiento del USRP con mayor profundidad, se describirán a continuación los componentes que lo constituyen:

- Controlador USB
- ADC (Analog to Digital Coverter)
- DAC (Digital to Analog Concerter)
- PGA (Programmable Gain Amplifier)
- Daugtherboards
- FPGA (Field Programmable Gate Array)

Controlador USB 2.0

El USRP se conecta con el ordenador a través de puerto USB. En particular, utiliza la versión 2.0, no permitiendo un buen funcionamiento con la versión 1.1. Esto permite disponer a la salida una tasa de datos de 32 MB/s. Esto puede provocar restricciones en el rendimiento del sistema, pudiendo no ser suficiente con esta tasa para unos requerimientos específicos.

ADC (Analog to Digital Converter)

El convertidor analógico a digital tiene la función de digitalizar las señales analógicas a su entrada. En concreto, el USRP consta de cuatro convertidores analógico a digitales que operan a 64x106 muestras por segundo con una precisión de 12 bits.

DAC (Digital to Analog Converter)

El convertidor digital a analógico convierte las señales digitales a su entrada en analógicas. En particular, el USRP está dotado de cuatro convertidores que operan a 128x106 con una precisión de 14 bits. En el USRP se emplean en el trayecto de transmisión para la emisión de señales definidas por software, por lo que no se contempla su empleo en este proyecto.

PGA (Programmable Gain Amplifier)

En el trayecto de recepción, el amplificador de ganancia programable amplifica la señal recibida, en caso de que ésta sea débil, antes de ser procesada por el convertidor analógico a digital para aprovechar el rango dinámico del mismo. La ganancia de este amplificador es configurable por software con valores que oscilan desde los 0 dB hasta los 20 dB.

Daughterboards

Para que el USRP pueda trabajar en diferentes bandas del espectro de radiofrecuencia se debe de dotar al mismo de alguna placa específica para la banda de interés. Estas placas se conocen con el nombre de "daughterboards" por la existencia de una placa base en la que se encuentran el resto de componentes del USRP y proporciona cuatro slots donde es posible conectar hasta dos placas receptoras y dos transmisoras, o bien únicamente dos placas transceptoras (RFX). Estas placas se utilizan como interfaces receptoras RF (escáner de frecuencia), o bien como transmisoras. Además cada placa tiene acceso a dos de los cuatro ADC/DAC (transmitiendo datos al ADC y recibiendo datos del DAC). Por lo tanto, es posible conectar múltiples placas a la placa base, permitiendo la transmisión y recepción simultánea en el USRP.

FPGA

La FPGA juega un papel muy importante en el USRP y es considerada el corazón del mismo. Está conectada a todos los convertidores ADCs y DACs. Básicamente, su función es llevar a cabo operaciones a alta frecuencia y reducir la tasa de datos para que el flujo de bits resultante se pueda transmitir por el puerto USB 2.0. Así, la FPGA está conectada al controlador del puerto USB. Ambos, el controlador USB y la FPGA son programables a través del bus USB.

Por configuración, la operación a alta frecuencia que realiza la FPGA es conocida como DDC (Digital Down Converting). Su función es la conversión a banda base de la frecuencia IF (Intermediate Frequency) presente a la salida del ADC. A partir de esta operación, la señal es diezmada para que la tasa de datos se adapte a la velocidad de transmisión USB y sea razonable para su posterior procesamiento en el ordenador.

GNU Radio

GNU Radio es un conjunto de herramientas software de código abierto que provee la funcionalidad de crear sistemas de radiocomunicaciones definidos por software. Para desempeñar esta función, hace uso de diversos lenguajes de programación, cada uno con objetivos diferentes. GNU Radio también incluye gran variedad de librerías de bloques de procesamiento de señal como moduladores, demoduladores, filtros, etc. que se pueden utilizar en el sistema de radiocomunicaciones que se esté diseñando.

Aunque en el principio de operación de GNU Radio está implícita la utilización del USRP, éste no es necesario si no hay necesidad de un procesamiento en tiempo real, ya que es posible trabajar con capturas de ficheros realizadas con este dispositivo.

El software de GNU Radio está organizado en una estructura de dos niveles. Todos los bloques de procesamiento de señal están implementados en C++, mientras que la organización de alto nivel, conectando los bloques de procesamiento de señal entre sí, se implementa en Python. El objetivo es implementar el sistema de comunicaciones en una aplicación en Python que maneje y planifique los bloques de procesamiento creados en C++, dejando toda la carga computacional presente en los mismos en un segundo nivel. Adicionalmente, hay disponible un entorno gráfico para facilitar el diseño del sistema de radiocomunicación, el GNU Radio Companion (GRC).

2.3.2 Fase de señalización

En esta sección se describe el proceso que se pretende llevar a cabo en la fase de señalización para la detección del inhibidor, se puede ver esquematizado en la siguiente figura:

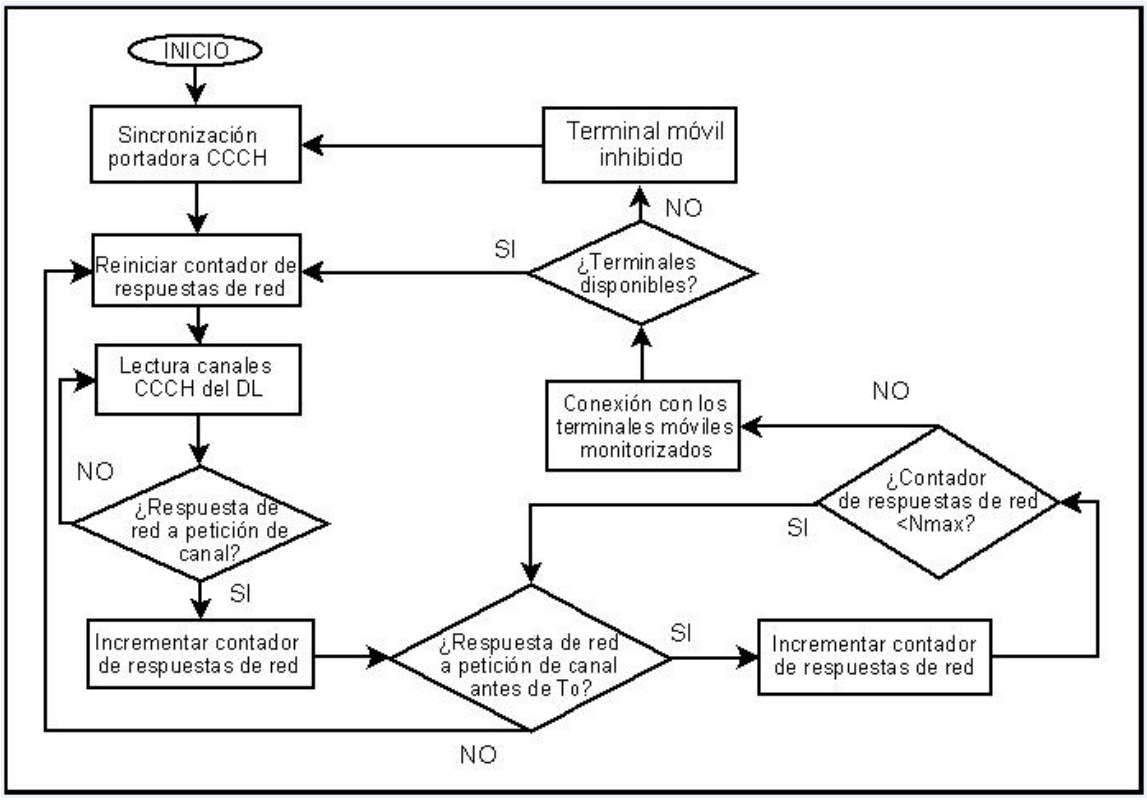

Figura 6. Diagrama de flujo del dispositivo de seguimiento.

El funcionamiento del dispositivo de seguimiento es analizar el tráfico en los canales de control en el descendente con el fin de detectar situaciones sospechosas de inhibición. Una vez que se ha sintonizado y sincronizado a la portadora de señalización, comienza la monitorización de los canales CCCHs en el DL. Cuando ha detectado la primera respuesta de la red a una petición de canal de señalización dedicado, se incrementa el contador de respuestas de red. Como ya se ha comentado anteriormente, en el apartado 2.2.1, un terminal inhibido repetirá sistemáticamente la petición de canal varias veces al no recibir respuesta de la red. Tras la lectura de cada respuesta de la red, el dispositivo de seguimiento espera un nuevo mensaje de respuesta en los siguientes T_0 segundos. En caso de no leer otra respuesta, se supone que la respuesta de la red anteriormente registrada no fue emitida por un móvil inhibido. En este caso, se resetea el contador de respuestas de

red. 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. Cuando dicho contador alcanza el umbral N_{max}^{jam}, la situación se considera como sospechosa de la existencia de un inhibidor y se activa la condición de alarma.

El siguiente paso es comprobar si realmente el terminal está inhibido. Esto puede lograrse con un intento de conexión o polling. El propio receptor envía un mensaje al conjunto de los terminales supervisados y espera asentimiento. En el caso de que no haya respuesta de alguno de los terminales, se considerará que éste está bajo la influencia de interferencias causadas por un inhibidor.

Si tomamos $N_{max}^{jam} > N_{max}$, cuando el contador alcance N_{max}, el dispositivo debe esperar la siguiente respuesta de red en un tiempo de T_0+T_{emp} segundos, donde T_{emp} es la duración del temporizador en la Figura 4. En este caso, la condición de contador de respuestas de red menor que N_{max} es modificada para asegurar dicha situación. Fijar $N_{max}^{jam} > N_{max}$ es una buena opción para minimizar el riesgo de falsa alarma.

2.4 Diagrama de paso de mensajes: terminal inhibido - estación base

A continuación se muestra un diagrama que ilustra los mensajes intercambiados por el terminal y la red una vez que el primero ha detectado una posible situación de inhibición. Los pasos seguidos coinciden con los descritos en los diagramas de flujo de los apartados anteriores, Figura 4 y Figura 6.

El primer mensaje de petición de canal (Channel Request message) (1), en la Figura 7, llega a la estación base con un determinado retardo de propagación. Tras un determinado tiempo de procesamiento, la BTS manda un mensaje de respuesta a dicha petición a través de los canales comunes del DL. Dicho mensaje no se recibe en el terminal en caso de inhibición pero sí se detecta en el dispositivo de seguimiento (4) puesto que éste se colocará siempre cerca de la BTS si no se programa en ella misma. En todo caso, lejos de la influencia del posible inhibidor de frecuencia. Cada T_0 segundos, tiempo que se diseña como mayor a la suma de los retardos de propagación y de procesamiento de la BTS, un nuevo mensaje de petición de canal se envía (6), siendo de nuevo detectado en el dispositivo de

seguimiento. Después de que éste detecte N_{max}^{jam} retransmisiones (12), se realiza un intento de conexión (13).

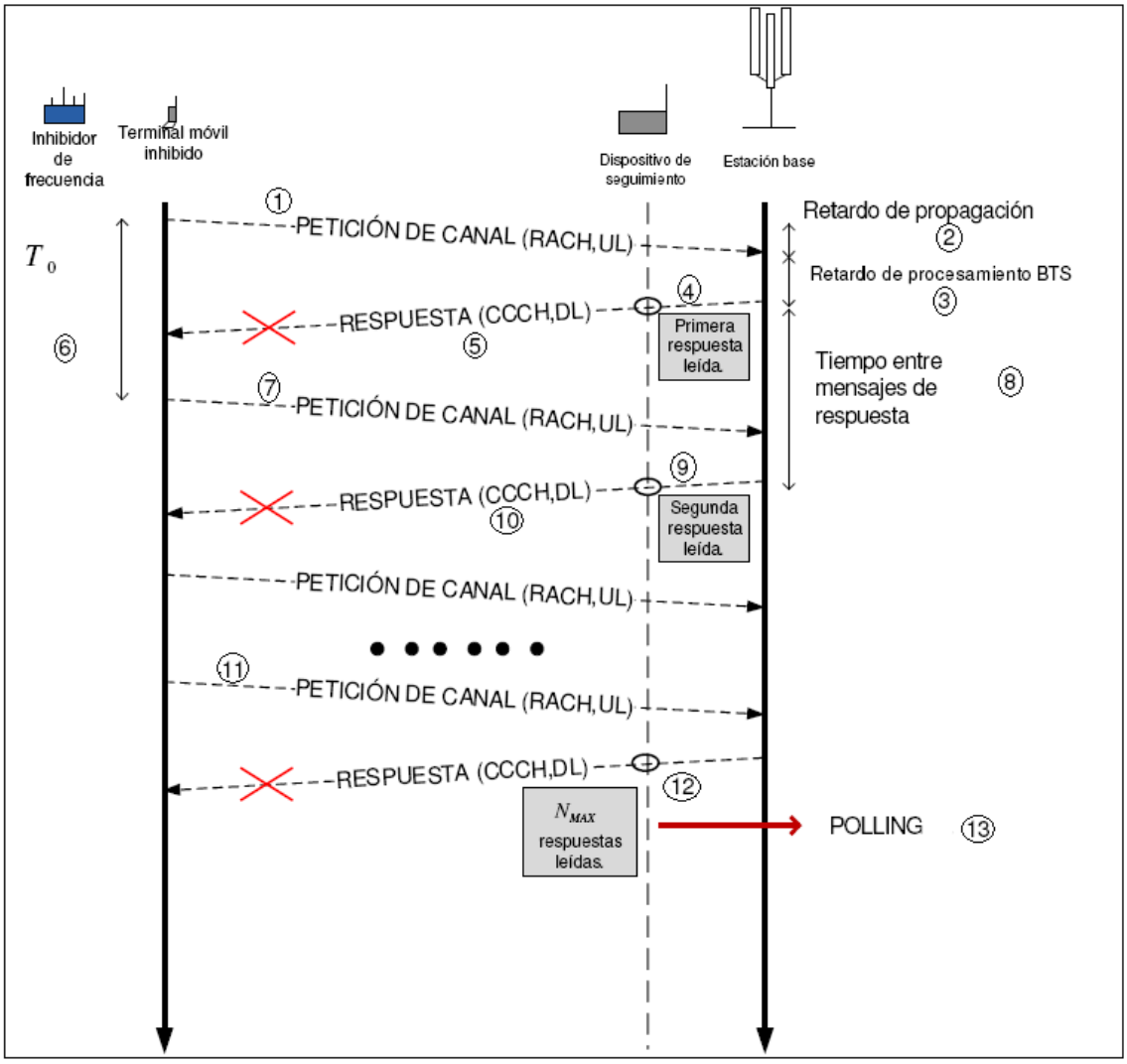

Figura 7. Paso de mensajes entre el terminal inhibido y la red.

Por tanto, el proceso completo de detección de un inhibidor implica un retardo máximo de $N_{max}^{jam} T_0$ segundos si $N_{max}^{jam} < N_{max}$ ó $N_{max}^{jam} (T_0+T_{emp})$ cuando $N_{max}^{jam} > N_{max}$. Por tanto, podemos detectar remotamente la presencia de un inhibidor en un tiempo estimablemente pequeño.

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 $N_{max}^{jam} > N_{max}$

respuestas de red a peticiones de canal separadas un tiempo menor que T_0 segundos.

El método de detección podría también implementarse 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, se fuerza la transmisión del mensaje de petición de canal en el momento en que se detecta una posible inhibición.