BLOQUE I

Descripción del sistema de detección

Capítulo 1

Introducción

En este proyecto se pretende dar solución a los problemas que surgen en redes de telecomunicaciones inalámbricas cuando determinados elementos interfieren en la comunicación del sistema móvil. Se desea obtener así, un dispositivo que detecta fallos en el enlace descendente (DL), entre la estación base y un terminal.

Los elementos interferentes serán inhibidores de frecuencia de corto alcance, ya que estos pueden evitar la transmisión de alarmas en sistemas inalámbricos. Por lo tanto el principal uso práctico del proyecto va a ser un sistema de seguridad contra estos inhibidores de frecuencia. El sistema permite detectar cuando un terminal no está en disposición de enviar una alarma debido a la presencia del inhibidor.

Se puede dividir el problema que se trata de resolver en dos fases, siguiendo con la metodología propuesta en [1] y [2] "Método de detección remota de interferencia en el enlace descendente de sistemas inalámbricos celulares de telecomunicación". Primero el terminal detecta inhibición analizando la fuerza de la señal recibida. Segundo, el terminal debe señalizar la situación observada a la red.

1.1 Objetivos

El objetivo del proyecto es hacer un prototipo para el sistema propuesto en [1] y [2], para ello se diseña un mecanismo que localice cuando un terminal móvil se encuentra afectado por altas interferencias en el enlace descendente. Además, el dispositivo es no intrusivo, es decir no es necesario modificar la estación base ni el protocolo. Se han diferenciado dos fases: detección y señalización.

En la fase de detección, cuando el terminal no reciba señal de la red, y por lo tanto se encuentre en una supuesta situación de inhibición, se iniciará el proceso de establecimiento de conexión. Esto se realiza añadiendo una funcionalidad al terminal, por lo que no es necesario modificar protocolos GSM o GPRS ni en el terminal ni en la estación base.

En la fase de señalización, se necesita un dispositivo capaz de detectar la señalización emitida por el terminal inhibido. Se ha optado por usar un terminal externo a la estación base, programando una plataforma SDR (Software Defined Radio).

El proyecto fin de carrera presentado se centra principalmente en la fase de detección, cuyo objetivo es desarrollar la funcionalidad del terminal, para que sea capaz de analizar la intensidad de la señal recibida en el teléfono desde la estación base y dependiendo de su valor, iniciar establecimientos de conexiones.

1.2 Contenido de la memoria

El proyecto se ha dividido en tres bloques principales, en el Bloque I se encuentran los dos primeros capítulos, donde se describe el sistema de detección diseñado.

En el primer Capítulo se ha pretendido hacer una breve presentación del trabajo realizado para la ejecución de este proyecto fin de carrera, resaltando los aspectos fundamentales que se van a tener en cuenta, así como los principales objetivos planteados.

En segundo lugar se detallará con más precisión el escenario estudiado, las dos fases en las que se ha dividido la solución propuesta y las principales características de los elementos que interfieren: inhibidor de frecuencia, terminal

inhibido y receptor. Se describen los pasos que siguen cada uno de estos elementos para actuar en este escenario.

En el Bloque II, se encuentran los cuatro capítulos siguientes, donde se ven principalmente las herramientas utilizadas para el diseño de la aplicación del terminal.

En el Capítulo tercero se hace una introducción al estándar GSM, describiendo las características más relevantes que intervienen en este proyecto. Se especificarán cuales son los diferentes mensajes y canales usados para la implementación del dispositivo en la red GSM.

A partir del cuarto Capítulo se entra en más detalle en el desarrollo de la implementación del terminal inhibido. Para esto primero se detallan la evolución, las características y la arquitectura del sistema operativo elegido para desarrollar la aplicación, así como también las características de otros sistemas operativos que podrían haberse usado.

En el quinto Capítulo se describen algunas características de la programación orientada a objeto en C++ y algunas características específicas del lenguaje empleado.

En el Capítulo sexto se especifica el software development kit (SDK), donde están incluidas todas las funciones y APIs para el desarrollo de la aplicación del terminal, que nos permiten el acceso a algunas de las funcionalidades de los teléfonos móviles.

Los tres capítulos anteriores son los más teóricos del proyecto, pero imprescindibles para el desarrollo de la implementación del terminal. Puesto que constituirán la base en el diseño de aplicaciones para smartphones.

En el Bloque III, se verá como se ha desarrollado en la práctica la aplicación del terminal.

En el Capítulo séptimo se describe en más profundidad la funcionalidad añadida al teléfono, con las principales clases y funciones que se han usado.

A continuación se dedica un capítulo para ver las pruebas realizadas y los resultados obtenidos.

Finalmente se incluyen las conclusiones obtenidas y se sugieren algunas mejoras al proyecto o líneas de avance a partir del trabajo realizado.

También se adjuntan un par de anexos, en el primero se dan los principales pasos para crear una aplicación en el entorno de desarrollo seleccionado y en el segundo anexo se incluye el código del programa diseñado para la funcionalidad del terminal.

1.3 Necesidades a cubrir en el proyecto

Para la localización de un inhibidor de frecuencia, es necesario el diseño de: primero, un mecanismo de detección en un terminal móvil que sea capaz de distinguir una posible situación de inhibición. Segundo la programación de un dispositivo capaz de seleccionar y filtrar los mensajes de señalización que la estación base envía al terminal inhibido.

Para cubrir estas necesidades se irán desarrollando tanto en este capítulo, como en los siguientes, todos los elementos que intervendrán en el proyecto, así como los pasos que se han seguido para su ejecución.

1.3.1 Descripción del escenario analizado

El proyecto consta de dos elementos encargados de la detección y señalización de interferencia o inhibición: el terminal inhibido, y el dispositivo de monitorización o seguimiento. En la siguiente figura se muestran todos los elementos que interfieren en el escenario analizado:

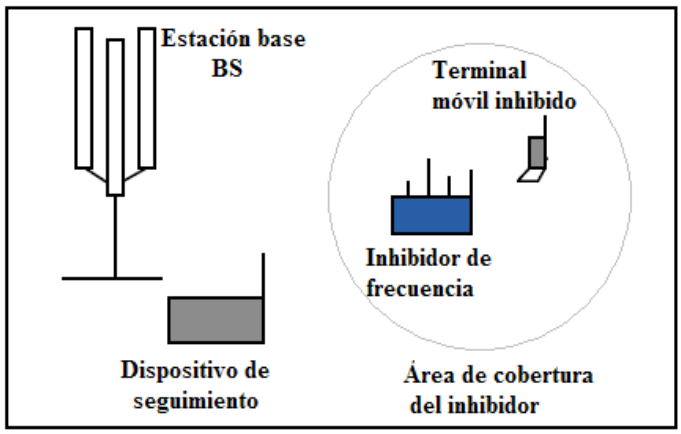

Figura 1. Escenario general propuesto.

Si el inhibidor se enciende y actúa únicamente en el enlace descendente, el enlace ascendente puede ser utilizado por el terminal para enviar información a la estación base, aunque no podrá recibir información alguna. Inicialmente, el terminal estará correctamente registrado a la red móvil, esto es, correctamente sincronizado y sintonizado a la configuración radio de la red. Además, en él se ha programado una funcionalidad añadida con respecto a un terminal estándar.

Cuando el terminal inalámbrico móvil se vea afectado por interferencias en el enlace descendente debido a la presencia de un inhibidor de frecuencia, primero detectará la inhibición, y seguidamente intentará establecer conexiones por el enlace ascendente para indicar dicha situación. Sin embargo, antes de poder establecerse la comunicación se debe crear un enlace de señalización para lo cuál es necesario el intercambio de mensajes entre el terminal y la estación base. Al encontrarse inhibido el descendente no se establece el enlace de señalización y mucho menos se podrá realizar la llamada. Por lo tanto, el terminal inhibido realiza sucesivas peticiones de canal de señalización para poder identificarse en la red.

El dispositivo externo utilizado para detectar la señalización, analiza los mensajes emitidos por la estación base, en respuesta a continuas peticiones de establecimientos de conexión, ya que el terminal inhibido es incapaz de recibir las contestaciones de la estación base y por lo tanto repite varias veces el mensaje, como se ha comentado anteriormente. Para realizar esta tarea tendrá que monitorizar el canal de control común CCCH, por donde la estación base envía la señalización. Al detectarse este comportamiento el receptor podrá comprobar si el terminal inhibido realmente lo está.

1.3.2 Inhibidores de frecuencia

Los inhibidores son dispositivos electrónicos que impiden o dificultan las transmisiones radioeléctricas en un determinado rango de frecuencias mediante la emisión de una señal de mayor intensidad que la señal útil que el emisor desea transmitir. Se utilizan principalmente por motivos de seguridad o malintencionadamente.

Figura 2. Inhibidor de frecuencia.

Básicamente el funcionamiento del inhibidor [3] es emitir una señal que carece de información útil, únicamente es una señal generada por un generador de onda, que al emitirse con mayor intensidad que los sistemas de transmisión a interferir, las suprime, evitando que emisor y receptor establezcan la comunicación.

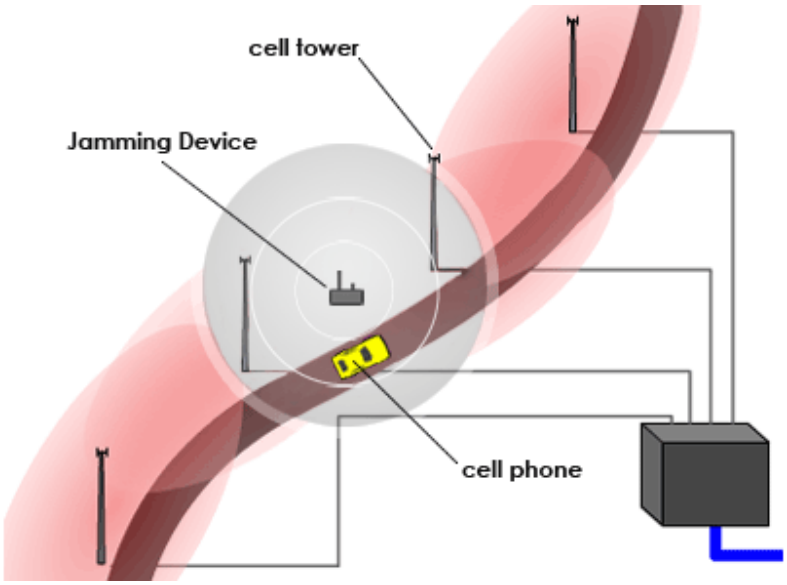

Figura 3. Ejemplo de inhibición en estaciones base y terminal móvil [3].

La transmisión de la señal de bloqueo se realiza en el mismo espectro de radiofrecuencia que los terminales móviles, interrumpiendo bien la comunicación bidireccional, o la unidireccional entre terminales y estaciones base que se encuentren dentro de la zona de cobertura del inhibidor.

Un inhibidor puede ser un dispositivo muy sencillo con un interruptor de encendido y apagado y un led, u otros más complejos pueden tener más interruptores que permitirán al usuario seleccionar la frecuencia que se quiera bloquear. Los principales componentes del inhibidor son:

- Antena: transmite la señal de inhibición. Pueden tener antenas internas o externas.

- Oscilador controlado por tensión: genera la señal de radio que interfiere con la señal del dispositivo a inhibir.

- Circuito de sintonización: controla la frecuencia central con la que el inhibidor emite su señal mediante el envío del oscilador de voltaje.

- Generador de ruido: es parte del circuito de sintonía, crea ruido eléctrico aleatorio de salida en un determinado rango de frecuencias que se usan para interrumpir la señal de la red inalámbrica.

- Amplificador RF (etapa de ganancia): controla los niveles de fuerza del circuito de sintonía. Es responsable de impulsar la energía necesaria para las señales de ruido.

- Fuente de alimentación: los inhibidores más pequeños pueden tener una batería o pilas, mientras que si el inhibidor es más potente necesitará conectarse a una toma de corriente.

La mayoría de los teléfonos móviles son dispositivos full-duplex que utilizan multiplexión en frecuencia, dos frecuencias separadas, una para hablar y otra para escuchar, que se usan simultáneamente. Si en una de estas se produce un bloqueo, se imposibilita la comunicación entre los dos terminales. Por lo tanto los inhibidores sólo necesitan actuar en una de ellas.

Los inhibidores fueron diseñados originalmente para aplicaciones militares y de defensa (evitar activación de bombas a través de teléfonos móviles, impedir espionaje corporativo…). Actualmente debido a lo fácil que resulta obtener un inhibidor (por ejemplo, a través de compras por Internet) se ha podido extender su uso para actuaciones fraudulentas, como anular radares o desactivación de alarmas para la detección de robos.

Inhibidores pareados y de enlace descendente

Es importante destacar, que aunque existen diferentes tipos de inhibidores de frecuencia, los que nos afectan en este proyecto son aquellos que han sido diseñados para pasar inadvertidos. Los inhibidores pareados radian ruido en todo el espectro, es decir, tanto en el enlace descendente (DL) como en el ascendente (UL) y por ello podrían ser fácilmente detectados en la estación base, ya que se estaría interrumpiendo gran cantidad de tráfico y también se notaría en los niveles de potencia recibidos. Por lo tanto los inhibidores que se tratan de localizar son aquellos que sólo radiarán ruido en el enlace descendente, evitando así la comunicación en el sentido de la estación base al terminal. Pero no se estaría interfiriendo la comunicación en el ascendente, por lo que el terminal si podrá comunicarse con la estación base, aunque no recibirá la información que la estación base le transmita.