(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 358 442**

(51) Int. Cl.:
H04W 64/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06755778 .5**
(96) Fecha de presentación : **17.07.2006**
(97) Número de publicación de la solicitud: **1908318**
(97) Fecha de publicación de la solicitud: **09.04.2008**

(54) Título: **Métodos de establecimiento de una llamada con un dispositivo móvil y determinación de la dirección del mismo.**

(30) Prioridad: **22.07.2005 GB 0515124**
31.01.2006 GB 0601957

(45) Fecha de publicación de la mención BOPI:
10.05.2011

(45) Fecha de la publicación del folleto de la patente:
10.05.2011

(73) Titular/es: **M.M.I. Research Limited**
Brooke Road
Wimborne, Dorset BH21 2BJ, GB

(72) Inventor/es: **Martin, Paul Maxwell;**
Pridmore, Andrew Paul;
Timson, Anthony Richard y
Dolby, Riki Benjamin

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Métodos de establecimiento de una llamada con un dispositivo móvil y determinación de la dirección del mismo.

La presente invención se refiere en un primer aspecto a un método, y un aparato asociado, para el establecimiento de una llamada con un dispositivo móvil de comunicaciones y la determinación de la dirección del dispositivo móvil de comunicaciones.

En aplicaciones de seguridad, tales como la búsqueda de dirección, es necesario establecer alguna forma de llamada con un dispositivo móvil de comunicaciones. Sin embargo un problema con los métodos convencionales de establecimiento de una llamada es que no es no están cubiertos.

En el documento WO 2005/011317 una estación base virtual (VBS) hace que la estación móvil (MS) transmita una señal de respuesta de paginación RES, y realiza el búsqueda de dirección sobre esa señal. La VBS distingue la señal de respuesta de paginación RES en base a la información de identificación ID contenida en la misma a partir de las señales de respuesta de paginación de otras estaciones móviles que también se reciben sobre este canal SDCCH o sobre otros canales. En otras palabras, puede haber otras MS transmitiendo sobre el mismo canal (esto es, no es un "canal silencioso") pero la señal requerida se extrae sobre la base de la información de identificación ID. El problema con el documento WO 2005/011317 es que se requiere un procesamiento extra en el equipo de búsqueda de la dirección para extraer la información de identificación ID y de este modo distinguirla sobre las señales de respuesta de paginación interferentes.

En el documento EP-A-1199903 una estación base virtual (VBTS) establece una "llamada silenciosa" con una estación móvil (MS) y a continuación realiza la búsqueda de dirección en base a las señales recibidas. Sin embargo, el documento EP-A-1199903 no presenta ninguna solución al problema de la interferencia del canal compartido por otras MS.

Un primer aspecto de la invención proporciona un método para la determinación de la dirección de un dispositivo móvil como se expone en la reivindicación 1.

El primer aspecto de la invención proporciona un método de establecimiento de la denominada "llamada ciega" – esto es, una conexión de señalización, con o sin intercambio de datos de usuario, que no proporciona una alerta visual o audible al usuario del dispositivo. Tal "llamada ciega" puede usarse entonces para la búsqueda de dirección.

La reciente disponibilidad de los teléfonos móviles de la Tercera Generación y dispositivos relacionados conduce a un requisito de nuevos métodos para localizar los teléfonos de 3G que usan las técnicas del Acceso Múltiple por División de Código (CDMA) sobre la interfaz aire. Se requieren nuevas técnicas para el seguimiento de los teléfonos que son completamente diferentes a las técnicas utilizadas para el seguimiento de los teléfonos de GSM.

Obsérvese que las redes 3G incluyen una protección de seguridad adicional mediante un mecanismo conocido como la autenticación mutua. Esta técnica involucra una autenticación de dos etapas en las que a) el UE se autentica con la red y b) la red se autentica con el UE. En GSM, sólo se aplica a), conduciendo a la posibilidad de un ataque de seguridad a través de una falsa estación base. La autenticación mutua inhibe el mecanismo convencional para el establecimiento de un teléfono móvil como una baliza de RF y posibilitando que el equipo de búsqueda de la dirección localice la baliza sobre una frecuencia/código/ranura temporal conocidos. Esto es porque el UE ignorará los mensajes que no son de un dispositivo de red adecuadamente autenticado conduciendo a transmisiones del UE que se terminan abruptamente en un punto tal en el intercambio de protocolos en el que el UE determina que la red con la que está hablando tiene datos de protección incorrectos o pérdida de protección de "integridad" cuando es obligatorio por las especificaciones.

Las redes UMTS transmiten sobre el aire usando la tecnología CDMA (acceso múltiple por división de Código). Esto significa que la señal procedente de un dispositivo de transmisión 3G único es muy difícil de distinguir del ruido de fondo, porque la transmisión se aleatoriza usando un patrón que difunde la potencia de señal a través de un amplio intervalo de frecuencia. Es posible decodificar la señal procedente de un dispositivo único si se conoce el código de aleatorización que se usó en el transmisor.

La naturaleza del espectro expandido de la señal CDMA hace la búsqueda de la dirección en el dominio de la frecuencia mucho más difícil porque la señal transmitida es muy difícil de distinguir del ruido.

De este modo, en una realización de la invención la señal de localización es una señal de localización codificada (por ejemplo desde un dispositivo CDMA) que se decodifica, y la señal de localización decodificada se usa para determinar la dirección del dispositivo.

Ahora se describirán realizaciones de la invención con referencia a los dibujos adjuntos, en los que:

la Figura 1 muestra un sistema para la determinación de la dirección de un dispositivo móvil de comunicaciones GSM;

la Figura 2 muestra una Estación Base Introducida Separadamente (SIBTS);

la Figura 3 muestra un sistema para la determinación de la dirección de un dispositivo móvil de comunicaciones 3G;

la Figura 4 muestra un NodoB introducido Separadamente (S|NodoB);

la Figura 5 muestra diversas asignaciones de canal en un sistema CDMA;

la Figura 6 muestra un buscador de dirección; y

la Figura 7 muestra un formato de representación.

1.0 GSM

Refiriéndonos a la Figura 1, tres estaciones base (BTS) 1-3 forman parte de una red para comunicar con un dispositivo móvil GSM (MS) 4.

También es conocida una Estación Base Introducida Separadamente (SIBTS) 10. La SIBTS 10 se muestra en detalle en la Figura 2. La SIBTS obtiene parámetros GSM a partir de un teléfono móvil de prueba 16, y realiza un subconjunto de funciones de una red GSM completa, que varía desde los intercambios de protocolo de la interfaz aire en el Sistema de Estación Base (BBS) 11 a las funciones orientas al conmutador en el Centro de Conmutación Móvil (MSC) 12 y las funciones de seguridad y autenticación del Registro de Localización Local (HLR) 13, el Registro de Localización de Visitantes (VLR) 14 y el Centro de Autenticación (AUC) 15.

La SIBTS 10 tiene una memoria 17 que almacena la Identidad del Abonado Móvil Internacional (IMSI), la Identidad del Abonado Móvil Temporal (TMSI) y la Identidad del Equipo Móvil Internacional (IMEI) de la MS 4 (y cualesquiera otras MS que se esté supervisando la SIBTS). La IMSI y la IMEI pueden obtenerse descargándolas directamente desde la MS 4. Esto es, la IMSI puede obtenerse extrayendo la tarjeta SIM de la MS 4, e invirtiendo la tarjeta SIM dentro de un lector de tarjetas SIM disponible comercialmente, y la IMEI puede obtenerse tecleando *#06# en el teclado de la MS. La IMSI y/o la IMEI también pueden obtenerse directamente del operador de red. Como alternativa, la SIBTS 10 puede interrogar a la MS 4 para adquirir su IMSI y su IMEI, siguiendo un método de la clase del descrito en el documento EP-A-1051043. Esto es, la MS 4 selecciona una estación base (BTS) 1 con el nivel de potencia más alto y acampa en esa BTS 1. La SIBTS 10 (que está tan cerca como sea posible de la MS 4) obtiene la lista BA desde la BTS 1, selecciona una estación base (BTS2) de la lista de BA adyacente a la BTS 1, y opera sobre la frecuencia del canal (BCCH) de la BTS2 a una potencia más alta que la de BTS 1. Esto causa que la MS 4 acampe en la SIBTS 10. La SIBTS 10 emite un código de área de localización (LAC) que difiere de los LAC en la proximidad de la MS. Esto causa que la MS 4 transmita sus códigos de IMSI y de IMEI a la SIBTS 10.

La SIMBTS 10 es típicamente un dispositivo móvil, que puede alojarse en un vehículo. En uso, la SIMBTS 10 se mueve a un área, y se opera para adquirir parámetros de identidad de un conjunto de MS registradas con la red GSM en esa área. Como alternativa la SIMBTS 10 puede estar localizada permanentemente en un área de interés. En ambos casos la SIMBTS 10 transmite eficazmente una falsa difusión de célula que no está bajo el control de la red GSM que proporciona cobertura de esa área.

Una vez que se está en posesión de la IMSI y la IMEI, es posible causar que un teléfono móvil específico transmita sobre una frecuencia de GSM como se haría en una llamada de voz normal. Esto puede conseguirse usando protocolos GSM normalizados, como en una infraestructura GSM convencional. Una vez en transmisión, el buscador de dirección 6 puede usarse para determinar la dirección de la MS 4 con relación al buscador de dirección 6.

El buscador de dirección 6 detecta la radiación procedente de la MS 4 con una disposición de N antenas (por ejemplo cuatro), e infiere la dirección de la MS 4 a partir de los diferentes tiempos de llegada en las N antenas. Ejemplos de buscadores de dirección adecuados son los productos Smart AIR y Esmeralda proporcionados por el Grupo Thales, estando disponibles los detalles en:

- http://www.thalesgroup.com/land-

  joint/portfolio/02_c4isr/05_monitoring/02_smartair/02_05_02.htm; y en

- http://www.thalesgroup.com/land-

  joint/portfolio/02_c4isr/05_monitoring/01_esmaralda/02_05_01.htm

El producto Esmeralda realiza la búsqueda de dirección por un método de interferometría de 2 canales correlativos, o por el método de Watson Watt.

La SIBTS 10 causa que la MS 4 comience la transmisión sin dar ninguna indicación al usuario de estarlo haciendo. Esto se denomina en este documento como una "llamada ciega". Una vez que se ha establecido la llamada ciega, el buscador de dirección 6 puede realizar la búsqueda de la dirección sin que el usuario sepa que esto está pasando.

1.1 Establecimiento de Llamada Ciega GSM

El establecimiento de una llamada ciega se ilustra por el mecanismo mostrado en la Tabla 1. Esto se especifica usando los mensajes de GSM de las capas 2 y 3 intercambiados entre la BSS y la MS. Estos mensajes son mensajes convencionales como se menciona en el documento GSM 04.08 "Mobile Radio Interface Layer 3 Specification". Los mensajes vienen con un número variable de parámetros que son significativos. Sin embargo un ingeniero especialista de GSM sería capaz de determinar qué parámetros deberían estar. El orden de los mensajes está implícito en la columna del Nº de Mensaje.

Tabla 1

Nº de Mensaje	Mensaje	Fuente
1	Petición de Canal RR	MS
2	Asignación Inmediata de RR	BSS
3	Respuesta a la Paginación de RR	MS
4	Petición de Autenticación de MM	BSS
5	Informe de Medición de RR	MS
6	Tipo de Información del Sistema [5 o 6]	BSS
7	Respuesta de Autenticación de MM	MS
8	Comando del Modo Cifrado de RR	BSS
9	Modo de Cifrado de RR Completo	MS
10	Petición de Identidad de MM	BSS
11	Respuesta de Identidad de MM	MS
12	Informe de Medición de RR	MS
13	Tipo de Información del Sistema [5 o 6]	BSS
14	Petición de Identidad de MM	BSS
15	Respuesta de Identidad de MM	MS
16	Petición de Identidad de MM	BSS
17	Respuesta de Identidad de MM	MS
18	Tipo de Información del Sistema [5 o 6]	BSS
19	Comando de Asignación de RR	BSS
20	Asignación Completa de RR	MS
21	Tipo de Información del Sistema [5 o 6]	BSS
22	A continuación repetición de la Información del Sistema y mensajes de Información de Medición de RR	
	Terminación de la Llamada Ciega	
1	Liberar el Canal de RR	BSS

El principio general es que se envía una petición de llamada al dispositivo (en este caso la petición de llamada

constituye números de mensajes 1, 2, 6, 8, 10, 13, 14, 16, 18, 19 y 21), y la petición de llamada se adapta para causar que el dispositivo transmita una señal de localización mientras que se bloquea un proceso de gestión de la conexión que de otro modo causaría que el dispositivo móvil de comunicaciones proporcionase una alerta visual o audible. En este caso, la petición de llamada omite los mensajes CC (Control de Conexión) originados por la BSS convencional. Por lo tanto, las máquinas de estado de protocolo de la MS asociadas con los mensajes CC no se mueven del estado de reposo.

Obsérvese que son posibles otros órdenes de mensajes. El orden dado anteriormente no es obligatorio. En particular el Informe de Medición de RR y todos los Mensajes de Información de Sistema es obligatorio que se transmitan dentro de un cierto tiempo, por lo tanto estos mensajes pueden aparecer en instantes impredecibles en las secuencias de mensajes.

El método descrito anteriormente manipula los protocolos de GSM normalizados para asegurar que el protocolo de gestión de la conexión (CC) no causa que el teléfono móvil produzca una "alerta". Los recursos de radio convencionales (RR) y los protocolos de gestión del nivel de movilidad de movilidad (MM) están permitidos para llegar al punto en el que se establece una portadora física de RF, pero se bloquean los procesos de gestión de conexión posteriores. Se establece un canal de tráfico GSM (TCH), pero no se da ninguna indicación de hacerlo sobre la MS 4.

La secuencia de mensajes mostrada en la Tabla 1 puede establecer una llamada ciega con una diversidad de diferentes teléfonos GSM de una diversidad de diferentes fabricantes (y por lo tanto diferentes protocolos de comunicación), tales como Sony Ericsson, y Nokia.

1.2 Búsqueda de la Dirección de GSM

Una vez que se ha establecido la llamada ciega por el método anterior, el buscador de dirección 6 realiza la búsqueda de la dirección sobre la señal de transmisión del enlace ascendente que se transmite por el MS 4 en una ranura temporal de las ocho ranuras en la tasa de trama de GSM. De este modo, en resumen, la SIBTS 10 establece una llamada ciega, causando que el dispositivo transmita una sucesión de señales del localizador (esto es, señales de transmisión del enlace ascendente); y el buscador de dirección 6 recibe las señales del localizador desde la MS 4 sobre un enlace sin hilos, y determina la dirección de la MS 4 midiendo la dirección de llegada de las señales del localizador.

La SIBTS 10 puede causar que la frecuencia del tráfico de GSM a asignar a la frecuencia especialmente seleccionada sea una frecuencia silenciosa donde no hay ningún otro tráfico. Para conseguir esto, la SIBTS 10 supervisa el tráfico sobre una pluralidad de frecuencias; selecciona una frecuencia en base a la supervisión; y causa que la señal de localización se transmita sobre la frecuencia seleccionada. Por lo tanto esto significa que el TCH para la MS 4 es el único transmisor sobre la frecuencia seleccionada y consecuentemente esa frecuencia puede usarse para una búsqueda de dirección única. Esto significa también que el buscador de dirección 6 puede realizarse de forma económica y no tiene que diferenciar entre ranuras temporales (de las cuales hay ocho en un canal GSM) ya que la MS 4 será el único transmisor sobe esa frecuencia de GSM.

Como alternativa, la SIBTS 10 puede causar que la ranura temporal de tráfico de GSM a asignar a una ranura temporal especialmente seleccionada sea una ranura temporal silenciosa en la que no hay ningún otro tráfico. En este caso, puede haber tráfico en otras ranuras temporales en la misma frecuencia.

Una alternativa al método anterior es invocar el Modo de Prueba A o el Modo de Prueba B de GPRS de GSM sobre el aire para causar que la MS 4 comience la transmisión. De nuevo puede aplicarse el principio de canal silencioso como se ha descrito anteriormente. Los Modos de Prueba A y B son modos de prueba de GSM normalizados.

Como se muestra en la Figura 1, la SIBTS 10 y el buscador de dirección 6 están conectados por un enlace de comunicaciones 7. En su forma más básica el enlace 7 puede conseguirse por el operador de la SIBTS 10 llamando al operador del buscador de dirección 6 sobre su teléfono móvil y comunicando la información verbalmente. Sin embargo, el enlace 7 puede ser alternativamente un enlace inalámbrico automatizado directamente entre la SIBTS 10 y el buscador de dirección 6.

El enlace 7 posibilita transmitir la información de canal al buscador de dirección 6. A la recepción de la información del canal, el buscador de dirección 6 está configurado para supervisar una señal de localización sobre un canal identificado por la información de canal. Por ejemplo, la información de canal puede ser un ARFCN particular más la información de la ranura temporal. Esto tiene la ventaja de que puede usarse cualquier canal de GSM que tiene una ranura temporal libre, en lugar de requerir que todo el canal ARFCN de GSM esté libre.

Adicionalmente, un medio en "tiempo real" de señalización desde la SIBTS al buscador de dirección 6 puede indicar cuándo se arranca y se termina una Llamada Ciega específica de GSM. De este modo, la SIBTS 10 envía una petición de supervisión al buscador de dirección 6 a través del enlace 7, y en respuesta a la petición de supervisión el buscador de dirección 6 se activa, y supervisa un canal seleccionado en búsqueda de una señal del buscador. Por lo tanto el operador del buscador de dirección 6, que está casi siempre localizado de forma separada de la SIBTS 10, puede ser más eficaz en sólo la búsqueda de dirección cuando la llamada ciega está activa.

El buscador de dirección 6 puede calcular un intervalo aproximado para la MS, en base a la intensidad de la señal. Esto es más preciso en las localizaciones rurales que en las áreas construidas debido a la carencia de reflexiones de señal.

También, la SIBTS 1 y/o el buscador de dirección 6 pueden causar que la MS 4 aumente la potencia de la señal de localización transmitiendo una petición de aumento de potencia a la MS 4.

2.0 3G

Las Figuras 1 y 2 anteriores muestran un método y un aparato para el establecimiento de una llamada ciega con una MS de GSM, usando una Estación Base Introducida Separadamente (SIBTS) 10, y el buscador de dirección para el dispositivo con un buscador de dirección 6. Las figuras 3 y 4 inferiores ilustran un método equivalente y un aparato que está configurado para funcionar con la red de Tercera Generación (3G).

2.1 Establecimiento de la Llamada Ciega de 3G

La Figura 3 muestra una red 3G que comprende tres NodosB 101-103 difundiendo a las tres células por transmisiones de enlaces descendentes 104-106 teniendo cada uno un código de aleatorización del enlace descendente único. Al moverse dentro de la vecindad de los otros tres NodosB, un dispositivo del Equipo de Usuario (UE) 120 evalúa sobre qué NodoB acampará.

Se requiere al UE 120 para que reevalúe constantemente las señales procedentes de las celdas de su alrededor. Hace esto para asegurar que durante la conexión (datos o voz) está siempre comunicando con el mejor NodoB (el más apropiado). Sin embargo un UE de 3G invertirá la mayor parte de su tiempo sin transmitir voz ni datos en estado de reposo. En este estado de reposo el UE supervisará la intensidad del NodoB en servicio y los otros NodosB vecinos, y si se cumplen los criterios especificados por la red se realizará una re-selección de célula convirtiendo uno de los NodosB vecinos anteriores en el nuevo NodoB en servicio. Si este nuevo NodoB en servicio está en una localización o área de encaminamiento diferente entonces el UE debe realizar un procedimiento de actualización del área de localización o área de encaminamiento para informar a la red de su nueva localización. Esto se hace de modo que la red siempre tendrá una idea de donde está el UE en la red, de modo que en el caso de una petición de llamada entrante al UE, la red puede usar la mínima cantidad de recursos para solicitar al UE el establecimiento de una conexión de señalización.

Cada uno de los NodoB transmite una información difundida que sirve para dos propósitos principales. En primer lugar, parte de esta información se transmite usando códigos y patrones de datos bien conocidos que permiten que el UE reconozca que la señal de RF que se está recibiendo es realmente una célula de UMTS y también permite que el UE realice mediciones de potencia sobre la señal recibida. En segundo lugar, se difunde información descriptiva acerca de la célula. Esta información del sistema se transmite en la forma de Bloques de Información del Sistema (SIBS) que describen muchos parámetros del NodoB y proporcionan suficiente información para que el UE identifique la red móvil a la que pertenece el NodoB, y también para establecer una conexión de señalización si es necesario.

La Figura 4 muestra un NodoB Introducido Separadamente (SINodoB) 100. El SINodoB 100 está configurado para adquirir un parámetro de identidad a partir de un UE registrado con la red 3G de la Figura 3. Esto se consigue emulando un NodoB que usa un método especialmente adaptado para el protocolo UMTS, como se describe con más detalle más adelante.

El SINodoB 100 es típicamente un dispositivo móvil, que puede estar alojado en un vehículo. En uso, el SINodoB 100 se mueve a un área, y se opera para adquirir parámetros de identidad desde un conjunto de dispositivos de Equipos de Usuario (UE) registrados con la red 3G en esa área. Como alternativa, el SINodoB 100 puede estar localizado permanentemente en un área de interés. En ambos casos, el SINodoB 100 transmite eficazmente una falsa difusión de célula que no está bajo el control de la red 3G que proporciona cobertura en esa área.

Para persuadir al UE para que se mueva sobre el SINodoB 100, deben cumplirse ciertos criterios. Principalmente la transmisión debe recibirse en el UE con una intensidad de señal más alta. Incluso una vez que el UE ha tomado la decisión de que el SINodoB 100 es preferente, normalmente se consideraría necesario pasar los procedimientos de seguridad de UMTS para poder recoger cualquier información útil o realizar cualesquiera tareas útiles.

No es necesario emular exactamente toda la configuración de un NodoB existente para ser un candidato adecuado para que el UE se conecte al mismo. Esto hace la tarea de configurar el SINodoB 100 mucho más simple. La razón para esto es que la información del sistema difundida define la configuración de la célula que está transmitiendo esos datos, y las células dentro de la misma red tendrán diferentes configuraciones, de modo que el UE siempre mira los datos de la célula actual para determinar la información necesaria.

Los parámetros clave en la difusión de la célula falsa que se necesitan considerar para su cambio son los que siguen:

- Frecuencia de Célula

- Código de Aleatorización Principal
- Código Móvil del País (MCC) [- en qué país está la célula]
- Código de la Red Móvil (MNC) [- a qué red pertenece esta célula]
- Código del área de Localización (LAC)
- Código del área de Encaminamiento (RAC)
- Potencia de la Célula
- Etiquetas del valor de SIB [- las etiquetas de valor se usan por el UE para detectar si la información de SIB ha cambiado entre lecturas de SIB]
- Contenidos de SIB 18 y SIB 11 para la célula en servicio [- SIB 11 contiene información de control de medición a utilizar por el UE en el modo de reposo / SIB 18 contiene las ID de PLMN de células vecinas a considerar en reposo y en modo conectado].

El MCC y el MNC deben ser los mismos que la célula en servicio para que el UE considere que SINodoB está en la misma red.

La Frecuencia de Célula debe ser la misma que la célula en servicio para hacer el proceso tan fácil como sea posible – las re-selecciones entre frecuencias tienen criterios y procesos más complejos.

Hay varias opciones para configurar los otros parámetros transmitidos por el SINodoB:

1) Los mismos LAC/RAC y códigos de Aleatorización Principal, diferentes etiquetas de valor SIB – Esto imita completamente la célula en servicio, y permite que el SINodoB se apropie activamente del UE.

2) Diferentes LAC/RAC y códigos de Aleatorización Principal– donde está presente el código de Aleatorización en el SIB 11 de la célula en servicio. Esto es imitando un NodoB vecino que el NodoB en servicio ha estado instruyendo al UE para que realice mediciones sobre el mismo – asegurando de este modo que el UE está buscando activamente una célula con las mismas características clave que las que se están transmitiendo por el SINodoB (código de aleatorización principal, y frecuencia). Esto causa que el UE realice una re-selección de célula hacia el SINodoB si la transmisión del SINodoB es de potencia suficientemente más alta que el NodoB en servicio. La cantidad en la cual el SINodoB necesita ser una señal más intensa se define en SIB3 del NodoB en servicio.

3) Diferentes LAC/RAC y código de Aleatorización – ninguna referencia en SIBS del NodoB en servicio.

Una vez que está transmitiendo una célula configurada y adecuadamente intensa, los UE en el área objetivo realizarán una re-selección de célula al SINodoB y establecerán una conexión de RRC con el propósito de realizar el procedimiento de actualización de la localización. La actualización de la localización se requiere porque el LAC del SINodoB es diferente del antiguo SINodoB en servicio. Una vez que se ha establecido la conexión RRC, el SINodoB tiene la oportunidad de realizar otros procedimientos de señalización como se desee.

El protocolo de UMTS está diseñado para mejorar las características de seguridad y de protección de identidad en el sistema GSM. Con este fin, se usan los mecanismos de autenticación e integridad además de las identidades temporales que se encuentran en el GSM. Estas identidades temporales evitan la transmisión frecuente de la identidad de la IMSI y de la IMEI, porque una vez que la red ha asignado al teléfono una identidad temporal a continuación mantiene un mapeo de la nueva identidad con la IMSI.

Existen mecanismos para permitir que la red interrogue a un teléfono por su IMSI y su IMEI y estos se usan para la primera conexión de un teléfono a la red o cuando se ha producido un error y la red necesita re-establecer el mapeo correcto entre una identidad temporal (tal como una TMSI) y su identidad real asociada (tal como una IMSI). En un funcionamiento normal de red casi todas las señalizaciones entre el UE y la red deben realizarse después de que el procedimiento de autenticación se ha completado satisfactoriamente y se ha posibilitado la integridad sobre la conexión de señalización. Esto hace que la falsificación o la modificación de la señalización por una tercera parte sea efectivamente imposible.

A menos que el NodoB esté provisto con un mecanismo para pasar satisfactoriamente los procedimientos de autenticación y de integridad, los protocolos de UMTS están diseñados de modo que no puede conseguirse casi ninguna comunicación útil con el UE. Sin embargo hay "huecos" en los protocolos de UMTS que permiten recuperar la IMEI, IMEI y TMSI desde el UE por el SINodoB 100 sin que se requieran estos mecanismos de seguridad.

Estos "huecos" se describen en el documento 3GPP TS 33.102 versión 3.13.0 Edición de 1999, y en el documento 3GPP TS 24.008 versión 3.19.0 Edición de 1999. Las porciones relevantes de estos protocolos se describirán ahora.

3GPP TS 33.102 versión 3.13.0 Edición de 1999

Este protocolo especifica en la Sección 6.5 que todos los mensajes de señalización excepto los siguientes se protegerán de forma integral:

TRANSFERENCIA A UTRAN COMPLETA

TIPO DE PAGINACIÓN 1

PROMOVER UNA PETICIÓN DE CAPACIDAD

ASIGNACIÓN DE CANAL FÍSICO COMPARTIDO

PETICIÓN DE CONEXIÓN RRC

ESTABLECIMIENTO DE CONEXIÓN RRC

ESTABLECIMIENTO DE CONEXIÓN RRC COMPLETA

RECHAZO DE CONEXIÓN RRC

LIBERACIÓN DE CONEXIÓN RRC (solo CCCH)

INFORMACIÓN DE SISTEMA (INFORMACIÓN DE DIFUSIÓN)

INDICACIÓN DE CAMBIO DE INFORMACIÓN DE SISTEMA

De esta forma estos mensajes no pueden protegerse de forma integral bajo ninguna circunstancias.

3GPP TS 24.008 versión 3.19.0 Edición 1999

Este protocolo especifica una lista de mensajes a los que puede responder el UE, en ciertas circunstancias sin tener que proteger primero la integridad de la red. Específicamente, los estados de protocolo son los siguientes:

Excepto los mensajes listados a continuación, no se procesará ningún mensaje de señalización de capa 3 por las entidades receptoras de MM y GMM o que los redirigen a las entidades CM, a menos que el procedimiento de control del modo de seguridad se active para ese dominio.

- Mensajes MM
- PETICIÓN DE AUTENTICACIÓN
- RECHAZO DE AUTENTICACIÓN
- PETICIÓN DE IDENTIDAD
- ACEPTACIÓN DE LA ACTUALIZACIÓN DE LOCALIZACIÓN (en la actualización de localización periódica sin ningún cambio en el área de localización o identidad temporal)
- RECHAZO DE ACTUALIZACIÓN DE LOCALIZACIÓN
- ACEPTACIÓN DEL SERVICIO CM, si se aplican las dos condiciones siguientes:
- no hay ninguna otra conexión MM establecida; y
- la ACEPTACIÓN DEL SERVICO MM es la respuesta a la PETICIÓN DE SERVICIO CM con IE DEL TIPO DE SERVICIO CM puesto a "establecimiento de llamada de emergencia"
- RECHAZO DEL SERVICIO CM
- ABORTAR
- mensajes de GSM:
- PETICIÓN DE AUTENTICACIÓN Y CIFRADO
- RECHAZO DE AUTENTICACIÓN Y CIFRADO
- PETICIÓN DE IDENTIDAD
- RECHAZO DE UNIÓN

- ACEPTAR ACTUALIZACIÓN DEL ÁREA DE ENCAMINAMIENTO (en la actualización periódica del área de encaminado sin ningún cambio del área de encaminamiento o identidad temporal)
- RECHAZO DE ACTUALIZACIÓN DEL ÁREA DE ENCAMINAMIENTO
- RECHAZO DEL SERVICIO
- ACEPTACIÓN DE SEPARACIÓN (para no apagados)

mensajes CC:

- todos los mensajes CC, si se aplican las siguientes dos condiciones:
- no está establecida ninguna otra conexión MM; y
- la entidad MM en la MS ha recibido un mensaje de ACEPTACIÓN DE SERVICIO CM sin ninguna protección de integridad o cifrado aplicada como respuesta a un mensaje de PETICIÓN DE SERVICIO CM, con el SERVICIO CM

TIPO puesto a 'establecimiento de llamada de emergencia' enviado a la red.

Por lo tanto una Conexión RRC puede establecerse sin requerir protección integral, ya que los mensajes de conexión de RRC están listados como que no requieren protección integral en el documento 3GPP TS 33.102 versión 3.13.0 Edición de 1999. Después de que se ha establecido una conexión RRC entre el SINodoB y el UE, para el propósito de un procedimiento de actualización de localización se envían una serie de Peticiones de Identidad de MM por el SINodoB 100 para recuperar la información de identificación del UE. De nuevo, el UE responde a estas Peticiones de Identidad de MM sin requerir protección integral porque la Petición de Identidad de MM se especifica en la lista dada anteriormente en el documento 3GPP TS 24.008 versión 3.19.0 Edición de 1999.

Específicamente, la serie de mensajes entre el UE y el SINodoB es como sigue:

UE <-> SINodoB

-> Petición de Conexión de RRC

<- Establecimiento de Conexión RRC

-> Establecimiento de Conexión RRC Completa

-> Petición de Actualización de Localización de MM

<- Petición de Identidad de MM (Solicitando la IMSI)

-> Respuesta de Identidad de MM (IMSI)

<- Petición de Identidad de MM (Solicitando la IMEI)

-> Respuesta de Identidad de MM (IMEI)

<- Petición de Identidad de MM (Solicitando IMEISV)

-> Respuesta de Identidad de MM (IMEISV)

Cuando el UE envía la Petición de Actualización de Localización de MM, también se arranca un temporizador de actualización de LAC. El SINodoB ignora esta petición. Si el UE no recibe una respuesta válida a la Petición de Actualización de Localización de MM dentro de un tiempo predeterminado, entonces el UE reenvía la Petición de Actualización de Localización de MM. Este proceso se repite unas pocas veces y a continuación el UE aborta la conexión.

De este modo, enviando la serie de tres Peticiones de Identidad de MM directamente después de que se establece la conexión de RRC, y antes de que el UE aborte la conexión, el SINodoB puede recibir mensajes de Respuesta de Identidad de MM desde el UE sin que se requiera protección de integridad.

Una vez que se ha recogido la información de la identidad, el SINodoB rechaza la petición de actualización de localización impidiendo de este modo que el UE intente repetidamente acampar sobre el SINodoB.

2.2 3G Mantenimiento de la Conexión de RRC

En las circunstancias descritas anteriormente, una vez que el UE establece la conexión de RRC transmitirá un mensaje de petición de Actualización de Localización. En funcionamiento normal la red realizará a continuación los procedimientos de autenticación y de integridad, que aseguran que el UE y la red están ambos confiados de que el otro

es legítimo. Después de esto, la red enviará un mensaje de aceptación de la actualización de la localización de integridad protegida. El UE se requiere por las normativas que ignore este mensaje si no está satisfactoriamente protegida la integridad, de modo que un SINodoB está impedido de realizar de forma eficaz esta etapa satisfactoriamente.

Una vez que el UE envía el mensaje de Petición de Actualización de Localización arranca un temporizador, y si no se recibe una aceptación de la actualización de localización satisfactoria antes de que expire el temporizador el UE abortará el intento y a continuación lo reintentará. Hay un contador de reintentos y si el UE lo ha reintentado demasiadas veces, abortará los intentos y se moverá a otra célula.

Los flujos normales de mensajes del protocolo de red darán como resultado que la Conexión de RRC se cae sin el UE aborta la conexión. Esto es también porque la red abandona la conexión por sus propias razones o porque el UE lo ha solicitado.

La liberación de la conexión de RRC se controla por la red y es posible en el SINodoB intentar mantener la conexión una vez que el UE ha solicitado la liberación.

Ciertos mensajes y procedimientos no requieren que esté protegida su integridad y de este modo pueden usarse para continuar la comunicación con el UE, independientemente del procedimiento de actualización de localización. Un ejemplo de esto es la petición de Capacidad del UE de RRC y los mensajes de respuesta.

De este modo un flujo que permite que la Conexión de RRC se mantenga durante unos pocos minutos podría ser tal como este:

<-> Establecimiento de Conexión de RRC

-> el UE envía un mensaje de petición de actualización de localización y arranca el temporizador de actualización de LAC

<-> la red envía repetidamente un mensaje de Petición de Capacidad del UE y el UE contesta (esto asegura que la Conexión de RRC se mantiene activa aunque la red no ha respondido a la petición de actualización de localización)

-> después de unos pocos segundos el UE envía una indicación de liberación de la conexión de Señalización de RRC, solicitando la liberación de la Conexión de RRC. El SINodoB ignora este mensaje.

-> el temporizador de actualización de LAC expira – de este modo el UE reenvía la actualización de localización

<-> el procedimiento se repite unas pocas veces y a continuación el UE aborta la conexión completamente y busca otras células.

Durante este proceso los mensajes de Petición de Capacidad del UE de RRC (o alguna otras petición de información) se usan para engañar a la capa de protocolo de RRC para que crea que el enlace está activo y de este modo incluso cuando termina por temporización el procedimiento de actualización de localización, la Conexión de RRC debería mantenerse.

Esta Conexión de RRC puede mantenerse durante varios minutos sin ninguna indicación para el usuario del UE de que está ocurriendo algo. De este modo durante este tiempo es posible utilizar las transmisiones desde el UE para propósitos de búsqueda de dirección como se describe más adelante en la sección 2.3.

Si se requiere un periodo de transmisión continua más largo entonces todo lo que se necesita es hacer que el UE intente realizar de nuevo otro procedimiento de actualización de localización. Esto puede conseguirse difundiendo una segunda falsa difusión de la célula con un LAC diferente desde el SINonoB. De este modo en este caso el SINodoB establece en primer lugar una conexión de RRC con el dispositivo donde el SINodoB está difundiendo una célula configurada con el primer código LAC para el UE; detecta que el UE ha liberado la conexión de RRC, y en respuesta a esa detección transmite inmediatamente una segunda célula con un segundo código LAC para hacer que el UE restablezca la conexión de RRC con el SINodoB. Este proceso puede repetirse a continuación con diferentes códigos LAC para mantener la conexión de RRC indefinidamente.

En lugar de transmitir los diferentes códigos LAC uno tras otro, en la forma descrita anteriormente, los múltiples NodosB (que están sustancialmente situados al lado del SINodoB) pueden transmitir simultáneamente las células con diferentes LAC.

De este modo, por los métodos descritos anteriormente, el SINodoB establece y mantiene una "llamada ciega" con el UE: esto es, una conexión de señal que no causa que el UE proporcione una alerta visual o audible.

2.3 Código 3G

Siguiendo el proceso descrito anteriormente en las secciones 2.1 y 2.2, el SINodoB 100 puede mantener una conexión de RRC durante un periodo prolongado de tiempo. Sin embargo para los propósitos de búsqueda de direcciones también es necesario asegurar que el UE está transmitiendo con un código de aleatorización fijo y conocido.

En la red real la señal recibida tiene que pasar por muchas etapas de de-multiplexación/decodificación antes de se extraigan datos útiles de usuario. Esto es porque los datos transmitidos sobre el aire consisten de múltiples canales lógicos que se mapean sobre canales de transporte. Estos canales de transporte se mapean a continuación sobre canales físicos. En cada una de las etapas de multiplexación, los diferentes canales que están mapeados sobre el mismo canal de portadora deben diferenciarse. Esto se hace usando etapas adicionales de codificación.

Por ejemplo la última etapa en este proceso, involucra la combinación de todos los canales físicos dentro de una transmisión única del UE. Los canales físicos se tratan todos con diferentes códigos de canalización y a continuación se suman y el resultado se trata con el código de aleatorización que hace la transmisión del UE distinguible de la de otros UE.

El proceso de decodificación/de-multiplexación realizado por el SINodoB y el UE se ilustra en la Figura 5. El espectro de UMTS se divide en múltiples canales de frecuencia (doce en el Reino Unido), definido cada uno por una banda de frecuencias con una frecuencia central definida por UARFCN y asociada con un Operador particular. En la dirección del canal ascendente cada canal se decodifica por un NodoB usando un código de des-aleatorización del enlace ascendente respectivo, estando asociado cada uno de los códigos de des-aleatorización del enlace ascendente asociado con un UE respectivo. Después de la des-aleatorización, la señal se decodifica además usando varios códigos de canalización, para dar N canales físicos dedicados asociado cada uno ellos con un código de canalización respectivo. En la dirección del enlace descendente cada uno de los canales se decodifica por el UE usando un código de aleatorización del enlace descendente respectivo, estando asociado cada uno de los códigos de aleatorización del enlace descendente con una célula respectiva.

En el UMTS hay dos modos principales en los que el UE puede realizar una conexión de señalización con la red. El primero es usar el canal RACH, que es una forma de mecanismo de acceso aleatorio en el cual todos los UE completan un recurso de comunicaciones compartido. El canal FACH se usa por la red para responder a la señalización recibida sobre el canal RACH. En este caso el mensaje se difundirá de modo que cada UE será capaz de recibirlo pero tendrá un identificador detallando a qué UE está dirigido el mensaje. En el caso del mecanismo donde se usan los canales RACH y FACH para la comunicación, el UE se dice que está usualmente en el estado FACH de célula. Este se usa por la red para señalización de bajo ancho de banda o transferencia de datos. El proceso de actualización de localización se realiza usualmente en el FACH de célula porque el proceso de señalización es corto y no merece asignar un recurso de red dedicado a este procedimiento corto y razonablemente normal.

En el caso en el que el objetivo de mantenimiento de la conexión sea para la búsqueda de dirección, el mecanismo de comunicación compartida de FACH de la célula no es útil, ya que muchos UE estarán usando los mismos códigos.

Cuando se establece una conexión RRC, el SINodoB instruye al UE para utilizar un canal dedicado (estado DCH de la célula) asociado con un código de aleatorización del enlace ascendente elegido y un código de canalización elegido. En este caso el mensaje de Establecimiento de la Conexión de RRC describe el canal dedicado (DCH) que usarán el UE y la red para comunicar.

2.4 Búsqueda de Dirección 3G

Una vez que el UE está transmitiendo sobre un DCH especificado, un buscador de dirección 106 puede realizar una búsqueda de dirección usando la técnica descrita a continuación.

La búsqueda de dirección en 3G difiere de la de 2G porque la señal de 2G está puramente en el dominio de la frecuencia, mientras que la señal 3G está en dominio de código. Esto significa que en 2G un algoritmo de búsqueda de dirección puede funcionar analizando las diferencias de temporización entre las señales filtradas adecuadamente recibidas en cada una de las antenas en la disposición de antenas. En 3G es necesario producir una entrada adecuada para proporcionar al algoritmo de búsqueda de dirección. Efectivamente esto significa que la señal filtrada recibida en cada una de las antenas de la disposición necesita seguirse y des-aleatorizarse/decodificarse independientemente.

Por lo tanto el buscador de dirección 106 determina la dirección de la señal codificada del localizador de 3G detectando la señal de localización con una disposición de N antenas, decodificando separadamente una salida de cada una de las antenas para generar N salidas decodificadas, y midiendo la dirección de llegada de la señal de localización analizando las N salidas decodificadas.

El buscador de dirección 106 está ilustrado con detalle en la Figura 6, y comprende un procesador que corre un algoritmo DF, una disposición de cinco antenas, y una disposición de cinco receptores RAKE y des-aleatorizadores, recibiendo cada uno señales del localizador codificadas desde una antena respectiva y generando una salida decodificada para el algoritmo DF.

Cada uno de los receptores RAKE tiene una colección de sub-receptores/des-aleatorizadores independientes. Cada uno de los sub-receptores /des-aleatorizadores rake está configurado para decodificar y seguir una señal de localización codificada asociada con una trayectoria de propagación diferente desde el dispositivo. Por ejemplo un sub-receptor/des-aleatorizador rake podría decodificar y seguir una trayectoria de propagación principal sobre una línea directa de visión con el dispositivo y otro sub-receptor rake podría decodificar y seguir una trayectoria de propagación secundaria causada por reflexión desde un objeto cercano. De este modo cada uno de los sub-receptores/des-aleatorizadores rake genera dos salidas:

- información de temporización: esto es datos indicando la desviación de fase del sub-receptor /des-aleatorizador rake; y
- datos de amplitud de la señal.

En un receptor rake convencional, un bloque que combina suma de forma coherente los datos de amplitud de la señal procedentes de todos los sub-receptores rake y la suma coherente se usa a continuación como entrada al siguiente proceso de decodificación en la cadena de recepción. En contraste, los receptores/des-aleatorizadores rake de la Figura 6 no pasan sobre tal suma coherente al algoritmo DF. Para la búsqueda de dirección, no son de interés los datos de amplitud de señal sumados de forma coherente, sino la información de temporización y los datos de amplitud de señal asociados con cada una de las trayectorias de propagación. Por lo tanto los receptores/des-aleatorizadores rake introducen esta información de temporización y los datos de amplitud de la señal al algoritmo DF.

Los receptores/des-aleatorizadores rake están todos sincronizados con una fuente de temporización precisa única, para asegurar que los pequeños retardos entre la señal de recepción en cada una de las antenas en la disposición están representadas de forma precisa en la información de temporización.

El algoritmo DF realiza a continuación las funciones de correlación usando la información de temporización y los datos de amplitud de la señal para generar una salida que puede presentarse al usuario. Un ejemplo de cómo podría presentarse la información se muestra en la Figura 7. Se representan varias flechas sobre un mapa, con la longitud y/o el ancho de la flecha indicando la amplitud de la señal, y la dirección de la flecha indicando la dirección que se deduce de la información de temporización. Cada una de las flechas está asociada con una trayectoria de propagación diferente desde el dispositivo.

Dado que hay un pequeño riesgo de que el código de aleatorización del enlace ascendente elegido por el SINodoB para el UE objetivo esté ya en uso por otro UE conectado a la red real, será necesario comprobar que no hay ninguna transmisión de UE usando el código de aleatorización que se va a asignar.

Esto puede realizarse de uno de los dos modos:

1. El buscador de dirección almacena una lista A de posibles códigos de aleatorización del enlace ascendente, y comprueba la existencia de señales del enlace ascendente sobre todos estos códigos de aleatorización, obteniendo un subconjunto B de la lista A. A continuación asigna un código de aleatorización C que está en la lista A pero no en la lista B. A continuación envía los datos al SINodoB que identifica el código de aleatorización C, y el SINodoB asigna ese código de aleatorización al UE.

2. El SINodoB envía un mensaje al buscador de dirección identificando un código de aleatorización que se propone utilizar. El buscador de dirección comprueba la existencia de una señal del enlace ascendente que utiliza el código propuesto. Si no se encuentra ninguna señal del enlace ascendente entonces el buscador de dirección informa al SINodoB, y el SINodoB asigna ese código de aleatorización al UE. Si se encuentra una señal del enlace ascendente entones el buscador de dirección informa al SINodoB, y el SINodoB inicia otra comprobación usando un código propuesto diferente. Esto se repite hasta que se asigna un código de aleatorización al UE.

Realizando sólo una única etapa de decodificación (usando el código de des-aleatorización del enlace ascendente), esta técnica proporciona una señal des-aleatorizada que contiene toda la potencia de RF del UE objetivo. La señal des-aleatorizada se analiza a continuación como se ha descrito anteriormente.

3. Verificación del Objetivo 2G/3G

Las secciones 1 y 2 anteriores describen métodos de adquirir parámetros de identidad de una MS/UE, estableciendo una llamada ciega con la MS/UE, y realizando la búsqueda de dirección.

En una versión mejorada de cualquiera de los métodos, puede usarse la adquisición de los parámetros de identidad para verificar que la MS/UE es la MS/UE objetivo.

De este modo el flujo del proceso es como sigue:

1. El buscador de dirección almacena la IMSI y/o la IMEI de una MS/UE objetivo.

2. La BTS/SINodoB adquiere la IMSI o la IMEI de una MS/UE candidata y las envía a una base de datos.

3. La base de datos comprueba la IMSI/IMEI en búsqueda de la MS/UE candidata frente a la IMSI/IMEI almacenada.

4. Si hay una coincidencia, entones la base de datos informa al BTS/SINodoB que complete el proceso de llamada ciega y el buscador de dirección procede a realizar la búsqueda de dirección.

5. Si no hay ninguna coincidencia, entones la base de datos informa a la BTS/SINodoB que aborte el proceso de llamada ciega.

4. 2G/3G Combinadas

Las Figuras 1, 2 describen un SIBTS 10 y un buscador de dirección 6 que están configurados para GSM, y las Figuras 3, 4 describen un SINodoB 100 y un buscador de dirección 106 que están configurados para 3G. En una realización alternativa (no mostrada), uno o ambos dispositivos pueden ser configurables para GSM y 3G.

REIVINDICACIONES

1. Un método para la determinación de la dirección de un dispositivo móvil de comunicaciones, comprendiendo el método hacer que el dispositivo transmita una señal de localización transmitiendo una petición de llamada al dispositivo sobre un enlace inalámbrico, en el que la petición de la llamada está adaptada para hacer que el dispositivo transmita una señal de localización mientras que bloquea un proceso de gestión de conexión que de otro modo causaría que el dispositivo móvil de comunicaciones proporcionase una alerta visual o audible; recibir la señal de localización desde el dispositivo sobre un enlace inalámbrico; y determinar la dirección del dispositivo midiendo la dirección de llegada de la señal de localización, caracterizado porque el método comprende además la supervisión del tráfico sobre una pluralidad de canales; seleccionar un canal en base a la supervisión; y causar que la señal de localización se transmita al canal seleccionado.

2. El método de la reivindicación 1 que comprende además transmitir una petición de supervisión al buscador de dirección (106), estando adaptada la petición de supervisión para causar que el buscador de dirección determine la dirección del dispositivo midiendo la dirección de llegada de la señal de localización.

3. Un método de acuerdo con la reivindicación 2 que comprende además transmitir la información del canal al buscador de dirección (106), identificando la información de canal, el canal de la señal de localización.

4. Un método de acuerdo con la reivindicación 3 en el que la información de canal incluye la información de la ranura temporal y/o la frecuencia.

5. Un método de acuerdo con cualquiera de las reivindicaciones anteriores que comprende además la adquisición de un parámetro de identidad del dispositivo, comprobando si hay una coincidencia con el parámetro de identidad objetivo almacenado; y determinar la dirección del dispositivo si hay una coincidencia.

6. Un método de acuerdo con cualquiera de las reivindicaciones anteriores en el que la dirección de llegada de la señal de localización se determina detectando la señal de localización con uno o más sensores espaciados entre sí; y determinando la dirección de llegada de la señal de localización por un proceso de triangulación.

7. Un método de acuerdo con cualquiera de las reivindicaciones anteriores en el que la petición de llamada bloquea el proceso de gestión de la conexión omitiendo una o más peticiones de gestión de conexión.

8. Un método de acuerdo con cualquiera de las reivindicaciones anteriores en el que la petición de llamada bloquea el proceso de gestión de la conexión causando que el dispositivo entre en un modo de prueba.

9. Un método de acuerdo con la reivindicación 8 en el que al modo de prueba es el modo de prueba de GPRS GSM A o B.

10. Un método de acuerdo con cualquiera de las reivindicaciones anteriores que comprende además causar que el dispositivo aumente la potencia de la señal de localización transmitiendo una petición de aumento de potencia al dispositivo.

11. Un método de acuerdo con cualquiera de las reivindicaciones anteriores en el que la petición de llamada es una petición de llamada GSM.

12. Un método de acuerdo con cualquiera de las reivindicaciones anteriores en el que la señal de localización es una señal codificada del localizador.

13. Un método de acuerdo con la reivindicación 12 en el que la petición de llamada instruye al dispositivo para que transmita la señal de localización usando un código específico.

14. Un método de acuerdo con cualquiera de las reivindicaciones anteriores en el que la petición de llamada bloquea el proceso de gestión de conexión recibiendo la petición desde el dispositivo para liberar la llamada, y enviando repetidamente una petición de información al dispositivo para impedir que el dispositivo libere la llamada.

15. Un aparato (10, 100) configurado para realizar un método de acuerdo con cualquiera de las reivindicaciones anteriores.

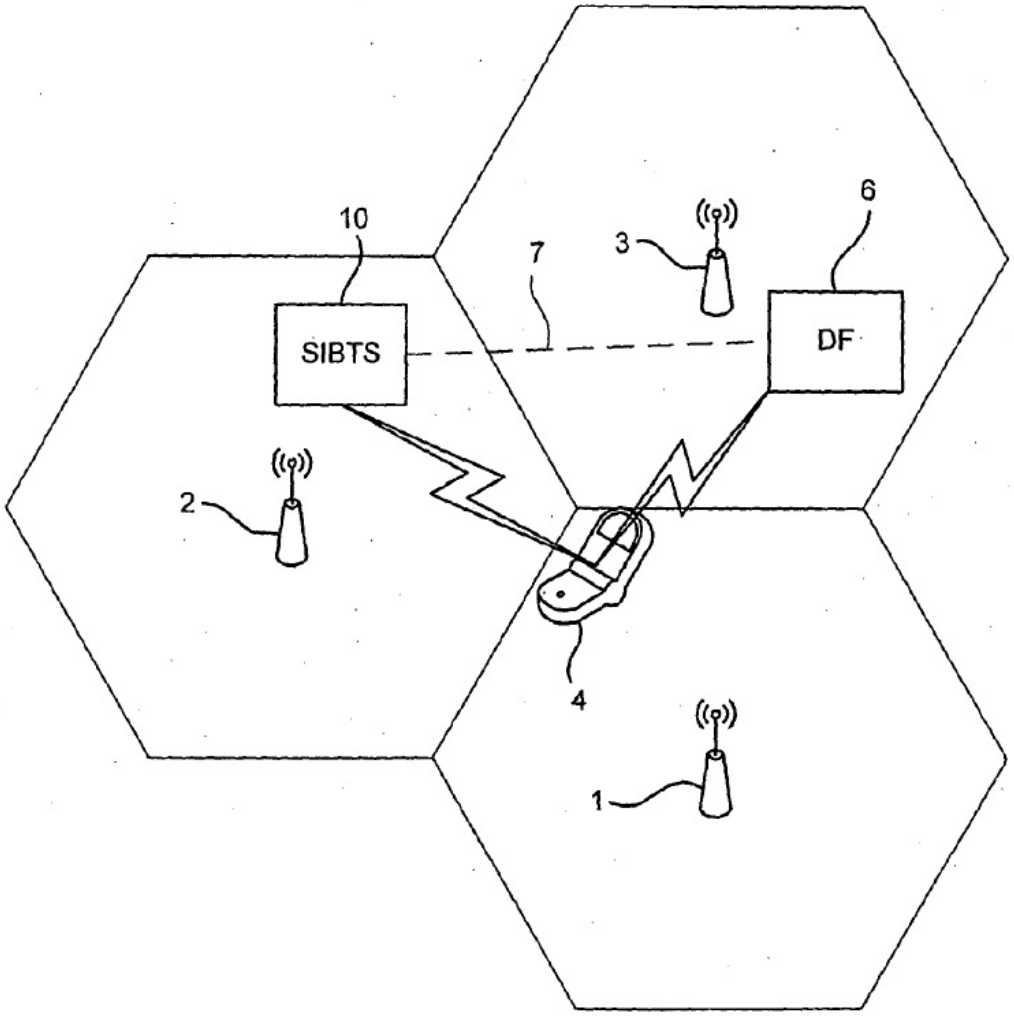

Figura 1

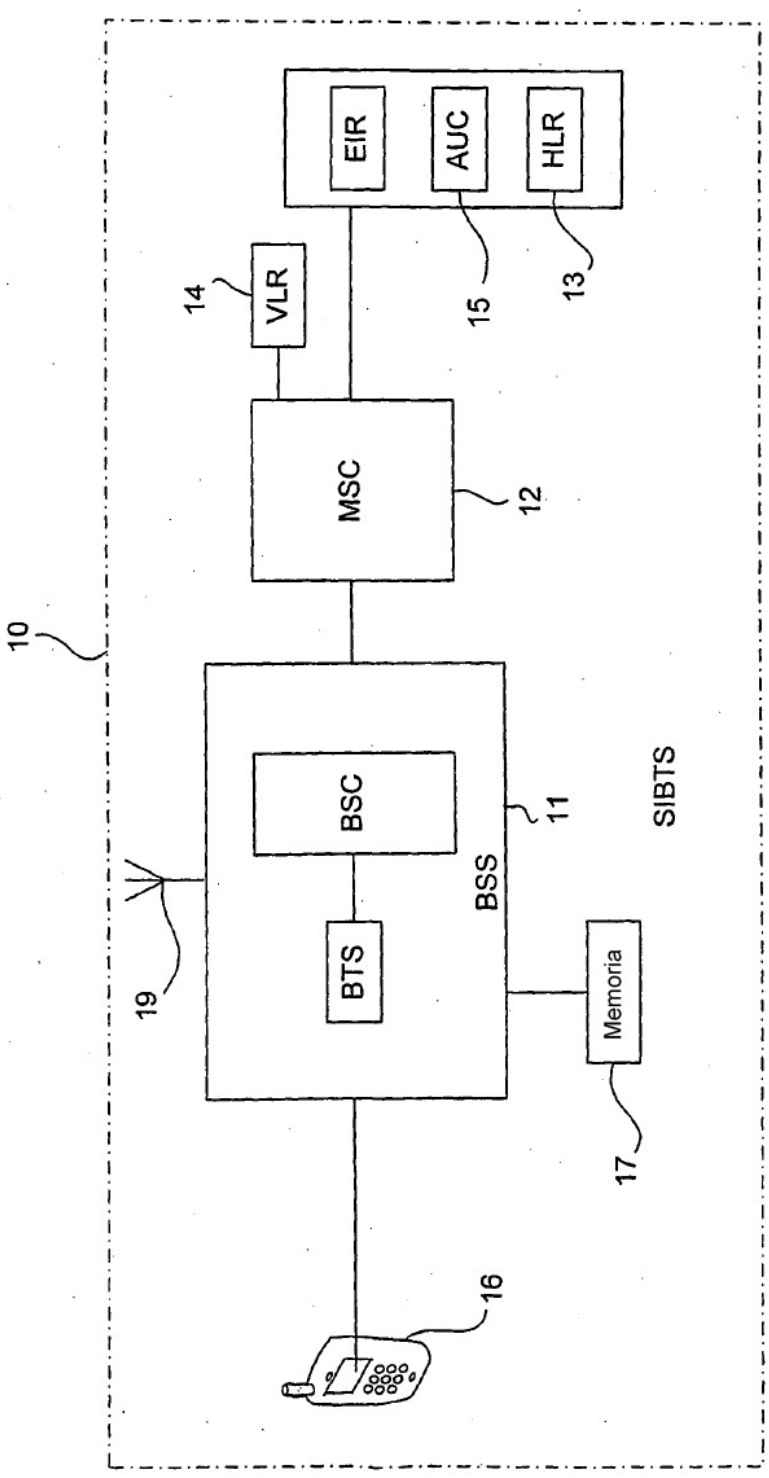
10
EIR
AUC
HLR
14
VLR
15
13
MSC
12
BSC
11
BSS
SIBTS
19
BTS
Memoria
17
16

Figura 2

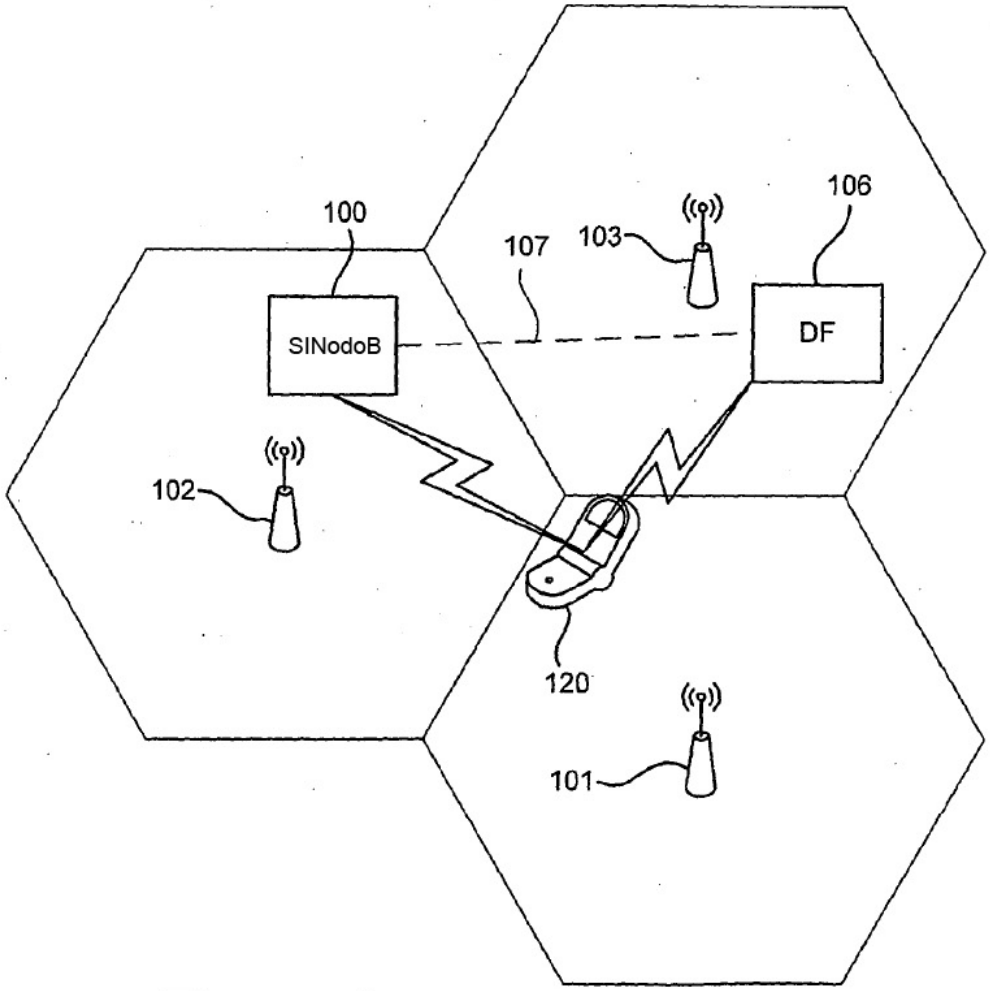

Figura 3

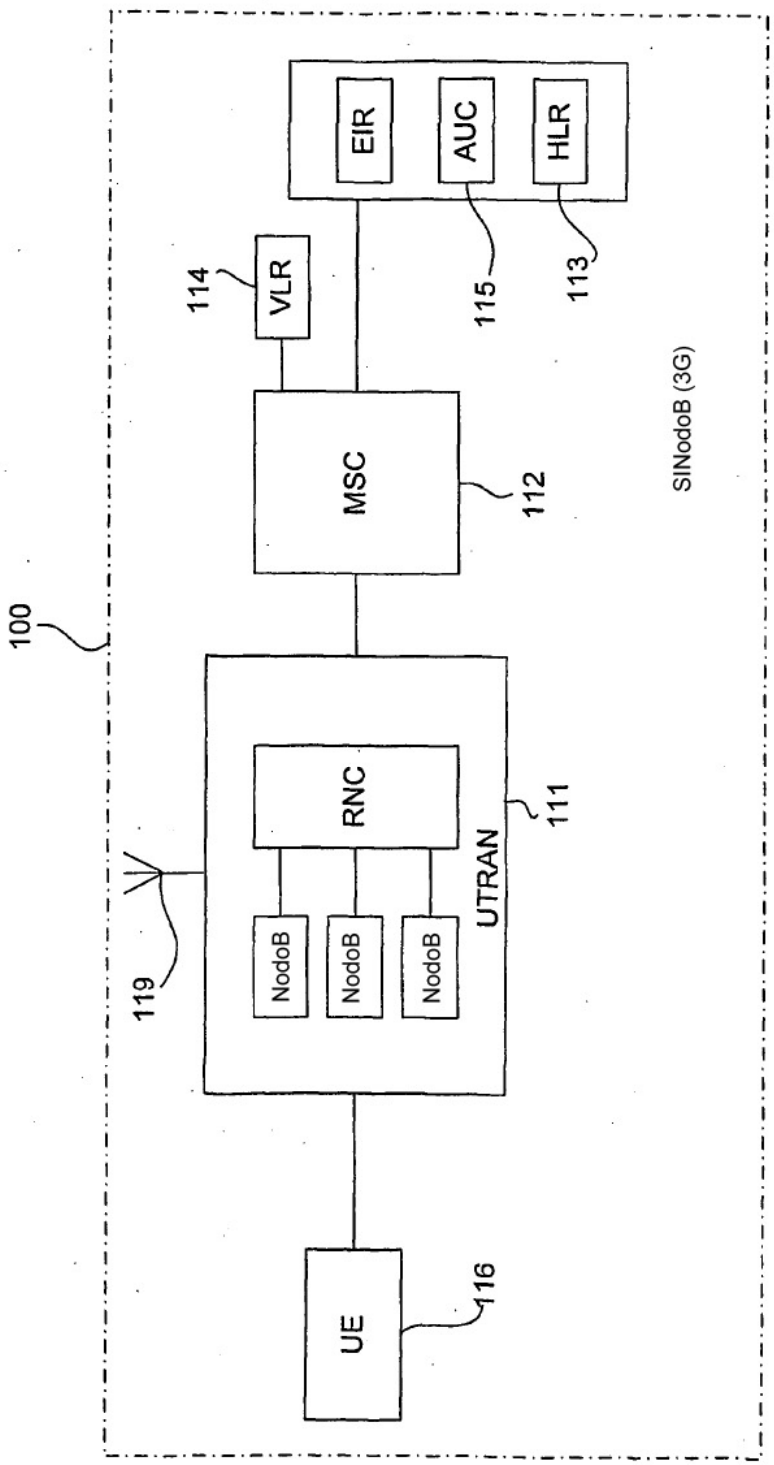
100
EIR
AUC
HLR
114
VLR
115
113
MSC
112
SINodoB (3G)
RNC
111
UTRAN
NodoB
NodoB
NodoB
119
UE
116

Figura 4

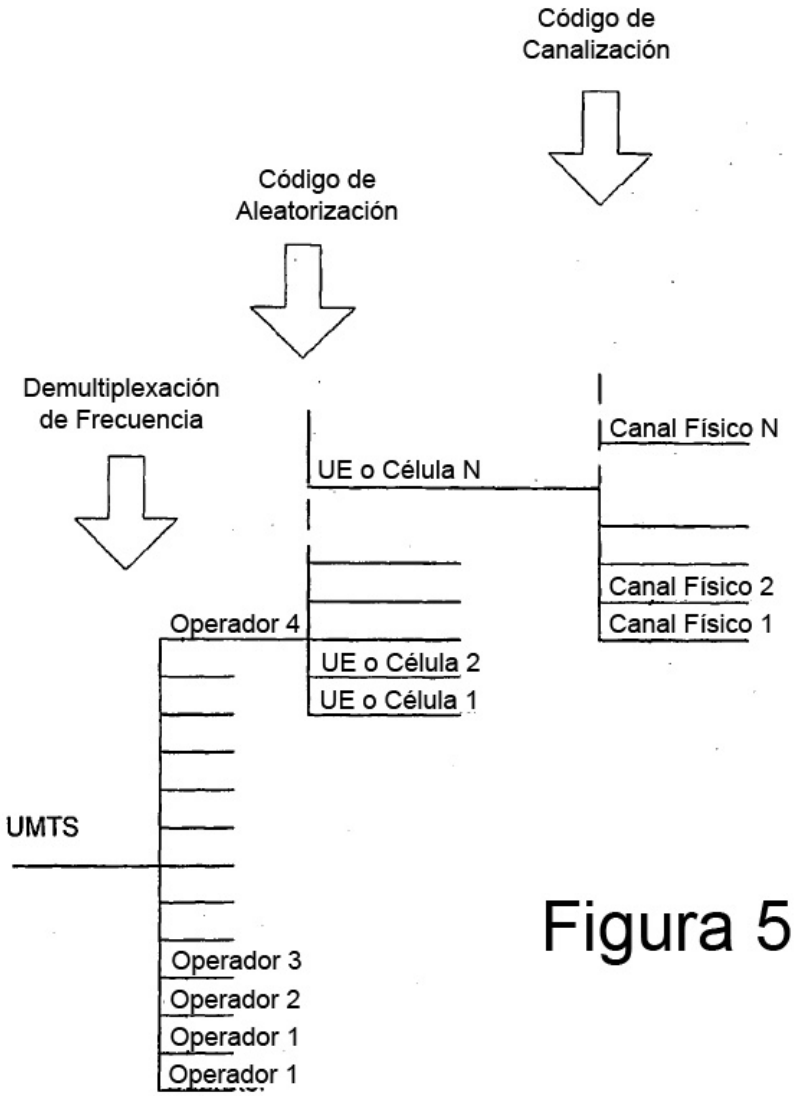
Código de Canalización
Código de Aleatorización
Demultiplexación de Frecuencia
Canal Físico N
UE o Célula N
Canal Físico 2
Canal Físico 1
Operador 4
UE o Célula 2
UE o Célula 1
UMTS
Operador 3
Operador 2
Operador 1
Operador 1

Figura 5

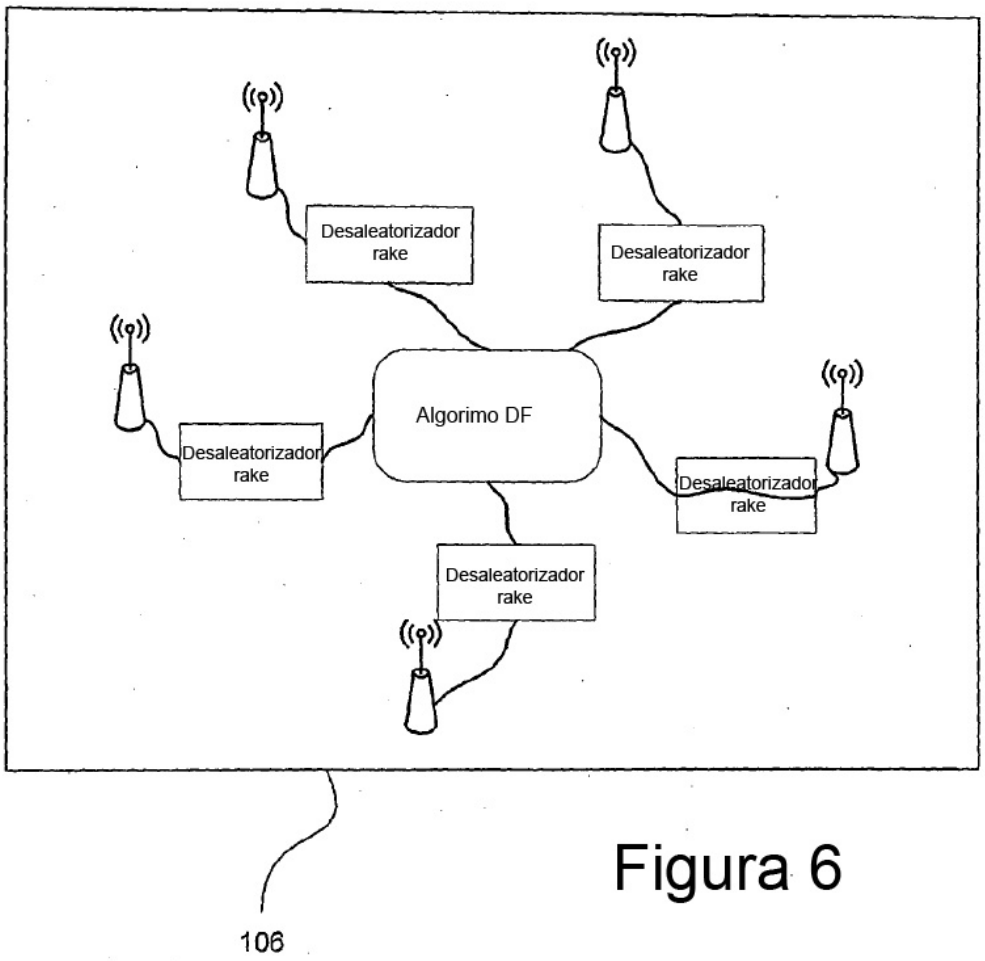

Figura 6

Figura 7