(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 356 289**

(51) Int. Cl.:
H04W 24/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07705068 .0**
(96) Fecha de presentación : **30.01.2007**
(97) Número de publicación de la solicitud: **1982430**
(97) Fecha de publicación de la solicitud: **22.10.2008**

(54) Título: **Método de determinar la dirección de llegada de una señal de un dispositivo móvil.**

(30) Prioridad: **31.01.2006 GB 0601952**

(45) Fecha de publicación de la mención BOPI:
06.04.2011

(45) Fecha de la publicación del folleto de la patente:
06.04.2011

(73) Titular/es: **M.M.I. RESEARCH LIMITED**
Brook Road
Wimborne, Dorset BH21 2BJ, GB

(72) Inventor/es: **Dolby, Riki, Benjamin y**
Martin, Paul, Maxwell

(74) Agente: **Ungría López, Javier**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

La presente invención se refiere a un método, y aparato asociado, para determinar la dirección de un dispositivo de comunicaciones móviles. Típicamente, aunque no exclusivamente, el dispositivo es un dispositivo de tercera generación (3G).

La reciente disponibilidad de teléfonos móviles de tercera generación y dispositivos relacionados da lugar al requisito de nuevos métodos para localizar teléfonos 3G que usan técnicas de acceso múltiple por división de código (CDMA) en la interface de aire. Para el seguimiento de los teléfonos se requieren nuevas técnicas que son completamente diferentes de las técnicas usadas para rastrear teléfonos GSM.

Obsérvese que las redes 3G incluyen mayor protección de seguridad mediante un mecanismo conocido como autenticación mutua. Esta técnica implica una autenticación en dos pasos donde a) el equipo de usuario (UE) es autenticado con la red y b) la red es autenticada con el UE. En GSM, solamente se aplica a), dando lugar a la posibilidad de un ataque contra la seguridad mediante una estación base falsa. La autenticación mutua inhibe el mecanismo convencional de establecer un teléfono móvil como una baliza RF y permitir que el equipo radiogoniométrico localice la baliza en una frecuencia/código/intervalo de tiempo conocidos. Esto es porque el UE ignorará mensajes que no sean de un dispositivo de red adecuadamente autenticado dando lugar a que las transmisiones UE que sean terminadas bruscamente en un punto en las centrales de protocolo donde el UE determina que la red con la que habla tiene datos de protección de “integridad” incorrecta o ausente cuando lo ordenan las especificaciones.

Las redes UMTS transmiten por el aire usando tecnología de acceso múltiple por división de código (CDMA). Esto significa que la señal de un solo dispositivo de transmisión 3G es muy difícil de distinguir del ruido de fondo, porque la transmisión está cifrada usando una configuración que dispersa la potencia de la señal a través de un amplio rango de frecuencia. Es posible decodificar la señal de un solo dispositivo si se conoce el código de cifrado que se utilizó en el transmisor.

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

WO-A-0191317 describe un receptor rake y método de recibir una señal deseada. Una bifurcación de búsqueda calcula la respuesta de impulso bidimensional de una señal recibida, y transmite a las bifurcaciones rake información acerca de los componentes más favorables hallados.

La invención proporciona un método de determinar la dirección de llegada de una señal de localización codificada de un dispositivo de comunicaciones móviles con relación a un radiogoniómetro según la reivindicación 1.

La invención proporciona un método adecuado para determinar la dirección de llegada de una señal de localización codificada de un dispositivo CDMA.

Se puede mantener una conexión con el dispositivo de comunicaciones móviles estableciendo una conexión con el dispositivo; recibiendo una petición del dispositivo de liberar la conexión; y enviando repetidas veces una petición de información al dispositivo para evitar que el dispositivo libere la conexión. La conexión puede ser una conexión RRC.

Se puede mantener comunicación con el dispositivo celular móvil de comunicaciones estableciendo una conexión con el dispositivo difundiendo una primera célula configurada con un primer código de localización al dispositivo; y restableciendo la conexión con el dispositivo después de que el dispositivo haya liberado la conexión difundiendo una segunda célula configurada con un segundo código de localización al dispositivo. La conexión puede ser una conexión RRC, y los códigos de localización pueden ser códigos LAC o códigos RAC.

Realizaciones de la invención se describirán ahora con referencia a los dibujos acompañantes, en los que:

La figura 1 representa un sistema para determinar la dirección de un dispositivo de comunicaciones móviles 3G.

La figura 2 representa un NodeB Introducido por Separado (SINodeB).

La figura 3 representa varias asignaciones de canal en un sistema CDMA.

La figura 4 representa un radiogoniómetro.

Y la figura 5 representa un formato de visualización.

La figura 1 representa una red 3G incluyendo tres NodeBs 101-103 que emiten a tres células por transmisiones de enlace descendente, teniendo cada uno un único código de cifrado de enlace descendente. Al aproximarse a los tres NodeBs, un dispositivo de equipo de usuario (UE) 120 evalúa en qué NodeB acampar.

El UE 120 tiene que reevaluar constantemente las señales de células alrededor de él. Lo hace para

asegurar que, durante una conexión (datos o voz), siempre comunique con el mejor NodeB (el más apropiado). Sin embargo un UE 3G pasará gran parte de su tiempo en el que no transmite tráfico de voz o datos en un estado inactivo. En este estado inactivo el UE supervisará la intensidad del NodeB sirviente y otros NodeBs contiguos, y si se cumplen los criterios especificados por la red, efectuará una reselección de célula convirtiendo uno de los NodeBs contiguos previos al nuevo NodeB sirviente. Si este nuevo NodeB sirviente está en una posición o zona de enrutamiento diferente, entonces el UE debe realizar un procedimiento de actualización de posición o zona de enrutamiento para informar a la red de su posición nueva. Esto se hace de modo que la red siempre tenga una idea de dónde está el UE en la red, de modo que, en caso de una petición de llamada entrante al UE, la red pueda usar la cantidad mínima de recursos para pedir al UE que establezca una conexión de señalización.

Cada NodeB transmite información difundida que cumple dos fines principales. Primero: parte de esta información es transmitida usando códigos conocidos y configuraciones de datos que permiten al UE reconocer que la señal de radio frecuencia (RF) recibida es realmente una célula UMTS y también permite al UE realizar mediciones de potencia en la señal recibida. Segundo: se difunde información descriptiva acerca de la célula. Esta información de sistema es transmitida en forma de Bloques de Información de Sistema (SIBS) que describen muchos parámetros del NodeB y proporcionan suficiente información para que el UE identifique la red móvil a la que pertenece el NodeB, y también que establezca una conexión de señalización si la necesita.

La figura 2 representa un NodeB Introducido por Separado (SINodeB) 100. El SINodeB 100 está configurado para adquirir un parámetro de identidad de un UE registrado con la red 3G de la figura 1. Esto se logra emulando un NodeB usando un método especialmente adaptado al protocolo UMTS, como se describe con más detalle a continuación.

El SINodeB 100 es típicamente un dispositivo móvil, que puede estar alojado en un vehículo. En el uso, el SINodeB 100 es movido a una zona, y operado para adquirir parámetros de identidad de un conjunto de dispositivos de equipo de usuario (UEs) registrados en la red 3G en dicha zona. Alternativamente, el SINodeB 100 puede estar situado permanentemente en una zona de interés. En ambos casos, el SINodeB 100 transmite efectivamente una difusión de célula falsa que no está bajo el control de la red 3G que proporciona cobertura a dicha zona.

Con el fin de persuadir al UE a que pase al SINodeB 100, hay que cumplir algunos criterios. La transmisión debe ser recibida primariamente en el UE con una intensidad de señal más alta. Incluso una vez que el UE ha decidido que el SINodeB 100 es preferente, normalmente se considerará necesario pasar los procedimientos de seguridad UMTS de manera que sea capaz de recoger cualquier información útil o de realizar tareas útiles.

No es necesario emular exactamente toda la configuración de un NodeB existente para que sea un candidato adecuado para un UE con el que conectar. Esto hace mucho más simple la tarea de configurar el SINodeB 100. La razón de esto es que la información de sistema difundida define la configuración de la célula que está transmitiendo esos datos, y las células dentro de la misma red tendrán configuraciones diferentes, de modo que el UE siempre considera los datos de la célula corriente para determinar la información necesaria.

Los parámetros clave en la difusión de célula falsa que tienen que ser considerados para cambiar son los siguientes:

- frecuencia de célula
- código de cifrado primario
- código de país móvil (MCC) [- en qué país está esta célula]
- código de red móvil (MNC) [- a qué red pertenece está célula]
- código de zona de localización (LAC)
- código de zona de enrutamiento (RAC)
- potencia de célula
- etiquetas de valor SIB [- las etiquetas de valor son utilizadas por el UE para detectar si la información SIB ha cambiado entre lecturas de los SIBs]
- contenido de SIB18 y SIB11 para la célula sirviente [- SIB11 contiene información de control de medición a usar por el UE en modo inactivo/ SIB18 contiene ids PLMN de células contiguas a considerar en modo inactivo y conectado]

MCC y MNC deben ser los mismos que la célula sirviente para que el UE considere que el SINodeB está en la misma red.

La frecuencia de célula debe ser la misma que la célula sirviente para hacer el proceso lo más fácil posible – las reselecciones de interfrecuencia tienen criterios y procesos más complejos.

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

1) Mismos LAC/RAC y código de cifrado primario, diferentes etiquetas de valor SIB - esto imita completamente la célula sirviente, y permite que el SINodeB capte activamente el UE.

2) Diferentes LAC/RAC y código de cifrado primario - donde el código de cifrado está presente en el SIB11 de la célula sirviente. Esto es imitar que un NodeB contiguo está ordenando que el NodeB sirviente realice mediciones en el UE, asegurando así que el UE esté buscando activamente una célula con las mismas características clave que las transmitidas por el SINodeB (primariamente código de cifrado, y frecuencia). Esto hace que un UE realice una reselección de célula al SINodeB si la transmisión del SINodeB es de potencia suficientemente más alta que el NodeB sirviente. La cantidad en que el SINodeB tiene que ser una señal más fuerte se define en SIB3 del NodeB sirviente.

3) Diferentes LAC/RAC y código de cifrado – ninguna referencia en SIBS del NodeB sirviente.

Una vez que se está transmitiendo una célula adecuadamente fuerte y configurada, los UEs en la zona deseada realizarán una reselección de célula al SINodeB y establecerá una conexión RRC al objeto de realizar un procedimiento de actualización de localización. La actualización de localización es necesaria porque el LAC del SINodeB es diferente del SINodeB sirviente antiguo. Una vez establecida la conexión RRC, el SINodeB tiene la oportunidad de realizar otros procedimientos de señalización a voluntad.

El protocolo UMTS está diseñado para mejorar las características de seguridad y protección de identidad en GSM. Para ello, se usan mecanismos de autenticación e integridad además de las identidades temporales halladas en GSM. Estas identidades temporales evitan la frecuente transmisión de la identidad del IMSI y el IMEI, porque, una vez que la red ha asignado el teléfono, una identidad temporal mantiene entonces una aplicación de dicha nueva identidad al IMSI.

Existen mecanismos para permitir que la red interrogue a un teléfono por su IMSI e 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 tiene que restablecer la aplicación correcta entre una identidad temporal (tal como un TMSI) y su identidad real asociada (tal como un IMSI). En operación de red normal casi toda la señalización entre el UE y la red debe ser realizada después de que el procedimiento de autenticación haya sido completada satisfactoriamente y la integridad haya sido habilitada en la conexión de señalización. Esto hace efectivamente imposible la falsificación o modificación de señalización por una tercera parte.

A no ser que un NodeB esté provisto de un mecanismo para pasar satisfactoriamente los procedimientos de autenticación e integridad, entonces los protocolos UMTS están diseñados de modo que casi no se pueda lograr comunicación útil con el UE. Sin embargo, hay “intervalos” en los protocolos UMTS que permiten que el IMSI, IMEI y TMSI sean recuperados del UE por el SINodeB 100 sin requerir estos mecanismos de seguridad.

Estos “intervalos” se describen en 3GPP TS 33.102 versión 3.13.0 edición 1999, y en 3GPP TS 24.008 versión 3.19.0 edición 1999. Ahora se describirán las porciones relevantes de estos protocolos.

3GPP TS 33.102 versión 3.13.0 edición 1999

Este protocolo especifica en la sección 6,5 que todos los mensajes de señalización excepto los siguientes serán de integridad protegida:

TRANSFERENCIA A UTRAN COMPLETA

TIPO DE BÚSQUEDA 1

PETICIÓN DE CAPACIDAD PUSCH

ASIGNACIÓN DE CANAL FÍSICO COMPARTIDO

PETICIÓN DE CONEXIÓN RRC

ESTABLECIMIENTO DE CONEXIÓN RRC

ESTABLECIMIENTO DE CONEXIÓN RRC COMPLETO

RECHAZO DE CONEXIÓN RRC

LIBERACIÓN DE CONEXIÓN RRC (CCCH solamente)

INFORMACIÓN DE SISTEMA (INFORMACIÓN EMITIDA)

INDICACIÓN DE CAMBIO DE INFORMACIÓN DE SISTEMA

Así, estos mensajes no pueden ser de integridad protegida bajo ninguna circunstancia.

3GPP TS 24.008 versión 3.19.0 edición 1999

Este protocolo especifica una lista de mensajes a los que el UE puede responder, en algunas circunstancias, sin que primero la red tenga que tener protegida la integridad. Específicamente, el protocolo especifica lo siguiente:

A excepción de los mensajes enumerados más adelante, ningún mensaje de señalización de capa 3 será procesado por las entidades MM y GMM receptoras o enviado a las entidades CM, a no ser que el procedimiento de control de modo de seguridad esté activado para dicho dominio.

- mensajes MM:
- PETICIÓN DE AUTENTICACIÓN
- RECHAZO DE AUTENTICACIÓN
- PETICIÓN DE IDENTIDAD
- ACEPTACIÓN DE ACTUALIZACIÓN DE LOCALIZACIÓN (en actualización periódica de localización sin cambio de zona de localización o identidad temporal)
- RECHAZO DE ACTUALIZACIÓN DE LOCALIZACIÓN
- ACEPTACIÓN DE SERVICIO CM, si se aplican las dos condiciones siguientes:
- no se establece ninguna otra conexión MM; y
- la ACEPTACIÓN DE SERVICIO CM es la respuesta a una PETICIÓN DE SERVICIO CM con SERVICIO CM

TIPO IE puesto a 'establecimiento de llamada de emergencia'

- RECHAZO DE SERVICIO CM
- INTERRUPCIÓN
- mensajes GMM:
- PETICIÓN DE AUTENTICACIÓN Y CIFRADO
- RECHAZO DE AUTENTICACIÓN Y CIFRADO
- PETICIÓN DE IDENTIDAD
- RECHAZO DE ADJUNTO
- ACEPTACIÓN DE ACTUALIZACIÓN DE ZONA DE ENRUTAMIENTO (en actualización periódica de zona de enrutamiento sin cambio de zona de enrutamiento o identidad temporal)
- RECHAZO DE ACTUALIZACIÓN DE ZONA DE ENRUTAMIENTO
- RECHAZO DE SERVICIO
- ACEPTACIÓN DE SALIDA (para no desconexión)

Mensajes CC:

- todos los mensajes CC, si se aplican las dos condiciones siguientes:
- no se establece ninguna otra conexión MM; y
- la entidad MM en la MS ha recibido un mensaje de ACEPTACIÓN DE SERVICIO CM sin cifrado o

Protección de integridad aplicada como respuesta a un mensaje de PETICIÓN DE SERVICIO CM, con SERVICIO CM

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

Por lo tanto, se puede establecer una conexión RRC sin requerir protección de integridad, dado que los mensajes de conexión RRC son enumerados como que no precisan protección de integridad en 3GPP TS 33.102 versión 3.13.0 edición 1999. Después de establecer una conexión RRC entre el SINodeB y el UE, al objeto de un procedimiento de actualización de localización, una serie de peticiones de identidad MM son enviadas por el SINodeB 100 para recuperar la información de identificación de UE. De nuevo, el UE responde a estas peticiones de identidad MM sin requerir protección de integridad porque la petición de identidad MM es especificada en la lista dada anteriormente en 3GPP TS 24.008 versión 3.19.0 edición 1999.

Específicamente, la serie de mensajes entre el UE y el SINodeB es la siguiente:

UE <-> SINodeB

-> petición de conexión RRC

<- establecimiento de conexión RRC

-> establecimiento de conexión RRC completo

-> petición de actualización de localización MM

<- petición de identidad MM (IMSI solicitante)

-> respuesta de identidad MM (IMSI)

<- petición de identidad MM (IMEI solicitante)

-> respuesta de identidad MM (IMEI)

<- petición de identidad MM ()

-> respuesta de identidad MM (IMEISV)

Cuando el UE envía la petición de actualización de localización MM, también pone en marcha un temporizador de actualización LAC. El SINodeB ignora esta petición si el UE no recibe una respuesta válida a la petición de actualización de localización MM dentro de un tiempo predeterminado, entonces el UE reenvía la petición de actualización de localización MM. Este proceso se repite unas pocas veces y después el UE interrumpe la conexión.

Así, enviando la serie de tres peticiones de identidad MM después de establecer la conexión RRC, y antes de que el UE interrumpa la conexión, el SINodeB puede recibir los mensajes de respuesta de identidad MM del UE sin requerir protección de integridad.

Una vez que la información de identidad ha sido recogida, el SINodeB rechaza la petición de actualización de localización, evitando así que el UE intente repetidas veces acampar en el SINodeB.

En las circunstancias descritas anteriormente, una vez que el UE establezca la conexión RRC transmitirá un mensaje de petición de actualización de localización. En operación normal, la red realizará entonces los procedimientos de autenticación e integridad, que aseguran que el UE y la red confíen en que el otro está legitimado. Después de esto, la red enviará un mensaje de aceptación de actualización de localización de integridad protegida. Las normas exigen al UE que ignore este mensaje si no es de integridad satisfactoriamente protegida, de modo que se evite efectivamente que un SINodeB realice este paso satisfactoriamente.

Una vez que el UE envía el mensaje de petición de actualización de localización, pone en marcha un temporizador, y si no se recibe una aceptación de actualización de localización exitosa antes de que expire el temporizador, el UE interrumpirá el intento y después reintentará. Hay un contador de reintentos, y si el UE ha reintentado demasiadas veces, interrumpirá los intentos y pasará a otra célula.

Los flujos normales de mensajes de protocolo de red darán lugar a la caída de la conexión RRC si el UE interrumpe la conexión; esto es porque la red deja caer la conexión por sus propias razones o porque el UE lo ha pedido.

La liberación de la conexión RRC es controlada por la red y es posible en el SINodeB intentar mantener la conexión una vez que el UE ha pedido que sea liberada.

No es preciso que algunos mensajes y procedimientos sean de integridad protegida y así estos pueden ser usados para continuar la comunicación con el UE, independientemente del procedimiento de actualización de localización. Un ejemplo de esto es la petición de capacidad RRC UE y los mensajes de respuesta.

Así, un flujo que permite mantener la conexión RRC durante unos pocos minutos podría ser como éste:

<-> Establecer conexión RRC

-> UE envía mensaje de petición de actualización de localización y pone en marcha un temporizador de actualización LAC

<-> La red envía repetidas veces un mensaje de petición de capacidad UE y el UE responde (esto asegura que la conexión RRC se mantenga activo incluso aunque la red no haya respondido a la petición de actualización de localización)

-> Después de unos pocos segundos el UE envía una indicación de liberación de conexión de señalización RRC, pidiendo la liberación de la conexión RRC. El SINodeB ignora este mensaje.

-> El temporizador de actualización LAC expira - así el UE reenvía la actualización de localización

<-> El procedimiento se repite unas pocas veces y entonces el UE interrumpe la conexión completamente y busca otras células.

Durante este proceso se usan los mensajes de petición de capacidad RRC UE (o alguna otra petición de información) engañar a la capa de protocolo RRC a que crea que el enlace está activo y así, incluso cuando el procedimiento de actualización de localización ha expirado, se mantiene la conexión RRC.

Esta conexión RRC se puede mantener durante varios minutos sin indicación al usuario UE de que algo está sucediendo. Durante este tiempo es así posible usar las transmisiones del UE a efectos radiogoniométricos, como se describe más adelante.

Si se requiere un período más largo de transmisión continua, todo lo necesario es hacer que el UE intente realizar de nuevo otro procedimiento de actualización de localización. Esto se puede lograr difundiendo una segunda célula con un LAC diferente del SINodeB. Así, en este caso, el SINodeB establece primero una conexión RRC con el dispositivo donde el SINodeB está difundiendo una célula configurada con un primer código LAC al UE; detecta que el UE ha liberado la conexión RRC, y en respuesta a dicha detección transmite inmediatamente una segunda célula con un segundo código LAC para hacer que el UE restablezca la conexión RRC con el SINodeB. Este proceso se puede repetir entonces con diferentes códigos LAC para mantener indefinidamente la conexión RRC.

En lugar de transmitir los diferentes códigos LAC uno tras otro de la forma descrita anteriormente, los múltiples NodeBs (que están sustancialmente cosituados en el SINodeB) pueden transmitir simultáneamente las células con diferentes LACs.

Así, por los métodos descritos anteriormente, el SINodeB establece y mantiene una “llamada ciega” con el UE: es decir, una conexión de señal que no hace que el UE proporcione una alerta visual o audible.

Siguiendo el proceso descrito anteriormente, el SINodeB 100 puede mantener una conexión RRC durante un período de tiempo prolongado. Sin embargo, a efectos radiogoniométricos, también hay que asegurar que el UE esté transmitiendo en un código de cifrado conocido y fijado.

En la red real, la señal recibida tiene que pasar por muchas etapas de demultiplexión/decodificación antes de que se envíen datos de usuario útiles. Esto es debido a que los datos transmitidos por el aire constan de múltiples canales lógicos que son mapeados sobre canales de transporte. Estos canales de transporte son mapeados entonces sobre canales físicos. En cada etapa de multiplexión, los diferentes canales mapeados sobre el mismo canal de transporte deben ser diferenciados. Esto se realiza usando pasos de codificación adicionales.

Por ejemplo, la última etapa en este proceso implica combinar todos los canales físicos en una sola transmisión UE. Todos los canales físicos son tratados con diferentes códigos de canalización y después se suman y el resultado es tratado con el código de cifrado que hace la transmisión UE distinguible de otros UEs.

El proceso de decodificación/demultiplexión realizado por el SINodeB y el UE se ilustra en la figura 3. El espectro UMTS se divide en múltiples canales de frecuencia (12 en el Reino Unido), cada uno definido por una banda de frecuencia con una frecuencia central definida por un UARFCN y asociada con un operador concreto. En la dirección de enlace ascendente cada canal es decodificado por un NodeB usando un código de descifrado de enlace ascendente respectivo, estando asociado cada código de descifrado de enlace ascendente con UN UE respectivo. Después del descifrado, la señal es decodificada también usando un número de códigos de canalización, obteniendo N canales físicos dedicados cada uno asociado con un código de canalización respectivo. En la dirección de enlace descendente cada canal es decodificado por el UE usando un código de cifrado de enlace descendente respectivo, estando asociado cada código de cifrado de enlace descendente con una célula respectiva.

En UMTS hay dos formas principales en las que el UE es capaz de hacer una conexión de señalización con la red. La primera es usar el canal RACH, que es una forma de mecanismo de acceso aleatorio en el que todos los UEs compiten por un recurso de comunicaciones compartido. El canal FACH es usado por la red para responder a la señalización recibida en el canal RACH. En este caso, el mensaje será emitido de modo que cada UE sea capaz de recibirlo, pero tendrá un identificador que detalle a qué UE va dirigido el mensaje. Cuando el mecanismo donde los canales RACH y FACH se usan para comunicación, se dice generalmente que el UE está en el estado cellFACH. Éste es utilizado por la red para señalización de baja anchura de banda o transferencia de datos. El proceso de actualización de localización se realiza generalmente en cellFACH porque este proceso de señalización es corto y no merece la pena asignar un recurso de red dedicado a este procedimiento corto y bastante regular.

En el caso donde la finalidad de mantener la conexión es radiogoniométrica, el mecanismo de comunicación compartido de cellFACH no es útil, puesto que muchos UEs estarán usando los mismos códigos.

Al establecer una conexión RRC, el SINodeB ordena al UE que use un canal dedicado (estado cellDCH), asociado con un código de cifrado de enlace ascendente elegido y un código de canalización elegido. En este caso el mensaje de establecimiento de conexión RRC describe el canal dedicado (DCH) que el UE y red usarán para comunicación.

Una vez que el UE está transmitiendo en un DCH especificado, un radiogoniómetro 106 puede realizar radiogonometría usando la técnica descrita a continuación.

La radiogoniometría en 3G difiere de la de 2G porque la señal 2G está puramente en el dominio de frecuencia, mientras que la señal 3G está en el dominio de código. Esto significa que en 2G un algoritmo radiogoniométrico puede operar analizando las diferencias de tiempo entre señales adecuadamente filtradas recibidas en cada una de las antenas en la serie de antenas. En 3G hay que producir una entrada adecuada para proporcionarla al algoritmo radiogoniométrico. Esto significa efectivamente que la señal filtrada recibida en cada antena en la serie tiene que ser rastreada y descifrada/decodificada independientemente.

Por lo tanto, el radiogoniómetro 106 determina la dirección de la señal de localización 3G codificada detectando la señal de localización con una serie de N antenas, decodificando por separado una salida de cada antena para generar N salidas decodificadas, y midiendo la dirección de llegada de la señal de localización analizando las N salidas decodificadas.

El radiogoniómetro 106 se ilustra con más detalle en la figura 4, e incluye un procesador que ejecuta un algoritmo DF, una serie de cinco antenas, y una serie de cinco receptores rake y descifradores, recibiendo cada uno señales de localización codificadas de una antena respectiva y generando una salida decodificada para el algoritmo DF.

Cada receptor rake tiene una serie de subreceptores/descifradores independientes. Cada subreceptor/descifrador rake está configurado para decodificar y rastrear una señal de localización codificada asociada con un recorrido de propagación diferente del dispositivo. Por ejemplo un subreceptor/descifrador rake podría decodificar y rastrear un recorrido de propagación principal en una línea directa de visión con el dispositivo y otro subreceptor rake podría decodificar y rastrear un recorrido de propagación secundario producido por reflexión de un objeto próximo. Así, cada subreceptor/descifrador rake genera dos salidas:

- Información de tiempo: es decir, datos que indican el desfase del subreceptor/descifrador rake; y
- Datos de amplitud de señal.

En un receptor rake convencional, un bloque combinador suma coherentemente los datos de amplitud de señal de todos los subreceptores rake y la suma coherente es usada entonces como la entrada al proceso de decodificación siguiente en la cadena de recepción. En contraposición, los receptores/descifradores rake de la figura 4 no pasan dicha suma coherente al algoritmo DF. Para radiogoniometría, lo que tiene interés no con los datos coherentemente sumados de amplitud de señal, sino la información de tiempo y los datos de amplitud de señal asociada con cada recorrido de propagación. Por lo tanto, los receptores/descifradores rake introducen esta información de tiempo y datos de amplitud de señal en el algoritmo DF.

Todos los receptores/descifradores rake están sincronizados a una sola fuente de tiempo exacta, para asegurar que los pequeños retardos entre recibir una señal en cada antena en la serie se representen exactamente en la información de tiempo.

El algoritmo DF realiza entonces funciones de correlación usando la información de tiempo y los datos de amplitud de señal para generar una salida que puede ser visualizado para el usuario. Un ejemplo de cómo la información podría ser presentada se representa en la figura 5. Se presentan varias flechas en un mapa, indicando la longitud y/o anchura de la flecha la amplitud de señal, e indicando la dirección de la flecha la dirección que se deduce de la información de tiempo. Cada flecha está asociada con un recorrido de propagación diferente del dispositivo.

Dado que hay un pequeño riesgo de que el código de cifrado de enlace ascendente elegido por el SINodeB para el UE deseado ya esté en uso por otro UE conectado a las redes reales, habrá que comprobar que no haya transmisión de UE usando el código de cifrado a punto de ser asignado.

Esto se puede realizar en una de dos formas:

1. El radiogoniómetro guarda una lista A de posibles códigos de cifrado de enlace ascendente, y comprueba las señales de enlace ascendente en todos estos códigos de cifrado, dando un subconjunto B de la lista A. Después asigna un código de cifrado C que está en la lista A, pero no en la lista B. Entonces envía al SINodeB datos que identifican el código de cifrado C, y el SINodeB asigna dicho código de cifrado al UE.

2. El SINodeB envía un mensaje al radiogoniómetro identificando un código de cifrado que propone usar. El radiogoniómetro comprueba una señal de enlace ascendente usando el código propuesto. Si no se halla señal de enlace ascendente, entonces el radiogoniómetro informa al SINodeB, y el SINodeB asigna dicho código de cifrado al UE. Si se halla una señal de enlace ascendente, el radiogoniómetro informa al SINodeB, y el SINodeB inicia otra comprobación usando un código propuesto diferente. Esto se repite hasta que un código de cifrado es asignado al UE.

Realizando solamente un solo paso de decodificación (usando el código de descifrado de enlace

ascendente), esta técnica proporciona una señal descifrada conteniendo toda la potencia rf del UE deseado. La señal descifrada es analizada posteriormente como se ha descrito anteriormente.

La comunicación entre el radiogoniómetro 106 y SINodeB 100 se realiza por medio de un enlace 107 representado en la figura 1. El enlace 107 puede ser un enlace inalámbrico o alámbrico fijo. En este último caso, el SINodeB 100 y el radiogoniómetro 106 pueden estar integrados en una sola unidad. En el primer caso, el enlace inalámbrico puede ser un enlace dedicado en el que los datos son transmitidos y recibidos automáticamente (es decir, sin intervención humana). Alternativamente, la comunicación puede ser realizada verbalmente por un operador humano del radiogoniómetro 106 telefoneando a un operador humano del SINodeB 100.

REIVINDICACIONES

1. Un método de determinar la dirección de una señal de localización codificada de un dispositivo de comunicaciones móviles (120) con relación a un radiogoniómetro (106), incluyendo el método recibir la señal de localización codificada del dispositivo por un enlace inalámbrico con el radiogoniómetro (106); y usar un código para decodificar la señal de localización codificada y generar una salida decodificada; incluyendo el método detectar la señal de localización codificada con una serie de N antenas, caracterizado por decodificar por separado una salida de cada antena para generar N salidas decodificadas, y medir la dirección de llegada de la señal de localización codificada analizando las N salidas decodificadas.

2. El método de la reivindicación 1, incluyendo además transmitir una orden al dispositivo (120) ordenándole que transmita usando un código específico; y usar el código específico para decodificar la señal de localización codificada.

3. El método de la reivindicación 2, incluyendo además verificar si el código está asignado actualmente a otro dispositivo de comunicaciones móviles; y transmitir la orden al dispositivo (120) ordenándole que transmita usando el código específico si el código no está asignado actualmente a otro dispositivo de comunicaciones móviles.

4. El método de cualquier reivindicación precedente, incluyendo además detectar una o más señales de localización codificadas adicionales, estando codificada cada señal de localización codificada con el mismo código, pero asociada con un recorrido de propagación diferente del dispositivo; decodificar cada señal de localización codificada adicional para generar una salida decodificada adicional; y medir la dirección de llegada de la(s) señal(es) de localización codificada(s) adicional(es) analizando la(s) salida(s) decodificada(s) adicional(es).

5. El método de cualquier reivindicación precedente, incluyendo además mantener una conexión con el dispositivo de comunicaciones móviles (120), incluyendo el método establecer una conexión con el dispositivo; recibir una petición del dispositivo de liberar la conexión; y enviar repetidas veces una petición de información al dispositivo para evitar que el dispositivo libere la conexión.

6. El método de la reivindicación 5, donde la conexión es una conexión RRC.

7. El método de la reivindicación 5 o 6 donde la petición es una petición de capacidad de dispositivo.

8. El método de cualquiera de las reivindicaciones 1 a 4, incluyendo además mantener comunicación con el dispositivo celular móvil de comunicaciones (120), incluyendo el método establecer una conexión con el dispositivo difundiendo una primera célula configurada con un primer código de localización al dispositivo; y restablecer la conexión con el dispositivo después de que el dispositivo haya liberado la conexión difundiendo una segunda célula configurada con un segundo código de localización al dispositivo.

9. El método de la reivindicación 8 incluyendo además detectar que el dispositivo ha liberado la conexión, y transmitir la segunda célula configurada con el segundo código de localización en respuesta a dicha detección.

10. El método de la reivindicación 8 o 9, incluyendo además difundir simultáneamente las células primera y segunda con diferentes códigos de localización desde dos transmisores sustancialmente cosituados.

11. El método de cualquier reivindicación precedente, incluyendo además generar una salida que es indicativa de la dirección del dispositivo de comunicaciones móviles.

12. El método de la reivindicación 11, incluyendo además presentar a un usuario la salida que es indicativa de la dirección del dispositivo de comunicaciones móviles.

13. Un producto de programa de ordenador que, al ejecutarse en uno o más ordenadores, hace que el (los) ordenador(es) realice(n) un método según cualquier reivindicación precedente.

14. Aparato (106) configurado para realizar un método según cualquier reivindicación precedente.

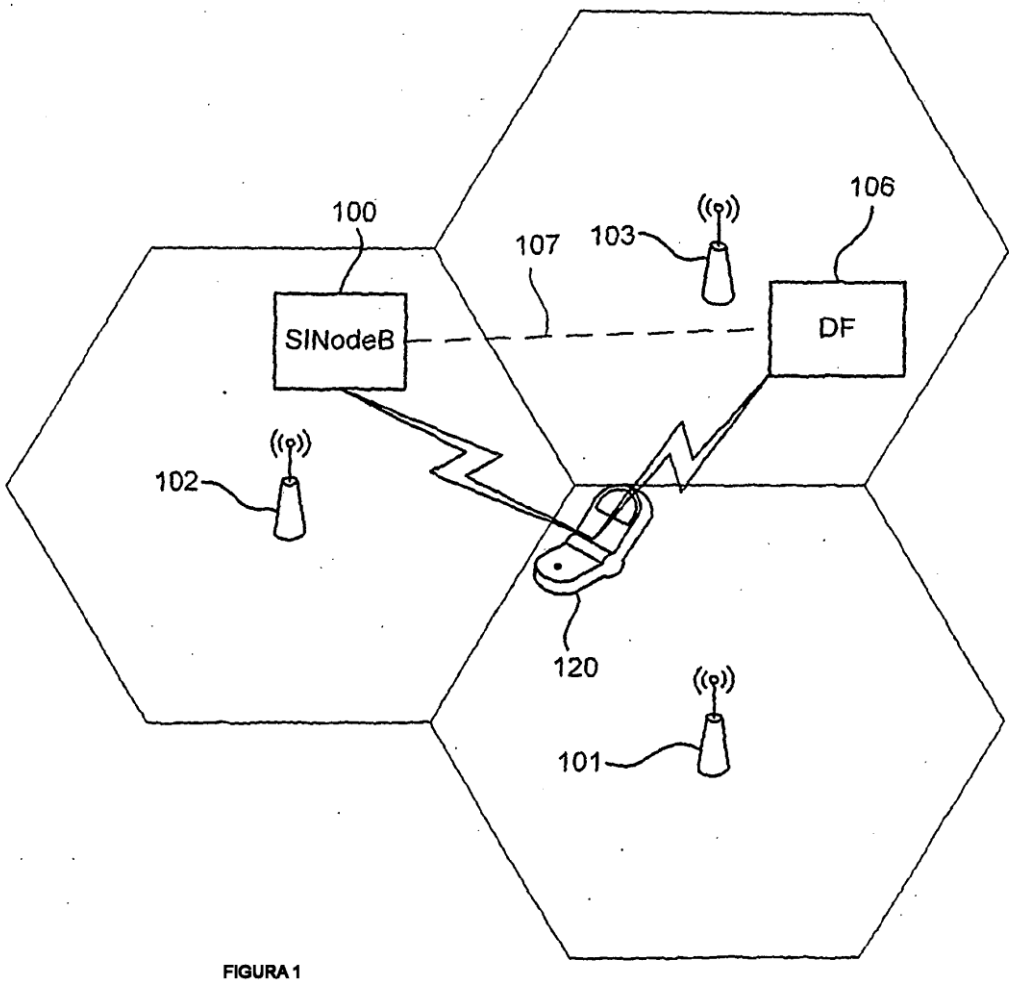

FIGURA 1

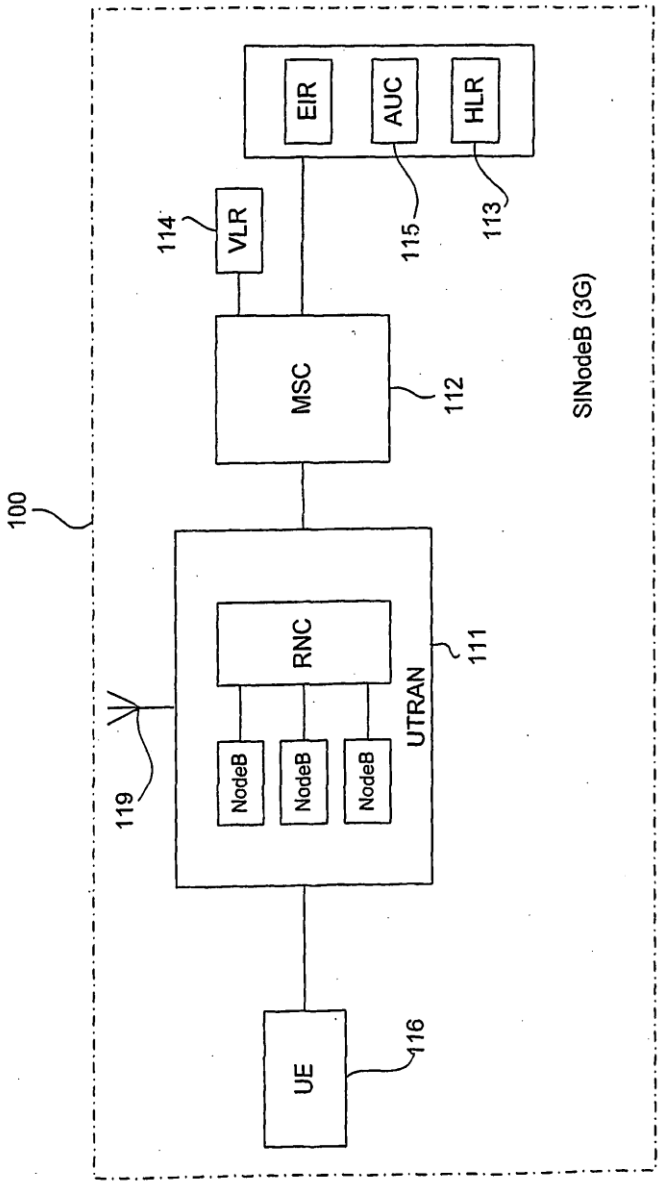
100
EIR
AUC
HLR
114
VLR
115
113
MSC
112
SINodeB (3G)
RNC
111
UTRAN
NodeB
NodeB
NodeB
119
UE
116

FIGURA 2

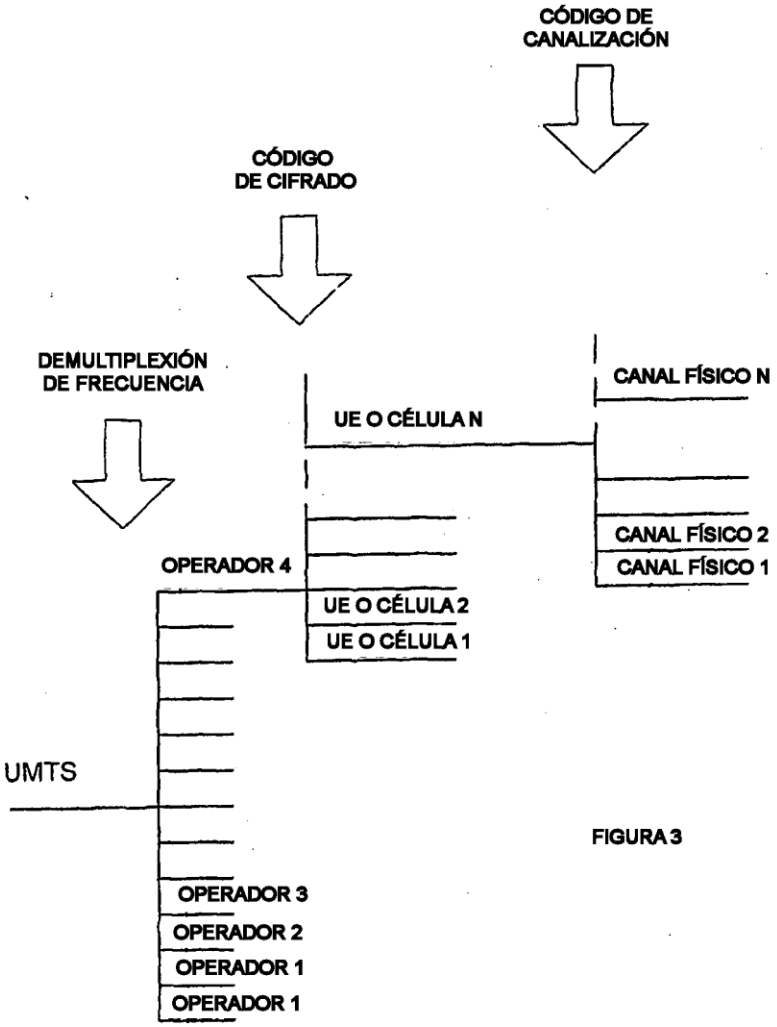
CÓDIGO DE CANALIZACIÓN
CÓDIGO DE CIFRADO
DEMULTIPLEXIÓN DE FRECUENCIA
CANAL FÍSICO N
UE O CÉLULA N
CANAL FÍSICO 2
CANAL FÍSICO 1
OPERADOR 4
UE O CÉLULA 2
UE O CÉLULA 1
UMTS
OPERADOR 3
OPERADOR 2
OPERADOR 1
OPERADOR 1

FIGURA 3

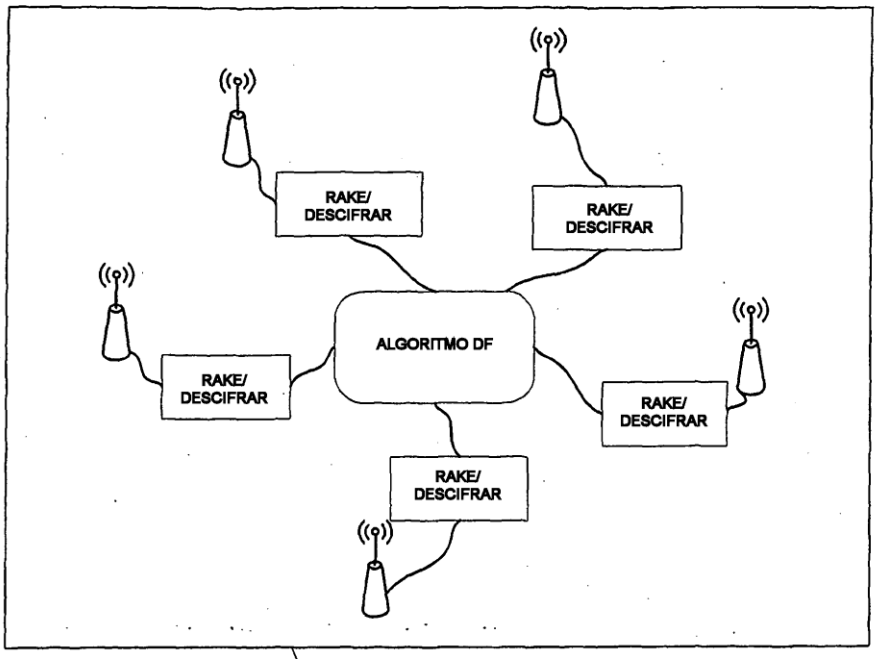

FIGURA 4

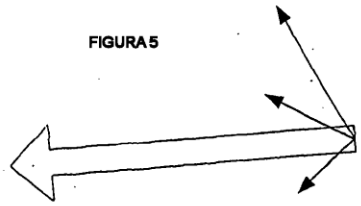

FIGURA 5