

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 780 177**

51 Int. Cl.:

H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04W 8/20 (2009.01)
G06Q 20/20 (2012.01)
H04W 60/04 (2009.01)
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **30.05.2011** **E 11360021 (7)**

97 Fecha y número de publicación de la concesión europea: **04.12.2019** **EP 2530962**

54 Título: **Autenticación**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
24.08.2020

73 Titular/es:

**ALCATEL LUCENT (100.0%)
Site Nokia Paris Saclay, Route de Villejust
91620 Nozay, FR**

72 Inventor/es:

**CLAUSSEN, HOLGER;
KENNEDY, IRWIN y
SAMUEL, LOUIS**

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 780 177 T3

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).

DESCRIPCIÓN

Autenticación

5 Campo de la invención

La presente invención se refiere a un método para establecer un conjunto de credenciales de verificación de equipos de usuario a partir de un protocolo de autenticación dentro de una red inalámbrica de comunicaciones, a un producto de programa informático y a un sistema operable para llevar a cabo ese método.

10

Antecedentes

Se conocen sistemas de telecomunicaciones inalámbricas. En tales sistemas, el equipo del usuario se desplaza a través de una red inalámbrica de telecomunicaciones. Se proporcionan estaciones base que soportan áreas de cobertura de radio. Se proporcionan varias de estas estaciones base y se distribuyen geográficamente para proporcionar una amplia área de cobertura al equipo del usuario. Cuando el equipo del usuario está dentro de un área servida por una estación base, la comunicación puede establecerse entre el equipo de usuario y la estación base a través de enlaces de radio asociados. Una estación base normalmente soporta varios sectores dentro de un área geográfica de servicio.

15

20

Se desea permitir que el equipo del usuario interactúe con objetos del mundo real. El uso de equipo de usuario, tales como teléfonos móviles, para acceder a interacciones con objetos del mundo real es particularmente atractivo, ya que los usuarios finales están familiarizados y cómodos con sus teléfonos móviles.

25

Las posibles interacciones con objetos del mundo real incluyen, por ejemplo, pago conveniente por teléfono móvil; el pago puede realizarse colocando un teléfono móvil u otro equipo de usuario similar en un área de pago en un mostrador de la tienda. Además, después del pago satisfactorio, se puede enviar un recibo SMS de la transacción al equipo del usuario.

30

Otros ejemplos de interacciones con objetos del mundo real pueden incluir permitir que el equipo del usuario descargue contenido del mundo real tocando un objeto. Por ejemplo, es posible descargar un horario de trenes directamente al equipo del usuario tocando el equipo del usuario contra una máquina de tickets o un horario relevante en una estación de tren. Se puede activar una descarga al equipo del usuario colocando el teléfono sobre el contenido; por ejemplo, una máquina expendedora de billetes en una estación de tren. Como alternativa, puede ser posible enviar un enlace al horario a través de un mensaje SMS o similar desde donde un usuario pueda acceder a él.

35

Además, el equipo del usuario puede usarse como un sistema de entrada sin llave para casas, coches y lugares de trabajo.

40

Se apreciará que los ejemplos de interacción dados representan solo unas pocas de un gran número posible de posibilidades con respecto a la interacción local entre el equipo del usuario y los objetos del mundo real.

45

Para proporcionar de manera fiable servicios interactivos entre el equipo del usuario y un objeto del mundo real, es necesario obtener una indicación de identidad del equipo del usuario ubicado en la región del objeto del mundo real y que la velocidad de activación de dichos sensores funcione de manera que perturbe la experiencia de un usuario final lo menos posible.

50

El documento US 2009/0029677 describe métodos de autenticación mutua en una red móvil. Un método descrito comprende: generar un ticket de servicio y una clave de sesión correspondiente a una estación móvil de acuerdo con una solicitud de datos de autenticación para la estación móvil. El cupón de servicio y la clave de sesión se cifran utilizando una clave de seguridad de usuario preasignada de acuerdo con la estación móvil. El cupón de servicio cifrado y la clave de sesión se envían a la estación móvil mediante un mensaje de control. La estación móvil se autentica analizando la información de autenticación mutua del usuario recibida de la estación móvil. Otro método de autenticación descrito comprende: enviar a una estación base un mensaje de respuesta de datos de usuario que incluye un identificador de abonado si se recibe un mensaje de solicitud de datos de usuario desde una estación base. A continuación, el usuario recibe, desde la estación base, un mensaje de solicitud de autenticación de usuario que incluye al menos un cupón de servicio y la clave de sesión cifrada con una clave de seguridad de usuario. El método incluye la etapa de descodificar el cupón de servicio y la clave de sesión utilizando la clave de seguridad de usuario previamente almacenada, y la etapa de enviar a la estación base un valor de respuesta de autenticación de usuario que incluye un valor aleatorio, un valor aleatorio cifrado con la clave de sesión descodificada y el cupón de servicio descodificado. Si se recibe un valor aleatorio de la estación base, un sistema de comunicación móvil se autentica comparando el valor aleatorio enviado con el valor aleatorio recibido.

55

60

65

El documento EP 1199903 describe un método para monitorizar un teléfono móvil sin activar el teléfono móvil. De acuerdo con el método descrito, una estación base es operable para activar un teléfono móvil para transmitir sus

parámetros de identificación, sin que el usuario del teléfono móvil se dé cuenta de la liberación de los parámetros de identificación. De acuerdo con el método descrito, una estación base opera para activar una llamada de un terminal móvil normal y solicitar parámetros de identificación móvil, pero el disparador finaliza antes de que se envíe un comando de establecimiento de llamada. Por lo tanto, antes de recibir una señal de establecimiento, la conexión al teléfono móvil se termina enviando una señal de liberación del canal.

El documento WO 2009/113057 describe un aparato mediante el cual se puede usar una estación móvil (equipo de usuario) como medio para iniciar, activar o confirmar pagos. En una realización, se proporciona un blindaje para definir un área de cobertura y un blindaje contra las señales de radio que se originan fuera del área de cobertura. Se proporciona una antena asociada con el área de cobertura y se acopla a un transmisor. El transmisor funciona comunicándose con cualquier estación móvil ubicada en el área de cobertura definida. Se proporciona una unidad de control de servicio y está dispuesta para responder a la comunicación entre el transmisor y la estación móvil. Una estación de servicio que proporciona un producto o servicio cerca del área de cobertura funciona proporcionando un producto o servicio que responda a la unidad de control de servicio. En una realización, el sistema comprende además un servidor de aplicaciones en comunicación con la red celular, operable para recibir la identificación de la estación móvil de la red y, en algunas realizaciones, operable para cargar a un usuario asociado con la estación móvil por la provisión de un producto o servicio.

Se desea proporcionar un método para verificar la identidad del equipo de usuario autenticado para permitir interacciones seguras rápidas.

Sumario

La presente invención se refiere a la materia objeto tal como se desvela en las reivindicaciones adjuntas.

Un primer aspecto proporciona un método de preautenticación según la reivindicación 1.

En un momento en que las entradas de voz y datos están disminuyendo, los operadores de telefonía móvil están interesados en diversificar sus negocios al proporcionar nuevos servicios más allá del simple acceso a las llamadas a través de una red central. Al permitir las interacciones con objetos del mundo real utilizando equipos de usuario, un usuario final puede usar su relación existente con la red celular y el teléfono, y un operador móvil generalmente tendrá la mayor parte de la infraestructura para proporcionar servicios basados en tales interacciones.

Tales disposiciones pueden ser particularmente ventajosas si las implementaciones aseguran que no se requieren modificaciones de software o hardware para el equipo de usuario existente y los métodos funcionan con el equipo de usuario 4Bn + existente. La provisión de una unidad de interrogación adecuada puede proporcionar información de posicionamiento extremadamente precisa, ya que puede funcionar en interiores y ser más precisa que el GPS o el WiFi, junto con la autenticación segura basada en SIM, lo que permite la reutilización de una relación de facturación existente entre el equipo del usuario y un operador de red móvil, creando así una nueva y potente plataforma.

Para proporcionar de manera fiable servicios interactivos entre el equipo del usuario y un objeto del mundo real, se requiere que las interacciones locales entre el equipo del usuario y los objetos del mundo real solo sean activadas por el equipo del usuario que desea descargar o tener acceso al contenido del mundo real. La extracción de un identificador único del equipo del usuario en la región de un objeto del mundo real puede garantizar que los servicios interactivos se proporcionen solo al equipo del usuario que los solicita.

Por lo general, la interacción entre un objeto del mundo real y el equipo del usuario requiere la presencia de algún tipo de unidad de interrogación o sensor para permitir que se extraiga del equipo de usuario un identificador único del equipo del usuario en un rango corto o pequeña escala, el área de cobertura proporcionada por la unidad de interrogación asociada con un objeto del mundo real. Cualquier unidad de interrogación de este tipo debe operar de tal manera que permita que la infraestructura de red celular existente suministrada por macro estaciones base habituales en una red inalámbrica de telecomunicaciones se complemente sin interrupciones significativas.

Las interacciones con objetos del mundo real requieren una detección de corto alcance y una autenticación completa de los equipos de los usuarios para aprovechar al máximo los recursos, por ejemplo, facturación del usuario final o información de pago, ya disponible para un operador de telefonía móvil. En las unidades de interrogación que proporcionan un sistema de detección de UE, la velocidad de disparo es un factor muy importante. Debido a las diferentes implementaciones de estándares en teléfonos móviles, se ha descubierto que la unidad de interrogación detecta las velocidades de disparo (por ejemplo, para sistemas basados en la extracción de identidad de UE utilizando técnicas de "Actualización de área local") puede ser variable, que suele oscilar entre 2 y 5 segundos. Existe un problema, sin embargo, de que, de acuerdo con tal sistema, la identidad de un UE puede no confirmarse como auténtica en el momento de interactuar con un objeto del mundo real. Puede haber sido previamente autenticado en la región de un sensor, pero, por ejemplo, en el momento de la interacción con un objeto del mundo real, una identidad de UE puede estar falsificada. Los aspectos descritos en el presente documento reconocen que es posible llevar adelante una relación de autenticación preestablecida hasta el momento de la ejecución de la transacción.

5 El primer aspecto proporciona un método para aumentar la velocidad de disparo efectiva de los sensores celulares, como las unidades de interrogación de identidad. La reducción del tiempo de disparo sin sacrificar la integridad de un sistema de identificación completo, por ejemplo, la autenticación completa de la identidad del equipo del usuario, es altamente deseable. El primer aspecto reconoce que la preautenticación de la indicación liberada de la identidad recibida del equipo del usuario puede ser ventajosa. En consecuencia, dicha autenticación puede producirse comunicándose con una red de comunicación mayor, tal como una red central de proveedores de redes móviles, para establecer la autenticación completa de un identificador de equipo de usuario. Dicha autenticación completa del identificador permite la facturación fiable de un usuario final y normalmente implica técnicas criptográficas u otras técnicas secretas compartidas.

15 El primer aspecto reconoce que un tiempo de disparo efectivo experimentado por un usuario final puede reducirse mediante la introducción de un método de detección de dos etapas, autenticación y validación. Se apreciará que es posible adquirir una indicación de identidad del equipo del usuario que opera cerca de un sensor antes de que el equipo del usuario se coloque contra un objeto del mundo real y se le pida que "interactúe" con ese objeto del mundo real. Es decir, antes de colocar el equipo del usuario en el sensor. También es posible autenticar previamente el equipo del usuario que opera cerca de un sensor.

20 El establecimiento de un conjunto compartido de credenciales de verificación del equipo del usuario para la validación futura de la identidad autenticada del equipo del usuario evita el requisito de una mayor autenticación de la identidad del equipo del usuario utilizando el protocolo de autenticación. En consecuencia, en lugar de requerir el tiempo requerido para realizar una autenticación y comunicación completas con una red central, las credenciales de verificación que comprenden un nuevo secreto compartido conocido solo por un equipo de usuario previamente autenticado y la unidad de interrogación puede usarse para verificar la identidad de un equipo de usuario previamente autorizado. Las credenciales de verificación pueden almacenarse localmente dentro de la unidad de interrogación y, por lo tanto, la necesidad de comunicarse con capas de una red de telecomunicaciones inalámbrica completa, por ejemplo, una red central, se puede evitar.

30 En una realización, la etapa de autenticación comprende comunicarse con una red central de un proveedor de servicios para autenticar la identidad del equipo del usuario utilizando el protocolo de autenticación. Los procedimientos de autenticación generalmente comprenden técnicas secretas compartidas criptográficas, de modo que una clave conocida solo por un operador móvil y un equipo de usuario asociado con ese operador móvil se usa para autenticar la identidad del equipo del usuario. En una realización, el protocolo de autenticación comprende la autenticación de la identidad del equipo del usuario por medio de un secreto criptográfico compartido.

35 En una realización, el conjunto compartido de credenciales de equipo de usuario comprende al menos un nuevo secreto compartido. En consecuencia, no es necesario volver a autenticar el equipo del usuario en una etapa posterior, siempre que el nuevo secreto compartido, generado como parte de un procedimiento de autenticación, se determine correcto. Es decir, el nuevo conjunto de credenciales de equipo de usuario puede reemplazar la autenticación y proporcionar seguridad de conocimiento de que la identidad de un equipo de usuario es correcta, mientras ocurre en una escala de tiempo más corta ya que no se requiere autenticación completa.

45 Para extraer un identificador de equipo de usuario, una unidad de interrogación (por ejemplo, que comprende una unidad de preautenticación y una unidad de verificación) puede ser operable para comunicarse con el equipo del usuario dentro de un área de cobertura de radio soportada por la unidad de interrogación. En consecuencia, una unidad de interrogación puede tener la capacidad de determinar el entorno de radio en el que se implementa. Es decir, es operable para escuchar señales de conexión descendente y ascendente dentro de la red en todos los operadores de interés potencial, de todas las estaciones base de potencial interés.

50 Para establecer comunicación con el equipo del usuario, una unidad de interrogación tiene la capacidad de configurar su señal o señales de radio de conexión descendente para que coincidan, por ejemplo, en frecuencia, código de rescate, código de área de localización y otros parámetros de comunicación de conexión descendente similares, una o más celdas en el área donde existe el equipo de usuario. La conexión descendente de una unidad de interrogación se puede configurar de tal manera que el equipo del usuario normalmente monitorizará esos canales de conexión descendente (o similar), o camping en esos canales de conexión descendente (o similar) en una red macro. Tal disposición busca minimizar el tiempo que requiere la unidad de interrogación para establecer una conexión de comunicación viable con el equipo del usuario en su área de cobertura.

60 Si varias señales de conexión descendente de red macro son posibles candidatos para la comunicación con el equipo del usuario en una localización, por ejemplo, en la superposición entre áreas de cobertura proporcionadas por estaciones base adyacentes, se pueden emular múltiples operadores para garantizar que todos los equipos de usuario que pasan, no importa en qué celda estén atendidos, todavía se pueden detectar. Se apreciará que en áreas en las que dos o más proveedores de servicios brindan cobertura en diferentes frecuencias, para que el detector funcione en todas las frecuencias, puede ser necesario permitir que un detector trabaje o se haga pasar por esas mismas frecuencias múltiples en su conexión descendente.

Como alternativa, los proveedores de servicios podrían acordar y designar una o más frecuencias para establecer la comunicación con el equipo del usuario. Esta frecuencia puede reservarse exclusivamente para este propósito o puede estar en uso. A continuación, cada proveedor de servicios puede indicar a todos sus equipos de usuario que busquen esta frecuencia con características particulares del canal de conexión descendente. Esto se puede hacer completando la lista de vecinos de todas las celdas para contener estos detalles, por ejemplo, en UMTS, un código de codificación particular y un área de localización para cada proveedor de servicios. El equipo de detección puede, a continuación, irradiar en estas frecuencias acordadas con las características de conexión descendente acordadas. Al reducir la cantidad de frecuencias que deben irradiarse, el coste de los detectores se reduce.

El resultado de la suplantación de las características de la conexión descendente de la mayor red de telecomunicaciones circundante es que las celdas soportadas por el detector, aunque celdas de corto alcance, se convierten automáticamente en candidatos adecuados para una selección de celdas o un procedimiento de reelección ya conocido por el equipo del usuario dentro de una red inalámbrica a escala macro.

Asegurar que la extracción de un identificador único ocurra rápidamente ayuda a minimizar la interrupción de la red más grande y los inconvenientes para un usuario final que busca servicios interactivos.

En una realización, la etapa de emular comprende las etapas de: transmitir una señal de conexión descendente que comprende características de comunicación por radio sustancialmente idénticas a al menos uno de los nodos de red reconocibles por el equipo de usuario determinado como un nodo de red de servicio de dicho equipo de usuario.

En consecuencia, emulando transmisiones de conexión descendente como si fueran de una estación base u otro nodo de red que admita el equipo de usuario que sirve la celda, se puede establecer una comunicación muy rápida con el equipo del usuario.

En una realización, la etapa de emular comprende las etapas de: transmitir una señal de conexión descendente que comprende características de comunicación por radio sustancialmente idénticas a al menos uno de los nodos de red reconocibles por el equipo de usuario que se determina que están en una lista vecina de nodos de red mantenidos por el equipo de usuario. En consecuencia, emulando transmisiones de conexión descendente como si fueran de una estación base u otro nodo de red que ya está en la lista de vecinos del equipo del usuario, es probable que el equipo del usuario esté monitorizando y esperando detectar transmisiones de tales estaciones base y se pueda establecer una comunicación muy rápida con el equipo del usuario.

En una realización, la etapa de emular comprende las etapas de: transmitir una primera señal de conexión descendente que comprende características de comunicación por radio sustancialmente idénticas a al menos uno de los nodos de red reconocibles por el equipo de usuario para descubrir el equipo de usuario en una primera área predeterminada, y transmitir una segunda señal de conexión descendente que comprende características de comunicación por radio sustancialmente idénticas a al menos uno de los nodos de red reconocibles por el equipo de usuario. En consecuencia, se puede usar una primera señal para determinar, en tiempo lento, una lista de identidades de equipos de usuario en un área de cobertura predeterminada, por ejemplo, en el edificio de una estación de tren y esa lenta lista de tiempo, o etapa de descubrimiento, puede ser particularmente útil si se usa una segunda señal de conexión descendente, por ejemplo, por torniquetes de la estación de tren, para efectuar la identificación autenticada completa del equipo del usuario, dado que la cantidad de posibles equipos de usuario que podrían estar en un torniquete no será una red completa de equipos de usuario, pero simplemente aquellos ya determinados a estar en el edificio de la estación. Tal emulación de descubrimiento preventivo puede ayudar a acelerar un proceso adicional, por ejemplo pago, o ayudar en la implementación de procesos de búsqueda, minimizando las opciones de búsqueda necesarias.

En una realización, la etapa de disparar, obtener o determinar una indicación de identidad del equipo del usuario comprende las etapas de: haciendo que el equipo del usuario inicie un procedimiento de actualización del área de localización.

Existen varios mecanismos en una red de comunicación inalámbrica para extraer o intercambiar identificadores únicos del equipo del usuario. Uno de esos mecanismos es un procedimiento de actualización del área de localización, durante el cual el equipo del usuario pasa un identificador único, generalmente su IMSI, a la red. También existen otros mecanismos para extraer identificadores únicos del equipo del usuario; por ejemplo, los mensajes de búsqueda pueden ser respondidos por el equipo del usuario y, a continuación, una vez que se establece la conexión, la unidad de interrogación puede instruir o consultar con el equipo del usuario, lo que da como resultado la liberación de un identificador único.

En una realización, la etapa de hacer que el equipo del usuario inicie una actualización del área de localización comprende las etapas de: emular las características de comunicación por radio de conexión descendente de al

menos uno de los nodos de la red con una intensidad de señal suficiente para ser recibida en el equipo del usuario mayor que una señal correspondiente transmitida por el nodo de red que se emula. En consecuencia, el equipo del usuario puede determinar, mientras está en un área de cobertura apoyada por la unidad de interrogación, que la unidad soporta una celda que parece ser un candidato más adecuado para una buena comunicación con la red más grande. Dicha determinación puede dar como resultado que el equipo del usuario solicite la reelección de la celda y, como parte de esa reelección de la celda, se puede activar una actualización del área de localización.

En una realización, el procedimiento comprende además las etapas de:
transmitir una instrucción para cambiar los parámetros de reelección de celda del equipo de usuario.

En consecuencia, una celda soportada por la unidad de interrogación puede verse obligada a aparecer ante el equipo del usuario como un candidato más adecuado para una buena comunicación con la red más amplia. Dicha determinación puede dar como resultado que el equipo del usuario solicite la reelección de la celda y, como parte de esa reelección de la celda, se puede activar una actualización del área de localización.

En una realización, el procedimiento comprende además las etapas de:
transmitir una instrucción al equipo del usuario para releer las comunicaciones del canal de comunicación de conexión descendente. Se apreciará que el equipo del usuario puede no leer automáticamente toda la información transmitida en un canal de conexión descendente soportado por la unidad de interrogación.

Si la unidad está emulando la celda de servicio, pero con un código de área de localización diferente, la transmisión de una instrucción para releer los canales de comunicación puede dar como resultado que el equipo del usuario determine que se ha alterado un código de área de localización y se puede activar un procedimiento de actualización del área de localización.

En una realización, el procedimiento comprende además las etapas de:
transmitir una señal de interferencia en un canal de radio correspondiente a un canal de comunicación de al menos uno de los nodos de red reconocibles por el equipo de usuario determinado para ser un nodo de red de servicio del equipo de usuario. En consecuencia, si el equipo del usuario en el área de cobertura soportada por una unidad de interrogación experimenta una interferencia significativa en la conexión descendente de la celda en servicio, puede ser operable solicitar una transferencia a una celda alternativa. Esa celda puede ser soportada por la unidad de interrogación y puede tener un área de localización diferente a la de la celda de servicio. La inyección de interferencia puede, por tanto, provocar que el equipo del usuario vuelva a seleccionar una celda, determinar que un código de área de localización ha cambiado y activar un procedimiento de actualización de área de localización.

En una realización, la indicación de identidad comprende un IMSI o TMSI.

Un segundo aspecto proporciona un producto de programa informático, operable cuando se ejecuta en un ordenador, para realizar las etapas del método del primer aspecto.

Un tercer aspecto proporciona un sistema como se reivindica en la reivindicación 10.

El establecimiento de un conjunto compartido de credenciales de verificación del equipo del usuario para la validación futura de la identidad autenticada del equipo del usuario evita el requisito de una mayor autenticación de la identidad del equipo del usuario utilizando el protocolo de autenticación.

En una realización, la lógica de autenticación es operable para comunicarse con una red central de un proveedor de servicios para autenticar dicha identidad de equipo de usuario utilizando dicho protocolo de autenticación. En consecuencia, la lógica de autenticación puede transmitir información relacionada con la identidad del equipo del usuario y recibir información para autenticar esa identidad.

En una realización, el protocolo de autenticación comprende la autenticación de la identidad del equipo del usuario por medio de un secreto criptográfico compartido.

En una realización, el conjunto compartido de credenciales de equipo de usuario comprende al menos un nuevo secreto compartido.

En una realización, en la que la lógica de transmisión es operable para transmitir una señal de conexión descendente que comprende características de comunicación por radio sustancialmente idénticas al menos a uno de los nodos de red reconocibles por el equipo de usuario determinado como un nodo de red de servicio del equipo de usuario.

En una realización, en la que la lógica de transmisión es operable para transmitir una señal de conexión descendente que comprende características de comunicación por radio sustancialmente idénticas al menos a uno de los nodos de red reconocibles por el equipo de usuario que se encuentra en una lista vecina de nodos de red mantenidos por el equipo de usuario.

- 5 En una realización, en la que la lógica de interrogación es operable para transmitir una solicitud de búsqueda al equipo de usuario en la señal de conexión descendente que comprende características de comunicación por radio sustancialmente idénticas al menos a uno de los nodos de red reconocibles por el equipo de usuario.
- 10 En una realización, la transmisión de la solicitud de búsqueda comprende la transmisión de una serie de páginas de equipos de usuario, cada uno dirigido a un equipo de usuario en la red inalámbrica de telecomunicaciones.
- 15 En una realización, la transmisión de la solicitud de búsqueda comprende la transmisión de una serie de páginas de equipos de usuario agrupados, cada uno dirigido a un grupo de equipos de usuario en la red inalámbrica de telecomunicaciones.
- 20 En una realización, la lógica de interrogación es operable para hacer que el equipo del usuario inicie un procedimiento de actualización del área de localización.
- 25 En una realización, la lógica de interrogación es operable para provocar que el equipo del usuario emule dichas características de comunicación de radio de conexión descendente de al menos uno de dichos nodos de red con una intensidad de señal suficiente para ser recibida en dicho equipo de usuario mayor que una señal correspondiente transmitida por dicho nodo de red que se emula.
- 30 En una realización, la lógica de transmisión es operable para transmitir una instrucción para cambiar los parámetros de reelección de celda del equipo de usuario.
- 35 En una realización, la lógica de transmisión es operable para transmitir una instrucción al equipo del usuario para volver a leer las comunicaciones del canal de comunicación de conexión descendente.
- 40 En una realización, la unidad comprende además lógica de interferencia operable para transmitir una señal de interferencia en un canal de radio correspondiente a un canal de comunicación desde al menos uno de los nodos de red reconocibles por el equipo de usuario determinado como un nodo de red de servicio del equipo de usuario.
- 45 En una realización, la indicación de identidad comprende un IMSI o TMSI.
- 50 Las credenciales de verificación establecidas como parte de la preautenticación se utilizan para verificar la identidad del equipo del usuario, sin la necesidad de volver a autenticarse y, por lo tanto, sin la necesidad de contactar a una red central de operadores móviles. Por lo tanto, añadiendo una etapa adicional, la preautenticación, en lugar de autenticar al mismo tiempo que un objeto del mundo real detecta que un equipo de usuario está cerca de un sensor de proximidad, un disparador efectivo y tiempos de autenticación efectivos experimentados en una proximidad, o el sensor de verificación se puede reducir.
- 55 El método comprende además: recibir una indicación de la identidad del equipo de usuario para aquellos equipos de usuario autenticados que se determina que están en un área de descubrimiento geográfica predeterminada; y buscar los equipos de usuario autenticados que se determina que están en el área de descubrimiento geográfico predeterminada. En consecuencia, la búsqueda puede ser un medio eficaz y eficiente para determinar qué equipo de usuario en la vecindad general de un sensor de proximidad está realmente "encendido" en el sensor. En consecuencia, el propio sensor de proximidad no necesita extraer activamente ninguna indicación de identidad del equipo del usuario del equipo del usuario, ya que la etapa de reconocer a los usuarios que podrían colocarse en el sensor ya ha ocurrido. Una vez que un móvil responde a un mensaje de búsqueda, el sensor utiliza la información obtenida por la celda más grande para interrogar al equipo del usuario y verificar su identidad sin la necesidad de realizar un protocolo de autenticación completo. Es decir, no se requiere un contacto completo con la red central y se realiza una "verificación de seguridad" basada en las credenciales de verificación predeterminadas por un proceso de autenticación completo. Esto acelerará el proceso de activación "efectivo", ya que el proceso de camping y autenticación que lleva la mayor parte del tiempo se realiza por adelantado cuando el móvil entra en una celda más grande.
- 60 El mensaje de búsqueda enviado por el sensor da como resultado el establecimiento de una comunicación de control de recursos de radio (RRC) con el UE. Sobre esta conexión, la estación base solicita que la integridad del UE proteja o cifre los mensajes transmitidos basándose en credenciales de verificación predeterminadas. Solo el UE autenticado podría proteger la integridad o cifrar la información transmitida, ya que conoce las credenciales de verificación predeterminadas. Por lo tanto, el sensor puede confiar en la identidad auténtica del UE y, por tanto, atribuir una transacción u otra acción al UE previamente autenticado correcto.
- 65 En una realización, el procedimiento comprende, además:
determinar una diferencia de tiempo entre el equipo de usuario autenticado que entra en dicha área de descubrimiento geográfica predeterminada y el equipo de usuario autenticado que responde a dicha búsqueda.
En una realización, el procedimiento comprende, además:

calcular una indicación de la diferencia de tiempo promedio en un conjunto de equipos de usuario autenticado. En una realización, el procedimiento comprende, además:
ajustando el área de descubrimiento geográfico predeterminada y / o un área de búsqueda predeterminada en respuesta a la diferencia de tiempo determinada.

5 En consecuencia, la cobertura de dos áreas soportadas por una unidad de interrogación (que comprende, por ejemplo, una unidad de preautenticación y una unidad de verificación) pueden optimizarse en algunas realizaciones observando diferencias de tiempo entre "camping y autenticación" realizado por una unidad de preautenticación, y un "evento de detección" real realizado por una unidad de verificación. Si hay una gran diferencia de tiempo entre los eventos de "camping y autenticación" y los de "detección", esto puede indicar que la cobertura piloto de una unidad de preautenticación es demasiado grande. Esto puede ser subóptimo, ya que un UE que se encuentra en un área de este tipo no puede hacer ni recibir ninguna llamada mientras está en la señal piloto de la unidad de preautenticación. En tal caso, la potencia piloto de un sensor puede reducirse en una etapa predeterminada. Si no hay diferencia de tiempo entre eventos, esto puede indicar que la cobertura de la señal piloto de una unidad de preautenticación es demasiado pequeña. Esto puede ser subóptimo, ya que puede provocar un retraso de detección / detección de proximidad. Si no hay una brecha entre los eventos, "camping y autenticación" no se completa antes del evento de "detección". En tal caso, la señal piloto puede reducirse en una etapa predeterminada. La diferencia de tiempo observada entre los eventos de "camping y autenticación" y de "detección" puede, de acuerdo con las realizaciones, monitorizarse y las áreas de cobertura de las unidades de preautenticación y verificación que comprenden una unidad de interrogación completa se pueden optimizar en función de valores predeterminados como un proceso iterativo.

En algunas realizaciones, una vez que se establece un enlace de comunicación con el equipo del usuario, por ejemplo, por búsqueda, el método puede comprender solicitar repetidamente un conjunto de informes de medición de potencia del UE. En algunas realizaciones, esos informes de medición pueden usarse para calcular una estimación de la distancia al equipo del usuario desde un sensor. En algunas realizaciones, tras una medición de la potencia que cruza un umbral predeterminado, se realiza una acción. En consecuencia, el contacto puede establecerse con un equipo de usuario preautorizado antes de que esté en contacto directo con un sensor de verificación, y solo una vez que se determine que está en estrecha proximidad, como lo indica un informe de medición que cruza un umbral predeterminado, el sensor de verificación realizará una acción predeterminada, por ejemplo, abriendo una puerta o descargando un horario.

Esta es una mejora para, por ejemplo, simplemente buscar el UE y recibir una respuesta y verificar las credenciales predeterminadas antes de activar una acción. La mejora reduce la latencia entre colocar un teléfono contra un sensor de verificación o proximidad y la transacción que se realiza. En algunas realizaciones, el uso de búsqueda para accionar una transacción puede introducir demoras. Por ejemplo, un UE puede requerir tiempo para responder a los mensajes de búsqueda debido a un ciclo de recepción discontinuo (ciclo DRx) utilizado para reducir el consumo de energía. Un ciclo DRx puede durar entre unos cientos de milisegundos y unos pocos segundos.

Para mitigar tales demoras y permitir que una acción se lleve a cabo de manera más rápida o inmediata, en algunas realizaciones se puede contactar con el equipo del usuario, por ejemplo, buscar, antes de estar en la localización crítica para configurar una conexión con el sensor. Un dispositivo sensor celular, como una unidad de verificación, solicita después una medición de potencia de recepción del UE para establecer su proximidad a él y / u otros transmisores, por ejemplo, otras unidades de verificación. Los transmisores pueden alojarse en la unidad del sensor y / o combinarse con transmisores alojados en unidades separadas, quizás femtoceldas u otras estaciones base. En algunas realizaciones, las mediciones se pueden solicitar con frecuencia, por ejemplo, muchas veces por segundo, la medición frecuente puede permitir un mejor conocimiento de la proximidad y / o velocidad de aproximación de un UE y, de este modo, acelerar el tiempo de detección.

En algunas realizaciones, tras una indicación de que la medición de potencia pasa un umbral crítico, se realiza otra acción o transacción.

Breve descripción de los dibujos

Se describirán además realizaciones preferidas de la presente invención ahora, con referencia a los dibujos adjuntos en los que:

- la figura 1 ilustra esquemáticamente los componentes principales de un sistema de telecomunicaciones inalámbricas de acuerdo con una realización;
- la figura 2 ilustra esquemáticamente una interacción entre una macrocelda y un detector de acuerdo con una realización;
- la figura 3 ilustra esquemáticamente una interacción entre una macrocelda y un detector de acuerdo con una realización adicional;
- la figura 4 ilustra esquemáticamente un método de acuerdo con una realización que emplea detección celular con preautenticación basada en femtoceldas; y
- la figura 5 ilustra esquemáticamente un método de acuerdo con una realización que emplea detección celular

con preautenticación basada en sensor.

Descripción detallada de realizaciones

5 la figura 1 ilustra esquemáticamente los componentes principales de un sistema de telecomunicaciones inalámbricas
 10 de acuerdo con una realización. El equipo del usuario 50 recorre el sistema de telecomunicaciones inalámbricas.
 Se proporcionan estaciones base 20 que soportan áreas de cobertura de radio 30. Algunas de estas estaciones
 base 20 se proporcionan distribuidas geográficamente para proporcionar una amplia área de cobertura al equipo de
 usuario 50. Cuando el equipo del usuario está dentro de un área servida por una estación base 30, se pueden
 15 establecer comunicaciones entre el equipo del usuario y la estación base a través de enlaces de radio asociados. Un
 detector 100, de acuerdo con realizaciones, se proporciona dentro de un área de cobertura 30 proporcionada por
 una estación base 20. El detector 100 es operable para detectar rápidamente la proximidad del equipo de usuario 50
 usando un sensor celular de corto alcance. El sensor celular irradia señales de conexión descendente de manera
 similar a una estación base 20. Las realizaciones descritas se relacionan con diferentes técnicas para lograr una
 20 identificación rápida, autenticación, después verificación adicional de un equipo de usuario 50 dentro de un área de
 cobertura proporcionada por un detector 100.

Aunque la siguiente realización se describe en relación con un sistema celular de UMTS, se apreciará que las
 técnicas se pueden generalizar a cualquier sistema celular incluyendo, por ejemplo, GSM, CDMA y LTE. En todos
 25 estos sistemas inalámbricos existe normalmente algún mecanismo mediante el cual el equipo del usuario informa a
 la red 10 de los cambios de localización a medida que se desplaza por la red. Dichas actualizaciones de localización
 son importantes tanto en el modo inactivo (en el que el equipo del usuario no tiene una recopilación activa con la red
 10; por ejemplo, una llamada de voz) y modo activo (en el que hay una conexión activa).

25 En modo inactivo, el equipo de usuario 50 informa a la red de su localización para que los mensajes de búsqueda
 entrantes de la red puedan enrutarse a una celda apropiada alojada por una estación base o colección de celdas.

En modo activo, el equipo de usuario y la red 10 trabajan juntos para que el equipo de usuario permanezca
 conectado a una o más estaciones base A, B y C como se muestra en la Figura 1 en todo momento. En modo activo,
 30 el equipo de usuario es operable para evaluar continuamente la intensidad de la señal recibida de cada estación
 base A, B y C en el área y reaccionar según corresponda. Las posibles reacciones incluyen cambiar el conjunto de
 estaciones base con las que un equipo de usuario mantiene un enlace activo y, además, pueden incluir encender o
 ajustar una red 10 o un equipo de usuario 50 de alguna manera, por ejemplo, cambiar estaciones base
 35 suplementarias en un área para mantener una buena conectividad con el equipo de usuario 50.

En el área de localización UMTS es un concepto utilizado para denotar un grupo de estaciones base o celdas que
 juntas forman una localización particular. El grupo de celdas que forman un área de localización particular son
 normalmente celdas vecinas. Por ejemplo, como se muestra en la Figura 1, a las estaciones base A, A B y C se les
 puede asignar la misma área de localización. Se apreciará que la red de telecomunicaciones móviles 10 comprende
 40 otras estaciones base que no se muestran en la figura 1. A las estaciones base ubicadas fuera del área de
 localización 1 normalmente se les asignará un código de área de localización diferente.

Se apreciará que en UMTS, el término "área de localización" se refiere a agrupaciones de celdas para equipos de
 usuario que operan en modo de conmutación de circuitos. Otra agrupación, denominada "área de enrutamiento"
 45 también puede existir para equipos de usuario en UMTS, aquellos equipos de usuario que operan en modo de
 conmutación de paquetes. En lo sucesivo, la expresión "área de localización" se usa para indicar tanto la agrupación
 de conmutación de circuitos como la agrupación de celdas de conmutación de paquetes. Es decir, la expresión "área
 de localización" se utiliza en su sentido más general y funcional.

50 El equipo de usuario 50 puede moverse dentro de un área de localización sin que se le solicite que proporcione una
 identidad o identificador. Cuando el equipo del usuario se desvía fuera del área de localización 1 (en este caso
 representado por las estaciones base A, B y C), la red 10 requiere saber hacia dónde se ha desplazado el equipo de
 usuario 50 y si el equipo de usuario 50 detecta que está fuera del área de localización 1, proporciona su
 55 identificación a la red 10 de acuerdo con los estándares de red existentes. Dichas actualizaciones de localización
 permiten además mensajes de búsqueda entrantes desde la red 10 a una estación base apropiada (en la
 localización de área 1, la agrupación apropiada de celdas sería A, B, C), para que el mensaje de búsqueda llegue al
 equipo de usuario deseado 50.

60 Para proporcionar de manera fiable servicios interactivos entre el equipo del usuario y un objeto del mundo real, se
 requiere que las interacciones locales entre el equipo del usuario y los objetos del mundo real solo sean activadas
 por el equipo del usuario que desea descargar o tener acceso al contenido del mundo real.

Además, la interacción entre un objeto del mundo real y el equipo de usuario 50 puede requerir la presencia de un
 65 detector 100 de acuerdo con las realizaciones para permitir que se extraiga un identificador de equipo de usuario
 único del equipo de usuario en un área de cobertura proporcionada por el detector 100. Un detector 100 debe
 funcionar de tal manera que permita que la infraestructura de red celular existente suministrada por las estaciones

base A, B y C se complemente sin interrupciones significativas. El detector debe permitir la coexistencia de interacciones con dispositivos del mundo real con redes macrocelulares existentes mientras reutiliza los mismos recursos de frecuencia y minimiza la perturbación de esas redes. La rápida extracción del identificador del equipo del usuario por el detector 100 permite que se ofrezcan nuevos servicios basados en las interacciones locales entre el equipo del usuario y los objetos del mundo real sin causar interrupciones significativas.

Para extraer un identificador de equipo de usuario, el detector 100 debe ser operable para comunicarse con el equipo del usuario dentro de un área de cobertura provista por un detector 100. En consecuencia, las realizaciones de un detector tienen la capacidad de determinar el entorno de radio en el que se implementa. Es decir, el detector 100 es operable para escuchar señales de conexión descendente y conexión ascendente dentro de la red 10 en todos los operadores de interés potencial. Dicha operación permite que el detector 100 descubra los niveles de potencia de transmisión de las celdas vecinas y lea la información de transmisión en esas celdas vecinas. En la realización mostrada en la figura 1, el detector 100 podrá escuchar señales de conexión descendente en operadores de interés transmitidos por la estación base A. Además, dado que la estación base A transmitirá una indicación de su lista de vecinos (aquellas estaciones base ubicadas en un área geográfica similar), el detector 100 será alertado de la posible existencia de estaciones base B y C.

De acuerdo con otras realizaciones, el comportamiento de "escucha" u "olfateo" del detector 100 puede ser tal que el detector 100 pueda utilizarse de modo que pueda adaptar sus propias señales de transmisión y conexión descendente según corresponda y sincronizar el tiempo de sus transmisiones con las de una celda en servicio o vecina. Por ejemplo, en una red de comunicaciones inalámbricas UMTS, el detector 100 puede sincronizar la sincronización de sus transmisiones (número de trama del sistema) con las de una celda en servicio o vecina.

Para que el detector 100 pueda comunicarse con el equipo de usuario 50, el detector 100 es operable para determinar el entorno de radio en el que existe. En particular, para comunicarse con el equipo de usuario 50, el detector tiene la capacidad de establecer su señal o señales de radio de conexión descendente para que coincidan con una o más celdas en el área donde existe el equipo de usuario 50 y, más importante aún, la conexión descendente del detector se establece de tal manera que el equipo de usuario 50 pueda monitorizar esos canales de conexión descendente o similar, o camping sobre esos canales de conexión descendente o similar en la macrored.

La expresión "señal de conexión descendente" se refiere a una entidad lógica que proporciona servicio a un equipo de usuario 50 y puede, por ejemplo, incluir señales de femto, pico u otras estaciones base que brindan un servicio de red completo en la red de comunicación inalámbrica 10. Si son posibles múltiples señales de conexión descendente en una localización, por ejemplo, en la superposición entre áreas de cobertura proporcionadas por estaciones base adyacentes, un detector 100 emplea múltiples operadores para asegurar que todos los equipos de usuario que pasan, no importa en qué celda estén atendidos, todavía se pueden detectar. Se apreciará que en áreas en las que dos o más proveedores de servicios brindan cobertura en diferentes frecuencias, para que el detector funcione en todas las frecuencias, puede ser necesario permitir que el detector 100 funcione o se haga pasar por esas mismas frecuencias múltiples en su conexión descendente.

El resultado de la suplantación del detector de las características de la conexión descendente de la mayor red de telecomunicaciones circundante es que las celdas soportadas por el detector, aunque sean celdas de alcance muy corto, se convierten automáticamente en candidatos adecuados para un procedimiento de selección o reelección de celdas ya conocido por el equipo de usuario 50 dentro de la red inalámbrica mayor 10.

El uso de un procedimiento de reelección de celda conocido permite una detección rápida independiente de la configuración de parámetros de una estación base o macrocelda en servicio. Por supuesto, puede haber alguna dependencia con respecto a los parámetros establecidos en el equipo de usuario 50, en términos de implementación de reelección celular.

La suplantación de celdas existentes que el equipo de usuario 50 espera ver permite una ruta conveniente para una comunicación sensible con el equipo de usuario 50 sobre un área de cobertura pequeña proporcionada por el detector 100. El detector 100 normalmente no proporcionará por sí mismo la funcionalidad completa de la red de radio. Es decir, el equipo del usuario no puede hacer ni recibir llamadas a través de la conexión al detector 100. No obstante, los procedimientos que existen dentro de la red de comunicación inalámbrica y los protocolos típicos de comunicación inalámbrica se pueden utilizar para que el detector 60 pueda extraer del equipo de usuario 50 el identificador único requerido para proporcionar una interacción fiable con un objeto del mundo real.

Existen varios mecanismos en una red de comunicación inalámbrica para extraer o intercambiar identificadores únicos del equipo de usuario 50. Uno de esos mecanismos es un procedimiento de actualización del área de localización, durante el cual el equipo del usuario pasa un identificador único, generalmente su IMSI, a la red. También existen otros mecanismos para extraer identificadores únicos del equipo de usuario 50; por ejemplo, los mensajes de búsqueda pueden usarse para obtener una respuesta del equipo del usuario antes de que el sistema instruya o consulte el equipo del usuario, lo que da como resultado la liberación de un identificador único. Con el fin de activar estos mecanismos, es esencial que el detector 100 sea operable para comunicarse con éxito con el equipo del usuario 50. Es decir, el detector 100 debe ser capaz de comunicarse de un modo que el equipo de

usuario 50 espere o es probable que los intentos de extraer cualquier información del equipo de usuario no tengan éxito.

5 En algunos sistemas de comunicación inalámbrica conocidos, cada equipo de usuario conoce su entorno de radio circundante. Es decir, cuando se establece comunicación con una estación base, esa estación base transmite información al equipo de usuario 50 con respecto a otras estaciones base que se pueden encontrar en el área geográfica. Esa lista de estaciones base circundantes se conoce como lista de vecinos. Se apreciará que una lista de vecinos y el mantenimiento de una lista de vecinos en el equipo del usuario, permite determinar la localización del equipo móvil de usuario 50 dentro de la red de telecomunicaciones 10 con un mínimo de señalización innecesaria de la red, dado que el equipo de usuario 50 es informado de las estaciones base con las que puede establecer una conexión de comunicación. La estación base con la que el equipo de usuario 50 se comunica principalmente y con la que se mantendría un estado activo si fuera necesario se denomina estación base en servicio y aloja una celda en servicio. La operación del equipo de usuario 50 dentro de una red normalmente se controlará mediante mensajes recibidos de la red y enviados por la celda en servicio. Es la celda en servicio la que determina, por ejemplo, un parámetro (conocido como reselección T) que determina cuánto tiempo debe esperar el equipo de usuario 50 y antes de realizar un proceso de reselección celular, en el caso de que una celda en servicio ya no represente la "mejor" opción para la comunicación entre el equipo de usuario 50 y la red en su conjunto.

20 En realizaciones del detector, es posible anular la configuración en el equipo de usuario establecido por una celda en servicio que podría evitar el descubrimiento rápido del detector. Es posible hacer esto suplantando efectivamente la celda en servicio para que el equipo de usuario 50 crea que todavía está escuchando a la celda en servicio cuando, de hecho, está escuchando transmisiones del detector 100. Como el detector puede controlarse con mucha precisión, el detector puede establecer varios parámetros normalmente establecidos por la celda en servicio. En un sistema celular UMTS, se puede lograr tal suplantación y establecer la conexión proporcionando al detector 100 la capacidad de tener una mayor potencia de recepción en el equipo de usuario 50 cuando está cerca del detector 100. El detector 100 puede usar el mismo código de área de localización y puede coincidir con precisión con la sincronización del marco y la sincronización de la celda en servicio proporcionada por la capa macro. Como resultado de simplemente ver el detector 100 con más fuerza, el resultado es que el equipo de usuario 50 escucha las transmisiones del detector 100. Una vez que el equipo del usuario está escuchando los canales de conexión descendente del detector 100, es posible controlarlo.

35 En una realización del sistema UMTS, el detector puede funcionar de manera tal que el contenido de su canal de transmisión incluya valores que establezcan parámetros en el equipo del usuario para adecuarse a los propósitos del detector y el detector indica al equipo del usuario que los vuelva a leer si es necesario. Al releer los canales de transmisión, el equipo del usuario cerca del detector puede, por ejemplo, descubrir que un código de área de localización ha cambiado, por lo tanto, se necesita una actualización del código de área de localización que extraiga un identificador de equipo de usuario del equipo de usuario 50 en el detector.

40 En realizaciones alternativas, si el equipo del usuario no reacciona rápidamente a un código de área de localización modificado, por ejemplo, detectándolo por sí mismo, el detector puede operar para localizar el equipo del usuario con un cambio en los parámetros de reselección celular, desencadenando así un procedimiento de evaluación de reselección celular.

45 En algunas realizaciones, el detector puede ser operable para llenar la lista de vecinos del equipo del usuario con otra celda bajo la creación y control del detector 100, luego forzar la reselección en el equipo de usuario de esa nueva celda, incluyendo la realización de una actualización del área de localización. En tales realizaciones, los niveles de potencia relativos y todos los parámetros relacionados se configuran para hacer que la segunda celda sea atractiva para el equipo del usuario de modo que tome una decisión rápida y, como resultado, realice una actualización del área de localización rápidamente, permitiendo así que el detector 100 extraiga un identificador único del equipo de usuario 50 en un período de tiempo corto.

La figura 2 es una ilustración esquemática de una posible interacción entre una macrocelda y un detector.

55 En la realización mostrada en la figura 2, la estación base 20 soporta una celda en una región de cobertura 30. Dentro de esa región de cobertura 30 se proporciona un detector 100 que a su vez proporciona una región de cobertura 110. La estación base 20 soporta una macrocelda 1 en la región geográfica 30, que tiene un código de codificación de 1 y un código de área local de 1. El detector 100 soporta dos celdas pequeñas en la región 110, siendo esas celdas pequeñas conocidas como celda pequeña 2 con un código de codificación de 1 y un código de área local de 1, y celda pequeña 3 con un código de codificación de 2 y un código de área local de 2.

60 El detector 100 puede suplantar la celda en servicio, en este caso la macrocelda 1, soportada por la estación base 20, extremadamente cerca. Lo hace olfateando y determinando las características de radio de la macrocelda 1 y, a continuación, rellenando sus propios canales de conexión descendente con exactamente la misma información que la contenida dentro de la celda en servicio. En esta realización, la celda pequeña 2 tiene una frecuencia idéntica, tiempo y otra información como la contenida en la macro celda 1. En esta realización, los tiempos (números de trama del sistema) también se sincronizan con la celda en servicio. La información solo se modifica en las realizaciones

según sea necesario para lograr una actualización del área de localización.

La celda que sirve al equipo de usuario en modo inactivo es soportada por la estación base 20 y es parte de la red macrocelular 10 existente. La configuración de sus parámetros es difícil y costosa de cambiar. Por lo tanto, es ventajoso que un detector pueda lidiar con los parámetros establecidos en los peores valores de caso con respecto a lo que el detector desea lograr. Como se ha analizado previamente, la reselección de tiempo de acuerdo con un sistema celular UMTS se transmite normalmente en mensajes de información del sistema transmitidos en un canal de la celda en servicio. Esa instrucción informa al equipo del usuario cuántos segundos debe esperar antes de seleccionar otra celda sobre la que actuar. La reselección de tiempo puede establecerse en un valor de caso peor por una estación base de 31 segundos que, dado que un detector ubicado en un objeto del mundo real tiene como objetivo extraer la identidad del equipo del usuario lo más rápido posible, causa algunos problemas y, por lo general, será deseable asegurarse de que el equipo del usuario revela su identificador en muchos menos segundos, normalmente una muralla de 5.

Como se muestra en la figura 2, el equipo de usuario 50 está dentro de la región geográfica 30 y acciona normalmente sobre la red de macroceldas proporcionada por la estación base 20. Esa macrocelda 1 tiene un código de codificación de 1, un código de área local de 1 y es compatible con la estación base 20. Actúa como la celda en servicio para el equipo del usuario 50. A medida que el equipo de usuario 50 se mueve hacia el área geográfica 110, que puede estar solo unos pocos centímetros alrededor del detector 100, entra en una región cubierta por la celda pequeña 2 y la celda pequeña 3 soportada por el detector 100. El detector suplanta a la celda en servicio, macrocelda 1, irradiando en la misma frecuencia operadora la sincronización de ranura y trama idéntica a la de la macrocelda. Debido a la proximidad del equipo de usuario 50 a la celda pequeña 2 soportada por el detector 100, la trayectoria perdida en la macrocelda 1 es muy grande. La potencia radiada por el detector 100 en relación con la celda 2 es menor que la celda 1, para minimizar la interrupción causada por el detector 100 al funcionamiento de la red inalámbrica de telecomunicaciones en general. Sin embargo, debido a la proximidad del equipo del usuario al detector 100, la potencia recibida del detector 100 con respecto a la celda 2 es mucho mayor que la recibida en el equipo del usuario desde la estación base 20 con respecto a la macrocelda 1.

En una realización, el detector 100 es operable para soportar dos celdas pequeñas. Cuando el equipo de usuario 50 se introduce en el área de cobertura del detector 100, el equipo de usuario escucha el canal de conexión descendente transmitido en la celda pequeña 2 que está bajo el control del detector. El detector transmite un mensaje de lectura del canal de transmisión a todos los equipos de usuario que existen en la celda pequeña 2. El mensaje de lectura del canal de transmisión se implementa enviando un mensaje de búsqueda tipo 1 que indica a todos los equipos de usuario que verifiquen los cambios en el canal de transmisión. El equipo del usuario dentro de la celda pequeña 2, que normalmente solo será 1 equipo de usuario, dado que el área de cobertura soportada por el detector 100 es muy pequeña, lee todos los bloques de información del sistema de cambios en el canal de transmisión y actualiza su almacén local de parámetros.

En esta realización, el detector es operable para garantizar que, como parte de esa información actualizada del canal de transmisión, hay una actualización de la lista de vecinos del equipo de usuario 50. El detector, dado que emula la celda en servicio, rellena la lista de vecinos del equipo del usuario para incluir la celda pequeña 3, también soportada por el detector 100. Los parámetros de reselección de celda también pueden cambiarse para hacer que la celda 3 sea una opción muy atractiva. Los parámetros a cambiar pueden incluir, por ejemplo, sintra, el factor de histéresis u otros parámetros análogos. El detector 100 es operable para garantizar que la celda 3 se irradie a una potencia mayor que la celda pequeña 2, por lo que es una opción atractiva para la reselección. Cambiar los parámetros de reselección celular usando la celda pequeña 2 activa otro procedimiento de reselección celular. El equipo de usuario 50 es, por tanto, operable para seleccionar la celda 3. Como resultado del código de área de localización diferente asignado a la celda pequeña 3 (área de localización 2, a diferencia del área de localización 1 soportada por la macrocelda 1 y la celda pequeña 2), el equipo del usuario intenta realizar una actualización del área de localización.

El detector 100 utiliza el mecanismo de actualización del área de localización y el establecimiento de comunicación iniciado por ese mecanismo para solicitar al equipo de usuario 50 un identificador único, normalmente un IMSI o TIMSI. Aunque el detector 100 en sí mismo no puede ofrecer un servicio de red completo al equipo de usuario 50, es operable para comunicarse con la red 10 a través de alguna forma de retroceso, ya sea inalámbrico o una red IP o por cable, de modo que pueda obtener más información sobre el equipo de usuario 50 de la red inalámbrica 10 una vez que se haya obtenido un identificador único. En particular, el detector 100 utiliza mecanismos de autenticación estándar y protocolos de autenticación para verificar la identidad del equipo del usuario. Dichos mecanismos de autenticación generalmente implican recuperar información de clave criptográfica y secretos compartidos de una red central (a través de, por ejemplo, un servidor AAA). El uso de mecanismos de autenticación de identidad permite que el detector 100 confirme la identidad del equipo del usuario con el mismo nivel de seguridad que el utilizado para la facturación celular. Una vez que se ha realizado la identificación del equipo del usuario, el detector 100 es operable para rechazar la solicitud de actualización del área de localización del equipo de usuario 50 con un mensaje apropiado; por ejemplo, que la celda está muy ocupada.

Asegurarse de que la solicitud de actualización del área de localización no tiene éxito sirve para minimizar el tráfico

innecesario de datos dentro de la red 10 y asegura que el servicio ofrecido al equipo de usuario 50 se interrumpa mínimamente mientras el equipo de usuario 50 interactúa con el detector 100.

5 Como el equipo de usuario 50 no ha realizado una actualización con éxito del área de localización, el equipo del usuario vuelve al recuento en modo inactivo normalmente en la macro celda 1. Si la potencia recibida de las celdas del detector (celda pequeña 2 y celda pequeña 3) es alta en relación con la potencia recibida de la macrocelda 1, el equipo de usuario 50 solo puede volver a monitorizar los operadores de macroceldas en el estado de camping en modo inactivo cuando se retira de estar cerca del sensor; es decir, cuando se retira del área de cobertura 110.

10 En algunas realizaciones, cuando el detector 100 envía el mensaje de rechazo de actualización del área de localización, el detector también es operable para apagar el par de celdas del detector (celda pequeña 2 y celda pequeña 3) al menos hasta que el equipo de usuario 50 se retira del sensor. Dichas realizaciones pueden permitir que el equipo de usuario 50 regrese inmediatamente para alojarse normalmente en la macrocelda 1.

15 Como alternativa, en el caso de que no se haya recibido con éxito ninguna actualización del área de localización, el equipo de usuario puede simplemente abandonar el área de cobertura de la celda del detector y volver a estar habitualmente acampado en la macrocelda 1.

20 Una realización alternativa a la que se muestra en la Figura 2 es usar solo una celda en un detector. De acuerdo con tal realización, la celda pequeña 2 se puede proporcionar con un código de área de localización diferente al de la macrocelda 1. Al emitir el mensaje de relectura del canal de transmisión emitiendo un mensaje de tipo de búsqueda, el equipo de usuario 50 puede, de acuerdo con las implementaciones de los fabricantes de equipos de usuario, realizar una actualización del área de localización si detecta un cambio en el código de área de localización. Si el equipo de usuario 50 es operable para hacerlo, el detector vuelve a establecer el identificador único del equipo del usuario (por ejemplo, IMSI o TIMSI) y puede autenticarlo utilizando el almacén criptográfico de la red central como se ha descrito anteriormente. De nuevo, el detector 100 es operable para enviar un mensaje de rechazo en relación con la solicitud del equipo del usuario para una actualización del área de localización y el equipo del usuario vuelve a estar normalmente alojado en la macrocelda 1.

30 En esta realización, de forma idéntica al método anterior, el objetivo de que el equipo del usuario vuelva a estar habitualmente alojado en la macrocelda 1 también se puede lograr apagando las celdas de control del detector o dejando que el equipo del usuario abandone el área de cobertura 110 del detector 100.

35 De acuerdo con una realización adicional, puede ser que el equipo de usuario 50 sea operable para detectar automáticamente la presencia de la celda 2 y, de manera más particular, habiendo cambiado el código del área de localización de la celda 2. En tales implementaciones del equipo de usuario, el equipo del usuario se sincroniza automáticamente con la potencia dominante en el código de codificación 1 proporcionado por el detector 1 con respecto a la celda pequeña 2. A continuación, el equipo de usuario lee automáticamente el canal de transmisión de la celda pequeña 2 y, al descubrir que el código de área local ha cambiado, realiza una actualización del área de localización. En dicha implementación, no es necesario que la sincronización de trama de la celda pequeña 2 coincida con la celda en servicio. Además, se puede ver que el detector no necesita ser operable para emitir un mensaje de búsqueda de modificación del canal de difusión para activar un mecanismo de actualización del código de área de localización en el equipo de usuario 50.

45 SUPLANTACIÓN DE CELDAS VECINAS

50 En realizaciones alternativas, el detector puede emular a un vecino en lugar de la celda en servicio. Como parte del procedimiento mediante el cual se detecta el código de codificación de la celda en servicio, se apreciará que también se puede leer una lista de vecinos transmitida por la celda en servicio. A continuación, el detector puede funcionar para seleccionar un código de codificación para emular una estación base en la lista de vecinos.

55 En una realización alternativa adicional, es posible seleccionar un código de codificación que no esté en uso por las celdas vecinas o las celdas en servicio, aunque esto puede llevar a algunos problemas de implementación. En cualquier caso, de acuerdo con estas realizaciones adicionales, el área de localización de la celda pequeña del detector está configurada para diferir de la del código de área de localización de la celda en servicio. De acuerdo con estas realizaciones, cuando el equipo del usuario se acerca a la celda pequeña soportada por el detector, el equipo del usuario realiza un procedimiento de reelección de celda a la celda soportada por el detector y, en consecuencia, solicita una actualización del área de localización.

60 Una técnica alternativa a la de la suplantación de una celda en servicio es presentar una celda detectora de manera que emule a una celda en servicio vecina. La figura 3 ilustra esquemáticamente la interacción entre una macrocelda y un detector, de acuerdo con una realización adicional. Se han utilizado números idénticos en toda la Figura 3, según corresponda. En el escenario ilustrado en la Figura 3, la macro celda 1, soportada por la estación base 20 que actúa como celda en servicio, tiene un código de codificación de 1 y un código de área de localización de 1. El equipo de usuario 50 en modo inactivo trata esta celda como su celda en servicio.

El detector 100 soporta una celda, la celda pequeña 2, en una región geográfica 110 que se rodea. En este caso, el detector es operable para soportar la celda pequeña 2 que tiene un código de codificación y un código de área de localización que han sido seleccionados para ser diferentes a los de la celda en servicio, pero para que coincida con los de una celda vecina; es decir, una celda en la lista de vecinos de la celda de servicio. Cuando un equipo de usuario inactivo 50 se mueve hacia un detector, como lo muestra la flecha, dentro de la macrocelda 1 y se encuentra dentro de la región 110, dentro de la cual el detector soporta la celda 2 del sensor, el equipo de usuario es operable para detectar la señal más fuerte relacionada con la celda 2 e invoca el mecanismo de actualización del área de localización ya que la celda 2 tiene un código de área de localización diferente.

Habiendo invocado un procedimiento de actualización del área de localización, el detector puede extraer un identificador único, por ejemplo un IMSI o TIMSI, desde el equipo del usuario 50. Como se ha descrito anteriormente, la solicitud de actualización del área de localización del equipo de usuario 50 es rechazada por el detector 100 después de la identificación formal y la autenticación mediante el uso de la comunicación entre el detector y la red 10. Además, como se ha descrito previamente, la solicitud de actualización del área de localización puede ser rechazada y el equipo de usuario 50 vuelve a estar alojado normalmente de nuevo en el servicio de la macrocelda 1.

En ciertas ocasiones, el equipo de usuario 50 puede tomar un tiempo significativo para detectar y volver a seleccionar la celda pequeña 2 soportada por el detector 100. Esto normalmente se debe a las diferencias de implementación del equipo del usuario y puede deberse al hecho de que el código de codificación del detector no está en la lista de vecinos de la celda 1 de servicio o debido a la configuración de los parámetros que rigen la reelección determinada por los mensajes de información del canal de transmisión enviados por la celda de servicio al usuario equipo 50. En tales casos, la señal de conexión descendente es transmitida por el detector, lo que garantiza que tenga una fuerza mayor que cualquier otra celda cercana. Un intento de establecer una conexión, por ejemplo haciendo una llamada o enviando un mensaje de texto, desencadenaría una reelección rápida y superaría la implementación y los parámetros establecidos por la celda en servicio.

En algunas realizaciones, la "llamada" podría ser a un número de varios dígitos que representa un PIN que puede enviarse al detector para su verificación. Como alternativa, el número podría indicar una selección para una aplicación de nivel superior. Es decir, en una aplicación de pago de proximidad, el número "llamado" desde el equipo de usuario 50 puede representar la cuenta de la cual se deducirá la transacción; por ejemplo, el monedero electrónico 1 o el monedero electrónico 2 podrían representarse como 0001 y 0002 respectivamente.

INICIACIÓN DE LOS PROCEDIMIENTOS DE ACTUALIZACIÓN DEL ÁREA DE localización

El objetivo central de las realizaciones descritas anteriormente es establecer la comunicación inicial de un equipo de usuario con el detector. En un sistema celular UMTS, se realiza una conexión inicial entre el equipo de usuario y una estación base en un intercambio RACH / FACH con una estación base. Una vez que el equipo de usuario 50 ha establecido una conexión de comunicación con una estación base, se realizan las siguientes etapas en consecuencia:

- 1 Un identificador único, por ejemplo un IMSI o TIMSI, se recupera del equipo del usuario;
- 2 La identidad del equipo de usuario se autentica mediante un procedimiento de autenticación celular estándar;
- 3 El equipo del usuario recibe un mensaje de rechazo. Ese mensaje de rechazo puede, por ejemplo, ser que la carga de la celda es demasiado alta; y
- 4 El equipo del usuario regresa a un modo inactivo y vuelve a estar acampado normalmente en la celda de servicio original.

En las etapas mencionadas anteriormente, el objetivo del procedimiento es utilizar un mecanismo conocido de actualización de localización, aunque no se realiza ninguna actualización de localización porque no es posible una actualización de localización a una celda compatible con el detector 100.

Como el equipo del usuario no realiza una actualización exitosa del área de localización, volver al estado de alojamiento normalmente en la celda de servicio original no implica más comunicaciones con la red y, por lo tanto, minimiza el tráfico innecesario de datos de la red.

El regreso al estado de alojamiento normal es asistido por el equipo de usuario 50 que se retira de la vecindad del detector 100. Para un detector de proximidad muy cercano, la remoción de la vecindad puede involucrar movimiento solo del orden de decenas de centímetros. Para un detector de mayor alcance que todavía funciona para atender solo un área de celda pequeña, El equipo del usuario puede necesitar moverse varios metros o decenas de metros. La naturaleza de corto alcance de la celda soportada por el detector 100 ayuda al retorno a la celda en servicio, dado que la potencia recibida en el equipo del usuario desde el sensor cae bruscamente a medida que el equipo del usuario se aleja del detector. Como resultado, los canales de conexión descendente de la celda en servicio original serán nuevamente leídos y alojados.

Para emular efectivamente una celda en servicio o una celda vecina, es deseable minimizar el tiempo que el equipo del usuario necesita para establecer una conexión con la celda detectora y revelar su identidad. En la mayoría de los

sistemas celulares, la información transmitida se transmite en canales de conexión descendente desde las estaciones base y, en particular, los bloques de programación de información del sistema se envían desde las estaciones base al equipo del usuario dentro de la celda. Es importante programar de manera óptima esta información o información similar para que se envíe desde un detector al equipo del usuario ubicado en el área de cobertura del detector para que la cantidad mínima de información se brinde con la mayor frecuencia posible para que el equipo del usuario establezca una conexión con éxito con la celda del detector. La programación de la información del sistema transmitida por la conexión descendente de la celda del detector puede programarse para que se repita con la mayor frecuencia posible, de modo que cualquier equipo de usuario que comience a leer la información transmitida en cualquier momento debe escuchar por un período mínimo de tiempo antes de tener toda la información que necesita para comenzar la comunicación con el detector.

En un sistema celular UMTS, los bloques de información del sistema son programados y transmitidos por una celda. El sensor celular en UMTS programa los bloques de información del sistema mínimamente y con la mayor frecuencia posible, por tanto, solo se transmitirán los bloques estrictos de la información del sistema requeridos para permitir el desencadenamiento del establecimiento de una conexión con una estación base y solo se transmitirán los elementos de información requeridos estrictamente.

EXTRACCIÓN DE UN IDENTIFICADOR ÚNICO MEDIANTE BÚSQUEDA

Para localizar el equipo del usuario, primero es necesario que el equipo del usuario escuche la celda del detector. Dicha emulación se ha descrito en relación con realizaciones anteriores.

El uso de mensajes de búsqueda requiere que el equipo del usuario escuche los canales de búsqueda de una celda bajo el control del detector. El uso de mensajes de búsqueda permite que las realizaciones renuncien a cierta dependencia de la necesidad de que difiera un código de área de localización, o la activación de un mecanismo de actualización de área de localización para extraer una identidad única. Además, el uso de mensajes de búsqueda asegura que no haya necesidad de confiar en que el equipo del usuario lea todos los bloques de información del sistema transmitidos por un canal de difusión del detector. Para usar mensajes de búsqueda, se requiere que un equipo de usuario esté sincronizado con una celda detectora y que escuche y reaccione cuando se dirige a mensajes de búsqueda.

Un mensaje de búsqueda puede evitar la necesidad de que el equipo del usuario lea los bloques de información del sistema y, por lo tanto, el proceso de establecer contacto y extraer un identificador único del equipo del usuario puede ser significativamente más rápido si un detector puede usar un mensaje de búsqueda.

OPCIONES DE BÚSQUEDA

Es posible buscar continuamente cada equipo de usuario en una red localizando continuamente todos los identificadores únicos de equipo de usuario. Esto se imagina fácilmente como un registro de identificadores únicos de equipos de usuario y puede, por ejemplo, ser una lista de identificadores IMSI y TMSI de equipos de usuario. Se apreciará que dicha "lista de asistencia" puede llevar una cantidad de tiempo significativa y, para extraer el identificador único de un equipo de usuario colocado en un detector de la manera más eficiente, puede ser necesario emplear un esquema de búsqueda más eficiente. Se pueden emplear varios esquemas para reducir el número de identificadores que se deben buscar continuamente. En una realización, solo se puede localizar un subconjunto de TMSI dentro de un área de interés de localización particular. El subconjunto puede determinarse por varios medios; por ejemplo, la celda detectora puede consultar una red celular de macroceldas regular para obtener una lista de equipos de usuario en un código de área de localización particular. En otras realizaciones, el número de identificadores de equipo de usuario que deben ser buscados puede reducirse asignando identificadores asignados a la red de una manera que el detector podría, independiente de la comunicación directa con la red central, deducir un subconjunto de identificadores de equipos de usuario a buscar. Por ejemplo, un conjunto de todos los TMSI posibles en un área de localización puede deducirse en función del código de área particular en uso. Es decir, el código de área de localización 10 puede corresponder al número fijado de 10 de identificadores TMSI. En tal disposición, el conjunto podría contener una lista de, por ejemplo, 100 identificadores únicos de equipos de usuario para buscar.

BÚSQUEDA DE GRUPOS DE EQUIPO DE USUARIO

En algunos sistemas celulares es posible incluir un equipo de usuario en un grupo y buscar por un identificador de grupo. El equipo del usuario escucha los mensajes de búsqueda a un identificador de grupo. El equipo de múltiples usuarios puede pertenecer a un identificador de grupo. Por lo tanto, se puede enviar un solo mensaje de búsqueda para activar una respuesta de muchos equipos de usuario. Cada equipo de usuario dentro de la red 10 puede asignarse temporalmente o en todo momento, una identidad grupal. Se pueden emplear varios arreglos para determinar qué subconjunto de grupos de búsqueda debe buscar un detector de forma continua o no continua. En algunas realizaciones, por ejemplo, se puede dividir un conjunto de identidades de grupo, dependiendo del área de localización.

En algunas realizaciones, es posible determinar un conjunto de identidades de equipo de usuario en un área desplegando una celda, una estación base o grupo de estaciones base que descubren todo el equipo del usuario en una vecindad particular. Esa determinación puede ser una etapa de preparación y puede realizarse con limitaciones de tiempo menos exigentes que las requeridas por el detector. Por ejemplo, una celda puede proporcionar un

5 servicio completo y, por lo tanto, transmitir a través de un área grande y descubrir todos los equipos de usuario que entran a esa área. Todas esas identidades de equipo de usuario pueden guardarse centralmente o enviarse a detectores en el área para propósitos de búsqueda. Una identidad de equipo de usuario puede ser cualquier

10 Un ejemplo de dicho método para determinar un conjunto de identificadores de equipos de usuario sería para su uso en un sistema de torniquete de transporte público. En dicho sistema, es importante que el tiempo de reacción al equipo del usuario presente sea lo más rápido posible en el torniquete. Cualquier retraso puede interrumpir el flujo de personas a través del torniquete. Por lo tanto, para garantizar la detección más rápida posible de un teléfono, puede ser necesario buscar continuamente el conjunto de teléfonos que se detectan en las proximidades. Cuando un equipo de usuario reacciona a un mensaje de búsqueda, se puede realizar la autenticación completa. Es decir, es posible proporcionar estaciones base en el área del torniquete que detectan la presencia de equipos de usuario cuando entra en el área por primera vez, esa lista de equipos de usuario en el área se mantiene localmente y luego se pone a disposición de los detectores ubicados en los propios torniquetes. Además, el detector "descubrimiento" separado puede proporcionarse por separado a un detector identificador del UE individual. Dicho detector de descubrimiento puede tener un área de cobertura mayor y soportar una celda más grande que el detector identificador del UE individual. El detector de UE individual puede soportar una celda más pequeña a una potencia menor, aunque operable para comunicar con la celda de descubrimiento, con el fin de acceder a la información descubierta por la celda de descubrimiento.

25 TÉCNICAS DE VECINOS UNIVERSALES

Es posible iniciar una PLMN equivalente o la misma PLMN o se puede usar una PLMN par permitida como PLMN doméstica del equipo de usuario. El equipo de usuario puede ser operable para realizar una reelección rápida a dicha celda de la PLMN. Un solo cambio en todas las celdas en todas las PLMN para incluir una celda adicional como vecina puede permitir que un detector y una red funcionen y descubran el equipo del usuario rápidamente. Los mismos detalles se pueden usar para todas y cada una de las celdas; por ejemplo, mediante el uso de una configuración de celda reservada y, en particular, un código de codificación reservado y un código de área de localización para representar una PLMN equivalente o la misma para todos los equipos de usuario.

30 Además de presentar un vecino universal que se encuentra en una nueva PLMN, un vecino podría ser universal dentro de una PLMN existente. Para cada PLMN en el área para la cual el dispositivo es para detectar los UE, el dispositivo suplanta a la PLMN con canales de conexión descendente a los que responderá el equipo del usuario. Si la PLMN indica a todo el equipo del usuario que busque una o más frecuencias (por ejemplo, relleno de las listas de vecinos en consecuencia) y todas las PLMN seleccionan la misma o más frecuencias, el detector solo necesita irradiar en este subconjunto de todas las frecuencias posibles. Esto reduce la complejidad del detector.

40 INYECCIÓN DE INTERFERENCIA EN UNA CELDA EN SERVICIO

45 La reelección celular puede ocurrir en un equipo de usuario por varias razones. Una razón para realizar la reelección celular sería que la intensidad de la señal en la celda en servicio se debilita. Por lo tanto, es posible en las realizaciones inducir artificialmente una señal de celda de servicio que se determine como débil en el equipo del usuario inyectando potencialmente una señal de interferencia en una región cubierta por el detector 100, tal que cualquier equipo de usuario dentro de esa región realice una reelección celular.

50 En un sistema celular UMTS, se puede inyectar interferencia durante el tiempo que se predice que el equipo del usuario realizará mediciones de LA intensidad de señal. Tal disposición tiene el propósito de ser solo intermitente, con el resultado de que minimiza la interferencia causada por el equipo de usuario en el área del detector en llamadas activas y para un equipo de usuario inactivo, el equipo de usuario solo recibe o controla durante el tiempo en que la interferencia se inyecta en el área atendida por el detector. En un sistema celular UMTS, El período de recepción discontinua y la temporización generalmente se determinan a partir del canal de transmisión de la celda EN servicio, de modo que la interferencia puede ser transmitida por un detector e inyectada solo en el momento en que el equipo del usuario realiza la medición.

60 Con respecto al equipo de usuario activo, la interferencia inyectada por un detector puede reducir ligeramente la calidad general del enlace de comunicación entre el equipo de usuario y la estación base en servicio, pero el tiempo extra total de potencia de interferencia es particularmente pequeño ya que solo ocurre por una pequeña fracción del tiempo.

65 Las realizaciones pueden permitir una gran cantidad de nuevos servicios móviles basados en la interacción del equipo del usuario (teléfonos móviles) con objetos del mundo real. Un beneficio de tal disposición es que impulsa los sistemas de red celular existentes y ampliamente desplegados de modo que los servicios pueden ser utilizados por

una gran cantidad de suscriptores de equipos de usuario.

De acuerdo con las realizaciones, la interacción con objetos del mundo real puede verse obligada a funcionar con teléfonos existentes sin necesidad de software especializado en el teléfono. Las realizaciones tienen como objetivo establecer conexiones rápidas con el equipo del usuario y, por lo tanto, una detección rápida por parte del sensor.

ACTIVADOR RÁPIDO CON PRE-AUTENTICACIÓN

El tiempo de activación efectivo experimentado por un usuario final puede reducirse mediante la introducción de una detección de dos etapas, Método de autenticación y validación.

Se apreciará que es posible adquirir una indicación de identidad del equipo del usuario que opera cerca de un sensor antes de que el equipo del usuario se coloque contra un objeto del mundo real y se le pida que "interactúe" con ese objeto del mundo real. Es decir, antes de colocar el equipo del usuario en el sensor. También es posible autenticar previamente el equipo del usuario que opera cerca de un sensor.

La búsqueda posterior del equipo del usuario puede usarse como una forma rápida de identificar el equipo del usuario en el momento más crítico de procesar una transacción.

Existe un problema, sin embargo, de acuerdo con dicho sistema, la identidad de un UE no se confirma como auténtica en el momento de una búsqueda posterior. Puede haber sido autenticado previamente, pero en el momento en que IMSI busca una transacción, La identidad de la UE puede ser falsificada. Los aspectos descritos en el presente documento reconocen que es necesario llevar adelante una relación de autenticación hasta el momento de la ejecución de la transacción.

En algunas realizaciones, una celda grande (por ejemplo, una femtocelda) es operable para identificar y autenticar el equipo del usuario en la vecindad de un sensor cuando el equipo del usuario acampa en la celda o se entrega. Estas ID de usuario capturadas y autenticadas se intercambian con el sensor. El sensor que funciona para proporcionar un área de cobertura de corto alcance transmite un mensaje de búsqueda de baja potencia para cada móvil "capturado" en la celda más grande. La potencia del mensaje de búsqueda se configura de tal manera que un móvil solo responde cuando se encuentra en el rango de detección del objetivo (por ejemplo, dentro de unos pocos centímetros del sensor para el pago móvil). Una vez que un móvil responde a un mensaje de búsqueda, el sensor utiliza la información obtenida por la celda más grande para interrogar al equipo del usuario y verificar su identidad sin la necesidad de realizar un protocolo de autenticación completo. Es decir, no se requiere un contacto completo con la red central, y se realiza una "verificación de seguridad" basada en las credenciales de verificación predeterminadas por un proceso de autenticación completo. Esto acelerará el proceso de activación "efectivo", ya que el proceso inicial de camping y autenticación que lleva la mayor parte del tiempo se realiza por adelantado cuando el móvil entra en una celda más grande.

El mensaje de búsqueda enviado por el sensor da como resultado el establecimiento de una comunicación de control de recursos de radio (RRC) con el UE. Sobre esta conexión, la estación base solicita que la integridad del UE proteja o cifre los mensajes transmitidos basándose en credenciales de verificación predeterminadas. Solo el UE autenticado podría proteger la integridad o cifrar la información transmitida, ya que conoce las credenciales de verificación predeterminadas. Por lo tanto, el sensor puede confiar en la identidad auténtica del UE y, por tanto, atribuir una transacción u otra acción al UE previamente autenticado correcto.

A continuación se describen realizaciones en las que se describen más detalladamente los principios de protección de integridad / cifrado de mensajes para probar la autenticidad.

De acuerdo con algunas realizaciones, se realizan las siguientes etapas:

1. Detección del UE "a distancia" desde el sensor (provisión de una celda de largo alcance);
2. Preautenticación del UE que se determina que está en esa celda de largo alcance;
3. Establecimiento de nuevas credenciales de validación de identidad autenticadas;
4. Búsqueda del UE en la celda de largo alcance continuamente en un canal de búsqueda de baja potencia en un rango más corto para solicitar solo una respuesta a una proximidad muy cercana;
5. En la respuesta del UE, solicitar información / establecer comunicaciones con el UE para probar la relación de autenticación, en función de las nuevas credenciales de verificación establecidas.
6. La transacción continúa si se verifica la relación de autenticación, es decir, las credenciales de verificación (la clave de cifrado / integridad que posee el UE se verifica criptográficamente como buena).

A modo de ejemplo, a continuación se escribe una aplicación de pago móvil en una tienda con múltiples cajas, además de la identificación segura del UE para facilitar la facturación correcta. En dicho ejemplo, se apreciará que es importante minimizar los retrasos en la obtención del identificador móvil en el sensor celular, para garantizar que no se produzca un retraso indebido en las cajas.

La figura 4 ilustra esquemáticamente un método de acuerdo con una realización que emplea detección celular con preautenticación basada en femtoceldas. En esta realización, una femtocelda cubre el área de la tienda, o alrededor de las cajas, como se muestra.

- 5 Cuando un usuario móvil (400) entra en la tienda, el UE (410, 420) se aloja / entrega desde una macrocelda (no mostrada) a la femtocelda (400). La identidad de un UE (410, 420) se autentica durante este proceso por la red central de macroceldas. Para ello, se utilizan procedimientos de movilidad conocidos y estandarizados. Según el teléfono, el proceso puede tardar unos segundos.
- 10 A continuación, la femtocelda (400) transmite la información requerida para localizar y verificar la identidad de cada móvil (identificación, una información de autenticación, claves de cifrado, etc.) a un sensor celular (450, 460) provisto en cada caja (430, 440). Esto permite que cada sensor celular busque continuamente cada UE (410, 420) en el área de cobertura de femtoceldas. La potencia de la señal de búsqueda está configurada de modo que pueda detectarse a solo unos centímetros de cada sensor celular de corto alcance. Para otras aplicaciones, se puede requerir un
- 15 rango de detección mayor, que puede configurarse mediante una potencia de transmisión de la señal de búsqueda aumentada apropiadamente.

La comunicación entre la femtocelda y los sensores celulares (450, 460) se realiza, preferentemente, a través de una conexión de retorno, ya sea directamente o mediante una red de operador móvil (MNO), pero son posibles otros

20 medios como el intercambio de información inalámbrica.

Cuando un usuario final desliza el UE (410, 420) sobre un sensor (450, 460) para facilitar el pago, el UE (410, 420) responde a un mensaje de búsqueda transmitido continuamente por los sensores (450, 460). Después de la respuesta a un mensaje de búsqueda, el sensor establece comunicaciones con el UE y prueba la relación de

25 autenticación. Si se verifica la relación de autenticación (clave de cifrado / integridad mantenida por el UE se verifica criptográficamente como buena), el pago se activa al enviar información sobre la identificación de usuario autenticada y el monto del pago al servicio del monedero móvil del usuario que reside en la red central de un MNO (operador de red móvil). Dado que el dispositivo móvil se ha autenticado previamente y se puede buscar directamente, responde mucho más rápido en el punto de venta, de lo que sería posible de otro modo. Esto reduce

30 significativamente el tiempo de activación efectivo en comparación con las soluciones existentes.

Tal enfoque se puede usar de manera más efectiva cuando un proveedor de la tienda proporciona servicio celular dentro de la tienda.

35 La figura 5 ilustra esquemáticamente un método de acuerdo con una realización que emplea detección celular con preautenticación basada en sensor. En una tal realización, en lugar de usar una femtocelda para la preautenticación, la preautenticación puede realizarse mediante un sensor celular que no proporciona cobertura celular. Este enfoque se puede usar cuando un proveedor de la tienda no está interesado en proporcionar un servicio celular completo utilizando una femtocelda.

40 Como se muestra en la figura 5, cada sensor (500) transmite una primera señal piloto que está configurada para cubrir un área más grande que el área de detección (búsqueda). Esto permite que el UE (550) utilice los procedimientos de "camp on" al entrar en la primera área 510, para que el sensor pueda realizar la autenticación del móvil antes de un evento de detección (búsqueda). Una vez que un UE está en el área 510 y ha sido identificado y

45 autenticado, el sensor puede comenzar a buscar el UE (550) a baja potencia, de modo que el mensaje de búsqueda solo puede detectarse dentro del área de detección prevista 520.

50 Cuando un usuario final pasa un UE (550a, 550b) sobre el sensor (500) para el pago, el UE responderá al mensaje de búsqueda. Después de una respuesta al mensaje de búsqueda, el sensor establece comunicaciones con el UE para probar la relación de autenticación. Si se verifica la relación de autenticación; a saber, la clave de cifrado / integridad que posee el UE se verifica criptográficamente como buena, el pago se activa al transmitir información sobre la identificación de usuario autenticada y el monto del pago al servicio del monedero móvil del usuario que reside en la red central de un MNO (operador de red móvil). Dado que el móvil está previamente autenticado en el momento en que se localiza directamente, puede responder y ser verificado rápidamente. Esto reduce

55 significativamente el tiempo efectivo de activación del sensor en comparación con las soluciones existentes.

La cobertura de las dos áreas soportadas por un único sensor o unidad de interrogación puede optimizarse en algunas realizaciones observando las diferencias de tiempo entre "camping y autenticación" y un "evento de

60 detección" real. Si hay una gran diferencia de tiempo entre los eventos de "camping y autenticación" y los de "detección", esto puede indicar que la cobertura piloto de un sensor es demasiado grande. Esto puede ser subóptimo ya que un UE que se encuentra en el área 510 no puede hacer ni recibir ninguna llamada mientras está en la señal piloto del sensor. En tal caso, la potencia piloto de un sensor puede reducirse en una etapa predeterminada. Si no hay diferencia de tiempo entre eventos, esto puede indicar que la cobertura piloto de un sensor es demasiado pequeña. Esto puede ser subóptimo, ya que puede provocar un retraso en la detección. Si no

65 hay una brecha entre los eventos, "camping y autenticación" no se completa antes del evento de "detección". En tal caso, la señal piloto puede reducirse en una etapa predeterminada. La diferencia de tiempo observada entre los

eventos de "camping y autenticación" y de "detección" puede, de acuerdo con las realizaciones, monitorizarse, y las áreas de cobertura 510, 520 optimizadas según valores predeterminados como un proceso iterativo.

5 En algunas realizaciones, una vez que se establece un enlace de comunicación con el equipo del usuario, por ejemplo, por búsqueda, el método puede comprender solicitar repetidamente un conjunto de informes de medición de potencia del UE. En algunas realizaciones, esos informes de medición pueden usarse para calcular una estimación de la distancia al equipo del usuario desde un sensor. En algunas realizaciones, tras una medición de la potencia que cruza un umbral predeterminado, se realiza una acción. En consecuencia, el contacto puede establecerse con un equipo de usuario preautorizado antes de que esté en contacto directo con un sensor de verificación, y solo una vez que se determine que está en estrecha proximidad, como lo indica un informe de medición que cruza un umbral predeterminado, el sensor de verificación realizará una acción predeterminada, por ejemplo, abriendo una puerta o descargando un horario.

15 Esta es una mejora para, por ejemplo, simplemente buscar el UE y recibir una respuesta y verificar las credenciales predeterminadas antes de activar una acción. La mejora reduce la latencia entre colocar un teléfono contra un sensor de verificación o proximidad y la transacción que se realiza. En algunas realizaciones, el uso de búsqueda para accionar una transacción puede introducir demoras. Por ejemplo, un UE puede requerir tiempo para responder a los mensajes de búsqueda debido a un ciclo de recepción discontinuo (ciclo DRx) utilizado para reducir el consumo de energía. Un ciclo DRx puede durar entre unos cientos de milisegundos y unos pocos segundos.

20 Para mitigar tales demoras y permitir que una acción se lleve a cabo de manera más rápida o inmediata, en algunas realizaciones se puede contactar con el equipo del usuario, por ejemplo, buscar, antes de estar en la localización crítica para configurar una conexión con el sensor. Un dispositivo sensor celular, como una unidad de verificación, solicita después una medición de potencia de recepción del UE para establecer su proximidad a él y / u otros transmisores, por ejemplo, otras unidades de verificación. Los transmisores pueden alojarse en la unidad del sensor y / o combinarse con transmisores alojados en unidades separadas, quizás femtoceldas u otras estaciones base. En algunas realizaciones, las mediciones se pueden solicitar con frecuencia, por ejemplo, muchas veces por segundo, la medición frecuente puede permitir un mejor conocimiento de la proximidad y / o velocidad de aproximación de un UE y, de este modo, acelerar el tiempo de detección.

30 En algunas realizaciones, tras una indicación de que la medición de potencia pasa un umbral crítico, se realiza otra acción o transacción.

35 **Protección de la integridad**

Es necesario proteger la integridad de los mensajes transferidos desde el UE a una estación base de red móvil o al sensor. Las realizaciones usan una relación de autenticación / cifrado preexistente para crear una relación de verificación de autenticación más simple implícitamente para probar una identidad del UE a través de mensajes de control y datos que se intercambian y protegen en un momento posterior. La relación de autenticación se puede establecer como parte de los procedimientos descritos anteriormente, por ejemplo, por una femtocelda de largo alcance o un piloto de alta potencia irradiado por el dispositivo sensor con el fin de identificar el UE en las proximidades. En el primer contacto con elementos de red del sensor, el UE está autenticado, una clave de cifrado y una relación de cifrado se comparten con los dispositivos sensores. Siempre que la relación de cifrado se comparta con cada dispositivo de búsqueda, dichos dispositivos de búsqueda pueden determinar si los UE son los UE previamente autenticados y, por lo tanto, determinar rápidamente si la transacción debe ejecutarse o no, sin la necesidad de realizar un procedimiento de autenticación adicional completo.

50 Por ejemplo, a una solicitud de búsqueda respondida puede seguirle una solicitud de un informe de medición. El informe de medición puede solicitarse desde el UE con protección de integridad. El informe de medición debe estar protegido con respecto a la integridad. Si se confirma la integridad del mensaje utilizando la relación de cifrado establecida con el UE, un sensor de búsqueda puede estar seguro de que el UE que se está comunicando es el UE previsto. Muchos otros mensajes con integridad protegida cifrados transmitidos por el UE pueden solicitarse de este modo.

55 Las realizaciones toman mecanismos de autenticación y posterior protección de integridad / cifrado y los usan para una identificación rápida y segura del UE. Esto permite que se use un UE, por ejemplo, para abrir una puerta, realizar un pago en el punto de venta en un establecimiento minorista o proporcionar detalles sobre la dirección, todo ello haciendo un barrido de un teléfono después de un sensor.

60 En otras palabras, las realizaciones proporcionan un método que puede reducir el tiempo de detección requerido por un sensor celular sin comprometer la seguridad. La preautenticación del UE antes de que entre en el rango de detección ayuda con la velocidad. La protección de la integridad de los mensajes y el cifrado de datos demuestran la autenticidad de los UE preautenticados en el momento crítico de la ejecución de una transacción. Se apreciará que un tiempo corto requerido para detectar / identificar / autenticar un teléfono móvil es crítico para algunas aplicaciones, tal como el pago móvil.

Las realizaciones reducen el tiempo de detección en el momento crítico de la ejecución de la transacción en sensores celulares de varios segundos a menos de un segundo sin comprometer la seguridad.

- 5 Un experto en la técnica reconocería fácilmente que las etapas de diversos procedimientos descritos anteriormente pueden realizarse mediante ordenadores programados. En el presente documento, algunas realizaciones también están destinadas a cubrir dispositivos de almacenamiento de programas, por ejemplo, medios de almacenamiento de datos digitales, que son legibles por máquina u ordenador, y que codifican programas de instrucciones ejecutables de máquina o por ordenador, en el que dichas instrucciones realizan algunas o todas las etapas de dichos procedimientos descritos anteriormente. Los dispositivos de almacenamiento de programas pueden ser, por
- 10 ejemplo, memorias digitales, un medio de almacenamiento magnético tal como discos magnéticos y cintas magnéticas, discos duros, o medios de almacenamiento de datos digitales legibles ópticamente. Las realizaciones también están pensadas para cubrir ordenadores programados para realizar dichas etapas de los procedimientos descritos anteriormente.
- 15 Las funciones de los diversos elementos mostrados en las figuras, incluyendo cualquier bloque funcional etiquetado como "procesadores" o "lógica", se puede proporcionar mediante el uso de hardware dedicado, así como hardware capaz de ejecutar software en asociación con el software apropiado. Cuando se proporcionan por un procesador, las funciones pueden proporcionarse por un único procesador especializado, por un único procesador compartido, o por una pluralidad de procesadores individuales, algunos de los cuales pueden compartirse. Asimismo, el uso explícito
- 20 del término "procesador" o "controlador" o "lógica" no debería interpretarse que hace referencia exclusivamente a hardware que puede ejecutar software, y puede incluir implícitamente, sin limitación, hardware de procesador de señales digitales (DSP), procesador de red, circuito integrado específico de la aplicación (ASIC), campo de matriz de puertas programables (FPGA), memoria de sólo lectura (ROM) para almacenar software, memoria de acceso aleatorio (RAM), y almacenamiento no volátil. Otro hardware, convencional y/o personalizado, también se puede
- 25 incluir. De manera similar, todos los interruptores que se muestran en las figuras son solo conceptuales. Su función puede llevarse a cabo a través de la operación de lógica de programa, a través de lógica especializada, a través de la interacción de control de programa y lógica especializada o incluso manualmente, siendo seleccionable la técnica particular por el implementador como se entienda más específicamente a partir del contexto.
- 30 Se debe apreciar por los expertos en la técnica que cualquier diagrama de bloques en el presente documento representa vistas conceptuales de circuitos ilustrativos que incorpora los principios de la invención. De manera similar, se apreciará que cualquier diagrama de flujo, diagramas de flujo, diagramas de transición de estado, pseudocódigo, y similares representan diversos procesos que pueden representarse sustancialmente en medio legible por ordenador y ejecutarse así por un ordenador o procesador, ya se muestre explícitamente o no tal
- 35 ordenador o procesador.

REIVINDICACIONES

1. Un método de preautenticación realizado por interacción entre una unidad de preautenticación y una unidad de verificación (500), en donde el método establece un conjunto de credenciales de verificación de equipos de usuario de un protocolo de autenticación dentro de una red de comunicaciones inalámbrica, comprendiendo dicho método, en la unidad de preautenticación:
- recibir una indicación representativa de las características de comunicación por radio de conexión descendente de nodos de red reconocibles por el equipo de usuario;
 - emular las características de comunicación por radio de conexión descendente de al menos uno de los nodos de la red para establecer comunicación con el equipo de usuario;
 - activar la liberación de una indicación de identidad por parte del equipo de usuario para esos equipos de usuario (550a, 550b) que se ha determinado que se encuentra en un área de descubrimiento geográfico predeterminada (510);
 - autenticar dicha identidad de equipo de usuario utilizando dicho protocolo de autenticación, y establecer un conjunto compartido de credenciales de verificación de equipo de usuario para la validación futura de dicha identidad de equipo de usuario autenticado;
 - transmitir la indicación de identidad del equipo de usuario y una indicación del conjunto compartido de credenciales de verificación de equipo de usuario, para aquellos equipos de usuario autenticados que se determinen que están en el área de descubrimiento geográfico predeterminada, a la unidad de verificación (500) que interactúa con la unidad de preautenticación de tal manera que el la unidad de verificación opera para verificar la identidad de los equipos de usuario autenticados (550a, 550b), en donde el establecimiento de un conjunto compartido de credenciales de verificación de equipos de usuario para la validación futura de dicha identidad de equipo de usuario autenticado evita un requisito de autenticación adicional de dicha identidad de equipo de usuario usando dicho protocolo de autenticación por dicha unidad de verificación (500).
2. El método según la reivindicación 1, en el que dicha etapa de autenticación comprende: comunicarse con una red central de un proveedor de servicios para autenticar dicha identidad de equipo de usuario utilizando dicho protocolo de autenticación.
3. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que dicho protocolo de autenticación comprende la autenticación de la identidad del equipo del usuario por medio de un secreto criptográfico compartido.
4. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que dicho conjunto compartido de credenciales de equipo de usuario comprende al menos un nuevo secreto compartido.
5. El método de acuerdo con cualquiera de las reivindicaciones 1 a 4, que además comprende, en la unidad de verificación:
- recibir, desde la unidad de preautenticación, la indicación de la identidad del equipo del usuario y la indicación del conjunto compartido de credenciales de verificación del equipo del usuario para aquellos equipos de usuario autenticados que se determinen que están en el área de descubrimiento geográfico predeterminada (510);
 - buscar los equipos de usuario autenticados que se determina que están en dicha área de descubrimiento geográfico predeterminada utilizando dicha indicación de identidad del equipo de usuario;
 - una vez que un equipo de usuario responde a su búsqueda, interrogar dicho equipo de usuario utilizando dicha indicación de un conjunto compartido de credenciales de equipo de usuario;
 - recibir una respuesta de dicho equipo de usuario; y
 - verificar dicha identidad de dicho equipo de usuario autenticado si dicha respuesta recibida coincide con la predicha por dicha indicación de un conjunto compartido de credenciales de verificación de equipo de usuario.
6. Un método de acuerdo con la reivindicación 5, que comprende además: determinar una diferencia de tiempo entre el equipo de usuario autenticado que entra en dicha área de descubrimiento geográfica predeterminada (510) y el equipo de usuario autenticado que responde a dicha búsqueda.
7. Un método de acuerdo con la reivindicación 6, que comprende además calcular una indicación de diferencia de tiempo promedio a través de un conjunto de equipos de usuario autenticado.
8. Un método de acuerdo con la reivindicación 6 o la reivindicación 7, que comprende además: ajustar dicha área de descubrimiento geográfico predeterminada y / o un área de búsqueda predeterminada en respuesta a dicha diferencia de tiempo determinada.
9. Un producto de programa informático, operable cuando se ejecuta en un ordenador, para realizar el método de una cualquiera de las reivindicaciones 1 a 8.

10. Un sistema que comprende una unidad de preautenticación y una unidad de verificación (500), la unidad de preautenticación operable para establecer un conjunto de credenciales de verificación de equipos de usuario a partir de un protocolo de autenticación dentro de una red de comunicaciones inalámbricas, comprendiendo dicha unidad de preautenticación:

- 5
- lógica de recepción operable para recibir una indicación representativa de las características de comunicación de radio de conexión descendente de nodos de red reconocibles por el equipo de usuario;
 - lógica de emulación operable para emular las características de comunicación de radio de conexión descendente de al menos uno de los nodos de la red para establecer comunicación con el equipo de usuario;
 - 10 lógica de activación operable para activar la liberación de una indicación de identidad por parte de dicho equipo de usuario para los equipos de usuario (5501, 550b) determinados en un área de descubrimiento geográfica predeterminada (510);
 - lógica de autenticación operable para autenticar dicha identidad de equipo de usuario utilizando dicho protocolo de autenticación,
 - 15 lógica de verificación operable para establecer un conjunto compartido de credenciales de verificación de equipo de usuario para la validación futura de dicha identidad de equipo de usuario autenticado;
 - lógica de transmisión operable para transmitir la indicación de identidad del equipo de usuario y una indicación del conjunto compartido de credenciales de verificación de equipo de usuario, para aquellos equipos de usuario autenticados que se determina que están en el área de descubrimiento geográfico predeterminada, a la unidad
 - 20 de verificación (500) que, en respuesta a ello, es operable para verificar la identidad de esos equipos de usuario autenticados (550a, 550b),
 - en donde el establecimiento de un conjunto compartido de credenciales de verificación de equipos de usuario para la validación futura de dicha identidad de equipo de usuario autenticado evita un requisito de autenticación adicional de dicha identidad de equipo de usuario usando dicho protocolo de autenticación por dicha unidad de
 - 25 verificación (500).

11. El sistema de la reivindicación 10, en el que dicha unidad de verificación comprende:

- 30
- lógica de recepción operable para recibir, desde la unidad de preautenticación, la indicación de la identidad del equipo de usuario y una indicación de un conjunto compartido de credenciales de verificación de equipo de usuario para aquellos equipos de usuario autenticados que se determine que están en el área de descubrimiento geográfico predeterminada (510);
 - medios para localizar los equipos de usuario autenticados que se determina que están en dicha área de descubrimiento geográfico predeterminada usando dicha indicación de identidad del equipo de usuario; lógica de
 - 35 recepción operable para recibir una respuesta del equipo de usuario localizado;
 - lógica de interrogación operable, una vez que un equipo de usuario responde a su búsqueda, para interrogar a dicho equipo de usuario (550a, 550b) usando dicha indicación de un conjunto compartido de credenciales de equipo de usuario;
 - lógica de recepción operable para recibir una respuesta de dicho equipo de usuario; y
 - 40 lógica de verificación operable para verificar dicha identidad de dicho equipo de usuario autenticado si dicha respuesta recibida coincide con la predicha por dicha indicación de un conjunto compartido de credenciales de verificación de equipo de usuario.

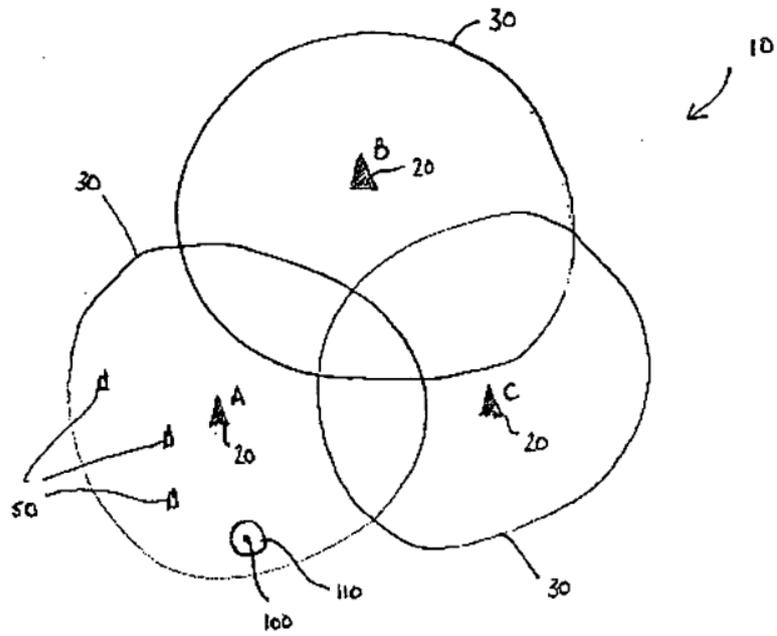


FIGURA 1

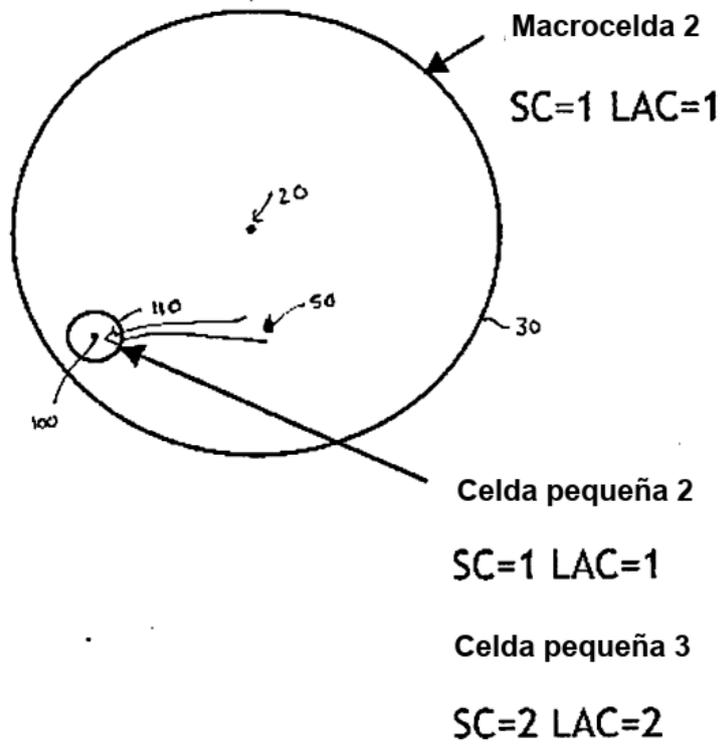


FIGURA 2

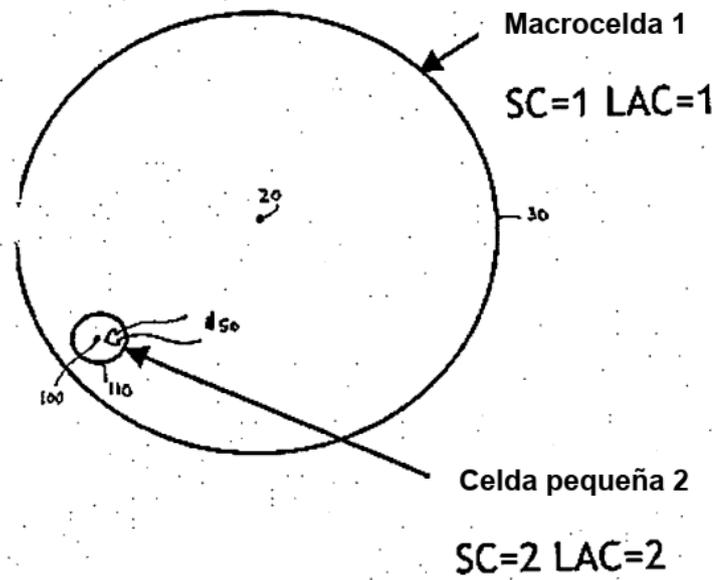


FIGURA 3

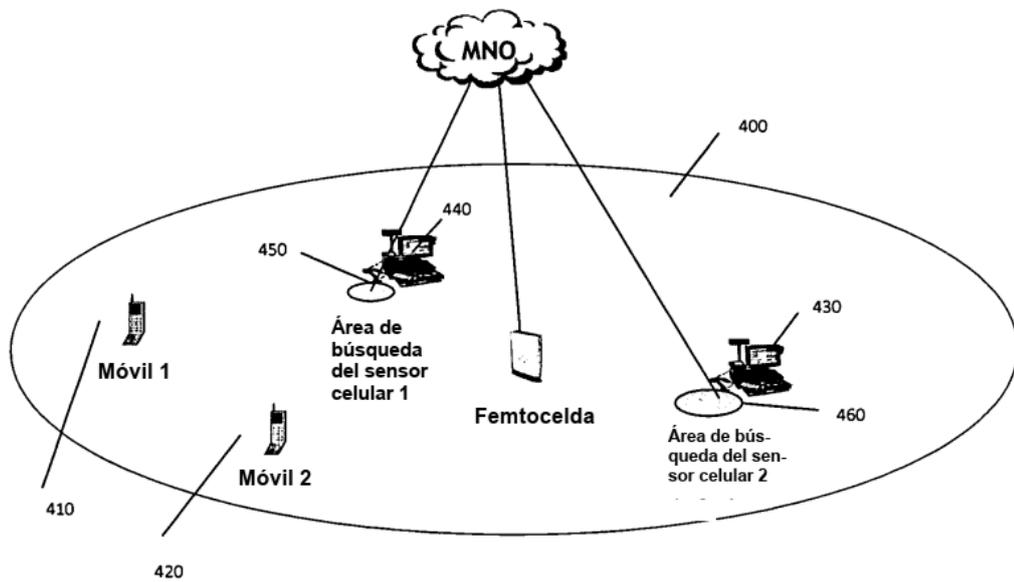


FIGURA 4

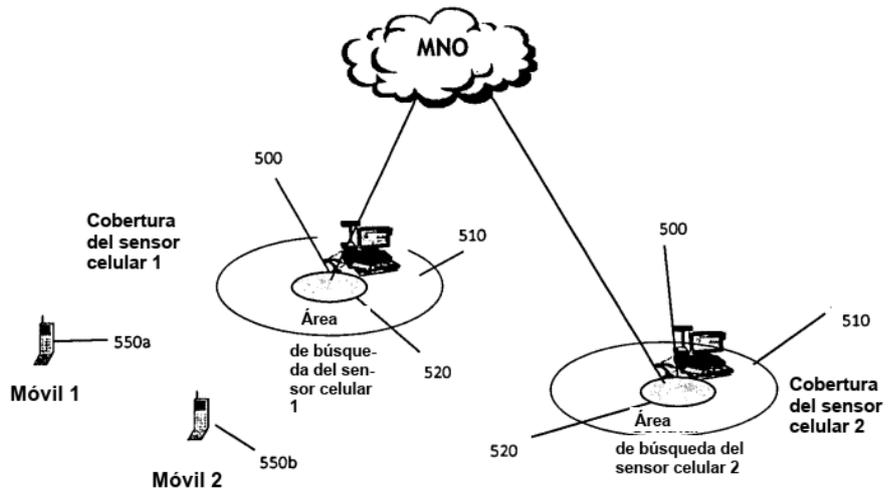


FIGURA 5