(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 575 881**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04W 4/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.05.2013 E 13726468 (5)**

(97) Fecha y número de publicación de la concesión europea: **06.04.2016 EP 2856789**

(54) Título: **Método para el rastreo de un dispositivo móvil en una unidad de visualización remota vía un centro de conmutación móvil y una cabecera**

(30) Prioridad:

30.05.2012 EP 12169948
30.05.2012 US 201261652883 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.07.2016

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

ANANTHARAMAN, SUBRAMANIAN

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para el rastreo de un dispositivo móvil en una unidad de visualización remota vía un centro de conmutación móvil y una cabecera

Campo técnico

[0001] La presente invención se refiere al campo de tecnología de televisión digital que proporciona servicios para abonados y se refiere a un método para el rastreo de la posición geográfica de un dispositivo móvil.
Este dispositivo móvil se conecta a un centro de conmutación móvil a través de una red de comunicación inalámbrica.
Este rastreo se realiza sobre una unidad de visualización remota, tal como una televisión digital, conectada a una cabecera a través de una segunda red de comunicación, tal como una red alámbrica/IP, diferente a la primera red de comunicación.

Antecedentes

[0002] Dispositivos móviles, tales como teléfonos móviles, a menudo están provistos de una unidad de ubicación capaz de determinar su ubicación actual bien basándose en señales satelitales (es decir, sistemas de ubicación GPS), o por cualquiera otra tecnología de determinación de posición, tal como posición obtenida por un procedimiento de triangulación con antenas de teléfono móvil.
Mediante la transmisión de la ubicación de un teléfono móvil sobre un sistema televisivo se hace posible, por ejemplo para amigos o familiares del usuario de teléfono móvil, conocer dónde está este usuario y rastrearlo él, por ejemplo en un mapa visualizado en la pantalla de TV, sin llamarlo a su teléfono móvil.

[0003] Para este propósito, el documento US 2006/0103551 divulga un sistema para el rastreo de una unidad móvil con un sistema GPS y para la visualización de un mapa electrónico en una unidad de visualización.
Los datos de posición de la unidad móvil se transmite a una estación de control maestra.
El usuario de la unidad de visualización necesita transmitir el identificador (ID) de la unidad móvil a la estación de control maestra, y luego esta transmite la posición de la unidad móvil a la unidad de visualización para mostrar al usuario dónde ha sido situada la unidad móvil.

[0004] El documento US 2006/0225108 divulga otro sistema para de comunicación entre un dispositivo televisivo y una o varias estaciones móviles en la vista para mostrar la ubicación de cada estación móvil en un mapa visualizado en una pantalla del dispositivo televisivo.
El dispositivo televisivo se acopla a una cabecera de red de difusión y esta acopla el dispositivo televisivo a un servidor de comunicación de grupo vía Internet.
El servidor de comunicación de grupo se acopla a una red inalámbrica y recopila y rellena una tabla de lista de mensaje con nuevos mensajes que vienen del dispositivo móvil por ser localizado.
El servidor gestiona solicitudes y respuestas de dispositivo televisivo.
Al recibir una solicitud de ubicación del dispositivo televisivo, el servidor comprueba si el dispositivo televisivo tiene los derechos requeridos para el acceso a información de ubicación.
Si el acceso es concedido, la información de ubicación se solicita al dispositivo móvil que manda su ubicación al servidor de comunicación de grupo.

[0005] El documento EP1631107 divulga un método para controlar el acceso entre un módulo de control y un módulo de localización autónomo.
El módulo de control puede ser un ordenador personal de un usuario que quiera conocer la posición del módulo de localización autónomo.
El método implica envío de un mensaje con un valor de control encriptado al módulo autónomo.
Este verifica este valor de control cada vez que recibe un mensaje.
Este valor de control se genera por el módulo de control y se envía al módulo de localización autónomo con el identificador del módulo de ubicación autónoma y con al menos un comando dentro de un mensaje encriptado.
Tras haber descifrado el mensaje mediante una clave secreta, el dispositivo móvil ejecuta el comando solo si el identificador y el valor de control son correctos.

[0006] Las soluciones de ubicación sugeridas por estos documentos presentan diferentes inconvenientes.
Por ejemplo, algunos documentos no sugieren ningún medio para evitar que un hacker intercepte un mensaje comprendiendo la información de ubicación enviado por el dispositivo móvil en respuesta a un mensaje de solicitud de ubicación.
Algunos sistemas revelan una estación de control maestra usada para almacenar información de ubicación y enviarla a petición de un usuario sin preocuparse de si la información de ubicación ha caducado o ha sido recientemente adquirida.
En otro caso, el dispositivo móvil no tiene ningún control sobre los datos en referencia a su ubicación respecto a un usuario enviándole un mensaje de solicitud de ubicación vía un servidor.

Además, las operaciones de gestión de mensaje, realizadas tanto por el emisor como el receptor, requieren recursos de ordenador significativos que son no optimizados.

Resumen de la invención

[0007] La presente invención sugiere superar, al menos parcialmente, los inconvenientes anteriormente mencionados por un método que de una parte protege datos sensibles intercambiados, vía diferentes redes de comunicación de diferentes tipos, entre una unidad de visualización y un dispositivo móvil rastreado, y que por otro lado optimiza las operaciones para preservar al menos los recursos del dispositivo móvil.

[0008] Con este fin, la presente invención sugiere un método para el rastreo de al menos un dispositivo móvil por una unidad de visualización remota, a través de un centro de conmutación móvil conectado al dispositivo móvil por una red de comunicación inalámbrica y a través de una cabecera enlazada al centro de conmutación móvil y conectada a la unidad de visualización por una segunda red de comunicación que es diferente de la red de comunicación inalámbrica.
El dispositivo móvil, la unidad de visualización y la cabecera se identifican respectivamente por un dispositivo móvil ID, una unidad de visualización ID y una cabecera ID.
El dispositivo móvil se proporciona por una parte con una unidad de localización capaz de decidir su ubicación actual y por otra con una unidad de comunicación para el soporte de al menos un servicio de mensajería instantánea.
La unidad de visualización dispone de un módulo para el tratamiento de mensajes que vienen al menos de la cabecera.

[0009] El método de la presente invención comprende una fase de inicialización y una fase operativa.
La fase de inicialización comprende los pasos de:

- generar una clave K, preferiblemente por la unidad de visualización, y encriptarla con una contraseña PW compartida entre la unidad de visualización y el dispositivo móvil,
- introducir, en una memoria de dicho dispositivo móvil, un primer registro en referencia a la unidad de visualización ID y que comprende la cabecera ID y la clave K.

[0010] La fase operativa comprende los pasos de:

- determinar la ubicación actual del dispositivo móvil mediante la unidad localizadora del dispositivo móvil, y encriptar esta ubicación actual usando la clave K,
- transmitir el dispositivo móvil ID y la ubicación actual encriptada a la unidad de visualización por el envío de un mensaje sucesivamente dirigido al centro de conmutación móvil, a la cabecera y a la unidad de visualización mediante su respectivo ID,
- desencriptar la ubicación actual encriptada con la clave K y visualizar la ubicación en la unidad de visualización.

[0011] Otras ventajas y formas de realización de la presente invención se describen en la siguiente descripción detallada.

Breve descripción de los dibujos

[0012] La presente invención será mejor entendida gracias a las figuras adjuntas, donde:
la Figura 1 muestra esquemáticamente las entidades principales de la infraestructura para el rastreo de un dispositivo móvil por una unidad de visualización vía una cabecera y un centro de conmutación móvil conforme a la presente invención,
las Figuras 2a a 2d son vistas esquemáticas de cada entidad mostrada en la Fig. 1 junto con sus componentes principales.

Descripción detallada

[0013] En referencia a la Fig. 1, ilustra esquemáticamente las entidades principales implicadas en la presente invención y la transmisión de mensajes entre estas entidades durante al menos la fase operativa del método.

[0014] Según la presente invención, las posiciones geográficas de al menos un dispositivo móvil 10 pueden ser rastreadas en una unidad de visualización remota 20.
El dispositivo móvil 10 puede ser un teléfono móvil, un dispositivo de seguidor GPS o cualquier otro dispositivo capaz de determinar y comunicar su ubicación actual a través de una red de comunicación inalámbrica 1.
La posición geográfica del dispositivo móvil 10 puede ser adquirida, por ejemplo, mediante el sistema de posición global (GPS) proporcionado por satélites 5 o por medio de un sistema de triangulación terrestre a través de antenas GSM 6.
La unidad de visualización 20 es preferiblemente una televisión digital ya que corresponde a la unidad de visualización más común en casas y pueden por lo tanto ser consideradas como medios completamente adecuados de entrega de información para gente en un ambiente doméstico.

Sin embargo, cualquier otra especie de unidad de visualización tal como un ordenador personal, un ordenador tablet o un smartphone, que se puede conectar a la cabecera a través de una segunda red de comunicación dedicada 2 para recibir, tratar y enviar mensajes, es también adecuada.

[0015] Como se muestra en la Fig. 1, el dispositivo móvil 10 se conecta a un centro de conmutación móvil (MSC) 30 a través de la red de comunicación inalámbrica 1 que es típicamente una red telefónica móvil.
El centro de conmutación móvil 30 se enlaza a la cabecera 40, bien por líneas de comunicación dedicadas a intercambio de datos específicos o por medios de otra red, tal como una red IP.
Finalmente, la cabecera 40 se conecta con la unidad de visualización 20 a través de una denominada segunda red de comunicación 2 que es una red de acceso fija, preferiblemente una red de comunicación terrestre hecha por ejemplo de fibras ópticas o líneas de teléfono comunes.
Uno de los objetivos de la presente invención es establecer un enlace entre el dispositivo móvil y la unidad de visualización para el cambio de al menos información confidencial usando sus redes respectivas.

[0016] En referencia a las Fig. 2a a 2d, cada una de las cuatro entidades principales de la figura 1 han sido esquemáticamente ilustradas, por separado, para mostrar los componentes principales que se usan para realizar el método de la presente invención.

[0017] La Fig. 2a muestra los componentes incluidos en el dispositivo móvil 10, es decir una interfaz de entrada/salida 11 para el cambio de mensajes M al menos a través del centro de conmutación móvil 30, una unidad de comunicación que es en particular una unidad de comunicación de mensaje 12 que soporta al menos un servicio de mensajería instantánea, una memoria 13 para el almacenamiento de al menos primeros registros $R1_{IDdisp}$ en referencia a las unidades de visualización que se autorizan por vía del dispositivo móvil, una unidad de localización 16 para la provisión de la ubicación actual del dispositivo móvil 10 y una unidad central de procesamiento (CPU) 18 para la administración de los componentes del dispositivo móvil.
Este dispositivo móvil se identifica por un identificador del dispositivo móvil ID_M almacenado en la memoria 13, en el dispositivo móvil.
El identificador del dispositivo móvil ID_M puede ser por ejemplo el número de llamada del dispositivo móvil 10 o cualquier número que es específico a la tarjeta de SIM (Módulo de Identidad del Suscriptor) del dispositivo móvil.
Cada primer registro $R1_{IDdisp}$ almacenado en la memoria 13 del dispositivo móvil comprende al menos 3-tuplas, es decir la clave K (es decir una clave compartida según un esquema de encriptación simétrica o un par de claves pública y privada según un esquema de encriptación asimétrica), el identificador de unidad de visualización ID_{Disp}, y el identificador de cabecera ID_{HE}.
No hay necesidad de también memorizar el identificador de unidad de visualización ID_{Disp} en el primer registro ya que este registro ya se refiere a este identificador, o al menos a la unidad de visualización correspondiente, debido a su nombre (es decir su propio identificador $R1_{IDdisp}$).
La unidad localizadora 16 puede usar típicamente una antena GPS para la determinación de la posición geográfica actual del dispositivo móvil.
Si esta antena no puede adquirir las señales de satélite requeridas para la determinación de la ubicación del dispositivo, la unidad localizadora 16 puede usar por ejemplo un procedimiento de triangulación con antenas de teléfono móvil.
Opcionalmente, el dispositivo móvil puede además incluir una unidad de aplicación 14 que será más detallada más adelante.

[0018] La Fig. 2b muestra los componentes del centro de conmutación 30 que está también provisto de una interfaz de entrada/salida 31 para el intercambio de mensajes M de una parte con la cabecera 40, y por otro lado con al menos un dispositivo móvil 10, una unidad de comunicación de mensajes 32 para el tratamiento de mensajes M, una unidad de facturación opcional 35 y un unidad central de procesamiento 38.
Como se describe en la presente invención, el centro de conmutación móvil 30 no se proporciona con un identificador específico éste, ya que se refiere aquí a un nombre genérico que incluye globalmente la infraestructura de teléfono móvil entera, es decir estaciones de base (interfaz aérea generalmente llamada de antenas de teléfono móvil) y el controlador de estación base al que se conectan estaciones de base (por ejemplo por conexiones de hilo) y que es responsable de la administración de distribución de recursos.

[0019] En referencia a la Fig. 2c, la cabecera 40 también comprende una interfaz de entrada/salida 41 para el intercambio de mensajes M, de una parte con al menos una unidad de visualización 20, y por otro lado con el centro de conmutación móvil 30.
De forma similar, incluye al menos una unidad de comunicación de mensaje 42 para el tratamiento de mensajes M (por ejemplo dentro de un módulo de tratamiento de mensaje) y un unidad central de procesamiento 48.
La cabecera se identifica por un identificador de cabecera única ID_{HE} que se puede almacenar en una memoria en la cabecera o en una base de datos opcional 43.
Opcionalmente, esto puede comprender además una unidad de aplicación 44 y/o una unidad de facturación 45 que se describe más en detalle más adelante.

[0020] Finalmente, la unidad de visualización 20, como se muestra en la Fig. 2d, comprende una interfaz de entrada/salida 21 para el intercambio de al menos mensajes con la cabecera 40, donde estos mensajes son preferiblemente formateados conforme al protocolo de la segunda red de comunicación 2.
Para manejar y procesar el tránsito de mensajes a través de la interfaz I/O, la unidad de visualización también comprende un módulo o una unidad de comunicación de mensaje 22, en particular para la preparación, envío de y recepción de al menos mensajes M que se refieren a la ubicación del dispositivo móvil.
También comprende una segunda base de datos 23 para el almacenamiento del clave K (es decir una clave compartida según un esquema de encriptación simétrica o un par de claves pública y privada según un esquema de encriptación asimétrica), para usarse para la codificación/descodificación de al menos datos sensibles contenidos en los mensajes M, y una contraseña PW usada para el encriptado de la clave K.
Esta clave debe ser intercambiada de forma segura entre la unidad de visualización 20 y el dispositivo móvil 10 si el intercambio se realiza a través de las redes de comunicación 1, 2, típicamente durante una fase de inicialización.
La unidad de visualización 20 se identifica por un identificador de unidad de visualización única ID_{Disp} que se puede almacenar bien en la segunda base de datos 23 o en una memoria en la unidad de visualización.
De la misma manera en cuanto a otras entidades principales, todos los componentes de la unidad de visualización se gestionan por un unidad central de procesamiento 28.

[0021] El método de la presente invención comprende dos fases principales, es decir una fase de inicialización y una fase operativa.

[0022] El paso de inicialización comprende dos pasos principales.
La primera fase es generar una clave K y encriptarla con una contraseña PW compartida entre la unidad de visualización 20 y el dispositivo móvil 10.
Compartir la contraseña puede hacerse por cualquier medio, por ejemplo a través de una llamada telefónica, por el envío de una carta o un correo electrónico, por vía oral en una reunión, etc. La clave K se puede generar por un generador aleatorio o pseudo-aleatorio de clave, preferiblemente en el lado de unidad de visualización.

[0023] Dependiendo del tipo de esquema criptográfico (es decir encriptación simétrica o asimétrica), la clave usada para la unidad de visualización puede ser la misma que la usada para el dispositivo móvil o puede referirse a pares únicos de claves pública y privada.
Claves públicas pueden ser además autentificadas por un certificado de clave pública firmado por una autoridad central de confianza.
Este certificado se puede enviar junto con una firma del mensaje que proporciona una asimilación del mensaje, por ejemplo mediante una función hash.
Al recibir el mensaje, esta asimilación se puede comparar con una asimilación obtenida usando la clave pública provista del certificado.
Si los dos digeridos son idénticos, el mensaje es auténtico y no ha sido alterado por una tercera parte.
Alternativamente, tal proceso de autentificación podría aplicarse a los datos en referencia a la clave K y/o a la ubicación actual en vez de a la totalidad del mensaje que contiene uno u otro de estos datos.
El algoritmo de clave simétrica, la criptografía de clave pública, digeridos y certificados firmados son herramientas de seguridad que son bien conocidas por el experto en la técnica y son por lo tanto no detallados más en la presente descripción.

[0024] Según la forma de realización preferida, la clave K es una clave simétrica y se genera por la unidad de visualización 20.
Sin embargo, podría ser también generado por un generador de clave situado fuera de la unidad de visualización 20, por ejemplo en el dispositivo móvil 10 o incluso en la cabecera 40 si la última ha obtenido previamente la información necesaria para transmitir la clave, tanto al dispositivo móvil 10 como a la unidad de visualización 20.

[0025] El segundo paso principal del paso de inicialización se refiere a introducir, en una memoria del dispositivo móvil 10, un primer registro $R1_{IDdisp}$ en referencia a la unidad de visualización 20, por ejemplo al identificador de unidad de visualización ID_{Disp}, y que comprende el identificador de cabecera ID_{HE} y la clave K.
Establecer tal primer registro se puede realizar de diferentes maneras.
Por ejemplo los datos podrían ser enviados de la unidad de visualización 20 al dispositivo móvil 10 a través de uno o más mensajes M (que pueden llamarse mensajes de inicialización), bien vía la cabecera 40 y el centro de conmutación móvil 30, o directamente al dispositivo móvil 10 a través del centro de conmutación móvil.
Esta solución última se puede realizar bien directamente por la unidad de visualización 20, si está provista de medios de comunicación para enviar directamente un mensaje instantáneo al dispositivo móvil, o por medio de un dispositivo intermedio (por ejemplo un teléfono móvil adicional) que sostiene un servicio de mensajería instantánea.
Según este último caso, podría ser previsto que la unidad de visualización muestre la clave K encriptada en su pantalla, luego esta clave encriptada se lee y es enviada a través de un mensaje instantáneo por un usuario que utiliza un teléfono móvil adicional.

[0026] Si el mensaje de inicialización se envía por el dispositivo de visualización sucesivamente a través de la cabecera y a través del centro de conmutación móvil, el contenido del mensaje enviado a la cabecera comprende al menos la clave K encriptada y los identificadores ID_M e ID_{Disp}.

En la variante, este mensaje de inicialización puede también comprender el identificador ID_{HE} de la cabecera 40.
Ventajosamente en este último caso, la cabecera solo necesita pasar este mensaje de inicialización al centro de conmutación móvil 30, sin tener que completar este mensaje.
Una vez recibido por el centro de conmutación móvil, este mensaje de inicialización ya no necesita incluir el identificador ID_M, ya que el centro de conmutación móvil ahora sabe que debe enviar este mensaje de inicialización final al dispositivo móvil identificado por este ID_M.

[0027] Se use la forma anterior que se use para enviar la clave K, esta clave nunca se envía en un texto claro sino que es siempre enviada en una forma encriptada.
Para el encriptado de la clave K, la contraseña PW se usa como una clave de encriptación de un algoritmo adecuado que es instalada, dentro de una unidad de codificación/descodificación, tanto en el dispositivo móvil como en la unidad de visualización.
Tal unidad de encriptación se puede situar por ejemplo en las unidades de comunicación de mensaje respectivo 12, 22.
Como la clave K nunca es enviada en el texto claro entre la unidad de visualización 20 y el dispositivo móvil 10, si es interceptada por una persona maliciosa, esta clave no se puede descifrar sin la contraseña PW que es mantenida secreta.

[0028] Alternativamente, la clave K se puede visualizar en texto claro en la pantalla de la unidad de visualización 20 y luego puede ser manualmente introducida en el dispositivo móvil 10 por el usuario de este dispositivo móvil.
Como la unidad de visualización se localiza en un área privada (típicamente una casa privada), no hay riesgo para mostrarlo en claro en la pantalla para introducirlo directamente en el dispositivo móvil 10.

[0029] Alternativamente, todos o una parte de los datos (es decir ID_{Disp}, ID_{HE}, K) por ser incluidos en el primer registro $R1_{IDDisp}$ podrían ser visualizados en texto claro en la pantalla de la pantalla de la unidad de visualización para ser manualmente introducidos en el dispositivo móvil 10, por ejemplo vía un teclado o cualquiera otra interfaz adecuada, requiriendo una conexión por cable (p. ej. cable USB) o una conexión inalámbrica (por ejemplo Bluetooth, Wi-Fi) con el dispositivo de visualización 20.

[0030] Al final de la fase de inicialización, el dispositivo móvil 10 ha almacenado todos los datos que son necesarios para el encriptado de la información sensible (es decir para el encriptado de la ubicación actual del dispositivo móvil), para luego enviar esta información a la unidad de visualización 20 sucesivamente a través del centro de conmutación móvil 30 y a través de la cabecera 40.
De hecho, el dispositivo móvil conoce la clave K, el identificador de cabecera ID_{HE} donde la dirección de cabecera se puede encontrar y el identificador de unidad de visualización ID_{Disp} donde la dirección de la unidad de visualización puede también encontrarse.
Ventajosamente, ningunos datos adicionales deberían ser almacenados en el dispositivo móvil 10 y estos datos no requieren ninguna actualización.
Por lo tanto, los recursos informáticos del dispositivo móvil se conservan en lo posible.
Si es necesario, la fase de inicialización puede ser fácilmente realizada tantas veces como sea necesario más tarde, por ejemplo para cambiar la clave K.
Además, la memoria 13 del dispositivo móvil 10 puede memorizar diferentes primeros registros $R1_{IDdisp}$ pertenecientes a unidades de visualización diferente 20, de modo que puede ser rastreado simultáneamente por diferentes unidades de visualización.

[0031] Una vez ha terminado la fase de inicialización, el dispositivo móvil puede opcionalmente enviar un mensaje de confirmación dirigido a la unidad de visualización 20 para la confirmación de que los pasos de la fase de inicialización han sido completados y que el dispositivo móvil 10 está preparado para ejecutar la fase operativa.
Tal mensaje de confirmación puede ser un mensaje que proporciona la ubicación actual del dispositivo móvil de la misma manera que un mensaje enviado por el dispositivo móvil según la fase operativa que es descrita de aquí en adelante.

[0032] La segunda fase del presente método es la fase operativa que se puede manejar tan pronto como la contraseña PW ha sido compartida (entre la unidad de visualización y el dispositivo móvil) y tan pronto como el primer registro $R1_{IDdisp}$ (junto con sus datos) ha sido almacenados en la memoria 13 del dispositivo móvil.
La fase operativa comprende los pasos de:

- determinar la ubicación actual del dispositivo móvil 10, mediante su unidad de localización 16, y encriptar esta ubicación actual usando la clave K,
- Transmitir el dispositivo móvil ID_M y la ubicación actual encriptada a la unidad de visualización 10 por el envío de un mensaje M sucesivamente dirigido al centro de conmutación móvil 30, a la cabecera 40 y a la unidad de visualización 20 mediante su identificador respectivo, es decir el ID_{HE} y el ID_{Disp}.
- desencriptar la ubicación actual encriptada con la clave K en la unidad de visualización 20 y visualizar la ubicación sobre esta unidad de visualización (es decir sobre la pantalla de esta unidad).

[0033] Ventajosamente, la invención según la forma de realización preferida sugiere solo la encriptación de la ubicación actual, para ayudar a guardar recursos informáticos.

Además, como la clave K es preferiblemente almacenada en una forma no encriptada en el dispositivo móvil, esta clave K puede ser inmediatamente usada por todas las operaciones de encriptación sucesiva, realizadas en el dispositivo móvil durante la fase operativa, sin pedir al usuario del dispositivo móvil que introduzca la contraseña PW.

[0034] Según una forma de realización, la fase operativa se inicia por la recepción, en el dispositivo móvil 10, de un mensaje de solicitud de ubicación que comprende al menos el identificador de unidad de visualización ID_{Disp} que es la única información que el dispositivo móvil necesita conocer para el envío de un mensaje a la unidad de visualización apropiada 20, por ejemplo en respuesta al mensaje de solicitud de ubicación.
Este mensaje de solicitud de ubicación se dirige al dispositivo móvil (por medios de su identificador) y se releva al menos por el centro de conmutación móvil.
Si este mensaje también transita a través de la segunda red de comunicación 2, es decir vía la cabecera, su contenido tiene que además incluir el identificador de cabecera ID_{HE} para ejecutar un enrutamiento de mensaje correcto.

[0035] Alternativamente, el dispositivo móvil 10 puede transmitir, a intervalos de tiempo regulares, su identificador ID_M y la ubicación actual encriptada a la unidad de visualización 20 por el envío de un mensaje M sucesivamente dirigido al centro de conmutación móvil 30, a la cabecera 40 y a la unidad de visualización 20 mediante su respectivo ID.
Así, los datos de ubicación actual también se pueden enviar sin recibir cada vez un mensaje de solicitud de ubicación de la unidad de visualización.
Un mensaje de solicitud de ubicación al dispositivo móvil podría comprender parámetros para la instrucción de este dispositivo móvil para enviar su ubicación actual (y su identificador ID_M) a un determinado intervalo temporal dentro de un período de tiempo que se pueden definir bien por una duración determinada o por una fecha/hora de inicio y una fecha/hora de finalización.
De todos modos, sea cual sea el método que inicia la transmisión de mensajes que comprende datos de ubicación en referencia al dispositivo móvil, estos mensajes siempre pasan primero a través de la red de comunicación inalámbrica 1, y luego a través de la segunda red de comunicación 2, antes de alcanzar el dispositivo de visualización 20.

[0036] Como se muestra en Fig. 1, los mensajes M enviados entre las cuatro entidades principales 10, 20, 30,40 necesariamente no proporcionan el mismo contenido.
Este es la razón por qué los mensajes M han sido también cada uno identificado en esta figura por un número (M1 a M6) que es diferente entre cada entidad y según la dirección del mensaje.

[0037] Para transmitir su ubicación actual a la unidad de visualización, el dispositivo móvil en primer lugar envió al centro de conmutación móvil 30 un mensaje M4 dirigido al identificador de unidad de visualización ID_{Disp}.
El contenido del mensaje M4 incluye al menos la ubicación actual encriptada y los identificadores ID_{HE} e ID_{Disp} para permitir un enrutamiento de mensaje correcto.
Luego, el centro de conmutación móvil 30 transmite al menos una parte de este contenido mediante el envío de un mensaje M5 a la cabecera 40.
El contenido del mensaje M5 comprende al menos la ubicación actual encriptada y los identificadores ID_M, ID_{Disp}.
Este contenido permite de una parte conocer el ID del emisor (es decir el ID del dispositivo móvil), y por otro lado continuar el enrutamiento del mensaje.
Finalmente, la cabecera 40 transmite, sucesivamente, al menos una parte del contenido del mensaje precedente M5 por el envío de un mensaje M6 a la unidad de visualización 20.
El contenido de este mensaje M6 incluye al menos la ubicación actual encriptada y los identificadores ID_M, de modo que la unidad de visualización sabe a qué dispositivo móvil la ubicación actual incluida se refiere.

[0038] Al complementar los mensajes M4 y M5 respectivamente con ID_M e ID_{HE}, estos mensajes pueden tener el mismo contenido y la tarea del centro de conmutación móvil 30 puede consistir simplemente en el envío del mensaje M4 recibido del dispositivo móvil a la cabecera.
De forma similar, si el mensaje M6 incluye el identificador ID_{Disp}, los mensajes M5 y M6 se vuelve idénticos y la cabecera puede justo enviar el mensaje M5 a la unidad de visualización sin ninguna enmienda de su contenido.
Finalmente, podría estar previsto que el dispositivo móvil 10 genere un mensaje M4 que está en última instancia dirigido al dispositivo de visualización y que comprenden todos los datos necesarios para evitar cualquier enmienda de su contenido a lo largo de su enrutamiento a través del centro de conmutación móvil 30 y a través de la cabecera 40.

[0039] Ventajosamente, los datos sensibles tales como la clave K y los datos acerca de la ubicación actual del dispositivo móvil nunca son descritos ni al centro de conmutación móvil ni a la cabecera.
Además, estos datos sensibles están inclusos no registrado en ninguna tal entidad intermedia y se mantienen encriptados siempre durante su tránsito entre el dispositivo móvil y la unidad de visualización.
Por lo tanto, una relación de confianza mutua se puede establecer entre el emisor y el receptor ya que confidencialidad ante los datos críticos es maximizada, reduciendo así cualquier riesgo de hacking.
Preferiblemente, estas medidas cautelosas son ventajosamente aplicadas y limitadas a datos confidenciales solo.

[0040] Los mensajes intercambiados entre el dispositivo móvil 10 y el centro de conmutación móvil 30 son mensajes instantáneos (mensajería a tiempo real), tales como SMS (servicio de mensaje corto), MMS (servicio de mensajería multimedia) o WhatsApp (una alternativa al SMS).
Estos mensajes se pueden procesar por la unidad de comunicación de mensaje 12 para la lectura de mensaje recibido del centro de conmutación móvil y para la preparación de mensajes a ser enviados como respuestas.

[0041] En cuanto al mensaje de solicitud de ubicación, se puede dirigir al dispositivo móvil 10 bien a través de la segunda red de comunicación 2, vía la cabecera 40, por el envío de un primer mensaje M1 que es sucesivamente transmitido mediante un segundo mensaje M2 enviado de la cabecera 40 al centro de conmutación móvil 30 y luego mediante el tercer mensaje M3 (es decir un mensaje instantáneo) enviado del centro de conmutación móvil 30 al dispositivo móvil 10.

[0042] En tal enrutamiento de mensaje donde el mensaje de solicitud de ubicación se inicia por la unidad de visualización y en primer lugar transmitido por la cabecera mediante su identificador ID_{HE}, el contenido del primer mensaje M1 comprende al menos el identificador del dispositivo móvil ID_M y el identificador de unidad de visualización ID_{Disp}.
El contenido del mensaje M2 es al menos el mismo que el del primer mensaje M1, y el contenido del mensaje instantáneo M3 comprende al menos el identificador de unidad de visualización ID_{Disp}.
Ventajosamente y según la forma de realización preferida de la presente invención, no hay necesidad de incluir una instrucción o un comando específico a tales mensajes porque pueden ser inmediatamente reconocidos (por ejemplo debido a su formato específico) como mensajes de solicitud de ubicación, al menos por el dispositivo móvil, por ejemplo a través de su unidad de comunicación de mensaje 12 y/o su unidad de aplicación 14.

[0043] Dependiendo del enrutamiento de mensaje sugerido por la presente invención, el contenido de este tercer mensaje M3 puede ser directamente enviado por la unidad de visualización 20 en el caso donde esta unidad 20 es capaz de enviar un mensaje instantáneo al dispositivo móvil 10 vía el centro de conmutación móvil.
Esta forma última se ilustra en la Fig. 1 mediante el mensaje M' enviado de la unidad de visualización 20 al centro de conmutación móvil 30 que a su vez la transmite por el envío del mensaje M3 al dispositivo móvil 10.
En el caso donde la unidad de visualización 20 no se proporciona para el envío de tal mensaje M3', este mensaje M3' podría ser enviado por un dispositivo móvil adicional conectado para este fin a la unidad de visualización 20.

[0044] Según otra forma de realización, el segundo registro $R2_{IDdisp}$ en referencia a la unidad de visualización 20 se almacena en una base de datos 43, preferiblemente situada en la cabecera 40.
El segundo registro incluye los identificadores del dispositivo móvil ID_M de cada dispositivo móvil 10 rastreado por la unidad de visualización 20.
Así, un mensaje de solicitud de ubicación (por ejemplo enviado por la unidad de visualización) puede ser dirigido, al menos parcialmente, a los dispositivos móviles 10 con su identificador del dispositivo móvil ID_M incluidos en el segundo registro $R2_{IDdisp}$ en referencia a la unidad de visualización 20.
Preferiblemente, tal mensaje de solicitud de ubicación se dirige a todos los dispositivos móviles 10 de una misma comunidad, es decir a todos los dispositivos móviles con su identificador del dispositivo móvil ID_M en el anteriormente mencionado segundo registro $R2_{IDdisp}$.
Ventajosamente, la misma clave K se puede compartir y usar para todos los dispositivos móviles de la misma comunidad así reduciendo la gestión de una pluralidad de claves, en particular dentro de un esquema de criptografía de clave pública.
Alternativamente, la base de datos 43 podría estar también situada en el dispositivo de visualización 20.
Sin embargo, en vez de enviar un solo un mensaje de solicitud de ubicación corto con solo un identificador del dispositivo móvil ID_M de la visualización a la cabecera, esta solución alternativa requiere el envío de bien un mensaje de solicitud de ubicación más largo incluyendo todos los identificadores del dispositivo móvil ID_M necesitados, o diferentes mensajes de solicitud de ubicación cortos, es decir un mensaje por identificador del dispositivo móvil.
Por lo tanto, es más eficaz y juicioso implementar la base de datos 43 en la cabecera y dejar a la cabecera administrar el contenido de esta base de datos.

[0045] Opcionalmente, el identificador del dispositivo móvil ID_M, identificando el dispositivo móvil 10 al que el mensaje de solicitud de ubicación es dirigido, se puede controlar por la verificación de si este identificador ID_M está ya incluido en el segundo registro $R2_{1Ddisp}$ en referencia al identificador de unidad de visualización ID_{Disp} donde dicho mensaje de solicitud de ubicación ha sido enviado.
En caso de resultados negativos, este identificador del dispositivo móvil ID_M se añade a este segundo registro $R2_{IDdisp}$.
De este modo, la lista de los dispositivos móviles rastreados por la unidad de visualización en referencia a este segundo registro puede ser fácilmente y automáticamente actualizada sin necesidad de una solicitud específica para la actualización del contenido del segundo registro $R2_{IDdisp}$.

[0046] Como una alternativa de la presente invención, en particular según una forma de realización más desarrollada de la fase de inicialización, el establecimiento del primer registro $R1_{IDdisp}$ almacenado en la memoria del dispositivo móvil 10 se realiza por el envío, a este dispositivo móvil 10, de un mensaje de inicialización transmitido al menos por el dispositivo de centro de conmutación móvil 30 a través de la red de comunicación inalámbrica 1 y que comprende

al menos el identificador de unidad de visualización ID_{Disp}, el identificador de cabecera ID_{HE} y la clave K en su forma encriptada.

[0047] Dependiendo de la forma de realización de la fase de inicialización del presente método, este mensaje de inicialización se puede enviar de la misma manera que el mensaje M3' mostrada en la Fig. 1, es decir bien directamente de la unidad de visualización 20 o de un dispositivo móvil adicional (por ejemplo un teléfono móvil que soporta un servicio de mensajería instantánea).

[0048] Según otro enrutamiento de mensaje, el mensaje de inicialización se envía al dispositivo móvil 10, y se envía sucesivamente a la cabecera 40 (de la unidad de visualización 20), luego al centro de conmutación móvil 30 (de la cabecera 40) y usando los identificadores respectivos, es decir el identificador de cabecera ID_{HE} y el identificador del dispositivo móvil ID_M.
Así según este enrutamiento de mensaje, el mensaje de inicialización pasa sucesivamente a través de la segunda red de comunicación 2, luego a través de la red de comunicación móvil 1.

[0049] Según otra forma de realización, el mensaje recibido de inicialización por el dispositivo móvil comprende además una aplicación a ser instalada en el dispositivo móvil 10, por ejemplo dentro de una unidad de aplicación 14 como se muestra en la Fig. 2a.
Tal aplicación se refiere a software diseñado para realizar tareas específicas.
En particular, esta aplicación se puede usar para automáticamente tratar mensajes de solicitud de ubicación entrantes.
Con el objetivo de solicitar una posición geográfica bien a la presentación de la unidad de visualización 20 o de la cabecera 40, tales mensajes se pueden reconocer por la aplicación, por ejemplo debido a su formato específico o por medios de una cabecera incluida en cada mensaje.

[0050] Como un ejemplo, esta aplicación una vez instalada en la unidad de aplicación del dispositivo móvil puede realizar los pasos siguientes antes de establecer el primer registro $R1_{IDdisp}$ durante la fase de inicialización:

- pedir la introducción de la contraseña PW,
- desencriptar la clave K con la contraseña introducida PW',
- verificar la conformidad de la clave descifrada y, en caso de resultados positivos, autorizarla el establecimiento (introducción) del primer registro en referencia al identificador de unidad de visualización ID_{Disp}.

[0051] Ventajosamente, no hay necesidad de memorizar la contraseña PW en la memoria del dispositivo móvil para la comparación con la contraseña introducida PW' para dar más acceso a la implementación del primer registro.
De hecho, la contraseña se usa como una clave de desencriptación para la desencriptación de la clave K encriptada.
Si la contraseña introducida PW' es idéntica a la contraseña PW que fue usada para la encriptación de la clave K, entonces el resultado de la desencriptación de la clave K corresponderá a la clave K correcta.
Esta clave K puede tener, por ejemplo, un formato específico o una cabecera específica para verificar la adaptabilidad de la clave descifrada y, en caso de resultados positivos, para autorizar el establecimiento del primer registro (en la memoria del dispositivo móvil) junto con su contenido, es decir el identificador de cabecera ID_{HE} y la clave K.

[0052] Aunque la etapa con el objetivo de verificar la conformidad de la clave descifrada antes de establecer el primer registro en referencia al identificador de unidad de visualización no es realmente necesaria, se recomienda no omitir esta operación de verificación para evitar la implementación de un primer registro que tenga un formato incorrecto o que comprenda datos incorrectos.

[0053] Otras aplicaciones se pueden implementar en una unidad de aplicación (tal como la unidad de aplicación 44) en la cabecera 40 y/o incluso en la unidad de visualización 20.
Una aplicación se puede implementar por ejemplo en la cabecera para administrar y manejar los segundos registros $R2_{IDdisp}$ almacenados en su base de datos 43.
Por ejemplo, tal aplicación podría ser usada para enviar un mensaje de solicitud de ubicación para todos los identificadores ID_M comprendido en un segundo registro $R2_{IDdisp}$.
El envío de tales mensajes de solicitud de ubicación se puede realizar tan pronto como la cabecera recibe, de la unidad de visualización 20, un mensaje M1 pidiendo una solicitud de ubicación de uno de estos identificadores.

[0054] Según otra forma de realización, al menos una parte de los mensajes M intercambiados entre el dispositivo móvil 10 y la unidad de visualización 20, vía el centro de conmutación móvil 30 y preferiblemente vía la cabecera 40, se cuenta por motivos de facturación en una cuenta que se refiere bien al identificador de unidad de visualización ID_{Disp} o al identificador del dispositivo móvil ID_M.
Las operaciones de facturación se pueden manejar por las unidades de facturación 35, 45, como se muestra en la Fig. 2b y la Fig. 2c.

[0055] Según una forma de realización preferida, la cuenta se sitúa en la base de datos 43, en la cabecera 40, y se usan para la cuenta de mensajes M6 transmitidos de la cabecera a la unidad de visualización 20.

[0056] Para compeler los mensajes enviados del dispositivo móvil a la unidad de visualización a transitar a través de una entidad de facturación, los datos sensibles en referencia a la ubicación actual del móvil se pueden proteger por una capa de sobreencriptación que se puede quitar por esta entidad solo.
Tal entidad puede preferiblemente ser la cabecera, aunque el interruptor móvil no es excluido.
Aplicar tal protección se puede realizar forzando el dispositivo móvil a sobreencriptar una parte del contenido comprendida en el mensaje M4 mediante una segunda clave K2 (junto con un algoritmo de codificación/descodificación que puede ser el mismo algoritmo usado con la clave K).
Esta segunda clave K2 es preferiblemente almacenada en el dispositivo móvil como datos en referencia a la unidad de visualización, por ejemplo en referencia al identificador de unidad de visualización ID_{Disp}.
Esta segunda clave K2 se puede generar por un generador de clave en la entidad anteriormente mencionada, preferiblemente en la cabecera 40 y tiene que permanecer desconocida a la unidad de visualización 20 y a cualquier usuario.
Una vez recibido por esta (cabecera) entidad, lo último procede a la eliminación de la capa de sobreencriptación usando esta segunda clave K2 (con el mismo algoritmo de codificación/descodificación que ha sido previamente usado para aplicar la capa de sobreencriptación).
Así, datos en referencia a ubicación actual del dispositivo móvil son meramente encriptados por la clave K y luego se pueden enviar al dispositivo móvil en el mensaje M6 como previamente explicado en las formas de realización que no se refieren a tal capa de sobreencriptación.
Ventajosamente, si esta entidad (por ejemplo la cabecera) es puenteada debido a hacking y mensajes no transitan a través de esta entidad, por ejemplo para evitar cualquier operación de facturación, la unidad de visualización será incapaz de acceder a datos en referencia a la ubicación actual del dispositivo móvil ya que esta información estará todavía encriptada por la segunda clave K2.

[0057] La segunda clave K2 se puede almacenar de una manera secreta en la memoria 13 del dispositivo móvil.
Según otra forma de realización, el acceso a esta segunda clave K2 se puede proteger con una segunda contraseña PW2 conocida por el dispositivo móvil y la entidad anteriormente mencionada (por ejemplo la cabecera), pero que permanece desconocida a la unidad de visualización y a cualquier usuario.

[0058] Para implementar la segunda clave K2 en el dispositivo móvil, este paso se puede realizar por ejemplo a través de la instalación de la aplicación en la unidad de aplicación 14, vía un mensaje de inicialización.
Alternativamente, la transmisión de la segunda clave K2 al dispositivo móvil se puede realizar a través de un mensaje de mantenimiento enviado por la entidad (cabecera) tras haberla generado mediante un generador de clave (por ejemplo el mismo generador de clave usado para generar la clave K).
Alternativamente, los mensajes de mantenimiento se pueden usar para la renovación de la segunda clave K2, preferiblemente a intervalos de tiempo imprevisibles, de forma la segunda clave K2 que se vuelve difícil de interceptar, en particular si esta segunda clave K2 no está protegida por la segunda contraseña PW2.

[0059] Al recibirse, tales mensajes de mantenimiento pueden ser automáticamente reconocidos (por ejemplo debido a su formato específico) por el dispositivo móvil, en particular a través de su unidad de comunicación de mensaje 12 o por medio de la aplicación en funcionamiento en la unidad de aplicación 14, que contiene dicha segunda clave K2 y pueden ser procesados como tal, por ejemplo por la aplicación anteriormente mencionada.

[0060] Además, esta segunda clave K2 se puede cambiar en cualquier momento por dicha entidad.
Alternativamente, la segunda clave K2 se puede encriptar por la segunda contraseña PW2 que puede ser previamente almacenada y oculta en el dispositivo móvil, por ejemplo dentro de su memoria o en la aplicación cuando se instala en la unidad de aplicación 14 mediante un mensaje de inicialización.
Tras la recepción de un mensaje de mantenimiento, la aplicación puede ser capaz de automáticamente recuperar la segunda contraseña PW2 extrayéndola del dispositivo móvil para desencriptar la segunda clave K2 contenida en este mensaje.

[0061] Según otra forma de realización, la capa de sobreencriptación podría ser extendida al mensaje entero M4, con la excepción sin embargo del identificador de cabecera IDHE que debe ser mantenido en texto claro para un enrutamiento de mensaje adecuado.
Luego, el mensaje M4 encriptado por la segunda clave K2 podría ser redirigido por el centro de conmutación móvil hacia la cabecera.
Así, el mensaje M4 sería convertido en el mensaje M5 cuyos datos encriptados por la segunda clave K2 serían idénticos a los contenidos en el mensaje M4.
Finalmente, la cabecera puede procesar el mensaje sobreencriptado M5 de la misma manera explicada aquí arriba para eliminar la capa sobreencriptada y transmitir el mensaje M6 a la unidad de visualización.

[0062] En cuanto a los identificadores, debe observarse que los identificadores ID_{HE} e ID_{Disp} pueden corresponder a cualquier número o cualquier dirección que permite encontrar la cabecera correspondiente, respectivamente la unidad de presentación visual correspondiente, para entregar el mensaje al receptor correcto.

[0063] Según una forma de realización, cuando un mensaje de solicitud de ubicación ha sido dirigido al dispositivo móvil 10, la unidad de visualización 20 puede regularmente preguntar la cabecera 40 si ha recibido uno o más mensajes dirigidos a la unidad de visualización 20, típicamente como una respuesta al mensaje de solicitud de ubicación previamente enviado.
Si al menos un mensaje ha sido recibido por la cabecera a la atención de la unidad de visualización, esta última puede recuperar este mensaje conforme a una denominada "tecnología pull".
Al contrario, si la unidad de visualización 20 no necesita ir a recoger los mensajes en la cabecera actuando como un servidor, la configuración corresponde a la "tecnología push" debido a que el servidor manda automáticamente el mensaje a la unidad de visualización.
Cualquiera de estas tecnologías puede ser aplicada por el dispositivo de visualización 20 para la recuperación, de la cabecera 40, de mensajes M6 comprendiendo los datos de ubicación actual del dispositivo móvil 10.
Dependiendo del método usado para llevar los mensajes a la unidad de visualización, esta última puede transmitir a la cabecera 40 su identificador ID_{Disp} junto con su dirección antes de cualquier intercambio, por ejemplo durante la fase de inicialización.

[0064] Debe tenerse también en cuenta que la unidad de visualización 20, como nombrada en la presente descripción, se refiere más particularmente a un equipo tal como una televisión digital conectada a un decodificador.
Este equipo puede ser además conectado a otros dispositivos (por ejemplo una unidad de grabación) y/o por lo menos a una red que es diferente de la primera y segunda redes 1 y 2, por ejemplo a una red interna (LAN).

[0065] La etapa que tiene como objetivo mostrar la ubicación del dispositivo móvil sobre la pantalla de la unidad de visualización se puede realizar de diferentes maneras, por ejemplo mediante la visualización de una marca en un mapa escalable, por la visualización de la dirección postal correspondiente o por visualización de las coordenadas del dispositivo móvil dentro de un sistema de coordenadas geográfico.

REIVINDICACIONES

1. Método para el rastreo de al menos un dispositivo móvil (10)en una unidad de visualización remota (20) a través de un centro de conmutación móvil (30) conectado al dispositivo móvil (10) por una red de comunicación inalámbrica (1) y a través de una cabecera (40) enlazada al centro de conmutación móvil (30) y conectada a la unidad de visualización (20) por una segunda red de comunicación (2) diferente a la red de comunicación inalámbrica (1), donde dicho dispositivo móvil (10) es identificado por un identificador del dispositivo móvil ID_M, donde dicha unidad de visualización (20) es identificada por un identificador de unidad de visualización ID_{Disp} y está provista de un módulo (22) para el tratamiento de mensajes que vienen de la cabecera (40) identificada por un identificador de cabecera ID_{HE}, donde dicho dispositivo móvil (10) está provisto de un unidad de localización (16) capaz de determinar su ubicación actual y de una unidad de comunicación (12) para el soporte de al menos un servicio de mensajería instantánea, donde dicho método incluye una fase de inicialización y una fase operativa,

a) donde dicha fase de inicialización incluye las etapas de:

- generar una clave K y encriptarla con una contraseña PW compartida entre la unidad de visualización (20) y dicho dispositivo móvil (10),
- establecer, en una memoria (13) de dicho dispositivo móvil (10), un primer registro $R1_{IDdisp}$ en referencia al identificador de unidad de visualización ID_{Disp} y que comprende el identificador de cabecera ID_{HE} y dicha clave K,

b) donde dicha fase operativa incluye las etapas de:

- determinar la ubicación actual del dispositivo móvil (10) por la unidad localizadora (16) de dicho dispositivo móvil (10) y encriptar la ubicación actual usando la clave K,
- transmitir el identificador del dispositivo móvil ID_M y la ubicación actual encriptada a la unidad de visualización (10) enviando un mensaje sucesivamente dirigido al centro de conmutación móvil (30), a la cabecera (40) y a la unidad de visualización (20) mediante sus identificadores respectivos,
- desencriptar la ubicación actual encriptada con la clave K y visualizar dicha ubicación en la unidad de visualización (20).

2. Método según la reivindicación 1, donde la fase operativa es desencadenada por la recepción, en el dispositivo móvil (10), de un mensaje de solicitud de ubicación que comprende al menos el identificador de unidad de visualización ID_{Disp}, donde dicho mensaje de solicitud de ubicación es dirigido al dispositivo móvil (10) y transmitido al menos por el centro de conmutación móvil (30) debido a sus identificadores respectivos.

3. Método según la reivindicación 2, donde dicho mensaje de solicitud de ubicación se inicia por la unidad de visualización (20) y es transmitido en primer lugar por la cabecera (40) debido a su identificador ID_{HE}.

4. Método según la reivindicación 2 o 3, donde un segundo registro $R2_{IDdisp}$ en referencia a dicha unidad de visualización (20) se almacena en una base de datos (43) situada bien en la cabecera (40) o en la unidad de visualización (20), donde dicho segundo registro $R2_{IDdisp}$ incluye identificadores de dispositivo móvil ID_M de cada dispositivo móvil (10) rastreado por dicha unidad de visualización (20) y dicho mensaje de solicitud de ubicación es dirigido, al menos parcialmente, a los dispositivos móviles (10) con su identificador de dispositivo móvil ID_M incluido en dicho segundo registro $R2_{IDdisp}$.

5. Método según la reivindicación 4, donde el identificador del dispositivo móvil ID_M que identifica el dispositivo móvil (10) al que se dirige el mensaje de solicitud de ubicación se controla mediante la verificación de si dicho identificador del dispositivo móvil ID_M está ya incluido en el segundo registro $R2I_{Ddisp}$ en referencia al identificador de unidad de visualización ID_{Disp}, en caso de resultados negativos dicho identificador del dispositivo móvil ID_M se añade a dicho segundo registro $R2_{IDdisp}$.

6. Método según la reivindicación 1, donde el establecimiento de dicho primer registro $R1_{IDdisp}$ en la memoria (13) del dispositivo móvil (10) se realiza por el envío de a dicho dispositivo móvil (10), de un mensaje de inicialización transmitido al menos por el centro de conmutación móvil (30) a través de la red de comunicación inalámbrica (1) y que comprende al menos el identificador de unidad de visualización ID_{Disp}, el identificador de cabecera ID_{HE} y la clave K encriptada.

7. Método según la reivindicación 6, donde dicho mensaje de inicialización es sucesivamente dirigido a la cabecera (40), de la unidad de visualización (20), y luego al centro de conmutación móvil (30), de la cabecera (40), usando sus identificadores respectivos.

8. Método según la reivindicación 6 o 7, donde el mensaje de inicialización recibido por el dispositivo móvil (10) comprende además una aplicación para ser instalada en el dispositivo móvil (10), para automáticamente tratar mensajes de solicitud de ubicación entrantes.

9. Método según la reivindicación 8, donde durante la fase de inicialización, dicha aplicación una vez instalada en el dispositivo móvil (10) ejecuta los pasos siguientes:

- pedir la introducción de la contraseña PW,

- desencriptar la clave K con la contraseña introducida PW,
- verificar la conformidad de la clave K descifrada y, en caso de resultados positivos, autorizar el establecimiento del primer registro $R1_{IDdisp}$ en referencia al identificador de unidad de visualización ID_{Disp}.

10. Método según cualquier reivindicación precedente, donde al menos una parte de los mensajes intercambiados entre el dispositivo móvil (10) y la unidad de visualización (20), a través del centro de conmutación móvil (30) y preferiblemente a través de la cabecera (40), se contabiliza para fines de facturación en una cuenta que se refiere bien al identificador de unidad de visualización ID_{Disp} o al identificador del dispositivo móvil ID_M.

11. Método según la reivindicación 10, donde dicha cuenta se sitúa en la base de datos (43) de la cabecera (40) para la contabilización de mensajes transmitidos a la unidad de visualización (20).

12. Método según cualquiera de las reivindicaciones de la 1 a la 11, donde dicha fase de inicialización comprende además el paso de:
- generar una segunda clave K2 que permanece desconocida a la unidad de visualización (20) y almacenar esta segunda clave en el dispositivo móvil (10) como datos en referencia a la unidad de visualización (20),

y dicha fase operativa comprende además los pasos de:
- utilizar dicha segunda clave K2 para la sobreencriptación de la ubicación actual encriptada antes de su transmisión en el mensaje sucesivamente dirigido al centro de conmutación móvil (30), a la cabecera (40) y a la unidad de visualización (20),
- eliminar dicha capa de sobreencriptación antes de que dicho mensaje haya alcanzado la unidad de visualización (20) usando dicha segunda clave K2.

13. Método según la reivindicación 12, donde dicha segunda clave K2 se almacena en la memoria (13) del dispositivo móvil (10) y su acceso se protege con una segunda contraseña PW2 que permanece desconocida a la unidad de visualización (20) y a cualquier usuario.

14. Método según la reivindicación 12 o 13, donde la implementación de la segunda clave K2 en el dispositivo móvil (10) se realiza a través de la instalación de la aplicación en dicho dispositivo móvil (10).

15. Método según cualquiera de las reivindicaciones de la 12 a la 14, donde la segunda clave K2 almacenada en el dispositivo móvil (10) se renueva a intervalos de tiempo imprevisibles mediante el envío a dicho dispositivo móvil (10) de un mensaje de mantenimiento en el que puede ser automáticamente reconocido que contiene dicha segunda clave K2 y que puede ser procesado como tal, al ser recibido por dicho dispositivo móvil (10).

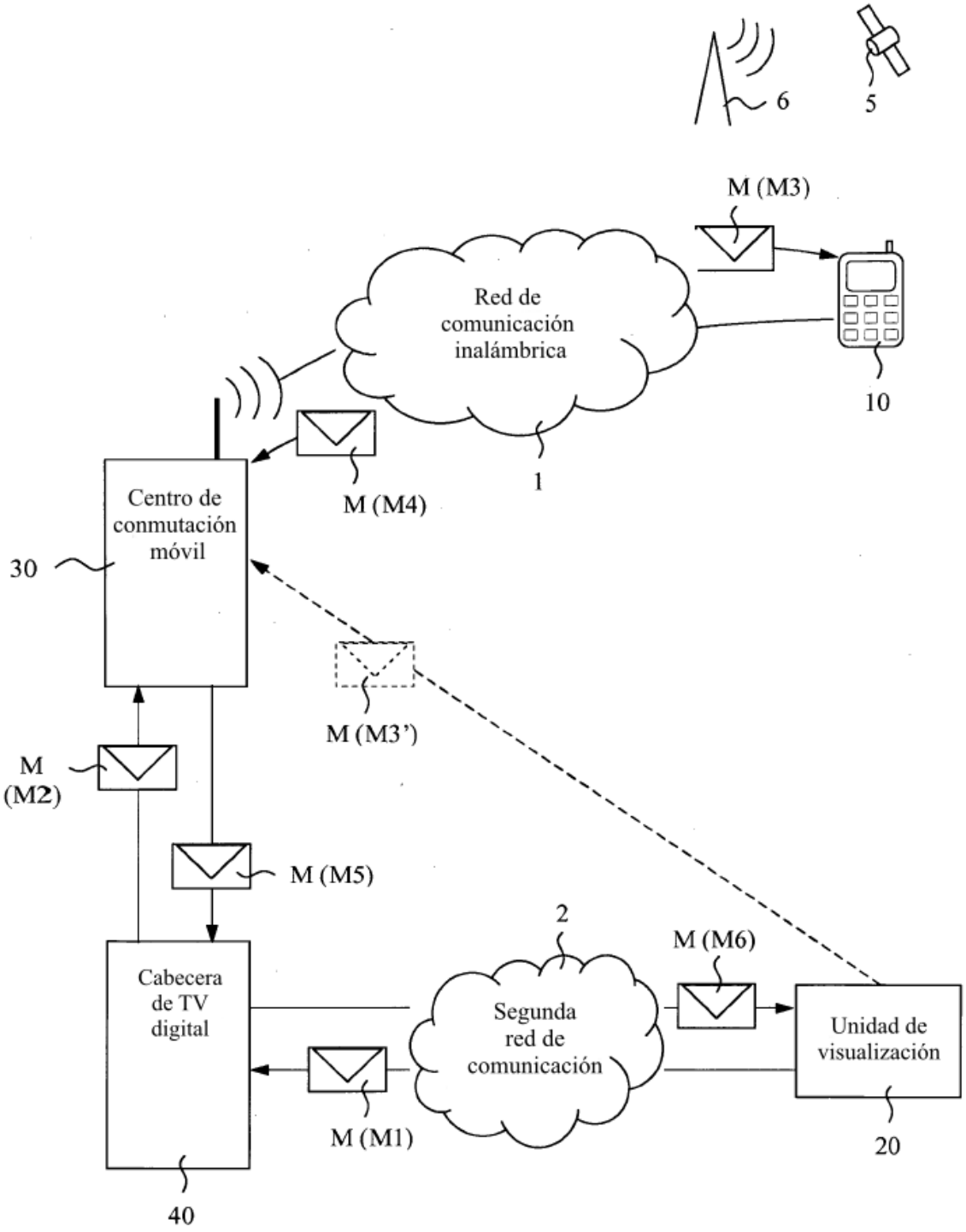
6
5
M (M3)
Red de comunicación inalámbrica
10
1
M (M4)
Centro de conmutación móvil
30
M (M3')
M (M2)
M (M5)
2
M (M6)
Cabecera de TV digital
Segunda red de comunicación
Unidad de visualización
M (M1)
20
40

Fig. 1

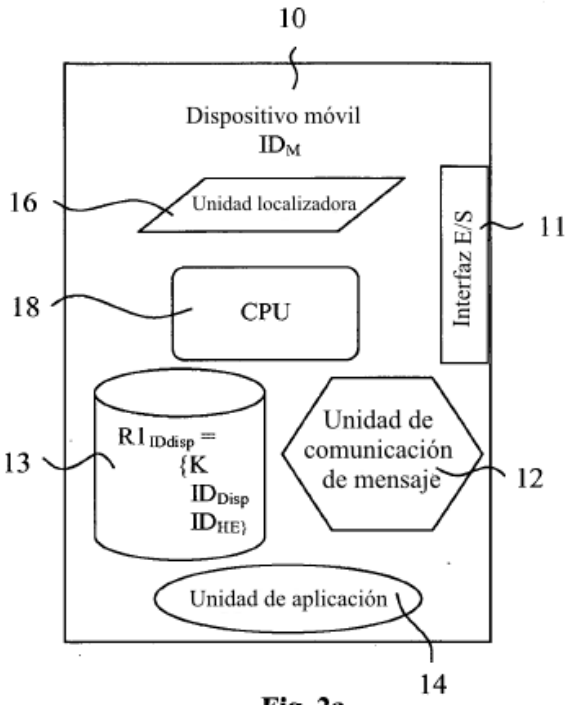

Fig. 2a

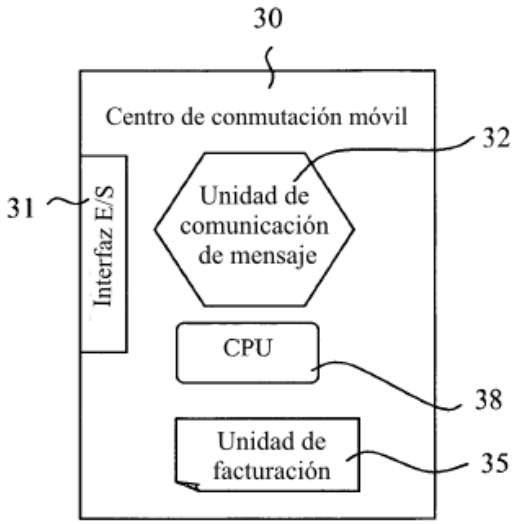

Fig. 2b

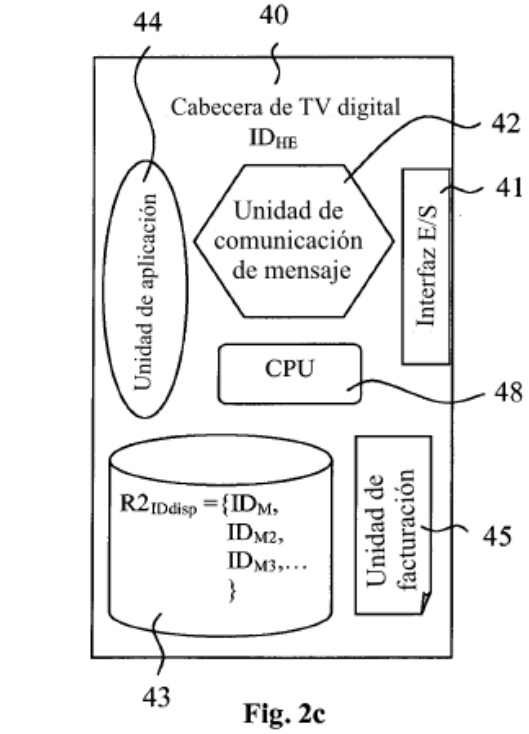

Fig. 2c

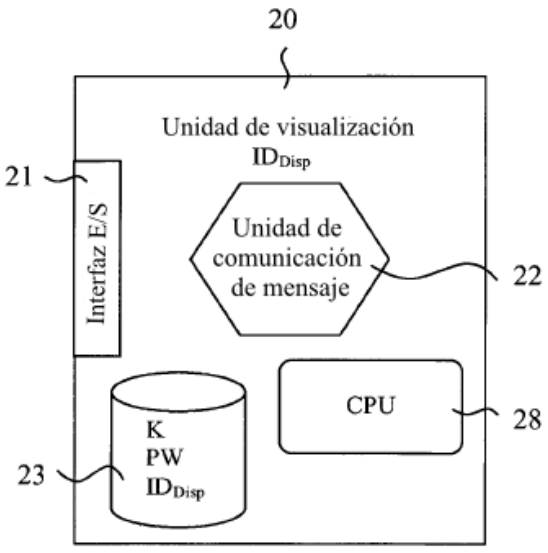

Fig. 2d