(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 271 503**

(51) Int. Cl.:
H04L 12/28 (2006.01)
H04Q 7/38 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03292926 .7**
(86) Fecha de presentación : **26.11.2003**
(87) Número de publicación de la solicitud: **1536592**
(87) Fecha de publicación de la solicitud: **01.06.2005**

(54) Título: **Autentificación entre una terminal móvil de red celular y un punto de acceso de la red de corto alcance.**

(45) Fecha de publicación de la mención BOPI:
16.04.2007

(45) Fecha de la publicación del folleto de la patente:
16.04.2007

(73) Titular/es: **FRANCE TELECOM**
6, place d'Alleray
75015 Paris, FR

(72) Inventor/es: **Calmels, Benoît;**
Maguy, Christophe y
Trillaud, Sébastien

(74) Agente: **Lehmann Novo, María Isabel**

DESCRIPCIÓN

Autentificación entre una terminal móvil de red celular y un punto de acceso de la red de corto alcance.

La presente invención concierne de manera general al establecimiento de una conexión entre un punto de acceso de una red inalámbrica de corto alcance, del tipo Bluetooth o Wi-Fi, y una terminal móvil de una red celular del tipo GSM equipada con un módulo emisor-receptor para comunicar con un punto de acceso de la red de corto alcance. La misma concierne más particularmente a la generación de una clave de enlace en la autentificación de la terminal móvil y del punto de acceso de manera de aparearlos.

En materia de seguridad de un enlace de radio específicamente Bluetooth, por ejemplo un usuario que desea establecer un enlace Bluetooth entre un ordenador personal portátil y una terminal móvil celular introduce un código de identificación PIN a modo de clave secreta en los teclados del ordenador y de la terminal móvil. El ordenador y la terminal móvil establecen cada uno una clave de enlace en función de números aleatorios intercambiados entre ellos, de la clave secreta, y de las direcciones Bluetooth del ordenador y de la terminal móvil. Si por ejemplo el ordenador personal es considerado como el autentificador del enlace, el mismo genera un número aleatorio (prueba) que comunica por la interfase radio Bluetooth con la terminal móvil. La terminal calcula una respuesta que depende del número aleatorio recibido, de la clave de enlace y de la dirección Bluetooth de la terminal móvil a fin de que el ordenador compare la respuesta de la terminal con aquella que el mismo ha calculado, lo que autentifica la terminal móvil cuando hay identidad de las respuestas comparadas.

El apareamiento del ordenador y de la terminal necesita una clave secreta (código PIN) para compartir la clave de enlace. La clave secreta debe ser suficientemente larga y ausente de diccionarios para que la clave secreta no sea expuesta a ataques cuyo objetivo es encontrar la misma para deducir la clave de enlace y otra clave de cifrado. Tales ataques ponen nuevamente en causa la autentificación y la integridad de los datos intercambiados.

Para prevenir esos ataques, la clave secreta debe ser relativamente larga, lo que provoca una introducción laboriosa y sujeta a errores, específicamente en la terminal móvil cuya interfase hombre-máquina es limitada.

La solicitud de patente US 2002/031228 A1 divulga un dispositivo de acceso por ejemplo para abrir una puerta de habitación de hotel. El dispositivo de acceso puede estar conectado por medio de un enlace Bluetooth a una terminal móvil de una red de telecomunicaciones celular. La terminal móvil requiere una conexión con un servidor asociado al hotel por medio de la red celular o un enlace Bluetooth. El servidor transmite entonces una clave a la terminal móvil. Después de una conexión al dispositivo de acceso, la terminal móvil envía la clave al dispositivo de acceso que compara la clave recibida con una clave memorizada en el dispositivo de acceso a fin de validarla y proporcionar el acceso a la habitación. No está prevista ninguna autentificación de la terminal móvil por el dispositivo de acceso.

El artículo de Uri Blumenthal y otros, "A Scheme for Authentification and Dynamic Key Exchange in Wireless Networks", Bell Labs Technical Journal 7(2), P. 37-48, 2002, describe una combinación de autentificaciones para una terminal móvil que depende de una red "doméstica" de corto alcance donde un servidor de autenticación contiene una clave secreta igualmente memorizada previamente en la terminal móvil, cuando está en enlace con un punto de acceso unido a un servidor de autentificación de otra red de corto alcance llamada red "extranjera". El servidor de la red doméstica autentifica a la vez la terminal móvil y el servidor de la red extranjera sobre la base de un primer "autentificador" que es calculado por la terminal móvil en función de la clave secreta, de números aleatorios proporcionados por el servidor de la red extranjera y la terminal y de un identificador de la terminal. El primer autentificador es transmitido al servidor de la red doméstica a través del punto de acceso y el servidor de la red extranjera. El servidor de la red doméstica recalcula el primer autentificador en función específicamente de la clave secreta memorizada encontrada en correspondencia con el identificador de la terminal transmitida por el servidor de la red extranjera.

Si la terminal es autentificada a continuación de una igualdad de los primeros autentificadores transmitidos y recalculados independientes de cualquier clave de sesión, el servidor de la red doméstica genera un segundo "autentificador" en función de la clave secreta, de los números aleatorios y del identificador de la terminal y calcula una clave de sesión en función de la clave secreta, de un tercer número aleatorio y del segundo autentificador. El segundo autentificador es transmitido a la terminal a través del servidor de la red extranjera y del punto de acceso para que la terminal recalcule el segundo autentificador y autentique el servidor de la red doméstica cuando los segundos autentificadores transmitidos y recalculados son iguales. Después de esta segunda autentificación independiente de la clave de sesión, la terminal genera la clave de sesión.

Todos los parámetros precedentes son transmitidos a través del enlace terminal móvil - punto de acceso - servidor de la red extranjera - servidor de la red doméstica, sin ningún enlace a través de la red doméstica entre la terminal móvil y el servidor de la red doméstica, lo que impone memorizar previamente la clave secreta en la terminal móvil y el servidor de la red doméstica para respetar una seguridad de las autentificaciones, debilitando las autentificaciones por la utilización de la misma clave secreta para generar la clave de sesión de cada sesión entre la terminal móvil y un punto de acceso.

La solicitud de patente WO 02/07135 A1 concierne a la activación de un borne interactivo unido a una red de telecomunicación desde una terminal móvil en una red de radiotelefonía. La terminal móvil señala su presencia en las cercanías del borne, específicamente por transmisión de un mensaje que comprende el identificador de terminal y un identificador de zona de localización de la red de radiotelefonía a un medio de gestión que invita al usuario de la terminal a aproximarse al borne más próximo sobre el cual el usuario es autentificado por medio de un código secreto leído en una tarjeta de memoria, o de una huella biométrica del usuario, transmitida por el borne a un servidor. La solicitud de patente WO 02/07135 A1 no sugiere ninguna autentificación mutua de la terminal móvil y el borne a través de la red de radiotelefonía.

La invención tiene como objetivo asegurar el establecimiento de una conexión entre una terminal móvil celular y un punto de acceso de una red inalámbrica de corto alcance sin necesitar la introducción de una clave secreta (código PIN), asegurando completamente la utilización de tal clave que puede ser muy larga y renovada en cada sesión entre la terminal móvil y un punto de acceso.

Para alcanzar este objetivo, un procedimiento de autentificación que precede una sesión entre una red inalámbrica de corto alcance que tiene puntos de acceso y una terminal móvil en una red de radiocomunicaciones celular, está caracterizado porque comprende las etapas siguientes:

- transmisión de una demanda que incluye una dirección de la terminal móvil y una dirección de un punto de acceso situado en la zona de cobertura de la terminal móvil relativa a la red de corto alcance, desde la terminal móvil a un medio de gestión por medio de la red celular,
- determinación de un código secreto por el medio de gestión,
- desde el medio de gestión, transmisión de un mensaje de confirmación que incluye el código secreto y la dirección del punto de acceso extraída de la demanda a la terminal móvil por medio de la red celular y de un mensaje de solicitud de conexión que incluye el código secreto y la dirección de la terminal móvil extraída de la demanda al punto de acceso,
- solicitud de conexión de la terminal móvil al punto de acceso designado por la dirección extraída del mensaje de confirmación a fin de que la terminal móvil y el punto de acceso determinen una clave de sesión en función de la dirección del punto de acceso, de la dirección de la terminal móvil y del código secreto extraído del mensaje de confirmación y del mensaje de solicitud de conexión, y
- autentificación de la terminal móvil por el punto de acceso en función de la clave de sesión.

La autentificación puede comprender una solicitud de determinación desde el punto de acceso de una respuesta en función de la clave de sesión a la terminal móvil que transmite la respuesta al punto de acceso, por medio de la red de corto alcance, y en el punto de acceso, una determinación de una respuesta en función de la clave de sesión y una comparación de las respuestas para autorizar la abertura de una sesión entre el punto de acceso y la terminal móvil cuando al menos las respuestas comparadas son idénticas.

De preferencia, la autentificación precedente de la terminal móvil por el punto de acceso es completada por una autentificación del punto de acceso por la terminal móvil en función de la clave de sesión, cuando el punto de acceso ha autentificado la terminal móvil. En ese caso, el procedimiento puede comprender a continuación de una identidad de las respuestas comparadas en el punto de acceso, una invitación trasmitida a la terminal móvil a fin de que la terminal móvil autentifique el punto de acceso solicitando al punto de acceso determinar una segunda respuesta en función de la clave de sesión y transmitir la segunda respuesta a la terminal móvil por medio de la red de corto alcance, determinando una segunda respuesta en función de la clave de sesión y comparando las segundas respuestas a fin de autorizar la abertura de la sesión solamente después de una identidad de las segundas respuestas comparadas en la terminal móvil.

En la práctica, es preferible que la terminal móvil busque varios puntos de acceso en la zona de cobertura de la terminal móvil a fin de introducir direcciones de los puntos de acceso encontrados en la demanda. El medio de gestión selecciona entonces la dirección de un punto de acceso óptimo entre las direcciones de punto de acceso extraídas de la demanda según uno o varios criterios predeterminados para introducir la dirección del punto de acceso óptimo en el mensaje de confirmación transmitido a la terminal móvil y el mensaje de solicitud de conexión transmitido al punto de acceso óptimo.

Según una variante, el medio de gestión determina la clave de sesión en lugar de las determinaciones de la clave de sesión en la terminal móvil y el punto de acceso, e introduce la clave de sesión determinada en lugar del código secreto en el mensaje de confirmación y el mensaje de solicitud de conexión a fin de que durante la autentificación las respuestas a comparar sean determinadas específicamente en función de la clave de sesión extraída de los mensajes precedentes.

La invención concierne igualmente a un sistema de autentificación entre una red inalámbrica de corto alcance que tiene puntos de acceso y una terminal móvil en una red de radiocomunicaciones celular que está caracterizada según la reivindicación 14.

En una variante, el medio de gestión puede determinar el mismo la clave de sesión y introducirla en lugar del código secreto en el mensaje de confirmación y el mensaje de solicitud de conexión.

Otras características y ventajas de la presente invención aparecerán más claramente con la lectura de la descripción que sigue de varias realizaciones preferidas de la invención, a título de ejemplos no limitativos, con referencia a los dibujos anexos correspondientes en los cuales:

- la figura 1 es un diagrama en bloque esquemático de un sistema de telecomunicaciones que comprende una terminal móvil en una red de radiocomunicaciones celular y al menos un punto de acceso en una red inalámbrica de corto alcance para llevar a cabo el procedimiento de autentificación según la invención; y
- la figura 2 muestra etapas principales de un algoritmo del procedimiento de autentificación entre la terminal móvil y el punto de acceso según la invención.

El sistema de telecomunicaciones mostrado en la figura 1 para llevar a cabo el procedimiento de autentificación según la invención comprende esencialmente una terminal celular móvil TM en una red de radiocomunicaciones celular RC, uno o varios puntos de acceso AP unidos por una red de distribución RD en una red inalámbrica de corto alcance RFP que da acceso a una red de paquetes de alto flujo RP, tal como Internet, y una plataforma de gestión PFG propia de la invención. A modo de ejemplo, la red celular RC es una red GSM y la red inalámbrica de corto alcance RFP es una red Bluetooth.

La terminal móvil TM comprende dos interfases radio respectivamente con la red celular RC y la red de corto alcance RFP.

Los puntos de acceso AP y en una variante las terminales móviles comprenden cada uno un generador pseudo-aleatorio y generan cada uno un algoritmo de autentificación AA para producir respuestas RP1, RP2 cada una en función de un número aleatorio, de un código secreto y de la dirección de terminal móvil o de punto de acceso en la red de corto alcance RFP.

Un algoritmo de clave de sesión AS es igualmente implementado en los puntos de acceso y la terminal móvil.

La red celular RC, tal como una red GSM, es representada esquemáticamente en la figura 1 por medios principales a los cuales la terminal móvil TM está conectada temporalmente tal como una estación de base BTS, un controlador de estación de base BSC, un conmutador del servicio móvil MSC asociado a un registrador de localización de los visitantes VLR, y un registrador de localización nominal HLR.

La plataforma de gestión PFG está unida al registrador de localización nominal HLR, tanto directamente como un centro de autentificación (no representado) unido al registrador HLR, o como servidor a través de una red intermedia tal como la Internet RP. La plataforma PFG puede estar igualmente unida a un centro de mensajes cortos SMSC (Short Mesage Service Center) cuando demandas RQ le son transmitidas bajo la forma de mensajes cortos por terminales móviles, y/o puede estar unida a un centro de mensaje de señalización USSD (Unstructured Supplementary Service Data) cuando demandas RQ le son transmitidas bajo la forma de mensajes USSD por terminales móviles. Los mensajes USSD son transmitidos en el curso de verdaderas sesiones establecidas y más rápidamente que los mensajes cortos. El centro de mensajes cortos y el centro de mensajes de señalización serán designados a continuación indiferentemente por "centro de mensajes CM". La plataforma PFG contiene específicamente un generador pseudo-aleatorio para generar códigos secretos CS a la solicitud de las terminales móviles, tal como la terminal TM. Los códigos secretos presentan según la invención, una gran longitud típicamente de al menos dieciséis octetos, o sea una longitud superior a 128 bits.

La plataforma PFG contiene, según variantes de la invención, una base de datos que lista las direcciones ADAP de los puntos de acceso AP de varias redes inalámbricas de corto alcance, en asociación con las localizaciones geográficas de los puntos de acceso AP con relación a zonas de localización determinadas ZL en la red celular RC. Se recuerda que una zona de localización en una red celular recubre varias células respectivamente asociadas a estaciones de base BTS y que un conmutador MSC administra una o varias zonas de localización.

Como se verá a continuación, la plataforma PFG constituye un medio de gestión intermedio entre una terminal móvil TM y un punto de acceso AP a fin de trasmitirles un código secreto CS para proceder a su autentificación. Según variantes descritas más adelante, la plataforma PFG sirve igualmente para seleccionar un punto de acceso óptimo en respuesta a una demanda RQ de una terminal móvil.

En la figura 1 está representada solamente una red inalámbrica de corto alcance; se comprenderá que la terminal móvil TM puede comunicar con cualquier red inalámbrica de corto alcance particularmente en un lugar público, tal como una estación, una galería de mercadería, una estación aérea, un hotel, etc. Un punto de acceso radio AP es por ejemplo un borne dotado de una interfase radio Bluetooth para poder comunicar en un radio de algunas decenas de metros con terminales móviles TM, y una interfase de línea para comunicar por una parte con otras puntos de acceso AP a través de la red de distribución RD, si existe, de la red inalámbrica de corto alcance, y por otra parte para ofrecer comunicaciones de paquetes de alto flujo a las terminales móviles gracias a un enlace de la red de distribución RD con la Internet RP. En ciertas configuraciones de la red inalámbrica de corto alcance, la red de distribución RD es una red intranet que está unida directamente por líneas xDSL a la Internet RP, o bien la red de distribución RD está confundida con la Internet RP y cada punto de acceso AP está unido directamente a la Internet RP a través de líneas xDSL.

Como se muestra en la figura 2, el procedimiento de autentificación según una realización preferida de la invención comprende esencialmente etapas E1 a E17. Inicialmente, la terminal móvil TM ha sido puesta en marcha y reconocida por la red celular RC en una zona cubierta radio-eléctricamente por ésta. La terminal TM en estado de vigilancia es así localizada en una zona de localización ZL de la red RC y una identidad temporal TMSI le ha sido atribuida por el registrador VLR conectado a esta zona de localización, como es conocido.

En la etapa E1, el usuario de la terminal TM que penetra en la zona de cobertura de la red inalámbrica de corto alcance RFP con los puntos de acceso AP decide seleccionar un menú Bluetooth sobre su terminal TM, y particularmente un sub-menú de búsqueda (inquiry mode) de puntos de acceso AP. Los puntos de acceso AP bajo la forma de bornes pueden ser buscados, es decir escrutan cada uno periódicamente la presencia de una terminal móvil para detectar una interrogación (inquiry) transmitida por las terminales móviles. Por esa vía, la terminal móvil TM recibe las direcciones ADAP de los puntos de acceso situados en la zona de cobertura de la terminal móvil TM relativa a la red de corto alcance RFP. La terminal TM escoge entre las respuestas a su búsqueda que la misma recibe, las direcciones de las entidades de la red de corto alcance RFP que corresponden a las clases de dispositivos asociados a los puntos de acceso, a fin de descartar cualquier dirección que provenga de un dispositivo cualquiera equipado con un módulo de emisión-recepción compatible con la red RFP, tal como una terminal telefónica móvil, un asistente numérico personal PDA, un ordenador portátil, etc.

En la etapa E2, las direcciones ADAP de los puntos de acceso disponibles y encontrados durante la búsqueda precedente son memorizados en la terminal TM e introducidos en una demanda RQ a transmitir a la plataforma de gestión PFG a través de la red fija de la red celular RC. La demanda RQ comprende la dirección ADTM de la terminal TM pre-memorizada en la misma a fin de que la plataforma PFG pueda comunicarla a los puntos de acceso seleccionados posteriormente. La demanda RQ comprende como dirección de destinatario un identificador IDPFG de la plataforma PFG que ha sido pre-memorizado en la terminal móvil TM. La demanda RQ puede estar bajo la forma de un mensaje corto o de un mensaje de señalización USSD y la plataforma PFG está entonces unida al centro de mensajes correspondientes CM.

Una vez que la demanda RQ ha sido emitida automáticamente por la terminal TM y recibida por la plataforma PFG, la plataforma examina la lista de las direcciones de punto de acceso ADAP extraída de la demanda RQ a fin de seleccionar el punto de acceso óptimo en función de uno o varios criterios predeterminados en la etapa E3. La selección del punto de acceso óptimo es precedida por una verificación del perfil del usuario de la terminal móvil TM identifi-

cado por un identificador permanente IMSI a fin de autorizarlo a acceder a un punto de acceso de la red inalámbrica de corto alcance RFP.

Según una primera variante, un criterio predeterminado es relativo a una comparación de niveles de potencia de señales de referencia emitidas por los puntos de acceso encontrados por la terminal móvil TM, recibidos por la terminal TM. En esta variante, la terminal TM incluye igualmente, en asociación con cada dirección ADAP de punto de acceso disponible y encontrado en la demanda transmitida RQ, un nivel de potencia NP recibido en la terminal. La terminal transmite entonces la demanda RQ con pares ADAP, NP a la plataforma de gestión PFG que compara los niveles de potencia recibidos NP a fin de determinar el mayor nivel de potencia recibido y seleccionar el punto de acceso AP asociado al nivel más alto de potencia recibido, como punto de acceso óptimo, para establecer una conexión con la terminal TM.

Según una variante cualquiera poco similar a la precedente, el punto de acceso óptimo que tiene el mayor nivel de potencia recibido por la terminal móvil es buscado y seleccionado en la etapa E1 entre puntos de acceso disponibles y encontrados en la zona de cobertura de la terminal móvil TM, por la terminal móvil TM propiamente en lugar de la plataforma PFG. La demanda RQ solo contiene la dirección ADAP del punto de acceso óptimo AP en lugar de la lista de los pares ADAP, NP.

Según una segunda variante, un criterio predeterminado es relativo a una comparación de cargas de tráfico de los puntos de acceso AP disponibles y encontrados por la terminal móvil TM a fin de que la plataforma de gestión PFG seleccione el punto de acceso que tiene la carga más pequeña de tráfico como punto de acceso óptimo. Las cargas de tráfico de los puntos de acceso AP de la red de corto alcance RFP son recibidas por la red de distribución RD que las comunica periódicamente, por medio de Internet RP o una línea especializada, con la plataforma PFG para una actualización de la base de datos relativos a los puntos de acceso.

Según una variante complementaria a combinar con la primera o segunda variante precedente, la plataforma PFG interroga al registrador de localización nominal HLR de la red celular RC a fin de leer el identificador IDZL de la zona de localización donde se encuentra la terminal TM en la red celular, antes de la selección de la dirección de punto de acceso óptimo. En función del indicador de zona de localización IDZL, la plataforma PFG elimina las direcciones ADAP de la lista incluida en la demanda RQ, que designan puntos de acceso disponibles y encontrados AP que están situados en el exterior de la zona de localización incluyendo la terminal móvil TM y definidos en la red celular. Esta variante complementaria evita que una terminal móvil se substituya en el punto de acceso declarándose con una dirección de un punto de acceso muy alejado de la terminal móvil, a fin de comunicar con la misma. Luego el punto de acceso óptimo es seleccionado por la plataforma PFG o tomando simplemente la dirección del primer punto de acceso de la lista extraída de la demanda RQ, o combinando esta variante con la variante de los niveles de potencia o de cargas de tráfico de los puntos de acceso a fin de seleccionar el punto de acceso que presenta el mayor nivel de potencia o la carga de tráfico más pequeña entre aquellas situadas en la zona de localización.

En la etapa E3, igualmente el generador pseudoaleatorio en la plataforma de gestión PFG determina un código secreto CS que tiene una gran longitud, al menos igual a 128 bits.

La plataforma PFG prepara entonces seguidamente dos mensajes.

En la etapa E4, un mensaje de confirmación MC que contiene la dirección ADAP del punto de acceso óptimo y el código secreto producido CS es establecido por la plataforma PFG para transmitirlo a la terminal móvil TM a través de la red celular RC. El mensaje MC es del mismo tipo que la demanda RQ, es decir un mensaje corto SM o un mensaje USSD, y transita a través del centro de mensajes correspondiente CM. El código secreto CS extraído del mensaje MC es memorizado en asociación con la dirección de punto de acceso óptimo ADAP en la terminal móvil TM. La terminal TM posee en la etapa E4 el código secreto CS, como si, según la técnica anterior, el usuario hubiera introducido el código PIN en el teclado de la terminal.

De manera paralela a la etapa E4, la plataforma PFG establece un mensaje de solicitud de conexión MDC que incluye la dirección ADTM de la terminal móvil TM, la dirección ADAP del punto de acceso óptimo y el código secreto generado CS con destino al punto de acceso óptimo AP en la red inalámbrica de corto alcance, en la etapa E5. El mensaje de solicitud de conexión MDC está bajo la forma de un paquete IP (Internet Protocol) que transita a través de la Internet RP hacia la red de distribución RD de la red inalámbrica de corto alcance RFP. El código secreto CS extraído del mensaje MDC es memorizado en asociación con la dirección ADTM en el punto de acceso óptimo AP.

En respuesta a la dirección ADAP del punto de acceso óptimo AP extraído del mensaje de confirmación MC recibido por la terminal móvil TM, la misma tiende a conectarse al punto de acceso óptimo AP así identificado invitando al punto de acceso óptimo a autentificarla. En la etapa E6, la terminal móvil TM emite una primera trama T1 que contiene la dirección de la terminal ADTM, la dirección ADAP del punto de acceso óptimo y un indicador de solicitud de conexión y de determinación de la clave de sesión DC.

El punto de acceso óptimo en modo de búsqueda periódica reconoce que la trama T1 le está destinada. La terminal móvil y el punto de acceso determinan entonces cada uno una clave de sesión común KS aplicando al algoritmo de clave de sesión AS la dirección de la terminal móvil ADTM, la dirección ADAP del punto de acceso, el código secreto CS y uno o varios números aleatorios RAND intercambiados entre ellos a través de la red de corto alcance RFP. El código secreto CS utilizado en la terminal móvil es así extraído en el mensaje de confirmación MC, mientras que el código secreto CS utilizado en el punto de acceso AP es aquel extraído del mensaje de solicitud de conexión MDC. La terminal móvil TM y el punto de acceso óptimo AP son así apareados. La clave de sesión KS es memorizada en la terminal y el punto de acceso, y es utilizada, específicamente para la autentificación y un cifrado de datos, solamente hasta la desconexión del punto de acceso AP y de la terminal móvil TM.

La autentificación de la terminal móvil TM es seguidamente desencadenada por el punto de acceso óptimo emitiendo en respuesta a la primera trama T1,

una trama T2 que incluye la dirección de punto de acceso óptimo ADAP, la dirección ADTM de la terminal TM, un número aleatorio RAP generado por el generador pseudo-aleatorio en el punto de acceso y un indicador de solicitud de respuesta DRP hacia la terminal móvil TM, en la etapa E7.

El procedimiento pasa seguidamente a las etapas E8, E9 y E10 relativas a una autentificación propiamente dicho de la terminal móvil TM por el punto de acceso óptimo AP. Con la recepción de la trama T2 con el indicador de solicitud de respuesta, en la etapa E8 la terminal móvil TM aplica el número aleatorio RAP extraído de la trama T2, la clave de sesión KS determinada en la etapa E6 y su dirección ADTM al algoritmo de autentificación AA que produce una respuesta RP1. Igualmente en la etapa E8, el punto de acceso óptimo AP ejecuta una aplicación análoga: RP1 = AA (RAP, KS, ADTM), pero en la cual la clave de sesión es aquella que el mismo ha determinado en la etapa E6 y asociada a la dirección ADTM. Luego la terminal móvil emite, en la etapa E9, una trama T3 que incluye, además de las direcciones ADTM y ADAP, la respuesta RP1 = AA (RAP, KS, ADTM) que ha sido determinada en la terminal móvil. La trama T3 es reconocida por el punto de acceso óptimo AP que en la etapa E10 compara la repuesta RP1 determinada en el punto de acceso óptimo con la respuesta RP1 extraída de la trama recibida T3. Si las respuestas RP1 comparadas son idénticas, el punto de acceso óptimo AP autoriza la abertura de una sesión a través del mismo desde la terminal móvil TM hacia la red de distribución RD y la Internet RP, en la etapa E16.

La clave de sesión KS para esta sesión abierta será utilizada para determinar la clave de sesión de una sesión siguiente entre la terminal móvil TM y el punto de acceso AP si la clave de sesión KS no ha sido mientras tanto borrada con la expiración de una duración a contar desde la memorización de la clave KS, predeterminada por el operador que administra el punto de acceso.

Según una variante más completa relativa a una autentificación mutua, cuando el punto de acceso óptimo AP ha autentificado la terminal móvil TM en la etapa E10, el punto de acceso óptimo AP emite en la etapa E11 una trama T4 que contiene las direcciones ADAP y ADTM y un indicador IA para invitar a la terminal TM a autentificarla.

En respuesta a la trama precedente T4, la terminal móvil TM desencadena la autentificación del punto de acceso óptimo emitiendo una trama T5 destinada al punto de acceso óptimo de dirección ADAP. La trama T5 incluye un número aleatorio RTM generado por el generador pseudo-aleatorio en la terminal móvil y un indicador de solicitud de respuesta DRP, en la etapa E12. A continuación de la trama T5, en la etapa E13 el punto de acceso AP aplica el número aleatorio RTM extraído de la trama T5, la clave de sesión KS determinada en la etapa E6 y su dirección ADAP al algoritmo de autentificación AA que produce una segunda respuesta RP2. Igualmente en la etapa E13, la terminal móvil TM ejecuta una aplicación: RP2 = AA (RTM, KS, ADAP), pero en la cual la clave de sesión es aquella que ha determinado en la etapa E6 y asociada a la dirección ADAP. Luego el punto de acceso óptimo AP emite una trama T6 que incluye, además las direcciones ADAP y ADTM, la respuesta RP2 = AA (RTM, KS, ADAP) que ha sido determinada en el punto de acceso óptimo. La trama T6 es reconocida por la terminal móvil TM quien en la etapa E15 compara la respuesta RP2 determinada en la terminal móvil con la respuesta RP2 extraída de la trama recibida T6. Si las respuestas RP2 comparadas son idénticas, la terminal TM confirma por la emisión de otra trama la abertura de la sesión solicitada en el punto de acceso óptimo AP en la etapa E16.

En una variante, la clave de sesión KS no es determinada separadamente por la terminal móvil TM y el punto de acceso óptimo AP en la etapa E6 sino que es determinada previamente por la plataforma de gestión PFG, en la etapa E3. La plataforma genera de una manera aleatoria una clave de sesión KS del mismo tamaño que aquella según la realización descrita precedentemente.

Sin embargo, a fin de asegurar una coherencia, la plataforma puede contener el algoritmo de clave de sesión AS. Al final de la etapa E3, la plataforma ha seleccionado el punto de acceso óptimo y ha asociado la dirección ADAP del punto de acceso óptimo a la dirección ADTM de la terminal móvil extraída de la demanda RQ, lo que le permite determinar la clave de sesión aplicando las direcciones ADAP y ADTM, el código secreto CS y uno o varios números aleatorios RAND al algoritmo AS, o sea:

KS = AS (ADAP, ADTM, CS, RAND).

En las etapas E4 y E5, la plataforma de gestión PFG introduce la clave de sesión determinada KS en el lugar del código secreto CS en el mensaje de confirmación MC transmitido a la terminal móvil y en el mensaje de solicitud de conexión MDC transmitido al punto de acceso óptimo para que el punto de acceso óptimo y la terminal móvil utilicen la clave de sesión KS para la autentificación E6 a E10 o E6 a E15 y después la sesión abierta en la etapa E16, la etapa E6 no comprendiendo la determinación de clave de sesión KS.

Como es indicado en la etapa E17, si la autentificación de la terminal móvil por el punto de acceso óptimo ha fracasado, es decir si las respuestas RP1 comparadas en la etapa E10 son diferentes, o si la autentificación mutua ha fracasado, es decir si las respuestas RP2 comparadas en la etapa E15 son diferentes, una tentativa de solicitud de abertura de sesión es reiterada procediendo a la ejecución de las etapas E6 a E10 según la realización de autentificación de la terminal por el punto de acceso óptimo, o de las etapas E6 a E15 según la variante de autentificación mutua.

En la práctica, las etapas de solicitud de conexión, de determinación de respuestas y de comparación de respuestas E6 a E10 o E6 a E15 pueden ser reiteradas a lo máximo N veces mientras que las respuestas comparadas RP1 o RP2 son diferentes, N siendo un número predeterminado de iteraciones por ejemplo igual a 3.

Si después de N iteraciones de solicitud de conexión en la etapa E17, la autentificación ha fracasado, es decir las respuestas comparadas son todavía diferentes, el procedimiento puede regresar automáticamente a la etapa E2 a fin de ejecutar las etapas siguientes E3 a E17 relativamente en la dirección ADAP de otro punto de acceso seleccionado según los criterios predeterminados, por ejemplo entre la lista incluida en la demanda RQ, como se indicó en una etapa intermedia E18. La selección de este otro punto de acceso en la lista excluye naturalmente el último punto de acceso óptimo que ha sido precedentemente

seleccionado y para el cual N tentativas de conexión han fracasado. El otro punto de acceso óptimo seleccionado está situado en la zona de cobertura de la terminal móvil TM relativa a la red de corto alcance RFP y puede ser el punto de acceso que presenta el mayor nivel de potencia recibida o la carga más pequeña de tráfico en la lista restante, o aquel que sucede al último punto de acceso óptimo seleccionado en la lista.

Aunque la invención haya sido descrita para una red celular de tipo GSM y una red inalámbrica de corto alcance del tipo Bluetooth, la invención es igualmente aplicable en el contexto de una red de radiocomunicaciones para móviles del tipo UMTS o más generalmente del tipo de tercera generación, y a otras redes inalámbricas de corto alcance por ejemplo del tipo según la norma IEEE 802.11b y según las otras normas siguientes a aquella, es decir para redes igualmente llamadas redes Wi-Fi (Wireless Fidelity).

REIVINDICACIONES

1. Procedimiento de autentificación entre una red inalámbrica de corto alcance (RFP) que tiene puntos de acceso y una terminal móvil (TM) en una red de radiocomunicaciones celular (RC), **caracterizado** porque comprende las etapas siguientes:

- transmisión (E2) de una demanda (RQ) que incluye una dirección (ADTM) de la terminal móvil y una dirección (ADAP) de un punto de acceso (AP) situado en la zona de cobertura de la terminal móvil (TM) relativa a la red de corto alcance, desde la terminal móvil a un medio de gestión (PFG) por medio de la red celular (RC),
- determinación (E3) de un código secreto (CS) por el medio de gestión,
- desde el medio de gestión (PFG), transmisión (E4, E5) de un mensaje de confirmación (MC) que incluye el código secreto y la dirección del punto de acceso extraída de la demanda a la terminal móvil por medio de la red celular y de un mensaje de solicitud de conexión (MDC) que incluye el código secreto y la dirección de la terminal móvil extraída de la demanda al punto de acceso (AP),
- solicitud (E6) de conexión de la terminal móvil al punto de acceso designado por la dirección (ADAP) extraída del mensaje de confirmación (MC) a fin de que la terminal móvil (TM) y el punto de acceso (AP) determinen una clave de sesión (KS) en función de la dirección (ADAP) del punto de acceso, de la dirección (ADTM) de la terminal móvil y del código secreto (CS) extraído del mensaje de confirmación (MC) y del mensaje de solicitud de conexión (MDC), y
- autentificación (E7-E10) de la terminal móvil (TM) por el punto de acceso (AP) en función de la clave de sesión (KS).

2. Procedimiento conforme a la reivindicación 1, según el cual la autentificación de la terminal móvil por el punto de acceso comprende una solicitud (E7) de determinación (E8) desde el punto de acceso de una respuesta (RP1) en función de la clave de sesión (KS) a la terminal móvil que transmite (E9) la respuesta al punto de acceso, por medio de la red de corto alcance, y en el punto de acceso (AP), una determinación (E8) de una respuesta (RP1) en función de la clave de sesión (KS) y una comparación (E10) de las respuestas para autorizar (E16) la abertura de una sesión entre el punto de acceso y la terminal móvil cuando al menos las respuestas comparadas son idénticas.

3. Procedimiento conforme a la reivindicación 1 o 2, que comprende una autentificación (E11-E15) del punto de acceso (AP) por la terminal móvil (TM) en función de la clave de sesión (KS), cuando el punto de acceso ha autentificado la terminal móvil.

4. Procedimiento conforme a la reivindicación 3, según el cual la autentificación del punto de acceso por la terminal móvil comprende una invitación (E11) del punto de acceso trasmitida a la terminal móvil (TM) a fin de que la terminal móvil autentifique el punto de acceso solicitando (E12) al punto de acceso determinar (E13) una segunda respuesta (RP2) en función de la clave de sesión (KS) y transmitir (E14) la segunda respuesta a la terminal móvil por medio de la red de corto alcance (RFP), determinando (E13) una segunda respuesta (RP2) en función de la clave de sesión (KS), y comparando (E15) las segundas respuestas (RP2) a fin de autorizar la abertura de la sesión solamente después de una identidad de las segundas respuestas comparadas en la terminal móvil.

5. Procedimiento conforme a una cualquiera de las reivindicaciones 1 a 4, que comprende a lo máximo un número predeterminado de iteraciones (E17) de las etapas de solicitud de conexión y de autentificación (E6-E10; E6-E15) cuando la autentificación ha fracasado.

6. Procedimiento conforme a la reivindicación 5, que comprende una iteración (E18) de las etapas (E2-E17) enunciadas en la reivindicación 1 relativamente a otro punto de acceso (AP) en la zona de cobertura de la terminal móvil (TM) cuando la autentificación ha fracasado (E17) un número predeterminado de veces.

7. Procedimiento conforme a una cualquiera de las reivindicaciones 1 a 6, que comprende en la terminal móvil (TM) una búsqueda (E1) de un punto de acceso óptimo (AP) que tiene el mayor nivel de potencia recibida por la terminal móvil entre puntos de acceso en la zona de cobertura de la terminal móvil a fin de que la terminal móvil (TM) introduzca la dirección (ADAP) del punto de acceso óptimo en la demanda (RQ).

8. Procedimiento conforme a una cualquiera de las reivindicaciones 1 a 6, que comprende en la terminal móvil (TM) una búsqueda (E1) de puntos de acceso en la zona de cobertura de la terminal móvil a fin de introducir direcciones (ADAP) de los puntos de acceso encontrados en la demanda (RQ), y en el medio de gestión (PFG) una selección (E3) de la dirección (ADAP) de un punto de acceso óptimo (AP) entre las direcciones de punto de acceso extraídas de la demanda (RQ) según un criterio predeterminado para introducir la dirección del punto de acceso óptimo en el mensaje de confirmación (MC) transmitido a la terminal móvil y el mensaje de solicitud de conexión (MDC) transmitido al punto de acceso óptimo (AP).

9. Procedimiento conforme a la reivindicación 8, según el cual el criterio predeterminado es relativo a una comparación de niveles de potencia (NP) de los puntos de acceso encontrados (AP) recibidos por la terminal móvil (TM) y transmitidos en asociación con las direcciones (ADAP) de los puntos de acceso encontrados en la demanda (RQ) a fin de que el medio de gestión (PFG) determine el punto de acceso que tiene el mayor nivel de potencia recibida como punto de acceso óptimo.

10. Procedimiento conforme a la reivindicación 8 o 9, según el cual el criterio predeterminado es relativo a una comparación de cargas de tráfico de los puntos de acceso (AP) encontrados (E1) por la terminal móvil (TM) a fin de que el medio de gestión (PFG) seleccione el punto de acceso que tiene la carga más pequeña como punto de acceso óptimo.

11. Procedimiento conforme a una cualquiera de las reivindicaciones 8 a 10, según el cual el criterio predeterminado es relativo además a una eliminación de las direcciones (ADAP) de los puntos de acceso encontrados (AP) que están situados en el exterior de una zona de localización que incluye la terminal móvil (TM) y definida en la red celular (RC), antes de la selección de la dirección del punto de acceso óptimo.

12. Procedimiento conforme a una cualquiera de las reivindicaciones 1 a 11, **caracterizado** porque el código secreto (CS) determinado por el medio de gestión (PFG) es generado de manera pseudo-aleatoria y tiene una longitud superior a 16 octetos.

13. Procedimiento conforme a una cualquiera de las reivindicaciones 1 a 12, que comprende en el medio de gestión (PFG) una determinación (E3) de la clave de sesión (KS) en el lugar de las determinaciones (E6) de la clave de sesión en la terminal móvil (TM) y el punto de acceso (AP), y una introducción (E4, E5) de la clave de sesión determinada (KS) en el lugar del código secreto en el mensaje de confirmación (MC) y el mensaje de solicitud de conexión (MDC).

14. Sistema de autentificación entre una red inalámbrica de corto alcance (RFP) que tiene puntos de acceso y una terminal móvil (TM) en una red de radiocomunicaciones celular (RC), **caracterizado** porque comprende:

un medio de gestión (PFG) para determinar un código secreto (CS) en respuesta a una demanda (RQ) que incluye la dirección (ADTM) de la terminal móvil y la dirección (ADAP) de un punto de acceso (AP) situado en la zona de cobertura de la terminal móvil (TM) relativa a la red de corto alcance y que es transmitida desde la terminal móvil por medio de red celular (RC), y para transmitir un mensaje de confirmación (MC) que incluye el código secreto y la dirección del punto de acceso extraída de la demanda (RQ) a la terminal móvil (TM) por medio de la red celular (RC) y un mensaje de solicitud de conexión (MDC) que incluye el código secreto y la dirección (ADTM) de la terminal móvil extraída de la demanda en el punto de acceso (AP),

la terminal móvil para solicitar una conexión al punto de acceso (AP) designado por la dirección (ADAP) extraída del mensaje de confirmación (MC) y para determinar una clave de sesión (KS) en función de la dirección (ADAP) del punto de acceso, de la dirección (ADTM) de la terminal móvil y del código secreto (CS) extraído del mensaje de confirmación (MC), y

el punto de acceso (AP) para determinar la clave de sesión (KS) en función de la dirección (ADAP) del punto de acceso, de la dirección (ADTM) de la terminal móvil y del código secreto (CS) extraído del mensaje de solicitud de conexión (MDC) y para autentificar la terminal móvil en función de la clave de sesión (KS).

15. Sistema conforme a la reivindicación 14, **caracterizado** porque el medio de gestión determina él mismo la clave de sesión y la introduce en lugar del código secreto en el mensaje de confirmación (MC) y el mensaje de solicitud de conexión (MDC).

FIG. 1

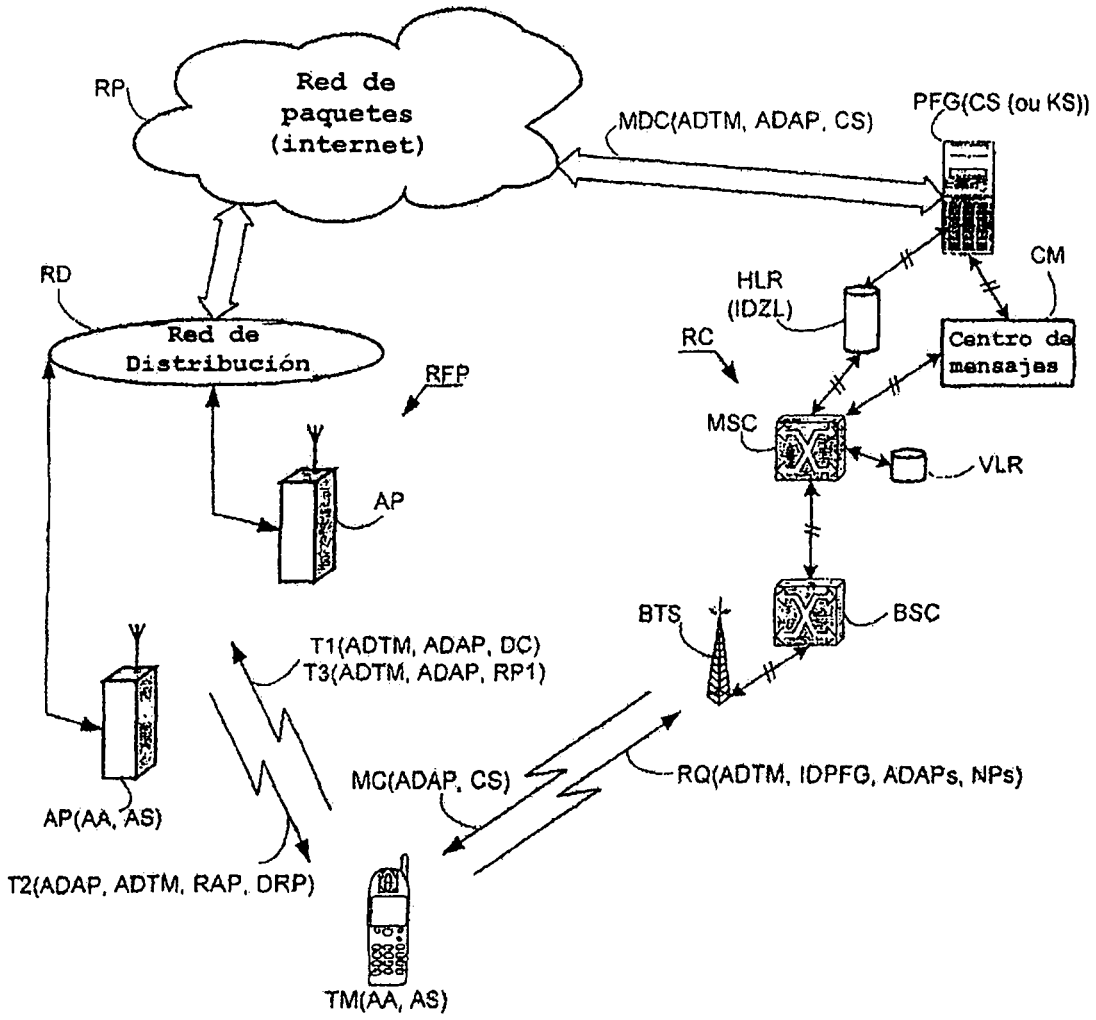
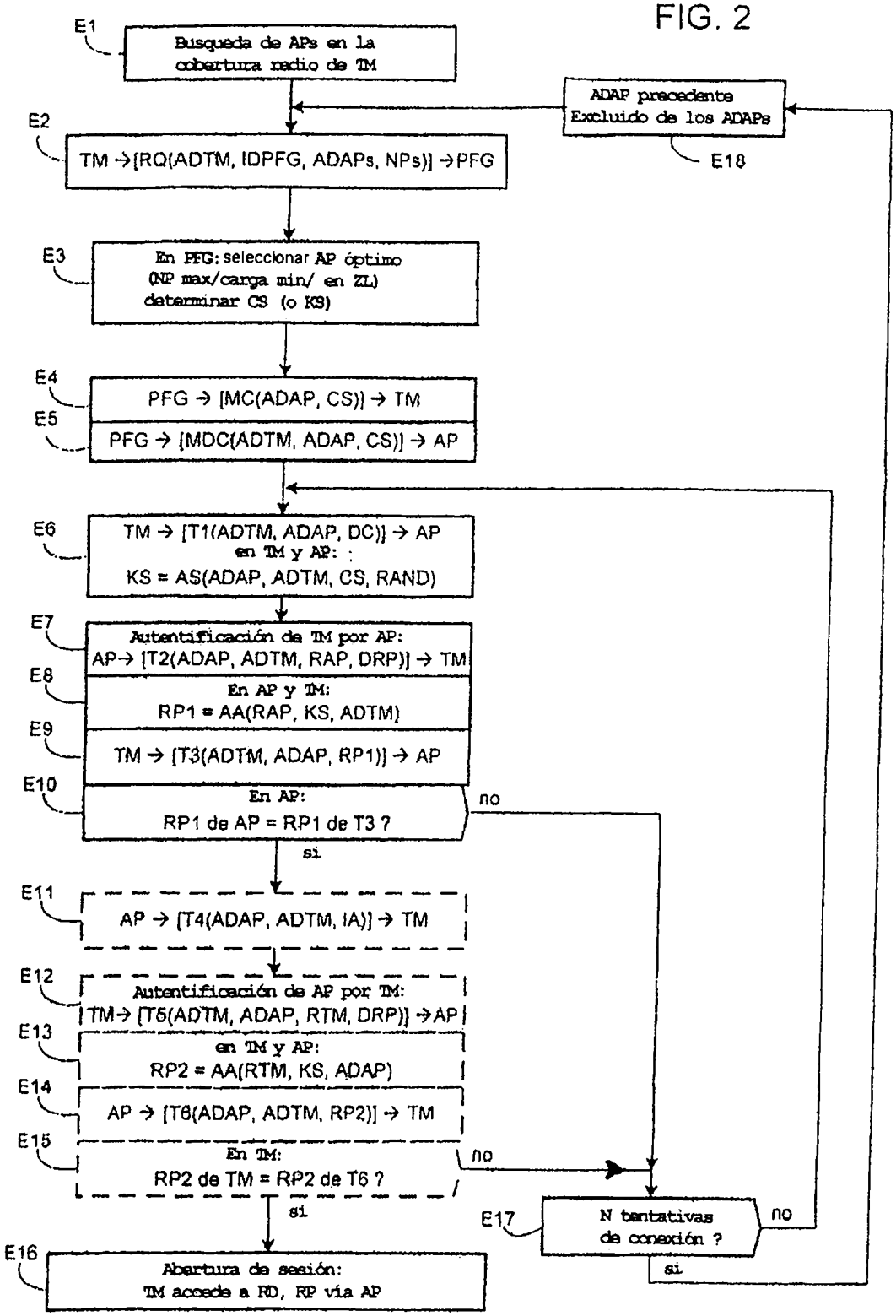

RP
Red de paquetes (internet)
MDC(ADTM, ADAP, CS)
PFG(CS (ou KS))
CM
RD
HLR (IDZL)
RC
Centro de mensajes
Red de Distribución
RFP
MSC
VLR
AP
BTS
BSC
T1(ADTM, ADAP, DC)
T3(ADTM, ADAP, RP1)
MC(ADAP, CS)
RQ(ADTM, IDPFG, ADAPs, NPs)
AP(AA, AS)
T2(ADAP, ADTM, RAP, DRP)
TM(AA, AS)

FIG. 2


E1
Busqueda de APs en la cobertura radio de TM
ADAP precedente Excluido de los ADAPs
E18
E2
TM →{RQ(ADTM, IDPFG, ADAPs, NPs)] →PFG
E3
En PFG: seleccionar AP óptimo (NP max/carga min/ en ZL) determinar CS (o KS)
E4
PFG → [MC(ADAP, CS)] → TM
E5
PFG → [MDC(ADTM, ADAP, CS)] → AP
E6
TM → [T1(ADTM, ADAP, DC)] → AP
en TM y AP: :
KS = AS(ADAP, ADTM, CS, RAND)
E7
Autentificación de TM por AP:
AP→ [T2(ADAP, ADTM, RAP, DRP)] → TM
E8
En AP y TM:
RP1 = AA(RAP, KS, ADTM)
E9
TM → [T3(ADTM, ADAP, RP1)] → AP
E10
En AP:
RP1 de AP = RP1 de T3 ?
no
si
E11
AP → [T4(ADAP, ADTM, IA)] → TM
E12
Autentificación de AP por TM:
TM→ [T5(ADTM, ADAP, RTM, DRP)] →AP
E13
en TM y AP:
RP2 = AA(RTM, KS, ADAP)
E14
AP → [T6(ADAP, ADTM, RP2)] → TM
E15
En TM:
RP2 de TM = RP2 de T6 ?
no
si
E17
N tentativas de conexión ?
no
si
E16
Abertura de sesión:
TM accede a RD, RP vía AP