(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 396 799**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/10 (2009.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.09.2008 E 08835932 (8)**

(97) Fecha y número de publicación de la concesión europea: **31.10.2012 EP 2208376**

(54) Título: **Procedimiento y aparatos para autenticar unidades móviles unidas a una femtocélula en comunicación con una red central segura, tal como un IMS**

(30) Prioridad:

04.10.2007 US 997579 P
10.01.2008 US 972262

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.02.2013

(73) Titular/es:

ALCATEL LUCENT (100.0%)
3, avenue Octave Gréard
75007 Paris, FR

(72) Inventor/es:

MORGAN, TODD CARTWRIGHT;
PATEL, SARVAR y
THOMPSON, ROBIN JEFFREY

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y aparatos para autenticar unidades móviles unidas a una femtocélula en comunicación con una red central segura, tal como un IMS

Antecedentes de la invención

1. Campo de la invención

La presente invención versa, en general, acerca de sistemas de comunicaciones y, más en particular, acerca de sistemas de comunicaciones inalámbricas.

2. Descripción de la técnica relacionada

Los sistemas convencionales de comunicaciones inalámbricas usan una red de estaciones base para proporcionar una conectividad inalámbrica con una o más unidades móviles. En algunos casos, las unidades clave pueden iniciar una comunicación inalámbrica con una o más estaciones base en la red; por ejemplo, cuando el usuario de la unidad móvil desease iniciar una llamada de voz o datos. Alternativamente, la red puede iniciar el enlace de comunicaciones inalámbricas con la unidad móvil. Por ejemplo, en comunicaciones inalámbricas jerárquicas convencionales, un servidor transmite voz y/o datos destinados para una unidad móvil diana a un elemento central tal como un controlador de red de radio (RNC). El RNC puede transmitir entonces mensajes de notificación a la unidad móvil diana a través de una o más estaciones base. La unidad móvil diana puede establecer un enlace inalámbrico a una o más de las estaciones base en respuesta a la recepción de la notificación del sistema de comunicaciones inalámbricas. Una función de gestión de recursos de radio dentro del RNC recibe la voz y/o los datos y coordina los recursos de radio y tiempo usados por el conjunto de estaciones base para transmitir la información a la unidad móvil diana. La función de gestión de recursos de radio puede llevar a cabo un control de alta resolución para asignar y liberar recursos para la transmisión de radiodifusión en un conjunto de estaciones base.

Se establecen comunicaciones seguras en un sistema jerárquico convencional, tal como un sistema CDMA, con base en información secreta (por ejemplo, una clave de autenticación) conocida únicamente a la unidad móvil y una entidad segura en la red. El HLR/AuC y la unidad móvil pueden derivar datos secretos compartidos (SSD) de la clave de autenticación (AK), por ejemplo usando el algoritmo CAVE. La AK es una clave secreta primaria de 64 bits conocida únicamente por la estación móvil y el HLR/AuC. Esta clave nunca es compartida con socios de itinerancia. La AK puede usarse para generar los SSD, que son una clave secundaria de 128 bits que puede ser calculada usando el algoritmo CAVE y que puede ser compartida con socios de itinerancia. Durante la autenticación, tanto el HLR/AuC como la unidad móvil calculan una respuesta de autenticación por separado e independientemente usando entradas compartidas, tales como los SSD, el número de serie electrónico (ESN), el número de identidad móvil (MIN) y un número aleatorio compartido (RAND). Si los resultados calculados independientemente coinciden, se aprueba la autenticación y se permite que la unidad móvil se dé de alta en la red.

La AK o los SSD pueden ser usados para autenticar unidades móviles que están dadas de alta en la red. Por ejemplo, una estación base puede generar periódicamente un número aleatorio (RAND) y transmitir el RAND. Las unidades móviles que reciben el RAND transmitido calculan una salida de algoritmo de autenticación (AUT) usando las entradas, incluyendo el RAND y la AK o los SSD. A veces se denomina par a la AUT y al RAND asociado (o a porciones seleccionadas del RAND). La estación móvil puede transmitir entonces el par AUT/RAND a la estación base, que puede pasar a continuación esta información, por medio de la red, al HLR/AuC. El HLR/AuC usa el algoritmo de autenticación, el valor almacenado de la AK o los SSD, otros datos correspondientes a cada unidad móvil y el RAND para calcular el valor esperado de AUT. Si este valor coincide con el valor transmitido por la unidad móvil, la unidad móvil es autenticada. La estación base cambia frecuentemente el valor de RAND para garantizar que el valor AUT sea reciente y reducir la posibilidad de que resultados AUT/RAND generados previamente puedan ser capturados monitorizando la interfaz aérea y reproducidos por una unidad móvil fraudulenta o un emulador de unidad móvil. Se considera que esta técnica es razonablemente fiable, al menos en parte, debido a que las estaciones base son típicamente dispositivos seguros que están bajo el control de proveedores de comunicaciones inalámbricas.

Una alternativa a la arquitectura de red jerárquica convencional es una arquitectura distribuida que incluya una red de puntos de acceso, tales como dispositivos de encaminamiento de estaciones base, que implementen una funcionalidad de red de comunicaciones distribuida. Por ejemplo, cada dispositivo de encaminamiento estación base puede combinar funciones de RNC y/o PDSN en una sola entidad que gestiones radioenlaces entre una o más unidades móviles y una red exterior, tal como Internet. En comparación con las redes jerárquicas, las arquitecturas distribuidas tienen el potencial de reducir los costes y/o la complejidad del despliegue de la red, así como el coste y/o la complejidad de añadir puntos adicionales de acceso inalámbrico, por ejemplo dispositivos de encaminamiento de estaciones base, para expandir la cobertura de una red existente. Las redes distribuidas también puede reducir (con respecto a las redes jerárquicas) los retardos experimentados por los usuarios, porque pueden reducirse o eliminarse los retardos debidos a la puesta en memoria temporal de paquetes en el RNC y el PDSN de las redes jerárquicas.

Al menos en parte, debido al coste y la complejidad reducidos del despliegue de un dispositivo de encaminamiento de estación base, los dispositivos de encaminamiento de estaciones base pueden ser desplegados en emplazamientos que son poco prácticos para estaciones base convencionales. Por ejemplo, puede desplegarse un dispositivo de encaminamiento de estación base en una vivienda o un edificio para proporcionar conectividad inalámbrica a los ocupantes o los residentes del edificio. Típicamente, los dispositivos de encaminamiento de estaciones base desplegados en una residencia son denominados dispositivos propios de encaminamiento de estaciones base o femtocélulas, porque están concebidos para proporcionar conectividad inalámbrica a una zona mucho más pequeña (por ejemplo, una femtocélula) que abarca una vivienda. Sin embargo, típicamente, la funcionalidad en una femtocélula es muy similar a la funcionalidad implementada en un dispositivo de encaminamiento convencional de estación base que esté concebido para proporcionar conectividad inalámbrica a una macrocélula que pueda abarcar un área de aproximadamente algunos kilómetros cuadrados. Una diferencia importante entre una femtocélula y un dispositivo de encaminamiento convencional de estación base es que los dispositivos propios de encaminamiento de estaciones base están diseñados para ser dispositivos económicos de conexión y uso inmediato que puedan ser comprados en puntos de venta al público e instalados con facilidad por una persona sin experiencia.

Típicamente, las femtocélulas no incluyen caros chips de seguridad para almacenar información que puedan ser usados para establecer comunicaciones seguras entre la femtocélula y las unidades móviles. Además, las femtocélulas están pensadas para ser desplegadas en emplazamientos no seguros, tales como el hogar o el negocio de una persona. En consecuencia, no se considera que las femtocélulas sean emplazamientos de confianza para almacenar claves secretas u otra información que pueda ser usada para autenticar unidades móviles. Por lo tanto, una femtocélula puede ser modificada para representar de manera fraudulenta a una unidad móvil si las femtocélulas están configuradas para generar los números aleatorios RAND usados para autenticar unidades móviles. Por ejemplo, una femtocélula ilegítima puede interceptar un par AUT/RAND válido transmitido entre una unidad móvil legítima y una estación base legítima. La femtocélula ilegítima puede emular entonces a la unidad móvil legítima usando el par AUT/RAND interceptado. Dado que la femtocélula es responsable de generar valores RAND, la red no puede determinar si el par AUT/RAND transmitido por la femtocélula ilegítima corresponde o no con un valor reciente de RAND.

Naslund et al. (publicación de solicitud de patente estadounidense nº 2006/0288407) describen un dispositivo de seguridad inviolable que implementa el protocolo de autenticación y concordancia de claves.

Resumen de la invención

La presente invención está dirigida a abordar los efectos de uno o más de los problemas presentados en lo que antecede. Lo que sigue presenta un resumen simplificado de la invención para proporcionar una comprensión básica de algunos aspectos de la invención. Este resumen no es una visión general exhaustiva de la invención. No se pretende identificar elementos clave o críticos de la invención ni delinear el alcance de la invención. Su único propósito es presentar algunos conceptos de forma simplificada como preludio de la descripción más detallada que se expone después.

En una realización de la presente invención, se proporciona un procedimiento que implica una femtocélula en comunicación con una red central segura, tal como una red de subsistemas multimedia con protocolo de Internet (IMS). El procedimiento incluye recibir de la femtocélula y en una primera entidad segura en la red IMS información que indica un número aleatorio. El procedimiento también incluye recibir una respuesta de autenticación calculada por una unidad móvil basada en el número aleatorio y la primera clave conocida por la unidad móvil y no conocida por la femtocélula. El procedimiento incluye también determinar, en la primera entidad segura, que el número aleatorio es un número aleatorio legítimo proporcionado a la femtocélula por la red IMS.

En una realización de la presente invención, se proporciona un procedimiento que implica una femtocélula en comunicación con una red central segura, tal como una red de subsistemas multimedia con protocolo de Internet (IMS). El procedimiento incluye recibir de la femtocélula y en una primera entidad segura en la red IMS información que indica un número aleatorio. El procedimiento también incluye proporcionar información que indica una respuesta de autenticación calculada por una unidad móvil basada en el número aleatorio y la primera clave conocida por la unidad móvil y no conocida por la femtocélula. La unidad móvil proporciona la información en respuesta a un reto global transmitido por la femtocélula. El procedimiento también incluye recibir, de la primera entidad segura, al menos una segunda clave determinada basada en el número aleatorio de la primera clave. La segunda clave se recibe en respuesta a la determinación por parte de la de la primera entidad segura de que el número aleatorio es un número aleatorio legítimo proporcionado a la a la femtocélula por la red IMS.

Breve descripción de los dibujos

La invención puede ser entendida con referencia a la siguiente descripción tomada en conjunto con los dibujos adjuntos, en los que números de referencia similares identifican elementos similares, y en los que:

la Figura 1 ilustra conceptualmente una realización ejemplar de un sistema de comunicaciones inalámbricas según la presente invención;

la Figura 2 ilustra conceptualmente una realización ejemplar de un procedimiento de uso de un reto global para autenticar una unidad móvil que está en comunicación con una femtocélula según la presente invención;
la Figura 3 ilustra conceptualmente una primera realización ejemplar de un procedimiento de provisión de números aleatorios a una femtocélula según la presente invención;
la Figura 4 ilustra conceptualmente una segunda realización ejemplar de un procedimiento de provisión de números aleatorios a una femtocélula según la presente invención; y
la Figura 5 ilustra conceptualmente una tercera realización ejemplar de un procedimiento de provisión de números aleatorios a una femtocélula según la presente invención.

Aunque la invención es susceptible de diversas modificaciones y de formas alternativas, se muestran realizaciones específicas de la misma a título de ejemplo en los dibujos y son descritas en detalle en el presente documento. Sin embargo, debería entenderse que no se pretende que la descripción del presente documento de realizaciones específicas limite la invención a las formas particulares dadas a conocer, sino que, al contrario, la intención es abarcar todas las modificaciones, los equivalentes y las alternativas que se encuentren dentro del alcance de la invención tal como es definida en las reivindicaciones adjuntas.

Descripción detallada de realizaciones específicas

En lo que sigue se describen realizaciones ilustrativas de la invención. En aras de la claridad, no se describen en esta memoria todas las características de una implementación real. Se apreciará, por supuesto, que en el desarrollo de cualquier realización real tal, deberían adoptarse numerosas decisiones específicas a la implementación para lograr las metas específicas de los diseñadores, tales como conformidad con limitaciones relativas al sistema y relativas al negocio, que variarán de una implementación a otra. Además, se apreciará que tal esfuerzo de desarrollo podría ser complejo y llevar mucho tiempo, pero sería, no obstante, una empresa rutinaria para las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente divulgación.

La presente invención será descrita ahora con referencia a las figuras adjuntas. En los dibujos se representan esquemáticamente diversas estructuras, diversos sistemas y dispositivos con fines de explicación únicamente y para no embrollar la presente invención con detalles que son bien conocidos para los expertos en la técnica. No obstante, los dibujos adjuntos se incluyen para describir y explicar ejemplos ilustrativos de la presente invención. Debería entenderse e interpretarse que las palabras y las frases usadas en el presente documento tienen un significado coherente con la comprensión de esas palabras y esas frases por parte de los expertos en la técnica relevante. No se pretende que haya implicada ninguna definición especial de un término o una frase, es decir, una definición que sea diferente del significado ordinario y habitual según entienden los expertos en la técnica, por el uso coherente del término o de la frase en el presente documento. Cuando se pretenda que un término o una frase tenga un significado especial, es decir, un significado distinto del entendido por expertos en la técnica, tal definición especial será formulada expresamente en la memoria de una manera definitoria que proporcione de manera directa e inequívoca la definición especial para el término o la frase.

La Figura 1 ilustra conceptualmente una realización ejemplar de un sistema 100 de comunicaciones inalámbricas. En la realización ilustrada, el sistema 100 de comunicaciones inalámbricas incluye una o más femtocélulas 105 para proporcionar conectividad inalámbrica. Las femtocélulas 105 pueden proporcionar conectividad inalámbrica según estándares y/o protocolos que incluyen, sin limitación, estándares y/o protocolos de acceso múltiple por división de código (CDMA), estándares y/o protocolos del servicio universal de telecomunicaciones móviles (UMTS), estándares y/o protocolos del sistema global para comunicaciones móviles (GSM), estándares y/o protocolos WiMAX, estándares y/o protocolos IEEE y similares. Además, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente divulgación deberían apreciar que la presente invención no está limitada al uso de femtocélulas 105 para proporcionar conectividad inalámbrica. En realizaciones alternativas, pueden usarse dispositivos tales como estaciones base, dispositivos de encaminamiento de estaciones base, puntos de acceso, redes de acceso y similares para proporcionar conectividad inalámbrica en el sistema 100 de comunicaciones inalámbricas.

La femtocélula 105 está concebida para proporcionar cobertura inalámbrica a una zona que abarque aproximadamente un edificio que incluya una o más unidades móviles 110 a las que se conceda acceso a la femtocélula 105. Las unidades móviles 110 pueden ser dadas de alta en la femtocélula 105 usando una variedad de técnicas, incluyendo hacer que un usuario introduzca, a través de una página electrónica, una identidad internacional de abonado móvil (IMSI) para las unidades móviles 110 dadas de alta, usando un protocolo de enlace entre las unidades móviles 110 y la femtocélula 105 y similares. A continuación, se pone a disposición de la femtocélula 105 una lista de las unidades móviles 110 dadas de alta. En una realización, la femtocélula 105 contiene una base de datos que incluye los valores IMSI de las unidades móviles 110 dadas de alta. En la realización ilustrada, la unidad móvil 110 es una unidad móvil 110 inalámbrica basada en el acceso múltiple por división de código (CDMA). Sin embargo, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente divulgación deberían apreciar que la presente invención no está limitada a unidades móviles 110 basadas en CDMA.

La femtocélula 105 proporciona acceso al sistema 100 de comunicaciones inalámbricas por medio de una red central segura 115. En la realización ilustrada, la red central segura es una red 115 de subsistemas multimedia con

protocolo de internet (IMS) (indicada por la caja de trazo discontinua). Sin embargo, también pueden usarse otros tipos de redes centrales seguras 115. Por ejemplo, podrían implementarse femtocélulas 105 usando otros tipos de tecnologías de red central, tal como tecnologías de red central basadas en IP, como el protocolo de inicio de sesión (SIP). En diversas realizaciones alternativas la femtocélula 105 puede estar acoplada a la red IMS 115 mediante varios elementos funcionales. Por ejemplo, en la Figura 1 la femtocélula 105 está acoplada a una línea digital de abonado (DSL) o una red 120 de módem de cable, que está acoplada a una pasarela 125 de femtorred. Puede acoplarse un servidor 130 de administración y mantenimiento de operaciones (OA & M) a la pasarela 125 de femtorred y puede usarse para establecer comunicaciones entre la femtocélula 105 y una red 135 de protocolo de Internet (IP) por medio de una pasarela 125 de femtorred (FNG). Sin embargo, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente divulgación deberían apreciar que no se pretende que esta realización ejemplar limite la presente invención a esta arquitectura particular de red.

La red IMS 115 es una red basada en el protocolo de inicio de sesión (SIP), que soporta la comunicación a través de Internet por parte de muchos tipos de terminales. Por ejemplo, estos terminales (tales como la unidad móvil 110 combinada con la femtocélula 105) pueden usar el protocolo de voz sobre Internet (VoIP) y otros procedimientos para transferir datos y voz en aplicaciones de tiempo real en la red IP 135. La red IMS 115 incluye un servidor local 140 de abonados (HSS), que es una base de datos maestra de usuarios que da soporte a las entidades de la red IMS que pueden gestionar llamadas. El HSS 140 puede contener información relacionada con abonos (perfiles de usuarios), llevar a cabo una autenticación y la autenticación del usuario, y pueden proporcionar información sobre la ubicación física del usuario. La red IMS 115 puede incluir también una o más entidades 145 de función de control de una sesión de llamadas (CSCF) que se usan para procesar paquetes de señalización SIP en la red IMS 115. Aunque en la Figura 1 las entidades 145 de CSCF son mostradas como un solo bloque funcional, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente divulgación deberían apreciar que las entidades 145 de CSCF pueden incluir múltiples entidades, tales como una CSCF servidora, una CSCF representante, una CSCF interrogadora y similares, que pueden ser implementadas en una o más entidades funcionales y/o físicas distintas. Se usa un servidor 150 de aplicaciones de gestión de la movilidad (MMAS) para coordinar y gestionar las funciones relativas a la movilidad de las unidades móviles 110.

La red IMS 115 también da soporte a la provisión de números aleatorios a la femtocélula 105 y a otras estaciones base o femtocélulas dentro del sistema 100 de comunicaciones inalámbricas. Estos números aleatorios pueden usarse para retos globales de las unidades móviles. Por ejemplo, el reto global puede incluir un número aleatorio transmitido continuamente por un canal administrativo. En cada acceso al sistema, se requiere de las unidades móviles que calculen una respuesta usando datos secretos (SSD o AK) y que devuelvan al sistema la respuesta y al menos una porción del número aleatorio para su verificación. Los retos globales son distintos de los retos únicos, que son retos presentados una sola vez que se dirigen a una unidad móvil y que se forman con base en un número aleatorio y una respuesta esperada generada para el reto único. En la realización ilustrada, la red IMS 115 incluye un servidor 155 de números aleatorios (MMAS-RAND) que genera los números aleatorios y los proporciona a la femtocélula 105. Por ejemplo, el servidor 155 de números aleatorios puede generar periódicamente números aleatorios cada 10 minutos y luego distribuirlos a la femtocélula 105 para su uso en la autenticación de unidades móviles 110. Alternativamente, el servidor 155 de números aleatorios puede generar información germinal y distribuir esta información a la femtocélula 105, y el MMAS 150 puede entonces usar la información germinal para generar periódicamente los números aleatorios. Por ejemplo, la información germinal puede ser generada una vez al día y luego la femtocélula 105 puede usar esta información (con otra información en la femtocélula 105 y también conocida al MMAS 150) para generar nuevos números aleatorios cada 10 minutos. Cada femtocélula 105 puede abonarse al servicio de números aleatorios proporcionado por el servidor 155 de número aleatorios para que reciba los números aleatorios generados. El MMAS 150 también puede estar abonado al servicio de números aleatorios para recibir una notificación cada vez que cambie el número aleatorio.

La femtocélula 105 usa el número aleatorio proporcionado para autenticar la unidad móvil 110 y para establecer un enlace seguro de comunicaciones por la interfaz aérea con la unidad móvil 110. Sin embargo, la femtocélula 105 puede no ser un elemento de confianza del sistema 100 de comunicaciones inalámbricas. Por ejemplo, la femtocélula 105 puede no ser físicamente segura, porque puede estar situada en la vivienda o el negocio de un usuario. En consecuencia, el proveedor del servicio puede ser incapaz de garantizar que la femtocélula 105 no pueda ser objeto de acceso por un usuario no autorizado que pueda intentar modificar o piratear la femtocélula 105. Además, la femtocélula 105 puede ser susceptible de piratería informática en una red. Por ejemplo, el usuario de la femtocélula 105 puede no proporcionar suficiente protección de cortafuegos, protección antivirus y similares, lo que puede permitir que usuarios no autorizados pirateen informáticamente la femtocélula 105. Dado que la femtocélula 105 no es un elemento de confianza del sistema 100, la femtocélula 105 puede ser usada para representar fraudulentamente a la unidad móvil 110. En consecuencia, la red IMS 115 puede verificar periódicamente que la información de autenticación y el número aleatorio proporcionados por la femtocélula 105 han sido formados por una unidad móvil 110 que tiene acceso a un número aleatorio válido proporcionado por el MMAS-RAND 155. Una vez que se han validado el resultado de la autenticación y el número aleatorio, la red IMS 115 puede proporcionar a la femtocélula 105 servicios de procesamiento de llamadas y/o información de seguridad, tal como una o más claves generadas en un registro propio de localización/centro de autenticación (HLR/AuC) 160.

Las entidades de la red IMS 115 (y de fuera de esta red) que se usan para verificar el RAND son entidades de confianza o seguras. Por ejemplo, el MMAS 150, el MMAS-RAND 155 y el HLR/AuC 160 pueden ser físicamente

seguros porque estén situado en un edificio que esté bajo el control del proveedor del servicio. En consecuencia, el proveedor del servicio puede ser capaz de garantizar que el MMAS 150, el MMAS-RAND 155 y/o el HLR/AuC 160 no puedan ser objeto de acceso por un usuario no autorizado que pueda intentar modificar o piratear informáticamente la femtocélula 105. Además, el MMAS 150, el el MMAS-RAND 155 y/o el HLR/AuC 160 pueden ser protegidos del pirateo informático usando una protección de cortafuegos, una protección antivirus y similares, lo que puede evitar el acceso no autorizado al MMAS 150, al MMAS-RAND 155 y al HLR/AuC 160. En la realización ilustrada, la pasarela 125 de la femtorred (FNG) también es una entidad de confianza y/o segura.

La Figura 2 ilustra conceptualmente una realización ejemplar de un procedimiento 200 de uso de un reto global para autenticar una unidad móvil que está en comunicación con una femtocélula. En la realización ilustrada, un agente de usuario SIP en la femtocélula (FEMTO) se da de alta en la red IMS comunicándose con las entidades CSCF apropiadas, tal como se indica con la flecha 205 de dos puntas. En la técnica se conocen técnicas para darse de alta en la red IMS y, en aras de la claridad, no se expondrán adicionalmente en el presente documento. La femtocélula también se da de alta (tal como se indica con la flecha 210) en el servidor de números aleatorios (RAND) para que pueda recibir números aleatorios que puedan ser usados en retos globales presentados a las unidades móviles (UE) el sistema de comunicaciones inalámbricas. Por ejemplo, la femtocélula puede ser configurada para que se abone (en 210) al servicio de números aleatorios al ser invocada y/o al arrancar. Una vez que la femtocélula se ha dado de alta (en 210) en el servidor de números aleatorios, el servidor de números aleatorios puede proporcionar periódicamente números aleatorios (o información que puede usarse para generar los números aleatorios) a la femtocélula, según se indica por medio de la flecha 215.

El servidor de aplicaciones de gestión de la movilidad (MMAS) de la red IMS también puede abonarse (en 220) al servidor de números aleatorios para que se le notifique (en 225) cuándo han cambiado los números aleatorios proporcionados a la femtocélula. En algunas realizaciones, el sistema de comunicaciones inalámbricas puede incluir múltiples entidades MMAS que actúan como nodos de verificación de los números aleatorios. En estas realizaciones, las múltiples entidades MMAS también pueden abonarse al servicio de números aleatorios para que se las mantenga informadas de los números aleatorios legítimos que pueden ser usados para el propósito del algoritmo de autenticación. En este punto del procedimiento (indicado por la línea discontinua 230), el servidor de números aleatorios proporciona periódicamente (en 215, 225) información de números aleatorios tanto a la femtocélula como al servidor o a los servidores de aplicaciones de gestión de la movilidad. El periodo de tiempo para proporcionar los números aleatorios puede seleccionarse con base en las necesidades contrapuestas de números aleatorios “nuevos” y una baja sobrecarga de la red.

La femtocélula radiodifunde periódicamente (en 235) un reto global de autenticación a las unidades móviles (MU) en el sistema de comunicaciones inalámbricas. En la realización ilustrada, se radiodifunde el reto global de autenticación (en 235) usando un mensaje administrativo que incluye el valor actual del número aleatorio que ha sido proporcionado a la femtocélula. Cuando una unidad móvil intenta acceder a la red, la unidad móvil transmite (en 240) a la femtocélula un mensaje de autenticación. En la realización ilustrada, la unidad móvil transmite (en 240) el resultado de un algoritmo de autenticación, tal como un algoritmo CAVE, que se lleva a cabo usando el número aleatorio proporcionado (RAND) como una de las entradas. La unidad móvil también puede transmitir (en 240) información que indica el número aleatorio que se usó para obtener la salida del algoritmo de autenticación (AUTHR). La combinación de la salida del algoritmo de autenticación y el número aleatorio puede denominarse par AUTHR/RAND. La femtocélula puede transmitir entonces (en 245) un mensaje que incluye el par CSCF a la CSCF, la cual puede remitir el mensaje (en 250) al MMAS. Por ejemplo, la femtocélula puede traducir el mensaje de origen a un mensaje de INVITACIÓN SIP que incluya los parámetros de autenticación en una cabecera SIP. El mensaje de INVITACIÓN SIP puede ser transmitido entonces (at 245, 250) al MMAS.

El MMAS verifica (en 255) el valor del RAND indicado en los parámetros de autenticación recibidos de la femtocélula. En una realización, el MMAS actúa como una función de interconexión entre la red IMS y el HLR/AuC. Por lo tanto, el MMAS puede traducir los parámetros de autenticación recibidos de la femtocélula a una solicitud de autenticación de mensaje ANSI 41 MAP que es transmitida (en 260) al HLR/AuC, el cual responde (en 265) con información que indica si el procedimiento de autenticación ha tenido éxito o ha fallado. En la técnica se conocen técnicas para determinar el éxito o el fracaso del procedimiento de autenticación llevado a cabo en el HLR/AuC con base en la solicitud de autenticación de mensaje ANSI 41 MAP, y, en aras de la claridad, no serán presentadas adicionalmente en el presente documento. El MMAS puede usar entonces la respuesta del HLR/AuC para determinar el éxito o el fracaso del procedimiento de autenticación. Si la autenticación tiene éxito, se permite que la llamada prosiga. En la realización ilustrada, el MMAS remite un mensaje de respuesta desde el extremo lejano e incluye las claves de privacidad de voz proporcionadas por el HLR/AuC como parte del procedimiento de autenticación. Por ejemplo, el MMAS puede incluir las claves de seguridad en un mensaje SIP tal como un mensaje 18x o un mensaje 200 OK y puede transmitir (en 270, 275) este mensaje a la femtocélula en respuesta al mensaje de INVITACIÓN SIP. La femtocélula puede usar entonces la información de claves de seguridad para establecer (en 280) un enlace seguro y/o privado entre la unidad móvil y la femtocélula.

La Figura 3 ilustra conceptualmente una primera realización ejemplar de un procedimiento 300 de provisión de números aleatorios a una femtocélula. En la realización ilustrada, la femtocélula (FEMTO) ya se ha dado de alta en la red IMS. La femtocélula (o un agente de usuario dentro de la femtocélula) está configurada para abonarse automáticamente a un servidor de números aleatorios con base en la red. Por lo tanto, en la realización ilustrada, la

femtocélula transmite (en 305) un mensaje de abono a la función CSCF delegada (P-CSCF). El mensaje de abono incluye información que solicita el abono al servicio de números aleatorios proporcionado por el servidor de números aleatorios (RAND). Por ejemplo, el mensaje de abono puede ser un mensaje SUBSCRIBE que se forme según el protocolo SIP definido en la RFC 3265. La P-CSCF remite (en 310) esta información a la CSCF servidora (S-CSCF), la cual, a su vez, remite (en 315) el mensaje al servidor de números aleatorios.

El servidor de números aleatorios puede entonces devolver (en 320) un mensaje que indique el abono con éxito de la femtocélula al servicio de números aleatorios. En la realización ilustrada, el mensaje devuelto (en 320) por el servidor de números aleatorios es una respuesta 200-OK que indica que se recibió el mensaje SUBSCRIBE. Sin embargo, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente divulgación deberían apreciar que, alternativamente, pueden usarse otros mensajes para indicar la recepción con éxito del mensaje de abono. El mensaje devuelto puede ser proporcionado (en 320) a la S-CSCF, la cual puede transmitir (en 325) este mensaje a la P-CSCF. El mensaje puede ser transmitido entonces (en 330) a la femtocélula para que la femtocélula sepa que se ha abonado con éxito al servicio de números aleatorios proporcionado por el servidor de números aleatorios.

El servidor de números aleatorios puede transmitir (en 335) un mensaje de notificación a la femtocélula que incluye el valor actual del número aleatorio que debería usarse para los retos globales. En la realización ilustrada, el servidor de números aleatorios transmite (en 335) un mensaje NOTIFY, que es una respuesta automática al mensaje SUBSCRIBE que contiene el valor actual del número aleatorio (RAND). Puede proporcionarse el mensaje NOTIFY (en 335) a la S-CSCF, la cual puede transmitir (en 340) este mensaje a la P-CSCF. El mensaje puede ser transmitido entonces (en 345) a la femtocélula para que la femtocélula conozca el valor actual del número aleatorio que ha de usarse para los retos globales. Tras la recepción del mensaje NOTIFY, la femtocélula puede proporcionar una confirmación que indique que ha recibido el mensaje NOTIFY. En la realización ilustrada, la femtocélula proporciona (en 350) un mensaje 200-OK para confirmar la recepción del mensaje NOTIFY. El mensaje 200-OK puede ser transmitido (en 350) desde la femtocélula a la P-CSCF, la cual puede remitir (en 355) este mensaje a la S-CSCF para su transmisión final (en 360) al servidor de números aleatorios.

El servidor de números aleatorios genera periódicamente nuevos números aleatorios y envía (en 365) información que indica los nuevos números aleatorios a cada femtocélula abonada. En la realización ilustrada, el servidor de números aleatorios transmite (en 365) a cada femtocélula un mensaje NOTIFY que incluye el nuevo número aleatorio. El servidor de números aleatorios también transmite (en 370) información que indica el valor actual del número aleatorio a uno o más servidores MMAS que pueden haberse abonado también al servicio de números aleatorios.

La Figura 4 ilustra conceptualmente una segunda realización ejemplar de un procedimiento 400 de provisión de números aleatorios a una femtocélula. Las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente divulgación deberían apreciar que no se pretende que la segunda realización ejemplar sea independiente de las otras técnicas descritas en el presente documento y que aspectos de la segunda realización ejemplar pueden incorporarse en otros procedimientos y/o algoritmos descritos en el presente documento. En la realización ilustrada, el sistema de comunicaciones inalámbricas incluye una pasarela de femtorred (FNG), que proporciona una pasarela de seguridad para conexiones procedentes de femtocélulas situadas en los hogares de los usuarios en la Internet pública. La pasarela de la femtorred puede abonarse a un servicio de notificación de la actualización de la base de datos proporcionado por el servidor de números aleatorios (RAND). Por ejemplo, la pasarela de la femtorred puede proporcionar un mensaje que solicite el abono al servicio de números aleatorios usando un mensaje de solicitud de notificaciones de abono formado según el protocolo Diámetro-sh según se define en 3GPP2 X.P0013.11. Este mensaje puede ser transmitido (en 405) desde la pasarela de la femtorred al servidor de números aleatorios, el cual puede responder con un mensaje que incluya el valor actual del número aleatorio usado para los retos globales. Por ejemplo, el servidor de números aleatorios puede proporcionar (en 410) un mensaje de respuesta de notificación de abono (incluyendo el número aleatorio) que se forma según el protocolo Diámetro-sh.

Cuando una femtocélula (FEMTO) arranca, puede estar configurada para que genere automáticamente (en 415) un túnel seguro a la pasarela de la femtorred. En la realización ilustrada, el túnel se forma según el protocolo IPSEC. Sin embargo, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente divulgación deberían apreciar que pueden usarse otros protocolos para formar (en 415) el túnel seguro entre la femtocélula y la pasarela de la femtorred. En respuesta a la formación del túnel seguro, la pasarela de la femtorred puede empezar a transmitir automáticamente (en 420) el valor actual del número aleatorio a la femtocélula. Cuando arrancan y se inicializan femtocélulas adicionales (FEMTO-n), también pueden formar (en 425) túneles seguros hacia la pasarela de la femtorred, la cual, a su vez, puede transmitir automáticamente (en 430) el valor actual del número aleatorio de retos globales a cada femtocélula (FEMTO, FEMTO-n).

El servicio de números aleatorios renueva y/o regenera periódicamente el número aleatorio de los retos globales. La pasarela de la femtorred (y cualquier otra entidad que se haya abonado al servicio de números aleatorios) puede entonces recibir información que indique el nuevo número aleatorio. En la realización ilustrada, el servidor de números aleatorios transmite (en 435) una solicitud de notificación de transmisión automática que indique a la pasarela de la femtorred el nuevo número aleatorio. La pasarela de la femtorred puede responder entonces (en 440)

con una respuesta de notificación de transmisión automática que indique la recepción con éxito del nuevo número aleatorio. La pasarela de la femtorred puede entonces transmitir automáticamente (en 445, 450) el nuevo número aleatorio a las femtocélulas; por ejemplo, multidifundiendo información que indique el nuevo número aleatorio.

La Figura 5 ilustra conceptualmente una tercera realización ejemplar de un procedimiento 500 de provisión de números aleatorios a una femtocélula. Las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente divulgación deberían apreciar que no se pretende que la segunda realización ejemplar sea independiente de las otras técnicas descritas en el presente documento y que aspectos de la tercera realización ejemplar pueden incorporarse en otros procedimientos y/o algoritmos descritos en el presente documento. En la realización ilustrada, el sistema de comunicaciones inalámbricas incluye una pasarela de femtorred (FNG), que proporciona una pasarela de seguridad para conexiones procedentes de femtocélulas situadas en los hogares de los usuarios en la Internet pública. La pasarela de la femtorred puede abonarse a un servicio de notificación de la actualización de la base de datos proporcionado por el servidor de números aleatorios (RAND). Sin embargo, a diferencia de la segura realización ejemplar del procedimiento 400 mostrado en la Figura 4, la pasarela de la femtorred de la tercera realización ejemplar incluye un agente de usuario IMS que puede autenticarse y darse de alto en una red IMS cuando arranca la pasarela de la femtorred.

El agente de usuario de la pasarela de la femtorred está configurado para proporcionar un mensaje que solicita el abono al servicio de números aleatorios usando el protocolo SIP según se define en la RFC 3265. Por ejemplo, el agente de usuario de la pasarela de la femtorred puede transmitir (en 505) un mensaje SUBSCRIBE al servidor de números aleatorios (RAND), el cual puede dar acuse de recibo del mensaje SUBSCRIBE transmitiendo (en 510) un mensaje de acuse de recibo, tal como un mensaje 200-OK. El servidor de números aleatorios puede transmitir entonces (en 515) un mensaje que incluya información que indique el valor actual del número aleatorio. Por ejemplo, el servidor de números aleatorios puede transmitir (en 515) un mensaje NOTIFY que incluya el valor actual del número aleatorio usado para los retos globales. El agente de usuario de la pasarela de la femtorred puede dar acuse de recibo del mensaje NOTIFY transmitiendo (en 520) un mensaje de acuse de recibo, tal como un mensaje 200-OK.

Cuando una femtocélula (FEMTO) arranca, puede estar configurada para que genere automáticamente (en 525) un túnel seguro a la pasarela de la femtorred. En la realización ilustrada, el túnel se forma según el protocolo IPSEC. Sin embargo, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente divulgación deberían apreciar que pueden usarse otros protocolos para formar (en 525) el túnel seguro entre la femtocélula y la pasarela de la femtorred. En respuesta a la formación del túnel seguro, la pasarela de la femtorred puede empezar a transmitir automáticamente (en 530) el valor actual del número aleatorio a la femtocélula. Por ejemplo, la pasarela de la femtorred puede transmitir automáticamente (en 530) un mensaje SIP que sea un mensaje SIP de tipo estándar que se usa normalmente para tipos de mensajes de mensajería instantánea. La femtocélula puede dar acuse de recibo de la información transmitida automáticamente transmitiendo (en 535) un mensaje de acuse de recibo tal como un mensaje 200-OK. Cuando arrancan y se inicializan femtocélulas adicionales (FEMTO-n), también pueden formar (en 540) túneles seguros hacia la pasarela de la femtorred, la cual, a su vez, puede transmitir automáticamente (en 545) el valor actual del número aleatorio de retos globales a cada femtocélula (FEMTO-n). La o las femtocélulas pueden dar acuse de recibo de la información transmitida automáticamente transmitiendo (en 550) un mensaje de acuse de recibo tal como un mensaje 200-OK.

El servicio de números aleatorios renueva y/o regenera periódicamente el número aleatorio de los retos globales. La pasarela de la femtorred (y cualquier otra entidad que se haya abonado al servicio de números aleatorios) puede entonces recibir información que indique el nuevo número aleatorio. En la realización ilustrada, el servidor de números aleatorios transmite (en 555) un mensaje NOTIFY que incluye información que indica a la pasarela de la femtorred el nuevo número aleatorio. La pasarela de la femtorred puede responder entonces (en 560) con un mensaje 200-OK que indica la recepción con éxito del nuevo número aleatorio. La pasarela de la femtorred puede entonces transmitir automáticamente (en 565, 570) el nuevo número aleatorio a las femtocélulas; por ejemplo, transmitiendo uno o más mensajes SIP o de otro protocolo de transferencia de datos que incluyan información que indique el nuevo número aleatorio.

Se presentan porciones de la presente invención y de la correspondiente descripción detallada en términos de soporte lógico o de algoritmos y representaciones simbólicas de operaciones en bits de datos dentro de la memoria de un ordenador. Estas descripciones y representaciones son aquellas mediante las cuales las personas con un dominio normal de la técnica transmiten de manera efectiva la sustancia de sus labores a otras personas con un dominio normal de la técnica. Se concibe que un algoritmo, según se usa el término aquí, y según se usa en general, es una secuencia internamente coherente de etapas que conducen a un resultado deseado. Las etapas son aquellas que requieren manipulaciones físicas de cantidades físicas. Normalmente, aunque no necesariamente, estas cantidades adoptan la forma de señales ópticas, eléctricas o magnéticas capaces de ser almacenadas, transferidas, combinadas, comparadas o manipuladas de otra forma. Se ha demostrado conveniente a veces, principalmente por razones de uso común, referirse a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números o similares.

Sin embargo, debería tenerse en cuenta que todos estos términos y similares han de estar asociados con las cantidades físicas apropiadas y son meramente etiquetas convenientes aplicadas a estas cantidades. A no ser que

se indique específicamente otra cosa, o como resulte evidente por la exposición, términos tales como "procesamiento" o "cálculo" o "calculando", o "determinando" o "mostrando" o similares se refieren a la acción y los procesos de un sistema de ordenador o un dispositivo informático electrónico similar que manipule y transforme datos representados como cantidades físicas electrónicas dentro de los registros y las memorias del sistema de ordenador en otros datos similarmente representados como cantidades físicas dentro de las memorias o los registros del sistema de ordenador o de otros dispositivos tales de almacenamiento, transmisión o presentación de la información.

Obsérvese también que los aspectos de la invención implementados mediante soporte lógico se codifican normalmente en alguna forma de medio de almacenamiento de programas o se implementan en algún tipo de medio de transmisión. El medio de almacenamiento de programas puede ser magnético (por ejemplo, un disquete o un disco duro) u óptico (por ejemplo, una memoria de solo lectura en disco compacto o "CD-ROM") y puede ser de solo lectura o de acceso aleatorio. De forma similar, el medio de transmisión pueden ser pares trenzados de hilo, cable coaxial, fibra óptica o algún otro medio de transmisión adecuado conocido en la técnica. La invención no está limitada por estos aspectos de ninguna implementación dada.

Las realizaciones particulares dadas a conocer en lo que antecede son únicamente ilustrativas, ya que la invención puede ser modificada y puesta en práctica de maneras diferentes, aunque equivalentes, evidentes a los expertos en la técnica que cuenten con el beneficio de las enseñanzas del presente documento. Además, no se contempla ninguna limitación a los detalles de construcción o de diseño mostrados en el presente documento salvo lo descrito en las reivindicaciones que siguen. Por lo tanto, resulta evidente que las realizaciones particulares dadas a conocer en lo que antecede pueden ser alteradas o modificadas y se considera que todas las variaciones de ese tipo están dentro del alcance de la invención. En consecuencia, la protección buscada en el presente documento es según se expone en las reivindicaciones que siguen.

REIVINDICACIONES

1. Un procedimiento (200, 300, 400, 500) de autenticación de una unidad móvil (110), estando la unidad móvil (110) en comunicación con una femtocélula (105), estando **caracterizado** el procedimiento (200, 300, 400, 500) **por** comprender las etapas de:

por radiodifundir (235) la femtocélula (105) a la unidad móvil (110) un reto global de autenticación que incluye un valor actual de un número aleatorio por un canal administrativo usando un mensaje administrativo,
transmitir (245, 250), desde la femtocélula (105) de una primera entidad segura (150) en una red central segura (115), información que indica dicho valor del número aleatorio y una respuesta de autenticación calculada por la unidad móvil (110) basada en dicho valor del número aleatorio y una primera clave conocida por la unidad móvil (110) y no conocida por la femtocélula (105) y
determinar (225), en la primera entidad segura (150), que dicho valor del número aleatorio es un número aleatorio legítimo proporcionado a la femtocélula (105) por la red central segura (115).

2. El procedimiento (200) de la reivindicación 1 en el que la determinación de que el número aleatorio es un número aleatorio legítimo comprende:

abonarse (220) a la provisión de números aleatorios por parte de una segunda entidad segura (155) de la red central segura (115); y
recibir (225), de la segunda entidad segura (155) información indicativa del número aleatorio.

3. El procedimiento (200) de la reivindicación 1 que comprende solicitar (260) a una entidad (160) de autenticación al menos una segunda clave determinada con base en la información que indica el número aleatorio y la respuesta de autenticación calculada por la unidad móvil (110), determinándose dicha al menos una segunda clave con base en el número aleatorio y la primera clave conocida por la unidad móvil (110) y la entidad (150) de autenticación y no conocida por la femtocélula (105).

4. El procedimiento (200) de la reivindicación 1 que comprende recibir (240) de la unidad móvil (110), y en respuesta a la radiodifusión del reto global, un mensaje que incluye la información que indica el número aleatorio y la respuesta de autenticación.

5. El procedimiento (200) de la reivindicación 1 que comprende establecer una comunicación segura entre la femtocélula (105) y la unidad móvil (110) basada en al menos dicha segunda clave.

6. El procedimiento (200) de la reivindicación 1 en el que la femtocélula (105) opera según estándares de acceso múltiple por división de código (CDMA) y en el que la red central segura (115) es una red de subsistemas multimedia con protocolo de Internet.

7. Una entidad segura (150) para autenticar una unidad móvil (110) en comunicación con una femtocélula (105), estando **caracterizada** la entidad segura (150) **porque** está adaptada para:

recibir de la femtocélula (105) información que indica un valor actual de un número aleatorio y una respuesta de autenticación calculada por la unidad móvil (110) basada en dicho valor del número aleatorio incluido en un reto global de autenticación radiodifundido por la femtocélula y una primera clave conocida por la unidad móvil (110) y no conocida por la femtocélula (105), y
determinar que el número aleatorio es un número aleatorio legítimo proporcionado a la femtocélula (105) por la red central segura (115).

8. La entidad (150) de seguridad según la reivindicación 7 en la que la entidad (150) de seguridad es un servidor de aplicaciones de gestión de la movilidad para coordinar y gestionar funciones relativas a la movilidad de la unidad móvil (110).

9. La entidad (150) de seguridad según la reivindicación 8 en la que se impide el pirateo informático del servidor (150) de aplicaciones de gestión de la movilidad usando una protección de cortafuegos y una protección antivirus, evitándose el acceso no autorizado al servidor (150) de aplicaciones de gestión de la movilidad.

10. Un sistema (100) de comunicaciones inalámbricas que comprende:

al menos una femtocélula (105),
una red central segura que comprende una entidad segura (150) según la reivindicación 7, y
al menos una unidad móvil (110).

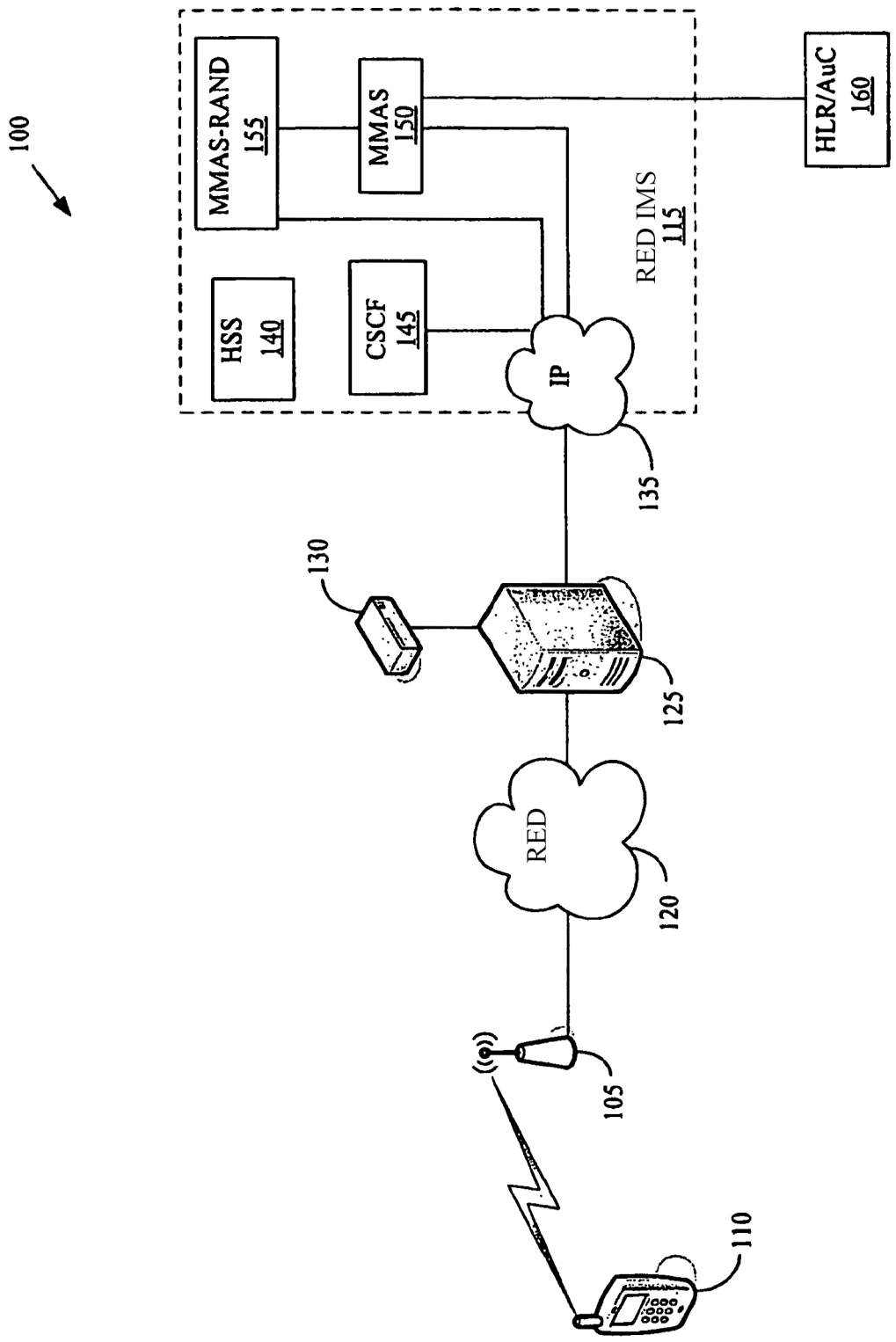
100
MMAS-RAND 155
MMAS 150
HLR/AuC 160
HSS 140
CSCF 145
IP
RED IMS 115
135
130
125
RED
120
105
110

Figura 1

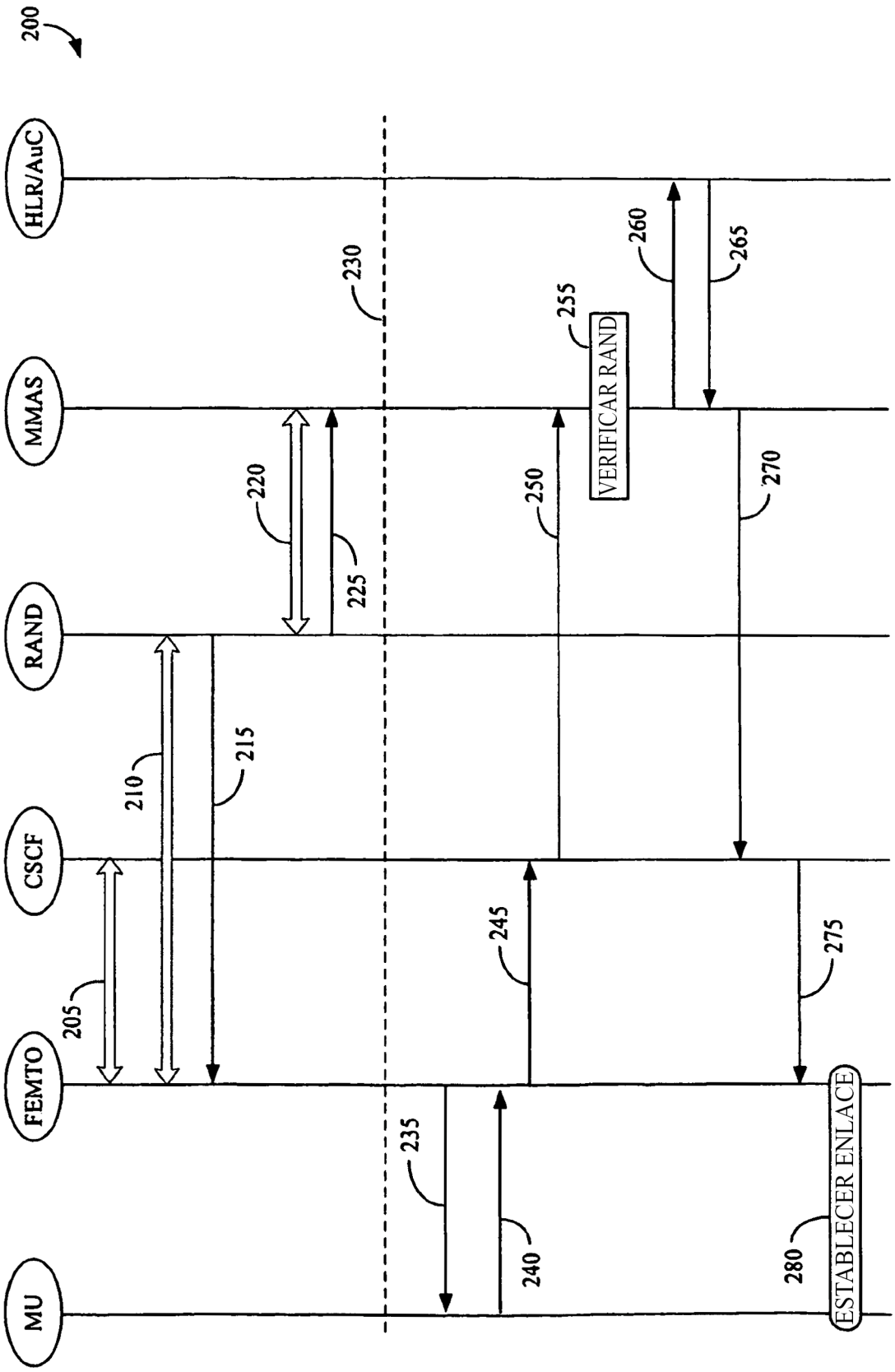
200
HLR/AuC
MMAS
RAND
CSCF
FEMTO
MU
205
210
215
220
225
230
235
240
245
250
255
VERIFICAR RAND
260
265
270
275
280
ESTABLECER ENLACE

Figura 2

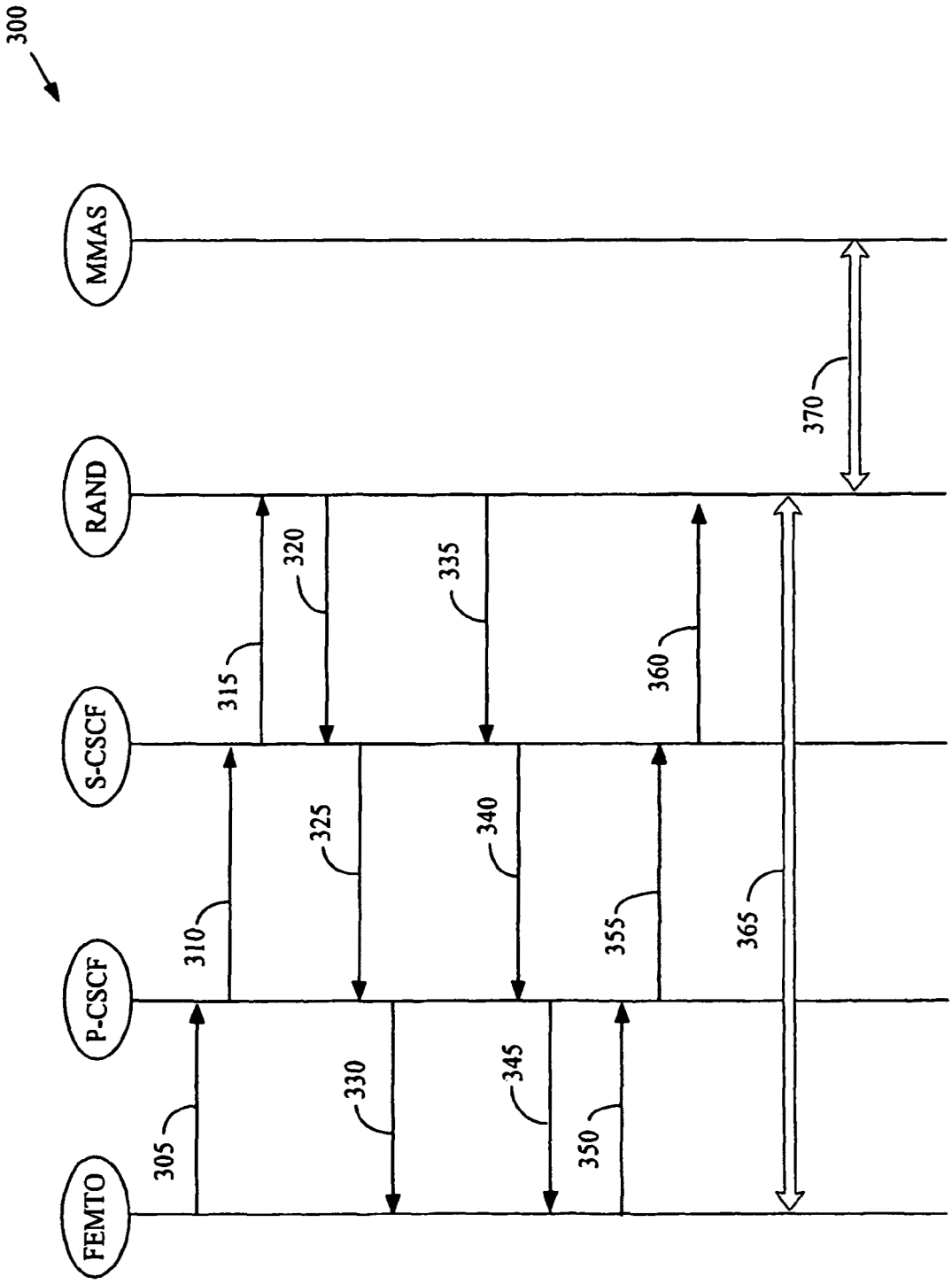
300
MMAS
RAND
S-CSCF
P-CSCF
FEMTO
305
310
315
320
325
330
335
340
345
350
355
360
365
370

Figura 3

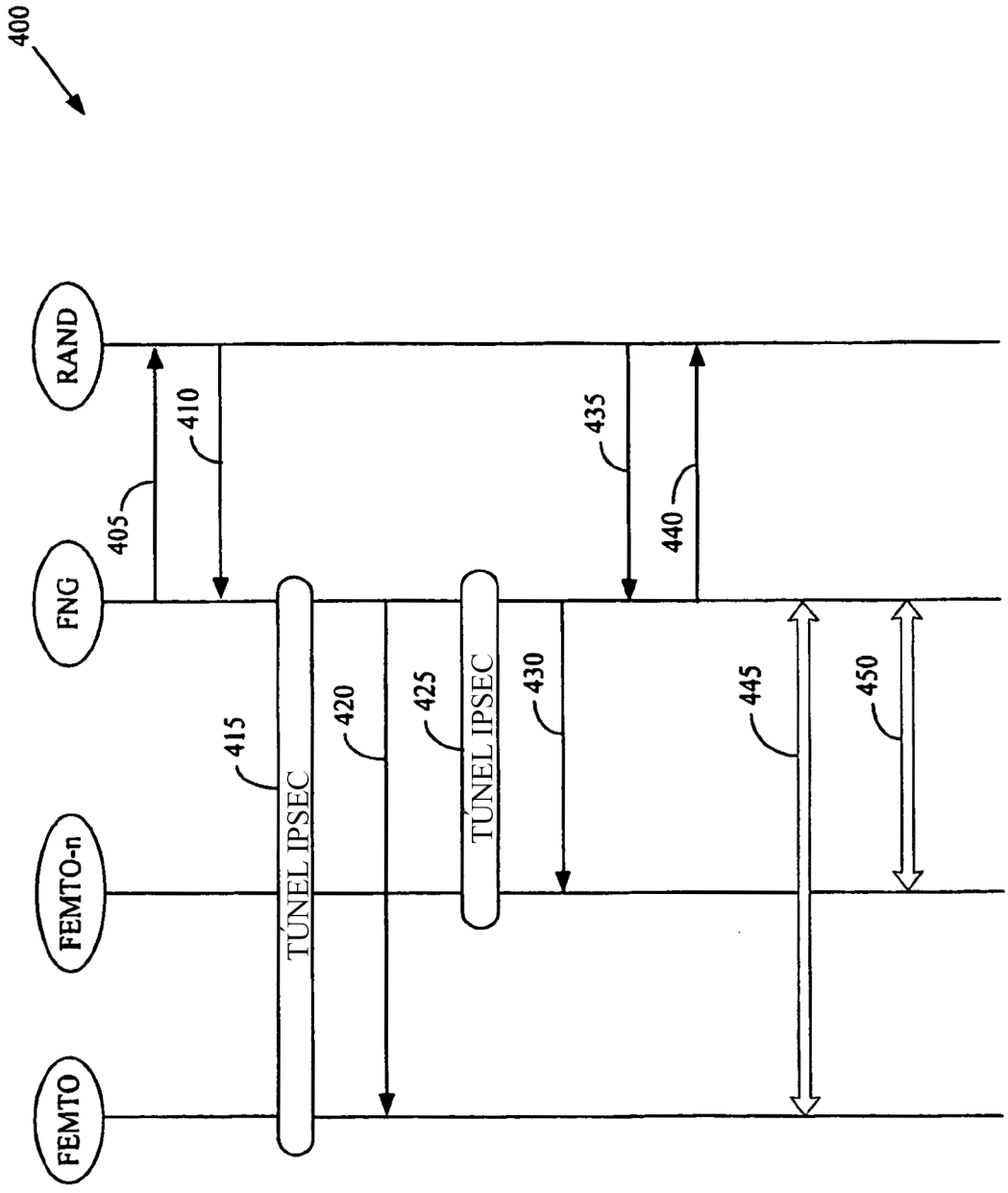
400
RAND
FNG
FEMTO-n
FEMTO
405
410
415
420
425
430
435
440
445
450
TÚNEL IPSEC
TÚNEL IPSEC

Figura 4

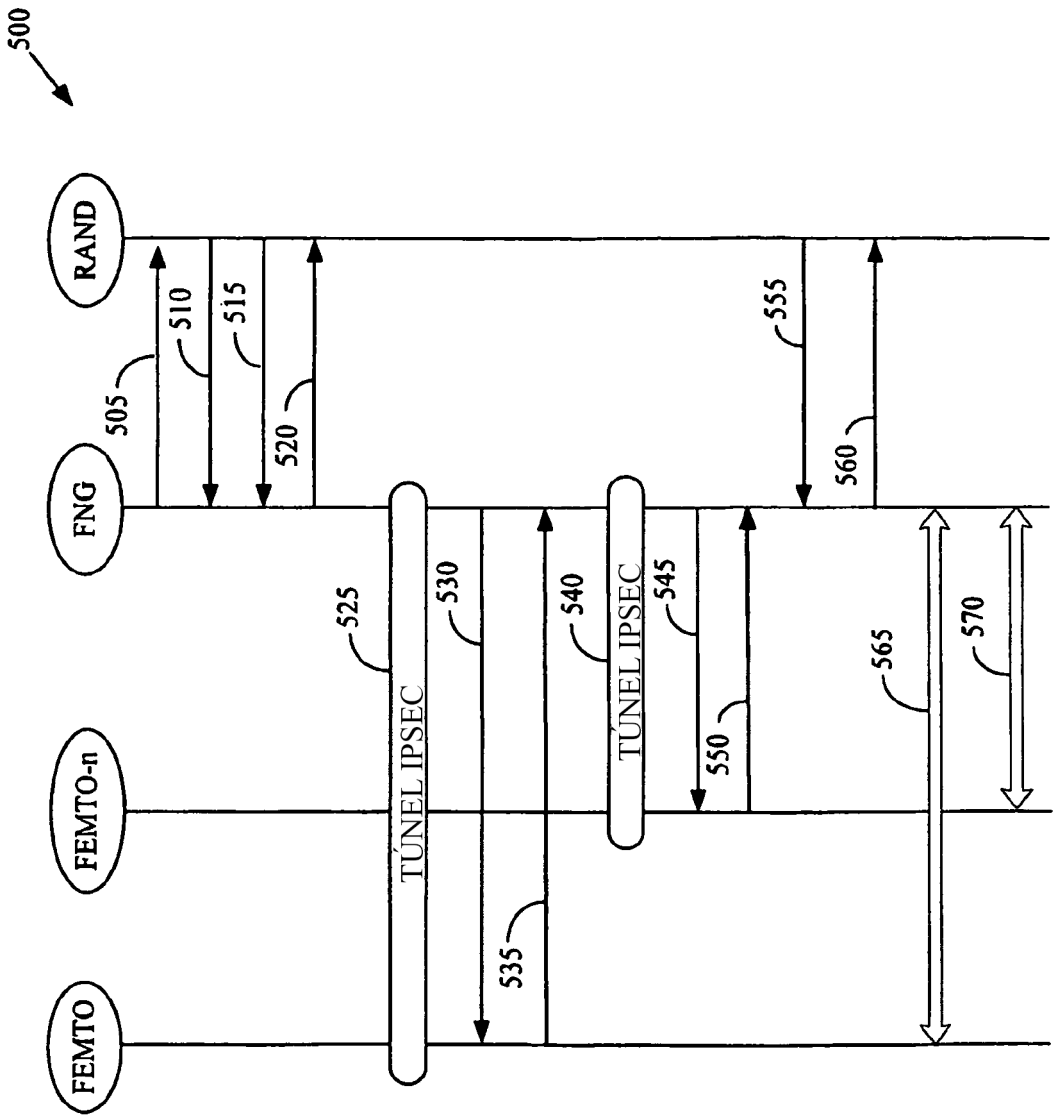
500
RAND
FNG
FEMTO-n
FEMTO
505
510
515
520
525
TÚNEL IPSEC
530
535
540
545
TÚNEL IPSEC
550
555
560
565
570

Figura 5