(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 384 326**

(51) Int. CI.:
H04L 29/06 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05752111 .4**
(96) Fecha de presentación: **20.06.2005**
(97) Número de publicación de la solicitud: **1894379**
(97) Fecha de publicación de la solicitud: **05.03.2008**

(54) Título: **Procedimiento y sistema para gestionar la autenticación de un terminal móvil en una red de comunicaciones, red correspondiente y producto de programa informático**

(45) Fecha de publicación de la mención BOPI:
03.07.2012

(45) Fecha de la publicación del folleto de la patente:
03.07.2012

(73) Titular/es:
Telecom Italia S.p.A.
Piazza degli Affari 2
20123 Milano, IT

(72) Inventor/es:
DELL'UOMO, Luca y
COLONNA, Massimo

(74) Agente/Representante:
Ponti Sales, Adelaida

DESCRIPCIÓN

Procedimiento y sistema para gestionar la autenticación de un terminal móvil en una red de comunicaciones, red correspondiente y producto de programa informático.

Campo de la invención

[0001] La presente invención se refiere a técnicas para la gestión de comunicación que permite la autenticación de un terminal móvil en una red de telecomunicaciones.

[0002] La invención ha sido desarrollada prestando particular atención a su posible uso en redes locales inalámbricas, redes metropolitanas o redes geográficas.

[0003] Tal como se usa en este documento, "autenticación" tiene por objeto designar, en general, aquellos procedimientos que conducen a que un terminal dado sea identificado (preferentemente de una manera segura) y capacitado para comunicarse (de nuevo, preferentemente, de una manera segura) por una red de comunicación dada. Como tal, esa designación se extiende a aquellas técnicas que permiten el intercambio de "secretos" (por ejemplo, claves de cifrado) para establecer una comunicación segura desde y/o hasta un terminal en una red de comunicación.

Descripción de la técnica relacionada

[0004] El documento WO-A-03/100348 ilustra un procedimiento para aumentar la seguridad en una red inalámbrica usando mediciones de distancia entre terminales móviles para proporcionar una capa de seguridad adicional en las comunicaciones. En ese procedimiento, la medición de la distancia entre dos terminales se usa para determinar la posibilidad de comunicación entre los dos terminales que pertenecen a la red. Las mediciones de distancia se realizan por triangulación de las distancias entre varios terminales o usando la conocida técnica TDOA (diferencia de tiempo de llegada).

[0005] El documento WO-A-01/93434 ilustra un procedimiento en el que, para el cálculo de las distancias entre un terminal móvil y un terminal remoto que pertenece a la red, se requiere el uso de un transmisor y un receptor UWB (banda ultra ancha). La comunicación entre un dispositivo local y el dispositivo remoto puede habilitarse o deshabilitarse según la distancia entre el dispositivo remoto y el dispositivo local. En la misma línea, en el procedimiento presentado en el documento US-A-2004/121787, la posición en la que el terminal móvil está situado en una WLAN (red de área local inalámbrica) se determina usando la conocida técnica TDOA (diferencia de tiempo de llegada) sobre las señales transmitidas por el propio terminal.

[0006] También el documento US-A-2003/217122 ilustra un procedimiento para gestionar la seguridad de una red inalámbrica/cableada basándose en la posición de los terminales. La posición de los terminales, en el caso de una red inalámbrica, puede ser suministrada por el propio terminal, por ejemplo mediante un dispositivo GPS integrado en el mismo o, si no, puede ser obtenida por la red a partir de mediciones de potencia o retardo realizadas por los puntos de acceso sobre las señales transmitidas por los terminales (por ejemplo, usando técnicas de triangulación). La información de localización se usa para permitir o denegar el acceso, ya sea total o parcialmente, a la red y a la información de que dispone.

[0007] Otros procedimientos y sistemas que establecen ellos mismos el mismo objetivo se describen en los documentos US-A-2004/028017, US-A-2004/059914 y US-A-2004/190718.

[0008] Todos los sistemas anteriores usan el cálculo de la distancia o la posición como procedimiento correcto de autenticación, además de los procedimientos usados comúnmente (por ejemplo, los basados en nombre de usuario y contraseña), en la medida en que la posición o la distancia se use para permitir las comunicaciones o no.

[0009] En un procedimiento adicional, ilustrado en el documento US-A-2003/140246, la posición del terminal se usa para decidir cuál ha de ser el nivel de seguridad que hay que usar en las comunicaciones entre el terminal y la red. En particular, en dicho documento, se prevén dos realizaciones diferentes, concretamente, una primera realización en la que el nivel de seguridad es gestionado por un sistema informático situado en la red, que recibe la posición del terminal desde un sistema de detección de localización provisto a propósito, y una segunda realización, en la que el nivel de seguridad es gestionado totalmente por el propio terminal móvil. A partir de un análisis específico únicamente de la primera realización, en la misma está comprendido el escenario en el que el sistema de

detección de localización está integrado en el terminal de usuario.

[0010] El documento WO2004/110026 desvela un procedimiento y aparato para aumentar la seguridad dentro de redes informáticas que incluyen uno o más puntos de acceso inalámbrico. Como parte de un proceso de autenticación de nodos de red, se intercambian parámetros de control de acceso que definen la capacidad de los nodos de red para acceder a otros recursos (por ejemplo, recursos de Internet) accesibles a través de una red informática transmitiendo una dirección MAC de un punto de acceso a través del cual el nodo de red accederá a la red informática en un intercambio con un servidor de autenticación para identificar el punto de acceso. El proceso de autenticación puede hacer uso de cualquiera de tales procesos, por ejemplo EAP TTLS, EAP TLS o PEAP.

[0011] El escenario analizado prevé que el sistema de detección de localización sea, por ejemplo, un receptor GPS o, alternativamente, que el terminal tenga algoritmos para calcular su propia posición (por ejemplo, basándose en mediciones realizadas por él). En ambos casos, el terminal transmite su propia posición al sistema informático mediante un sistema de comunicación.

[0012] En este caso se hace necesaria la creación de un segundo sistema de comunicación paralelo al empleado para uso de los servicios o, si no, alternativamente, se hace necesario el uso del mismo sistema de comunicación, y por lo tanto de los mismos protocolos de comunicación empleados para uso de los servicios (por ejemplo, encapsulando la información de localización en paquetes TCP/IP).

[0013] Las dos disposiciones presentan una desventaja considerable: la primera opción (sistema de comunicación paralelo) implica un considerable incremento de costes en la medida en que requiere la provisión de una segunda red para transmitir solamente la información de localización, mientras que la segunda opción (encapsulación de la información de localización en paquetes TCP/IP) pone en peligro la seguridad de la red en la medida en que los aparatos intermedios, por ejemplo puntos de acceso, conmutadores y enrutadores, no pueden verificar el contenido efectivo de los paquetes que reciben y, por consiguiente, reenvían (lo importante para estos aparatos es que los paquetes deberían ser de un tipo Ethernet, un tipo IP, o similares.

[0014] En este segundo caso, un usuario no autorizado a acceder a un área dada aun así podría llevar a cabo ataques sobre la red recurriendo, por ejemplo, al envío continuo de paquetes de control ICMP/IP (por ejemplo, el denominado “envío de ping”) que hace uso del mismo protocolo de comunicación (el protocolo IP) usado para los datos de usuario y los datos de localización.

[0015] Los mismos problemas también están presentes en otro posible escenario en el que la localización es realizada por un sistema de detección de localización mediante las mediciones hechas por el terminal, que luego han de ser transferidas por el propio terminal al sistema de detección de localización.

Objeto y resumen de la invención

[0016] A partir de la descripción precedente de la situación actual, se desprende que existe la necesidad de definir soluciones capaces de tratar la autenticación de un terminal móvil en una red de telecomunicaciones de una manera más satisfactoria comparada con las soluciones según la técnica conocida descrita previamente. Más específicamente, aun cuando las técnicas que permiten el condicionamiento, ya sea de manera total o parcial, de la autenticación de un terminal en su posición pueden considerarse más o menos consolidadas, sigue abierto el problema de permitir que un terminal que aún no está autenticado envíe a la red, de una manera sencilla y eficiente, la información de localización que ha de usarse para la autenticación.

[0017] Un objeto particular de la presente invención es proporcionar un procedimiento y un sistema que permitan la gestión de la autenticación de un terminal inalámbrico basándose en la posición adoptada por éste sin requerir que se cree un sistema de comunicación paralelo y sin poner en peligro la seguridad de la red.

[0018] Por lo tanto, el objeto de la invención es proporcionar una respuesta totalmente satisfactoria a las necesidades anteriores.

[0019] Según la presente invención, ese objeto se consigue por medio de un procedimiento que tiene las características expuestas en las reivindicaciones de más adelante. La invención también se refiere a un sistema correspondiente, una red relacionada, así como un producto de programa informático, que puede ser cargado en la memoria de al menos un ordenador y que incluye porciones de código de software para ejecutar las etapas del procedimiento de la invención cuando el producto se ejecuta en un ordenador. Tal como se usa en este documento,

el término “producto de programa informático” se usa para hacer referencia a un medio legible por ordenador que contiene instrucciones para controlar un sistema informático para coordinar la ejecución del procedimiento de la invención. La intención de la referencia a “al menos un ordenador” es, evidentemente, destacar la posibilidad de que la presente invención sea implementada de una manera distribuida/modular.

[0020] Las reivindicaciones forman una parte integral de la exposición de la invención provista en este documento.

[0021] Una realización preferida de la invención es, así, un procedimiento de autenticación de un terminal para la inclusión de dicho terminal en una red de comunicación (es decir, para permitir que el terminal se comunique por dicha red de comunicación), en el que la autenticación está condicionada a la información de localización transmitida desde dicho terminal hasta al menos un servidor de la red:

- proporcionando en la red al menos un punto de acceso para el terminal, estando dicho punto de acceso configurado para permitir que un terminal no autenticado transmita a un servidor de autenticación de la red mensajes de autenticación basados en un protocolo de autenticación dado (por ejemplo, EAP); y

- transmitiendo dicha información de localización desde dicho terminal hasta dicho servidor de autenticación transmitiendo dicha información de localización sobre dicho protocolo de autenticación dado.

[0022] En las realizaciones preferidas actualmente, la disposición descrita en este documento está basada en dos escenarios diferentes para transmitir la información de localización del terminal móvil.

[0023] En un primer escenario, la información de localización es transmitida a un sistema de autenticación por un sistema de detección de localización integrado en el terminal.

[0024] Alternativamente, en un segundo posible escenario, las mediciones realizadas por el terminal son transferidas a un sistema de detección de localización, externo al terminal, que, procesando estas mediciones, puede calcular la posición del terminal.

[0025] En la realización preferida anteriormente mencionada, la transferencia de la información de localización del terminal se realiza preferentemente por medio de un protocolo de señalización, y de una manera preferida particularmente, por medio del EAP (protocolo de autenticación extensible). El protocolo EAP es desarrollado por el IETF (Grupo de Trabajo de Ingeniería de Internet) y se describe en el siguiente documento: RFC3748, B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz; “Extensible Authentication Protocol (EAP)”, disponible en el sitio de Internet del IETF http://www.ietf.org.

[0026] El protocolo se usa normalmente en redes para transferencia de todos los mensajes de autenticación entre un terminal y un servidor de autenticación.

[0027] Para permitir el uso de este protocolo en la disposición descrita en este documento, sus funciones se extienden de tal manera que puede transmitir la información de localización anteriormente mencionada o las mediciones para el cálculo de la localización. De esta manera, la disposición descrita en este documento presenta la ventaja de no requerir la creación de una segunda red de comunicación ad hoc y ofrece la máxima garantía de seguridad gracias a las propiedades del EAP.

[0028] La seguridad se garantiza por el hecho de que los puntos de acceso (AP) bloquean el tráfico procedente de un terminal dado hasta que dicho terminal ha concluido positivamente el procedimiento de autenticación. El EAP impide la entrada en una red de un usuario que no está autenticado y, por lo tanto, no autorizado a acceder a un área dada de la red.

[0029] Aunque el procedimiento de autenticación haya producido un resultado negativo, el servidor de autenticación continúa recibiendo, a través del EAP, las localizaciones o las mediciones procedentes del terminal. Esta función puede ser útil para una posible autenticación posterior en caso de que el usuario fuera a entrar en un área de la red para la que está habilitado.

[0030] Las propiedades del EAP habilitan esta función ya que los AP permiten el paso a la red de todos los mensajes EAP, incluso los de un terminal no autenticado.

[0031] Además, es posible usar todos los protocolos de autenticación basándose en el EAP, denominados procedimientos EAP, por ejemplo, el EAP-SIM Protocolo de Autenticación Extensible-Gestión de Información de Seguridad, tal como se describe en el documento draft-haverinen-pppext-eap-sim-16.txt, H. Haverinen, J. Salowey, "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)", disponible en el sitio de Internet del IETF http://www.ietf.org, PEAP Protocolo de Autenticación Extensible Protegido (Avaya, Inc.), LEAP (Protocolo de Autenticación Extensible Ligero (Cisco Systems, Inc.), usados comúnmente en las redes inalámbricas, sin introducir ninguna modificación en las mismas.

[0032] Como los nuevos mensajes para transmitir la información de localización, añadidos al EAP, tienen el mismo formato de campo y adoptan, para rellenar esos campos, los mismos códigos usados en los mensajes EAP estándar, pueden ser usados por cualquier tecnología de radio que use el EAP para gestión de seguridad y pueden ser transmitidos así por los protocolos correspondientes sin ninguna modificación a dichos mensajes.

[0033] La extensión de las funciones del EAP requiere exclusivamente una actualización del software que reside en los puntos de acceso, de tal manera que puedan reconocer los nuevos mensajes. En cambio, no se requieren modificaciones en los otros aparatos de la red (enrutadores, conmutadores), en la medida en que estos son transparentes para el EAP.

[0034] En cualquier caso, la actualización está lejos de ser costosa en la medida en que puede realizarse a distancia y simultáneamente para todos los puntos de acceso implicados.

[0035] Con referencia a una realización preferida actualmente de la disposición descrita en este documento, en un primer escenario en el que el terminal puede determinar autónomamente su propia posición, es decir, el terminal está provisto de un sistema de detección de localización integrado, la disposición prevé un intercambio de información entre un servidor de autenticación y un terminal según el siguiente procedimiento:

- el servidor de autenticación recibe una solicitud de autenticación desde el terminal;

- el servidor de autenticación pide al terminal su posición mediante un mensaje EAP definido a propósito;

- el terminal envía su propia posición, mediante otro mensaje EAP definido a propósito, al servidor de autenticación; dicho mensaje comprende posiblemente la estimación del error absoluto;

- basándose en la información recibida, el servidor de autenticación decide qué procedimiento de autenticación es el más apropiado para su uso con el terminal en cuestión; y

- al final del procedimiento de autenticación, si ha tenido éxito o no, el terminal, una vez más en el momento de la solicitud del servidor de autenticación, envía periódicamente su propia posición al servidor de autenticación, mediante dos nuevos mensajes EAP definidos a propósito, para las autenticaciones posteriores.

[0036] Una vez más con referencia a una de las realizaciones preferidas actualmente de la disposición descrita en este documento, en un segundo escenario en el que el terminal solamente realiza mediciones sobre la señal recibida sin poder determinar su propia posición, la disposición prevé un intercambio de información entre un servidor de localización y un servidor de autenticación que cooperan entre sí y con el terminal según el siguiente procedimiento:

- el servidor de autenticación recibe una solicitud de autenticación desde el terminal;

- el servidor de autenticación indica, mediante un mensaje EAP definido a propósito, que el terminal debe transmitir las mediciones hechas en la señal recibida desde los diversos puntos de acceso;

- el terminal envía dichas mediciones al servidor de autenticación mediante un mensaje EAP definido a propósito;

- el servidor de autenticación envía las mediciones al servidor de localización;

- el servidor de localización, basándose en las mediciones recibidas, estima la posición del terminal;

- el servidor de localización envía al servidor de autenticación la posición estimada del terminal y, posiblemente, si está disponible, el error absoluto cometido en la estimación;

- basándose en la información recibida, el servidor de autenticación decide qué procedimiento de autenticación es el más apropiado para su uso con el terminal en cuestión;

- al final del procedimiento de autenticación, si ha tenido éxito o no, el terminal, una vez más en el momento de la solicitud desde el servidor de autenticación, envía periódicamente su propia posición al servidor de autenticación, mediante dos nuevos mensajes EAP definidos a propósito, para las autenticaciones posteriores.

[0037] La solicitud de posición o medición hecha al terminal y las respuestas de éste se llevan a cabo mediante mensajes EAP. De esta manera, es posible autenticar correctamente un terminal en el momento de su entrada en la red y también es posible seguirlo aun cuando el procedimiento de autenticación no haya tenido éxito. Usando la propiedad del EAP que permite el bloqueo del tráfico de todos los usuarios no autenticados permitiendo solamente el paso de los mensajes EAP, dicha disposición garantiza la seguridad de la red.

[0038] Resulta evidente que la disposición descrita anteriormente también puede usarse sin ninguna modificación sustancial para gestionar el cifrado y/o el procedimiento de protección de integridad y las longitudes/los tiempos de validez correspondientes de las claves que han de usarse en las comunicaciones seguras entre el terminal y la red con posterioridad a la autenticación correcta. Asimismo, la disposición puede usarse solamente para gestionar la actualización del cifrado y/o las claves de protección de integridad (y/o los procedimientos) y/o la longitud de las claves basándose en la posición.

Breve descripción de los dibujos adjuntos

[0039] A continuación se describirá la invención, meramente a modo de ejemplo no limitador, con referencia a las figuras de la lámina de dibujos adjunta, en la que:

- La Figura 1 ilustra un primer ejemplo de un escenario de aplicación de la disposición descrita en este documento;

- la Figura 2 ilustra un ejemplo de un mapa que representa un entorno cubierto por diferentes áreas de autenticación en el esquema de la disposición descrita en este documento;

- la Figura 3 ilustra el procedimiento que corresponde a la primera autenticación de un usuario en la red de la Figura 1;

- la Figura 4 ilustra el procedimiento que corresponde a las autenticaciones posteriores del usuario;

- la Figura 5 ilustra una variante del procedimiento de la Figura 4;

- la Figura 6 ilustra un segundo ejemplo de escenario de aplicación de la disposición descrita en este documento;

- la Figura 7 ilustra una variante del procedimiento que corresponde a la primera autenticación de un usuario en la red de la Figura 6;

- la Figura 8 ilustra una variante del procedimiento que corresponde a las autenticaciones posteriores del usuario;

- la Figura 9 ilustra una variante del procedimiento de la Figura 8;

- la Figura 10 ilustra el procedimiento de autenticación en el caso en que en la red de la Figura 6 hay terminales capaces de determinar su posición y terminales que hacen la medición de la señal recibida desde los diversos puntos de acceso;

- la Figura 11 ilustra un segundo ejemplo de mapa que representa un entorno cubierto por diferentes áreas de autenticación en el contexto de la disposición descrita en este documento; y

- la Figura 12 ilustra un ejemplo adicional de un mapa que representa un entorno cubierto por diferentes áreas de autenticación.

Descripción detallada de realizaciones de ejemplo de la invención

[0040] Se describe una realización preferida de la invención con referencia a una WLAN (red de área local inalámbrica); sin embargo, la disposición también es aplicable a redes metropolitanas y redes celulares independientemente de las características específicas de la tecnología de radio empleada.

[0041] La Figura 1 representa una WLAN, designada de manera global por el número de referencia 1, constituida por un conjunto de puntos de acceso 2, 3, 4 y 5, equipados con una antena integrada 31 o con una antena no integrada 6. En el caso de antenas no integradas 6, estas están conectadas a los puntos de acceso 3, 4, 5 mediante un cable 7 de longitud apropiada. Los usuarios que deseen usar los servicios puestos a disposición por la red 1 usan dispositivos constituidos por terminales de usuario inalámbricos provistos a propósito 9 como, por ejemplo, PC de sobremesa o portátiles, u ordenadores manuales tipo PDA, equipados con un aparato WLAN 10 como, por ejemplo, una tarjeta PCMCIA (Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales), un adaptador PCI (Interconexión de Componentes Periféricos), etc., integrado o de otro modo en el propio terminal, y las comunicaciones se obtienen a través de un medio de radio 11 con un protocolo patentado o estandarizado como, por ejemplo, el protocolo IEEE 802.11 o el protocolo HYPERLAN Tipo 2.

[0042] Los puntos de acceso 2, 3, 4, 5 proporcionan una cobertura de radio del área de interés constituida por células no superpuestas, designadas por los números de referencia 27 y 28 o células superpuestas, designadas por los números de referencia 28, 29 y 30, y están conectados a una red cableada 19 a través de los enlaces 21, 22, 23 y 24.

[0043] Usando la red cableada 19, los usuarios 9 obtienen acceso a todos los servicios a su disposición. En la red está presente un servidor de autenticación 14 para gestión de autenticación de los usuarios 9 que deseen obtener acceso a la red y una base de datos 16 que gestiona el perfil de los usuarios 9 (esta base de datos puede ser común a la de otras redes, como la de GPRS y/o UMTS y puede estar situada a distancia en la red doméstica del usuario, en cuyo caso el acceso a esta base de datos estaría gobernado por acuerdos de itinerancia). Estos objetos están localizados en un conjunto de servidores 20 conectado a la red 19 a través de un enlace 17.

[0044] El terminal 9 puede determinar su propia posición ya sea porque dispone de un aparato ad hoc integrado en el mismo, como, por ejemplo, un receptor GPS, o porque está configurado para implementar uno o más algoritmos que determinan la posición basándose en las características de la señal recibida por los diferentes puntos de acceso 2, 3, 4, 5. En el segundo caso, el terminal 9 también dispone de una base de datos propia, en la que se almacena la información necesaria para la localización, como, por ejemplo, la posición de los puntos de acceso, sus parámetros radioeléctricos, etc.

[0045] El servidor de autenticación 14 dispone de una base de datos 34 propia, que puede estar integrada o no con el servidor de autenticación 14 en sí y que contiene:

- un mapa que representa el área dentro de la cual está provista la WLAN y en la cual es necesario gestionar la autenticación de los terminales basándose en sus posiciones;

- una lista de todos los terminales activos con la indicación para cada uno de ellos de:

- el identificador (por ejemplo, la dirección de control de acceso al medio - MAC);

- la última posición estimada;

- la exactitud de la estimación;

- la hora en que se hizo la estimación;

- el estado de autenticación del terminal, es decir, autenticado, desautenticado, no autenticado.

[0046] La información es contenida luego en una tabla similar a la Tabla 1 ilustrada a continuación:

Tabla 1

ID del terminal	Hora (última localización)	Última posición (x,y)	Hora (última autenticación)	Área de autenticación	Procedimiento de autenticación	Resultado	Temporizador
Id1	h1:m1:s1	(x1,y1)	h'1:m'1:s'1	A1	M1	Autent.	t1
Id2	h2:m2:s2	(x2,y2)	h'2:m'2:s'2	A2	M2	No autent.	t2
Idn	hn:mn:sn	(xn,yn)	h'n:m'n:s'n	An	Mn	Autent.	tn

[0047] El servidor de autenticación 14 dialoga a través del enlace 35 (que puede ser un enlace físico en el propio conjunto de servidores 20 o un enlace lógico y puede atravesar otras redes) con la base de datos de perfiles de usuario 16.

[0048] La disposición descrita es independiente de la construcción física de la red 19: esta puede estar constituida por una red local cableada aislada del "resto del mundo" o, si no, puede estar formada por el conjunto de una red local y de una red geográfica interconectadas entre sí mediante dispositivos provistos a propósito, como puentes, conmutadores o enrutadores.

[0049] Además, la disposición es independiente de la tecnología con la que está construida la red 19: esta puede estar basada en los protocolos de la familia IEEE 802 (Ethernet, Token Ring, FDDI, etc.) y/o en los protocolos de conexión en red TCP/IP, ATM y Frame-Relay. Por último, la red 19 puede ser una red de radio. Se aplica un razonamiento similar a los enlaces 21, 22, 23, 24 y 17.

[0050] La disposición propuesta, por otra parte, es independiente de la posición y la construcción física del conjunto de servidores 20: por lo tanto, esta puede estar ubicada localmente, es decir, directamente en el área en la que ha de suministrarse el servicio o, si no, puede estar ubicada en un centro de servicio remoto para proporcionar el servicio en varias áreas simultáneamente; además, uno de los dos servidores puede estar situado localmente, mientras que el otro puede estar ubicado en el centro de servicio remoto. Cuando la base de datos 34 no está integrada en el servidor, puede estar ubicada en las inmediaciones de su propio servidor, ya sea localmente o a distancia o, si no, puede estar situada en un punto diferente de la red.

[0051] Se aplica lo mismo a la base de datos 16, que contiene los perfiles de usuario. Esta base de datos 16 puede, en algunos casos, estar constituida por dos o más bases de datos diferentes, la primera de las cuales pertenece al operador que gestiona el servicio y contiene los perfiles de sus propios usuarios, mientras que las otras pertenecen a otros operadores, como, por ejemplo, operadores de radio móviles, que tienen un acuerdo de itinerancia con el operador del proveedor de servicios. Estas otras bases de datos están situadas, en general, en la red de los otros operadores, en algunos casos son compartidas con las propias redes de radio móviles, y por lo tanto el enlace 35 para conexión con el servidor de autenticación 16 está constituido por una red geográfica basada en protocolos de comunicación normales.

[0052] La Figura 2 muestra un ejemplo de un mapa contenido en la base de datos 34 que representa un entorno de interior (por ejemplo, el plano de un piso en un edificio de la compañía) que está constituido por una multitud de oficinas y laboratorios. En el mapa, el administrador de sistemas dibuja las diferentes áreas de autenticación (A1, A2, A3, A4, A5), es decir, las áreas dentro de las cuales un terminal es autenticado mediante un procedimiento dado, y asocia dicho procedimiento a la propia área.

[0053] Una vez más con referencia a la Figura 2, el procedimiento M1 está asociado al área A1, el procedimiento M2 al área A2, etc. Ha de observarse que en un área dada podría ser posible tener también diferentes procedimientos de autenticación cuando el perfil de usuario varía, y los servicios disponibles en las áreas individuales podrían ser diferentes.

[0054] Alternativamente, las áreas de autenticación pueden hacerse coincidir con las células individuales, es decir, un área diferente para cada célula o, si no, con una combinación de células, es decir, un área diferente para varias células. De esta manera, las áreas de autenticación pueden obtenerse automáticamente a partir de la salida de las herramientas de planificación de células normales, que permiten el cálculo preciso del área cubierta por cada célula.

[0055] El procedimiento usado para gestionar la autenticación de un terminal basándose en su posición se ofrece en las Figuras 3 y 4. En particular, la Figura 3 ilustra el procedimiento para la primera autenticación cuando el usuario entra en la red, mientras que la Figura 4 ilustra el procedimiento que corresponde a las autenticaciones posteriores.

[0056] Los nuevos mensajes EAP definidos por la presente disposición se indican en las figuras con la línea más gruesa.

[0057] Cuando el terminal 9 entra en la red, recibe de un punto de acceso (por ejemplo, el punto de acceso 3), según lo que se define en la norma EAP, un mensaje de solicitud 50 en el que se le pide que indique su propia identidad. El terminal 9 responde al punto de acceso 3 suministrando su propia identidad con un mensaje 51, y el punto de acceso 3 reenvía, con un mensaje 52, dicha identidad al servidor de autenticación 14. En este momento, el servidor de autenticación 14 necesita saber la posición del terminal 9 y, con este fin, envía al mismo un mensaje de solicitud de posición 53 (mensaje de solicitud de posición EAP). El terminal 9 responde introduciendo su propia posición en el mensaje de respuesta de posición 54 (mensaje de respuesta de posición EAP), que permite al servidor de autenticación 14, en una etapa 55, decidir qué procedimiento de autenticación usar con el terminal 9 y iniciar el procedimiento de autenticación 56. Este procedimiento termina con un mensaje de éxito o fracaso 57, enviado por el servidor de autenticación 14 al terminal 9, indicando dicho mensaje si la autenticación ha tenido éxito o no.

[0058] En el primer caso (Éxito EAP), el terminal 9 puede iniciar sus propias comunicaciones y usar los servicios puestos a disposición por la red, usando los protocolos de comunicación normales (por ejemplo, TCP/IP o ATM). En el segundo caso (Fracaso EAP), el tráfico del terminal 9 es bloqueado por el punto de acceso 3 tal como se especifica por la norma EAP, y por lo tanto el terminal 9 no puede llevar a cabo ataques sobre la red. Durante el procedimiento de autenticación 56, el servidor de autenticación 14 dialoga con la base de datos 16 para obtener de ésta la información necesaria para la autentificación en sí, como, por ejemplo, el nombre de usuario y la contraseña de usuario 9.

[0059] Cualquiera que sea el resultado del procedimiento de autenticación 56, el servidor de autenticación 14 continúa siguiendo los movimientos del terminal 9 para una posible nueva autenticación en caso de que este fuera a cambiar el área de autenticación. Con este fin, el servidor de autenticación 14 ajusta un temporizador 58, en el momento en el que expira (véase la Figura 4, etapa 59) el servidor 14 envía un nuevo mensaje de solicitud de posición EAP 60 al terminal. El terminal 9 responde al servidor 14 enviándole su posición con un mensaje de respuesta de posición EAP 61.

[0060] En este momento, en una etapa 62, el servidor 14 vuelve a determinar, basándose en la posición recibida, el procedimiento de autenticación y, en una etapa 63, verifica si es necesaria una nueva autenticación.

[0061] Si no es necesaria la nueva autenticación (esto es cierto si el procedimiento determinado en la etapa 62 es el mismo que el usado en la autenticación previa), el servidor 14, en una etapa 64, ajusta el temporizador una vez más, en el momento en el que expira (etapa 59) repite la solicitud de posición. Opcionalmente, en una etapa 65, el servidor 14 puede hacer una estimación de la velocidad del terminal 9 y fija el temporizador, en la etapa 64, de una manera que depende de dicha velocidad. Si en la etapa 63 el servidor 14 deduce que es necesaria una nueva autenticación (esto es cierto si el procedimiento determinado en la etapa 62 es diferente del usado en la autenticación previa), se inicia un nuevo procedimiento de autenticación 66, que termina, como el anterior, con un mensaje de éxito o fracaso 67 enviado por el servidor 14 al terminal 9.

[0062] Al final de este procedimiento 66, el servidor 14, en una etapa 64, ajusta el temporizador una vez más, en el momento en el que expira (etapa 59) repite la solicitud de posición al terminal 9.

[0063] También en este caso, opcionalmente, el servidor 14 puede hacer, en una etapa 65, una estimación de la velocidad del terminal 9 y ajusta el temporizador en consecuencia en la etapa 64. También en este caso, durante el procedimiento de autenticación 66, el servidor de autenticación 14 dialoga con la base de datos 16 para obtener la información necesaria para la autenticación del terminal 9.

[0064] La Figura 5 ilustra una variante del procedimiento de la Figura 4 en la que, en el momento en el que expira el temporizador en la etapa 59, el servidor 14 pide al terminal 9 que le comunique la posición continuamente a intervalos regulares (el intervalo está especificado por el valor del parámetro del temporizador contenido en el mensaje), tal como se indica en un mensaje de solicitud proporcionado a propósito 68 (mensaje de solicitud de

posición continua EAP enviado por el servidor 14 al terminal 9).

[0065] El terminal 9 responde a la solicitud anterior enviando su propia posición al servidor 14 en un mensaje de respuesta de posición continua EAP 69. El mensaje de solicitud de posición continua EAP 68 se envía al terminal 9 siempre que, en la etapa 70, el servidor de autenticación 14 determine que el valor del temporizador obtenido en la etapa 64 sea diferente del usado hasta ese momento, y en este caso el mensaje 68 enviado al terminal 9 contiene el nuevo valor del temporizador. Una vez que el terminal 9 ha recibido el mensaje 68, envía, mediante el mensaje de respuesta de posición continua EAP 69, las respuestas al servidor 14, con la nueva periodicidad. En cambio, en el caso en que en la etapa 70 el servidor de autenticación 14 determina que el valor del temporizador obtenido en la etapa 64 es el mismo que el usado hasta ese momento, no se envía el mensaje de solicitud de posición continua 68, mientras que el terminal 9 envía su propia posición mediante el mensaje de respuesta de posición continua EAP 69 sin ningún cambio de periodicidad.

[0066] En la Figura 6 se ilustra un segundo escenario de uso de la disposición. Este escenario se diferencia del de la Figura 1 por la presencia de un servidor de localización 15 en el conjunto de servidores 20. En este escenario, el terminal 9 no puede determinar su posición sino que puede realizar exclusivamente la medición de la señal recibida desde los diversos puntos de acceso 2, 3, 4, 5 (por ejemplo, la dirección MAC de los puntos de acceso desde los cuales recibe una señal, el nivel de potencia recibido desde los diversos puntos de acceso, etc.), que luego se envía al servidor de localización 15 para su localización.

[0067] El servidor de localización 15 dispone de una base de datos 32 propia, que puede estar integrada o no con el servidor 15, en la que se almacena la información necesaria para la localización de los terminales, como, por ejemplo, la posición de los puntos de acceso, sus parámetros radioeléctricos, etc.

[0068] El servidor de localización 15, por otra parte, contiene un motor de localización con los diversos algoritmos que han de usarse para el cálculo de la posición de los terminales según el tipo de mediciones que estos pueden realizar. El servidor de localización 15 puede estar situado en el conjunto de servidores 20 o, si no, localmente en la red 19. Cuando la base de datos 32 no está integrada en el servidor 15, puede estar ubicada en las inmediaciones de su propio servidor 15, ya sea localmente o a distancia o, si no, puede estar ubicada en un punto diferente de la red.

[0069] El servidor de localización 15 está conectado al servidor de autenticación 14 mediante un enlace 36. Según la disposición de los dos servidores 14 y 15, el enlace 36 que los conecta puede ser un enlace punto a punto dedicado o puede ser un enlace lógico que forma parte de una red local o, si no, que forma parte de una red geográfica. Las comunicaciones entre los dos servidores 14 y 15 usan los protocolos de comunicación normales como TCP/IP, ATM o Frame Relay. En algunos casos, por ejemplo cuando la carga computacional no es excesiva, los dos servidores 14 y 15 pueden estar integrados en un mismo aparato, como asimismo pueden estar las bases de datos respectivas.

[0070] Las Figuras 7, 8 y 9 ilustran los procedimientos de autenticación del terminal en el momento de la entrada en la red y las autenticaciones posteriores causadas por el movimiento del terminal. Dichos procedimientos son idénticos a los ilustrados en las Figuras 3, 4 y 5 con la diferencia de que ahora los mensajes de posición (solicitud y respuesta) son sustituidos por mensajes de medida (mensaje de solicitud de medida EAP 53B, mensaje de respuesta de medida EAP 54B, mensaje de solicitud de medida EAP 60B, mensaje de solicitud de medida EAP 61B, mensaje de solicitud de medida continua EAP 67B, y mensaje de respuesta de medida continua EAP 68B) con el que el servidor de autenticación 14 solicita las mediciones procedentes del terminal 9 (solicitud) y éste las envía (respuesta). Por otra parte, hay presente un mensaje 71 con el que el servidor de autenticación 14 envía las mediciones recibidas al servidor de localización 15, y un mensaje 72 con el que el servidor de localización 15 envía la posición del terminal 9 al servidor de autenticación 14. Estos dos mensajes usan los protocolos de comunicación normales previstos por el enlace de conexión 36 como, por ejemplo, TCP/IP o ATM.

[0071] La Figura 10 ilustra la secuencia de mensajes en el caso en que, en la red de la Figura 6, hay presentes tanto terminales que pueden determinar su posición como terminales que realizan la medición de la señal recibida desde los diversos puntos de acceso.

[0072] En esta situación, cuando el terminal 9 entra en la red, el servidor de autenticación 14 envía un mensaje 73 de solicitud de capacidades EAP, con el cual pide al terminal 9 que indique sus propias capacidades (determinación de la posición o ejecución de las mediciones); éste responde con un mensaje 74 de respuesta de capacidades EAP. En este momento, el servidor 14 puede empezar la primera localización enviando un mensaje de

solicitud de posición EAP 53 o un mensaje de respuesta de medida EAP 53B según el contenido del mensaje de respuesta de capacidades EAP 74.

[0073] Las posiciones enviadas por el terminal 9 al servidor de autenticación 14 y las enviadas por el servidor de localización 15 al servidor de autenticación 14 contienen las coordenadas (x, y) del terminal y posiblemente una estimación del error cometido en el cálculo de la posición. Las coordenadas identifican el centro c de un círculo, mientras que la estimación del error identifica el radio r del mismo; la posición de ese círculo en el mapa de las áreas permite al servidor de autenticación 14 determinar el área de autenticación en la que el terminal 9 está localizado y, por lo tanto, el procedimiento de autenticación que ha de aplicarse al mismo (en la etapa 55 de las Figuras 3, 7 y 10 y en la etapa 62 de las Figuras 4, 5, 8 y 9).

[0074] El procedimiento adoptado es el siguiente:

- si el círculo está contenido completamente dentro de un área de autenticación, tal como se ilustra en la Figura 11, el procedimiento de autenticación que ha de usarse es el apropiado al área (en el ejemplo específico de la Figura 11, es el procedimiento M4);

- si el círculo corta varias áreas de autenticación, tal como se ilustra, por ejemplo, en la Figura 12, el servidor de autenticación 14 usa una de las siguientes opciones, que pueden ser configuradas por el administrador del sistema en la fase de configuración:

- selecciona el procedimiento del área en la que cae el centro c del círculo (procedimiento M5 en el ejemplo de la Figura 11); o, si no
- calcula el porcentaje del área del círculo que cae en cada área de autenticación y elige el procedimiento del área con el porcentaje más alto (procedimiento M5 en el ejemplo de la Figura 11); o, si no
- elige el procedimiento que es el más robusto (o el más débil según la elección inicial hecha por el administrador del sistema) entre los que corresponden a las áreas de autenticación cortadas; o, si no
- espera a recibir una nueva posición (para prevenir un círculo infinito, el administrador del sistema decide el número máximo de intentos que el servidor de autenticación 14 puede hacer antes de tomar una decisión sobre el procedimiento según los tres puntos previos).

[0075] El servidor de autenticación 14 guarda, en su base de datos 34, una tabla similar a la Tabla 1 que apareció previamente, en la que introduce el resultado de todas las operaciones ejecutadas. Los campos que la forman son los siguientes:

- Id del terminal: esto contiene el identificador del terminal y se introduce en la tabla cuando el terminal entra en la red (primera autenticación);

- Hora (última localización): esto indica la hora a la que se ha obtenido la última localización para el terminal;

- Última posición (x, y, err): esto contiene las coordenadas de la última posición ocupada por el terminal y el posible error asociado a la posición;

- Hora (última autenticación): esto indica la hora a la que se hizo la última autenticación para el terminal;

- Área de autenticación: esto indica el área de autenticación que corresponde a la posición del terminal; se introduce la primera vez en la etapa 55 y se modifica posiblemente en la etapa 63 si la última área es diferente de la decidida en la etapa 62;

- Procedimiento de autenticación: esto indica el procedimiento de autenticación usado para la autenticación del terminal; se introduce la primera vez en la etapa 55 y se modifica posiblemente en la etapa 63 si el último procedimiento usado es diferente del decidido en la etapa 62;

- Resultado: esto indica el resultado de la operación de autenticación (etapas 56 y 66) y puede ser “Autenticado” o “No autenticado”;

- Temporizador: esto indica el valor del temporizador que ha de usarse entre dos localizaciones consecutivas y se establece la primera vez en la etapa 58 y después se actualiza posiblemente con el resultado de la etapa 64.

[0076] En el proceso de localización, el servidor de localización 15 usa las mediciones realizadas por el terminal 9. En general, un terminal 9 puede medir las siguientes cantidades: punto de acceso al servidor (denominado en lo que sigue como punto de acceso principal), es decir, el identificador del punto de acceso a través del cual el terminal accede a la red; puntos de acceso adyacentes, es decir, los identificadores de los puntos de acceso desde los cuales el terminal recibe una señal; uno o más parámetros radioeléctricos como, por ejemplo, la potencia, o parámetros de rendimiento, como la BER (tasa de bits erróneos) o la PER (tasa de paquetes erróneos), medidos en la señal recibida por el terminal y transmitida por el punto de acceso principal; y uno o más parámetros radioeléctricos o parámetros de rendimiento medidos en todas las señales recibidas por el terminal y transmitidas por los puntos de acceso adyacentes.

[0077] El servidor de localización 15 dispone de diferentes algoritmos de localización, es decir, un algoritmo para cada clase de mediciones que el terminal 9 puede hacer (es decir, punto de acceso principal, punto de acceso principal + puntos de acceso adyacentes, etc.). Tal servidor de localización puede localizar cualquier terminal. El procedimiento usado en el proceso de localización es el siguiente:

- el servidor de localización 15 recibe del servidor de autenticación 14 el conjunto de mediciones realizadas por el terminal 9;

- el servidor de localización 15, y en particular su motor de localización, selecciona el algoritmo que ha de usarse basándose en las mediciones recibidas; y

- el servidor de localización 15 devuelve al servidor de autenticación 14 la posición estimada del terminal 9, concretamente, sus coordenadas x, y, y la estimación del error en la posición.

[0078] Es evidente que la disposición recién descrita puede usarse sin ninguna modificación sustancial incluso para gestionar el cifrado y/o el procedimiento de protección de integridad y las longitudes/los tiempos de validez de las claves que han de usarse en las comunicaciones seguras entre el terminal y la red con posterioridad a la autenticación correcta. La disposición propuesta puede usarse asimismo solamente para gestionar la actualización del cifrado y/o las claves (y/o los procedimientos) de protección de integridad y/o la longitud de las claves basándose en la posición.

[0079] En los casos adicionales de aplicación de la solución anteriormente mencionados, está claro que se usan extensiones que implican, entre otras cosas, los mensajes EAP y los contenidos de las diversas bases de datos. De hecho, por ejemplo, la Tabla 1 puede extenderse para contener campos de información que corresponden a las claves de cifrado/protección de integridad (por ejemplo, la longitud, la duración de validez, el algoritmo con el que ha de usarse la clave, etc.) que se refieren al caso en que la solución puede usarse para realizar la regeneración de las claves y/o variar sus longitudes y/o variar los algoritmos de cifrado/protección de integridad.

[0080] En lo que viene a continuación se ilustran varios ejemplos de formatos de los mensajes descritos previamente.

[0081] En particular, el formato de un mensaje de solicitud de posición EAP (por ejemplo, el mensaje 53 de la Figura 3 y el mensaje 60 de la Figura 4) se ilustra más abajo:

Código (= 1)	Identificador	Longitud
Tipo	Identificador del terminal	

mientras que el formato de un mensaje de respuesta de posición EAP (por ejemplo, el mensaje 54 de la Figura 3 y el mensaje 61 de la Figura 4) se ilustra más abajo:

Código (= 2)	Identificador	Longitud
Tipo	Identificador del terminal	
Posición del terminal		
Error de posición del terminal		

[0082] Los campos Código, Identificador y Longitud son conformes a la norma EAP y adoptan los valores

especificados por la misma en el párrafo 4 del documento RFC 3748. En particular, el campo Código adopta el valor 1 en el mensaje de solicitud de posición EAP y el valor 2 en el mensaje de respuesta de posición EAP.

[0083] El campo Tipo tiene el formato conforme al definido en el párrafo 5 del documento RFC 3748, mientras que su valor se define apropiadamente de tal manera que es diferente de cualquier Tipo definido hasta ahora. Por ejemplo, puede establecerse igual a 100 tanto en el mensaje de solicitud de posición EAP como en el mensaje de respuesta de posición EAP. El resto del mensaje de solicitud de posición EAP contiene el identificador del terminal que ha de medir su propia posición (campo Identificador del terminal), mientras que el resto del mensaje de respuesta de posición EAP contiene los tres campos siguientes:

- el identificador del terminal que ha medido su propia posición (campo Identificador del terminal);

- su propia posición, es decir, sus propias coordenadas (x, y, z) con respecto a un sistema de referencia conocido (campo Posición del terminal); y

- el error cometido en la estimación de la posición (campo Error de posición del terminal).

[0084] El formato de un mensaje de solicitud de posición continua EAP (por ejemplo, el mensaje 68 de la Figura 5) se ilustra más abajo:

Código (= 1)	Identificador	Longitud
Tipo	Identificador del terminal	
Temporizador		

mientras que el formato de un mensaje de respuesta de posición continua EAP (por ejemplo, el mensaje 69 de la Figura 5) se ilustra más abajo:

Código (= 2)	Identificador	Longitud
Tipo	Identificador del terminal	
Posición del terminal		
Error de posición del terminal		
Temporizador		

[0085] También para estos mensajes los campos Código, Identificador y Longitud son conformes a la norma EAP y adoptan los valores especificados por la misma en el párrafo 4 del documento RFC 3748. También en este caso, el campo Código adopta el valor 1 en el mensaje de solicitud de posición continua EAP y el valor 2 en el mensaje de respuesta de posición continua EAP. El campo Tipo tiene el formato conforme al definido en el párrafo 5 del documento RFC 3748, mientras que su valor se define apropiadamente de tal manera que es diferente de cualquier tipo definido hasta ahora.

[0086] Por ejemplo, puede establecerse igual a 101 tanto en el mensaje de solicitud de posición continua EAP como en el mensaje de respuesta de posición continua EAP. El resto del mensaje de solicitud de posición continua EAP, además del identificador del terminal que debe medir su propia posición (campo Identificador del terminal), también contiene el periodo (campo Temporizador) con el cual ha de medirse la posición. El campo Temporizador, que tiene el mismo significado, también está incluido en el mensaje de respuesta de posición continua EAP junto con los tres campos definidos para el mensaje de respuesta de posición EAP.

[0087] De manera similar, es posible definir los mensajes de solicitud de medida EAP, respuesta de medida EAP, solicitud de medida continua EAP y respuesta de medida continua EAP. Los mensajes de solicitud de medida EAP y respuesta de medida continua EAP tienen un campo Tipo igual a 102, mientras que la solicitud de medida continua EAP y la respuesta de medida continua EAP tienen un campo tipo igual a 103. El mensaje de solicitud de medida EAP contiene el identificador del terminal que ha de realizar las mediciones en la señal recibida, mientras que el mensaje de respuesta de medida EAP contiene el identificador del terminal que ha hecho la medición, así como las mediciones hechas. Los mensajes de solicitud de medida continua EAP y de respuesta de medida continua EAP también contienen el periodo (campo Temporizador) con el cual ha de medirse la posición y con el cual se ha medido, respectivamente.

[0088] Más abajo se ilustra una modalidad alternativa por medio de la cual pueden definirse los mensajes descritos previamente:

Código (= 1)	Identificador	Longitud
Tipo	Subtipo	
Identificador del terminal		

[0089] El formato propuesto se refiere en particular al mensaje de solicitud de posición EAP (mensaje 53 de la Figura 3 y el mensaje 60 de la Figura 4).

[0090] En el mismo está insertado el campo Subtipo, que diferencia todos los mensajes nuevos introducidos por la disposición descrita en este documento, adoptando, por ejemplo, el valor 1 para el mensaje de solicitud de posición EAP y el mensaje de respuesta de posición EAP, el valor 2 para el mensaje de solicitud de posición continua EAP y el mensaje de respuesta de posición continua EAP, etc. En cambio, el valor del campo Tipo es único para todos los mensajes e igual a un valor definido de tal manera que es diferente de cualquier Tipo definido hasta ahora. El resto de los mensajes permanecen inalterados.

[0091] Por consiguiente, sin perjuicio de los principios subyacentes de la invención, los detalles y las realizaciones pueden variar, incluso apreciablemente, con respecto a lo que se ha descrito y mostrado únicamente a modo de ejemplo, sin apartarse del alcance de la invención tal como se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento de autenticación de un terminal (9) para la inclusión de dicho terminal en una red de comunicación (1), en el que la autenticación está condicionada a la información de localización transmitida desde dicho terminal (9) hasta al menos un servidor de la red, incluyendo el procedimiento la etapa de:

- proporcionar en la red al menos un punto de acceso (2, 3, 4, 5) para el terminal (9), estando dicho punto de acceso configurado para permitir que un terminal no autenticado transmita a un servidor de autenticación (14) de la red mensajes de autenticación basados en un protocolo de autenticación dado, **caracterizado porque** incluye la etapa de:

- transmitir dicha información de localización desde dicho terminal (9) hasta dicho servidor de autenticación (14) transmitiendo dicha información de localización sobre dicho protocolo de autenticación dado.

2. El procedimiento de la reivindicación 1, **caracterizado porque** incluye las etapas de:

- proporcionar un sistema de localización integrado en dicho terminal (9) para generar información de localización que identifica la posición del terminal (9); y

- transmitir dicha información de localización que identifica la posición del terminal (9) desde dicho terminal (9) hasta dicho servidor de autenticación (14).

3. El procedimiento de la reivindicación 2, **caracterizado porque** incluye las etapas de:

- dicho servidor de autenticación (14) recibe de dicho terminal (9) una solicitud de autenticación;

- dicho servidor de autenticación (14) solicita de dicho terminal (9) dicha información de localización que identifica la posición del terminal (9);

- dicho terminal (9) envía a dicho servidor de autenticación (14) dicha información de localización que identifica la posición del terminal (9); y

- dicho servidor de autenticación (14) realiza un procedimiento de autenticación de dicho terminal (9) con dicha red (1).

4. El procedimiento de la reivindicación 1, **caracterizado porque** incluye las etapas de:

- asociar con dicha red (1) un servidor de localización (15);

- transmitir dicha información de localización desde dicho terminal (9) hasta dicho servidor de localización (15);

- dicho servidor de localización (15) produce, según dicha información de localización transmitida desde dicho terminal (9), información de localización que identifica la posición del terminal (9); y

- transmitir dicha información de localización que identifica la posición del terminal (9) hasta dicho servidor de autenticación (14).

5. El procedimiento de la reivindicación 4, **caracterizado porque** incluye las etapas de:

- dicho servidor de autenticación (14) recibe de dicho terminal (9) una solicitud de autenticación así como dicha información de localización;

- dicho servidor de autenticación (14) envía dicha información de localización a dicho servidor de localización (15), por medio de lo cual dicho servidor de localización (15) produce, basándose en dicha información de localización transmitida desde dicho terminal (9), información de localización que identifica la posición del terminal (9);

- dicho servidor de localización (15) envía dicha información de localización que identifica la posición del terminal (9) a dicho servidor de autenticación (14); y

- dicho servidor de autenticación (14) realiza un procedimiento de autenticación de dicho terminal (9) con dicha red (1).

6. El procedimiento de una cualquiera de las reivindicaciones 3 a 5, **caracterizado porque** incluye la etapa de que dicho terminal (9) envía a dicho servidor de autenticación (14), después de dicho procedimiento de autenticación, información de localización adicional para uso en procedimientos de autenticación posteriores.

7. El procedimiento de la reivindicación 6, **caracterizado porque** incluye la etapa de que dicho terminal (9) envía a dicho servidor de autenticación (14) dicha información de localización adicional independientemente del resultado de dicho procedimiento de autenticación.

8. El procedimiento de la reivindicación 1, **caracterizado porque** incluye la etapa de que dicho al menos un punto de acceso (2, 3, 4, 5) bloquea, siempre que dicho terminal (9) no sea autenticado con dicha red (1), el tráfico procedente de dicho terminal (9) aparte del tráfico transmitido sobre dicho protocolo de autenticación dado.

9. El procedimiento de la reivindicación 1, **caracterizado porque** incluye la etapa de que dicho servidor de autenticación (14) continúa recibiendo desde dicho terminal (9) dicha información de localización transmitida sobre dicho protocolo de autenticación dado después de que dicho terminal (9) es autenticado con dicha red (1).

10. El procedimiento de la reivindicación 1, **caracterizado porque** incluye la etapa de seleccionar dicho protocolo de autenticación como un protocolo de señalización, como un protocolo del tipo EAP (Protocolo de Autenticación Extensible).

11. El procedimiento de la reivindicación 10, **caracterizado porque** incluye la etapa de seleccionar dicho protocolo de autenticación del grupo que está constituido por los procedimientos denominados EAP, como EAP-SIM; PEAP; y LEAP.

12. El procedimiento de la reivindicación 1, **caracterizado porque** incluye la etapa de asociar con dicha información de localización transmitida sobre dicho protocolo de autenticación secretos para garantizar la seguridad de la información intercambiada por dicho terminal (9).

13. Un sistema para autenticar un terminal (9) para la inclusión de dicho terminal en una red de comunicación (1), en el que la autenticación está condicionada a la información de localización transmitida desde dicho terminal (9) hasta al menos un servidor de la red, en el que el sistema está configurado para realizar el procedimiento de cualquiera de las reivindicaciones 1 a 12.

14. Una red de comunicaciones (1) equipada con el sistema de la reivindicación 13.

15. La red de comunicaciones de la reivindicación 14, en la forma de una red inalámbrica.

16. Un producto de programa informático, que puede cargarse en la memoria de al menos un ordenador y que incluye porciones de código de software para realizar el procedimiento de cualquiera de las reivindicaciones 1 a 12.

Fig_1

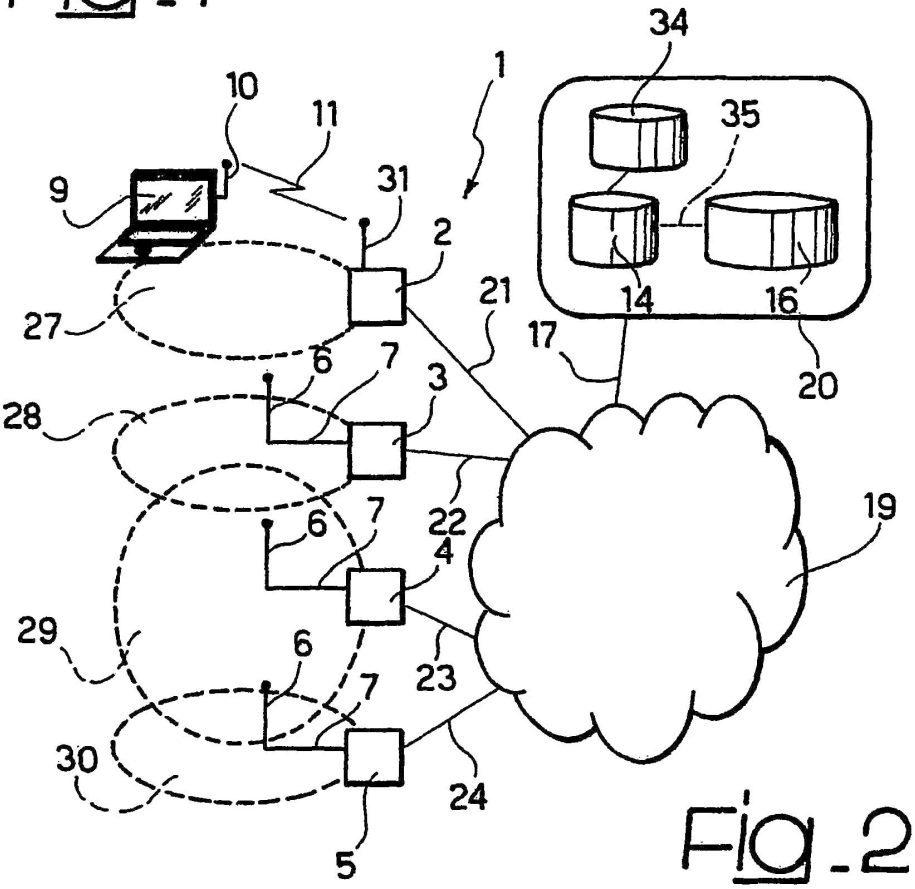

34
1
10
11
35
9
31
2
21
27
14
16
17
6
7
3
20
28
19
22
4
29
23
30
24
5

Fig_2

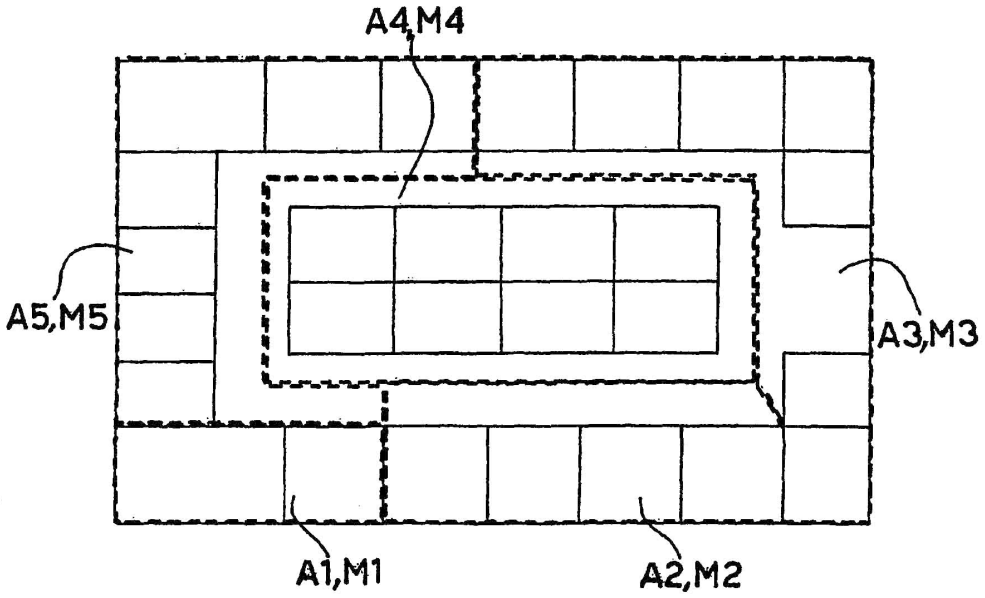

A4,M4
A5,M5
A3,M3
A1,M1
A2,M2

Fig.3

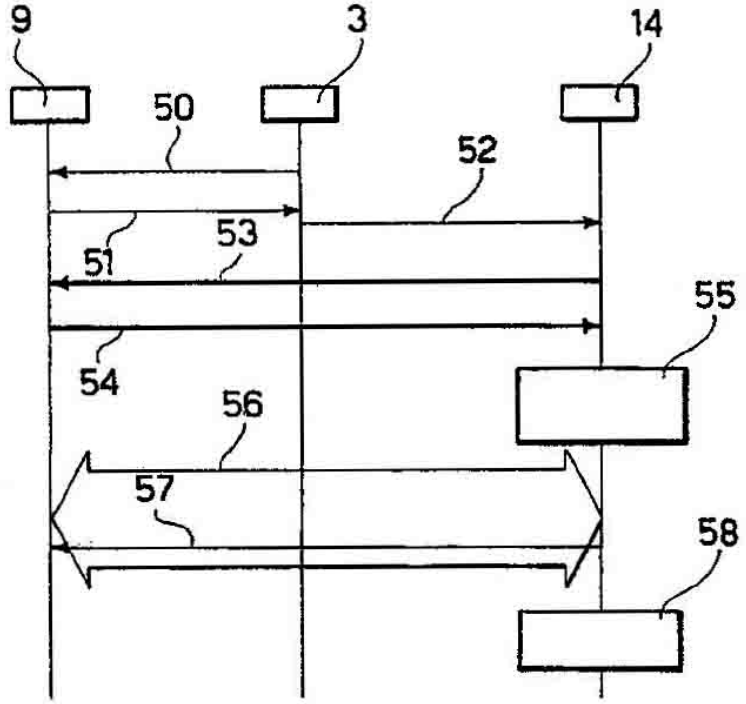

9
3
14
50
52
53
51
55
54
56
57
58

Fig.4

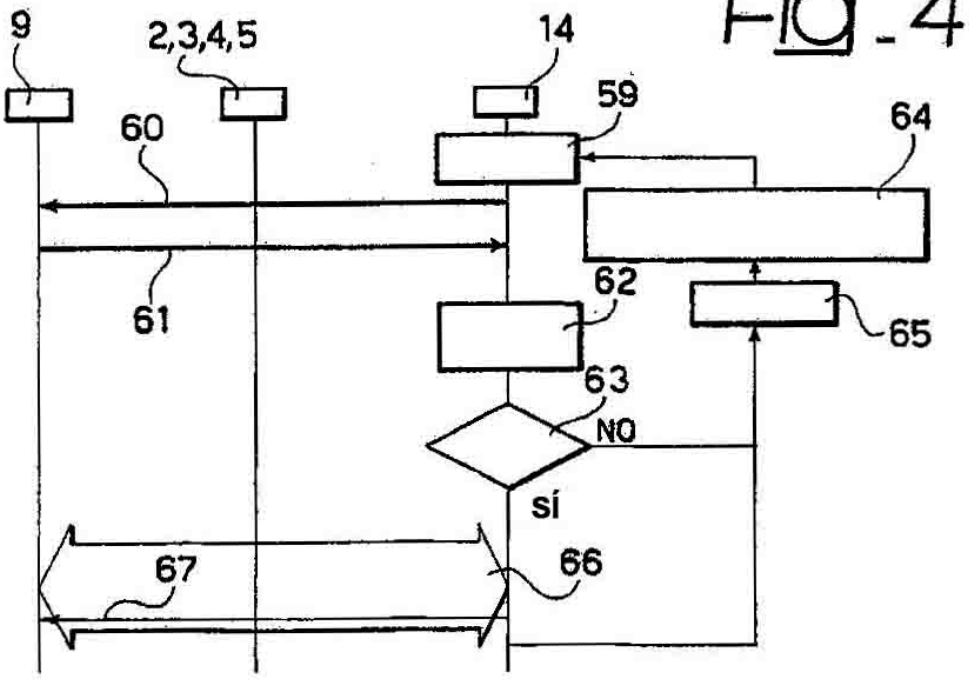

9
2,3,4,5
14
59
64
60
61
62
65
63
NO
sí
67
66

Fig. 5

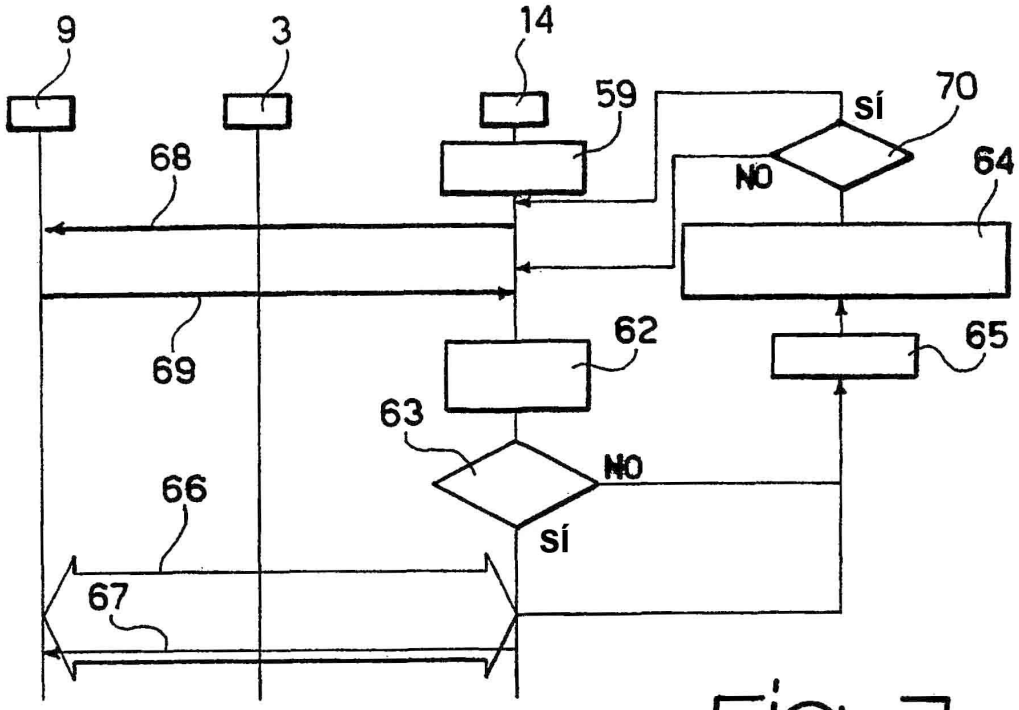
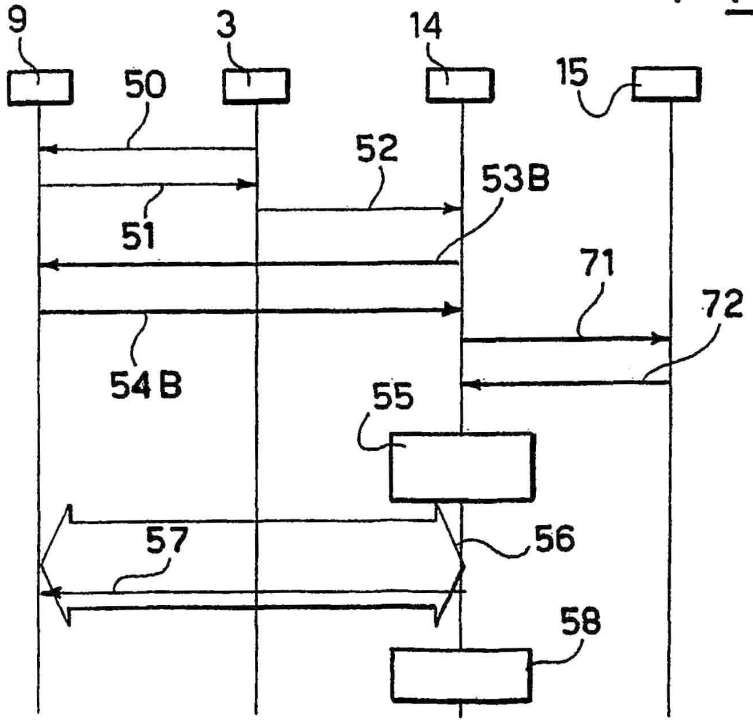

9
3
14
59
SÍ
70
68
NO
64
69
62
65
63
NO
66
SÍ
67

Fig. 7


9
3
14
15
50
52
53B
51
71
72
54B
55
57
56
58

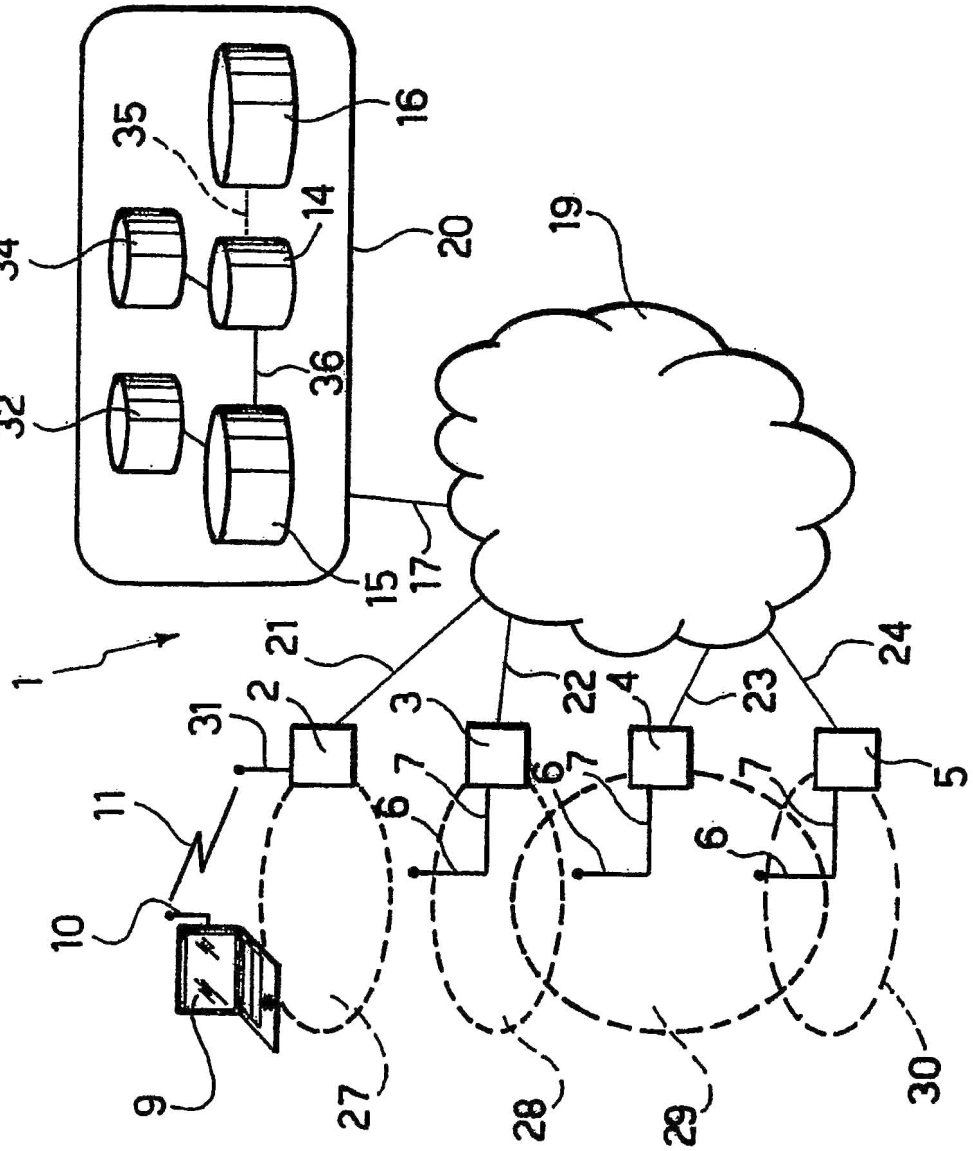

1
2
3
4
5
6
7
9
10
11
14
15
16
17
19
20
21
22
23
24
27
28
29
30
31
32
34
35
36

Fig.6

Fig.8

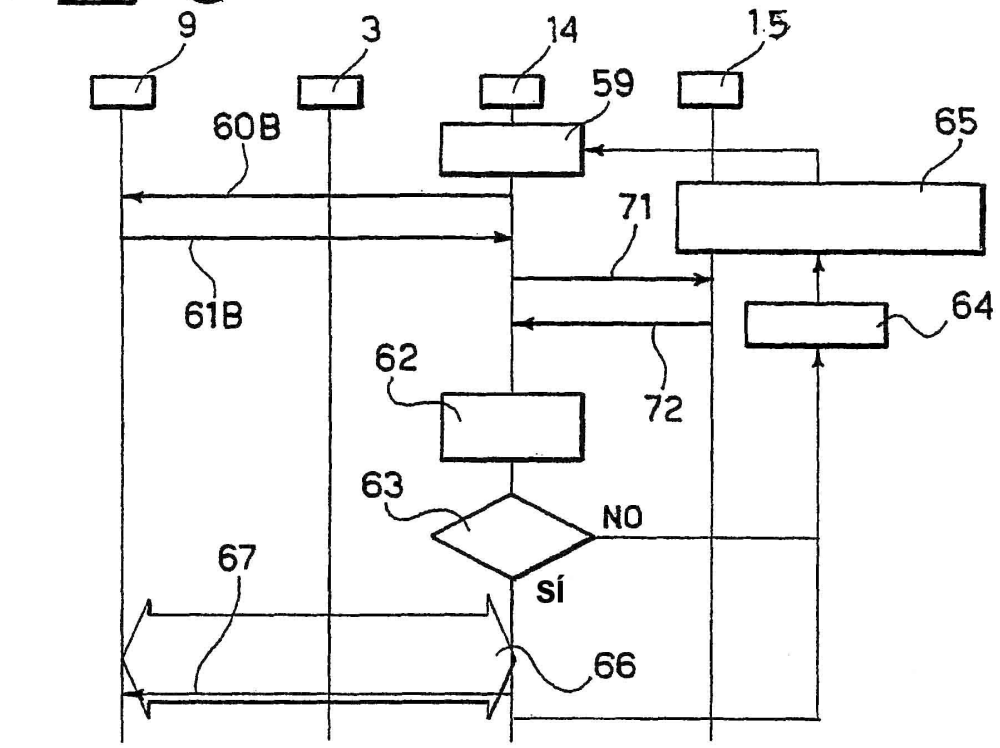

9
3
14
15
59
60B
65
71
61B
64
62
72
63
NO
67
SÍ
66

Fig.9

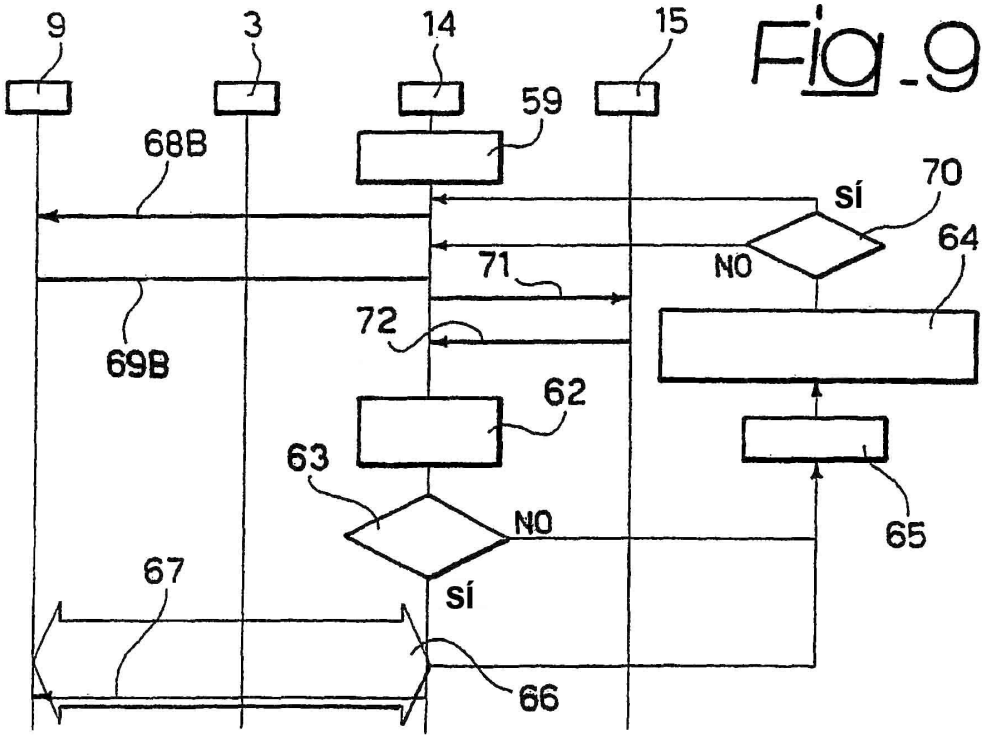

9
3
14
15
59
68B
SÍ
70
NO
64
71
72
69B
62
63
NO
65
67
SÍ
66

Fig. 10

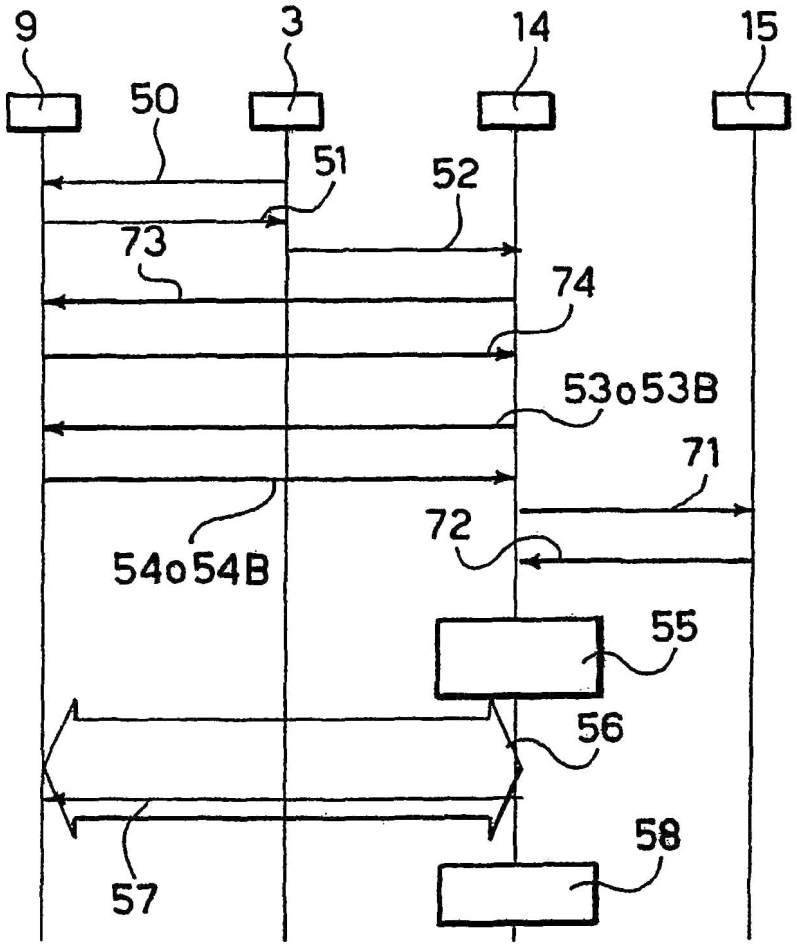


Fig. 11

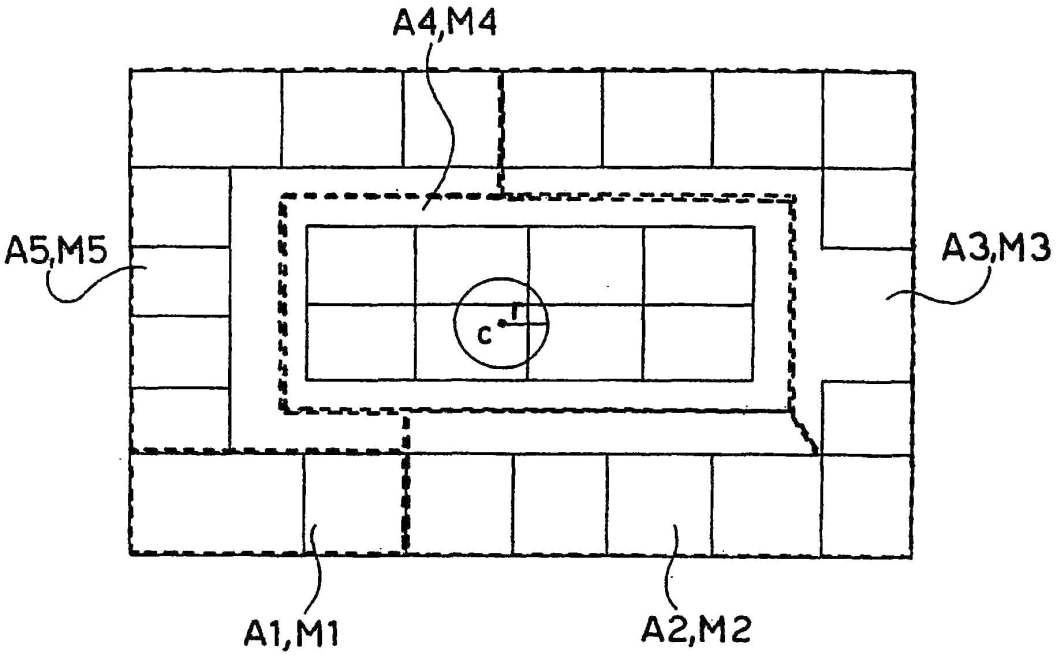


Fig. 12