(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 609 835**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/08 (2009.01)
H04W 64/00 (2009.01)
H04W 4/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.02.2011 PCT/US2011/026393**

(87) Fecha y número de publicación internacional: **01.09.2011 WO11106755**

(96) Fecha de presentación y número de la solicitud europea: **26.02.2011 E 11748218 (2)**

(97) Fecha y número de publicación de la concesión europea: **05.10.2016 EP 2540029**

(54) Título: **Sistema y procedimiento para seguridad y acceso teniendo en cuenta la localización**

(30) Prioridad:

26.02.2010 US 308551 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2017

(73) Titular/es:

DIGITAL AUTHENTICATION TECHNOLOGIES, INC. (100.0%)
1800 NW Corporate Blvd Suite 303
Boca Raton, FL 33431, US

(72) Inventor/es:

HANNA, DAVID, A., JR.

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistema y procedimiento para seguridad y acceso teniendo en cuenta la localización.

ANTECEDENTES DE LA INVENCIÓN

1. Campo de la invención

Esta invención se refiere en general a la seguridad de red y, más específicamente, a un sistema y procedimiento para autentificar la identidad de un usuario (o cliente) de dispositivo electrónico remoto que busca acceso electrónico a, o que trata de realizar una transacción electrónica con, un dispositivo anfitrión.

2. Descripción de la técnica relacionada

Siguiendo las enseñanzas de R. Dube en la patente de EE. UU. 7.231.044, las señales de temporización que se propagan desde fuentes de RF remotas tales como satélites GPS se retrasan de manera diferencial debido a la presencia de contenido de electrones libres a lo largo de la línea de visión entre el satélite y el receptor. Las fuentes de tales retardos pueden incluir fluctuaciones en el contenido total de electrones de la ionosfera, el movimiento de objetos tales como árboles a lo largo de la línea de visión, y la presencia de estructuras, tales como madera, hormigón, placa de yeso, etc. Todos estos añaden, en diferentes grados, retardos al tiempo de propagación total de las señales a través de ellos. En general, tales retardos son una función de la frecuencia específica, y la patente 7.231.044 describe el procedimiento de uso de retardos de tiempo diferenciales para extraer fluctuaciones aleatorias que después pueden usarse como la base para crear claves criptográficas no algorítmicas.

También se sabe que los materiales interpuestos contribuyen a la dispersión de estas señales, reduciendo de este modo la intensidad de las señales (comparada con un caso ideal donde no estaban presentes tales materiales interpuestos) que llegan al receptor. Correlacionando el grado de atenuación con la dirección de propagación de la señal (habitualmente caracterizada por los ángulos de altitud y acimut de un satélite con respecto al horizonte y la dirección neutral septentrional, meridional o ecuatorial), es posible desarrollar un mapa de la “firma” de atenuación alrededor de un receptor en una localización dada. En la medida en que esta firma sea estable, puede usarse en un momento posterior para verificar si un receptor está o no, de hecho, en una localización caracterizada anteriormente.

Por otra parte, Dube, en la patente de EE. UU. 7.177.426 enseña además un medio para emplear caracterización de localización y números aleatorios medidos en tiempo real para asegurar archivos basándose en la localización. El sistema puede emplear un procedimiento de puesta a prueba/respuesta entre un cliente y un servidor que además eleva la dificultad a la hora de derrotar tal sistema empleando números aleatorios dinámicos cuyos valores cambian y son actualizados tan en el cliente como en el servidor en el momento de una autentificación exitosa de un usuario.

Los edificios de oficinas muy grandes, los que están dentro de un área metropolitana grande que tiene muchos edificios de gran altura, y las localizaciones interiores o subterráneas pueden limitar gravemente o incluso eliminar la presencia de señales en esas localizaciones profundas. Esto hace difícil o imposible el funcionamiento de un sistema que emplea esta tecnología.

Sin embargo, Dube y R.L. Morgenstern en la patente de EE. UU. 7.551.739, que corresponde a la solicitud publicada US2005/0201560, enseña que las señales procedentes del interior de un espacio identificado y/o protegido que emplean números aleatorios, tales como las de la patente de EE. UU. de R. Dube 7.231.044, pueden usarse en una difusión para detectar cualquier anomalía, tal como un movimiento no autorizado, del objeto monitorizado cuando la aplicación de la tecnología prevista por la patente de EE. UU. 7.231.044 no es factible.

Considerando que la patente de EE. UU. 7.551.739 cubre la difusión de números aleatorios desde el interior de un espacio identificado y/o protegido (fijo o móvil) a objetos cercanos con el propósito de detección de anomalías, todavía existe una necesidad de desarrollar una solución en la cual puedan proporcionarse señales externas a zonas interiores de estructuras físicas tal como se describe, sin permitir la usurpación de identidad de tales señales por parte de usuarios con inclinaciones maliciosas.

La solicitud publicada US2003/0008668 describe un procedimiento para determinar la localización de una unidad móvil en un sistema de comunicación inalámbrica. La localización se determina comparando una instantánea de una porción predefinida del espectro de radiofrecuencia tomada por la unidad móvil con instantáneas tomadas en diversas localizaciones. Este procedimiento, sin embargo, no es suficientemente fiable para autentificar un

dispositivo inmóvil, ya que el espectro de radiofrecuencia en una localización dada puede ser calculado, como se menciona en la propia solicitud. Un procedimiento de autentificación basado en este procedimiento de localización podría así ser engañado fácilmente.

La solicitud PCT publicada WO97/13341 describe un sistema para autentificar la localización de usuarios remotos usando información específica de la localización geodésica de la entidad de usuario que cambia constantemente.

RESUMEN DE LA INVENCIÓN

En líneas generales, las realizaciones de la presente invención abordan estas necesidades proporcionando un sistema y procedimiento para un sistema de seguridad y acceso teniendo en cuenta la localización para autentificar usuarios remotos de recursos de red protegidos verificando la localización del usuario remoto. En una realización, se describe un sistema para proporcionar seguridad para un recurso de red protegido. El sistema incluye un aparato de acceso a red en comunicación con un receptor que recibe señales procedentes de una fuente remota. El aparato de acceso a red es capaz de recoger datos de microimpresión actuales para el receptor, que son una pluralidad de valores basados en valores de datos recibidos en el receptor a lo largo de un periodo de tiempo predefinido, por ejemplo, cuarenta y cinco segundos. El sistema también incluye un servidor de autentificación en comunicación con el aparato de acceso a red. El servidor de autentificación tiene acceso a una LSDF para el receptor, que es una pluralidad de valores basados en valores de datos recibidos en el receptor a lo largo de un periodo de tiempo predefinido, por ejemplo, un periodo de tiempo de veinticuatro horas. En funcionamiento, el aparato de acceso a red proporciona datos de microimpresión actuales para el receptor al servidor de autentificación, y el servidor de autentificación compara los datos de microimpresión actuales con la LSDF para el receptor para autentificar una petición de acceso. En un aspecto, los valores para la microimpresión actual y la LSDF son valores de inestabilidad. Aquí, cada valor de inestabilidad está basado en una diferencia en los tiempos de llegada de al menos dos señales de temporización procedentes de la misma fuente remota, tal como un satélite del sistema de posicionamiento global (GPS). Para aumentar la seguridad, el aparato de acceso a red puede estar en comunicación con una pluralidad de receptores, teniendo cada receptor una LSDF asociada accesible al servidor de autentificación. En este caso, el aparato de acceso a red puede proporcionar datos de microimpresión actuales para cada receptor de la pluralidad de receptores al servidor de autentificación, y el servidor de autentificación puede comparar los datos de microimpresión actuales para cada receptor con la LSDF asociada con cada receptor para autentificar una petición de acceso. Alternativamente, el aparato de acceso a red puede proporcionar datos de microimpresión actuales para un muestreo aleatorio de receptores seleccionados de la pluralidad de receptores al servidor de autentificación, y el servidor de autentificación puede comparar los datos de microimpresión actuales para cada receptor seleccionado con la LSDF asociada con cada receptor seleccionado para autentificar una petición de acceso.

En una realización adicional, se describe un procedimiento para proporcionar seguridad para un recurso de red protegido. El procedimiento incluye enviar una petición de puesta a prueba a un aparato de acceso a red en comunicación con un receptor que recibe señales procedentes de una fuente remota. La petición de puesta a prueba solicita datos de microimpresión actuales para el receptor. A continuación, los datos de microimpresión actuales para el receptor son enviados a un servidor de autentificación a través del aparato de acceso a red. Como antes, el servidor de autentificación tiene acceso a una LSDF para el receptor. Los datos de microimpresión actuales son comparados con la LSDF para el receptor para autentificar una petición de acceso. Al igual que antes, el aparato de acceso a red puede estar en comunicación con una pluralidad de receptores, teniendo cada receptor una LSDF asociada accesible al servidor de autentificación. Aquí, los datos de microimpresión actuales para cada receptor de la pluralidad de receptores pueden ser enviados al servidor de autentificación, y el servidor de autentificación puede comparar los datos de microimpresión actuales para cada receptor con la LSDF asociada con cada receptor para autentificar una petición de acceso. Alternativamente, los datos de microimpresión actuales para un muestreo aleatorio de receptores seleccionados de la pluralidad de receptores pueden ser enviados al servidor de autentificación, y el servidor de autentificación puede comparar los datos de microimpresión actuales para cada receptor seleccionado con la LSDF asociada con cada receptor seleccionado para autentificar una petición de acceso.

En una realización adicional más de la presente invención, se describe un sistema adicional para proporcionar seguridad para un recurso de red protegido. El sistema incluye un recurso de red protegido y un aparato de acceso a red en comunicación con el recurso de red protegido y una pluralidad de receptores, donde cada receptor recibe señales procedentes de una fuente remota. El aparato de acceso a red es capaz de recoger datos de microimpresión actuales para cada receptor. El sistema también incluye un servidor de autentificación en comunicación con el aparato de acceso a red. El servidor de autentificación tiene acceso a una LSDF asociada con cada receptor. En funcionamiento, el aparato de acceso a red proporciona datos de microimpresión actuales para

cada receptor al servidor de autentificación, que compara los datos de microimpresión actuales con la LSDF asociada con cada receptor para autentificar una petición de acceso y proporcionar acceso al recurso de red protegido. Como antes, en una realización los valores son valores de inestabilidad basados en una diferencia en los tiempos de llegada de al menos dos señales de temporización procedentes de la misma fuente remota. Otros aspectos y ventajas de la invención resultarán evidentes a partir de la siguiente descripción detallada, tomada conjuntamente con los dibujos adjuntos, que ilustran a título de ejemplo los principios de la invención.

La invención se define en las reivindicaciones independientes 1 y 4.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La invención, junto con ventajas adicionales de la misma, puede comprenderse mejor por referencia a la siguiente descripción tomada conjuntamente con los dibujos adjuntos, en los cuales:

la fig. 1 es un diagrama de bloques que muestra un sistema de seguridad y acceso teniendo en cuenta la localización ejemplar de acuerdo con una realización de la presente invención;
la fig. 2 es una ilustración que muestra un receptor de RF que utiliza datos de GPS para facilitar la autentificación, de acuerdo con una realización de la presente invención;
la fig. 3 es un diagrama de temporización que ilustra señales de temporización procedentes de un satélite de un sistema GPS;
la fig. 4 es un diagrama conceptual que ilustra una LSDF y microimpresiones para el receptor ejemplar, de acuerdo con una realización de la presente invención;
la fig. 5 es un diagrama de flujo que muestra un procedimiento para autentificar el acceso a un recurso de red protegido, de acuerdo con una realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES PREFERENTES DE LA INVENCIÓN

Se describe una invención para un sistema de seguridad y acceso teniendo en cuenta la localización para autentificar usuarios remotos de recursos de red protegidos verificando la localización del usuario remoto. En general, las realizaciones de la presente invención crean una pluralidad de huellas digitales específicas de la localización para una pluralidad de receptores localizados por todo un espacio particular. Para crear una huella digital específica de la localización para un receptor particular, señales de temporización en dos frecuencias diferentes que llegan de la misma fuente remota son captadas en un receptor de radiofrecuencia (RF) y la diferencia en los tiempos de llegada de señal de temporización es extraída y comparada. Estas diferencias en los tiempos de llegada son convertidas en números discretos, recogidas y almacenadas a lo largo de un periodo de tiempo predefinido (por ejemplo, veinticuatro horas) para crear una huella digital específica de la localización para cada receptor particular. Cuando después se accede a un recurso de red protegido, las realizaciones de la presente invención solicitan datos actuales procedentes de los receptores y verifican los datos recibidos frente a las huellas digitales específicas de la localización para cada receptor. Si los datos recibidos pueden ser verificados, se concede acceso al recurso protegido.

En la siguiente descripción, se exponen numerosos detalles específicos con el fin de proporcionar una perfecta compresión de la presente invención. Resultará evidente, sin embargo, para alguien experto en la materia que la presente invención puede ponerse en práctica sin algunos o todos estos detalles específicos. En otros casos, las etapas de procedimiento bien conocidas no se han descrito en detalle con el fin de no oscurecer innecesariamente la presente invención.

La fig. 1 es un diagrama de bloques que muestra un sistema de seguridad y acceso teniendo en cuenta la localización ejemplar (100) de acuerdo con una realización de la presente invención. En una realización, el sistema de seguridad y acceso teniendo en cuenta la localización (100) proporciona seguridad a recursos de red protegidos restringiendo el acceso a tales recursos por medio de un equipo de red autentificado responsable de proporcionar ordenadores cliente de acceso a red, tales como un conmutador de red. Por ejemplo, el sistema de seguridad y acceso teniendo en cuenta la localización ejemplar (100) de la fig. 1 incluye un conmutador de red (104) en comunicación con una pluralidad de receptores (102a)-(102d). El conmutador de red (104) es responsable de proporcionar ordenadores cliente de acceso a red (106) que están localizados localmente al conmutador de red (104), por ejemplo, conectados directamente al conmutador de red (104).

Ta como se ilustra en la fig. 1, el conmutador de red (104) está en comunicación con una pluralidad de receptores (102a)-(102d). Cada receptor (102a)-(102d) puede estar localizado en cualquier área dentro de, o alrededor de una

localización particular. Por ejemplo, un receptor (102a) y (102b) puede estar localizado dentro de la misma sala que el conmutador de red (104) dentro de un edificio, mientras que el receptor (102c) puede estar localizado en otra sala del mismo edificio, y el receptor (102d) puede estar localizado en el tejado del edificio. Aunque en la fig. 1 se muestra que el conmutador de red (104) está en comunicación con cuatro receptores (102a)-(102d), cabe destacar que el conmutador de red (104) podría estar en comunicación con cualquier número de receptores, aunque al menos un receptor debería estar en comunicación con el conmutador de red (104). En general, los receptores (102a)-(102d) proporcionan datos de autentificación al conmutador de red (104) cuando es necesario durante un procedimiento de puesta a prueba de autentificación y respuesta, como se describirá con mayor detalle posteriormente.

El conmutador de red (104) además está en comunicación con un cortafuegos (110), que en el ejemplo de la fig. 1 es responsable de restringir el acceso a recursos de red protegidos, tales como el activo de red protegido (108). Para facilitar la autentificación de los activos de red, el cortafuegos (110) está en comunicación con un servidor de autentificación (112). En líneas generales, cuando un recurso de red tal como el conmutador de red (104) intenta proporcionar acceso a un recurso de red protegido, tal como el activo de red protegido (108), el servidor de autentificación (112) proporciona un mecanismo para que el cortafuegos (110) autentifique el conmutador de red (104) antes de permitir el acceso al recurso de red protegido por medio de una base de datos de huella de localización específica de la localización preconstruida (114), que almacena datos de huella de localización específica de la localización (LSDF) para cada receptor (102a)-(102d) del sistema de seguridad y acceso teniendo en cuenta la localización (100). Los datos de LSDF para cada receptor están basados en valores de inestabilidad recibidos de cada receptor de radiofrecuencia (RF) (102a)-(102d), como se describe con mayor detalle con referencia a la fig. 2.

La fig. 2 es una ilustración que muestra un receptor de RF (102) que utiliza datos de GPS para facilitar la autentificación, de acuerdo con una realización de la presente invención. El receptor de RF (102) incluye una antena (200). El receptor de RF (102) hace uso de fuentes de señal remotas, tales como satélites (202) del Sistema de Posicionamiento Global (GPS), para proporcionar señales de temporización (204). Aunque la siguiente descripción es en términos de tecnología GPS, cabe destacar que cualquier señal de temporización externa puede ser utilizada por las realizaciones de la presente invención. Como se describirá con mayor detalle más adelante, puede usarse cualquier señal de temporización externa en dos o más frecuencias diferentes que llegue de la misma fuente remota. Señales de temporización externas ejemplares adicionales pueden incluir torres celulares, LORAN, y el sistema mundial de navegación orbital por satélite (GLONASS). Además, puede utilizarse una multiplicidad de tales pares de señales de temporización para generar tablas de autentificación más complejas.

Las señales de temporización (204) incluyen información de tiempo y fecha codificada que puede ser extraída por el receptor de RF (102). Mediante triangulación de las señales procedentes de tres satélites (202), el receptor de RF (102) puede ubicar con exactitud su localización geofísica actual en cualquier parte sobre la tierra, generalmente dentro de unos pocos metros. Sin embargo, las variaciones en la ionosfera y la atmósfera (206) debidas al clima, la presión barométrica, la actividad solar, y otros parámetros variables e impredecibles hacen que la pureza de las señales de temporización (204) fluctúe. En particular, las variaciones en la ionosfera y la atmósfera causan retardos impredecibles en las señales de temporización (204). Para compensar estas variaciones, cada satélite (202) del sistema GPS transmite dos señales de temporización (204) en dos frecuencias diferentes (L1 y L2). En realizaciones adicionales, pueden usarse frecuencias de banda lateral procedentes de la misma fuente de temporización para permitir la extracción de variaciones de la línea de visión en el tiempo de retardo rechazando las variaciones del “modo común”.

La fig. 3 es un diagrama de temporización que ilustra señales de temporización (204) procedentes de un satélite de un sistema GPS. Las señales de temporización (204) incluyen una primera señal de temporización (204a) en una primera frecuencia y una segunda señal de temporización (204b) en una segunda frecuencia. Como ilustra la fig. 3, la primera y la segunda señales de temporización (204a) y (204b) están desplazadas una de otra como resultado de variaciones atmosféricas. El retardo de una señal de radio es inversamente proporcional al cuadrado de la frecuencia portadora (es decir, L2 se retrasará más que L1) y proporcional al número total de electrones a lo largo del camino desde el satélite (202) hasta el dispositivo de seguridad (200). El número total de electrones variará de acuerdo con la actividad solar actual, la hora del día (en el receptor), y la longitud y latitud del receptor. Es sabido por alguien experto en la materia que midiendo el retardo entre las señales L1 y L2 desde un satélite particular, se puede calcular el efecto debido a la ionosfera y la troposfera y corregir la variación, mejorando de ese modo la exactitud posicional. Para compensar las variaciones atmosféricas, las realizaciones de la presente invención normalizan la primera y segunda señales de temporización (204a) y (204b) antes de determinar la localización geofísica. Como resultado, se mejora en gran medida la exactitud para el cálculo de localización.

Las realizaciones de la presente invención utilizan las variaciones en las señales de temporización (204) como fuente para un número aleatorio impredecible, denominado en lo sucesivo “valor de inestabilidad”. En particular, la medición de la fluctuación en el retardo de señal de temporización produce un número aleatorio e impredecible cuyo valor depende del valor de momento a momento de los diversos parámetros a lo largo del camino desde el satélite (202) hasta el receptor de RF (102). Por lo tanto, este retardo es específico de cada satélite (202) y el receptor de RF (102) en un momento específico y una localización específica, y es sumamente difícil, si no imposible, de calcular a distancia. Por otra parte, cada satélite GPS (202) está moviéndose continuamente a lo largo de su órbita, introduciendo de ese modo variaciones de retardo adicionales a medida que diferentes partes de la atmósfera de la Tierra se interponen secuencialmente entre el satélite y el dispositivo de seguridad (200). Esto añade un elemento adicional de variabilidad e imprevisibilidad, que se extiende más allá de simples variaciones en las condiciones atmosféricas de la línea de visión. Por consiguiente, esencialmente el único modo de obtener tal retardo es mediante medición directa en el dispositivo de seguridad específico (200). Cabe destacar que aunque la presente descripción se refiere a señales de temporización L1 y L2 procedentes de satélites GPS, cualquier señal de temporización que comparta la misma fuente original pero se propague en diferentes frecuencias, tales como bandas laterales procedentes de una estación de TV o de FM, puede emplearse para permitir la extracción de una medición de inestabilidad similar. Como se ilustra en la fig. 2, la antena de RF (200) en el receptor de RF (102) se utiliza para recibir valores de inestabilidad y proporcionar estos valores al sistema de seguridad y acceso teniendo en cuenta la localización (100) cuando se solicite.

Volviendo a hacer referencia a la fig. 1, la base de datos de LSDF (114) generalmente se construye antes del uso del sistema de seguridad y acceso teniendo en cuenta la localización (100). Más en particular, antes del uso, se construye una LSDF para cada receptor (102a)-(102d) del sistema de seguridad y acceso teniendo en cuenta la localización (100). Como se mencionó anteriormente, los materiales interpuestos contribuyen a la dispersión de las señales de temporización (204), reduciendo de ese modo la intensidad de las señales (comparada con un caso ideal donde no están presentes tales materiales interpuestos) que llegan a cada receptor (102a)-(102d). Correlacionando el grado de atenuación con la dirección de propagación de la señal (caracterizada habitualmente por los ángulos de altitud y acimut de un satélite con respecto al horizonte y la dirección neutral septentrional, meridional o ecuatorial), es posible desarrollar un mapa de la “firma” de atenuación alrededor de un receptor en una localización dada. En la medida en que esta firma sea estable, puede usarse en un momento posterior para verificar si un receptor está o no, de hecho, en una localización caracterizada anteriormente. Así, cada LSDF comprende una pluralidad de valores de inestabilidad atenuada recibidos y procesados en cada receptor (102a)-(102d) para crear una LSDF para cada receptor (102a)-(102d).

La fig. 4 es un diagrama conceptual que ilustra una LSDF (400) y microimpresiones (402) para el receptor ejemplar (102), de acuerdo con una realización de la presente invención. En el ejemplo de la fig. 4, la LSDF (400) representa el espacio de datos de valores basados en valores de inestabilidad recibidos en un receptor particular (102) a lo largo de un periodo de tiempo predefinido. Cada microimpresión (402) representa una menor cantidad de datos basados en valores de inestabilidad recogidos a lo largo de un periodo de tiempo mucho más corto. Por ejemplo, la LSDF (400) puede representar datos recogidos en el receptor (102) a lo largo de un periodo de tiempo de veinticuatro horas, mientras que cada microimpresión (402) representa, por ejemplo, 45 segundos de datos recogidos en el receptor (102). La LSDF (400) para cada receptor (102a)-(102d) es almacenada en la base de datos de LSDF (114) conectada al servidor de autentificación (112). En términos generales, cuando las realizaciones de la presente invención tienen que realizar la verificación, se realiza una petición de los datos de microimpresión actuales (402) desde un receptor particular. Los datos de microimpresión actuales (402) son comparados entonces con la LSDF (400) para el receptor particular. Si los datos de microimpresión actuales (402) entran dentro del alcance de la LSDF (400) para el receptor particular, la autentificación es exitosa, de lo contrario, la autentificación falla.

La fig. 5 es un diagrama de flujo que muestra un procedimiento (500) para autentificar el acceso a un recurso de red protegido, de acuerdo con una realización de la presente invención. En una operación inicial (502) se realizan operaciones preproceso. Las operaciones preproceso pueden incluir, por ejemplo, generar huellas digitales específicas de la localización (LSDF) para cada receptor en el sistema de seguridad, almacenar las LSDF en una base de datos de LSDF, y operaciones adicionales que resultarán evidentes para los expertos en la materia después de una revisión detenida de la presente descripción.

En la operación (504), una petición para acceder a un recurso protegido es recibida en un punto de acceso a red. Volviendo a hacer referencia a la fig. 1, cuando un usuario que usa el ordenador cliente (106) intenta acceder al activo de red protegido (108), el ordenador cliente (106) envía una petición para acceder al recurso protegido (108) al conmutador de red (104). En una realización, se requiere que los ordenadores cliente (106) estén conectados directamente al punto de acceso a red, tal como el conmutador de red (104) para que se les permita acceder al

recurso de red protegido, tal como el activo de red protegido (108).

Es decir, en esta realización, al ordenador cliente (106) no se le permite estar en comunicación con el punto de acceso a red a través de otro nodo de red, sino que se requiere que esté conectado directamente al conmutador de red (104) como se ilustra en la fig. 1. Como se describirá con mayor detalle posteriormente, el equipo de red al cual están conectados los ordenadores cliente, tal como el conmutador de red (104), actúa en nombre del ordenador cliente (106) durante un procedimiento de autentificación para autentificar el acceso al recurso protegido. De esta manera, no se requiere que haya hardware especial integrado dentro de cada ordenador cliente (106) que accede al conmutador de red (104) con el fin de que tenga lugar una autentificación correcta.

En la operación (506), una petición de puesta a prueba es enviada al punto de acceso a red para proporcionar datos de microimpresión actuales para uno o más receptores en comunicación con el punto de acceso a red. Como se ilustra en la fig. 1, una vez que el conmutador de red (104) intenta acceder al activo de red protegido (108), el cortafuegos (110) reconoce que la petición es para acceder a un recurso de red protegido y consulta al servidor de autentificación (112) para autentificar la petición. En respuesta, el servidor de autentificación (112) envía una petición de puesta a prueba al punto de acceso a red, el conmutador de red (104) en la fig. 1. La petición de puesta a prueba es una petición al conmutador de red (104) para proporcionar datos de microimpresión actuales procedentes de uno o más receptores (102a)-(102d). La petición de puesta a prueba puede pedir datos de microimpresión actuales procedentes de todos los receptores (102a)-(102d) o menos receptores. En una realización, el servidor de autentificación (112) puede pedir datos de microimpresión actuales procedentes de un muestreo aleatorio de receptores que pueden cambiar cada vez que es enviada una petición de puesta a prueba. Por ejemplo, el servidor de autentificación (112) puede pedir datos de microimpresión actuales procedentes del receptor (102a), (102c) y (102d).

En respuesta, el conmutador de red (104) reúne datos de microimpresión actuales procedentes de los receptores seleccionados y proporciona los datos al servidor de autentificación (112). Como se mencionó anteriormente, cada microimpresión (402) representa una cantidad de datos basada en valores de inestabilidad recogidos a lo largo de un periodo de tiempo relativamente corto. Por ejemplo, cada microimpresión puede representar, por ejemplo, 45 segundos de datos recogidos en un receptor particular (102). Los datos de microimpresión recogidos para cada receptor seleccionado son utilizados después para autentificar la petición de acceso al recurso de red protegido.

Los datos de microimpresión actuales recogidos son autentificados después con la LSDF para cada receptor seleccionado, en la operación (508). Volviendo a hacer referencia a la fig. 4, cada LSDF (400) representa el espacio de datos de valores basados en valores de inestabilidad recibidos en un receptor particular (102) a lo largo de un periodo de tiempo predefinido. Por ejemplo, la LSDF (400) puede representar datos recogidos en el receptor (102) a lo largo de un periodo de tiempo de veinticuatro horas, mientras que cada microimpresión (402) representa, por ejemplo, 45 segundos de datos recogidos en el receptor (102). La LSDF (400) para cada receptor (102a)-(102d) es almacenada en la base de datos de LSDF (114) conectada al servidor de autentificación (112). Volviendo a la fig. 5, los datos de microimpresión actuales para cada receptor son comparados con la LSDF para el receptor particular. Si los datos de microimpresión actuales entran dentro del alcance de la LSDF para el receptor particular, la autentificación es exitosa para ese receptor. Este procedimiento se repite para cada receptor seleccionado. Si la autentificación es exitosa para cada receptor, la autentificación para la petición de puesta a prueba es exitosa.

Después se toma una decisión en cuanto a si la autentificación para la petición de puesta a prueba es exitosa, en la operación (510). Si la autentificación para la petición de puesta a prueba es exitosa, el procedimiento (500) se ramifica a la operación (512) donde se permite el acceso al recurso de red protegido. De lo contrario, el acceso al recurso de red protegido es bloqueado, en la operación (514). El procedimiento (500) se termina entonces y se realizan operaciones de postproceso en la operación (516). Las operaciones de postproceso pueden incluir emitir un testigo de autentificación temporal al punto de acceso a red que permite el acceso al recurso de red protegido durante un periodo de tiempo predefinido, facilitar el acceso al recurso de red protegido, y operaciones de postproceso adicionales que resultarán evidentes para los expertos en la materia después de una lectura detenida de la presente descripción.

Aunque la invención precedente se ha descrito con cierto grado de detalle con fines de claridad de comprensión, resultará evidente que pueden ponerse en práctica ciertos cambios y modificaciones dentro del alcance de las reivindicaciones adjuntas. Por consiguiente, las presentes realizaciones han de considerarse como ilustrativas y no restrictivas, y la invención no ha de estar limitada a los detalles ofrecidos en este documento, sino que puede modificarse dentro del alcance y los equivalentes de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Sistema para proporcionar seguridad para un recurso de red protegido (108), que comprende:

un aparato de acceso a red (104) en comunicación con una pluralidad de receptores (102a, 102b, 102c, 102d) para recibir señales (204) procedentes de una fuente remota (202), donde el aparato de acceso a red (104) es capaz de recoger datos de microimpresión actuales para cada receptor (102a; 102b; 102c; 102d) de dicha pluralidad de receptores (102a, 102b, 102c, 102d), siendo los datos de microimpresión actuales para un receptor (102a, 102b, 102c, 102d) de dicha pluralidad de receptores (102a, 102b, 102c, 102d) una pluralidad de valores de inestabilidad, estando basado cada valor de inestabilidad en una diferencia en los tiempos de llegada de al menos dos señales de temporización (204a, 204b) recibidas desde dicha fuente remota (202) en dicho receptor (102a, 102b, 102c, 102d) a lo largo de un periodo de tiempo predefinido; y

un servidor de autentificación (112) en comunicación con el aparato de acceso a red (104), teniendo el servidor de autentificación (112) acceso a una huella digital específica de la localización (LSDF-Location Specific Digital Fingerprint) para cada receptor (102a; 102b; 102c; 102d) de dicha pluralidad de receptores (102a, 102b, 102c, 102d), donde la LSDF para un receptor (102a, 102b, 102c, 102d) de dicha pluralidad de receptores (102a, 102b, 102c, 102d) es una pluralidad de valores de inestabilidad, estando basado cada valor de inestabilidad en una diferencia en los tiempos de llegada de al menos dos señales de temporización (204a, 204b) recibidas desde dicha fuente remota (202) en dicho receptor (102a; 102b; 102c; 102d) a lo largo de un periodo de tiempo predefinido anterior al periodo de tiempo predefinido para los valores de datos de microimpresión,

donde el aparato de acceso a red (104) está configurado para proporcionar datos de microimpresión actuales para cada receptor (102a; 102b; 102c; 102d) de dicha pluralidad de receptores al servidor de autentificación (112), y donde el servidor de autentificación (112) está configurado para comparar los datos de microimpresión actuales para cada receptor (102a; 102b; 102c; 102d) de dicha pluralidad de receptores (102a, 102b, 102c, 102d) con la LSDF asociada con el receptor (102a; 102b; 102c; 102d) para autentificar una petición de acceso.

2. Sistema de acuerdo con la reivindicación 1, donde el periodo de tiempo predefinido para los valores de LSDF es más largo que el periodo de tiempo predefinido para los valores de datos de microimpresión.

3. Sistema de acuerdo con la reivindicación 1, donde el aparato de acceso a red (104) está configurado para proporcionar datos de microimpresión actuales para un muestreo aleatorio de receptores seleccionados de la pluralidad de receptores (102a, 102b, 102c, 102d) al servidor de autentificación (112), y donde el servidor de autentificación (112) está configurado para comparar los datos de microimpresión actuales para cada receptor seleccionado con la LSDF asociada con dicho receptor seleccionado para autentificar una petición de acceso.

4. Procedimiento para proporcionar seguridad para un recurso de red protegido (108), que comprende:

enviar mediante un servidor de autentificación (112) una petición de puesta a prueba a un aparato de acceso a red (104) en comunicación con una pluralidad de receptores (102a, 102b, 102c, 102d) que reciben señales (204) procedentes de una fuente remota (202), solicitando la petición de puesta a prueba datos de microimpresión actuales para receptores de dicha pluralidad de receptores (102a, 102b, 102c, 102d), siendo los datos de microimpresión actuales una pluralidad de valores de inestabilidad, estando basado cada valor de inestabilidad en una diferencia en los tiempos de llegada de al menos dos señales de temporización (204a, 204b) recibidas en un receptor de dicha pluralidad de receptores (102a, 102b, 102c, 102d) a lo largo de un periodo de tiempo predefinido;

enviar los datos de microimpresión actuales para los receptores (102a, 102b, 102c, 102d) al servidor de autentificación (112) por medio del aparato de acceso a red (104), teniendo el servidor de autentificación (112) acceso a una LSDF para cada receptor (102a; 102b; 102c;102d) de la pluralidad de receptores (102a, 102b, 102c, 102d), donde la LSDF para un receptor (102a, 102b, 102c, 102d) de dicha pluralidad de receptores (102a, 102b, 102c, 102d) es una pluralidad de valores de inestabilidad, estando basado cada valor de inestabilidad en una diferencia en los tiempos de llegada de al menos dos señales de temporización (204a, 204b) recibidas en dicho receptor a lo largo de un periodo de tiempo predefinido anterior al periodo de tiempo predefinido para los valores de datos de microimpresión; y

comparar mediante el servidor de autentificación (112) los datos de microimpresión actuales para dichos receptores (102a; 102b; 102c; 102d) de dicha pluralidad de receptores (102a, 102b, 102c, 102d) con la LSDF asociada con dichos receptores de dicha pluralidad de receptores (102a, 102b, 102c, 102d) para autentificar una petición de

acceso.

5. Procedimiento de acuerdo con la reivindicación 4, donde el periodo de tiempo predefinido para los valores de LSDF es más largo que el periodo de tiempo predefinido para los valores de datos de microimpresión.

6. Procedimiento de acuerdo con la reivindicación 4, que comprende además enviar datos de microimpresión actuales para cada receptor (102a; 102b; 102c; 102d) de la pluralidad de receptores (102a; 102b; 102c; 102d) al servidor de autentificación (112), y donde el servidor de autentificación (112) compara los datos de microimpresión actuales para cada receptor (102a; 102b; 102c; 102d) con la LSDF asociada con cada receptor (102a; 102b; 102c; 102d) para autentificar una petición de acceso.

7. Procedimiento de acuerdo con la reivindicación 4, que comprende además enviar datos de microimpresión actuales para un muestreo aleatorio de receptores seleccionados de la pluralidad de receptores (102a, 102b, 102c, 102d) al servidor de autentificación (112), y donde el servidor de autentificación (112) compara los datos de microimpresión actuales para cada receptor seleccionado con la LSDF asociada con cada receptor seleccionado para autentificar una petición de acceso.

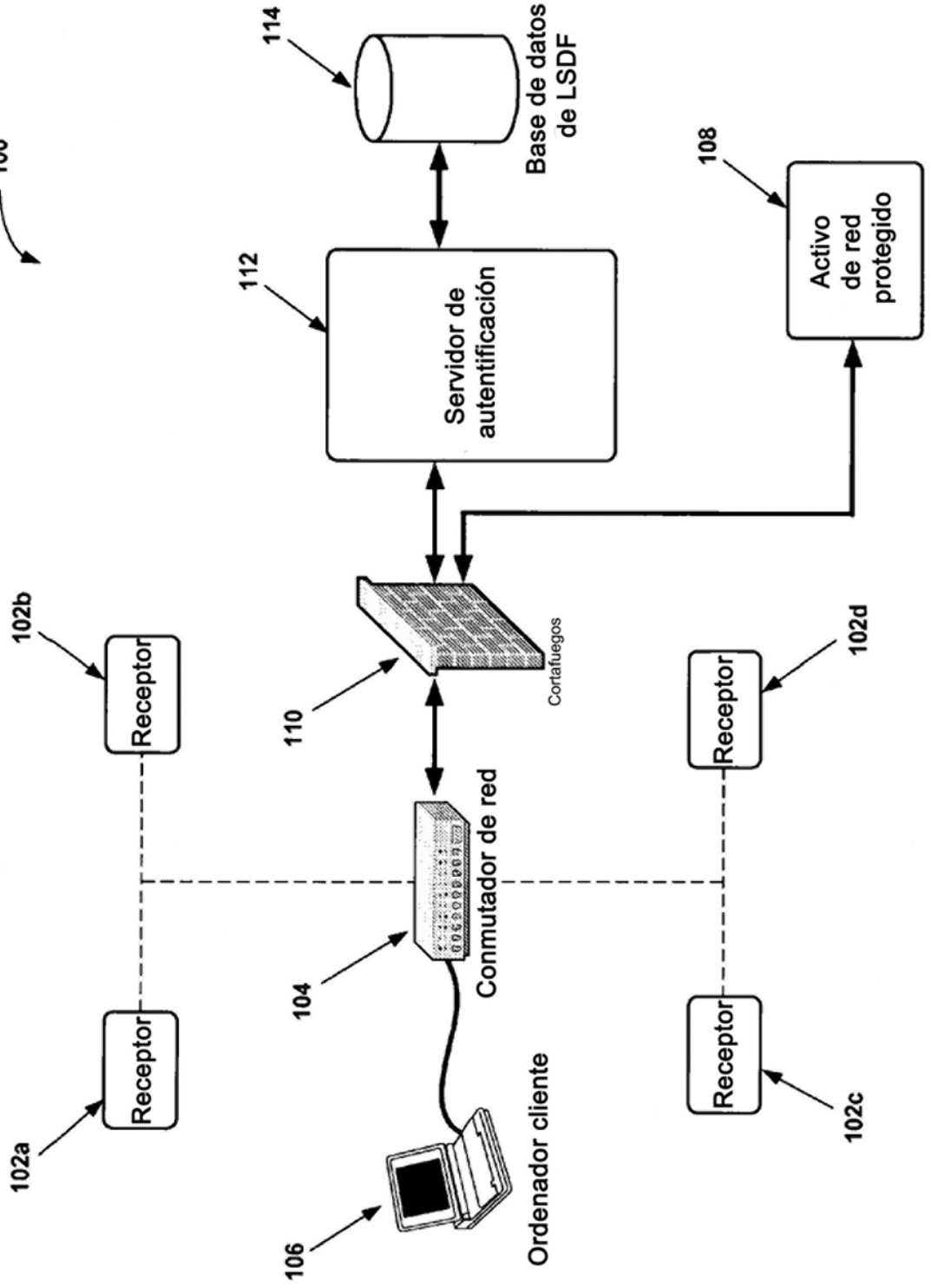
100
114
Base de datos de LSDF
112
Servidor de autentificación
108
Activo de red protegido
110
Cortafuegos
102b
Receptor
102d
Receptor
104
Conmutador de red
102a
Receptor
102c
Receptor
106
Ordenador cliente

FIG. 1

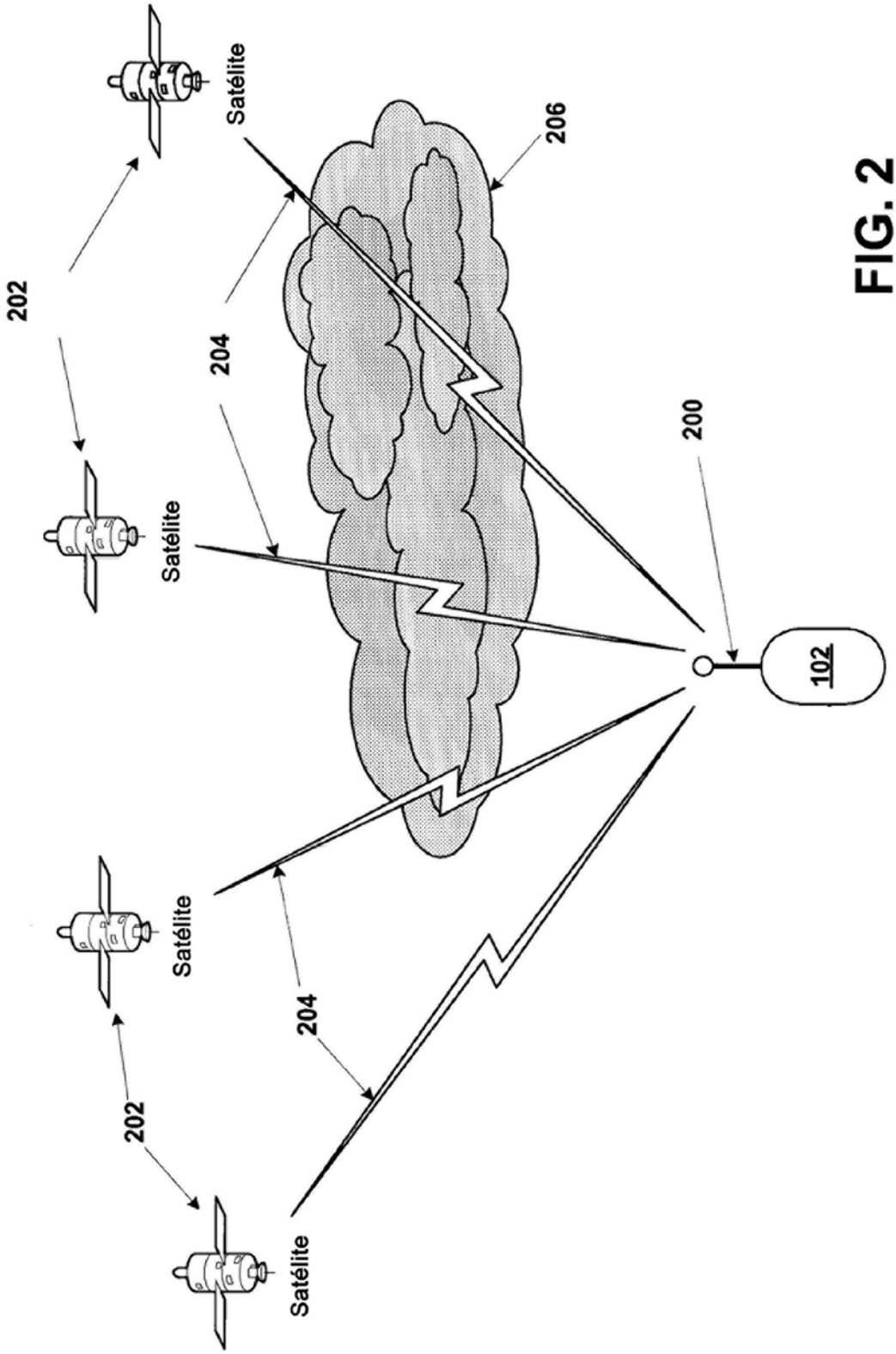
Satélite
206
202
204
200
Satélite
102
Satélite
204
202
Satélite

FIG. 2

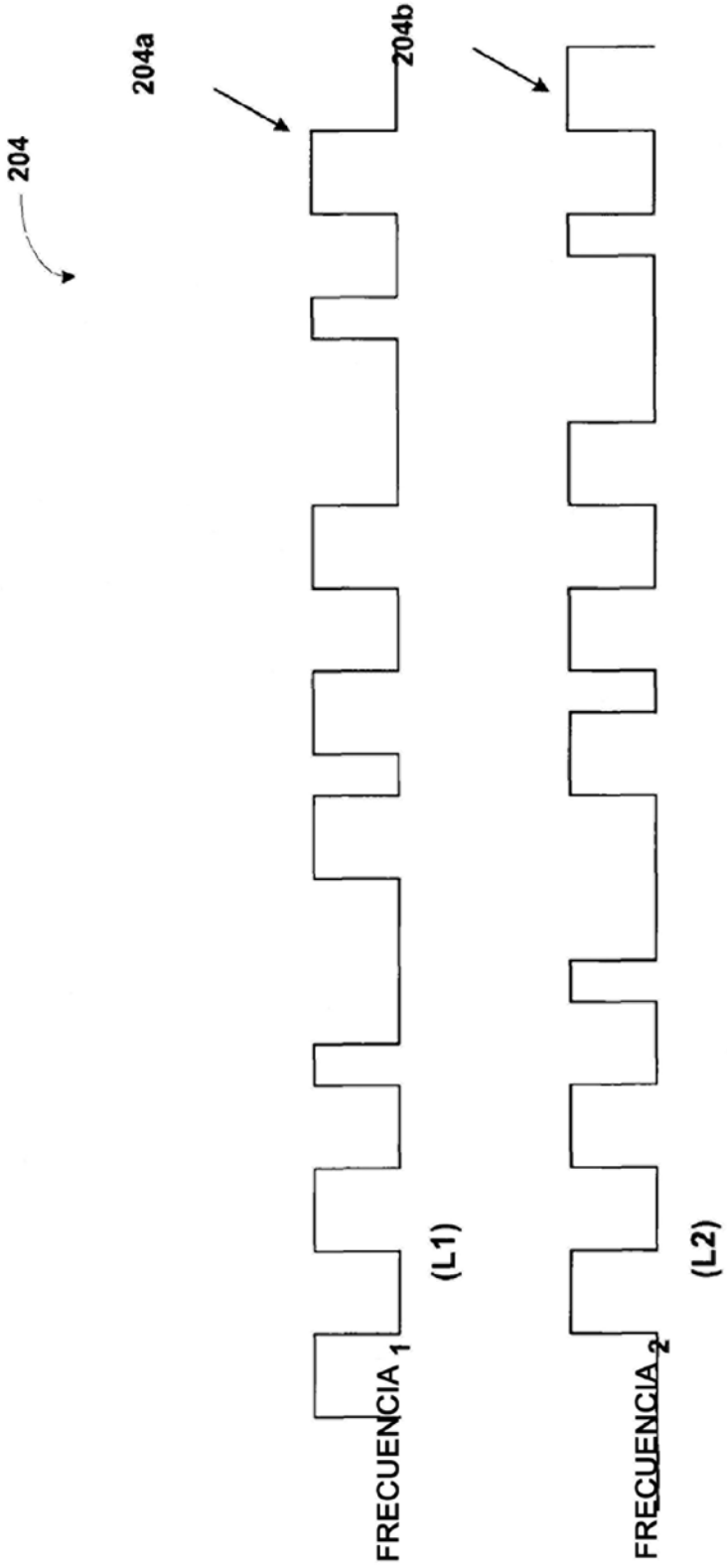

FIG. 3

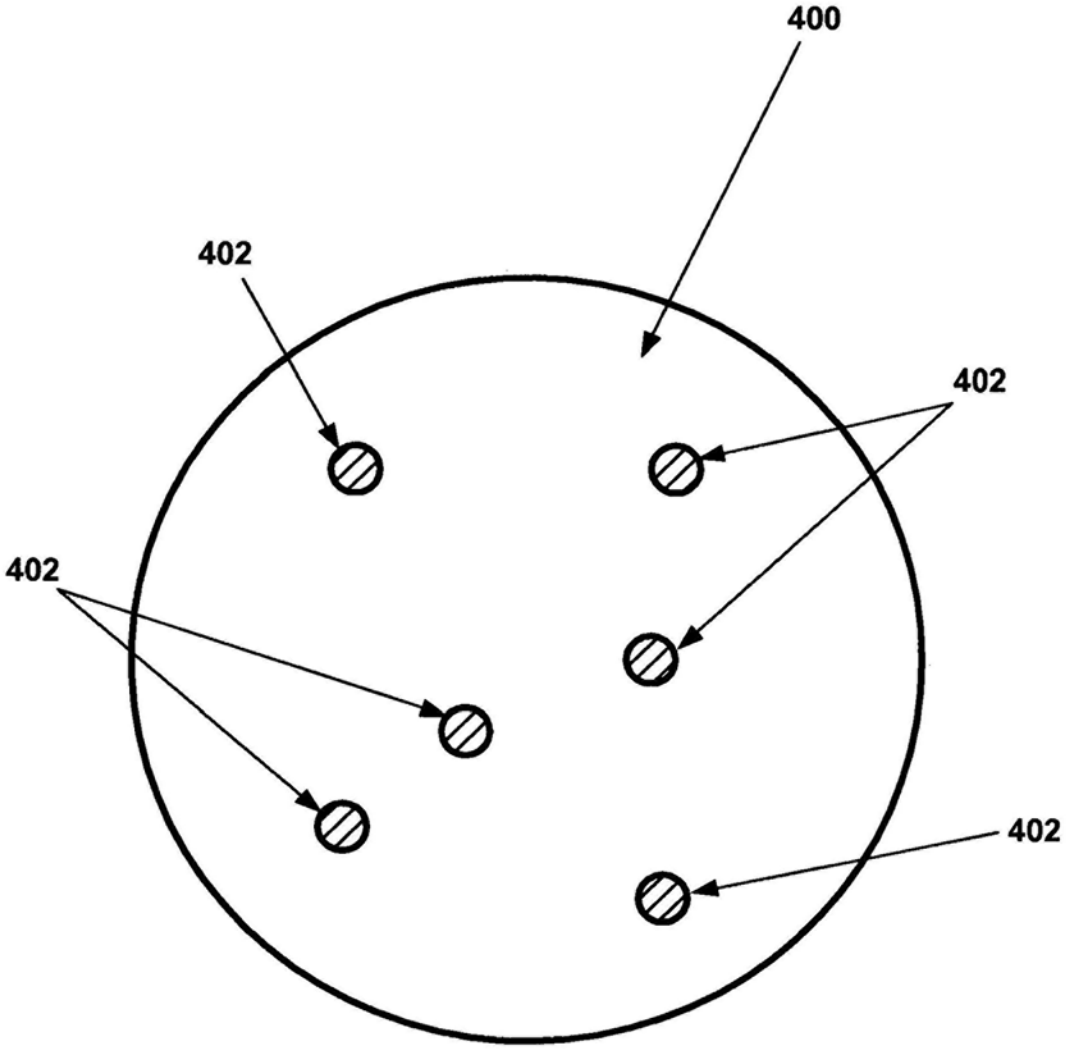

FIG. 4

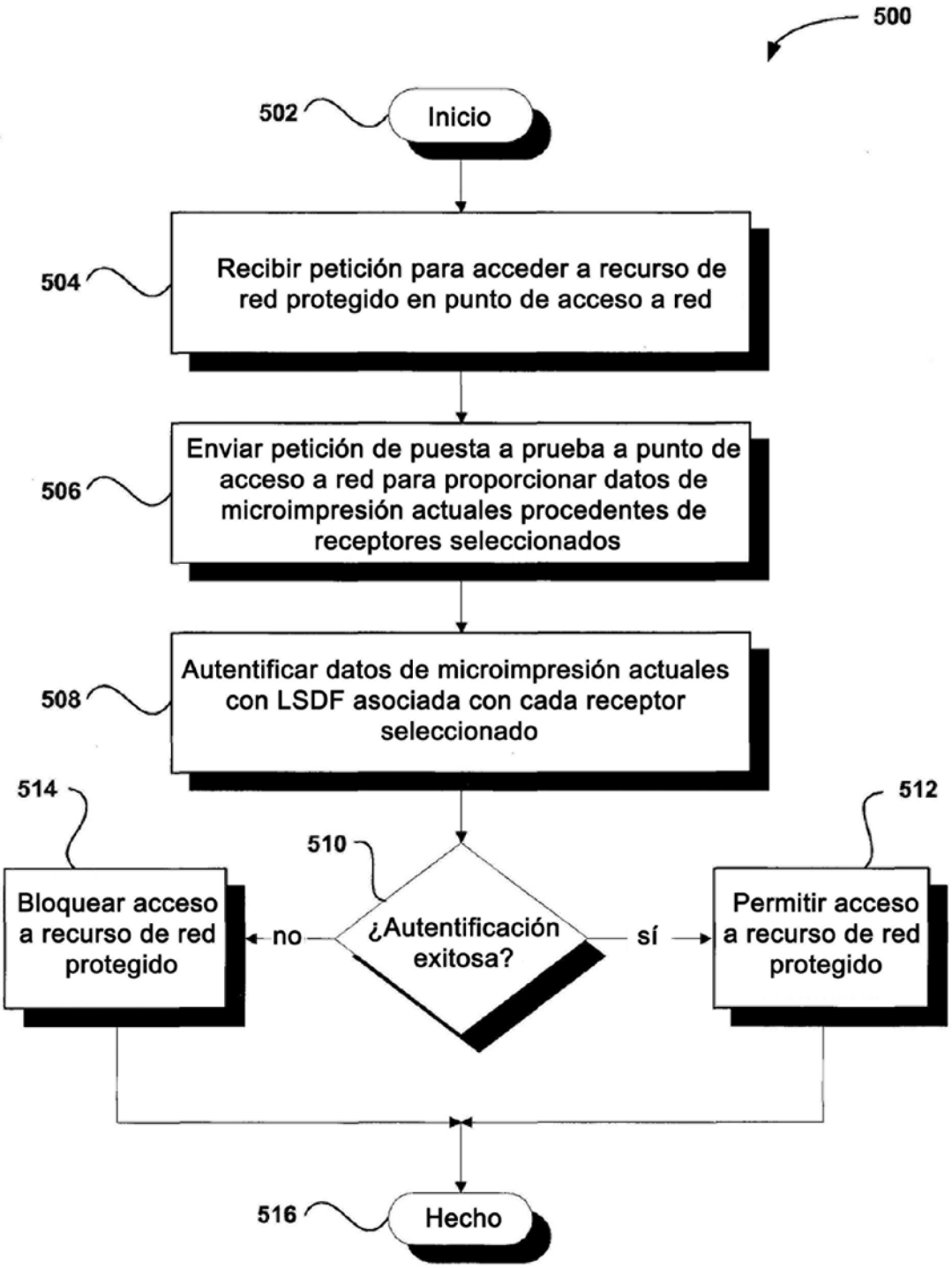
500
502
Inicio
504
Recibir petición para acceder a recurso de red protegido en punto de acceso a red
506
Enviar petición de puesta a prueba a punto de acceso a red para proporcionar datos de microimpresión actuales procedentes de receptores seleccionados
508
Autentificar datos de microimpresión actuales con LSDF asociada con cada receptor seleccionado
510
¿Autentificación exitosa?
no
sí
514
Bloquear acceso a recurso de red protegido
512
Permitir acceso a recurso de red protegido
516
Hecho

FIG. 5