(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 376 499**

(51) Int. CI.:
H04L 12/24 (2006.01)
G07C 9/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08162494 .2**
(96) Fecha de presentación: **18.08.2008**
(97) Número de publicación de la solicitud: **2031801**
(97) Fecha de publicación de la solicitud: **04.03.2009**

(54) Título: **MÉTODO PARA CALCULAR EL VALOR DE ENTROPÍA DE UN SISTEMA DE MEMORIA DINÁMICA.**

(30) Prioridad:
24.08.2007 US 968009 P
08.07.2008 US 166221

(45) Fecha de publicación de la mención BOPI:
14.03.2012

(45) Fecha de la publicación del folleto de la patente:
14.03.2012

(73) Titular/es:
ASSA ABLOY AB
KLARABERGSVIADUKTEN 90 P.O. BOX 70340
107 23 STOCKHOLM, SE

(72) Inventor/es:
Hulusi, Tam y
Wamsley, Robert

(74) Agente/Representante:
Curell Aguilá, Mireia

DESCRIPCIÓN

Método para calcular el valor de entropía de un sistema de memoria dinámica.

Campo de la invención

La presente invención se refiere en general a sistemas, dispositivos, y métodos de control de acceso. Más específicamente, la presente invención está relacionada con la diseminación de información en un sistema de control de acceso que tiene por lo menos un lector no conectado en red.

Antecedentes

Históricamente, los sistemas de acceso de control se han interconectado en su totalidad mediante conexiones por cable y/o inalámbricas. Más específicamente, los lectores y otros tipos de anfitriones de mensajes están generalmente en comunicación con un sistema de control centralizado tal como un panel de control centralizado. La interconectividad del sistema permite diseminar de manera rápida y eficaz actualizaciones de las políticas por todo el sistema de control de acceso. Si es necesaria una actualización de una política (por ejemplo, el envío de permisos de acceso nuevos a todos los lectores), entonces el panel de control centralizado enviaría un mensaje a los anfitriones de mensajes conectados en red notificándoles la nueva política.

Aunque estos sistemas interconectados en su totalidad ayudan a facilitar actualizaciones de políticas eficaces, los mismos resultan caros de instalar y mantener, especialmente en grandes instalaciones en las que se requiere una cantidad significativa de dispositivos de comunicación por cable y/o inalámbricos para conseguir que cada anfitrión de mensajes esté en comunicación con el panel de control centralizado. De este modo, los anfitriones de mensajes no conectados en red (es decir, anfitriones de mensajes que no están en comunicación con un sistema de control centralizado a través de una vía de comunicación directa o anfitriones de mensajes que tienen una vía de comunicación que resulta no estar disponible), a los cuales se hace referencia también como anfitriones locales, están resultando cada vez más deseables debido a su autonomía y el bajo coste asociado a su instalación y mantenimiento. El lado negativo de instalar anfitriones de mensajes no conectados en red es que resulta más difícil garantizar que el anfitrión de mensajes no conectado en red recibe actualizaciones de políticas.

El artículo de BEAUFOUR A *ET AL*. “Smart-tag based data dissemination” PROCEEDINGS OF THE ACM INTERNATIONAL WORKSHOP ON WIRELESS SENSOR NETWORKS AND APPLICATIONS 2002 ASSOCIATION FOR COMPUTING MACHINERY US, [Online] 2002, páginas 68 a 77, XP002552171, da a conocer un método de diseminación de etiquetas inteligentes, de acuerdo con el preámbulo de la reivindicación 1.

El documento EP 1 351 441 da a conocer una disposición en la que un gestor de políticas genera automáticamente actualizaciones de archivos de configuración para los encaminadores en la red, según resulte necesario, envía dichas actualizaciones a los encaminadores apropiados, y provoca que los encaminadores instalen las actualizaciones de los archivos de configuración en tiempo real. La generación automática de actualizaciones de archivos de configuración se lleva a cabo en respuesta a información que es entregada al gestor de políticas desde un sistema de medición de tráfico y de análisis de flujo que sustituye al sistema de analizador de la técnica anterior. La información que es generada por el sistema de medición de tráfico y de análisis de flujo es sensible a umbrales que son instalados por el gestor de políticas en el sistema de medición de tráfico y de análisis de flujo.

El documento EP 1 026 855 da a conocer un método de medición del rendimiento de comunicaciones de una red en el que se envían paquetes de medición a intervalos iguales desde una unidad emisora hacia un trayecto de la red. Los paquetes de sondeo son recibidos por una unidad de recepción, la cual mide el tiempo de transmisión de los paquetes para estimar un ancho de banda disponible de un trayecto de la red a partir de un parámetro Q indicativo de una correlación en el tiempo de transmisión de paquetes entre paquetes adyacentes.

Sumario

Las colonias en sistemas de acceso de control que carecen de una comunicación de largo alcance o directa entre anfitriones de mensajes pueden propagar mensajes entre anfitriones de mensajes por medio de un portador de mensajes intermediario. Los anfitriones de mensajes son típicamente objetos estacionarios, tales como un lector de control de acceso. Los portadores de mensajes son típicamente objetos móviles, tales como un testigo de control de acceso. Un objeto de mensaje contiene datos o información, tal como políticas de control de acceso, que pueden ser entendidos y usados por los anfitriones de mensajes. Los objetos de mensaje se pueden originar en uno o más anfitriones de mensajes y pueden ser usados por anfitriones de mensajes para realizar una acción, tal como conceder acceso a un área segura. Un objeto de mensaje se puede introducir utilizando uno o más miembros existentes de cualquier colonia o puede ser miembros de la colonia recién introducidos. En un sistema que contiene una colonia de anfitriones de mensajes y una colonia de portadores de mensajes, los portadores de mensajes pueden transportar un mensaje desde un anfitrión de mensajes a otro, propagando de este modo el objeto de mensaje entre la colonia de anfitriones de mensajes.

Un mensaje que se origina en uno o más anfitriones de mensajes se puede llevar desde el anfitrión de mensajes a un portador de mensajes cuando el anfitrión de mensajes y el portador de mensajes están muy próximos entre ellos. Si posteriormente un segundo portador de mensajes se sitúa muy próximo a un anfitrión de mensajes que origina un objeto de mensaje, el objeto de mensaje se puede llevar desde el anfitrión de mensajes al segundo portador de mensajes. Un portador de mensajes, después de tener conocimiento del objeto de mensaje, puede transportar el objeto de mensaje desde un anfitrión de mensajes con conocimiento del objeto de mensaje, tal como un anfitrión de mensajes que origina un objeto de mensaje, a un segundo anfitrión de mensajes que no tiene conocimiento del objeto de mensaje y, a continuación, puede llevar el objeto de mensaje desde el portador de mensajes al segundo anfitrión de mensajes cuando el portador de mensajes está muy próximo al segundo anfitrión de mensajes. Después de llevar el objeto de mensaje al segundo anfitrión de mensajes, el segundo anfitrión de mensajes tiene conocimiento del objeto de mensaje.

Los sistemas de dos colonias se usan, por ejemplo, en modelos de control de acceso desconectados. Dichos sistemas proporcionan una solución sencilla y elegante para el control del acceso sin la necesidad de conectar lectores a una red por cable. Estos sistemas proporcionan una solución segura y elegante para el control del acceso cuando se rechaza el coste o la instalación de una red por cable. Aunque estos sistemas se han estado usando durante más de veinte años, todavía no se ha logrado la optimización de los mismos.

Es por lo tanto un aspecto de la presente invención mejorar el estado actual de la técnica proporcionando un resultado útil, concreto, y tangible que se pueda usar para entender y diseñar una comunicación óptima en sistemas de dos colonias. Este programa se puede aplicar de forma más general al entendimiento y la optimización de sistemas de dos colonias tales que se basen en portadores de mensajes para distribuir objetos de mensaje a anfitriones de mensajes no conectados en red.

Las formas de realización de la presente invención definen un parámetro que proporciona una medida del comportamiento de diseminación de información en un sistema que tiene anfitriones de mensajes que se pueden comunicar entre sí usando un portador de mensajes como intermediario. Entre los sistemas ejemplificativos del tipo descrito en el presente documento se encuentran el reparto de correo, en el que un mensaje, en forma de una carta, es transportado desde una ubicación a otra o, en la naturaleza, una colonia de abejas que transportan polen de una planta a otra. Lo que tienen en común estos sistemas es que los portadores de mensajes forman una red. La red está compuesta por conexiones transitorias y asimétricas entre los anfitriones. Un sistema de alto rendimiento se define en el presente documento como el que tiene capacidad de entregar eficazmente un mensaje por medio de los portadores de mensajes y que está distribuido entre los anfitriones. Por lo menos una forma de realización de la presente invención proporciona un método de medición de la eficacia de diseminación de información en estos sistemas y, cuando resulta posible, mejora esa eficacia.

Las redes de Mundo Pequeño están caracterizadas por redes localizadas que están conectadas entre sí por enlaces críticos que proporcionan un atajo entre agrupamientos por otro lado distantes o no conectados. Un ejemplo popular es el juego de Kevin Bacon en el que el objetivo es encontrar un camino entre cualquier actor de una película y Kevin Bacon usando apariciones en las mismas películas como conexiones. Las conexiones entre agrupamientos locales (películas) son realizadas por un actor que aparece en ambas películas.

Una diferencia importante entre la red de actores del juego de Kevin Bacon y una red definida por anfitriones de mensajes y portadores de mensajes en un sistema de control de acceso es que una conexión realizada por dos actores que aparecen en la misma película es permanente y bidireccional, mientras que la conexión entre dos anfitriones de mensajes de nuestro sistema es un acontecimiento transitorio y unidireccional. Esta diferencia requiere una táctica ligeramente diferente a la usada típicamente para estudiar redes de Mundo Pequeño. En lugar de tratar la población de portadores de mensajes como vértices y los anfitriones de mensajes como bordes, o al revés, dos poblaciones diferenciadas se tratan ambas como vértices mientras que el transporte de un objeto de mensaje entre estas poblaciones se trata como un borde.

Esta diferencia requiere modificaciones en muchas de las herramientas convencionales de teoría de grafos usadas para estudiar redes. Por ejemplo, si se tratase como una red convencional, una distribución de grados se definiría usando las conexiones de anfitrión de mensajes-a-anfitrión; sin embargo, de acuerdo con por lo menos algunas formas de realización de la presente invención, la distribución de grados describirá conexiones de anfitrión de mensajes-a-portador y portador de mensajes-a-anfitrión.

En relación con la distribución de grados, una matriz de adyacencia no será un retículo cuadrado de nxn sino que tendrá dimensiones con el número de portadores de mensajes en un lado y el número de anfitriones de mensajes en el otro. Puesto que cada acontecimiento representa efectivamente medio paso en el proceso de compartir un objeto de mensaje entre dos componentes similares, la matriz de adyacencia tradicional se puede hallar cuadrando la matriz del sistema de dos vértices.

Otra consecuencia de la conexión transitoria es que la conexión definida en una matriz de adyacencia se debe sustituir por un peso de probabilidad que representa la fuerza de la conexión para crear una matriz de adyacencia ponderada. Para simular la propagación de objetos de mensaje en el sistema de dos colonias se puede usar un

Monte Carlo de Cadenas de Markov basado en una matriz de adyacencia ponderada, modelada. La matriz de adyacencia ponderada de portador de mensajes-a-anfitrión de mensajes, W, es el motor que describe el flujo de información en esta red de dos colonias.

La invención se define a través del método de la reivindicación 1 y el dispositivo de la reivindicación 14. En las reivindicaciones dependientes respectivas se proporcionan varias formas de realización.

Es un objetivo de la presente invención proporcionar un sistema de control de acceso seguro, capaz de funcionar con anfitriones de mensajes no conectados en red (es decir, lectores que contienen una conexión que no es por cable con una base de datos centralizada y que funcionan de forma casi autónoma).

Se puede usar un modelo Monte Carlo de Cadenas de Markov con el fin de examinar el rendimiento de una colonia de portadores de mensajes para distribuir objetos de mensajes entre una colonia de anfitriones de mensajes. Se puede definir una medida del rendimiento para estimar la posibilidad de que una actualización no llegue a su objetivo antes de que sea necesario.

Las redes desconectadas de control de acceso se pueden modelar como dos poblaciones separadas aunque interdependientes, portadores de mensajes y anfitriones de mensajes. La interdependencia se crea debido a que cada población solamente puede recibir información de la otra población cuando no hay ningún acontecimiento directo de portador de mensajes-a-portador de mensajes o de puerta-a-puerta, dando como resultado una ecuación diferencial parcial acoplada.

Las relaciones halladas en redes desconectadas pueden incluir un escalamiento para el número total de conexiones que sigue la media geométrica del número de portadores de mensajes y anfitriones de mensajes. De acuerdo con por lo menos algunas formas de realización de la presente invención, las fuerzas de conexión entre portadores de mensajes y anfitriones de mensajes siguen una distribución Zipf-Mandelbrot con una potencia de 2.

La entropía de seguridad del sistema se puede definir como una medida del estado de orden correspondiente al sistema, por ejemplo, se podría definir como la probabilidad de que una actualización no llegue a su objetivo dado un estado del sistema dependiente del tiempo. La entropía de seguridad se puede calcular y comparar con datos muestreados de control de acceso y se puede usar para medir el valor de seguridad con respecto a un punto de referencia de rendimiento del sistema. La entropía de seguridad de un sistema completamente conectado sería cero, lo cual indica que el sistema está actualizado en su totalidad. Los sistemas desconectados o parcialmente conectados tendrán una entropía de seguridad que puede ser mayor que cero. También se pueden proponer remedios para reducir la entropía de seguridad y, por lo tanto, mejorar el rendimiento del sistema. Dichas proposiciones pueden incluir sugerencias para modificar una configuración propuesta de anfitriones de mensajes (por ejemplo, modificando el número, ubicación, y/o capacidades de comunicación de red de los anfitriones) y de portadores de mensajes (por ejemplo, modificando el número, tipo, y permisos de portadores).

El Sumario ni está destinado ni debería considerarse como representativo del alcance y ámbito completos de la presente invención. La presente invención se expone con varios niveles de detalle en el Sumario así como en los dibujos adjuntos y en la descripción detallada de la invención, y ni la inclusión ni la no inclusión de elementos, componentes, etcétera, en el Sumario pretenden limitar el alcance de la presente invención. Se pondrán más fácilmente de manifiesto aspectos adicionales de la presente invención, a partir de la descripción detallada, cuando la misma se considere en particular junto con los dibujos.

Breve descripción de los dibujos

La figura 1 representa unas instalaciones protegidas, de acuerdo con formas de realización de la técnica anterior;

la figura 2 representa un sistema de control de acceso de acuerdo con formas de realización de la presente invención;

la figura 3 representa componentes de un lector de acuerdo con formas de realización de la presente invención;

la figura 4 representa una estructura de datos usada para organizar historiales de comunicación e información de políticas de acuerdo con formas de realización de la presente invención;

la figura 5 representa componentes de una credencial de acuerdo con formas de realización de la presente invención;

la figura 6 representa una herramienta de análisis de red usada para optimizar la diseminación de información en el sistema de control de acceso de acuerdo con formas de realización de la presente invención;

la figura 7 es un diagrama de flujo que representa un método de optimización de una configuración de red con respecto a la diseminación de información, de acuerdo con formas de realización de la presente invención;

la figura 8 es un diagrama de flujo que representa un método de determinación de información de diseminación de información de acuerdo con formas de realización de la presente invención;

la figura 9 es un diagrama de flujo que representa un método de optimización de diseminación de información en una configuración de red fija de acuerdo con formas de realización de la presente invención;

la figura 10 es un diagrama que ilustra una distribución de grados de conexiones con miembros de acuerdo con formas de realización de la presente invención; y

la figura 11 es un diagrama que ilustra la propagación de mensajes a través del sistema de control de acceso en función del tiempo, de acuerdo con formas de realización de la presente invención.

Descripción detallada

La invención se describirá a continuación conjuntamente con un sistema ejemplificativo de control de acceso. Aunque resulta muy adecuada para su uso con, por ejemplo, un sistema que use lectores y/o credenciales de control de acceso, la invención no se limita a su uso con ningún tipo particular de sistema de control de acceso o configuración de elementos del sistema. Los expertos en la materia reconocerán que las técnicas dadas a conocer se pueden usar en cualquier aplicación de mensajería de datos en la que resulte deseable optimizar la diseminación de información por toda la red.

Los sistemas y métodos ejemplificativos de esta invención se describirán también en relación con software de análisis, módulos, y hardware de análisis asociado. No obstante, para evitar complicar innecesariamente la presente invención, la siguiente descripción omite estructuras, componentes y dispositivos bien conocidos que se pueden mostrar en forma de diagrama de bloques, que son bien conocidos, o que se sintetizan de otra manera.

Con fines explicativos, se exponen numerosos detalles para proporcionar una comprensión minuciosa de la presente invención. No obstante, debería apreciarse que la presente invención se puede llevar a la práctica de varias maneras más allá de los detalles específicos expuestos en el presente documento.

Las formas de realización de la presente invención están relacionadas en general con dispositivos y métodos de uso de dichos dispositivos en un sistema de acceso seguro. Aunque resultan muy adecuadas para su uso en sistemas y métodos que utilizan protocolos de comunicación de RF, las formas de realización de la presente invención pueden resultar adecuadas para su uso en sistemas que utilicen otros protocolos de comunicación incluyendo, entre otros, protocolos de comunicación óptica, protocolos de comunicación magnética, mensajes químicos, y similares.

En referencia inicialmente a la figura 1, se describirán unas instalaciones protegidas 100 de acuerdo con por lo menos algunas formas de realización de la presente invención. Las instalaciones protegidas 100 presentadas se pueden corresponder con unas instalaciones reales que dispongan de equipos de control de acceso. Alternativamente, las instalaciones protegidas 100 pueden ser simuladas y la ubicación representada de los equipos se puede corresponder con ubicaciones posibles. Por ejemplo, las instalaciones se pueden presentar en una interfaz de usuario de una estación informática tal como un ordenador personal, un ordenador portátil, o similares, y cada uno de los equipos de control de acceso puede representar equipos concretos que se pueden usar en unas instalaciones reales.

De acuerdo con por lo menos una forma de realización de la presente invención, las instalaciones protegidas 100 pueden comprender una pluralidad de puntos de acceso 104 que presenten, cada uno de ellos, un anfitrión de mensajes asociado al mismo. Los puntos de acceso 104 pueden comprender puntos de acceso al interior de las instalaciones 100. Alternativamente, los puntos de acceso 104 pueden comprender puntos de acceso a salas dentro de las instalaciones 100.

En la forma de realización representada, los anfitriones de mensajes se corresponden con lectores de control de acceso 108. Además de puntos de acceso 104, las instalaciones 100 pueden comprender uno o más activos 106. Los ejemplos de activos 106 pueden incluir recursos informáticos protegidos (por ejemplo, bases de datos, ordenadores, ordenadores portátiles, servidores, etcétera), recursos financieros (por ejemplo, cuentas bancarias, cuentas de crédito, información financiera, etcétera), recursos físicos (por ejemplo, equipos de oficina, cajas fuertes, archivos, etcétera).

Los activos 106 también pueden comprender un anfitrión de mensajes correspondiente para controlar/restringir/monitorizar el acceso al activo 106. De acuerdo con por lo menos algunas formas de realización de la presente invención, los lectores 108 se pueden usar para controlar el acceso de un usuario a través de un punto de acceso asociado 104 ó a un activo asociado 106. Se puede emitir, destinada a un usuario, una credencial 112, la cual puede ser presentada a un lector 108 cuando un usuario desee acceder a través de un punto de acceso 104 ó a un activo 106. Las credenciales 112 pueden comprender información de autenticación que se puede comunicar de forma inalámbrica a los lectores 108 para la verificación de los permisos de acceso del usuario.

Cuando un lector 108 verifica que al mismo se le ha presentado una credencial válida 112, a continuación el lector 108 puede permitir que el usuario acceda al punto de acceso asociación 104 y/o activo 106. De acuerdo con al menos una forma de realización de la presente invención, la decisión de control de acceso se puede tomar basándose en las credenciales 112 en lugar de los lectores 108. En la solicitud de patente U.S. n.º 11/778.145, titulada "Method and Apparatus for Making a Decision on a Card", cuyo contenido completo se incorpora por la presente en este documento con esta referencia, se describen otros detalles de una forma de realización tal en la que se pueden tomar decisiones basándose en la credencial 112.

Además de transportar la información de validación de un usuario, las credenciales 112 se pueden usar como portadores de mensajes para transportar objetos de mensaje a los anfitriones de mensajes (es decir, lector 108). Las credenciales ejemplificativas 112 pueden incluir, entre otros, tarjetas de proximidad de Radiofrecuencia (RF), tarjetas inteligentes de RF, tarjetas de banda magnética, credenciales de acceso basadas en medios ópticos, credenciales de autenticación biométrica, llaveros, CD-ROMS, memorias flash, y cualquier otro soporte portátil capaz de almacenar un objeto de mensaje y de comunicar el objeto de mensaje a un anfitrión de mensajes. De acuerdo con al menos algunas formas de realización de la presente invención, por lo menos algunos de los anfitriones de mensajes (es decir, lector 108) en las instalaciones son no conectados en red, lo cual significa que no tienen ningún mecanismo directo de comunicación con ningún otro anfitrión de mensajes. En su lugar, dichos anfitriones de mensajes no conectados en red se basan en los portadores de mensajes para recibir un objeto de mensaje y compartir objetos de mensaje con otros anfitriones de mensajes no conectados en red.

La figura 2 representa otros detalles de un sistema de acceso seguro 200 de acuerdo con al menos algunas formas de realización de la presente invención. El sistema de acceso seguro 200 incluye en general una población de anfitriones de mensajes, típicamente en forma de lectores de control de acceso. La población de anfitriones de mensajes se puede dividir en dos tipos, a saber, anfitriones de mensajes conectados en red 204 y anfitriones de mensajes no conectados en red 208. Los anfitriones de mensajes conectados en red 204 comprenden la capacidad de comunicarse directamente con por lo menos otro dispositivo de control de acceso, tal como otro anfitrión de mensajes conectado en red 204 ó un servidor 212. La conexión directa entre los anfitriones de mensajes conectados en red 204 y los otros dispositivos de control de acceso la puede facilitar una conexión de red 216. La conexión de red 216 puede presentarse en forma de un enlace de comunicaciones por cable y/o inalámbrico.

Debido a su conectividad directa con otros dispositivos de control de acceso, los anfitriones de mensajes conectados en red 204 pueden compartir objetos de mensaje entre sí sin requerir un portador de mensajes intermediario 220. El servidor 212 puede comprender un servidor de permisos o algún otro tipo de panel de control centralizado que distribuya objetos de mensaje, tales como información de políticas de control de acceso, a otros anfitriones de mensajes conectados en red 204. De acuerdo con por lo menos una forma de realización de la presente invención, los anfitriones de mensajes conectados en red 204 se pueden usar como dispositivos de control de acceso que den origen a objetos de mensaje en todo el sistema de acceso seguro 200. Los anfitriones de mensajes conectados en red 204 pueden recibir originalmente objetos de mensaje desde el servidor 212 a través de la conexión de red 216. A continuación, cuando un portador de mensajes 220, tal como una credencial 112, entra dentro del alcance de comunicaciones del anfitrión de mensajes conectado en red 204, el anfitrión de mensajes conectado en red 204 puede comunicar el objeto de mensaje al portador de mensajes 220. A continuación, el portador de mensajes 220 puede almacenar el objeto de mensaje y llevar el objeto de mensaje a cualquier otro anfitrión de mensajes con el que se comunique. De esta manera, el portador de mensajes 220 se puede usar para transportar un objeto de mensaje desde un anfitrión de mensajes conectado en red 204 a un anfitrión de mensajes no conectado en red 208.

De acuerdo con por lo menos una forma de realización de la presente invención, el portador de mensajes 220 comprende una credencial habilitada para RF y los anfitriones de mensajes 204, 208 comprenden lectores habilitados para RF. Cuando el portador de mensajes 220 se lleva dentro de un alcance de comunicaciones predefinido del anfitrión de mensajes 204, 208, se puede establecer un diálogo de RF entre el anfitrión de mensajes 204, 208 y el portador de mensajes 220. Durante este diálogo de comunicación, el anfitrión de mensajes 204, 208 puede comunicar cualquier tipo de objetos de mensaje activos o más actuales al portador de mensajes 220. El portador de mensajes 220, de una manera similar, puede comunicar cualquier tipo de objetos de mensaje activos o más actuales que tenga almacenados en su memoria al anfitrión de mensajes 204, 208. Esto permite que el portador de mensajes 220 suministre objetos de mensaje nuevos al anfitrión de mensajes 204, 208 y que reciba objetos de mensaje nuevos desde el anfitrión de mensajes 204, 208. Por lo tanto, el portador de mensajes 220 se puede usar como un mecanismo para que los anfitriones de mensajes no conectados en red 208 compartan cualesquiera objetos de mensaje que tengan con otros dispositivos en el sistema de acceso seguro 200.

De acuerdo con por lo menos algunas formas de realización de la presente invención, a los portadores de mensajes 220 únicamente se les puede permitir enviar y/o recibir objetos de mensaje hacia/desde anfitriones de mensajes 204, 208 después de que el portador de mensajes 220 haya sido autenticado por el anfitrión de mensajes 204, 208 y el anfitrión de mensajes 204, 208 haya determinado que el portador de mensajes 220 tiene actualmente permiso para acceder al punto de acceso 104 ó activo 106 asociado al anfitrión de mensajes 204, 208. Esto resulta particularmente útil para ayudar a impedir la transmisión de objetos de mensaje malos o alternativamente no autorizados, por todo el sistema de acceso seguro 200. Los anfitriones de mensajes 204, 208 pueden restringir la aceptación de un objeto de mensaje de un portador de mensajes 220 hasta que el mismo haya autenticado el

portador de mensajes y determinado que sus permisos de acceso son válidos. Adicionalmente, los anfitriones de mensajes 204, 208 pueden abstenerse de enviar un objeto de mensaje a portadores de mensajes 220 hasta que se hayan producido una autenticación y validación correctas del portador de mensajes 220.

En referencia a continuación a la figura 3, se describirán detalles de un lector 108 ó tipo similar de anfitrión de mensajes 204, 208 de acuerdo con por lo menos algunas formas de realización de la presente invención. El lector 108 comprende en general la capacidad de leer automáticamente datos, típicamente en forma de un objeto de mensaje y/o información de validación, de una credencial 112. El lector 108 también puede tener la capacidad de escribir datos, típicamente en forma de un objeto de mensaje, de nuevo en la credencial 112.

El lector 108, de acuerdo con por lo menos una forma de realización, comprende una interfaz de comunicación con credenciales 304 usada para comunicarse una y otra vez con la credencial 112. La interfaz de comunicación con credenciales 304 puede comprender una interfaz de comunicación de RF (por ejemplo, una antena de RF), una interfaz de comunicación magnética (por ejemplo, un lector de banda magnética), una interfaz de comunicación óptica (por ejemplo, un detector y transmisor de infrarrojos), una interfaz de comunicación por contacto eléctrico, o cualesquiera otros medios de comunicación de información a/desde una credencial 112.

Conectado con la interfaz de comunicación 304 se encuentra un controlador 308. En una forma de realización, el controlador 308 incluye un microprocesador, un generador de números aleatorios, y un co-procesador criptográfico. El controlador 308 tiene la capacidad de modular/demodular apropiadamente datos enviados a y recibidos desde dispositivos externos tales como la credencial 112. El controlador 308 controla y determina cómo se comporta el lector 108 cuando al mismo se le presenta una credencial 112. El controlador 308 puede incluir cualquier procesador programable de propósito general, procesador de señal digital (DSP) o controlador para ejecutar una programación de aplicaciones. Alternativamente, el controlador 308 puede comprender un Circuito Integrado de Aplicación Específica (ASIC) configurado especialmente.

El controlador 308 también puede estar provisto de circuitería de control capaz de manipular un dispositivo de control de acceso. El dispositivo de control de acceso está diseñado para proteger el punto de acceso 104 ó activo 106 que está siendo protegido por el lector 108. El controlador 308 está habilitado para comunicarse con el dispositivo de control de acceso a través de la interfaz de dispositivo de control de acceso 332. Los ejemplos de un dispositivo típico de control de acceso incluyen, entre otros, una cerradura electrónica, una cerradura magnética, o un pestillo eléctrico para una puerta, un mecanismo de bloqueo para un sistema de ordenador, un mecanismo de bloqueo para una base de datos, un mecanismo de bloqueo en una cuenta bancaria, o un mecanismo de bloqueo en una aplicación informática. En una forma de realización, el controlador 308 acciona el dispositivo de control de acceso enviando una señal al dispositivo de control de acceso a través de la interfaz de dispositivo de control de acceso 332 basándose en resultados de una decisión de acceso tomada por el controlador 308. Opcionalmente, el dispositivo de control de acceso puede ser enterizo con el lector 108 en una forma de realización, en cuyo caso no sería necesaria una interfaz de dispositivo de control de acceso 332. En una forma de realización alternativa, un dispositivo de control de acceso es externo con respecto al lector 108, siendo necesaria de este modo la interfaz 332. Los ejemplos de una interfaz de dispositivo de control de acceso 332 incluyen cualquier tipo de puerto de datos tal como un puerto USB, un puerto de datos serie, un puerto de datos paralelo, un cable convencional, un puerto de comunicaciones inalámbricas tal como una interfaz de datos Bluetooth, o cualquier otro tipo de interfaz de comunicación por cable o inalámbrica.

Además de una interfaz de dispositivo de control de acceso 332, el lector 108 puede comprender adicionalmente una memoria 312. La memoria 312 se puede usar para almacenar datos de aplicación, la ID exclusiva del anfitrión, un fichero registro de historial de comunicaciones 316, un conjunto de políticas de acceso 320 u otros tipos de objetos de mensaje, y cualesquiera otras funciones que puedan ser ejecutadas por el controlador 308. La memoria 312 puede comprender memoria volátil y/o no volátil. Los ejemplos de memoria no volátil incluyen Memoria de Solo Lectura (ROM), ROM Programable Borrable (EPROM), PROM Borrable Electrónicamente (EEPROM), Memoria flash, y similares. Los ejemplos de memoria volátil incluyen Memoria de Acceso Aleatorio (RAM), RAM Dinámica (DRAM), RAM Estática (SRAM), o memoria intermedia. En una forma de realización, la memoria 312 y el controlador 308 están diseñados para utilizar características de seguridad conocidas, con el fin de evitar el acceso no autorizado al contenido de la memoria 312 tal como un análisis de canales colaterales y similares.

El fichero registro de historial de comunicación 316 puede proporcionar una posición en memoria en la que se almacena un registro de todas las comunicaciones para el lector 108. El fichero registro de historial de comunicaciones 316 se puede usar en relación con la determinación de qué credenciales 112 se presentan típicamente a un lector particular 108, así como cuándo y con qué frecuencia se presentan dichas credenciales 112 al lector 108. De este modo, el fichero registro de historial de comunicaciones 316 puede servir como un mecanismo para modelar el flujo de información en un sistema de acceso seguro particular 200.

El lector 108 puede comprender además un reloj 324. El reloj 324 se representa de manera que es interno con respecto al lector 108, aunque el reloj también puede ser externo al lector 108. El reloj 324 realiza un seguimiento del tiempo actual. El controlador 308 puede estar adaptado para leer el tiempo del reloj 324 y proporcionar ese tiempo a una credencial 112, para el fichero registro de historial de comunicaciones de la credencial. El reloj 324 se

puede utilizar además para determinar si el titular de una credencial particular 112 tiene permitido actualmente el acceso a un activo protegido por el dispositivo de control de acceso 312. El controlador 308 también puede remitir a las políticas 320 en la memoria 312 para determinar si una credencial 112 tiene permitido el acceso a un punto de acceso asociado 104 ó activo 106 basándose en el tiempo actual según determine el reloj 324. El controlador 308 también puede remitir al reloj 324 para determinar cuándo debería implementarse una política particular 320, en el caso de que se fije que una o más políticas 320 presentan un inicio retardado, y comprende un mecanismo temporizador.

En el lector 108 se puede incluir también una fuente de alimentación 328 para proporcionar alimentación a los diversos dispositivos contenidos dentro del lector 108. La fuente de alimentación 328 puede comprender baterías internas y/o un conversor de AC-DC tal como una fuente de alimentación en modo de conmutación o un regulador de voltaje conectado a una fuente de alimentación de AC, externa.

Aunque no se ha representado, un lector 108 puede incluir además una interfaz de comunicaciones que proporciona capacidades de comunicación entre el lector 108 y servidores externos u otros nodos de red. Una interfaz de comunicaciones de este tipo puede incluir un puerto USB, un módem, un adaptador de red tal como una tarjeta Ethernet, o cualquier otro adaptador de comunicaciones conocido en la técnica. Estos tipos de interfaces de comunicación se incluyen típicamente solo en anfitriones de mensajes conectados en red 204.

En referencia a continuación a la figura 4, se describirán detalles adicionales del fichero registro de historial de comunicaciones 316 de acuerdo con por lo menos algunas formas de realización de la presente invención. El fichero registro de historial de comunicaciones 316 puede comprender varios campos de datos diferentes, tales como, un campo de ID de credencial 404, un campo de tiempo de lectura 408, un campo indicador de objeto de mensaje 412, un campo de detalles del objeto de mensaje 416, y un campo de mecanismo de temporizador 420. El fichero registro de historial de comunicaciones 316 se puede usar para almacenar un historial de comunicaciones para un lector asociado 108. El historial de comunicaciones 316 se puede renovar de una manera periódica (por ejemplo, diariamente, semanalmente, mensualmente, anualmente). Alternativamente, el historial de comunicaciones 316 se puede mantener durante el tiempo de vida del lector 108, en cuyo caso puede ser necesario añadir capacidad de memoria adicional al lector 108 durante el transcurso de su tiempo de vida.

El campo de ID de credencial 404 puede comprender información de identificación para cada credencial 112 presentada al lector 108. La información en el campo de ID de credencial 404 puede incluir un número de tarjeta exclusivo asignado a la credencial 112, un nombre del usuario asociado a la credencial 112, o alguna otra información que identifique de forma exclusiva la credencial 112. En el campo de ID de credencial 404 también se puede mantener información no exclusiva tal como códigos de sitio u otra información que identifique un grupo al cual pertenece la credencial 112.

El campo de tiempo de lectura 408 puede comprender información referente al tiempo en el que una credencial particular 112 se comunicó con el lector 108. El valor en el campo de tiempo de lectura 408 se puede obtener por remisión al reloj 324. El tiempo de lectura se puede mantener en cualquier tipo de granularidad (por ejemplo, meses, semanas, días, horas, segundos, etcétera), dependiendo de la precisión requerida del tiempo de lectura. Si no se requiere un tiempo de lectura preciso, entonces el campo de tiempo de lectura 408 puede proporcionar simplemente una indicación de la secuencia en la que se leyó una credencial particular 112 con respecto a otra credencial 112.

El campo indicador de objeto de mensaje 412 puede contener información que muestre si una credencial particular 112 envió una política o tipo similar de objeto de mensaje al lector 108 y/o si el lector envió una política o tipo similar de objeto de mensaje a la credencial 112. El campo indicador de objeto de mensaje 412 puede proporcionar también información de identificación para ciertos objetos de mensaje. Más específicamente, se pueden hacer circular objetos de mensaje por todo el sistema de acceso seguro 200 con un nombre o identificador particular. Cuando el objeto de mensaje es recibido por un nuevo dispositivo de control de acceso, el identificador del objeto de mensaje se puede mantener en el campo indicador de objeto de mensaje 412 de manera que un lector 108 disponga de un registro de referencia rápida de los objetos de mensaje que ha recibido. Adicionalmente, se pueden proporcionar indicadores de objetos de mensaje para objetos de mensaje que sean transmitidos a credenciales 112. Esto permite que un administrador del sistema determine qué credenciales 112 tienen un objeto de mensaje particular almacenado en las mismas, sin comprobar realmente la propia credencial 112.

El campo de detalles de objeto de mensaje 416 puede contener detalles sobre la política u objeto de mensaje que se transmitió hacia/desde el lector 108. De acuerdo con por lo menos una forma de realización de la presente invención, cuando un objeto de mensaje se corresponde con una nueva política de control de acceso, el campo de detalles de objeto de mensaje 416 incorpora una definición de la actualización de control de acceso. Dichas actualizaciones de control de acceso incluyen generalmente un cambio en los derechos de acceso para por lo menos una credencial 112 que accede a por lo menos un punto de acceso 104 ó activo 106 asociado al lector 108. Por ejemplo, si se han revocado permisos de acceso para una credencial particular 112 (por ejemplo, debido a que un usuario asociado a la credencial 112 ya no trabaja para una empresa que mantiene las instalaciones 100), entonces el campo de detalles de objeto de mensaje 416 puede incorporar instrucciones que comuniquen a todos los lectores 108 que dejen de permitir que la credencial identificada 112 acceda a puntos de acceso 104 y/o activos

106 asociados. De este modo, la información mantenida en el campo de detalles de objeto de mensaje 416 (y los objetos de mensaje en general) incluye típicamente una identificación de por lo menos una credencial 112 y una regla de acceso para esa por lo menos una credencial 112. Alternativamente, el objeto de mensaje se puede corresponder con una actualización de aplicación para una o más aplicaciones almacenadas en el lector 108, en cuyo caso el campo de detalles de objeto de mensaje 416 puede comprender la aplicación actualizada así como instrucciones para que el lector 108 instale la aplicación nueva. Otro tipo de objeto de mensaje usado de acuerdo con por lo menos algunas formas de realización de la presente invención puede incluir una actualización de habilitación del lector. En esta forma de realización particular, los lectores 108 se pueden adaptar para dejar de permitir el acceso a cualquier credencial 112 después de una cantidad de tiempo predeterminada a no ser que el lector reciba un objeto de mensaje nuevo que renueve la suscripción de la actividad del lector 108.

El objeto de mensaje, además de proporcionar instrucciones para el lector 108 (o credencial 112 en algunas aplicaciones) también puede incluir un mecanismo de temporizador 420. El mecanismo de temporizador 420 puede definir una vida útil, para un objeto de mensaje particular. La información en el campo de mecanismo de temporizador 420 puede incluir detalles relacionados con la vida útil del objeto de mensaje. Más específicamente, el mecanismo de temporizador 420 asociado a un objeto de mensaje particular puede hacer que el objeto de mensaje resulte activo solamente después de un tiempo predeterminado. En otras palabras, se puede implementar una actualización de políticas retardada, con objetos de mensaje que tengan un mecanismo de temporizador 420, los cuales definen un cierto tiempo después de que el objeto de mensaje fuera distribuido por primera vez antes de que el objeto de mensaje se haga activo (es decir, el mecanismo de temporizador puede definir un tiempo predeterminado en el que un lector 108 debería comenzar a implementar las instrucciones contenidas dentro del objeto de mensaje). El mecanismo de temporizador 420 también puede definir durante cuánto tiempo va a permanecer activo un objeto de mensaje particular. Esta implementación particular puede utilizar el mecanismo de temporizador para desactivar el objeto de mensaje después de una cantidad de tiempo predeterminada, a no ser que se reciba un objeto de mensaje nuevo que prolongue el mecanismo de temporizador. Por consiguiente, la información contenida en el campo de mecanismo de temporizador 420 se puede usar para definir el comienzo y final del tiempo de vida de un objeto de mensaje asociado. De acuerdo con por lo menos algunas formas de realización de la presente invención, el mecanismo de temporizador se puede añadir a un objeto de mensaje en el comienzo/final de los detalles del objeto de mensaje o en un encabezamiento del objeto de mensaje. También se puede incluir una bandera en las comunicaciones que contienen un objeto de mensaje, en caso de que el objeto de mensaje contenga un mecanismo de temporizador 420. Una bandera de este tipo permitirá que el dispositivo de control de acceso receptor busque el mecanismo de temporizador pertinente en el objeto de mensaje.

La figura 5 representa una credencial ejemplificativa 112 que se describirá a continuación de acuerdo con por lo menos algunas formas de realización de la presente invención. La credencial 112 puede incluir una interfaz de comunicaciones 504 que permite que la credencial 112 se comunique con dispositivos externos tales como el lector 108. La interfaz de comunicaciones 504 puede comprender una antena de RF que permite que la credencial 112 reciba y transmita datos sin contacto. En otras formas de realización, se puede utilizar una interfaz de comunicaciones de contacto magnético, óptico, o eléctrico 504.

A la interfaz de comunicaciones 504 se puede conectar un controlador 508. El controlador 508, en una forma de realización, incluye un microprocesador, un generador de números aleatorios, y un coprocesador criptográfico. El controlador 508 puede incluir cualquier procesador programable de propósito general, procesador de señal digital (DSP) o controlador para ejecutar programación de aplicaciones. Alternativamente, el controlador 508 puede comprender un circuito integrado de aplicación específica (ASIC) configurado especialmente. De modo similar al controlador 308 en el lector 108, el controlador 508 incluye características de seguridad conocidas que evitan sustancialmente el acceso no autorizado al contenido de la memoria 512.

La memoria 512 comprende típicamente memoria no volátil, tal como memoria flash. La memoria no volátil se usa generalmente debido a que la credencial 112 es preferentemente una credencial pasiva, lo cual significa que no dispone de una fuente de alimentación interna. En su lugar, la credencial 112 usa energía proveniente de un campo de RF creado por el lector 108 para alimentar sus componentes. El contenido de la memoria 512 puede incluir un fichero registro de historial de comunicaciones 516, políticas 520 y otros objetos de mensaje, y cualesquiera otras aplicaciones a ejecutar por la credencial 112. El fichero registro de historial de comunicaciones 516 es similar al fichero registro de historial de comunicaciones 316 almacenado en el lector 108 excepto que el campo de ID de credencial 404 se sustituye por un campo de ID de lector, en el que el campo de ID de lector identifica el lector con el que se ha comunicado la credencial 112. Más particularmente, el campo de ID de lector identifica lectores 108 a los cuales ha transmitido objetos de mensaje de credencial 112 y lectores 108 desde los cuales ha recibido objetos de mensaje la credencial 112.

En una forma de realización alternativa, la credencial 112 puede estar provista de una fuente de alimentación incorporada. Dichas credenciales 112 se conocen como credenciales activas 112. Una credencial activa 112 puede mantener su propio tiempo de confianza que se puede sincronizar con los dispositivos de red durante interacciones, por ejemplo, con lectores 108. De esta manera, la credencial 112 también puede controlar cuándo se deberían activar y/o desactivar ciertos objetos de mensaje que tienen un mecanismo de temporizador 420, basándose en una referencia al reloj interno.

En referencia a continuación a la figura 6, se describirá una herramienta de análisis de red 604 de acuerdo con por lo menos algunas formas de realización de la presente invención. La herramienta de análisis de red 604 puede residir en y ser ejecutada por una plataforma de procesado tal como un servidor, ordenador, ordenador portátil, etcétera. La herramienta de análisis de red 604 se puede usar para analizar tanto los sistemas de acceso seguro simulados 200 como los sistemas de acceso seguro reales 200. Más específicamente, la herramienta de análisis de red 604 puede utilizar un agente de optimización 608 para optimizar la eficacia con la cual se disemine información (por ejemplo, un objeto de mensaje) a través de un sistema de control de acceso que tiene por lo menos un anfitrión de mensajes no conectado en red 208. De acuerdo con por lo menos algunas formas de realización de la presente invención, el agente de optimización 608 se puede adaptar para analizar una configuración propuesta de dispositivos de control de acceso (por ejemplo, capacidades de localización y de red de anfitriones de mensajes 204, 208 y número de credenciales 112) y, a continuación, sugerir cambios en la configuración propuesta, que optimizarían la diseminación de objetos de mensaje a través del sistema de acceso seguro 200. El agente de optimización 608 también se puede adaptar para analizar configuraciones reales de dispositivos de control de acceso y, a continuación, o bien proporcionar estadísticas relacionadas con el flujo de objetos de mensaje en el sistema de acceso seguro 200 ó bien proporcionar sugerencias para optimizar la diseminación de objetos de mensaje a través del sistema de acceso seguro 200.

Las entradas a la herramienta de análisis de red 604 pueden incluir, por ejemplo, información de configuración de anfitriones de mensajes 612, información de configuración de portadores de mensajes 616, información de flujo de red 620, y requisitos de diseminación de políticas 624. La información de configuración de anfitriones de mensajes 612 puede incluir el número y la ubicación de anfitriones de mensajes 204, 208 en el sistema de acceso seguro 200 así como las capacidades de red de cada anfitrión de mensajes. Más específicamente, la información de configuración de anfitriones de mensajes 612 puede indicar si un anfitrión de mensajes particular es un anfitrión de mensajes conectado en red 204 ó un anfitrión de mensajes no conectado en red 208, y, si el mismo es un anfitrión de mensajes conectado en red 204, con qué otros dispositivos de control de acceso es capaz de comunicarse directamente el anfitrión de mensajes conectado en red 208. La información de configuración de anfitriones de mensajes se puede proporcionar como datos reales que representan una disposición real de los anfitriones de mensajes 204, 208 ó como datos de simulación que representan una disposición propuesta de los anfitriones de mensajes 204, 208.

La información de portadores de mensajes 616 puede incluir el número y el tipo de portadores de mensajes 220 en el sistema de acceso seguro 200. Adicionalmente, la información de portadores de mensajes 616 puede definir los permisos de acceso de ciertas credenciales 112. Esta información puede tener valor en formas de realización en las que las credenciales 112 se limitan al envío y la recepción de objetos de mensaje con anfitriones de mensajes 204, 208 únicamente cuando las mismas están autorizadas a acceder a activos 106 ó puntos de acceso 104 asociados a los anfitriones de mensajes 204, 208. Es en estas formas de realización particulares en las que dicha información afectará a la diseminación de un objeto de mensaje a través del sistema de acceso seguro 200.

En un sistema de acceso seguro simulado 200, la información de flujo de red 620 se puede estimar basándose en condiciones típicas del flujo de información. Más específicamente, la información de flujo de red 620 se puede basar en la información de flujo de red real de otros sistemas de acceso seguro 200 que tengan una configuración similar al sistema de acceso seguro 200 que se está simulando. Sin embargo, en un análisis de un sistema de acceso seguro real 200 la información de flujo de red 620 se puede o bien simular o bien determinar basándose en flujos de red históricos del sistema 200. Más específicamente, la información de flujo de red 620 se puede determinar por remisión al historial de comunicaciones 316, 516 de los dispositivos de control de acceso para determinar qué portadores de mensajes 220 se comunican tradicionalmente con qué anfitriones de mensajes 204, 208. El nivel de detalle de esta información 620 se puede basar en el nivel de detalle de la información mantenida en los ficheros registro de comunicaciones 316, 516. Por ejemplo, si el tiempo de lectura se almacena con un detalle de un segundo, entonces en la información de flujo de red 620 se puede incorporar la misma granularidad de información.

Los requisitos de diseminación de políticas 624 pueden estar definidos por el usuario. Estos requisitos se pueden proporcionar según una serie de diferentes maneras (por ejemplo, o bien como restricciones o bien como objetivos). Los requisitos de diseminación de políticas 624 especifican con qué rapidez se deberían compartir objetos de mensaje en todo un sistema de acceso seguro particular 200. Los requisitos de diseminación de políticas 624 se pueden definir en términos de un número requerido de dispositivos de control de acceso (por ejemplo, un porcentaje de anfitriones de mensajes 204, 208 y/o portadores de mensajes 220) que necesitan recibir un objeto de mensaje particular dentro de un cierto tiempo o la cantidad de tiempo en la que es necesario que un cierto número de dispositivos de control de acceso reciba un objeto de mensaje particular.

La herramienta de análisis de red 604 puede recibir la totalidad de la información de entrada antes descrita y utilizar el agente de optimización 608 para determinar varias maneras según las cuales se pueden distribuir objetos de mensaje a través del sistema de acceso seguro 200 de una forma más eficaz. De acuerdo con por lo menos algunas formas de realización de la presente invención, una medida del rendimiento del sistema según determina el agente de optimización 608 es el grado de separación entre un anfitrión originador de mensajes 204, 208 y otros anfitriones de mensajes 204, 208 ó portadores de mensajes 220 en el sistema 200. El grado de separación cuenta el número

mínimo de etapas de transporte de un mensaje esperadas para que el objeto de mensaje llegue a un anfitrión de mensajes 204, 208 ó portador de mensajes 220 seleccionado, en un sistema de dos colonias (por ejemplo, un sistema de acceso seguro 200 que comprenda anfitriones de mensajes conectados en redes y no conectados en red 204, 208).

De acuerdo con por lo menos algunas formas de realización de la presente invención, la definición convencional para la conectividad, k, de una red no satisface los requisitos de un sistema de dos colonias. La conectividad, k_c, de un portador de mensajes se puede definir alternativamente como el número de anfitriones de mensajes exclusivos 204, 208 que fueron visitados por ese portador de mensajes 220 por lo menos una vez durante un periodo de tiempo dado. De modo similar, cada anfitrión de mensajes 204, 208 tiene un valor, k_h, que representa el número de portadores de mensajes exclusivos 220 con los que compartir una transacción durante el mismo periodo de tiempo. Se pueden usar histogramas de k para portadores de mensajes y anfitriones de mensajes con el fin de clasificar el tipo de red, uno de cuyos ejemplos se representa en la figura 10.

La mayoría de las redes, en general, encajan en una de tres clasificaciones de distribuciones de grados: las Redes Libres de Escala tienen colas anchas, lo cual indica más conexiones de largo alcance, y están caracterizadas por una ley de potencias; las Redes Geométricas pueden ser jerárquicas y tienen una distribución exponencial en k; las Redes Aleatorias están más localizadas y siguen una distribución de Poisson.

Una alternativa a la comparación de una distribución con la distribución de grados es realizar un análisis espectral sobre la matriz de adyacencia de anfitrión de mensajes-a-anfitrión de mensajes W_{hh} o matriz de portador de mensajes-a-portador de mensajes W_{cc} que se halla cuadrando la matriz de adyacencia de portador de mensajes-a-anfitrión de mensajes W_{ch}. El espectro de las redes aleatorias seguirá el Semicírculo de Wigner, mientras que las redes libres de escala tendrán una forma triangular. Las redes estructuradas, tales como las redes jerárquicas, tendrán espectros más complejos.

Valor experimental y modelado de k

El modelado de la distribución de grados requiere dos elementos de información, uno es la suma de todas las conexiones, $\sum k$, y el otro es la forma de la distribución. A efectos de esta ilustración, se supone que la distribución en k es exponencial.

Los valores medidos de $\sum k$ indican que el número total de conexiones se puede modelar basándose en el número de portadores de mensajes, n_c, y el número de puertas, n_r.

Dispersión de la matriz de adyacencia de portador de mensajes – anfitrión de mensajes (A_{ch})

La suma total de conexiones en el sistema 200 se puede usar para calcular la dispersión de la matriz de adyacencia. La fracción conectada se puede hallar dividiendo por el número de conexiones posibles el número de conexiones esperadas. A continuación, la fracción de ceros, ZF, se halla restando de uno la fracción conectada.

$$FracciónCeros = 1 - \frac{\sum k}{n_r \cdot n_c}$$

Modelado de la matriz de adyacencia de portador de mensajes – anfitrión de mensajes (A_{ch})

Cuando la distribución de grados es bien conocida (por ejemplo, en un sistema de acceso seguro real 200), se puede usar un planteamiento general para hallar una función de generación apropiada para la matriz de adyacencia. Si se supone que los grados siguen un perfil de distribución en k exponencial y restricciones coincidentes para el valor modelado de k para las poblaciones tanto de portadores de mensajes como de anfitriones de mensajes, entonces la matriz de adyacencia se llena asignando a elementos aleatorios en A_{ch} un valor de conexión de 1 basándose en la probabilidad *P(C, H)*, en la que C y H son, respectivamente, portadores de mensajes y anfitriones de mensajes. Este proceso se repite hasta que se ha asignado la totalidad de las $\sum k$ conexiones.

Matriz de adyacencia ponderada (W_{ch})

A continuación, la matriz de adyacencia, A, se modifica para convertirse en una matriz de adyacencia ponderada, W, sustituyendo las conexiones en A por la probabilidad de los eventos. La probabilidad se puede hallar experimentalmente muestreando los eventos de sitios de control de acceso operativos durante un periodo de tiempo especificado. En la matriz de adyacencia, un valor de uno indica que hubo una conexión transitoria por lo menos una vez durante el periodo de medición, y la matriz ponderada especifica la fuerza de esa conexión. Un cero en la matriz de adyacencia indica una probabilidad de cero para la conexión especificada en la matriz ponderada.

La representación del número de eventos en cada elemento diferente de cero en datos experimentales presenta una

distribución de ley de potencias para la función de masa de probabilidad de la frecuencia de las conexiones.

La función de masa de probabilidad de las fuerzas de conexión puede seguir una distribución basada en ley de potencias para el tiempo de espera, particularmente la función de Zipf generalizada, conocida como ley de Zipf-Mandelbrot:

$$P_w(k; N, q, s) = \frac{\frac{1}{(k+q)^s}}{\sum_{i=1}^{N} \frac{1}{(i+q)^s}}$$

Una ventaja de usar esta función en el agente de análisis es el corte de la cola ancha típico en las distribuciones de ley de potencias por la restricción de normalización, k<N. El valor experimental de s en la ecuación es muy próximo a 2 para algunos sistemas. El agente de análisis puede utilizar esta definición de P_w fijando s=2 y definiendo una relación para q basándose en entradas de población.

A cada elemento en A_{ch} se le asigna una fuerza de conexión extraída de esta distribución para crear la matriz de adyacencia ponderada, W_{ch}. Después de asignar pesos a W_{ch} la matriz se normaliza para hacer que la suma de probabilidades sea igual a uno.

El agente de análisis puede utilizar un sesgo para representar los fenómenos observados en sistemas reales con el fin de producir una distribución de probabilidad que tenga una fuerza de conexión probable mayor en la matriz de adyacencia ponderada W_{cr} para vértices que están conectando miembros de una colonia de k elevada. El agente de análisis también puede modificar la fuerza de conexión basándose en el tiempo.

Monte Carlo con Cadenas de Markov

La matriz de adyacencia ponderada se usa junto con un par de vectores de estado para cada actualización emitida hacia el sistema. Los dos vectores de estado registran respectivamente qué portadores de mensajes y qué anfitriones de mensajes han recibido la actualización a través de un objeto de mensaje. En cada etapa de un Monte Carlo por Cadenas de Markov (MCMC) se extrae aleatoriamente una conexión a partir de la matriz de adyacencia ponderada. Los estados de los miembros seleccionados se comprueban, y si uno y solamente uno de los componentes tiene la actualización, entonces la actualización se propaga al otro miembro. Si ambos miembros o ninguno de ellos tiene una actualización, entonces el resultado es nulo. Aquí el interés reside en seguir el vector de estado, Γ, con cada etapa en lugar de hallar un estado de equilibrio (el cual se puede considerar como un vector de componentes completamente actualizados).

La propagación de información en la población de portadores de mensajes, Γ_c, depende tanto del número de anfitriones de mensajes que tienen la información, Λ_r, como del número de portadores de mensajes sin conocimiento del objeto de mensaje disponible para recibir un objeto de mensaje. De modo similar, la velocidad de información en la población de anfitriones de mensajes depende tanto del número de portadores de mensajes como de los anfitriones de mensajes con el mensaje.

$$\Gamma_c = f_c(\Lambda_c, \Lambda_h) \qquad \Gamma_h = f_f(\Lambda_c, \Lambda_h)$$

La velocidad, r, es la derivada, con respecto al tiempo (o eventos), de la posición (o número), A. Esto conduce a dos ecuaciones diferenciales parciales acopladas en A, por ejemplo, si A es una función del tiempo:

$$\frac{\delta \Lambda_c}{\delta t} = f_c(\Lambda_c, \Lambda_h) \qquad \text{y} \qquad \frac{\delta \Lambda_h}{\delta t} = f_h(\Lambda_c, \Lambda_h)$$

Esta codependencia del flujo de información da como resultado un sistema autolimitado en el que ni la población de portadores de mensajes ni la población de anfitriones de mensajes tenderá a ir muy por delante una con respecto a la otra. Aunque esto es una regla general, existen condiciones en la que una velocidad puede ser inicialmente mayor que la otra.

En las ecuaciones anteriores, la velocidad se puede medir como la propagación de la actualización o bien por evento, A(e) o bien por tiempo, A(t). La unidad natural usada por el agente de análisis en sus cálculos se basa en eventos. Se puede usar una relación entre unidades de eventos y unidades de tiempo para convertir los resultados a unidades de tiempo.

Resultados del modelo

El rendimiento del reparto de mensajes en un sistema operativo de dos colonias se puede estudiar (por ejemplo, por

medio de la herramienta de análisis de red 604) construyendo la matriz de adyacencia ponderada, W_{cr}, sobre la base de datos de un sistema de una colonia, deduciéndose el transporte de un objeto de mensaje cuando un portador de mensajes 220 visita un primer anfitrión de mensajes 204, 208 y a continuación un segundo anfitrión de mensajes 204, 208. La matriz de adyacencia ponderada se usa para propagar información en un proceso de Markov. El modelo más sencillo tiene solamente dos valores de entrada, el número de portadores de mensajes, n_c, y el número de anfitriones de mensajes, n_r. Un mensaje se inicializa en uno o más miembros de la colonia y se permite que el mismo fluya a través del sistema. En la figura 11 se representan resultados del modelo ejemplificativos (por ejemplo, salida 628) obtenidos mediante la herramienta de análisis de red 604.

En la gráfica se representa en general la población o bien de los portadores de mensajes, Λ_c, o bien de los anfitriones de mensajes, Λ_h, modelados a partir de datos de sitios reales (por ejemplo, ficheros archivo de historial de comunicaciones 316, 516), que han recibido o se inicializaron con un objeto de mensaje. De acuerdo con por lo menos una forma de realización de la presente invención, la línea es el promedio de múltiples experimentos de MCMC.

Mejoras del modelo

De acuerdo con por lo menos algunas formas de realización de la presente invención, el agente de optimización 608 se puede hacer funcionar para generar una serie de salidas diferentes 628 en función de si está analizando una disposición propuesta de un sistema de acceso seguro 200 ó una disposición real de un sistema de acceso seguro 200. Posteriormente se describirán más detalladamente ejemplos de los tipos de salidas 628 que se pueden generar por medio del agente de optimización 608.

Eventos de bucle

Los eventos de bucle se identifican como componentes diagonales en la matriz de adyacencia de anfitrión-a-anfitrión, W_{hh}, en la que W_{hh} es una matriz cuadrada resultante de multiplicar la matriz de adyacencia ponderada por su transpuesta. Estos eventos afectan al rendimiento del sistema por sustracción del número de evento posiblemente productivo, actuando esencialmente de manera que reducen el número efectivo de eventos en un periodo de tiempo dado. El agente de optimización 608 puede sugerir cambios de configuración para reducir el número de eventos de bucle.

Matriz de adyacencia dependiente del tiempo (W_{cr})

Tal como se ha mencionado anteriormente, las fuerzas de conexión en la matriz de adyacencia ponderada cambian con el tiempo. Las fuerzas de conexión pueden tener un ciclo diurno provocado por variaciones en niveles de actividad durante el día. Las fuerzas de conexión pueden tener también componentes semanales debido a una menor actividad los fines de semana y también pueden tener ciclos anuales debido a las vacaciones, etcétera. Las fuerzas de conexión también pueden cambiar una con respecto a otra debido a patrones de tráfico que varían periódicamente. En un sistema de dos colonias que contiene objetos de mensaje transportados por portadores de mensajes 220 que están restringidos a pasar por anfitriones de mensajes particulares 204, 208, se producirá un efecto beneficioso sobre la eficacia del sistema. Por consiguiente, el agente de optimización 608 puede proporcionar como salida 628 sugerencias para potenciar las fuerzas de conexión, por ejemplo, sugiriendo la inclusión de puntos de restricción adicionales en el sistema de acceso seguro 200.

Eventos de balde

En un sistema que plantea restricciones sobre los portadores de mensajes 220 requiriendo así que los mismos visiten anfitriones de mensajes específicos 204, 208, esto puede hacer que aumente la posibilidad de que un segundo o segundos portadores de mensajes 220 se “monten encima” o “vayan a remolque” de otro al pasar por un anfitrión de mensajes 204, 208, saltándose el anfitrión de mensajes cuando un primer portador de mensajes contemporáneo se comunica con el anfitrión de mensajes y satisface los requisitos de comunicación. Cuando se produce el movimiento a remolque, es posible que los portadores de mensajes 220 se salten anfitriones de mensajes 204, 208 sin entregar o recibir un objeto de mensaje. Se producirán además más oportunidades de movimiento a remolque cuando la población de los portadores de mensajes 220 sea grande en comparación con la población de los anfitriones de mensajes 204, 208, de modo que la k_r promedio sea alta. De este modo, el agente de optimización 608 puede sugerir maneras con las cuales se puede reducir el movimiento a remolque, por ejemplo, incrementando el número de anfitriones de mensajes 204, 208 en el sistema 200 ó sugiriendo medidas de seguridad adicionales que pueden ser adoptadas para reducir el movimiento a remolque.

Entropía de seguridad

Una medida importante de un sistema de mensajes de dos colonias es su capacidad de mantener un entorno que es actual con respecto a actualizaciones de objetos de mensaje. Estos sistemas presentan un nivel de incertidumbre de la vigencia de la información para todos los miembros del sistema. La expresión “entropía de seguridad” se usa en el presente documento para describir la posibilidad de que una actualización de mensaje (es decir, un objeto de

mensaje) esté disponible pero no sea entregada a tiempo debido a la incertidumbre en el sistema. Un fallo se puede definir como un evento entre un portador de mensajes 220 y un anfitrión de mensajes 204, 208, que se produce antes de que la actualización se haya propagado a cualquiera de los miembros. La posibilidad de que una actualización falle es el producto de la posibilidad de un evento y la posibilidad de que ningún miembro haya recibido el objeto de mensaje actualizado. El valor determinado mediante este cálculo puede ser proporcionado por la herramienta de análisis en la salida 628 ó bien para ayudar a diseñar la configuración de un sistema de comunicaciones 200 ó bien para realizar mejoras en la configuración de un sistema de comunicaciones operativo 200.

Mejora del rendimiento del sistema

Además de proporcionar, como salida 628, estadísticas relacionadas con el flujo de información en el sistema de acceso seguro 200, la herramienta de análisis de red 604 puede utilizar el agente de optimización 608 para determinar si hay alguna manera de diseminar de forma más rápida un objeto de mensaje por todo el sistema de acceso seguro 200. Dichas determinaciones realizadas por el agente de optimización 608 se pueden proporcionar como sugerencias a un usuario en forma de una salida 628. Posteriormente se describirán de forma más detallada ejemplo de dichas sugerencias.

Selección de individuos para la actualización inicial

La invención descrita en este análisis hasta el momento se basa en general en la distribución de objetos de mensaje en un sistema de dos colonias, en el que la actualización del objeto de mensaje se inicia con un único miembro y a continuación se permite que se propague por todo el sistema 200. Cuando una actualización se inicia a través de un único individuo en el sistema (por ejemplo, un único dispositivo de control de acceso originador), las características exclusivas del individuo escogido pueden tener un impacto significativo sobre el rendimiento del sistema. No siempre es posible escoger el punto de inicio, aunque en sistemas que proporcionan esta opción, se puede escoger un individuo en el sistema para optimizar los costes, la comodidad, y el rendimiento. Típicamente, un valor alto de k es beneficioso en la propagación de la información, pero también es importante observar que la inicialización de portadores de mensajes 220 puede propagar la información más rápidamente en la población anfitriones de mensajes 204, 208 y viceversa. Otra consideración importante es el aprovechamiento de las restricciones que provocan que los portadores de mensajes 220 visiten anfitriones de mensajes particulares 204, 208, lo cual tiene la ventaja doble de producir un componente con un valor alto de k con la ventaja adicional de una fuerza de conexión alta con los anfitriones de mensajes 204, 208. Además, en sistemas con un ciclo diurno fuerte, la ventaja de dichos puntos de restricción puede ser más acentuada en el comienzo del día, haciendo que el sistema 200 resulte eficaz en la distribución de objetos de mensajes al principio del ciclo de actualización. Todos estos factores se pueden considerar cuando el agente de optimización 608 sugiere un dispositivo de acceso seguro originador, el cual se puede corresponder o bien con un portador de mensajes 220 ó bien con un anfitrión de mensajes 204, 208.

Más componentes conectados

El disponer de más miembros de la colonia inicializados con la actualización de los objetos de mensaje tiene un impacto directo sobre la probabilidad de actualización, $P_{nu}(t)$. Esta mejora proporciona tanto una mejor posición de inicio como una mejor velocidad inicial para que la actualización se propague consiguiendo que la misma resulte una herramienta útil para controlar el rendimiento. Por consiguiente, el agente de optimización 608 puede sugerir que uno o más anfitriones de mensajes previamente no conectados en red 208 hagan que se modifiquen sus capacidades de comunicación para convertirlos en un anfitrión de mensajes conectado en red 204. El agente de optimización 608 también puede sugerir con qué dispositivo de control de acceso se debería conectar el anfitrión de mensajes.

Actualizaciones pre-lanzadas

Cuando se pueden liberar objetos de mensaje a un sistema con antelación de su necesidad final, en ese caso un pre-lanzamiento de las actualizaciones con una “activación” retardada mejorará considerablemente el rendimiento aparente del sistema de reparto de mensajes. La activación retardada se puede facilitar incorporando un mecanismo de temporizador 420 en el objeto de mensaje de tal manera que el objeto de mensaje se active en algún instante de tiempo después de que el mismo se haya distribuido inicialmente en el sistema 200.

Actualizaciones forzadas

Una de las cuestiones problemáticas para el reparto de objetos de mensaje en una red de dos colonias es la preocupación de que un individuo en una o ambas colonias se pierda totalmente en el proceso de actualización. Aunque un sistema 200 con un buen mantenimiento puede conservar los componentes actualizados por norma general, algunos componentes pueden perderse las actualizaciones durante periodos prolongados del tiempo. Para hacer frente a esta preocupación, el sistema puede requerir una actualización forzada. Las actualizaciones forzadas se pueden implementar o bien según una planificación regular o bien pueden ser requeridas después de un periodo de inactividad. Nuevamente, se puede utilizar el mecanismo de temporizador 420 para hacer que un anfitrión de

mensajes 204, 208 ó portador de mensajes 220 particular resulte inactivo después de una cantidad de tiempo predeterminada a no ser que reciba un objeto de mensaje nuevo. Esto obligará a los usuarios de los portadores de mensajes 220 a movilizarse y obtener un objeto de mensaje nuevo de una forma periódica.

Se puede usar una combinación de Actualizaciones de Pre-Lanzamiento y Actualizaciones Forzadas para producir una actualización retardada de entropía cero.

En referencia a continuación a la figura 7, se describirá un método de optimización de la configuración de un sistema de acceso seguro 200, particularmente en un entorno de simulación, de acuerdo con por lo menos algunas formas de realización de la presente invención. El método se inicia cuando la herramienta de análisis de red 604 recibe información de configuración de anfitriones de mensajes 612 (etapa 704). La información de anfitriones de mensajes 612 puede incluir información relacionada con el número, ubicación, y tipo (por ejemplo, capacidades de conexión en red o sin conexión en red) de cada anfitrión de mensajes 204, 208 en un sistema de acceso seguro 200.

A continuación, la herramienta de análisis de red 604 recibe la información de configuración de portadores de mensajes 616 (etapa 708). Esta información puede incluir el número y los tipos de portadores de mensajes 220 en el sistema de acceso seguro 200 así como los permisos de acceso asociados a cada portador de mensajes 220.

Después de esto, la herramienta de análisis de red 604 recibe la información de flujo de red 620, la cual define formas potenciales según las cuales los portadores de mensajes 220 se desplazarán a través del sistema de acceso seguro 200 (etapa 712). Más específicamente, la información de flujo de red 620 se puede basar en datos recibidos desde ficheros registro de comunicaciones de otros dispositivos de control de acceso en sistemas de acceso seguro similares. En una simulación, la información de flujo 620 puede incluir también tiempos previstos en los que ciertos portadores de mensajes 220 se comunicarán con ciertos anfitriones de mensajes 204, 208.

Una vez que la herramienta de análisis de red 604 ha recibido las entradas necesarias para simular la actividad del sistema de acceso seguro 200, la herramienta de análisis de red 604 prosigue mediante la generación de una matriz de probabilidad basándose en el flujo de red (etapa 716). La matriz de probabilidad puede incluir probabilidades relacionadas con si ciertos dispositivos de control de acceso (por ejemplo, anfitriones de mensajes 204, 208 y/o portadores de mensajes 220) recibirán un objeto de mensaje dentro de un tiempo predeterminado después de que el objeto de mensaje se introduzca en el sistema de acceso seguro. Adicionalmente, la matriz de probabilidad puede proporcionar también información que muestre el número de dispositivos de control de acceso que recibirán un objeto de mensaje dentro de un tiempo predeterminado y dentro de una probabilidad predeterminada.

Un proceso de Markov puede generar la matriz de probabilidad según se ha descrito anteriormente. A continuación, la matriz de probabilidad resultante se puede comparar con requisitos de flujo de información (por ejemplo, en forma de un objeto de mensaje que sea portador de información de políticas de control de acceso) para el sistema de acceso seguro (etapa 720). Seguidamente, los resultados de esa comparación se pueden proporcionar como una salida 628 a un usuario de la herramienta de análisis de red 604 (etapa 724). Más específicamente, si las probabilidades en la matriz cumplen o superan los requisitos de flujo de información, entonces la herramienta de análisis de red 604 puede indicar que la configuración propuesta cumple los requisitos. Alternativamente, si los requisitos de flujo de información se superan notablemente, la herramienta de análisis de red 604 puede sugerir maneras de reducir el coste de implementación del sistema de acceso seguro propuesto 200. Por ejemplo, la herramienta de análisis de red 604 puede indicar en la interfaz de usuario qué anfitriones conectados en red 204 se pueden cambiar a un anfitrión no conectado en red 208 aunque cumpliendo todavía los requisitos de flujo de información. Esta indicación se puede realizar coloreando el anfitrión de mensajes identificado con un color diferente o sombreándolo de una manera diferente a la de los otros anfitriones de mensajes 204, 208. Alternativamente, si no se cumplen los requisitos de flujo de información, entonces la herramienta de análisis de red 604 puede identificar ciertos anfitriones de mensajes 204, 208 que deberían o bien reubicarse o bien hacer que cambiasen sus capacidades de comunicación. Estos anfitriones de mensajes identificados 204, 208 también se pueden destacar en la interfaz de usuario, y la herramienta de análisis de red 604 puede destacar adicionalmente el área de las instalaciones 100 en las que debería situarse otro anfitrión de mensajes 204, 208.

En referencia a continuación a la figura 8, se describirá de acuerdo con por lo menos algunas formas de realización de la presente invención un método de determinación de estadísticas de diseminación de información (por ejemplo, objeto de mensaje). El método comienza cuando en la herramienta de análisis de red 604 se recibe información de configuración de anfitriones real 612 e información de portadores real 616 (etapas 804 y 808). La información de configuración de anfitriones real 612 se puede recuperar directamente de un servidor o un tipo similar de plataforma informática que esté controlando el sistema de acceso seguro 200. Alternativamente, la información de configuración 612 la puede introducir manualmente un usuario de la herramienta de análisis de red 604.

Después de esto, los flujos de información se simulan basándose en información recibida desde los ficheros registro de historial de comunicaciones 316, 516 de los anfitriones de mensajes 204, 208 y los portadores 220 (etapa 812). Esta simulación recrea, dentro de un cierto grado de aproximación, cómo se distribuirá un objeto de mensaje por todo un sistema de acceso seguro real. Por otra parte, la información histórica se puede usar para proyectar estadísticas de flujos futuros para el mismo sistema de acceso seguro 200.

Después de que se haya simulado la actividad de flujo de información, la herramienta de análisis de red 604 continúa generando la matriz de probabilidad que presenta las estadísticas de probabilidad para el flujo de información (etapa 816). A continuación, la matriz de probabilidad se puede usar para determinar estadísticas de diseminación de información (etapa 820). El tipo de estadísticas de diseminación de información puede incluir estadísticas relacionadas con la rapidez con la que se compartirá un objeto de mensaje con el sistema de acceso seguro 200 completo, la rapidez con la que se compartirá un objeto de mensaje con una cierta parte del sistema de acceso seguro 200, cuál es la probabilidad de que un objeto de mensaje se proporcione a un dispositivo de control de acceso particular dentro de un tiempo predeterminado, cuál es la probabilidad de que un objeto de mensaje no sea compartido con un dispositivo de control de acceso particular dentro de un tiempo predeterminado, una indicación de tiempo necesario para que un objeto de mensaje llegue a un dispositivo de control de acceso particular dentro de una probabilidad predeterminada, y otros.

A continuación, la herramienta de análisis de red 604 puede generar salidas 628 que proporcionen a un usuario las estadísticas de diseminación de información determinadas (etapa 824). Se puede permitir que el usuario interaccione con una interfaz de usuario para cambiar la manera en la que se visualiza la información así como qué información se visualiza al usuario. Por ejemplo, se puede permitir que el usuario seleccione un anfitrión de mensajes particular en la interfaz de usuario, y todas las probabilidades asociadas a ese anfitrión de mensajes (por ejemplo, probabilidad de que reciba un objeto de mensaje antes de un tiempo predeterminado, probabilidad de que no reciba un objeto de mensaje antes de un tiempo predeterminado, cantidad de tiempo requerida para que el mismo reciba un objeto de mensaje dentro de una probabilidad predeterminada, número de interacciones con portadores de mensajes 220 que necesitará antes de que reciba el objeto de mensaje, etcétera) así como cualquier otra información pertinente relacionada con el anfitrión de mensajes seleccionado. Se puede realizar una función similar para un portador de mensajes seleccionado 220 ó una población de anfitriones de mensajes 204, 208 y/o portadores de mensajes 220.

En referencia a continuación a la figura 9, se describirá de acuerdo con por lo menos algunas formas de realización de la presente invención un método de optimización de la diseminación de información (por ejemplo, objetos de mensaje) a través de un sistema de acceso seguro 200. El método se inicia cuando se recibe información real de anfitriones 204, 208 y portadores 220 en la herramienta de análisis de red 604 (etapas 904 y 908). A continuación, la herramienta de análisis de red 604 puede utilizar el agente de optimización 608 para analizar la configuración del sistema de acceso seguro 200 con el fin de determinar si hay alguna manera de mejorar la eficacia con la que se distribuye un objeto de mensaje por todo el sistema 200 (etapa 912). El agente de optimización 608 puede analizar simulaciones pasadas así como distribuciones reales de objetos de mensaje para el sistema de acceso seguro 200 ó sistemas de acceso que tengan configuraciones similares al sistema de acceso seguro 200 bajo escrutinio.

Durante su análisis de la configuración del sistema 200, la herramienta de análisis de red 604 utilizará el agente de optimización 608 para determinar si existen cualesquiera puntos de restricción posibles en el sistema 200 (etapa 916). Típicamente, los puntos de restricción se corresponden con puntos de las instalaciones 100 por los que tendrá que pasar una proporción elevada de portadores de mensajes 220. Los puntos de restricción típicos son puertas de entrada/salida para el edificio, entradas principales, vestíbulos, servicios, etcétera. Si hay por lo menos un punto de restricción posible identificado, entonces el agente de optimización 608 sugerirá uno o más de los puntos de restricción identificados como punto en el que se debería dar origen a un objeto de mensaje (etapa 920). Más específicamente, el agente de optimización 608 identificará dispositivos de control de acceso (por ejemplo, un anfitrión de mensajes 204, 208) asociados al punto de restricción identificado y sugerirá que el anfitrión de mensajes identificado se use como dispositivo de control de acceso de origen. Adicionalmente, si el anfitrión de mensajes se corresponde con un anfitrión de mensajes no conectado en red 208, entonces el agente de optimización 608 puede sugerir también que se cambien las capacidades de conexión en red del anfitrión 208 de tal manera que se convierta en un anfitrión de mensajes conectado en red 204. Esto facilitaría la introducción del objeto de mensaje en el sistema 200, puesto que entonces un administrador del sistema podría proporcionar el objeto de mensaje al anfitrión 204 de forma remota en lugar de tener que transportar el objeto de mensaje al anfitrión de mensajes 208 sobre un portador de mensaje 220.

El agente de optimización 608 también puede analizar la configuración del sistema 200 para determinar si hay cualesquiera portadores de mensajes 220, tales como credenciales 112, que son típicamente más activos que otros portadores de mensajes 220 (etapa 924). Por ejemplo, puede haber ciertos usuarios que tengan que visitar una parte mayor de unas instalaciones 100 que otros usuarios. Como ejemplo, con frecuencia se requiere que el personal de mantenimiento visite unas instalaciones completas 100 de forma diaria mientras que otros tipos de personal visitarán únicamente ciertas partes de unas instalaciones de forma regular. El portador de mensajes 220 asociado a dichos usuarios activos puede proporcionar un buen portador de mensajes originador 220. Estos portadores de mensajes activos 220 se pueden identificar analizando y comparando los ficheros registro de historial de comunicaciones 316 de los anfitriones de mensajes 204, 208 para buscar portadores de mensajes 220 que se comunicaron con un número elevado de los anfitriones de mensajes 204, 208.

En el caso de que se identifique un portador de mensajes activo 220 ó un número de portadores de mensajes activos 220, entonces el agente de optimización 608 puede sugerir que uno o más de los portadores de mensajes

activos identificados 220 se usen como punto de origen para el objeto de mensaje (etapa 928). A continuación, a dichos portadores de mensajes 220 se les puede proporcionar una actualización forzada para iniciar la diseminación del objeto de mensaje por todo el sistema 200.

El agente de optimización 608 puede analizar además el sistema 200 para determinar si sería posible una actualización retardada, y en caso afirmativo, si se puede permitir una actualización de este tipo basándose en preferencias del administrador del sistema (etapa 932). Si es posible una actualización retardada, entonces el agente de optimización 608 puede sugerir que se ejecute una actualización retardada (etapa 936). Para lograr esto, el agente de optimización 608 puede proporcionar una sugerencia de que, en lugar de hacer que el objeto de mensaje se distribuya de una manera activa, el objeto de mensaje se debería distribuir con un mecanismo de temporizador, el cual retardará la activación del objeto de mensaje (etapa 940). El agente de optimización 608 también puede analizar estadísticas de diseminaciones previas de información para el sistema 200 con el fin de determinar el valor correspondiente al mecanismo de temporizador. Más específicamente, el agente de optimización 608 puede fijar el valor del mecanismo de temporizador de manera que sea igual a la cantidad de tiempo promedio que se requiere para que un objeto de mensaje sea compartido con un porcentaje predeterminado de los dispositivos de control de acceso en el sistema. Por ejemplo, el valor del mecanismo de temporizador se puede fijar igual a 2 días si se tarda históricamente dos días para que el 99% de los dispositivos de control de acceso reciban un objeto de mensaje.

Después de que el agente de optimización 608 haya generado varias sugerencias, las mismas se proporcionan al usuario del sistema 200 (etapa 944). Las optimizaciones sugeridas se pueden implementar a discreción del administrador del sistema dependiendo de la naturaleza y la importancia del objeto de mensaje y de la cantidad de seguridad requerida para el sistema de acceso seguro 200.

Aunque el diagrama de flujo antes descrito se ha expuesto en relación con una secuencia particular de eventos, debería apreciarse que se pueden producir cambios en esta secuencia sin influir materialmente en el funcionamiento de la invención. Adicionalmente, no es necesario que la secuencia exacta de eventos se produzca tal como se expone en las formas de realización ejemplificativas. Las técnicas ejemplificativas ilustradas en el presente documento no se limitan a las formas de realización ilustradas específicamente, sino que se pueden utilizar también con las otras formas de realización ejemplificativas, y cada características descrita es reivindicable de forma individual y por separado.

Los sistemas, métodos y protocolos de esta invención se pueden implementar en un ordenador de función especializada, además o en lugar de los equipos de control de acceso descritos, un microprocesador o microcontrolador programado y elemento(s) de circuitos integrados periféricos, un ASIC u otro circuito integrado, un procesador de señal digital, un circuito electrónico o lógico de conexión permanente, tal como un circuito de elementos discretos, un dispositivo lógico programable tal como un PLD, PLA, FPGA, PAL, un dispositivo de comunicaciones, tal como un servidor, un ordenador personal, cualesquiera medios comparables, o similares. En general, para implementar los diversos métodos, protocolos y técnicas de mensajería de datos de acuerdo con esta invención se puede usar cualquier dispositivo capaz de implementar una máquina de estados que, a su vez, sea capaz de implementar la metodología ilustrada en el presente documento.

Además, los métodos dados a conocer se pueden implementar fácilmente en software usando entornos de desarrollo de software de objetos u orientado a objetos, que proporcionen código fuente portable que se pueda usar en una variedad de plataformas de ordenadores o estaciones de trabajo. Alternativamente, el sistema dado a conocer se puede implementar de forma parcial o completa en hardware usando circuitos lógicos convencionales o diseño de VLSI. El uso de software o hardware para implementar los sistemas de acuerdo con esta invención depende de los requisitos de velocidad y/o eficacia del sistema, de la función particular, y los sistemas particulares de software o hardware o sistemas de microprocesador o microordenador que se estén utilizando. Los sistemas, métodos y protocolos de análisis ilustrados en el presente documento se pueden implementar fácilmente en hardware y/o software usando cualesquiera sistemas o estructuras, dispositivos y/o software, conocidos o que se desarrollen posteriormente, por expertos en la materia, a partir de la descripción funcional proporcionada en el presente documento y con un conocimiento básico general de las técnicas informáticas.

Por otra parte, los métodos dados a conocer se pueden implementar fácilmente en software que se puede almacenar en un soporte de almacenamiento, y se puede ejecutar en un ordenador programado de uso general con la cooperación de un controlador y memoria, un ordenador de función especializada, un microprocesador, o similares. En estos casos, los sistemas y métodos de esta invención se pueden implementar como un programa incorporado en un ordenador personal, tal como una miniaplicación, un guión de instrucciones JAVA® o CGI, como un recurso residente en un servidor o estación de trabajo informática, como una rutina incorporada en un sistema o componente de sistema de comunicaciones dedicado, o similares. El sistema también se puede implementar incorporando físicamente el sistema y/o método en un sistema de software y/o hardware, tal como los sistemas de hardware y software de un dispositivo o sistema de comunicaciones.

Se pone de manifiesto, por lo tanto, que se han proporcionado, de acuerdo, con la presente invención, sistemas, aparatos y métodos para optimizar la mensajería de datos en un sistema de acceso seguro que tiene por lo menos

un lector no conectado en red. Aunque esta invención se ha descrito conjuntamente con una serie de formas de realización, es evidente que muchas alternativas, modificaciones y variaciones resultarían o son evidentes para los expertos en la materia. Por consiguiente, se pretende abarcar todas estas alternativas, modificaciones, equivalentes y variaciones que se sitúan dentro del alcance de la presente invención.

REIVINDICACIONES

1. Método para el análisis de la diseminación de información en un sistema de control de acceso que tiene por lo menos un lector no conectado en red, que comprende:

recibir información de anfitriones de mensajes;

recibir información de portadores de mensajes, en el que se pueden hacer funcionar portadores de mensajes (112, 220) para transportar objetos de mensaje entre anfitriones de mensajes (108, 204, 208);

analizar, con un módulo de análisis de red (604), la información de anfitriones de mensajes y de portadores de mensajes para determinar por lo menos uno de (i) una cantidad de tiempo requerida para comunicar un primer objeto de mensaje a un número predeterminado de anfitriones de mensajes (108, 204, 208) y/o un número predeterminado de portadores de mensajes (112, 220) y (ii) un número de anfitriones de mensajes (108, 204, 208) y/o portadores de mensajes (112, 220) que recibirán el primer objeto de mensaje antes de una cantidad predeterminada de tiempo; y

proporcionar, con el módulo de análisis de red (604), una salida a un usuario (724), que indica resultados de la etapa de análisis, en el que el método comprende además:

recibir requisitos de diseminación de mensajes, que definen el tiempo requerido en el que el número predeterminado de anfitriones de mensajes y/o portadores de mensajes deberían recibir un objeto de mensaje;

determinar si el primer objeto de mensaje se diseminará en por lo menos el número predeterminado de anfitriones de mensajes y/o portadores de mensajes dentro del tiempo requerido; e

incluir en la salida resultados de la etapa de determinación, y caracterizado porque la información de anfitriones de mensajes comprende ubicaciones y capacidades de red propuestas, para anfitriones de mensajes en un sistema de control de acceso, porque la información de portadores de mensajes (616) comprende un número propuesto de portadores de mensajes asociados al sistema de control de acceso, y porque la salida comprende por lo menos uno de (a) una ubicación diferente sugerida, para por lo menos un anfitrión de mensajes, (b) una capacidad de red diferente sugerida, para por lo menos un anfitrión de mensajes, y (c) un número diferente sugerido de portadores de mensajes.

2. Método según la reivindicación 1, en el que la salida comprende una capacidad de red diferente para por lo menos un anfitrión de mensajes identificado, y en el que la capacidad de red diferente comprende proporcionar un enlace de comunicación directo entre el por lo menos un anfitrión de mensajes identificado y otro dispositivo de red en el sistema de control de acceso.

3. Método según la reivindicación 1, en el que el objeto de mensaje comprende un mensaje legible por máquina.

4. Método según la reivindicación 1, en el que la información de anfitriones de mensajes comprende ubicaciones y capacidades de red reales para anfitriones de mensajes en un sistema de control de acceso, y en el que la información de portadores de mensajes comprende un número real de portadores de mensajes asociados al sistema de control de acceso.

5. Método según la reivindicación 1, en el que la salida comprende estadísticas de diseminación para el primer objeto de mensaje.

6. Método según la reivindicación 5, en el que las estadísticas de diseminación comprenden por lo menos una de (a) una probabilidad de que el primer objeto de mensaje llegue a un primer anfitrión de mensajes dentro del tiempo requerido, (b) una indicación de tiempo necesario para que el primer objeto de mensaje llegue al primer anfitrión de mensajes dentro de una probabilidad predeterminada, (c) una probabilidad de que el primer anfitrión de mensajes no reciba el objeto de mensaje, y (d) una probabilidad de que un primer portador de mensajes no reciba el objeto de mensaje.

7. Método según la reivindicación 1, en el que la salida comprende sugerencias para optimizar la diseminación del primer objeto de mensaje en el número predeterminado de anfitriones de mensajes.

8. Método según la reivindicación 7, en el que las sugerencias para optimizar la diseminación del primer objeto de mensaje incluyen por lo menos una de (a) un anfitrión de mensajes sugerido en el cual introducir el primer objeto de mensaje en un sistema de control de acceso, (b) un portador de mensajes sugerido en el cual introducir el primer objeto de mensaje en el sistema de control de acceso, y (c) una actualización retardada sugerida.

9. Método según la reivindicación 8, en el que las sugerencias para optimizar la diseminación del primer objeto de mensaje comprenden una actualización retardada sugerida y en el que el primer objeto de mensaje comprende un

mecanismo de temporizador que activa el primer objeto de mensaje en un tiempo predeterminado después de que el primer objeto de mensaje se haya introducido en el sistema de control de acceso.

10. Método según la reivindicación 1, en el que anfitriones de mensajes comprenden lectores de control de acceso, en el que portadores de mensajes comprenden credenciales de control de acceso, y en el que el primer objeto de mensaje comprende información de políticas para los lectores de control de acceso que incluyen una actualización de control de acceso que cambia derechos de acceso para por lo menos una credencial de control de acceso con el fin de acceder a por lo menos un activo asociado a un lector de control de acceso.

11. Método según la reivindicación 1, en el que la salida comprende un número mínimo esperado de etapas de reparto necesarias para transportar un primer objeto de mensaje desde un dispositivo de control de acceso de origen a un dispositivo de control de acceso de destino.

12. Método según la reivindicación 1, en el que la etapa de análisis comprende por lo menos una de las siguientes:

leer un fichero registro de por lo menos uno de un anfitrión de mensajes y un portador de mensajes;

calcular una matriz de adyacencia ponderada para un tiempo de un evento correspondiente al tiempo requerido;

calcular una distribución para el flujo de datos entre anfitriones de mensajes y portadores de mensajes;

identificar portadores de mensajes que contactarán con cada anfitrión de mensajes durante el tiempo del evento;

identificar anfitriones de mensajes que serán contactados por cada portador de mensajes durante el tiempo del evento;

identificar agrupamientos de portadores de mensajes que contactarán con un número predeterminado de anfitriones de mensajes durante el tiempo del evento;

identificar agrupamientos de anfitriones de mensajes que serán contactados por un número predeterminado de portadores de mensajes durante el tiempo del evento; y

calcular una velocidad de propagación para el primer objeto de mensaje durante el tiempo del evento, en el que la velocidad de propagación se basa en la iniciación del mensaje en uno o más dispositivos de control de acceso.

13. Soporte legible por ordenador que comprende instrucciones ejecutables por procesador que se pueden hacer funcionar para realizar el método según la reivindicación 1.

14. Dispositivo de herramienta de análisis de red, para el análisis de la diseminación de información en un sistema de control de acceso que tiene por lo menos un lector no conectado en red, que comprende:

un módulo de análisis de red (604) que se puede hacer funcionar para analizar flujos de información en un sistema de control de acceso que comprende una pluralidad de anfitriones de mensajes (108, 204, 208), siendo por lo menos uno de ellos un anfitrión de mensajes no conectado en red (208), y una pluralidad de portadores de mensajes (112, 220) que se pueden hacer funcionar para transportar objetos de mensaje entre anfitriones de mensajes (108, 204, 208), en el que el módulo de análisis de red (604) se puede hacer funcionar además para determinar por lo menos uno de (i) una cantidad de tiempo requerida para comunicar un primer objeto de mensaje a un número predeterminado de anfitriones de mensajes (108, 204, 208) y/o un número predeterminado de portadores de mensajes (112, 220) y (ii) un número de anfitriones de mensajes (108, 204, 208) y/o portadores de mensajes (112, 220) que recibirán el primer objeto de mensaje antes de una cantidad de tiempo predeterminada, en el que el módulo de análisis de red se puede hacer funcionar además para recibir requisitos de diseminación de mensajes que definen el tiempo requerido en el que el número predeterminado de anfitriones de mensajes (108, 204, 208) y/o portadores de mensajes (112, 220) deberían recibir un objeto de mensaje, determinar si el primer objeto de mensaje se diseminará en por lo menos el número predeterminado de anfitriones de mensajes (108, 204, 208) y/o portadores de mensajes (112, 220) dentro del tiempo requerido e incluir resultados de la determinación en la salida, y caracterizado porque la información de anfitriones de mensajes comprende ubicaciones y capacidades de red propuestas, para anfitriones de mensajes en un sistema de control de acceso, porque la información de portadores de mensajes (616) comprende un número propuesto de portadores de mensajes (112, 220) asociados al sistema de control de acceso, y porque la salida comprende por lo menos una de (a) una ubicación diferente sugerida, para por lo menos un anfitrión de mensajes (108, 204, 208), (b) una capacidad de red diferente sugerida, para por lo menos un anfitrión de mensajes (108, 204, 208), y (c) un número diferente sugerido de portadores de mensajes (112, 220).

15. Dispositivo según la reivindicación 14, en el que la salida comprende una capacidad de red diferente para por lo menos un anfitrión de mensajes identificado (108, 204, 208), y en el que la capacidad de red diferente comprende proporcionar un enlace de comunicación directo entre el por lo menos un anfitrión de mensajes identificado (108, 204, 208) y otro dispositivo de red en el sistema de control de acceso.

16. Dispositivo según la reivindicación 14, en el que el objeto de mensaje comprende un mensaje legible por máquina.

17. Dispositivo según la reivindicación 14, en el que la información de anfitriones de mensajes comprende ubicaciones y capacidades de red reales para anfitriones de mensajes (108, 204, 208) en un sistema de control de acceso, y en el que la información de portadores de mensajes comprende un número real de portadores de mensajes (112, 220) asociados al sistema de control de acceso.

18. Dispositivo según la reivindicación 14, en el que la salida comprende estadísticas de diseminación para el primer objeto de mensaje, en el que las estadísticas de diseminación comprenden por lo menos una de (a) una probabilidad de que el primer objeto de mensaje llegue a un primer anfitrión de mensajes (108, 204, 208) antes del tiempo requerido, (b) una indicación de tiempo necesario para que el primer objeto de mensaje llegue al primer anfitrión de mensajes (108, 204, 208) dentro de una probabilidad predeterminada, (c) una probabilidad de que el primer anfitrión de mensajes (108, 204, 208) no reciba el objeto de mensaje, y (d) una probabilidad de que un primer portador de mensajes (112, 220) no reciba el objeto de mensaje.

19. Dispositivo según la reivindicación 14, en el que las sugerencias para optimizar la diseminación del primer objeto de mensaje incluyen por lo menos una de (a) un anfitrión de mensajes sugerido (108, 204, 208) en el cual introducir el primer objeto de mensaje en un sistema de control de acceso, (b) un portador de mensajes sugerido (112, 220) en el cual introducir el primer objeto de mensaje en el sistema de control de acceso, y (c) una actualización retardada sugerida.

20. Dispositivo según la reivindicación 19, en el que las sugerencias para optimizar la diseminación del primer objeto de mensaje comprenden una actualización retardada sugerida y en el que el primer objeto de mensaje comprende un mecanismo de temporizador que activa el primer objeto de mensaje en un tiempo predeterminado, después de que el primer objeto de mensaje se haya introducido en el sistema de control de acceso.

21. Dispositivo según la reivindicación 14, en el que los anfitriones de mensajes (108, 204, 208) comprenden lectores de control de acceso, en el que portadores de mensajes (112, 220) comprenden credenciales de control de acceso, y en el que el primer objeto de mensaje comprende información de políticas para los lectores de control de acceso, que incluyen una actualización de control de acceso que cambia derechos de acceso para por lo menos una credencial de control de acceso con el fin de acceder a por lo menos un activo asociado a un lector de control de acceso.

22. Dispositivo según la reivindicación 14, en el que la salida comprende un número mínimo esperado de etapas de reparto necesarias para transportar un primer objeto de mensaje desde un dispositivo de control de acceso de origen a un dispositivo de control de acceso de destino.

23. Dispositivo según la reivindicación 14, en el que se puede hacer funcionar el módulo de análisis de red para realizar además por lo menos una de las siguientes:

leer un fichero registro de por lo menos uno de un anfitrión de mensajes (108, 204, 208) y un portador de mensajes (112, 220);

calcular una matriz de adyacencia ponderada para un tiempo de un evento correspondiente al tiempo requerido;

calcular una distribución para el flujo de datos entre anfitriones de mensajes (108, 204, 208) y portadores de mensajes (112, 220);

identificar portadores de mensajes (112, 220) que contactarán con cada anfitrión de mensajes (108, 204, 208) durante el tiempo del evento;

identificar anfitriones de mensajes (108, 204, 208) que serán contactados por cada portador de mensajes (112, 220) durante el tiempo del evento;

identificar agrupamientos de portadores de mensajes (112, 220) que contactarán con un número predeterminado de anfitriones de mensajes (108, 204, 208) durante el tiempo del evento;

identificar agrupamientos de anfitriones de mensajes (108, 204, 208) que serán contactados por un número predeterminado de portadores de mensajes (112, 220) durante el tiempo del evento; y

calcular una velocidad de propagación para el primer objeto de mensaje durante el tiempo del evento, en el que la velocidad de propagación se basa en la iniciación del mensaje en uno o más dispositivos de control de acceso.

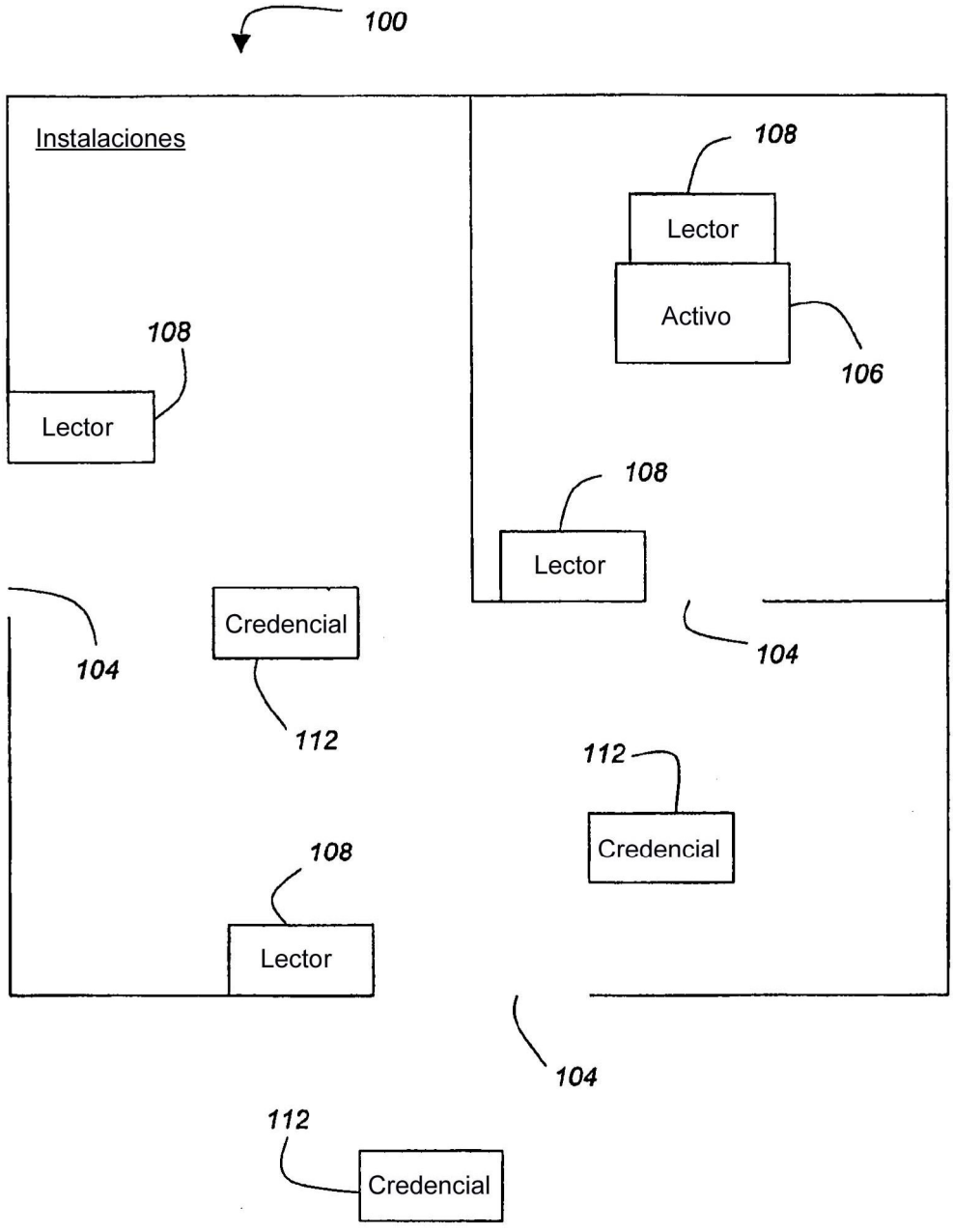
100
Instalaciones
108
Lector
Activo
106
108
Lector
108
Lector
104
Credencial
112
104
112
Credencial
108
Lector
104
112
Credencial

Fig. 1

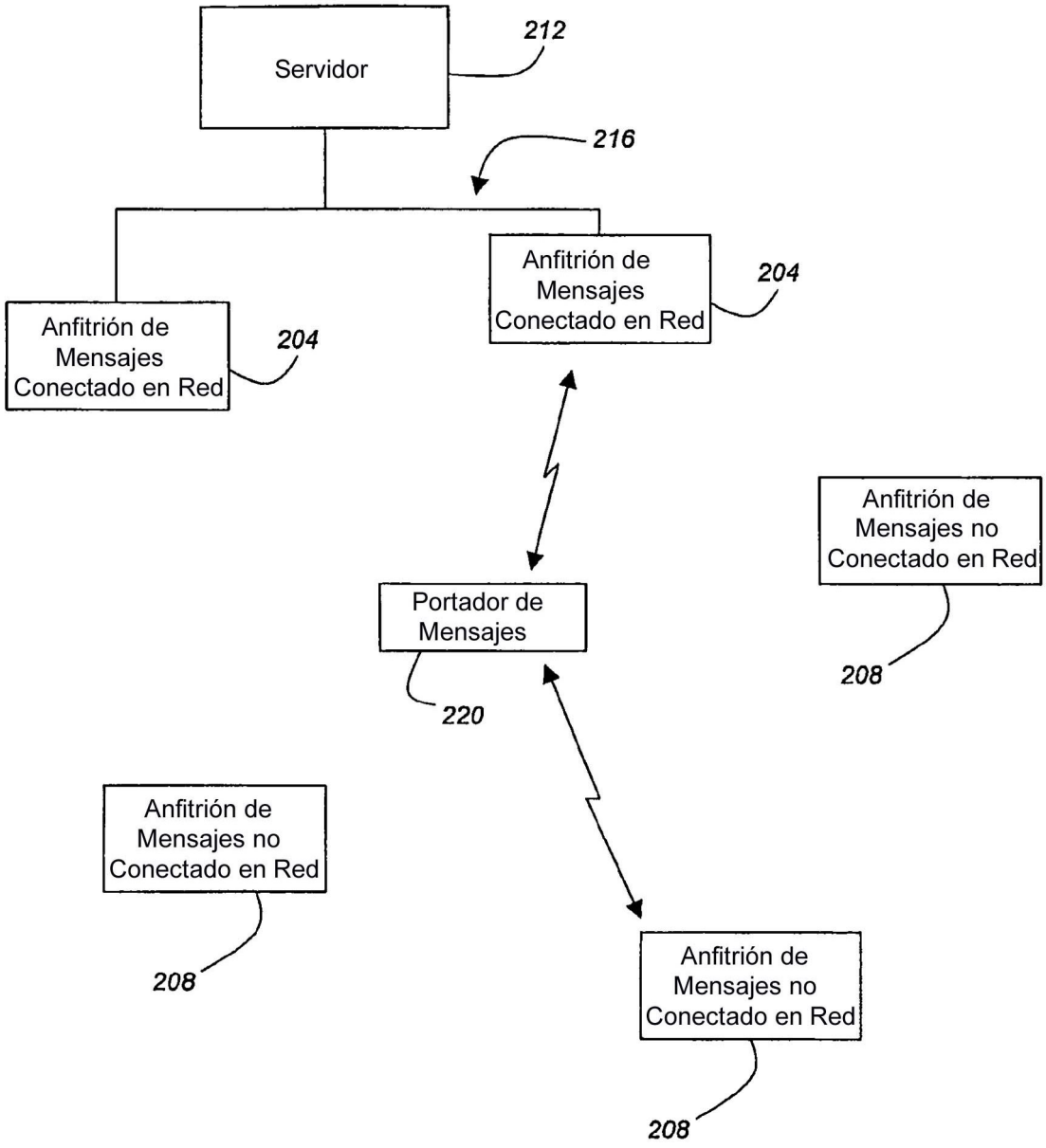
Servidor
212
216
Anfitrión de Mensajes Conectado en Red
204
Anfitrión de Mensajes Conectado en Red
204
Portador de Mensajes
220
Anfitrión de Mensajes no Conectado en Red
208
Anfitrión de Mensajes no Conectado en Red
208
Anfitrión de Mensajes no Conectado en Red
208

Fig. 2

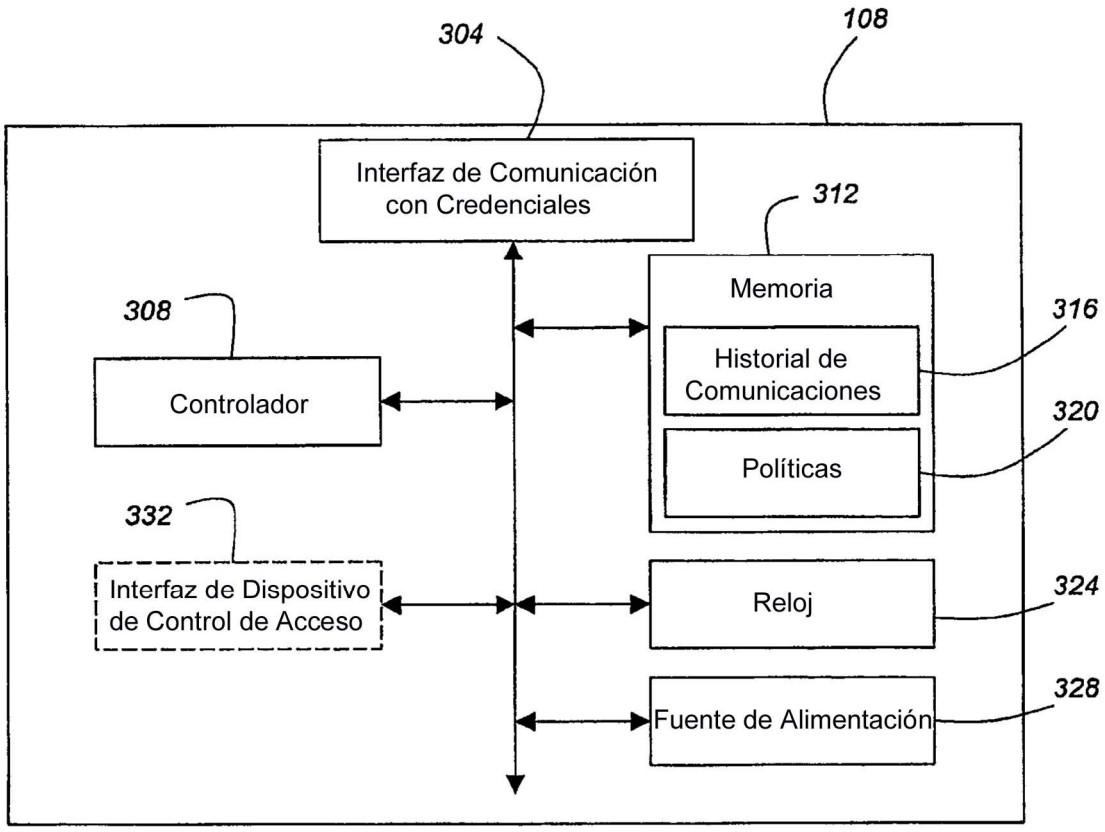
304
108
Interfaz de Comunicación con Credenciales
312
Memoria
316
Historial de Comunicaciones
320
Políticas
308
Controlador
332
Interfaz de Dispositivo de Control de Acceso
Reloj
324
Fuente de Alimentación
328

Fig. 3

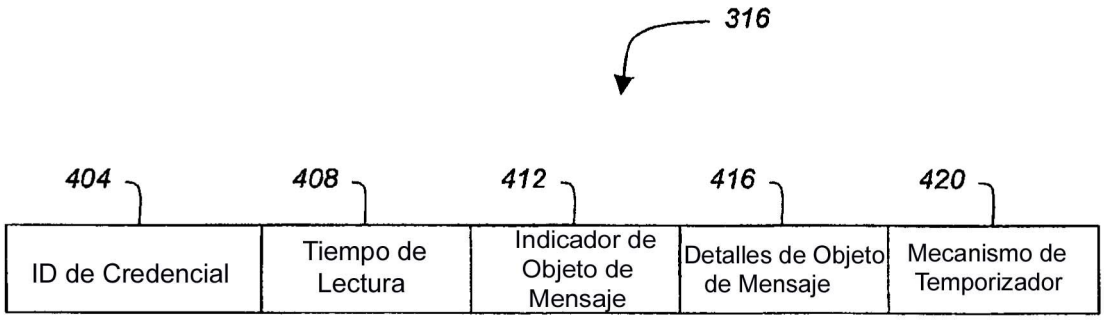
316
404
408
412
416
420
ID de Credencial
Tiempo de Lectura
Indicador de Objeto de Mensaje
Detalles de Objeto de Mensaje
Mecanismo de Temporizador

Fig. 4

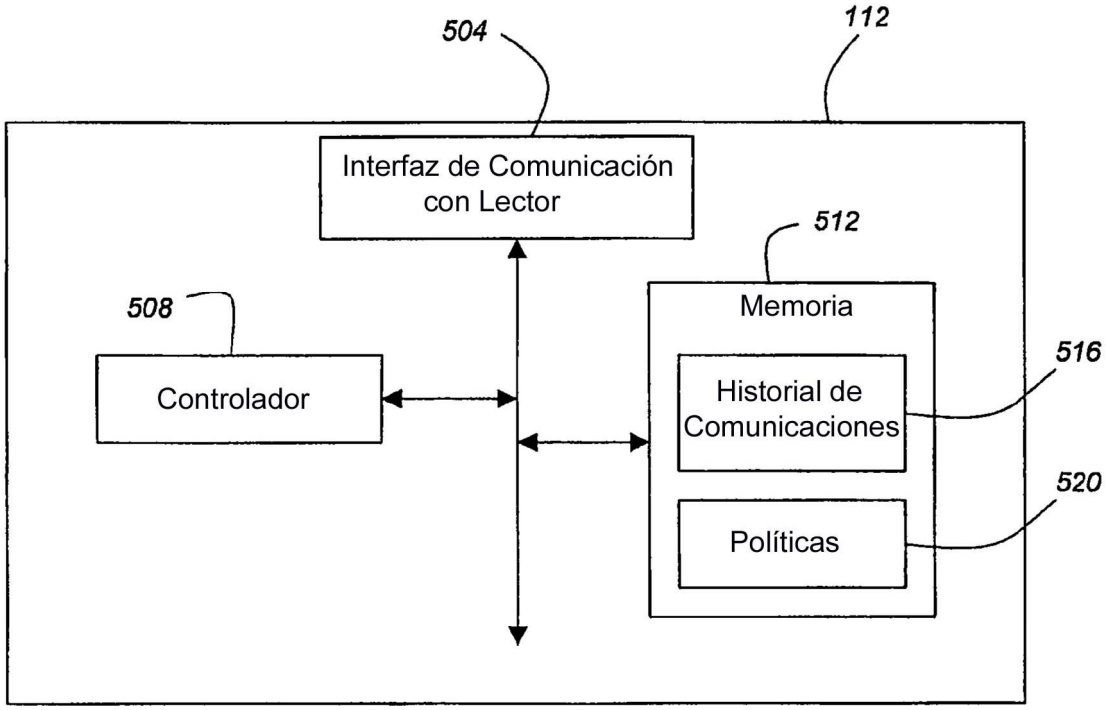
504
112
Interfaz de Comunicación con Lector
512
508
Memoria
Controlador
516
Historial de Comunicaciones
520
Políticas

Fig. 5

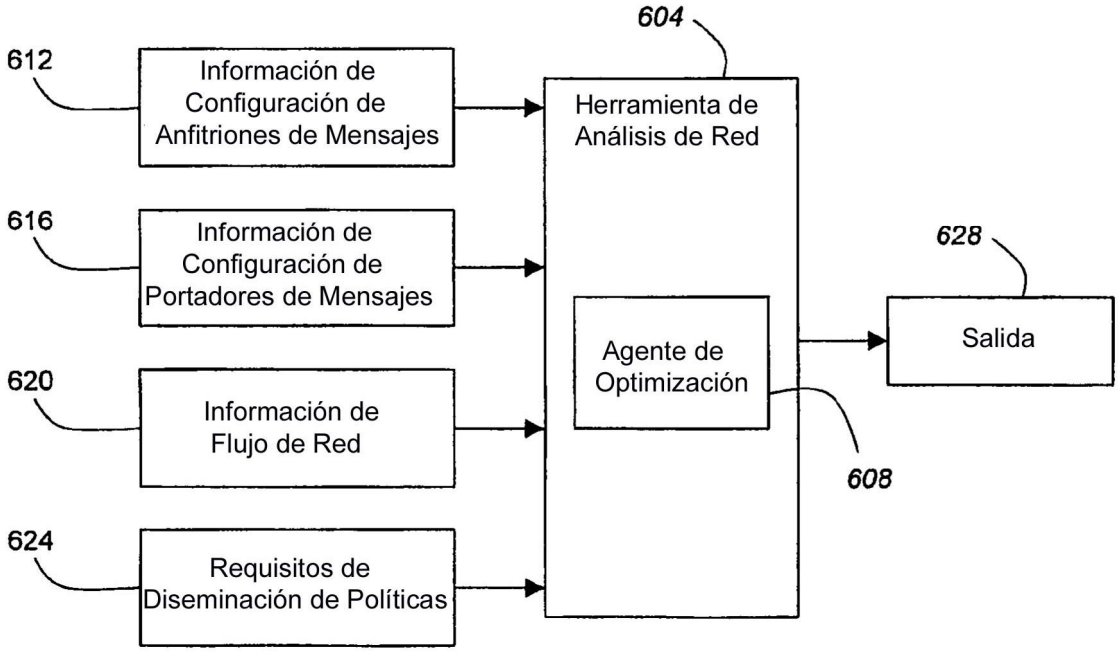
604
612
Información de Configuración de Anfitriones de Mensajes
Herramienta de Análisis de Red
616
Información de Configuración de Portadores de Mensajes
628
Agente de Optimización
Salida
620
Información de Flujo de Red
608
624
Requisitos de Diseminación de Políticas

Fig. 6

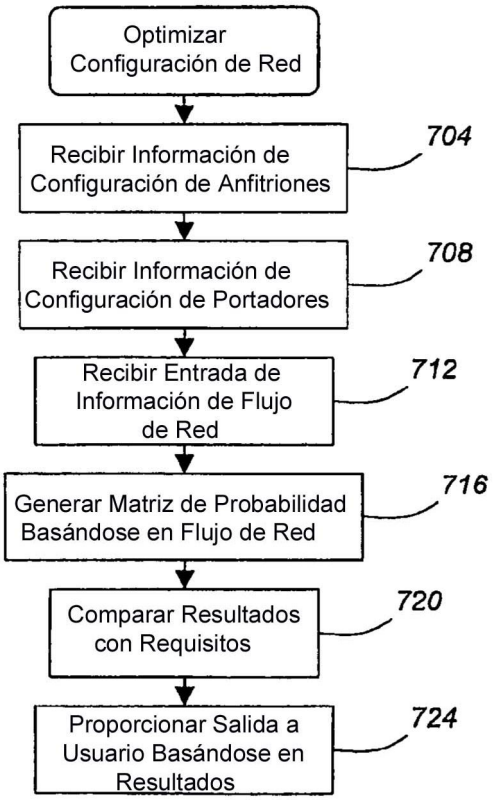
Optimizar Configuración de Red
Recibir Información de Configuración de Anfitriones
704
Recibir Información de Configuración de Portadores
708
Recibir Entrada de Información de Flujo de Red
712
Generar Matriz de Probabilidad Basándose en Flujo de Red
716
Comparar Resultados con Requisitos
720
Proporcionar Salida a Usuario Basándose en Resultados
724

Fig. 7

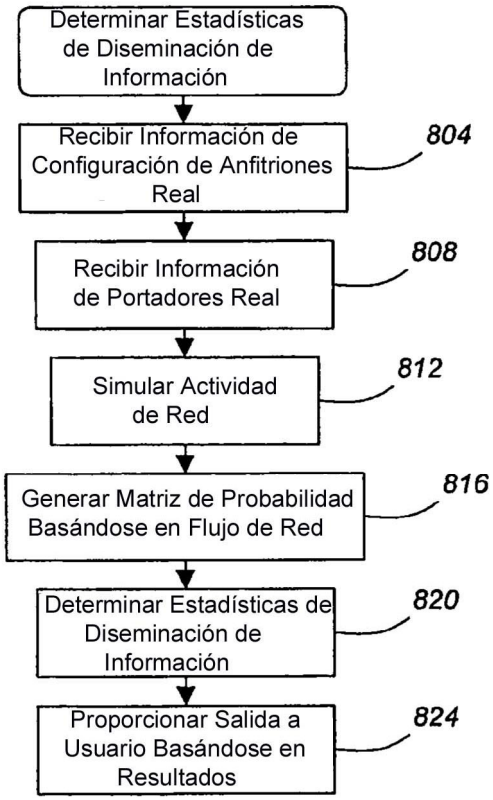
Determinar Estadísticas de Diseminación de Información
Recibir Información de Configuración de Anfitriones Real
804
Recibir Información de Portadores Real
808
Simular Actividad de Red
812
Generar Matriz de Probabilidad Basándose en Flujo de Red
816
Determinar Estadísticas de Diseminación de Información
820
Proporcionar Salida a Usuario Basándose en Resultados
824

Fig. 8

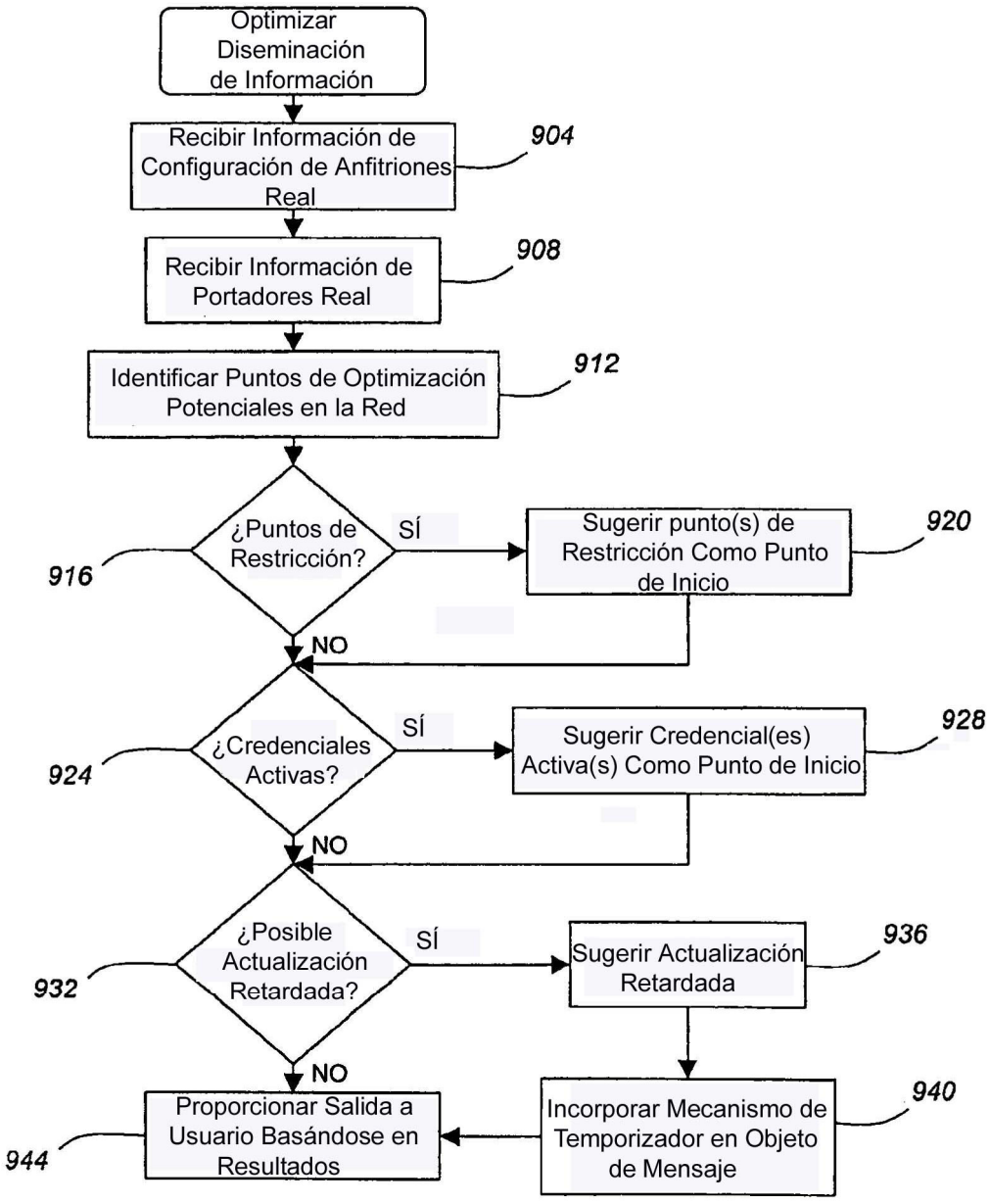
Optimizar Diseminación de Información
Recibir Información de Configuración de Anfitriones Real
904
Recibir Información de Portadores Real
908
Identificar Puntos de Optimización Potenciales en la Red
912
¿Puntos de Restricción?
916
SÍ
Sugerir punto(s) de Restricción Como Punto de Inicio
920
NO
¿Credenciales Activas?
924
SÍ
Sugerir Credencial(es) Activa(s) Como Punto de Inicio
928
NO
¿Posible Actualización Retardada?
932
SÍ
Sugerir Actualización Retardada
936
NO
Incorporar Mecanismo de Temporizador en Objeto de Mensaje
940
Proporcionar Salida a Usuario Basándose en Resultados
944

Fig. 9

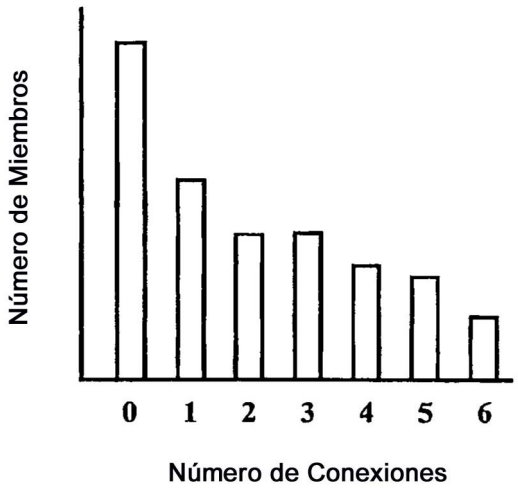

Fig. 10

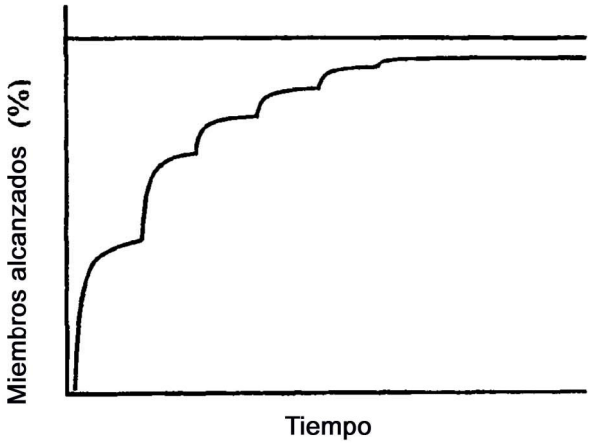

Fig. 11