(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 380 684**

(51) Int. CI.:
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06821187 .9**
(96) Fecha de presentación: **12.10.2006**
(97) Número de publicación de la solicitud: **1946524**
(97) Fecha de publicación de la solicitud: **23.07.2008**

(54) Título: **Método de detección de proximadad mejorado**

(30) Prioridad:
14.10.2005 US 726956 P

(45) Fecha de publicación de la mención BOPI:
17.05.2012

(45) Fecha de la publicación del folleto de la patente:
17.05.2012

(73) Titular/es:
KONINKLIJKE PHILIPS ELECTRONICS N.V.
GROENEWOUDSEWEG 1
5621 BA EINDHOVEN, NL

(72) Inventor/es:
EPSTEIN, Michael y
KRASINSKI, Raymond, J.

(74) Agente/Representante:
Zuazo Araluze, Alexander

DESCRIPCIÓN

Método de detección de proximidad mejorado

En los últimos años, el número de sistemas de protección de contenido disponibles ha crecido rápidamente. Algunos de estos sistemas sólo protegen el contenido frente a la copia no autorizada, mientras que otros limitan la capacidad del usuario para acceder al contenido. Estos sistemas suelen denominarse sistemas de Gestión de Derechos Digitales (DRM).

Los consumidores desean disfrutar de contenido sin problemas y con las menores limitaciones posibles. Desean conectar sus dispositivos en red para habilitar todo tipo de aplicaciones diferentes y acceder fácilmente a cualquier tipo de contenido. También desean poder compartir/transferir contenido en su entorno doméstico sin limitaciones.

Un modo de proteger contenido en forma de datos digitales es garantizar que el contenido sólo se transferirá desde un dispositivo de transmisión (dispositivo de origen, por ejemplo un grabador de vídeo digital, DVR) hasta un dispositivo de recepción (dispositivo de destino, por ejemplo un dispositivo de visualización de televisión) si el dispositivo de recepción ha sido autenticado como un dispositivo conforme y si el usuario del contenido tiene derecho a transferir (mover, copiar) ese contenido a otro dispositivo. Si se permite la transferencia de contenido, esto se realizará normalmente en un modo cifrado para asegurarse de que el contenido no pueda capturarse en un formato digital de alta calidad, no protegido.

La tecnología para realizar autenticación de dispositivo y transferencia de contenido cifrado está disponible y se denomina canal autenticado seguro (SAC). En muchos casos, se establece un SAC usando un protocolo de Intercambio de Clave y Autenticación (AKE) que se basa en criptografía de clave pública. Suelen usarse normas tales como la Norma Internacional ISO/IEC 11770-3 y la ISO/IEC 9796-2, y algoritmos de clave pública tales como RSA y algoritmos *hash* como SHA- 1.

Para establecer un SAC, cada dispositivo normalmente contiene una clave de cifrado única que se usa en un protocolo de desafío/respuesta con otro dispositivo para calcular una clave temporal, compartida mutuamente. Los dos dispositivos usan a continuación esta clave compartida para proteger el contenido y la información de derechos de uso intercambiados.

Un problema que queda es que un SAC puede establecerse entre dispositivos que están, físicamente o en cuanto a red, alejados entre sí. Para limitar esta posibilidad, se han realizado diversas propuestas para cierta forma de medición de distancia que va a realizarse cuando se establece el SAC. Si los dispositivos de origen y destino están demasiado alejados entre sí, el SAC no debe establecerse o debe rechazarse o limitarse el intercambio de contenido.

Normalmente tal medición de distancia implica un protocolo desafío-respuesta en la que el tiempo entre el envío del desafío y la recepción de la respuesta se mide y se usa para estimar la distancia entre los dispositivos de origen y destino. La medición de distancia puede combinarse con el protocolo de autenticación del establecimiento de SAC, tal como se enseña, por ejemplo, en la solicitud de patente internacional WO 2004/014037 (expediente PHNL020681).

Otros métodos de medición de distancia se dan a conocer en las solicitudes de patente internacional WO 2003/079638 (expediente PHUS020086), WO 2004/030311 (expediente PHUS010314) y WO 2004/030312 (expediente PHUS020358).

La patente estadounidense 5.812.524 da a conocer un algoritmo de restauración distribuido (DRA) de red autorrestaurada (SHN) usado para restaurar tráfico interrumpido entre dos nodos adyacentes. Al detectar un fallo, el nodo remitente construye una señal de restauración que incluye un campo de identificador ponderado. El mensaje de restauración se difunde a nodos tándem a los que se había proporcionado, a cada uno, una tabla de memoria con una pluralidad de pesos almacenados en la misma asociado cada uno con un enlace libre particular conectado al nodo. Al detectar un mensaje de restauración entrante, un nodo tándem recupera de su tabla el peso asociado con el enlace libre desde el que se recibió el mensaje de restauración. El identificador ponderado se recupera del mensaje de restauración y se actualiza con el peso que el nodo tándem había recuperado de su tabla. El identificador ponderado actualizado se reinserta en el mensaje de restauración y el mensaje de restauración actualizado se difunde a nodos aguas abajo para su propagación adicional al nodo seleccionador. Cuando el mensaje de restauración llega a cada nodo tándem con éxito, el identificador ponderado continúa actualizándose. El nodo seleccionador, al recibir el mensaje de restauración, recupera el identificador ponderado y compara el identificador ponderado con otros identificadores ponderados de otros mensajes de restauración recibidos antes de exceder el tiempo de espera de restauración. Basándose en esta comparación, el nodo seleccionador selecciona una ruta alternativa con el mejor identificador ponderado.

La solicitud PCT WO 01/57665 da a conocer un método en el que un centro de datos recibe una petición de contenido desde una búsqueda de un cliente. El centro de datos determina si el contenido solicitado está disponible

en el centro de datos. El contenido está disponible cuando el contenido está presente en el centro de datos y además es actual. El contenido puede expirar y marcarse como no disponible en respuesta a una instrucción de expiración. Cuando el contenido solicitado está disponible en el centro de datos, el centro de datos devuelve el contenido solicitado al centro de datos. Cuando el contenido solicitado no está disponible localmente en el centro de datos, el contenido solicitado se recupera desde un servidor de origen. La recuperación del contenido desde el servidor de origen puede retardarse basándose en la carga de procesamiento en el servidor de origen. Cuando se retarda la recuperación del contenido, la petición se prioriza y se coloca en una cola para su gestión por el servidor de origen basándose en la prioridad de la petición. Asimismo, cuando se retarda la recuperación del contenido, puede comunicarse una página de estatus al navegador para informar a un usuario del retardo y proporcionar contenido alternativo e información de estatus relacionada con la petición determinada en función de la petición o el estado actual del servidor de origen.

Un dispositivo de destino puede funcionar como dispositivo de origen para otros dispositivos de destino adicionales. Puede informarse de estos dispositivos de destino adicionales al dispositivo de origen, de modo que el dispositivo de origen conozca que no sólo está conectado a un dispositivo de destino sino que en realidad lo está a múltiples dispositivos de destino.

Todos estos dispositivos de origen y destino conectados pueden visualizarse en forma de árbol. Habitualmente hay un nodo “raíz” que hace que el contenido esté disponible para muchos nodos “intermedios”. Los nodos intermedios pueden conectarse a otros nodos intermedios y/o a “nodos” hoja. Los nodos hoja contienen medios de salida para entregar contenido. Los nodos intermedios también pueden contener tales medios de salida, o pueden servir únicamente para pasar contenido de un nodo a otro.

En general no es fácil para el nodo raíz determinar de manera segura si todos los nodos intermedios y hoja están dentro de la proximidad requerida al nodo raíz. El nodo raíz sólo tiene acceso seguro a cualquier nodo conectado directamente al mismo. La información acerca de nodos más remotos puede obtenerse haciendo que los nodos remotos proporcionen esta información al nodo raíz. Sin embargo, estos mensajes deben pasar a través de uno o más nodos intermedios. Esto introduce el riesgo de que un atacante bloquee o elimine tales mensajes, o los altere de modo que la proximidad de uno o más de estos nodos remotos no pueda determinarse.

Un objeto de la presente invención es mejorar lo anterior. Este objeto se logra según la invención en un método según la reivindicación 1. La proximidad entre un nodo hoja y el nodo raíz se determina añadiendo los valores de proximidad de enlace de todos los enlaces en el trayecto entre ese nodo hoja y el nodo raíz. Esta suma representa el tiempo de ida y vuelta entre ese nodo hoja y el nodo raíz. Si esta suma supera un valor predeterminado máximo, el nodo hoja y el nodo raíz están demasiado alejados entre sí. Preferiblemente el nodo inicial es el nodo hoja, y el nodo final es el nodo raíz.

Si el nodo raíz inicia el método, entonces un atacante puede bloquear los mensajes de petición de cálculo de proximidad y los nodos hoja nunca podrán determinar si están dentro de la proximidad requerida. Haciendo que los nodos hoja inicien el método, se vuelve posible requerir que los nodos hoja se nieguen a procesar el contenido si no se recibió respuesta o acuse de recibo en un tiempo predeterminado. Por tanto se requiere que un atacante deje que pasen las peticiones.

El espacio asignado en la petición para almacenar el valor de proximidad puede ser de tamaño limitado. De manera ventajosa a continuación puede proporcionarse una etiqueta de desbordamiento en la petición. Si la adición de un valor de proximidad de enlace al valor de proximidad almacenado da como resultado un valor que no puede almacenarse en dicho espacio, la etiqueta de desbordamiento se ajusta a “activado”. Esto permite al nodo final determinar que el valor de proximidad total calculado supera el máximo que puede almacenarse en la petición. Con una elección apropiada del espacio que va a asignarse, se deduce que el valor de proximidad total calculado debe superar la proximidad máxima permitida.

En las reivindicaciones dependientes se exponen realizaciones ventajosas.

La invención se analizará ahora en más detalle con referencia a las figuras, en las que:

la figura 1 muestra esquemáticamente un sistema que comprende dispositivos interconectados a través de una red;

la figura 2 ilustra esquemáticamente un dispositivo de origen y un dispositivo de destino; y

la figura 3 ilustra esquemáticamente un árbol de dispositivos interconectados.

A lo largo de las figuras, los mismos números de referencia indican características similares o correspondientes. Algunas de las características indicadas en los dibujos se implementan normalmente en software, y como tal representan entidades de software, tales como módulos u objetos de software.

La figura 1 muestra esquemáticamente un sistema 100 que comprende dispositivos 101-105 interconectados a

través de una red 110. Una red doméstica digital típica incluye un número de dispositivos, por ejemplo un receptor de radio, un sintonizador/decodificador, un reproductor de CD, un par de altavoces, una televisión, un VCR, un grabador digital, un teléfono móvil, una unidad de cinta, un ordenador personal, un asistente digital personal, una unidad de visualización portátil, un sistema de entretenimiento para vehículo, etc. Estos dispositivos habitualmente están interconectados para permitir a un dispositivo, por ejemplo, la televisión, controlar otro, por ejemplo el VCR. Un dispositivo, tal como por ejemplo el sintonizador/decodificador o un decodificador de Internet (STB), es habitualmente el dispositivo central, que proporciona control central sobre los otros.

El contenido, que normalmente comprende cosas como música, canciones, películas, animaciones, discursos, vídeos musicales, programas de televisión, imágenes, juegos, tonos de llamada, audiolibros y similares, pero que también puede incluir servicios interactivos, se recibe a través de una pasarela residencial o decodificador 101 de Internet. El contenido también puede entrar en casa a través de otros orígenes, tales como medios de almacenamiento como discos o usando dispositivos portátiles. El origen puede ser una conexión a una red cableada de banda ancha, una conexión a Internet, un enlace descendente de satélite, etc. El contenido puede transferirse entonces a través de la red 110 a un destino para entregarla. Un destino puede ser, por ejemplo, la pantalla 102 de televisión, el dispositivo 103 de visualización portátil, el teléfono 104 móvil y/o el dispositivo 105 de reproducción de audio.

El modo exacto en que un elemento de contenido se entrega depende del tipo de dispositivo y del tipo de contenido. Por ejemplo, en un receptor de radio, la entrega comprende generar señales de audio y alimentarlas a altavoces. Para un receptor de televisión, la entrega generalmente comprende generar señales de audio y vídeo y alimentarlas a una pantalla de visualización y a unos altavoces. Para otros tipos de contenido, debe adoptarse una acción apropiada similar. La entrega también puede incluir operaciones tales como descifrar o desaleatorizar una señal recibida, sincronizar señales de audio y vídeo, etc.

El decodificador 101 de Internet, o cualquier otro dispositivo en el sistema 100, puede comprender un medio de almacenamiento SI tal como un disco duro de tamaño adecuado, que permite la grabación y reproducción posterior del contenido recibido. El medio de almacenamiento SI puede ser un Grabador Digital Personal (PDR) de cualquier tipo, por ejemplo un grabador DVD+RW, al que está conectado el decodificador 101 de Internet. El contenido también puede entrar en el sistema 100 almacenado en un soporte 120 tal como un Disco Compacto (CD) o un Disco Versátil Digital (DVD).

El dispositivo 103 de visualización portátil y el teléfono 104 móvil se conectan de manera inalámbrica a la red 110 usando una estación 111 base, por ejemplo, usando Bluetooth o IEEE 802.1 lb. Los otros dispositivos se conectan usando una conexión cableada convencional. Para permitir a los dispositivos 101-105 interactuar, están disponibles varias normas de interoperabilidad, que permiten a diferentes dispositivos intercambiar mensajes e información y controlarse entre sí. Una norma ampliamente conocida es la norma *Universal Plug and Play* (http: //www.upnp.org).

Es importante garantizar que los dispositivos 101-105 en la red doméstica no permiten la creación de copias no autorizadas del contenido mediante la interceptación del contenido cuando se desplaza a través de la red. Por tanto, los dispositivos 101-105 están dotados de un sistema de protección de datos para una interfaz de visualización digital. Este sistema de protección de datos garantiza que sólo pueden producirse transferencias de contenido autorizado y protegido desde un primer dispositivo, denominado a continuación en el presente documento dispositivo de origen o simplemente origen, hasta un segundo dispositivo, denominado a continuación en el presente documento dispositivo de destino o simplemente destino.

La figura 2 ilustra esquemáticamente un dispositivo 200 de origen y un dispositivo 220 de destino. Ambos dispositivos comprenden una interfaz digital IF, un procesador CPU y un componente de almacenamiento MEM. Normalmente el dispositivo 200 de origen es un dispositivo que tiene contenido que va a reproducirse en tiempo real (o transmitirse de otro modo) al dispositivo 220 de destino. El dispositivo 220 de destino normalmente entonces es un dispositivo que recibe este contenido reproducido en tiempo real y lo entrega, por ejemplo, a una pantalla de visualización.

Cualquiera de los dispositivos 101-105 mencionados anteriormente puede funcionar como dispositivo 200 de origen y/o como dispositivo 220 de destino. Cabe indicar que un dispositivo puede funcionar como dispositivo de origen respecto a otro dispositivo, y como dispositivo de destino respecto a un dispositivo adicional. Esto puede incluso suceder simultáneamente.

Un ejemplo de un dispositivo 200 de origen y un dispositivo 220 de destino es un grabador de vídeo digital (DVR) conectado a una pantalla de televisión. El contenido audiovisual digital grabado por el DVR se reproduce en tiempo real en la pantalla de modo que el usuario puede ver el contenido. El origen también puede ser un ordenador (portátil o de sobremesa), en el que el destino es su pantalla de visualización.

Tal como se muestra en la figura 2, la interfaz entre el dispositivo 200 de origen y el dispositivo 220 de destino comprende un enlace 211 principal unidireccional de alta velocidad y un canal 212 auxiliar bidireccional relativamente de baja velocidad. En una realización prevista por los inventores, el enlace 211 principal puede

transportar hasta 10 Gigabits por segundo y el canal 212 auxiliar tiene una tasa de transferencia de 1 Megabit por segundo. El enlace 211 principal se usa para transportar datos digitales comprimidos o descomprimidos tales como datos de audio y/o vídeo.

La tecnología para realizar la autenticación del dispositivo y la transferencia de contenido cifrado está disponible y se denomina canal autenticado seguro (SAC). Un SAC 210 se supone que se ha establecido tal como se muestra en la figura 2 para proteger los datos transferidos a través del enlace 211 principal y el enlace 212 auxiliar. Alternativamente sólo el enlace 211 principal o sólo el enlace 212 auxiliar puede protegerse por el SAC 210. Por ejemplo, si el contenido que va a transferirse ya está cifrado, no es necesario transferir el contenido a través de un SAC, puesto que eso conllevaría operaciones de cifrado dobles innecesarias. Aún alternativamente el SAC puede derivarse para algunas transferencias de mensaje, por ejemplo, para mensajes ya cifrados o para mensajes que pueden enviarse de manera segura sin protección.

Los SAC y las tecnologías subyacentes son ampliamente conocidos. Pueden usarse criptografía de clave pública y certificados digitales para la autenticación mutua entre los dispositivos de origen y destino. Los datos se transfieren a través del enlace principal en forma cifrada.

Se supone que los dispositivos de origen y destino ya han establecido el canal 210 autenticado seguro. Son posibles muchos modos de establecer un SAC. Qué técnica particular se elija queda fuera del alcance de la presente invención. También se supone que ambos dispositivos comparten una clave de autenticación secreta común (indicada por K) y otro secreto común (denominado semilla e indicado por R). Estos valores se calculan o intercambian preferiblemente durante la fase de establecimiento de SAC.

Tal como se comentó anteriormente, la estructura de los dispositivos 101-105 interconectados puede considerarse en forma de árbol. Esta estructura se ilustra esquemáticamente en la figura 3. Hay un nodo 301 raíz que hace que el contenido esté disponible para los nodos 302 intermedios. Los nodos 302 intermedios están a su vez conectados a otros nodos 302 intermedios y a nodos 303 hoja.

El nodo 301 raíz inicia el protocolo de detección de proximidad, recopila los mensajes desde los nodos 302, 303 intermedio y hoja y determina si hay dispositivos (nodos) que estén demasiado alejados. Si no, el nodo raíz no distribuye contenido a lo largo de cualquiera de los otros nodos hasta que el (los) dispositivo(s) que está(n) demasiado alejados se han eliminado de la red.

Por ejemplo, un requisito puede ser que un mensaje pueda desplazarse desde el nodo raíz hasta un nodo hoja y de vuelta en 7 milisegundos. Esto es lo suficientemente poco para saber con certeza razonable que un nodo hoja debe estar próximo al nodo raíz. La elección depende de muchos parámetros, tales como el tiempo de desplazamiento esperado de los datos a través de la red.

El requisito puede complementarse con un requisito relativo a cada enlace individual entre un dispositivo de origen y un dispositivo de destino. Por ejemplo, puede requerirse que el tiempo de ida y vuelta de un mensaje entre un dispositivo de origen y un dispositivo de destino sea inferior a 500 microsegundos, además del requisito anterior de que el tiempo de ida y vuelta entre el nodo raíz y el nodo hoja sea inferior a 7 milisegundos.

Hay uno o más dispositivos que sólo sirven como dispositivos de destino. Éstos son los nodos 303 hoja. Un dispositivo que sea un nodo hoja tiene medios de salida para entregar contenido, por ejemplo, una pantalla de visualización y/o altavoces. Un grabador de DVD u otro dispositivo para exportar contenido puede o puede no considerarse un dispositivo de destino.

Además hay cero o más dispositivos que funcionan como dispositivos de destino y como dispositivos de origen. Éstos son los nodos 302 intermedios. Estos dispositivos pueden comprender medios de salida aunque esto no es necesario. Los nodos intermedios también pueden servir para pasar contenido desde un nodo a otro.

Por ejemplo, un grabador de disco duro portátil puede servir como dispositivo de destino para recibir contenido desde un receptor de televisión digital. El grabador en sí mismo no comprende una pantalla. Cuando se conecta a una pantalla externa (por ejemplo, una pantalla de televisión TFT), la pantalla actúa como el dispositivo de destino, y como nodo hoja. El grabador ahora es tanto un destino como un origen.

La conexión entre dos nodos se denomina enlace. Dos nodos cualesquiera en la red inician un protocolo de medición de distancia para determinar sus propias distancias respectivas, habitualmente determinando el tiempo que se tarda en intercambiar mensajes. Este tiempo, el tiempo de ida y vuelta, está directamente relacionado con la distancia entre ellos.

Normalmente tal medición de distancia implica un protocolo desafío-respuesta en el que el tiempo entre el envío del desafío y la recepción de la respuesta se mide y usa para estimar la distancia entre los dispositivos de origen y destino. La medición de distancia puede combinarse con el protocolo de autenticación del establecimiento de SAC, tal como se enseña por ejemplo en la solicitud de patente internacional WO 2004/014037 (expediente

PHNL020681).

La solicitud de patente internacional WO 2003/079638 (expediente PHUS020086) menciona que el tiempo entre la consulta y la respuesta comprende tanto el tiempo para comunicar la consulta y su respuesta como el tiempo necesario para calcular la respuesta. El documento también insinúa la substracción del tiempo de procesamiento del tiempo medido entre el envío de la consulta y la recepción de la respuesta.

La distancia determinada entre un origen y destino particulares se almacena preferiblemente por el dispositivo de origen, aunque también puede almacenarse por el dispositivo de destino. Esta distancia se denomina a continuación en el presente documento “valor de proximidad de enlace”. La distancia puede recalcularse a intervalos regulares. La distancia puede recalcularse siempre que se haya transferido una determinada cantidad de datos desde el dispositivo de origen hasta el dispositivo de destino.

La proximidad entre un nodo hoja y el nodo raíz se determina añadiendo los valores de proximidad de enlace de todos los enlaces en el trayecto entre ese nodo hoja y el nodo raíz.

La determinación preferiblemente se inicia por un nodo hoja que envía una petición de cálculo de proximidad al nodo raíz. Esta petición contiene el valor de proximidad de enlace del enlace que conecta ese nodo hoja con su nodo de origen. Si este nodo de origen de hecho conserva este valor de proximidad de enlace, entonces el nodo hoja incluye el valor cero (0) en la petición.

Preferiblemente las peticiones de cálculo de proximidad están cifradas o firmadas. Si las peticiones no están ni cifradas ni firmadas, un atacante puede alterar los valores de proximidad contenidos en las peticiones. Además, preferiblemente las peticiones contienen un número de “desafío” aleatorio (o hápax). Sin un hápax de este tipo, un atacante puede registrar una petición antigua y reenviarla posteriormente, tras haber movido el dispositivo que envió la distancia máxima permitida. Mediante la reutilización de la petición grabada, puede engañarse al nodo raíz para que concluya que el dispositivo en cuestión todavía está dentro de la proximidad requerida. Esto se conoce como ataque de repetición.

Cada nodo intermedio que recibe la petición de cálculo de proximidad verifica en primer lugar la firma o descifra la petición, si es necesario. A continuación el nodo intermedio añade el valor de proximidad de enlace al valor incluido en la petición y a continuación envía el valor aumentado hacia la raíz junto con el hápax original. Cuando la petición llega al nodo raíz, este valor representa ahora el tiempo necesario para enviar un mensaje desde el nodo raíz hasta el nodo hoja que inició la determinación, y viceversa.

Una realización para transferir peticiones y respuestas entre nodos hoja y el nodo raíz funciona de la manera siguiente. El nodo 303 hoja envía la petición de cálculo de proximidad al nodo 302 intermedio al que está conectado. El nodo 302 intermedio lee el hápax y guarda el hápax en una tabla de encaminamiento asociada con un identificador para el nodo 303 hoja. El nodo 302 intermedio pasa entonces el mensaje de petición de cálculo de proximidad al nodo al que este nodo 302 intermedio está conectado.

Finalmente la petición llegará al nodo raíz. Si una respuesta se envía de vuelta, esta respuesta incluirá el hápax que estaba presente en la petición. El nodo 302 intermedio busca este hápax en su tabla de encaminamiento y reenvía la respuesta al nodo identificado por el identificador asociado con ese hápax en la tabla de encaminamiento.

Naturalmente, también son posibles otros modos de encaminar mensajes en una red.

El nodo raíz recibirá múltiples mensajes de petición de cálculo de proximidad de este tipo, uno desde cada nodo hoja. De nuevo, puede ser necesario verificar o descifrar la firma de cada mensaje. El nodo raíz también puede comprobar si se ha recibido con anterioridad el hápax en la petición. Si es así, la petición debe rechazarse, dado que es probable que se trate de un ataque de repetición (o un error de red).

Cada mensaje incluye un valor de tiempo de proximidad. El nodo raíz guarda los valores de tiempo de proximidad recibidos, o alternativamente sólo guarda el valor de tiempo de proximidad recibido más grande. El nodo raíz comprueba si cualquier valor de tiempo de proximidad recibido supera el tiempo máximo predeterminado permitido. Si este es el caso, entonces el nodo raíz no enviará ningún dato a ninguno de los nodos a los que está conectado, o alternativamente no a cualquier nodo en un trayecto cuyo valor de tiempo de proximidad supere el tiempo máximo permitido. El nodo raíz puede enviar un acuse de recibo a nodos cuyos valores de tiempo de proximidad estén dentro del tiempo máximo permitido.

Preferiblemente el nodo raíz realiza la comprobación de proximidad en un tiempo predeterminado, por ejemplo, periódicamente cada diez segundos.

Preferiblemente un nodo hoja debe dejar de recibir y/o entregar cualquier contenido cuando no ha recibido un acuse de recibo desde el nodo raíz en un tiempo predeterminado. Esto hace imposible para un atacante simplemente bloquear o filtrar mensajes de petición de cálculo de proximidad en un intento de ocultar el hecho de que un nodo

hoja está muy alejado.

El valor incluido en la petición normalmente se graba como una secuencia de bits, por ejemplo, como un número de 32 bits. Puede suceder que la adición de valores de proximidad de enlace al valor grabado en la petición dé como resultado un número que desborda el número de bits disponible. Para indicar este evento puede proporcionarse una etiqueta de indicación de desbordamiento especial en la petición, que se activa cuando se produce un desbordamiento.

La etiqueta de indicación de desbordamiento permite determinar al nodo raíz que se produjo un desbordamiento. Si este es el caso, se deduce que el tiempo de ida y vuelta total debe superar lo que puede grabarse en la petición. Si el número de bits para este valor se elige lo suficientemente grande, entonces un desbordamiento es una indicación de que el tiempo de ida y vuelta total debe ser mayor que el máximo permitido. Por tanto, el nodo raíz debe en este caso guardar un registro del desbordamiento y no enviar ningún dato a ninguno de los nodos a los que está conectado.

A intervalos regulares durante la transferencia de datos puede repetirse la detección de proximidad para verificar si los dispositivos están todavía a la proximidad requerida entre sí. Por ejemplo, la detección de proximidad puede realizarse cada minuto o tras cada 1024 paquetes de datos recibidos a través del enlace 211 principal.

La determinación de la distancia de los dispositivos en la red también puede iniciarse por el nodo raíz. El nodo raíz puede entonces limitar o bloquear la transferencia del contenido si no se han recibido respuestas en un periodo de tiempo predeterminado.

Debe observarse que las realizaciones mencionadas anteriormente ilustran en lugar de limitar la invención, y que los expertos en la técnica podrán diseñar muchas realizaciones alternativas sin alejarse del alcance de las reivindicaciones adjuntas.

En las reivindicaciones, ningún símbolo de referencia colocado entre paréntesis debe interpretarse como limitativo de la reivindicación. La palabra “que comprende” no excluye la presencia de elementos o etapas distintos de los enumerados en una reivindicación. La palabra “un” o “una” antes de un elemento no excluyen la presencia de una pluralidad de tales elementos.

La invención puede implementarse por medio de hardware que comprende varios elementos distintos, y por medio de un ordenador programado adecuadamente. En la reivindicación de dispositivo en la que se enumeran varios medios, varios de estos medios pueden realizarse mediante uno y el mismo elemento de hardware. El mero hecho de que se mencionen determinadas medidas en reivindicaciones dependientes diferentes entre sí no indica que no pueda usarse de manera ventajosa una combinación de estas medidas.

REIVINDICACIONES

1. Método de determinación de una proximidad entre un nodo (301) raíz y un nodo (303) hoja en una red, comprendiendo el método:

calcular un valor de proximidad de enlace entre dos nodos conectados entre sí cualesquiera en la red, en un nodo inicial, siendo uno del nodo raíz y el nodo hoja, enviando un mensaje de petición de cálculo de proximidad que contiene un contador de proximidad a un nodo intermedio al que está conectado dicho nodo inicial,

en un nodo (302) intermedio que está conectado a un primer nodo y a un segundo nodo, al recibir el mensaje de petición de cálculo de proximidad que contiene un contador de proximidad desde el primer nodo, añadir el valor de proximidad de enlace calculado al contador de proximidad y pasar el mensaje de petición de cálculo de proximidad al segundo nodo,

en un nodo final, que es el otro del nodo raíz y el nodo hoja, al recibir el mensaje de petición de cálculo de proximidad, determinar la proximidad entre el nodo raíz y el nodo hoja como el valor indicado por el contador de proximidad,

en el nodo raíz limitar o bloquear una comunicación de datos si se determina que la proximidad supera un umbral predeterminado.

2. Método según la reivindicación 1, en el que el nodo inicial es el nodo hoja.

3. Método según la reivindicación 2, en el que el valor de proximidad de enlace entre el nodo hoja y el nodo intermedio al que está conectado dicho nodo inicial se calcula y almacena por dicho nodo intermedio.

4. Método según la reivindicación 3, en el que el nodo hoja envía el mensaje de petición de cálculo de proximidad en el que el contador de proximidad está ajustado a cero.

5. Método según la reivindicación 1, en el que el mensaje de petición de cálculo de proximidad contiene además una etiqueta de desbordamiento, que se ajusta a un estado “desactivado” por el nodo inicial, en el que el nodo intermedio ajusta la etiqueta de desbordamiento a un estado “activado” si la adición del valor de proximidad de enlace calculado al contador de proximidad supera un máximo predeterminado, y en el que el nodo raíz restringe o bloquea la comunicación de datos si la etiqueta de desbordamiento está en el estado “activado”.

6. Sistema que comprende una pluralidad de dispositivos interconectados a través de una red y que están configurados para determinar una proximidad entre un nodo (301) raíz y un nodo (303) hoja en la red, estando configurados dos nodos conectados entre sí cualesquiera en la red para calcular un valor de proximidad de enlace entre sí,

un nodo inicial, siendo uno del nodo raíz y el nodo hoja, que está configurado para enviar un mensaje de petición de cálculo de proximidad que contiene un contador de proximidad a un nodo intermedio al que está conectado dicho nodo inicial,

un nodo (302) intermedio que está conectado a un primer nodo y a un segundo nodo, que está configurado para al recibir el mensaje de petición de cálculo de proximidad que contiene un contador de proximidad desde el primer nodo, añadir el valor de proximidad de enlace calculado al contador de proximidad y pasar el mensaje de petición de cálculo de proximidad al segundo nodo,

un nodo final, siendo el otro del nodo raíz y el nodo hoja, que está configurado para al recibir el mensaje de petición de cálculo de proximidad, determinar la proximidad entre el nodo raíz y el nodo hoja como el valor indicado por el contador de proximidad,

en el que el nodo raíz está configurado para limitar o bloquear una comunicación de datos si se determina que la proximidad supera un umbral predeterminado.

7. Dispositivo configurado para funcionar como el nodo inicial en el sistema según la reivindicación 6, en el que el dispositivo está configurado además para impedir la recepción y/o entrega de contenido si no se recibe ninguna respuesta al mensaje de petición de cálculo de proximidad en un periodo de tiempo predeterminado.

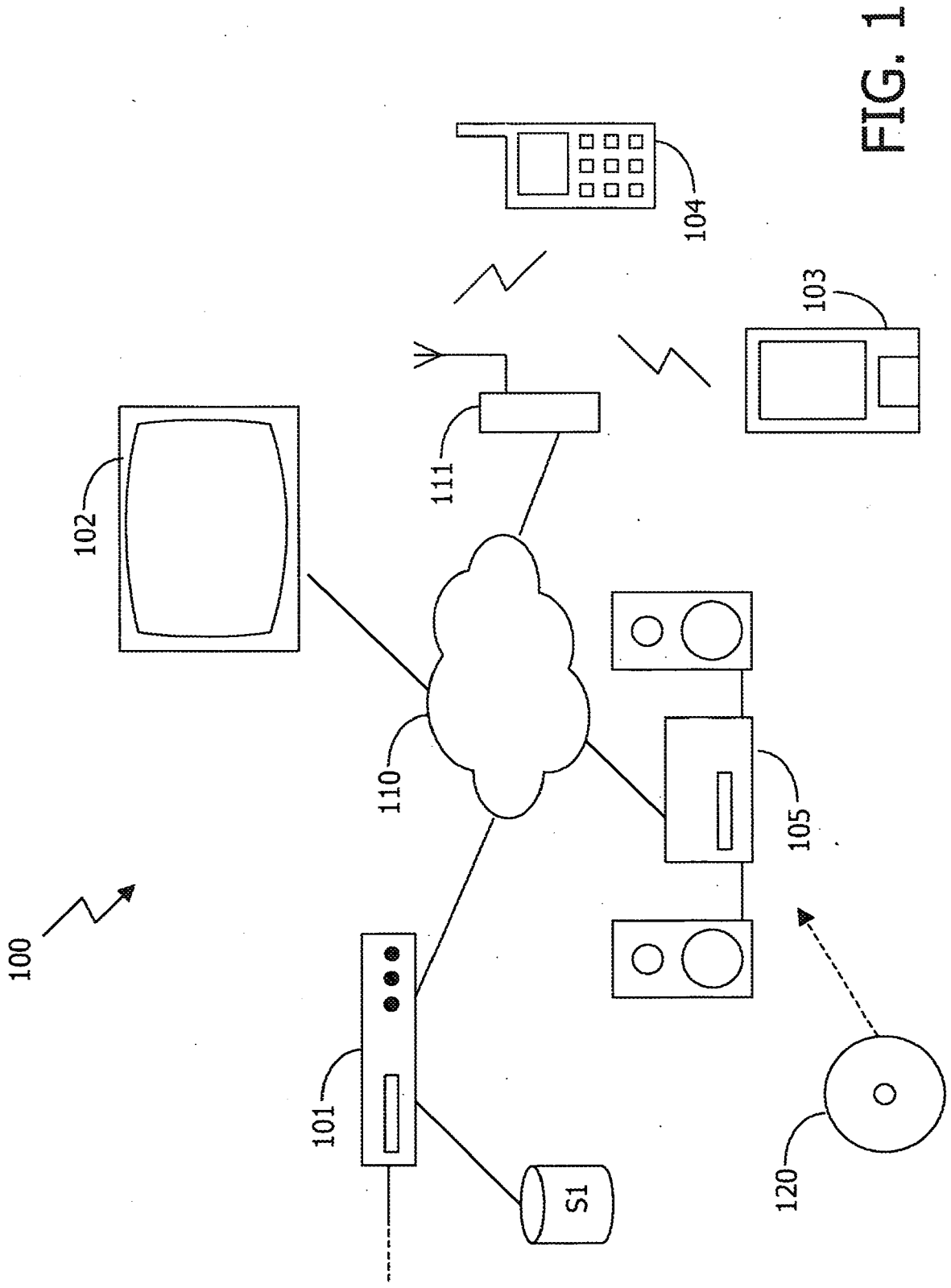

FIG. 1

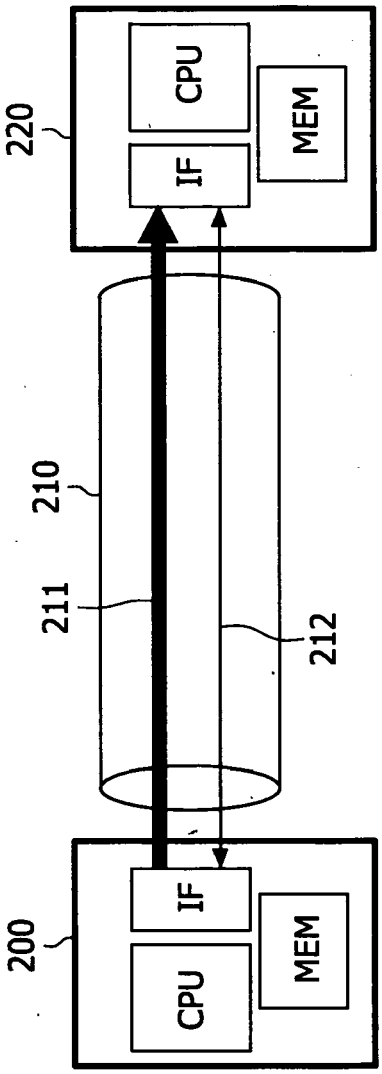
220
CPU
IF
MEM
210
211
212
200
IF
CPU
MEM

FIG. 2

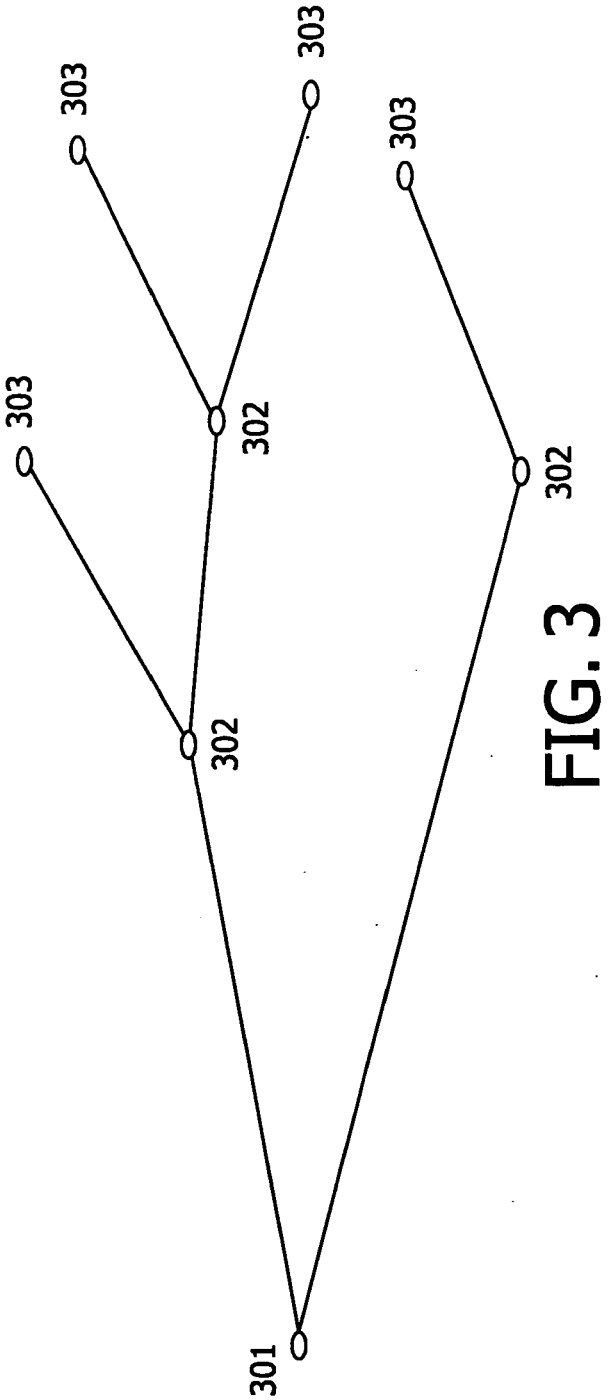
303
303
303
303
302
302
302
301

FIG. 3