(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 306 917**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03798316 .0**
(86) Fecha de presentación : **22.09.2003**
(87) Número de publicación de la solicitud: **1550285**
(87) Fecha de publicación de la solicitud: **06.07.2005**

(54) Título: **Verificación de un nodo en una red.**

(30) Prioridad: **30.09.2002 US 414944 P**
05.02.2003 US 445263 P

(45) Fecha de publicación de la mención BOPI:
16.11.2008

(45) Fecha de la publicación del folleto de la patente:
16.11.2008

(73) Titular/es: **Koninklijke Philips Electronics N.V.**
Groenewoudseweg 1
5621 BA Eindhoven, NL

(72) Inventor/es: **Epstein, Michael, A. y**
Grumiaux, Frederic

(74) Agente: **Zuazo Araluze, Alexander**

DESCRIPCIÓN

Verificación de un nodo en una red.

Esta invención se refiere al campo de seguridad de comunicaciones, y en particular, a un sistema y procedimiento que verifica la proximidad de un nodo en una red.

La seguridad de red puede a menudo mejorarse distinguiendo entre nodos "locales" y nodos "remotos" en la red. Los nodos locales, por ejemplo, están ubicados normalmente dentro de un entorno físico particular, y puede suponerse que los usuarios dentro de este entorno físico están autorizados para acceder a la red. Los nodos remotos, por otro lado, son susceptibles de acceso físico no autorizado. Adicionalmente, los intrusos no autorizados en una red normalmente acceden a la red de manera remota, a través de teléfono u otros canales de comunicación. Debido a la susceptibilidad de la red a acceso no autorizado a través de nodos remotos, la seguridad de red puede mejorarse imponiendo medidas de seguridad rigurosas, o restricciones de acceso, en los nodos remotos, mientras que no se carga a los nodos locales con estas mismas restricciones.

En Stevens *et al.*: "*TCP/IP Illustrated, Vol. 1: The Protocols*", Professional Computing Series, Reading, MA: Addison Wesley, EE.UU, 1994, páginas 85 a 96, ISBN 0-201-63346-9, se describe el programa Ping. El programa Ping prueba si puede alcanzarse otro ordenador central. El programa envía un mensaje de solicitud de eco ICMP a un ordenador central, esperando que se devuelva una respuesta de eco ICMP. Ping también mide el tiempo de ida y vuelta al ordenador central, dando alguna indicación de cómo de "lejos" está ese ordenador central. Ping puede calcular el tiempo de ida y vuelta almacenando el tiempo en el que envía la respuesta de eco en la parte de datos del mensaje ECMP. Cuando se devuelve la respuesta, resta este valor del tiempo actual.

Es un objeto de esta invención proporcionar un sistema y procedimiento que facilitan una determinación de si un nodo en una red es local o remoto. Es un objeto adicional de esta invención proporcionar un sistema y procedimiento que facilitan una determinación segura de si un nodo en una red es local o remoto. Es un objeto adicional de esta invención integrar esta determinación con un sistema o procedimiento que verifica la autenticidad del nodo en la red.

Estos y otros objetos se consiguen mediante un sistema y procedimiento que incluyen parámetros de temporización dentro de un protocolo de verificación de nodo, tal como el sistema de protección de copia abierto (OCPS, *Open Copy Protection System*), para facilitar una determinación de la proximidad de un nodo objetivo a un nodo fuente. El protocolo de verificación de nodo incluye una secuencia de petición-respuesta, en la que el nodo fuente comunica una petición al nodo objetivo, y el nodo objetivo comunica una respuesta correspondiente al nodo fuente. El nodo fuente establece un límite inferior en la distancia entre el nodo fuente y el nodo objetivo, basándose en una medida del tiempo requerido para efectuar esta secuencia de petición-respuesta. El tiempo requerido para efectuar esta secuencia incluye el tiempo requerido para comunicar la petición y respuesta, así como el tiempo requerido para procesar la petición y generar la respuesta. El nodo objetivo incluye una medida del tiempo requerido para procesar la petición y generar la respuesta al nodo fuente. El nodo fuente resta este tiempo del tiempo de petición-respuesta total para determinar el tiempo consumido para la comunicación. Este tiempo de comunicación se compara con un valor umbral para determinar si el nodo objetivo es local o remoto con respecto al nodo fuente.

La figura 1 ilustra un diagrama de bloques de ejemplo de una red de nodos.

La figura 2 ilustra un diagrama de bloques de ejemplo de un nodo fuente y objetivo que efectúan un protocolo de petición-respuesta según esta invención.

En todos los dibujos, los mismos números de referencia se refieren al mismo elemento, o un elemento que realiza sustancialmente la misma función.

La figura 1 ilustra un diagrama de bloques de ejemplo de una red 150 de nodos 110. Uno de los nodos, NodoD 110, se ilustra como estando distante de los otros nodos 110. Según esta invención, cada uno de los nodos 110 está configurado para poder determinar la proximidad de cada otro nodo 110. En una realización típica de esta invención, la determinación de proximidad se limita a una determinación de si el otro nodo es "local" o "remoto", aunque puede efectuarse una determinación más detallada de distancias utilizando las técnicas dadas a conocer en el presente documento.

La figura 2 ilustra un diagrama de bloques de ejemplo de un nodo 110S fuente y nodo 110T objetivo que efectúan un protocolo de petición-respuesta para determinar la proximidad del nodo 110T objetivo al nodo 110S fuente según esta invención. El nodo 110S fuente incluye un procesador 210 que inicia una petición, y un dispositivo 220 de comunicaciones que transmite la petición al nodo 110T objetivo. El nodo 110T objetivo recibe la petición y devuelve una respuesta correspondiente, a través de su dispositivo 230 de comunicaciones. Para garantizar que la respuesta corresponde a la petición comunicada, el protocolo pide al nodo 110T objetivo procesar al menos una parte de la petición e incluir un resultado de este procesamiento en la respuesta, a través de un procesador 240.

El nodo 110S fuente está configurado para medir el tiempo consumido por el proceso de petición-respuesta, ilustrado en la figura 2 como $T_{\text{petición}-\text{respuesta}}$ 280. Este tiempo 280 de petición-respuesta incluye el tiempo para comunicar

la petición y respuesta, $T_{comunicación}$ 260, así como el tiempo para procesar la petición y generar la respuesta en el nodo 110T objetivo, $T_{procesamiento}$ 270. Según esta invención, el nodo 110T objetivo está configurado para incluir una medida de este tiempo 270 de procesamiento dentro de la respuesta proporcionada al nodo 110S fuente. El nodo 110S fuente resta el tiempo 270 de procesamiento del tiempo 280 de petición-respuesta para determinar el tiempo 260 de comunicación. Utilizando técnicas conocidas, puede calcularse la distancia entre la fuente 110S y el objetivo 110T utilizando este tiempo 260 de comunicación determinado. Tal como se comentó anteriormente, en una realización típica, el tiempo 260 de comunicación se utiliza para determinar si el objetivo 110T es local o remoto desde la fuente 110S. Esta determinación se realiza en una realización preferida de esta invención comparando el tiempo 260 de comunicación con un valor umbral nominal, normalmente no más de unos pocos milisegundos. Si el tiempo 260 de comunicación está por debajo del umbral, se determina que el objetivo 110T es local; si no, se determina que es remoto.

En una realización típica, la fuente 110S utiliza la determinación de proximidad remoto/local para controlar comunicaciones posteriores con el objetivo 110T. Por ejemplo, puede permitirse transferir algunos archivos sólo a nodos locales, puede requerirse que todas las comunicaciones con un nodo remoto se encripten, etc. De manera opcional, pueden definirse múltiples niveles umbrales para distinguir diferentes intervalos de distancias, tal como si un nodo objetivo remoto está ubicado dentro del mismo país que el nodo fuente, etc.

Obsérvese que un nodo no autorizado puede derrocar el proceso anterior proporcionando un tiempo de procesamiento falso. En una realización preferida de esta invención, el proceso de petición-respuesta anterior está integrado dentro de un proceso de autenticación de nodo, tal como un proceso de intercambio de clave, que incluye normalmente una o más secuencias de petición-respuesta. Integrando el proceso de petición-respuesta dentro del proceso de autenticación de nodo, se verifica el tiempo de procesamiento notificado como auténtico.

El protocolo OCPS, por ejemplo, incluye una etapa de autenticación, una etapa de intercambio de clave, una fase de generación de clave, y fases de transmisión de datos posteriores. La fase de intercambio de clave se efectúa a través de un protocolo de intercambio de clave de Needham-Schroeder modificado, tal como se describe en "*Handbook of Applied Cryptography*", Menezes *et al*.

En la fase de autenticación, cada uno de los nodos fuente 110S y objetivo 110T autentifica una clave pública de cada uno de los otros.

Al inicio de la fase de intercambio de clave, la fuente 110S encripta un número aleatorio y una clave aleatoria, utilizando la clave pública del objetivo 110T, y transmite ambas encriptaciones al objetivo 110T. Según esta invención, el nodo 110S fuente inicia un temporizador cuando se transmiten estas encriptaciones al objetivo 110T.

El objetivo 110T desencripta el número aleatorio y la clave aleatoria, utilizando la clave privada del objetivo. El objetivo 110T genera un nuevo número aleatorio y una nueva clave aleatoria, y encripta el nuevo número aleatorio, la nueva clave aleatoria, y el número aleatorio desencriptado a partir de la fuente 110S, utilizando la clave pública de la fuente 110S, para formar una respuesta que ha de comunicarse a la fuente 110S. El objetivo 110T firma de manera opcional la respuesta, utilizando la clave privada del objetivo. Según esta invención, el objetivo 110T también incluye una medida del tiempo requerido para efectuar la desencriptación, encriptación y firma dentro de la respuesta firmada. Este tiempo de procesamiento se encripta de manera opcional utilizando la clave pública de la fuente. Debido a que este proceso de desencriptación, encriptación y firma consume generalmente la misma cantidad de tiempo en un nodo objetivo dado, el nodo objetivo está configurado preferiblemente para proporcionar un tiempo de procesamiento predefinido como la medida de tiempo para efectuar este procesamiento. Firmando la respuesta, el objetivo 110T une el tiempo de procesamiento notificado con los otros parámetros en la respuesta actual, impidiendo de ese modo una sustitución no autorizada del tiempo de procesamiento encriptado con un tiempo alternativo que se encripta utilizando la clave pública de la fuente 110S.

Cuando el nodo 110S fuente recibe la respuesta, finaliza el temporizador mencionado anteriormente. El nodo 110S fuente verifica el mensaje firmado, utilizando la clave pública del objetivo 110T, y desencripta los números aleatorios y la clave aleatoria a partir de la respuesta, utilizando la clave privada de la fuente 110S. Si el tiempo de procesamiento dentro de la respuesta está encriptado, también se desencripta en este tiempo mediante la fuente 110S, utilizando la clave privada de la fuente 110S. Según esta invención, la fuente 110S resta el tiempo de procesamiento de la duración de tiempo medida por el temporizador entre la transmisión de la petición encriptada desde la fuente 110S y la recepción de la respuesta encriptada del objetivo 110T para determinar el tiempo de comunicación de ida y vuelta entre la fuente 110S y el objetivo 110T.

Para confirmar el intercambio de clave, la fuente 110S transmite el nuevo número aleatorio desencriptado de vuelta al objetivo 110T. Tanto la fuente 110S como el objetivo 110T controlan las comunicaciones posteriores basándose en la recepción de los números aleatorios desencriptados apropiados. Según esta invención, la fuente 110S también controla las comunicaciones posteriores basándose en el tiempo de comunicación determinado.

Si se verifican ambos nodos, las comunicaciones posteriores entre la fuente 110S y el objetivo 110T encriptan las comunicaciones utilizando una clave de sesión que es una combinación de las claves aleatorias, las claves públicas, y un índice de sesión.

Lo anterior ilustra simplemente los principios de la invención. Por tanto, se apreciará que los expertos en la técnica podrán concebir diversas disposiciones que, aunque no se describen o muestran explícitamente en el presente documento, realizan los principios de la invención. Por ejemplo, en el protocolo OCPS descrito anteriormente, el nodo 110T objetivo también puede configurarse para determinar la proximidad del nodo 110S fuente, temporizando el proceso entre la transmisión de la respuesta encriptada y la recepción del número aleatorio desencriptado desde la fuente 110S. En esta realización, la fuente 110S está configurada para incluir una medida del tiempo requerido para procesar la respuesta encriptada y transmitir el número aleatorio desencriptado en el último mensaje de intercambio de clave que incluye el número aleatorio desencriptado, firmado digitalmente por la fuente 110S. El objetivo 110T resta este tiempo de procesamiento de su tiempo medida entre transmisión y recepción para determinar el tiempo de comunicación de ida y vuelta objetivo-fuente-objetivo, y por tanto la proximidad de la fuente 110S al objetivo 110T. Estas y otras características de configuración y optimización del sistema serán evidentes para un experto habitual en la técnica a la vista de esta descripción.

REIVINDICACIONES

1. Procedimiento de determinación de proximidad de un nodo (110T) objetivo a un nodo (110S) fuente, que comprende:

comunicar una petición desde el nodo (110S) fuente al nodo (110T) objetivo,

comunicar una respuesta desde el nodo (110T) objetivo al nodo (110S) fuente,

recibir la respuesta en el nodo (110S) fuente, y

determinar una medida de tiempo (280) de petición-respuesta entre la comunicación de la petición y la recepción de la respuesta,

caracterizado por

la respuesta desde el nodo (110T) objetivo que incluye una medida de tiempo (270) de procesamiento requerido para procesar la petición y producir la respuesta, y el nodo (110S) fuente

determinar la proximidad del nodo (110T) objetivo basándose en un tiempo (260) de comunicación que depende de una diferencia entre la medida de tiempo (280) de petición-respuesta y la medida de tiempo (270) de procesamiento.

2. Procedimiento según la reivindicación 1, en el que

la petición y respuesta corresponden a al menos una parte de un protocolo criptográfico de intercambio de clave.

3. Procedimiento según la reivindicación 2, en el que

el protocolo de intercambio de clave corresponde a un protocolo de intercambio de clave de Needham-Schroeder.

4. Procedimiento según la reivindicación 1, en el que

la petición y respuesta corresponden a al menos una parte de un protocolo OCPS.

5. Procedimiento según la reivindicación 1, en el que

la medida de tiempo de procesamiento en el nodo objetivo está predefinida.

6. Procedimiento según la reivindicación 1, en el que

la determinación de la proximidad incluye comparar el tiempo de comunicación con un valor umbral que distingue entre nodos locales y remotos.

7. Procedimiento según la reivindicación 1, que incluye además

restringir comunicaciones con el nodo objetivo basándose en la proximidad.

8. Procedimiento según la reivindicación 1, en el que

la respuesta se firma criptográficamente por el nodo objetivo.

9. Nodo (110) en una red que incluye:

un dispositivo (110T) de comunicación que está configurado para recibir una petición desde un nodo (110S) fuente y para transmitir una respuesta correspondiente al nodo (110S) fuente,

un procesador (240) que está configurado para procesar la petición y producir a partir de la misma la respuesta,

caracterizado porque la respuesta incluye una medida de tiempo (270) de procesamiento requerido para procesar la petición y producir la respuesta.

10. Nodo según la reivindicación 9, en el que

el procesador (240) está configurado para procesar la petición y producir la respuesta como parte de un protocolo criptográfico de intercambio de clave.

11. Nodo según la reivindicación 10, en el que

el protocolo de intercambio de clave corresponde a un protocolo de intercambio de clave de Needham-Schroeder.

12. Nodo según la reivindicación 9, en el que

la petición y respuesta corresponden a al menos una parte de un protocolo OCPS iniciado por el nodo fuente.

13. Nodo según la reivindicación 9, en el que

la medida de tiempo (270) de procesamiento está predefinida.

14. Nodo según la reivindicación 9, en el que

el procesador (240) está configurado además para firmar criptográficamente la respuesta.

15. Nodo (110) en una red que incluye:

un dispositivo (110S) de comunicación que está configurado para transmitir una petición a un nodo (110T) objetivo y para recibir una respuesta correspondiente desde el nodo (110T) objetivo,

un procesador (210) que está configurado para:

generar la petición,

recibir la respuesta, y

medir un tiempo (280) de petición-respuesta entre la generación de la petición y la recepción de la respuesta,

caracterizado por

la respuesta desde el nodo (110T) objetivo que incluye una medida de tiempo (270) de procesamiento requerido para procesar la petición y producir la respuesta en el nodo (110T) objetivo, y

estando configurado el procesador (210) para:

determinar una proximidad del nodo (110T) objetivo con respecto al nodo (110) basándose en un tiempo (260) de comunicación que depende de una diferencia entre el tiempo (280) de petición-respuesta y la medida de tiempo (270) de procesamiento.

16. Nodo según la reivindicación 15, en el que

el procesador (210) está configurado para generar la petición y recibir la respuesta como parte de un protocolo criptográfico de intercambio de clave.

17. Nodo según la reivindicación 16, en el que

el protocolo de intercambio de clave corresponde a un protocolo de intercambio de clave de Needham-Schroeder.

18. Nodo según la reivindicación 15, en el que

la petición y respuesta corresponden a al menos una parte de un protocolo OCPS iniciado por el nodo.

19. Nodo según la reivindicación 15, en el que

la medida de tiempo (270) de procesamiento está predefinida.

20. Nodo según la reivindicación 15, en el que

el procesador (210) está configurado para determinar la proximidad basándose en una comparación del tiempo (260) de comunicación con un valor umbral que distingue entre nodos locales y remotos.

21. Nodo según la reivindicación 15, en el que

el procesador (210) está configurado además para controlar comunicaciones posteriores con el nodo (110T) objetivo basándose en la proximidad.

22. Procedimiento de determinación de una proximidad de un nodo (110T) objetivo a un nodo (110S) fuente, que comprende, en el nodo (110T) objetivo:

recibir una petición desde el nodo (110S) fuente;

transmitir una respuesta correspondiente al nodo (110S) fuente; y

procesar la petición y producir a partir de la misma la respuesta;

caracterizado porque

la respuesta incluye una medida de tiempo (270) de procesamiento requerido para procesar la petición y producir la respuesta.

23. Procedimiento de determinación de proximidad de un nodo (110T) objetivo a un nodo (110S) fuente, que comprende, en el nodo (110S) fuente:

transmitir una petición a un nodo (110T) objetivo;

recibir una respuesta correspondiente desde el nodo (110T) objetivo; y

determinar una medida de tiempo (280) de petición-respuesta entre la transmisión de la petición y la recepción de la respuesta;

caracterizado por

la respuesta desde el nodo (110T) objetivo que incluye una medida de tiempo (270) de procesamiento requerido para procesar la petición y producir la respuesta en el nodo (110T) objetivo, y

determinar una proximidad del nodo (110T) objetivo con respecto al nodo (110) basándose en un tiempo (260) de comunicación que depende de una diferencia entre la medida de tiempo (280) de petición-respuesta y la medida de tiempo (270) de procesamiento.

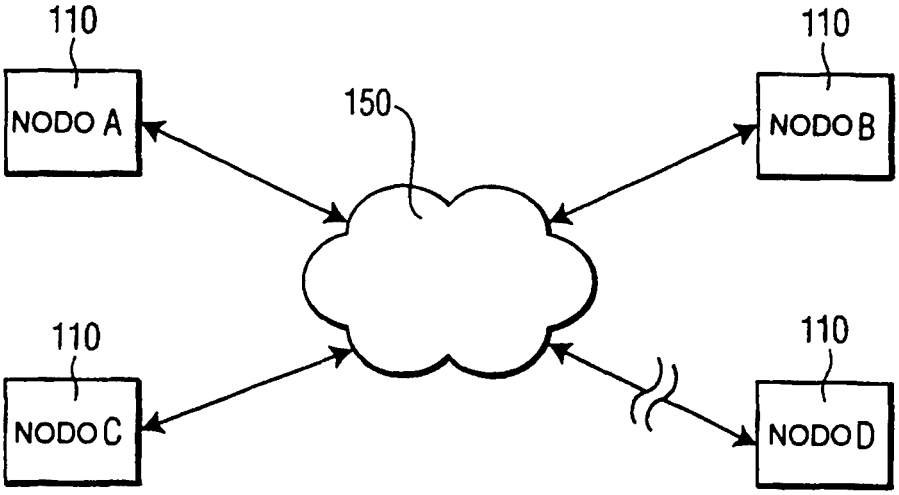
110
NODO A
110
NODO B
150
110
NODO C
110
NODO D

FIG. 1

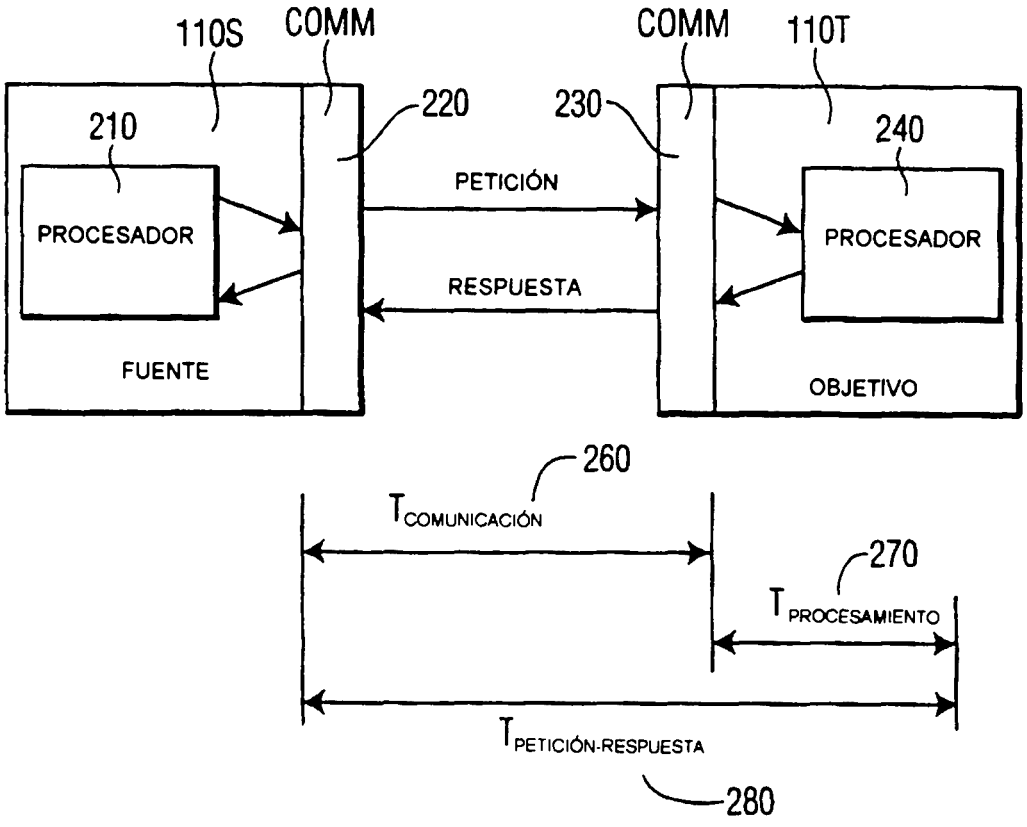
110S
COMM
COMM
110T
210
220
230
240
PETICIÓN
PROCESADOR
PROCESADOR
RESPUESTA
FUENTE
OBJETIVO
260
T COMUNICACIÓN
270
T PROCESAMIENTO
T PETICIÓN-RESPUESTA
280

FIG. 2