(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 394 214**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/24 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.06.2006 E 06754106 (0)**

(97) Fecha y número de publicación de la solicitud europea: **05.03.2008 EP 1894383**

(54) Título: **Método y dispositivos para medidas seguras de distancia basada en tiempo entre dos dispositivos**

(30) Prioridad:

20.06.2005 EP 05300494

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.01.2013

(73) Titular/es:

THOMSON LICENSING (100.0%)
1-5, RUE JEANNE D'ARC
92130 ISSY-LES-MOULINEAUX, FR

(72) Inventor/es:

COURTAY, OLIVIER;
KARROUMI, MOHAMED y
DURAND, ALAIN

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCION

Método y dispositivos para medidas seguras de distancia basada en tiempo entre dos dispositivos.

Campo de la invención

La presente invención se refiere en general a redes de comunicación, y en particular a la seguridad en tales redes.

Antecedentes de la invención

La distancia basada en tiempo se utiliza a menudo en el campo de las redes y se mide como la duración de una transmisión de paquete entre dos dispositivos. Existe un protocolo estándar de Internet, el Protocolo de Mensajes de Control de Internet (RFC 792; http://www.ietf.org/rfc/rfc792.txt), que permite el cálculo de una distancia en milisegundos entre dos anfitriones o "hosts". El comando asociado se llama "ping" y la distancia basada en tiempo se denomina Tiempo de Ida y Vuelta (en inglés, Round Trip Time (RTT)). Esta distancia basada en tiempo se utiliza, por ejemplo, para decidir si dos dispositivos se encuentran en proximidad local.

La Figura 1 ilustra el concepto de proximidad local en una red 100. La red 100 comprende dos redes de área local (en inglés, Local Area Network (LAN)), LAN L1 110 y LAN L2 120, interconectadas por la Internet 130. LAN L1 110 comprende el dispositivo A 112 y el dispositivo C 114, ambos dentro de un círculo 116 que ilustra la proximidad local, es decir, se considera que los dispositivos situados dentro del círculo están cercanos a un punto de referencia, en este caso el dispositivo A. La red LAN L2 120 comprende el dispositivo 122 B, que está situado fuera del círculo 116, lo que significa que no se considera cercano al dispositivo A.

En la técnica anterior, un método habitual para que el dispositivo A determine si el dispositivo B se encuentra en su proximidad cercana se basa en la duración basada en tiempo. El dispositivo A envía una serie de comandos ping al dispositivo B y mide los RTTs asociados. En cuanto el dispositivo A obtiene un RTT inferior a un límite determinado (por ejemplo 7 ms) considera que el dispositivo B se encuentra en su proximidad local. Si no es así, después de un número - típicamente 50 ó 100 – de RTTs superiores a este límite, considera que el dispositivo B no está en su proximidad local.

Existen otros métodos en los cuales el dispositivo A no determina directamente si el dispositivo B está o no cerca de él. Por ejemplo, el dispositivo A puede enviar mensajes al dispositivo de manera tal que sólo los reciban los dispositivos situados en su proximidad local. Un método típico es enviar mensajes con bajo "tiempo de vida" (en inglés, Time to Live (TTL)). Estos mensajes sólo pueden pasar a través de un número limitado (en concreto, el TTL) de nodos de red.

Sin embargo, la solución "ping" proporciona un bajo nivel de seguridad. El dispositivo A no tiene medios para asegurar que la respuesta a su comando ping provenga del dispositivo B, y por lo tanto que la distancia en tiempo que está midiendo se refiera a B. Un atacante (situado en la red LAN L1) puede bloquear todos los pings destinados a dispositivos fuera de la red LAN L1 y contestar en su nombre. El dispositivo A consideraría entonces que todos esos dispositivos se encuentran en su proximidad local. Este fallo se debe a la falta de seguridad de la técnica anterior.

Una solución básica para ese problema sería la autentificación de respuestas de ping utilizando medios criptográficos estándar: el dispositivo A envía un reto (en su comando ping hacia el dispositivo B) y espera la respuesta. Cuando la recibe, puede comprobar que sólo el dispositivo B podría haber calculado la respuesta. Por ejemplo, el dispositivo A puede enviar un número aleatorio al dispositivo B y el dispositivo B lo autentifica por ejemplo, firmándolo. El dispositivo A verifica a continuación el código de autentificación. En un segundo ejemplo, el dispositivo A encripta un reto y lo envía al dispositivo B, que responde con el reto descifrado.

Para demostrar que la respuesta de ping procede de él mismo, el dispositivo B tiene que realizar cálculos criptográficos antes de responder al dispositivo A. El tiempo necesario para los cálculos puede variar de un dispositivo a otro y ser muy importante en el caso de dispositivos de bajos recursos. El tiempo de cálculo puede llevar al dispositivo A a considerar que tales dispositivos de bajos recursos no están en su proximidad local, cuando en la realidad ocurre lo contrario. Claramente, esto no es deseable siempre. Naturalmente, el dispositivo A podría ampliar el límite de modo que los dispositivos de bajos recursos tuvieran tiempo de realizar los cálculos y responder. Sin embargo, el hacerlo así significaría que muchas veces serían considerados dentro de la proximidad local dispositivos de altos recursos que se encuentran fuera de la misma, lo que habitualmente no es deseable.

El documento WO 2004/014037 describe un método para medir de manera segura y autentificada una distancia entre un primer y un segundo dispositivos. El primer dispositivo autentifica al segundo dispositivo, intercambia un secreto con él, y transmite una señal para medir la distancia al mismo. A continuación, el segundo dispositivo modifica la señal recibida de acuerdo con el secreto y devuelve la señal modificada. Cuando el primer dispositivo recibe la señal modificada, mide el tiempo de ida y vuelta y verifica que la señal recibida ha sido modificada de acuerdo con el secreto intercambiado. Como se observará, el documento WO 2004/014037 puede ser considerado

como una implementación de la solución básica anterior al presente documento, y adolece de al menos algunos de sus inconvenientes.

Por tanto, se puede apreciar que existe la necesidad de un método para calcular distancia basada en tiempo que sea seguro e independiente de los recursos de los dispositivos. La presente invención proporciona tal método.

Compendio de la invención

La invención está definida por las reivindicaciones independientes.

En un primer aspecto, la invención está dirigida a un método para calcular en un primer dispositivo, de manera segura, distancia basada en tiempo a un segundo dispositivo de una red. El primer dispositivo envía un primer mensaje al segundo dispositivo y recibe como respuesta un segundo mensaje, y calcula la distancia en tiempo basándose en el momento de la transmisión del primer mensaje y el momento de la recepción del segundo mensaje. El primer dispositivo también recibe un mensaje adicional que contiene datos de autentificación vinculados criptográficamente al menos al primer mensaje o al menos al segundo mensaje o al menos al primer mensaje y al segundo mensaje, y verifica los datos de autentificación.

En una realización preferida, el primer dispositivo envía además un mensaje para solicitar el mensaje adicional que contenga datos de autentificación si la distancia basada en tiempo que se ha calculado se sitúa por debajo de un límite predeterminado.

En una realización preferida adicional, el primer mensaje contiene un primer elemento criptográfico y el segundo mensaje contiene un segundo elemento criptográfico, y los datos de autentificación se calculan basándose en el primer y el segundo elementos criptográficos.

Resulta ventajoso que los elementos criptográficos sean números aleatorios y los datos de autentificación sean el resultado de una función calculada utilizando los números aleatorios, siendo la función dependiente de un secreto. También resulta ventajoso que el primer dispositivo envíe un cuarto mensaje al segundo dispositivo para hacerle saber que se ha iniciado el método, y genere el primer elemento criptográfico. Resulta además ventajoso que el primer dispositivo espere un tiempo predeterminado a fin de dar tiempo al segundo dispositivo para que termine la generación del segundo elemento criptográfico.

En una realización alternativa, el primer dispositivo calcula los datos de autentificación, y el mensaje, enviado al segundo dispositivo para solicitar el mensaje adicional que contenga datos de autentificación del segundo dispositivo, contiene los datos de autentificación del primer dispositivo.

En otra realización preferida, el primer dispositivo valida además el cálculo de la distancia basada en tiempo hasta el segundo dispositivo tras la verificación satisfactoria de los datos de autentificación.

En un segundo aspecto, la invención está dirigida a un método para responder en un segundo dispositivo de una red a un protocolo para el cálculo seguro, en un primer dispositivo, de la distancia basada en tiempo hasta el segundo dispositivo. El segundo dispositivo recibe, desde el primer dispositivo, un primer mensaje que solicita una respuesta para el cálculo de la distancia basada en tiempo. En respuesta al primer mensaje, éste envía un segundo mensaje. A continuación, el segundo dispositivo calcula datos de autentificación, vinculados criptográficamente a uno de: al menos el primer mensaje, al menos el segundo mensaje, y al menos el primer mensaje y el segundo mensaje, y envía, al primer dispositivo, un tercer mensaje que contiene los datos de autentificación.

En un tercer aspecto, la invención está dirigida a un primer dispositivo adaptado para el cálculo seguro de la distancia basada en tiempo hasta un segundo dispositivo de una red. El primer dispositivo comprende una unidad de entrada/salida adaptada para enviar un primer mensaje al segundo dispositivo y recibir desde el segundo dispositivo un segundo mensaje enviado en respuesta al primer mensaje. El primer dispositivo comprende además un procesador adaptado para calcular la distancia en tiempo basándose en el momento de la transmisión del primer mensaje y el momento de la recepción del segundo mensaje. La unidad de entrada/salida está adaptada además para recibir un mensaje adicional que contenga datos de autentificación criptográficamente vinculados a uno de: al menos el primer mensaje, al menos el segundo mensaje, y al menos el primer mensaje y el segundo mensaje, y el procesador está adaptado además para verificar los datos de autentificación.

En una realización preferida, la unidad de entrada/salida está adaptada además para enviar un mensaje a fin de solicitar el mensaje adicional que contenga datos de autentificación sólo si la distancia basada en tiempo que se ha calculado se sitúa por debajo de un límite predeterminado.

Puede resultar ventajoso que el procesador esté adaptado además para calcular datos de autentificación del primer dispositivo, y que la unidad de entrada/salida esté adaptada además para incluir los datos de autentificación del primer dispositivo en el mensaje enviado al segundo dispositivo a fin de solicitar el mensaje adicional que contenga datos de autentificación del segundo dispositivo.

En una realización preferida adicional, el procesador está adaptado además para generar un primer elemento criptográfico y para verificar los datos de autentificación, vinculados criptográficamente por estar basados en el primer elemento criptográfico y un segundo elemento criptográfico, y la unidad de entrada/salida está adaptada además para incluir el primer elemento criptográfico en el primer mensaje, y para recibir el segundo elemento criptográfico en el segundo mensaje.

En un cuarto aspecto, la invención está dirigida a un segundo dispositivo de una red adaptado para responder a un protocolo, lanzado en un primer dispositivo, para el cálculo seguro de la distancia basada en tiempo hasta el segundo dispositivo. El segundo dispositivo comprende un procesador adaptado para calcular datos de autentificación, criptográficamente vinculados a uno de: al menos un primer mensaje, al menos el segundo mensaje, y al menos el primer mensaje y el segundo mensaje, y una unidad de entrada/salida adaptada para recibir desde el primer dispositivo el primer mensaje, enviar el segundo mensaje al primer dispositivo, en respuesta al primer mensaje, y enviar al primer dispositivo un tercer mensaje que contenga los datos de autentificación.

En una realización preferida, la unidad de entrada/salida está adaptada además para recibir un mensaje desde el primer dispositivo, en donde el mensaje contiene datos de autentificación calculados por el primer dispositivo. El procesador está adaptado además para verificar los datos de autentificación recibidos y calcular sus propios datos de autentificación sólo si los datos de autentificación recibidos han sido verificados satisfactoriamente.

Breve descripción de los dibujos

A continuación se describirán características preferidas de la presente invención, a modo de ejemplo, haciendo referencia a los dibujos adjuntos, en los cuales:

la Figura 1, discutida anteriormente en esta memoria, es una ilustración de una red y del concepto de proximidad local;

la Figura 2 ilustra un diagrama de flujo de una realización preferida del método de acuerdo con la invención;

la Figura 3 ilustra un diagrama de flujo de una realización alternativa del método de acuerdo con la invención; y

la Figura 4 ilustra un diagrama de flujo de una realización alternativa adicional del método de acuerdo con la invención.

Descripción detallada de realizaciones preferidas

La Figura 2 ilustra un diagrama de flujo de una realización preferida del método de acuerdo con la invención. El método consta de tres fases generales:

1. Una fase de cálculo previo en la cual se inicia el método y se realizan los primeros cálculos criptográficos.
2. Una fase de medición basada en tiempo de la distancia entre dos dispositivos, intercambiando resultados de la fase de cálculo previo en un comando de tipo "ping".
3. Una fase de verificación criptográfica, en la cual se calculan y se intercambian, en caso necesario, datos adicionales de autentificación, vinculados criptográficamente a los resultados intercambiados en los mensajes "ping" y se verifica la autentificación. En otras palabras, se comprueba que el remitente de la respuesta al comando "ping" es el remitente de los datos de autentificación, y se verifica adicionalmente la identidad del dispositivo que contesta.

En la descripción que sigue, se supone que el dispositivo A 212 requiere una medición segura del RTT hasta el dispositivo B 216. En otras palabras, el dispositivo A pone en marcha el protocolo y el dispositivo B le responde.

En una realización, el dispositivo A y el dispositivo B tienen cada uno un certificado X.509, certificado por una entidad de confianza común, y una clave privada RSA asociada. Antes del inicio del método, cada dispositivo tiene conocimiento del certificado y de la clave pública del otro dispositivo. Sin embargo, de aquí en adelante se describe una realización preferida.

El dispositivo A 212 comprende un procesador 213 para los cálculos y una unidad 214 de entrada/salida para la comunicación. El dispositivo B 216 también comprende un procesador 217 para los cálculos y una unidad 218 de entrada/salida para la comunicación.

La fase de cálculo previo comienza cuando el dispositivo A 212 envía un nuevo mensaje 222 de medición al dispositivo B 216. El mensaje 222 indica que el dispositivo A desea realizar una nueva medición del RTT. Una vez recibido este mensaje 222, el dispositivo B calcula 224 un elemento criptográfico, preferiblemente un número aleatorio (Random_B) que es nuevo para cada cálculo. El dispositivo A calcula 226 un elemento criptográfico independiente, preferiblemente un número aleatorio (Random_A) que es nuevo para cada cálculo, y espera 227 un

tiempo predeterminado para dar al dispositivo B el tiempo necesario para el cálculo. En una realización preferida, el dispositivo A conoce el tiempo máximo necesario para el cálculo de B, pero también es posible utilizar un valor de tiempo general predeterminado, por ejemplo, en caso de que el tiempo máximo sea desconocido para el dispositivo A.

La fase de medición comienza cuando el dispositivo A envía un mensaje 242 que contiene su elemento criptográfico al dispositivo B, y también anota 244 el momento de la transmisión. Una vez que ha recibido el mensaje 242 del dispositivo A, el dispositivo B responde con un mensaje 246 que contiene su elemento criptográfico. El dispositivo A recibe el mensaje 246 y anota 248 el momento de la recepción. Después, el dispositivo A calcula, basándose en el momento de la transmisión y el momento de la recepción, el RTT 250 hasta el dispositivo B. Hay que señalar, sin embargo, que en este punto el dispositivo A no tiene manera de saber si el mensaje 246, supuestamente procedente del dispositivo B, proviene efectivamente de ese dispositivo.

En una realización preferida, al calcular 250 el RTT, el dispositivo A también verifica si el RTT se sitúa por debajo del límite dado, es decir, si el dispositivo B se encuentra en su proximidad local. Si no es así, es decir, si el dispositivo B no está cerca, entonces no merece la pena verificar que el dispositivo B fuera el remitente del mensaje 246, y o bien se detiene el método o bien se comienza de nuevo - se ha mencionado antes que es habitual enviar una serie de hasta 50 ó 100 mensajes ping para calcular el RTT hasta un dispositivo y parar en cuanto un RTT se sitúa por debajo de un valor determinado. También es posible que el dispositivo A reinicie el método sin haber recibido una respuesta desde el dispositivo B, si se ha excedido el límite. No obstante, si el dispositivo A considera que el dispositivo B está en su proximidad local, entonces solicita datos de autentificación mediante el envío de un mensaje 252 que indica que el RTT es correcto, pero que son necesarios datos de autentificación. En una realización alternativa, no se envía ningún mensaje 252 "el RTT es correcto" y el resto del método se realiza de forma automática.

Así pues, la fase de verificación criptográfica comienza cuando el dispositivo B, ya sea automáticamente o en respuesta al mensaje 252 "el RTT es correcto", calcula 262 los datos de autentificación requeridos - criptográficamente vinculados a los mensajes "ping" 242, 246, basados en este caso en elementos criptográficos de ambos dispositivos A y B - para confirmar que era el remitente del mensaje 246 que fue enviado al dispositivo A. Los datos de autentificación consisten preferiblemente en una concatenación de los dos elementos criptográficos, firmados con la clave privada del dispositivo B. La forma preferida de cálculo de la prueba utiliza la criptografía de clave pública, pero también son posibles otras formas tales como, por ejemplo, utilizar una criptografía de clave secreta. Después, el dispositivo B envía al dispositivo A un mensaje 264, que contiene los datos de autentificación. En una realización preferida, el mensaje 264 de datos de autentificación contiene además el certificado del dispositivo B.

Una vez recibido este mensaje 264, el dispositivo A verifica 266 los datos de autentificación. Una verificación satisfactoria significa que el mensaje 246 del dispositivo B procede realmente del dispositivo B en respuesta al mensaje 242 enviado al mismo por el dispositivo A. La verificación se lleva preferiblemente a cabo verificando que el certificado del dispositivo B es un certificado conforme, es decir, verificando la cadena de confianza X.509; desencriptando la firma; y comprobando que el resultado concuerda con la concatenación de los elementos criptográficos, Random_A y Random_B. Cuando la verificación es satisfactoria, el dispositivo A valida el cálculo de la distancia basada en tiempo hasta el dispositivo B. El dispositivo A está ahora seguro de que ha enviado el "ping" al dispositivo B y, de que, si el RTT es correcto, el dispositivo B se encuentra en su proximidad local.

Considérese la Figura 1, donde el dispositivo B no está próximo al dispositivo A, y donde un atacante C (situado en LAN L1) es capaz de bloquear todos los "pings" hacia dispositivos externos a la red LAN L1 y responder en su nombre. Cuando el dispositivo A utiliza la presente invención, el dispositivo C no tiene manera de calcular los datos de autentificación de B, ya que no posee la clave privada de B. El dispositivo C podría obtener previamente datos de autentificación del dispositivo B lanzando el protocolo y haciéndose pasar por el dispositivo A. Pero en tal caso el dispositivo C tendría que predecir el elemento criptográfico generado por el dispositivo A, lo que no es posible. Por tanto, los datos de autentificación obtenidos del dispositivo B no serían válidos si el dispositivo C los envía al dispositivo A, quien entonces considerará que el dispositivo B no se encuentra en su proximidad local. El método de acuerdo con la invención es por lo tanto más seguro que los métodos de la técnica anterior.

La Figura 3 ilustra un diagrama de flujo de una realización alternativa del método de acuerdo con la invención. La realización ilustrada en la Figura 3 es similar a la realización preferida, y los mismos números de referencia designarán los mismos pasos.

Antes de que dé comienzo el método, el dispositivo B ha calculado y almacena al menos un elemento criptográfico, preferentemente un número aleatorio.

El dispositivo A inicia el método calculando 226 un elemento criptográfico, que es enviado al dispositivo B en el mensaje 242. El dispositivo A también anota 244 el momento de la transmisión. Tras haber recibido el mensaje 242, el dispositivo B usa 345 su elemento criptográfico almacenado y lo envía en un mensaje 246 al dispositivo A. El dispositivo A anota el momento de la recepción 248 y calcula 250 el tiempo de ida y vuelta (RTT).

Si el RTT se sitúa por debajo de un cierto límite, el dispositivo A envía un mensaje 252 al dispositivo B para hacerle saber que el RTT es aceptable y que necesita datos de autentificación. Entonces, el dispositivo B calcula los datos de autentificación tal como se ha descrito anteriormente en la presente memoria y envía los datos de autentificación al dispositivo A en el mensaje 264. A continuación, el dispositivo A verifica 266 los datos de autentificación, y por tanto el origen del mensaje "ping" 246 recibido y la identidad del dispositivo B.

Después de haber enviado el mensaje 264 que contiene los datos de autentificación, si el dispositivo B sólo tuviera un elemento criptográfico almacenado, calcula 368 un nuevo elemento criptográfico.

La Figura 4 ilustra un diagrama de flujo de una realización alternativa adicional del método de acuerdo con la invención. La realización ilustrada en la Figura 4 es similar a la realización preferida, y los mismos números de referencia designarán mismos pasos.

El dispositivo A inicia el método enviando al dispositivo B un nuevo mensaje 422 de medición, que contiene preferiblemente el certificado del dispositivo A. El dispositivo A y el dispositivo B calculan 226, 228 cada uno un elemento criptográfico, y el dispositivo A espera 227 para dar tiempo al dispositivo B a terminar el cálculo.

El dispositivo A envía un mensaje 242 que contiene su elemento criptográfico al dispositivo B y anota 244 el momento de la transmisión. Tras la recepción del mensaje 242, el dispositivo B utiliza su elemento criptográfico calculado y lo envía en un mensaje 246 al dispositivo A. El dispositivo A anota el momento de la recepción 248 y calcula 250 el tiempo de ida y vuelta (RTT).

Si el RTT se sitúa por debajo de un umbral determinado, el dispositivo A calcula 451 datos de autentificación (datos de aut._A) para probar su identidad y envía al dispositivo B un mensaje 452 que contiene los datos de autentificación. El mensaje 452 también hace saber al dispositivo B que el RTT es aceptable y que el dispositivo A solicita datos de autentificación (datos de aut._B) del dispositivo B. Entonces, tras recibir el mensaje 452, el dispositivo B verifica 454 los datos de autentificación recibidos del dispositivo A, lo que significa que el mensaje 242 del dispositivo A ha procedido verdaderamente del dispositivo A. Si el dispositivo B está seguro de que ha sido llamado (mediante un "ping") por el dispositivo A, calcula 262 los datos de autentificación requeridos tal como se ha descrito anteriormente en la presente memoria y envía los datos de autentificación al dispositivo A en el mensaje 264. A continuación, el dispositivo A verifica 266 los datos de autentificación, y por tanto el origen de la respuesta ping 246 y la identidad del dispositivo B.

Esta invención puede ser utilizada, por ejemplo, en la difusión de vídeo en una red para asegurarse de que únicamente reciban el vídeo dispositivos que se encuentren en la proximidad local de una fuente.

Así pues, se puede apreciar que la presente invención mejora la técnica anterior al proporcionar un método para calcular distancia basada en tiempo que es seguro e independiente de los recursos de los dispositivos.

Se comprenderá que la presente invención ha sido descrita meramente a modo de ejemplo, y que se pueden realizar modificaciones de detalle sin salir del alcance de la invención.

Cada una de las características divulgadas en la memoria descriptiva y (en su caso) en las reivindicaciones y dibujos puede ser proporcionada de manera independiente o en cualquier combinación adecuada. Las características pueden ser, en su caso, ser implementadas en el equipo físico (en inglés "hardware"), en los programas informáticos (en inglés "software"), o en una combinación de ambos. En su caso, las conexiones pueden ser implementadas bien como conexiones inalámbricas o bien por cable, sin que sean necesarias conexiones directas o dedicadas.

Los números de referencia que aparecen en las reivindicaciones lo son sólo a modo de ilustración y no tendrán ningún efecto limitante en el alcance de las reivindicaciones.

REIVINDICACIONES

1. Un método para calcular de manera segura en un primer dispositivo (212) distancia basada en tiempo a un segundo dispositivo (216) de una red (100), que comprende los pasos de:

enviar un primer mensaje (242) al segundo dispositivo;

recibir del segundo dispositivo un segundo mensaje (246) enviado en respuesta al primer mensaje:

calcular (244; 248; 250) la distancia en tiempo basándose en el momento de la transmisión del primer mensaje y el momento de la recepción del segundo mensaje;

caracterizado por los pasos posteriores de:

recibir un mensaje posterior (264) que comprende datos de autentificación vinculados criptográficamente a uno de: al menos el primer mensaje (242), al menos el segundo mensaje (246), y al menos el primer mensaje (242) y el segundo mensaje (246); y

verificar (266) los datos de autentificación.

2. El método según la reivindicación 1, que comprende además el paso de enviar un mensaje (252) para solicitar el mensaje adicional (264) que contenga datos de autentificación si la distancia basada en tiempo que se ha calculado se sitúa por debajo de un límite predeterminado.

3. El método según la reivindicación 1 ó 2, en donde el primer mensaje (242) comprende un primer elemento criptográfico y el segundo mensaje (246) comprende un segundo elemento criptográfico, y los datos de autentificación se calculan basándose en el primer y el segundo elementos criptográficos.

4. El método según la reivindicación 3, en donde los elementos criptográficos son números aleatorios y los datos de autentificación son el resultado de una función calculada utilizando los números aleatorios, siendo la función dependiente de un secreto.

5. El método según la reivindicación 3, que comprende además los pasos de:

enviar un cuarto mensaje (222) al segundo dispositivo para hacerle saber que se ha dado comienzo al método;

generar (226) el primer elemento criptográfico.

6. El método según la reivindicación 5, que comprende además el paso de esperar (228) un plazo determinado, con el fin de dar tiempo al segundo dispositivo para que acabe la generación del segundo elemento criptográfico.

7. El método según la reivindicación 2, en donde los datos de autentificación son segundos datos de autentificación, el método comprende además el paso de calcular (451) primeros datos de autentificación, y en donde el mensaje (252) enviado al segundo dispositivo para solicitar el mensaje adicional (264) que contenga segundos datos de autentificación, contiene los primeros datos de autentificación.

8. El método según la reivindicación 1, que comprende además el paso de validar el cálculo de la distancia basada en tiempo al segundo dispositivo una vez que se han verificado satisfactoriamente los datos de autentificación.

9. Un método para responder en un segundo dispositivo (216) de una red (100) a un protocolo para el cálculo seguro en un primer dispositivo (212) de distancia basada en tiempo hasta el segundo dispositivo, que comprende los pasos de:

recibir, desde el primer dispositivo, un primer mensaje (242) cuyo momento de transmisión es utilizado por el primer dispositivo para el cálculo de la distancia basada en tiempo;

en respuesta al primer mensaje, enviar al primer dispositivo un segundo mensaje (246), cuyo momento de recepción es utilizado por el primer dispositivo para el cálculo de la distancia basada en tiempo;

calcular (262) datos de autentificación, vinculados criptográficamente a uno de: al menos el primer mensaje (242), al menos al segundo mensaje (246), y al menos el primer mensaje (242) y el segundo mensaje (246); y

enviar, al primer dispositivo, un mensaje posterior (264) que contiene los datos de autentificación.

10. Un primer dispositivo (212) adaptado para el cálculo seguro de la distancia basada en tiempo a un segundo dispositivo (216) de una red (100), en donde el primer dispositivo comprende:

una unidad (214) de entrada/salida adaptada para:

enviar un primer mensaje (242) al segundo dispositivo; y

recibir desde el segundo dispositivo un segundo mensaje (246) enviado en respuesta al primer mensaje (242); y

un procesador (213) adaptado para:

calcular la distancia en tiempo basándose en el momento de la transmisión del primer mensaje y el momento de la recepción del segundo mensaje;

caracterizado porque:

la unidad de entrada/salida está adaptada además para recibir un mensaje posterior (264) que contenga datos de autentificación, estando los datos de autentificación criptográficamente vinculados a uno de: al menos el primer mensaje (242), al menos el segundo mensaje (246), y al menos el primer mensaje (242) y el segundo mensaje (246); y

el procesador está adaptado además para verificar los datos de autentificación.

11. El dispositivo según la reivindicación 10, en donde la unidad (214) de entrada/salida está adaptada además para enviar un mensaje (252) a fin de solicitar datos de autentificación sólo si la distancia basada en tiempo que se ha calculado se sitúa por debajo de un límite predeterminado.

12. El dispositivo según la reivindicación 10 u 11, en donde el procesador (213) está adaptado además para calcular primeros datos de autentificación, y en donde la unidad (214) de entrada/salida está adaptada además para incluir los primeros datos de autentificación en el mensaje (252) enviado al segundo dispositivo para solicitar datos de autentificación, que son segundos datos de autentificación.

13. El dispositivo según la reivindicación 10, en donde:

el procesador está adaptado además para:

generar un primer elemento criptográfico; y

verificar los datos de autentificación recibidos, en donde los datos de autentificación están vinculados criptográficamente por estar basados en el primer elemento criptográfico y un segundo elemento criptográfico; y

la unidad de entrada/salida está adaptada además para:

incluir el primer elemento criptográfico en el primer mensaje (242); y

recibir el segundo elemento criptográfico en el segundo mensaje (246).

14. Un segundo dispositivo (216) de una red (100) adaptado para responder a un protocolo, lanzado en un primer dispositivo (212), para el cálculo seguro de distancia basada en tiempo hasta el segundo dispositivo, en donde el segundo dispositivo comprende:

un procesador (217) adaptado para:

calcular datos de autentificación, criptográficamente vinculados a uno de: al menos un primer mensaje (242), al menos al segundo mensaje (246), y al menos el primer mensaje (242) y el segundo mensaje (246); y

una unidad (218) de entrada/salida adaptada para:

recibir, desde el primer dispositivo, el primer mensaje (242), cuyo momento de transmisión es utilizado por el primer dispositivo para el cálculo de la distancia basada en tiempo;

en respuesta al mensaje, enviar al primer dispositivo el segundo mensaje (246), cuyo momento de recepción es utilizado por el primer dispositivo para el cálculo de la distancia basada en tiempo; y

enviar, al primer dispositivo, un mensaje posterior (264) que contenga los datos de autentificación.

15. El dispositivo según la reivindicación 14, en donde la unidad (218) de entrada/salida está adaptada además para recibir un mensaje (452) desde el primer dispositivo, en donde el mensaje contiene datos de autentificación calculados por el primer dispositivo, y el procesador (217) está adaptado además para verificar los datos de autentificación recibidos y calcular sus propios datos de autentificación sólo si los datos de autentificación recibidos han sido verificados satisfactoriamente.

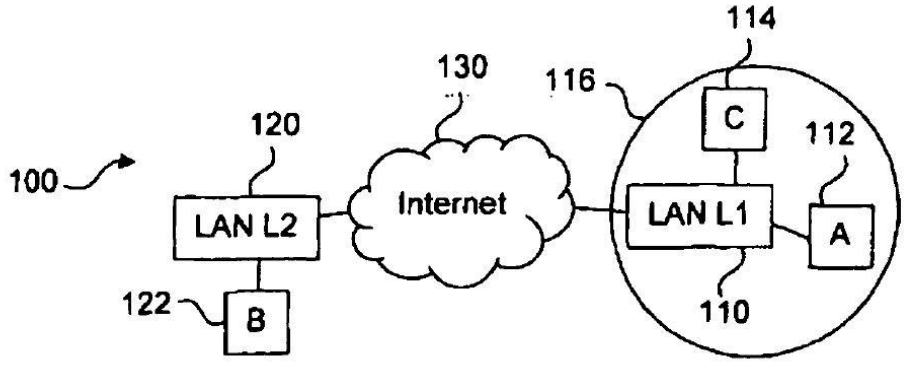

Figura 1 (técnica anterior)

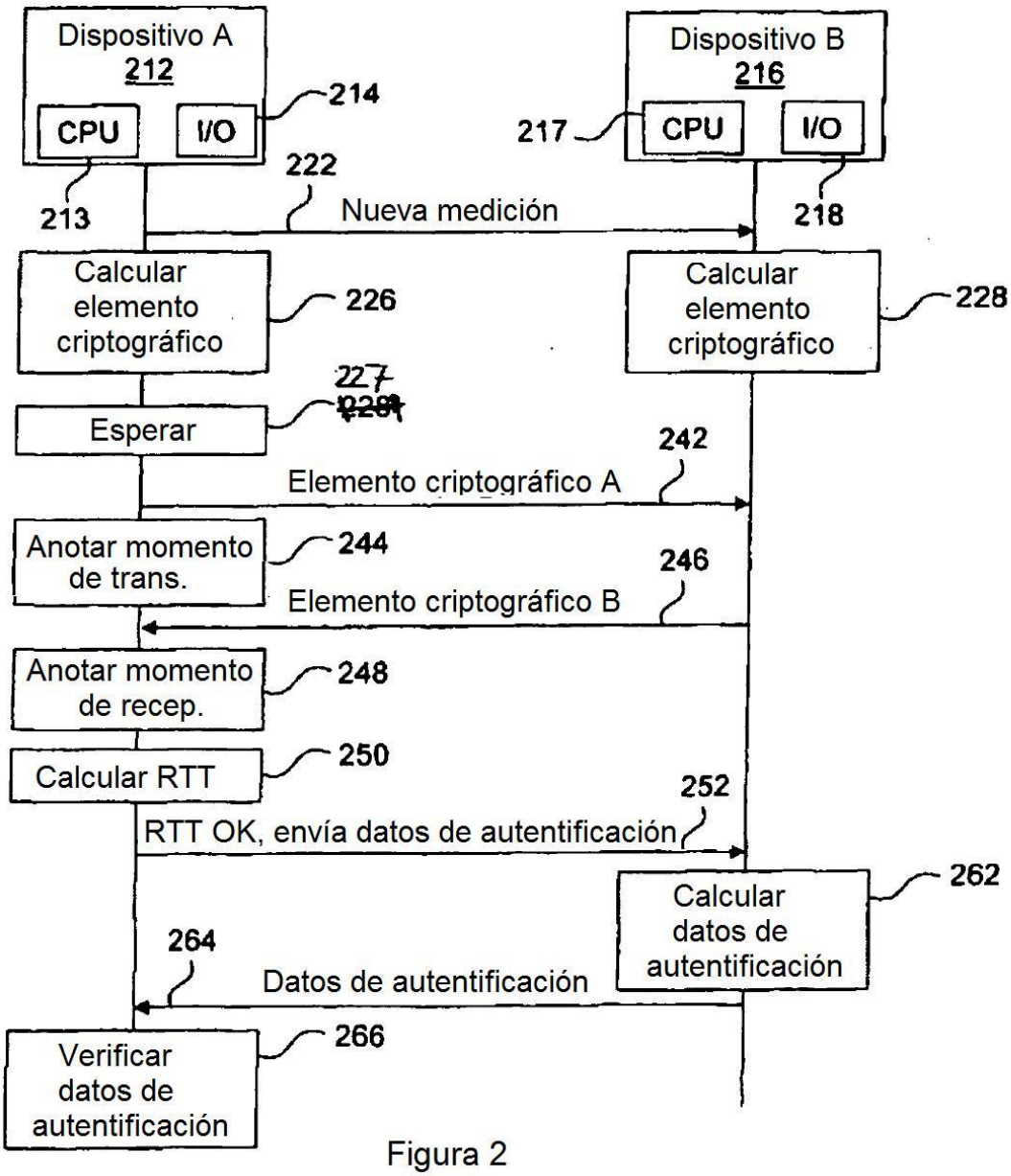

Figura 2

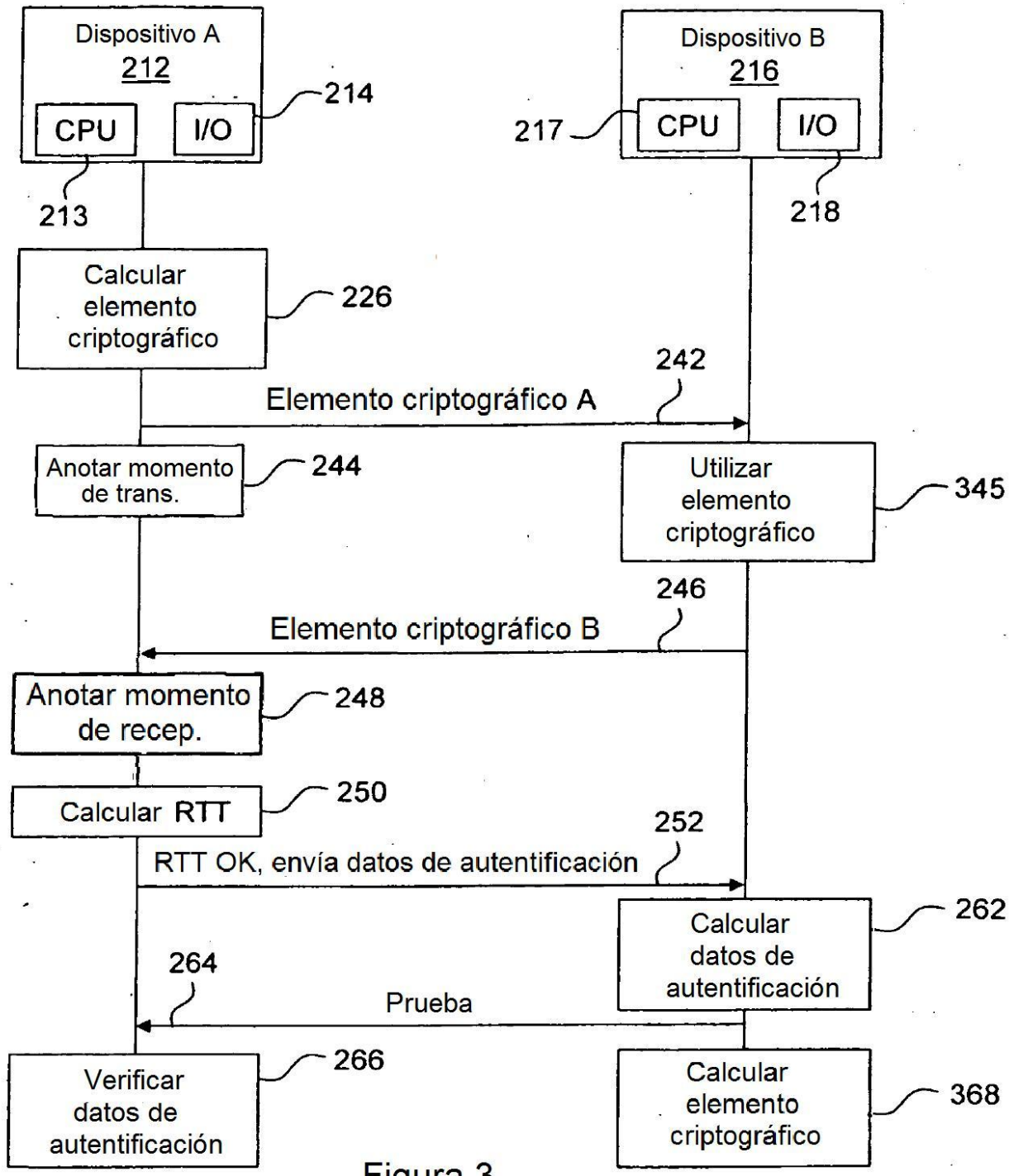
Dispositivo A
212
CPU
I/O
214
213
Dispositivo B
216
217
CPU
I/O
218
Calcular elemento criptográfico
226
242
Elemento criptográfico A
Anotar momento de trans.
244
Utilizar elemento criptográfico
345
246
Elemento criptográfico B
Anotar momento de recep.
248
Calcular RTT
250
252
RTT OK, envía datos de autentificación
Calcular datos de autentificación
262
264
Prueba
Verificar datos de autentificación
266
Calcular elemento criptográfico
368

Figura 3

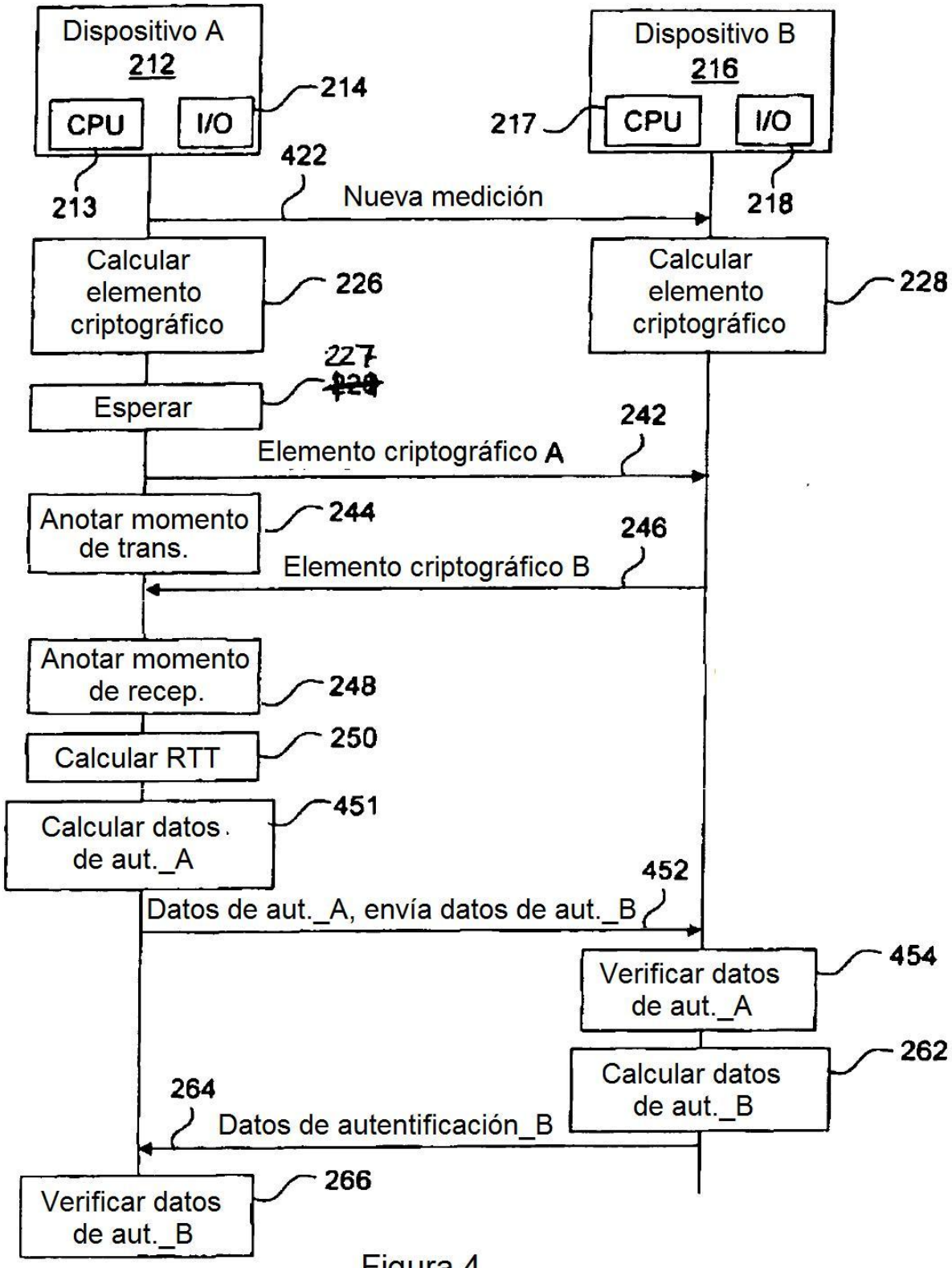
Dispositivo A
212
CPU
I/O
214
213
Dispositivo B
216
217
CPU
I/O
218
422
Nueva medición
Calcular elemento criptográfico
226
Calcular elemento criptográfico
228
227
Esperar
242
Elemento criptográfico A
Anotar momento de trans.
244
246
Elemento criptográfico B
Anotar momento de recep.
248
Calcular RTT
250
Calcular datos de aut._A
451
452
Datos de aut._A, envía datos de aut._B
Verificar datos de aut._A
454
Calcular datos de aut._B
262
264
Datos de autentificación_B
Verificar datos de aut._B
266

Figura 4