(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 656 058**

(51) Int. CI.:

***H04L 29/06*** (2006.01)
***H04L 12/741*** (2013.01)
***H04L 29/08*** (2006.01)
*H04L 12/749* (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.12.2013 E 13198495 (7)**

(97) Fecha y número de publicación de la concesión europea: **18.10.2017 EP 2887604**

(54) Título: **Procedimiento y red de telecomunicación para aumentar la seguridad en el intercambio de datos en modo de paquetes**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**22.02.2018**

(73) Titular/es:

**DEUTSCHE TELEKOM AG (100.0%)**
**Friedrich-Ebert-Allee 140**
**53113 Bonn, DE**

(72) Inventor/es:

**VAN DEN BERGE, FRIDTJOF y**
**KUMAR, AMIT**

(74) Agente/Representante:

**AZNÁREZ URBIETA, Pablo**

## DESCRIPCIÓN

**Procedimiento y red de telecomunicación para aumentar la seguridad en el intercambio de datos en modo de paquetes**

*Estado actual de la técnica*

La invención se refiere a un procedimiento para aumentar la seguridad en el intercambio de datos en modo de paquetes según un Protocolo de Internet entre nodos de red de una red de telecomunicaciones.

La invención se refiere además a una red de telecomunicaciones para aumentar la seguridad en el intercambio de datos en modo de paquetes según un Protocolo de Internet entre nodos de red de la red de telecomunicaciones.

Una adaptación de los protocolos SS#7 a los protocolos IP abrirá, con la ampliación de las redes de Internet, nuevos escenarios de fraude y encubrirá éstos también con mayor facilidad y seguridad.

Las aplicaciones y los servicios disponibles utilizando Protocolos de Internet son cada vez más extensos y variados. Por ejemplo, actualmente las compañías telefónicas adaptan cada vez más servicios, que hasta ahora se desarrollaban en el campo de la telefonía móvil todavía por señalización SS7, a la utilización del Protocolo de Internet (IP). La voz también desaparece lentamente de los canales de voz (enrutamiento) y se empaqueta en paquetes de datos del Protocolo de Internet, enviándose con una alta priorización en Internet. Así, también pueden multiplicarse ostensiblemente en particular las posibilidades de fraude y lo harán, dado que la utilización de la señalización SS7 va acompañada de un mayor nivel de seguridad, por ejemplo con vistas a la rastreabilidad. Utilizando el Protocolo de Internet se hacen posibles en las redes de telecomunicaciones nuevos escenarios de fraude, por ejemplo el encubrimiento de direcciones de Protocolo de Internet (direcciones IP) mediante, por ejemplo, servidores *proxy*, la transcripción de direccionamientos de correo electrónico a direccionamientos de correo electrónico ficticios y simulados o también la autoconfiguración para crear direcciones IP.

Entre la versión 4 del Protocolo de Internet (IPv4) y la versión 6 del Protocolo de Internet (IPv6) existen diferencias, pero la seguridad del usuario contra el fraude no ha mejorado mucho.

Por ejemplo, utilizando IPv4 resulta fácil introducir direcciones IP de fuente ficticias (esto es de Protocolo de Internet de origen) en los datos del encabezamiento (es decir en el denominado *header*). Si además se enruta el mensaje a través de muchos nodos intermedios o servidores *proxy* hasta el destino, por ejemplo para la policía resulta casi imposible descubrir la procedencia del paquete de datos de Protocolo de Internet. Incluso utilizando IPv6 existe la posibilidad de dificultar o incluso excluir cualquier rastreo (*tracking*), por ejemplo mediante extensiones de privacidad (*privacy extensions*) para direcciones IP sin nacionalidad (RFC 4941).

El, así llamado, identificador de interfaz (*interface identifier*) o la dirección MAC al final de un paquete de datos de Protocolo de Internet en la información del encabezamiento IPv6 puede modificarse, según RFC 4941, en los llamados identificadores de alcance global (*global scope identifiers*), que para ello no han de ser únicos. En otras palabras, podrían existir al mismo tiempo varios mensajes idénticos con una dirección MAC idéntica. Además, con las llamadas direcciones de alcance global o direcciones de unidifusión global existe la posibilidad de dificultar de nuevo un rastreo de la dirección IPv6, visible en los datagramas. La publicación MURALI BHASKARAN V et al, “Tracebacking the Spoofed IP Packets in Multi ISP Domains with Secured Communication”, ICSCN ’07, IEEE, 22- 24 de febrero de 2007, páginas 579-584, da a conocer un sistema para el rastreo de un paquete IP que identifica el origen de una serie de paquetes IP cuando la dirección de fuente de estos paquetes es ficticia. La publicación FERGUSON P et al, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, RFC 2827, IETF, mayo de 2000, da a conocer un procedimiento para filtrar el tráfico de entrada con el fin de impedir la propagación de ataques DoS (de denegación de servicio) que utilizan direcciones IP de fuentes ficticias. El documento US 2013/152189 da a conocer un procedimiento para detectar e impedir paquetes de datos con direcciones de fuente ficticias.

Por tanto, existe la necesidad de mejorar, en lo que se refiere a su seguridad, los protocolos conocidos en la transmisión de paquetes de datos de Protocolo de Internet.

*Descripción de la invención*

La invención tiene el objetivo de proporcionar un procedimiento y una red de telecomunicaciones para aumentar la seguridad en el intercambio de datos en modo de paquetes según un Protocolo de Internet entre nodos de red de una red de telecomunicaciones, consiguiendo una mejora del nivel de seguridad de la

comunicación de datos, especialmente en lo referente a la rastreabilidad o la trazabilidad de mensajes. Este objetivo se logra según la invención mediante un procedimiento para aumentar la seguridad en el intercambio de datos en modo de paquetes según un Protocolo de Internet entre nodos de red de una red de telecomunicaciones, cooperando para la transmisión de un paquete de datos de Protocolo de Internet al menos un primer nodo de red de un primer proveedor de servicios de telecomunicación y un segundo nodo de red, siendo el segundo nodo de red un nodo vecino del primer nodo de red, teniendo asignada el primer nodo de red una información de identificación, teniendo el segundo nodo de red acceso a la información de identificación asignada al primer nodo de red, comprendiendo el procedimiento los siguientes pasos:

- en un primer paso de procedimiento, el primer nodo de red añade al paquete de datos de Protocolo de Internet la información de identificación del primer nodo de red,
- en un segundo paso de procedimiento se transmite el paquete de datos de Protocolo de Internet al segundo nodo de red,
- en un tercer paso de procedimiento, el segundo nodo de red lleva a cabo una comprobación del paquete de datos de Protocolo de Internet, comprendiendo la comprobación por parte del segundo nodo de red la comprobar la información de identificación, siendo el paquete de datos de Protocolo de Internet rechazado por el segundo nodo de red cuando la información de identificación del paquete de datos de Protocolo de Internet no coincide con la información de identificación asignada al primer nodo de red con el que el segundo nodo de red tiene un enlace.

Así, según la presente invención, ventajosamente es posible perseguir mejor, más rápidamente y más inequívocamente un fraude.

Según la invención, es particularmente ventajoso que sea posible lograr estas ventajas sin necesidad de cambiar un RFC existente o las características del Protocolo de Internet (es decir *features*). En particular se haría o sería necesario por ejemplo un campo de información decimal de 6 posiciones (es decir seis posiciones decimales codificadas en binario (es decir codificadas con, en cada caso, cuatro posiciones binarias) bajo IPv4 y/o un campo de información hexadecimal de 5 posiciones bajo IPv6 como campo obligatorio para la pasarela expedidora del proveedor en el encabezamiento IP con un indicador (*flag*) (valor binario de una posición).

En caso de utilizarse IPv4, la información de identificación (es decir el campo de información de 6 posiciones arriba mencionado) contiene por ejemplo un valor decimal de seis posiciones, con lo que como máximo es posible representar un número de 0 a 999.999. Análogamente, en la notación hexadecimal f423f (es decir 1111.01000010.00111111 en binario) podrían hacerse reconocibles en Internet, es decir identificables, casi 1 millón de nodos de red de todo el mundo mediante una información de identificación de este tipo como pasarela de acceso para un mensaje enviado.

En caso de utilizarse IPv6, la información de identificación (es decir el campo de información hexadecimal de 5 posiciones arriba mencionado) contiene el valor hexadecimal de cinco posiciones, con lo que como máximo puede representarse un valor hexadecimal de fffff, es decir 1024·1024 = 1.048.576 (en notación decimal) posibilidades diferentes. Correspondientemente, según la invención, pueden hacerse reconocibles en Internet, es decir identificables, 1.048.576 en decimal (es decir 00000000.00001111.11111111.11111111 en binario), o sea más de 1 millón, de nodos de red de todo el mundo mediante una información de identificación de este tipo como pasarela de acceso para un mensaje enviado.

En caso de una la llamada pila doble (*dual-stack*), es decir IPv4 paralelo a IPv6 – transmisiones IP para el tiempo de transición para la migración pendiente de IPv4 a IPv6–, se escriben ambas características de información de identificación en el encabezamiento IP respectivo. Correspondientemente, en tal caso el campo de información decimal de 6 posiciones del encabezamiento IPv4 es igual al campo de información hexadecimal de 5 posiciones del encabezamiento IPv6 desde el punto de vista del valor binario.

Según la invención se prefiere especialmente que sólo los nodos adicionales reciban un nuevo número secuencial de un intervalo numérico asignado a un proveedor de Internet. Los nodos de red ya existentes que se sustituyan entregan su identificación a las nuevas máquinas, es decir los nuevos nodos de red. Correspondientemente, se conservan los números de los intervalos numéricos cuando se cambian nodos en una red.

Según la invención, está previsto que, para la transmisión del paquete de datos de Protocolo de Internet, coopere un tercer nodo de red además del primer y el segundo nodos de red, y que el paquete de datos de Protocolo de Internet incluya una información de salto que se modifique en cada transmisión de un nodo de red previo a otro nodo de red, reconociendo el tercer nodo de red en virtud de la

información de salto del paquete de datos de Protocolo de Internet que la comprobación de la información de identificación en el segundo nodo de red ha sido satisfactoria y transmitiendo el tercer nodo de red el paquete de datos de Protocolo de Internet.

De este modo, según la invención se consigue mantener muy pequeño el esfuerzo de comprobación en el tercer nodo de red y, por ello, ésta requiere pocos recursos adicionales.

Según la invención está previsto además preferiblemente que la información de identificación comprenda, en caso de utilizar IPv4 y en caso de utilizar IPv6, al menos 24 posiciones binarias o 3 bytes.

Además, según la invención está previsto preferiblemente

- que la información de identificación, en caso de utilizar IPv4, comprenda al menos seis posiciones decimales codificadas en binario, es decir en total 24 posiciones binarias (es decir 6 posiciones decimales codificadas en binario, codificada cada una con 4 bits), o
- que la información de identificación, en caso de utilizar IPv6, comprenda al menos cinco posiciones hexadecimales (es decir en total 20 posiciones binarias).

Según la invención, de manera especialmente preferente, está previsto que el primer nodo de red añada al paquete de datos de Protocolo de Internet una información de comprobación, además de la información de identificación del primer nodo de red, indicando la información de comprobación que la información de identificación asignada al primer nodo de red se ha añadido al paquete de datos de Protocolo de Internet.

Así, según la invención es ventajosamente posible que también por medio de la información de comprobación pueda determinarse que la información de identificación ha sido introducida en el paquete de datos de Protocolo de Internet. La información de comprobación arriba mencionada está prevista por ejemplo como un llamado indicador (*flag*), es decir un valor binario de una posición (que puede adoptar bien el valor “0”, bien el valor “1”). En un encabezamiento IP así adaptado, el valor “0” significaría que el mensaje (es decir el paquete de datos de Protocolo de Internet) no está provisto de la información de identificación del nodo de red (es decir, en IPv4, de la habitual identificación decimal de 6 posiciones o, en IPv6, de

la identificación hexadecimal de 5 posiciones o la información de identificación del enrutador (*router*) o servidor inicial) que se utiliza en Internet como pasarela para el mensaje (o el paquete de datos de Protocolo de Internet) y, por tanto, no debe ser enviado ni transmitido por un enrutador vecino (o segundo nodo de red). Un valor "1" se coloca como indicador cuando está incluida la información de identificación, es decir se escribe en el campo de información (es decir en la información de identificación) la información hexadecimal de 5 posiciones (en IPv6) o la información decimal de 6 posiciones (en IPv4) como identificación del enrutador inicial (o del primer nodo de red) que sirve en Internet de pasarela para el mensaje (o el paquete de datos de Protocolo de Internet).

Según la invención, está previsto preferiblemente que la información de comprobación del indicador sea un valor binario de una posición.

Otro objeto de la presente invención es una red de telecomunicaciones para aumentar la seguridad en el intercambio de datos en modo de paquetes según un Protocolo de Internet entre nodos de red de la red de telecomunicación, cooperando para la transmisión de un paquete de datos de Protocolo de Internet al menos un primer nodo de red de un primer proveedor de servicios de telecomunicación y un segundo nodo de red, siendo el segundo nodo de red un nodo vecino del primer nodo de red, teniendo asignada el primer nodo de red una información de identificación, teniendo el segundo nodo de red acceso a la información de identificación asignada al primer nodo de red, estando la red de telecomunicación configurada de manera que:

- el primer nodo de red añade al paquete de datos de Protocolo de Internet la información de identificación del primer nodo de red,
- se transmite el paquete de datos de Protocolo de Internet al segundo nodo de red,
- el segundo nodo de red lleva a cabo una comprobación del paquete de datos de Protocolo de Internet, comprendiendo la comprobación por parte del segundo nodo de red comprobar la información de identificación, siendo el paquete de datos de Protocolo de Internet rechazado por el segundo nodo de red cuando la información de identificación del paquete de datos de Protocolo de Internet no coincide con la información de identificación asignada al primer nodo de red, a la que el segundo nodo de red tiene acceso. Según la invención, se prefiere además –especialmente en atención a la red de telecomunicación– que la red de telecomunicación sea una red

de área amplia. Además, está previsto según la invención –especialmente en atención a la red de telecomunicación– que para la transmisión del paquete de datos de Protocolo de Internet coopere un tercer nodo de red, además del primer y el segundo nodos de red, y que el paquete de datos de Protocolo de Internet incluya una información de salto que se modifique en cada transmisión de un nodo de red previo a otro nodo de red, reconociendo el tercer nodo de red en virtud de la información de salto del paquete de datos de Protocolo de Internet que la comprobación de la información de identificación en el segundo nodo de red ha sido satisfactoria y transmitiendo el tercer nodo de red el paquete de datos de Protocolo de Internet.

Además, según la invención se prefiere –especialmente con vistas a la red de telecomunicación– que la información de identificación comprenda, en caso de utilizar IPv4 y en caso de utilizar IPv6, al menos 24 posiciones binarias o 3 bytes. Además, según la invención se prefiere –especialmente con vistas a la red de telecomunicación– que el primer nodo de red añada al paquete de datos de Protocolo de Internet una información de comprobación, además de la información de identificación del primer nodo de red, indicando la información de comprobación que la información de identificación asignada al primer nodo de red se ha añadido al paquete de datos de Protocolo de Internet.

Además, la presente invención se refiere también a un programa informático con líneas de código de programa con los cuales pueden llevarse a cabo todos los pasos del procedimiento según la invención cuando el programa informático se ejecuta en un dispositivo programable y/o en un equipo terminal de telecomunicación programable y/o en un módulo de interfaz de comunicación, en particular en parte en un equipo terminal de telecomunicación programable y en parte en un módulo de interfaz de comunicación.

Además es objeto de la presente invención un producto de programa informático con un medio legible por ordenador y con un programa informático, almacenado en el medio legible por ordenador, con líneas de código de programa adecuados para que puedan llevarse a cabo todos los pasos del procedimiento según la invención cuando el programa informático se ejecuta en un dispositivo programable y/o en un equipo terminal de telecomunicación programable y/o en un módulo de interfaz de comunicación, en particular en parte en un equipo terminal de telecomunicación programable y en parte en un módulo de interfaz de comunicación.

Según la invención, está previsto que –después del envío de un paquete de datos de Protocolo de Internet por parte de un primer nodo de red– el primer enrutador siguiente (es decir el segundo nodo de red) que obtenga el paquete de datos de Protocolo de Internet (o un mensaje) para su recepción o para su transmisión compruebe la información de identificación. De este modo se asegura según la invención que la identificación introducida, es decir la información de identificación, sea comprobada por nodos de red vecinos (en relación con el primer nodo de red) (como vecinos conocidos). El mensaje o el paquete de datos de Protocolo de Internet puede procesarse sólo si ésta (es decir la información de identificación) es correcta. Sin embargo, si la información de salto, es decir la secuencia de salto, indica que el mensaje o el paquete de datos de Protocolo de Internet ya ha sido comprobado (por el siguiente vecino, es decir el segundo nodo de red, del nodo expedidor, es decir del primer nodo de red), no tiene lugar (en virtud del valor de la información de salto o la secuencia de salto) ninguna comprobación posterior en cuanto a la información de identificación y/o la información de comprobación.

Cuando se introduce en una red de telecomunicación un nuevo enrutador (o un nuevo nodo de red), éste transmitirá, paralelamente a sus actividades *Neighbour Discovery* (es decir de detección de nodos vecinos), también su información de identificación (es decir la identificación hexadecimal de 5 bytes (IPv6) o la identificación decimal de 6 bytes (IPv4)). De este modo todos los enrutadores (o nodos de red) introducidos como salto además de los enrutadores (adicionales) de nueva introducción en la red del proveedor son informados sobre su direccionamiento (así como la información de identificación, es decir su identificación hexadecimal de 5 bytes o su identificación decimal de 6 bytes).

Por tanto, según la invención se prefiere que, además de la información de identificación (es decir el campo de información de 5 o 6 posiciones o esta identificación), se utilice la información de comprobación (o el indicador arriba mencionado), que indica que el campo de información (o la información de identificación) arriba mencionado está incluido (o se ha cargado con una identificación) y que, según el software del enrutador, permite a éste enviar el mensaje o el paquete de datos de Protocolo de Internet en cuestión.

En un escenario de este tipo según la invención, tales nodos de red (o enrutadores/servidores) con tal ajuste pueden enviar paquetes IP satisfactoriamente sólo si la información de comprobación (o la identificación de indicador) indica que el campo de información de 5 o 6 posiciones (o la información

de identificación) está incluido, es decir ha recibido una entrada. Los mensajes o paquetes de datos de Protocolo de Internet no pueden ser recibidos ni en caso dado transmitidos por otros nodos de red (o concentradores o enrutadores) cuando la información de comprobación (o el indicador) no corresponda al valor para un campo de información (o información de identificación) de 5 o 6 posiciones introducido (o cargado).

La pasarela original (es decir el primer nodo de red) del operador/proveedor de red inicial para el acceso a Internet o de los operadores de red de la fuente del mensaje (o de la fuente del paquete de datos de Protocolo de Internet) debe escribir en su enrutador (de red) receptor del mensaje de fuente su identificación reconocible o su valor ID en el encabezamiento IP del mensaje por enviar, como primer salto en la conmutación, antes de que éste pueda seguir siendo enrutado. Con este fin existe, además de la información de identificación (es decir la identificación de 5 o 6 posiciones), también la información de comprobación (es decir el indicador), que cambia tras la introducción del valor ID (es decir la información de identificación) a través del software de “0” a “1” en binario (o viceversa).

Con la información de comprobación (es decir el indicador) que tiene el valor (o la magnitud binaria) “1”, el primer enrutador de salto (es decir el segundo nodo de red) puede enviar mensajes enviados por la fuente (es decir por el primer nodo de red). El segundo enrutador de salto (es decir el segundo nodo de red) comprueba las entradas del primer salto (es decir del primer nodo de red), el enrutador vecino que ha enrutado el mensaje en Ethernet / Internet, y lo transmitido o enviado por todos los enrutadores subsiguientes. Dado que en este contexto los enrutadores deben transmitir o enviar el mensaje a continuación del primer salto, debido al salto pasado (> 1) no se comprueba ni la información de comprobación (es decir el indicador) ni la información de identificación (es decir el valor ID en el mensaje).

Por ejemplo en China existen aproximadamente 220 proveedores de Internet. Así, el número total de proveedores diferentes debería oscilar por debajo de aproximadamente 40.000. Correspondientemente, una información de identificación con seis posiciones decimales (codificadas en binario) o con cinco posiciones hexadecimales (codificadas en binario) debería ser suficiente.

De las figuras y de la siguiente descripción de formas de realización preferidas en referencia a las figuras se desprenden otros detalles, características y ventajas de la invención. Las figuras ilustran aquí solamente ejemplos de formas de realización de la invención, sin limitar la idea esencial de la misma.

*Breve descripción de las figuras*

Figura 1: vista esquemática de una red de telecomunicaciones según la invención con distintos nodos de red.

*Formas de realización de la invención*

En las distintas figuras, los elementos iguales están provistos siempre de símbolos de referencia iguales y, por tanto, en general se nombran o mencionan sólo una vez.

En la Figura 1 se muestra esquemáticamente una vista de una red de telecomunicaciones 100 según la invención con distintos nodos de red. A modo de ejemplo, se muestra una primera red privada 10, por ejemplo un emisor de un mensaje de correo electrónico, y una segunda red privada 30, por ejemplo un receptor del mensaje de correo electrónico. La primera red privada 10 está conectada a un nodo de red 11 de un proveedor de servicios de telecomunicaciones. La segunda red privada 30 está conectada a un tercer nodo de red 13, por ejemplo de otro proveedor de servicios de telecomunicaciones. Entre el primer y el tercer nodos de red 11, 13 hay otra área de red 15. La otra área de red 15 corresponde por ejemplo a una red pública de Internet o una parte de la misma. En la otra área de red 15 existe un segundo nodo de red 12, que está conectado tanto al primer nodo de red 11 como al tercer nodo de red 13. Si ahora se debe enviar un mensaje, por ejemplo un correo electrónico, de la primera red privada 10 a la segunda red privada 30, se emiten paquetes de datos de Protocolo de Internet desde el primer nodo de red 11, que se transmiten a través del segundo nodo de red 12 al tercer nodo de red 13. En la imagen están representados arriba gráficamente el envío y la recepción de un mensaje de correo electrónico. El cliente (por ejemplo de la primera red privada 10, por ejemplo con la identificación AQZ, Fridtjof van den Berge) crea (por ejemplo con un ordenador portátil / teléfono móvil / pad / ordenador / servidor / tableta) un mensaje de correo electrónico y lo envía, a través de su proveedor Z-Mail (es decir el primer nodo de red 11), al receptor, es decir la segunda red privada 30 (por ejemplo Amit Kumar, con la dirección amit.kumar@topa.message.com). El mensaje de correo electrónico abandona la red Z-Mail (es decir el primer nodo de red 11) en dirección al tercer nodo de red 13 (red TopA-Message). El proveedor TopA-Message (es decir el tercer nodo de red 13) transmite el mensaje de correo electrónico al, por ejemplo, ordenador portátil / teléfono móvil / pad / ordenador / servidor / tableta de Amit Kumar.

Un correo electrónico fraudulento (por ejemplo con un troyano en un archivo ZIP adjunto) se envía a una dirección de destino en un país A, por ejemplo a través de la red de un proveedor de servicios de telecomunicación XY del país B. Sin embargo, en este ejemplo, XY recibe el mensaje de correo electrónico a través de otro proveedor de servicios de telecomunicación YZ del país B. Así, el proveedor de servicios de telecomunicación YZ (por ejemplo E-Mailprovider) está obligado a escribir la información de identificación (es decir el valor ID) de su pasarela (es decir del primer nodo de red), que envía el mensaje (o el paquete de datos de Protocolo de Internet), en la información de encabezamiento del paquete de datos de Protocolo de Internet en cuestión (es decir en el encabezamiento IP). En cuanto ha pasado esto (automáticamente a través del software del enrutador), se realiza el cambio del indicador de “0” a “1”, es decir la modificación de la información de comprobación.

De este modo se determina qué primer nodo de red (es decir qué red del cliente o que nodo del cliente) es el origen del mensaje (o del paquete de datos de Protocolo de Internet) y, a pesar de que se utilicen por ejemplo servidores *proxy* para llegar al destino o al “cliente” final (es decir al tercer nodo de red 13), estará claro quién ha iniciado el fraude o el “ataque” para, por ejemplo, espiar.

El proveedor que ha pasado inicialmente el mensaje puede ahora ser consultado en un tiempo breve sobre una sospecha de fraude IP y el proveedor puede ahora comprobar de manera encauzada en su pasarela de dónde o de cuál de sus clientes procedía el mensaje.

## Reivindicaciones

**1.** Procedimiento para aumentar la seguridad en el intercambio de datos en modo de paquetes según un Protocolo de Internet entre nodos de red de una red de telecomunicaciones (100), cooperando para la transmisión de un paquete de datos de Protocolo de Internet al menos un primer nodo de red (11) de un primer proveedor de servicios de telecomunicaciones y un segundo nodo de red (12), siendo el segundo nodo de red (12) un nodo vecino del primer nodo de red (11), teniendo asignada el primer nodo de red (11) una información de identificación, teniendo el segundo nodo de red (12) acceso a la información de identificación asignada al primer nodo de red (11), comprendiendo el procedimiento los siguientes pasos:

- en un primer paso de procedimiento, el primer nodo de red (11) añade al paquete de datos de Protocolo de Internet la información de identificación del primer nodo de red (11),
- en un segundo paso de procedimiento se transmite el paquete de datos de Protocolo de Internet al segundo nodo de red (11),
- en un tercer paso de procedimiento, el segundo nodo de red (12) lleva a cabo una comprobación del paquete de datos de Protocolo de Internet, comprendiendo la comprobación por parte del segundo nodo de red comprobar la información de identificación, siendo el paquete de datos de Protocolo de Internet rechazado por el segundo nodo de red (12) cuando la información de identificación del paquete de datos de Protocolo de Internet no coincide con la información de identificación asignada al primer nodo de red (11), a la que el segundo nodo de red (12) tiene acceso,

caracterizado porque, para la transmisión del paquete de datos de Protocolo de Internet, coopera un tercer nodo de red (13), además del primer y el segundo nodos de red (12), y porque el paquete de datos de Protocolo de Internet incluye una información de salto que se modifica en cada transmisión de un nodo de red previo a otro nodo de red, reconociendo el tercer nodo de red (13) en virtud de la información de salto del paquete de datos de Protocolo de Internet que la comprobación de la información de identificación en el segundo nodo de red (12) ha sido satisfactoria y transmitiendo el tercer nodo de red (13) el paquete de datos de Protocolo de Internet.

**2.** Procedimiento según la reivindicación 1, caracterizado porque la información de identificación comprende, en caso de utilizar IPv4 y en caso de utilizar IPv6, al menos 24 posiciones binarias.

**3.** Procedimiento según una de las reivindicaciones anteriores, caracterizado porque la información de identificación comprende, en caso de utilizar IPv4, al menos seis posiciones decimales codificadas en binario.

**4.** Procedimiento según una de las reivindicaciones anteriores, caracterizado porque la información de identificación comprende, en caso de utilizar IPv6, al menos cinco posiciones hexadecimales.

**5.** Procedimiento según una de las reivindicaciones anteriores, caracterizado porque el primer nodo de red (11) añade al paquete de datos de Protocolo de Internet una información de comprobación, además de la información de identificación del primer nodo de red (11), indicando la información de comprobación que la información de identificación asignada al primer nodo de red (11) se ha añadido al paquete de datos de Protocolo de Internet.

**6.** Procedimiento según una de las reivindicaciones anteriores, caracterizado porque la información de comprobación es un valor binario de una posición.

**7.** Red de telecomunicaciones (100) para aumentar la seguridad en el intercambio de datos en modo de paquetes según un Protocolo de Internet entre nodos de red de la red de telecomunicaciones (100), estando la red de telecomunicaciones (100) configurada de manera que, para la transmisión de un paquete de datos de Protocolo de Internet, cooperan al menos un primer nodo de red (11) de un primer proveedor de servicios de telecomunicaciones y un segundo nodo de red (12), siendo el segundo nodo de red (12) un nodo vecino del primer nodo de red (11), teniendo asignada el primer nodo de red (11) una información de identificación, teniendo el segundo nodo de red (12) acceso a la información de identificación asignada al primer nodo de red (11), estando la red de telecomunicación (100) configurada además de manera que:

- el primer nodo de red (11) añade al paquete de datos de Protocolo de Internet la información de identificación del primer nodo de red (11),
- se transmite el paquete de datos de Protocolo de Internet al segundo nodo de red (12),

- el segundo nodo de red (12) lleva a cabo una comprobación del paquete de datos de Protocolo de Internet, comprendiendo la comprobación por parte del segundo nodo de red comprobar la información de identificación, siendo el paquete de datos de Protocolo de Internet rechazado por el segundo nodo de red (12) cuando la información de identificación del paquete de datos de Protocolo de Internet no coincide con la información de identificación asignada al primer nodo de red (11), con el que el segundo nodo de red (12) tiene una conexión,

caracterizada porque la red de telecomunicación (100) está además configurada de manera que, para la transmisión del paquete de datos de Protocolo de Internet, coopera un tercer nodo de red (13), además del primer y el segundo nodos de red (12), y porque el paquete de datos de Protocolo de Internet incluye una información de salto que se modifica en cada transmisión de un nodo de red previo a otro nodo de red, estando el tercer nodo de red (13) configurado para, en virtud de la información de salto del paquete de datos de Protocolo de Internet, reconocer que la comprobación de la información de identificación en el segundo nodo de red (12) ha sido satisfactoria y transmitir el paquete de datos de Protocolo de Internet.

**8.** Red de telecomunicaciones (100) según la reivindicación 7, caracterizada porque la red de telecomunicación (100) es una red de área amplia.

**9.** Red de telecomunicaciones (100) según una de las reivindicaciones 7 u 8, caracterizada porque la información de identificación comprende, en caso de utilizar IPv4 y en caso de utilizar IPv6, al menos 24 posiciones binarias.

**10.** Red de telecomunicaciones (100) según una de las reivindicaciones 7, 8 o 9, caracterizada porque el primer nodo de red (11) está configurado de manera que el primer nodo de red (11) añade al paquete de datos de Protocolo de Internet una información de comprobación, además de la información de identificación del primer nodo de red (11), indicando la información de comprobación que la información de identificación asignada al primer nodo de red (11) se ha añadido al paquete de datos de Protocolo de Internet.

**11.** Programa informático con líneas de código de programa por medio de los cuales se llevan a cabo todos los pasos de un procedimiento según una de las reivindicaciones 1 a 6 cuando el programa informático se ejecuta en un

dispositivo programable y/o en un nodo de red (11, 12, 13), en particular en parte en varios nodos de red (11, 12, 13) de una red de telecomunicaciones.

**12.** Producto de programa informático con un medio legible por ordenador y un programa informático, almacenado en el medio legible por ordenador, con líneas de código de programa adecuados para que se lleven a cabo todos los pasos de un procedimiento según una de las reivindicaciones 1 a 6 cuando el programa informático se ejecuta en un dispositivo programable y/o en un nodo de red (11, 12, 13), en particular en parte en varios nodos de red (11, 12, 13) de una red de telecomunicaciones (100).

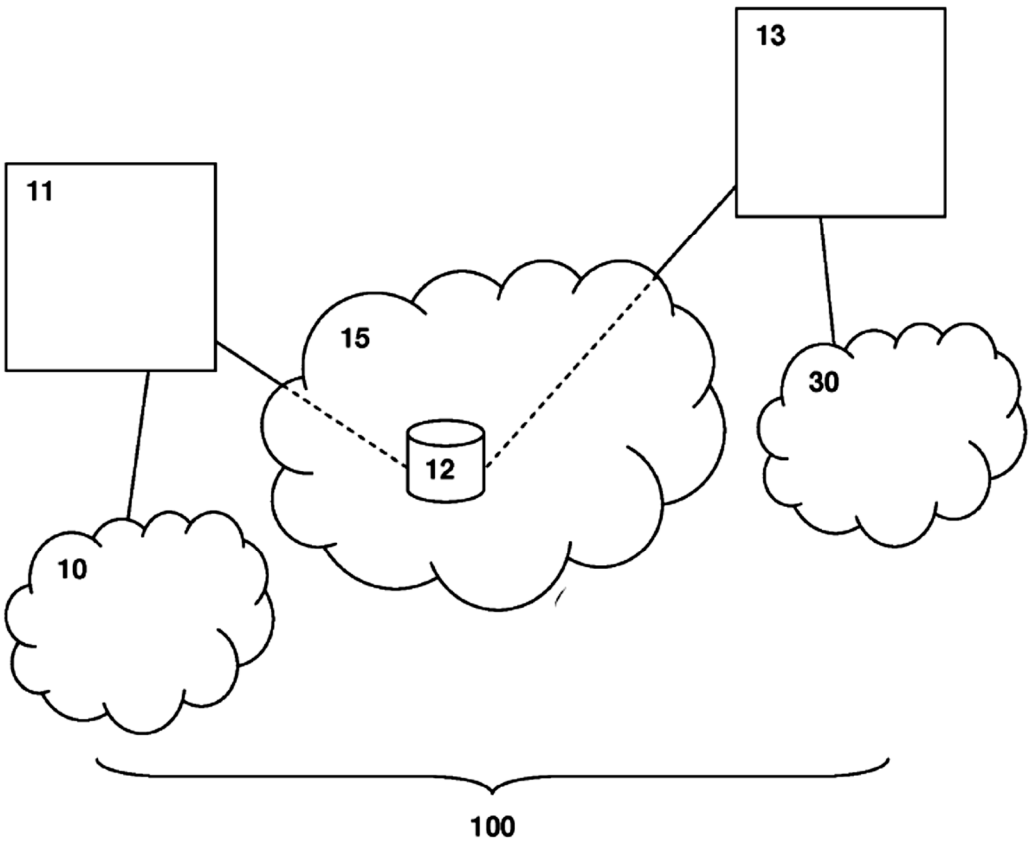


Fig. 1