(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 703 762**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.08.2013 PCT/CN2013/080991**

(87) Fecha y número de publicación internacional: **08.05.2014 WO14067310**

(96) Fecha de presentación y número de la solicitud europea: **07.08.2013 E 13851231 (4)**

(97) Fecha y número de publicación de la concesión europea: **10.10.2018 EP 2916508**

(54) Título: **Método para procesado de paquetes, dispositivo electrónico y medio de almacenamiento**

(30) Prioridad:

01.11.2012 CN 201210430244

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.03.2019

(73) Titular/es:

HUIZHOU TCL MOBILE COMMUNICATION CO., LTD. (100.0%)
70 Huifeng 4th Road Zhongkai Hi-Tech Development District
Huizhou, Guangdong 516006, CN

(72) Inventor/es:

XIANG, JINMING;
ZHOU, DAN;
LU, XIAOFENG y
WU, JUN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para procesado de paquetes, dispositivo electrónico y medio de almacenamiento

Antecedentes de la invención

1. Campo de la invención

La presente invención se refiere al campo de la comunicación en red, más particularmente, a un método para procesado de paquetes, a un dispositivo electrónico y a un medio de almacenamiento.

2. Descripción de la técnica anterior

La Denegación de Servicio (DoS) es un ataque convencional a redes que es relativamente eficaz y en gran medida indefendible. El objetivo principal del DoS es incapacitar un servidor para proporcionar servicio para usuarios regulares. Como consecuencia, el DoS representa una amenaza considerable para empresas y organizaciones que se basan fuertemente en internet.

A medida que las redes de telefonía móvil crecen, los teléfonos inteligentes se convierten en dispositivos de internet primarios. A medida que el 4G y el IPV6 prosperan, los teléfonos inteligentes jugarán un papel más importante en la internet de telefonía móvil. No obstante, los teléfonos móviles son usados cada vez más como puntos de acceso por software (AP por software) por ordenadores; al mismo tiempo, el número de aplicaciones para ordenadores que usan teléfonos móviles para navegar en internet está aumentando. Puesto que los teléfonos inteligentes están completamente expuestos en internet, los mismos son muy vulnerables a ataques de redes externas, especialmente el DoS que sitúa los teléfonos móviles bajo un enorme riesgo en red y con una baja seguridad. La publicación de patente de Estados Unidos n.º 2007/0201474 propone un dispositivo y un sistema de red con un método de encaminamiento para implementar un control de comunicaciones ilegales en múltiples puntos en contacto con la red del proveedor de servicios de comunicación. El documento CN 101594359 propone un método de establecimiento de una conexión TCP entre un extremo de agencia TCP y un extremo de cliente después de tres tomas de contacto TCP entre el extremo de agencia TCP y el extremo de cliente. No obstante, la publicación de patente de Estados Unidos n.º 2007/0201474 y el documento CN 101594359 no describen cómo determinar si el terminal móvil está en basándose en el número de paquetes de toma de contacto a procesar.

Sumario de la invención

Teniendo en cuenta los defectos antes mencionados de la técnica convencional, la presente invención consiste en proporcionar un método para procesado de paquetes, un dispositivo electrónico y un medio de almacenamiento, de acuerdo con las reivindicaciones 1, 6 y 11, respectivamente, para resolver el problema por el que los dispositivos electrónicos, especialmente los teléfonos móviles, son convencionalmente vulnerables a un DoS.

El método para procesado de paquetes, el dispositivo electrónico y el medio de almacenamiento resuelven eficazmente el problema de que los dispositivos electrónicos convencionales, especialmente los teléfonos móviles, sean vulnerables al DOS, y evitan eficazmente un ataque DoS, especialmente un ataque con señales de toma de contacto (SYN), al mismo tiempo que ofrecen eficazmente una defensa para el ataque en dispositivos electrónicos internos con respecto a la red externa cuando los dispositivos electrónicos, especialmente teléfonos móviles, se usan como ap de software.

Breve descripción de los dibujos

La Fig. 1 muestra un dispositivo electrónico en un entorno de funcionamiento.

La Fig. 2 muestra un diagrama de bloques de un dispositivo electrónico de acuerdo con una realización preferida de la presente invención.

La Fig. 3 muestra un diagrama de flujo de un método para procesar paquetes de acuerdo con una realización preferida de la presente invención.

La Fig. 4 ilustra el funcionamiento del dispositivo electrónico y el método para procesar paquetes de acuerdo con una realización preferida de la presente invención.

Descripción detallada de las realizaciones preferidas

Para ilustrar la técnica y los efectos de la presente invención, se dará a conocer una descripción detallada por medio de la siguiente exposición en combinación con las figuras. Debe indicarse que los componentes iguales se indican con el mismo número.

En las siguientes ilustraciones, la realización detallada de la presente invención se refiere a etapas y señales en uno o una pluralidad de proceso prácticos de ordenador, a no ser que existan otras ilustraciones. Por lo tanto, los lectores entenderán estas etapas y prácticas, de manera que algunas de ellas serán puestas en funcionamiento por

ordenadores, incluyendo unidades de procesado de ordenadores que presentan señales electrónicas de datos de tipo estructurado. El funcionamiento transforma los datos o mantiene los datos en su posición en el sistema de memoria del ordenador, el cual se puede reconfigurar, o el funcionamiento del ordenador se cambia a través de otras maneras con las cuales está familiarizado un experto en la materia. La estructura de datos que mantienen los datos es una posición física del sistema de memoria, que tiene propiedades particulares que son definidas por la estructura de datos. No obstante, la ilustración anterior sobre el fundamento de la presente invención no está limitada; un experto en la materia percibirá que una pluralidad de etapas y prácticas que se exponen a continuación también se pueden materializar en hardware.

Las terminologías de la solicitud, tales como componente, módulo, sistema e interfaz, se refieren todas ellas a entidades de ordenador relativas: hardware, combinación de hardware y software, software o software en práctica. Por ejemplo, el término conjunto puede ser, aunque sin carácter limitativo, acciones procesadas en procesadores, procesadores, objetos, aplicaciones ejecutables, hilos de ejecución y/u ordenadores. Tal como indican las figuras, tanto las aplicaciones que se procesan en un controlador como el propio controlador pueden ser un componente. Uno o una pluralidad de componentes puede existir en acciones y/o hilos de ejecución, al mismo tiempo que situados en un ordenador y/o distribuidos entre dos o más ordenadores.

Por otra parte, los sujetos que buscan protección se pueden materializar en forma de métodos, dispositivos o fabricantes que producen software, microprogramas, hardware o cualquier combinación aleatoria para controlar ordenadores usando habilidades convencionales de programación y/o ingeniería. El término “fabricante” usado aquí se refiere a cualquier programa de ordenador al que se puede acceder desde cualquier equipo, soporte o medio legible por ordenador. Naturalmente, alguien versado en la materia observará que esta configuración se puede modificar de múltiples maneras aún permaneciendo en el ámbito o dentro de los principios del sujeto que busca protección.

La Fig. 1 y la siguiente descripción proporcionan un breve sumario del entorno de funcionamiento de los dispositivos electrónicos de la presente invención. El entorno de funcionamiento de la Fig. 1 es simplemente una realización de entorno de funcionamiento adecuado sin ninguna pretensión de sugerir ningún límite sobre el alcance de los objetivos o la función del entorno de funcionamiento. Un dispositivo electrónico 112 en la realización comprende, aunque sin carácter limitativo, ordenadores personales, ordenadores servidores, dispositivos de mano o portátiles, dispositivos móviles (tales como teléfonos móviles, asistentes personales digitales (PDA), reproductores de medios, etcétera), múltiples sistemas de procesador, electrónica de consumo, miniordenadores, megaordenadores, entornos de informática distribuida que comprenden cualquier sistema o dispositivo antes mencionado, etcétera...

La realización se describe con los antecedentes generales de que las “instrucciones legibles por ordenador” son procesadas por uno o múltiples dispositivos electrónicos, aunque esto no sea demandado. Una instrucción legible por ordenador puede ser distribuida por un soporte legible por ordenador (tal como se describe posteriormente). La instrucción legible por ordenador se puede materializar en forma de módulos de programa, tales como tareas particulares de procesado o una función de procesado, un objeto, una interfaz de programación de aplicaciones (API) y una estructura de datos del tipo particular datos abstractos. Típicamente, la función de la instrucción legible por ordenador se puede combinar o distribuir aleatoriamente en cualquier entorno.

La Fig. 1 indica un ejemplo del dispositivo electrónico 112 de una o una pluralidad de realizaciones de un método para proceso de paquetes de la presente invención. El dispositivo electrónico 112 comprende por lo menos un procesador 116 y una memoria 118. De acuerdo con la configuración y el tipo específicos del dispositivo electrónico, la memoria 118 puede ser volátil (tal como una RAM) o no volátil (tal como una ROM o memoria *flash*), o una combinación de los dos tipos anteriores. La configuración se indica por medio de líneas de trazos en la Fig. 1.

En otras realizaciones, el dispositivo electrónico 112 también puede comprender dispositivos de almacenamiento adicionales (tales como extraíbles y/o no extraíbles), que incluyen, aunque sin carácter limitativo, dispositivos de almacenamiento magnético, dispositivos de almacenamiento óptico, etcétera. Estos dispositivos de almacenamiento adicionales se indican con el dispositivo 120 de almacenamiento en la Fig. 1. En una realización, la instrucción legible por ordenador para materializar una o una pluralidad de realizaciones de la presente invención se puede almacenar en el dispositivo 120 de almacenamiento. El dispositivo 120 de almacenamiento también puede almacenar otras instrucciones legibles por ordenador para materializar sistemas operativos o programas de aplicación, etcétera. Las instrucciones legibles por ordenador se pueden cargar en la memoria 118 y pueden ser procesadas por la unidad 116 de procesado.

El término “soporte legible por ordenador” en la presente invención comprende un medio de almacenamiento de ordenador. El medio de almacenamiento de ordenador comprende un soporte volátil o no volátil, extraíble o no extraíble, el cual se puede materializar mediante cualquier método o tecnología usado para almacenar información, tal como instrucciones legibles por ordenador u otros datos. La memoria 118 y el dispositivo 120 de almacenamiento ejemplifican el medio de almacenamiento de ordenador. El medio de almacenamiento de ordenador comprende, aunque sin carácter limitativo, una RAM, una ROM, una EEPROM, una memoria *flash* u otros mecanismos de memorización, un CD-ROM, un DVD u otros dispositivos de almacenamiento óptico, casetes, cintas, dispositivos de almacenamiento de disco u otros dispositivos de almacenamiento magnético, o cualquier otro soporte que se pueda usar para almacenar información esperada y al que pueda acceder el dispositivo electrónico 112. Cualquier medio

de almacenamiento de ordenador similar puede formar parte del dispositivo electrónico 112.

El dispositivo electrónico 112 también comprende un enlace 126 de comunicaciones que permite que el dispositivo electrónico 112 se comunique con otros dispositivos. El enlace 126 de comunicaciones comprende, aunque sin carácter limitativo, un módem, una tarjeta de interfaz de red (NIC), una interfaz de red integrada, un transmisor/receptor de radiofrecuencia (RF), un puerto de infrarrojos, una interfaz de USB u otras interfaces que enlacen el dispositivo electrónico 112 con otros dispositivos electrónicos. El enlace 126 de comunicaciones comprende conexión por cable o conexión inalámbrica. El enlace 126 de comunicaciones transmite/recibe medios de comunicación.

El término “soporte legible por ordenador” comprende un soporte de comunicaciones. Típicamente, el soporte de comunicaciones comprende instrucciones legibles por ordenador u otros datos en señales de datos moduladas, tales como una onda portadora, u otros mecanismos de transmisión, y comprende cualquier soporte de distribución de información. El término “señales de datos moduladas” comprende señales tales que tienen una o una pluralidad de propiedades a configurar o cambiar por medio de codificación de información en las señales.

El dispositivo electrónico 112 comprende un dispositivo 124 de entrada, tal como un teclado, un ratón, un dispositivo de entrada de voz, un dispositivo de entrada táctil, una cámara de infrarrojos, un dispositivo de entrada de vídeo y/o cualquier otro dispositivo de entrada. El dispositivo 112 también comprende un dispositivo 122 de salida, tal como uno o una pluralidad de dispositivos de visualización, un altavoz, una impresora y/o cualquier otro dispositivo de salida. El dispositivo 124 de entrada y el dispositivo 122 de salida se pueden conectar al dispositivo electrónico 112 a través de conexión por cable, conexión inalámbrica o cualquier otra combinación. En una realización, como dispositivo 124 de entrada o dispositivo 122 de salida del dispositivo electrónico 112 se pueden usar dispositivos de entrada o dispositivos de salida de otro dispositivo electrónico.

Componentes del dispositivo electrónico 112 se pueden conectar a través de diversas interconexiones, tales como buses. Dichas interconexiones comprenden la interconexión de componentes periféricos (PCI) (tal como la PCI rápida), buses serie universales (USB), IEEE 1394, estructuras de buses ópticos, etcétera. En otra realización, componentes del dispositivo electrónico 112 se pueden interconectar a través de una red. Por ejemplo, la memoria 118 se puede formular mediante una pluralidad de unidades de memoria físicas interconectadas a través de red cuyas posiciones físicas son diferentes.

Un experto en la materia percibirá que los dispositivos de almacenamiento usados para almacenar instrucciones legibles por ordenador se pueden distribuir sobre redes. Por ejemplo, un dispositivo electrónico 130 al que se puede acceder a través de una red 128 puede almacenar instrucciones legibles por ordenador cuya finalidad es materializar una o una pluralidad de realizaciones proporcionadas en la presente invención. El dispositivo electrónico 112 puede acceder al dispositivo electrónico 130, y descargar y ejecutar parte o la totalidad de las instrucciones legibles por ordenador. Alternativamente, el dispositivo electrónico 112 puede descargar una pluralidad de instrucciones legibles por ordenador según se requiera; o, algunas instrucciones se pueden ejecutar en el dispositivo electrónico 112 y algunas instrucciones se pueden ejecutar en el dispositivo electrónico 130.

El artículo proporciona un funcionamiento diverso de las realizaciones. En una realización, una o diversas operaciones mencionadas pueden formar una o una pluralidad de instrucciones legibles por ordenador almacenadas en soporte legible por ordenador, que permiten que dispositivos informáticos lleven a cabo el funcionamiento mencionado cuando son ejecutadas por dispositivos electrónicos. La secuencia descrita de algunas o la totalidad de las operaciones no significa que estas operaciones deban seguir dicha secuencia. Una persona experta en la materia asimilará secuencias alternativas con los mismos beneficios de la presente invención. Por otra parte, es entendible que no todas las operaciones tengan que existir en cada realización que proporciona el artículo.

Además, el término “preferible” en el artículo se aplica a ejemplos, ilustraciones y casos. Cualquier aspecto o diseño “preferible” en el artículo no requiere ser explicado como más ventajoso que otros aspectos y diseños. Por el contrario, el término “preferible” se usa para plantear un concepto de manera práctica. Por ejemplo, el término “o” en la solicitud significa “además” no “excepto”. En otras palabras, a no ser que se mencione específicamente o el contexto indique lo contrario, “X usa A o B”, significa una cualquiera de las disposiciones incluidas intrínsecamente. Es decir, si X usa A, X usa B, o X usa A y B, entonces “X usa A o B” da cumplimiento a cualquiera de las realizaciones antes mencionadas.

Además, aunque la presente invención se ha ejemplificado y descrito por medio de una o una pluralidad de realizaciones, a alguien versado en la materia se le ocurrirán variantes equivalentes y modificaciones al leer y entender esta ilustración y las figuras adjuntas. La presente invención comprende todas estas variantes y modificaciones las cuales quedan únicamente limitadas por el alcance de las reivindicaciones adjuntas. En particular, en cuanto a las diversas funciones que llevan a cabo los componentes mencionados (tales como elementos y recursos), los términos que describen dichos componentes están destinados a corresponderse con cualquier componente (a no ser que se indique lo contrario) capaz de realizar las funciones del componente en cuestión (es decir, de función equivalente). Adicionalmente, aunque una propiedad particular de la presente invención únicamente da a conocer algunas de las diversas realizaciones, dicha propiedad se puede combinar con otras propiedades de otras realizaciones que se esperan o que son beneficiosas para una o una pluralidad de

aplicaciones. Por otra parte, en cuanto a los términos “incluir”, “comprender” y “constar de” usados en realizaciones prácticas o reivindicaciones, su significado es idéntico al de “contener”.

En el proceso de la transmisión de datos, cada paquete del Protocolo de Control de Transmisión (TCP) comprende un número de secuencia (SEQ) y un número de acuse de recibo (ACK), estando ambos en el orden de bytes de la red. El número SEQ es un número de secuencia del paquete TCP que indica la secuencia de transmisión del paquete TCP, mientras que el número ACK es un número de confirmación del paquete TCP que indica que el paquete se ha recibido. Por ejemplo, cuando un cliente establece conexión con un servidor a través del principio de tres tomas de contacto, el servidor envía al cliente un paquete TCP que transporta datos, aunque el número SEQ y el número ACK del paquete TCP son iguales al número SEQ y al número ACK de un paquete de la tercera fase de establecimiento de conexión. Cuando el cliente recibe el paquete TCP enviado desde el servidor, envía un paquete de acuse de recibo de vuelta al servidor, siendo el número SEQ del paquete de acuse de recibo el número ACK del último paquete, y siendo el número ACK del paquete de acuse de recibo el número SEQ del último paquete más el tamaño de datos que está transportando el paquete de acuse de recibo.

La idea básica de la presente invención es: resolver el problema por el que los terminales móviles convencionales, especialmente los teléfonos móviles, son vulnerables a un DoS, estableciendo de antemano un módulo de defensa en los terminales móviles, y verificando una solicitud de conexión de una red externa o una red interna a través del módulo de defensa. En primer lugar, sobre la base del principio de tres tomas de contacto de los acuerdos TCP, cuando una red externa o red interna envía un primer paquete SYN (es decir, un paquete SYN), el módulo de defensa forja un paquete de acuse de recibo de toma de contacto (es decir, un paquete SYN+ACK) destinado a enviarse a la red externa o red interna. El lado atacante se define como el lado solicitante de conexión. Si la red externa es el lado solicitante de conexión, cuando el módulo de defensa recibe un paquete sucesivo de acuse de recibo (es decir, un paquete ACK) del lado solicitante, el módulo de defensa crea un paquete SYN, y decide si enviar el paquete SYN a terminales móviles o equipos de LAN enlazados por debajo de terminales móviles sobre la base de una pila de protocolos TCP/IP. Cuando el módulo de defensa recibe un paquete SYN+ACK enviado desde los terminales móviles, el módulo de defensa abandona el paquete SYN+ACK, y crea un paquete ACK para que sea enviado a terminales móviles o equipos de LAN enlazados por debajo de terminales móviles. Los terminales móviles o equipos de LAN enlazados por debajo de terminales móviles verifican la solicitud de conexión a través del paquete ACK; si la solicitud de conexión queda verificada, se establece la conexión entre el lado solicitante y terminales móviles o equipos de LAN enlazados por debajo de terminales móviles. El módulo de defensa incrementará la inmunidad de los terminales móviles a un ataque DoS y reforzará la seguridad de los mismos.

Consúltese la Fig. 2 para ver un diagrama de bloques de un dispositivo electrónico de acuerdo con una realización preferida de la presente invención. Un dispositivo electrónico 20 comprende uno o más procesadores, una memoria y uno o más programas almacenados en la memoria, un método configurado de procesado de paquetes llevado a cabo por uno o más procesadores, uno o más programas divididos en particiones por función, que incluyen un módulo 21 de defensa, una pila 22 de protocolos TCP/IP y un módulo 23 de procesado de paquetes.

Cuando el dispositivo electrónico de la realización preferida 20 está en funcionamiento, cuando recibe un primer paquete SYN de solicitud de conexión desde un lado solicitante 24 de conexión, el módulo 21 de defensa del dispositivo electrónico 20 crea un primer paquete SYN+ACK, y envía el primer paquete SYN+ACK para responder al lado solicitante 24 de conexión;

cuando recibe el primer paquete SYN+ACK desde el lado solicitante 24 de conexión, el módulo 21 de defensa crea un segundo paquete SYN+ACK con el mismo número SEQ y el mismo número ACK que el primer paquete SYN+ACK, y envía el segundo paquete SYN+ACK al módulo 23 de procesado de paquetes del dispositivo electrónico 20 a través de la pila 22 de protocolos TCP/IP, en donde el segundo paquete SYN+ACK comprende el número SEQ Y del primer paquete SYN+ACK;

la pila 22 de protocolos TCP/IP recibe el segundo paquete SYN+ACK del módulo 23 de procesado de paquetes, y modifica el número SEQ Z del segundo paquete SYN+ACK al número SEQ Y del primer paquete SYN+ACK, y envía el segundo paquete modificado SYN+ACK al módulo 21 de defensa mientras almacena el valor diferencia R de dos números SEQ, donde R=Z-Y;

cuando recibe el segundo paquete modificado SYN+ACK, el módulo 21 de defensa crea un segundo paquete ACK con un número ACK Y+1, y envía el segundo paquete ACK a la pila 22 de protocolos TCP/IP;

basándose en el valor diferencia R de números SEQ, la pila 22 de protocolos TCP/IP modifica el número ACK del segundo paquete ACK a Z+1, y envía el segundo paquete ACK modificado al módulo 23 de procesado de paquetes, de manera que la toma de contacto entre el módulo 21 de defensa y el módulo 23 de procesado de paquetes se produce con éxito, y se crea la conexión entre el lado solicitante 24 de conexión y el módulo 23 de procesado de paquetes. Sobre la base de una tabla de encaminamiento, el TCP/IP decide si el destino del segundo paquete ACK es el módulo 23 de procesado de paquetes del dispositivo electrónico 20 ó el dispositivo de red enlazado con el dispositivo electrónico 20 (con una función similar del módulo 23 de procesado de paquetes).

Cuando se establece la conexión entre el lado solicitante 24 y el módulo 23 de procesado de paquetes, la pila 22 de

protocolos TCP/IP procesará todos los paquetes intercambiados entre el lado solicitante 24 y el módulo 23 de procesado de paquetes. Por ejemplo: la pila de protocolos TCP/IP recibe un paquete del lado solicitante 24 de conexión, modifica un número ACK A del paquete a A+R, y envía el paquete modificado al módulo 23 de procesado de paquetes; la pila 22 de protocolos TCP/IP recibe el paquete ACK del módulo 23 de procesado de paquetes, modifica un número ACK B del paquete ACK a B-R, y envía el paquete ACK modificado al lado solicitante 24 de conexión. De esta manera, el lado solicitante 24 de conexión y el módulo 23 de procesado de paquetes pueden intercambiar datos de manera normal a través de la pila 22 de protocolos TCP/IP.

Cuando el módulo 21 de defensa se establece entre el lado solicitante 24 de conexión y el módulo 23 de procesado de paquetes, el módulo 21 de defensa decide si procesar nuevos primeros paquetes SYN basándose en el número de los primeros paquetes SYN a procesar; donde los primeros paquetes SYN a procesar son aquellos que no reciben primeros paquetes ACK correspondientes.

Si el número de los primeros paquetes SYN es igual o inferior a un primer valor predeterminado (tal como 100), el dispositivo electrónico 20 está funcionando de manera normal, y el módulo 21 de defensa procesa todos los primeros paquetes SYN nuevos.

Si el número de los primeros paquetes SYN es mayor que el primer valor predeterminado (tal como 100) e igual o inferior a un segundo valor predeterminado (tal como 300), el dispositivo electrónico 20 se encuentra en un estado de riesgo moderado, y el módulo 21 de defensa procesa los primeros paquetes SYN a procesar. Los nuevos primeros paquetes SYN a procesar son aquellos primeros paquetes SYN sin ningún registro de información de paquete en el módulo 21 de defensa. En otras palabras, en el módulo 21 de defensa se establece un historial de valores *hash*; si la información de paquete de un nuevo primer paquete SYN (tal como puerto de origen, dirección de origen, puerto de destino y dirección de destino del primer paquete SYN) no está registrada en el historial de valores *hash*, el módulo 21 de defensa procesa el nuevo primer paquete SYN (es decir, se da prioridad a una conexión de una nueva IP).

Si el número de los primeros paquetes SYN es mayor que el segundo valor predeterminado (tal como 300), el dispositivo electrónico 20 se encuentra en un estado de riesgo, y el módulo 21 de defensa no procesará ningún primer paquete SYN nuevo excepto los primeros paquetes SYN que están en procesado.

Preferentemente, si el número de los primeros paquetes SYN a procesar con una misma dirección IP es mayor que un cuarto valor predeterminado (tal como 5), se decide que la conexión de datos de la dirección IP es una conexión de datos agresiva, y el módulo 21 de defensa abandona la conexión de datos correspondiente de los primeros paquetes SYN a procesar directamente.

El dispositivo electrónico de la realización preferida resuelve eficazmente el problema por el que dispositivos electrónicos convencionales, especialmente teléfonos móviles, son vulnerables a un ataque DoS; evitan eficazmente un ataque DoS, especialmente un ataque con señales de toma de contacto (SYN). Cuando los dispositivos electrónicos, especialmente teléfonos móviles, son puntos de acceso por software, se puede evitar eficazmente un ataque sobre dispositivos electrónicos internos desde una red externa.

Consúltese la Fig. 3 para ver un diagrama de flujo de la realización preferida del método de procesado de paquetes de la presente invención. El método de procesado de paquetes de la presente invención comprende:

S301, cuando recibe el primer paquete SYN de solicitud de conexión desde el lado solicitante de conexión, el módulo de defensa del dispositivo electrónico crea un primer paquete SYN+ACK y envía el primer paquete SYN+ACK al lado solicitante de conexión

S302, cuando recibe el primer paquete ACK del lado solicitante de conexión, el módulo de defensa crea un segundo paquete SYN con el mismo número SEQ y el mismo número ACK que el primer paquete SYN, y envía el segundo paquete SYN al módulo de procesado de paquetes del dispositivo electrónico a través de la pila de protocolos TCP/IP, en donde el segundo paquete SYN comprende el número SEQ Y del primer paquete SYN+ACK;

S303, la pila de protocolos TCP/IP recibe el segundo paquete ACK del módulo de procesado de paquetes, y modifica el número SEQ Z del segundo paquete SYN+ACK al número SEQ Y del primer paquete SYN+ACK, y envía el segundo paquete modificado SYN+ACK al módulo de defensa, mientras tanto almacena el valor diferencia de los números SEQ R, donde R=Z-Y;

S304, cuando recibe el segundo paquete modificado SYN+ACK, el módulo de defensa crea un segundo paquete ACK con un número ACK Y+1 y envía el segundo paquete ACK a la pila de protocolos TCP/IP;

S305, la pila de protocolos TCP/IP modifica el número ACK del segundo paquete ACK a Z+1 de acuerdo con el valor diferencia de los números SEQ R, y envía el segundo paquete ACK modificado al módulo de procesado de paquetes, de manera que se produce con éxito la toma de contacto entre el módulo de defensa y el módulo de procesado de paquetes, y se crea una conexión entre el lado solicitante y el módulo de procesado de paquetes;

S306, la pila de protocolos TCP/IP recibe un paquete del lado solicitante de conexión, y modifica el número ACK A

del paquete A+R, y envía el paquete modificado al módulo de procesado de paquetes;

S307, la pila de protocolos TCP/IP recibe un paquete ACK del módulo de procesado de paquetes, y modifica el número SEQ B del paquete ACK a B-R, y envía el paquete ACK modificado al lado solicitante de conexión;

El método de procesado de paquetes de la realización preferida finaliza en la etapa S307.

Cuando el módulo 21 de defensa se establece entre el lado solicitante 24 y el módulo 23 de procesado de paquetes, el módulo 21 de defensa decide si procesar nuevos primeros paquetes SYN en función del número de los primeros paquetes SYN a procesar; donde los primeros paquetes SYN a procesar son aquellos que no reciben los primeros paquetes ACK correspondientes.

Si el número de los primeros paquetes SYN es igual o inferior a un primer valor predeterminado (tal como 100), el dispositivo electrónico 20 está funcionando de manera normal, y el módulo 21 de defensa procesa todos los primeros paquetes SYN nuevos.

Si el número de los primeros paquetes SYN es mayor que el primer valor predeterminado (tal como 100) e igual o inferior a un segundo valor predeterminado (tal como 300), el dispositivo electrónico 20 se encuentra en un estado de riesgo moderado, y el módulo 21 de defensa procesa los primeros paquetes SYN a procesar. Los nuevos primeros paquetes SYN a procesar son aquellos primeros paquetes SYN sin ningún registro de información de paquete en el módulo 21 de defensa. En otras palabras, en el módulo 21 de defensa se establece un historial de valores *hash*; si la información de paquete de un nuevo primer paquete SYN (tal como puerto de origen, dirección de origen, puerto de destino y dirección de destino del primer paquete SYN) no está registrada en el historial de valores *hash*, el módulo 21 de defensa procesa el nuevo primer paquete SYN (es decir, se da prioridad a una conexión de una nueva IP).

Si el número de los primeros paquetes SYN es mayor que el segundo valor predeterminado (tal como 300), el dispositivo electrónico 20 se encuentra en un estado de riesgo, y el módulo 21 de defensa no procesará ningún primer paquete SYN nuevo excepto aquellos primeros paquetes SYN que están en procesado.

Preferentemente, si el número de los primeros paquetes SYN a procesar con una misma dirección IP es mayor que un cuarto valor predeterminado (tal como 5), se decide que la conexión de datos de la dirección IP es una conexión de datos agresiva, y el módulo 21 de defensa abandona directamente la conexión de datos correspondiente de los primeros paquetes SYN a procesar.

El dispositivo electrónico de la realización preferida resuelve eficazmente el problema por el que dispositivos electrónicos convencionales, especialmente teléfonos móviles, son vulnerables a un ataque DoS; evitan eficazmente un ataque DoS, especialmente un ataque con señales de toma de contacto (SYN). Cuando los dispositivos electrónicos, especialmente teléfonos móviles, son puntos de acceso por software, se puede evitar eficazmente un ataque sobre dispositivos electrónicos internos desde una red externa.

Consúltese la Fig. 4 para ver un diagrama del fundamento de la realización detallada del método de procesado de paquetes y el dispositivo electrónico de la presente invención. El método de procesado de paquetes proporciona una función de defensa contra DoS que comprende las siguientes etapas:

preinstalar un módulo 41 de defensa para defenderse de un DoS en un terminal móvil 43;

cuando un lado solicitante 44 de conexión envía un primer paquete SYN de solicitud de conexión al módulo 41 de defensa, el módulo 41 de defensa forja un primer paquete SYN+ACK, y envía el primer SYN+ACK al lado solicitante 44 de conexión;

cuando el módulo 41 de defensa recibe un primer paquete ACK del lado solicitante 44 de conexión, el módulo 41 de defensa crea un segundo paquete SYN con el mismo número SEQ y el mismo número ACK que el primer paquete SYN, y envía el segundo paquete SYN al terminal móvil 43 a través de la pila de protocolos TCP/IP como el lado solicitante 44 de conexión;

la pila 42 de protocolos TCP/IP recibe el segundo paquete SYN+ACK del terminal móvil 43, y obtiene un primer valor diferencia de SEQ restando el número SEQ del primer paquete SYN+ACK con respecto al número SEQ del segundo paquete SYN+ACK;

la pila 42 de protocolos TCP/IP modifica el número SEQ del segundo paquete SYN+ACK enviado desde el terminal móvil 43 al módulo 41 de defensa, y resta el valor diferencia de los números SEQ con respecto al número SEQ del segundo paquete SYN+ACK; y modifica el número ACK del segundo paquete ACK del módulo 41 de defensa al terminal móvil 43, y modifica el número ACK del segundo paquete SYN+ACK sumando el valor diferencia de los números SEQ al número ACK del segundo paquete SYN+ACK;

el número ACK modificado del segundo paquete ACK es igual al número SEQ del segundo paquete SYN+ACK más uno, de manera que la toma de contacto entre el módulo 41 de defensa y el terminal móvil 43 se produce con éxito, y se establece la conexión entre el lado solicitante 44 de conexión y el terminal móvil 43.

La siguiente parte es una descripción detallada de las etapas antes mencionadas con realizaciones concretas.

En la realización, el móvil 43 es un teléfono móvil u otro terminal móvil de internet. El módulo 41 de defensa se materializa a través de software, y se ejecuta en forma de una aplicación del terminal móvil 43.

En primer lugar, se inicializa el módulo 41 de defensa y el mismo crea un historial de valores *hash* para almacenar información de paquetes SYN del TCP. En segundo lugar, el terminal móvil 43 realiza una comprobación de tipo de protocolo y proporciona en consecuencia un procesado diferente a tipos diferentes de protocolo. Cuando recibe un paquete de tipo de protocolo TCP, el terminal móvil 43 lleva a cabo las etapas anteriores.

Tal como indica la Fig. 4, el lado solicitante 44 de conexión establece una conexión con el módulo 41 de defensa basándose en el principio de tres tomas de contacto del TCP, y el módulo 41 de defensa envía un paquete SYN al terminal móvil 43 como lado solicitante 44 de conexión, cuyo número SEQ es igual al del paquete SYN enviado por el lado solicitante 41 de conexión al módulo 41 de defensa. Definimos el paquete SYN enviado desde el lado solicitante 44 de conexión al módulo 41 de defensa como primer paquete SYN, y el paquete SYN enviado desde el lado solicitante 44 de conexión al terminal móvil 43 como segundo paquete SYN que es procesado por la pila 42 de protocolos TCP/IP del terminal móvil 43. Para facilitar el procesado del segundo paquete SYN por la pila 42 de protocolos TCP/IP, el módulo 41 de defensa establece en el segundo paquete SYN una etiqueta que significa datos contenidos. La etiqueta significa que el paquete SYN ha sido procesado por el módulo 41 de defensa y contiene datos. Los primeros 4 bytes de la etiqueta significan que el paquete SYN ha sido procesado (por ejemplo, el contenido de los 4 primeros bytes puede ser 0x123456), y los segundos 4 bytes significan contenido del paquete, el cual es el número SEQ del paquete SYN+ACK que el módulo 41 de defensa envía al lado solicitante 44 de conexión, es decir, el número SEQ del primer paquete SYN+ACK definido como Y. Cuando recibe el segundo paquete SYN, la pila de protocolos TCP/IP extrae el número SEQ y el número ACK del segundo paquete SYN basándose en la etiqueta que establece el módulo 41 de defensa, en donde el número SEQ del segundo paquete SYN se obtiene restando uno del número SEQ del primer paquete SYN+ACK. De esa manera los números SEQ del segundo y del primer paquetes SYN son iguales, lo cual le facilita al módulo 41 de defensa conectarse con el terminal móvil 43 como lado solicitante 44 de conexión. La pila de protocolos TCP/IP extrae el número SEQ Y del primer paquete SYN+ACK, que es idéntico a los datos del segundo paquete SYN basado en la etiqueta.

El protocolo TCP/IP 42 envía el segundo paquete SYN al terminal móvil 43 el cual responde con un paquete SYN+ACK definido como segundo paquete SYN+ACK. El segundo paquete SYN+ACK con un número SEQ definido como Z es procesado por la pila 42 de protocolos TCP/IP. La pila 42 de protocolos TCP/IP extrae el número SEQ Z del segundo paquete SYN+ACK y resta el número SEQ Y del primer paquete SYN+ACK con respecto al número SEQ Z del segundo paquete SYN+ACK para obtener un valor diferencia R (R=Z-Y) de números SEQ. La pila 42 de protocolos TCP/IP modifica el número SEQ del segundo paquete SYN+ACK, es decir, restando el número SEQ del segundo paquete SYN+ACK con respecto al valor diferencia R de números SEQ, y envía el paquete SYN+ACK modificado al módulo 41 de defensa. El módulo 41 de defensa abandona el paquete SYN+ACK modificado y crea un paquete ACK definido como segundo paquete ACK. El número ACK del segundo paquete ACK es el número SEQ del paquete SYN+ACK modificado más uno. El módulo 41 de defensa envía el paquete ACK a la pila 42 de protocolos TCP/IP para su procesado. La pila 42 de protocolos TCP/IP modifica el segundo paquete ACK, es decir, sumando el valor diferencia R de números SEQ al número ACK del paquete ACK, y el número SEQ del segundo paquete ACK modificado es (Z-R+1) +R=Z+1. El número SEQ del segundo paquete ACK modificado y recibido por el terminal móvil 43 es igual al número SEQ del segundo paquete SYN+ACK más 1. Por lo tanto, el módulo 41 de defensa realiza satisfactoriamente una toma de contacto triple con el terminal móvil 43 como lado solicitante 44 de conexión, y, a través del módulo 41 de defensa, se crea una conexión fiable entre la red externa del lado solicitante 44 de conexión y el terminal móvil 43.

Después de que se haya establecido la conexión entre el lado solicitante 44 de conexión y el terminal móvil 43, la pila 42 de protocolos TCP/IP modifica el número ACK del paquete TCP que envía el lado solicitante 44 de conexión y el número SEQ del paquete ACK con el que responde el terminal móvil 43, y suma el valor diferencia de los números SEQ al número ACK del paquete TCP que envía el lado solicitante 44 de conexión, restando al mismo tiempo el valor diferencia de los números SEQ con respecto al número SEQ del paquete ACK con el que responde el terminal móvil 43 para evitar el DoS.

En el proceso antes mencionado, el terminal móvil 43 cuenta el número de los paquetes SYN recibidos y decide si el terminal móvil 43 es atacado por DoS a partir del TCP comprobando los números de paquete SYN y paquetes con solamente SYN pero sin ACK dentro de un periodo de tiempo. Por ejemplo, contando el número de paquetes SYN actuales en cada 3 segundos incluyendo aquellos que envían solamente paquetes SYN pero no paquetes ACK. Cuando el número de paquetes SYN actuales es menor que 100, el terminal móvil 43 está funcionando de forma normal; cuando el número de paquetes SYN actuales es mayor que 100 y menor que 300, el terminal móvil 43 está en un estado de riesgo moderado; cuando el número de paquetes SYN actuales es mayor que 300, el terminal móvil 43 está en un estado de riesgo. Independientemente de en qué estado se encuentre, si una dirección IP dada envía cinco paquetes SYN sin enviar ningún paquete ACK, esta dirección se considera como dirección atacante, y el paquete será abandonado directamente para evitar un ataque DoS.

Normalmente el terminal móvil 43 procesa todos los paquetes SYN. No obstante, en un estado de riesgo, puesto que

el terminal móvil 43 está ocupado con el procesado de datos, es muy probable que el paquete sea abandonado directamente. En esos momentos únicamente se procesan paquetes recibidos y el número de los paquetes SYN que envía cada dirección es menor que 5, si no el paquete será abandonado. Cuando el terminal móvil 43 se encuentra en un estado de riesgo moderado, en otras palabras el número de paquetes SYN que envía el lado solicitante 44 de conexión está en un intervalo predeterminado de [100,300] tal como se ha mencionado anteriormente, únicamente se procesaron los paquetes SYN que no dejan ningún registro en el historial de valores *hash*. El procesado incluye extraer un puerto de origen, una dirección de origen, un puerto de destino y una dirección de destino contenidos en los datos SYN; marcar con *hash* esos cuatro valores y almacenarlos en el historial de valores *hash*. Si el terminal móvil 43 se encuentra en un estado de riesgo, el paquete es abandonado directamente.

En el proceso antes mencionado, la pila de protocolos TCP/IP busca una tabla de encaminamiento para decidir si el destino del segundo paquete SYN es el terminal móvil 43 ó el equipo de red del terminal móvil 43. Cuando el terminal móvil 43 es un punto caliente de red, el dispositivo de LAN enlazado por debajo de terminal móvil 43 establece una conexión fiable con la red externa usando el terminal móvil 43 como punto de transferencia de datos.

La realización anterior ilustra principalmente el escenario en el que el tipo de paquete que envía el lado solicitante 44 de conexión es del protocolo TCP. Cuando el tipo de paquete que envía el lado solicitante 44 de conexión al terminal móvil 43 es del protocolo ICMP o UDP, el terminal móvil 43 contará el número de paquetes ICMP o UDP recibidos para decidir si existe un ataque a la red. El número limitado de paquete ICMP se establece como un quinto valor predeterminado, y el número limitado de paquetes UDP se establece como un sexto valor predeterminado. Cuando el número de paquetes ICMP supera el quinto valor predeterminado o el número de paquetes UDP supera el sexto valor predeterminado, se controla el número de paquetes ICMP o UDP a recibir. Por ejemplo, el quinto valor predeterminado es 100, y el sexto valor predeterminado es 200; si se predetermina que únicamente se pueden recibir 100 paquetes ICMP y 200 paquetes UDP cada segundo, cuando se superan los valores predeterminados, el excedente de paquetes ICMP o UDP será abandonado directamente.

El terminal móvil 43 es, en la presente invención, un terminal de comunicaciones tal como un teléfono móvil o un ordenador tipo tableta.

El método de procesado de paquetes de la presente invención preestablece un módulo de defensa que evita un DoS en el terminal móvil. El lado solicitante de conexión establece una conexión con el módulo de defensa de acuerdo con el principio de tres tomas de contacto del TCP, y el módulo de defensa envía un paquete SYN al terminal móvil como lado solicitante de conexión. Cuando el módulo de defensa realiza una toma de contacto satisfactoria con el terminal móvil, se crea la conexión entre el lado solicitante de conexión y el terminal móvil, de manera que puede evitarse eficazmente un ataque DoS, especialmente un ataque SYN. Cuando los terminales móviles, especialmente teléfonos móviles, son un punto caliente de la red, se puede evitar eficazmente un ataque sobre un terminal móvil interno desde una red externa.

La presente invención se ha descrito en referencia a ciertas realizaciones preferidas y alternativas las cuales están destinadas únicamente a ser ejemplificativas y no se limitan al alcance completo de la presente invención según se expone en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para procesado de paquetes, comprendiendo el método:

cuando se recibe un primer paquete de toma de contacto (SYN) de solicitud de conexión desde un lado solicitante (24) de conexión, establecer un primer paquete de acuse de recibo de toma de contacto (SYN-ACK) usando un módulo (21) de defensa de un dispositivo electrónico (20), y responder al lado solicitante (24) de conexión enviando el primer paquete de acuse de recibo de toma de contacto al lado solicitante (24) de conexión;

cuando se recibe un primer paquete de acuse de recibo (ACK) desde el lado solicitante (24) de conexión, crear un segundo paquete de toma de contacto con el mismo número SEQ y el mismo número ACK que el primer paquete de toma de contacto, y enviar el segundo paquete de toma de contacto a un módulo (23) de procesado de paquetes del dispositivo electrónico (20) a través de una pila (22) de protocolos del protocolo de control de transmisión/protocolo de internet (TCP/IP), en donde el segundo paquete de toma de contacto comprende un número SEQ Y del primer paquete de acuse de recibo de toma de contacto;

recibir un segundo paquete de acuse de recibo de toma de contacto desde el módulo (23) de procesado de paquetes a través de la pila (22) de protocolos TCP/IP, y modificar un número SEQ Z del segundo paquete de acuse de recibo de toma de contacto al número SEQ Y del primer paquete de acuse de recibo de toma de contacto, y enviar el segundo paquete modificado de acuse de recibo de toma de contacto al módulo (21) de defensa, al mismo tiempo almacenando un valor diferencia R de números SEQ, en donde R=Z-Y;

cuando se recibe el segundo paquete modificado de acuse de recibo de toma de contacto, establecer un segundo paquete de acuse de recibo con un número ACK Y+1 usando el módulo (21) de defensa, y enviar el segundo paquete de acuse de recibo a la pila (22) de protocolos TCP/IP; y

en función del valor diferencia R de números SEQ, modificar el número ACK del segundo paquete de acuse de recibo a Z+1 a través de la pila (22) de protocolos TCP/IP, y enviar el segundo paquete de acuse de recibo modificado al módulo (23) de procesado de paquetes, de manera que la toma de contacto entre el módulo (21) de defensa y el módulo (23) de procesado de paquetes se produce con éxito, y se crea una conexión entre el lado solicitante (24) de conexión y el módulo (23) de procesado de paquetes;

en función del número de los primeros paquetes de toma de contacto a procesar por el módulo (21) de defensa, averiguar si se deben procesar nuevos primeros paquetes de toma de contacto, en donde los primeros paquetes de toma de contacto a procesar son los primeros paquetes de toma de contacto que no reciben primeros paquetes de acuse de recibo correspondientes;

caracterizado por que

si el número de los primeros paquetes de toma de contacto a procesar es igual o inferior a un primer valor predeterminado, el módulo (21) de defensa procesa los nuevos primeros paquetes de toma de contacto;

si el número de los primeros paquetes de toma de contacto a procesar es mayor que el primer valor predeterminado e igual o inferior a un segundo valor predeterminado, el módulo (21) de defensa procesa los primeros paquetes de toma de contacto no registrados, en donde los primeros paquetes de toma de contacto no registrados son los primeros paquetes de toma de contacto sin ninguna información de paquete registrada en el módulo (21) de defensa;

si el número de los primeros paquetes de toma de contacto a procesar es mayor que el segundo valor predeterminado, el módulo (21) de defensa no procesa los nuevos primeros paquetes de toma de contacto.

2. El método de la reivindicación 1, caracterizado por que el método comprende, además:

cuando se establece la conexión entre el lado solicitante (24) de conexión y el módulo (23) de procesado de paquetes, recibir un paquete desde el lado solicitante (24) de conexión usando la pila (22) de protocolos TCP/IP, y modificar un número ACK A del paquete a A+R, y enviar el paquete modificado al módulo (23) de procesado de paquetes; y

recibir un paquete de acuse de recibo desde el módulo (23) de procesado de paquetes usando la pila (22) de protocolos TCP/IP, y modificar un número SEQ B del paquete de acuse de recibo a B-R, y enviar el paquete de acuse de recibo modificado al lado solicitante (24) de conexión.

3. El método de la reivindicación 1, caracterizado por que se establece un historial de valores *hash* en el módulo (21) de defensa, si la información de paquete de los nuevos primeros paquetes de toma de contacto no está registrada en el historial de valores *hash*, el módulo (21) de defensa procesa los nuevos primeros paquetes de toma de contacto.

4. El método de la reivindicación 1, caracterizado por que el número de los primeros paquetes de toma de contacto a procesar con una dirección IP dada es mayor que un cuarto valor predeterminado, el módulo (21) de defensa

abandona la conexión de datos correspondiente de los primeros paquetes de toma de contacto a procesar.

5. Método de la reivindicación 1, caracterizado por que la pila (22) de protocolos TCP/IP decide si el destino del segundo paquete de acuse de recibo es el módulo (23) de procesado de paquetes del dispositivo electrónico (20) o un dispositivo de red conectado con el dispositivo electrónico (20) de acuerdo con una tabla de encaminamiento.

6. Un dispositivo electrónico (20) que comprende:

uno o más procesadores;

una memoria;

uno o más programas almacenados en la memoria, que son ejecutados por el procesador o procesadores para llevar a cabo un método de procesado de paquetes, comprendiendo el programa o programas un módulo (21) de defensa, una pila (22) de protocolos TCP/IP y un módulo (23) de procesado de paquetes;

cuando se recibe un primer paquete de toma de contacto (SYN) de solicitud de conexión desde un lado solicitante (24) de conexión, el módulo (21) de defensa establece un primer paquete de acuse de recibo de toma de contacto (SYN-ACK), y responde al lado solicitante (24) de conexión enviando el primer paquete de acuse de recibo de toma de contacto al lado solicitante (24) de conexión;

cuando se recibe un primer paquete de acuse de recibo (ACK) desde el lado solicitante (24) de conexión, el módulo (21) de defensa crea un segundo paquete de toma de contacto con el mismo número SEQ y el mismo número ACK que el primer paquete de toma de contacto, y envía el segundo paquete de toma de contacto al módulo (23) de procesado de paquetes a través de una pila (22) de protocolos del protocolo de control de transmisión/protocolo de internet (TCP/IP), en donde el segundo paquete de toma de contacto comprende un número SEQ Y del primer paquete de acuse de recibo de toma de contacto;

la pila (22) de protocolos TCP/IP recibe un segundo paquete de acuse de recibo de toma de contacto desde el módulo (23) de procesado de paquetes a su través, y modifica un número SEQ Z del segundo paquete de acuse de recibo de toma de contacto al número SEQ Y del primer paquete de acuse de recibo de toma de contacto, y envía el segundo paquete modificado de acuse de recibo de toma de contacto al módulo (21) de defensa, al mismo tiempo almacenando un valor diferencia R de números SEQ, en donde R=Z-Y;

cuando se recibe el segundo paquete modificado de acuse de recibo de toma de contacto, el módulo (21) de defensa establece un segundo paquete de acuse de recibo con un número ACK Y+1, y envía el segundo paquete de acuse de recibo a la pila (22) de protocolos TCP/IP; y

la pila (22) de protocolos TCP/IP modifica el número ACK del segundo paquete de acuse de recibo a Z+1 en función del valor diferencia R de números SEQ, y envía el segundo paquete de acuse de recibo modificado al módulo (23) de procesado de paquetes, de manera que la toma de contacto entre el módulo (21) de defensa y el módulo (23) de procesado de paquetes se produce con éxito, y se crea una conexión entre el lado solicitante (24) de conexión y el módulo (23) de procesado de paquetes;

el módulo (21) de defensa determina si se deben procesar nuevos primeros paquetes de toma de contacto en función del número de los primeros paquetes de toma de contacto a procesar, en donde los primeros paquetes de toma de contacto a procesar son los primeros paquetes de toma de contacto que no reciben primeros paquetes de acuse de recibo correspondientes;

caracterizado por que

si el número de los primeros paquetes de toma de contacto a procesar es igual o inferior a un primer valor predeterminado, el módulo (21) de defensa procesa los nuevos primeros paquetes de toma de contacto;

si el número de los primeros paquetes de toma de contacto a procesar es mayor que el primer valor predeterminado e igual o inferior a un segundo valor predeterminado, el módulo (21) de defensa procesa los primeros paquetes de toma de contacto no registrados, en donde los primeros paquetes de toma de contacto no registrados son los primeros paquetes de toma de contacto sin ninguna información de paquete registrada en el módulo (21) de defensa;

si el número de los primeros paquetes de toma de contacto a procesar es mayor que el segundo valor predeterminado, el módulo (21) de defensa no procesa los nuevos primeros paquetes de toma de contacto.

7. El dispositivo electrónico (20) de la reivindicación 6, caracterizado por que

cuando se establece la conexión entre el lado solicitante (24) de conexión y el módulo (23) de procesado de paquetes, la pila (22) de protocolos TCP/IP recibe un paquete desde el lado solicitante (24) de conexión, y modifica un número ACK A del paquete a A+R, y envía el paquete modificado al módulo (23) de procesado de paquetes; y

la pila (22) de protocolos TCP/IP recibe un paquete de acuse de recibo desde el módulo (23) de procesado de paquetes, y modifica un número SEQ B del paquete de acuse de recibo a B-R, y envía el paquete de acuse de recibo modificado al lado solicitante (24) de conexión.

8. El dispositivo electrónico (20) de la reivindicación 6, caracterizado por que se establece un historial de valores *hash* en el módulo (21) de defensa, si la información de paquete de los nuevos primeros paquetes de toma de contacto no está registrada en el historial de valores *hash*, el módulo (21) de defensa procesa los nuevos primeros paquetes de toma de contacto.

9. El dispositivo electrónico (20) de la reivindicación 6, caracterizado por que el número de los primeros paquetes de toma de contacto a procesar con una dirección IP dada es mayor que un cuarto valor predeterminado, el módulo (21) de defensa abandona la conexión de datos correspondiente de los primeros paquetes de toma de contacto a procesar.

10. El dispositivo electrónico (20) de la reivindicación 6, caracterizado por que la pila (22) de protocolos TCP/IP decide si el destino del segundo paquete de acuse de recibo es el módulo (23) de procesado de paquetes del dispositivo electrónico (20) o un dispositivo de red conectado con el dispositivo electrónico (20) de acuerdo con una tabla de encaminamiento.

11. Un medio de almacenamiento que almacena instrucciones ejecutadas por un procesador para llevar a cabo un método de procesado de paquetes, caracterizado por que el método comprende:

cuando se recibe un primer paquete de toma de contacto (SYN) de solicitud de conexión desde un lado solicitante (24) de conexión, establecer un primer paquete de acuse de recibo de toma de contacto (SYN-ACK) usando un módulo (21) de defensa de un dispositivo electrónico (20), y responder al lado solicitante (24) de conexión enviando el primer paquete de acuse de recibo de toma de contacto al lado solicitante (24) de conexión;

cuando se recibe un primer paquete de acuse de recibo (ACK) desde el lado solicitante (24) de conexión, crear un segundo paquete de toma de contacto con el mismo número SEQ y el mismo número ACK que el primer paquete de toma de contacto, y enviar el segundo paquete de toma de contacto a un módulo (23) de procesado de paquetes del dispositivo electrónico (20) a través de una pila de protocolos del protocolo de control de transmisión/protocolo de internet (TCP/IP), en donde el segundo paquete de toma de contacto comprende un número SEQ Y del primer pauete de acuse de recibo de toma de contacto;

recibir un segundo paquete de acuse de recibo de toma de contacto desde el módulo (23) de procesado de paquetes a través de la pila (22) de protocolos TCP/IP, y modificar un número SEQ Z del segundo paquete de acuse de recibo de toma de contacto al número SEQ Y del primer paquete de acuse de recibo de toma de contacto, y enviar el segundo paquete modificado de acuse de recibo de toma de contacto al módulo (21) de defensa, al mismo tiempo almacenando un valor diferencia R de números SEQ, en donde R=Z-Y;

cuando se recibe el segundo paquete modificado de acuse de recibo de toma de contacto, establecer un segundo paquete de acuse de recibo con un número ACK Y+1 usando el módulo (21) de defensa, y enviar el segundo paquete de acuse de recibo a la pila (22) de protocolos TCP/IP; y

en función del valor diferencia R de números SEQ, modificar el número ACK del segundo paquete de acuse de recibo a Z+1 a través de la pila (22) de protocolos TCP/IP, y enviar el segundo paquete de acuse de recibo modificado al módulo (23) de procesado de paquetes, de manera que la toma de contacto entre el módulo (21) de defensa y el módulo (23) de procesado de paquetes se produce con éxito, y se crea una conexión entre el lado solicitante (24) de conexión y el módulo (23) de procesado de paquetes;

en función del número de los primeros paquetes de toma de contacto a procesar por el módulo (21) de defensa, averiguar si se deben procesar nuevos primeros paquetes de toma de contacto, en donde los primeros paquetes de toma de contacto a procesar son los primeros paquetes de toma de contacto que no reciben primeros paquetes de acuse de recibo correspondientes;

caracterizado por que

si el número de los primeros paquetes de toma de contacto a procesar es igual o inferior a un primer valor predeterminado, el módulo (21) de defensa procesa los nuevos primeros paquetes de toma de contacto;

si el número de los primeros paquetes de toma de contacto a procesar es mayor que el primer valor predeterminado e igual o inferior a un segundo valor predeterminado, el módulo (21) de defensa procesa los primeros paquetes de toma de contacto no registrados, en donde los primeros paquetes de toma de contacto no registrados son los primeros paquetes de toma de contacto sin ninguna información de paquete registrada en el módulo (21) de defensa;

si el número de los primeros paquetes de toma de contacto a procesar es mayor que el segundo valor predeterminado, el módulo (21) de defensa no procesa los nuevos primeros paquetes de toma de contacto.

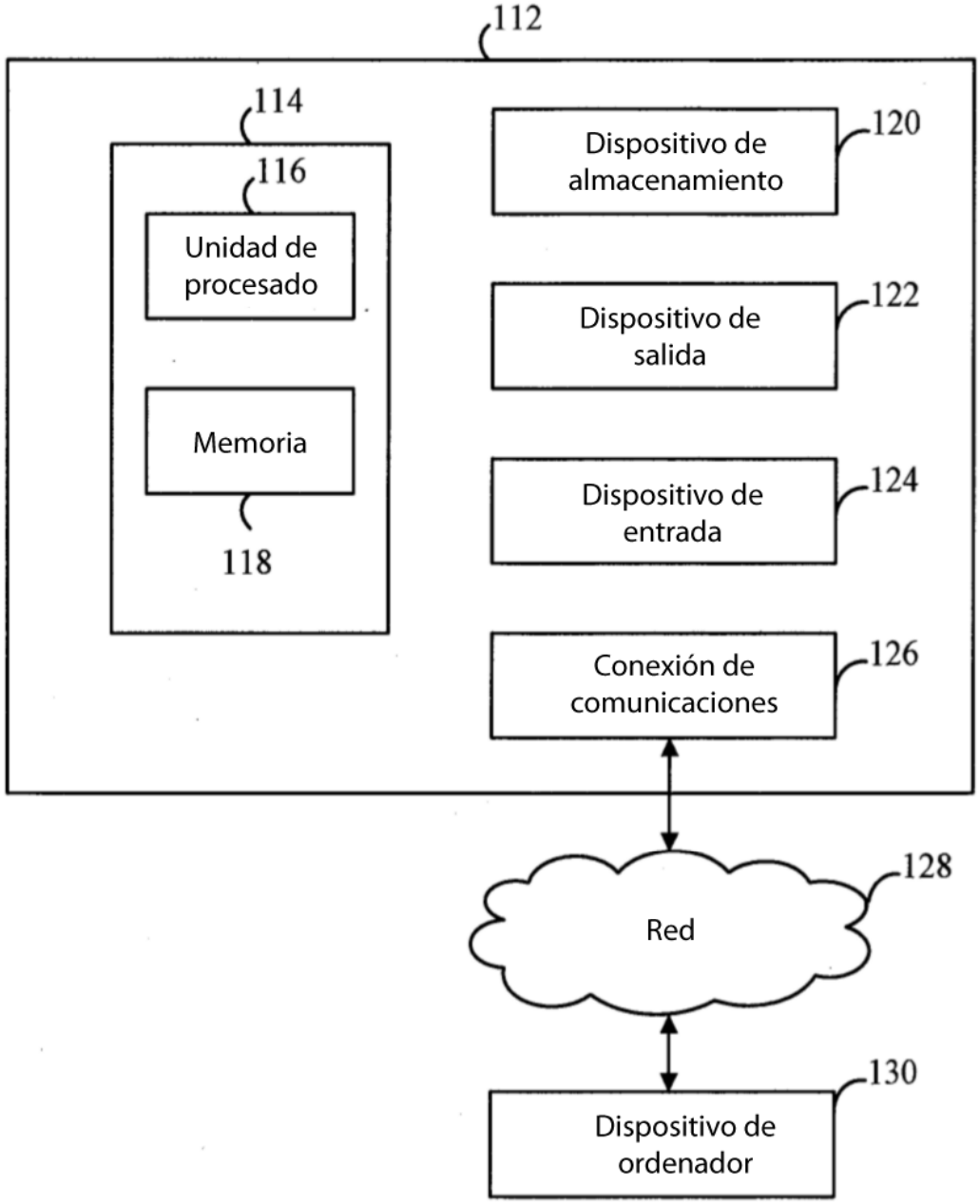
112
114
116
Unidad de procesado
Memoria
118
Dispositivo de almacenamiento
120
Dispositivo de salida
122
Dispositivo de entrada
124
Conexión de comunicaciones
126
Red
128
Dispositivo de ordenador
130

FIG. 1

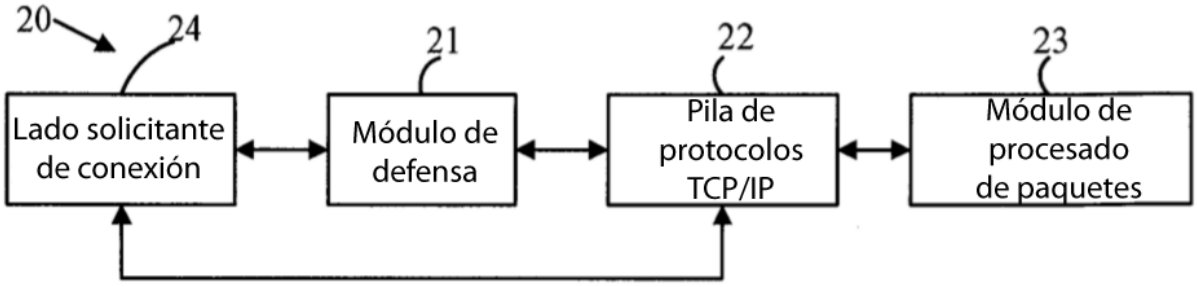
20
24
Lado solicitante de conexión
21
Módulo de defensa
22
Pila de protocolos TCP/IP
23
Módulo de procesado de paquetes

FIG. 2

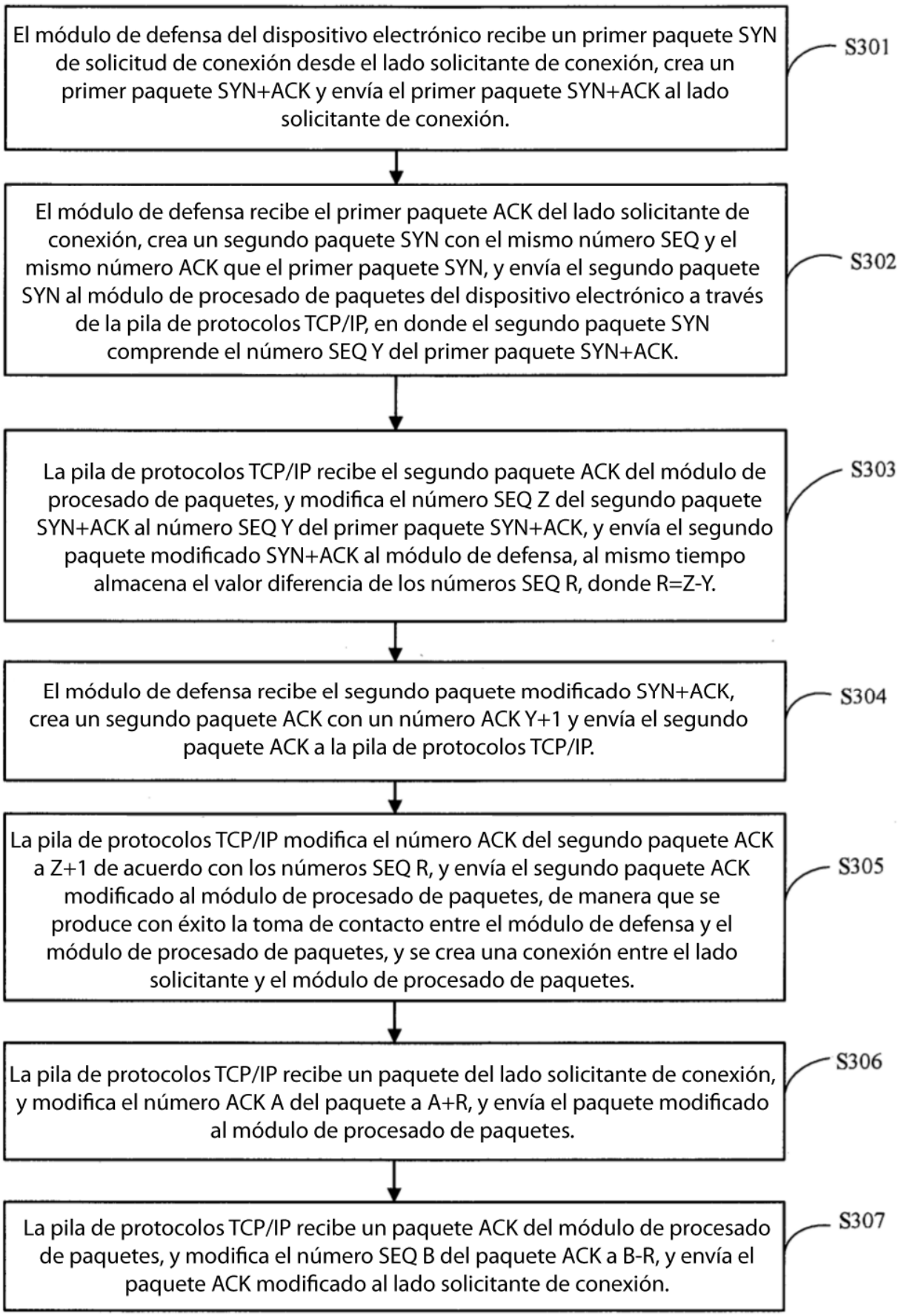
El módulo de defensa del dispositivo electrónico recibe un primer paquete SYN de solicitud de conexión desde el lado solicitante de conexión, crea un primer paquete SYN+ACK y envía el primer paquete SYN+ACK al lado solicitante de conexión.
S301
El módulo de defensa recibe el primer paquete ACK del lado solicitante de conexión, crea un segundo paquete SYN con el mismo número SEQ y el mismo número ACK que el primer paquete SYN, y envía el segundo paquete SYN al módulo de procesado de paquetes del dispositivo electrónico a través de la pila de protocolos TCP/IP, en donde el segundo paquete SYN comprende el número SEQ Y del primer paquete SYN+ACK.
S302
La pila de protocolos TCP/IP recibe el segundo paquete ACK del módulo de procesado de paquetes, y modifica el número SEQ Z del segundo paquete SYN+ACK al número SEQ Y del primer paquete SYN+ACK, y envía el segundo paquete modificado SYN+ACK al módulo de defensa, al mismo tiempo almacena el valor diferencia de los números SEQ R, donde R=Z-Y.
S303
El módulo de defensa recibe el segundo paquete modificado SYN+ACK, crea un segundo paquete ACK con un número ACK Y+1 y envía el segundo paquete ACK a la pila de protocolos TCP/IP.
S304
La pila de protocolos TCP/IP modifica el número ACK del segundo paquete ACK a Z+1 de acuerdo con los números SEQ R, y envía el segundo paquete ACK modificado al módulo de procesado de paquetes, de manera que se produce con éxito la toma de contacto entre el módulo de defensa y el módulo de procesado de paquetes, y se crea una conexión entre el lado solicitante y el módulo de procesado de paquetes.
S305
La pila de protocolos TCP/IP recibe un paquete del lado solicitante de conexión, y modifica el número ACK A del paquete a A+R, y envía el paquete modificado al módulo de procesado de paquetes.
S306
La pila de protocolos TCP/IP recibe un paquete ACK del módulo de procesado de paquetes, y modifica el número SEQ B del paquete ACK a B-R, y envía el paquete ACK modificado al lado solicitante de conexión.
S307

FIG. 3

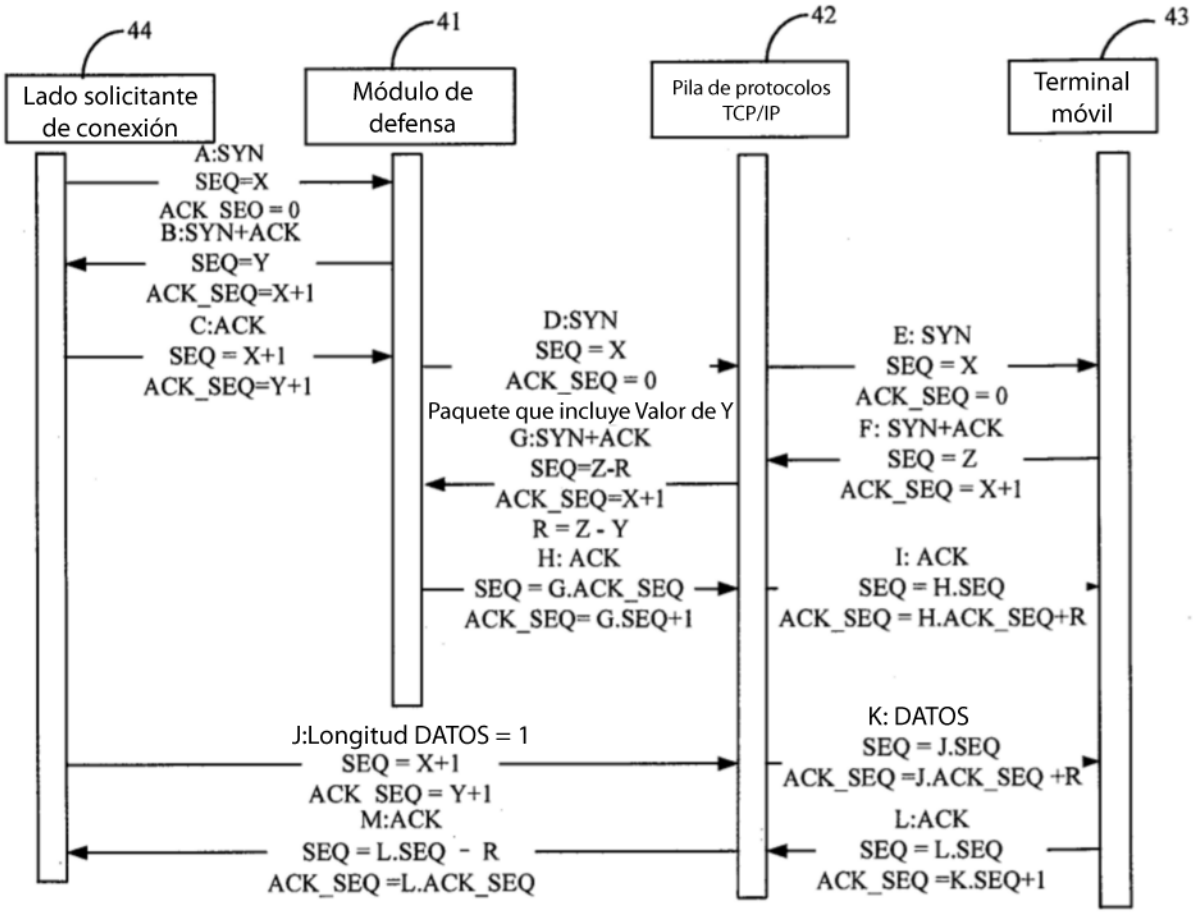
44
Lado solicitante de conexión
41
Módulo de defensa
42
Pila de protocolos TCP/IP
43
Terminal móvil
A:SYN
SEQ=X
ACK_SEO = 0
B:SYN+ACK
SEQ=Y
ACK_SEQ=X+1
C:ACK
SEQ = X+1
ACK_SEQ=Y+1
D:SYN
SEQ = X
ACK_SEQ = 0
Paquete que incluye Valor de Y
E: SYN
SEQ = X
ACK_SEQ = 0
F: SYN+ACK
SEQ = Z
ACK_SEQ = X+1
G:SYN+ACK
SEQ=Z-R
ACK_SEQ=X+1
R = Z - Y
H: ACK
SEQ = G.ACK_SEQ
ACK_SEQ= G.SEQ+1
I: ACK
SEQ = H.SEQ
ACK_SEQ = H.ACK_SEQ+R
J:Longitud DATOS = 1
SEQ = X+1
ACK_SEQ = Y+1
K: DATOS
SEQ = J.SEQ
ACK_SEQ =J.ACK_SEQ +R
M:ACK
SEQ = L.SEQ - R
ACK_SEQ =L.ACK_SEQ
L:ACK
SEQ = L.SEQ
ACK_SEQ =K.SEQ+1

Fig. 4