(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 524 716**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.08.2009 E 09011173 (3)**

(97) Fecha y número de publicación de la concesión europea: **22.10.2014 EP 2161898**

(54) Título: **Procedimiento y sistema de defensa contra un ataque DDoS**

(30) Prioridad:

04.09.2008 KR 20080087234

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.12.2014

(73) Titular/es:

ESTSOFT CORPORATION ESTSOFT R&D CENTER (100.0%)
867-12 BONGCHEON 4-DONG GWANAK-GU
SEOUL 151-836, KR

(72) Inventor/es:

KIM, JANG-JOONG

(74) Agente/Representante:

ISERN JARA, Jorge

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento y sistema de defensa contra un ataque DDoS

ANTECEDENTES DE LA INVENCIÓN

Referencia cruzada con solicitudes relacionadas

Esta solicitud reivindica el beneficio de la solicitud de patente coreana n.º 10-2008-0087234, presentada el 4 de septiembre de 2008.

Campo de la invención

La presente invención se refiere a un procedimiento y sistema de defensa contra un ataque distribuido de denegación de servicio (DDoS).

Antecedentes de la técnica relacionada

Un ataque DDoS se refiere a que varios ordenadores funcionan al mismo tiempo y atacan un sitio web específico.

En mayor detalle, un ataque DDoS es un esquema para distribuir un programa de ataque de denegación de servicio (DoS) que puede inundar numerosos ordenadores centrales, interconectados a través de una red, con paquetes en los ordenadores centrales provocando que los ordenadores centrales generen un lento funcionamiento de la red y la parálisis del sistema en un sistema objetivo de ataques de manera integrada. El ataque DoS se refiere a todas las acciones que colapsan el hardware o el software de un sistema objetivo de ataques, generando así problemas en un sistema que tiene un funcionamiento normal. Los procedimientos de ataque que permiten una gran variedad de ataques y que pueden obtener resultados inmediatos y notables pueden incluir, por ejemplo, Smurf, Trinoo e inundación SYN. Si un pirata informático instala herramientas para atacar servicios en varios ordenadores con el fin de atacar un sitio web específico e inunda simultáneamente un sistema informático del sitio web objetivo con una gran cantidad de paquetes que no pueden ser procesados por el sistema informático, el funcionamiento de una red se ralentiza o el sistema informático queda colapsado.

La posibilidad de ataques a través de una red es cada vez mayor debido al aumento de los sistemas distribuidos y a la proliferación de Internet. Para proteger los sistemas contra la amenaza de posibles ataques, un sistema convencional se defiende contra un ataque DDoS a través de un control de red basado en una red principal.

Sin embargo, los dispositivos de seguridad convencionales son problemáticos ya que no pueden detectar ataques en un terminal agente de ataque y no pueden hacer frente al foco origen correspondiente de manera apropiada y eficaz, incluso si se detectan tales ataques.

El documento US 2006/0143709 A1 muestra un sistema para evitar el ataque a una red con un ordenador que usa un programa de protección. El programa de protección transfiere un agente a cada uno o más nodos de la red en respuesta a un ataque dirigido a la red.

El documento "*A novelty approach to detecting DDoS attacks at an early stage*" de Bin Xiao et al. en THE JOURNAL OF SUPERCOMPUTING, KLUWER ACADEMIC PUBLISHERS, BO, Vol. 36, n.º 3, 1 de junio de 2006, páginas 235 a 248, ISSN: 1573-0484, sugiere un procedimiento para detectar posibles ataques distribuidos de denegación de servicio. Este documento sugiere utilizar el hecho de que la mayoría de ataques DDoS utilizan el establecimiento de comunicación de tres vías descrito por el protocolo TCP para identificar los ataques.

RESUMEN DE LA INVENCIÓN

Por consiguiente, la presente invención se ha realizado en vista de los problemas anteriores que se producen en la técnica anterior, y es un objeto de la presente invención proporcionar un procedimiento de defensa contra un ataque DDoS que sea capaz de defender de manera eficaz contra un ataque DDoS.

Otro objeto de la presente invención es proporcionar un sistema de defensa contra un ataque DDoS que sea capaz de defender de manera eficaz contra un ataque DDoS.

Los objetos técnicos a conseguir por la presente invención no están limitados a los objetos mencionados anteriormente, y otros objetos técnicos que no se han mencionado anteriormente resultarán evidentes a los expertos en la técnica a partir de la siguiente descripción.

Para lograr los objetos anteriores se proporciona un procedimiento de defensa contra un ataque DDoS según la reivindicación 1 y un sistema de defensa contra un ataque DDoS según la reivindicación 5. Un aspecto de la presente invención comprende las etapas de que un servidor objetivo de ataques determine si está sufriendo un

ataque DDoS desde una pluralidad de terminales y, según el resultado de la determinación, informe a un servidor de control de que está sufriendo el ataque DDoS; que el servidor de control transmita un mensaje de prevención de ataque a la pluralidad de terminales; y que cada uno de la pluralidad de terminales que haya recibido el mensaje de prevención de ataque determine si está llevando a cabo el ataque DDoS y bloquee el ataque DDoS según el resultado de la determinación.

Para conseguir los objetos anteriores, un procedimiento de defensa contra un ataque DDoS según otro aspecto de la presente invención comprende las etapas de que un servidor objetivo de ataques informe a un servidor de control de que está sufriendo el ataque DDoS desde una pluralidad de terminales; que el servidor de control transmita un mensaje de prevención de ataque a la pluralidad de terminales; y que cada uno de la pluralidad de terminales que haya recibido el mensaje de prevención de ataque bloquee el ataque DDoS.

En este caso, la etapa en la que el servidor objetivo de ataques determina si está sufriendo el ataque DDoS desde la pluralidad de terminales puede comprender las etapas de fijar la cantidad de datos que puede procesarse, determinar si la cantidad de datos que debe procesarse supera la cantidad fijada de datos y, si como resultado de la determinación se determina que la cantidad de datos que debe procesarse supera la cantidad fijada de datos, considerar los datos que deben procesarse como el ataque DDoS.

Además, la etapa en la que el servidor objetivo de ataques informa al servidor de control de que está sufriendo el ataque DDoS puede comprender la etapa de informar al servidor de control de que está sufriendo el ataque DDoS transmitiendo su propia información al servidor de control. La etapa en la que el servidor de control transmite el mensaje de prevención de ataque a la pluralidad de terminales puede comprender la etapa de confirmar la pluralidad de terminales que transmiten datos al servidor objetivo de ataques y transmitir el mensaje de prevención de ataques a la pluralidad de terminales confirmados.

Además, la información del servidor objetivo de ataques puede incluir información TCP/IP o UDP/IP.

El procedimiento puede comprender además la etapa de registrar la información del servidor objetivo de ataques con el servidor de control. En este caso, la etapa en la que el servidor objetivo de ataques informa al servidor de control de que está sufriendo el ataque DDoS puede comprender la etapa de, si el servidor objetivo de ataques determina que está sufriendo el ataque DDoS, informar al servidor de control de que está sufriendo el ataque DDoS enviando un comando acordado al servidor de control. La etapa en la que el servidor de control transmite el mensaje de prevención de ataque a la pluralidad de terminales puede comprender la etapa de que el servidor de control que ha recibido el comando acordado confirme la pluralidad de terminales, transmita datos al servidor objetivo de ataques y transmita el mensaje de prevención de ataque a la pluralidad de terminales confirmados.

Además, la etapa en la que cada uno de la pluralidad de terminales determina si está llevando a cabo el ataque DDoS puede comprender las etapas de, cuando se recibe el mensaje de prevención de ataque desde el servidor de control, determinar si está transmitiendo datos al servidor objetivo de ataques y, si como resultado de la determinación se determina que el terminal no transmite los datos al servidor objetivo de ataques, considerar los datos como el ataque DDoS.

Para conseguir los objetos anteriores, un sistema de defensa contra un ataque DDoS según otro aspecto adicional de la presente invención comprende una pluralidad de terminales, un servidor objetivo de ataques y un servidor de control acoplado a la pluralidad de terminales y al servidor objetivo de ataques. Aquí, el servidor objetivo de ataques determina si está sufriendo un ataque DDoS desde la pluralidad de terminales e informa al servidor de control de que está sufriendo el ataque DDoS según el resultado de la determinación. Si el servidor de control es informado de que el servidor objetivo de ataques está sufriendo el ataque DDoS, el servidor de control transmite un mensaje de prevención de ataque a la pluralidad de terminales. Cada uno de la pluralidad de terminales que haya recibido el mensaje de prevención de ataque determina si está llevando a cabo el ataque DDoS y bloquea el ataque DDoS según el resultado de la determinación.

Para conseguir los objetos anteriores, un sistema de defensa contra un ataque DDoS según otro aspecto adicional de la presente invención comprende una pluralidad de terminales, un servidor objetivo de ataques y un servidor de control acoplado a la pluralidad de terminales y al servidor objetivo de ataques. Aquí, cada uno de los terminales comprende un módulo de conexión configurado para acceder al servidor de control y para transmitir su propia información al servidor de control a intervalos predeterminados, un módulo de supervisión configurado para gestionar información de acceso del terminal al servidor de control y para determinar si se ha recibido una solicitud para evitar un ataque DDoS, y un módulo de bloqueo configurado para determinar si el terminal está llevando a cabo el ataque DDoS contra el servidor objetivo de ataques cuando se recibe un mensaje de prevención de ataque desde el servidor de control y para bloquear el ataque DDoS según el resultado de la determinación.

Para conseguir los objetos anteriores, un sistema de defensa contra un ataque DDoS según otro aspecto adicional de la presente invención comprende una pluralidad de terminales, un servidor objetivo de ataques y un servidor de control acoplado a la pluralidad de terminales y al servidor objetivo de ataques. Aquí, el servidor de control comprende un módulo de almacenamiento de información configurado para almacenar información acerca de la

pluralidad de terminales, un módulo de recepción configurado para recibir desde el servidor objetivo de ataques una solicitud de defensa contra un ataque DDoS, y un módulo de solicitud de defensa configurado para solicitar a una pluralidad de terminales que están transmitiendo datos al servidor objetivo de ataques que eviten el ataque DDoS.

Aquí, el que el módulo de bloqueo determine si el terminal está llevando a cabo el ataque DDoS contra el servidor objetivo de ataques puede comprender, cuando el mensaje de prevención de ataque se recibe desde el servidor de control, determinar si el terminal está transmitiendo datos al servidor objetivo de ataques y, si como resultado de la determinación se determina que el terminal no transmite los datos al servidor objetivo de ataques, considerar los datos como el ataque DDoS.

Además, la información del terminal puede comprender información TCP/IP o UDP/IP.

Los detalles de otras realizaciones están incluidos en la descripción detallada y en los dibujos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Objetos y ventajas adicionales de la invención podrán entenderse en mayor profundidad a partir de la siguiente descripción detallada tomada junto con los dibujos adjuntos, en los que:

la FIG. 1 es una vista explicativa que muestra un sistema de defensa contra un ataque DDoS según una realización de la presente invención;
la FIG. 2 es un diagrama de flujo que ilustra el sistema de defensa contra un ataque DDoS según una realización de la presente invención;
la FIG. 3 es un diagrama de bloques interno de un terminal que tiene un controlador de red instalado en el mismo según una realización de la presente invención; y
la FIG. 4 es un diagrama de bloques de un servidor de control según una realización de la presente invención.

<Descripción de números de referencia de los elementos principales de los dibujos>
100: atacante maestro; 110: servidor objetivo de ataques; 130: servidor de control; 135: módulo interno; 140 a 190: terminal; 120 a 125: controlador de red.

DESCRIPCIÓN DETALLADA DE LA REALIZACIÓN PREFERIDA

A continuación se describirá en detalle la presente invención en relación con realizaciones preferidas con referencia a los dibujos adjuntos.

Los méritos y las características de la presente invención, y los procedimientos para llevarlos a cabo, resultarán más evidentes a partir de las siguientes realizaciones tomadas junto con los dibujos adjuntos. Sin embargo, la presente invención no está limitada a las realizaciones dadas a conocer, sino que puede implementarse de varias maneras. Las realizaciones se proporcionan para completar la divulgación de la presente invención y para permitir que los expertos en la técnica entiendan el alcance de la presente invención. La presente invención está definida por la categoría de las reivindicaciones. Los mismos números de referencia se usarán a lo largo de los dibujos para hacer referencia a las mismas partes o a partes similares.

Debe entenderse que aunque los términos ‘primero’, ‘segundo’, etc. pueden usarse en el presente documento para describir varios dispositivos, elementos o secciones, los dispositivos, elementos o secciones no estarán limitados por estos términos. Estos términos solo se usan para distinguir un elemento de otro. Por ejemplo, un primer dispositivo, un primer elemento o una primera sección descritos en el presente documento podrían describirse como un segundo dispositivo, un segundo elemento o una segunda sección sin apartarse del alcance de la presente invención.

Las terminologías usadas en el presente documento solo tienen como objetivo describir realizaciones particulares y no pretenden limitar la presente invención. Tal y como se usa en el presente documento, las formas en singular pretenden incluir las formas en plural, a no ser que el contexto indique claramente lo contrario. Se entenderá además que los términos “comprende” o “que comprende”, cuando se usan en el presente documento, especifican la presencia de elementos, etapas, operaciones o dispositivos señalados, pero no excluyen la presencia o la adición de uno o más elementos, etapas, operaciones o dispositivos diferentes. Además, “A o B” se refiere a A, B, A y B. Además, los mismos números de referencia se usarán a lo largo de los dibujos para hacer referencia a las mismas partes o partes similares.

A no ser que se defina lo contrario, todos los términos (incluidos términos técnicos y científicos) usados en el presente documento pueden usarse con significados que pueden ser entendidos comúnmente por los expertos en la técnica. Además, los términos definidos en diccionarios generales no deben interpretarse de manera ideal o genérica, a no ser que se defina lo contrario.

Además, debe entenderse que combinaciones de bloques de procesamiento y de diagramas de flujo mostrados en los dibujos pueden ser llevadas a cabo mediante instrucciones de programa informático. Las instrucciones de

programa informático pueden introducirse en ordenadores de propósito general, ordenadores diseñados de manera especial o un procesador de otro equipo programable de procesamiento de datos. Las instrucciones ejecutadas por los ordenadores o el procesador de otro equipo programable de procesamiento de datos generan medios para ejecutar las funciones descritas en el (los) bloque(s) del diagrama de flujo. Las instrucciones de programa informático también pueden almacenarse en memorias disponibles para ordenadores o en memorias legibles por ordenador que pueden estar destinadas para un ordenador u otro equipo programable de procesamiento de datos con el fin de implementar las funciones de manera específica. Las instrucciones almacenadas en la memoria disponible para ordenador o en la memoria legible por ordenador también pueden usarse para producir artículos de producción que incluyen medios de instrucción para llevar a cabo las funciones descritas en el (los) bloque(s) del flujo de datos. Las instrucciones de programa informático también pueden introducirse en un ordenador u otro equipo programable de procesamiento de datos. Por tanto, las instrucciones que hacen funcionar al ordenador o al otro equipo programable de procesamiento de datos mediante la generación de un proceso ejecutado por un ordenador a través de una serie de etapas de funcionamiento llevadas a cabo en el ordenador u otro equipo programable de procesamiento de datos también pueden proporcionar etapas para ejecutar las funciones descritas en el (los) bloque(s) del diagrama de flujo.

La FIG. 1 es una vista explicativa que muestra un sistema de defensa contra un ataque DDoS según una realización de la presente invención.

Haciendo referencia a la FIG. 1, el sistema de defensa contra un ataque DDoS 1 según una realización de la presente invención incluye un atacante maestro 100, un servidor objetivo de ataques 110, un servidor de control 130 y una pluralidad de terminales 140 a 190.

El atacante maestro 100 determina el servidor objetivo de ataques 110 (es decir, un objetivo para el ataque) y usa uno o más terminales 140 a 190 para atacar al servidor objetivo de ataques 110 determinado.

El uno o más terminales 140 a 190 pueden llevar a cabo un ataque DDoS enviando una gran cantidad de datos al servidor objetivo de ataques 110 bajo el control del atacante maestro 100. Es decir, el uno o más terminales 140 a 190 transmiten, al servidor objetivo de ataques 110, una gran cantidad de datos que no pueden ser procesados por el servidor objetivo de ataques 110. Aquí, los datos pueden transmitirse en forma de, por ejemplo, un paquete.

El servidor objetivo de ataques 110 es un blanco que será atacado por el uno o más terminales 140 a 190.

En una realización de la presente invención, el servidor objetivo de ataques 110 puede determinar si está sufriendo un ataque DDoS y puede informar al servidor de control 130 de que está sufriendo el ataque DDoS según el resultado de la determinación.

En mayor detalle, la cantidad de datos que puede procesarse se fija previamente en el servidor objetivo de ataques 110. El servidor objetivo de ataques 110 puede determinar si la cantidad de datos que debe procesarse en este momento supera una cantidad predeterminada de datos en tiempo real. Si como resultado de la determinación se determina que la cantidad de datos que debe procesarse en este momento supera la cantidad predeterminada de datos, el servidor objetivo de ataques 110 puede determinar que está sufriendo un ataque DDoS. El servidor objetivo de ataques 110 informa al servidor de control 130 de que está sufriendo un ataque DDoS y solicita al servidor de control 130 que evite un ataque DDoS.

Un procedimiento del servidor objetivo de ataques 110 que solicita un ataque DDoS puede llevarse a cabo automáticamente por el servidor objetivo de ataques 110 cuando el servidor objetivo de ataques 110 determina que está sufriendo un ataque DDoS o puede llevarse a cabo manualmente por un administrador del servidor objetivo de ataques 110.

El servidor de control 130 recibe información acerca de la pluralidad de terminales 140 a 190, incluyendo información TCP/IP o UDP/IP de la pluralidad de terminales 140 a 190, e información de acceso de los terminales, incluyendo un puerto de acceso y un protocolo de acceso, y almacena la información. El servidor de control 130 controla o gestiona la pluralidad de terminales 140 a 190 o se comunica con la pluralidad de terminales 140 a 190 basándose en la información anterior.

Además, el servidor de control 130 determina si el servidor objetivo de ataques 110 ha solicitado impedir un ataque DDoS. Si como resultado de la determinación se determina que el servidor objetivo de ataques 110 ha solicitado impedir un ataque DDoS, el servidor de control 130 transmite un mensaje de prevención de ataque al uno o más terminales 140 a 190 que están transmitiendo datos al servidor objetivo de ataques 110. Dicho de otro modo, el servidor de control 130 solicita al uno o más terminales 140 a 190 que eviten un ataque DDoS.

En particular, controladores de red 120 a 125 pueden instalarse en la pluralidad de terminales respectivos 140 a 190. Los controladores de red 120 a 125 pueden implementarse mediante software o mediante hardware. Cada uno de los controladores de red 120 a 125, como se describe posteriormente con referencia a la FIG. 3, puede incluir un módulo de conexión 310, un módulo de supervisión 320 y un módulo de bloqueo 330.

Aquí, el servidor de control 130 confirma la pluralidad de terminales 140 a 190 que están transmitiendo datos al servidor objetivo de ataques 110 cuando los terminales 140 a 190 reciben el mensaje de prevención de ataque y transmite el mensaje de prevención de ataque a la pluralidad de terminales 140 a 190 según el resultado de la confirmación.

Cada uno de los usuarios de los terminales 140 a 190 que hayan recibido el mensaje de prevención de ataque determina si el terminal está transmitiendo datos al servidor objetivo de ataques 110. Si como resultado de la determinación se determina que el terminal está transmitiendo datos al servidor objetivo de ataques 110 aunque no haya ningún comando de transmisión de datos del usuario, el usuario considera los datos como un ataque DDoS. Un procedimiento para determinar si están transmitiéndose datos puede llevarse a cabo manualmente por un usuario o puede determinarse automáticamente por los terminales 140 a 190. El procedimiento de un usuario que determina manualmente si están transmitiéndose datos puede llevarse a cabo enviando contenidos que indican que no tiene intención de transmitir los datos, o una respuesta que indica que detendrá el ataque DDoS.

El uno o más terminales 140 a 190 que han determinado tal transmisión como un ataque DDoS bloquean el ataque DDoS. Un procedimiento para bloquear un ataque DDoS puede llevarse a cabo por los controladores de red 120 a 125 bloqueando la transmisión de datos hacia el servidor objetivo de ataques 110.

A continuación se describe en detalle, con referencia a las FIG. 1 y 2, un procedimiento para evitar un ataque DDoS. Resulta evidente que aunque, para simplificar la descripción, solo se describe el terminal 140 de la pluralidad de terminales 140 a 190 como un ejemplo con referencia a la FIG. 2, el procedimiento anterior puede aplicarse al resto de terminales 150 a 190.

La FIG. 2 es un diagrama de flujo que ilustra el procedimiento para evitar un ataque DDoS descrito con referencia a la FIG. 1. Aquí, información acerca del servidor objetivo de ataques 110 y del terminal 140 puede comprender información TCP/IP o UDP/IP.

Haciendo referencia a las FIG. 1 y 2, el servidor objetivo de ataques 110 determina si está sufriendo un ataque DDoS en la etapa S210.

En mayor detalle, un procedimiento del servidor objetivo de ataques 110 que determina si está sufriendo un ataque DDoS se lleva a cabo fijando la cantidad de datos que puede procesarse en este momento y determinando si la cantidad de datos que debe procesarse en este momento supera la cantidad fijada de datos en tiempo real.

La cantidad de datos puede basarse, por ejemplo, en la cantidad de paquetes. Por ejemplo, la cantidad de datos que puede procesarse puede ser 1518 octetos.

Si como resultado de la determinación se determina que la cantidad de datos que debe procesarse en este momento supera la cantidad fijada de datos, el servidor objetivo de ataques 110 los considera como un ataque DDoS y solicita al servidor de control 130 que evite un ataque DDoS manualmente o automáticamente.

En mayor detalle, en un procedimiento del servidor objetivo de ataques 110 que solicita evitar un ataque DDoS automáticamente, cuando la cantidad de datos que debe procesarse en este momento supera la cantidad fijada de datos, el servidor objetivo de ataques 110 transmite automáticamente información acerca del servidor objetivo de ataques 110, incluyendo su propia información TCP/IP, UDP/IP, un puerto o un protocolo al servidor de control 130.

Además, en un procedimiento del servidor objetivo de ataques 110 que solicita evitar un ataque DDoS manualmente, cuando la cantidad de datos que debe procesarse en este momento supera la cantidad fijada de datos, un administrador del servidor objetivo de ataques 110 confirma el servidor objetivo de ataques 110 y transmite manualmente información acerca del servidor objetivo de ataques 110, incluyendo un puerto y un protocolo del servidor objetivo de ataques 110, al servidor de control 130 a través del servidor objetivo de ataques 110.

Por otro lado, la información del servidor objetivo de ataques 110 puede almacenarse de antemano en el servidor de control 130. En este caso, si la recepción de datos se considera un ataque DDoS, el servidor objetivo de ataques 110 solicita al servidor de control 130 que evite un ataque DDoS enviando un comando acordado al servidor de control 130 cuando la cantidad de datos que debe procesarse por el servidor objetivo de ataques 110 supera la cantidad fijada de datos.

Si como resultado de la determinación de la etapa S210 se determina que el servidor objetivo de ataques 110 está sufriendo un ataque DDoS, el servidor de control 130 transmite un mensaje de prevención de ataque al al menos un terminal 140 en la etapa S220.

Si se recibe una solicitud para evitar un ataque DDoS desde el servidor objetivo de ataques 110, el servidor de control 130 transmite el mensaje de prevención de ataque al al menos un terminal 140 que están transmitiendo

datos al servidor objetivo de ataques 110. En mayor detalle, el mensaje de prevención de ataque es información acerca del servidor objetivo de ataques 110 y puede incluir información acerca de un puerto y un protocolo.

El terminal 140 que ha recibido el mensaje de prevención de ataque determina en la etapa S230 si está llevándose a cabo un ataque DDoS basándose en el mensaje de prevención de ataque recibido.

Un usuario del terminal 140 determina si el terminal está transmitiendo datos al servidor objetivo de ataques 110 según su intención. Si el terminal 140 está transmitiendo datos al servidor objetivo de ataques 110 aunque el usuario del terminal 140 que ha recibido el mensaje de prevención de ataque no haya emitido ningún comando para transmitir los datos al servidor objetivo de ataques 110, el terminal considera los datos un ataque DDoS.

El terminal 140 que tiene el controlador de red 120 instalado en el mismo bloquea tal transmisión de datos de ataque DDoS usando el controlador de red 120 en la etapa S240.

Si se determina que tal transmisión de datos es un ataque DDoS, el terminal 140 que ha recibido el mensaje de prevención de ataque solicita bloquear tal transmisión de datos a través del controlador de red 120. El controlador de red 120 que ha recibido la solicitud para bloquear la transmisión de datos impide que el terminal 140 correspondiente transmita datos al servidor objetivo de ataques 110.

A continuación se describe, con referencia a las FIG. 3 y 4, construcciones a modo de ejemplo del terminal y del servidor de control. Aunque el terminal 140 de la pluralidad de terminales 140 a 190 se describe como un ejemplo para facilitar la descripción, resulta evidente que tal descripción puede aplicarse al resto de terminales 150 a 190.

La FIG. 3 es un diagrama de bloques interno del terminal 140 que tiene el controlador de red 120 instalado en el mismo, mostrado en la FIG. 1.

Haciendo referencia a la FIG. 3, el controlador de red 120 incluye el módulo de conexión 310, el módulo de supervisión 320 y el módulo de bloqueo 330.

El módulo de conexión 310 del controlador de red 120 transmite información del terminal 140 al servidor de control 130 a intervalos predeterminados. Aquí, el controlador de red 120 puede fijar los intervalos predeterminados a, por ejemplo, 3 meses o 6 meses.

En mayor detalle, la información del terminal 140 puede incluir, como se ha descrito anteriormente, información acerca del terminal 140, tal como información TCP/IP o UDP/IP del terminal 140, e información de acceso del terminal 140, tal como un puerto de acceso o un protocolo de acceso. El módulo de conexión 310 del servidor de control 130 almacena la información acerca del terminal 140 y la información de acceso del terminal 140 y controla al terminal 140 acoplado al servidor de control 130.

El módulo de supervisión 320 gestiona la información de acceso del terminal 140 y determina si se ha recibido una solicitud para evitar un ataque DDoS.

La información de acceso del terminal 140 incluye un puerto de acceso y un protocolo de acceso.

El módulo de bloqueo 330 impide que el terminal 140 transmita datos al servidor objetivo de ataques 110. Si el terminal 140 que está transmitiendo datos al servidor objetivo de ataques 110 recibe un mensaje de prevención de ataques desde el servidor de control 130, un usuario del terminal 140 determina si el terminal 140 está transmitiendo los datos al servidor objetivo de ataques 110 según su intención. Si, aunque el usuario del terminal 140 no tiene intención de transmitir los datos, se determina que el terminal 140 está transmitiendo los datos al servidor objetivo de ataques 110, el módulo de bloqueo 330 considera los datos como un ataque DDoS y bloquea tal transmisión de datos usando el controlador de red 120.

La FIG. 4 es un diagrama de bloques del servidor de control 130 mostrado en la FIG. 1.

Haciendo referencia a la FIG. 4, el módulo interno 135 del servidor de control 130 incluye un módulo de almacenamiento de información 410 para almacenar la información TCP/IP o UDP/IP del terminal 140, un módulo de recepción de solicitud de defensa contra ataques DDoS 420 y un módulo de solicitud de defensa contra ataques DDoS 430.

El módulo de almacenamiento de información 410 del servidor de control 130 almacena la información TCP/IP o UDP/IP del terminal 140.

El módulo de recepción de solicitud de defensa contra ataques DDoS 420 recibe una solicitud de prevención de ataque DDoS desde el servidor objetivo de ataques 110. La información de solicitud recibida incluye información del servidor objetivo de ataques 110, incluyendo un puerto y un protocolo del servidor objetivo de ataques 110.

Si se recibe una solicitud de prevención de ataque DDoS desde el servidor objetivo de ataques 110, el módulo de solicitud de defensa contra ataques DDoS 430 solicita al terminal 140 que está transmitiendo datos al servidor objetivo de ataques 110 y que tiene el controlador de red 120 instalado en el mismo que evite un ataque DDoS.

Cabe mencionar que las realizaciones anteriores de la presente invención pueden escribirse en forma de un programa que puede ser ejecutado por un ordenador y que puede implementarse en un ordenador digital de propósito general que ejecuta el programa usando un medio de grabación legible por ordenador.

El medio de grabación legible por ordenador puede incluir medios de grabación, tales como medios de grabación magnéticos (por ejemplo, una ROM, un disco flexible y un disco duro), medios de lectura ópticos (por ejemplo, un CD-ROM y un DVD) y ondas portadoras (por ejemplo, transmisión a través de Internet).

Aunque la presente invención se ha descrito con referencia a las realizaciones ilustrativas particulares, no está limitada por las realizaciones sino solamente por las reivindicaciones adjuntas.

REIVINDICACIONES

1.- Un procedimiento de defensa contra un ataque distribuido de denegación de servicio (DDoS), que comprende las etapas siguientes:

que un servidor objetivo de ataques (110) determine (S210) si el servidor objetivo de ataques está sufriendo el ataque DDoS desde una pluralidad de terminales (140, 150, 160, 170, 180, 190) e informe a un servidor de control (130) de que el servidor objetivo de ataques está sufriendo el ataque DDoS enviando información acerca del servidor objetivo de ataques, incluyendo su propia información TCP/IP o UDP/IP, al servidor de control basándose en el resultado de la determinación;
que el servidor de control que ha recibido la información acerca del servidor objetivo de ataques confirme que la pluralidad de terminales está transmitiendo datos al servidor objetivo de ataques, envíe datos al servidor objetivo de ataques y transmita (S220) un mensaje de prevención de ataque a la pluralidad de terminales confirmados;
que la pluralidad de terminales que hayan recibido el mensaje de prevención de ataque determinen si los terminales están enviando datos al servidor objetivo de ataques;
determinar, en función de información de un usuario de cualquiera de los terminales, si el terminal está transmitiendo datos al servidor objetivo de ataques según su intención;
si, aunque el usuario no haya emitido un comando para enviar los datos, se determina que el terminal está enviando los datos al servidor objetivo de ataques, que el terminal correspondiente determine que el envío de los datos es el ataque DDoS; y
que el terminal correspondiente que haya determinado que el envío de los datos es el ataque DDoS bloquee (S240) el envío de los datos al servidor objetivo de ataques.

2.- El procedimiento según la reivindicación 1, en el que la etapa en que el servidor objetivo de ataques determina si el servidor objetivo de ataques está sufriendo el ataque DDoS desde una pluralidad de terminales comprende las etapas de:

fijar una cantidad de datos que puede procesarse en el servidor objetivo de ataques;
determinar si una cantidad de datos que debe procesarse en el servidor objetivo de ataques supera la cantidad fijada de datos; y
si como resultado de la determinación se determina que la cantidad de datos que debe procesarse en el servidor objetivo de ataques supera la cantidad fijada de datos, considerar los datos que deben procesarse en el servidor objetivo de ataques como el ataque DDoS.

3.- El procedimiento según la reivindicación 1, en el que la información acerca del servidor objetivo de ataques comprende uno o más uno de entre información TCP/IP, información UDP/IP, un puerto y un protocolo del servidor objetivo de ataques.

4.- El procedimiento según la reivindicación 1, que comprende además la etapa de registrar la información acerca del servidor objetivo de ataques con el servidor de control,
donde la etapa en la que el servidor objetivo de ataques informa al servidor de control de que el servidor objetivo de ataques está sufriendo el ataque DDoS comprende la etapa de, si el servidor objetivo de ataques determina que el servidor objetivo de ataques está sufriendo el ataque DDoS, informar al servidor de control de que el servidor objetivo de ataques está sufriendo el ataque DDoS enviando un comando acordado al servidor de control, y
la etapa en la que el servidor de control envía el mensaje de prevención de ataque a la pluralidad de terminales comprende la etapa de que el servidor de control que ha recibido el comando acordado confirme la pluralidad de terminales que están enviando los datos al servidor objetivo de ataques y envíe el mensaje de prevención de ataque a la pluralidad de terminales confirmados.

5.- Un sistema de defensa contra un ataque DDoS, comprendiendo el sistema:

una pluralidad de terminales (140, 150, 160, 170, 180, 190);
un servidor objetivo de ataques (110); y
un servidor de control (130) acoplado a la pluralidad de terminales y al servidor objetivo de ataques,
donde el servidor de control comprende:

un módulo de recepción (420) configurado para recibir una solicitud para defender al servidor objetivo de ataques frente al ataque DDoS;
un módulo de solicitud de defensa (430) configurado para solicitar a la pluralidad de terminales, que están enviando datos al servidor objetivo de ataques, que eviten el ataque DDoS,

en el que cada uno de los terminales comprende:

un módulo de conexión (310) configurado para acceder al servidor de control y para transmitir su propia información al servidor de control a intervalos predeterminados;

un módulo de supervisión (320) configurado para gestionar información de acceso del terminal y para comprobar si se ha recibido una solicitud para evitar el ataque DDoS; y
un módulo de bloqueo (330) configurado para, cuando se recibe un mensaje de prevención de ataque desde el servidor de control, determinar si el terminal está enviando datos al servidor objetivo de ataques en función de información de un usuario del terminal; si como resultado de la determinación se determina que el terminal está enviando datos al servidor objetivo de ataques aunque el usuario del terminal no haya emitido un comando para enviar los datos, considerar que el envío de los datos es el ataque DDoS y bloquear el ataque DDoS.

6.- El sistema de defensa contra un ataque DDoS según la reivindicación 5, en el que el servidor de control comprende:

un módulo de almacenamiento de información (410) configurado para almacenar información acerca de los terminales e información de acceso de los terminales.

7.- El sistema según la reivindicación 6, en el que la información del terminal comprende información acerca del terminal e información de acceso del terminal.

Fig. 1

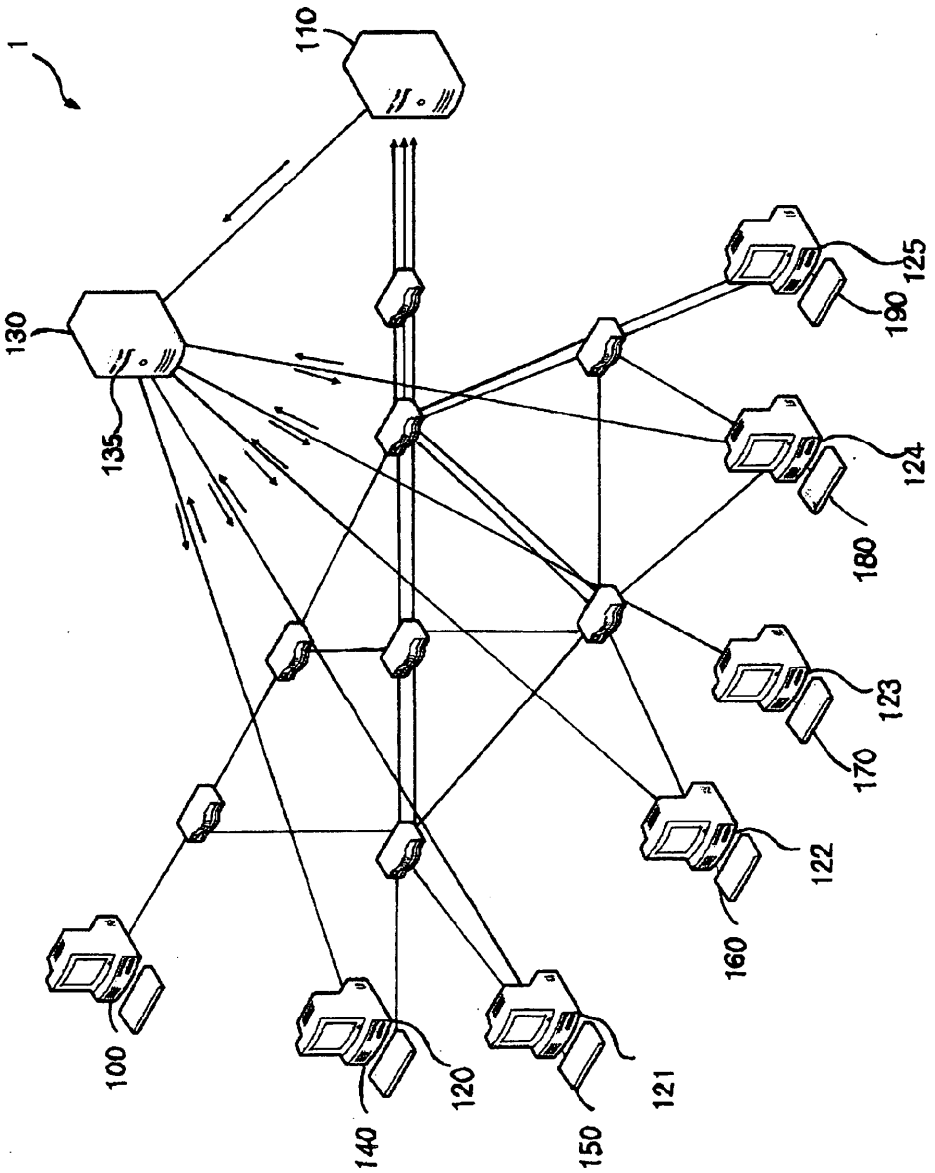


Fig. 2

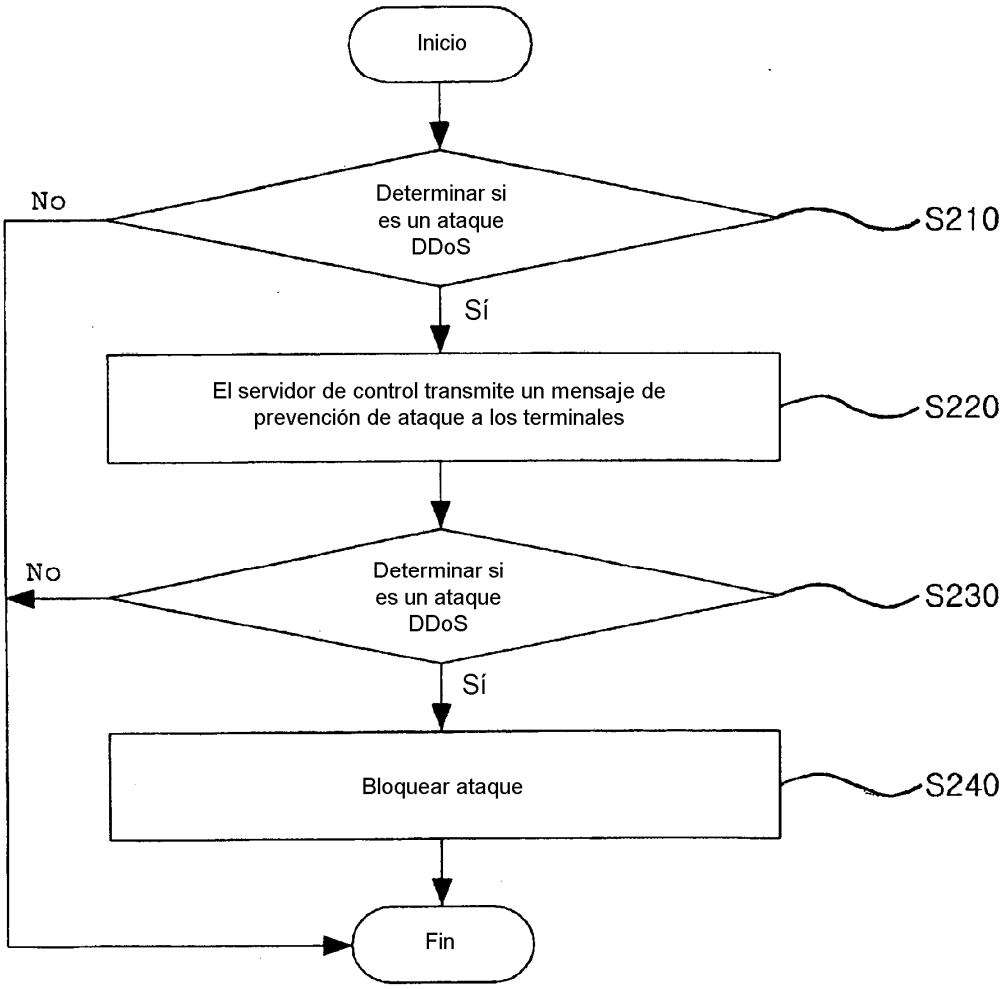

Inicio
Determinar si es un ataque DDoS
S210
No
Sí
El servidor de control transmite un mensaje de prevención de ataque a los terminales
S220
Determinar si es un ataque DDoS
S230
No
Sí
Bloquear ataque
S240
Fin

Fig. 3

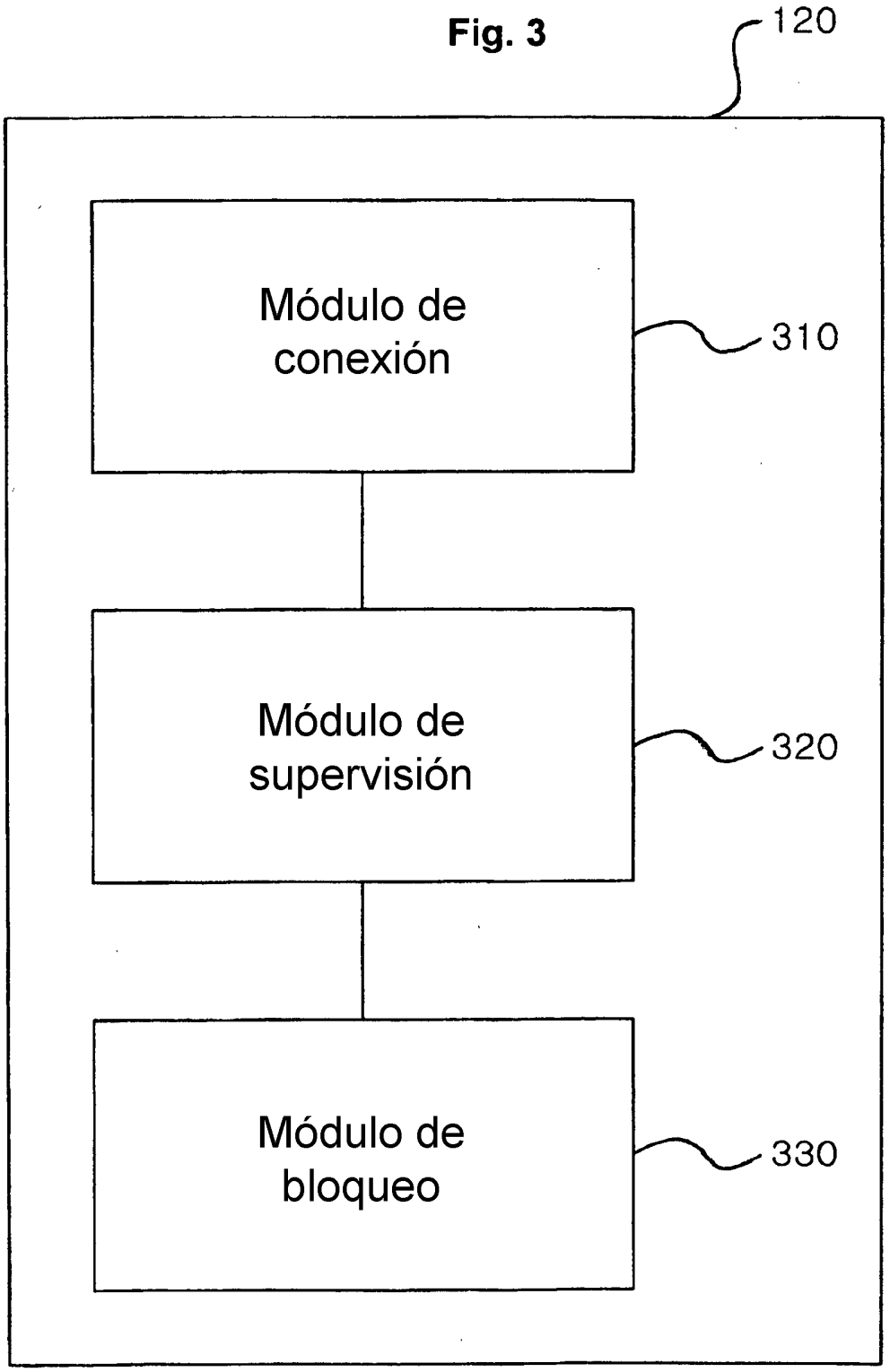
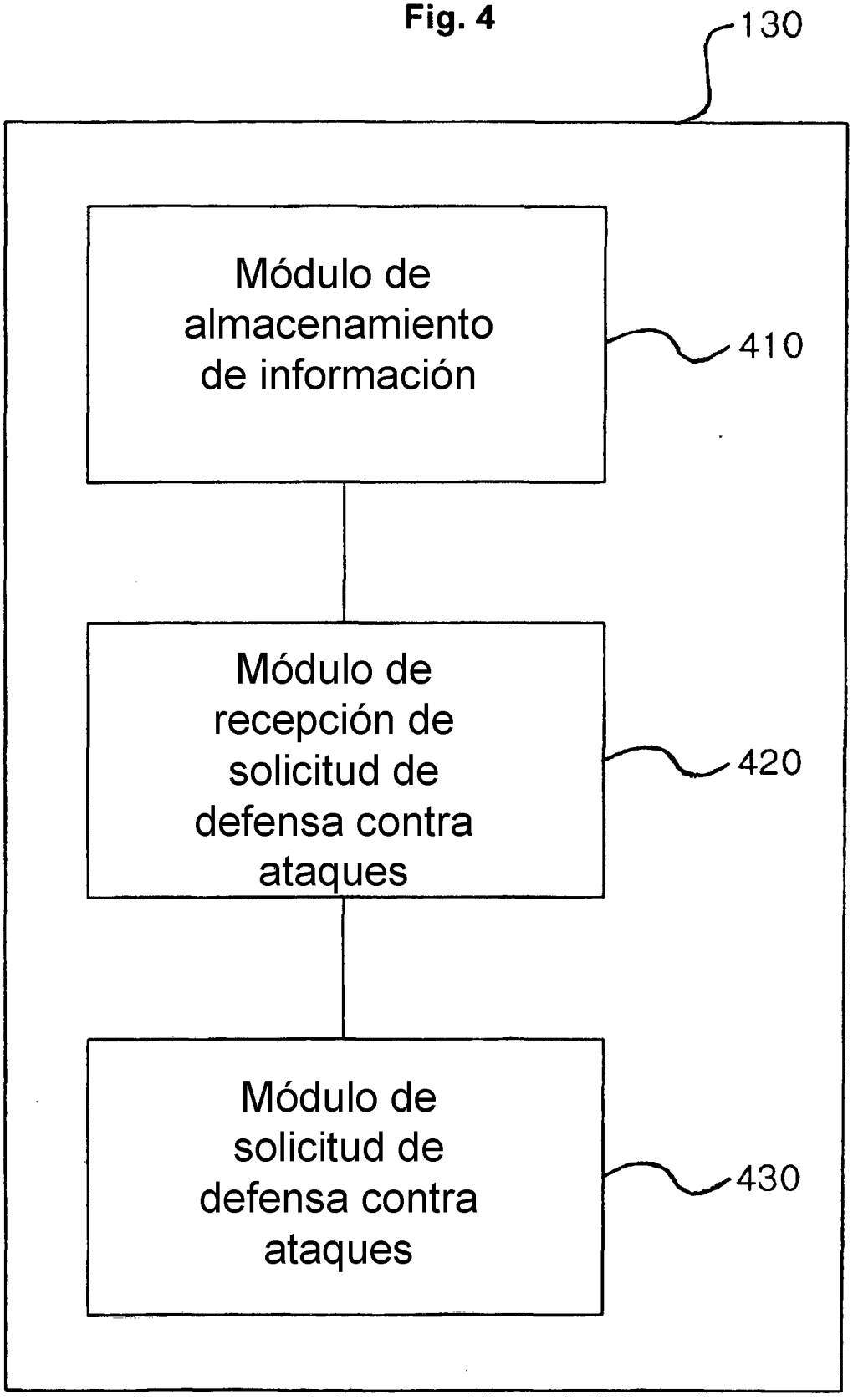

120
Módulo de conexión
310
Módulo de supervisión
320
Módulo de bloqueo
330

Fig. 4


130
Módulo de almacenamiento de información
410
Módulo de recepción de solicitud de defensa contra ataques
420
Módulo de solicitud de defensa contra ataques
430