(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 560 109**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.07.2011 E 11748600 (1)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2015 EP 2612481**

(54) Título: **Procedimiento y sistema de clasificación de tráfico**

(30) Prioridad:

03.09.2010 ES 201031320 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.02.2016

(73) Titular/es:

TELEFÓNICA, S.A. (100.0%)
Gran Vía, 28
28013 Madrid, ES

(72) Inventor/es:

AMAYA CALVO, ANTONIO MANUEL y
PÉREZ IGLESIAS, SANTIAGO

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y sistema de clasificación de tráfico

Campo de la invención

La presente invención se refiere al campo de la seguridad en las Tecnologías de la Información, más concretamente, se refiere a un nuevo procedimiento y sistema para la detección automática y la clasificación de los patrones generados por software malicioso en una red de comunicaciones.

Estado de la Técnica

El panorama actual de la seguridad en las Tecnologías de la Información es sombrío. Hoy en día, las amenazas contra la seguridad se incrementan rápidamente. Nuevas variantes de software malicioso (también llamado malware) se desarrollan y distribuyen continuamente. Se estima que solo en los últimos seis meses se ha desarrollado más malware que en el resto de la historia de la informática.

En la actualidad todos los aspectos de la experiencia de una red de comunicaciones son afectados por amenazas contra la seguridad, desde la calidad de la experiencia hasta la infraestructura de la red. De acuerdo con el último "Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles",8ª oleada, primer trimestre 2009. INTECO, octubre 2009 (versión española), aproximadamente el 44 % de los usuarios considera la seguridad una limitación principal a la hora de utilizar nuevos servicios.

A pesar de las fuertes inversiones efectuadas en antivirus, el malware es aún el número uno en lo que se refiere a problemas de seguridad:

- Mientras que más del 99 % de las organizaciones utilizan antivirus y el 98 % usan cortafuegos, el daño causado por el malware sobrepasa los 55 millones de dólares al año *[Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) 2004 Computer Crime and Security Survey http://www.gocsi.com/forms/csi_survey.jhtml].*

- Los incidentes relacionados con seguridad informática que ocupan el segundo lugar entre los más caros son aquellos relacionados con "*bots*" (programas o aplicaciones utilizadas para hacerse pasar por una persona en la red), donde la pérdida total media anual fue poco menos de 300.000 dólares *[Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) 2008 Computer Crime and Security Survey http://www.gocsi.com/forms/csi_survey.jhtml]*. Intentar controlar el problema directamente desde los sistemas afectados es una causa perdida:

- Más del 10 % de incremento en malware en el primer trimestre de 2009 (Fuente: PandaLabs)

- Mientras más del 91,2 % de los usuarios, encuestados en el estudio mencionado anteriormente "Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles", utilizan antivirus, el 63,8 % de ellos tienen al menos un programa malicioso en sus ordenadores. Esto significa que al menos el 84,32 % de los mismos tienen un antivirus completamente actualizado ejecutándose en su ordenador.

Casi todas las amenazas actuales tienen un punto en común: utilizan la red para coordinarse, distribuirse, infiltrarse, controlar y en última instancia beneficiarse.

La figura 1 muestra un esquema de alto nivel de la protección y los factores de mitigación que pueden ser utilizados para proteger a los usuarios, donde 15 representa el Origen o Controlador del Malware. Comprende:

- Protección en el Extremo 11, que define todas las protecciones que se pueden desplegar y ejecutar directamente en el ordenador del usuario.

- La Información de Seguridad y Gestión de Eventos (SIEM) 12, Detección de Intrusos (ID) 13 y Servicios de Cortafuegos/Filtrado 14 son protecciones que deben ser desplegadas a nivel de red.

Algunas de las soluciones y factores de mitigación utilizados generalmente se describen a continuación:

- **Protección basada en el extremo**

"Tras unos pocos meses de la aparición de los primeros virus informáticos en el mundo en 1987, las empresas tuvieron que empezar a vender software antivirus. Esto condujo a una carrera de armas en la que cada cual intentaba superar al adversario. El primer software apareció básicamente en dos modalidades: "Escáneres y comprobadores de errores" [Security Engineering, 2ª edición. Ross Anderson, Wiley Publishinc Inc. ISBN: 978-0-470-06852-6].

'La protección basada en el extremo' se refiere al conjunto de soluciones que deben ser desplegadas y ejecutadas directamente en el ordenador del usuario. Estas soluciones funcionan controlando lo que otros procesos están ejecutando en la máquina y qué acciones realizan.

La figura 2 muestra la interacción típica entre un proceso que se está ejecutando 24 (en el ordenador del usuario) y la Suite de Protección en el Extremo 21.

Generalmente, las protecciones originales en el extremo 21 se pueden dividir en dos grandes grupos:

- Los escáneres 22 son programas que buscan 'firmas' en los ficheros del sistema en el cual se encuentran instalados. Una 'firma' en este contexto es una pequeña parte de dígitos binarios (una cadena) que se encuentra dentro del código malicioso que el escáner quiere detectar.

- Los sumadores de verificación 22 por otro lado funcionan elaborando 'listas blancas'. El proceso consiste en generar una lista de programas cuya ejecución debería estar permitida (lista blanca). Así, para cada uno de los programas de dicha lista se calcula una suma de verificación. Cuando cualquier programa va a ejecutarse en el sistema es calculada su suma de verificación y comparada con las sumas de verificaciones de la lista para así comprobar si está autorizado o no.

Tras la aparición del primer virus, la carrera de armas empezó. Para cada nueva técnica que se incluye en el antivirus, el malware incluye una contra-medida, y así sucesivamente. Algunas de las técnicas que los virus utilizan para eludir los antivirus son:

- Polimorfismo: El virus se modifica a sí mismo cada vez que es replicado, para evitar ser detectado por los escáneres.

- Encriptación: El código del virus está encriptado, para dificultar su análisis y detección. Normalmente la encriptación forma parte del polimorfismo (simplemente cambiando la clave de encriptación se genera una nueva firma).

- Sigilo: Para evitar ser detectado por los comprobadores de errores, los virus tratan de evitar las llamadas de monitorización que realiza el sistema y ellos mismos son capaces de monitorizar dichas llamadas para ocultarse de los comprobadores de errores cuando se producen.

Desde esos principios, sin embargo, la protección en el extremo se ha complicado mucho.

En la actualidad, cualquier suite de seguridad incluye dos o más de los siguientes elementos, como puede verse en la figura 2:

- Cortafuegos Personal 23: se encarga de bloquear las conexiones de red indeseables, en ambos sentidos: entrante y saliente. Puede bloquear conexiones por proceso base, o simplemente por las características de la red (origen/destino)

- Antivirus/antimalware: examina los ficheros locales y los procesos en ejecución, utilizando una variedad de técnicas de las descritas anteriormente, con gran cantidad de variaciones (soporte para ficheros encriptados y polimórficos, por ejemplo). Este software no solo busca virus sino otro tipo de infecciones (como troyanos, gusanos y etcétera).

- Anti-*Spam* 25: Filtro que trata de bloquear correos no deseados (*spam*).

- Sistema de Detección de Intrusos (IDS) 26: Algunas soluciones también incluyen un tipo rudimentario de IDS 26. Los IDSs 26 se describirán más adelante.

- **Protección basada en la red**

Las defensas desplegadas sobre la red se encuentran en herramientas que se pueden clasificar, en general, en tres grupos:

1. Filtrado
2. Detección de Intrusión
3. Información de Seguridad y Gestión de Eventos

Las herramientas de **filtrado** comprenden elementos como cortafuegos, filtros de *spam* y software de control de contenidos. Los cortafuegos son cuellos de botella que examinan los flujos de paquetes que los atraviesan y deciden permitir su paso o rechazarlos de acuerdo a un conjunto de reglas determinado. Los filtros de *spam* son herramientas que examinan tanto el correo entrante como el saliente e intentan determinar si se trata de correo legal o indeseable (*spam*), antes de que el usuario final se vea involucrado. Un filtro de *spam* puede ejecutarse en cualquier parte del circuito del correo (desde su punto de origen, pasando por cualquiera de los servidores que reenvían el correo recibido a su destino hasta la aplicación de gestión de correo instalada en el dispositivo del usuario final). El software de control de contenidos es una serie de herramientas que controlan que contenidos son los que los usuarios están autorizados a ver. Funciona de modo similar a un cortafuegos (permite el paso de flujo de

tráfico o lo bloquea), pero lo hace a nivel de aplicación. Básicamente cualquier herramienta de seguridad que decida si debería atravesar o bloquear cualquier parte del flujo de tráfico de red puede ser encuadrada en este grupo. El filtrado se puede realizar a cualquier nivel, IP, TCP, nivel de aplicación, etc.

Los **Sistemas de Detección de Intrusión** (IDS) 26 son sistemas utilizados para analizar flujo de tráfico e intentan detectar determinados patrones que son categorizados como dañinos. A continuación se citan algunos ejemplos de tráfico que un IDS puede detectar:

- *Spam* procedente de una máquina integrada en una red controlada.
- Paquetes con direcciones de origen falsas.
- Máquinas que intentan contactar con servicios maliciosos conocidos, tales como canales IRC utilizados para controlar programas espías.
- 'Firmas de red' conocidas de virus u otro malware. Una 'firma de red' es un paquete o conjunto de paquetes que genera un malware conocido.

Normalmente los IDS 26 no detienen el flujo de tráfico, sino que solo lo reportan de modo que se pueda llevar a cabo una acción correctora. El procedimiento más simple de detección de intrusión es generar una alarma cuando cierto umbral es superado. Por ejemplo, tres o más intentos fallidos de *logon*, o una llamada de teléfono móvil que dure más de seis horas podrían dar lugar a un aviso de atención en la cuenta en cuestión. Sistemas más sofisticados se pueden clasificar en dos categorías:

- Los sistemas de detección de mal uso, que operan utilizando un modelo del comportamiento probable de un intruso.
- Los sistemas de detección de anomalías que se encargan de una tarea bastante más compleja como la búsqueda de patrones anómalos de comportamiento, en ausencia de un modelo claro del *modus operandi* del atacante, con la esperanza de detectar ataques que no hayan sido reconocidos ni catalogados previamente.

Las herramientas de **Información de Seguridad y Gestión de Eventos (SIEM)** 12 son herramientas que recogen información tanto de los sistemas de defensa de la red (tales como los cortafuegos 14 23 y los IDS 26) como de los sistemas monitorizados (*logs* de servidores, *logs* de LDAP, etcétera) en un punto central. La información recogida puede ser automáticamente correlacionada mediante un conjunto de reglas determinadas para detectar problemas que no podrían ser detectados en un punto individual. La información también puede ser utilizada para realizar auditorías forenses una vez que el problema ha tenido lugar.

"Recientemente, los antivirus parecen ser cada vez menos efectivos. La comercialización de "botnets" ha dado lugar a que los autores de malware dispongan de herramientas decentes e incluso formación. Casi todos los troyanos y otros virus son indetectables en su lanzamiento – ya que sus autores los han testado convenientemente- y muchos de ellos consiguen ejecutarse (reclutando su número de máquinas objetivo) sin llamar la atención de la industria del antivirus. El efecto neto de esto es que mientras que el software de antivirus podría haber detectado casi todas las amenazas en circulación a principios de los 2000, en 2007 un producto típico puede detectar solo una tercera parte de ellos" [Security Engineering, 2nd edition. Ross Anderson, Wiley Publisinc Inc. ISBN: 978-0-470-06852-6].

A continuación, se mencionan varios de los problemas actuales existentes en relación con la protección en el extremo:

La protección en el extremo 21 depende del análisis previo del *malware* para poder luchar contra él. Así, la industria de antivirus/*antimalware* va siempre a la zaga de las amenazas, debido, entre otras cosas, a la propia naturaleza de ambas actividades (defensa y ataque). Los atacantes (la industria de *malware*) pueden elegir la dirección del ataque mientras que los defensores solo pueden adaptarse y reaccionar frente a los nuevos ataques una vez que éstos aparecen.

A pesar de que el nuevo *malware* es catalogado rápidamente e inmediatamente después se crea una solución para corregirlo, existe siempre una ventana de tiempo durante la cual el nuevo *malware* puede instalarse sin ser detectado en una máquina. Y una vez que se ha instalado, es bastante probable que no sea detectado ni eliminado sin un arranque de la máquina formateada. Después de todo, el programa *antimalware* depende del sistema operativo para ejecutarse, y el sistema operativo puede ser afectado por un *malware* que se esté ejecutando con privilegios suficientes (por ejemplo reescribir o interceptar llamadas del sistema).

Otro problema es que la comprobación remota (verificación del estado de salud de un ordenador desde una localización remota) basada en software ejecutable en el ordenador que debe ser diagnosticado no es fiable. Cualquier cosa que un programa de diagnóstico pueda enviar para comprobar su propia integridad puede ser duplicada por un virus que se ejecuta en el mismo ordenador. Existen algunos trabajos (TPM – *Trusted Platform Module*) que son capaces de comprobar remotamente el estado de seguridad de un dispositivo, pero por el momento los dispositivos finales, simplemente, no son fiables ni controlables con efectividad.

Por todas esas razones, la protección en el extremo por sí sola no es suficiente y debe ser complementada con algún tipo de análisis de red.

Algunos de los problemas de la protección en la red existente en la actualidad para detectar o controlar ataques en la red son:

* Internet es un entorno muy ruidoso, incluso a nivel de paquetes. Existe una gran cantidad de paquetes aleatoriamente mal construidos que puede generar una tasa bastante significativa de falsas alarmas. Una falsa alarma repercute en un incremento en los costes de operación.

* Existen pocos ataques. Si hubiera diez ataques reales por cada millón de sesiones, entonces, incluso si el sistema tuviera una tasa de falsas alarmas del orden del 0,1%, la relación de falsas alarmas frente a alarmas reales sería de 100. Además del incremento en costes de operación que esto supondría, probablemente las alarmas reales se perderían en todo el ruido existente.

* Muchos ataques a redes son específicos a versiones particulares de software, por lo que una herramienta general de detección de mal uso debería tener una biblioteca enorme y constantemente actualizada de firmas de amenazas.

* Las amenazas contra la seguridad se distribuyen por naturaleza; tienen diferentes orígenes, diversos objetivos, y diversas taxonomías. Por otro lado las herramientas actuales de análisis se encuentran centralizadas en algunos cuellos de botella y la mayoría de las veces aisladas.

* El tiempo de respuesta es crítico; los ataques deben ser detenidos mientras que están sucediendo. Pero las herramientas de seguridad, la mayoría de las veces, funcionan de acuerdo a un conjunto de reglas predeterminadas, no muy efectivas cuando se trata de nuevas amenazas.

* Las herramientas de seguridad son más adecuadas para una red de tamaño pequeño a mediano que para una red ISP, ya que los sistemas centralizados simplemente no soportan estas grandes cargas.

* Los sistemas actuales tienen necesidad de supervisión constante, pero tanto por razones económicas como operativas (respuesta en tiempo real), la intervención humana debe ser mínima.

Un ejemplo de posible solución de detección de la presencia de intrusiones de red mediante la clasificación del tráfico en la red se enseña en el documento WO 2004/012603, que describe un sistema de detección de ataque que extrae el flujo de tráfico de red mediante un rastreador de paquetes. El rastreador de paquetes analiza sintácticamente los paquetes extraídos en componentes constituyentes (por ejemplo, tipo de paquete, direcciones de IP de fuente y de destino, carga útil,…) y los usa para construir vectores multidimensionales, con el fin de clasificar comportamientos anómalos basándose en un análisis de correlación y en métricas aplicadas a una selección de los vectores construidos.

Sumario de la invención

La presente invención trata de resolver los inconvenientes mencionados anteriormente por medio de un procedimiento y un sistema configurado para clasificar el tráfico basándose en una red neuronal en la que se implementa un algoritmo de agrupamiento. La base de la invención es la detección automática y la clasificación de los patrones generados por malware en la red.

Para ello a todos los paquetes de la red se les asigna automáticamente una ‘clase’. Dicha clase, también llamada conjunto de valores de clasificación, representa el tipo de paquete y se utiliza para filtrar o marcar paquetes o flujos para un análisis posterior.

En particular, en un aspecto de la presente invención se proporciona un procedimiento para clasificar tráfico de una red de comunicaciones, según la reivindicación 1.

El conjunto de valores de clasificación calculados preferentemente comprende dos bytes V_1 y V_2, donde: V_1 es el resultado de proyectar C_2 en un espacio uni-dimensional utilizando una transformación dentro de una red neuronal que preserva el orden topológico (distancia relativa entre nodos) y V_2 es el resultado de proyectar C_3 en un espacio uni-dimensional utilizando una transformación dentro de una red neuronal que preserva el orden topológico (distancia relativa entre nodos).

La distancia entre nodos se calcula preferentemente como:

$$D(A, B, p, i) = \sum_j W_{pij} \left(C(A)_{pij} - C(B)_{pij} \right)^2$$

donde: $C(X)_{pij}$ se utiliza para referirse a un elemento concreto de la caracterización del paquete X, p es el protocolo, i es la coordenada de dicho vector (C_1, C_2, C_3) asignado por el segundo módulo (32) del sistema para la que se aplica

la función distancia, *j* indica las coordenadas del vector C_i, *A y B* son los paquetes entre los cuales se mide la distancia, y W_{pij} es un vector, adaptado para cada protocolo *p*, y coordenadas *j*, *i*, utilizado para dar más peso a algunas componentes del paquete que a otras.

Preferentemente, el vector C_2 comprende al menos una de las siguientes coordenadas, tal y como se leen de la cabecera IP de dicho paquete capturado:

i. Longitud de Cabecera de Internet,

ii. Tipo de Servicio,

iii. Longitud Total,

iv. Indicadores IP,

v. Tiempo de Vida,

vi. Desplazamiento del Fragmento,

vii. Clasificación Previa, correspondiente al último valor de clasificación calculado por el sistema en el último nodo de red que el paquete ha atravesado.

El vector C_3, en el caso de un paquete del protocolo *Transmission Control Protocol* (TCP) comprende, preferentemente, al menos, una de las siguientes coordenadas, tal y como se leen de los segmentos de TCP del paquete capturado:

i. Puerto Origen,

ii. Puerto Destino,

iii. Indicadores,

iv. Ventana,

v. Urgente,

vi. Opciones,

vii. Suma de Verificación,

viii. Clasificación Previa, correspondiente al último valor de clasificación calculado por el sistema en el último nodo de red que el paquete ha atravesado, tal y como se lee de la cabecera IP.

En el caso de un paquete del protocolo *User Datagram Protocol* (UDP) el vector C_3 comprende, preferentemente, al menos, una de las siguientes coordenadas, tal y como se leen de los segmentos de UDP del paquete capturado:

i. Puerto Origen,

ii. Puerto Destino,

iii. Longitud,

iv. Suma de Verificación,

v. Clasificación Previa, correspondiente al último valor de clasificación calculado por el sistema (30 51 68) en el último nodo de red que el paquete ha atravesado, tal y como se lee de la cabecera IP.

El vector C_3, en el caso del protocolo *Internet Control Message Protocol* (ICMP) comprende preferentemente, al menos, una de las siguientes coordenadas, tal y como se leen de los segmentos de ICMP del paquete capturado:

i. Tipo,

ii. Código,

iii. Suma de Verificación,

iv. Clasificación Previa, correspondiente al último valor de clasificación calculado por el sistema en el último nodo de red que el paquete ha atravesado, tal y como se lee de la cabecera IP.

En una realización particular, el procedimiento utiliza además el campo de opciones de la cabecera de IP del paquete capturado para almacenar dicho conjunto de valores de clasificación.

En otro aspecto de la invención, se presenta un sistema de clasificación de tráfico en una red de comunicaciones. El sistema comprende medios para llevar a cabo el procedimiento descrito anteriormente.

En particular, este sistema comprende: un primer módulo, configurado para capturar paquetes IP de dicha red de comunicaciones; un segundo módulo, configurado para perfilar dichos paquetes capturados asignando un vector a cada paquete capturado de acuerdo a un conjunto de determinadas características; un tercer módulo, configurado para calcular un conjunto de valores de clasificación para cada uno de dichos paquetes perfilados de acuerdo a la información contenida en su cabecera de IP y la información contenida en la cabecera de su protocolo específico; y un cuarto módulo, configurado para reescribir las cabeceras de dichos paquetes capturados, incluyendo dichos valores de clasificación en una cabecera IP.

El sistema se conecta a, al menos, un nodo de dicha red de comunicaciones.

Opcionalmente, el sistema tiene dos modos de operación: un modo de entrenamiento, en el que dichos nodos pertenecientes a dicha red neuronal se generan automáticamente, utilizando las coordenadas (C_1, C_2, C_3) de los paquetes capturados a partir de tráfico real conocido; y un modo de representación, en el que los paquetes capturados se clasifican utilizando nodos ya generados de una red neuronal.

Finalmente se proporciona un programa informático que comprende medios de código de programa informático adaptados para realizar el procedimiento descrito anteriormente.

Breve descripción de los dibujos

Para completar esta descripción y con objeto de ayudar a una mejor comprensión de la invención, se proporciona un dibujo. Dicho dibujo forma parte integrante de la descripción e ilustra una realización preferente de arquitectura para implementar el procedimiento de la invención, que no debería ser interpretado como restringiendo el ámbito de la invención, sino solo como un ejemplo de cómo se puede realizar la invención.

La figura 1 es un esquema de alto nivel de los factores de protección y mitigación que se pueden desplegar para proteger a los usuarios.

La figura 2 muestra la interacción típica entre un proceso que se ejecuta (en el ordenador del usuario) y la Suite de Protección en el extremo.

La figura 3 muestra un esquema de un Elemento del Sistema (SE)

La figura 4 muestra un Mapa de Auto-Organización (SOM), basado en una red neuronal para clasificación del protocolo UDP.

La figura 5 es un esquema simplificado de la integración del sistema de la invención en una red de Provisión del Servicio de Internet (ISP).

La figura 6 muestra el modo en que un paquete es reclasificado en cada elemento de la red.

Descripción de la realización preferente

La presente divulgación se refiere a un procedimiento y un sistema, que comprende *hardware* y *software* específicos residentes en o cerca de (conectados) los nodos de una red de comunicaciones, que clasifica el tráfico basándose en un algoritmo de agrupamiento en una red neuronal que será descrito más adelante en detalle. La base de la invención es la detección y clasificación automáticas de los patrones de tráfico generados por malware en la red.

A todos los paquetes de la red se les asigna automáticamente una 'clase', que representa el tipo de paquete, y que es utilizada para filtrar o marcar paquetes o flujos de paquetes en un análisis posterior.

Los paquetes de datos de la red son clasificados mediante el uso de dos Mapas de Auto-Organización (SOM) que hacen corresponder dos conjuntos de valores n-dimensionales que representan el paquete, perfilado por el sistema, en dos valores uni-dimensionales. Los dos valores uni-dimensionales, junto con un byte que representa el tipo de protocolo, son agrupados en un valor tri-dimensional que representa la 'clase' del paquete. Un Mapa de Auto-Organización es un tipo de red neuronal artificial que es entrenada, mediante un aprendizaje no supervisado, para producir un valor representativo de una dimensión inferior (en este caso uni-dimensional) a partir de un valor de entrada de una dimensión superior (el paquete de red perfilado).

El sistema tiene dos modos de operación:

- Un modo de entrenamiento, en el que los grupos se generan automáticamente, y la red es "entrenada", basándose en tráfico de red real.
- Un modo de representación, en el que los paquetes se clasifican utilizando una red ya "entrenada".

Debido a que cada nodo de red tiene una visibilidad parcial del tráfico de la red, la información de grupos se comparte entre todos los nodos utilizando los propios paquetes de la red como vectores de transmisión. La información de grupos, es, de este modo, una parte de la función distancia (descrita más adelante) utilizada por el algoritmo SOM.

El procedimiento y sistema se integra en o cerca (conectado) de al menos uno de los nodos de la red. Como dicho sistema contiene algunas características de Inspección Detallada de Paquetes (DPI), puede también integrarse en cualquier parte de la red que exista un sistema DPI.

Se incorpora un Elemento del Sistema (SE) en cada nodo de la red. En la figura 3 se muestra un esquema de un Elemento del Sistema SE 30. Los componentes de un SE son:

- A. Módulo de Captura de Paquetes 31: Este módulo captura paquetes IP 35 de la red. Si existiera un DPI, éste podría, opcionalmente, realizar esta función.

- B. Módulo de Perfilado de Paquetes 32: Este componente perfila un paquete capturado 36 de acuerdo a un conjunto de coordenadas predeterminadas (por ejemplo, longitud del paquete, origen y destino, protocolo,…). Los paquetes perfilados 37 constituyen la capa de entrada de la red neuronal 40, como se puede ver en la figura 4. También este módulo podría implementarse en un DPI, en caso de estar presente. Más adelante se describen en profundidad los detalles de éste módulo, en esta sección.

- C. Módulo de Red Neuronal de Agrupamiento 33: Este componente toma como entrada un paquete perfilado 37, tal y como se proporcionan a la salida del módulo de perfilado de paquetes 32, y, utilizando una red neuronal, calcula un 'valor de grupo' 38. Un 'valor de grupo' 38 es una representación numérica tri-dimensional del conjunto o 'grupo' al que la Red Neuronal cree que el paquete pertenece. La primera de estas dimensiones representa el protocolo (y puede opcionalmente omitirse en el siguiente paso – en el módulo D- ya que de hecho el protocolo se encuentra ya de forma explícita en el paquete). La segunda dimensión representa el grupo de paquetes al que cada paquete procesado pertenece, clasificándolo únicamente de acuerdo a su cabecera IP. La tercera dimensión representa la clasificación atendiendo a la cabecera específica de su protocolo. El algoritmo de agrupamiento en una red neuronal que utiliza el sistema es un Mapa de Auto-Organización (SOM). Más adelante se incluyen detalles concretos relativos a la implementación de este componente.

- D. Modulo de Reescritura de Paquetes 34: Este módulo reescribe la cabecera de cada paquete, incluyendo el 'valor de grupo', en la cabecera IP. La salida del módulo de reescritura de paquetes 34 es un paquete clasificado 39. También más adelante se incluyen detalles concretos de la implementación de el módulo de reescritura de paquetes 34, en esta sección.

Nótese que la Red Neuronal 40 mostrada en la figura 4 representa el Mapa de Auto-Organización (SOM) utilizado para el agrupamiento en el caso del protocolo UDP. La capa de salida 41 en dicha figura está simplificada para mayor claridad. La capa real de salida 41 tiene 266 nodos (desde el Grupo 0 42 hasta el Grupo 255 43). La Red Neuronal 40, por lo tanto, tal y como se define en el SOM, tiene dos capas, una capa de entrada 44 con un nodo 45 46 47 48 49 por cada una de las coordenadas, y una capa de salida 41 que contiene tantos nodos 42 43 como grupos contenga la información clasificada (utilizando un único byte para su representación se obtienen hasta 256 grupos).

Así pues, a cualquier paquete que atraviese un nodo de red que tenga un Elemento del Sistema SE 30 asociado, se le aplica el siguiente procedimiento:

- El paquete es perfilado de acuerdo a un conjunto dado de coordenadas.

- Las coordenadas del paquete (su perfilado) son la entrada de una red neuronal, que calcula un valor de grupo 38, que indica la categorización del paquete de acuerdo a un conocimiento previo de la red.

- El paquete es, entonces, modificado de modo que se incluye dicha categorización en una cabecera, y, transferido al siguiente nodo de la red del modo habitual.

Debido a que el paquete atraviesa más de uno nodo de red, este procedimiento puede repetirse más de una vez para cada paquete (tantas veces como nodos de red atraviese). Además, como una de las coordenadas de perfilado del paquete es el valor de clasificación asignado en el nodo anterior (45 en la figura 4), esto significa que aunque cada SE 30 solo vea parte de la información, la Red Neuronal 40 incluye información de toda la red.

En este sentido, la red de Provisión del Servicio de Internet ISP crea una red meta-neuronal, en la que cada SE 30 actúa como una neurona (la cual constituye también por sí misma una red neuronal 40).

La figura 5 presenta un esquema simplificado de la integración en la red ISP, donde se muestran una red de comunicaciones que comprende varios usuarios residenciales 54 y sus enlaces hacia otras redes 53. En cada Elemento de la Red 52 se dispone de un SE 30 51, y las propias conexiones de red existentes 55 se utilizan para comunicar los SEs 30 51 entre sí.

La figura 6 muestra el modo en que un paquete es reclasificado en cada elemento de red 52 62 64 66 que atraviesa, por medio de los SEs 30 51 68. Cuando el paquete aparece por primera vez, no tiene aún ninguna información de clasificación 61. El primer elemento de la red 62 clasifica el paquete, generando un paquete clasificado 63, que es posteriormente transferido hacia su destino, al siguiente elemento de la red 64. El segundo elemento 64 clasifica el paquete de nuevo. Debido a que el Mapa de Auto-Organización SOM utilizado para clasificar incluye en su capa de entrada la clasificación del paquete, dicha clasificación es refinada. De este modo se genera un paquete reclasificado 65. El paquete 65 puede pertenecer al mismo grupo que el paquete sin reclasificar 63, o puede ser movido a un grupo diferente (ya que la red neuronal en 64 puede tener un entrenamiento diferente).

Antes de que el paquete pase a una red externa 67, la información de clasificación debe ser eliminada. El último elemento de la red 66 implementa esta función.

Hasta el momento no se han descrito acciones adicionales a llevar a cabo sobre los paquetes, pero, una vez que el paquete ha sido clasificado, es fácil utilizar el valor de grupo del mismo para filtrar los paquetes, bien en el perímetro de la red (justo antes de transferirlos a un usuario residencial u otras redes 67), o incluso dentro de las propias redes residenciales. Esta nueva información de seguridad es fácilmente integrable con otras medidas de seguridad existentes, como IDSs, cortafuegos, etc.

A continuación se describen en detalles los módulos del sistema B, C y D, y sus respectivas funciones:

- Módulo B. Perfilación de Paquetes 32

Este módulo lee el contenido de los paquetes tal y como son entregados por el módulo A, y extrae información de los mismos.

Un paquete de red es perfilado inicialmente por un vector tri-dimensional (C1, C2, C3) donde:

- C1 es el protocolo específico del paquete, tal y como se lee del paquete IP.

- C2 es un vector que representa las características IP del paquete. El contenido del vector es (en el orden descrito):

    1. Longitud de Cabecera de Internet
    2. Tipo de Servicio
    3. Longitud Total
    4. Indicadores *IP*
    5. Tiempo de Vida
    6. Desplazamiento del Fragmento
    7. Clasificación Previa

- C3 es un vector que representa las características específicas del protocolo del paquete. La dimensión de este vector y su contenido dependen del protocolo concreto del paquete. Como ejemplo se muestra el contenido de dicho vector para los protocolos más habituales:

- Protocolo: TCP

    1. Puerto Origen
    2. Puerto Destino
    3. Indicadores
    4. Ventana
    5. Urgente
    6. Opciones
    7. Suma de Verificación
    8. Clasificación Previa

- Protocolo: UDP

1. Puerto Origen
2. Puerto Destino
3. Longitud del Mensaje
4. Suma de Verificación
5. Clasificación Previa

- Protocolo: ICMP
  1. Tipo
  2. Código
  3. Suma de Verificación
  4. Clasificación Previa

Se utiliza la nomenclatura $C(X)_{pij}$ para referirse a un elemento concreto de la caracterización del paquete *X*, *p* es el protocolo, como se muestra a continuación:

- *t* se refiere al protocolo TCP
- *u* se refiere al protocolo UDP
- *i* se refiere al protocolo ICMP

Así, por ejemplo:

$C(X)_{t33}$ se refiere al campo de indicadores de un paquete TCP,

$C(X)_{u33}$ se refiere a la longitud de un paquete UDP,

$C(X)_{t27}$ se refiere a la clasificación previa (de cualquier paquete IP independientemente de su protocolo), así $C(X)_{t27}$, $C(X)_{u27}$ y $C(X)_{i27}$ son sinónimos.

- Módulo C. Algoritmo de Agrupamiento 33

El módulo C realiza la clasificación de los paquetes ya perfilados, proporcionados por el módulo B. El módulo C genera dos bytes de información, que representan en grupo (o conjunto) al que el paquete pertenece de acuerdo a su cabecera IP, y el grupo (o conjunto) al que el paquete pertenece de acuerdo a la cabecera de su protocolo específico (TCP, UDP, ICMP o cualquier otro).

El módulo C implementa un Mapa de Auto-Organización (SOM) multi-capa que constituye la pieza clave de su sistema de clasificación. Un mapa de Auto-Organización (SOM) es un tipo de red neuronal artificial entrenada mediante aprendizaje no supervisado para producir una representación discretizada de baja dimensión (típicamente bidimensional) del espacio de entrada de las muestras de entrenamiento. Esta representación es lo que se denomina mapa. Los Mapas de Auto-Organización son diferentes de otras redes neuronales artificiales porque utilizan una función de proximidad para preservar las propiedades topológicas del espacio de entrada.

Como la mayoría de las redes neuronales artificiales, los SOMs operan en dos modos distintos: entrenamiento y clasificación. En el modo de entrenamiento se construye el mapa utilizando ejemplos de entrada. Se trata de un procedimiento competitivo también llamado vector de cuantificación. En el modo de representación se clasifica automáticamente un nuevo vector de entrada.

Un mapa de Auto-Organización (SOM) comprende un número determinado de componentes llamados nodos o neuronas. En cada nodo existe un vector asociado, llamado vector de ponderación de la misma dimensión que los vectores que contienen los datos de entrada. Estos nodos ocupan una posición en el espacio del mapa. La disposición normal de los nodos es una distribución hexagonal o rectangular con un espaciado regular entre ellos. El Mapa de Auto-Organización representa una clasificación de un espacio de entrada de dimensión superior a un espacio de dimensión inferior. El procedimiento para situar un vector de entrada en el mapa es encontrar el nodo con el vector de ponderación más próximo al vector de entrada y asignar las coordenadas de este nodo, en el mapa, a dicho vector de entrada.

El módulo B realiza una clasificación de dos capas utilizando dos Mapas de Auto-Organización (SOMs). La primera capa clasifica el paquete de acuerdo a sus características de IP. La segunda capa clasifica el paquete de acuerdo a las características específicas de su protocolo (C_3).

Cada SOM es mapa uni-dimensional, como se muestra en la figura 4. La capa de entrada tiene uno nodo por cada coordenada definida (seis nodos para IP, nueve nodos para TCP y así con el resto de protocolos) y 256 en la capa de salida.

El procedimiento para clasificar cualquier paquete es:

1.- Clasificar el paquete de acuerdo al Mapa de Auto-Organización de IP. Generar V_1.

2.- Clasificar el paquete de acuerdo al Mapa de Auto-Organización de protocolo. Generar V_2.

3.- Devolver V_1, V_2 como valor de clasificación,

donde, V_1 es el resultado de proyectar C_2 en un espacio uni-dimensional utilizando una transformación en una red neuronal que preserva el orden topológico (la distancia relativa entre nodos) y V_2 es el resultado de proyectar C_3 en un espacio uni-dimensional utilizando un transformación en una red neuronal que preserva el orden topológico (la distancia relativa entre nodos). De este modo, si C y C' son dos vectores n-dimensionales, V y V' son sus respectivas proyecciones y, $D_n(A,B)$ y $D_m(A,B)$ son las distancias entre 2 puntos A y B en un espacio n-dimensional y m-dimensional, respectivamente, entonces $D_n(0_n,C)<D_n(0_n,C')$ implica que $D_m(0_m,V)<D_m(0_m,V')$, donde 0_n y 0_m son los vectores cero n-dimensional y cero m-dimensional, respectivamente.

Así pues, la red neuronal clasifica (agrupa) datos n-dimensionales en un espacio m-dimensional manteniendo la posición relativa entre nodos, de acuerdo a una función distancia. Por eso para el procedimiento de clasificación es necesario definir una función distancia entre vectores.

V_1 y V_2 son valores independientes, ya que proceden de proyectar vectores diferentes (C_2 y C_3) en un espacio uni-dimensional.

Por lo tanto, como se ha podido comprobar una parte importante del algoritmo SOM es la función distancia (función que proporciona la distancia entre dos puntos). Para ello se utiliza la función distancia euclídea ponderada.

La distancia D entre dos puntos (paquetes) A y B, para el protocolo p, y la capa i, se define como:

$$D(A,B,p,i) = \sum_j W_{pij}\left(C(A)_{pij} - C(B)_{pij}\right)^2$$

Donde:

- p es el protocolo,
- i es la capa de entrada del SOM para la que se aplica la función distancia,
- A y B son los paquetes cuya distancia se mide,
- W_{pij} es un vector de ponderación, adaptado a cada protocolo y capa de entrada.

El propósito del vector de ponderación W es permitir la adaptación del algoritmo de agrupamiento a diferentes escenarios de la red, dando más peso a unas componentes del paquete que a otras. Es posible, incluso, ignorar alguna componente, tan solo ajustando la coordenada apropiada de W a 0.

- Modulo D. Reescritura de Paquetes 34

Este módulo incluye la información de clasificación del paquete (V_1, V_2) dentro del paquete, de manera tal que no afecta a su curso a través de otros elementos de red.

Para ello, el sistema utiliza el campo o*pciones* de la cabecera IP para almacenar los valores V1, V2. El formato de dicho campo contiene:

- Tipo (26)
- Indicador de Copia (1 bit)
- Clase de Opción (2)

El valor hexadecimal *D6* se utiliza como cabecera opcional. Este campo tiene una longitud de 4 bytes. El contenido de estos bytes es (hexadecimal):

- Cabecera de Opciones: *0xD6*
- Longitud Opciones: *0x04*

- Contenido byte 1: *V1*
- Contenido byte 2: *V2*

El procedimiento y sistema de la invención reducen significativamente el coste computacional y operacional de la clasificación del tráfico de red para incrementar la seguridad, ya que incluye protocolos de auto aprendizaje (en la red neuronal).

No afecta a otras medidas ya existentes, y puede ser integrado fácilmente con éstas proporcionando un nuevo parámetro (la categorización del tráfico) con el que trabajar.

Este nuevo parámetro describe una clasificación de seguridad del tráfico, a nivel de paquete. Permite un fácil filtrado del tráfico malicioso. Puede ser utilizado para desviar tráfico a un 'área de limpieza de la red' donde los flujos de red seleccionados pueden ser analizados más profundamente. Mientras que no es práctico analizar todo el tráfico que atraviesa una ISP, este sistema permite una fácil pre-clasificación del tráfico, que permite la posibilidad de analizar solamente el tráfico sospechoso.

REIVINDICACIONES

1. Un procedimiento de clasificación de tráfico en una red de comunicaciones, en el que dicho procedimiento comprende los siguientes pasos:

   - capturar paquetes IP (35) de dicha red de comunicaciones;
   - perfilar dichos paquetes capturados (36) asignando un vector a cada uno de dichos paquetes capturados (36) de acuerdo con un conjunto de determinadas características;
   - calcular un conjunto de valores de clasificación para cada uno de dichos paquetes perfilados (37) de acuerdo a la información contenida en su cabecera de IP y la información contenida en la cabecera de un protocolo encapsulado en los paquetes IP (36) capturados;

   caracterizado porque el procedimiento comprende además el siguiente paso:

   - reescribir las cabeceras de dichos paquetes capturados (35), incluyendo dichos valores de clasificación calculados en una cabecera IP;

   y **porque** el vector asignado es un vector tri-dimensional (C_1, C_2, C_3), donde:

   - C_1 es el protocolo encapsulado de dicho paquete capturado (35), tal y como se lee de la cabecera IP;
   - C_2 es un vector que comprende información de la cabecera de IP de dicho paquete capturado (35);
   - C_3 es un vector que comprende información de los datos de cabecera del protocolo encapsulado de dicho paquete capturado (35), cuya dimensión depende del contenido de la coordenada C_1.

2. El procedimiento según la reivindicación 1, en el que dicho conjunto de valores de clasificación calculados comprende dos bytes V_1 y V_2, donde:

   - V_1 es el resultado de proyectar C_2 en un espacio uni-dimensional utilizando una transformación dentro de una red neuronal que preserva el orden topológico, basado en la distancia relativa entre nodos y
   - V_2 es el resultado de proyectar C_3 en un espacio uni-dimensional utilizando una transformación dentro de una red neuronal que preserva el orden topológico, basado en la distancia relativa entre nodos.

3. El procedimiento según la reivindicación 2, en el que dicha distancia relativa entre nodos se calcula como:

$$D(A, B, p, i) = \sum_{j} W_{pij} \left(C(A)_{pij} - C(B)_{pij} \right)^2$$

   donde:

   - $C(X)_{pij}$ se utiliza para indicar un elemento concreto de la caracterización del paquete X,
   - p es el protocolo,
   - i es la coordenada de dicho vector (C_1, C_2, C_3) asignada por un segundo módulo (32) del sistema, para la cual se aplica la función distancia,
   - j indica las coordenadas del vector C_i,
   - A y B son los paquetes entre los cuales se mide la distancia,
   - W_{pij} es un vector, adaptado para cada protocolo p, y coordenadas j, i, utilizado para dar más peso a algunas componentes del paquete que a otras.

4. El procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que el vector C_2 comprende al menos una de las siguientes coordenadas, tal y como se leen de la cabecera IP del paquete capturado:

   i. Longitud de Cabecera de Internet,
   ii. Tipo de Servicio,
   iii. Longitud Total,
   iv. Indicadores IP,

v. TTL (Tiempo de Vida),

vi. Desplazamiento del Fragmento,

vii. Clasificación Previa, correspondiente al último valor de clasificación calculado en el último nodo de red que el paquete ha atravesado.

5. El procedimiento según cualquiera de las reivindicaciones, 1 a 4, en el que el vector C_3, en el caso del Protocolo de Control de Transmisión (TCP) comprende, al menos, una de las siguientes coordenadas, tal y como se leen de los segmentos de TCP del paquete capturado:

i. Puerto Origen,

ii. Puerto Destino,

iii. Indicadores,

iv. Ventana,

v. Urgente,

vi. Opciones,

vii. Suma de Verificación,

viii. Clasificación Previa, correspondiente al último valor de clasificación calculado en el último nodo de red que el paquete ha atravesado, tal y como se lee de la cabecera IP.

6. El procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que el vector C_3, en el caso del Protocolo de Datagramas de Usuario (UDP) comprende, al menos, una de las siguientes coordenadas, tal y como se leen de los segmentos de UDP del paquete capturado:

i. Puerto Origen,

ii. Puerto Destino,

iii. Longitud,

iv. Suma de Verificación,

v. Clasificación Previa, correspondiente al último valor de clasificación calculado en el último nodo de red que el paquete ha atravesado, tal y como se lee de la cabecera IP.

7. El procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que el vector C_3, en el caso del Protocolo de Mensajes de Control de Internet (ICMP) comprende, al menos, una de las siguientes coordenadas, tal y como se leen de los segmentos de ICMP del paquete capturado:

i. Tipo,

ii. Código,

iii. Suma de Verificación,

iv. Clasificación Previa, correspondiente al último valor de clasificación calculado en el último nodo de red que el paquete ha atravesado, tal y como se lee de la cabecera IP.

8. El procedimiento según cualquiera de las reivindicaciones anteriores, que comprende además la utilización del campo de opciones de la cabecera de IP del paquete capturado para almacenar dicho conjunto de valores de clasificación calculados.

9. Un sistema (30 51 68) de clasificación de tráfico en una red de comunicaciones, en el que dicho sistema (30 51 68) comprende medios para llevar a cabo el procedimiento según cualquiera de las reivindicaciones anteriores.

10. El sistema (30 51 68) según la reivindicación 9, comprendiendo dicho sistema:

- un primer módulo (31), configurado para capturar paquetes IP (35) de dicha red de comunicaciones;

- un segundo módulo (32), configurado para perfilar dichos paquetes capturados (36) asignando un vector a cada uno de dichos paquetes capturados (36) de acuerdo a un conjunto de determinadas características;

- un tercer módulo (33), configurado para calcular un conjunto de valores de clasificación para cada uno de dichos paquetes perfilados (37) de acuerdo a la información contenida en su cabecera de IP y la información contenida en la cabecera de su protocolo específico;

- un cuarto módulo (34), configurado para reescribir las cabeceras de dichos paquetes capturados (35), incluyendo dichos valores de clasificación calculados en una cabecera IP.

11. El sistema (30 51 68) según la reivindicación 10, en el que dicho sistema (30 51 68) puede ser conectado a, al menos, un nodo de red (52 62 64 66) de dicha red de comunicaciones.

12. El sistema (30 51 68) según la reivindicación 11, en el que dicho sistema (30 51 68) está configurado para operar en uno de dos modos de operación:

a. un modo de entrenamiento, en el que nodos de una red neuronal (40) se generan automáticamente, utilizando las coordenadas (C_1, C_2, C_3) de los paquetes capturados (35) a partir de tráfico de red real conocido;

b. un modo de representación, en el que los paquetes capturados (35) se clasifican utilizando nodos ya generados de una red neuronal (40).

13. Un programa informático que comprende medios de código de programa informático adaptados para realizar el procedimiento según cualquiera de las reivindicaciones 1 a 8, cuando dicho programa se ejecuta en un ordenador, un procesador de señal digital, una disposición de puertas de campo programable, un circuito integrado de aplicación específica, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.

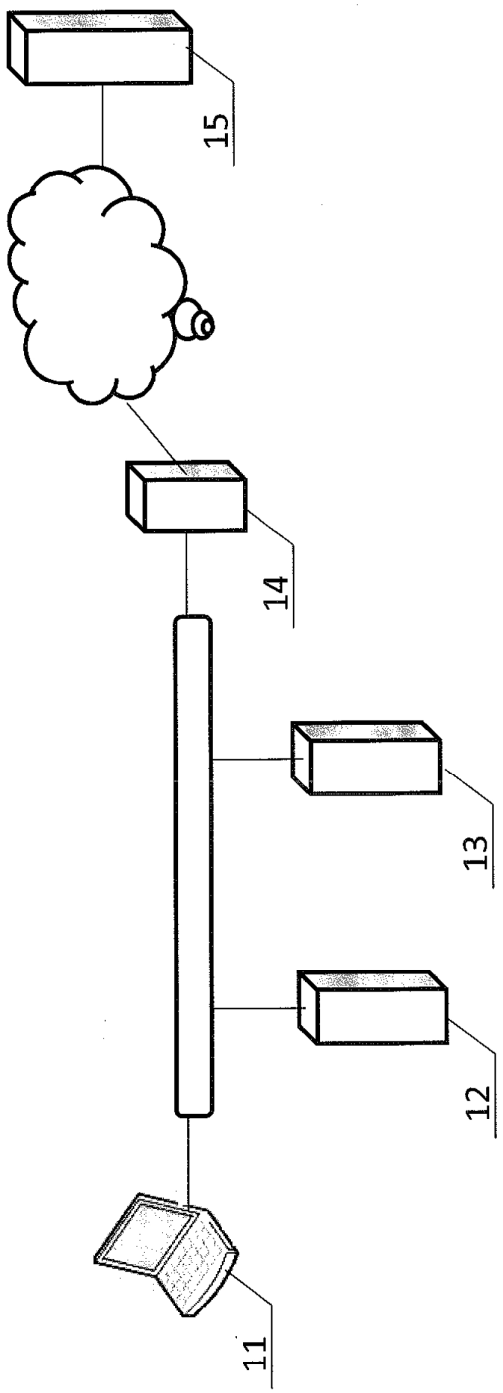

FIG. 1 (técnica anterior)

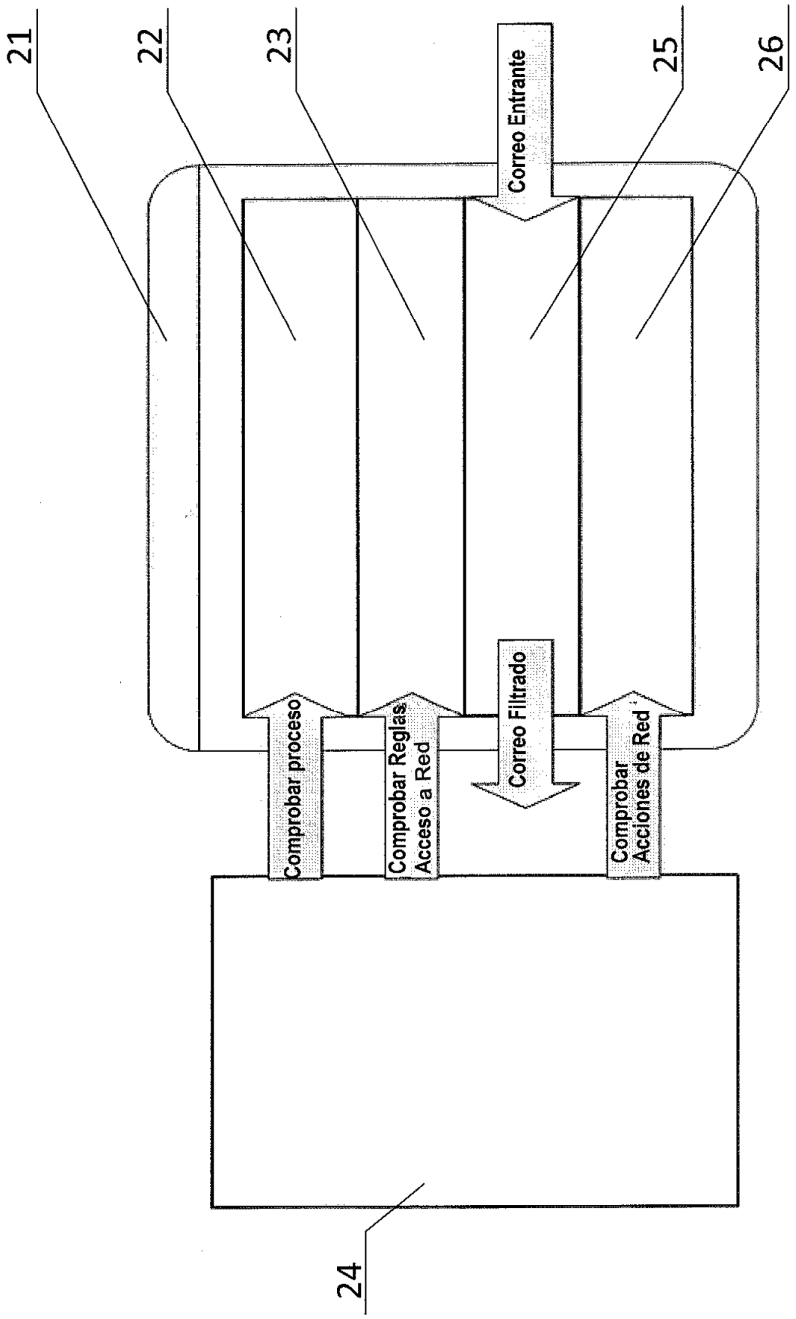

FIG. 2 (técnica anterior)

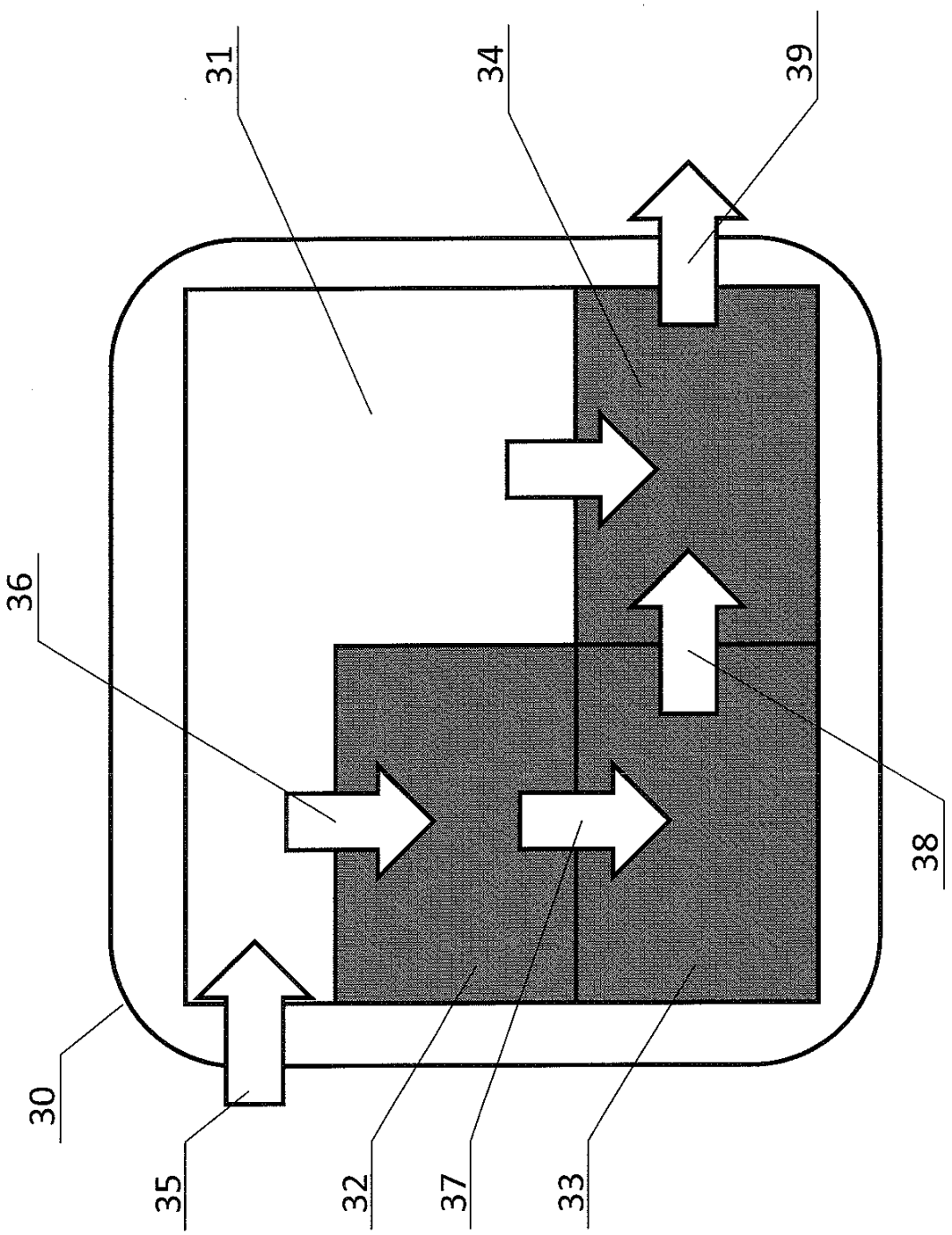

FIG. 3

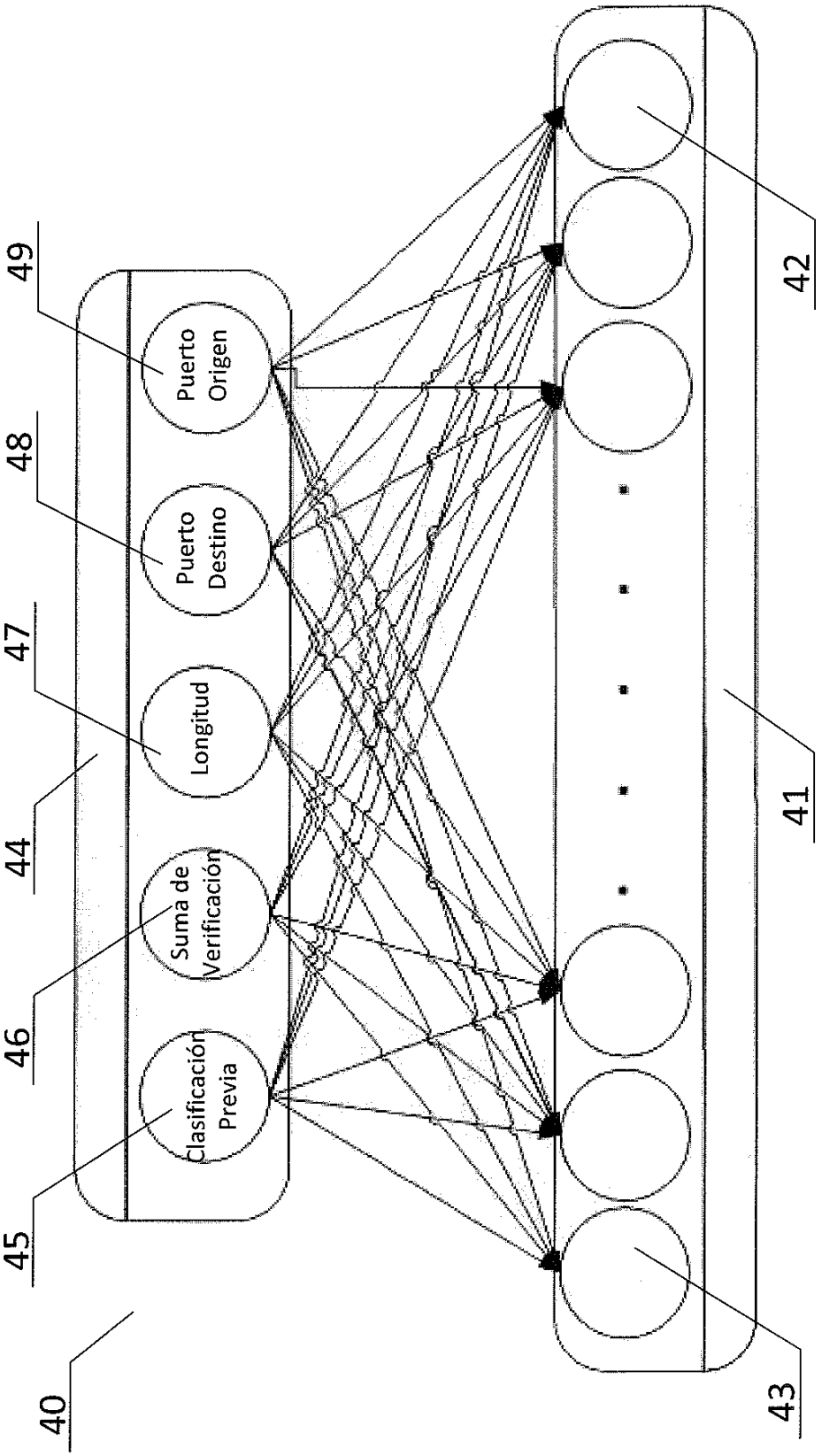
Puerto Origen
Puerto Destino
Longitud
Suma de Verificación
Clasificación Previa
40
41
42
43
44
45
46
47
48
49

FIG. 4

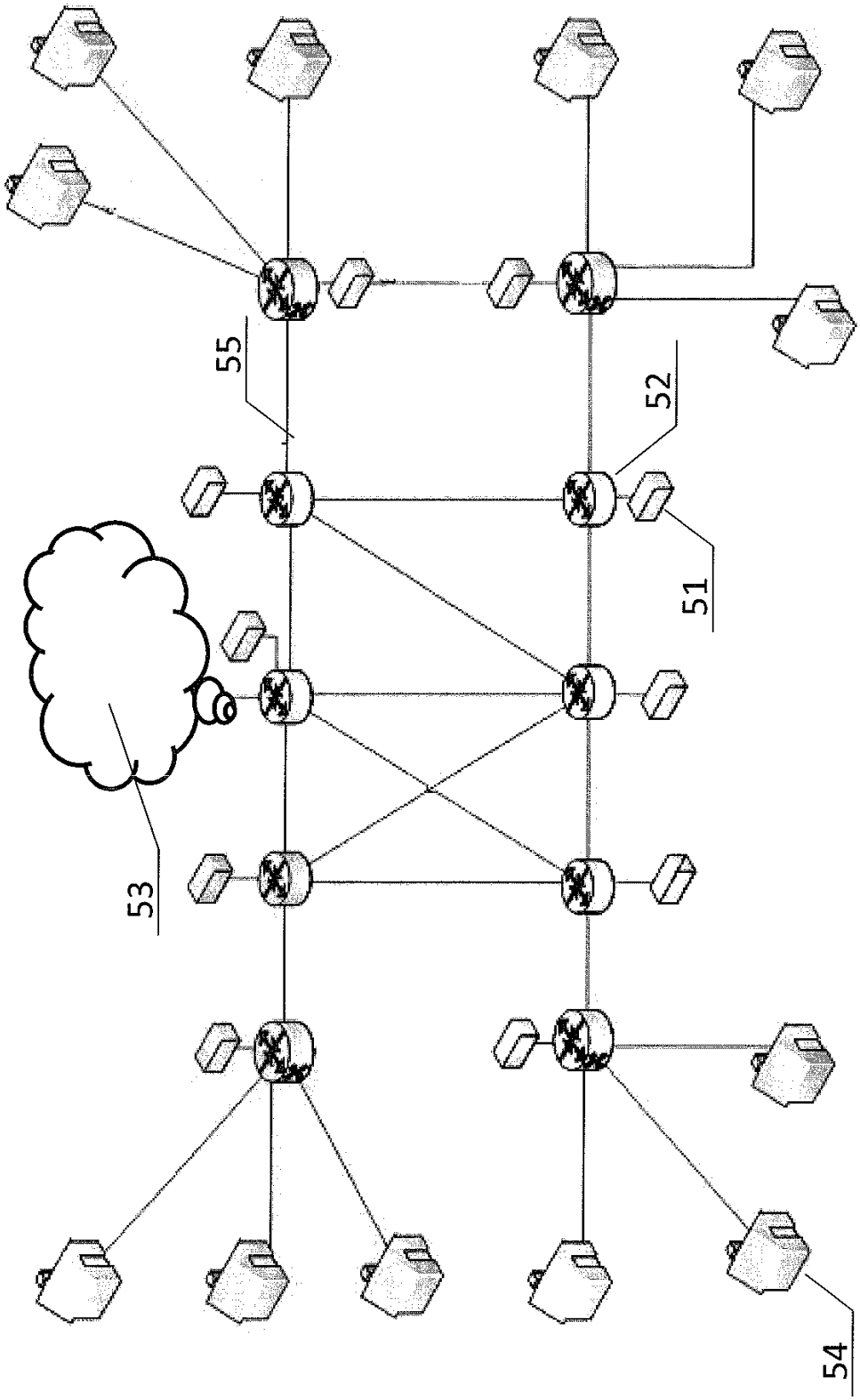

FIG. 5

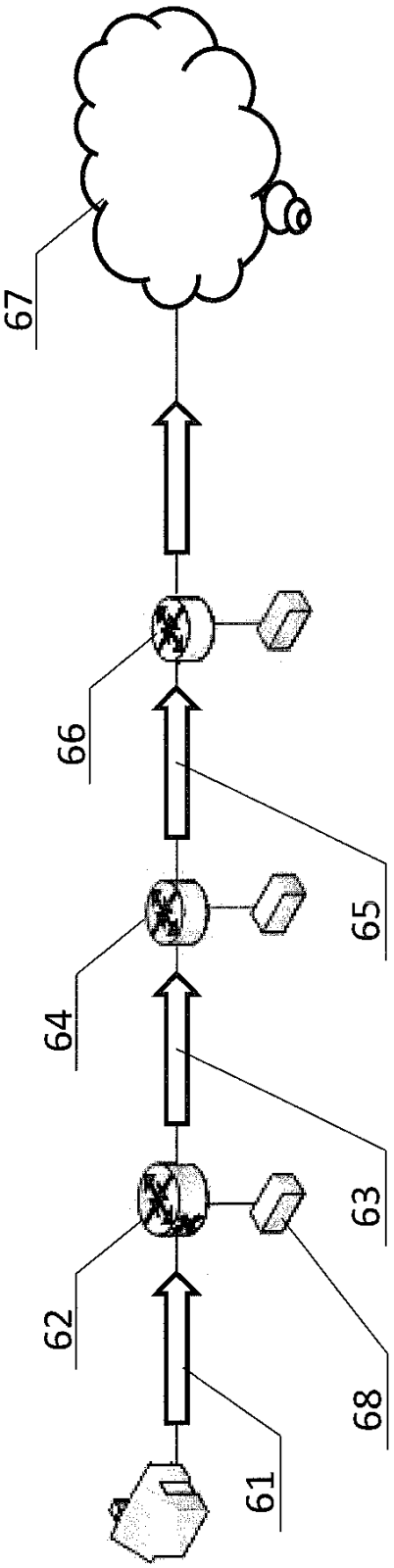

FIG. 6