(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 398 374**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.06.2007 E 07012405 (2)**

(97) Fecha y número de publicación de la concesión europea: **24.10.2012 EP 2051468**

(54) Título: **Método, dispositivo de procesamiento de datos y red informática para la detección de anomalías**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.03.2013

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
FRIEDRICH-EBERT-ALLEE 140
53113 BONN, DE

(72) Inventor/es:

BYE, RAINER;
LUTHER, KATJA;
ALPCAN, TANSU, DR.;
ALBAYRAK, SAHIN, PROF. DR. y
MÜLLER, ACHIM

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Método, dispositivo de procesamiento de datos y red informática para la detección de anomalías.

Campo de la invención

La invención se refiere a redes de comunicación en general, y especialmente a un método, un dispositivo de procesamiento de datos y una red informática para detectar un funcionamiento anómalo dentro de una red informática, en particular debido a una intrusión maliciosa desde el exterior de la red.

Antecedentes de la invención

Se conoce por software malicioso o malware (de "malicious software"), un software que está diseñado para atacar sistemas informáticos, en el que el malware se difunde a través de una red de comunicación a la que el sistema informático es conectable. Actualmente, los atacantes se dirigen fundamentalmente a ordenadores personales (PCs) para suplantación, escucha furtiva, violar autorizaciones, modificar o destruir, manipular, falsificar y sabotear datos. Esto ocurre sobre todo utilizando o liberando cierto software malicioso (malware), que puede clasificarse por ejemplo como troyanos, virus o gusanos. Se utilizan diferentes técnicas para defender y asegurar sistemas potencialmente atacados, tales como por ejemplo software de cortafuegos basado en listas blancas, software de antivirus basado en listas negras, y sistemas de detección de intrusión y de prevención de intrusión (IDS/IPS, intrusion detection and intrusion prevention systems) basados en anomalías.

La gran mayoría de los sistemas de detección de intrusión utilizan enfoques basados en firmas, para detectar ataques. Sin embargo, esto no permite la detección de ataques de día cero, puesto que las firmas sólo pueden generarse retrospectivamente, es decir, después de que el ataque se ha llevado a cabo por lo menos una vez.

La detección basada en anomalías es una alternativa viable a los enfoques basados en firmas, cuando se intenta detectar un comportamiento anómalo del sistema provocado por instrucciones exitosas.

A partir del documento US 6 711 615 B2, por ejemplo, se conoce un método de vigilancia de redes que comprende monitorización y análisis jerárquico de eventos dentro de una red corporativa, en el que mediante monitores de la red se detecta una actividad sospechosa de la red, en base al análisis de los datos de tráfico de la red, para lo cual se proporciona en el monitor una unidad de inferencia basada en firmas y una unidad de detección de anomalías estadísticas. Se generan informes de la actividad sospechosa mediante los monitores de la red, que son recibidos automáticamente por monitores jerárquicos.

Sin embargo, el punto débil de los sistemas basados en anomalías es la elevada tasa de falsos positivos, lo que significa que a menudo se emiten alarmas cuando el sistema de hecho se comporta normalmente. Como consecuencia, esto conduce elevados costes de mantenimiento y, lo que es peor, a situaciones en las que las alarmas correctas son ignoradas por los usuarios debido a la elevada frecuencia de falsas alarmas.

La utilización de sistemas inmunes artificiales (AIS, Artificial Immune System) para vigilancia de redes se describe, por ejemplo, en la tesis de máster de K. Luther "Entwurf eines Künstlichen Immunsystems zur Netzwerküberwachung auf Basis eines Multi-Agenten-Systems", TU Berlín, 2006.

El documento "On decision support for distributed systems protection: A perspective based on the human immune response system and epidemiology", de S. Goel y otros, International Journal of Information Management, Elsevier Science Ltd., GB, volumen 27, número 4, 12 de junio de 2007, páginas 266 a 278, se refiere a un sistema de seguridad de redes basado en AIS, en el que la detección de virus se realiza mediante la inspección aleatoria de paquetes, para limitar los recursos utilizados para la exploración de paquetes. Múltiples sistemas inmunes en un vecindario comparten información entre sí, de manera que la detección del virus en un vecindario puede utilizarse como disparador para incrementar la frecuencia de muestreo de la inspección de paquetes.

En el documento WO 03/029934 A1 se describe un sistema de detección de intrusión basado en agentes, en el que los agentes individuales comparten firmas de ataques y soluciones a través de un mecanismo de intercambio de mensajes, y en el que puede utilizarse una medida interna global de la salud general del grupo de agentes, como un indicador de un posible ataque. Sin embargo, la incidencia de falsos positivos sigue siendo un problema.

Por lo tanto, un objetivo de la presente invención es mostrar una manera novedosa y mejorada de detectar un comportamiento anómalo dentro de una red informática, en el que, en particular, se reduce la tasa de detecciones de falsos positivos.

Resumen de la invención

La solución inventiva del objetivo se consigue mediante cada uno de los contenidos de las respectivas reivindicaciones independientes adjuntas. Los contenidos de las respectivas reivindicaciones dependientes adjuntas son realizaciones ventajosas y/o preferidas, o mejoras.

Para detectar un funcionamiento anómalo dentro de una red informática que comprende múltiples nodos interconectados de procesamiento de datos, el método inventivo propone un enfoque cooperativo, en el que mediante un primer nodo de procesamiento de datos de la red informática se determina un primer valor de estado, que es una medida de la probabilidad de un funcionamiento anómalo, y mediante un segundo nodo de procesamiento de datos de la red informática se determina un segundo valor de estado, que es asimismo una medida de la probabilidad de un funcionamiento anómalo. Para conseguir cooperación, dicho segundo valor de estado se transmite mediante comunicación entre pares desde dicho por lo menos un segundo nodo de procesamiento de datos al primer nodo de procesamiento de datos, a partir de dichos primer y segundo valores de estado se determina un tercer valor de estado mediante el primer nodo de procesamiento de datos, y en función del tercer valor de estado se determina si se ha producido un funcionamiento anómalo.

Para determinar el tercer valor del estado se determina un valor promedio de los segundos valores de estado, el primer valor de estado se pondera con un primer factor de ponderación, el valor promedio se pondera con un segundo factor de ponderación, y se suman el primer valor de estado ponderado y el valor promedio ponderado, obteniéndose de ese modo un tercer valor de estado.

El primer y el segundo nodos de procesamiento de datos son habitualmente ordenadores estacionarios, pero pueden disponerse asimismo como cualesquiera otros dispositivos capaces de procesamiento de datos, tales como por ejemplo dispositivos informáticos móviles o teléfonos inteligentes. Por consiguiente, los nodos de procesamiento de datos pueden interconectarse utilizando cualquier clase de medio de comunicación adecuado, tales como por ejemplo una LAN, una WLAN, Bluetooth o una red celular basada en GSM o UMTS.

Para determinar el primer valor de estado se monitoriza habitualmente el tráfico de red del primer nodo de procesamiento de datos. Por lo tanto, el primer valor de estado en concreto es una medida de la probabilidad de un funcionamiento anómalo del primer nodo de procesamiento. Para reducir las detecciones de falsos positivos de funcionamiento anómalo, se propone una cooperación con otros nodos de procesamiento de datos de la red informática, que tiene como resultado dicho tercer valor de estado que incorpora asimismo los segundos valores de estado recibidos desde los segundos nodos de procesamiento de datos, y en función de este tercer valor se decide si existe un funcionamiento anómalo.

Puesto que muchos ataques maliciosos de la red informática tienen como resultado la difusión de cierto malware dentro de la red informática, la probabilidad de que un nodo de procesamiento de datos dado que detecta una actividad de red anómala esté infectado, aumenta si otros nodos de procesamiento de datos detectan asimismo la actividad de red anómala. Por lo tanto, mediante el enfoque cooperativo del método descrito se aumenta la precisión de la detección, reduciéndose por lo tanto las detecciones de falsos positivos.

Para una detección en curso, las etapas descritas anteriormente de determinación del primer valor de estado, determinación y transmisión de dicho por lo menos un segundo valor de estado, determinación del tercer valor de estado y, en función del tercer valor de estado, decisión sobre si se ha producido un funcionamiento anómalo, se repiten preferentemente en tiempos predefinidos, en particular con una frecuencia predefinida.

En principio, el primer valor de estado puede determinarse mediante cualquier algoritmo de detección de anomalías adecuado, o incluso mediante un algoritmo de detección basado en firmas. Sin embargo, de manera especialmente ventajosa, la determinación de dicho primer valor de estado se realiza mediante un algoritmo basado en un sistema inmune artificial (AIS).

Por lo tanto, de manera especialmente ventajosa, el método comprende además la etapa de almacenar en el primer nodo de procesamiento de datos, por lo menos un conjunto de vectores de referencia que están asociados con un funcionamiento anómalo. Los inventores descubrieron que para determinar estos vectores de referencia es especialmente adecuado un algoritmo de selección negativa.

Por consiguiente, preferentemente cada conjunto de vectores de referencia se determina inicialmente realizando una selección negativa mediante el primer nodo de procesamiento. Con este propósito, monitorizando el tráfico de red durante una fase de aprendizaje, se determinan y se almacenan datos de aprendizaje que representan un comportamiento normal del sistema, en el que los datos de aprendizaje comprenden múltiples vectores de datos de tráfico. Hasta que el conjunto de vectores de referencia alcanza un número predefinido de vectores de referencia, se generan repetidamente vectores de datos aleatorios y se comparan con cada vector de datos de tráfico de dichos datos de aprendizaje. Si el respectivo vector de datos aleatorio no se corresponde con ninguno de los vectores de datos de tráfico de dichos datos de aprendizaje, se añade al conjunto de vectores de referencia, en el que se define que los vectores coinciden si su distancia está por debajo de un umbral predefinido, donde la distancia se determina mediante una medida predefinida de la distancia.

En base a los vectores de referencia que representan la anomalía, el primer nodo de procesamiento de datos determina preferentemente el primer valor de estado monitorizando tráfico de datos de red, determinando por lo menos un vector de datos de tráfico a partir del tráfico de red monitorizado, y determinando las distancias entre cada vector de datos de tráfico y cada vector de referencia de un conjunto respectivo de dichos conjuntos almacenados de vectores de referencia, por medio de una medida predefinida de la distancia.

El enfoque AIS de medición de la distancia entre vectores de datos de tráfico y vectores de referencia que representan la anomalía, es especialmente adecuado para un espacio vectorial asociado con funcionamiento normal, que no esté organizado en una pequeña cantidad de grupos grandes, sino en muchos grupos pequeños, lo que es típico en la comunicación de red de una red informática.

Cada uno de los componentes vectoriales de un vector de datos de tráfico determinado está asociado con una respectiva característica predefinida del tráfico de datos de red monitorizado. Los vectores de referencia, y asimismo los vectores aleatorios generados en la fase de aprendizaje descrita anteriormente para determinar inicialmente los vectores de referencia, tienen la misma estructura y por consiguiente se proporcionan como vectores de características con componentes vectoriales que están asociados con los mismos valores predefinidos del tráfico de datos de red.

Dichas características pueden comprender, por ejemplo, información de direcciones tales como puertos o direcciones IP utilizadas, o información estadística tal como el número de conexiones, el número de paquetes, el número de puertos utilizados o el número de puertos explorados.

Puesto que utilizar un número elevado de características para cada vector de características tiene como resultado un espacio vectorial correspondientemente grande que, a su vez, tiene como resultado distancias menos significativas entre vectores, se utilizan preferentemente dos o más vectores de características con respectivas características diferentes del tráfico de datos de red. Por consiguiente, de manera ventajosa se almacenan por lo menos dos conjuntos diferentes de vectores de referencia y se determinan por lo menos dos vectores de datos de tráfico diferentes.

Ejemplos de mediciones de distancia adecuadas son la distancia de Hamming y la distancia euclídea, donde en el caso de la distancia de Hamming los vectores son representables preferentemente como cadenas binarias.

En una realización preferida del método, el primer valor de estado está representado por un contador que se incrementa para cada vector de referencia para el que se determina que la distancia hasta el respectivo vector de datos de tráfico está por debajo de un umbral predefinido. De manera ventajosa, el contador se incrementa mediante un valor que es inversamente proporcional a dicha distancia, de manera que un vector de referencia con el que dicho vector de datos de tráfico tiene una afinidad elevada, es decir una distancia reducida, tiene un gran efecto.

Puesto que es poco práctico almacenar y comparar vectores de referencia que cubran el espacio vectorial completo, de manera ventajosa se proporciona una sustitución continua de los vectores de referencia. Con este propósito, cada vector de referencia de cada conjunto de vectores de referencia se asocia con una vida útil predefinida, transcurrida la cual se borra del conjunto y se sustituye por un nuevo vector de referencia, que se determina generando aleatoriamente vectores de datos y comparándolos con los datos de aprendizaje almacenados, tal como se ha descrito anteriormente.

Otra mejora ventajosa del AIS utilizado es la selección clonal, en la que un vector de referencia que se ha detectado coincide con un vector de datos de tráfico es clonado. Por consiguiente el método comprende además, de manera ventajosa, las etapas de seleccionar por lo menos un vector de referencia para el cual se ha determinado que la distancia hasta un vector de datos de tráfico está por debajo del umbral predefinido, generar por lo menos un vector modificado, modificando cada componente vectorial de dicho vector de referencia seleccionado en una cantidad aleatoria comprendida dentro de un intervalo predefinido, y añadir dicho vector modificado al respectivo conjunto de vectores de referencia.

Los valores de estado son una medida de la probabilidad de un funcionamiento anómalo global de la red informática. Sin embargo, en particular, el primer y asimismo el tercer valor de estado son medidas de la probabilidad de un funcionamiento anómalo del primer nodo de procesamiento de datos. Por lo tanto, preferentemente, el primer valor de estado que se determina mediante el primer vector de referencia está asociado con una ponderación fuerte, es decir, el primer factor de ponderación es mayor que el segundo factor de ponderación.

Para que el tercer valor de estado sea de la misma escala que el primer y segundo valores de estado, preferentemente la suma del primer y el segundo factores de ponderación es igual a 1. Ejemplos de relaciones adecuadas entre el primer y el segundo factores de ponderación son 60:40, 70:30, 80:20 y 90:10.

La definición sobre si se ha producido un funcionamiento anómalo se realiza ventajosamente comparando el tercer valor de estado con un umbral predefinido, donde se define que se ha producido el funcionamiento anómalo cuando dicho tercer valor de estado supera dicho umbral. Preferentemente, tras la detección de un funcionamiento anómalo se lanza una alarma. Por consiguiente, el método comprende ventajosamente generar una señal de alarma mediante el primer nodo de procesamiento de datos, cuando el tercer valor de estado supera un umbral predefinido.

Con propósitos prácticos, dicha señal de alarma se transmite desde el primer nodo de procesamiento de datos a un nodo central administrativo, donde un administrador de la red informática puede comprobar si se ha lanzado una alarma.

Los vectores de tráfico de datos que no lanzan una alarma, es decir que tienen como resultado un tercer valor de estado que queda por debajo del umbral predefinido, se incluyen ventajosamente en los datos de aprendizaje almacenados, permitiendo de este modo un aprendizaje continuo y una adaptación a las variaciones del entorno.

El primer y el segundo nodos de procesamiento de datos son, preferentemente, de configuración similar, de manera que cada uno de los segundos nodos de procesamiento de datos puede actuar asimismo como un primer nodo de procesamiento de datos.

Por lo tanto, cada uno de los segundos valores de estado se determina preferentemente mediante el respectivo segundo nodo de procesamiento de datos, de la manera que se ha descrito anteriormente con respecto a la determinación del primer o el tercer valor de estado mediante el primer nodo de procesamiento de datos.

Preferentemente, el primer y el segundo nodos de procesamiento de datos intercambian sus valores de estado a intervalos temporales regulares, consiguiendo de ese modo un efecto cooperativo. En consecuencia, la transmisión tiene lugar automáticamente, por ejemplo disparada por un temporizador del respectivo nodo de procesamiento de datos. En otra realización preferida del método, se propone asimismo una cooperación dirigida por eventos. En esta realización, si el primer nodo de procesamiento de datos determina que se ha producido un funcionamiento anómalo, éste transmite automáticamente en respuesta el tercer valor de estado y los respectivos vectores de referencia asociados con el funcionamiento anómalo, a cada uno de los segundos nodos de procesamiento de datos. A continuación, los segundos nodos de procesamiento de datos incluyen preferentemente en sus respectivos conjuntos de vectores de referencia los vectores de referencia recibidos.

Un dispositivo de procesamiento de datos inventivo adaptado para la detección de un funcionamiento anómalo dentro de una red informática, comprende una interfaz de red que está adaptada para recibir, mediante una comunicación entre pares desde por lo menos otro dispositivo de procesamiento de datos predefinido, un segundo valor de estado que es una medida de la probabilidad de un funcionamiento anómalo dentro de la red informática, una unidad de monitorización para monitorizar tráfico de datos de la red, por lo menos una unidad de detección de anomalías adaptada para determinar un primer valor de estado que es una medida de la probabilidad de un funcionamiento anómalo dentro de la red informática, una unidad de colaboración adaptada para determinar un tercer valor de estado a partir de dicho primer valor de estado y de dichos segundos valores de estado, y medios de determinación para determinar si se ha producido un funcionamiento anómalo en función de dicho tercer valor de estado.

Tal como se ha descrito anteriormente con respecto al método, el primer y el tercer valores de estado son preferentemente una medida de la probabilidad de un funcionamiento anómalo del propio dispositivo de procesamiento de datos inventivo, mientras que dicho por lo menos un segundo valor de estado es una medida de la probabilidad de un funcionamiento anómalo dicho respectivo por lo menos otro dispositivo de procesamiento de datos.

Preferentemente, cada unidad de dispositivo de procesamiento de datos y la unidad de colaboración están adaptadas respectivamente para determinar automáticamente primeros y terceros valores de estado a intervalos predefinidos.

Las unidades de detección de anomalías utilizan ventajosamente un algoritmo basado en un sistema inmune artificial. Por lo tanto, ventajosamente se disponen medios de almacenamiento para almacenar, para cada unidad de detección de anomalías, un conjunto de vectores de referencia que están asociados con un funcionamiento anómalo. Preferentemente, cada unidad de dispositivo de procesamiento de datos está adaptada para determinar vectores de tráfico de datos a partir de tráfico de red monitorizado, en la que cada uno de los componentes vectoriales de dichos vectores de datos de tráfico están asociados con una respectiva característica predefinida del tráfico de datos de red monitorizado. Además, cada unidad de detección de anomalías está adaptada preferentemente para determinar las distancias entre un respectivo vector de datos de tráfico y cada vector de referencia de dicho conjunto respectivo de entre los conjuntos almacenados de vectores de referencia, mediante una medición predeterminada de la distancia.

Para mantener bajas las dimensiones vectoriales, ventajosamente se disponen por lo menos dos unidades de detección de anomalías, donde cada una está adaptada para determinar vectores de tráfico de datos con características que constituyen los componentes vectoriales.

En una realización preferida, cada unidad de detección de anomalías comprende un contador, en la que la lectura del contador representa el primer valor de estado, y cada unidad de detección de anomalías está adaptada para incrementar dicho contador para cada vector de referencia para el cual se determina que la distancia hasta el respectivo vector de datos de tráfico está por debajo de un umbral predefinido, en la que preferentemente cada unidad de detección de anomalías está adaptada para aumentar dicho contador mediante un valor que es inversamente proporcional a dicha distancia.

Además, el dispositivo está adaptado ventajosamente para llevar a cabo una fase de monitorización en la que el tráfico de datos de red asociado con un funcionamiento normal es monitorizado y almacenado como datos de aprendizaje, comprendiendo dichos datos de aprendizaje múltiples vectores de datos de tráfico. Preferentemente, el

dispositivo está adaptado además para llevar a cabo una fase de aprendizaje, en la que se generan repetidamente vectores de datos aleatorios, se comparan con cada vector de datos de tráfico de dichos datos de aprendizaje y se añaden al respectivo conjunto de vectores de referencia, si no coinciden con ninguno de los vectores de datos de tráfico de dichos datos de aprendizaje, en el que se define que los vectores coinciden si su distancia está por debajo de un umbral predefinido, hasta que el conjunto de vectores de referencia comprende un número predefinido de vectores de referencia. Mediante la realización de dichas fases de monitorización y aprendizaje, el dispositivo está adaptado para determinar cada conjunto de vectores de referencia.

Preferentemente, el dispositivo está adaptado además para eliminar cada vector de referencia de cada conjunto de vectores de referencia transcurrida una vida útil asociada predefinida, y para sustituirlo por un nuevo vector de referencia que, de nuevo, se determina de la manera descrita anteriormente.

En otra realización preferida el dispositivo está adaptado para la selección clonal de vectores de referencia, en el que, en este sentido, cada unidad de detección de anomalías está adaptada para seleccionar por lo menos un vector de referencia del conjunto respectivo de vectores de referencia para el cual se ha determinado que la distancia hasta un vector de datos de tráfico está por debajo de un umbral predefinido, generar un vector modificado, modificando cada componente vectorial dicho vector de referencia en una cantidad aleatoria que queda dentro de un intervalo predefinido, y añadir dicho vector modificado al conjunto respectivo de vectores de referencia.

La unidad de colaboración del dispositivo está adaptada para determinar dicho tercer valor de estado, determinando un valor promedio de dichos segundos valores de estado, ponderando el primer valor de estado con un primer factor de ponderación, ponderando dicho valor promedio con un segundo factor de ponderación, y sumando el primer valor de estado ponderado y el valor promedio ponderado, obteniendo de ese modo dicho tercer valor de estado.

Además, el dispositivo está adaptado ventajosamente para generar una señal de alarma cuando el tercer valor de estado supera un umbral predefinido, y para transmitir preferentemente la señal de alarma a un nodo central administrativo de la red informática.

De manera especialmente ventajosa, el dispositivo está adaptado para transmitir el primer y/o el tercer valor de estado mediante una comunicación entre pares, por lo menos a otro dispositivo de procesamiento de datos predefinido, en particular a todos los dispositivos equipados similarmente, dentro de la red informática. Estos otros dispositivos de procesamiento de datos utilizan, a su vez, estos valores de estado recibidos, como segundos valores de estado para determinar su tercer valor de estado. Normalmente, el dispositivo inventivo está adaptado para transmitir el primer y/o el tercer valor de estado a intervalos temporales regulares, controlados por ejemplo mediante un respectivo temporizador.

En otra realización preferida, el dispositivo inventivo está adaptado para transmitir el tercer valor de estado en un esquema dirigido por eventos. Por consiguiente, el dispositivo está adaptado ventajosamente para transmitir automáticamente, cuando determina que se ha producido un funcionamiento anómalo, el tercer valor de estado y los respectivos vectores de referencia asociados con el funcionamiento anómalo, por lo menos a otro dispositivo de procesamiento de datos predefinido, en especial equipado de manera similar. Por consiguiente, el dispositivo está asimismo adaptado preferentemente para incluir por lo menos el vector de referencia recibido desde otro dispositivo en, por lo menos, uno de sus conjuntos almacenados de vectores de referencia.

Cualquier otra mejora descrita anteriormente con respecto al método inventivo aplica asimismo al dispositivo de procesamiento de datos inventivo.

Una red informática inventiva con múltiples nodos de procesamiento de datos que están interconectados con propósitos de comunicación de datos, comprende por lo menos dos de dichos nodos de procesamiento de datos descritos anteriormente, como dispositivos de detección de anomalías.

Para la supervisión mediante un administrador, la red informática comprende además, preferentemente, un nodo central administrativo adaptado para recibir señales de alarma desde dichos dispositivos de detección de anomalías.

Para permitir la cooperación descrita anteriormente, los dispositivos de detección de anomalías están adaptados ventajosamente para comunicar mediante comunicación entre pares. Para la comunicación entre pares, cada dispositivo de detección de anomalías mantiene ventajosamente una lista de pares, que preferentemente se actualiza automáticamente. Con este propósito, cada uno de los dispositivos de detección de anomalías está adaptado para funcionar como un nodo maestro para la comunicación entre pares, en el que dicho nodo maestro está adaptado para proporcionar una lista de todos los dispositivos de detección de anomalías que están conectados a la red informática.

Breve descripción de las figuras

Se muestra, en

la figura 1 una vista esquemática de una realización ejemplar de un dispositivo de procesamiento de datos conectable a una red informática, que está adaptado para detectar un funcionamiento anómalo de

la red informática,

la figura 2 una vista esquemática de una realización preferida de una red informática que comprende múltiples dispositivos de procesamiento de datos como el mostrado en la figura 1, y

la figura 3 esquemáticamente, una comunicación entre pares, entre múltiples dispositivos de procesamiento de datos tal como el que se muestra en la figura 1.

Descripción detallada de la invención

A continuación se describen en mayor detalle con respecto a las figuras, realizaciones de la invención preferidas pero ejemplares.

En la figura 1 se muestra una vista esquemática de una realización ejemplar de un dispositivo 100 de procesamiento de datos, que está adaptado para detectar un funcionamiento anómalo dentro de una red informática a la que está conectado.

Para la detección de anomalías, el dispositivo comprende dos unidades 111 y 112 de detección de anomalías, que funcionan en base a un sistema inmune artificial (AIS). Se dispone un conjunto respectivo de vectores de referencia 121 y 122 para cada una de las unidades 111 y 112 de detección de anomalías, que está asociado con un funcionamiento anómalo. En lo que sigue, los vectores de referencia se denominan asimismo detectores dado que se utilizan para detectar un funcionamiento anómalo, y las unidades de detección de anomalías se denominan asimismo agentes AIS dado que están basadas en un sistema inmune artificial. Ventajosamente, puede disponerse asimismo un número arbitrario de unidades de detección de anomalías y conjuntos respectivos de vectores de referencia adicionales, que se indican mediante los numerales de referencia 11N y 12N.

El dispositivo 100 está dispuesto como un ordenador y, por consiguiente, comprende una unidad de control 130 con un microprocesador para controlar el dispositivo 100, y asimismo una memoria 140 que puede comprender, por ejemplo, RAM y memoria de disco duro.

Con propósitos de comunicación, el dispositivo 100 está dotado de una interfaz de red 160, que está adaptada para comunicación entre pares. Mediante una unidad de monitorización 170, puede monitorizarse el tráfico de datos de la red. A partir del tráfico monitorizado de datos de la red, se extraen características predefinidas para formar vectores de datos de tráfico que se proporcionan a las unidades 111 y 112 de detección de anomalías, las cuales los comparan con los respectivos vectores de referencia de los conjuntos asociados de vectores de referencia 121 y 122. Mediante esta comparación, se determina un primer valor de estado que es una medida de la probabilidad de un funcionamiento anómalo, en particular de un funcionamiento anómalo del dispositivo 100.

Mediante la unidad de colaboración 150, a partir de dicho primer valor de estado y de dichos segundos valores de estado recibidos mediante la interfaz de red 160 desde otros dispositivos, equipados de manera similar al dispositivo 100, se determina un tercer valor de estado, en función del cual se determina si se ha producido un funcionamiento anómalo.

Este tercer valor de estado es, asimismo, una medida de la probabilidad de un funcionamiento anómalo, en particular de un funcionamiento anómalo del dispositivo 100. Puesto que los segundos valores de estado representan el estado de funcionamiento anómalo de otros dispositivos de la red informática a la que está conectado el dispositivo 100, el tercer valor de estado refleja asimismo el estado de salud de estos otros dispositivos. Por consiguiente, los segundos valores de estado pueden inhibir o amplificar el estado representado por el primer valor de estado, reduciendo por lo tanto la tasa de detecciones de falsos positivos de funcionamiento anómalo.

En la figura 2 se muestra una realización ejemplar de una red informática inventiva 10 que comprende tres ordenadores 101 a 103 que actúan como dispositivos de detección de anomalías, los cuales están equipados como el dispositivo 100 mostrado en la figura 1 y, por consiguiente, están adaptados para detectar un funcionamiento anómalo dentro de la red informática 10.

Los dispositivos 201, 202 y 210 de la red informática 10 no están adaptados para detectar un funcionamiento anómalo. Sin embargo, el dispositivo 210 está dispuesto como un dispositivo central administrativo para la red informática 10, al cual son transmitidas señales de alarma desde los dispositivos de detección de anomalías 101 a 103, para su supervisión mediante un administrador.

En la realización mostrada, los dispositivos 101-103, 201, 202 y 210 están interconectados mediante conmutadores 311 y 312. Para acceder a internet 400, se dispone una pasarela 320 que está conectada con ambos conmutadores 311 y 312. A través de la red internet 400, un ordenador atacante 500 puede intentar infiltrarse en la red informática 10, por ejemplo utilizando o liberando cierto software malicioso (malware) tal como troyanos, virus o gusanos.

Para detectar un ataque de este tipo, los ordenadores 101 a 103 están equipados respectivamente con unidades de detección de anomalías, y asimismo con unidades de colaboración que permiten un enfoque cooperativo para la

detección de anomalías. Para cooperar, los ordenadores 101 a 103 comunican mediante comunicación entre pares, tal como se muestra esquemáticamente en la figura 3.

A continuación, se describe en mayor detalle la arquitectura AIS.

Como algoritmo básico para la selección de los detectores para los datos de aprendizaje proporcionados, se utiliza el algoritmo de selección negativa. La idea principal del algoritmo de selección negativa es producir detectores aleatoriamente y compararlos con los patrones normales obtenidos durante el aprendizaje. Cada detector que coincide con estos patrones normales es eliminado y, por lo tanto, los detectores restantes reconocen solamente patrones anómalos. A continuación se muestra un pseudocódigo para el algoritmo de selección negativa:

```
SET ConjuntoDetectores como el conjunto de Detectores
SET ConjuntoNormal a partir de los datos de aprendizaje
SET NúmeroDetectores como el número de Detectores
    WHILE tamaño de ConjuntoDetectores menor que NúmeroDetectores
        CREATE un Detector
        FOR cada VectorCaracterísticas en el ConjuntoNormal
            COMPARE Detector con VectorCaracterísticas
            IF son similares
                DELETE Detector
            ELSE
                PUT Detector en ConjuntoDetectores
```

Los vectores de características se componen de las estadísticas del tráfico de red en un cliente. A continuación se proporciona una descripción detallada de los vectores de características, con respecto a simulaciones llevadas a cabo. Después del periodo de aprendizaje, los nuevos vectores de características son presentados a los detectores restantes y se calcula a la distancia entre los vectores de características y los detectores. Si la distancia es menor que el umbral del detector, se incrementa un contador. Cuando el contador alcanza un umbral predefinido se lanza una alarma, y en la siguiente etapa tiene lugar una selección clonal.

Selección clonal, describe la selección de los detectores que reconocen los patrones anómalos. Los detectores se comparan continuamente con los patrones producidos, y si uno es similar a un patrón de este tipo, se clona. La similitud entre un detector y un vector de características se denomina afinidad, y los detectores con afinidad máxima son seleccionados y clonados. Alternativamente, los detectores mutan para una cobertura mejor del espacio no propio. Mutación significa que no solamente producen copias de sí mismos, sino asimismo copias con pequeñas diferencias. Preferentemente, la tasa de mutación es inversamente proporcional a la afinidad del detector. En la realización descrita, selección clonal significa por lo tanto que el detector se copia pero con pequeñas diferencias en los valores del vector de características.

Para detectar anomalías, en la realización descrita se utiliza un simple esquema de detección de anomalías que utiliza solamente la selección positiva. Si el detector no alcanza su umbral durante un periodo de vida predefinido, es eliminado del conjunto de detectores y se crea un detector nuevo. Los datos para los vectores de características se reúnen mediante un componente de monitorización del agente. El agente reúne los datos de paquetes y crea vectores de características continuamente. Durante el periodo de aprendizaje, cada coincidencia entre un detector y los patrones presentados incrementa un contador específico del detector. Si se alcanza cierto umbral, entonces el detector es eliminado, es decir se lleva a cabo selección negativa. La distancia entre los detectores y los vectores de características se calcula mediante la distancia de Hamming.

Los inventores han descubierto que varios anfitriones 101 a 103 en una red de 10 que ejecuta instancias de la arquitectura AIS presentada, pueden conseguir mejores rendimientos de detección si cooperan compartiendo sus resultados de detección y su propio estado. En la realización descrita, se propone una infraestructura P2P que permite que diferentes agentes AIS colaboren con este propósito.

Los sistemas P2P pueden clasificarse, en general, en tres categorías: totalmente descentralizados, parcialmente descentralizados y descentralizados híbridos. La infraestructura P2P utilizada en la realización descrita se basa en una arquitectura descentralizada híbrida. Los nodos tienen las mismas capacidades, pero uno actúa siempre como el "súper nodo" con el propósito de búsqueda inicial de otros pares que contienen sistemas AIS. Aparte de esto, los clientes comunican con otros pares de manera autónoma. A continuación se describe la forma de proceder para un cliente AIS que desea compartir información con otros pares. La entidad central se denomina el servidor y los otros

agentes AIS se denominan simplemente clientes o nodos pares. La estructura de datos PEER (PAR) contiene la dirección IP del par, un contador con fines de mantenimiento y datos aplicables al sistema que utiliza la infraestructura P2P.

A continuación se proporciona un pseudocódigo para la comunicación entre pares:

```
Lista de pares listaPares
INITIALIZATION
        Enviar Mensaje de Registro al servidor
SEND UPDATE MESSAGE
        Enviar Mensaje de Actualización a los pares de la lista
RECEIVE MESSAGE
        CASE Tipo de Mensaje OF
                Mensaje de lista de Pares procedente del servidor:
                        Añadir pares a la propia lista
                Mensaje de Actualización:
                        FOR todos los pares en la lista
                                IF remitente del Mensaje es igual al par
                                        actualizar par con Actualización
                        ELSE
                                incrementar contador de edad
                        IF contador edad > umbral
                                borrar par de la lista
                        IF remitente del Mensaje no estaba en la lista
                                añadir remitente a la lista de pares.
                Mensaje Quitar:
                        eliminar remitente de la lista de pares
                Mensaje Solicitar Lista:
                        Enviar lista de pares a cliente
DISCONNECT
Enviar al remitente Mensaje Quitar
Enviar a los pares de la lista Mensaje Quitar
```

A continuación se describen las partes respectivas del pseudocódigo:

Initialization (inicialización)

Un nodo que desea conectar a la red superpuesta P2P contacta al servidor con un mensaje de registro.

Send Update Message (enviar mensaje de actualización)

Informa a todos los otros nodos acerca de actualizaciones interesantes, tal como el estado de las unidades de detección. Nos remitimos a la sección siguiente para detalles relacionados con el contenido de los mensajes intercambiados entre los agentes AIS.

Receive Message (recibir mensaje)

Se manejan cuatro tipos de mensajes:

1. En el caso de una lista de pares procedente de un mensaje del servidor, el nodo se añade a la lista de nodos cliente.

2. Tras la recepción de un mensaje de actualización, se actualiza el estado de información acerca de un nodo en la lista de pares. Para todos los demás nodos, se incrementa un contador de edad. Si el contador alcanza un umbral específico que indica que un nodo no ha enviado mensajes de actualización en cierto intervalo de tiempo, éste se elimina de la lista. Esto es importante cuando un cliente no es capaz de desconectar adecuadamente. Este enfoque puede utilizarse para el mantenimiento de la lista, dado que los mensajes periódicos son parte esencial del sistema. Si el remitente del mensaje de actualización no es un elemento de la lista de pares, se añade automáticamente a dicha lista.

3. Un mensaje de quitar, tiene como resultado la eliminación del nodo remitente de la lista.

4. El mensaje de solicitar lista, es respondido transmitiendo la lista de nodos al solicitante.

Disconnect (desconectar)

Un mensaje desde un nodo al servidor central pero asimismo a los clientes de la lista de pares, de que el agente desea desconectar.

En la realización descrita se asume que la red informática 10 es una subred propiedad de una compañía o de un departamento universitario. Por lo tanto, existe un intervalo válido de direcciones IP conocidas en dichas subredes. Si un atacante exterior intenta llevar a cabo un ataque de suplantación, es decir, manipula los paquetes con direcciones IP desde dentro de la red, esto puede detectarse fácilmente en la pasarela 320 a otras redes, respectivamente a la red internet 400. Por lo tanto, este mecanismo proporciona cierta protección frente a los atacantes exteriores que desean ser añadidos a la lista de pares y falsificar resultados de detección.

El éxito de un sistema inmune biológico es el resultado de la cooperación de sus diversos componentes. Una respuesta del sistema inmune se inicia solamente si tienen lugar simultáneamente diferentes eventos. En el entorno distribuido descrito, se consigue un efecto similar utilizando una variedad de vectores de características y explotando la cooperación entre los agentes AIS basados en anfitrión. De este modo, cada agente AIS está asociado con una métrica de estado que representa la posibilidad de infección, es decir, de anomalía, que se comparte a través del sistema P2P descrito anteriormente.

Una segunda posibilidad de cooperación se presenta cuando un anfitrión detecta una anomalía. Si su propio estado alcanza un umbral predefinido, envía un mensaje a sus vecinos que contiene su estado así como los detectores reales asociados con la alarma. Dichos mensajes se denominan dirigidos por evento. Si un anfitrión obtiene un mensaje dirigido por evento, entonces añade los nuevos detectores a su propio conjunto de detectores y actualiza su propio estado. El nuevo estado se calcula como una función de su propio estado después de ejecutar el módulo de detección, y del estado obtenido a partir de los mensajes recibidos. Sin embargo, en este proceso los agentes proporcionan una ponderación menor al estado de los vecinos que al propio.

Los inventores han realizado simulaciones para mostrar la utilidad del método inventivo. Con este propósito, como parte de una caracterización de un comportamiento cliente "típico", se han registrado diariamente tcpdump de varias estaciones de trabajo Windows en una subred universitaria. Después de un análisis del tráfico capturado, se ha modelado el tráfico de fondo UDP en una red de ejemplo, consistente en clientes no activos.

El perfil de fondo del cliente UDP se proporciona a continuación:

Número de puerto	Protocolo	Paquetes por hora
88	Kerberos	3
123	NTP	1
137	Servicio de Nombres NETBIOS	1
138	Servicio de Datagramas NETBIOS	2
389	CLDAP	6

Los protocolos escogidos y resumidos anteriormente incluyen NETBIOS, que se utiliza para servicios de nombre y de sesión, NTP para sincronización de reloj, Kerberos como protocolo de autenticación estándar para Windows y CLDAP para acceso de directorio X.500. NETBIOS es el único protocolo que utiliza mensajes de difusión, los otros son de unidifusión. El volumen de tráfico en modo inactivo consiste en 13 paquetes por hora y anfitrión. Además, los clientes producen tráfico HTTP para representar interacción de usuarios. Se ha modelado una utilización mayor de

tráfico HTTP por los clientes, en horas específicas del día referidas al comienzo de la jornada de trabajo, después de la pausa del almuerzo y después del horario de trabajo.

Para modelar el comportamiento del cliente se han utilizado perfiles basados en temporizador, en los que HTTP se emula fielmente. Para el tráfico de fondo UDP se han utilizado paquetes UDP con puertos y comportamiento (unidifusión, difusión) correctos, pero sin contenido útil. El contenido de los paquetes UDP individuales no juega ninguna función importante debido a que los flujos de paquetes, puertos utilizados y direcciones IP se han considerado para el análisis sin recurrir a un enfoque de inspección profunda. Cada cliente tiene un subconjunto definido de puertos en los que acepta paquetes. Los paquetes que llegan a estos puertos se consideran intentos de conexión válidos. Se utilizan los siguientes puertos para servicios basados en UDP: 123 (NTP), 137 (Servicio de Nombres NETBIOS), 138 (Servicio de Datagramas NETBIOS) y 1500 (comunicación P2P).

La infraestructura P2P está implementada en base al protocolo UDP proporcionado por una herramienta de simulación de red. Por lo tanto, el puerto 1500 está reservado para ésta. No se consideran puertos TCP válidos, debido a que las conexiones en el protocolo HTTP de la capa de aplicaciones se inician en el lado del cliente. Por lo tanto, ningún cliente necesita escuchar intentos de conexión TCP. En las simulaciones, cada cliente mide conexiones entrantes y salientes utilizando un componente de estadísticas de red que registra datos tales como los puertos utilizados, número de paquetes y si un intento de conexión ha sido válido o no. De estos datos se extraen vectores de características que sirven como entrada para el AIS.

Se simularon dos escenarios en los que cada cliente ejecuta el perfil de cliente de acuerdo con un temporizador global, y en el que parte de los clientes ejecuta un agente AIS. Inhabilitar y habilitar, respectivamente, la infraestructura P2P permite la comparación de los resultados de la detección entre los enfoques cooperativo y no cooperativo.

El AIS en los anfitriones tiene tres fases diferentes: monitorización, aprendizaje y detección. En la fase de monitorización, el componente de medición de los clientes muestrea todos los paquetes entrantes y salientes. Los vectores de características son creados y almacenados a intervalos de tiempo especificados previamente. A continuación se proporcionan los vectores de características utilizados:

Vector de características 1	Vector de características 2
jornada	jornada
TCP de direcciones IP principales	número de conexiones TCP
UDP de direcciones IP principales	número de paquetes UDP
puertos principales	número de puertos utilizados
	número de exploraciones de puertos
	número de paquetes TCP

Durante el periodo de aprendizaje se crea un conjunto de detectores y se compara con los datos de aprendizaje reunidos en la fase de monitorización. Tal como se ha descrito anteriormente, todos los detectores que coinciden con un vector de características del conjunto de aprendizaje son eliminados y se crean detectores nuevos. Los detectores no se crean de manera completamente aleatorizada debido a que el espacio a cubrir sería enorme. En el entorno de la simulación, se utilizó un intervalo limitado de direcciones IP, de manera que se redujo el espacio de direcciones posibles. Lo mismo aplica a los puertos. Por lo tanto, se utilizaron solamente de los números de puerto entre 1 y 450. Se escogió un intervalo de 20 segundos con un multiplicador de 50, que corresponde a 16 minutos en tiempo real.

Durante el periodo de detección, los detectores se compararon con los vectores de características entrantes creados mediante el mismo componente estadístico que el del periodo de monitorización. Si uno o varios detectores coincidían con un vector de características, el estado del AIS se incrementó proporcionalmente a la afinidad y al número de detectores coincidentes. Si el estado alcanza un umbral, se emite una alarma. Los vectores de características que no lanzaron una alarma son almacenados y utilizados para el futuro aprendizaje, de manera que el sistema es adaptativo a las variaciones del entorno.

La cooperación del AIS en la red está basada en el estado compartido. Después de cada cálculo de estado, cada componente AIS envía su estado y un contador a los otros pares a través del sistema P2P, y actualiza su propio estado de acuerdo con el estado entrante de los pares adyacentes. Cada cliente utiliza solamente el estado más reciente durante la actualización, es decir, se ignoran si los valores del estado entrante no están actualizados. Con este propósito puede proporcionarse, por ejemplo, una marca de tiempo.

Los dos escenarios simulados son escenarios de ataque diferentes en una subred típica, tal como un departamento de una universidad o una pequeña empresa.

El primer escenario se refiere a un anfitrión en peligro en una subred. En este escenario, uno de los ordenadores cliente ha sido puesto en peligro por un atacante. Esto significa que se ha explotado una vulnerabilidad del cliente, y el atacante tiene acceso total a los recursos del cliente. De acuerdo con las cinco P "probar, penetrar, persistir, propagar y paralizar", el atacante intenta persistir en la máquina que ha puesto en peligro, por ejemplo instalando una puerta trasera. La siguiente etapa es la etapa de "propagar", en la que se explora la subred en busca de otras vulnerabilidades adicionales. En este escenario, se modela un perfil de exploración de puertos que extiende el perfil de cliente definido previamente. Este perfil incluye una exploración de varios puertos en todos los clientes en la red en su conjunto, durante un periodo de tiempo variable.

El segundo escenario se refiere a la detección de un ataque de gusano. En este escenario, un anfitrión es infectado por un gusano que se difunde mediante solamente un paquete UDP, tal como lo hizo el tristemente célebre gusano Slammer. El gusano utiliza solamente un único puerto (puerto 137). Sin embargo, si alcanza un anfitrión que proporciona el puerto, el anfitrión es infectado con una probabilidad de 0,7. Si un cliente es infectado por el gusano, comienza a enviar el mismo paquete UDP a direcciones IP creadas aleatoriamente, e intenta infectar a otros clientes.

Como resultado de la simulación, a continuación se proporciona la tasa de detección y la tasa de falsos positivos, para un solo AIS y para el enfoque colaborativo, en los dos escenarios descritos anteriormente.

Escenario	falsos positivos	positivos verdaderos
1, uno solo	25%	79%
1, cooperativo	18%	100%
2, uno solo	16%	54%
2, cooperativo	10%	57%

Tal como puede verse a partir de los resultados de la simulación, el enfoque cooperativo propuesto por la invención para detectar un funcionamiento anómalo dentro de una red informática, consigue no sólo una precisión incrementada con respecto a los positivos verdaderos, sino asimismo una reducción significativa de las tasas de falsos positivos.

REIVINDICACIONES

1. Un método para detectar un funcionamiento anómalo dentro de una red informática (10) con múltiples nodos de procesamiento de datos (101-103, 201, 202, 210) que están interconectados a efectos de comunicación de datos, en el que:

a) mediante un primer nodo de procesamiento de datos (101; 102; 103) de la red informática (10) se determina un primer valor de estado, que es una medida de la probabilidad de un funcionamiento anómalo,

b) mediante por lo menos un segundo nodo de procesamiento de datos (102, 103; 101, 103; 101, 102) de la red informática (10) se determina un segundo valor de estado, que es una medida de la probabilidad de un funcionamiento anómalo,

c) dicho segundo valor de estado se transmite desde dicho por lo menos un segundo nodo de procesamiento de datos (102, 103; 101, 103; 101, 102) a dicho primer nodo de procesamiento de datos (101; 102; 103) a través de una comunicación entre pares,

d) a partir de dichos primer y segundo valores de estado se determina un tercer valor de estado mediante el nodo de procesamiento de datos (101; 102; 103), y

e) dependiendo del tercer valor de estado, se determina si ha ocurrido un funcionamiento anómalo, **caracterizado porque** la etapa de determinar dicho tercer valor de estado comprende las etapas de

- determinar un valor promedio de dichos segundos valores de estado,

- ponderar el primer valor de estado con un primer factor de ponderación,

- ponderar dicho valor promedio con un segundo factor de ponderación, y

- sumar el primer valor de estado ponderado y el valor promedio ponderado, obteniéndose de ese modo dicho tercer valor de estado.

2. El método acorde con la reivindicación 1, en el que las etapas a) a e) se repiten en momentos predefinidos.

3. El método acorde con la reivindicación 1 ó 2, en el que la determinación de dicho primer valor de estado se realiza por medio de un algoritmo basado en un sistema inmune artificial.

4. El método acorde con la reivindicación 3, que comprende además la etapa de almacenar en el primer nodo de procesamiento de datos, por lo menos un conjunto de vectores de referencia que están asociados con un funcionamiento anómalo,

en el que la etapa de determinar dicho primer valor de estado comprende las etapas de

- monitorizar tráfico de datos de la red,

- determinar por lo menos un vector de datos de tráfico a partir del tráfico de red monitorizado, en el que cada uno de los componentes del vector de dicho vector de datos de tráfico está asociado con una respectiva característica predefinida del tráfico de datos de la red monitorizado,

- determinar las distancias entre cada vector de datos de tráfico y cada vector de referencia de un conjunto respectivo de los conjuntos almacenados de vectores de referencia (121, 122, 12N), mediante una medida predeterminada de la distancia.

5. El método acorde con la reivindicación 4, en el que se almacenan por lo menos dos conjuntos diferentes de vectores de referencia (121, 122, 12N), y se determinan por lo menos dos vectores de datos de tráfico diferentes.

6. El método acorde con la reivindicación 4 ó 5, en el que la medida predefinida de la distancia es la distancia de Hamming o la distancia euclídea.

7. El método acorde con cualquiera de las reivindicaciones 4 a 6, en el que el primer valor de estado está representado por un contador, y en el que dicho contador se incrementa para cada vector de referencia para el que se determina que la distancia al respectivo vector de datos de tráfico está por debajo de un umbral predefinido.

8. El método acorde con la reivindicación 7, en el que dicho contador se incrementa mediante un valor que es inversamente proporcional a dicha distancia.

9. El método acorde con cualquiera de las reivindicaciones 4 a 8, en el que cada conjunto de vectores de referencia (121, 122, 12N) se determina inicialmente mediante el primer nodo de procesamiento (101; 102; 103), llevando a cabo las etapas de

aa) determinar datos de aprendizaje que representan un comportamiento normal del sistema, mediante monitorizar el tráfico de red durante una fase de aprendizaje, comprendiendo dichos datos de aprendizaje múltiples vectores de datos de tráfico,

bb) generar un vector de datos aleatorio,

cc) comparar dicho vector de datos aleatorio con cada vector de datos de tráfico de dichos datos de aprendizaje,

dd) añadir dicho vector de datos aleatorio al conjunto de vectores de referencia (121, 122, 12N) si no coincide con ninguno de los vectores de datos de tráfico de dichos datos de aprendizaje, en el que se define que los vectores coinciden si su distancia está por debajo del umbral predefinido, y

ee) repetir las etapas bb) a dd) hasta que el conjunto de vectores de referencia (121, 122, 12N) comprende un número predefinido de vectores de referencia.

10. El método acorde con la reivindicación 9, en el que cada vector de referencia de cada conjunto de vectores de referencia (121, 122, 12N) está asociado con una vida útil predefinida, después de la cual es eliminado del conjunto (121, 122, 12N) y sustituido por un nuevo vector de referencia que se determina realizando las etapas bb) a ee).

11. El método acorde con cualquiera de las reivindicaciones 4 a 10, que comprende además las etapas de

- seleccionar por lo menos un vector de referencia para el cual se ha determinado que la distancia a un vector de datos de tráfico está por debajo del umbral predefinido,

- generar por lo menos un vector modificado, modificando cada componente de vectorial de dicho vector de referencia seleccionado, mediante una cantidad aleatoria que queda dentro de un intervalo predefinido, y

- añadir dicho vector modificado al respectivo conjunto de vectores de referencia (121, 122, 12N).

12. El método acorde con cualquiera de las reivindicaciones anteriores, en el que dicho primer factor de ponderación es mayor que dicho segundo factor de ponderación.

13. El método acorde con cualquiera de las reivindicaciones anteriores, en el que la suma de dichos primer y segundo factores de ponderación vale 1.

14. El método acorde con cualquiera de las reivindicaciones anteriores,

en el que la relación entre el primer y el segundo factores de ponderación es esencialmente igual a una relación seleccionada entre el grupo que consiste en 60:40, 70:30, 80:20 y 90:10.

15. El método acorde con cualquiera de las reivindicaciones anteriores, en el que una señal de alarma es generada por el primer nodo de procesamiento de datos (101; 102; 103) cuando el tercer valor de estado supera un umbral predefinido.

16. El método acorde con la reivindicación 15, en el que dicha señal de alarma se transmite desde el primer nodo de procesamiento de datos (101; 102; 103) a un nodo administrativo de monitorización (210).

17. El método acorde con cualquiera de las reivindicaciones anteriores, en el que cada uno de los segundos valores de estado se determina mediante el respectivo segundo nodo de procesamiento de datos (102, 103; 101, 103; 101, 102), tal como se define mediante cualquiera de las reivindicaciones 3 a 11, con respecto al primer valor de estado.

18. El método acorde con cualquiera de las reivindicaciones anteriores, en el que cada uno de los segundos valores de estado se determina mediante el respectivo segundo nodo de procesamiento de datos (102, 103; 101, 103; 101, 102), tal como se define mediante cualquiera de las reivindicaciones 12 a 15, con respecto al tercer valor de estado.

19. El método acorde con cualquiera de las reivindicaciones 4 a 18, en el que el primer nodo de procesamiento de datos (101; 102; 103) transmite, en respuesta a la determinación de que se ha producido un funcionamiento anómalo, el tercer valor de estado y los respectivos vectores de referencia asociados con el funcionamiento anómalo, a dicho por lo menos un segundo nodo de procesamiento de datos (102, 103; 101, 103; 101, 102).

20. Un dispositivo de procesamiento de datos (101; 102; 103) adaptado para la detección de funcionamiento anómalo dentro de una red informática (10), que comprende

- una interfaz de red (160) que está adaptada para recibir, mediante una comunicación entre pares desde por lo menos otro dispositivo de procesamiento de datos (102, 103; 101, 103; 101, 102) predefinido, un segundo valor de estado que es una medida de la probabilidad de un funcionamiento anómalo dentro de la red informática (10),

- una unidad de monitorización (170) para monitorizar el tráfico de datos de la red,

- por lo menos una unidad de detección de anomalías (111, 112, 11N) adaptada para determinar un primer valor de estado, que es una medida de la probabilidad de un funcionamiento anómalo dentro de la red informática (10),

- una unidad de colaboración (150) adaptada para determinar un tercer valor de estado a partir de dicho primer valor de estado y de dichos segundos valores de estado, y

- medios de determinación para determinar, en función de dicho tercer valor de estado, si se ha producido un funcionamiento anómalo, **caracterizado porque**

la unidad de colaboración (150) está adaptada para determinar dicho tercer valor de estado mediante

- determinar un valor promedio de dichos segundos valores de estado,

- ponderar el primer valor de estado con un primer factor de ponderación,

- ponderar dicho valor promedio con un segundo factor de ponderación, y

- sumar el primer valor de estado ponderado y el valor promedio ponderado, obteniéndose de ese modo dicho tercer valor de estado.

21. El dispositivo acorde con la reivindicación 20, en el que cada unidad de detección de anomalías (111, 112, 11N) y la unidad de colaboración (10) están adaptadas respectivamente para determinar automáticamente primeros y terceros valores de estado en tiempos predefinidos.

22. El dispositivo acorde con la reivindicación 20 ó 21, en el que cada unidad de detección de anomalías (111, 112, 11N) está adaptada para determinar primeros valores de estado mediante un algoritmo basado en un sistema inmune artificial.

23. El dispositivo acorde con la reivindicación 22, adaptado para determinar para cada unidad de detección de anomalías un vector de datos de tráfico a partir de tráfico de red monitorizado, en el que cada uno de los componentes vectoriales de dicho vector de datos de tráfico está asociado con una respectiva característica predefinida del tráfico de datos de red monitorizado, y que comprende medios de almacenamiento para almacenar, para cada unidad de detección de anomalías (111, 112, 11N), un conjunto de vectores de referencia (121, 122, 12N) que están asociados con un funcionamiento anómalo, en el que

cada unidad de detección de anomalías (111, 112, 11N) está adaptada para determinar las distancias entre un respectivo vector de datos de tráfico y cada vector de referencia del respectivo conjunto de entre los conjuntos almacenados de vectores de referencia (121, 122, 12N), mediante una medida predefinida de la distancia.

24. El dispositivo acorde con la reivindicación 23, que comprende por lo menos dos unidades de detección de anomalías (111, 112, 11N).

25. El dispositivo acorde con cualquiera de las reivindicaciones 23 ó 24, en el que cada unidad de detección de anomalías (111, 112, 11N) comprende un contador, en el que la lectura del contador representa el primer valor de estado, y está adaptada para incrementar dicho contador para cada vector de referencia para el cual se determina que la distancia hasta el respectivo vector de datos de tráfico está por debajo de un umbral predefinido.

26. El dispositivo acorde con la reivindicación 25, en el que cada unidad de detección de anomalías (111, 112, 11N) está adaptada para incrementar dicho contador en un valor que es inversamente proporcional a dicha distancia.

27. El dispositivo acorde con cualquiera de las reivindicaciones 23 a 26, adaptado para determinar cada conjunto de vectores de referencia (121, 122, 12N), mediante la realización de las etapas de

aa) determinar datos de aprendizaje que representan un comportamiento normal del sistema, mediante monitorizar el tráfico de red durante una fase de aprendizaje, comprendiendo dichos datos de aprendizaje múltiples vectores de datos de tráfico,

bb) generar un vector de datos aleatorio,

cc) comparar dicho vector de datos aleatorio con cada vector de datos de tráfico de dichos datos de aprendizaje,

dd) añadir dicho vector de datos aleatorio al conjunto de vectores de referencia (121, 122, 12N) si no coincide con ninguno de los vectores de datos de tráfico de dichos datos de aprendizaje, en el que se define que los vectores coinciden si su distancia está por debajo del umbral predefinido, y

ee) repetir las etapas bb) a dd) hasta que el conjunto de vectores de referencia (121, 122, 12N) comprende un número predefinido de vectores de referencia.

28. El dispositivo acorde con la reivindicación 27, adaptado para eliminar cada vector de referencia de cada conjunto de vectores de referencia (121, 122, 12N) después de una vida útil predefinida asociada, y para sustituirlo por un nuevo vector de referencia que se determina llevando a cabo las etapas bb) a ee).

29. El dispositivo acorde con cualquiera de las reivindicaciones 23 a 28, en el que cada unidad de detección de anomalías (111, 112, 11N) está adaptada para

- seleccionar por lo menos un vector de referencia del respectivo conjunto de vectores de referencia (121, 122, 12N) para el que se ha determinado que la distancia hasta un vector de datos de tráfico está por debajo del umbral predefinido,

- generar un vector modificado, modificando cada componente vectorial de dicho vector de referencia seleccionado, en una cantidad aleatoria que está dentro de un intervalo predefinido, y

- añadir dicho vector modificado al respectivo conjunto de vectores de referencia (121, 122, 12N).

30. El dispositivo acorde con cualquiera de las reivindicaciones anteriores, adaptado para generar una señal de alarma cuando el tercer valor de estado supera un umbral predefinido.

31. El dispositivo acorde con cualquiera de las reivindicaciones anteriores, adaptado para transmitir el primer y/o el tercer valor de estado, mediante una comunicación entre pares, por lo menos a otro dispositivo de procesamiento de datos predefinido (102, 103; 101, 103; 101, 102).

32. El dispositivo acorde con cualquiera de las reivindicaciones 23 a 31, adaptado para transmitir, en respuesta a la determinación de que se ha producido un funcionamiento anómalo, el tercer valor de estado y los respectivos vectores de referencia asociados con el funcionamiento anómalo, por lo menos a otro dispositivo de procesamiento de datos predefinido (102, 103; 101, 103; 101, 102).

33. Una red informática (10) con múltiples nodos de procesamiento de datos (101-103, 201, 202, 210) que están interconectados a efectos de comunicación de datos,

en la que por lo menos dos de dichos nodos de procesamiento de datos (101-103) están dispuestos como dispositivos de detección de anomalías, de acuerdo con cualquiera de las reivindicaciones 20 a 32.

34. La red informática acorde con la reivindicación 33, que comprende además un nodo central administrativo (210) adaptado para recibir señales de alarma desde dichos dispositivos de detección de anomalías (101-103).

35. La red informática acorde con la reivindicación 33 ó 34, en la que dichos dispositivos de detección de anomalías (101-103) están adaptados para comunicar mediante comunicación entre pares.

36. La red informática acorde con la reivindicación 35, en la que cada uno de dichos dispositivos de detección de anomalías (101-103) está adaptado para funcionar como un nodo maestro para la comunicación entre pares, en la que dicho el nodo maestro está adaptado para proporcionar una lista de todos los dispositivos de detección de anomalías (101-103) que están conectados a la red informática (10).

Fig. 1

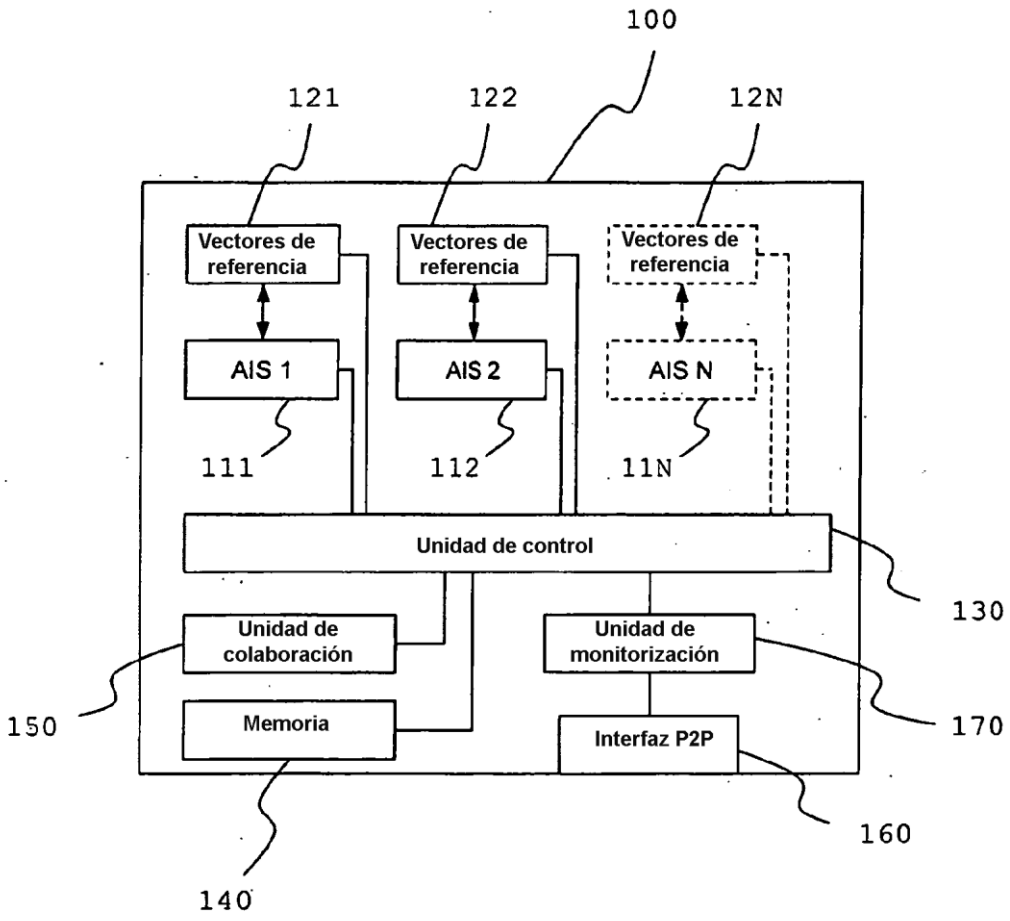

100
121
122
12N
Vectores de referencia
Vectores de referencia
Vectores de referencia
AIS 1
AIS 2
AIS N
111
112
11N
Unidad de control
130
Unidad de colaboración
Unidad de monitorización
150
170
Memoria
Interfaz P2P
160
140

Fig. 2

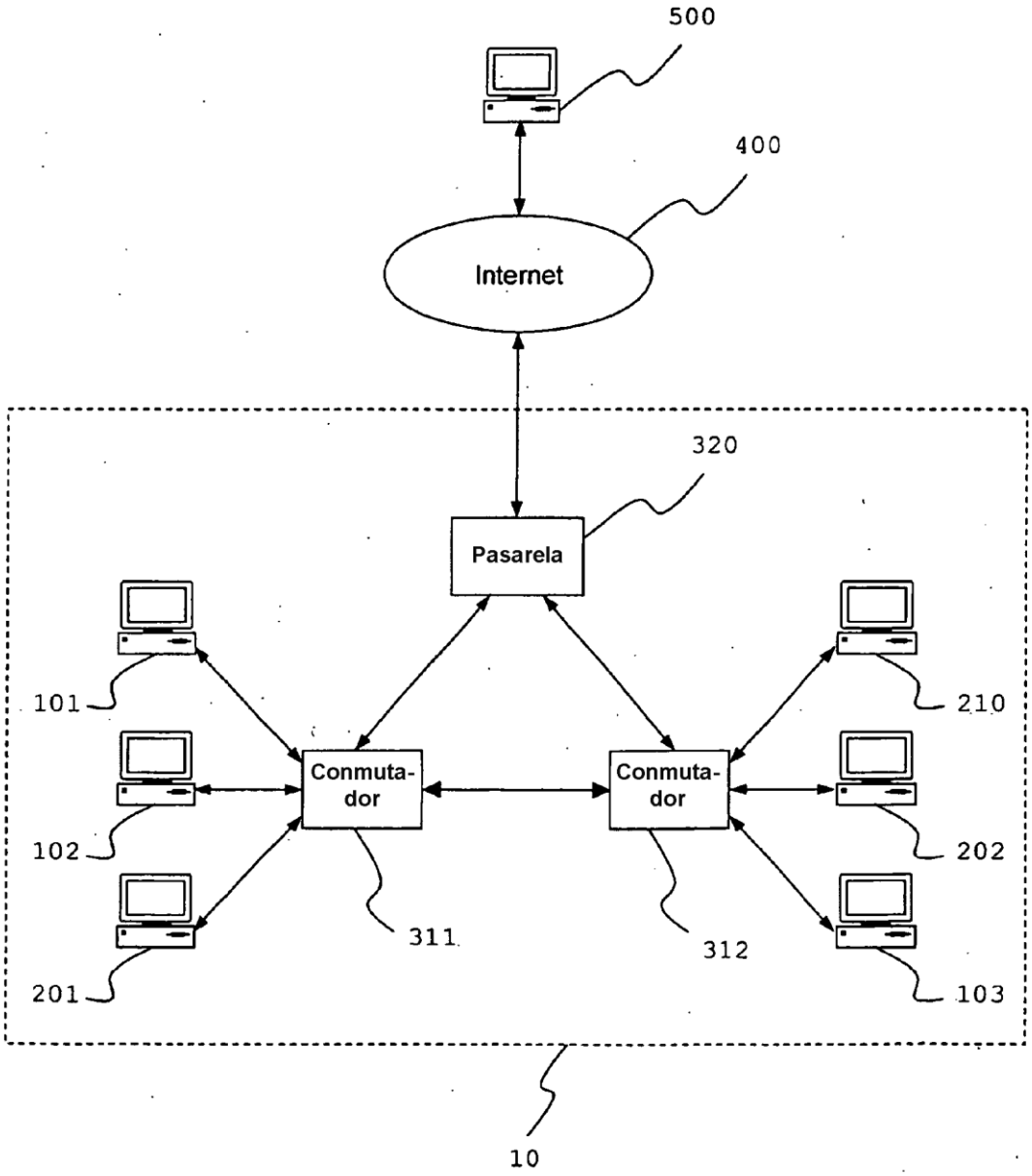
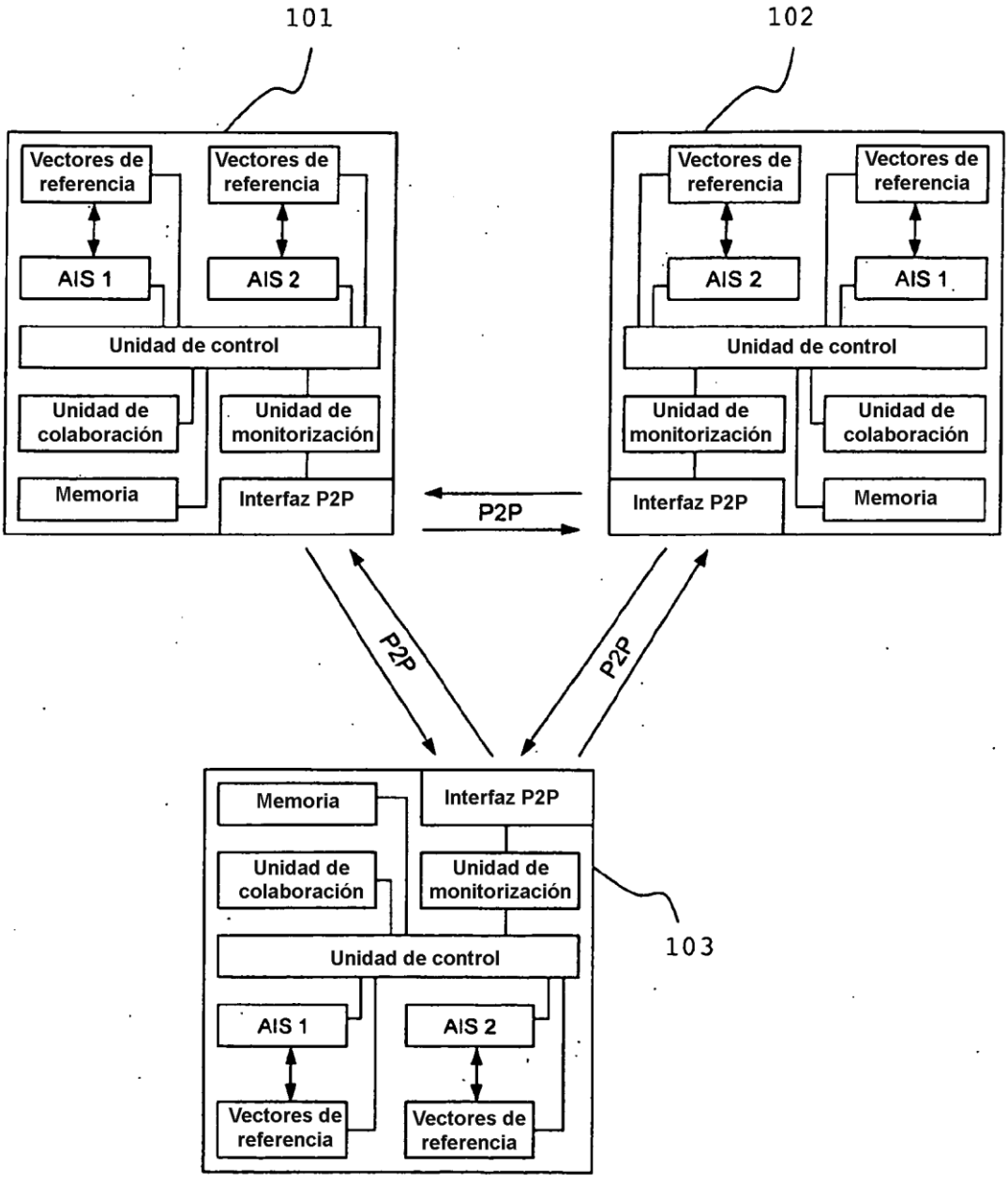

500
400
Internet
320
Pasarela
101
102
201
Conmuta-
dor
311
Conmuta-
dor
312
210
202
103
10

Fig. 3


101
102
Vectores de referencia
Vectores de referencia
AIS 1
AIS 2
Unidad de control
Unidad de colaboración
Unidad de monitorización
Memoria
Interfaz P2P
P2P
Vectores de referencia
Vectores de referencia
AIS 2
AIS 1
Unidad de control
Unidad de monitorización
Unidad de colaboración
Interfaz P2P
Memoria
P2P
P2P
Memoria
Interfaz P2P
Unidad de colaboración
Unidad de monitorización
Unidad de control
AIS 1
AIS 2
Vectores de referencia
Vectores de referencia
103