(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 602 802**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.09.2007 PCT/US2007/080023**

(87) Fecha y número de publicación internacional: **10.04.2008 WO08042824**

(96) Fecha de presentación y número de la solicitud europea: **29.09.2007 E 07843575 (7)**

(97) Fecha y número de publicación de la concesión europea: **17.08.2016 EP 2082555**

(54) Título: **Detección de anomalía de red de inteligencia usando una red neuronal difusa de tipo II**

(30) Prioridad:

29.09.2006 US 536842

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.02.2017

(73) Titular/es:

ALCATEL LUCENT (100.0%)
148/152 route de la Reine
92100 Boulogne-Billancourt, FR

(72) Inventor/es:

YEH, CHIANG;
TOUVE, JEREMY y
SANGRONIZ, R., LEON

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Detección de anomalía de red de inteligencia usando una red neuronal difusa de tipo II

Campo técnico

La presente invención se refiere a un detector de anomalía y a un procedimiento para usar una red neuronal difusa de tipo II para identificar síntomas de un ataque/anomalía (que se dirige a una red privada) y para sugerir escalar acciones correctivas (que pueden implementarse por un dispositivo de red) hasta que empiecen a desaparecer los síntomas del ataque/anomalía.

Antecedentes

Los dispositivos de interconexión en red actuales (por ejemplo, conmutador de Ethernet de capa 3) a menudo usan técnica post mortem o técnica de medidas preventivas para detectar y corregir anomalías/ataques de red. En el primer caso, el dispositivo de interconexión en red recopila una cantidad extensiva de estadísticas de red y a continuación envía esta información a una instalación externa para identificar patrones conocidos o firmas de ataques/anomalías organizados o actividades de red indeseables. Puesto que los requisitos para cotejar, contabilizar y analizar estas estadísticas de red exigen una cantidad exhaustiva de número de capacidades de compresión y búsqueda, esta instalación externa identifica la anomalía/ataque después de que ya ha dañado la red.

En el último caso, el dispositivo de interconexión en red está programado con un conjunto de máscaras de filtro, árboles de decisión, o heurística complicada que corresponde a patrones conocidos o firmas de ataques/anomalías organizados o actividades de red indeseables. Estos mecanismos únicamente reconocen los ataques/anomalías usando reglas permanentes y rápidas que son bastante eficaces en rastreo fijo y patrones organizados de ataques/anomalías. Una vez identificados, el dispositivo de interconexión en red toma las etapas apropiadas para tratar los síntomas de los ataques/anomalías ofensores. Esta técnica particular funciona bien si el ataque/anomalía tiene un intervalo estricto de comportamientos y deja una firma bien conocida.

Algunos dispositivos de interconexión en red usan una combinación de la técnica post mortem y la técnica de medidas preventivas para detectar y corregir anomalías/ataques de red. Puesto que los procedimientos de ataque más dañinos y reconocibles, por ejemplo, denegación de servicio, exploración de puertos, etc., tienen firmas muy distintas, este tipo de dispositivo de interconexión en red puede identificar satisfactoriamente y corregir muchos de estos ataques/anomalías. Por ejemplo, un administrador de red puede programar fácilmente un conjunto de máscaras de filtro, árboles de decisión, o heurística complicada para detectar y corregir los problemas producidos por un ataque/anomalía que muestra un intervalo estricto de comportamientos y deja una firma bien conocida. Sin embargo, los tipos más nuevos de ataques/anomalías que se usan comúnmente hoy en día no se comportan de una manera predecible o dejan una firma distinta. Por ejemplo, existe una nueva generación de gusanos que tienen un intervalo de actividades que no son fácilmente identificables cuando migran a través de una red, puesto que estos gusanos más nuevos usan algoritmos biológicos que les produce que transmuten sus comportamientos a medida que migran y se reproducen en una red.

Como resultado, estas técnicas bien conocidas pueden no rendir muy bien puesto que dependen del conocimiento íntimo acerca de la causa del ataque/anomalía antes de que puedan reconocer el ataque/anomalía y tomar acciones correctivas para corregir los síntomas del ataque/anomalía. Además, estas técnicas a menudo necesitan tomar un curso discreto de acciones correctivas independientemente del grado del ataque/anomalía (a menos que el administrador de red defina específicamente cada grado del ataque que desea tratar, que, en esencia, presenta cada grado del ataque como una nueva clase de ataque). Por consiguiente, existe una necesidad para una nueva técnica que pueda detectar un ataque/anomalía (especialmente uno de los tipos más nuevos de gusanos transmutables) y sugiera escalar acciones hasta que los síntomas del ataque/anomalía empiecen a desaparecer. Esta y otras necesidades se tratan por el detector de anomalía y el procedimiento de detección de anomalía de la presente invención.

La publicación de Solicitud de Patente de Estados Unidos N. º 2004/0250124 A1 desvela un procedimiento para proteger una red de un ataque que incluye medir una propiedad de tráfico que entra en la red, y analizar la propiedad usando al menos un algoritmo de lógica difusa para detectar el ataque.

Breve descripción de la invención

Un detector de anomalía y un procedimiento se indican en las reivindicaciones independientes 1 y 7, respectivamente. La presente invención incluye un detector de anomalía y un procedimiento para usar una red neuronal difusa de tipo II que puede rastrear síntomas de un ataque y sugerir escalar acciones correctivas hasta que los síntomas del ataque empiecen a desaparecer. En una realización, el detector de anomalía usa una red neuronal difusa de tipo II en tres niveles donde el primer nivel tiene múltiples funciones de pertenencia μ_1-μ_i que recopilan estadísticas acerca de diferentes aspectos de la “salud” de un dispositivo de red y procesan estos números en métricas que tienen valores entre 0 y 1. El segundo nivel tiene múltiples sumadores Π_1-Π_m cada uno de los cuales interconecta con funciones de pertenencia seleccionadas μ_1-μ_i para obtener sus métricas y a continuación emiten una suma continua (probabilística, no numérica). El tercer nivel 206 tiene múltiples agregadores Σ_1-Σ_k cada uno de

los cuales agrega las sumas de los sumadores seleccionados Π_1-Π_m y calcula una media continua que se compara a reglas de control de lógica difusa (localizadas dentro de una tabla si-entonces-sino) para determinar un curso particular de acción que el dispositivo de red puede seguir para tratar los síntomas de un ataque.

Breve descripción de los dibujos

Un entendimiento más completo de la presente invención puede obtenerse por referencia a la siguiente descripción detallada cuando se toma en conjunto con los dibujos adjuntos en los que:

La Figura 1 es un diagrama de un dispositivo de red que interactúa con un detector de anomalía que funciona para proteger una red privada de acuerdo con la presente invención;
La Figura 2 es un diagrama del detector de anomalía que usa una red neuronal difusa de tipo II en tres niveles para proteger la red privada de acuerdo con una realización de la presente invención; y
La Figura 3 es un diagrama que ilustra las etapas básicas que pueden realizarse por el detector de anomalía que usa la red neuronal difusa de tipo II en tres niveles para proteger la red privada de acuerdo con una realización de la presente invención.

Descripción detallada de las figuras

Haciendo referencia a la Figura 1, se muestra un diagrama que se usa para ayudar a explicar cómo un dispositivo 100 de red puede interconectar con un detector 102 de anomalía que identifica síntomas de un ataque y sugiere escalar acciones correctivas que el dispositivo 100 de red puede a continuación seguir para tratar los síntomas del ataque de acuerdo con la presente invención. En este escenario ejemplar, el dispositivo 100 de red interconectando con el detector 102 de anomalía (que también puede estar localizado en el dispositivo 100 de red) puede proteger una red 104 privada de ataques y posibles amenazas que se originan desde una red 106 pública. Además, el dispositivo 100 de red interconectando con el detector 102 de anomalía puede proteger la red 104 privada de ataques y abusos potenciales de sus propios usuarios. Se proporciona un análisis detallado a continuación para explicar cómo el detector 102 de anomalía recibe estadísticas 108 de red, procesa estas estadísticas 108 de red y a continuación emite la acción o acciones 110 correctivas que pueden implementarse por el dispositivo 100 de red para proteger la red 104 privada.

El detector 102 de anomalía usa inteligencia artificial para introducir una medida de adaptabilidad en el procedimiento de detección de anomalía que es deseable debido a que la naturaleza de los ataques de red más nuevos (por ejemplo, gusanos transmutables) a menudo es convoluta, y más a menudo, desconocida. En una realización, el detector 102 de anomalía posibilita esta medida de adaptabilidad usando una forma de inteligencia artificial denominada en el presente documento como una red 112 neuronal difusa de tipo II (véanse las Figuras 2 y 3). La red 112 neuronal difusa de tipo II puede usar conocimiento parcial tomado a partir de las estadísticas 108 de red recopiladas para identificar y rastrear los síntomas de un ataque antes de que sugiera escalar acciones 110 correctivas para tratar los síntomas del ataque. Por lo tanto, la red 112 neuronal difusa de tipo II no necesita deducir la causa raíz de un ataque antes de que pueda detectar un ataque y sugerir las acciones 110 correctivas necesarias para tratar los síntomas del ataque.

La red 112 neuronal difusa de tipo II es diferente de una red neuronal tradicional en que sus condiciones para aprender están basadas en heurística sencilla en lugar de filtros adaptativos complicados. Esta heurística sencilla permite errores numéricos indefinidos en la adaptación denominados “difusividad”. Es esta naturaleza “difusa” la que permite al detector 102 de anomalía rastrear un problema esquivo descubriendo una tendencia general sin necesitar tener la precisión de datos que se requieren por una red neuronal tradicional que usa filtros adaptativos complicados. Una realización ejemplar de una red 112 neuronal difusa de tipo II que tiene una estructura de control en tres niveles se analiza a continuación con respecto a las Figuras 2 y 3.

Haciendo referencia a la Figura 2, se muestra un diagrama de una red 112 neuronal difusa de tipo II en tres niveles ejemplar que se usa por el detector 102 de anomalía para identificar síntomas de un ataque y para sugerir escalar acciones correctivas que pueden implementarse hasta que los síntomas del ataque empiecen a desaparecer de acuerdo con la presente invención. Como se muestra, el primer nivel 202 tiene múltiples funciones de pertenencia μ_1-μ_i que recopilan estadísticas 108 acerca de diferentes aspectos de la “salud” del dispositivo 100 de red y procesan estos números en métricas que tienen valores que están entre 0 y 1. El segundo nivel 204 tiene múltiples sumadores Π_1-Π_m cada uno de los cuales interconecta con funciones de pertenencia seleccionadas μ_1-μ_i para obtener sus métricas y a continuación procesa/emite una suma continua (probabilística, no numérica). El tercer nivel 206 tiene múltiples agregadores Σ_1-Σ_k cada uno de los cuales agrega las sumas de los sumadores seleccionados Π_1-Π_m y calcula una media continua que se compara a reglas de control de lógica difusa localizadas dentro de una correspondiente tabla 208_1 y 208_k si-entonces-sino para determinar un curso de la acción 110 que el dispositivo 100 de red puede a continuación seguir para tratar los síntomas de un ataque. En particular, el tercer nivel 206 tiene múltiples tablas 208_1 y 208_k si-entonces-sino cada una de las cuales recibe una media continua desde un respectivo agregador Σ_1-Σ_k y basándose en esa entrada realiza un análisis si-entonces-sino y a continuación emite la acción 110 que el dispositivo 100 de red puede a continuación implementar para tratar los síntomas de un ataque.

En una aplicación particular, cada función de pertenencia μ_1-μ_i recopila las estadísticas 108 acerca de un aspecto específico del dispositivo 100 de red y a continuación produce una única métrica para representar la "salud" de ese aspecto particular del dispositivo 100 de red. Esta métrica tiene una puntuación entre 0 y 1 que significa que la correspondiente función de pertenencia puede representarse como $\mu \varepsilon \{0..1\}$. La puntuación de métrica es una fracción de una estadística de red que el dispositivo 100 de red está recopilando actualmente, por ejemplo el número de paquetes a través de una interfaz particular, el número de bits a través de una interfaz particular, el número de conexiones de http a través de una interfaz particular, etc..., frente a un máximo teórico. Por ejemplo: μ_1 = caudal del puerto A = (número de bits transmitidos por el puerto A/segundo)/(velocidad de enlace por segundo del puerto A). Por lo tanto, una puntuación más alta de una métrica es más deseable que una puntuación más baja puesto que la primera es indicativa de un estado superior de salud. Como puede apreciarse, no hay límite en cuanto a qué tipo de aspecto (estadística asociada con el dispositivo 100 de red) puede transmitir una función de pertenencia en su valor de μ. Además, cuanto más precisas define un administrador de red las funciones de pertenencia μ_1-μ_i mejor va a comportarse el detector 102 de anomalía total.

En el segundo nivel 204, las métricas a partir de funciones de pertenencia seleccionadas μ_1-μ_i se suman por uno de los sumadores Π_1-Π_m para producir una puntuación total μ_{total}. Puesto que ciertas funciones de pertenencia individuales μ_1-μ_i pueden influenciar la puntuación total de diferentes maneras. Los sumadores Π_1-Π_m pueden modelar una o más de las funciones de pertenencia individuales μ_1-μ_i con pesos variables "w" por lo que pueden tener un efecto compensatorio deseado en la puntuación total μ_{total}. En un ejemplo, esta puntuación total μ_{total} puede calcularse como sigue (ecuación n .º 1):

$$\mu_{total} = \left(\prod \left(\mu_i^{w(i)} * \mu'_i{}^{w(i)}\right)\right)^{\beta} * \left(1 - \prod \left((1 - \mu_i)^{w(i)} * (1 - \mu'_i)^{w(i)}\right)\right)^{\gamma}$$

donde $\beta = \gamma - 1$, $\mu_i \varepsilon \{0..1\}$, w(i) = i-ésimo peso para μ_i

La ecuación anterior resulta ser una media geométrica ponderada de μ_i y μ'_i, donde u_i es el i-ésimo factor que afecta a la puntuación total μ_{total}, y μ'_i es la tasa de cambio de μ_i, es decir $\mu'_i = d\mu_i/dt$

En el tercer nivel 206, se suman las seleccionadas de las medias geométricas ponderadas (puntuaciones totales μ_{total}) por uno de los agregadores Σ_1-Σ_k y el resultado se compara frente a una correspondiente tabla 208_1 y 208_k de acciones si-entonces-sino. Como se muestra, cada agregador Σ_1-Σ_k tiene únicamente una asociación de tabla y cada tabla 208_1 y 208_k puede haberse programado para buscar un ataque/anomalía específico y para tratar los síntomas de ese ataque/anomalía específico. Lo siguiente es una ilustración de una tabla 208_1 y 208_k de muestra:

TABLA 1

Si Sum_1 > Th1	…	Y si Sum_m > Th4	Entonces tomar acción 1	Sino no hacer nada
Si (Sum_1 < Th1 & Sum_1 > Th2)	…	Y si (Sum_m < Th4 & Sum_m > Th5)	Entonces tomar acción 2	Sino no hacer nada
…	…	…	Entonces tomar acción 3	Sino tomar acción 4
Si Sum_1 < Th3	…	Y si (Sum_m < Th6)	Entonces tomar acción 5	Sino tomar acción 6
Nota: la tabla 208_1 y 208_k puede contener también múltiples acciones, por ejemplo si (agregador 1 > umbral 1) entonces hacer (acción 1 y acción 2 y acción 3) sino hacer (acción 4 y acción 5).				

Las acciones 110 anteriormente ilustradas son las etapas que puede tomar el dispositivo 100 de interconexión en red para protegerse a sí mismo de un ataque/anomalía. Por ejemplo, el detector 102 de anomalía puede haber detectado congestión de red potencial en una interfaz particular en el dispositivo 100 de red basándose en el patrón de tráfico actual, es decir cuando su agregador Σ_1 para congestión supera un umbral particular. Si esta suma del agregador está entre un umbral grave y un umbral leve, entonces la acción 110 desencadenada por el agregador Σ_1 puede ser tener que marcar el dispositivo 100 de interconexión en red todo el tráfico posterior con una prioridad de Punto de Código de Servicios Diferenciados (DSCP) baja. Si la suma del agregador supera el umbral grave, entonces la acción 110 desencadenada por el agregador Σ_1 puede ser tener que interrumpir el dispositivo 100 de interconexión en red todo el tráfico posterior en la interfaz bajo congestión.

En otro ejemplo, el dispositivo 100 de interconexión en red puede presenciar un número sospechosamente grande de solicitudes de Protocolo de Transferencia de Hipertexto (HTTP), seguido por un número grande de abortos de HTTP de un pequeño número de direcciones de Protocolo de Internet (IP), en un patrón predictivo e intervalo fijo. El detector 102 de anomalía podría rastrear este patrón agregando ambas de estas variables y a continuación tratar este problema emitiendo una acción 110 que puede implementarse por el dispositivo 100 de interconexión en red. En este ejemplo, se supone que el operador de red tiene conocimiento a priori acerca de esta anomalía particular, por lo tanto puede configurar apropiadamente las funciones de pertenencia μ_1-μ_n (y ponderar también las funciones de pertenencia μ_1-μ_n), los sumadores Π_1-Π_m, los agregadores Σ_1-Σ_k y/o las tablas 208_1 y 208_k si-entonces-sino. Como alternativa, el detector 102 de anomalía podría usarse también para detectar y tratar ataques/anomalías

inesperados (esta capacidad particular se analiza en más detalle a continuación).

Como una realización de muestra, se puede implementar la red 112 neuronal difusa de tipo II en tres niveles en una pieza de un equipo 100 de interconexión en red, por ejemplo, un conmutador 100 de Ethernet de capa 3, que ya mantiene un extenso conjunto de estadísticas. En este caso, las funciones de pertenencia de nivel 1 μ_1-μ_i tomarían periódicamente estas estadísticas y las convertirían en métricas/fracciones que se alimentan en uno o más sumadores de nivel 2 Π_1-Π_m. Por ejemplo, una de las funciones de pertenencia μ_1 podría tomar la estadística relacionada con el número de bits que pasa una interfaz por segundo y dividir este número frente a la velocidad de puerto para producir una métrica/fracción entre {0..1} que sería indicativa de la utilización de enlace. Además, para calcular la primera métrica/fracción (μ_1), la función de pertenencia de nivel 1 μ_1 calcularía también el diferencial de tiempo de esa métrica/fracción (μ_1'). Para conseguir esto, la función de pertenencia μ_1 podría calcular por ejemplo la pendiente de puntos sucesivos μ_1(t), extraer un valor angular de manera trigonométrica, y dividir el ángulo frente a 2n.

Posteriormente, los sumadores de nivel 2 Π_1-Π_m reciben cada uno un conjunto único de métricas/fracciones (μ_1-μ_i) y sus correspondientes métricas/fracciones diferenciales de tiempo (μ_1'-μ_i') y calculan la media geométrica ponderada μ_{total} basándose en la ecuación n. º 1 (por ejemplo). Si se desea, los sumadores Π_1-Π_m pueden ponderar cada uno las métricas/fracciones (μ_1-μ_i) con un número entre 0 y 1. El peso asignado de las métricas/fracciones (μ_1-μ_i) indica la importancia relativa de la correspondiente función de pertenencia μ_1-μ_i. Por ejemplo, si se desea rastrear la congestión de red, entonces se ponderaría la utilización de enlace con una potencia superior que el número de conexiones de Protocolo de Control de Transmisión (TCP) abiertas. Por supuesto, la red 112 neuronal difusa de tipo II debería converger independientemente de los pesos asignados a las funciones de pertenencia μ_1-μ_i. Sin embargo, la red 112 neuronal difusa de tipo II se adaptaría más rápido si las funciones de pertenencia μ_1-μ_i hubieran elegido apropiadamente pesos en lugar de si las funciones de pertenencia μ_1-μ_i hubieran elegido pesos malos. Finalmente, los sumadores Π_1-Π_m alimentan sus salidas $\mu_{totales}$ en las seleccionadas de los agregadores de nivel 3 Σ_1-Σ_k cada uno de los cuales agrega las $\mu_{totales}$ recibidas y calcula una media continua que se compara a reglas de control de lógica difusa (localizadas en la correspondiente tabla 208_1 y 208_k si-entonces-sino) para determinar un curso de la acción 110 que el dispositivo 100 de red puede implementar para tratar los síntomas de un ataque.

Haciendo referencia a la Figura 3, existe un diagrama que se usa para explicar de una manera diferente cómo la red 112 neuronal difusa de tipo II en tres niveles ejemplar funciona para ayudar a proteger la red 104 privada de acuerdo con la presente invención. En la etapa 302, las entidades 202 de primer nivel funcionan para observar el estado de sistema recopilando estadísticas y procesándolas en valores fraccionales que pueden manipularse usando matemática de lógica difusa. En la etapa 304, las entidades 204 de segundo nivel funcionan para vincular diversas estadísticas para extraer inferencias. En la etapa 306, las entidades 206 de tercer nivel (únicamente se muestra un Σ_1 y una tabla 208_1 si-entonces-sino) funcionan para usar una serie de las sospechas recibidas desde las entidades 204 de segundo nivel seleccionadas para tomar una decisión acerca de qué acción 110 puede tomar el dispositivo 100 de red para proteger la red 104 privada.

Una ventaja de usar una red 112 neuronal difusa de tipo II es que se puede entrenar la red 112 neuronal difusa de tipo II para aprender acerca de ataques y problemas de red futuros. Por ejemplo, cuando un administrador de red anticipa un brote de nuevos ataques de gusano en la red 106 pública, a continuación pueden soltar el gusano sospechoso en una red experimental y usar este mecanismo para rastrear el patrón del ataque. Posteriormente, el administrador de red puede programar este patrón nuevamente aprendido en un detector 102 de anomalía en directo y entonces la red 104 privada estaría inoculada a tales ataques. El operador puede efectuar la inoculación de dos maneras: (1) puede modificar las tablas 208_1-208_k de reglas con acciones que pueden suprimir el ataque inminente; y/o (2) puede alterar cómo evalúa el segundo nivel 204 la observación u observaciones actualizando la función o funciones de pertenencia μ_1-μ_n (por ejemplo, la ponderación de una observación) o añadiendo nueva función o funciones de pertenencia.

En otro ejemplo, si un administrador de red desea entrenar la red 112 neuronal difusa de tipo II para buscar un nuevo ataque/anomalía, podría programar una de las tablas 208_1 si-entonces-sino para no tomar ninguna acción y a continuación simplemente observar las salidas del agregador correspondiente Σ_1. A continuación, puede diseñar un conjunto específico de acciones que están adaptadas para ese nuevo ataque/anomalía particular. Además, si la red 112 neuronal difusa de tipo II se entrena para proteger frente a amenazas específicas, entonces el procedimiento de entrenamiento en sí mismo junto con las modificaciones de los parámetros difusos puede ayudar también frente a ataques nunca vistos antes. Estos ataques inesperados únicamente necesitan compartir alguno de los mismos elementos asociados con los ataques conocidos para la red neuronal difusa 112 para decidir que son “malos” y aprobar una respuesta. Estos elementos pueden medirse e identificarse fácilmente (por ejemplo pueden ser los paquetes por segundo de un tipo de tráfico específico) y cuantos más de ellos estén agregando el mecanismo, más variados serán los tipos de ataques inesperados que pueden identificarse.

Aunque se ha ilustrado una realización de la presente invención en los dibujos adjuntos y se ha descrito en la anterior descripción detallada, debería entenderse que la presente invención no está limitada a la realización desvelada, sino que pueden hacerse numerosas reorganizaciones, modificaciones y sustituciones sin alejarse de la invención como se expone y define mediante las siguientes reivindicaciones.

REIVINDICACIONES

1. Un detector (102) de anomalía que comprende una red neuronal difusa de tipo II que tiene una estructura (112) de control en tres niveles que rastrea síntomas de un ataque y sugiere escalar acciones (110) correctivas hasta que los síntomas del ataque empiezan a desaparecer, en el que la estructura de control incluye:

un primer nivel (202) que incluye una pluralidad de funciones de pertenencia, donde cada función de pertenencia está adaptada para:

recopilar una estadística (108) de red; y
procesar la estadística recopilada en una métrica

que es la estadística recopilada divida por un máximo teórico de la estadística recopilada;
un segundo nivel (204) que incluye una pluralidad de sumadores, donde cada sumador está adaptado para:

recibir un conjunto único de métricas asociadas con las funciones de pertenencia; y
calcular una media basándose en el conjunto único

de métricas y en una tasa de cambio de cada una de las métricas en el conjunto único; y
un tercer nivel (206) que incluye al menos un agregador y al menos una tabla (208_1, 208_k), donde cada agregador está adaptado para:

recibir un conjunto único de las medias calculadas; y
sumar el conjunto único de las medias calculadas; y
en el que cada tabla se usa para analizar las medias calculadas sumadas para determinar si es necesario un curso de la acción para tratar los síntomas del ataque.

2. El detector de anomalía de la reivindicación 1, en el que dicha estadística de red recopilada incluye:

un número de paquetes a través de una interfaz particular en un dispositivo de red;
un número de bits a través de una interfaz particular en dicho dispositivo de red; o
un número de conexiones de HTTP a través de una interfaz particular en dicho dispositivo de red.

3. El detector de anomalía de la reivindicación 1, en el que dicho cada sumador calcula una media que es una media calculada geométrica ponderada.

4. El detector de anomalía de la reivindicación 1, en el que dicho ataque es un gusano de transmutación que implementa una pluralidad de algoritmos biológicos.

5. El detector de anomalía de la reivindicación 1, en el que dicho ataque es un ataque inesperado.

6. El detector de anomalía de la reivindicación 1, en el que dicho ataque es un ataque esperado.

7. Un procedimiento para tratar un síntoma de un ataque usando una red neuronal difusa de tipo II, comprendiendo dicho procedimiento las etapas de:

recopilar (302) una pluralidad de estadísticas (108) de red;
procesar (302) cada una de las estadísticas de red recopiladas en una métrica que es una fracción de la estadística de red recopilada
dividida por un máximo teórico de la estadística de red recopilada;
calcular (304) una pluralidad de medias cada una de las cuales está basada en un conjunto único de las métricas y una tasa de cambio del conjunto único de las métricas;
agregar (306) un conjunto único de las medias calculadas; y
comparar (306) las medias calculadas agregadas con los valores en una tabla de reglas de decisión si-entonces-sino para determinar una acción para tratar el síntoma del ataque.

8. El procedimiento de la reivindicación 7, en el que dicha etapa de comparación incluye adicionalmente revisar la tabla de reglas de decisión si-entonces-sino para tratar mejor el síntoma del ataque después de revisar las estadísticas de red recopiladas, las medias calculadas y/o las medias calculadas agregadas.

9. El procedimiento de la reivindicación 7, en el que dichas estadísticas de red recopiladas incluyen:

un número de paquetes a través de una interfaz particular en dicho dispositivo de red;
un número de bits a través de una interfaz particular en dicho dispositivo de red; o
un número de conexiones de HTTP a través de una interfaz particular en dicho dispositivo de red.

10. El procedimiento de la reivindicación 7, en el que dicho ataque es un gusano de transmutación que implementa una pluralidad de algoritmos biológicos.

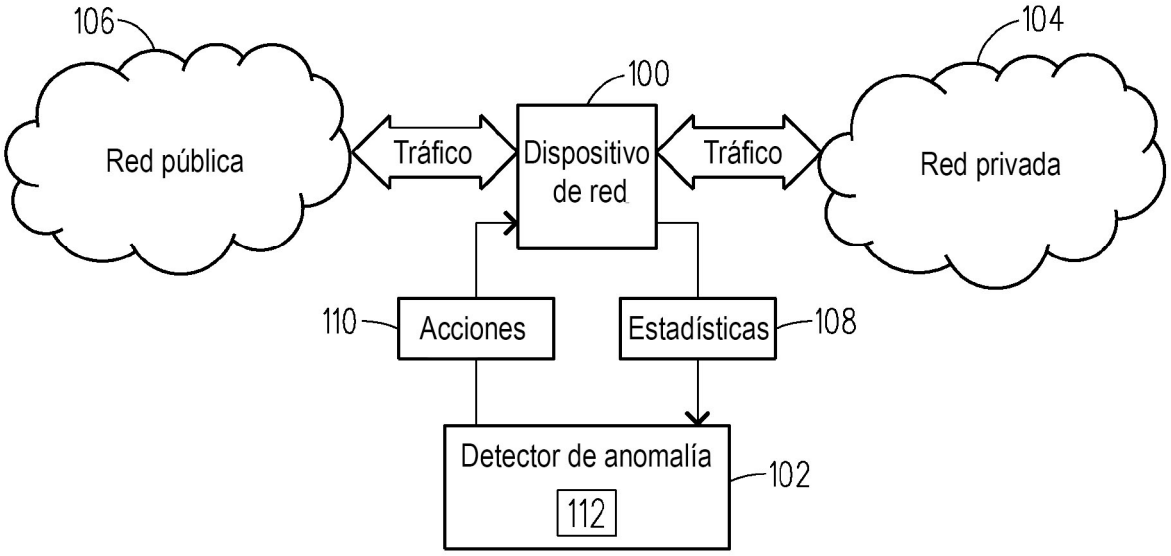
106
Red pública
Tráfico
100
Dispositivo de red
Tráfico
104
Red privada
110
Acciones
Estadísticas
108
Detector de anomalía
112
102

FIG. 1

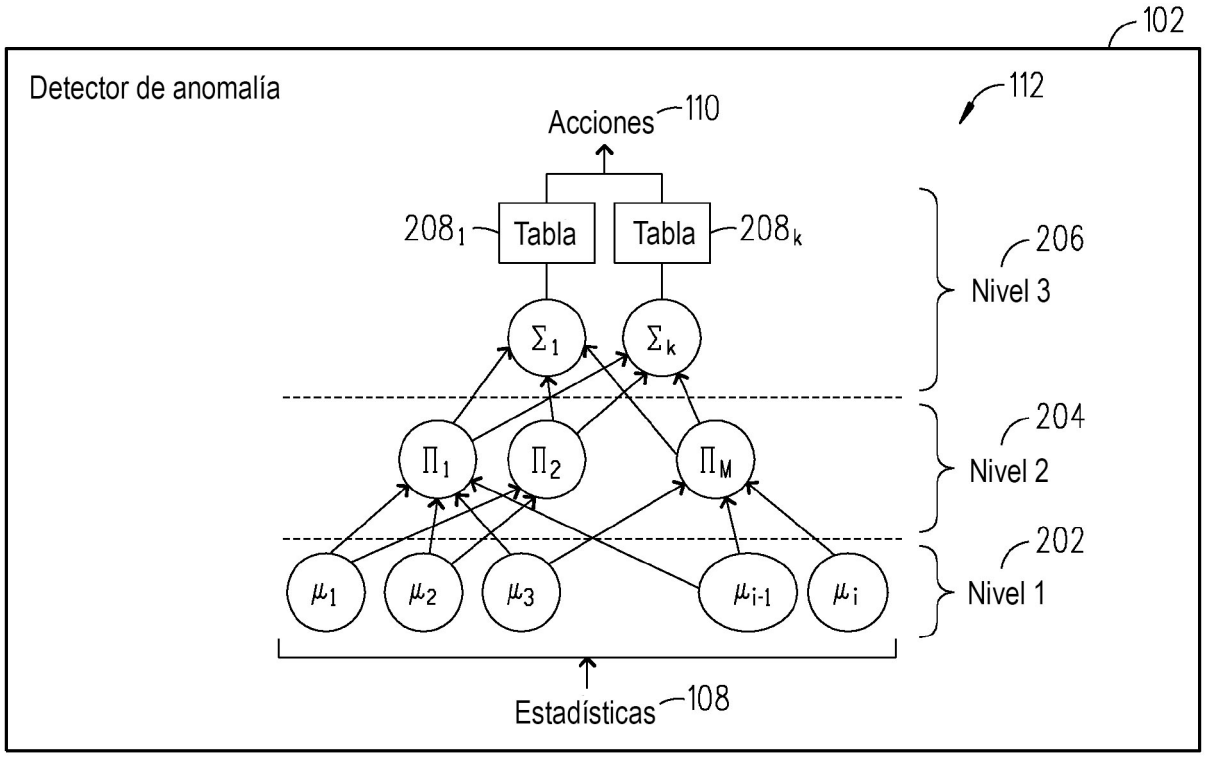
102
Detector de anomalía
112
Acciones
110
208_1
Tabla
Tabla
208_k
206
Nivel 3
Σ_1
Σ_k
204
Nivel 2
Π_1
Π_2
Π_M
202
Nivel 1
μ_1
μ_2
μ_3
μ_{i-1}
μ_i
Estadísticas
108

FIG. 2

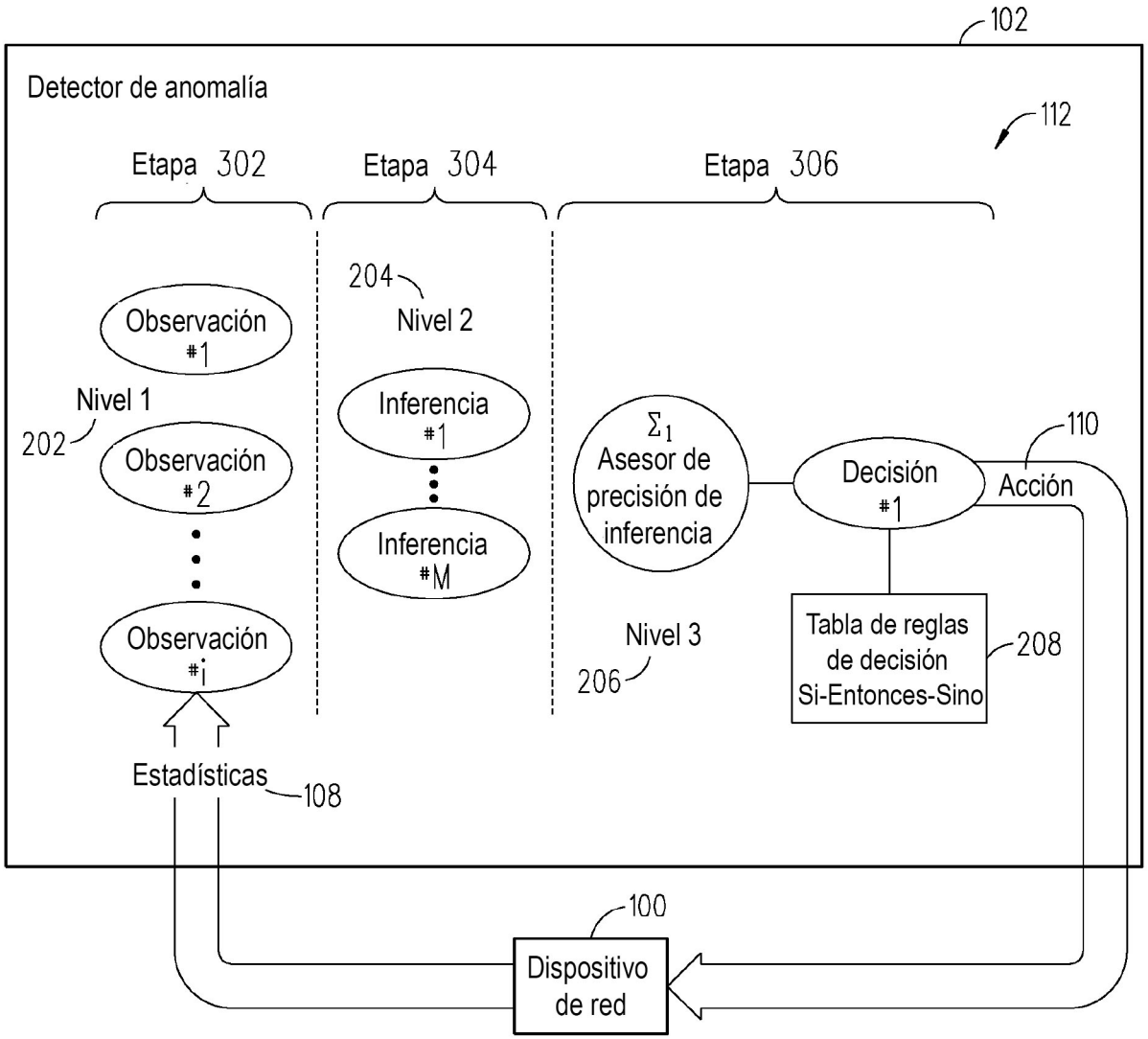
102
Detector de anomalía
112
Etapa 302
Etapa 304
Etapa 306
204
Nivel 2
Observación #1
Nivel 1
202
Observación #2
Observación #i
Inferencia #1
Inferencia #M
Σ1 Asesor de precisión de inferencia
Decisión #1
110
Acción
Nivel 3
206
Tabla de reglas de decisión Si-Entonces-Sino
208
Estadísticas
108
100
Dispositivo de red

FIG. 3