(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 546 129**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 29/06 (2006.01)
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.03.2011 E 11721809 (9)**

(97) Fecha y número de publicación de la concesión europea: **17.06.2015 EP 2548337**

(54) Título: **Procedimiento de identificación de un protocolo en el origen de un flujo de datos**

(30) Prioridad:

17.03.2010 FR 1001062

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.09.2015

(73) Titular/es:

THALES (100.0%)
45, rue de Villiers
92200 Neuilly-sur-Seine, FR

(72) Inventor/es:

DUBOIS, RENAUD;
MOREL, MATHIEU y
GOMPEL, PAUL

(74) Agente/Representante:

PONTI SALES, Adelaida

DESCRIPCIÓN

Procedimiento de identificación de un protocolo en el origen de un flujo de datos

[0001] La presente invención se refiere a un procedimiento de identificación de un protocolo en el origen de un flujo de datos del tipo que incluye las etapas siguientes:

- una captura del flujo del protocolo que se va a identificar,

- una clasificación estadística del flujo, que comprende una extracción de parámetros de clasificación y una comparación de los parámetros de clasificación con modelos estadísticos construidos durante una fase de aprendizaje.

[0002] En el campo de la seguridad de los sistemas de información, el control de los flujos de entrada y de salida de una red de defensa o de una empresa es crucial. El control de estos flujos se realiza generalmente en un equipo de pasarela, situado en la frontera entre la red local y el mundo exterior, es decir, la red Internet. El objetivo de dicho control es asegurar la conformidad de los flujos que pasan con la política de seguridad de la empresa. Esta política puede consistir, por ejemplo, en autorizar únicamente la navegación web, a la vez que se prohíben los intercambios de archivos de tipo FTP o entre homólogos (P2P) con el exterior, así como cualquier conexión directa con servidores distantes SMTP, SSH u otros.

[0003] Se han desarrollado numerosas herramientas para asegurar el respeto de estas políticas de seguridad. Los procedimientos que las usan pueden clasificarse en tres grandes categorías:

• filtrado de nivel red y transporte por análisis de protocolos (*cortafuegos*);

• filtrado por análisis del contenido de los datos de aplicación del flujo (servidores obligatorios); y

• análisis comportamental elemental para identificar los comportamientos sospechosos (*IDS o IDPS comportamentales*).

[0004] El conjunto de estas protecciones puede ser, no obstante, sorteado por un usuario de la red local, usando un túnel de aplicación con un servidor distante controlado.

[0005] Este procedimiento consiste en encapsular los datos de aplicación de un protocolo prohibido en el interior de tramas de un protocolo autorizado para que atraviese la pasarela. El servidor controlado distante, controlado por el usuario, extrae las tramas encapsuladas y las retransmite hacia su verdadero destino.

[0006] El protocolo más usado para establecer esta clase de túneles es el protocolo HTTP, ya que este último casi siempre es autorizado por las pasarelas. Así, el software GNU httptunnel, http//www.nocrew.org/software/httptunnel.html, Lars Brinkhoff permite encapsular las tramas de un protocolo cualquiera (por ejemplo, SSH o P2P) en peticiones HTTP. Los datos útiles se camuflan en campos determinados de la petición, con ayuda de técnicas próximas a las de la esteganografía.

[0007] De forma similar, el software Stunnel universal SSL wrapper, http//www.stunnel.org/ permite encapsular la mayor parte de los protocolos en una conexión SSL/TLS, en el puerto 443. Los flujos resultantes son identificados así por las herramientas de filtrado como flujos HTTPs legítimos.

[0008] Si se puede esperar que un servidor obligatorio perfeccionado detecte una anomalía en las peticiones HTTP generadas por *HTTPTunnel,* los flujos generados por *Stunnel* están cifrados, lo que impide realizar inspecciones del contenido de los paquetes.

[0009] Un enfoque para identificar el flujo no deseable que circula por dicho túnel consiste en determinar el protocolo en el origen de un flujo de datos (es decir, el protocolo encapsulado en el caso de un túnel), usando un número reducido de parámetros difícilmente falsificables por un atacante. Una vez identificado este protocolo, se puede aplicar la política de seguridad de la red local para decidir el filtrado o no del flujo.

[0010] Para detectar la presencia de túneles ilegítimos, el uso de números de puerto se manifiesta inútil, y la inspección en profundidad del contenido de los paquetes es a menudo fuente de errores, dado que los diseñadores

de los programas de software de tunelización son especialmente ingeniosos cuando se trata de ocultar los datos en un flujo legítimo, por no decir imposible si el flujo se cifra como en el caso de los túneles HTTPs.

[0011] Los procedimientos presentados a continuación usan herramientas estadísticas para aprovechar las informaciones residuales en los flujos después del cifrado o encapsulación en otro protocolo. En particular, se busca identificar una huella estadística inherente para cada protocolo a partir de un número reducido de parámetros.

[0012] Para que un procedimiento de clasificación de flujos estadísticos pueda usarse, es necesario realizar dos hipótesis:

• cada protocolo o clase de protocolo (HTTP, SSH, P2P, VoIP, ...) induce un comportamiento característico en términos de paquetes de datos generados, tanto para el tamaño de estos paquetes como para el tiempo entre paquetes. Por ejemplo, un flujo SSH estará compuesto mayoritariamente por “pequeños” paquetes intercambiados en los dos sentidos (las pulsaciones del teclado, y después sus respuestas de “eco”), mientras que un flujo HTTP típico consistirá en una petición de tamaño medio, seguida de la respuesta del servidor en varios paquetes de gran tamaño; y

• la encapsulación de un protocolo en un túnel HTTP/HTTPs o similar no modifica notablemente su comportamiento característico (o al menos los comportamientos de los diferentes protocolos encapsulados siguen siendo distintos).

[0013] El uso de procedimientos de clasificación estadística para identificar el protocolo en el origen de un flujo se ha descrito en la bibliografía en la que se estudian diferentes procedimientos. En particular en N. Williams, S. Zander and G. Armitage, a preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification, ACM SIGICOMM’06, 2006.

[0014] El artículo presenta una síntesis comparativa de varios procedimientos de clasificación aplicados en la clasificación de flujos de datos. Williams muestra que entre los numerosos algoritmos (procedimiento de Bayes, redes bayesianas, C4.5, árboles de Bayes, SVM, etc.), los de mayor rendimiento son SVM y C4.5.

[0015] El documento WO-2009/021.892-A1 describe un procedimiento y una instalación de clasificación de tráficos en las redes IP. La invención que describe aplica un procedimiento estadístico basado en un árbol de decisión (algoritmo C4.5) para determinar el protocolo en el origen de un flujo cifrado.

[0016] MAHBOD TAVALLAEE Y COL.: "Online Classification of Network Flows", COMMUNICATION NETWORKS AND SERVICES RESEARCH CONFERENCE, 2009. CNSR ’09. SEVENTH ANNUAL, IEEE, PISCATAWAY, NJ, EE.UU., 11 de mayo de 2009 (2009-05-11), páginas 78-85, describe un procedimiento de clasificación de flujos de paquetes que aplica varios niveles de clasificación.

[0017] DUSI M Y COL.: "Using GMM and SVM-Based Techniques for the Classification of SSH-Encrypted Traffic", COMMUNICATIONS, 2009. ICC ’09. IEEE INTERNATIONAL CONFERENCE SE, IEEE, PISCATAWAY, NJ, EE.UU., 14 de junio de 2009 (2009-06-14), páginas 1-6, describe dos procedimientos de clasificación de flujos cifrados.

[0018] Todos estos procedimientos son eficaces pero producen un número importante de falsos positivos, es decir, de clarificación de flujos que se sabe que están prohibidos pero que son autorizados.

[0019] La invención tiene por objeto proponer un procedimiento de clasificación que permita reducir el número de falsos positivos.

[0020] Para este fin, la invención tiene por objeto un procedimiento de identificación de un protocolo en el origen de un flujo de datos del tipo citado anteriormente, caracterizado porque la clasificación estadística incluye:

- una primera fase de clasificación estadística global que comprende una etapa de extracción de parámetros globales de clasificación calculados por aplicación de fórmulas estadísticas en una parte o la totalidad del flujo, y una etapa de tratamiento de los parámetros globales de clasificación a partir de un modelo estadístico construido durante una fase de aprendizaje;

- una segunda fase de clasificación secuencial que comprende una etapa de extracción de parámetros secuenciales de clasificación representativos de la cadena temporal de paquetes que constituyen el flujo, y una etapa de

tratamiento de los parámetros secuenciales de clasificación a partir de un modelo estadístico construido durante una fase de aprendizaje; y

- una etapa de síntesis de los resultados de las fases de clasificación primera y segunda para identificar el protocolo en el origen del flujo.

[0021] Según una forma de aplicación en concreto, el procedimiento incluye una o varias de las características siguientes:

- la etapa de tratamiento de los parámetros globales de clasificación a partir de modelos estadísticos construidos durante una fase de aprendizaje comprende la aplicación del algoritmo Random Forest;

- los parámetros globales de clasificación incluyen al menos un parámetro entre:

• el número de paquetes transmitidos, en sentido cliente→servidor;

• el número de octetos transmitidos, en sentido cliente→servidor;

• el tamaño medio de los paquetes IP, en sentido cliente→servidor;

• el tamaño máximo de los paquetes IP, en sentido cliente→servidor;

• el tiempo mínimo entre llegadas de dos paquetes IP, en sentido cliente→servidor;

• el tiempo máximo de llegadas entre dos paquetes IP, en sentido cliente→servidor;

• el número de octetos transmitidos, en sentido servidor→cliente;

• el tamaño máximo de los paquetes IP, en sentido servidor→cliente;

• la varianza del tamaño de los paquetes IP, en sentido servidor→cliente; y

• la relación número octetos de subida/número total octetos intercambiados;

- la etapa de tratamiento de los parámetros secuenciales de clasificación a partir de modelos estadísticos construidos durante una fase de aprendizaje comprende la aplicación de modelos ocultos de Markov;

- la fase de aprendizaje incluye una etapa de construcción de un modelo oculto de Markov para cada protocolo identificable y la etapa de tratamiento incluye la determinación del modelo oculto de Markov cuya probabilidad de que el flujo haya sido emitido por el protocolo asociado es la mayor;

- los parámetros secuenciales de clasificación comprenden al menos un parámetro entre el tamaño del paquete y el tiempo entre paquetes;

- la etapa de síntesis de los resultados comprende la aplicación de la fórmula de Bayes para proporcionar la probabilidad de la existencia de un protocolo

$$p''_i = \frac{\sum_{k=1}^{n} p_k\, p(i \mid k) + \sum_{k=1}^{n} p'_k\, p'(i \mid k)}{2}$$

en la que

dado un flujo F y un conjunto de protocolos posibles [$a_1 ... a_n$], p_i y p'_i representan respectivamente la probabilidad de que F pertenezca al protocolo a_i según el método *RandomForest* aplicado en la fase y según el método del banco de modelos ocultos de Markov aplicado en la fase,

• p''_i es la probabilidad fusionada de que F pertenezca al protocolo a_i;

• *p(i/k)* (respectivamente *p'(i/k)*) es la probabilidad de que el flujo pertenezca al protocolo a_i sabiendo que la primera fase de clasificación, respectivamente la segunda fase de clasificación, ha clasificado el flujo como perteneciente al protocolo a_k;

- el procedimiento incluye, al final de la etapa de síntesis, una etapa de filtrado adicional;

- la etapa de filtrado comprende la consideración de la historia de los resultados según una heurística predeterminada.

[0022] La invención tiene asimismo por objeto una instalación de identificación de un protocolo en el origen de un flujo de paquetes tal como se describe a continuación, caracterizada porque los medios de clasificación estadística incluyen:

- primeros medios de clasificación estadística global que comprenden medios de extracción de parámetros globales de clasificación calculados por la aplicación de una fórmula estadística en una parte o la totalidad del flujo, y medios de tratamiento de los parámetros globales de clasificación a partir de un modelo estadístico construido durante una fase de aprendizaje;

- segundos medios de clasificación secuencial que comprenden medios de extracción de parámetros secuenciales de clasificación representativos de la cadena temporal de paquetes que constituyen el flujo, y medios de tratamiento de los parámetros secuenciales de clasificación a partir de un modelo estadístico construido durante una fase de aprendizaje; y

- medios de síntesis de los resultados de los medios de clasificación primeros y segundos para identificar el protocolo en el origen del flujo.

[0023] La invención se comprenderá mejor con la lectura de la descripción que se ofrece a continuación, suministrada únicamente a modo de ejemplo y realizada con referencia a los dibujos en los que:

- la figura 1 es una vista esquemática de una instalación en la que se aplica el procedimiento según la invención;

- la figura 2 es un organigrama del procedimiento según la invención;

- la figura 3 es un esquema de un árbol como el aplicado por una fase del procedimiento; y

- la figura 4 es un esquema de un grafo aplicado en otra fase del procedimiento según la invención.

[0024] En la figura 1 se representa un esquema típico de una comunicación que establece un túnel entre un puesto local 12 y un servidor distante 14. El puesto local 12 forma parte de una red local 16 por ejemplo de una empresa cuyos puestos están interconectados entre sí y unidos a la red Internet 18 a través de una pasarela 20.

[0025] Esta pasarela integra un cortafuegos 22 que, como es conocido de por sí, es capaz de asegurar la gestión y la autorización de los flujos de entrada y de salida de la red local 16.

[0026] Como es conocido de por sí, la pasarela 20 incluye primeros medios de filtrado que prohíben la transmisión de datos desde la red Internet 18 hacia uno de los puestos de la red local 16 cuando esta transmisión usa un cierto número de protocolos prohibidos, tales como el protocolo SSH o P2P. Por el contrario, la pasarela 20 autoriza la navegación “Web” autorizando el tráfico según el protocolo http o https.

[0027] Para el establecimiento del túnel, un servidor controlado 24 está presente en la red Internet 18 fuera de la red local 16 aislada por la pasarela 20 y el cortafuegos 22 de la red Internet 18.

[0028] Como es conocido de por sí, el puesto 12 incluye medios de software para establecer un túnel de software 26 entre el puesto 12 y el servidor controlado 24. Este túnel de software es capaz de encapsular los datos de aplicación de un protocolo prohibido por la pasarela 20 en el interior de tramas de otro protocolo autorizado por esta pasarela. Para este fin, los datos de aplicación requeridos por el puesto 12 en el servidor distante 14 son vehiculados desde el servidor distante 14 hacia el servidor controlado 24 según el protocolo prohibido, y después el servidor controlado 24 asegura una encapsulación de los datos de aplicación en el interior de tramas de otro

protocolo autorizado por la pasarela 24 y finalmente estos datos son dirigidos al puesto 12 usando este protocolo autorizado por el servidor 24.

[0029] El protocolo autorizado es, por ejemplo, el protocolo http mientras que las tramas de aplicación encapsuladas en este protocolo son transmitidas desde el servidor 14 al servidor 24 por el protocolo SSH o P2P.

[0030] Asimismo, los datos de aplicación dirigidos desde el puesto 12 al servidor 14 son transmitidos a través del servidor controlado 24 en el que los datos son desencapsulados según un proceso inverso al descrito anteriormente.

[0031] Según la invención, la pasarela 20 incluye, además de primeros medios de filtrado, medios de análisis del protocolo en el origen de un flujo de datos cuando estos datos son encapsulados en un protocolo autorizado por la pasarela 20.

[0032] Así, la pasarela 20 incluye dos medios de filtrado sucesivos de los flujos, un primer filtrado que prohíbe los intercambios de datos usando un protocolo prohibido entre un puesto de la red local e Internet, y después un segundo medio de filtrado que prohíbe las transmisiones de datos entre la red Internet y un puesto con un protocolo autorizado en el caso en que los datos de aplicación encapsulados en el interior de las tramas del protocolo autorizado sean emitidos desde un protocolo prohibido.

[0033] Para la aplicación de este segundo filtrado, la pasarela 20 incluye medios de almacenamiento 30A de un software que aplica las etapas sucesivas del procedimiento de análisis, una base de datos 30B que contiene datos emitidos desde un aprendizaje previo usado por el procedimiento y una base de datos 30C de almacenamiento temporal de los flujos en curso de tratamiento, por ejemplo de tipo MySQL.

[0034] La figura 2 presenta el organigrama del procedimiento aplicado.

[0035] Constantemente, se realiza una escucha de la red en la etapa 102 con ayuda de un programa conocido de por sí como tcpdump/Libpcam disponible en http://ww.tcpdump.org/. Esta etapa asegura la interceptación de los diferentes flujos multiplexados y su almacenamiento temporal en la base 30C.

[0036] En la etapa 104, la demultiplexación de los diferentes flujos interceptados se efectúa a continuación mediante cualquier medio apropiado y, por ejemplo, por scripts *perl.*

[0037] En cada uno de los flujos demultiplexados se aplican dos fases 108, 110 de clasificación del flujo de datos.

[0038] La primera fase 108 de clasificación se denomina global en el sentido de que comprende una etapa 112 de extracción de parámetros globales de clasificación calculados por un análisis estadístico en una parte o la totalidad del flujo, y una etapa 114 de tratamiento de los parámetros globales de clasificación a partir de modelos estadísticos construidos durante una fase previa de aprendizaje

[0039] La segunda fase 110 de clasificación estadística se denomina secuencial en el sentido de que comprende una etapa 116 de extracción de parámetros secuenciales de clasificación representativos de la cadena temporal de paquetes sucesivos que constituyen el flujo, y una etapa 118 de tratamiento de los parámetros secuenciales de clasificación a partir de modelos estadísticos construidos durante una fase previa de aprendizaje.

[0040] Estos parámetros extraídos en las etapas 112 y 116 así como algunas informaciones elementales en cada flujo (*timestamp,* direcciones IP de origen y destino, etc.) se almacenan en la base de datos 30C.

[0041] Las herramientas de tratamiento propiamente dichas que aplican las etapas de tratamientos 114, 118 se desarrollan en Java, o cualquier otro lenguaje adaptado. Los resultados de clasificación se almacenan igualmente en la base de datos 30C.

[0042] En la etapa 112, se extraen parámetros globales calculados por un análisis estadístico en una parte o la totalidad del flujo (por ejemplo, el tamaño medio de los paquetes, etc.) para cada flujo. Los parámetros globales son el resultado de tratamientos estadísticos efectuados en los valores elementales de estos parámetros retransmitidos en cada uno de los paquetes que constituyen la parte del flujo analizado. Se trata por ejemplo de medias de desviaciones típicas, de varianzas, etc...

[0043] Estos parámetros se eligen de manera que sean evaluables con independencia de cuál sea el flujo TCP considerado.

[0044] Se deducen de los datos contenidos en las capas 1 a 4 del modelo OSI.

[0045] Además, para hacer más difícil aún la vulneración del sistema, los parámetros se eligen de manera que sean difíciles de modificar por un atacante. Por ejemplo, los *flags* TCP no se consideran. Se extraen sólo los parámetros derivados de los tamaños de los paquetes y de los tiempos entre paquetes. Se trata por ejemplo del tamaño medio de los paquetes cliente hacia el servidor, de la varianza de los tiempos entre paquetes, etc.

[0046] En la presente solicitud, el término “paquete” se entiende a modo de ejemplo en el sentido de “paquete TCP que transporta datos de aplicación”. Sin embargo, el procedimiento no se limita al caso de los protocolos que usan la pila TCP/IP y el procedimiento puede aplicarse con independencia de cuál sea el modo de transmisión.

[0047] Entre todos los parámetros que pueden plantearse, sólo se conservan entre 5 y 15 parámetros, preferentemente una decena, para asegurar la rapidez de la clasificación ulterior. Estos parámetros se eligen como los más discriminatorios en relación con el protocolo en el origen del flujo, es decir, como un subconjunto de parámetros con un poder de discriminación máximo, conservando un bajo valor de intracorrelación.

[0048] En otros términos, estos parámetros son tales que dependen fuertemente del protocolo del flujo, estando en todo caso muy poco relacionados entre sí. Esta última condición sirve para no ponderar en exceso determinados parámetros durante la clasificación.

[0049] Para la fase 108, parte o la totalidad de los parámetros siguientes se usan ventajosamente:

- el número de paquetes transmitidos, en sentido cliente→servidor;
- el número de octetos transmitidos, en sentido cliente→servidor;
- el tamaño medio de los paquetes IP, en sentido cliente→servidor;
- el tamaño máximo de los paquetes IP, en sentido cliente→servidor;
- el tiempo mínimo entre llegadas de dos paquetes IP, en sentido cliente→servidor;
- el tiempo máximo de llegadas entre dos paquetes IP, en sentido cliente→servidor;
- el número de octetos transmitidos, en sentido servidor→cliente;
- el tamaño máximo de los paquetes IP, en sentido servidor→cliente;
- la varianza del tamaño de los paquetes IP, en sentido servidor→cliente;
- la relación número octetos de subida/número total octetos intercambiados.

[0050] La etapa de tratamiento de parámetros globales 114 aplica ventajosamente el algoritmo *RandomForest* aplicado en los diez parámetros para clasificar cada flujo.

[0051] Este algoritmo ha sido inventado por Leo Breiman y Adele Cutler en 2001, y se describe en detalle en L. Breiman, Random Forests, Machine Learning 45 (1): 5-32, 2001.

[0052] El algoritmo *RandomForest* consiste en un bosque de árboles de decisiones aleatorias.

[0053] En la figura 3 se presenta un ejemplo de árbol de decisión. Cada nodo de dicho árbol representa una prueba en uno de los parámetros, denotados aquí como param. 4, param. 8, param. 2 y param. 1 en relación con un valor discriminante, en este caso 5,5; 0,1; 91,6 y 10,1. Cada hoja del árbol representa un protocolo, en este caso, HTTP, P2P, SSH, HTTP y TELNET.

[0054] Para clasificar un flujo dado, el árbol es recorrido, a partir de la raíz, descendiendo por las ramas según los resultados de las pruebas. La hoja a la que se llega es el resultado de la clasificación.

[0055] Toda la dificultad del empleo de árboles de decisión reside en la construcción de estos árboles. Esta se realiza a partir de la base de aprendizaje, usando un algoritmo que determina de forma recursiva, para cada nodo, el mejor parámetro para considerar y el valor discriminante más pertinente para este parámetro. Al actuar así, se pretende minimizar la entropía entre clases resultante de la separación según este valor.

[0056] El algoritmo *RandomForest* consiste en usar no uno sino varios árboles, una veintena en la práctica, introduciendo un suceso diferente durante el aprendizaje para cada árbol de tal manera que todos los árboles sean diferentes. Este suceso se refiere a la elección del parámetro que se someterá a prueba para cada uno de los nodos.

[0057] Para determinar el protocolo encapsulado en un flujo, el flujo se clasifica por cada uno de los árboles del bosque. El porcentaje de árboles que han conducido a cada uno de los protocolos posibles se interpreta como la probabilidad de que el flujo pertenezca a este protocolo. En particular, el protocolo elegido por una mayoría de árboles constituye el resultado de la clasificación y de la etapa 114.

[0058] El método de clasificación de los flujos descrito anteriormente da buenos resultados. No obstante, usa exclusivamente los diez parámetros globales citados anteriormente para clasificar los flujos. En particular, toda la información relativa a las cadenas temporales de paquetes se pierde, dado que estos parámetros son medias, varianzas, valor mínimo o máximo, calculados en el conjunto del flujo. Ahora bien, la “signatura” de un protocolo se encuentra igualmente en el desarrollo temporal de los intercambios de datos y sobre todo en la cadena temporal de paquetes.

[0059] Así, una pulsación de teclado en el protocolo SSH se seguirá de forma casi sistemática de un paquete “eco” del servidor. Por el contrario, con el protocolo HTTP, una petición del cliente será seguida por varios paquetes enviados por el servidor, etc.

[0060] Para aprovechar estas informaciones temporales perdidas por el algoritmo *RandomForest,* la fase 110 de clasificación secuencial de los flujos aplica otro procedimiento de análisis estadístico de los flujos, que se basa en modelos ocultos de Markov (MOM).

[0061] La mayor parte de los protocolos actuales son gestionados por un autómata en estado subyacente sobre todo para cadenas del tipo: establecimiento de la conexión, intercambio de parámetros, régimen “permanente”, cierre de la conexión. Además, a cada estado de este autómata le corresponden intercambios de paquetes particulares.

[0062] El uso de modelos ocultos de Markov para representar los protocolos resulta así apropiado. En la práctica, se usa un banco de modelos ocultos de Markov, es decir, se construye un modelo oculto de Markov para representar cada protocolo. Los símbolos observables son pares [tamaño del paquete, tiempo entre paquetes].

[0063] Dado que los tamaños de los paquetes y los tiempos entre paquetes pueden tomar un gran número de valores, se efectúa una cuantificación vectorial de estos parámetros para discretizarlos. Para ello, se usan los paquetes de los flujos de una base de aprendizaje, y se determinan los centroides de cuantificación usando el algoritmo *K-means.* La inicialización de este último se realiza trazando aleatoriamente puntos en una bola alrededor del centro de gravedad. Los paquetes cliente→servidor y servidor→cliente se cuantifican de manera independiente (el algoritmo *K-means* se realiza dos veces).

[0064] En la figura 4 se representa un ejemplo de modelo oculto de Markov simple. Este modelo está así constituido por un conjunto de estados, entre ellos uno o varios estados iniciales. Para cada estado, es posible un conjunto de transiciones hacia otros estados, siendo cada transición ponderada por una probabilidad. En el curso del tiempo, se produce un desplazamiento en los estados de Markov ocultos.

[0065] Los modelos ocultos de Markov considerados se dicen “ocultos”, porque la sucesión de estados en los que se encuentran no es observable. Por el contrario, se observa una sucesión de símbolos, emitidos durante cambios de estados sucesivos. Así, a un modelo oculto de Markov se le asocia un alfabeto A, y a cada estado de este modelo oculto de Markov le corresponde una distribución de probabilidades de emisión de símbolos de A. En la figura ofrecida más adelante, el alfabeto es {T,t} con T = tamaño del paquete y t = tiempo entre paquetes.

[0066] Existen varios tipos de problemas clásicos para los modelos ocultos de Markov:

• dado un modelo oculto de Markov y una secuencia de observación (es decir, una sucesión de símbolos de A), ¿cuál es la secuencia de estados oculta más probable correspondiente?

• dado un modelo oculto de Markov y una secuencia de observación, ¿cuál es la probabilidad de que este modelo zoculto de Markov haya producido esta secuencia de observaciones?

• dado el esqueleto de un modelo oculto de Markov y un conjunto de secuencias de observaciones, ¿cuáles son las probabilidades de transición y de emisión que elevan al máximo la probabilidad de que este modelo oculto de Markov haya emitido este conjunto de secuencias?

[0067] Los dos primeros problemas se resuelven con ayuda del algoritmo de Viterbi, y el tercero con el de Baum-Welsh. Se proporcionan informaciones más amplias sobre estos algoritmos en L.R. Rabiner, A tutorial on Hidden Markov Models and selected applications in speech recognition, Proceedings of the IEEE 77 (2): 257-286, 1989.

[0068] El “esqueleto” de los modelos ocultos de Markov que se usa para cada protocolo se representa en la figura 4. Comprende dos “líneas” de estados. Los estados de la línea superior sólo pueden emitir paquetes en el sentido cliente→servidor, mientras que los estados de la línea inferior sólo pueden emitir paquetes en el sentido servidor→cliente.

[0069] Estableciendo la hipótesis de que un protocolo está constituido por una sucesión de “estados” para los cuales las probabilidades de emisión de paquetes [tamaño de paquete, tiempo entre paquetes] son constantes, cada “columna” de modelos ocultos de Markov usados representa un estado de protocolo, y se autorizan únicamente las transiciones “hacia la derecha”.

[0070] Cada modelo oculto de Markov posee además dos estados iniciales situados en la primera columna.

[0071] Dados los esqueletos de los modelos ocultos de Markov precedentes, todas las probabilidades de transición y de emisiones de símbolos son calculadas usando la base de datos de aprendizaje, aplicando el algoritmo de Baum-Welsh. La inicialización de este algoritmo se realiza a partir de un modelo oculto de Markov cuyas probabilidades son uniformes.

[0072] Se construye un modelo oculto de Markov para cada protocolo que se desea saber reconocer. La probabilidad de que un flujo pertenezca al protocolo i viene dada por la probabilidad de que este flujo haya sido producido por el i-ésimo modelo oculto de Markov. Esta última se calcula mediante el algoritmo de Viterbi. Para clasificar un flujo, se busca así el modelo oculto de Markov que proporcione la mayor probabilidad de emisión para este flujo.

[0073] En la práctica, se usan los modelos ocultos de Markov indicados más adelante con 6 u 8 estados, y se usa un diccionario de cuantificación de 20 a 30 vectores.

[0074] Las dos fases de clasificación paralelas 108, 110 permiten cada una determinar la probabilidad de que un flujo dado pertenezca a cada uno de los protocolos posibles. En la etapa 120, las probabilidades reenviadas por cada una de las fases 108 y 110 se combinan para deducir un resultado final de clasificación y un índice de confianza en este resultado.

[0075] Dado un flujo F y un conjunto de protocolos posibles $[a_1...a_n]$, se dispone de dos vectores de probabilidades $[p_1...p_n]$ y $[p'_1...p'_n]$, en los que p_i y p'_i representan respectivamente la probabilidad de que F pertenezca al protocolo a_i según el método *RandomForest* aplicado en la fase 108 y según el método del banco de modelos ocultos de Markov aplicado en la fase 110.

[0076] Los resultados de clasificación de los dos procedimientos se sintetizan en la etapa 120 mediante la fórmula de Bayes:

$$p''_i = \frac{\sum_{k=1}^{n} p_k\, p(i \mid k) + \sum_{k=1}^{n} p'_k\, p'(i \mid k)}{2}$$

en la que

• p''_i es la probabilidad fusionada de que F pertenezca al protocolo a_i;

• $p(i/k)$ (respectivamente $p'(i/k)$ es la probabilidad de que el flujo pertenezca al protocolo a_i sabiendo que el método RandomForest (respectivamente el método del banco de modelos ocultos de Markov) ha clasificado el flujo como perteneciente al protocolo a_k. Estas probabilidades se estiman mediante manipulaciones en la base de datos de aprendizaje.

[0077] La etapa 120 engendra en salida un vector de probabilidad [$p''_1 ... p'_n$]. El resultado de clasificación global viene dado así por $argmax_i(p''_i)$, en el que max es la función argumento máximo. El índice de confianza asociado es p''_{imax}.

[0078] Estos valores son salvaguardados para cada flujo así como el anfitrión en el origen de la emisión y/o de receptor de este flujo de datos.

[0079] Con el fin de limitar aún más el número de falsos positivos, se aplica un modelo de inteligencia artificial de filtrado en la etapa 122. Según un primer modo de aplicación, el modelo comprende heurísticas obtenidas por medidas experimentales en la red en la que se instala el dispositivo.

[0080] Como variante, se aplica un cierto número de heurísticas en la etapa 122 a la historia de los resultados de clasificación para activar o no una alerta que señale el uso de un protocolo prohibido. Una heurística consiste así por ejemplo en no activar la alerta si el índice de confianza en la clasificación es inferior a un umbral predeterminado, o si el anfitrión del que se trata ha tenido siempre un comportamiento irreprochable antes, es decir, que se trata de una primera detección de un flujo que encapsula un protocolo no autorizado desde o hacia este papel.

[0081] La aplicación de estas heurísticas en la etapa 124 genera un informe de análisis, actualizado en tiempo real, que contiene las alertas activadas y su nivel de valor crítico. Este informe puede estar en el formato *Syslog,* por ejemplo, por razones de interoperatividad.

REIVINDICACIONES

1. Procedimiento de identificación de un protocolo en el origen de un flujo de paquetes que incluye las etapas siguientes:

- una captura (102) del flujo del protocolo que se va a identificar,

- una clasificación estadística del flujo, que comprende una extracción de parámetros de clasificación y una comparación de los parámetros de clasificación con modelos estadísticos construidos durante una fase de aprendizaje,

caracterizado porque la clasificación estadística incluye:

- una primera fase (108) de clasificación estadística global que comprende una etapa (114) de extracción de parámetros globales de clasificación calculados por aplicación de fórmulas estadísticas en una parte o la totalidad del flujo, y una etapa (114) de tratamiento de los parámetros globales de clasificación a partir de un modelo estadístico construido durante una fase de aprendizaje;

- una segunda fase (110) de clasificación secuencial que comprende una etapa (116) de extracción de parámetros secuenciales de clasificación representativos de la cadena temporal de paquetes que constituyen el flujo, y una etapa (118) de tratamiento de los parámetros secuenciales de clasificación a partir de un modelo estadístico construido durante una fase de aprendizaje; y

- una etapa (120) de síntesis de los resultados de las fases de clasificación primera y segunda (108, 110) para identificar el protocolo en el origen del flujo.

2. Procedimiento según la reivindicación 1, **caracterizado porque** la etapa (114) de tratamiento de los parámetros globales de clasificación a partir de modelos estadísticos construidos durante una fase de aprendizaje comprende la aplicación del algoritmo Random Forest.

3. Procedimiento según la reivindicación 1 ó 2, **caracterizado porque** los parámetros globales de clasificación incluyen al menos un parámetro entre:

• el número de paquetes transmitidos, en sentido cliente→servidor;

• el número de octetos transmitidos, en sentido cliente→servidor;

• el tamaño medio de los paquetes IP, en sentido cliente→servidor;

• el tamaño máximo de los paquetes IP, en sentido cliente→servidor;

• el tiempo mínimo entre llegadas de dos paquetes IP, en sentido cliente→servidor;

• el tiempo máximo de llegadas entre dos paquetes IP, en sentido cliente→servidor;

• el número de octetos transmitidos, en sentido servidor→cliente;

• el tamaño máximo de los paquetes IP, en sentido servidor→cliente;

• la varianza del tamaño de los paquetes IP, en sentido servidor→cliente; y

• la relación número octetos de subida/número total octetos intercambiados.

4. Procedimiento según una cualquiera de las reivindicaciones precedentes, **caracterizado porque** la etapa (118) de tratamiento de los parámetros secuenciales de clasificación a partir de modelos estadísticos construidos durante una fase de aprendizaje comprende la aplicación de modelos ocultos de Markov.

5. Procedimiento según la reivindicación 4, **caracterizado porque** la fase de aprendizaje incluye una etapa de construcción de un modelo oculto de Markov para cada protocolo identificable y **porque** la etapa (118) de

tratamiento incluye la determinación del modelo oculto de Markov cuya probabilidad de que el flujo haya sido emitido por el protocolo asociado es la mayor.

6. Procedimiento según una cualquiera de las reivindicaciones precedentes, **caracterizado porque** los parámetros secuenciales de clasificación comprenden al menos un parámetro entre el tamaño del paquete y el tiempo entre paquetes.

7. Procedimiento según una cualquiera de las reivindicaciones precedentes, **caracterizado porque** la etapa (120) de síntesis de los resultados comprende la aplicación de la fórmula de Bayes para proporcionar la probabilidad de la existencia de un protocolo

$$p''_i = \frac{\sum_{k=1}^{n} p_k\, p(i \mid k) + \sum_{k=1}^{n} p'_k\; p'(i \mid k)}{2}$$

en la que

dado un flujo F y un conjunto de protocolos posibles [$a_1 ... a_n$], p_i y p'_i representan respectivamente la probabilidad de que F pertenezca al protocolo a_i según el método *RandomForest* aplicado en la fase (108) y según el método del banco de modelos ocultos de Markov aplicado en la fase (110).

• p''_i es la probabilidad fusionada de que *F* pertenezca al protocolo a_i;

• *p(i/k)* (respectivamente *p'(i/k)*) es la probabilidad de que el flujo pertenezca al protocolo a_i sabiendo que la primera fase de clasificación (108), respectivamente la segunda fase de clasificación (110), ha clasificado el flujo como perteneciente al protocolo a_k.

8. Procedimiento según una cualquiera de las reivindicaciones precedentes, **caracterizado porque** incluye, al final de la etapa de síntesis, una etapa (122) de filtrado adicional.

9. Procedimiento según la reivindicación 8, **caracterizado porque** la etapa de filtrado comprende la consideración de la historia de los resultados según una heurística predeterminada.

10. Instalación de identificación de un protocolo en el origen de un flujo de paquetes que incluye:

- medios de captura del flujo del protocolo que se va a identificar,

- medios de clasificación estadística del flujo, que comprende medios de extracción de parámetros de clasificación y medios de comparación de los parámetros de clasificación con modelos estadísticos construidos durante una fase de aprendizaje,

caracterizada porque los medios de clasificación estadística incluyen:

- primeros medios de clasificación estadística global que comprenden medios de extracción de parámetros globales de clasificación calculados por la aplicación de una fórmula estadística en una parte o la totalidad del flujo, y medios de tratamiento de los parámetros globales de clasificación a partir de un modelo estadístico construido durante una fase de aprendizaje;

- segundos medios de clasificación secuencial que comprenden medios de extracción de parámetros secuenciales de clasificación representativos de la cadena temporal de paquetes que constituyen el flujo, y medios de tratamiento de los parámetros secuenciales de clasificación a partir de un modelo estadístico construido durante una fase de aprendizaje; y

- medios de síntesis de los resultados de los medios de clasificación primeros y segundos para identificar el protocolo en el origen del flujo.

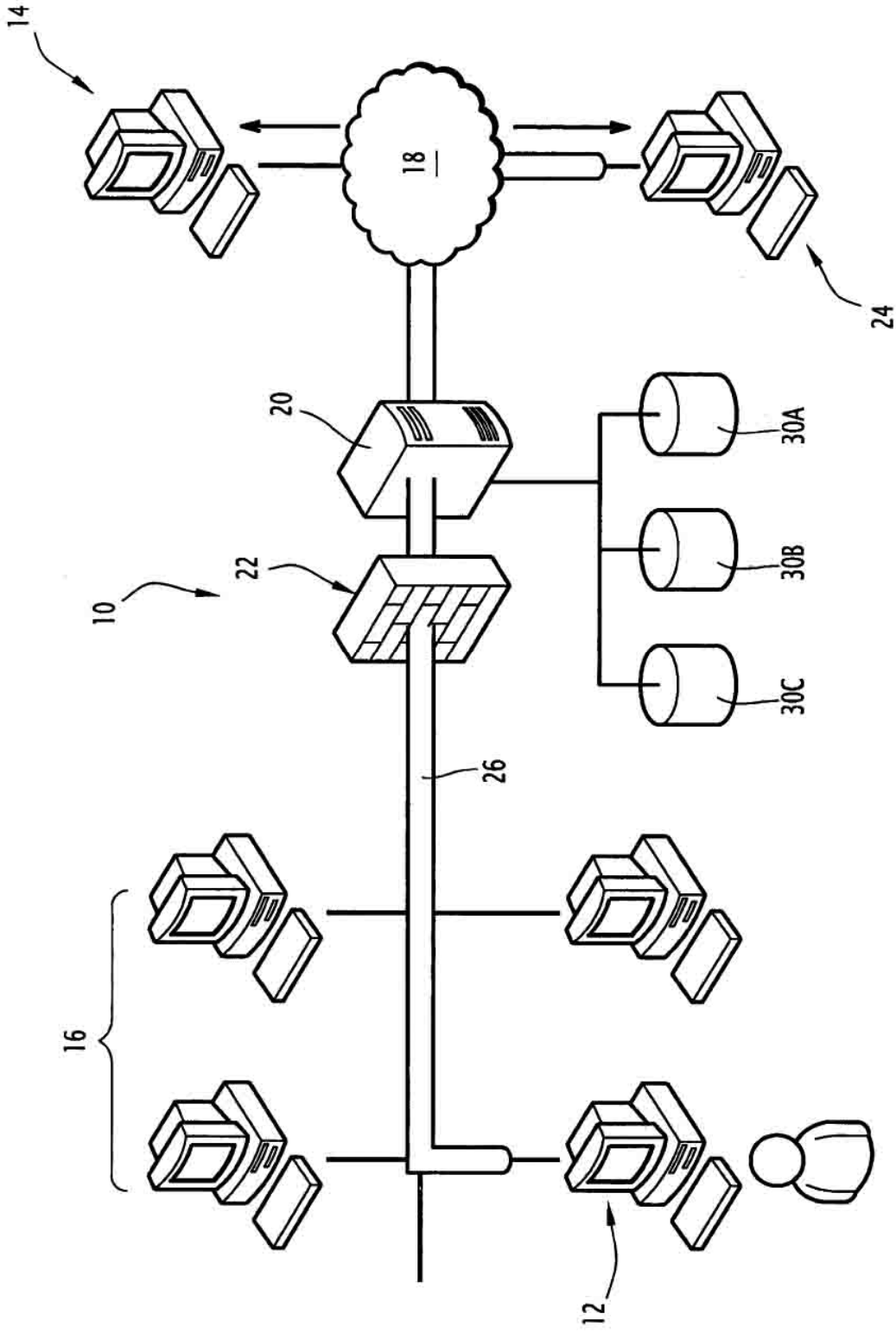

FIG.1

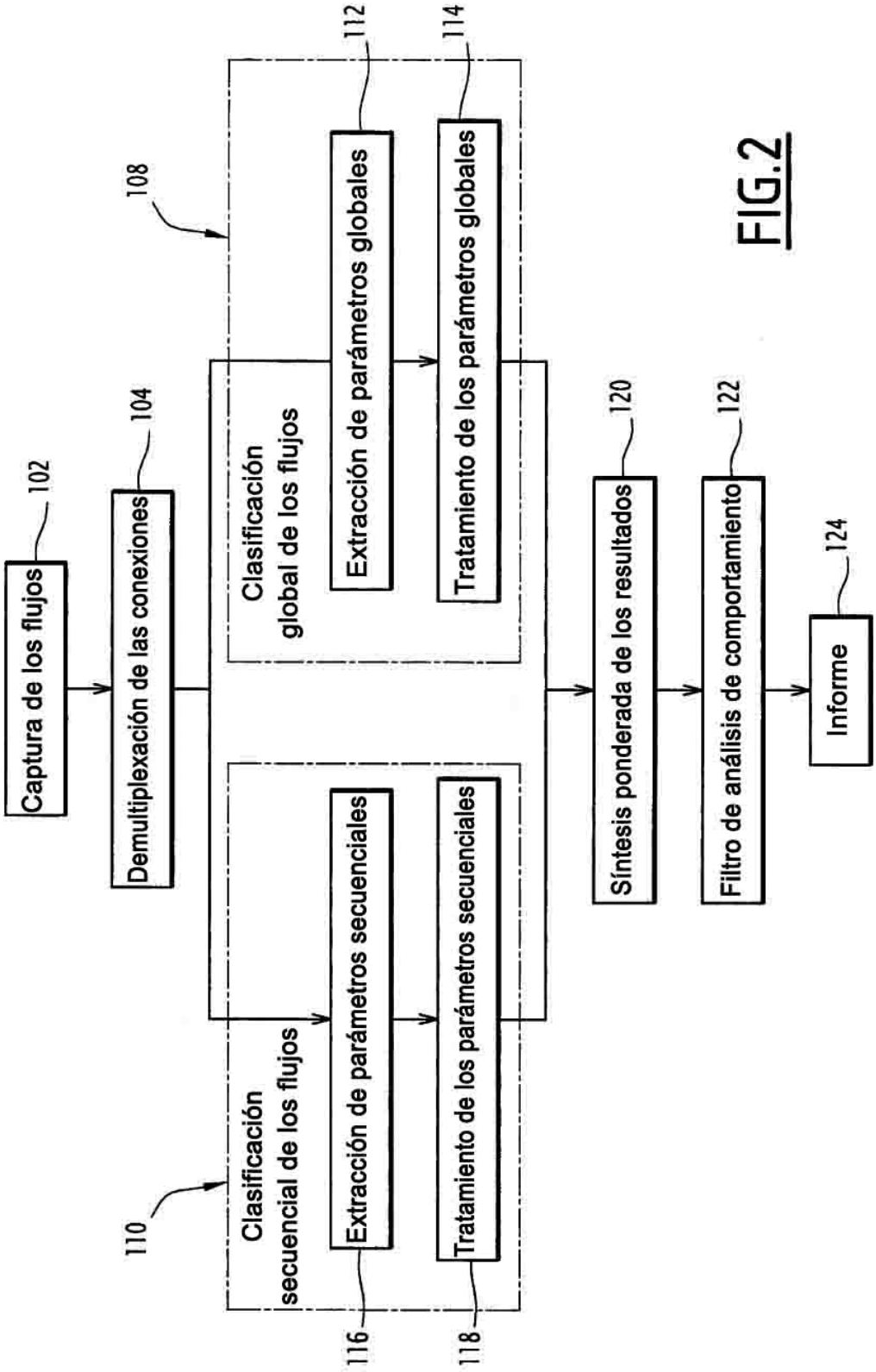
Captura de los flujos
102
Demultiplexación de las conexiones
104
108
Clasificación global de los flujos
Extracción de parámetros globales
112
Tratamiento de los parámetros globales
114
110
Clasificación secuencial de los flujos
Extracción de parámetros secuenciales
116
Tratamiento de los parámetros secuenciales
118
Síntesis ponderada de los resultados
120
Filtro de análisis de comportamiento
122
Informe
124

FIG.2

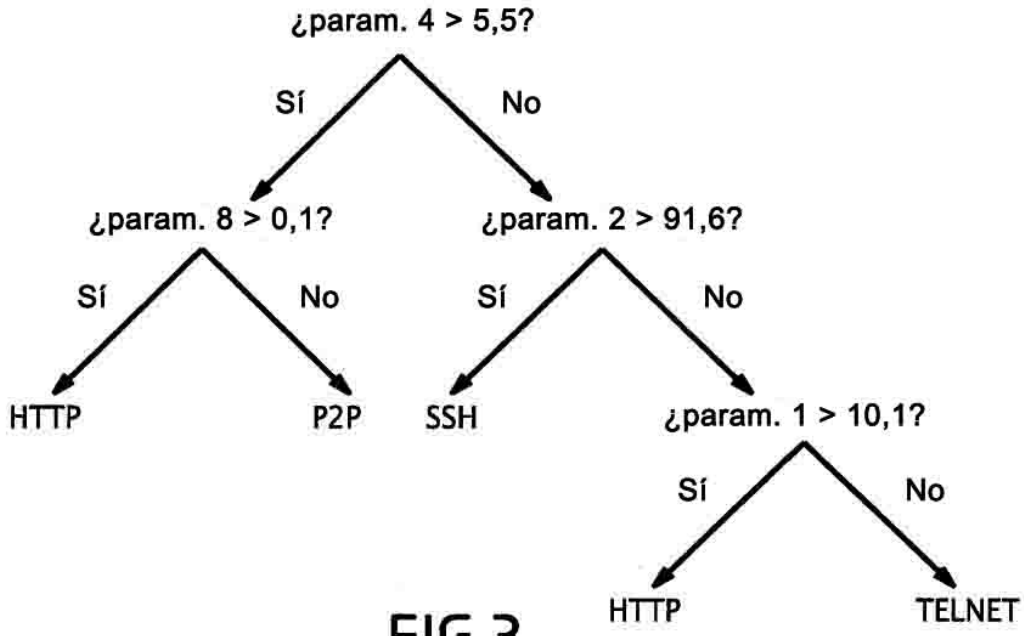
¿param. 4 > 5,5?
Sí
No
¿param. 8 > 0,1?
¿param. 2 > 91,6?
Sí
No
Sí
No
HTTP
P2P
SSH
¿param. 1 > 10,1?
Sí
No
HTTP
TELNET

FIG.3

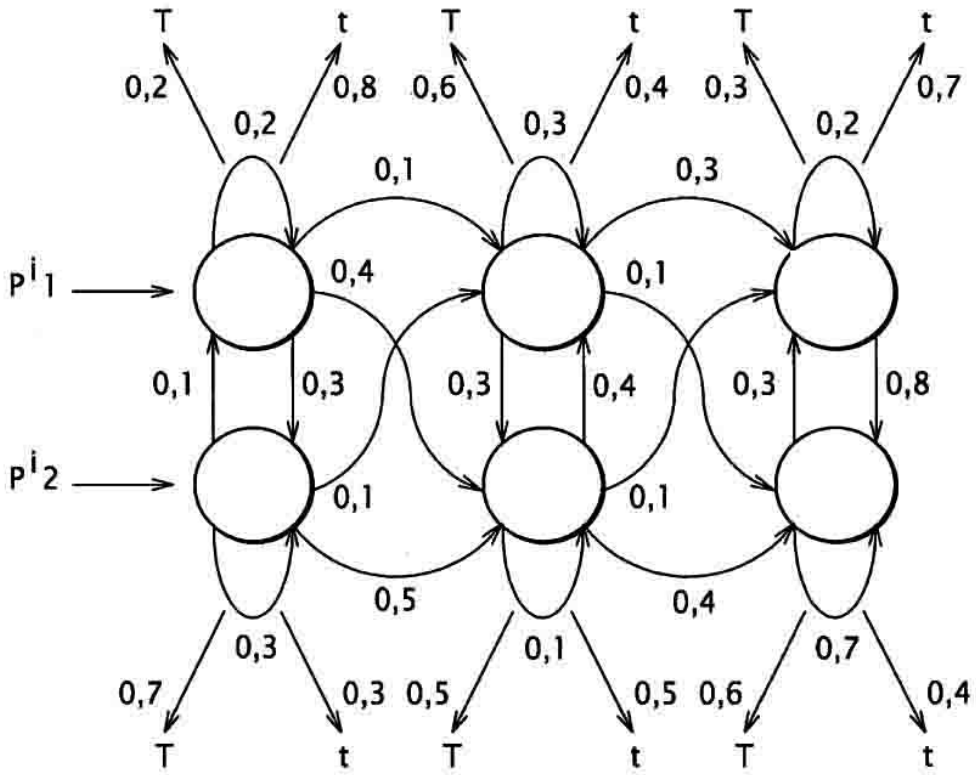
T
t
0,2
0,8
0,6
0,4
0,3
0,7
0,2
0,3
0,2
0,1
0,3
p^i_1
0,4
0,1
0,1
0,3
0,3
0,4
0,3
0,8
p^i_2
0,1
0,1
0,5
0,4
0,3
0,1
0,7
0,7
0,3
0,5
0,5
0,6
0,4

FIG.4