(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 496 982**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/55 (2013.01)
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.09.2009 E 09753148 (7)**

(97) Fecha y número de publicación de la concesión europea: **04.06.2014 EP 2353272**

(54) Título: **Procedimiento de caracterización de entidades al principio de variaciones en un tráfico de red**

(30) Prioridad:

30.09.2008 FR 0856580

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.09.2014

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

VEYSSET, FRANCK y
ANSEL, PIERRE

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Procedimiento de caracterización de entidades al principio de variaciones en un tráfico de red

La presente invención se refiere a un procedimiento de caracterización de entidades al principio de al menos una variación en un tráfico de red.

La invención se sitúa en el campo de las redes de telecomunicaciones. Encuentra una aplicación particularmente interesante en la seguridad de una red informática, y particularmente en la identificación de un conjunto de máquinas comprometidas, controladas por un mismo usuario malintencionado (el término corrientemente utilizado para designar este conjunto de máquinas es “botnet”). Un botnet puede reagrupar varios miles de máquinas, llamadas máquinas zombis, que son infectadas por un programa nefasto instalado en la máquina a espaldas de un usuario legítimo. El programa nefasto permite al usuario malintencionado accionar las máquinas del botnet desde una máquina de control. Un botnet se utiliza por ejemplo para perpetrar acciones malintencionadas contra otras máquinas, para hacer comercio ilícito, o para ganar dinero deshonestamente.

Las redes de tipo botnet han evolucionado a lo largo del tiempo. Se conocen varios procedimientos de identificación de máquinas de un botnet. Por ejemplo, el artículo *Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic*, R. Villamarin y JC. Brustoloni, publicado en los Proceedings IEEE CCNC 2008, propone un procedimiento para identificar servidores de mando y de control de una red de tipo botnet. Este procedimiento se basa en un análisis de peticiones DNS (de *Domaine Name Service*). Un primer modo de realización del procedimiento consiste en buscar las tasas de peticiones con nombres de dominio particulares anormalmente elevadas. Un segundo modo de realización del procedimiento consiste en buscar peticiones recurrentes con nombres de dominios que no existen. Estos métodos se adaptan a casos en los que todos los clientes intentan acceder a un mismo servidor y hacen peticiones DNS relativas a un mismo nombre de dominio.

La solicitud de patente publicada con el nº EP 1906620 divulga un método para detectar clientes comprometidos que constituyen un botnet. En un primer tiempo, el procedimiento identifica clientes sospechosos, por ejemplo clientes que efectúan escáneres de vulnerabilidades, y después analiza precisamente el tráfico de estos clientes con el fin de identificar otras actividades sospechosas, como por ejemplo una conexión con un servidor específico tal como un servidor de mensajería instantánea. En este caso el cliente es marcado como que forma parte potencialmente de un grupo de máquinas. Un análisis y un cotejo de todos los datos cosechados en los clientes sospechosos permite identificar grupos de máquinas conectados a un mismo servidor, cada uno de los miembros del grupo siendo identificado como que forma parte de un botnet. No obstante el procedimiento se apoya en la hipótesis según la cual todos los clientes sospechosos de un grupo acceden a un mismo servidor y utilizan por lo tanto un mismo canal.

Ahora bien, las redes de tipo botnet evolucionan. Así, actualmente se ven aparecer redes de máquinas zombis, que constituyen un botnet, que se organizan en redes “P2P” (de *peer-to-peer*). Se vuelve difícil entonces identificar un canal utilizado para las máquinas zombis del botnet. Resulta que los métodos precitados son totalmente inadaptados para identificar las máquinas zombis del botnet.

Uno de los objetos de la invención es remediar insuficiencias del estado de la técnica. La invención responde a esta necesidad proponiendo un procedimiento de caracterización de entidades al principio de al menos una variación detectada en un tráfico de red, dicho procedimiento siendo definido según la reivindicación 1.

La invención ofrece una técnica que permite identificar el origen de comportamientos en la red que provocan fuertes variaciones en el tráfico de red con respecto a un tráfico, llamado normal, habitualmente observado.

El procedimiento según la invención permite analizar los comportamientos de red analizando las entidades IP de los paquetes que constituyen el tráfico. El procedimiento identifica a través de un comportamiento macroscópico visiblemente anormal, una lista de clientes que tienen el mismo comportamiento anormal. Así, los clientes de la lista parece que tienen todos un comportamiento similar, por ejemplo, una fase de despertar en el transcurso de la cual todo se pone aproximadamente al mismo tiempo de emitir el tráfico, y una fase de adormecimiento en el transcurso de la cual todo para aproximadamente simultáneamente de emitir tráfico.

Por tanto, cuando se dispone del tráfico global con destino a un servidor particular, es fácil observar un comportamiento macroscópico que se desvía del comportamiento normal, por tanto es difícil identificar el origen de tal comportamiento que se desvía provocado por una pluralidad de máquinas. El procedimiento según la invención remedia este problema caracterizando todas las máquinas correlacionadas a este comportamiento que se desvía, es decir, que tienen un comportamiento similar al comportamiento que se desvía.

En una realización de la invención, la etapa de identificación del grupo de entidades comprende:

- una etapa de clasificación de la pluralidad de entidades (c_k) que contribuye al tráfico de red en un conjunto ordenado, según un orden predefinido de similitud de tráfico (s_k),

- una etapa de selección de x entidades consecutivas en el conjunto ordenado con el fin de formar dicho grupo, el valor de similitud de tráfico (cov($C_{x \to P}$)) entre el tráfico acumulado atribuible a las entidades restantes (s_{x+1},…, s_p) del conjunto ordenado y el tráfico de red siendo inferior a un umbral predefinido.

Observando el tráfico de manera macroscópica, una dificultad es identificar mejor las entidades responsables de las variaciones macroscópicas en el tráfico. Con el fin de identificar un grupo de x clientes sospechosos, se procede a un filtrado del tráfico global observado repitiendo para una pluralidad de clientes una operación de supresión de un tráfico atribuible a un cliente. Con cada iteración, es el tráfico del cliente cuya covarianza con el tráfico global es la más fuerte que se suprime. La operación de supresión de un tráfico de cliente se repite hasta obtener una covarianza entre el tráfico filtrado y el tráfico global inferior a un umbral predefinido. Así, para cada una de las entidades P que contribuyen al tráfico global, se calcula la covarianza del tráfico de la entidad con el tráfico global, las entidades s_1,…, s_p siendo entonces clasificadas por covarianzas decrecientes. Se define igualmente una covarianza acumulada, cov($C_{u \to v}$), con u<v, como siendo la covarianza entre el tráfico generado por los clientes s de índices comprendidos entre u y v, y el tráfico global. El procedimiento identifica después el número x de clientes más implicados en la variación macroscópica del tráfico global identificando el índice x de la entidad a partir de la cual la covarianza acumulada cov($C_{x \to p}$)≤0. El tráfico de las entidades de índice x a P no presentando ya correlación con el tráfico global, mientras que las entidades x de índices 1 a x son las que presentan la correlación más fuerte con el tráfico global.

En una realización de la invención, la etapa de determinación de un periodo de análisis adecuado comprende:

- una etapa de selección de una zona de (m) tramos horarios pasados consecutivos,

- si el número de tramos sospechosos en dicha zona es inferior a una tasa (p) predefinida, mientras que una selección de una nueva zona comprende los tramos horarios pasados (m-1) más recientes, y

- si el número de tramos sospechosos en dicha zona es superior o igual a dicha tasa, mientras que el periodo de análisis adecuado es igual a dicha zona.

De forma ventajosa, el procedimiento permite determinar un periodo de análisis adecuado óptimo.

Con el procedimiento según la invención, la entidad (c_k) que contribuye al tráfico global se identifica por medio de un criterio (c), dicho criterio siendo un campo de un paquete IP emitido por dicha entidad que pertenece al grupo que comprende: dirección IP fuente, puerto fuente, petición DNS.

Se utilizan varios criterios con el fin de caracterizar variaciones macroscópicas en un tráfico de red. Típicamente, cualquier campo de un paquete IP puede ser utilizado. El procedimiento según la invención retiene no obstante varios campos pertinentes. Así, la dirección IP fuente, utilizada como criterio por el procedimiento según la invención, permite identificar cualquiera de las máquinas al principio de variaciones macroscópicas en el tráfico. En caso de ataque masivo de un servidor cuyo tráfico se observa por una pluralidad de máquinas organizadas en botnet, entonces el procedimiento según la invención permite identificar las máquinas que constituyen esta red de máquinas zombis.

Además de la identificación de máquinas al principio de variaciones macroscópicas en la red, el procedimiento se adapta para explicar el origen de las variaciones macroscópicas. Así, un criterio posible corresponde a una cuestión contenida en una petición DNS. Utilizando este criterio, es entonces posible identificar una avería de un servidor asociado a un nombre de dominio específico. En efecto, si las máquinas son registradas junto a este servidor, una avería del servidor va a conllevar un registro de estas máquinas junto al servidor. Para hacerlo, las máquinas precedentemente registradas, van a emitir peticiones DNS junto a los servidores DNS para recuperar la dirección IP del servidor junto al que desean registrase. Estas emisiones simultáneas de peticiones DNS provocan una variación macroscópica visible del tráfico de peticiones DNS.

Otro criterio interesante retenido por el procedimiento según la invención es el puerto fuente. En caso de ataque por denegación de servicio, este campo puede permitir identificar una firma de ataque. En efecto, durante el ataque masivo automatizado, que consiste en enviar un gran número de peticiones hacia un mismo servidor, es raro que todos los campos de los paquetes IP enviados de manera automática sean aleatorios. El puerto fuente forma parte de estos campos a menudo no vueltos aleatorios.

La invención se refiere también a un dispositivo de caracterización de tráfico adaptado para caracterizar entidades al principio de al menos una variación detectada en un tráfico de red, al menos una variación superior a un valor predeterminado siendo detectada en dicho tráfico, dicho dispositivo estando definido según la reivindicación 5.

La invención trata igualmente de un programa de ordenador en un soporte de datos y cargable en la memoria interna de un ordenador, comprendiendo el programa porciones de código para la ejecución de las etapas del procedimiento según la invención, cuando el programa es ejecutado en dicho ordenador.

La invención se refiere también a un soporte de datos en el que se registra el programa de ordenador según la invención.

Otras características y ventajas de la presente invención se comprenderán mejor a partir de la descripción y los dibujos adjuntos entre los que:

- la figura 1 representa las etapas del procedimiento de caracterización de entidades al principio de variaciones en un tráfico de red, según un modo particular de realización de la invención;

- la figura 2 representa un ejemplo de realización detallada de las etapas de observación continua del tráfico y de determinación de un periodo de análisis adecuado del procedimiento de caracterización de entidades según la figura 1;

- la figura 3 es un gráfico de tráfico de red observado que presenta variaciones importante, y que puede hacer el objeto de un análisis según el procedimiento de la invención;

- las figuras 4a, 4b y 4c son gráficos que presentan tráficos de cliente cuya covarianza con el tráfico total es representativa;

- la figura 5 es un ejemplo de arquitectura que pone en marcha el procedimiento según la invención.

Las etapas del procedimiento de caracterización de entidades al principio de variaciones significativas con respecto a un tráfico habitualmente observado en un tráfico de red según un ejemplo de realización de la invención van ahora a ser descritas en relación con la figura 1.

En una etapa inicial E10 de observación continua de un tráfico de red global hacia un servidor no representado, se identifica entre N_max tramos horarios de duración T correspondientes a una periodo de observación inicial del tráfico, n_susp tramos horarios de duración T sospechosos durante los que se observan variaciones comportamentales macroscópicas del tráfico global. Un ejemplo de tales variaciones se ilustra por la curva según la figura 3. El tráfico global corresponde al tráfico que entra para este servidor, es decir, el tráfico recibido por este servidor que proviene de una pluralidad de fuentes.

En este ejemplo de realización descrito aquí, la identificación de n_susp tramos horarios sospechosos consiste en identificar una fuerte variación de tráfico entre dos tramos horarios sucesivos T_{i-1} y T_i de duración T, que pasa un valor predefinido. La variación corresponde tanto a un aumento de tráfico como a una disminución. En este caso, los tramos horarios T_{i-1} y T_i se etiquetan como sospechosos.

Al final de la etapa 10, y seguido de la identificación de n_susp tramos horarios sospechosos entre N_max tramos horarios de observación inicial del tráfico global con destino al servidor, conviene efectuar un análisis preciso del tráfico para analizar los orígenes de las variaciones macroscópicas observadas en el tráfico global.

En una etapa E11 de determinación de un periodo de análisis adecuado, se determina un periodo de análisis adecuado y el tráfico correspondiente a este periodo. El periodo de análisis adecuado es en general más pequeño que el periodo de observación inicial y más rico en informaciones relativamente a las variaciones de tráfico, para permitir un análisis preciso de la variación macroscópica de tráfico. Con este fin, el periodo de análisis adecuado es evaluado como que es un número m de tramos horarios sucesivos de duración T entre los N_max de observación inicial que comprende al menos una tasa p de tramos sospechosos. La tasa p utilizada permite especificar un peso más importante en los tramos sospechosos. Habitualmente, la tasa p de tramos sospechosos está comprendida entre 30% y 70%. Por ejemplo, una tasa de 50% permite obtener un periodo de análisis adecuado que comprende al menos el 50% de tramos horarios sospechosos.

Una variante de realización de las etapas E10 de observación continúa, y E11 de determinación de un periodo de análisis adecuado será descrita más tarde en relación con la figura 2.

Una vez determinado el periodo de análisis adecuado, se procede, en una etapa E12 de recorte, a un recorte del tráfico global observado durante el periodo de análisis adecuando en n tramos horarios de análisis de duración t. La duración t es diferente de la duración T de los tramos horarios de observación inicial y en general más pequeña que T con el fin de disponer de un gran número de informaciones. Más el número n de tramos horarios de análisis t es importante, además habrá informaciones por tramo t de tiempo, no obstante más pesado será el análisis. Por ejemplo, se puede recortar el periodo de análisis adecuado en 100 tramos horarios de análisis.

En una etapa E13 de elección de criterio, se selecciona un criterio c para efectuar el análisis con el fin de explicar la variación detectada en el tráfico de red. El criterio c es un campo entre los campos de un paquete IP del tráfico de red. En el ejemplo de realización descrito aquí, el criterio c de análisis es la dirección IP fuente de los paquetes observados en el tráfico global. El valor c_k del criterio representa la dirección IP del cliente k, utilizado como dirección IP fuente en los paquetes emitidos por el cliente k. El cliente k puede así ser identificado por el valor c_k del criterio c.

Otros ejemplos de criterios se presentan más tarde.

Se señala que la etapa E13 de selección de un criterio es independiente de las etapas precedentes E11 y E12 y puede ser realizada previamente a la etapa E12, o a la etapa E11.

En una etapa E14 de identificación de clientes sospechosos, se identifica un conjunto de x clientes sospechosos implicados en la variación detectada en el tráfico entre P clientes que participan en el tráfico global cuyo comportamiento está fuertemente correlacionado con el comportamiento macroscópico observado.

Con este fin, en una subetapa E14-1 de evaluación de una similitud de tráfico entre un tráfico atribuible a una entidad y el tráfico de red, se calcula para cada cliente k que participa en el tráfico global, $1 \leq k \leq P$, e identificado por un valor c_k del criterio c, una covarianza $\text{cov}(c_k)$ según la fórmula siguiente:

$$\text{cov}(c_k) = \sum_{i=1}^{n} (r_{c_k,i} - r_{c_k}^0) * (R_i - R^0),$$

donde $r_{ck.i}$ representa el número de paquetes que responde al criterio c_k y observados en el tráfico global durante el tramo horario i de duración t.$r_{ck.i}$ es por lo tanto el número de paquetes de dirección IP fuente c_k observados en el tráfico global durante el tramo horario de análisis i.

$r_{c_k}^0$ representa la media del número de paquetes que responden al criterio c_k durante el periodo de análisis adecuado constituido por n tramos horarios de análisis, y se calcula como sigue:

$$r_{c_k}^0 = \frac{1}{m+1} \sum_{i=1}^{n} r_{c_k,i},$$

R_i representa el volumen de tráfico, en términos de número de paquetes, todos los clientes confundidos durante el tramo horario de análisis i de duración t, y se calcula como sigue:

$$R_i = \sum_{k=1}^{P} r_{c_k,i}$$

R_0 representa la media del tráfico global durante el periodo de análisis adecuado y se calcula como sigue:

$$R^0 = \frac{1}{n+1} \sum_{i=1}^{n} R_i$$

Por definición, la covarianza permite evaluar el sentido de variación de dos variables y, de ese modo, calificar la independencia de estas variables. En este caso particular, la covarianza $\text{cov}(c_k)$ calculada para el cliente k permite evaluar la dependencia entre el tráfico resultante del cliente k y el tráfico global. Representa por lo tanto una similitud de tráfico entre una parte del tráfico, atribuible al cliente k, y el tráfico de red. Cuanto más positiva y elevada es la covarianza calculada para el cliente k, más similares son las variaciones observadas en el tráfico resultante del cliente k a las observadas en el tráfico global.

Más precisamente, la covarianza $\text{cov}(c_k)$ asociada a un cliente k es tan grande como los intervalos entre los comportamientos instantáneos del cliente k con respecto a su medio comportamental, y el volumen total de tráfico con respecto a su media en el periodo de análisis son frecuentemente en el mismo sentido.

Se suministran ejemplos de tráficos de cliente cuya covarianza con el tráfico total es representativa en relación con las figuras 4a, 4b y 4c.

En una subetapa E14-2 de identificación de un grupo de x clientes sospechosos, se procede a un filtrado del tráfico global observado repitiendo para una pluralidad de clientes una operación de supresión de un tráfico atribuible a un cliente. Con cada iteración, es el tráfico del cliente cuya covarianza con el tráfico global es la más fuerte que se suprime. La operación de supresión de un tráfico de cliente se repite hasta obtener una covarianza entre el tráfico

filtrado y el tráfico global inferior a un umbral predefinido. En este ejemplo de realización de la invención, el umbral predefinido se fija en 0. La operación de supresión por lo tanto se repite hasta anular la covarianza. Se identifican así x clientes implicados en estas supresiones sucesivas. Estos clientes se identifican como los x clientes sospechosos entre los P clientes que participan en el tráfico global observado. El principio de la subetapa E14-2 es por lo tanto suprimir en el tráfico global el tráfico de los x clientes más sospechosos hasta obtener un tráfico filtrado exento de variaciones visibles, siendo un problema distinguir los x clientes sospechosos de estos que no lo son en un tráfico global.

Con este fin, se define un conjunto ordenado, señalado $C_{1\to P}$ de clientes de índices respectivos que van de 1 a P. En este ejemplo de realización, el conjunto de clientes se ordena según un orden decreciente de covarianza, cada cliente siendo identificado por su valor de criterio c, es decir, en este caso particular por su dirección IP. Se señala este conjunto $C_{1\to P}=\{s_1, s_2,\ldots, s_p)$, s_1 representando el cliente que genera un tráfico de cliente que tiene la covarianza más fuerte con el tráfico global, y s P el cliente generando un tráfico de cliente que tiene la covarianza más baja con el tráfico global. Se señala que para cualquier cliente de índice j, representado por el elemento s_j, con $1\leq j\leq P$, existe un valor c_i del criterio c, que corresponde aquí a la dirección IP de este cliente de índice j, con $1\leq i\leq P$, tal como $s_j=c_i$.

Se define una covarianza acumulada, $\text{cov}(C_{u\to v})$, con u<v, como que es la covarianza entre el tráfico generado por los clientes de índices comprendidos entre u y v, y el tráfico global. Más precisamente,

$$\text{cov}(C_{u\to v}) = \sum_{i=1}^{n}\left(\sum_{k=u}^{v}(r_{s_k,i} - r_{s_k}^0)\right) * (R_i - R^0) = \sum_{k=u}^{v}\left(\sum_{i=1}^{n}(r_{s_k,i} - r_{s_k}^0) * (R_i - R^0)\right)$$

$$= \sum_{k=u}^{v}\text{cov}(s_k)$$

Se señala que $\text{cov}(C_{1\to p})$ representa la covarianza del tráfico global con él mismo.

El objetivo es por lo tanto determinar el número x de clientes más implicados en la variación detectada en el tráfico global y por lo tanto el número x de clientes, tal como:

$$\text{cov}(C_{x+1\to P}) \leq 0\,.$$

Los clientes x, señalados s_1 a s_x, son los que generan un tráfico acumulado que presenta la correlación más fuerte con el tráfico global.

En otro ejemplo de realización de la invención, la identificación de los n-susp tramos horarios sospechosos efectuada en la etapa inicial E10 de observación del tráfico consiste en comparar el tráfico global observado en un tráfico medio, evaluado consecutivamente con un aprendizaje previo en un periodo de tiempo determinado. En general, el periodo de tiempo de aprendizaje corresponde a varios días consecutivos, que permiten así observar variaciones habituales en ciertos momentos del día, o ciertos días de la semana. Desviaciones del tráfico global observado superiores a un valor predeterminado con respecto al tráfico medio permiten etiquetar tramos horarios como sospechosos.

En otro ejemplo de realización de la invención, otro criterio que la dirección IP es retenido para efectuar el análisis con el fin de explicar la variación macroscópica de tráfico. Así, en la etapa E13 de selección de un criterio, un criterio seleccionado es el campo que corresponde a la petición DNS emitida (de *Domain Name Service*), por ejemplo www.monsite.com. En este ejemplo, el análisis permite descubrir que una avería de uno o varios servidores específicos está al principio de la variación macroscópica de tráfico. En otro ejemplo de realización de la invención, el criterio es el puerto fuente del paquete IP. En este ejemplo, el análisis permite identificar un punto común entre los paquetes que participan en la variación macroscópica. Este punto común es un índice que puede ser asimilado a una firma en caso de ataque. Así el procedimiento según la invención va a identificar entidades, identificadas por su dirección IP, su puerto fuente, la petición DNS, según el criterio elegido.

Una realización alternativa de las etapas E10 de observación continua del tráfico, y E11 de determinación de un periodo de análisis va ahora a ser descrita en relación con la figura 2.

En una etapa inicial E10-1 de vigilancia, se observa durante un tramo unitario corriente de duración T, el tráfico con destino a un servidor 56 según la figura 5.

En una etapa E10-2 de detección, se detecta una fuerte variación del tráfico entre el tramo unitario corriente de duración T y el tramo unitario precedente. La variación corresponde ya sea a un aumento brutal, ya sea una

disminución brutal del tráfico con destino al servidor.

En una etapa E11-1 de determinación de una ventana inicial de análisis, se determina una ventana inicial de estudio del tráfico observado que comprende el tramo unitario corriente así como los N_max-1 tramos horarios de duración T precedentes. El tráfico global observado durante la ventana inicial de estudio es suministrado por el colector 58 de tráfico según la figura 5. La ventana inicial de estudio, de duración N_Max tramos horarios de duración T representa por ejemplo el tráfico observado durante una duración de 24 horas.

En una etapa E11-2 de parametrización de la ventana de análisis, se tiene en cuenta un factor de ponderación p que precisa una tasa mínima de tramos sospechosos que desean encontrar en la ventana de análisis. Por ejemplo, se desea una tasa de 50% de tramos sospechosos. Después se evalúa el número de tramos sospechosos de tráfico observado durante la ventana inicial de estudio de duración N_max tramos horarios.

En una etapa E11-3 de ajuste del tamaño de la ventaja, mientras que la tasa de tramos sospechosos en la ventana de análisis corriente es inferior a la tasa deseada correspondiente al factor de ponderación p, entonces el tamaño de la ventana de análisis corriente es decrementado de 1 en términos de número de tramos horarios, el tramo horario más antiguo siendo el tramo que es quitado antes de reejecutar la etapa E11-3 de ajuste al tamaño de la ventana.

En una etapa E11-4 final, la ventana de análisis adecuada se determina; corresponde a la ventana corriente de análisis obtenido después de tantas ejecuciones de la etapa E11-3 de ajuste como sea necesario. Se constituyen m tramos horarios pasados y comprende una tasa de al menos p tramos sospechosos de duración T.

De forma ventajosa, la determinación de la ventana de análisis adecuado permite ajustar mejor el tráfico a analizar. Así, la ventana de análisis adecuado puede comprender varias variaciones macroscópicas de tráfico sucesivas que hacen aparecer, en un primer tiempo una variación positiva del tráfico observado, después en un segundo tiempo una variación negativa del tráfico. La variación positiva indica un aumento masivo de tráfico, que puede ser asociado a un envío masivo de peticiones desde un conjunto de máquinas, y la variación negativa una disminución masiva, signo de un paro simultáneo de los envíos de peticiones. Tal observación es reveladora de un ataque, y el periodo de análisis adecuado comprende al menos la variación positiva y la variación negativa del tráfico. En otro caso de figura en el que variaciones puntuales y regulares, por ejemplo diarias, se observan, un periodo de análisis adecuado de varios días, incluso una semana se adapta.

La figura 3 es una capa que ilustra un tráfico observado con destino a un servidor no representado. En la curva según la figura 3, se observa que entre las 20.50 h y las 21.00 h, el tráfico observado ha caído brutalmente. Igualmente, ha crecido brutalmente un poco antes de las 21.20 h, hasta las 21.40 h.

Van ahora a ser descritos ejemplos que ilustran tráficos de contribuidores cuya covarianza con el tráfico total es representativa en relación con las figuras 4a, 4b y 4c.

La figura 4a es una curva que representa el tráfico total con destino a un servidor no representado para la que ya se ha procedido a un recorte según un periodo de análisis adecuado. El periodo de análisis ha sido recortado aquí en 400 tramos. Se señalan variaciones macroscópicas importantes del tráfico en los tramos comprendidos entre 150 y 200, y entre 240 y 300.

La figura 4b es una curva que representa el tráfico de un cliente cuya covarianza con el tráfico total es fuerte. La covarianza calculada para este cliente es positiva. Se señala una similitud del comportamiento del cliente con el tráfico global: el cliente cesa de emitir paquetes en un tramo próximo a 150, y reemite de nuevo paquetes en un tramo próximo a 250.

En definitiva, la figura 4c es una curva que representa el tráfico de un cliente cuya covarianza con el tráfico es débil. La covarianza calculada para este cliente es negativa. Se señala un comportamiento completamente diferente en relación al tráfico global: el cliente emite en continuo paquetes entre los tramos 100 y 350.

Un ejemplo de arquitectura de red en el que se implanta un servidor capaz de poner en marcha el procedimiento según la invención va ahora a ser descrito en relación con la figura 5.

En una red 50, por ejemplo, la red de Internet, una pluralidad de clientes 51, 52, 53, 54 de los cuales solo cuatro se representan en la figura 5 emiten un tráfico constituido de paquetes IP hacia un servidor S 56. El tráfico con destino al servidor 56 transita por un equipo 55 de red, por ejemplo, un rúter, próximo geográficamente al servidor 56. El rúter 55 ve transitar el tráfico global con destino al servidor 56.

Un detector 57 de anomalías en un tráfico de red se adapta para supervisar todo el tráfico que transita por el rúter 55 por un mecanismo de reflejo (el término corrientemente utilizado es el término inglés *mirroring*), para transmitir a un colector 58 de tráfico la totalidad del tráfico supervisado y para detectar una anomalía en el tráfico con destino al servidor 56. La anomalía corresponde a una variación del tráfico en términos de número de paquetes, superior a un valor determinado. El detector 57 de anomalías en un tráfico es además adaptado para informar un dispositivo 59 de

caracterización de tráfico según un modo de realización particular de la invención de la detección de una anomalía en el tráfico observado.

El colector 58 de tráfico se adapta para almacenar en una memoria no representada, uno o varios diarios (el término corrientemente utilizado es el término *log*) que contiene toda la información pertinente relativamente al tráfico observado, como los paquetes IP que constituyen el tráfico, sellos temporales de dichos paquetes.

En la realización de la invención descrita aquí, el dispositivo 59 de caracterización de tráfico es un servidor informático que comprende módulos clásicos como:

- interfaces de red (no representadas) adaptadas para comunicar con el detector 57 de anomalías en un tráfico, el colector 58 de tráfico;

- una interfaz hombre-máquina (no representada), tal como una consola, adaptada para presentar a un operario humano resultados de una caracterización de entidades al principio de variaciones macroscópicas en una red, según la invención;

- un microprocesador (no representado), o CPU que es una unidad de tratamiento;

- una memoria de tratamiento (no representada) adaptada para efectuar cálculos, cargar instrucciones de programas que corresponden a las etapas del procedimiento de caracterización según la invención descrita precedentemente, y para hacerlos ejecutar por el microprocesador.

Para la puesta en marcha del procedimiento según la invención, el dispositivo 59 de caracterización de tráfico comprende además los módulos siguientes:

- un módulo 59-1 de determinación de un periodo de análisis adecuado, comprendiendo dicho periodo al menos el tramo horario sospechoso correspondiente a la variación detectada en el tráfico por el detector 57 de anomalías en un tráfico,

- un módulo 59-2 de evaluación, dispuesto para evaluar para cada entidad c_k, $1 \leq k \leq P$, que contribuye al tráfico de red, una similitud de tráfico entre una parte del tráfico atribuible a dicha entidad y el tráfico global. En el ejemplo de realización descrito aquí el módulo de evaluación evalúa una covarianza $\text{cov}(c_k)$ entre la parte del tráfico asociado a dicha entidad y el tráfico de red durante el periodo de análisis adecuado, y

- un módulo 59-3 de identificación, adaptado para identificar entre la pluralidad de entidades que contribuyen al tráfico de red, un grupo de entidades responsables de la variación detectada en la red, a partir de los valores de similitud de tráfico evaluados por el módulo 59-2 de evaluación. Con este fin, el módulo 59-3 de identificación está dispuesto para clasificar la pluralidad de entidades (c_k) que contribuye al tráfico de red en un conjunto ordenado, según un orden predefinido de similitud de tráfico (s_k), y para seleccionar x entidades consecutivas en el conjunto ordenado con el fin de formar dicho grupo, el valor de similitud de tráfico ($\text{cov}(C_{x \to P})$) entre el tráfico acumulado atribuible a las entidades restantes ($s_{x+1}, \ldots, s_P$) del conjunto ordenado y el tráfico de red siendo inferior a un umbral predefinido. En este ejemplo de realización de la invención, el umbral predefinido está fijado en 0.

Los módulos descritos precedentemente se unen al microprocesador a través de un bus de comunicación.

Los módulos 59-1, 59-2 y 59-3 están dispuestos para poner en macha las etapas del procedimiento de caracterización según la invención descrita precedentemente. Se trata preferentemente de módulos de programas que comprenden instrucciones de programas para hacer ejecutar las etapas del procedimiento de evaluación según la invención.

La invención se refiere por lo tanto también a:

- un programa de ordenador que comprende instrucciones para la puesta en marcha del procedimiento de caracterización de entidades al principio de variaciones macroscópicas en el tráfico tal como el descrito precedentemente, mientras este programa es ejecutado por un procesador;

- un soporte de registro legible por un lector en el que se registra el programa de ordenador descrito anteriormente.

Los módulos de programas pueden ser almacenados, o transmitidos por un soporte de datos. Este puede ser un soporte material de almacenaje, por ejemplo un CD-ROM, un disquete magnético o un disco duro, o bien un soporte de transmisión tal como una señal, o una red de telecomunicaciones.

REIVINDICACIONES

1.- Procedimiento de caracterización de entidades al principio de al menos una variación detectada en un tráfico de red, comprendiendo el procedimiento:

- una etapa (E11) de determinación de un periodo de análisis adecuado que comprende al menos un tramo horario sospechoso, conteniendo el tramo horario sospechoso la variación detectada en el tráfico,

- una etapa (E14-1) de evaluación, para una entidad (c_k) que contribuye al tráfico de red, de un valor representativo de una similitud de tráfico entre una parte del tráfico atribuible a dicha entidad y el tráfico de red durante el periodo de análisis adecuado, siendo realizada dicha etapa de evaluación para una pluralidad de entidades que contribuyen al tráfico de red, y

- una etapa (E14-2) de identificación, entre la pluralidad de entidades que contribuyen al tráfico de red, de un grupo de entidades responsables de la variación de tráfico, a partir de los valores de similitud de tráfico evaluados;

estando caracterizado dicho procedimiento porque dicha etapa de identificación comprende:

- una operación de supresión del tráfico atribuible a la entidad cuya similitud de tráfico con el tráfico de red es más fuerte, repitiéndose la operación de supresión hasta que la similitud de tráfico entre el tráfico filtrado y el tráfico global sea inferior a un umbral predefinido, comprendiendo el grupo de entidades las entidades cuyo tráfico ha sido filtrado.

2.- Procedimiento según la reivindicación 1, en el que la etapa (E14-2) de identificación del grupo de entidades comprende:

- una etapa de clasificación de la pluralidad de entidades (c_k) que contribuyen al tráfico de red en un conjunto ordenado, según un orden predefinido de similitud de tráfico (s_k),

- una etapa de selección de x entidades consecutivas en el conjunto ordenado con el fin de formar dicho grupo, siendo inferior a un umbral predefinido el valor de similitud de tráfico ($cov(C_{x \rightarrow P})$) entre el tráfico acumulado atribuible a las entidades restantes ($s_{x+1}, \ldots, s_p$) del conjunto ordenado y el tráfico de red.

3.- Procedimiento según la reivindicación 1, en el que la etapa de determinación de un periodo de análisis adecuado comprende:

- una etapa de selección de una zona de (m) tramos horarios pasados consecutivos,

- si el número de tramos sospechosos en dicha zona es inferior a una tasa (p) predefinida, entonces una selección de una nueva zona que comprende los tramos horarios pasados (m-1) más recientes, y

- si el número de tramos sospechosos en dicha zona es superior o igual a dicha tasa, entonces el periodo de análisis adecuado es igual a dicha zona.

4.- Procedimiento según la reivindicación 1, en el que la entidad (c_k) que contribuye al tráfico global se identifica por medio de un criterio, siendo dicho criterio un campo de un paquete IP emitido por dicha entidad que pertenece al grupo que comprende: dirección IP fuente, puerto fuente, petición DNS.

5.- Dispositivo (59) de caracterización de tráfico adaptado para caracterizar entidades al principio de al menos una variación detectada en un tráfico de red, siendo detectada en dicho tráfico al menos una variación superior a un valor predeterminado, comprendiendo dicho dispositivo:

- un módulo (59-1) de determinación de un periodo de análisis, dispuesto para determinar un periodo de análisis adecuado que comprende al menos un tramo horario sospechoso, conteniendo el tramo horario sospechoso la variación detectada en el tráfico,

- un módulo (59-2) de evaluación, dispuesto para evaluar, para cada entidad (c_k) que contribuye al tráfico de red, un valor representativo de una similitud de tráfico entre una parte del tráfico atribuible a dicha entidad y el tráfico de red durante el periodo de análisis adecuado, estando dispuesto dicho módulo igualmente para realizar la evaluación para una pluralidad de entidades que contribuyen al tráfico de red, y

- un módulo (59-3) de identificación, dispuesto para identificar entre la pluralidad de entidades que contribuyen al tráfico de red un grupo de entidades responsables de la variación de tráfico, a partir de los valores de similitud de tráfico evaluados por el módulo de evaluación;

estando caracterizado dicho dispositivo porque dicho módulo de identificación comprende unos medios de supresión

de tráfico, dispuestos para suprimir el tráfico atribuible a la entidad cuya similitud de tráfico con el tráfico de red es más fuerte, repitiéndose la operación de supresión hasta que la similitud de tráfico entre el tráfico filtrado y el tráfico global sea inferior a un umbral predefinido, comprendiendo el grupo de entidades las entidades cuyo tráfico ha sido filtrado.

6.- Programa de ordenador en un soporte de datos y cargable en la memoria interna de un ordenador, comprendiendo el programa porciones de código para la ejecución de las etapas del procedimiento según una de las reivindicaciones 1 a 4, cuando el programa es ejecutado en dicho ordenador.

7.- Soporte de datos en el que está registrado el programa de ordenador según la reivindicación 6.

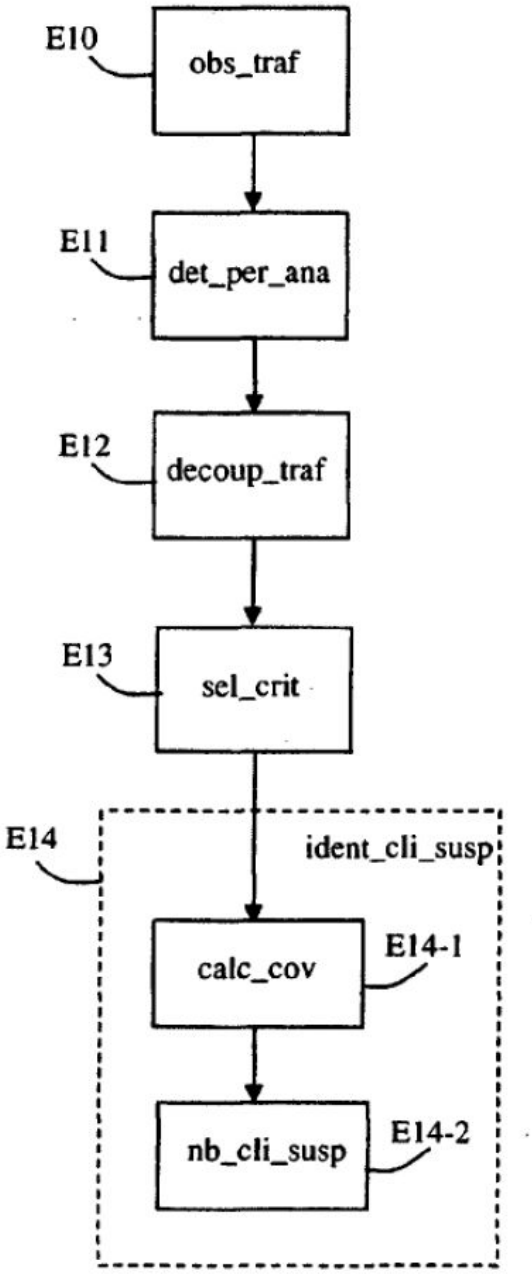
E10
obs_traf
E11
det_per_ana
E12
decoup_traf
E13
sel_crit
E14
ident_cli_susp
calc_cov
E14-1
nb_cli_susp
E14-2

Figura 1

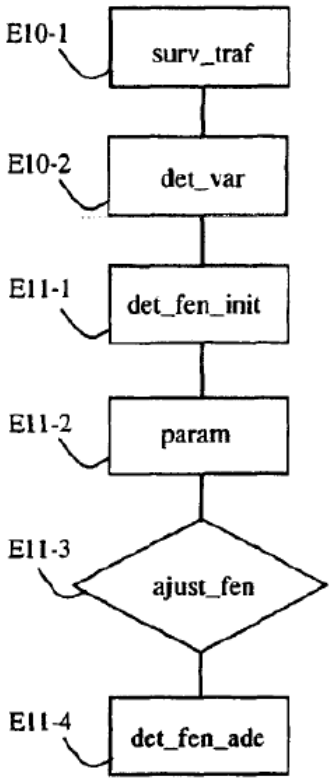

Figura 2

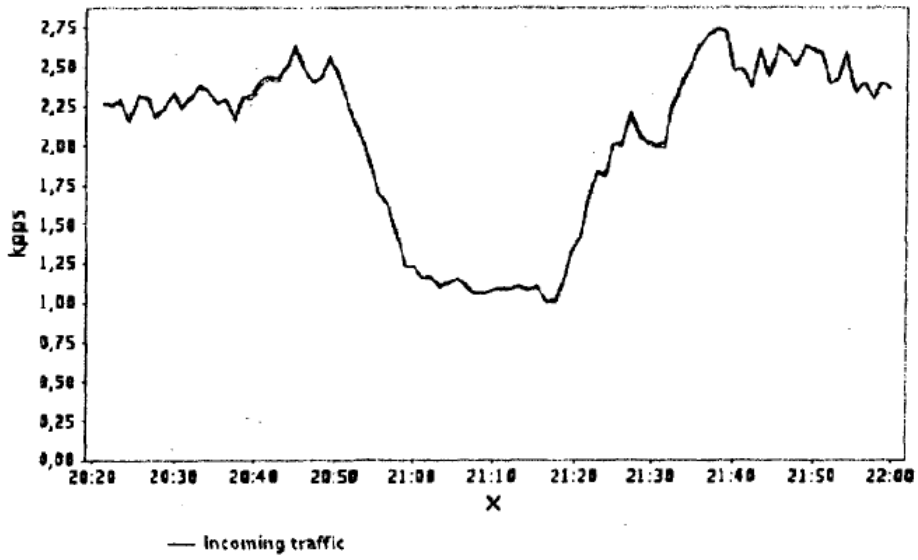

Figura 3

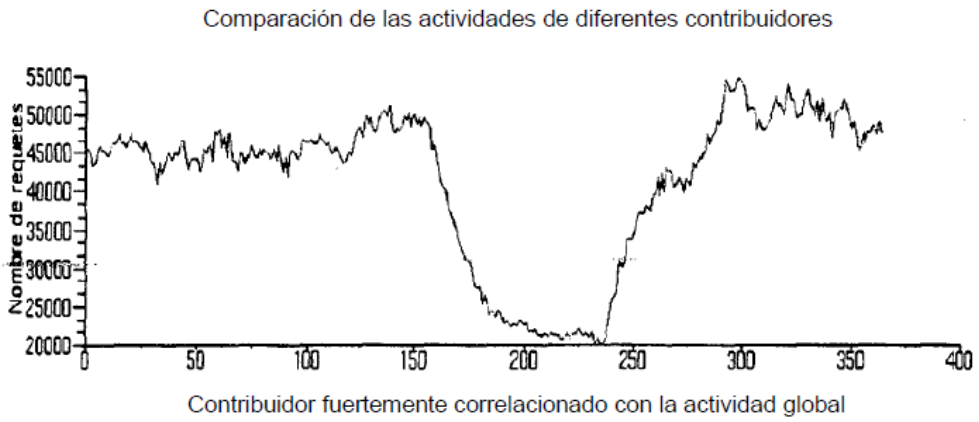

Figura 4a

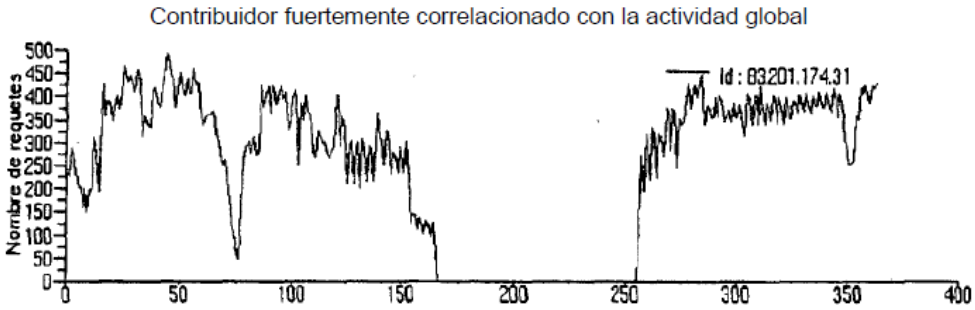

Figura 4b

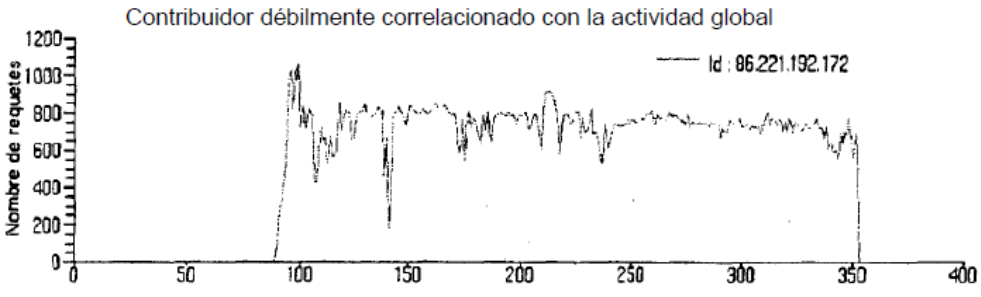

Figura 4c

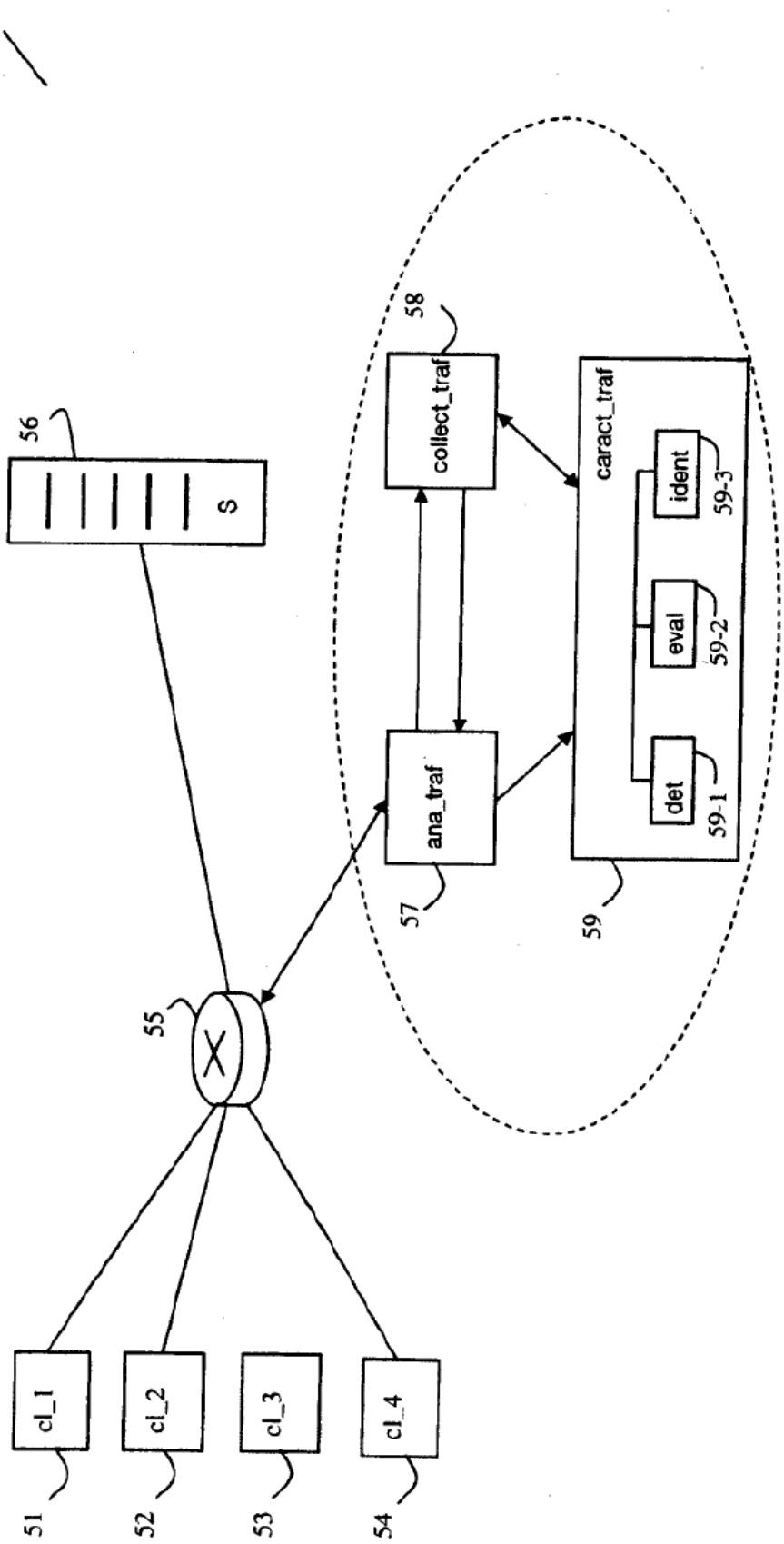
40
56
S
58
collect_traf
caract_traf
ident
59-3
eval
59-2
det
59-1
ana_traf
57
59
55
cl_1
cl_2
cl_3
cl_4
51
52
53
54

Figura 5