(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 651 215**

(51) Int. CI.:

H04W 12/08 (2009.01)
H04L 29/06 (2006.01)
H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.09.2012 PCT/EP2012/067341**

(87) Fecha y número de publicación internacional: **18.04.2013 WO13053550**

(96) Fecha de presentación y número de la solicitud europea: **05.09.2012 E 12758448 (0)**

(97) Fecha y número de publicación de la concesión europea: **22.11.2017 EP 2767112**

(54) Título: **Procedimiento y dispositivo para el control de una interfaz de telefonía móvil en terminales móviles**

(30) Prioridad:

14.10.2011 DE 102011054509

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.01.2018

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

LIEBERGELD, STEFFEN;
LANGE, MATTHIAS y
MULLINER, COLLIN

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCION

Procedimiento y dispositivo para el control de una interfaz de telefonía móvil en terminales móviles

La invención se refiere a un procedimiento y a un dispositivo para el control de una interfaz de telefonía móvil en terminales móviles, en particular un Modem virtual para el control de accesos-AT.

Estado de la técnica

En los años pasados se han emprendido muchas acciones para asegurar mejor los sistemas operativos de Smartphone. En este caso, el objetivo es proteger al usuario contra ataques y contra software nocivo (troyanos, virus de ordenador). Ejemplos de tales medidas son:

- Mandatory Access Control (MAC) (Control de Acceso Obligatorio), para poder limitar y controlar accesos a recursos sensibles (por ejemplo, datos de lugar, base de datos-SMS, agenda de direcciones
- Data Caging (almacenamiento de datos)
- Address Space Layout Randomization (ASLR), (Disposición aleatoria del diseño del espacio de direcciones) para dificultar la utilidad de huecos de seguridad.

A pesar de los ataques conocidos a redes de telefonía móvil a través de telefónicos móviles pirateados, hasta ahora apenas se conocen métodos para la protección de la infraestructura de las redes de telefonía móvil. El operador de la red de telefonía móvil sólo tiene hasta ahora la posibilidad de instalar en su red un filtro-SMS para poder filtrar SMS no deseados. Más bien estos ataques han mostrado que las medidas actuales de seguridad siguen la protección del aparato contra ataques y menos el entorno (red de telefonía móvil), en el que trabajan.

La patente US 5.628.030 describe un Modem virtual como un aparato, que proporciona un canal de comunicación a varias aplicaciones de comunicación activas al mismo tiempo. El Modem virtual conecta entonces de forma selectiva la aplicación de comunicación con el Modem físico. El Modem virtual implementa una interfaz de Modem abstracta.

En oposición a ello, la presente invención no publica ningún método para la multiplexión de un Modem físico, sino un método, con el que se puede controlar el acceso de un terminal móvil a una red de telefonía móvil en el terminal móvil de una manera segura. La patente US 5.628.030 se refiere, por lo demás, a un ordenador de sobremesa.

El documento DE 000069925732 T2 describe un teléfono móvil con Firmware de seguridad incorporado. Se describe un método con el que se puede acceder con seguridad a través de redes no aseguradas a una Intranet. La capa de seguridad se realiza en este caso en el teléfono móvil en forma de un Firmware, o de un módulo de Hardware externo.

El documento US 7 490 350 muestra un Firewall (cortafuegos) de hardware/software integrado, que es un nivel de seguridad adicional, que está intercalado.

El documento US 2009/0209291 muestra un procedimiento en el que se verifica la fiabilidad de mensajes de tráfico sobre la base de reglas en una base de datos.

A partir de la publicación Collin Mulliner ET AL "Poster: Honey Droid-Creating a Smartphone HoneyPot" IEEE-Security Mayo de 2011.

En cambio, la presente invención no necesita ningún Firmware asegurado o un módulo de hardware externo. Además, no se describe ningún método para asegurar relaciones de comunicación.

Los mensajes de señalización son generados a través del teléfono móvil y son enviados normalmente hacia el Mobile Switching Center (MSC) (Centro de Conmutación Móvil) y el Home Location Register (HLR) (Registro originario de posiciones). En el caso de conexiones de datos están implicados todavía Serving GPRS Support Node (SGSN) (Nodo de soporte de servicio GPRS) y el Gateway GPRS Support Node (GGSN) (Nodo de soporte de puerta GPRS).

Los datos son enviados en la red de telefonía móvil a través del llamado Packet Data Protocol (PDP) (Protocolo de datos en paquetes). El establecimiento de las conexiones-PDP es un proceso complejo. En primer lugar, el terminal móvil envía un mensaje "GPRS-Attach" a la SGSN. La SGSN autentifica el terminal móvil con la ayuda de HLR. A continuación, se genera un contexto PDP y se almacena en el SGSN y GGSN. En el contexto-PDP están almacenadas, entre otras cosas, informaciones para la interrupción, calidad de servicio y dirección IP de esta conexión. La administración y transmisión de un contexto-PDP a través de los diferentes componentes son muy costosas.

La conexión de un terminal móvil con la red de telefonía móvil se realiza a través de un componente, la llamada banda de base, que puede estar constituida por una pluralidad de componentes individuales, como, por ejemplo,

procesador de banda de base, módulos de radio, software, etc. Esta banda de base contiene normalmente un procesador estándar, un procesador de señales digitales (DSP) y los componentes de radio/telefonía móvil necesarios para la comunicación de telefonía móvil. La banda de base y sus componentes, como el procesador de banda de base y el software que se ejecuta en el mismo, antes de poder ser insertados en la red de telefonía móvil, deben ser certificados y homologados a través de diferentes instituciones. Este proceso es costoso e intensivo de costes. Por lo tanto, existen en todo el mundo sólo pocos fabricantes.

Normalmente, en terminales móviles existe, además de la banda de base, todavía un llamado procesador de la aplicación. En el caso de teléfonos móviles, en el procesador de la aplicación se ejecuta el sistema operativo del teléfono (por ejemplo, iOS o Android). En el caso de las llamadas palancas UMTS, el procesador de la aplicación es el procesador del ordenador. En cualquier caso, la banda de base y el procesador de la aplicación sólo están conectados entre sí en pocos lugares, entre otros a través de un canal de control. A través de este canal de control se comunica el procesador de la aplicación con la ayuda de instrucciones de control, para controlar la banda de base.

Sumario de la invención

La presente invención (llamada a continuación Modem virtual) para el control del canal de señalización de un terminal móvil no necesita modificaciones en el hardware o el software de la banda de base. A tal fin, se utilizan las características de acuerdo con las reivindicaciones. El Modem virtual se ejecuta totalmente en el procesador de la aplicación y tiene control exclusivo sobre la banda de base. El sistema operativo existente en el procesador de la aplicación no puede acceder ya directamente a la banda de base. En su lugar, el Modem virtual ofrece al sistema operativo una interfaz con la base de base y de esta manera puede controlar todos los accesos a la banda de base. Una representación de esta arquitectura se encuentra en la figura 1. La interfaz está constituida con preferencia por dos canales, son concebibles más canales. Uno de los canales se utiliza en una forma de realización para la corriente del comando de control, el segundo se utiliza para la corriente de datos.

El Modem virtual lleva a cabo de esta manera exclusivamente el intercambio de datos entre el sistema operativo y la banda de base, y acondiciona la funcionalidad de la banda de base, para contener de esta manera acceso a datos y para filtrar de este modo datos no autorizados.

En particular, se trata de un procedimiento para el control de una interfaz de telefonía móvil en un terminal móvil, que comprende una banda de base y un procesador de la aplicación. El procedimiento comprende las etapas:

- Ejecución de un sistema operativo en el procesador de aplicación. En este caso, se ejecutan Inter-aplicaciones, como navegador de Internet o una cámara de fotos en el procesador de la aplicación.

Como otra etapa, el procedimiento comprende la ejecución de un Modem virtual en el procesador de la aplicación, que lleva a cabo exclusivamente el intercambio de datos entre el sistema operativo y la banda de base, y acondiciona la funcionalidad de la banda de base, para obtener de esta manera acceso a datos y para filtrar de este modo datos y accesos no autorizados. De acuerdo con la invención, el Modem virtual acondiciona un canal virtual de señales y un canal virtual de datos, siendo transmitidas a través de la señal virtual de señales unas instrucciones de control, que controlar el Modem virtual. Además, a través del canal de datos se transmiten, además de otros datos, también datos-IP. También se pueden transmitir datos de voz como Voice-over-IP, que se transmiten como datos-IP. De acuerdo con la invención, un filtro de instrucciones de control es un componente del Modem virtual, que controla la corriente de la instrucción de control entre el sistema operativo y la banda de base y la filtra de acuerdo con las previsiones.

Además, un filtro-IP es un componente del Modem virtual que, a través de la implementación de un Firewall (cortafuegos), impide accesos no deseados desde fuera o desde dentro.

El Modem virtual acondiciona en una de una interfaz abstracta de Modem una banda de base, en la que se acondicionan la funcionalidad y las interfaces de las bandas de base. De esta manera, no se necesita ninguna o sólo pocas modificaciones en el sistema operativo y en el hardware. Con preferencia, se trata de una solución de software. Naturalmente, también es concebible una combinación de hardware y de software.

Adicionalmente, el Modem virtual presenta un actuador de banda de base, que acondiciona una interfaz con la banda de base. Este actuador tiene una estructura similar o igual que el actuador del sistema operativo, que tiene acceso normalmente directamente a la banda de base. A través de este actuador se establece de esta manera una conexión con el actuador de la banda de base del sistema operativo.

Un componente central del Modem virtual es el filtro de instrucciones de control. Éste controla y filtra la corriente de instrucciones de control entre el sistema operativo y la banda de base. Aquí se imponen las directrices de seguridad para el canal de señalización frente a la banda de base.

El componente de filtro-IP implementa un Firewall (cortafuegos), que impide, por ejemplo, accesos no deseados desde fuera o desde dentro. Supervisa el tráfico de datos que se ejecuta a través del mismo y con la ayuda de reglas establecidas decide si se dejan pasar o no determinados paquetes de la red. De esta manera, trata de impedir accesos no autorizados a la red. El cortafuegos puede trabajar en el plano del protocolo, en el plano de puertos, en el plano del contenido, puede reconocer ataque con determinados patrones (por ejemplo, DoS) y preparar Stateful Inspection (Inspección por estados). Además son concebibles sistemas de detección y prevención de la intrusión.

Desde el punto de vista del sistema operativo, el Modem virtual se comporta como una banda de base "auténtica". El sistema operativo existente no tiene que modificarse, Sólo son necesarias las adaptaciones habituales para la integración de una banda de base nueva.

La presente invención, que utiliza un Modem virtual, se puede utilizar, por ejemplo, para las siguientes aplicaciones:

- filtro de SMS Premium-SMS
- filtro de Números Premium
- protección de la infraestructura de telefonía móvil contra ataques-DoS basados en el canal de señalización
- supresión de redes zombie móviles
- actualización de las directrices de acceso a través de mantenimiento remoto (Remote Update)
- especialización / actualización definidas por el usuario de directrices de acceso para los llamados servicios Premium
- acceso VPN inevitable
- cortafuegos en el terminal móvil

El Modem virtual ofrece las siguientes mejoras frente al estado de la técnica:

- no son necesarias ninguna o sólo pocas modificaciones en el sistema operativo existente, según la implementación;
- no son necesarias modificaciones en el hardware móvil existente;
- protección de la red de telefonía móvil contra terminales móviles pirateados;
- filtración de los mensajes de señalización directamente sobre el terminal móvil, para que se evite la sobrecarga de la infraestructura de telefonía móvil;
- empleo económico porque el Modem móvil está implementado directamente en el terminal móvil, no son necesarias modificaciones en la infraestructura;
- supresión de servicios caros de valor añadido (los llamados SMA Premium o Números Premium
- Control sobre el acceso de datos.

La invención posibilita de esta manera

- una supresión con éxito de un troyano-SMS
- reconocimiento heurístico de canales de instrucciones-y-control sobre SMD
- los ataques a la infraestructura del operador de la red de telefonía móvil son más costosos (elevación de los abonados al menos en 700 %)
- reducción de la carga sobre la infraestructura de telefonía móvil a través de la limitación de tasas de instrucciones críticas.

Descripción de las figuras

A continuación se describen brevemente las figuras.

La figura 1 muestra un concepto y una estructura de capas del Modem virtual.

La figura 2 muestra un diagrama de flujo del procedimiento de principio del filtro de instrucciones de control.

Descripción de una forma de realización

La figura 1 muestra la estructura de capas de un terminal móvil de la presente invención. El sistema operativo es ejecutado en un procesador de la aplicación, es decir, en general, en un hardware real, en el caso individual también se puede virtualizar. Durante la virtualización, el sistema operativo, por ejemplo Android, es ejecutado en una capa de virtualización, llamada también Hypervisor, en la que el Modem virtual o bien está dispuesto en el Hypervisor como hardware virtual o es también una máquina virtual. que es ejecutada en el Hypervisor. El sistema operativo comprende una pila de software de aplicación, en la que se ejecutan aplicaciones para el usuario. Esta pila puede comprender, por ejemplo, bibliotecas y armazones, que son utilizados por las aplicaciones. Además, éstos ofrecen interfaces con el sistema operativo-Kernel. Dentro de este Kernel se forman un canal virtual de señales y un canal

virtual de datos hacia un Modem virtual, que está conectado como capa intermedia entre la banda de base y el sistema operativo. El sistema operativo tiene acceso, por lo tanto, a la banda de base solamente a través del Modem virtual. A través del canal virtual de señales se emiten, en general, instrucciones de control, que sirven para controlar el Modem virtual. A través del canal virtual de datos se transmiten entonces los datos después del ajuste del Modem, por ejemplo como corriente de datos. La corriente de datos puede comprender una corriente de voz, pero también datos de Internet (datos-IP). Sobre la corriente de datos respectiva se aplican entonces filtros (filtros de instrucciones-AT y filtros-IP), para eliminar por filtración datos no autorizados o no deseados en ambas direcciones. Así, por ejemplo, sobre el filtro-IP se pueden aplicar escáneres, que reconocen contenidos de software nocivo, o también otros filtros de contenido, como filtros de protocolos. Dentro del Modem virtual está dispuesto un actuador de la banda de base, que agrupa las dos corrientes, cuando es necesario, y las transmite a la banda de base/unidad, como ya se ha descrito anteriormente. De manera alternativa, los datos se pueden transmitir también a través de dos canales separados.

La figura 2 muestra un ejemplo para una aplicación de la presente invención.

En este caso, se reconocen y se filtran determinados ataques.

Ataque de desvío de llamadas

Muchos teléfonos móviles comprometidos modifican continuamente los ajustes para la transmisión de la llamada y de esta manera generar una carga considerable en la infraestructura del proveedor de la red de telefonía móvil.

El software de aplicación genera una instrucción para la modificación de los ajustes de transmisión de llamadas. Esta instrucción se transmite a través del canal virtual de señales al Modem virtual. El filtro de instrucciones de control verifica con la ayuda de un umbral si se ha excedido el número permitido de instrucciones por unidad de tiempo para esta función y, dado el caso, bloquea la instrucción hasta el comienzo del siguiente intervalo de tiempo. Si no se ha excedido todavía el número permitido, se conduce la instrucción al actuador de la banda de base y se envía finalmente desde la banda de base hasta la red de telefonía móvil. La figura 2 muestra que en el caso de que el instante de la última instrucción más un intervalo sea mayor que el instante actual, se realiza una verificación del contador; y en el caso de que el contador esté por encima de un valor límite, entonces se bloquea el mensaje. En otro caso, se transmite el mensaje.

Premium-SMS

Troyanos-SMS envían sin conocimiento del usuario sus Premium-SMS y de esta manera pueden conducir a un daño económico considerable para el usuario.

El troyano-SMS deposita un mensaje-SMS en un número Premium a través el canal virtual de señales. El filtro de instrucciones de control verifica con la ayuda de una lista negra / lista blanca si debe enviarse el SMS. Si el número del receptor se encuentra en la lista negra, entonces se indica al usuario una alarma correspondiente y, dado el caso, se solicita una confirmación del usuario. Si se rechaza la emisión por el usuario, se derecha el mensaje-SMS. Estas listas pueden actualizarse, por ejemplo, regularmente en-línea.

REIVINDICACIONES

1.- Procedimiento para el control de una interfaz de telefonía móvil en un terminal móvil, en el que el terminal móvil comprende un procesador de banda de base y un procesador de la aplicación, que comprende las etapas:

- ejecución del sistema operativo en el procesador de la aplicación;
- ejecución de un Modem virtual en el procesador de la aplicación, de manera que el Modem virtual emula un procesador de la banda de base, en el que se acondicionan la funcionalidad y las interfaces del procesador de la banda de base, en el que el Modem virtual realiza exclusivamente el intercambio de datos entre el sistema operativo y el procesador de la banda de base, y acondiciona la funcionalidad del procesador de la banda de base para conseguir de esta manera acceso a datos no permitir para eliminarlos por filtración, en el que el Modem virtual acondiciona una señal de señalización virtual y un canal de datos virtual, en el que a través del canal de señalización virtual se transmiten instrucciones de control-AT, que controlan el Modem virtual, y a través del canal de datos se transmiten datos-IP, en el que un filtro de instrucciones de control-AT es un componente del Modem virtual, que controla la corriente de instrucciones de control-AT entre el sistema operativo y el procesador de la banda de base y la filtra según las previsiones, y en el que un filtro-IP es un componente del Modem virtual que, a través de la implementación de un cortafuegos impide accesos no deseados desde fuera o desde dentro.

2.- El procedimiento de acuerdo con la reivindicación anterior, en el que se emplean uno o varios de los siguientes componentes en el filtro, para filtrar los datos:

- filtro de números;
- filtro para la protección de la infraestructura de telefonía móvil contra ataques-DoS basados en el canal de señalización;
- filtro para la supresión de redes zombie móviles;
- componente de actualización de las directrices de acceso, que está sujeto a actualizaciones regulares;
- componente para la especialización / actualización definidas por el usuario de directrices de acceso para los llamados servicios Premium
- componente de control para la limitación de accesos-VPN.

3.- El procedimiento de acuerdo con la reivindicación anterior, en el que el Modem virtual presenta un actuador de la banda de base, que acondiciona una interfaz con el procesador de la banda de base.

4.- Terminal móvil con una interfaz de telefonía móvil, que comprende:

un procesador de la banda de base y un procesador de la aplicación, en el que el procesador de la aplicación presenta medios para ejecutar un sistema operativo;
el procesador de la aplicación contiene también medios, que realizan un Modem virtual, en el que el Modem virtual emula un procesador de banda de base, en el que se acondicionan la funcionalidad y las interfaces del procesador de la banda de base, en el que el Modem virtual lleva a cabo el intercambio de datos entre el sistema operativo y la banda de base y acondiciona la funcionalidad de la banda de base, para obtener de esta manera acceso a datos no autorizados para eliminar estos datos por filtración;
en el que el Modem virtual acondiciona un canal de señales virtual y un canal de datos virtual, en el que a través del canal de señalización virtual se pueden recibir instrucciones de control-AT, que controlan el Modem virtual, y a través del canal de datos se pueden transmitir datos-IP; y en el que un filtro de instrucciones de control-AT es un componente del Modem virtual, que controla la corriente de instrucciones de control-AT entre el sistema operativo y la banda de base y la filtra de acuerdo con las previsiones, y
en el que un filtro-IP es un componente del Modem virtual, que impide a través de la implementación de un cortafuegos accesos no autorizados desde fuera o desde dentro.

5.- Terminal móvil de acuerdo con la reivindicación precedente, en el que uno o varios de los siguientes componentes están presentes en el filtro, para filtrar los datos:

- filtro de números;
- filtro para la protección de la infraestructura de telefonía móvil contra ataques-DoS basados en el canal de señalización;
- filtro para la supresión de redes zombie móviles;
- componente de actualización de las directrices de acceso, que está sujeto a actualizaciones regulares;
- componente para la especialización / actualización definidas por el usuario de directrices de acceso para los llamados servicios Premium
- componente de control para la limitación de accesos-VPN.

6.- Terminal móvil de acuerdo con la reivindicación precedente, en el que el Modem virtual presenta un actuador de la banda de base, que acondiciona una interfaz con la banda de base.

5

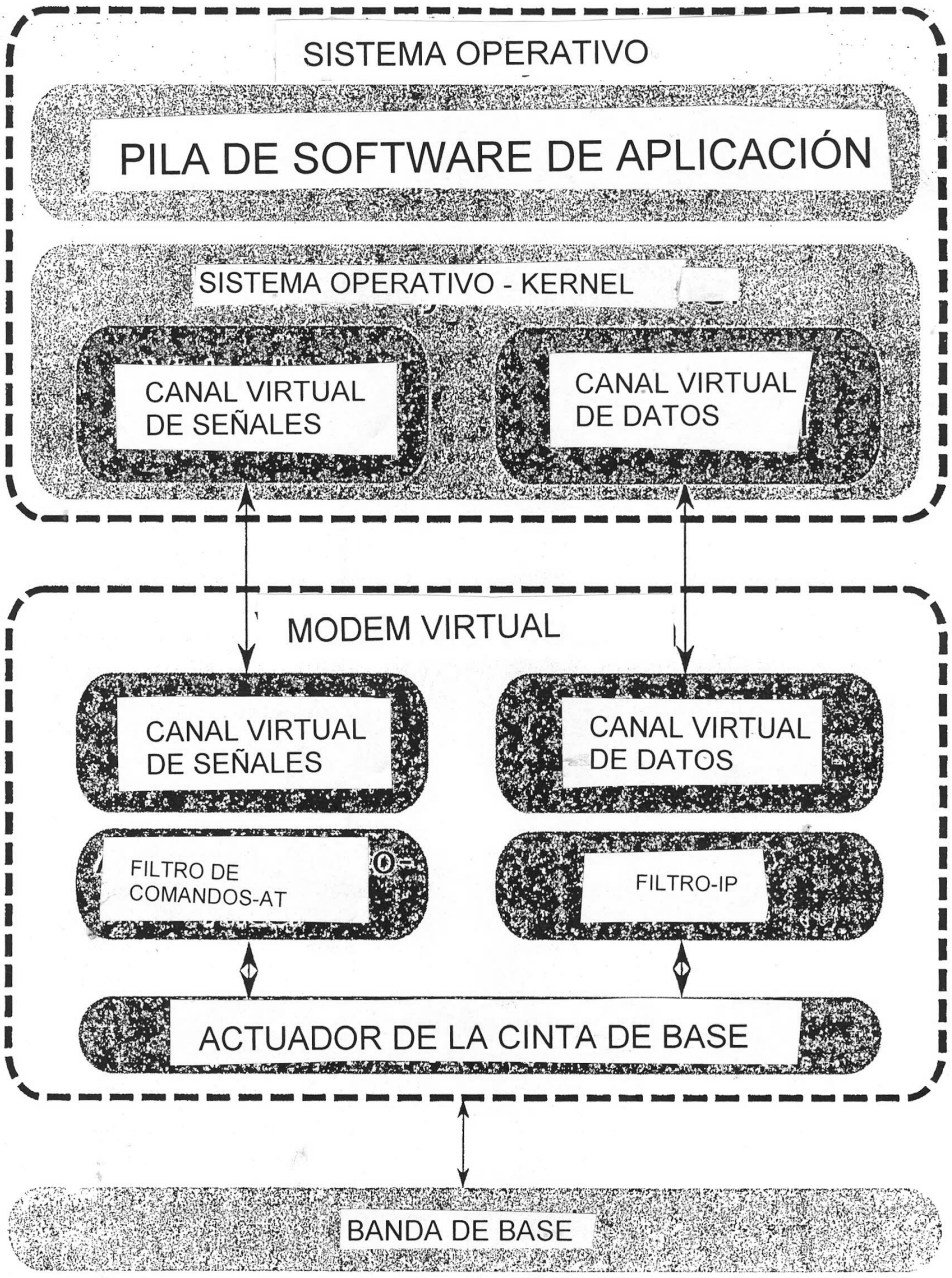
SISTEMA OPERATIVO
PILA DE SOFTWARE DE APLICACIÓN
SISTEMA OPERATIVO - KERNEL
CANAL VIRTUAL DE SEÑALES
CANAL VIRTUAL DE DATOS
MODEM VIRTUAL
CANAL VIRTUAL DE SEÑALES
CANAL VIRTUAL DE DATOS
FILTRO DE COMANDOS-AT
FILTRO-IP
ACTUADOR DE LA CINTA DE BASE
BANDA DE BASE

Fig. 1

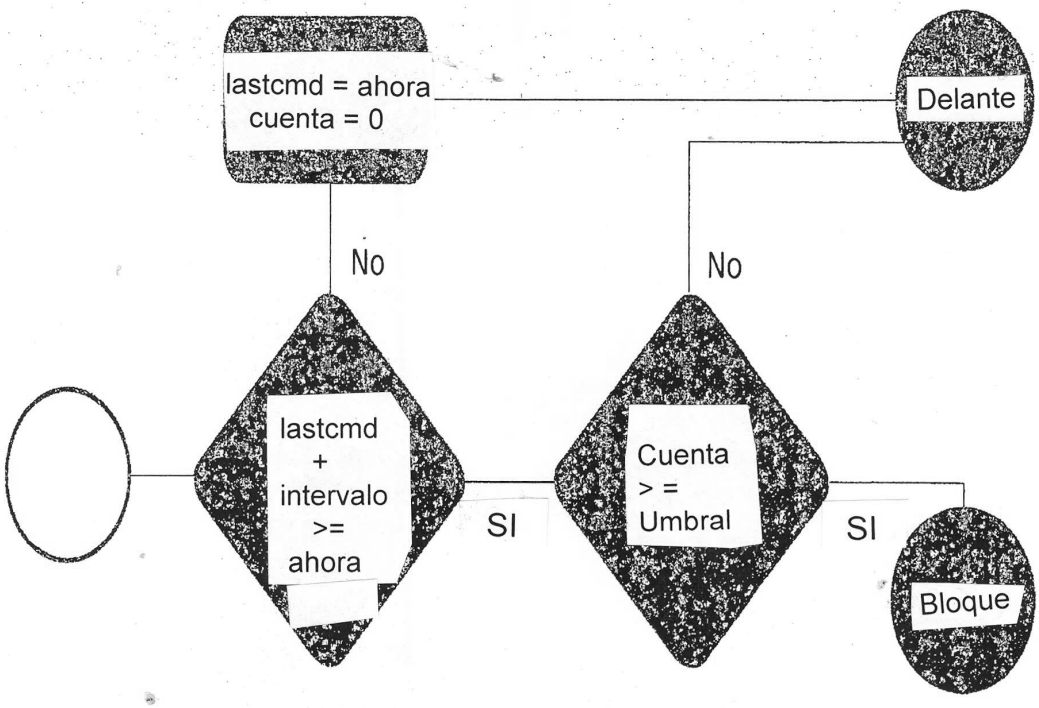
lastcmd = ahora
cuenta = 0
Delante
No
No
lastcmd
+
intervalo
>=
ahora
SI
Cuenta
> =
Umbral
SI
Bloque

Fig. 2