(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 464 343**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.02.2009 E 09715823 (2)**

(97) Fecha y número de publicación de la concesión europea: **26.03.2014 EP 2283629**

(54) Título: **Procedimiento de gestión en los equipos de seguridad y entidad de seguridad**

(30) Prioridad:

26.02.2008 FR 0801037

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.06.2014

(73) Titular/es:

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

(72) Inventor/es:

MAXIMILIEN, BENOIT y
KSINANT, VLADIMIR

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento de gestión en los equipos de seguridad y entidad de seguridad

La invención se refiere a un procedimiento y una entidad utilizados particularmente en el campo de la seguridad de los sistemas de información. Se aplica, por ejemplo, en el campo de la gestión de los equipos de seguridad que se colocan en la separación de flujo de informaciones en el seno de una red.

Actualmente, por lo que el Solicitante conoce, para asegurar la seguridad durante los intercambios de datos o de informaciones entre equipos en el seno de una red, es conocida la utilización de unos centros de gestión y de seguridad específicos. Esto engendra una carga importante para los operadores, tal como los bancos o cualquier otro operador que trabaje en el campo de la seguridad de los sistemas de información (SSI). Esta carga es tanto más importante cuanto más grande sea el número de equipos a gestionar. Existe por tanto una necesidad de encontrar una solución de gestión transparente que permita racionalizar a la vez los medios humanos y materiales.

Diferentes aplicaciones conocidas en la técnica anterior necesitan un centro de gestión para:

- los equipos criptográficos que están colocados en la separación material en una red denominada sensible, como los codificadores de alta velocidad, los codificadores de rutas de seguridad (en particular Ethernet), los codificadores individuales,
- los equipos de filtrado que están colocados en la separación material en una red sensible, por ejemplo, los cortafuegos,
- los programas de seguridad instalados en los terminales y los servidores que manipulan la información: los cortafuegos programados, los programas de codificación, los programas antivirus, los programas de autentificación de usuarios, etc.

En lo que sigue de la descripción, la abreviatura ES designa las Entidades de Seguridad que agrupan el conjunto de los equipos y productos citados anteriormente.

En materia de seguridad en el intercambio de información o de datos y de los sistemas de información, es primordial gestionar unas entidades de seguridad. En efecto, es necesario un cierto número de servicios para la administración de los equipos criptográficos tanto si son civiles como militares. Si bien hay una especificidad en las redes sensibles, debido al hecho de los protocolos utilizados, de las protecciones particulares, de los algoritmos utilizados o incluso del nivel de seguridad buscado, frecuentemente se encuentra el mismo tipo de gestión:

- la gestión de la política de las seguridades: dicho de otra manera, el establecimiento de las asociaciones de seguridad o SA, o incluso la constitución de comunidades o la creación de redes privadas virtuales conocidas con la abreviatura anglosajona VPN que llegan a determinar quién puede dialogar con quién, cómo generar las claves; es lo que se puede denominar “los derechos”,
- la gestión de la supervisión, es decir la recreación de informaciones que proceden de las entidades: alarmas, eventos, conexiones o registros, la base común de información o la base de la información de gestión conocida bajo la abreviatura anglosajona “MIB” para el mundo IP (Internet Protocol), la gestión de la configuración, la gestión de los hechos técnicos, y de los incidentes, etc.; es lo que se puede denominar “la notificación”,
- la administración de productos de seguridad que asegura la integridad de la red y de la confianza (garantía aportada por los certificados, unas infraestructuras de clave pública o “PKI”, unos anuarios, …); es lo que se denomina “la autoridad”.

La figura 1 esquematiza los 3 bloques integrados antes citados que constituyen el módulo de gestión: los derechos, la notificación y la autoridad.

La figura 2 es un esquema que describe una unidad central de gestión ES vinculada con varios equipos ES_i, ES_i, pudiendo comunicarse entre sí los diferentes equipos.

Uno de los problemas presentados por la técnica anterior es que cada equipo puede tener su propia política de seguridad y utilizar unos elementos propietarios en términos de interfaces, de protocolos, de algoritmos, de usos y de contextos de uso. Estas especificidades impiden u obstaculizan la interoperabilidad entre los equipos y su puesta en común. O, todos los actores del campo antes citado SSI buscan actualmente racionalizar los medios tanto humanos como materiales.

Por otro lado, el sistema centralizado conocido en la técnica anterior constituye un serio freno a la implementación de funciones de seguridad en unos entornos de redes muy evolutivos como las redes de radios ad hoc, es decir unas redes en las que los nodos y los equipos son móviles. Aunque los problemas de las redes estén hoy en día en curso de resolución, la utilización de una gestión centralizada de la seguridad en tales entornos camina hacia el objetivo de flexibilidad y de descentralización.

En lo que sigue la descripción hace referencia a unas denominaciones conocidas para el experto en la técnica para designar diferentes equipos utilizados en el sistema y el procedimiento según la invención.

De ese modo, el término confianza designa la determinación por una ES de su futuro comportamiento frente a otra ES. Esta confianza puede elaborarse en base a pruebas firmes tales como la existencia de un secreto compartido entre las ES. Este o estos secretos pueden ser unas claves, unas palabras clave, un algoritmo criptográfico o cualquier otro dato confidencial. En ausencia de pruebas firmes, la confianza puede fundarse igualmente sobre:

- el comportamiento pasado de las ES en cuestión,
- el grado de amenaza a que están sometidas las ES.

Una plataforma de confianza, expresión conocida en el campo de la seguridad, es un dispositivo material, tal como un procesador, un circuito programable del tipo FPGA (Field Programmable Gate Array), un circuito integrado específico más conocido bajo la abreviatura anglosajona “ASIC” y un programa en el que los expertos de seguridad tengan confianza, es decir que tienen:

- el dominio completo de los componentes y las tarjetas electrónicas (circuito impreso, cableado), en los mecanismos de protección de las ES (etiquetas holográficas, caja resistente a la radiaciones electromagnéticas),
- la ausencia de puertas traseras, más conocidas bajo el término anglosajón “Back door” que presentan el riesgo de dejar pasar en claro, sin cifrar, unas informaciones consideradas como sensibles sin pasar por el módulo de codificación,
- el dominio de los códigos y la ausencia de errores en la ejecución de los programas o “bug” (ensayo de cobertura, regla de codificación, análisis del código).

La mayor parte de los elementos citados anteriormente son conocidos para el experto en la materia que trabaja en el campo de la seguridad y no se detallarán.

Frecuentemente se coloca una plataforma de confianza en la separación y no como recurso con el fin de garantizar un alto nivel de seguridad y ser el paso obligado de todos los mensajes entre dominios, entre el dominio sensible A y el dominio libre no sensible B.

La palabra “voto” se relaciona con un mecanismo de diálogo entre entidades en el que una entidad solicita a otras su opinión con el objetivo de tomar una decisión colegiada. La decisión se notifica a continuación al conjunto de las entidades afectadas. El voto se basa por tanto en un mecanismo de red de pregunta/respuesta/notificación de decisión conocido para el experto en la técnica. La palabra “padrino” corresponde a la entidad por medio de la que se decide la adhesión de un recién llegado (o ahijado) en el seno de una comunidad. El padrino tiene por misión igualmente transmitir al ahijado todos los elementos de configuración que le permitan comunicar en el seno de la comunidad.

El documento WO 2000/78004 describe un procedimiento de gestión de varias entidades de seguridad ESi programadas o materiales colocadas en la separación del flujo de la información en el seno de una red existente en el que varias entidades de seguridad ESi comunican entre sí. El documento presenta un sistema de gestión de política unificada para una organización que incluye un servidor de política central y unas entidades de seguridad ESi de software o hardware colocadas en la separación del flujo de información colocadas a distancia. Uno de los objetivos de la presente invención es suministrar unas entidades capaces de autogestionarse entre ellas sin tener que recurrir a una instancia superior. Esta gestión automática implica que existe la confianza durante los intercambios de información entre los miembros de la red y que se propaga de manera dinámica y descentralizada. El procedimiento y sistema según la invención reposa particularmente en la implementación simultánea de ciertas reglas:

- la supervisión de una entidad por las otras entidades, la propagación de las informaciones a través de la red formada por varias entidades. Para ello, el sistema implementa, por ejemplo, las reglas siguientes: unas reglas de adopción de una entidad en el seno de una red constituida por varias entidades que comunican entre sí, unas reglas de comunicación entre estas entidades y unas reglas de exclusión o de integración de una entidad.

La invención se refiere a un procedimiento de gestión de varias entidades de seguridad ESi de software o hardware colocadas en la separación del flujo de información en el seno de una red existente en la que varias entidades de seguridad ESi comunican entre sí, caracterizado porque comprende al menos las etapas siguientes:

- designar una entidad que juega el papel de padrino para una nueva entidad o ahijado que desea unirse a la red,
- dicho ahijado contacta con dicho padrino y tras la recepción de la solicitud de conexión de dicho ahijado, dicho padrino determina si acepta o no la conexión,
- si el padrino acepta la conexión de dicho ahijado, entonces el padrino se conecta a dicho ahijado y se desconecta de los otros equipos de ES que forman la red,
- al menos una de las entidades y/o el padrino verifican el nivel de seguridad de dicho ahijado,

  - si el padrino o al menos una de las entidades decide dar la confianza a dicho ahijado, entonces, el padrino transmite al ahijado unas informaciones de configuración adaptadas para permitirle entrar en comunicación con las otras entidades de la red,
  - si el padrino o al menos una de las entidades decide no dar la confianza al ahijado, entonces este último

no puede acceder a la red y se genera una alarma hacia las otras entidades de la red

El procedimiento comprende una etapa de acceso del ahijado a la red después de la etapa de inicialización que comprende las etapas siguientes: si el ahijado es aceptado por las entidades a las que ha contactado, los registros de direcciones de las entidades contactadas son puestos al día con los datos del ahijado, y el ahijado comunica entonces libremente con las entidades con las que ha contactado.

Cada entidad supervisa, por ejemplo, el comportamiento de las entidades que forman parte de su registro de direcciones utilizando unas reglas de comunicación establecidas.

Una entidad que detecte una anomalía de funcionamiento o un comportamiento anormal por parte de otra entidad advierte, por ejemplo, a todas las entidades de la red de esta anomalía.

Todas las entidades prevenidas se advierten entonces mutuamente de sus opiniones respectivas sobre la decisión de exclusión y, según la naturaleza de los mensajes recibidos y según un algoritmo, las entidades toman la decisión:

- de excluir a la entidad que ha sido denunciada, siendo excluida dicha entidad denunciada de todos los registros de direcciones,
- de no hacer nada,
- de excluir a la entidad que ha denunciado, siendo excluida a continuación esta última entidad de todos los registros de direcciones.

La invención se refiere también a una entidad de seguridad de software o hardware colocada en la posición de separación de los flujos de informaciones en el seno de una red que comprenda varias entidades de ES que comunican entre sí, caracterizada porque comprende al menos los elementos siguientes:

- un medio de conexión de una entidad a un equipo a proteger, estando adaptado dicho medio para ejecutar las etapas del procedimiento antes citadas
- dicho medio está en conexión con un multiplexor, que recibe por un lado unas órdenes que provienen de un dispositivo de control lo que permite el cambio de modo de funcionamiento de los equipos,
- el multiplexor tiene una entrada para los datos protegidos que proceden del puerto de entrada/salida, una entrada para los datos que proceden del puerto utilizado para la fase de inicio, una entrada que recibe las órdenes, una salida que transmite los datos hacia una plataforma de confianza,
- la plataforma de confianza posee una salida que se conecta a un puerto de salida hacia una red no protegida.

Dicho medio de conexión comprende funcionalmente (el medio puede implementarse o bien de manera material o bien de manera programada):

- un puerto de entrada/salida estándar conectado a una red o a una estación o a un programa a proteger,
- un puerto de contacto o de entrada que tiene por función permitir ejecutar la fase de inicio implementada por el procedimiento antes citado.

Dicho medio de conexión comprende por ejemplo dos módulos de software, estando adaptado uno de los dos módulos para ejecutar la fase de inicio implementada por el procedimiento antes citado.

La plataforma de confianza puede comprender un módulo de generación aleatorio y/o un módulo de memorización.

Dicho medio de conexión comprende un módulo de software adaptado para ejecutar la fase de inicialización de un ahijado en una red ejecutando las etapas del procedimiento antes citado y un módulo de software adaptado para gestionar las entradas/salidas entre una entidad y una red.

Surgirán mejor otras características y ventajas del dispositivo según la invención con la lectura de la descripción que sigue de un ejemplo de realización dado a título ilustrativo y en ningún caso limitativo con la adición de las figuras que representan:

- Las figuras 1 y 2, unos esquemas de funcionamiento del sistema con una gestión centralizada según la técnica anterior,
- La figura 3, un esquema del sistema de gestión descentralizado según la invención,
- La figura 4, las etapas implementadas durante la inicialización del sistema,
- La figura 5, las etapas ejecutadas durante la fase de acceso de un equipo al sistema,
- La figura 6, ejemplo de comunicación a continuación del primer acceso a la red del sistema de una nueva entidad,
- La figura 7, el organigrama correspondiente a la fase del primer acceso a la red,
- La figura 8, un ejemplo de organigrama de notificación y de comunicación que permite la actualización dinámica de los registros de direcciones de las diferentes entidades de una comunidad,
- La figura 9, un ejemplo detallado de una estructura de equipo criptográfico de alto nivel de seguridad según la invención, y

- La figura 10, un ejemplo de realización del procedimiento según la invención que muestra el interés del procedimiento para unas aplicaciones múltiples, particularmente en los casos de redes de topología pequeña.

Con el fin de hacer comprender mejor el procedimiento y el sistema de gestión descentralizado según la invención, el ejemplo que sigue se da en el marco de una red que comprende varias entidades.

Estructura interna de una ES

En este ejemplo, una entidad ES puede corresponder a un equipo criptográfico 1 de acuerdo con el esquema detallado de la figura 9.

Un equipo 1 que forme parte del sistema tiene particularmente por objetivo proteger una red local privada (LAN) de una red compartida de amplio alcance (WAN). El equipo 1 comprende un puerto 2 de entrada/salida estándar conectado a la red local y un puerto 3 dedicado a la fase de inicialización. Estos dos puertos pueden presentarse según la realización de acuerdo con diferentes formas, que tienen en cuenta particularmente el grado de seguridad buscado por un usuario. En el ejemplo desarrollado a título no limitativo para comprender mejor el funcionamiento y las especificidades del procedimiento según la invención, los dos puertos se presentan como unos elementos físicamente separados y cumpliendo cada uno una función. En otros ejemplos, el equipo tendrá un único puerto físico que permita los intercambios de datos y el puerto comprenderá al menos un módulo de software que tenga por función ejecutar la fase de inicialización del procedimiento descrito a continuación en el presente documento y un módulo de software dedicado a la gestión de las entradas/salidas estándar entre el equipo de la ES y la red local.

Un equipo de control 4 permite seleccionar el modo de funcionamiento del multiplexado entre: el modo de inicialización (modo 1 que utiliza el puerto 3) y un modo de comunicación (modo 2 que utiliza el puerto 2).

Los dos puertos 2 y 3 están en conexión con un multiplexor 5 (por ejemplo, un dispositivo “O” exclusiva) que recibe unas órdenes que emanan de un dispositivo de control 4. Este dispositivo de control 4 tiene particularmente por función gestionar el cambio de modo de funcionamiento de los equipos. Por ejemplo, el modo 1 se refiere a la fase de inicialización de la red cuando un nuevo equipo va a unirse con el sistema constituido por varios equipos, el modo 2 se refiere a la fase de acceso a la red, es decir la fase que comienza una vez que el equipo es aceptado por los otros equipos de la red.

El multiplexor 5 tiene una entrada-salida 5p para los datos protegidos que proceden del puerto de la red de entrada/salida 2 (lado LAN), una entrada-salida 5i para los datos que proceden del puerto 3 utilizado para la fase de inicialización (puerto de contacto dedicado a las nuevas entidades, dicho de otra manera el acceso exclusivo a los ahijados), una entrada 5c que recibe las órdenes, una entrada-salida 5s que transmite los datos hacia una plataforma de confianza 6.

Una plataforma de confianza 6 es en el marco de la presente invención un dispositivo que comprende particularmente un medio de generación aleatorio 6a y un módulo de memorización 6b de los elementos secretos. Estos últimos pueden ser unas claves, unos parámetros de configuración de la red, unos parámetros de comunidades o unos parámetros del equipo.

La plataforma de confianza 6 posee una entrada-salida 6s que se conecta a un puerto 7 hacia una red de comunicación extendida conocida bajo la abreviatura anglosajona “WAN” 8 por Wide Area Network. El equipo criptográfico se coloca en la separación entre la red 9 a proteger y la red WAN 8.

Una red operativa con una gestión ARD

La figura 3 esquematiza una red que comprende varios equipos criptográficos ESi que tienen una estructura interna que se parece a la descrita en la figura 9, comunicando entre sí a través de unos enlaces de comunicación Aij.

El procedimiento según la invención ejecuta diferentes etapas detalladas a continuación que comprende particularmente:

- la entrada de un nuevo equipo en una red en el curso del funcionamiento normal,
- la supervisión de las diferentes entidades presentes en el seno de la red, del padrino y del ahijado o del recién llegado,
- el aviso en caso de mal funcionamiento de las entidades,
- la aceptación del recién llegado y lo que se deriva.

Llegada de una nueva ES siguiendo dos etapas:

primera etapa: la inicialización

La figura 4 representa a las etapas realizadas en el curso de la fase de inicialización o primera etapa de un recién llegado que desea conectarse a la red. Esta fase corresponde a una entrada de un nuevo equipo en la red por ejemplo de la figura 3, estando ya esta red operativa. Un nuevo equipo 10 desea conectarse al sistema compuesto por varios equipos 5i que comunican ya entre sí mediante unas arterias de comunicación Aij. Para ello uno de los

equipos 11 va a jugar el papel de padrino. Todos los equipos tienen la capacidad de convertirse en el padrino de un nuevo equipo. Para ello los equipos de ES poseen por ejemplo un programa adaptado para ejecutar los diferentes procedimientos según la invención que comprenden particularmente la primera etapa de inicialización y la segunda etapa del acceso al sistema para el recién llegado.

El equipo 11 que tiene un papel de padrino, interrumpirá su diálogo con los otros equipos de la ESi gracias al multiplexor 5 puesto en evidencia gracias a su estructura interna (compárese con la figura 9). Esta es la fase denominada de inicialización. El equipo 10 que desea conectarse a la red intercambia unas informaciones con el equipo padrino 11. La primera conexión del recién llegado 10 sobre la entrada reservada 5i o puerto de contacto del padrino 11 implica la desconexión de las otras entradas y salidas del equipo padrino (figura 5), a saber los puertos 5p, 6s. Esta desconexión está representada en la figura por las letras Cij. Esta fase se considera como muy sensible y puede corresponder en ciertos casos al intercambio de los primeros secretos entre el padrino 11 y el recién llegado 10. El padrino 11 recibirá unos datos de parte del recién llegado 10 y verificará, por ejemplo, la configuración del recién llegado. Esta configuración comprende, por ejemplo, los elementos siguientes:

- unos parámetros ligados a las capacidades de red del recién llegado tales como, por ejemplo, el número de interfaces de red, las limitaciones eventuales de velocidad, los protocolos de enrutado soportados,
- la lista de las aplicaciones soportadas por el recién llegado,
- unos parámetros ligados a las aplicaciones soportadas por el recién llegado, por ejemplo, los tipos de codificación de voz para una aplicación de telefonía, los puertos TCP o UDP utilizados por la aplicación,
- unos parámetros ligados a las funciones de seguridad del recién llegado:

  ○ la definición de las políticas de seguridad soportadas,
  ○ los algoritmos de cifrado soportados así como el tamaño de las claves, de los contadores anti-repetición y el periodo de cifrado.

Por ejemplo, el padrino verifica si el recién llegado es compatible:

- con unas aplicaciones utilizadas en el sistema,
- con el nivel de seguridad pretendido en el sistema.

El padrino 11 puede controlar de ese modo el histórico de las comunicaciones ya efectuadas por el recién llegado o ahijado 10, por ejemplo: ¿con quién ha comunicado ya el recién llegado?, ¿ha sido ya el padrino de otras entidades?, ¿ha sufrido recientemente unos cambios de configuración? Estos controles se efectúan por medio de un software contenido en las entidades ES. Si el padrino 11 decide dar la confianza al ahijado 10, entonces el padrino 11 transmite al ahijado 10 unas informaciones que le permitirán entrar en comunicación con el resto del sistema. Estas informaciones puede ser unas claves, la definición detallada de las políticas de seguridad en vigor en el sistema, el registro de direcciones, los parámetros de seguridad de la comunidad, o cualquier otro elemento necesario para la autonomía comunicativa del ahijado con la comunidad.

En el caso de los equipos criptográficos antes citados, cada equipo está adaptado para generar un secreto gracias a la plataforma de confianza 6, componente que contiene el generador aleatorio 6a. En este modelo, por ejemplo, un equipo criptográfico es una autoridad de confianza competente para crear y distribuir unas claves. Esta fase es crítica y necesita una fuerte relación de confianza entre 2 equipos. Esta fase comprende la ejecución del algoritmo de cifrado específico y/o una autentificación firme con el fin de utilizar la ES en este modo bien particular: esto puede pasar por unos mecanismos tales como la palabra clave, el obstáculo CIK (Crypto Ignition Key), un algoritmo de intercambio criptográfico reservado para ese intercambio, etc.

Llegada de una nueva ES siguiendo 2 etapas; segunda etapa: el acceso al sistema

Tras esta fase de inicialización, el nuevo equipo 10 se inserta en el sistema, esta es la etapa descrita en las figuras 5 y 6. Esta fase de inserción en la red se desarrolla en tres etapas, dándose el procedimiento a título indicativo porque depende del nivel de seguridad buscado:

1. Opcionalmente, verificación por el ahijado de la validez del padrino en la etapa 1.1: esta etapa permite validar y medir la confianza del padrino en el sistema (flecha I). La ES entrante envía una consulta de voto al conjunto de las ES de cada comunidad del registro de direcciones recibido del padrino (o eventualmente a un subconjunto de las ES listadas en el registro de direcciones recibido del padrino). Esta consulta se envía también al padrino. Si el resultado del sondeo es un voto negativo (flecha II), entonces el recién llegado envía una alarma al conjunto de la comunidad. El proceso se detiene aquí en la etapa 1.2.
2. Si el padrino es validado, el procedimiento ensaya la validez del ahijado: esta etapa 1.3 (opcional) permite validar y medir la confianza del ahijado (flecha III). Todos los equipos que constituyen la red son consultados y notifican al padrino si validan o no la llegada del recién llegado. Según la naturaleza de los mensajes recibidos (por ejemplo, a continuación de un voto negativo de la mayoría de los miembros de la comunidad), el padrino puede decidir invalidar la entrada del nuevo recién llegado, etapa 1.4. Envía entonces una alarma (etapa 1.5) al conjunto de la comunidad o al menos a la parte de la comunidad afectada (flecha IV). Si no hay problema (etapa 1.6), entonces el padrino envía un acuse de recibo a la parte afectada de la comunidad para avisarles de su

decisión. El ahijado es advertido igualmente y puede entonces (si es necesario) hacer llegar a la parte afectada de la comunidad las informaciones que le permitirán a continuación comunicar entre sí, por ejemplo, nuevas claves, nuevos parámetros, etc. (flecha V).
3. Un tratamiento de las alarmas se puede realizar siguiendo dos casos de la figura:

- o bien no se envía la alarma al conjunto de la comunidad porque todos los equipos ES que han sido sondeados han respondido (estado de las ES "activo") o bien son desconectados después del aviso (estado del equipo de ES "inactivo"): compárese con las reglas de notificación.
- o bien la alarma se genera y envía a toda la comunidad porque hay asimismo un problema (una de las ES sondeada se ha desconectado sin aviso ante de la comunidad, o bien el padrino o bien el ahijado no son de confianza).

La ES ahijada 11 es completamente acogida en el sistema. Los miembros afectados de la comunidad la añaden a sus registros de direcciones respectivos.

Ejemplo de un proceso de acceso a la red de una nueva ES (organigrama)

La figura 7 representa el organigrama que desarrolla las etapas antes citadas que constituyen la síntesis de la regla de adopción de un nuevo equipo en una red.

Una vez integrado en su comunidad, es decir el conjunto de los equipos criptográficos que constituyen inicialmente una red, el equipo ahijado se convierte en autónomo.

Las etapas que se desarrollan según el procedimiento son las siguientes:

Etapa 0: fase de inicialización que realiza el intercambio entre el padrino y el ahijado: por ejemplo el intercambio de los primeros elementos secretos y del registro de direcciones,
Etapa 1: llegada del ahijado que corresponde a la conexión a la red. Realiza una prueba opcional sobre la validez del padrino ante al menos una parte de la comunidad, posteriormente comprende la respuesta de los miembros afectados de la comunidad.

Etapa 1.1: ¿es válido el padrino?

No, entonces etapa 1.2: el padrino es excluido y el sistema emite una alarma hacia todos los participantes de la red para eliminar al padrino y al alejado,
Sí, entonces etapa 1.3: prueba opcional sobre la validez del ahijado.
Etapa 1.4: el ahijado no ha sido validado, entonces el sistema transmite una señal de exclusión del ahijado y eventualmente del padrino.
Etapa 1.5: el ahijado es validado, entonces hay una aceptación de ahijado en la comunidad.

Las reglas de comunicación: definición de un comportamiento de ES para con la comunidad

Toda ES debe respetar los parámetros de la comunidad definidos durante la inicialización (el padrino indica así un comportamiento de la red y de la seguridad al ahijado: respeto de las renovaciones de claves, respeto de los periodos criptográficos, respeto de las reglas de notificación, etc.). Debe supervisar igualmente el comportamiento de los otros miembros de la comunidad con los que comunica y enviar unas alarmas a la comunidad en caso de sospecha hacia un miembro de la comunidad. Sin embargo, la denuncia puede ser percibida como un ataque a la red y el denunciante se expone a una condena si la denuncia no ha estado fundada.

Dicho de otra manera, los equipos criptográficos que constituyen el sistema comunican libremente en el seno de la comunidad. Si un equipo criptográfico constata que otro equipo no respeta las reglas de la comunidad entonces advierte a los otros, y puede solicitar la exclusión tomando el riesgo de su propia exclusión.

Reglas de notificación (a continuación de la reglas de comunicación):

La figura 8 representa un ejemplo de las reglas de notificación implementadas por el procedimiento según la invención.

Cuando un equipo se conecta o se desconecta de la red, debe obedecer a las dos reglas siguientes:

- si el equipo acaba de conectarse o de volverse a conectar a la red, entonces el estado del equipo criptográfico es "activo",
- si el equipo deja la red, entonces el estado del equipo es "inactivo".

En cada ocasión, un equipo criptográfico advierte a su comunidad, esto puede ser primordial en efecto para el caso de tratamiento de las alarmas en caso de acceso a la red de un nuevo equipo o de un sondeo.

Esta indicación "activo/inactivo" se introduce en las tablas "registro de direcciones/comunidad de cada equipo".

Comportamiento general de las ES de una comunidad

Los equipos de una comunidad son iguales entre sí, lo que significa que tienen las mismas funcionalidades:

- Elección: pueden y deben responder a los sondeos y a las consultas de recién llegados.
- Justicia: todas las ES pueden denunciar a otra ES o emitir un voto negativo o enviar una alarma en su comunidad, inicializar e introducir a un ahijado (es decir convertirse en padrino).
- Leyes: todas las ES pueden y deben respetar los parámetros de la comunidad (regla de denuncia, periodo criptográfico, contadores anti-repetición no respetados; etc.)

Exclusión de una ES

El proceso de exclusión es el siguiente:

Opcionalmente, la ES que haya detectado la anomalía advierte a todos o a un subconjunto de los miembros de la comunidad. Todas las ES consultadas se advierten entonces mutuamente de sus opiniones respectivas sobre la decisión de exclusión. Según la naturaleza de los mensajes recibidos y según un algoritmo no específico de la invención, las ES pueden entonces tomar la decisión:

- de excluir a la ES que ha sido denunciada
- de no hacer nada
- de excluir a la ES que ha denunciado.

Si se excluye a una ES, el conjunto de la comunidad es advertido entonces de la exclusión. Las ES de la comunidad retiran entonces al miembro excluido de sus registros de direcciones.

El procedimiento y el sistema de gestión descentralizada en un campo de seguridad de las redes presenta particularmente las ventajas siguientes: unas gestiones homogéneas de los diferentes equipos que constituyen el sistema, no específicas y una gestión más simple, un incremento de la seguridad porque todos los equipos que forman la red se supervisan y se controlan entre sí, una posibilidad de red más fácilmente evolutiva que en el caso de una red de gestión centralizada.

El procedimiento presenta un interés para unas aplicaciones múltiples particularmente el caso de redes de topología pequeña. El procedimiento según la invención ofrece particularmente la posibilidad de gestionar unas topologías de redes pequeñas mezclando a la vez unos equipos fijos de infraestructura o unas unidades móviles. Está también muy adaptada a las redes de topologías grandes puesto que permite evitar una gestión centralizada que es la fuente de la vulnerabilidad de los sistemas.

La figura 10 es un ejemplo de realización de la invención para una red ad hoc en la que los equipos pueden variar y ser de pequeño tamaño. Los equipos de cifrado según la invención están integrados, por ejemplo en un primer grupo de infantería 20, un puesto de comando 21 permite generar las maniobras a efectuar. El sistema comprende también unos vehículos de intervención 23 y un segundo grupo de infantería. Cada equipo está equipado con una entidad de seguridad según la invención. Los diferentes equipos se comunican entre sí y pueden realizar las etapas del procedimiento según la invención detalladas anteriormente en el presente documento.

REIVINDICACIONES

1. Procedimiento de gestión de varias entidades de seguridad ESi de software o hardware colocadas en la separación del flujo de información en el seno de una red existente en el que varias entidades de seguridad ESi se comunican entre sí, **caracterizado porque** comprende al menos las etapas siguientes:

- designar una entidad que juega el papel de padrino (11) para una nueva entidad (10) o ahijado que desea unirse a la red,
- dicho ahijado (10) contacta con dicho padrino (11) y tras la recepción de la solicitud de conexión de dicho ahijado (10), dicho padrino (11) determina si acepta o no la conexión,
- si el padrino acepta la conexión de dicho ahijado (10), entonces el padrino (11) se conecta a dicho ahijado y se desconecta de los otros equipos de ES que forman la red,
- al menos una de las entidades y/o el padrino verifican el nivel de seguridad de dicho ahijado,

  - si el padrino (11) o al menos una de las entidades decide dar la confianza a dicho ahijado (10), entonces, el padrino transmite al ahijado (10) unas informaciones de configuración adaptadas para permitirle entrar en comunicación con las otras entidades de la red,
  - si el padrino (11) o al menos una de las entidades decide no dar la confianza al ahijado (10), entonces este último no puede acceder a la red y se genera una alarma hacia las otras entidades de la red

2. Procedimiento según la reivindicación 1, **caracterizado porque** comprende una etapa de acceso del ahijado (10) a la red después de la etapa de inicialización que comprende las etapas siguientes: si el ahijado (10) es aceptado por las entidades con las que ha contactado, los registros de direcciones de las entidades contactadas son puestos al día con los datos del ahijado (10), y el ahijado (10) se comunica entonces libremente con las entidades con las que ha contactado.

3. Procedimiento según una de las reivindicaciones 1 o 2, **caracterizado porque** cada entidad supervisa el comportamiento de las entidades que forman parte de su registro de direcciones utilizando unas reglas de comunicación establecidas.

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado porque** una entidad que detecta una anomalía de funcionamiento o un comportamiento anormal por parte de otra entidad, advierte a todas las entidades de la red de esta anomalía.

5. Procedimiento según la reivindicación 4, **caracterizado porque** todas las entidades prevenidas se advierten entonces mutuamente de sus opiniones respectivas sobre la decisión de exclusión y según la naturaleza de los mensajes recibidos y según un algoritmo, las entidades toman la decisión:

  - de excluir la entidad que ha sido denunciada, siendo excluida dicha entidad denunciada de todos los registros de direcciones,
  - de no hacer nada,
  - de excluir a la entidad que ha denunciado, siendo excluida a continuación esta última entidad de todos los registros de direcciones.

6. Entidad de seguridad de software o hardware colocada en la posición de separación de los flujos de informaciones en el seno de una red que comprende varias entidades ES que se comunican entre sí, **caracterizada porque** comprende al menos los elementos siguientes:

- un medio (2, 3) de conexión de entrada/salida de una entidad a un equipo (9) a proteger, estando adaptado dicho medio (2, 3) para ejecutar las etapas de la fase de inicialización del procedimiento según la reivindicación 1,
- dicho medio (2, 3) está en conexión con un multiplexor (5), que recibe parte de las órdenes que salen de un dispositivo de control (4) que permiten el cambio del modo de funcionamiento del equipo,
- el multiplexor tiene una entrada (5p) para los datos protegidos que proceden del medio de conexión de entrada/salida (2), una entrada (5i), para los datos que proceden del medio de conexión (3) utilizado para la fase de inicialización, una entrada (5c) que recibe las órdenes, una salida (5s) que transmite los datos hacia una plataforma de confianza (6),
- la plataforma de confianza posee una salida (6s) que está conectada a un puerto de salida (8) hacia una red no protegida.

7. Entidad de seguridad de software o hardware según la reivindicación 6, **caracterizada porque** dicho medio de conexión (2, 3) comprende funcionalmente:

- un puerto (2) de entrada/salida estándar conectado a una red o una estación (9) o a un software a proteger,
- un puerto (3) de contacto o de entrada que tiene por función permitir ejecutar la fase de inicialización implementada por el procedimiento según la reivindicación 1.

8. Entidad de seguridad según la reivindicación 7, **caracterizada porque** dicho medio de conexión comprende dos módulos de software, estando adaptado uno de los dos módulos para ejecutar la fase de inicialización implementada por el procedimiento según la reivindicación 1.

9. Entidad de seguridad según la reivindicación 6, **caracterizada porque** la plataforma de confianza (6) comprende un módulo de generación aleatorio (6a) y/o un módulo de memorización (6b).

10. Entidad de seguridad según la reivindicación 6, **caracterizada porque** dicho medio de conexión (2, 3) comprende un módulo de software adaptado para ejecutar la fase de inicialización de un ahijado en una red ejecutando las etapas según la reivindicación 1 y un módulo de software adaptado para gestionar las entradas/salidas entre una entidad y una red.

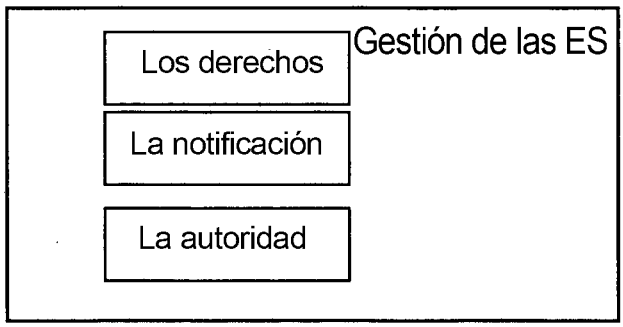

Gestión de las ES
Los derechos
La notificación
La autoridad

FIG.1

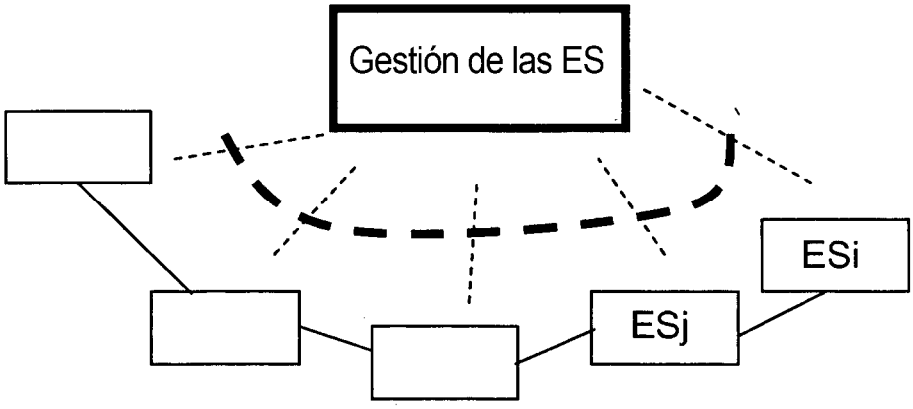

Gestión de las ES
ESi
ESj

FIG.2

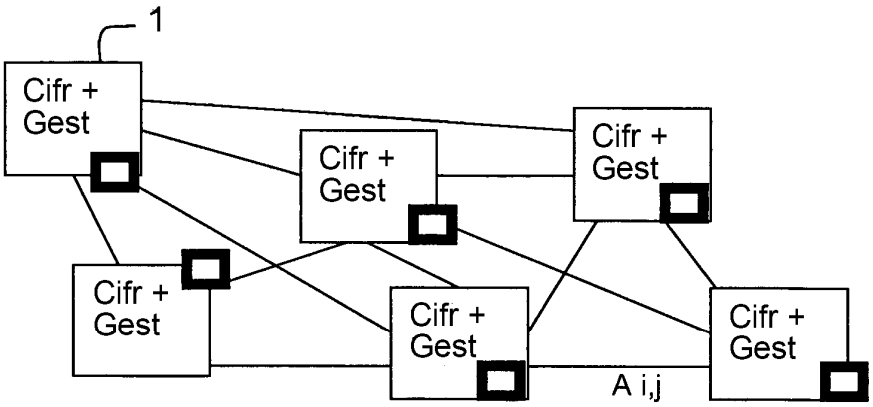


FIG.3

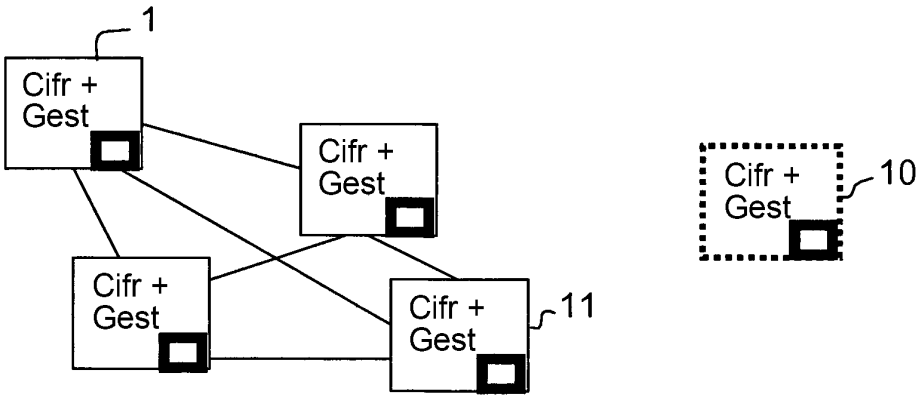


FIG.4

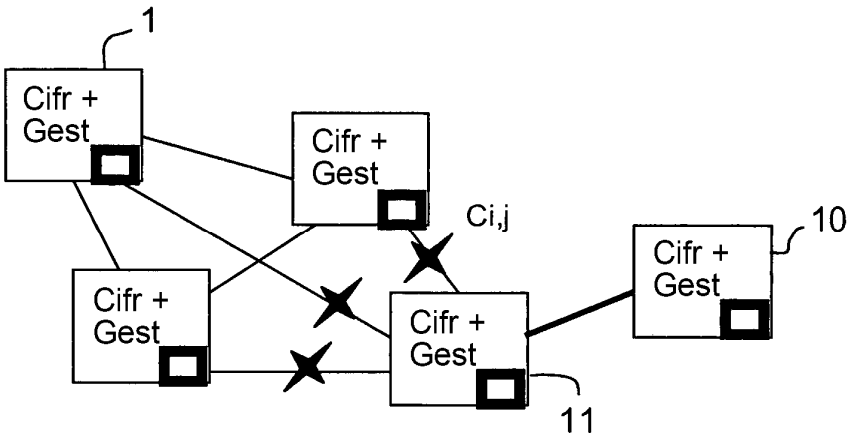


FIG.5

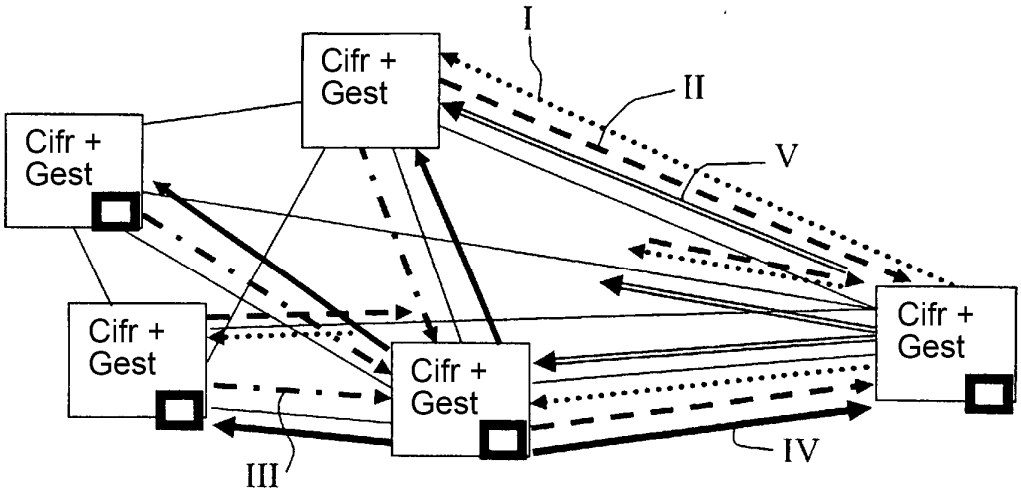

I
II
V
Cifr + Gest
Cifr + Gest
Cifr + Gest
Cifr + Gest
Cifr + Gest
III
IV

FIG.6

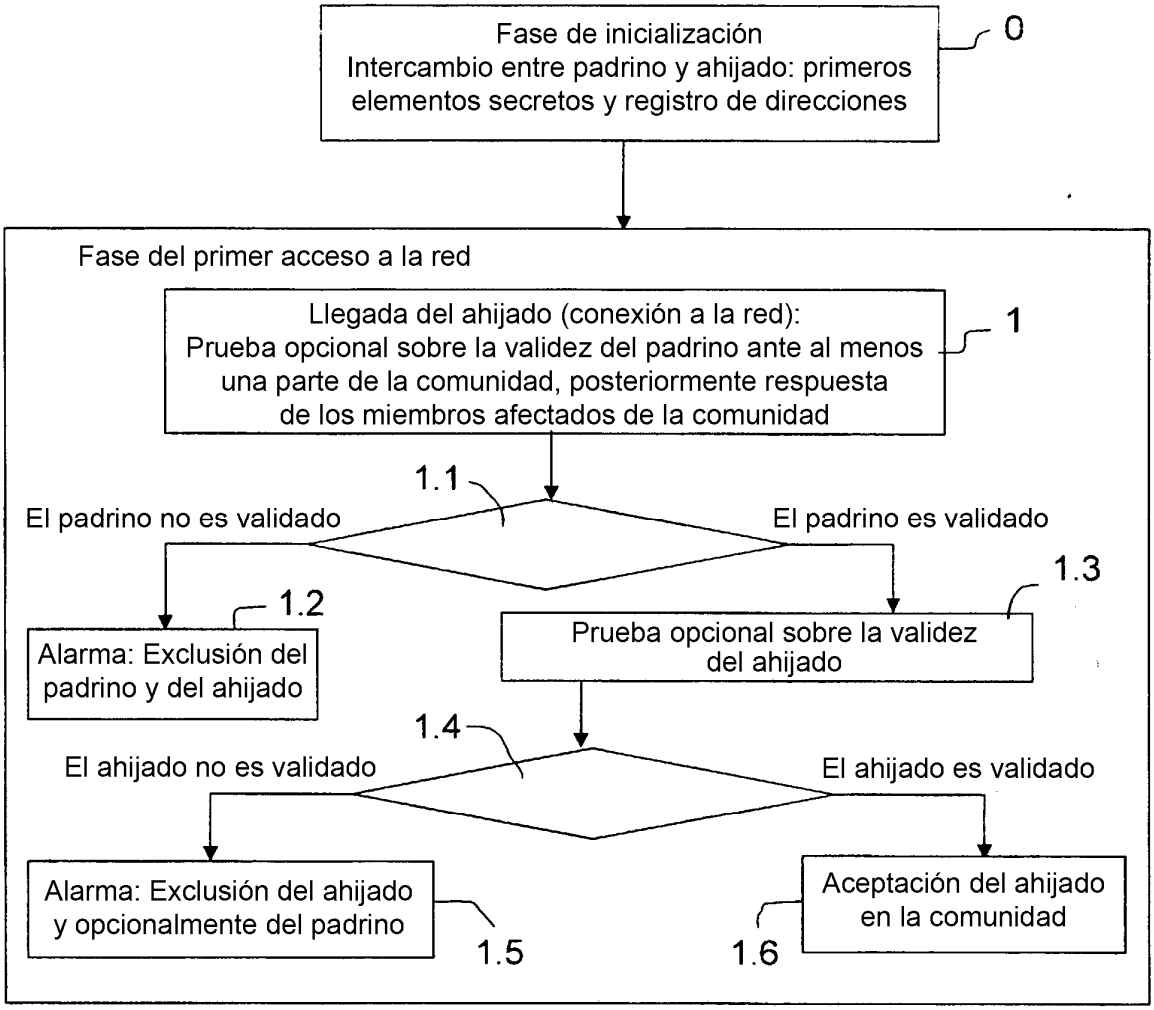

Fase de inicialización
Intercambio entre padrino y ahijado: primeros elementos secretos y registro de direcciones
0
Fase del primer acceso a la red
Llegada del ahijado (conexión a la red):
Prueba opcional sobre la validez del padrino ante al menos una parte de la comunidad, posteriormente respuesta de los miembros afectados de la comunidad
1
1.1
El padrino no es validado
El padrino es validado
1.2
Alarma: Exclusión del padrino y del ahijado
1.3
Prueba opcional sobre la validez del ahijado
1.4
El ahijado no es validado
El ahijado es validado
Alarma: Exclusión del ahijado y opcionalmente del padrino
1.5
1.6
Aceptación del ahijado en la comunidad

FIG.7

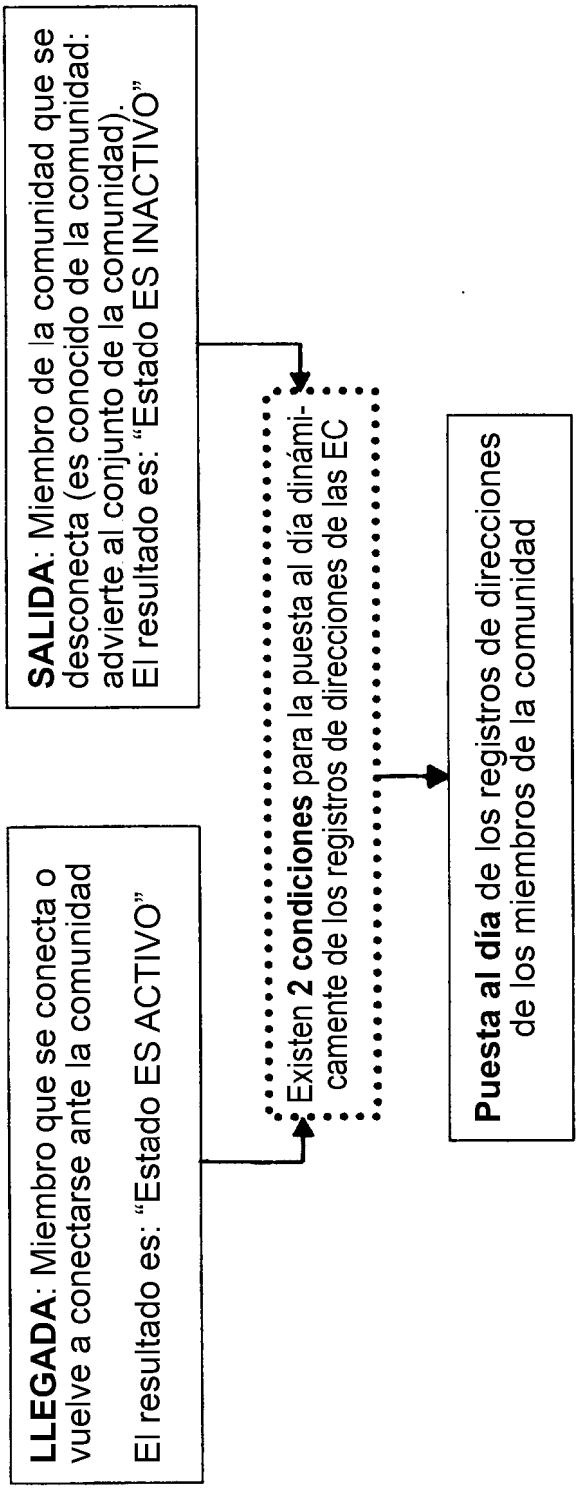

SALIDA: Miembro de la comunidad que se desconecta (es conocido de la comunidad: advierte al conjunto de la comunidad).
El resultado es: "Estado ES INACTIVO"
LLEGADA: Miembro que se conecta o vuelve a conectarse ante la comunidad
El resultado es: "Estado ES ACTIVO"
Existen **2 condiciones** para la puesta al día dinámicamente de los registros de direcciones de las EC
Puesta al día de los registros de direcciones de los miembros de la comunidad

FIG.8

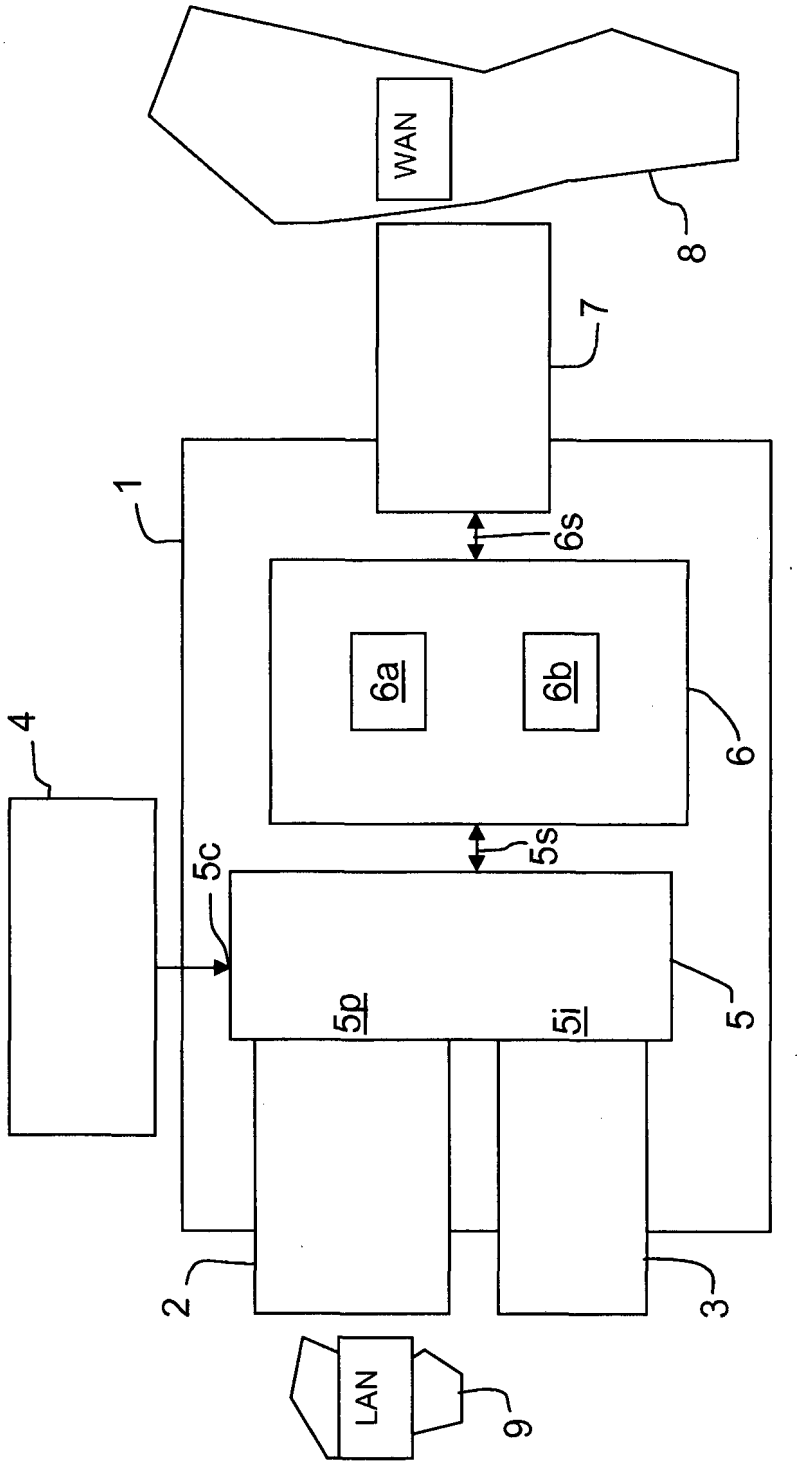


FIG.9

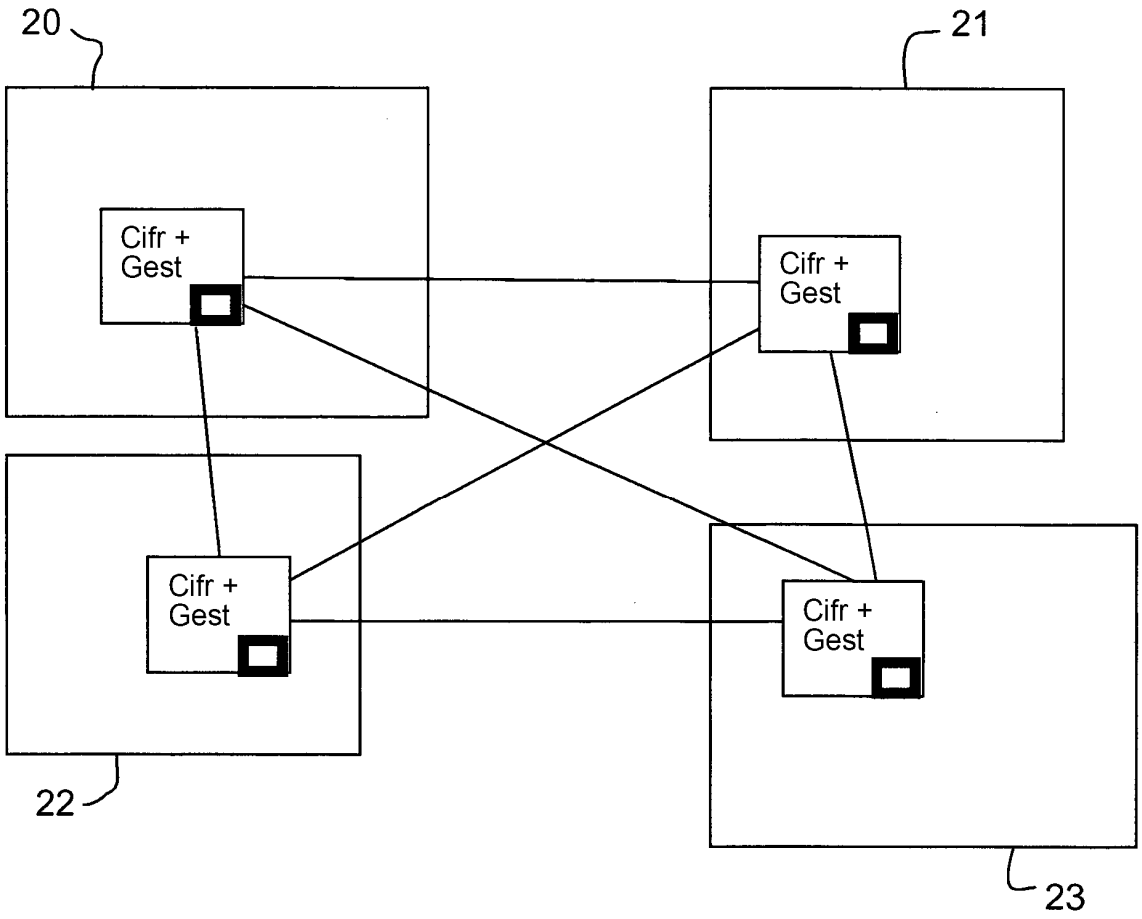


FIG.10