(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 650 982**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.09.2005 PCT/EP2005/054896**

(87) Fecha y número de publicación internacional: **06.04.2006 WO06035054**

(96) Fecha de presentación y número de la solicitud europea: **28.09.2005 E 05797059 (2)**

(97) Fecha y número de publicación de la concesión europea: **13.09.2017 EP 1797695**

(54) Título: **Procedimiento de actualización de una tabla de consulta entre una dirección y un número de identificación**

(30) Prioridad:

30.09.2004 EP 04104784

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.01.2018

(73) Titular/es:

NAGRAVISION SA (100.0%)
22, ROUTE DE GENÈVE
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

STRANSKY, PHILIPPE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Procedimiento de actualización de una tabla de consulta entre una dirección y un número de identificación

Campo de la invención

[0001] La presente invención se refiere a un procedimiento de actualización de una tabla de consulta entre una dirección lógica asociada a una unidad de usuario en una red de comunicación y un número único de identificación asociado a dicha unidad de usuario de un grupo de unidades de usuario.

[0002] La unidad de usuario permite en particular el acceso a un contenido o datos de acceso condicional, en el que estos datos se transmiten por una red como, por ejemplo, Internet.

[0003] En el contexto de la presente invención, se utilizan simultáneamente dos tipos de envío. Así, un contenido como, por ejemplo, acontecimientos de televisión de pago, se envía en modo difusión a varias unidades de usuarios, habitualmente un gran número de unidades. Habitualmente, el contenido se cifra de manera que un usuario que no tiene las claves de descifrado requeridas no puede acceder al contenido cifrado. Estas claves se envían según un segundo tipo de envío, en mensajes dirigidos de manera individual a cada unidad de usuario, pasando por una red de medios de comunicación en el que cada usuario es identificado mediante una dirección lógica.

Estado de la técnica

[0004] De forma convencional, una unidad de usuario incluye medios de tratamiento de datos, que pueden ser un ordenador, un descodificador u otro elemento similar, y un módulo de seguridad a cargo de las operaciones criptográficas asociadas al acceso o al tratamiento de los datos. De manera bien conocida, este módulo de seguridad se puede realizar esencialmente según cuatro formas distintas. Una de ellas es una tarjeta con microprocesador, una tarjeta inteligente, o más habitualmente, un módulo electrónico (con forma de llave, de etiqueta de identificación, ...). Tal módulo es habitualmente desmontable y conectable al descodificador. La forma con contactos eléctricos es la más utilizada, pero no excluye un enlace sin contacto por ejemplo de tipo ISO 14443.

[0005] Una segunda forma conocida es la de un encapsulado de circuito integrado colocado, habitualmente de manera definitiva e inamovible, en el encapsulado del descodificador. Una variante se constituye de un circuito instalado sobre una base o conector como un conector de tarjeta SIM.

[0006] En una tercera forma, el módulo de seguridad se integra en un encapsulado de circuito integrado que tiene igualmente otra función, por ejemplo en un módulo de desaleatorización del descodificador o en el microprocesador del descodificador.

[0007] En una cuarta forma de realización, el módulo de seguridad no se realiza en forma material, sino que su función se efectúa en forma de software únicamente. Dado que en los cuatro casos, aunque el nivel de seguridad difiera, la función es idéntica, se hablará de módulo de seguridad sea cual sea la forma de realizar su función o la forma que pueda tomar dicho módulo.

[0008] La unidad de usuario comprende un número único de identificación que se puede almacenar en los medios de tratamiento de los datos y/o en el módulo de seguridad.

[0009] De forma convencional, varias unidades de usuario forman un grupo que se administra mediante un centro de gestión. En el marco de la presente invención, las unidades de usuario y el centro de gestión pueden comunicarse entre ellos a través de una red de comunicación que puede ser particularmente una red global, como Internet. Según la configuración de la red, un centro de gestión puede tener dificultades para iniciar una comunicación con una unidad de usuario. Es preferible que sea la unidad de usuario quien inicie la comunicación mandando una solicitud al centro de gestión. Dicha solicitud puede pasar por varios dispositivos de encaminamiento antes de alcanzar el centro de gestión. En el momento en que la unidad de usuario empieza la comunicación con el centro de gestión, se mantiene abierto un canal de comunicación entre el centro de gestión y la unidad de usuario, de forma que de las comunicaciones también puedan ser transmitidas desde el centro de gestión hacia la unidad de usuario.

[0010] Se atribuye una dirección dinámica a la unidad de usuario para permitir la comunicación con el centro de gestión. Habitualmente, esta dirección dinámica es diferente en cada sesión de comunicación.

[0011] Cuando un mensaje debe ser reenviado a la unidad multimedia que ha iniciado la comunicación y transmitido la solicitud, el centro de gestión envía su mensaje utilizando el canal o la dirección dinámica que se ha mantenido abierto durante la sesión.

[0012] La patente N° US 5,278,829 describe un procedimiento que permite a un centro de gestión enviar mensajes a una unidad de usuario. Más precisamente, esta patente describe un procedimiento de control de direcciones físicas de un huésped receptor, generalmente un ordenador, dentro de una red. Esta red está compuesta de un huésped emisor y de varios huéspedes receptores. Cada huésped se identifica mediante una dirección física. Estas direcciones físicas se memorizan en el huésped emisor y se asocian a un valor temporal como la fecha de su último uso.

[0013] Cuando el emisor debe enviar un mensaje a un receptor, busca la dirección física de dicho receptor en su memoria. Si la encuentra, determina si la fecha memorizada es más antigua que un valor umbral. En caso negativo, envía el mensaje al receptor. Si la fecha es más antigua que el valor umbral, el emisor envía un primer mensaje al receptor utilizando la dirección física memorizada. A continuación, espera un acuse de recibo por parte del receptor. Si recibe este acuse de recibo, envía el contenido al receptor. Si, al contrario, no recibe el acuse de recibo, difunde un mensaje a todos los receptores solicitando que acusen recibo de dicho mensaje. Si recibe un acuse de recibo, podrá entonces memorizar la nueva dirección física del receptor que ha reenviado el acuse de recibo.

[0014] El procedimiento descrito en esta patente solo funciona en los casos muy particulares en los que un huésped receptor no cambia casi nunca de dirección física. Efectivamente, como se transmite un mensaje a una dirección física memorizada en el huésped emisor, si se modifican las direcciones físicas en cada conexión, las posibilidades de que un mensaje llegue a la unidad de usuario correcta son prácticamente nulas.

[0015] Además, como las direcciones físicas son habitualmente reatribuidas, es posible que el centro de gestión envíe un mensaje a otra unidad de usuario que no es la deseada aunque esta unidad de usuario reenvíe un acuse de recibo al centro de gestión para confirmar la correcta recepción del mensaje.

[0016] Por lo tanto, en los sistemas convencionales en los cuales las direcciones físicas cambian y se reatribuyen en cada conexión, el procedimiento descrito en la patente US 5,278,829 no funciona.

[0017] Este procedimiento presenta el inconveniente de que los mensajes enviados son muy a menudo inútiles y ocupan el ancho de banda que podría ser utilizado de manera más juiciosa. Además, la recepción del mensaje por una unidad de usuario no deseada puede tener consecuencias desde el punto de vista de la seguridad.

[0018] Otra procedimiento consiste en poner en marcha una etapa de reinicialización cuando la unidad de usuario ya no funciona. Este procedimiento tiene como objetivo transmitir el número de identificación único al centro de gestión a través de la red de comunicación, utilizando una dirección específica.

[0019] En tal caso, el abonado debe esperar hasta que la reinicialización termine. Esto puede tomar un tiempo relativamente largo, normalmente varios minutos, durante los cuales no es posible el descifrado de datos.

[0020] Otro problema de los procedimientos del estado de la técnica se conoce bajo el término de "Address spoofing" o usurpación de dirección. Utilizando este procedimiento, una unidad de usuario puede modificar un identificador asociado a la dirección de comunicación de tal forma que el centro de gestión cree comunicarse con una unidad de usuario específica mientras que en realidad transmite información a otra unidad. Un método para contrarrestar tal "Address spoofing" se divulga en la publicación número WO 2004/025926A1.

Objetivos de la invención

[0021] La presente invención se propone paliar los inconvenientes de los procedimientos del estado de la técnica realizando un procedimiento que permite una actualización automática de una tabla de consulta entre direcciones lógicas de la red de comunicación y el número único de identificación de unidades de usuario. Esta actualización se hace de manera óptima por el hecho de que solo se emprende la búsqueda de las direcciones para las direcciones que han cambiado. Por lo tanto, no se ocupa ancho de banda inútilmente. Del mismo modo, tiene como objetivo transmitir un contenido o datos a una unidad de usuario de forma rápida, sin pérdida de tiempo para el usuario. Además, la actualización se lleva a cabo sin que el usuario pierda el acceso al servicio momentáneamente.

[0022] Asimismo, la presente invención tiene como objetivo asegurarse de que el centro de gestión se comunica realmente con la unidad de usuario registrada en la dirección memorizada. Esto tiene dos funciones. Por un lado, sirve para evitar que se envíe un mensaje a una dirección falsa. Por el otro, sirve para evitar que una unidad de usuario se haga pasar fraudulentamente para otra unidad de usuario (address spoofing). Estos objetivos se alcanzan en las reivindicaciones adjuntas.

[0023] Según el procedimiento de la invención, el centro de gestión detecta automáticamente un cambio de dirección de comunicación asociada a una unidad de usuario específica. Esta detección automática es posible gracias al uso de un mensaje de retorno o de un acuse de recibo. De manera más detallada, el acuse de recibo puede hacerse de diferentes formas. Según una primera forma, el centro de gestión envía una solicitud a una

unidad de usuario, utilizando la dirección lógica conocida por el centro de gestión. Si la unidad de ususario devuelve un mensaje al centro de gestión, la dirección lógica será considerada como correcta. Este procedimiento muy sencillo solo funciona si las direcciones lógicas que ya no están en servicio no se reatribuyen a otra unidad de usuario, lo que habitualmente es el caso en la práctica.

[0024] Según otra forma, cuando el centro de gestión reenvía a una unidad de usuario una respuesta a una solicitud proveniente de dicha unidad, la respuesta contiene el número único de identificación de la unidad de usuario a la que se dirige la respuesta. La unidad de usuario comprueba a continuación su propio número único de identificación y reenvía un mensaje de retorno o acuse de recibo al centro de gestión indicando si, efectivamente, su número de identificación corresponde al contenido en la respuesta.

[0025] Según una tercera forma, el centro de gestión solicita a la unidad de usuario que envíe su número único de identificación. Este se compara en el centro de gestión y no en la unidad de usuario como en el caso precedente.

[0026] Según una cuarta forma, se efectúa una verdadera autenticación de la unidad de usuario. Para ello, uno de los procedimientos de autenticación posibles consiste en enviar a la unidad de usuario que se quiere autenticar un mensaje que contiene un número, por ejemplo un número aleatorio generado por el centro de gestión. A continuación, la unidad de ususario recibe este mensaje y se cifra mediante una clave contenida en dicha unidad, en el descodificador o en el módulo de seguridad. Se puede utilizar cualquier otra forma de modificación matemática que se sirva de una variable única por unidad de usuario. Este número aleatorio cifrado se reenvía al centro de gestión. El centro de gestión descifra el mensaje recibido a través de una clave memorizada en el centro de gestión y que corresponde a la unidad de usuario deseada. El valor descifrado se compara con el número aleatorio inicial. Si son iguales, la unidad de usuario se considera auténtica. Si no lo son, se considera fraudulenta y no se le envían los mensajes destinados a dicha unidad. Estos mensajes pueden en particular ser derechos o claves que permiten el acceso al contenido cifrado.

[0027] Por supuesto, las claves utilizadas para la autenticación pueden ser claves simétricas o asimétricas.

[0028] Cabe señalar que esta fase de detección puede llevarse a cabo sin interferir en el acceso a los datos por parte del usuario, es decir, este podrá continuar utilizando el servicio y, por ejemplo, visualizar los datos durante la detección.

[0029] Cuando la dirección lógica de una unidad de usuario ha cambiado, esta envía una solicitud al centro de gestión indicando la nueva dirección lógica así como los datos de identificación asociados a la unidad de usuario. Esta nueva dirección podrá ser memorizada en el centro de gestión tras la autenticación.

[0030] Durante todas estas operaciones, no se impide al usuario utilizar el servicio. Esta actualización se hace, por lo tanto, de manera totalmente transparente para él.

Breve descripción de las figuras

[0031] La presente invención y sus ventajas serán mejor comprendidas en referencia a una forma de realización preferida de la invención y a los dibujos anexos en los cuales:

- La figura 1 representa el conjunto del sistema al que se aplica el procedimiento de la invención; y
- la figura 2 representa las etapas del procedimiento de la invención.

Formas de realizar la invención

[0032] En referencia a las figuras, el procedimiento de la invención se desarrolla en un entorno en el cual un contenido o datos tales como, en particular, datos de acceso condicional se emiten dirigidos a unidades de usuarios STB. Estos datos pueden ser en particular un contenido del ámbito de la televisión de pago o datos asociados a servicios. Las unidades de usuario pueden ser un descodificador o un ordenador por ejemplo, con un módulo de seguridad. Los datos se emiten mediante un proveedor de datos y se difunden desde un centro de difusión con destino a todas las unidades de usuario o a una gran parte de ellas. Los derechos de acceso, por el contrario, se distribuyen en forma punto a punto únicamente a los usuarios autorizados. Estos derechos de acceso son tratados desde un centro de gestión CG. El centro de difusión y el centro de gestión pueden ser dos entidades distintas o, al contrario, una misma entidad. Los datos se transmiten a las unidades de usuario por medio de una línea en una red de comunicación RC como, por ejemplo, la red Internet. A esta línea le corresponde una dirección física de comunicación. De manera más detallada, la dirección física de comunicación se puede formar a partir de una cadena de direcciones físicas y de puertos de comunicación que corresponden a las direcciones físicas de los dispositivos utilizados entre el centro de gestión y una unidad de usuario específica.

[0033] Las unidades de usuario STB administradas por un mismo centro de gestión CG forman parte de un grupo de unidades de usuario. Cada unidad tiene un número único de identificación UA que es habitualmente

memorizado en un módulo de seguridad asociado a un descodificador, en el que el descodificador y el módulo de seguridad forman dicha unidad de usuario. Cabe señalar que este número de identificación UA está en un formato propietario del centro de gestión. Esto significa que no hay notificación alguna en la red de comunicación entre el centro de gestión y los descodificadores.

[0034] Cada unidad de usuario se asocia a una dirección lógica AD de la red de comunicación. Esta dirección lógica es la que utiliza el centro de gestión para transmitir un mensaje a una unidad de usuario específica. Esta dirección lógica está formada por una dirección IP estática, una dirección MAC o una secuencia de carácteres alfanuméricos que pueden, por ejemplo, constituir un nombre. Una dirección lógica podría ser, por ejemplo, "descodificador.nagra.com". La dirección lógica se memoriza habitualmente en el descodificador.

[0035] La asociación entre la dirección física variable y la dirección lógica fija se establece de forma conocida, mediante un servidor conocido bajo el acrónimo de servidor DHCP (Dynamic Host Configuration Protocol). Por otra parte, el servidor DNS mantiene una lista de correspondencia entre la dirección definida por el servidor DHCP y la dirección lógica de la unidad de usuario.

[0036] El centro de gestión contiene una tabla de consulta TC entre la dirección lógica AD de un descodificador en la red de comunicación y el número único de identificación UA del módulo de seguridad correspondiente. Esta tabla de consulta puede contener, además, una clave que se asocia a cada unidad de usuario.

[0037] Por regla general, la dirección física de comunicación entre una unidad de usuario y el centro de gestión cambia con frecuencia, por ejemplo en cada conexión de la unidad de usuario. En cambio, es posible asociar el módulo de seguridad a otro descodificador. Así, un mensaje que llega a una unidad de usuario no es correctamente dirigido porque el módulo de seguridad (la dirección UA) ya no es el mismo y el mensaje no será recibido por el módulo de seguridad deseado.

[0038] En el procedimiento de la invención, cuando un mensaje debe ser enviado a una unidad de usuario específica STB*, el centro de gestión CG busca en la tabla de consulta TC cuál es la dirección lógica de comunicación AD* de la red de comunicación que corresponde al número único de identificación UA* de la unidad de usuario específica STB*. Esto se ilustra en la etapa 20 de la figura 2. En caso de que la dirección lógica no sea una dirección real (IP, MAC), el centro de gestión colaborará con dispositivos de encaminamiento intermedios entre el centro de gestión y la unidad de usuario en cuestión para determinar de manera convencional la dirección física que utilizar para enviar el mensaje a la dirección lógica que corresponde a dicha unidad de usuario, en la etapa 21. Esta etapa puede, por ejemplo, realizarse a través de un servidor de tipo DNS (Domain Name System) que define una jerarquía en los nombres utilizados. Esta jerarquía permite, por una parte, asegurar la unicidad de las direcciones lógicas y, por otra, hallar la dirección física que corresponde a esta dirección lógica. En la etapa 22 siguiente, el centro de gestión comprueba si ha obtenido un mensaje de retorno o acuse de recibo de parte de la unidad de usuario en cuestión, indicando la correcta recepción del mensaje. Si recibe este acuse de recibo, los datos de la tabla se conservan sin cambios en lo que respecta a la unidad de usuario específica. Esto se representa en la etapa 23 de la figura 2. Por el contrario, en caso de que no se reciba un acuse de recibo, la tabla debe ser actualizada. La ausencia de recepción de un acuse de recibo se puede señalar mediante un "mensaje de ausencia de emisión" que indique que el mensaje inicial no ha podido ser emitido o, por el contrario, por la ausencia de recepción de un acuse de recibo después un tiempo determinado.

[0039] Para la actualización de la tabla TC cuando el mensaje no ha podido ser emitido, el centro de gestión emite una solicitud dirigida a un conjunto de unidades de usuario o a la totalidad de las unidades de usuario administradas por dicho centro de gestión. En la forma de realización ilustrada, se envía la solicitud, en la etapa que lleva la referencia 24, a un primer conjunto de unidades de usuario. Esta solicitud contiene al menos un identificador de la unidad de usuario específica deseado así como una petición que solicita a la unidad de usuario que reenvíe un mensaje al centro de gestión. El identificador puede ser en particular el número único de identificación UA*.

[0040] Durante una etapa 25, el centro de gestión comprueba si ha recibido un mensaje de retorno de parte de la unidad de usuario específica STB*. En caso afirmativo, determina la dirección lógica AD* en la red de comunicación que ha sido utilizada para enviar el mensaje de retorno.

[0041] Antes de memorizar la nueva dirección lógica, se genera un procedimiento de autenticación para asegurar que la nueva dirección efectivamente corresponde a la de la unidad de usuario deseada y no a otra unidad de usuario que ha usurpado una dirección. Como se indica anteriormente, un procedimiento de autenticación posible consiste en enviar a la unidad de usuario que se quiere autenticar un número aleatorio generado por el centro de gestión. Este número es a continuación cifrado con una clave contenida en la unidad de usuario. Este número aleatorio cifrado se reenvía al centro de gestión en el cual se descifra a través de una clave memorizada en el centro de gestión y que corresponde a la unidad de usuario deseada. El valor descifrado se compara con el número aleatorio inicial. Si son iguales, la unidad de usuario se considera auténtica.

[0042] En general, se puede utilizar cualquier procedimiento de autenticación de una unidad de usuario. Entre los procedimientos posibles, es posible determinar una firma de una unidad a través de una función de un solo sentido, como una función Hash u otras operaciones matemáticas adecuadas.

[0043] La dirección lógica autenticada se memoriza en la tabla de consulta del centro de gestión, de acuerdo con el número único de identificación UA* de la unidad de usuario específica. Esto corresponde a la etapa 26 de la figura 2. Los mensajes pueden a continuación ser enviados a la unidad de usuario específica STB* utilizando la dirección lógica específica AD*, conforme a la etapa 21 mencionada previamente. Las tablas de direcciones contenidas en los servidores DNS implicados también se actualizan.

[0044] Si, durante la etapa 25 precedente, el centro de gestión determina que no ha recibido un mensaje de retorno, envía una solicitud a otro conjunto de unidades de usuario. Esto corresponde a una etapa que lleva la referencia 27. El centro de gestión verifica a continuación, durante una etapa 28, si ha recibido un mensaje de retorno y actualiza la tabla de consulta, durante la etapa 26 siguiente, si se ha recibido un mensaje. Si no se ha recibido ningún mensaje, el centro de gestión envía un mensaje a todas las unidades de usuario que gestiona. Esto corresponde a una etapa 29. A continuación, verifica durante una etapa 30 si ha recibido un mensaje de retorno y actualiza la tabla de consulta en caso afirmativo.

[0045] Si, por el contrario, no se recibe ningún mensaje en retorno, se pueden plantear varias soluciones, ilustradas por la referencia 31. Una de ellas consiste en reanudar el procedimiento de actualización después de haber esperado un tiempo determinado. Otra consiste en no enviar más mensajes a la unidad de usuario considerada y en memorizar una indicación en la tabla según la cual esta unidad de usuario no está disponible. En tal caso, el abonado que posee dicha unidad de usuario podrá pedir la reactivación, por ejemplo llamando por teléfono al centro de gestión.

[0046] El procedimiento de la invención ha sido descrito según una forma de realización particular en la cual la solicitud se manda en primer lugar a un subconjunto de unidades de usuario, y, a continuación, si la unidad específica no ha sido hallada en este subconjunto, a otro subconjunto de unidades de usuario y, finalmente, a todas las unidades de usuario. Evidentemente, el número de subconjuntos puede ser mayor o menor. También es posible enviar la solicitud a todas las unidades de usuario desde el primer envío.

[0047] Los subconjuntos se pueden formar sobre la base de "subredes" de comunicación, donde cada subred está asociada a un equipo de comunicación particular como, por ejemplo, un encaminador. El conjunto de dichas subredes forma la red de comunicación entre el centro de gestión y el grupo de unidades de usuario.

[0048] También es posible optimizar la búsqueda eligiendo, como miembros del primer subconjunto al que se envía la solicitud, un cierto número de unidades de usuario entre las cuales las posibilidades de hallar la unidad de usuario específica deseada son mayores. Esto se puede determinar, por ejemplo, a partir de la última dirección memorizada por dicha unidad de usuario y utilizando la jerarquía definida en un servidor DNS.

REIVINDICACIONES

1. Procedimiento de actualización de una tabla de consulta (TC) entre una dirección lógica (AD) asociada a una unidad de usuario (STB*) en una red de comunicación y un número único de identificación (UA) asociado a la unidad de usuario mencionada, donde dicha unidad de usuario pertenece a un grupo de unidades de usuario administradas por un centro de gestión (CG), en el cual la unidad de usuario mencionada comprende medios de tratamiento de datos y estos medios de tratamiento de datos están asociados a la dirección lógica mencionada, y donde la unidad de usuario mencionada incluye además un módulo de seguridad asociado al número único de identificación mencionado, donde el procedimiento mencionado comprende una etapa de intercambio de mensajes entre el centro de gestión mencionado y al menos la unidad de usuario específica mencionada (STB*) de dicho grupo mediante la red de comunicación mencionada, donde estos mensajes son encaminados a la (STB*) utilizando la dirección lógica (AD*) de la unidad de usuario mencionada en la red mencionada, **caracterizado** unidad de usuario específica **por** comprender las etapas siguientes:

- búsqueda en la tabla de consulta mencionada (TC) de la dirección lógica (AD*) de la unidad de usuario en la red de comunicación mencionada utilizando el número único de identificación (UA*) que corresponde a la unidad de usuario (STB*);
- envío de mensajes a la unidad de usuario (STB*) con el número único de identificación mencionado (UA*) utilizando la dirección lógica (AD*) correspondiente a la red de comunicación mencionada;
- espera de un mensaje de retorno de la unidad de usuario específica mencionada (STB*) con el número único de identificación en cuestión (UA*);
- en caso de que no se reciba un mensaje de retorno, envío de una solicitud por parte del centro de gestión a todas o parte de las unidades de usuario (STB) que forman parte del grupo mencionado, donde dicha solicitud contiene al menos el número único de identificación mencionado (UA*) de dicha unidad de usuario para la cual la tabla de consulta debe ser actualizada, y una petición que solicita el envío de un mensaje de retorno al centro de gestión;
- detección de un mensaje de retorno de una unidad de usuario (STB*) cuyo número de identificación único (UA*) se corresponde con el identificador mencionado contenido en la solicitud;
- determinación de la dirección lógica (AD*) en la red mencionada, utilizada por la unidad de usuario (STB*) que ha emitido el mensaje de retorno;
- verificación de la dirección lógica (AD) estableciendo una comunicación entre el centro de gestión y la unidad de usuario (STB*) y autenticando la unidad de usuario específica por parte del centro de gestión;
- memorización en la tabla de consulta (TC) del centro de gestión, de la dirección lógica mencionada (AD*) de la unidad de usuario en la red mencionada, en relación con el número de identificación único mencionado (UA*) de la unidad de usuario (STB*) que ha emitido el mensaje de retorno.

2. Procedimiento de actualización de una tabla de consulta según la reivindicación 1, **caracterizado por el hecho de que** la autenticación de una unidad de usuario específica incluye las etapas:

- de envío de un mensaje que contiene un valor generado por el centro de gestión;
- de recepción de dicho mensaje por una unidad de usuario;
- de extracción del valor mencionado y de transformación de este valor a través de una clave contenida en la unidad de usuario mencionada;
- de reenvío de un mensaje que contiene dicho valor transformado al centro de gestión;
- de recepción de dicho mensaje por el centro de gestión;
- de comparación de dicho valor devuelto con el valor esperado por el centro de gestión.

3. Procedimiento de actualización de una tabla de consulta según la reivindicación 1, **caracterizado por el hecho de que** el identificador de la unidad de usuario específica mencionada (STB*) es el número de identificación único mencionado (UA*) de dicha unidad de usuario.

4. Procedimiento de actualización de una tabla de consulta según la reivindicación 3, **caracterizado por el hecho de que** la unidad de usuario incluye un módulo de seguridad y **por el hecho de que** el número de identificación único mencionado (UA*) se memoriza en el módulo de seguridad.

5. Procedimiento de actualización de una tabla de consulta según la reivindicación 1, **caracterizado por el hecho de que** se envía la solicitud a un subconjunto de unidades de usuarios, donde este subconjunto está asociado a una subred de comunicación que forma una parte de la red de comunicación entre el centro de gestión y el grupo de unidades de usuario.

6. Procedimiento de actualización de una tabla de consulta según la reivindicación 5, **caracterizado por el hecho de que** el subconjunto de unidades de usuario se elige en función de criterios de probabilidad de manera que la probabilidad de que la unidad de usuario específica (STB*) buscada pertenezca a este subconjunto sea mayor que la probabilidad de que pertenezca a otro subconjunto que contiene el mismo número de unidades de usuario.

7. Procedimiento de actualización de una tabla de consulta según la reivindicación 1, **caracterizado por el hecho de que** se transmiten datos cifrados a las unidades de usuario en modo difusión y los mensajes se transmiten en modo punto a punto, donde estos mensajes contienen medios para acceder a dichos datos.

8. Procedimiento de actualización de una tabla de consulta según cualquiera de las reivindicaciones precedentes, **caracterizado por el hecho de que** la dirección lógica (AD) se forma a partir de un código alfanumérico.

9. Procedimiento de actualización de una tabla de consulta según cualquiera de las reivindicaciones precedentes, **caracterizado por el hecho de que** la dirección lógica (AD) se memoriza en el descodificador (STB) de la unidad de usuario

10. Procedimiento de actualización de una tabla de consula según cualquiera de las reivindicaciones precedentes, **caracterizado por el hecho de que** el número de identificación (UA) se memoriza en el módulo de seguridad de la unidad de usuario.

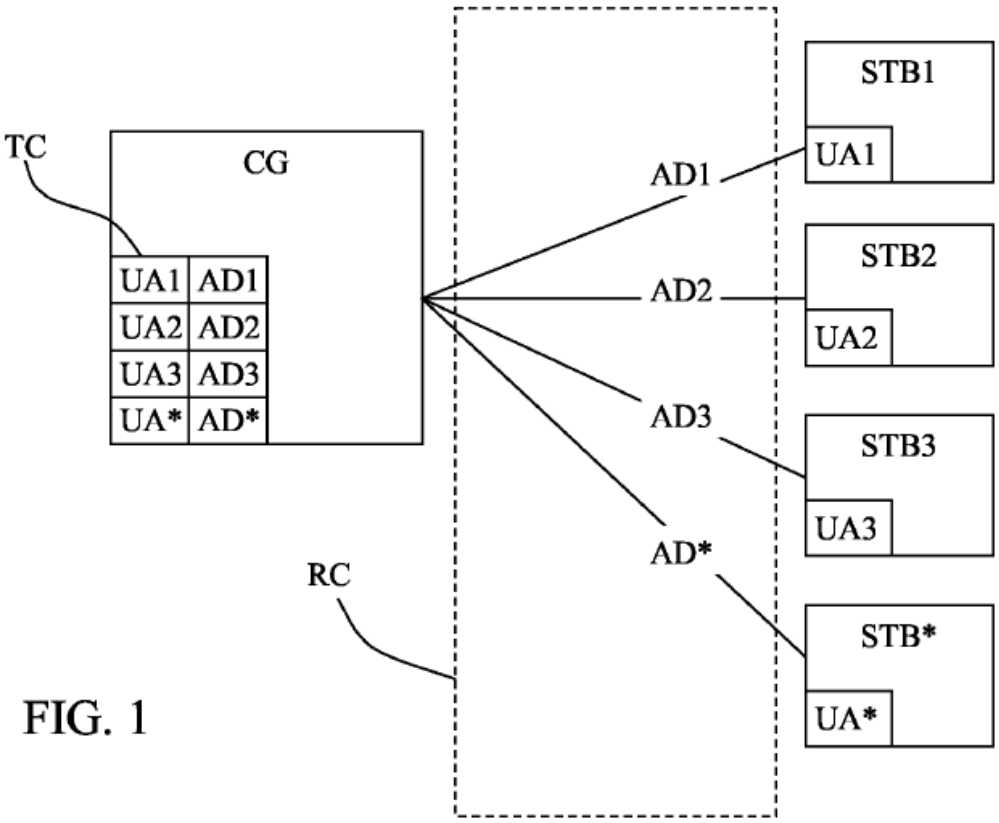
TC
CG
UA1
AD1
UA2
AD2
UA3
AD3
UA*
AD*
RC
AD1
AD2
AD3
AD*
STB1
UA1
STB2
UA2
STB3
UA3
STB*
UA*

FIG. 1

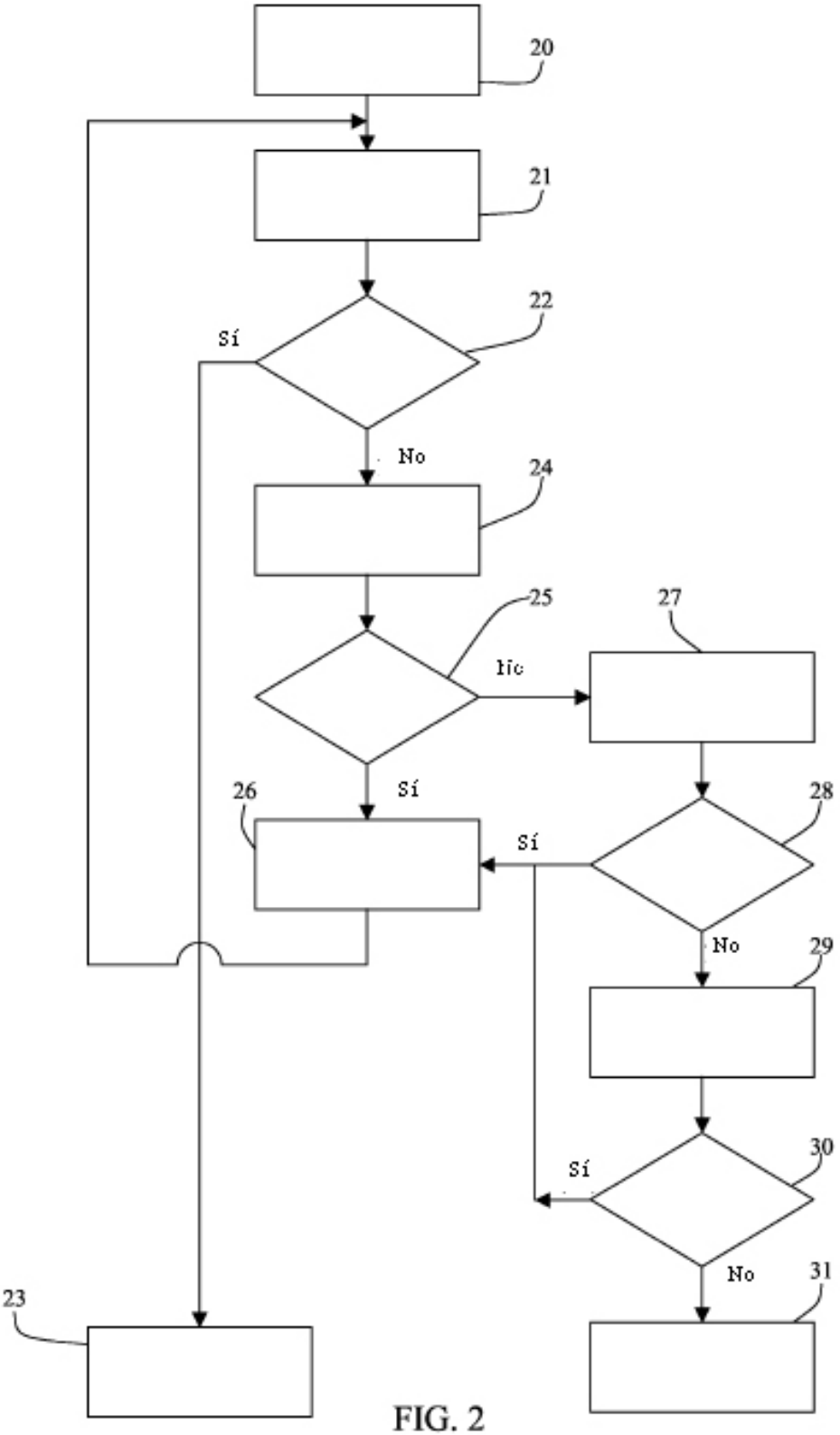

FIG. 2