(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 612 011**

(51) Int. CI.:

H04N 21/266 (2011.01)
H04N 21/4623 (2011.01)
H04N 7/167 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.07.2009 PCT/EP2009/059262**

(87) Fecha y número de publicación internacional: **07.01.2010 WO10000876**

(96) Fecha de presentación y número de la solicitud europea: **17.07.2009 E 09772576 (6)**

(97) Fecha y número de publicación de la concesión europea: **19.10.2016 EP 2304944**

(54) Título: **Procedimiento de protección de datos de seguridad transmitidos por un dispositivo emisor a un dispositivo receptor**

(30) Prioridad:

01.07.2008 FR 0854457

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.05.2017

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche Opéra C
92057 Paris La Defense Cedex, FR

(72) Inventor/es:

CHEVALLIER, ANTHONY y
PHIRMIS, MATHIEU

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

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 protección de datos de seguridad transmitidos por un dispositivo emisor a un dispositivo receptor

Campo técnico

La invención se sitúa en el campo de las telecomunicaciones y se refiere más específicamente a un procedimiento de protección de datos de seguridad transmitidos por un dispositivo emisor a un dispositivo receptor.

La invención se refiere igualmente a un terminal emisor dispuesto en cabecera de red de un operador y configurado para transmitir mensajes útiles a un terminal receptor.

La invención se refiere, además, a un programa informático memorizado en un soporte y destinado a ejecutarse en el terminal emisor para poner en práctica el procedimiento según la invención del lado emisión.

La invención también se refiere a un terminal receptor configurado para recibir los mensajes transmitidos por dicho terminal emisor y a un programa informático memorizado en un soporte y destinado a ejecutarse en un terminal receptor para poner en práctica el procedimiento según la invención.

La invención tiene por objeto de manera más precisa una mejora de la protección de los mensajes EMM enviados por la cabecera de red de un operador al sistema de recepción de un cliente. Sin embargo, se aplica de manera más general a la protección de cualquier transmisión de mensajes entre entidades unidas por unas redes de comunicación independientemente de la naturaleza y de las características de dichas entidades y de dichas redes.

Estado de la técnica anterior

Con el desarrollo creciente de la distribución de contenidos por medio de las redes de comunicación, el riesgo de pirateo de estos contenidos se convierte en una preocupación importante, tanto de los proveedores como de los destinatarios de estos contenidos.

Por consiguiente, es primordial proteger los contenidos distribuidos contra, por una parte, los riesgos de uso indebido de los derechos de acceso asociados a estos contenidos y, por otra parte, contra la falsificación de estos derechos por un usuario.

De hecho, en los sistemas de control de acceso de tipo CAS, los contenidos distribuidos están, por lo general, aleatorizados y su desaleatorización está condicionada por permisos lógicos (un usuario puede acceder al contenido durante una duración determinada) combinados con unas claves, llamadas claves de explotación, permitiendo estas últimas descifrar otros mensajes que permiten acceder a los contenidos. Los permisos lógicos y las claves de explotación se transmiten, por lo general, a los terminales receptores en mensajes de control de acceso específicos EMM (para Entitlement Management Message) y ECM (para Entitlement Control Message) que deben ellos mismos estar protegidos.

Para una mejor comprensión en lo que se refiere a la terminología propia de este campo técnico, podrá consultarse el siguiente documento: “FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM” EBU REVIEW-TECHNICAL EUROPEAN BROADCASTING UNION. BRUSSELS, BE, n.º 266, 21 de diciembre de 1995.

Un inconveniente de la técnica anterior proviene del hecho de que estos mensajes pueden interceptarse y analizarse con el fin de determinar las condiciones de acceso y las claves necesarias para la desaleatorización de los contenidos.

En algunos casos, el operador puede desear suprimir o limitar los derechos de acceso de algunos destinatarios. En este caso, los mensajes EMM y ECM incluyen unas informaciones para ello.

Otra forma de fraude consiste en filtrar estos mensajes transmitidos por el operador para impedir su toma en cuenta por el procesador de seguridad del terminal receptor.

Por otra parte, un pirata que desee recuperar un mensaje EMM puede determinar los efectos de este por la experiencia sometiéndolo, por ejemplo, a un sistema de recepción reservado para sus pruebas.

Además, la explotación del sistema de control de acceso por el operador introduce mensajes EMM de adición, de modificación o de supresión de derechos en unas fechas específicas mensuales, lo que es el resultado del tratamiento informático por lotes (“batch”) y puede contribuir a ayudar al pirata a hacer la distinción entre los mensajes nuevos EMM que resultan de este tratamiento y le permite construir una estrategia de filtrado.

En el caso en el que la autentificación de los mensajes de control de acceso se hace por una redundancia criptográfica, esta medida no tiene efecto en los siguientes casos:

- si el pirata ha conseguido obtener la clave o si ha conseguido obtener una redundancia criptográfica correcta. Esto es particularmente posible si dicha redundancia criptográfica es simétrica. - si el pirata ha conseguido hacer aceptar un mensaje, por el procesador de seguridad, como que incluye una redundancia criptográfica correcta y, por lo tanto, como auténtico. Esto es posible, en concreto, perturbando físicamente el entorno de funcionamiento del procesador de seguridad del sistema de recepción encargado de verificar esta autenticidad. Entre estas perturbaciones figuran, por ejemplo, la elevación brusca de la temperatura, la variación de la señal de alimentación eléctrica o del reloj, la exposición del componente a impulsos láser, emisiones electromagnéticas o radiaciones de partículas radioactivas.

En el caso en el que la protección de los mensajes se realiza por transmisión al terminal receptor de una combinación de órdenes positivas y negativas, la medida solo es interesante cuando el pirata tiene algo que perder. En particular, algunos ataques consisten en añadir de manera ilegal derechos en procesadores de seguridad oficiales (casos denominados MOSC, Modified Official SmartCard). En este caso, el pirata solo experimenta una pérdida filtrando los mensajes si el operador cambia las claves de explotación.

Ahora bien, es preferible no transferir estas claves en un múltiplex, con el fin de no exponerlas inútilmente.

Por lo tanto, resulta que no siempre es posible para un sistema de control de acceso (CAS) contrarrestar los ataques de los piratas y, en particular, contrarrestar la supresión de mensajes no deseados o la inserción de mensajes que no deberían someterse al procesador de seguridad.

La finalidad de la invención es paliar las carencias de los sistemas de control de acceso de la técnica anterior descritos más arriba.

El documento de los Estados Unidos US 2005/039025 A1 describe un método para controlar un acceso remoto de un cliente a una red que tiene al menos un servidor.

Este método incluye una comunicación entre el cliente y el servidor y una verificación por el servidor de una clave de dicho cliente cuando dicho cliente se inicializa, cuando dicho servidor requiere una verificación de dicho cliente, durante un acontecimiento predeterminado cuyo timing es al azar, a la expiración de un período predeterminado, o incluso a la desconexión de dicho cliente del servidor.

El documento europeo EP-A-1 353 511 A2 describe un procedimiento de gestión de derecho de acceso a servicios de televisión para impedir la utilización de una tarjeta fraudulenta.

Exposición de la invención

La invención está basada en la idea de mantener un flujo regular de mensajes entre el emisor y el receptor de modo que se transmitan mensajes aunque el operador no ha formulado la solicitud de ello.

La invención preconiza un procedimiento que consiste en transmitir periódicamente a dicho receptor, alternativamente a dichos datos de seguridad, datos neutros destinados a impedir el filtrado de dichos datos de seguridad.

Esta regularidad permite aleatorizar la comunicación entre el emisor y el receptor para un observador externo, haciendo de esta manera difícil el filtrado fraudulento de los mensajes de seguridad. Además, puede permitir que el receptor detecte un eventual filtrado de estos mensajes.

Según la implementación realizada de la invención y la naturaleza de los mensajes secundarios de la secuencia, puede estar seguida de operaciones de detección o de contramedidas. La detección puede ser de diferentes tipos, como la memorización de un log o el incremento de un contador de detecciones. Las contramedidas pueden, por ejemplo, consistir en una invalidación temporal o en la destrucción de la tarjeta que aloja al procesador de seguridad.

Según otra característica de la invención, la transmisión de dichos datos neutros se desencadena al cabo de un plazo predeterminado desde la última transmisión de datos del emisor hacia el receptor.

Preferentemente, dichos datos neutros presentan una estructura similar a las de los datos de seguridad.

En una variante, el procedimiento según la invención incluye las siguientes etapas:

- definir una duración DR que separa dos recepciones sucesivas por el receptor de datos emitidos por el emisor, y
- en un instante t dado, medir el intervalo de tiempo TR transcurrido desde una recepción por el receptor de datos emitidos por el emisor,
- si el intervalo de tiempo TR es superior a dicha duración DR, transmitir una señal de alarma a una unidad de gestión de contramedidas.

En esta variante, el procedimiento incluye, además, una etapa que consiste en contar el número de señales de alarma N transmitido por el receptor a dicha unidad de gestión de contramedidas, en memorizar el número N en dicha unidad de gestión de contramedidas, en definir un número SA de señales de alarmas que representa un umbral de desencadenamiento de una sanción, en comparar el número SA con el número N memorizado en la unidad de gestión de contramedidas y en ejecutar un procedimiento de contramedidas si el número N supera el número SA.

Dicho procedimiento de contramedidas puede activarse localmente por el receptor o en remoto por el emisor y consiste en una suspensión temporal o definitiva del funcionamiento del receptor.

En una aplicación particular del procedimiento según la invención destinada a reforzar la seguridad de un sistema de control de acceso de tipo CAS, los datos de seguridad y los datos neutros se transmiten al receptor en mensajes EMM.

Dichos datos de seguridad y dichos datos neutros pueden cifrarse con el fin de reforzar la seguridad. Sin embargo, pueden transmitirse en forma no cifrada.

Los datos de seguridad y los datos neutros pueden transmitirse al receptor en un flujo de datos que incluye, además, programas audiovisuales aleatorizados. En este caso, la suspensión temporal o definitiva de funcionamiento consiste en no tratar ya los mensajes EMM durante la lectura de un contenido multimedia.

El procedimiento según la invención se pone en práctica por medio de un terminal emisor dispuesto en cabecera de red de un operador y configurado para transmitir mensajes útiles a un terminal receptor entre una pluralidad de terminales conectados a la red de dicho operador.

Este terminal incluye medios para almacenar una duración máxima D para el plazo entre dos transmisiones sucesivas de mensajes en dicho flujo, medios para medir el plazo T transcurrido desde la última transmisión de un mensaje y medios para insertar en dicho flujo un mensaje neutro si el intervalo de tiempo T transcurrido desde la última transmisión de un mensaje es superior o igual a dicha duración D.

El procedimiento según la invención se implementa, del lado cabecera de red, por medio de un programa informático memorizado en un soporte y destinado a ejecutarse en el terminal emisor para almacenar una duración máxima D para el plazo entre dos transmisiones sucesivas de mensajes en dicho flujo, medir el plazo T transcurrido desde la última transmisión de un mensaje e insertar en dicho flujo un mensaje neutro si el intervalo de tiempo T transcurrido desde la última transmisión de un mensaje es superior o igual a dicha duración D.

El terminal receptor según la invención incluye medios para almacenar una duración máxima DR superior o igual a la duración D para el plazo entre dos recepciones sucesivas de mensajes en dicho flujo, medios para medir el intervalo de tiempo TR transcurrido desde la última recepción de un mensaje y medios para notificar que se ha superado el plazo a la unidad de desencadenamiento de contramedidas si el intervalo de tiempo TR transcurrido desde la última recepción de un mensaje es superior o igual a dicha duración DR.

El procedimiento según la invención se implementa, del lado receptor, por medio de un programa informático memorizado en un soporte y destinado a ejecutarse en un terminal receptor para almacenar una duración máxima DR o igual a la duración D para el plazo entre dos recepciones sucesivas de mensajes en dicho flujo, medir el intervalo de tiempo TR transcurrido desde la última recepción de un mensaje y notificar que se ha superado el plazo a la unidad de desencadenamiento de contramedidas si el intervalo de tiempo TR transcurrido desde la última recepción de un mensaje es superior o igual a dicha duración DR.

Breve descripción de los dibujos

Otras características y ventajas de la invención se desprenderán de la descripción que va a seguir, tomada a título de ejemplo no limitativo, con referencia a las figuras adjuntas en las que:

- la figura 1 representa un organigrama general que ilustra las etapas esenciales del procedimiento según la invención.
- la figura 2 representa esquemáticamente un organigrama que ilustra la detección de filtrado de mensaje por un terminal receptor según la invención.

Exposición detallada de modos de realización particulares

La descripción que va a seguir se refiere a una puesta en práctica del procedimiento según la invención en aplicación particular en la que un terminal emisor, dispuesto en cabecera de red de un operador, transmite un contenido digital a receptores conectados a la red de dicho operador. El contenido digital está previamente aleatorizado por una palabra de control que se transmite a los terminales receptores en mensajes EMM.

El operador puede utilizar diferentes vías para difundir los mensajes EMM y diferentes modos de direccionamiento con el fin de enviar mensajes a diferentes audiencias. De esta manera, un EMM-GA está destinado a todos los usuarios (GA – global audience), un EMM-S está destinado a un grupo de usuarios (S – Shared) y un EMM-U está destinado a un usuario único (U – User). Tradicionalmente se utiliza una vía para la difusión de los mensajes EMM de cada uno de estos modos de direccionamiento.

Es igualmente posible, incluso en el caso de un modo de direccionamiento único, tener diferentes vías EMM. Por ejemplo, en teléfono móvil, algunos mensajes pueden enviarse en el mismo múltiplex que el que contiene el video y otros pueden vehicularse en SMS. Es igualmente probable que varios usuarios deban recibir mensajes. Cada EMM-U enviado a un usuario debe considerarse como que es una vía EMM en el contexto de la invención.

Con el fin de mantener un tráfico regular en cada una de las vías EMM abiertas entre el terminal emisor y cada terminal receptor, el procedimiento según la invención se aplica para cualquier tipo de vía EMM, independientemente del tipo de mensaje transportado por esta vía.

Como en un sistema CAS clásico, el operador hace sus peticiones de envío de mensajes al sistema CAS. En la continuación de esta descripción, asociaremos el epíteto “útil” a estos mensajes.

Si no está asociado ningún mensaje a una vía EMM, esta puede, no obstante, permanecer activa: de esta manera, un mensaje “funcionalmente neutro” se insertará por el sistema CAS en la vía considerada. Un mensaje funcionalmente neutro es un mensaje sintácticamente válido y destinado a analizarse por los terminales destinatarios, pero que no contiene información que proviene del operador y, en particular, sin solicitud de activación de tratamiento en el terminal.

Los flujos de mensajes en salida del sistema CAS son, por lo tanto, flujos de mensajes, compuestos por mensajes útiles o neutros.

La figura 1 ilustra esquemáticamente las etapas esenciales del procedimiento según la invención en el caso en el que los mensajes útiles se transmiten en unas vías EMMs independientes que tienen cada una su propio contexto de “constancia” en el flujo.

La etapa 2 es una fase previa de configuración por el operador de los terminales emisor y receptor. Esta fase consiste en definir una duración máxima de inactividad permitida para un flujo dado y para un usuario dado, en caso de flujo personal. Se fija un valor por defecto de esta duración.

Hay que señalar que el operador puede modificar la duración máxima de inactividad permitida para un flujo dado. Por ejemplo, en caso de duda sobre la integridad de un usuario, el operador puede forzar la necesidad de recepción de un mensaje al día en la vía EMM-U.

El terminal receptor se configura entonces para aceptar un cierto plazo entre varios mensajes, para cada vía que le está destinada.

Durante la explotación, el programa informático implantado en el terminal de emisión en cabecera de red efectúa la prueba de la etapa 4 que consiste en determinar si el operador desea enviar un mensaje útil a los terminales receptores.

En caso afirmativo, se define un mensaje útil en la etapa 6, y en la etapa 8, el mensaje útil se envía al terminal receptor. A continuación, el proceso se reproduce a partir de la etapa 4.

En caso negativo, se ejecuta una prueba para saber si se ha transmitido un mensaje al receptor al cabo de un plazo inferior a la duración D definida en la etapa 2.

En caso afirmativo, el proceso se reproduce a partir de la etapa 4.

En caso negativo, se define un mensaje neutro en la etapa 12, después se transmite (etapa 8) al terminal receptor.

La figura 2 ilustra esquemáticamente las etapas que permiten la detección de un filtrado fraudulento de mensajes útiles transmitidos por el terminal emisor al terminal receptor. Señalemos que el operador puede activar o desactivar la detección, por el terminal receptor, del filtrado eventual de mensajes útiles por envío de un comando específico al receptor designado.

Señalemos que para poner en práctica este procedimiento de detección, el operador define una duración DR que separa dos recepciones sucesivas por el receptor de datos emitidos por el emisor y, en un instante t dado, el software implantado en el terminal receptor mide el intervalo de tiempo TR transcurrido desde una recepción por el receptor de datos emitidos por el emisor y transmite si el intervalo de tiempo TR es superior a dicha duración DR una señal de alarma a una unidad de gestión de contramedidas.

En este ejemplo, la unidad de gestión de contramedidas está dispuesta en el terminal receptor de modo que el terminal no emite ninguna información hacia la cabecera de red.

En la etapa 20, el operador envía al receptor un comando para activar la detección de filtrado fraudulento.

En la etapa 22, el software implantado en el terminal receptor mide el plazo entre dos mensajes sucesivos transmitidos en la vía considerada y compara, en la etapa 24, el plazo medido con la duración DR.

Si el intervalo de tiempo TR es superior a la duración DR, el terminal receptor considera que hay intento de filtrado fraudulento y transmite esta alarma a la unidad de gestión de contramedidas (etapa 26) y la unidad de gestión de contramedidas ejecuta una sanción (etapa 30).

La sanción puede consistir en no tratar ya los mensajes ECM durante la lectura de un contenido multimedia, lo que hace imposible la desaleatorización de este último.

Otra sanción puede consistir en el borrado del conjunto de las claves de explotación y del conjunto de los derechos contenidos en el procesador de seguridad del terminal receptor.

En una primera variante, la unidad de gestión de contramedidas solo ejecuta el procedimiento de sanción después de un número N predefinido de señales de alarma transmitido por el receptor a la unidad de gestión de contramedidas.

En una segunda variante, la unidad de gestión de contramedidas selecciona gradualmente el procedimiento de contramedidas que hay que aplicar según el número de señales de alarmas consignadas. La contramedida puede, por ejemplo, consistir en no tratar ya los ECM al cabo de dos señales de alarma o incluso en borrar los derechos y las claves de explotación del procesador de seguridad al cabo de diez señales de alarma.

Si el intervalo de tiempo TR es inferior a la duración DR, en la etapa 28, el software implantado en el terminal receptor ejecuta los comandos transmitidos en los mensajes útiles.

Señalemos que el tratamiento por el terminal receptor se ejecuta según las siguientes etapas:

- Durante su arranque o su salida de en reposo, el terminal se pone en espera de mensajes EMM,
- A la recepción de un mensaje EMM, ya se trate de un mensaje útil o de un mensaje funcionalmente neutro, este se trata igualmente de manera conocida en la técnica anterior.

En el caso en el que la detección de filtrado fraudulento de mensajes está activada, el tratamiento se modifica de modo que durante la recepción de un mensaje EMM, su fecha (de emisión o de recepción) se memoriza o la fecha máxima esperada de la próxima emisión o recepción de mensajes EMM se calcula como suma de la anterior fecha y de la duración máxima de inactividad, después se memoriza, y a la recepción de un mensaje EMM, si la fecha calculada es superior a la anterior fecha memorizada de emisión o de recepción de mensajes EMM, en más de la duración máxima de inactividad, o si esta fecha es superior a la anterior fecha máxima esperada de la próxima emisión o recepción de mensajes EMM memorizada, entonces el terminal memoriza la detección del filtrado de mensaje(s).

Hay que señalar que los tiempos de tratamiento de un mensaje útil y de un mensaje neutro no permiten diferenciar el tipo de mensaje.

En una tercera variante de la invención, la unidad de gestión de contramedidas está dispuesta en cabecera de red y está controlada por el operador. En este caso, el procedimiento de contramedidas consiste en configurar el terminal emisor para enviar un mensaje EMM de sanción con destino al terminal receptor. Este mensaje EMM de sanción y tratado por el terminal receptor, e indica qué contramedida debe aplicar este último en el caso en el que estén previstos varios niveles de contramedidas.

La invención puede ponerse en práctica de forma selectiva, en concreto, en función de la vía EMM considerada o de forma común al conjunto de estas vías, o en función de la naturaleza de los mensajes útiles que hay que difundir.

REIVINDICACIONES

1. Procedimiento de protección de datos de seguridad transmitidos por un emisor a un receptor que incluye una etapa que consiste en transmitir periódicamente a dicho receptor, alternativamente a dichos datos de seguridad, mensajes funcionalmente neutros, sintácticamente válidos y destinados a analizarse por dicho receptor, pero que no contienen solicitud de activación de tratamiento en dicho receptor, **caracterizado por que** incluye las siguientes etapas:

- definir (20) una duración DR que separa dos recepciones sucesivas por el receptor de datos emitidos por el emisor, y
- en un instante t dado, medir (22) el intervalo de tiempo TR transcurrido desde una recepción por el receptor de datos emitidos por el emisor,
- si el intervalo de tiempo TR es superior a dicha duración DR, transmitir (28) una señal de alarma a una unidad de gestión de contramedidas.

2. Procedimiento según la reivindicación 1, en el que la transmisión de dichos datos neutros se desencadena al cabo de un plazo predeterminado desde la última trasmisión de datos del emisor hacia el receptor.

3. Procedimiento según la reivindicación 1, en el que dichos datos neutros presentan una estructura similar a las de los datos de seguridad.

4. Procedimiento según la reivindicación 1, que incluye una etapa que consiste en contar el número de señales de alarma N transmitido por el receptor a dicha unidad de gestión de contramedidas y en memorizar el número N en dicha unidad de gestión de contramedidas.

5. Procedimiento según la reivindicación 4, que incluye además las siguientes etapas:

- definir un número SA de señales de alarmas que representa un umbral de desencadenamiento de una sanción;
- comparar el número SA con el número N memorizado en la unidad de gestión de contramedidas, y
- ejecutar un procedimiento de contramedidas si el número N supera el número SA.

6. Procedimiento según la reivindicación 5, en el que dicho procedimiento de contramedidas se activa localmente por el receptor.

7. Procedimiento según la reivindicación 5, en el que dicho procedimiento de contramedidas se activa en remoto por un emisor.

8. Procedimiento según una de las reivindicaciones 6 o 7, en el que el procedimiento de contramedidas consiste en una suspensión temporal o definitiva del funcionamiento del receptor.

9. Procedimiento según una cualquiera de las reivindicaciones 1 a 8, en el que los datos de seguridad y los datos neutros se transmiten al receptor en mensajes EMM.

10. Procedimiento según la reivindicación 9, en el que los datos de seguridad y los datos neutros están cifrados.

11. Procedimiento según una cualquiera de las reivindicaciones 1 a 10, en el que los datos de seguridad y los datos neutros se transmiten al receptor en un flujo de datos que incluye, además, programas audiovisuales aleatorizados.

12. Procedimiento según la reivindicación 8, en el que la suspensión temporal o definitiva de funcionamiento consiste en no tratar más los mensajes ECM durante la lectura de un contenido multimedia.

13. Terminal emisor dispuesto en cabecera de red de un operador y configurado para transmitir periódicamente a un receptor en un flujo de datos que incluye, además, programas audiovisuales aleatorizados, alternativamente, datos de seguridad y mensajes funcionalmente neutros, sintácticamente válidos y destinados a analizarse por dicho receptor, pero que no contienen solicitud de activación de tratamiento en dicho receptor, terminal emisor **caracterizado por que** incluye:

a) medios para definir una duración máxima DR para el plazo entre dos transmisiones sucesivas de mensajes en dicho flujo,
b) medios para transmitir la duración máxima DR al terminal receptor,
c) medios para medir el plazo T transcurrido desde la última transmisión de un mensaje al receptor, y
d) medios para insertar en dicho flujo un mensaje funcionalmente neutro si el plazo T transcurrido desde la última transmisión de un mensaje al receptor es superior a la duración DR.

14. Programa informático memorizado en un soporte y destinado a ejecutarse en el terminal emisor según la reivindicación 13 para realizar las etapas:

- definir una duración máxima DR para el plazo entre dos transmisiones sucesivas de mensajes en dicho flujo,
b) transmitir la duración máxima DR al terminal receptor,
c) medir el plazo T transcurrido desde la última transmisión de un mensaje al receptor, y
d) insertar en dicho flujo un mensaje funcionalmente neutro si el plazo T transcurrido desde la última transmisión de un mensaje al receptor es superior a la duración DR.

15. Terminal receptor configurado para recibir periódicamente de un emisor en un flujo de datos que incluye, además, programas audiovisuales aleatorizados, alternativamente, datos de seguridad y mensajes funcionalmente neutros, sintácticamente válidos y destinados a analizarse por dicho receptor, pero que no contienen solicitud de activación de tratamiento en dicho receptor, terminal receptor **caracterizado por que** incluye:

a- medios para almacenar una duración DR que separa dos recepciones sucesivas por el receptor de datos emitidos por el emisor, y
b- medios para medir (22) el intervalo de tiempo TR transcurrido desde una recepción por el receptor de datos emitidos por el emisor,

- medios para notificar que se ha superado el plazo a una unidad de desencadenamiento de contramedidas si el intervalo de tiempo TR es superior o igual a dicha duración DR.

16. Programa informático memorizado en un soporte y destinado a ejecutarse en un terminal receptor según la reivindicación 15 para:

a- almacenar una duración DR que separa dos recepciones sucesivas por el receptor de datos emitidos por el emisor, y
b- medir (22) el intervalo de tiempo TR transcurrido desde una recepción por el receptor de datos emitidos por el emisor,

- notificar que se ha superado el plazo a una unidad de desencadenamiento de contramedidas si el intervalo de tiempo TR es superior o igual a dicha duración DR.

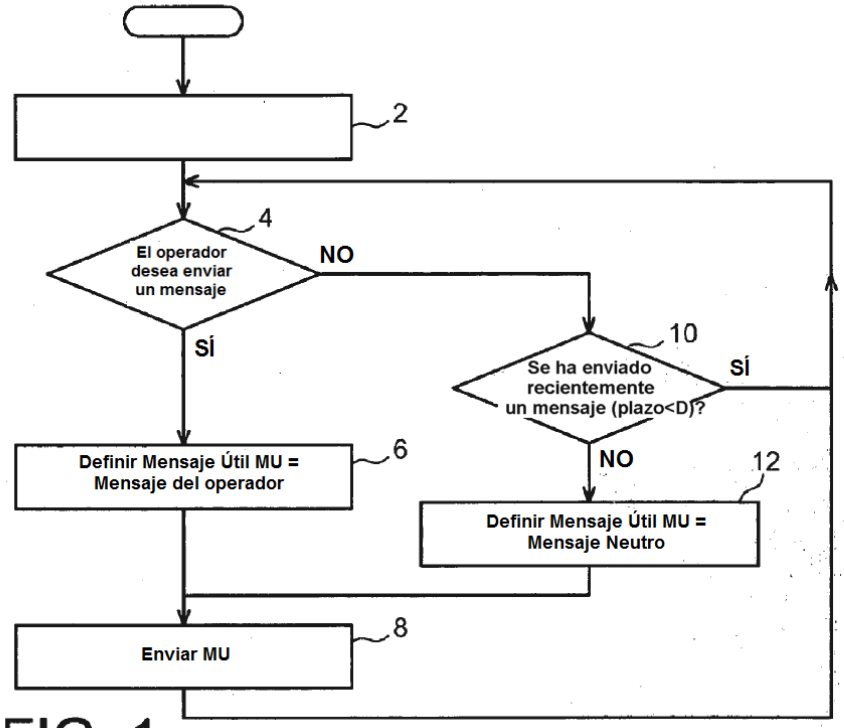
2
4
El operador desea enviar un mensaje
NO
SÍ
10
Se ha enviado recientemente un mensaje (plazo<D)?
SÍ
NO
Definir Mensaje Útil MU = Mensaje del operador
6
12
Definir Mensaje Útil MU = Mensaje Neutro
Enviar MU
8

FIG. 1

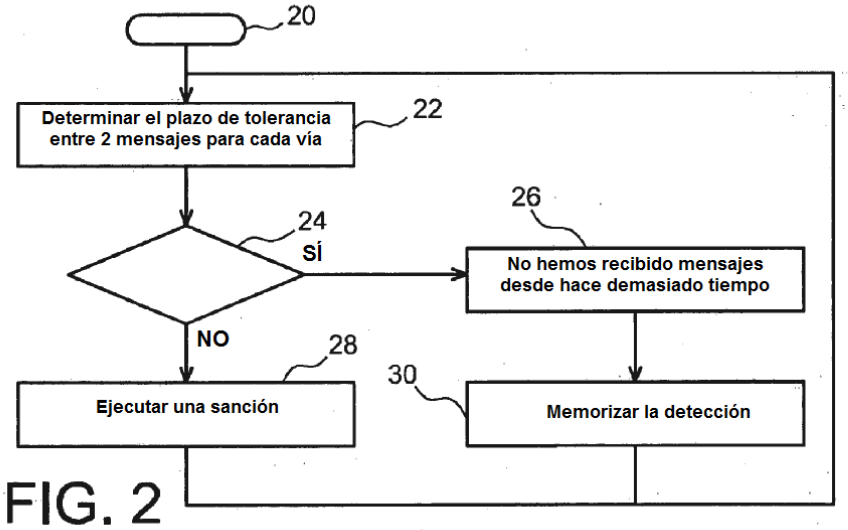
20
Determinar el plazo de tolerancia entre 2 mensajes para cada vía
22
24
SÍ
26
No hemos recibido mensajes desde hace demasiado tiempo
NO
28
30
Ejecutar una sanción
Memorizar la detección

FIG. 2