(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 706 976**

(51) Int. CI.:

H04N 21/266 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/239 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.01.2016 PCT/FR2016/050032**

(87) Fecha y número de publicación internacional: **28.07.2016 WO16116681**

(96) Fecha de presentación y número de la solicitud europea: **08.01.2016 E 16702180 (7)**

(97) Fecha y número de publicación de la concesión europea: **24.10.2018 EP 3248379**

(54) Título: **Procedimiento de difusión de un contenido multimedia protegido**

(30) Prioridad:

20.01.2015 FR 1550453

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.04.2019

(73) Titular/es:

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

(72) Inventor/es:

PHIRMIS, MATHIEU

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento de difusión de un contenido multimedia protegido

La invención se refiere a un procedimiento de difusión de un contenido multimedia protegido por derechos de acceso a terminales mecánicamente independientes los unos de los otros y conectados con un mismo servidor de derechos de acceso por mediación de una red de larga distancia de transmisión de informaciones. La invención tiene igualmente por objeto un soporte de registro de informaciones, así como un servidor de derechos de acceso para la puesta en práctica de este procedimiento.

El procedimiento considerado puede ser puesto en práctica en cualquier sistema de suministro en línea de contenidos multimedia protegidos en el cual una cabecera de red asegura la protección de los contenidos y su transmisión a una pluralidad de terminales.

TERMINOLOGÍA

Antes de continuar la descripción de esta solicitud de patente, se define ahora la terminología utilizada en lo que sigue.

Acceder a un contenido multimedia protegido, significa:

- cargar en memoria fragmentos sucesivos del contenido multimedia, luego
- eliminar la protección, rápidamente, mientras lo recibe, luego
- decodificarlo, luego
- transmitirlo a un aparato multimedia apto para jugarlo, registrarlo, o realizar cualquier otro uso ofrecido por el servicio de suministro de contenidos multimedia protegidos.

Aquí, por «eliminar la protección rápidamente», se designa el hecho de que los fragmentos del contenido multimedia son tratados a medida que se va produciendo su recepción, sin esperar que el contenido de multimedia completo, es decir el conjunto de sus fragmentos, haya sido completamente recibido.

Los contenidos multimedia son típicamente:

- contenidos audiovisuales, por ejemplo, programas de televisión,
- contenidos de audio solamente, por ejemplo, un programa radiofónico, o
- más generalmente, cualquier contenido digital que contenga video y/o audio tal como una aplicación informática, un juego, un diaporama, una imagen o cualquier conjunto de datos.

Entre estos contenidos multimedia, se considera más particularmente en lo que sigue los contenidos multimedia llamados temporales. Un contenido multimedia temporal es un contenido multimedia cuyo juego es una sucesión en el tiempo de sonidos, en el caso de un contenido temporal de audio, o de imágenes, en el caso de un contenido temporal de video, o de sonidos y de imágenes temporalmente sincronizadas entre sí en el caso de un contenido multimedia temporal audiovisual. Un contenido multimedia temporal puede igualmente comprender componentes temporales interactivos temporalmente sincronizados con los sonidos o las imágenes.

El contenido multimedia protegido transmitido se difunde en continuo después de haber sido protegido, por ejemplo, por un sistema de acceso condicional más conocido bajo el acrónimo CAS (Conditional Access System). En lo que sigue, se utiliza la terminología del ámbito de los sistemas de acceso condicional. El lector interesado podrá por ejemplo encontrar una presentación más completa en el documento: «*Functional Model of a Conditional Access System»,* EBU Review, Technical European Broadcasting Union, Bruxels, BE, Nº 266, el 21 de diciembre 1995.

Una conexión punto a punto es una conexión «unicast». Se designa igualmente aquí por el término conexión punto a multipuntos una conexión seleccionada entre el grupo compuesto por una conexión de teledifusión, más conocida bajo los términos de conexión «broadcast», y una conexión multidifusión, más conocida bajo el término de conexión «multicast». La conexión punto a punto es una conexión bidireccional. La conexión punto a multipuntos es una conexión unidireccional del emisor hacia los receptores.

Por «red híbrida», se designa una red en la cual:

- una cabecera de red difunde, con la ayuda de una conexión punto a multipuntos, a un conjunto de terminales, los derechos de acceso necesarios para acceder al contenido multimedia, y, además
- es posible, particularmente a iniciativa de los terminales, establecer una conexión punto por punto entre cada terminal y la cabecera de red.

Los términos de codificado («scrambling» en inglés) y de descodificado («descrambling» en inglés) son utilizados para el contenido multimedia protegido por un CAS, como sinónimos de los términos de cifrado y de descifrado que se utilizan para los otros datos, como particularmente las palabras de control y claves.

Los derechos de acceso son datos que permiten a un terminal acceder al contenido multimedia protegido. Típicamente, los derechos de acceso conllevan por consiguiente al menos una clave de descifrado que permite

descodificar el contenido multimedia protegido o los datos necesarios para el descodificado del contenido multimedia protegido. Pueden además comprender otros derechos adquiridos por el terminal, como consecuencia, por ejemplo, de la suscripción de un abono o de la compra de sesiones por un usuario del terminal, llamados derechos complementarios en lo que sigue. Si el terminal no tiene los derechos de acceso necesarios, el terminal inhibe el acceso al contenido multimedia. Por eso, generalmente, el contenido multimedia no es descodificado o no está descodificado correctamente. Por el contrario, si el terminal tiene los derechos de acceso necesarios, descodifica el contenido multimedia para obtener un contenido multimedia en claro.

Aquí, por «en claro», se designa el hecho de que el contenido multimedia no tiene ya necesidad de ser descifrado para ser jugado, por un aparato multimedia, de forma directamente perceptible e inteligible por un ser humano.

Por «aparato multimedia», se designa además cualquier dispositivo apto para jugar con el contenido multimedia en claro, tal como un televisor o un lector multimedia.

ESTADO DE LA TÉCNICA

El solicitante conoce los procedimientos de difusión de un contenido multimedia protegido a terminales conectados con un mismo servidor de derechos de acceso por mediación de una red de larga distancia de transmisión de informaciones. En estos procedimientos conocidos:

- el terminal envía, al servidor de derechos de acceso, una petición de derechos de acceso para recibir los derechos de acceso que le permitan acceder al contenido multimedia,
- en respuesta a la petición de los derechos de acceso, el servidor de derechos de acceso añade un identificador del terminal a una lista de difusión,
- el servidor de derechos de acceso difunde, a intervalos predeterminados, cada nuevo derecho de acceso al contenido multimedia difundido, solamente a los terminales cuyo identificador figura en la lista de difusión y sin esperar para ello a que estos terminales hayan pedido este nuevo derecho de acceso enviando una nueva petición de derechos de acceso,
- en respuesta a la recepción de cada derecho de acceso, el terminal accede al contenido multimedia difundido y, en ausencia de recepción del derecho de acceso, el terminal inhibe el acceso al contenido multimedia difundido,
- en cualquier momento, el terminal bascula, independientemente, de los otros terminales:
  • de un estado listo en el cual el terminal es capaz de enviar, por mediación de una conexión punto a punto, la petición de derechos de acceso, y de recibir el derecho de acceso requerido,
  • a un estado ocupado en el cual el terminal es incapaz de enviar, por mediación de la conexión punto a punto, la petición de derechos de acceso o de recibir el derecho de acceso.

En el caso del contenido multimedia protegido por un CAS, los derechos de acceso están contenidos en mensajes EMM (Entitlement Management Message). Más precisamente, un mensaje EMM contiene un derecho de acceso DA_i. Este derecho de acceso DA_i contiene típicamente un criptograma $K_s^*(K_i)$ de una clave de explotación K_s cifrada con una clave K_i propia de un terminal T_i. Este derecho de acceso DA_i es específico del terminal T_i ya que solo este terminal T_i tiene la clave K_i y puede por consiguiente descifrar el criptograma $K_s^*(K_i)$ para obtener la clave K_s que le permite acceder al contenido multimedia protegido. En particular, incluso si el derecho de acceso DA_i es recibido por otros terminales, estos otros terminales no pueden explotarlo ya que no tienen la clave K_i. Esto refuerza la seguridad del procedimiento de difusión del contenido multimedia protegido. Por el contrario, el servidor de derechos de acceso debe preparar y enviar tantos derechos de acceso específicos DA_i como terminales diferentes existan que deseen acceder a este contenido multimedia protegido. Dado que el número de terminales puede ser muy grande, por ejemplo, superior a 10 000 o 1 000 000, eso consume una cantidad de ancho de banda en la red de transmisión.

Para remediar este problema, la solicitud WO2009094502A1 propone repartir los terminales en varios grupos y asignar a cada grupo de terminales un intervalo horario específico. A continuación, el servidor de derechos de acceso difunde los derechos de acceso DA_i para un grupo de terminales dado únicamente durante el intervalo horario asociado con este grupo de terminales. Eso permite efectivamente reducir el ancho de banda necesario para enviar los derechos de acceso DA_i a los terminales. Por el contrario, esta solución impone formar y gestionar grupos de terminales, lo cual no siempre es deseable.

Por el estado de la técnica también se conocen:

- EP2317767A1,
- FR2835371A1,
- US2010/131973A1,
- WO2005/091635A2.

La invención trata, por consiguiente, en el contexto de las redes híbridas, de proponer otra solución para reducir el ancho de banda utilizado por la transmisión de los derechos de acceso DA_i a los terminales, pero sin que esta solución imponga formar y gestionar grupos de terminales. La invención tiene por consiguiente por objeto un procedimiento de difusión de un contenido multimedia protegido conforme a la reivindicación 1.

En el procedimiento anteriormente indicado, la transmisión de los derechos de acceso a los terminales que están en su estado ocupado es automáticamente detenida. Eso permite por consiguiente reducir el número de derechos de acceso DA_i transmitidos y por consiguiente limitar el ancho de banda utilizado para esta transmisión. En este procedimiento, la disminución del ancho de banda necesario para transmitir los derechos de acceso se obtiene sin que sea por ello necesario reagrupar los terminales en grupos, como se ha descrito en la solicitud WO2009094502A1.

Los modos de realización de este procedimiento de difusión pueden comprender una o varias de las características de las reivindicaciones dependientes.

Estos modos de realización de este procedimiento de difusión presentan además las ventajas siguientes:

- La utilización de perfiles de ocupación de los terminales para añadir automáticamente un terminal a la lista de difusión antes incluso de que este terminal envíe al servidor de derechos de acceso una petición de derecho de acceso, permite mejorar la calidad de servicio. En efecto, cuando un terminal bascula de su estado ocupado a su estado listo durante un intervalo horario donde es habitual, con una probabilidad superior a un umbral predeterminado, en su estado listo, el terminal recibe directamente los derechos de acceso necesarios para acceder al contenido multimedia protegido incluso sin que tenga necesidad de solicitarlos al servidor de derechos de acceso, y por consiguiente esperar a recibirlos en respuesta a su petición.
- Utilizar los mensajes de estado para actualizar el valor del indicador de probabilidad asociado con cada intervalo horario del perfil de ocupación de un terminal permite actualizar automáticamente este perfil de ocupación y por consiguiente adaptarlo permanentemente a la utilización del terminal.
- Retirar automáticamente el identificador de un terminal de la lista de difusión únicamente después de la ausencia de recepción de varios mensajes de estado esperados consecutivos permite aumentar la robustez del procedimiento de difusión con respecto a la no recepción, accidental de dicho mensaje de estado por el servidor de derechos de acceso. Por ejemplo, la no recepción accidental puede ser causada por una imposibilidad temporal de establecer una conexión punto a punto entre el terminal y la cabecera de red. Eso evita que cada vez que un mensaje de estado no haya sido recibido por el servidor de derechos de acceso, eso conduzca sistemáticamente a la retirada del identificador de un terminal de la lista de difusión.
- Utilizar derechos de acceso específicos con cada terminal permite reforzar la seguridad del procedimiento de difusión ya que incluso si estos derechos de acceso son interceptados o recibidos por otros terminales, no son explotables por estos otros terminales.
- Utilizar el mensaje de acuse de recibo de los derechos de acceso como mensaje de estado permite la ayuda con un mismo mensaje a la vez acusar recibo del derecho de acceso y, al mismo tiempo, indicar al servidor de acceso que el terminal se encuentra en su estado listo. Además, es así posible poner en práctica el procedimiento reivindicado sin tener que modificar los terminales existentes.
- Parar la difusión cíclica del mismo derecho de acceso una vez que el servidor de derecho de acceso ha recibido un acuse de recibo para este derecho de acceso permite reducir todavía más el ancho de banda necesario para la transmisión de los derechos de acceso.
- Retirar automática y sistémicamente de la lista de difusión el identificador de un terminal para el cual la diferencia entre una fecha actual y la última fecha registrada en la cual un mensaje de estado ha sido recibido para este terminal ha franqueado un umbral predeterminado, permite reducir aún el ancho de banda necesario para la transmisión de los derechos de acceso.

La invención tiene igualmente por objeto un soporte de registro de informaciones que comprende instrucciones para la puesta en práctica del procedimiento indicado anteriormente de difusión de un contenido multimedia protegido, cuando estas instrucciones son ejecutadas por un ordenador electrónico.

La invención tiene igualmente por objeto un servidor de derechos de acceso para la puesta en práctica del procedimiento reivindicado.

La invención se comprenderá mejor con la lectura de la descripción que sigue, dada únicamente a título de ejemplo no limitativo, y realizada con referencia a los dibujos en los cuales:

- la figura 1 es una representación esquemática de un sistema de difusión de un contenido multimedia protegido,
- las figuras 2 y 3 son ilustraciones esquemáticas de tablas utilizadas en el sistema de la figura 1; y
- la figura 4 es un organigrama de un procedimiento de difusión de contenidos multimedia con la ayuda del sistema de la figura 1.

En estas figuras, las mismas referencias son utilizadas para designar los mismos elementos. En lo que sigue de esta descripción, las características bien conocidas por el experto en la materia no se describen en detalle.

La figura 1 representa un sistema 2 de difusión de contenidos multimedia protegidos. Los contenidos multimedia difundidos son contenidos multimedia temporales. Por ejemplo, un contenido multimedia corresponde a una secuencia de un programa audiovisual tal como una emisión de televisión o una película.

Los contenidos multimedia en claro son generados por una o varias fuentes 4 y transmitidos a una cabecera de red 6. La cabecera 6 difunde los contenidos multimedia simultáneamente hacia una multitud de terminales de recepción a través de una red 8 de transmisión de informaciones. Típicamente, el número de terminales es superior a 1000 0 10 000. Para simplificar la figura 1, solo tres terminales T_{10}, T_{11} y T_{12} están representados. En lo que sigue de esta descripción, cada terminal del sistema 2 es identificado por una referencia T_i, donde el índice «i» identifica de forma única el terminal T_i del sistema 2 entre el conjunto de terminales de este sistema.

La red 8 es una red de larga distancia de transmisión de informaciones a través de la cual:

- la cabecera de red 6 establece una conexión punto a multipuntos entre la misma y un grupo cualquiera de terminales del sistema 2, y
- una conexión punto a punto entre uno cualquiera de los terminales del sistema 2 y la cabecera de red 6 puede ser establecida.

Por ejemplo, la red 8 es la red Internet igualmente conocida bajo el término de «tela de araña mundial» («Word Wide Web» en inglés).

La cabecera 6 comprende un dispositivo 14 de difusión, a través de la red 8, de los contenidos multimedia protegidos a los terminales. Este dispositivo 14 comprende un codificador 16 que comprime los contenidos multimedia que recibe. El codificador 16 trata contenidos multimedia digitales. Por ejemplo, este codificador funciona conforme a la norma MPEG2 (Moving Picture Expert Group – 2) o la norma UIT-T H264.

Los contenidos multimedia comprimidos son enviados a una entrada 20 de un codificador 22. El codificador 22 protege los contenidos multimedia. Para ello, aquí el codificador 22 codifica cada contenido multimedia comprimido para condicionar su visualización a algunas condiciones de acceso tales como la compra de un título de acceso por los usuarios de los terminales de recepción. Los contenidos multimedia codificados son restituidos en una salida 24 conectada con la entrada de un multiplexor 26.

Más precisamente, el codificador 22 codifica cada contenido multimedia comprimido con la ayuda de una palabra de control CW_t que le es proporcionada, así como a un sistema de acceso condicional, por un generador 32 de claves. El sistema 28 es más conocido bajo el acrónimo CAS (Condicional Access System). El índice «t» es un número de orden que identifica el criptoperiodo CP_t del contenido multimedia codificado con esta palabra de control CW_t. Aquí, todos los criptoperiodos CP_t tienen la misma duración. Un criptoperiodo de contenido designa por consiguiente aquí, en términos generales, una secuencia de contenido cuya duración de juego es por un tiempo predeterminado, estando esta duración predeterminada definida como siendo el criptoperiodo del sistema. Por ejemplo, esta duración está comprendida entre 5s y 1 min y, a menudo, igual a 10s.

Típicamente, este codificado es conforme a una norma tal como la norma DVB-CSA (Digital Video Broadcasting – Common Scrambling Algorithm), ISMA Cryp (Internet Streaming Media Alliance Cryp), SRTP (Secure Real-Time Transport Protocol), AES (Advanced Encryption Standard), etc.

El sistema 28 genera mensajes ECM_t (Entitlement Control Message) que contienen al menos un criptograma CW_t^* de la palabra de control CW_t generada por el generador 32 y utilizada por el codificador 22 para codificar el criptoperiodo CP_t. Este criptograma CW_t^* es obtenido cifrando la palabra de control CW_t con una clave de explotación K_s. Es típicamente construido por el sistema 28. El sistema 28 introduce también, generalmente, en cada ECM_t condiciones de acceso CA destinadas para ser comparadas con derechos de acceso adquiridos por el usuario para permitir o no el acceso al contenido multimedia protegido. Estos mensajes ECM_t y los contenidos multimedia codificados son multiplexados por el multiplexor 26 antes de ser transmitidos a la red 8. La clave de explotación K_s utilizada por el sistema 28 es la misma para todos los terminales. La misma es modificada después de un tiempo de utilización predeterminado superior a al menos dos y, típicamente, al menos diez, cien, mil o diez mil criptoperiodos CP_t sucesivos. Por ejemplo, esta duración es superior a 5 min, 30 min, o 1h y, generalmente, inferior a 36h o 24h.

A título de ilustración, aquí, el codificado y el multiplexado de los contenidos multimedia es conforme al protocolo DVB-CSA (ETSI TS 103 197).

La cabecera 6 comprende igualmente un servidor 40 de derechos de acceso igualmente directamente conectado con la red 8. Aquí, este servidor 40 prepara y difunde los derechos de acceso DA_i requeridos por cada uno de los terminales T_i para acceder al contenido multimedia protegido. Para ello, en este modo de realización, el servidor 40 transmite los derechos de acceso DA_i preparados al sistema 28. El sistema 28 los incorpora entonces en un mensaje EMM (Entitlement Management Message) que es transmitido al multiplexor 26. A este respecto, el servidor 40 comprende un ordenador electrónico 42 programable apto para ejecutar instrucciones registradas en un soporte de registro de informaciones. Aquí, el servidor 40 comprende una memoria 44 que contiene las instrucciones necesarias para la ejecución del procedimiento de la figura 4.

En este modo de realización, la memoria 44 comprende también:

- una tabla 46 que contiene las informaciones necesarias para la gestión de la difusión de los derechos de acceso a cada uno de los terminales, y
- una tabla 48 que contiene perfiles de ocupación para cada terminal T_i.

Además, la tabla 46 contiene una lista 50 de difusión. Esta lista 50 contiene el identificador de cada terminal hacia el cual los derechos de acceso deben ser difundidos.

Para simplificar, se considera que los terminales T_{10} a T_{12} son idénticos y solo el terminal T_{10} se describe más en detalle.

La cabecera 6 de red puede, o no, ocupar un único emplazamiento y, particularmente, el dispositivo 14 y el servidor 40 estar o no distantes. En todos los casos, una conexión punto a punto puede ser establecida entre un terminal y la cabecera 6 generalmente considerada, es decir uno al menos de los emplazamientos de la cabecera 6, cuya conexión punto a punto permite una comunicación bidireccional entre el terminal y el servidor 40.

El terminal T_{10} comprende al menos una línea 60 de descodificado. La línea 60 descodifica el contenido multimedia para visualizarlo en un visualizador 84 o para registrarlo con la ayuda de un registrador.

La línea 60 comprende un receptor 70 de los contenidos multimedia difundidos en la red 8. Este receptor 70 está conectado con la entrada de un desmultiplexor 72 que transmite por un lado el contenido multimedia recibido a un descodificador 74 y por otro lado los mensajes ECM_t y EMM a un procesador 76 de seguridad.

El descodificador 74 descodifica el criptoperiodo CP_t del contenido multimedia codificado a partir de la palabra de control CW_t transmitida por el procesador 76. El contenido multimedia descodificado es transmitido a un decodificador 80 que lo descodifica y lo descomprime. El contenido multimedia descodificado es transmitido a una tarjeta gráfica 82 y/o a una tarjeta de sonido que controla el juego de este contenido multimedia en el aparato 84 equipado con una pantalla 86 o de un altavoz. El aparato 84 juega en claro el contenido multimedia en la pantalla 86.

El procesador 76 trata las informaciones confidenciales tales como las claves criptográficas. Para preservar la confidencialidad de estas informaciones, se ha concebido para ser lo más robusto posible con respecto a las tentativas de ataque llevadas a cabo por piratas informáticos. Por consiguiente, se considera más robusto con respecto a estos ataques que los otros componentes del terminal 10. Por ejemplo, a este respecto, el procesador 76 es una tarjeta con circuito integrado.

El procesador 76 es realizado con la ayuda de un ordenador electrónico 77 programable apto para ejecutar instrucciones registradas en un soporte de registro de informaciones. A este respecto, el procesador 76 comprende una memoria 78 que contiene las instrucciones necesarias para la ejecución del procedimiento de la figura 4.

El terminal T_{10} puede bascular, de forma independiente de los demás terminales, entre un estado listo y un estado ocupado. En el estado listo, el terminal T_{10} es capaz de realizar todas las operaciones necesarias para acceder al contenido multimedia. En particular, en el estado listo, el terminal T_{10} es capaz:

- de recibir el contenido multimedia protegido y los derechos de acceso difundidos por el dispositivo 14 en una conexión punto a multipuntos,
- de establecer una conexión punto a punto a través de la red 8 con el servidor 40 para solicitar la recepción de un derecho de acceso que le permita acceder al contenido multimedia transmitido por el dispositivo 20, y
- de enviar en una conexión punto a punto un acuse de recibo al servidor 40 cada vez que haya recibido correctamente el derecho de acceso transmitido por la cabecera 6.

En el estado ocupado, el terminal T_{10} está desprovisto de al menos una de las capacidades mencionadas más arriba. Por ejemplo, el estado ocupado corresponde a un estado donde el terminal está apagado o en espera o también desconectado de la red 8. Así, en el estado apagado o en espera el terminal consume típicamente diez o cien veces menos energía eléctrica que en el estado listo. Por ejemplo, su consumo eléctrico es inferior a 1W. El terminal T_{10} bascula de su estado listo a su estado ocupado, por ejemplo, automáticamente después de un tiempo predeterminado durante el cual ninguna interacción con el usuario se ha producido. El terminal T_{10} puede también bascular a su estado ocupado en respuesta a la recepción de un comando del usuario, o a iniciativa de la red 8. De igual modo, generalmente, el terminal T_{10} bascula del estado ocupado al estado listo en respuesta a la recepción de un comando de encendido transmitida por el usuario, o a iniciativa de la red 8.

La figura 2 representa más en detalle un ejemplo de realización de la tabla 46. En este ejemplo, la tabla 46 contiene una línea por terminal del sistema 2.

En las figuras 2 y 3, las líneas onduladas indican que solo una parte de las tablas 46 y 48 han sido representadas. En estas figuras 2 y 3, cada columna contiene un campo particular. Estas columnas se identifican en estas figuras por el nombre del campo que contienen.

La tabla 46 asocia con cada terminal T_i cuatro campos llamados respectivamente i, T_i.State, T_i.CM y T_i.DAck. El campo T_i.State caracteriza el estado del terminal T_i, del punto de vista de la cabecera 6. El campo T_i.State puede tomar tres valores distintos:

- «C» para indicar que este terminal T_i es considerado por la cabecera 6 como que se encuentra en su estado listo,

- «D» para indicar que el terminal T_i es considerado por la cabecera 6 como que se encuentra en su estado ocupado, y
- «PC» para indicar que el estado del terminal es considerado como impreciso por la cabecera 6.

El campo « i » contiene el identificador del terminal T_i.

El campo T_i.CM contiene el valor de un contador que se incrementa por paso regular. Aquí, el paso regular es igual a 1. En lo que sigue, este campo T_i.CM es igualmente llamado contador T_i.CM.

El campo T_i.DAck contiene la última fecha en la cual el servidor 40 ha establecido con seguridad que el terminal T_i estaba en su estado listo.

En lo que sigue, la lista 50 es la lista de los identificadores de todos los terminales contenidos en la tabla 46 cuyo campo T_i.State toma un valor comprendido entre el grupo compuesto por el valor «C» y el valor «PC». Esta lista 50 no comprende por consiguiente los identificadores de los terminales T_i para los cuales el valor del campo T_i.State es igual a «D».

A título de ilustración únicamente, la tabla 46 comprende igualmente un campo suplementario $T_i.K_i$ que contiene una clave criptográfica K_i propia del terminal T_i. Así, cada terminal del sistema 2 tiene una clave K_i diferente de la de los otros terminales del mismo sistema. Por ejemplo, la clave K_i es pre-registrada en la memoria 78 de cada terminal. Por el contrario, en este modo de realización, solo el servidor 40 y el terminal T_i conocen esta clave K_i.

La figura 3 representa más en detalle un ejemplo posible de tabla 48. La tabla 48 asocia con cada terminal T_i del sistema 2 un perfil de ocupación. A este respecto, la tabla 48 contiene:

- una línea por terminal T_i del sistema 2,
- una columna « i » que contiene el identificador del terminal T_i, y
- una columna para cada intervalo horario PH_j predefinido que contiene el valor de un campo $T_i.PH_j$.

Aquí, el índice « j » identifica un intervalo horario predefinido entre el conjunto de intervalos horarios predefinidos utilizados en el sistema 2. Los intervalos horarios PH_j dividen un periodo continuo de observación en varios intervalos horarios. Típicamente, el número de intervalos horarios PH_j es estrictamente superior a dos y, de preferencia, superior a cuatro u ocho. Este número es igualmente generalmente inferior a 50 o 100.

Aquí, el periodo de observación es igual a una jornada, es decir a 24 horas y la duración de cada intervalo horario PH_j es igual a una hora. Por consiguientes, existen 24 intervalos PH_j indicados respectivamente por PH_1 a PH_{24}. Las horas de comienzo y de final de cada intervalo horario PH_j son conocidas. Por ejemplo, el intervalo PH_1 comienza a las 0h y acaba a las 1h de la mañana. El intervalo PH_2 comienza a las 1 h de la mañana y acaba a las 2h de la mañana. Así, cada intervalo PH_j comienza a las (j-1) hora(s) y acaba a las j (módulo 24) hora(s).

El valor del campo $T_i.PH_j$ aumenta a medida que aumenta la probabilidad de que el terminal T_i se encuentre en el estado listo durante el intervalo horario PH_j. Para ello, en este modo de realización, el campo $T_i.PH_j$ es incrementado y, alternativamente disminuido por un paso regular como se ha descrito con referencia a la figura 4. Aquí este paso regular es igual a uno.

El funcionamiento del sistema 2 se describirá ahora con la ayuda del procedimiento de la figura 4.

Cuando un terminal T_i cuyo identificador no figura ya en la lista 50 desea recibir sus derechos de acceso DA_i para acceder al contenido multimedia protegido actualmente difundido por el dispositivo 14, procede a una fase 100 de inscripción en la lista 50.

Para ello, en una etapa 102, el terminal T_i establece, a través de la red 8, una conexión punto a punto con el servidor 40.

Luego, en una etapa 104, envía al servidor 40 a través de esta conexión punto a punto, una petición de derecho de acceso.

Unicamente si el usuario ha adquirido los derechos que le permiten acceder a este contenido multimedia, entonces, en una etapa 106, en respuesta, el servidor 40 añade el identificador i de este terminal T_i a la lista 50. Más precisamente, para eso, el servidor 40 asigna, en la tabla 46, el valor «C» al campo T_i.State. En esta etapa 106, el servidor 40 inicializa igualmente el valor del contador T_i.CM a cero y el valor del campo T_i.DAck a la fecha actual. La fecha actual se obtiene por el servidor 40, por ejemplo, a partir de un reloj interno en este servidor 40 o preguntando entonces a un reloj externo a través de la red 8.

Al término de la fase 100, el identificador i del terminal T_i ha sido por consiguiente añadido a la lista 50.

En paralelo, el dispositivo 14 procede de forma permanente a una fase 110 de difusión del contenido multimedia protegido.

Para ello, en una etapa 112, el dispositivo 14 difunde el contenido multimedia codificado multiplexado con los mensajes ECM_t preparados por el sistema 28 y los mensajes EMM que contienen los derechos de acceso DA_i preparados por el servidor 40. Este múltiplex se difunde simultáneamente a todos los terminales del sistema 2 a través de la red 8. Para ello, típicamente, el dispositivo 14 utiliza una conexión «broadcast» entre él y el conjunto de terminales del sistema 2. Así, todos los terminales pueden recibir el contenido multimedia codificado y los mensajes ECM_t y EMM a partir del momento en que se encuentran en su estado listo.

En paralelo, en una etapa 114, cada vez que la clave K_s es modificada, el servidor 40 prepara nuevos derechos de acceso DA_i solamente para todos los terminales cuyo identificador figura en la lista 50. Para ello, por cada terminal cuyo identificador figura en la lista 50, el servidor 40 cifra particularmente la clave K_s con la clave K_i de este terminal T_i obtenida a partir de la tabla 46 para construir el criptograma $K_s^*(K_i)$. Típicamente, el algoritmo de cifrado de la clave K_s utilizado por el servidor 40 es un algoritmo de cifrado simétrico. El derecho de acceso DA_i así preparado es específico del terminal T_i ya que contiene el criptograma $K_s^*(K_i)$, que solo este terminal T_i puede descifrar correctamente. Luego, los derechos de acceso DA_i preparados son transmitidos al sistema 28. El sistema 28 difunde periódicamente estos derechos de acceso DA_i. Por ejemplo, la transmisión del derecho de acceso DA_i se realiza introduciéndolo en un mensaje EMM y difundiendo periódicamente este mensaje EMM. Este derecho de acceso DA_i, incluso si es recibido por otros terminales que el terminal T_i no puede ser explotado por estos otros terminales para acceder en claro al contenido multimedia. En este modo de realización, solo los derechos de acceso DA_i permiten acceder al contenido multimedia protegido.

El periodo de difusión de los derechos de acceso DA_i es típicamente superior a 5 min o 30 min y generalmente inferior a 1 mes o una semana o 24 horas o al doble de la duración de los intervalos horarios. Aquí, la duración de este periodo es seleccionado igual a la duración de los intervalos horarios PH_j, es decir igual a una hora.

Durante una etapa 116, si el terminal T_i se encuentra en su estado listo, recibe el contenido multimedia codificado multiplexado con los mensajes ECM_t y los mensajes EMM. El desmultiplexor 72 transmite entonces el contenido multimedia codificado en el descodificador 74 y los mensajes ECM_t y EMM hacia el procesador 76. En respuesta a la recepción de este mensaje EMM, el procesador 76 explota el derecho de acceso DA_i descifrando el criptograma $K_s^*(K_i)$ con la ayuda de su clave K_i para obtener la clave K_s en claro. Seguidamente, esta clave K_s en claro es por ejemplo registrada en la memoria 78.

Una vez este trabajo concluido, en una etapa 118, el terminal T_i establece una conexión punto a punto con la cabecera 6, luego envía un acuse de recibo al servidor 40 por mediación de esta conexión punto a punto. Seguidamente, la conexión punto a punto se interrumpe. En respuesta, a cada vez que un terminal T_i acusa recibo del derecho de acceso DA_i, el servidor 40 suspende la difusión de este derecho de acceso DA_i, hasta que este derecho de acceso DA_i requerido para acceder al contenido multimedia cambie. Una vez que un nuevo derecho de acceso DA_i se ha preparado para este terminal T_i, es entonces de nuevo automáticamente difundido hacia este terminal sin esperar a que el terminal T_i envíe para ello una nueva petición de derecho de acceso. Eso permite evitar continuar enviando el mismo derecho de acceso DA_i al mismo terminal T_i después de que éste haya ya acusado recepción de este derecho de acceso.

En una etapa 120, el terminal T_i accede al contenido multimedia protegido. Para ello, el procesador 76 utiliza la clave K_s registrada en su memoria 78 para descifrar los criptogramas CW_t^* contenidos en los mensajes ECM_t recibidos para extraer de ellos la palabra de control CW_t en claro. La palabra de control CW_t en claro es transmitida al descodificador 74 que la utiliza para descodificar el criptoperiodo CP_t del contenido multimedia codificado. La secuencia del funcionamiento del terminal T_i para visualizar en claro el criptoperiodo CP_t descodificado y descodificado en la pantalla 86 ha sido ya anteriormente descrita y no será por consiguiente retomada aquí.

Después de la etapa 114, si el terminal T_i se encuentra en su estado ocupado, no recibe el derecho de acceso DA_i enviado por el servidor 40 o es incapaz de enviar el acuse de recibo al servidor 40. En este caso, no puede ejecutar, al menos, la etapa 118. Así, en este caso, el terminal T_i no envía el acuse de recibo al servidor 40.

Paralelamente a las fases 100 y 110, el servidor 40 procede igualmente a una fase 130 de gestión del estado de los terminales, así como a la actualización automática de la lista 50.

Durante una etapa 132, cada vez que el servidor 40 recibe de un terminal T_i un acuse de recepción, utiliza este mensaje como mensaje de estado que le indica que este terminal T_i se encuentra en estado listo. Así, en respuesta a la recepción de este acuse de recibo, el servidor 40 asigna automáticamente el valor « C » al campo T_i.State asociado con este terminal T_i por la tabla 46. Además, procede a las inicializaciones siguientes:

- asigna al campo T_i.DAck la fecha actual,
- asigna el valor « 0 » al contador T_i.CM.

Seguidamente, procede a una etapa 146 de actualización automática del perfil de ocupación del terminal T_i contenido en la tabla 48 y de explotación de este perfil.

La etapa 146 comienza por una operación 148 en la cual el servidor 40 compara el valor del campo T_i.State con el valor « C ».

Si el valor del campo T_i.State es igual a « C », el servidor 40 procede a una operación 150. Durante la operación 150, el servidor 40 incrementa en uno el valor del campo $T_i.PH_j$, donde el intervalo horario PH_j es el intervalo horario actual, es decir el que contiene la hora actual. La hora actual es por ejemplo obtenida a partir del reloj interno del servidor 40 o por interrogación de un reloj externo.

En el caso contrario, es decir si el valor del campo T_i.State es igual al valor « PC » o al valor « D » y solamente si el valor del campo $T_i.PH_j$ es estrictamente superior a cero, entonces, durante una operación 152, el servidor 40 disminuye en uno el valor del campo $T_i.PH_j$. Más generalmente, esta disminución se realiza por un paso igual o no al paso de incremento ya descrito, y que presenta las mismas propiedades que él. Como él, es aquí tomado igual a 1.

El servidor 40 asocia igualmente con cada campo $T_i.PH_j$, un indicador $I_{i,j}$. El valor «verdadero» de este indicador $I_{i,j}$ indica que la probabilidad de que el terminal T_i se encuentre en el estado listo durante el intervalo horario PH_j es importante. En el caso contrario, el valor de este indicador $I_{i,j}$ es igual a «falso».

Después de la actualización del campo $T_i.PH_j$, durante una operación 154, el servidor 40 actualiza los indicadores $I_{i,j}$. Aquí, el valor «verdadero» es asignado al indicador $I_{i,j}$:

- si el valor del campo $T_i.PH_j$ es superior o igual a un umbral S_{PH}, y
- si el valor del campo $T_i.PH_{j-1}$ es superior al umbral S_{PH} o si el valor del campo $T_i.PH_{j+1}$ es superior al umbral $S_{PH.}$

El valor del umbral S_{PH} es predeterminado. Por ejemplo, es superior o igual a dos o cuatro y, generalmente, inferior a 50. Aquí, el valor del umbral S_{PH} es igual a dos.

Dicho de otro modo, se considera que la probabilidad de que el terminal T_i se encuentre en el estado listo es importante:

- si la probabilidad de que el terminal T_i se encuentre en el estado listo durante el intervalo PH_j es importante, y
- si este intervalo PH_j es contiguo al menos a otro intervalo PH_{j-1} o PH_{j+1} durante el cual es también fuertemente probable que el terminal T_i se encuentre en su estado listo.

Seguidamente, durante una operación 156, si el valor del campo T_i.State es igual al « PC» o « D » y si el intervalo horario PH_j actual está asociado con un indicador $I_{i,j}$ cuyo valor es «verdadero», entonces el servidor 40 asigna el valor « PC» al campo T_i.State. En el caso contrario, durante la etapa 156, el valor del campo T_i.State se deja sin cambiar.

Así, cada vez que el servidor 40 reciba un acuse de recibo por parte de un terminal T_i, el valor del campo T_i.State asociado con este terminal T_i es sistemáticamente basculado hacia el valor « C ».

En paralelo, durante una etapa 134, cada vez que el servidor 40 envía en la etapa 114 un derecho de acceso DA_i a un terminal T_i, comprueba si el valor del campo T_i.State es igual al el valor « C ». En caso afirmativo, durante una etapa 136, hace inmediatamente bascular el campo T_i.State del valor « C » al valor « PC » sin esperar el acuse de recibo que le debe transmitir, en respuesta, este terminal T_i en la etapa 118. A continuación, el procedimiento vuelve a la etapa 134. Así, si el terminal T_i se encuentra en su estado listo, el valor del campo T_i.State se repone al valor « C » una vez que el acuse de recibo enviado por este terminal T_i sea recibido por el servidor 40 en la etapa 132. Al contrario, si el terminal T_i no envía ningún acuse de recibo en respuesta al envío de este derecho de acceso DA_i, entonces el valor del campo T_i.State permanece igual a « PC » hasta el próximo envío de un derecho de acceso DA_i para este terminal.

En el caso en que el valor del campo T_i.State sea diferente del valor « C », el servidor 40 procede a una etapa 138 en la cual compara el valor del campo T_i.State con el valor « PC ».

Si el valor del campo T_i.State es igual al valor « PC » entonces el servidor 40 procede a una etapa 140.

En la etapa 140, el servidor 40 compara el valor del contador T_i.CM con un umbral predeterminado M. Típicamente, M es un número entero superior o igual a dos y, generalmente, inferior o igual a 20 o 10. Aquí, M es igual a tres.

Si el valor del contador T_i.CM es superior o igual a M, entonces, en una etapa 142, el servidor 40 asigna el valor « D ». al campo T_i.State en la tabla 46. Eso excluye por consiguiente automáticamente este terminal T_i de la lista 50. Así, a partir de este momento, los derechos de acceso DA_i para este terminal no son ya difundidos por el dispositivo 14 hacia este terminal T_i. Se limita así la cantidad de informaciones transmitidas en la red 8. Eso permite por consiguiente economizar la banda ancha.

Si, en la etapa 140, el servidor 40 determina que el valor del campo T_i.CM es inferior al umbral M, entonces, en una etapa 144, incrementa en uno el valor de este campo Ti.CM y registra el valor incrementado en la tabla 46. Por el contrario, no asigna el valor « D » al campo T_i.State.

Al término de la etapas 142 o 144, el servidor 40 ejecuta una etapa 166 para actualizar el perfil de ocupación del terminal T_i y para explotar este perfil. Esta etapa 166 es idéntica a la etapa 146.

Al término de la ejecución de esta etapa 166, el valor del campo T_i.State es igual a « PC » incluso si el valor « D » le había sido asignado durante la etapa 142 si su perfil de ocupación indica que es fuertemente probable que este terminal T_i bascule hacia su estado listo durante el intervalo horario PH_j actual.

Después de la etapa 166, durante una etapa 168, el servidor 40 calcula la diferencia entre la fecha actual y la fecha contenida en el campo T_i.DAck. Si esta diferencia es superior a un umbral T_{off}, entonces el servidor 40 asigna el valor « D ». al campo T_i.State. En el caso contrario, el valor del campo T_i.State permanece inalterado. El umbral T_{off} es un umbral predeterminado superior o igual a la duración de M intervalos horarios PH_j, donde M es el mismo umbral que el definido anteriormente para el contador T_i.CM. Por ejemplo, el umbral T_{off} es superior a la duración de al menos diez intervalos horarios PH_j. Aquí, el umbral T_{off} es tomado igual a 48 horas.

Después de la etapa 168, el procedimiento retorna a la etapa 134.

Al término de las etapas 140 a 168, el valor del campo T_i.State es igual al valor « PC » incluso si el terminal T_i no ha enviado acuse de recibo al servidor 40 con la condición de que:

- el intervalo horario PH_j actual sea marcado como un intervalo horario donde es muy probable que el terminal T_i bascule hacia su estado listo, y
- la ausencia de envío de acuse de recibo no ha durado más que el valor del umbral T_{off}.

El hecho de mantener en estas condiciones el valor del campo T_i.State igual al valor «PC» permite mantener el terminal T_i en la lista 50 incluso si el servidor 40 no sabe con seguridad si este terminal T_i se encuentra en su estado listo. Por lo tanto, si el terminal T_i bascula de su estado ocupado a su estado listo en la mitad del intervalo horario PH_j asociado con el valor «verdadero» del indicador $I_{i,j}$, no tiene que ejecutar la fase 100 de inscripción. El identificador del terminal T_i se encuentra ya en la lista 50. Se limita por consiguiente así el número de peticiones de derecho de acceso a tratar por el servidor 40 y se mejora la calidad de servicio.

A la inversa, al término de estas etapas 140 a 168, el identificador del terminal T_i es automáticamente retirado de la lista 50:

- si no ha enviado acuse de recibo en respuesta a los M últimos envíos de derecho de acceso DA_i, y
- si el intervalo horario PH_j actual es un intervalo horario donde la probabilidad que el terminal T_i, se encuentre en el estado listo no es importante.

El servidor 40 retira por consiguiente así automáticamente de la lista 50 el identificador de un terminal T_i que no indica que se encuentra en el estado listo durante los intervalos horarios donde la probabilidad de que este terminal bascule hacia su estado listo no es importante. Se observará que el servidor 40 retira igualmente sistemáticamente el identificador de un terminal T_i, de la lista 50 si éste no ha enviado acuse de recibo durante un tiempo superior al valor del umbral T_{off}.

Si durante la etapa 138, el servidor 40 determina que el valor del campo T_i.State es igual al valor « D », entonces procede a una etapa 170. La etapa 170 es una etapa de actualización y de explotación del perfil de ocupación del terminal T_i. Esta etapa 170 es idéntica a la etapa 146.

La etapa 170 es sistemáticamente seguida de una etapa 172 idéntica a la etapa 168.

Así, si el valor del campo T_i.State es igual al valor « D », este se vuelve automáticamente igual al valor « PC » al término de las etapas 170 y 172 únicamente si:

- el intervalo horario PH_j actual es un intervalo horario donde la probabilidad de que el terminal T_i bascule hacia su estado listo es importante, y
- si el terminal T_i ha enviado al menos un acuse de recibo al servidor 40 después del límite «Fecha corriente - T_{off}».

La figura 5 representa un cronograma que ilustra el funcionamiento del servidor 40 y de un terminal T_i cuando el procedimiento de la figura 4 es ejecutado. Este cronograma comprende cuatro ejes horizontales 200, 202, 204 y 206. El eje 200 está graduado en horas. Sobre este eje, cada flecha vertical representa el comienzo de una hora y por consiguiente el comienzo de un intervalo horario PH_j.

El eje 202 representa los periodos de tiempo durante los cuales el terminal T_i se encuentra realmente en el estado listo y, alternativamente, en el estado ocupado. Sobre este eje, cada periodo de tiempo donde el terminal T_i se encuentra en el estado ocupado está representado por una doble flecha horizontal bajo el símbolo « OFF ». De forma similar, cada periodo de tiempo donde el terminal T_i se encuentra en el estado listo, está representado por una doble flecha horizontal bajo el símbolo « ON ».El comienzo y el final de estas dobles flechas corresponden a los instantes en que el terminal T_i bascula entre estos dos estados.

El eje 204 representa los periodos de tiempo durante los cuales el valor del campo T_i.State es igual el valor « C », « PC » o « D ». Como para el eje 202, cada periodo de tiempo está representado por una doble flecha horizontal. Cuando esta doble flecha se encuentra bajo el símbolo « D », se trata de un periodo de tiempo donde el valor del campo T_i.State es igual al valor « D ». Cuando estas dobles flechas se encuentran bajo los símbolos « PC » y « C », se trata de un periodo de tiempo donde los valores del campo T_i.State son iguales, respectivamente, a los valores « PC » y « C ».

El eje 206 representa esquemáticamente bajo la forma de un gráfico de barras la evolución con el transcurso del tiempo del ancho de banda utilizado por el servidor 40 para enviar a los terminales los derechos de acceso DA_i. En este gráfico de barras, cuanto más alta es la barra, más importante es el consumo de ancho de banda.

La evolución del ancho de banda está representada en el caso particular donde:

- solo los intervalos horarios PH_7, PH_8, PH_{19}, PH_{20}, PH_{21} y PH_{22} están asociados con un indicador $I_{i,j}$ cuyo valor es igual a «verdadero»,
- el valor del campo T_i.DAck es inicialmente igual a la fecha corriente correspondiente al comienzo del intervalo PH_1, y
- el valor del contador T_i.CM es inicialmente igual a cero.

Se supone igualmente que los derechos de acceso DA_i son enviados al terminal T_i una sola vez por intervalo horario PH_j. Por ejemplo, al comienzo del intervalo horario PH_j.

A las 7h, el valor del campo T_i.State bascula automáticamente del valor « D » al valor « PC » mientras que el terminal T_i no está aún realmente en el estado listo. Eso se debe al hecho de que se encuentra al comienzo del intervalo horario PH_7. Por lo tanto, cuando hacia las 8h30, el terminal T_i bascula de su estado ocupado a su estado listo, no tiene necesidad de enviar la petición de derecho de acceso al servidor 40 para recibir los derechos de acceso DA_i. Estos derechos de acceso DA_i estaban ya difundidos en su intención desde las 7h de la mañana.

El terminal T_i pasa a su estado ocupado sobre las 10h30 pero eso solo es detectado por primera vez por el servidor 40 a partir de las 11h. A partir de ese momento, el identificador del terminal T_i es mantenido en la lista 50 durante tres intervalos horarios sucesivos PH_{11}, PH_{12} y PH_{13} antes de ser retirado sobre las 14h. Por lo tanto, a partir de las 14h, los derechos de acceso DA_i no son ya ni preparados ni enviados al terminal T_i. Eso permite por consiguiente disminuir el ancho de banda necesario para transmitir estos derechos de acceso DA_i hacia el conjunto de terminales.

Numerosos otros modos de realización son posibles. Por ejemplo, la red utilizada para difundir el contenido multimedia protegido puede ser una red diferente de la red 8. Por ejemplo, puede tratarse de una red de transmisión por satélite o de una red TNT (televisión digital terrestre). La difusión del contenido multimedia y de los derechos de acceso DA_i puede ser realizada en multicast más bien que en broadcast.

En otra variante, el contenido multimedia es difundido por una primera red y los derechos de acceso DA_i son difundidos por una segunda red distinta. En este caso, no es necesario que las dos redes permitan el establecimiento de conexión punto a punto.

El procedimiento de la figura 4 ha sido descrito en el caso particular donde los contenidos multimedia están protegidos por un sistema 28 de acceso condicional conocido bajo el acrónimo de CAS. No obstante, lo que ha sido anteriormente descrito en este caso particular se aplica igualmente para la difusión de contenidos multimedia protegidos por otros medios que el sistema 28. Por ejemplo, el sistema 28 es sustituido por un sistema de gestión de derechos digitales conocido bajo el acrónimo de DRM (digital rights management). Un sistema de DRM es en efecto un sistema de protección de contenidos multimedia. El lector interesado podrá, por ejemplo, encontrar una presentación más completa en el documento: DRM Architecture, Draft versión 2.0, OMA-DRM-ARCH-V2_0-20040518-D, Open Mobile Alliance, 18 mayo 2004. En este sistema de DRM, el cifrado del contenido multimedia se realiza generalmente por medio de una clave de cifrado, por un algoritmo simétrico. El derecho de acceso que permite acceder al contenido multimedia así cifrado es típicamente transmitido en un mensaje llamado una «licencia». De estructura bien conocida, dicha licencia comprende al menos una clave, llamada de contenido, necesaria para el descifrado del contenido multimedia protegido por el algoritmo de cifrado simétrico. La clave contenida generalmente se introduce en la licencia en forma de un criptograma obtenido por cifrado de la clave de contenido con una clave de cifrado, llamada «de terminal», propia del terminal o conocida por él. Para acceder al contenido, el terminal extrae de la licencia la clave del contenido, descifrando su criptograma por medio de su clave de terminal. Seguidamente el descodificador del terminal descodifica, es decir descifra, el contenido por medio de la clave de contenido así extraída de la licencia, eliminado así la protección. Por ejemplo, el sistema de DRM es el descrito en la solicitud de patente presentada bajo el número FR 1451666 del 2 de marzo de 2014. Por analogía, en este último caso, la clave de contenido específico, la clave de contenido y la clave de terminal corresponden, respectivamente, a la palabra de control CW_t y a las claves K_s y K_i del sistema CAS descrito aquí.

Un derecho de acceso puede hacerse específico a un terminal sin utilizar una clave K_i. Por ejemplo, el mensaje EMM comprende un identificador del terminal para el cual está destinado. Durante la recepción de este mensaje EMM por los terminales, estos comparan sus identificadores con el contenido en el mensaje EMM recibido. Si no existe correspondencia entre estos identificadores, el terminal no trata el mensaje EMM. Solo el terminal cuyo

identificador corresponde con el identificador contenido en el mensaje EMM recibido trata este mensaje. En este caso, la clave K_s contenida en el mensaje EMM es por ejemplo cifrada con una clave K_G y no con la clave K_i del terminal T_i. La clave K_G es por ejemplo una clave común para un grupo restringido de varios terminales del sistema 2.

En otra variante, la clave K_i es común para un grupo restringido de terminales del sistema 2.

En una variante preferida, es el sistema 28 el que gestiona y utiliza las claves K_i. En esta variante, el sistema 28 recibe del servidor 40 los identificadores de los terminales pertenecientes a la lista 50 y para los cuales es preciso construir y difundir los derechos de acceso DA_i. Luego, para cada uno de los identificadores de terminales recibidos y solamente para estos identificadores, el sistema 28 construye el derecho de acceso DA_i y, en particular, el criptograma K_s*K_i, después lo incorpora en un mensaje EMM difundido con destino al terminal T_i. En esta variante, el servidor 40 solo gestiona los derechos complementarios de los terminales y la lista 50 pero no construye el mismo los criptogramas K_s*K_i contenidos en los derechos de acceso DA_i. Transmite en efecto por ejemplo los derechos complementarios de los terminales al sistema 28, el cual construye los criptogramas K_s*K_i y los derechos de acceso DA_i.

La utilización del contador T_i.CM puede ser omitida. En este caso, el campo T_i.State bascula del valor « PC » al valor « D » desde la primera ausencia de recepción de un acuse de recibo.

En otra variante, solo se utilizan dos valores para el campo T_i.State a saber los valores « C » y « D ». En este caso, todas las operaciones del procedimiento de la figura 4 que utilizan el valor « PC » son omitidas.

Otros modos de realización del perfil de ocupación son posibles. Por ejemplo, el periodo de observación dividido en intervalos horarios puede extenderse en más de una jornada. Por ejemplo, este periodo de observación puede ser igual a una semana o a un mes. La duración de los intervalos horarios puede ser modificada. Por ejemplo, pueden ser más cortos de una hora o por el contrario, más largos. Típicamente, la duración de un intervalo horario está comprendida entre un minuto y 24h y, de preferencia, entre 5min y 3h o entre 30min y 3h. Los diferentes intervalos horarios pueden también tener duraciones diferentes los unos de los otros. Por ejemplo, los intervalos horarios son más cortos en los momentos de gran audiencia y más largos en el momento de poca audiencia como por ejemplo durante la noche.

Los perfiles de ocupación pueden también ser construidos y gestionados de diferente modo. Por ejemplo, en variante, el usuario indica el mismo los intervalos horarios en que tiene la costumbre de utilizar su terminal. Estos intervalos horarios son seguidamente registrados por el servidor 40 en la tabla 48. Después, estos márgenes horarios nunca son actualizados automáticamente. Así, el procedimiento de la figura 4 puede simplificarse pues todas las etapas que provocan la actualización automática del perfil de ocupación son omitidas. Otros métodos para construir automáticamente el perfil de ocupación de los terminales son igualmente posibles. Por ejemplo, en variante, el perfil de ocupación del terminal T_i es construido automáticamente teniendo en cuenta los instantes en que este terminal T_i bascula entre sus estados listo y ocupado, pero también a partir de los instantes en que los otros terminales basculan en paralelo, entre sus estados listo y ocupado.

En otra variante, cada campo $T_i.PH_j$ contiene la probabilidad de que el terminal T_i se encuentre en el estado listo durante el intervalo horario PH_j. Para eso, en cada comienzo de un intervalo horario PH_j, el servidor 40 incrementa en «uno» un contador TPH_j. El contador TPH_j contiene por consiguiente el número de veces en que el intervalo horario PH_j ha sido encontrado. En paralelo, el servidor 40 incrementa un contador $T_i.PPH_j$ cada vez que el terminal T_i se encuentra en su estado listo durante el intervalo horario PH_j. A continuación, el valor del campo T_iPH_j se obtiene dividiendo el valor del contador $T_i.PPH_j$ por el valor del contador TPH_j. En esta variante, el umbral S_{PH} es típicamente tomado superior o igual al 50% de posibilidades de que el terminal T_i se encuentre en el estado listo. De preferencia, los contadores TPH_j y $T_i.PPH_j$ son actualizados teniendo en cuenta únicamente los datos contenidos en una ventana móvil.

En una variante simplificada, la construcción y la gestión de los perfiles de ocupación para cada terminal es omitida. En este caso, todas las operaciones del procedimiento de la figura 4 que utilizan un perfil de ocupación son omitidas.

El número de intervalos horarios contiguos a tener en cuenta para hacer pasar el indicador $I_{i,j}$ al valor «verdadero» puede ser superior o igual a dos o al contrario igual a uno. En este último caso, el indicador $I_{i,j}$ toma el valor «verdadero» una vez que el valor del campo $T_i.PH_j$ es superior al umbral S_{PH}.

En variante, para conocer el estado de un terminal T_i, el servidor 40 envía una petición de estado a este terminal T_i y el terminal T_i responde a esta petición enviando al servidor 40, por mediación de una conexión punto a punto, un mensaje de estado indicando que se encuentra en su estado listo. Si el terminal no está en su estado listo, es incapaz de enviar este mensaje de estado en respuesta a la petición de estado. En este modo de realización, la petición de estado es típicamente un mensaje diferente del mensaje que contiene los derechos de acceso DA_i transmitidos a este terminal. La petición de estado es transmitida por mediación de una conexión punto a punto o punto a multipunto, en instantes predeterminados o determinados en función del perfil de ocupación.

En los modos de realización descritos anteriormente, el acontecimiento en respuesta al cual el terminal envía un mensaje de estado es un mensaje transmitido desde la cabecera 6 hacia el terminal. Sin embargo, este acontecimiento puede también ser la circunstancia de un instante predeterminado. Por ejemplo, en otra variante, mientras que el terminal T_i se encuentra en su estado listo, envía a intervalos regulares, por mediación de una conexión punto a punto, un mensaje de estado al servidor 40. En este modo de realización, el mensaje de estado no es por consiguiente transmitido en respuesta a una petición o a un mensaje enviado por el servidor 40. El servidor 40 trata entonces estos mensajes de estado como se ha descrito anteriormente. En particular, el contador T_i.CM es incrementado en uno cada vez que ningún mensaje de estado es recibido en el instante predeterminado donde dicho mensaje de estado habría debido ser recibido si el terminal T_i se hubiera encontrado en su estado listo.

Las etapas 168 y 172 pueden ser omitidas.

Cada vez que un acuse de recibo es recibido por parte del terminal T_i, la fecha actual es registrada en el campo T_i.DAck. Por lo tanto, la fecha contenida en el campo T_i.DAck puede ser utilizada como fecha actual para identificar el intervalo horario actual durante la ejecución de la etapa 146.

En variante, cada vez que un terminal T_i acusa recibo del derecho de acceso DA_i, la difusión de este derecho de acceso DA_i no se suspende hasta que este derecho de acceso DA_i requerido para acceder al contenido multimedia cambia. Por lo tanto, el mismo derecho de acceso DA_i es difundido periódicamente hacia el terminal T_i mientras el identificador de este terminal figure en la lista 50.

El procedimiento descrito aquí puede combinarse con el procedimiento descrito en la solicitud WO2009094502A1. En este caso, durante cada intervalo horario donde los derechos de acceso DA_i son únicamente preparados y difundidos a un grupo restringido de terminales, el servidor 40 retira automáticamente de este grupo restringido, los terminales que se encuentran en el estado ocupado y que por consiguiente no envían mensajes de estado.

REIVINDICACIONES

1. Procedimiento de difusión de un contenido multimedia protegido por derechos de acceso a terminales mecánicamente independientes los unos de los otros y conectados con un mismo servidor de derechos de acceso por mediación de una red de larga distancia de transmisión de informaciones, en el cual:

- el terminal envía (104), al servidor de derechos de acceso, una petición de derechos de acceso para recibir los derechos de acceso que le permitan acceder al contenido multimedia,
- en respuesta a la petición de los derechos de acceso, el servidor de derechos de acceso añade (106) un identificador del terminal a una lista de difusión,
- el servidor de derechos de acceso difunde (114), a intervalos predeterminados, cada nuevo derecho de acceso al contenido multimedia difundido, solamente a los terminales cuyo identificador figura en la lista de difusión y sin esperar para ello que estos terminales hayan pedido este nuevo derecho de acceso enviando una nueva petición de derechos de acceso,
- en respuesta a la recepción de cada derecho de acceso, el terminal accede (120) al contenido multimedia difundido y, en ausencia de recepción del derecho de acceso, el terminal inhibe el acceso al contenido multimedia difundido,
- en cualquier momento, el terminal bascula, independientemente, de los otros terminales:
  • de un estado listo en el cual el terminal es capaz de enviar, por mediación de una conexión punto a punto, la petición de derechos de acceso, y de recibir el derecho de acceso requerido,
  • a un estado ocupado en el cual el terminal es incapaz de enviar, por mediación de la conexión punto-por-punto, la petición de derechos de acceso o de recibir el derecho de acceso,

caracterizado por que:

- en respuesta a un acontecimiento predeterminado, el terminal envía (118) al servidor de derechos de acceso, por mediación de una conexión punto a punto, un mensaje de estado que indica al servidor de derechos de acceso que se encuentra en su estado listo y, alternativamente, no envía este mensaje de estado si se encuentra en su estado ocupado, y
- en ausencia de recepción del mensaje de estado esperado en respuesta al acontecimiento predeterminado, el servidor de derechos de acceso retira (166, 168, 170, 172) automáticamente el identificador de este terminal de la lista de difusión.

2. Procedimiento según la reivindicación 1, en el cual el procedimiento comprende:

- la memorización, para cada terminal, de un perfil de ocupación que comprende intervalos horarios y para cada intervalo horario un indicador de la probabilidad de que el terminal se encuentre en su estado listo durante este intervalo horario, y

- para cada terminal y únicamente para cada intervalo horario del perfil de ocupación de este terminal donde el indicador corresponde a una probabilidad de que este terminal se encuentre en su estado listo superior a un umbral predeterminado: al comienzo de este intervalo horario, el servidor de derechos de acceso añade (156) automáticamente el identificador de este terminal a la lista de difusión sin esperar que este terminal haya enviado una petición de derechos de acceso.

3. Procedimiento según la reivindicación 2, en el cual, en respuesta a la recepción de cada mensaje de estado en el instante predeterminado, el servidor de derechos de acceso incrementa (150) el valor del indicador asociado con el intervalo horario durante el cual este mensaje de estado ha sido recibido y, alternativamente, en ausencia de recepción de este mensaje de estado en el instante predeterminado, disminuye (152) el valor de este indicador.

4. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual en ausencia de recepción de un mensaje de estado por parte de un terminal, el servidor de derechos de acceso incrementa (144) un contador asociado específicamente con este terminal, luego retira (142) automáticamente el identificador de este terminal de la lista de difusión únicamente cuando este contador ha sobrepasado un umbral predeterminado, y, alternativamente, en caso de recepción de un mensaje de estado por parte del terminal, reinicializa el contador.

5. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual:

- el servidor de derechos de acceso prepara (114) para cada terminal del cual el identificador figura en la lista de difusión y solamente para estos terminales, un derecho de acceso específico que solo este terminal puede explotar para eliminar la protección del contenido multimedia protegido y acceder así en claro a este contenido multimedia, siendo los otros terminales incapaces de explotar este derecho de acceso específico para acceder en claro al contenido multimedia, y

- en respuesta a la recepción de cada derecho de acceso específico preparado para este terminal, el terminal accede (120) al contenido multimedia difundido y, en ausencia de recepción del derecho de acceso específico, el terminal inhibe el acceso al contenido multimedia difundido.

6. Procedimiento según la reivindicación 5, en el cual, mientras el terminal se encuentre en su estado listo, solamente en respuesta a la recepción de cada derecho de acceso específico preparado para este terminal, el terminal envía (118), por mediación de una conexión punto a punto, un acuse de recibo al servidor de derecho de acceso para confirmar la recepción de este derecho de acceso específico, y el servidor de derechos de acceso utiliza este acuse de recibo como mensaje de estado que indica que el terminal se encuentra en su estado listo.

7. Procedimiento según la reivindicación 6, en el cual el servidor de derechos de acceso difunde periódicamente el mismo derecho de acceso mientras ningún acuse de recibo de este derecho de acceso haya sido recibido y, en respuesta a la recepción del acuse de recibo de este derecho de acceso, el servidor de derechos interrumpe la difusión de este derecho de acceso.

8. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual cada vez que el servidor de derechos de acceso recibe un mensaje de estado de un terminal, registra la fecha en la cual este mensaje de estado ha sido recibido, luego, paralelamente, el servidor de derecho de acceso compara (168, 172), a intervalos regulares, un umbral un umbral predeterminado con la diferencia entre una fecha actual y la última fecha registrada en la cual un mensaje de estado ha sido recibido para este terminal y, solamente si este umbral predeterminado es franqueado, el servidor de derecho de acceso retira automática y sistemáticamente el identificador de este terminal de la lista de difusión.

9. Soporte (44) de registro de informaciones, caracterizado por que comprende instrucciones para la puesta en práctica de un procedimiento de difusión de un contenido multimedia protegido conforme a una cualquiera de las reivindicaciones anteriores, cuando estas instrucciones son ejecutadas por un ordenador electrónico conforme a la reivindicación 10.

10. Servidor de derecho de acceso para la realización de un procedimiento conforme a una cualquiera de las reivindicaciones 1 a 8, en el cual el servidor de derecho de acceso comprende un ordenador electrónico (42) programado para:

- recibir una petición de derechos de acceso enviada por un terminal que desea recibir los derechos de acceso que le permitan acceder al contenido multimedia,

- en respuesta a la petición de derechos de acceso recibida, añadir un identificador del terminal a una lista de difusión,

- difundir, a intervalos predeterminados, cada nuevo derecho de acceso al contenido multimedia difundido, solamente a los terminales cuyo identificador figura en la lista de difusión y sin esperar para eso que los terminales hayan solicitado este nuevo derecho de acceso enviando una nueva petición de derechos de acceso,

caracterizado por que el ordenador electrónico (42) está igualmente programado para:

- en respuesta a un acontecimiento predeterminado, recibir por parte del terminal, por mediación de una conexión punto a punto, un mensaje de estado indicando al servidor de derechos de acceso que este terminal se encuentra en su estado listo y, alternativamente, la ausencia de recepción de este mensaje de estado si el terminal se encuentra en su estado ocupado, y
- en respuesta a la ausencia de recepción del mensaje de estado esperado en respuesta al acontecimiento predeterminado, retirar automáticamente el identificador de este terminal de la lista de difusión.

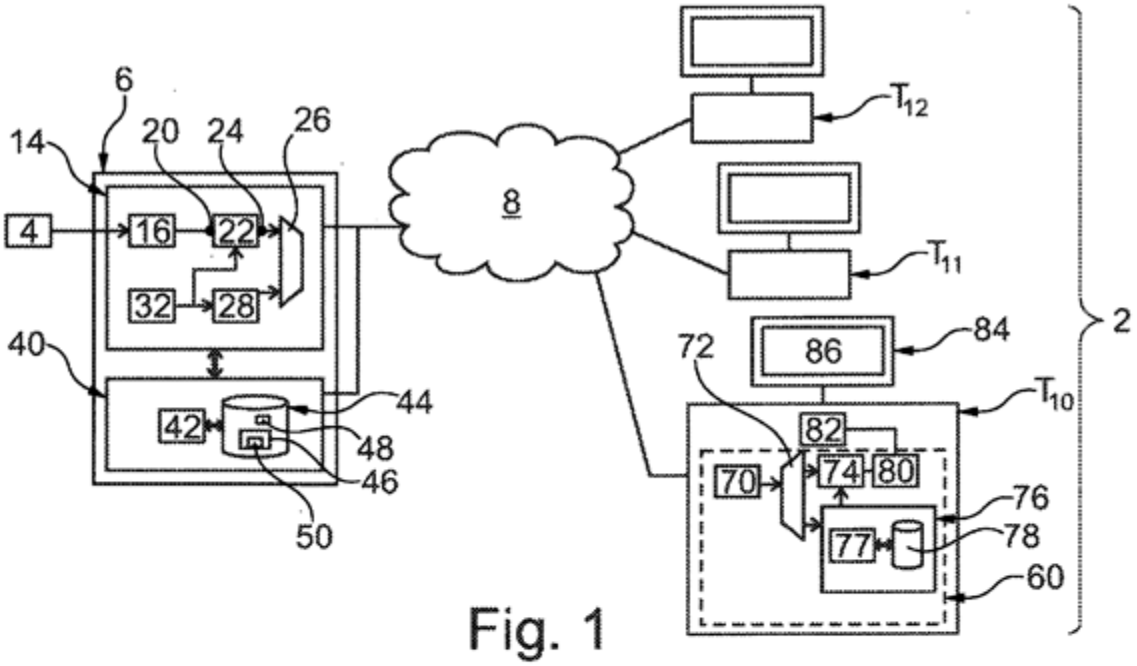

Fig. 1

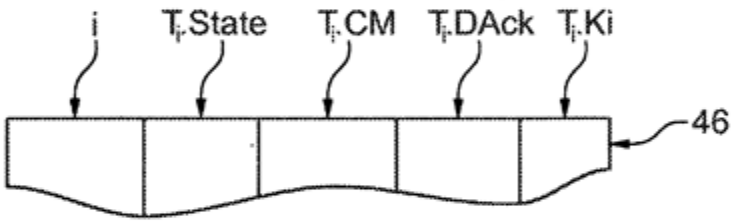

Fig. 2

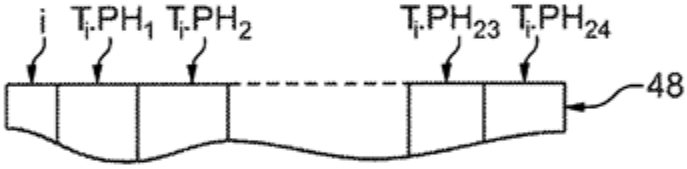

Fig. 3

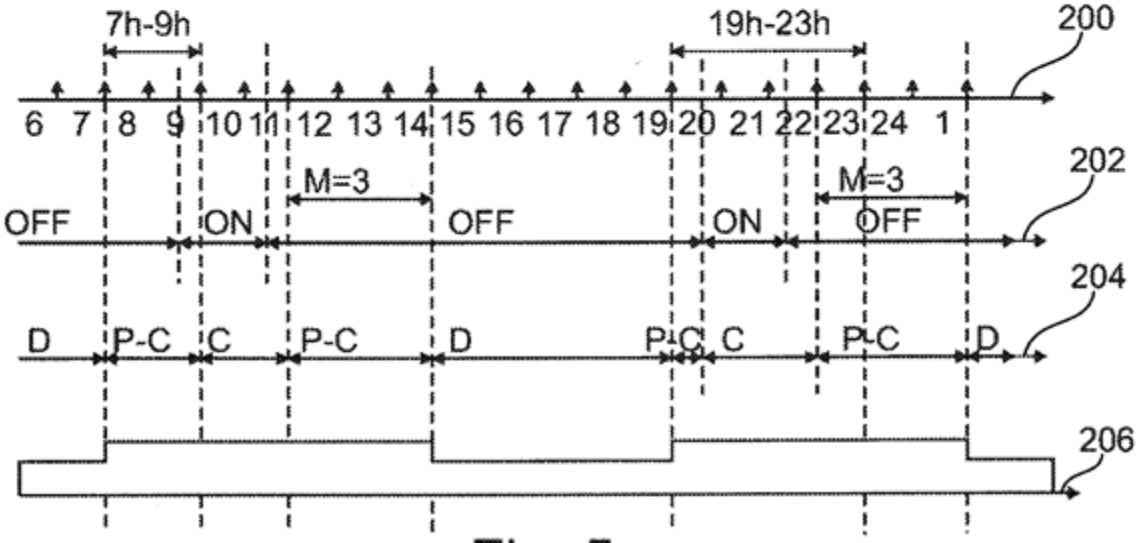

Fig. 5

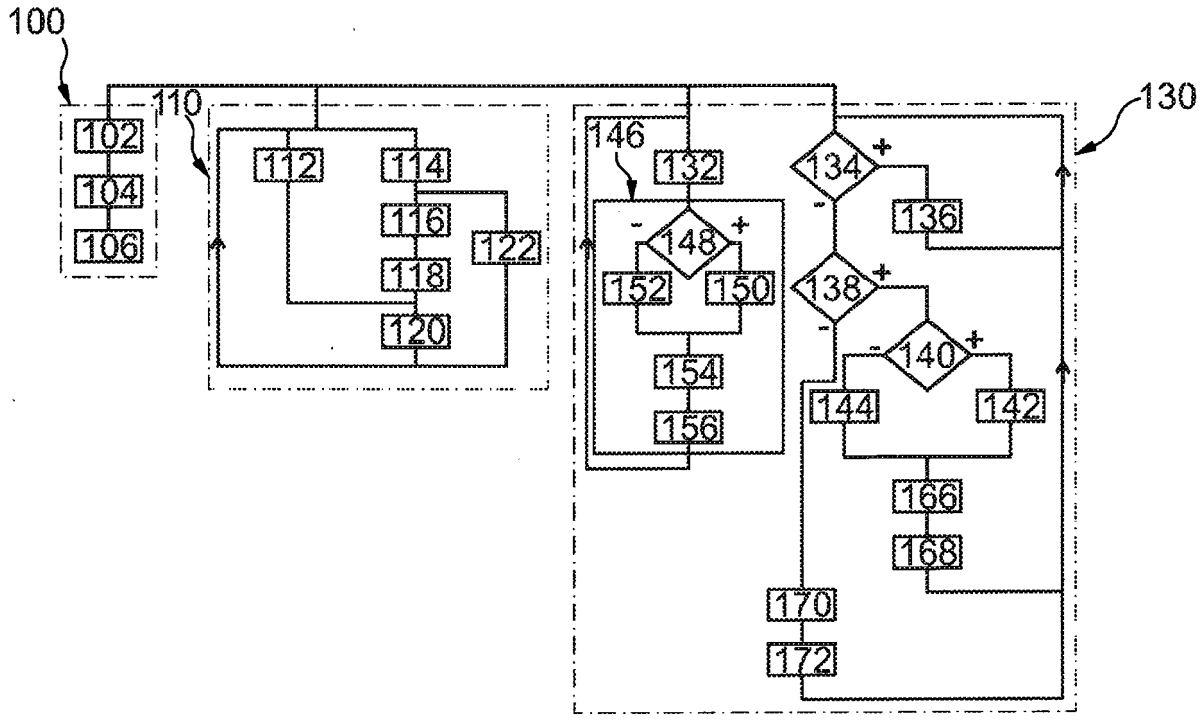
100
110
130
102
104
106
112
114
116
118
120
122
146
132
148
152
150
154
156
134
136
138
140
144
142
166
168
170
172

Fig. 4