(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 605 112**

(51) Int. CI.:

H04N 21/266 (2011.01)
H04N 21/418 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/45 (2011.01)
H04N 21/8358 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.04.2012 PCT/EP2012/055938**

(87) Fecha y número de publicación internacional: **18.10.2012 WO12139913**

(96) Fecha de presentación y número de la solicitud europea: **02.04.2012 E 12713129 (0)**

(97) Fecha y número de publicación de la concesión europea: **28.09.2016 EP 2697979**

(54) Título: **Método para identificar el origen de un módulo de seguridad en un sistema descodificador de televisión de pago**

(30) Prioridad:

15.04.2011 US 201161475754 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.03.2017

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

KUDELSKI, HENRI

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para identificar el origen de un módulo de seguridad en un sistema descodificador de televisión de pago

Introducción

[0001] La presente invención se refiere al dominio de los sistemas de acceso condicional y más particularmente a métodos para descubrir la identidad de un equipo usado en la práctica de redistribución no autorizada de claves de encriptación secretas.

Estado de la técnica

[0002] Un área donde la presente invención puede ser de particular interés es en el dominio de la TV de pago, donde un operador difunde contenido audio/video con derechos de propiedad a una pluralidad de consumidores suscritos a cambio del pago de una cuota. Los sistemas de acceso condicional se emplean para manejar el procesamiento de contenido de TV de pago, con el propósito de asegurar que realmente solo los consumidores que estén suscritos a ciertos servicios, normalmente a cambio de pagar una cuota al operador o proveedor de aquellos servicios, tengan acceso al contenido proporcionado para aquellos servicios. De acuerdo a tales sistemas de acceso condicional, el operador encripta el contenido mediante palabras de control. Estas últimas se suministran a los consumidores suscritos por medio de mensajes de seguridad, que o bien son emitidos en un flujo de datos junto con el contenido o se pueden distribuir por otros medios. A cada consumidor suscrito se le suministra un receptor apropiado que comprende un módulo de seguridad para permitir la extracción de las palabras de control de los mensajes de seguridad y una unidad de desaleatorización para la desencriptación del contenido audio/video encriptado difundido.

[0003] Los contenidos audio/video encriptados tienen un valor, por lo que los sistemas de acceso condicional han sido el objetivo de ataques por terceros que intentan obtener acceso al contenido audio/video sin suscribirse a los servicios del operador y sin estar en la posesión del equipo de recepción autorizado necesario. Una práctica comúnmente conocida como compartir la palabra de control, por la cual las palabras de control difundidas junto con el contenido encriptado son extraídos por un tercero que usa módulos de seguridad válidos, y los redistribuye libremente a otros terceros. Esto supone una amenaza particularmente significativa para operadores que ofrecen servicios de TV de pago ya que esto los priva de ingresos de los que ellos de otro modo se habrían beneficiado.

[0004] Los operadores de TV de pago, por lo tanto, tienen un gran interés en poder rastrear unidades receptoras que son usadas en actividades de compartir la palabra de control, dado que esto permite al operador tomar acciones contra aquellos implicados en tales actividades. La publicación de solicitud de patente estadounidense No. 2002/0,133,701A describe un método para rastrear los receptores traidores en un sistema de encriptación de difusión. El método incluye utilizar una clave falsa para codificar receptores representantes de subconjuntos plurales en el sistema. Los subconjuntos son derivados a partir de una ramificación que utiliza un sistema Subset-Cover, y el receptor traidor está asociado a una o más claves comprometidas que han sido obtenidos por un posible receptor pirata clonado. Utilizando un clon del receptor pirata, se determina la identidad del receptor traidor. Este sistema, sin embargo, tiene la desventaja de que se deben difundir múltiples codificaciones del mismo contenido, lo cual tiene un impacto negativo en la eficiencia de difusión del ancho de banda.

[0005] El documento US 2009/0097659 describe una solución para rastrear un receptor pirata mediante el encriptado de al menos algunos paquetes del flujo transmitido por diferentes claves de grupo. Cada receptor pertenece a un grupo y recibe las claves necesarias para desencriptar el paquete perteneciente a dicho grupo.

[0006] Cuando una de dichas claves de grupo es descubierta en una persona ilegítima, esto es la prueba de que un receptor de dicho grupo ya no es fiable. El grupo luego es dividido en grupos menores para indicar al receptor pirata, repitiendo los pasos.

[0007] El documento US 2009/0080689 describe una solución para añadir una marca de agua a un contenido. Una unidad de procesamiento previo genera uno o más valores alternos para un valor original del contenido. Los valores alternos son agregados al contenido como metadatos. En el lado receptor, los metadatos son procesados y un valor alterno (o el valor original) es seleccionado de acuerdo con un parámetro interno tal como un identificador que identifica al receptor de manera unívoca. El valor alterno seleccionado se utiliza para actualizar el contenido para producir un contenido con marca de agua.

[0008] El documento US 2010/0169349 describe una solución similar al documento precedente. El contenido es analizado para producir Metadatos según un esquema de marca de agua. En la recepción, los metadatos y una carga útil, que podría ser el número de serie del reproductor, se utiliza para introducir modificaciones en el contenido original. El resultado final es un contenido con marca de agua que comprende información que más tarde permite recuperar la carga útil.

[0009] El documento WO 2004/082286 describe un sistema de acceso condicional en el que el contenido es encriptado mediante palabras de control. La palabra de control luego es introducida en un ECM y encriptada por una clave de servicio. Dicha clave de servicio es a su vez introducida en un EMM que comprende direcciones únicas o de grupo de receptores a los que va destinado. El objetivo de este documento es reducir el daño provocado por la filtración de una clave de servicio. Para tal fin, la misma palabra de control es encriptada por dos claves de servicio diferentes y enviadas en dos ECM diferentes. La primera clave de servicio es enviada a través de un EMM a una primera serie de decodificadores y la segunda clave de servicio es enviada a un segundo conjunto de receptores. En caso de haber un conjunto comprometido, este conjunto es dividido en un grupo menor y las claves deben ser cambiadas para permitir acceso sólo a los participantes del grupo.

Breve descripción de la invención

[0010] Esta invención propone una solución para identificar el origen de un módulo de seguridad en el sistema de TV de pago según el método siguiente:

[0011] Método para identificar el origen de un módulo de seguridad en el sistema de decodificador de TV de pago que incluye las etapas de:

- recibir por el sistema de decodificador de TV de pago un servicio que comprende al menos un primer stream, un segundo stream y un stream de palabra de control, el segundo stream siendo un duplicado del primero, con el primer stream encriptado por una primera palabra de control (CW1) y el segundo stream encriptado por un segundo stream de palabra de control (CW2),
- extraer, del stream de palabra de control, mensajes de autorización que contienen al menos una palabra de control principal (CW) que permite recuperar la primera y la segunda palabra de control, y las condiciones de acceso,
- transferir el stream de palabra de control al módulo de seguridad,
- extraer los mensajes de autorización del stream de palabra de control y controlar las condiciones de acceso,
- si se cumplen las condiciones de acceso, determinar las primeras y segundas palabras de control a partir de la palabra de control principal en el mensaje de autorización,
- determinar un parámetro interno del módulo de seguridad, con este parámetro interno siendo único para cada módulo de seguridad,

caracterizado por el hecho de que, además comprende los pasos de:

- seleccionar una palabra de control actual a partir de la primera o la segunda palabra de control basada en parte del parámetro interno, correspondiente al primer o el segundo stream,
- transmitir la palabra de control actual al decodificador de TV de pago,
- seleccionar un stream actual desde el primero o el segundo stream conforme a la selección de la primera o la segunda palabra de control,
- desencriptar el stream actual con la palabra de control actual.

Breve descripción de las figuras

[0012] Esta invención se entenderá mejor gracias a las figuras adjuntas en las que:

- la figura 1 muestra los dispositivos de la invención, es decir un sistema de decodificador de TV de pago,
- la figura 2 muestra el stream resultante.

Descripción de la invención

[0013] La presente invención propone duplicar al menos uno de los streams elementales de un servicio y encriptar este stream adicional mediante una palabra de control particular. Un servicio comprende diferentes streams elementales ensamblados para formar un servicio, tal como un stream de vídeo, un stream audio y stream de datos (para llevar los mensajes de control ECM).

[0014] Estos streams elementales son descritos en el PMT (mapa de programa tabla). Las tablas de mapa de programa (PMT) contienen información acerca de servicios. Para cada servicio, hay un PMT. Los PMT proporcionan información sobre cada servicio presente en el stream de transporte, incluyendo el número del programa, y hacen una lista de los streams elementales que comprenden el programa MPEG-2 descrito. También hay ubicaciones para descriptores opcionales que describen el programa MPEG-2 entero, al igual que un descriptor opcional para cada stream elemental. Cada stream elemental está marcado con un valor del tipo de stream.

[0015] La presente invención describirá como un ejemplo la duplicación de un stream de audio. Sin embargo, el mismo método puede ser aplicado con un stream de vídeo cuando el ancho de banda no es un problema.

[0016] Como es bien conocido por los expertos en la técnica, el módulo de seguridad puede esencialmente ser realizado de acuerdo a cuatro formas diferentes. Una de estas formas es una tarjeta de microprocesador, una tarjeta inteligente, o más generalmente un módulo electrónico (tomando la forma de clave, una insignia,...). Tal módulo generalmente es desmontable y conectable al decodificador.

[0017] La forma con contactos eléctricos es la más usada, pero no se excluyen conexiones sin contacto por ejemplo del tipo ISO 14443.

[0018] Una segunda forma conocida es la de una caja de circuito integrado, generalmente colocada inamovible y de forma definitiva en el decodificador. Una alternativa se compone de un circuito montado sobre una base o conector como por ejemplo un conector de módulo SIM.

[0019] En una tercera forma, el módulo de seguridad está integrado en una caja de circuito integrado que también tiene otra función, como por ejemplo en un módulo de desaleatorización del decodificador o en el microprocesador del decodificador.

[0020] En una cuarta forma de realización, el módulo de seguridad no está realizado en forma de hardware, sino que su función se implementa sólo en forma de software. Suponiendo que en los cuatro casos la función es idéntica aunque el nivel de seguridad difiere, se puede hablar de un módulo de seguridad, independientemente de la forma en que realiza su función o la forma que este módulo pueda tener.

[0021] Se duplica el stream de audio y cada stream de audio luego es encriptado con una clave o palabra de control diferente.

[0022] Ambos streams encriptados (audio1, audio2) luego son ensamblados con los otros streams para formar el servicio. Los varios streams son identificados en el PMT y las claves para el primer y el segundo stream de audio se incluyen en el flujo de datos.

[0023] Las claves, también llamadas palabras de control, son introducidas en mensajes de control de derecho de acceso que comprenden también los requisitos adecuados para tener acceso al contenido encriptado. En general, un mensaje contiene la palabra de control actual y la palabra de control siguiente, es decir, la palabra de control que se aplica en los datos futuros después de un cambio de clave.

[0024] Según una primera forma de realización, el mensaje comprende cuatro palabras de control, dos por cada stream (actual y siguiente). De acuerdo a otra forma de realización, se envían dos mensajes al módulo de seguridad, cada uno de los cuales estando dedicado a un único stream.

[0025] Ya que el servicio comprende diferentes streams, y sólo uno es duplicado, el método de la invención se basa preferiblemente en el uso de tres palabras de control. Una (CW1) para el primer stream, una (CW2) para el duplicado primer stream, y una (CW3) para los otros streams. En lo que al decodificador se refiere, el módulo de seguridad sólo proporcionará dos palabras de control a la vez, es decir CW1 y CW3 o CW2 y CW3.

[0026] El módulo de seguridad procesa el mensaje recibido, es decir, desencripta el mismo con una clave de transmisión perteneciente al sistema de radiodifusión y extrae las condiciones de acceso al igual que las palabras de control.

[0027] El módulo de seguridad verifica que se cumplen las condiciones de acceso, es decir que la memoria del módulo de seguridad contiene los derechos referidos por las condiciones de acceso.
Estos derechos son cargados en el módulo de seguridad preferiblemente por mensajes únicamente dirigidos a dicho módulo de seguridad y encriptados mediante una clave personal de este módulo de seguridad.

[0028] Cada módulo de seguridad (SM) de una colección de módulos de seguridad (SM) gestionada por el operador (OP) es identificable de forma única por un ajuste interno (UA) que es particular al módulo de seguridad (SM).
Cada módulo de seguridad (SM) está instruido para seleccionar una de las palabras de control (CW) según a su ajuste interno único (UA). El ajuste interno (UA) podría ser por ejemplo el valor de un registro que representa la dirección única del módulo de seguridad. Preferiblemente, el módulo de seguridad (SM) está instruido para seleccionar la palabra de control (CW) según el valor del enésimo bit de su dirección única, por ejemplo.

[0029] Para facilitar la comprensión, la palabra de control para el primer stream será nombrada primera palabra de control CW1, la palabra de control para el vapor duplicado (segundo stream) será nombrada segunda palabra de control CW2, y la palabra de control para el otro stream (o streams) será la tercera palabra de control nombrada CW3.

[0030] En consecuencia, basándose en un parámetro interno, el módulo de seguridad selecciona la primera de la segunda palabra de control y devuelve ésta al decodificador. Las palabras de control usadas para la desencriptación

de los streams no son necesariamente extraídos para el ECM. El módulo de seguridad puede extraer una palabra de control principal desde el ECM y producir las primeras y las segundas palabras con una función criptográfica a partir de la tercera palabra de control. Esta función será preferiblemente inicializada por un parámetro conocido por todos los módulos de seguridad. Por supuesto, cualquiera de las palabras de control puede ser usada como palabra de control inicial para generar las otras palabras de control.

[0031] Es importante que el decodificador seleccione el stream correcto con la palabra de control correspondiente. Esto puede hacerse mediante medios diferentes, es decir, por una instrucción del módulo de seguridad o por el mismo decodificador.

[0032] De la misma manera que el módulo de seguridad manda instrucciones al decodificador DEC, el módulo de seguridad informa al decodificador del stream para ser procesado. Cabe observar que el decodificador tiene ajustado el filtro FI del elemental para ambos streams. Sólo uno de entre el primer o segundo stream es seleccionado para ser pasado al descodificador DSC. La información recibida desde el módulo de seguridad será usada para seleccionar el stream apropiado entre los streams, preferiblemente cuando la palabra de control cambia. El decodificador almacena temporalmente la selección de stream y analiza el stream actual. Cuando un cambio de palabra de control es detectado, la nueva selección de stream es aplicada de modo que el descodificador recibe el stream correcto que coincide con la palabra de control recibida previamente.

[0033] Cuando el decodificador puede decidir por sí mismo sobre el stream a procesar, el decodificador es consciente del parámetro interno usado para la selección y se aplica la misma selección. La dirección única UA del módulo de seguridad es conocida por el decodificador.

[0034] En una forma de realización particular de la presente invención, un registro de barrido inicializado (CNTR) se utiliza para apuntar a un bit particular en la dirección única del módulo de seguridad. Cuando es inicializado, el registro de barrido apunta al primer bit de la dirección única y el estado de este bit se utiliza para seleccionar una de las dos palabras de control. Cuando la selección ha sido hecha el registro de barrido incrementa y el siguiente bit de la dirección única se utiliza para seleccionar una de las primeras o segundas palabras de control. Este proceso continua hasta que todos los bits de la dirección única han sido usados, a partir de lo cual el registro de barrido es reinicializado. Las palabras de control de los mensajes de seguridad pueden ser procesados como y cuando llegan o pueden ser almacenados en una tabla de palabra de control (CWT) y ser procesadas según la demanda o según un régimen basado en el tiempo.

[0035] La figura 2 ilustra el resultado de los streams después de la selección del primer (ST1) o segundo (ST2) stream según el estado del bit correspondiente del parámetro interno UA.

[0036] Según otra forma de realización de la presente invención, en vez del procesamiento controlado por órdenes anteriormente descrito, se puede utilizar un método más automatizado. En esta forma de realización el mensaje de seguridad (ECM) o el mensaje de gestión (EMM) además comprende información relacionada con tiempo - el momento del día, por ejemplo. Esta información puede ser utilizada para indicar adicionalmente a qué hora la selección de la palabra de control debería ser hecha. Entonces es posible enviar una orden a un grupo de módulos de seguridad para determinar si un miembro de este grupo se usa fraudulentamente. En el caso positivo, el tamaño del grupo puede ser reducido hasta que el módulo de seguridad apropiado está localizado.

[0037] La ventaja de activar y desactivar este método de palabra de control doble es que se puede seleccionar el tiempo cuando un stream duplicado está presente. No es necesario duplicar un stream todo el tiempo, el método puede ser inicializado por un periodo corto, así reduciendo el impacto en el ancho de banda.

[0038] Además, una función de control realizada en la información relativa al tiempo produce un valor que puede ser usada para apuntar a un bit particular de la dirección única para usar en la selección de una de las palabras de control. Por ejemplo, para una dirección única de 32 bits, un módulo-32 del resultado del control de la información relativa al tiempo señalaría a uno de los 32 bits de la dirección única.

[0039] Según otro aspecto de la invención, el stream duplicado no es una copia del primer stream. El segundo stream contiene alguna modificación tal como una marca de agua de manera que las modificaciones no son visualmente detectables por el usuario final. A consecuencia, la emisión resultante del descodificador contendrá alternativamente el primer o el segundo stream, el cambio siendo dictado por el parámetro interno del descodificador.

REIVINDICACIONES

1. Método para identificar el origen de un módulo de seguridad en un sistema decodificador de TV de pago, que incluye las etapas de:

- recibir por el sistema de decodificador de TV de pago un servicio que comprende al menos un primer stream, un segundo stream y un stream de palabra de control, con el segundo stream siendo un duplicado del primer stream, dicho primer stream estando encriptado por una primera palabra de control (CW1) y dicho segundo stream estando encriptado por una segunda palabra de control (CW2),
- extraer, desde el stream de palabra de control, mensajes de autorización que contienen al menos una palabra de control principal (CW) que permite obtener la primera y la segunda palabra de control, y condiciones de acceso,
- transferir el stream de palabra de control al módulo de seguridad,
- extraer los mensajes de autorización del stream de palabra de control y controlar las condiciones de acceso,
- si se cumplen las condiciones de acceso, determinar la primeras y segunda palabras de control a partir de la palabra de control principal en el mensaje de autorización,
- determinar un parámetro interno del módulo de seguridad, este parámetro interno siendo único para cada módulo de seguridad,
- seleccionar una palabra de control actual a partir de la primera o la segunda palabra de control basada en parte del parámetro interno, correspondiente al primer o segundo stream,
- transmitir la palabra de control actual al decodificador de TV de pago,
- seleccionar un stream actual desde el primer o segundo stream conforme a la selección de la primera o la segunda palabra de control,
- desencriptar el stream actual con la palabra de control actual,

caracterizado por el hecho de que el parámetro interno es una dirección única del módulo de seguridad y que tiene una pluralidad de bits, y el método comprende los pasos de:

a. inicializar un registro de barrido (CNTR) apuntando hacia el primer bit de la dirección única,
b. utilizar el registro de barrido para apuntar a un bit de la dirección única,
c. utilizar el estado de dicho bit para seleccionar la palabra de control actual,
d. incrementar el registro de barrido para apuntar al bit siguiente de la dirección única cada vez que se realiza la selección de una palabra de control corriente a partir de la primera o la segunda palabra de control,
e. repetir los pasos b a d hasta que todos los bits de la dirección única han sido usados, y reinicializar del registro de barrido.

2. Método según la reivindicación 1, donde el mensaje de autorización comprende la primera y la segunda palabra de control.

3. Método según la reivindicación 1, donde la primera y la segunda palabra de control son calculadas a partir de la palabra de control principal usando una función criptográfica.

4. Método según la reivindicación 3, donde la función criptográfica es inicializada por un parámetro común para todos los módulos de seguridad.

5. Método de cualquiera de las reivindicaciones 1 a 4, donde la selección del stream actual por el decodificador de TV de pago es desencadenado por una instrucción recibida desde el módulo de seguridad.

6. Método de cualquiera de la reivindicación 1 a 4, donde la selección del stream actual por el decodificador de TV de pago es desencadenado por la selección de la misma parte del parámetro interno por el decodificador de TV de pago.

7. Método de cualquiera de las reivindicaciones 1 a 6, donde el primer y el segundo stream transportan la misma información de audio o de vídeo.

8. Método de cualquiera de las reivindicaciones 1 a 6, donde al menos el primer stream comprende una marca que permite distinguir dicho primer stream de dicho segundo stream.

9. Método según la reivindicación 8, donde el primer stream es un stream de audio y la marca es una marca de audio desapercibida.

10. Método según la reivindicación 8, donde el primer stream es un stream de vídeo y la marca es una marca de vídeo desapercibida.

11. Un sistema de decodificador de TV de pago (DEC) que comprende un módulo de seguridad (SM) para identificar el origen de un módulo de seguridad de un sistema de decodificador de TV de pago, con el sistema de decodificador de TV de pago estando configurado para:

- recibir un servicio que comprende al menos un primer stream, un segundo stream y un stream de palabra de control, el segundo stream siendo un duplicado del primer stream, dicho primer stream estando encriptado por una primera palabra de control (CW1) y dicho segundo stream estando encriptado por una segunda palabra de control (CW2),
- extraer, del stream de palabra de control, mensajes de autorización que contienen al menos una palabra de control principal (CW) que permiten recuperar la primera y la segunda palabra de control, y las condiciones de acceso,
- transferir el stream de palabra de control al módulo de seguridad,
- seleccionar un stream actual del primer o segundo stream conforme a la selección de la primera o la segunda palabra de control,
- desencriptar el stream actual con una palabra de control actual,

dicho módulo de seguridad estando configurado para:

- determinar un parámetro interno del módulo de seguridad, este parámetro interno siendo único para cada módulo de seguridad,
- extraer los mensajes de autorización del stream de palabra de control y verificar las condiciones de acceso,
- si se cumplen las condiciones de acceso, determinar la primera y la segunda palabra de control a partir de la palabra de control principal en el mensaje de autorización,
- seleccionar la palabra de control actual a partir de la primera o la segunda palabra de control basada en parte del parámetro interno, correspondiente al primer o segundo stream,
- transmitir la palabra de control actual al decodificador de TV de pago (Dec),

caracterizado por el hecho de que el parámetro interno es una dirección única del módulo de seguridad y que tiene una pluralidad de bits, dicho módulo de seguridad (SC) estando además configurado para:

a. inicializar un registro de barrido (CNTR) apuntando al primer bit de la dirección única,

b. usar el registro de barrido para apuntar a un bit de la dirección única,

c. usar el estado de dicho bit para seleccionar la palabra de control actual,

d. incrementar el registro de barrido para apuntar al bit siguiente de la dirección única cada vez que se realiza la selección de una palabra de control actual de la primera o segunda palabra de control,

e. repetir los pasos b a d hasta que todos los bits de la dirección única han sido usados, y reinicializar el registro de barrido.

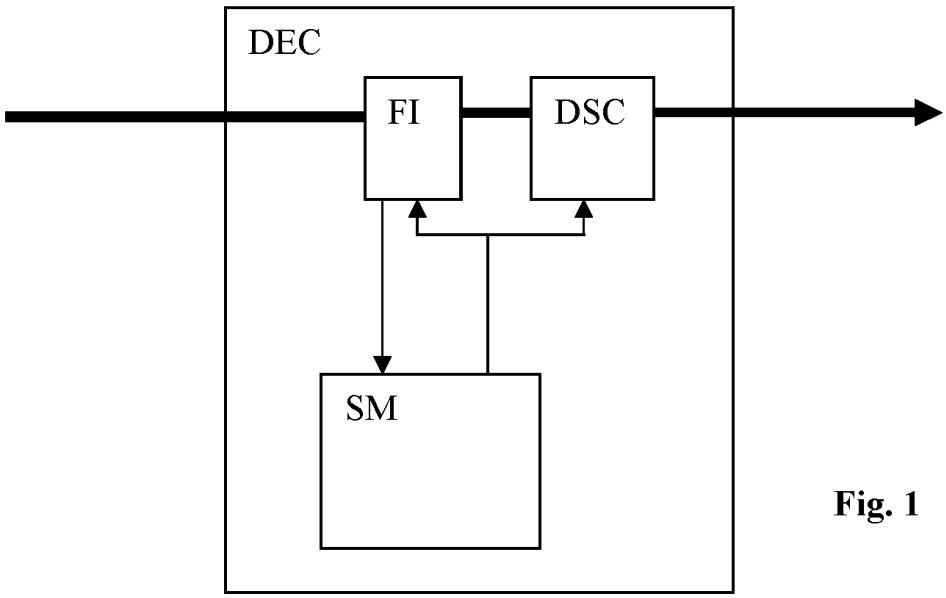

Fig. 1

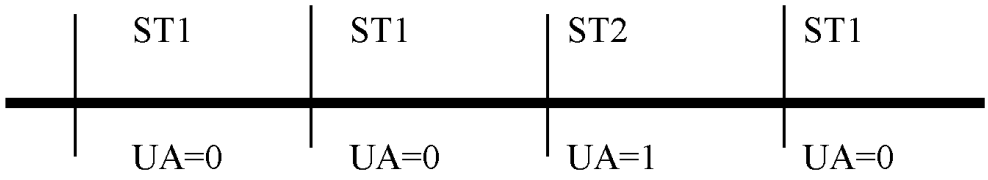

Fig. 2