(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 453 077**

(51) Int. CI.:

H04N 21/2347 (2011.01)
H04N 21/236 (2011.01)
H04N 21/2389 (2011.01)
H04N 21/4385 (2011.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.11.2010 E 10189587 (8)**

(97) Fecha y número de publicación de la concesión europea: **08.01.2014 EP 2448259**

(54) Título: **Método para crear un flujo de datos mejorado**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.04.2014

(73) Titular/es:

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

(72) Inventor/es:

AUMASSON, JEAN-PHILIPPE y
SCHWARZ, CHRISTIAN

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para crear un flujo de datos mejorado

Introducción

[0001] La presente invención se refiere a la transmisión de información digital entre dispositivos electrónicos, particularmente en el dominio de la comunicación multimedia digital, donde tal información digital es sometida a limitaciones de acceso condicional.

Estado de la técnica

[0002] Como es bien conocido en el dominio de transmisión de datos multimedia digitales, y especialmente en la transmisión de información digital audio/video, tal información es generalmente transmitida como parte de un flujo de transporte. Un flujo de transporte se compone por paquetes de datos, cada paquete de datos que comprende una pluralidad de bits de información. Los flujos de transporte en el campo de la comunicación multimedia digital generalmente se adhieren a un formato MPEG como MPEG 2.

[0003] La patente estadounidense con número de publicación 6,226,291 B1 divulga que un flujo de transporte se compone por varios paquetes de datos y da detalles de la construcción de un paquete de datos. El paquete de datos comprende dos partes, es decir una cabecera y una carga útil. En general, para una longitud de un paquete de datos de I bits, I es mayor o igual a 2. De aquellos I bits, la cabecera comprende n bits, donde n es mayor o igual a 1 y la carga útil comprende el restante I menos n bits. En la publicación mencionada, el paquete de datos tiene 188 bytes de largo, 4 bytes (32 bits) de los cuales comprenden la cabecera, con los restantes 184 bytes que comprenden la carga útil. Estos son los valores generalmente aceptados en el estado de la técnica. La información digital útil real que forma el objetivo de la comunicación está comprendida dentro de la carga útil. La cabecera por otro lado comprende metainformación tal como identificador de paquete (PID) por ejemplo.

[0004] Diferentes tipos de paquetes de datos se conocen en el dominio afectado, incluyendo paquetes de contenido y paquetes de relleno. Paquetes de contenido, o más particularmente, las cargas útiles de los paquetes de contenido, comprenden la información digital real para ser transmitida mientras que los paquetes de relleno comprenden información simulada no necesariamente relacionada con el contenido audio/video real. Por información digital real para ser transmitida se entiende incluir partes de programación (es decir contenido audio/video), información de sistema y/o otra información relacionada. El uso de paquetes de relleno se conoce en la industria y se describe en la solicitud de patente estadounidense con número de publicación 2003/0133446 A1, donde son usados en un entorno de red de conmutación de paquete de banda ancha para permitir la reconstrucción de un flujo de transporte sincrónico de un flujo de transporte asincrónico recibido, los paquetes de relleno sirviendo como marcadores para reservar espacio en el que se insertan los paquetes de contenido una vez que se reciben.

[0005] Ya que la transmisión de datos multimedia puede comprender contenido de valor comercial, distribuidores de tales datos multimedia, tales como operadores de televisión de pago por ejemplo, generalmente transmiten los datos en el formato encriptado. Con el objetivo de poder desencriptar los datos de una recepción final, se requiere un usuario equipado con un módulo de recepción multimedia apropiada que comprende un módulo de acceso condicional para obtener la autorización apropiada para desencriptar los datos, normalmente a través de la compra de los derechos necesarios del operador. El módulo de recepción multimedia funciona junto con un modulo de seguridad en el que los derechos son almacenados, al igual que cualquier clave de desencriptación necesaria y otra información segura de este tipo. El módulo de seguridad es normalmente desmontable y portátil y adquiere generalmente la forma de un chip alojado en uno o más dispositivos con las dimensiones de una tarjeta de crédito. La solicitud de patente estadounidense con número de publicación 2006/0176909 A1 da unos antecedentes al uso de tales módulos de seguridad en el dominio de la televisión de pago.

[0006] A pesar de las precauciones de seguridad empleadas en los sistemas de acceso condicional de hoy en día, todavía es concebible posible para un tercero interceptar una comunicación entre por ejemplo un módulo de recepción multimedia y un módulo de seguridad. Aunque la información así interceptada puede estar en el formato encriptado, puede todavía ser posible para un tercero determinado obtener conocimiento del algoritmo de encriptación y/o claves de desencriptación y podeer desencriptar la información interceptada. En la patente estadounidense con número de solicitud 2009/0172171 A1, está descrito un método para ocultar un flujo de paquetes de datos en una sesión de comunicación. Este método dificulta el trabajo de reconstrucción de la transmisión por una parte interceptora. Por ocultado, en este contexto, se hace referencia a que la sesión de comunicación tiene una o más características, incluyendo su origen o fuente, cambiado para evitar su identificación por una parte de intercepción. El uso puede estar hecho de una pluralidad de diferentes vías de comunicación para completar una única comunicación, así dificultando adicionalmente que una parte interceptora reconstruya la comunicación.

[0007] La solicitud de patente estadounidense con número de publicación 2002/154631 A1 divulga un método para transmitir un mensaje como paquetes sobre una red. Paquetes simulados se incluyen en la transmisión para confundir a un tercero potencial malicioso. Una clave de pedido se añade a los paquetes en posiciones al azar, la clave de pedido

de paquetes simulados siendo diferente de la clave de pedido de paquetes reales y permitiendo la posición de los paquetes simulados en la transmisión que debe ser predicha.

[0008] En la solicitud de patente internacional con número de publicación 99/55052 A1 se ha descrito un método para filtrar paquetes usando firmas digitales. La firma se crea por el encriptado de una huella digital correspondiente a los datos en el paquete. La validez de la firma puede por lo tanto ser evaluada y la filtración realizada basándose en el resultado de la prueba.

[0009] La solicitud de patente europea con número de publicación 2058982 A1 se refiere a una comunicación WLAN entre un transmisor y un receptor. El documento describe cómo la intercepción no autorizada de la comunicación entre el transmisor y el receptor puede volverse más difícil haciendo que parezca como si el transmisor estuviera transmitiendo cuando en realidad no lo hace.

Breve resumen de la invención

[0010] Es un objetivo de la presente invención proporcionar un método para transmitir el contenido encriptado eficazmente en un flujo de transporte, donde el flujo de transporte puede ser fácilmente ensamblado por una entidad de transmisión y fácilmente desensamblado por una entidad legítima o autorizada de recepción mientras siendo prácticamente imposible de desmontar por un dispositivo no autorizado.

[0011] Para conseguir, un método está provisto para crear un flujo de datos mejorado de un flujo de transporte que comprende una pluralidad de paquetes de datos estándar cada uno con una cabecera y una carga útil, dicho flujo de datos mejorado que comprende al menos un paquete mejorado de relleno y al menos un paquete de contenido mejorado, el paquete de relleno mejorado y el paquete del contenido mejorado cada uno con una cabecera y una carga útil mejorada, la cabecera del paquete de contenido mejorado siendo indistinguible de la cabecera del paquete de relleno mejorado, comprendiendo dicho método:
generar el paquete de relleno mejorado, los primeros b bits de la carga útil mejorada siendo una etiqueta basada en un código correspondiente a una cadena aleatoria seleccionada de un subconjunto predeterminado de códigos;
generar el paquete de contenido mejorado, la carga útil mejorada estando basada en al menos la carga útil de un paquete de datos estándar, donde sus primeros b bits comprenden una etiqueta que no se basa en un código seleccionado del subconjunto predeterminado de códigos;
y creando el flujo de datos mejorado por ensemblaje de los paquetes de relleno mejorados y los paquetes de contenido mejorados.

[0012] A la recepción de un flujo de datos ensamblado según una forma de realización de la presente invención, un método es posteriormente proporcionado para crear un flujo de transporte de un flujo de datos mejorado comprendiendo al menos un paquete de relleno mejorado y al menos un paquete de contenido mejorado, el paquete de relleno mejorado y el paquete de contenido mejorado cada uno con una cabecera y una carga útil mejorada, la cabecera del paquete de contenido mejorado siendo indistinguible de la cabecera del paquete de relleno mejorado, dicho flujo de transporte que comprende al menos un paquete de datos estándar con una cabecera y una carga útil, dicho método comprendiendo:
pruebas de los primeros b bits de cada carga útil para determinar si dijeron o no que los primeros b bits corresponden a un valor de un conjunto predeterminado de valores;
y creando el flujo de transporte por el descarte de paquetes mejorados para que dicha prueba produzca una correspondencia.

Breve descripción de los dibujos

[0013] La presente invención será mejor entendida gracias a la descripción detallada que sigue y los dibujos anexos, que se dan como ejemplos no limitativos de formas de realización de la invención, es decir:

Fig. 1 que muestra un flujo de transporte según el estado de la técnica;
Fig. 2 que muestra un flujo de transporte según una forma de realización de la presente invención;
Fig. 3 que muestra detalles del contenido de un primer tipo de paquete mejorado según una forma de realización de la presente invención;
Fig. 4 que muestra detalles del contenido de un segundo tipo de paquete mejorado según una forma de realización de la presente invención.

Descripción detallada

[0014] Una forma de realización de la presente invención se puede desplegar en un sistema que comprende un primer dispositivo electrónico y un segundo dispositivo electrónico que están conectados juntos a través de un canal de comunicación. La comunicación bidireccional puede que en un tiempo dado durante una comunicación cualquiera del primer dispositivo electrónico o el segundo dispositivo electrónico puede funcionar como un transmisor mientras que el dispositivo electrónico restante funciona como un receptor.

[0015] En tal sistema, un tercero puede intentar interceptar una transmisión hecha en el canal de comunicación, tal transmisión estando destinada a ser mantenida en secreto de un tercero. Como es práctica habitual en el ámbito de la comunicación multimedia digital, especialmente la transmisión de contenido de audio/video, donde el contenido para ser transmitido tiene valor comercial, el contenido se transmite generalmente en formato encriptado. No obstante, es todavía posible para un tercero determinado interceptar la transmisión. Un tercero puede ser capaz de desencriptar la transmisión y luego puede enviar la transmisión descifrada a otras partes no autorizadas. A modo de ejemplo, un tercero puede interceptar una transmisión entre un módulo multimedia o descodificador de señales digitales y un módulo de seguridad desmontable.

[0016] La Fig. 1 ilustra un flujo de transporte como es generalmente usado en el estado de la técnica para transmitir contenido audio/video en el formato de MPEG por ejemplo. El flujo de transporte comprende una pluralidad de paquetes de datos cada uno con una cabecera y una carga útil.

[0017] De acuerdo con una forma de realización de la presente invención, la información digital que debe ser transmitida entre una entidad de transmisión y una entidad de recepción se ensambla en la entidad de transmisión en un flujo de transporte que comprende paquetes mejorados. Un paquete mejorado que incluye una cabecera mejorada y una carga útil mejorada se muestra en la Fig. 2. La cabecera mejorada es similar a la cabecera de un paquete de contenido estándar como se ha usado generalmente en el estado de la técnica, y de hecho es diseñado de manera que un tercero no autorizado es incapaz de detectar que ésta no puede ser la cabecera de un paquete de contenido estándar. La carga útil mejorada se puede interpretar como teniendo dos partes: una etiqueta y una carga útil. La etiqueta se representa por los primeros b bits de la carga útil mejorada y la carga útil se representa por los bits restantes de la carga útil mejorada.

[0018] En otra forma de realización de la presente invención, la longitud total de un paquete mejorado es aumentada respecto a un paquete de datos estándar. En esta forma de realización la carga útil mejorada comprende un paquete de datos estándar entero introducido dentro de ésta, es decir la carga útil mejorada comprende la cabecera y la carga útil del paquete de datos estándar. En este caso, la etiqueta de la carga útil mejorada se representa por la cabecera del paquete estándar comprendida en la carga útil mejorada y la carga útil de la carga útil mejorada es toda la carga útil del paquete de datos estándar.

[0019] Aunque la cabecera mejorada de paquetes de contenido mejorados y paquetes de relleno mejorados parecen, a todos los efectos, los mismos que en una cabecera de un paquete de contenido estándar para un tercero, la estructura de estas cabeceras se pueden definir según sea necesario por la aplicación particular en la restricción dada de que parezca ser una cabecera estándar. Por lo tanto estas cabeceras pueden incluir tales indicadores como una marca de tiempo, un número de serie o un identificador de paquete por ejemplo.

[0020] Como es el caso con paquetes de datos estándar, paquetes mejorados pueden ser de dos tipos: paquetes de contenido mejorado o paquetes de relleno mejorado. Un paquete de contenido mejorado, es decir un paquete mejorado que se utiliza para comunicar un contenido válido dado, comprende una cabecera mejorada y una carga útil mejorada, donde la carga útil mejorada comprende una etiqueta (de b bits) y una carga útil, la carga útil estando basada en la carga útil de un paquete de contenido estándar destinado a comunicar el mismo contenido válido dado. Según una forma de realización de la presente invención, la etiqueta se considera que son los primeros b bits de la carga útil mejorada. Según otra forma de realización, la etiqueta se basa en la cabecera de un paquete de contenido estándar destinado a comunicar el mismo contenido válido dado. La longitud total del paquete de contenido mejorado en este caso es por lo tanto más largo que un paquete de datos estándar. Según formas de realización diferentes de la invención, la etiqueta puede ser en el formato encriptado o en el formato claro. De forma similar, la carga útil puede estar en el formato claro o encriptado. No obstante, es preferible para la etiqueta y la carga útil que ambos estén en un formato encriptado.

[0021] En el caso de que el paquete mejorado sea un paquete de relleno mejorado, la carga útil mejorada comprende una etiqueta y una carga útil. La etiqueta se basa en un código seleccionado de un subconjunto de códigos y está preferiblemente en forma encriptada aunque en algunas formas de realización ésta puede ser clara. La carga útil se puede basar en un número pseudo-aleatorio o se puede basar en una carga útil de un paquete de contenido mejorado existente. El contenido de la carga útil no es importante para un paquete de relleno mejorado ya que tales cargas útiles serán ignoradas por receptores autorizados. El punto principal es que las estructuras de paquetes de relleno mejorados y paquetes de contenido mejorados deben ser tales que no se puedan diferenciar por simple inspección.

[0022] Cabe observar a este punto que aunque el paquete mejorado de términos, paquete de contenido mejorado, cabecera mejorada, carga útil mejorada, etiqueta y carga útil se usan en toda esta descripción, en la práctica real de un sistema en el que una forma de realización de la presente invención se desarrolla un paquete mejorado puede ser exactamente el mismo que un paquete de datos estándar. Por ejemplo, podría ocurrir que un paquete de contenido mejorado tenga una cabecera mejorada que sea idéntica a una cabecera de un paquete estándar y una carga útil que sea idéntica a la carga útil de un paquete estándar. La diferencia es que nos referimos a la carga útil como una carga útil mejorada con el fin de describir la invención. De hecho, podríamos hacer referencia tanto a un paquete mejorado con una cabecera y una carga útil, de los cuales los primeros b bits son una etiqueta. En un paquete de contenido mejorado de la etiqueta más el resto de la carga útil mejorada es idéntico a la carga útil de un paquete de datos estándar equivalente que transmite el mismo contenido. En otras palabras el paquete de contenido mejorado es idéntico a un

paquete de datos estándar equivalente. El paquete de relleno mejorado tendrá una cabecera similar al paquete de datos estándar, una etiqueta que se crea en la entidad de transmisión y el resto de la carga útil mejorada ya sea al azar o con datos copiados.

[0023] Según la invención, los paquetes mejorados son fáciles de construir para una entidad de transmisión. Además es fácil para una entidad de recepción válida, o autorizada, detectar que los paquetes mejorados son paquetes de contenido mejorados y los cuales son paquetes de relleno mejorados. Es por lo tanto fácil para la entidad de recepción autorizada descartar eficazmente los paquetes de relleno mejorados, incluso cuando los paquetes de relleno mejorados aparecen en posiciones imprevisibles entre el contenido de paquetes mejorados en el flujo de transporte. No obstante, es prácticamente irrealizable para una entidad de recepción no autorizada decir la diferencia entre los paquetes de contenido mejorados y los paquetes de relleno mejorados y así no perder en una tentativa lo que podrían ser datos importantes, un tercero está obligado a intentar tratar todos los paquetes mejorados, perdiendo así tiempo de procesamiento. Además, aunque un tercero fuera a idear un medio para el procesamiento de todos los datos transmitidos, éste todavía no sería capaz de reconstruir el contenido útil.

[0024] Obteniendo ventaja de la oportunidad ofrecida por la capacidad de construir de manera eficiente paquetes de relleno mejorados y paquetes de contenido mejorados por una entidad de transmisión y la capacidad de una entidad de recepción para reconocer de manera eficiente tales paquetes, un número muy grande de paquetes de relleno mejorados se pueden incluir en un flujo de transporte en posiciones imprevisibles entre los paquetes de contenido mejorados. De hecho, según la invención, el flujo de transporte se transmite a través del canal de datos a un índice de transmisión que es en gran medida aumentado con respecto a los índices de transmisión estándares usados en los protocolos de transmisión generalmente aceptados en la industria, tal como un formato MPEG usado dentro de una red IP por ejemplo. Típicamente, una transmisión de contenido audio/video en el formato MPEG entre dos componentes de un sistema de acceso condicional, por ejemplo, sería hecho a un índice de 30-40 megabits por segundo. En un sistema en el que una forma de realización de la presente invención es desplegada, tal comunicación puede ser hecha a un índice de 500 megabits por segundo por ejemplo. De esta manera, es posible un uso máximo del ancho de banda disponible, usando paquetes de relleno mejorados para ocupar el ancho de banda. Como se ha mencionado previamente, los paquetes mejorados de relleno son muy difíciles de reconocer por una entidad de recepción no autorizada o espía y por lo tanto un espía potencial es conducido a intentar interceptar y procesar la integridad del flujo de transporte puesto que es incapaz de detectar y rechazar paquetes de relleno. Para ello será capaz de interceptar la búsqueda de una gran cantidad de datos, debe recurrir al uso de un dispositivo de intercepción de hardware dedicado en lugar de un dispositivo estándar tal como un ordenador personal por ejemplo. Además, aunque el espía lograra procesar todos los datos interceptados, no sería capaz de establecer un sentido de éste.

[0025] Según una forma de realización preferida de la presente invención, un contenido de paquete mejorado de longitud de bit l comprende una cabecera mejorada de n bits y una carga útil mejorada de l menos n bits. La cabecera mejorada está en un formato claro. La carga útil mejorada comprende dos partes: una etiqueta y una carga útil. La etiqueta tiene una longitud de b bits y está preferiblemente en el formato encriptado. Dado que la carga útil mejorada, comprendiendo la etiqueta y la carga útil, tiene una longitud de bit l menos n bits, la carga útil por lo tanto tiene una longitud de bit l menos n menos b bits. La carga útil está preferiblemente en el formato encriptado y comprende el contenido que debe ser transmitido. Según una forma de realización de la presente invención la etiqueta se basa en la cabecera de un paquete de datos estándar que comunicaría el mismo contenido que debe ser transmitido. En otra forma de realización de la etiqueta de b bits se basa en los primeros b bits de la carga útil de un paquete de datos estándar que comunicaría el mismo contenido que debe ser transmitido.

[0026] Un paquete de relleno mejorado, también de la longitud de bits de l bits, tiene una cabecera mejorada de n bits, que está también en formato claro, y una carga útil mejorada de l menos n bits. La carga útil mejorada también comprende una etiqueta, preferiblemente en el formato encriptado, de la longitud de bits de b bits, no obstante en este caso, la carga útil de l menos n menos b bits está preferiblemente basada en un número pseudoaleatorio o se puede basar en cualquier otro dato ya que será ignorada por receptores autorizados. La estructura del paquete de relleno mejorado es la misma que la estructura del paquete de contenido mejorado.

[0027] La creación de un paquete de relleno mejorado, según una forma de realización de la presente invención puede ser descrita en dos partes. En primer lugar está la preparación de la etiqueta y luego hay una encriptación. Para la preparación de la etiqueta, la entidad de transmisión tiene conocimiento de un algoritmo eficiente probabilístico, la muestra (), que devuelve una cadena aleatoria de un subconjunto predeterminado, S, de cadenas de datos digitales. La entidad de recepción tiene conocimiento de un algoritmo eficiente, de prueba (x), que devuelve (con una probabilidad alta) un valor de 1 si x es un elemento del subconjunto S y devuelve un 0 si x no es un elemento del subconjunto S. En otras palabras, la entidad de transmisión puede seleccionar un código de un subconjunto predeterminado de códigos, que una entidad de recepción autorizada puede probar para determinar si el código vino del subconjunto predeterminado o no.

[0028] Si un código se evalúa o no como perteneciente al subconjunto predeterminado indica si el paquete mejorado asociado debería ser descartado o no. Tales algoritmos se relacionan con el dominio de prueba de propiedad combinatoria. Aplicaciones de ello han sido realizadas en los campos de teoría del aprendizaje, teoría de codificación y teoría de la complejidad, como se describe por Avrim Blum, Adam Kalai, Hal Wasserman en "Noise-tolerant Learning,

the Parity Problem, and the Statistical Query Model" en Journal of the ACM 50(4): 506-519, 2003, y por Dana RON en "Handbook on Randomization, Volume II, 2001, Property Testing". Un simple ejemplo de un subconjunto adecuado S es un código lineal aleatorio de longitud b y rango estrictamente menor que b, donde las palabras de código tienen por lo menos B errores para algunos B fijos. Para una buena elección de B, la entidad de recepción eficiente puede poner a prueba si la palabra recibida pertenece a S, por ejemplo usando ecuaciones de control de paridad. Esta tarea es irrealizable por un tercero que no conoce S, como se muestra en "On Lattices, Learning with Errors, Random Linear Codes , and Cryptography" por Oded Regev en el Symposium on Theory of Computing, 2005, en páginas 84-93.

[0029] El tipo de código anteriormente descrito es conveniente para la presente invención en el sentido de que la aplicación de los algoritmos Muestra () y Prueba (x) sean convenientes y eficaces. La parte de encriptación requiere que la entidad de transmisión y la entidad de recepción autorizada en ambos tengan un conocimiento de proporción de una clave secreta (K) de k bits de longitud (es decir, una cadena de bits secreta de k bits) y un conocimiento de un cifrado por bloques (o algoritmo criptográfico) usando bloques de b bits de datos y una clave de k bits. Los dos algoritmos Muestra () y Prueba (x) y la descripción del subconjunto S se mantienen en secreto de terceras personas nos autorizadas. No obstante, la elección del cifrado por bloques no tiene que ser mantenida en secreto: si un tercero no autorizado llegara a tener conocimiento del cifrado del bloque o la clave de k bits, entoneces gracias a la invención, la seguridad de la transmisión no se vería comprometida.

[0030] Los paquetes de relleno mejorados se crean por la entidad de transmisión. La Fig. 3 muestra una ilustración de un paquete de relleno mejorado. La cabecera mejorada es construida de manera que esta parece la cabecera de un paquete de contenido estándar. Por ejemplo, la cabecera podría ser idéntica a la cabecera de un contenido de paquete mejorado previamente transmitido. Los detalles reales de la construcción de una cabecera dependen de la especificación de una cabecera legítima según el sistema en cuestión. El punto principal es que la cabecera no debe dar ninguna indicación en cuanto a si la carga útil mejorada comprende información de contenido o información de relleno. En un flujo de transporte que comprende paquetes mejorados de relleno a continuación, ya que las cabeceras de estos paquetes son copiados a partir de paquetes de contenido mejorados, es posible que muchos paquetes existan con cabeceras idénticas. Para no permitir que un tercero adivine donde está el paquete de contenido mejorado en la pluralidad de paquetes con cabeceras idénticas, es conveniente ajustar el orden de los paquetes por variar de manera que el paquete de contenido mejorado no aparezca sistemáticamente en la misma posición en la pluralidad de paquetes.

[0031] La carga útil mejorada de un paquete mejorado de relleno se construye en cuatro pasos:
- la función de la muestra () es llamada para determinar un valor x de b bits de longitud;
- el valor de x se cifra mediante el cifrado por bloques en la clave (K), dando (Enc_K (x));
- los primeros b bits de la carga útil mejorada se fijan en el valor encriptado de x (en otras palabras la etiqueta se fija en (Enc_K (x));
- el l menos n menos b bits restantes de la carga útil mejorada se fijan a un valor pseudoaleatorio

[0032] Los paquetes de contenido mejorados son también creados por la entidad de transmisión. Un paquete de contenido mejorado se ilustra en la Fig. 4. La cabecera se construye de la misma manera que el anterior. La carga útil mejorada de un paquete de contenido mejorado está en realidad basada en un paquete de datos de contenido estándar correspondiente, incluyendo su cabecera y su carga útil. La etiqueta, es decir los primeros b bits, se generan mediante el encriptado de los b bits del paquete de contenido estándar correspondiente que utiliza el cifrado por bloques y la clave de k bits. Los restantes l menos n menos b bits de la carga útil mejorada también se pueden generar por el encriptado de la carga útil que utiliza el cifrado por bloques y la clave de k bits. La encriptación se puede realizar mediante el uso del cifrado en el modo CBC (bloque de cifrado encadenado).

[0033] A la recepción de un paquete, la entidad de recepción desencripta la etiqueta del paquete mejorado, es decir los primeros b bits de la carga útil mejorada, utilizando el cifrado por bloques (es decir, Enc_k^{-1} (b)). La entidad de recepción luego aplica el algoritmo Prueba (x) en la etiqueta desencriptada. Si el resultado obtenido es 1, entonces el paquete mejorado es reconocido como un paquete mejorado de relleno y el paquete es descartado. Si el resultado es 0, entonces el paquete es reconocido como un paquete de contenido mejorado y la carga útil es desencriptada utilizando el cifrado por bloques. Un flujo de transporte encriptado se descifra cuando los paquetes de contenido mejorados comprendidos en éste son desencriptados y ensamblados para formar un flujo de transporte desencriptado.

[0034] Ejemplos de parámetros que se pueden usar en una forma de realización preferida de la presente invención para dar una probabilidad suficientemente alta de detectar correctamente paquetes de relleno por una entidad de recepción autorizada son los siguientes:
Longitud de paquete, l = 1536 bits;
Longitud de cabecera, n = 64 bits;
Longitud de bloque (Longitud de etiqueta), b = 128 bits;
Carga útil de paquetes de relleno mejorados: valor pseudoaleatorio;
Cifrado por bloques: AES-128 (estándar de encriptación avanzada) (es decir, con b=k=128) usado en modo de CBC;
Subconjunto, S: palabra en clave de 128 bits de longitud de un código lineal de dimensión 64 con un número limitado de errores; reconocimiento basado en la detección de que el número de errores está por debajo del límite.

[0035] Con la úlima opción de subconjunto comprobable y demostrable de forma eficiente, S, el problema de reconocimiento de paquetes de relleno mejorados para un espía que conoce el cifrado por bloques y la clave está relacionado con el problema informático del aprendizaje con errores (LWE), que se describe en el informe "On Lattices, learning with errors, random linear codes" por Oded Regev en el Symposium on Theory of Computing, 2005, en páginas 84-93.

[0036] En otra forma de realización de la presente invención, en vez de usar los algoritmos Muestra () y Prueba (x), la entidad de transmisión genera una lista de códigos que se consideran útiles como marcadores en cuanto a que la probabilidad de que tales códigos aparezcan como una etiqueta en un paquete de contenido mejorado es insignificantemente pequeña. En esta forma de realización, la entidad de transmisión comunica su lista de códigos a las entidades de recepción autorizadas. La entidad de transmisión luego selecciona códigos de la lista generada, encripta los códigos y usa los códigos encriptados como etiquetas para marcar paquetes de relleno mejorados antes de incluirlos en una transmisión. Dado que las entidades de recepción autorizadas tienen conocimiento de las claves de cifrado actualmente válidas, se pueden generar en un momento dado una lista válida de etiquetas cifradas y, por simple comparación de las etiquetas encriptadas entrantes recibidas, pueden detectar de manera eficiente y rechazar paquetes de relleno mejorados.

[0037] Diferentes métodos pueden ser utilizados para reducir al mínimo la probabilidad de que uno o más de los códigos seleccionados para generar etiquetas coincidentes con un código que en realidad puede aparecer en los primeros b bits de una carga útil. Por ejemplo, se podría determinar que los primeros b bits de una carga útil sólo cubren un cierto rango, en cuyo caso los códigos utilizados para la etiqueta vendrían desde el exterior de este rango. No obstante, todavía puede ser posible que se produzca una colisión, una colisión significa un caso en que los primeros b bits de una carga útil son iguales a uno de los valores seleccionados para ser utilizables para generar una etiqueta. Si existe una carga útil de este tipo, entonces la entidad de recepción rechazará erróneamente el paquete como un paquete de relleno. Según una forma de realización alternativa de la presente invención, la entidad de transmisión es capaz de predecir una colisión por una comparación sistemática de los primeros b bits de todas las cargas útiles con todos los elementos del subconjunto de códigos usados para generar etiquetas. La información estadística se puede mantener relacionada con el número de colisiones así encontradas con el propósito de mejorar continuamente la calidad del conjunto de códigos usados para crear etiquetas. Si la longitud b se selecciona para que sea suficientemente grande, entonces la probabilidad de que tales colisiones aparezcan es muy pequeña y la consecuencia de que una entidad de recepción rechace un paquete insignificante, no obstante con tal mecanismo de predicción desplegado en el sistema son posibles mejoras constantes en la calidad del subconjunto de etiqueta. En lugar de limitarse tan solo a proporcionar estadísticas, el subconjunto de los códigos podría simplemente ser actualizado de forma continua mediante la eliminación de cada código que se ha detectado que ha causado una colisión.

REIVINDICACIONES

1. Método para crear un flujo de datos mejorado de un flujo de transporte que comprende una pluralidad de paquetes de datos estándar cada uno con una cabecera y una carga útil, dicho flujo de datos mejorado comprendiendo al menos un paquete de relleno mejorado y al menos un paquete de contenido mejorado, el paquete de relleno mejorado y el paquete de contenido mejorado cada uno con una cabecera y una carga útil mejorada, la cabecera del paquete de contenido mejorado siendo indistinguible de la cabecera del paquete de relleno mejorado, dicho método comprendiendo:
generación del paquete de relleno mejorado, los primeros b bits de la carga útil mejorada siendo una etiqueta basada en un código correspondiente a una cadena aleatoria seleccionada de un subconjunto predeterminado de códigos;
generación del paquete de contenido mejorado, la carga útil mejorada estando basada en al menos la carga útil de un paquete de datos estándar, donde sus primeros b bits es una etiqueta que no se basa en un código seleccionado del subconjunto predeterminado de códigos;
y creación del flujo de datos mejorado por ensamblaje de paquetes de relleno mejorados y el paquete de contenido mejorado.

2. Método según la reivindicación 1, donde la etiqueta del paquete de contenido mejorado se basa en la cabecera de la pluralidad de paquetes de datos estándar.

3. Método según cualquiera de las reivindicaciones 1 o 2, donde todos o parte del flujo de datos mejorado es encriptado utilizando una clave.

4. Método según cualquiera de las reivindicaciones 1 a 3, donde dicho paquete de relleno mejorado es incluido en las posiciones aleatorias en el flujo de datos mejorado.

5. Método según cualquiera de las reivindicaciones 1 a 4, donde dichos paquetes de relleno mejorados sustancialmente exceden en número sobre dichos paquetes de contenido mejorados.

6. Método según cualquiera de las reivindicaciones 1 a 5, donde el subconjunto predeterminado de códigos es actualizado, dicho método comprendiendo:
comparación del valor de la etiqueta con una parte de las cargas útiles de los paquetes de datos estándar;
y eliminación del valor del subconjunto predeterminado de códigos.

7. Método según cualquiera de las reivindicaciones 1 a 6, donde se hace un uso máximo del ancho de banda disponible, con paquetes de relleno mejorados que se usan para ocupar el ancho de banda disponible.

8. Método según cualquiera de las reivindicaciones 1 a 7, donde el flujo de transporte comprende el contenido multimedia digital.

9. Método para crear un flujo de transporte de un flujo de datos mejorado, el flujo de datos mejorado comprendiendo al menos un paquete de relleno mejorado y al menos un paquete de contenido mejorado, el paquete de relleno mejorado y el contenido de paquete mejorado cada uno con una cabecera y una carga útil mejorada, la cabecera del paquete de contenido mejorado siendo indistinguible de la cabecera del paquete de relleno mejorado, dicho flujo de transporte que comprende al menos un paquete de datos estándar con una cabecera y una carga útil, dicho método comprendiendo:
prueba de los primeros b bits de la carga útil mejorada para determinar si dichos primeros b bits corresponden o no a un valor de un subconjunto predeterminado de códigos;
y creación del flujo de transporte por el descarte de paquetes mejorados para que dicha prueba produzca una correspondencia.

10. Método según la reivindicación 9, donde los primeosr b bits de la carga útil mejorada es encriptada bajo una clave, dicho método comprendiendo además el desciframiento de los primeros b bits que utilizan la clave antes de la prueba.

11. Entidad de transmisión para la construcción de paquetes de relleno mejorados y paquetes de contenido mejorados comprendidos en un flujo de datos mejorados, dicha construcción basada en un flujo de transporte que comprende al menos un paquete de datos estándar con una cabecera y una carga útil, dicho paquete de relleno mejorado y dicho paquete de contenido mejorado cada uno con una cabecera y una carga útil mejorada, la cabecera del paquete de contenido mejorado siendo indistinguible de la cabecera del paquete de relleno mejorado, dicha entidad de transmisión **caracterizada por el hecho de que** es configurada:
para generar el paquete de relleno mejorado con una etiqueta basada en un código correspondiente a una cadena aleatoria seleccionada de un subconjunto predeterminado de códigos, la etiqueta siendo los primeros b bits de la carga útil mejorada del paquete de relleno mejorado;
para generar el paquete de contenido mejorado con una etiqueta que no se basa en un código seleccionado del subconjunto predeterminado de códigos, la etiqueta que siendo el primer b bits de la carga útil mejorada del paquete de contenido mejorado, la carga útil mejorada del paquete de contenido mejorado estando además basada en al menos la carga útil de una de la pluralidad de paquetes de datos estándar.

12. Entidad de recepción para detectar y descartar paquetes de relleno mejorados dentro de un flujo de datos mejorado para producir un flujo de transporte, el flujo de datos mejorado comprendiendo al menos un paquete de relleno mejorado y al menos un paquete de contenido mejorado, el paquete de relleno mejorado y el paquete de contenido mejorado cada uno con una cabecera y una carga útil mejorada, la cabecera del paquete de contenido mejorado siendo indistinguible de la cabecera del paquete de relleno mejorado, dicho flujo de transporte comprendiendo al menos un paquete de datos estándar con una cabecera y una carga útil, dicha entidad de recepción **caracterizada por el hecho de que** está configurada:
para poner a prueba los primeros b bits de la carga útil mejorada para determinar si corresponden o no los primeros b bits a un valor de un subconjunto predeterminado de códigos;
para crear el flujo de transporte por el descarte de paquetes mejorados para el cual dicha prueba produce una correspondencia.

13. Sistema para la comunicación de contenido multimedia digital, el sistema caracterizado por el hecho de que comprende:
la entidad de transmisión según la reivindicación 11;
y la entidad de recepción según la reivindicación 12;
la entidad de transmisión y la entidad de recepción estando configuradas para ejecutar dicha comunicación de contenido multimedia digital a través de un canal de datos.

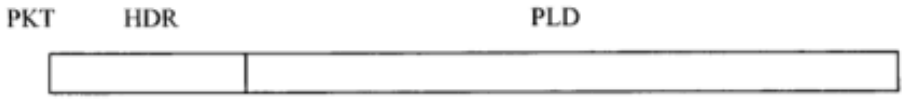

Fig. 1

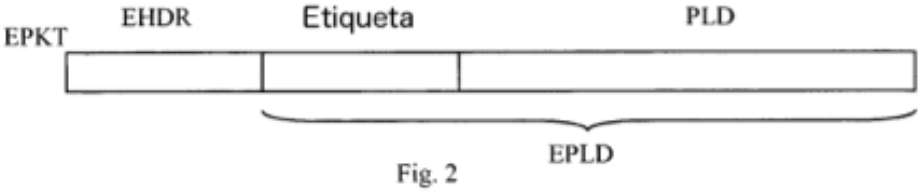

Fig. 2

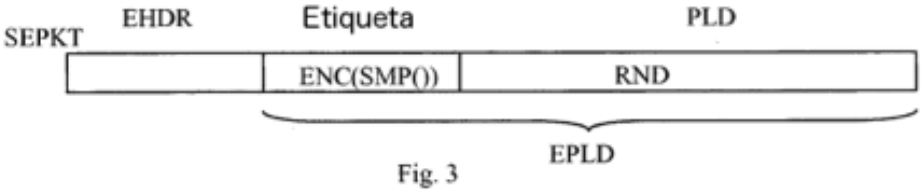

Fig. 3

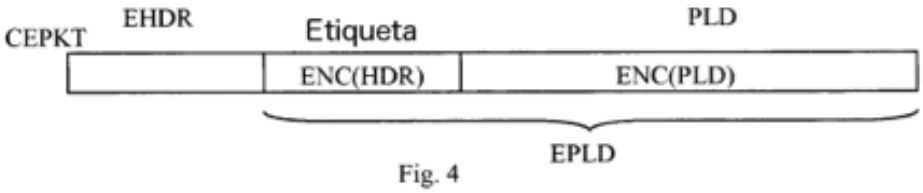

Fig. 4