(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 313 560**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04N 7/167 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06114977 .9**
(96) Fecha de presentación : **10.12.2001**
(97) Número de publicación de la solicitud: **1694028**
(97) Fecha de publicación de la solicitud: **23.08.2006**

(54) Título: **Paquetes RTP con punteros no cifrados en lugares de control para tramas.**

(30) Prioridad: **18.12.2000 EP 00204639**

(45) Fecha de publicación de la mención BOPI:
01.03.2009

(45) Fecha de la publicación del folleto de la patente:
01.03.2009

(73) Titular/es: **Irdeto Eindhoven B.V.**
Jupiterstraat 42
2132 HD Hoofddorp, NL

(72) Inventor/es: **Van Rijnsoever, Bartholomeus, J.**

(74) Agente: **Durán Moya, Carlos**

DESCRIPCIÓN

Paquetes RTP con punteros no cifrados en lugares de control para tramas.

Un método para transmitir continuamente datos formateados en tramas en paquetes, que comprende una etapa de cifrado antes de transmitir continuamente dichos datos, y un método de recepción, un sistema, un servidor de transmisión continua, un aparato receptor y una señal generada mediante dicho servidor de transmisión continua para utilizarse con dicho método.

La invención se refiere a un sistema como el descrito en el preámbulo de la reivindicación 1. Los datos, y en particular los datos multimedia, sin que ello sirva de limitación, actualmente se cifran para implementar entre otras cosas diversos esquemas de acceso condicional para permitir a los creadores y distribuidores del material original cobrar una cantidad apropiada de retribuciones de los usuarios por dicha información. En el receptor, los datos de usuario se deben recuperar para poder, de forma adecuada, representarlos, visualizarlos, escucharlos, ejecutarlos y realizar otras operaciones asociadas con el usuario. La transmisión real a través de algún medio de transmisión, como por ejemplo una red, tendrá lugar en un nivel de paquetes, en donde los paquetes se estandarizan para la red o redes en cuestión.

Un primer enfoque consiste en realizar el cifrado basándose en un paquete de transmisión mediante un protocolo en tiempo real, que es un procedimiento relativamente sencillo y es correcto para proteger la transmisión propiamente dicha, dicho cifrado se describe en el documento WO 99/37056. Alternativamente, se puede conseguir un nivel de protección superior que también se mantendrá vigente en el lado del receptor: esto se puede realizar implementando el cifrado basándose en la estructura de tramas de los datos de origen o de los datos de usuario. También es factible implementar una combinación de los dos enfoques anteriores. No obstante, el cifrado se debería ejecutar de manera ventajosa en un componente estándar que no necesite realizar un procesamiento previo complicado para encontrar el inicio de una trama. Por lo tanto, todos los procedimientos anteriores necesitarán un mecanismo sencillo para encontrar de manera directa el inicio de las tramas.

En consecuencia, entre otras cosas, un objetivo de la presente invención es añadir información de localización específica para que el mecanismo del codificador y, posiblemente, también el mecanismo del decodificador puedan encontrar rápida y fácilmente el inicio de las diversas tramas.

Por lo tanto, según uno de sus aspectos la invención se caracteriza según la parte caracterizadora de la reivindicación 1.

Además de lo anterior, el presente inventor ha descubierto que una leve modificación de lo anterior puede permitir que se cifre eficazmente sólo una parte de los datos de usuario, mientras que simultáneamente posibilita la localización inmediata de dichas partes cifradas, tal y como se ha descrito en la reivindicación 2. La invención también se refiere a un método para recibir un flujo continuo de datos creado con el método reivindicado en la reivindicación 1, a un sistema dispuesto para implementar el método reivindicado en la reivindicación 1, a un aparato transmisor y a un aparato receptor para utilizarse en dicho sistema y a una señal generada por dicho aparato transmisor. Otros aspectos ventajosos de la invención se describen en las reivindicaciones dependientes.

Estos y otros aspectos y ventajas de la invención se describirán con más detalle en adelante haciendo referencia a la descripción de las realizaciones preferentes, y en concreto haciendo referencia a las figuras adjuntas, que muestran:

la figura 1, un sistema dispuesto para implementar el método de la invención;

la figura 2, una implementación del formato de datos para utilizarse en la presente invención;

la figura 3, un formato modificado con respecto a la figura 2 que tiene un cifrado parcial.

Se ha mejorado la calidad de información de contenidos, como por ejemplo audio o vídeo en Internet, debido a los continuos avances en tecnología de codificación y en ancho de banda de transmisión. Los proveedores de contenidos se proponen vender dichos contenidos de alto valor, y, por lo tanto, surge la necesidad de llevar a cabo un acceso condicional o, como se le denomina, una gestión de derechos digitales. Dicho sistema de acceso condicional cifrará un elemento de contenidos y a continuación gestionará las claves de descrifrado asociadas de tal modo que sólo los usuarios finales autorizados podrán descifrar y por lo tanto reconstituir completamente los contenidos originales.

En la actualidad, los datos multimedia se estructuran generalmente en tramas, en las que el tamaño de una trama está relacionado con la categoría de la información. Además, el tamaño de una trama transmitida puede estar relacionado con el grado de compresión y otros procesamientos a los que haya estado sujeta antes del cifrado. De hecho, las tramas pueden ser más grandes o más pequeñas que los paquetes utilizados para la transmisión real. Por lo tanto, un único paquete de transmisión puede contener una o más tramas, o fracciones de una trama. La transmisión continua es una tecnología en la que un cliente reproducirá o utilizará de otro modo los contenidos tan pronto como lleguen, de manera que no se realizará la descarga de la totalidad, o de una parte sustancial de los contenidos completos, antes de reproducirlos. La transmisión continua no permite la retransmisión de paquetes. El usuario de los contenidos tendrá que tener en cuenta los datos que se han perdido.

No obstante, para una protección óptima, los contenidos se cifran mejor en el nivel de trama, incluso con un tamaño de trama no uniforme. Dicho cifrado en el nivel de trama permitirá un cifrado persistente o extremo a extremo que se aplica tanto al contenido transmitido como al almacenado. Preferiblemente, el componente del sistema que implementa el cifrado real es un componente genérico, y por lo tanto debería ser independiente de servidores de transmisión continua específicos e independiente de formatos de trama específicos. Una forma de conseguirlo es definir el componente de cifrado como un protocolo de transmisión en tiempo real o traductor RTP. En la actualidad, prácticamente todos los servidores de transmisión continua utilizan el protocolo de transmisión continua RTP. Por lo tanto, el componente de cifrado podría recibir los paquetes RTP, cifrar la carga útil y, a continuación, enviar los paquetes RTP cifrados. Alternativamente, el cifrado podría integrarse con el servidor de transmisión continua.

Alternativamente, el cifrado podría ejecutarse en el nivel del paquete RTP. Esto protegerá la transmisión propiamente dicha, mientras que se renunciará a parte de la protección en el receptor tras la recepción. También es factible una combinación de estos dos enfoques para el cifrado, como por ejemplo asignar el nivel de cifrado apropiado basándose en una estrategia de contingencia con respecto a las utilidades de hardware disponibles.

Se plantea un problema con el hecho de que las cabeceras de las tramas deben permanecer sin cifrar, como por ejemplo cuando el cifrado se realiza en el nivel de trama. Esto requiere que el componente de cifrado genérico analice la carga útil de los paquetes RTP para identificar las posiciones de las cabeceras de las tramas. Sin embargo, esto disminuiría el rendimiento del componente de cifrado, y también haría depender el componente de cifrado de los formatos de trama reales.

La presente invención da a conocer una solución para el problema en cuestión ampliando las cabeceras de los paquetes RTP para incluir punteros a dichas partes de la carga útil del paquete RTP que realmente necesitan cifrarse. El servidor de transmisión continua establece los punteros. El servidor puede llevar a cabo esta operación como parte del denominado proceso de sugerencias, que es un análisis fuera de línea de los datos multimedia, para que los datos puedan transmitirse continuamente de manera más eficaz más adelante. El resultado del proceso de indicaciones se almacena en paralelo con los contenidos en la denominada pista de sugerencias.

La figura 1 muestra un sistema dispuesto para implementar el método de la invención. La entrada (23) recibe las tramas de datos de usuario, que se almacenan temporalmente en el dispositivo de almacenamiento (22), el cual tiene capacidad para almacenar una serie de dichas tramas. El bloque de procesamiento (24) añade inmediatamente en estas tramas de datos informaciones de localización de cabecera de trama en el contexto de un paquete RTP que puede incluir una serie de dichas tramas de usuario, pero no necesariamente un número entero de las mismas. El resultado de este procesamiento se almacena temporalmente en el bloque (26), que tiene capacidad para varias cargas útiles RTP. A efectos de brevedad, la pista de sugerencias específica mencionada anteriormente no se ha mostrado por separado. De hecho, el medio de pista de sugerencias será considerado por los expertos en la técnica como un medio estándar. En la práctica, dicha pista de sugerencias se implementará en la entrada del bloque (23) para que pueda indicar las diferentes ubicaciones de tramas. Antes de la transmisión, los datos de usuario se cifran en el módulo de cifrado (28) y se transmiten a través del medio de comunicación (30), como por ejemplo Internet. Todo el procedimiento en el transmisor del sistema mostrado se puede sincronizar mediante el dispositivo de sincronización general (20) tal y como indican las líneas de trazos que proceden del mismo.

En el lado de recepción, el descifrado se realiza a través del dispositivo de descifrado (34), y el resultado del mismo se almacena temporalmente en el bloque (36). La reconstrucción de las tramas de usuario se realiza en el dispositivo de procesamiento (38), seguido por el almacenamiento temporal en el bloque (40). A continuación, la aplicación de usuario se simboliza mediante el bloque (42). Los bloques de almacenamiento (36), (40) no admiten la descarga de un programa completo o de una parte sustancial del mismo, sino que facilitarán la sincronización para tener en cuenta las variaciones de velocidad de transferencia del dispositivo de comunicación (30). De nuevo, en el receptor, la sincronización general se realiza a través del bloque sincronizador (32).

La figura 2 muestra una implementación de un formato de datos a título de ejemplo para utilizarse en la presente invención. A efectos de brevedad, sólo se ha mostrado una única implementación. Los diversos bloques de datos (50) a (60) de la configuración RTP se muestran en la figura. De ellos, los bloques (54) a (60) constituyen la carga útil RTP, donde los bloques (56), (60) contienen cada uno una carga útil de trama cifrada, y los bloques (54), (58) contienen las cabeceras de tramas asociadas. Se debe observar que las longitudes de los bloques (56), (60) no tienen porque ser uniformes. El bloque (50) contiene una cabecera RTP, y es seguido por el bloque (52) que contiene punteros. Tal y como se muestra en la figura, los punteros (62) indican tanto el inicio como el final de la carga útil de cada trama cifrada. En este caso, la cabecera (50) se encuentra en la pista de sugerencias; los punteros (52) son extensiones de la cabecera RTP (50). Esta pista de sugerencias se utiliza por el servidor de transmisión continua para empaquetar los paquetes RTP.

La figura 3 muestra un formato modificado con respecto a la figura 2 que tiene un cifrado parcial de los datos de usuario. A efectos de brevedad, sólo se han indicado específicamente los aspectos diferentes con respecto a la figura 2. Dentro de la carga útil de la trama, la distinción entre los datos de usuario cifrados (E) y no cifrados se ha indicado mediante una línea inclinada. La información de localización indicada por (62) en este caso ahora indicará específicamente (-63-, -65-) los extremos de las respectivas partes cifradas, suponiendo que el cifrado comienza desde el inicio de los datos de usuario de la trama. Por supuesto, se pueden utilizar otros cifrados parciales. El propio cifrado

se puede realizar en el nivel de una trama o de una trama parcial, en el nivel de un paquete o puede basarse en una combinación de los mismos.

La invención se puede realizar mediante un primer método para transmitir o retransmitir en tiempo real datos de usuario formateados en tramas mientras que se lleva a cabo en los mismos el procedimiento de cifrado antes de dicha (re)transmisión,

estando dicho método caracterizado por la fase de, asociada a someter dichos datos de usuario a dicho procedimiento de cifrado, añadir a dichos datos de usuario datos de localización de trama apropiados y colocar dichos datos de localización de trama en lugares de control predeterminados que, igual que las informaciones de cabecera, se excluyen de dicho procedimiento de cifrado posterior.

La invención se puede realizar mediante un segundo método, que está realizado como en el primer método, aunque sólo se somete una parte de dichos datos de usuario a dicho procedimiento de cifrado mientras que se facilitan datos de localización de cifrado en dichos lugares de control para distinguir entre partes cifradas y sin cifrar de dichos datos de usuario.

La invención se puede realizar mediante un tercer método, que está realizado como en el primer o el segundo método, en el que dichos lugares de control son lugares de información de extensión de cabecera.

La invención se puede realizar mediante un cuarto método, que está realizado como en el primer o el segundo método, en el que dichos datos de usuario tras el cifrado se transmiten en paquetes RTP, y en el que dichos datos de usuario se cifran en el nivel de dicho paquete RTP.

La invención se puede realizar mediante un quinto método, que está realizado como en el primer o el segundo método, en el que dichos datos de usuario se cifran en el nivel de trama.

La invención se puede realizar mediante un sexto método, que está realizado como en el cuarto o el quinto método, en el que dicha transmisión permite atribuir tramas parciales a un paquete, así como permite atribuir varias tramas a un único paquete.

La invención se puede realizar mediante un séptimo método, que está realizado como en el tercer método, en el que dicho lugar de información de extensión de cabecera tiene una serie de datos de localización de trama.

La invención se puede realizar mediante un octavo método, que está realizado como en el primer o el segundo método, en el que dichos lugares de control se colocan dentro de una pista de sugerencias independiente.

La invención se puede realizar mediante un primer sistema dispuesto para implementar el primer método y que dispone de medios de transmisión para transmitir o retransmitir en tiempo real datos de usuario formateados en tramas y de medios de cifrado para llevar a cabo un procedimiento de cifrado basado en dichos datos de usuario antes de dicha (re)transmisión,

estando dicho sistema caracterizado por incluir junto a dichos medios de cifrado medios de adición para añadir a dichos datos de usuario datos de localización de trama y colocar dichos datos de localización de trama en lugares de control predeterminados, que, igual que la información de las cabeceras, se excluyen de dicho cifrado posterior.

La invención se puede realizar mediante un segundo sistema realizado igual que el primer sistema y dispuesto para interconectarse a Internet como medio de transmisión.

La invención se puede realizar mediante un primer aparato transmisor dispuesto para utilizarse como una estación en el primer sistema.

La invención se puede realizar mediante una primera señal generada por el primer aparato transmisor.

La invención se puede realizar mediante un primer aparato receptor dispuesto para utilizarse como una estación en el primer sistema y que dispone de medios de descifrado para descifrar, tras la recepción, datos de usuario que han sido sometidos a dicho procedimiento de cifrado para dar salida a datos de usuario descifrados basándose en tramas que contienen dichos datos de usuario.

La invención se puede realizar mediante un segundo aparato receptor realizado igual que el primer aparato receptor, en el que dichos medios de descifrado están operativos en el nivel de trama.

La invención se puede realizar mediante un tercer aparato receptor realizado igual que el primer aparato receptor, en el que dichos medios de descifrado están operativos en el nivel de paquete.

REIVINDICACIONES

1. Método para transmitir continuamente datos formateados en tramas en paquetes, que incluye una etapa de cifrado antes de transmitir continuamente dichos datos,

estando dicho método **caracterizado** por la etapa de, asociado a la etapa de cifrado, añadir a dichos datos datos apropiados de localización de trama y colocar dichos datos de localización de trama en los paquetes en lugares de control que, igual que la información de las cabeceras, están excluidas de dicha etapa de cifrado posterior.

2. Método, según la reivindicación 1, en el que sólo se somete una parte de dichos datos formateados en tramas a dicha etapa de cifrado, mientras que se facilitan datos de localización de cifrado en dichos lugares de control para distinguir entre partes cifradas y sin cifrar de dichos datos formateados en tramas.

3. Método, según la reivindicación 1, en el que dichos datos de localización de trama incluyen una indicación de la longitud de las tramas.

4. Método, según las reivindicaciones 1, 2 ó 3, en el que dichos lugares de control están en las cabeceras extendidas.

5. Método, según la reivindicación 4, en el que dicha cabecera extendida tiene una serie de datos de localización de trama.

6. Método, según las reivindicaciones 4 ó 5, en el que las cabeceras extendidas se asocian a los paquetes.

7. Método, según las reivindicaciones 4 ó 5, en el que las cabeceras extendidas se asocian a las tramas.

8. Método, según cualquiera de las reivindicaciones anteriores, en el que dicha transmisión permite atribuir tramas parciales a un paquete, así como permite atribuir una serie de tramas a un único paquete.

9. Método, según cualquiera de las reivindicaciones anteriores, en el que dichos datos de localización de trama se añaden en el contexto de un paquete RTP.

10. Método, según cualquiera de las reivindicaciones anteriores, en el que dichos datos formateados en tramas representan audio o vídeo.

11. Método, según cualquiera de las reivindicaciones anteriores, en el que dichos datos se cifran en un nivel de trama.

12. Método, según las reivindicaciones 1, 2 ó 3, en el que dichos lugares de control se colocan en una pista de sugerencias independiente.

13. Sistema dispuesto para implementar un método según la reivindicación 1 y que dispone de medios de transmisión continua para transmitir continuamente datos formateados en tramas en paquetes y de medios de cifrado para realizar una etapa de cifrado a dichos datos antes de transmitir continuamente dichos datos,

estando dicho sistema **caracterizado** porque incluye junto a dichos medios de cifrado medios de adición para añadir a dichos datos datos de localización de trama y colocar dichos datos de localización de trama en los paquetes en lugares de control que, igual que la información de cabecera, se excluyen de dicho cifrado posterior.

14. Sistema, según la reivindicación 13, que se configura para interconectarse a Internet como medio de transmisión continua.

15. Servidor de transmisión continua dispuesto para utilizarse como una estación en un sistema según la reivindicación 13.

16. Señal generada por un servidor de transmisión continua según la reivindicación 15.

17. Aparato receptor dispuesto para utilizarse como una estación en un sistema según la reivindicación 13 y que dispone de medios de descifrado para, tras la recepción, descifrar datos que han sido sometidos a dicha etapa de cifrado para obtener datos descifrados basándose en las tramas que contienen dichos datos.

18. Aparato receptor, según la reivindicación 17, en el que dichos medios de descifrado están operativos en el nivel de trama.

19. Aparato receptor, según la reivindicación 17, en el que dichos medios de descifrado están operativos en el nivel de paquete.

20. Método para recibir un flujo continuo de datos formateados en tramas cifrados en paquetes, que incluye una etapa de descifrado tras recibir dichos datos,

estando dicho método **caracterizado** por la etapa de, asociada a la etapa de descifrado, separar, a partir de los paquetes con dichos datos, lugares de control con datos de localización de trama y utilizar dichos datos de localización de trama, que, igual que las informaciones de cabecera, se excluyen de dicha etapa de descifrado posterior, para encontrar el inicio de las tramas en los paquetes.

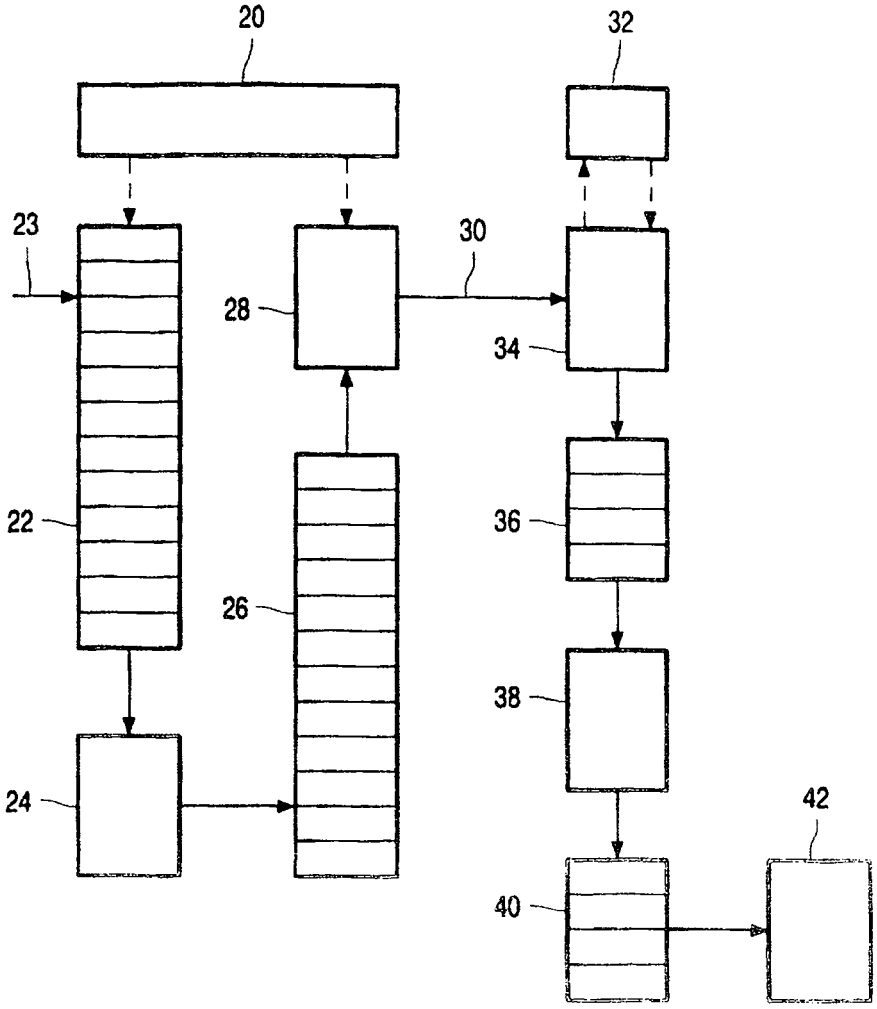

FIG. 1

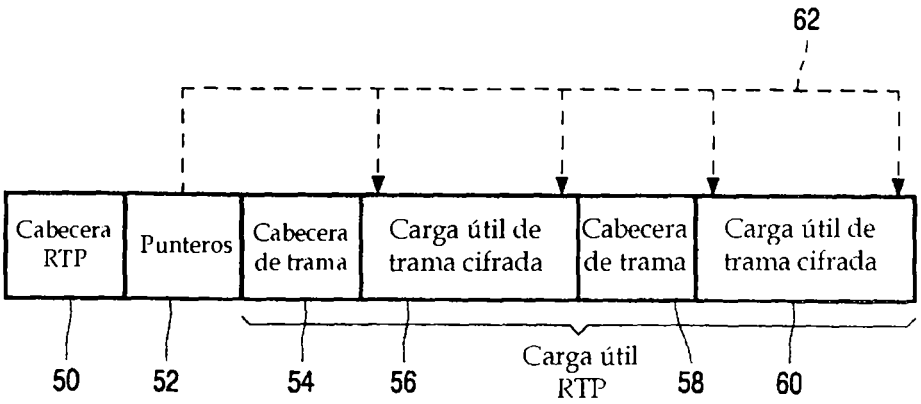
62
Cabecera RTP
Punteros
Cabecera de trama
Carga útil de trama cifrada
Cabecera de trama
Carga útil de trama cifrada
Carga útil RTP
50
52
54
56
58
60

FIG. 2

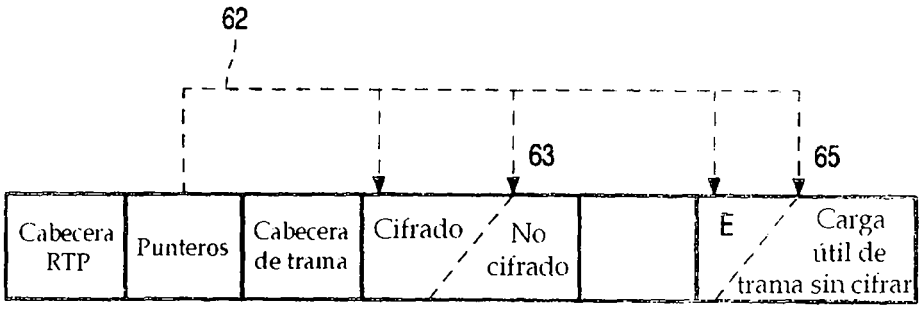
62
63
65
Cabecera RTP
Punteros
Cabecera de trama
Cifrado
No cifrado
E
Carga útil de trama sin cifrar

FIG. 3