(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 295 089**

(51) Int. Cl.:
H04L 9/06 (2006.01)
H04L 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01117538 .7**
(86) Fecha de presentación : **20.07.2001**
(87) Número de publicación de la solicitud: **1193904**
(87) Fecha de publicación de la solicitud: **03.04.2002**

(54) Título: **Procedimiento de transmisión para garantizar la confidencialidad de los datos.**

(30) Prioridad: **11.08.2000 IT VA00A0030**

(45) Fecha de publicación de la mención BOPI:
16.04.2008

(45) Fecha de la publicación del folleto de la patente:
16.04.2008

(73) Titular/es: **Siemens S.p.A.**
Viale Piero e Alberto Pirelli 10
20126 Milano, IT

(72) Inventor/es: **Santacesaria, Claudio**

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procedimiento de transmisión para garantizar la confidencialidad de los datos.

Campo de la invención

La presente invención encuentra particular aplicación en los sistemas de transmisión de radio del tipo de punto a punto o punto multipunto, pero también en otros campos de transmisión de diferentes medios físicos, como optical fiber, coaxial cable y copper twisted pair.

Antecedentes de la invención

Los sistemas cifrados de clave simétrica se utilizan generalmente para el dato cifrado en los sistemas de telecomunicación, mientras que la autentificación y el apoyo para el intercambio seguro de las claves, para ser utilizados en la clave simétrica cifrada, se asignan a los sistemas de cifrado asimétrico.

Los sistemas de cifrado de clave simétrica disponibles son:

- Del tipo en bloque (block cipher)
- Del tipo de flujo (stream cipher)

Por ejemplo, el método DES (Data Encryption Standard), en su modo básico, pertenece a la primera clase, mientras que el DES en el modo OFB (Output Feedback) pertenece a la segunda.

Para incrementar la seguridad, los cifrados de bloque se utilizan a menudo en un modo denominado CBC (Chipre Block Chaining), consistente en el encadenamiento de los siguientes bloques de acuerdo con lo que se describe a continuación.

Suponiendo que para cifrar el bloque tenga la secuencia M_1, M_2 etc., E denota la función de cifrado, IV denota un vector de inicialización arbitraria del mismo tamaño que un bloque de datos y C_1, C_2 etc. denotan los correspondientes bloques de cifras, el encadenamiento se produce usando la función lógica bit XOR en el bloque.

C_1 = E(M_1 XOR IV);

C_2 = E(M_2XOR C_1);

....

C_6 = E(M_6XOR C_5).

En la recepción, el descifrar se lleva a cabo con la función D, utilizado de la siguiente manera:

M_1 = D(C_1)XOR IV;

M_2 = D(C_2)XOR C_1;

M_3 = D(C_3)XOR C_2;

....

M_6 = D(C_6) XOR C_5.

El cifrado por flujo tiene el inconveniente de que requiere la sincronización de la estación transmisora y de la receptora en un nivel de función criptográfico, es decir, los estatutos de la función correspondiente deben de ser alineados en las dos estaciones. En caso de desplazamiento, amplias cantidades de tráfico se pierden.

Por el contrario, el cifrado por bloque multiplica los errores de la transmisión dentro del bloque y en el caso de la modalidad CBC, también en el bloque siguiente. Es decir, la recepción incorrecta de un bit único de C_2 por ejemplo, causa la corrupción total de M_2 y M_3.

Objeto y resumen de la invención

En los sistemas de transmisión equipados con forward error correction code (FEC) y cifrados, haciendo caso omiso de la interacción entre FEC y el cifrado en términos de la corrección de errores del canal, puede conducir a los problemas indicados en el párrafo anterior; esto es que la selección de los códigos del tipo de cifrado por flujo requiere de un mecanismo de sincronización de los estados que debe de ser resistente para evitar el desplazamiento, con las subsiguientes perdidas de porciones enteras de tráfico, mientras que la selección de códigos del tipo cifrado por bloque

puede conducir a la propagación de error, empeorando considerablemente el rendimiento del sistema frente a los del sistema sin criptografía.

El artículo de J. Fernández González, G. B. Agnew y A. Ribagorda, titulado: "Encryption and error correction codes for reliable file storage", publicado por Elsevier Science Publisher Ltd, Amsterdam ND, en la revista Computer & Security, de 1 de agosto de 1993, volumen 12, paginas 501 a 510, XP000398173 ISSN: 0167-4048, aborda el problema de la reacción contra la propagación de error en el tipo de cifrado por bloque. Un modelo de sistema de criptografía se propone con este objetivo. En la rama de la trasmisión el modelo incluye los bloques funcionales siguientes: codificador previa encriptación, interleaver, dispositivo de encriptación y codificador del canal, mientras en la rama de la recepción se incluyen: descodificador de canal, dispositivo de descodificación, de-interleaver, y descodificador posterior encriptación. La valoración de muchos de los parámetros indicados como *L, M, R, J, I, S, α, β, i, H, d,* es necesaria para una operación correcta. Debido a su complicación, un bajo costo de aplicación para tal modelo de sistema de criptografía sería muy difícil.

Por el contrario, de acuerdo a la presente invención que se describe en las reivindicaciones que figuran en el anexo, una cifra del bloque tradicional, con la CBC chaining, se ajusta al bloque codificado con FEC, por lo que se cancelan los efectos negativos de la propagación del error. La colocación correcta de la funcionalidad cifrada antes de la inserción de la codificación FEC en la transmisión y de la función de desciframiento después de la descodificación FEC en la recepción, permite obtener las máximas ventajas.

Un nuevo aspecto de la invención es la inserción de un número entero (uno o más) de bloques cifrados en un bloque FEC. Opcionalmente, la codificación de corrección de error puede efectuarse también en un número entero de bloques cifrados y en los bloques de bits no cifrados adicionales.

CBC se vuelve a iniciar con un vector de inicialización, al menos que coincida con cualquier nuevo bloque de FEC.

Breve descripción de los dibujos

La invención junto con otros objetos y las ventajas del mismo, se puede entender de la siguiente descripción detallada, en relación con los dibujos adjuntos, en los cuales:

La figura 1 muestra la posición correcta de los bloques lógicos en la cadena de transmisión.

Descripción de la manera de realizar la invención

Para describir la invención más en detalle, se considera el caso de interés significante, en el que el código de corrección de error es un Reed Solomon, mientras que el cifrado se obtiene por el método DES con el modo CBC. Se supone que la información de la cifra y la protección se organiza en bloques de 48 bits, igual a la longitud de la carga admisible de una célula ATM (Asynchronous Transfer Mode). Por supuesto, la invención puede ser convenientemente aplicada también a códigos, cifrados y bloques diferentes de los mencionados.

En la transmisión (figura 1), se identifica un bloque de información básica que tiene una dimensión fija, que nosotros consideraremos de 48 byte de longitud, sin reducir por esta razón la generalidad de la invención. Este bloque esta cifrado con el DES CBC, conexión de 6 bloques DES de acuerdo al modo CBC e inicia el CBC con un vector de inicialización antes de el primero de dichos 6 bloques. El vector de linicialización puede ser siempre el mismo o diferente en cualquier momento, siempre que su valor en el primer caso o la secuencia de valores en el segundo caso sea conocida tanto por el transmisor como por el receptor.

Elemento esencial de esta particular ejecución es la reiniciación de la conexión CBC con el vector de inicialización en cada bloque.

Esta operación de cifrado produce un bloque cifrado de 48 Bits.

Uno o más de dichos bloques cifrados son enviados, posiblemente junto con otras informaciones no cifradas, al codificador FEC que añade la redundancia apropiada para la corrección de los errores de canal en el receptor y los bloques cifrados y codificados así obtenidos se transmiten al receptor. El receptor realiza la descodificación FEC como primera operación para conseguir la corrección de los errores de canal en cada uno de dichos bloques cifrados y codificados.

Si esta operación tiene éxito, el receptor mantiene los bloques de cifrado original y puede enviarlos a la función de descifrado sin ningún riesgo de propagación de error. Si la operación falla y lo detecta el código, el cifrado entero y el bloque codificado, que no pueden ser corregido a través del FEC, se rechazan y por lo tanto, el desciframiento de la función, también en este caso, no recibe datos incorrectos y por lo tanto no hay riesgo para la propagación de error.

En la posibilidad remota de que un error de canal no se pueda corregir por el FEC y este no sea aun detectado, el FEC por si mismo introducirá una multiplicación del error de los bloques cifrados tal que el error subsiguiente debido al desciframiento de los bloques erróneos será insignificante y por lo tanto no empeora el funcionamiento frente al sistema sin cifrado.

Siendo el CBC reiniciado en cada bloque, los errores nunca se propagan mas allá de los límites del bloque, dando este sistema las mejores características de funcionamiento y estabilidad frente a los sistemas del tipo conocido descritos anteriormente.

Mientras que una ejecución particular de la presente invención se ha demostrado y descrito, debe de ser entendido que la presente invención no se limita a ella, ya que los expertos en la materia podrían hacer otras incorporaciones, sin que eso la aparte de su alcance. Es lo que contempla que la presente invención abarca cualquiera de las incorporaciones cubiertas por las siguientes reivindicaciones.

REIVINDICACIONES

1. Procedimiento de transmisión de datos de una estación emisora a una estación receptora adecuada para proteger la confidencialidad de los datos y la estabilidad de la transmisión, que incluye los pasos siguientes:

en la estación emisora

a) cifrado de los datos a transmitir según el método Cipher Block Chaining denominado CBC, dicho cifrado de bloques está ajustado a los bloques que deben cifrarse con una codificación de corrección de errores (FEC);

b) codificación de corrección de errores (FEC) de dicho bloque cifrado, produciendo bloques cifrados codificados;

en la estación receptora

c) desciframiento de dichos bloques cifrados codificados con el código de corrección de errores, produciendo un bloque cifrado descodificado.

d) descifrado de los bloques cifrados descodificados con el descifrado correspondiente a dicho método CBC,

caracterizado porque:

- a la estación emisora, dicho encadenado CBC es reinicia en la puesta en marcha de un nuevo bloque que debe de ser cifrado con dicha codificación de corrección de errores (FEC) por la utilización de un vector de inicialización conocido tanto en la estación emisora y en la estación receptora.

2. Procedimiento según la reivindicación 1,

caracterizado porque

la reiniciación de el encadenado CBC se hace siempre por el hecho de emplear un mismo vector de iniciación.

3. Procedimiento según la reivindicación 1 o 2,

caracterizada porque

dicha codificación de corrección de errores se hace en un número entero de bloques cifrados.

4. Procedimiento según la reivindicación 3,

caracterizado porque

dicha codificación de corrección de errores también incluye bloques de bits adicionales no cifrados.

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4,

caracterizado porque

dicho algoritmo de cifrado de bloques es la norma de inscripción de datos, denominada DES.

6. Procedimiento según la reivindicación 5

caracterizado porque,

dicho algoritmo de cifrado de bloques es el triple DES.

7. Procedimiento según cualquiera de las reivindicaciones 1 a 6

caracterizado porque,

dicho código de corrección de error es el Reed Salomon.

8. Procedimiento según la reivindicación 7,

caracterizado porque,

dicho código Reed Solomon está conectado con un código convolucional interno.

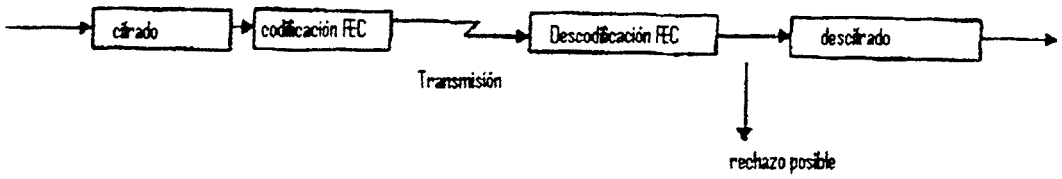
cifrado
codificación FEC
Transmisión
Descodificación FEC
descifrado
rechazo posible

FIG.1