(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 617 627**

(51) Int. CI.:

H04N 21/266 (2011.01)
H04N 7/16 (2006.01)
H04N 21/418 (2011.01)
H04N 21/4623 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.03.2009 PCT/EP2009/053008**

(87) Fecha y número de publicación internacional: **17.09.2009 WO2009112580**

(96) Fecha de presentación y número de la solicitud europea: **13.03.2009 E 09719938 (4)**

(97) Fecha y número de publicación de la concesión europea: **30.11.2016 EP 2253142**

(54) Título: **Procedimiento de aseguramiento de mensajes transmitidos por un terminal emisor a un terminal receptor remoto**

(30) Prioridad:

14.03.2008 FR 0851652

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.06.2017

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche Tour Opéra C 76, Route de la Demi-Lune
92057 Paris La Défense Cedex, FR

(72) Inventor/es:

CHEVALLIER, ANTHONY y
PHIRMIS, MATHIEU

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Procedimiento de aseguramiento de mensajes transmitidos por un terminal emisor a un terminal receptor remoto

Campo técnico

La invención se sitúa en el campo de las telecomunicaciones y se refiere más específicamente a un procedimiento de aseguramiento de un número n superior o igual a 1 de mensajes MUi (i = 1 a n) transmitidos por un terminal emisor a un terminal receptor.

La invención se refiere igualmente a un terminal emisor adaptado para transmitir un número n superior o igual a 1 de mensajes MUi (i = 1 a n) a un terminal receptor remoto.

La invención se refiere también a un terminal receptor configurado para recibir los mensajes MUi (i = 1 a n) transmitidos por dicho terminal emisor.

La invención se refiere además a un programa de ordenador memorizado en un soporte y destinado a ser ejecutado en el terminal emisor para implementar el procedimiento en el lado de emisión, y un programa de ordenador memorizado en un soporte y destinado a ser ejecutado en el terminal receptor para implementar el procedimiento en el lado de recepción.

La invención se dirige más precisamente a una mejora de la protección de los mensajes EMM enviados por la cabecera de red de un operador al sistema de recepción de un cliente. Se aplica sin embargo más generalmente a la protección de cualquier transmisión de mensajes entre entidades vinculadas por unas redes de comunicación independientemente de la naturaleza y de las características de dichas entidades y de dichas redes.

Estado de la técnica anterior

Con el desarrollo creciente de la distribución de contenidos a través de las redes de comunicación, el riesgo de pirateado de estos contenidos se convierte en una preocupación importante tanto en los suministradores como en los destinatarios de estos contenidos.

Es primordial en consecuencia proteger los contenidos distribuidos contra, por un lado, los riesgos de desviación de los derechos de acceso asociados a estos contenidos y, por otro lado, contra la falsificación de estos derechos por un usuario.

En efecto, en los sistemas de control de acceso de tipo CAS (por Conditional Access System), los contenidos distribuidos están encriptados y su desencriptado condicionado por la posesión de permisos lógicos (un usuario puede acceder al contenido durante una duración determinada), y de claves, denominadas claves de explotación, que permiten acceder a los contenidos.

Los permisos lógicos y las claves de explotación se transmiten generalmente a los terminales receptores en unos mensajes de control de acceso específicos EMM (por Entitlement Management Message). Unos mensajes EMM pueden incluir igualmente unos controles destinados a limitar o suprimir unos derechos anteriormente adquiridos por el usuario.

Las condiciones de acceso se transmiten igualmente a los terminales receptores en unos mensajes de control de acceso específicos ECM (por Entitlement Control Message).

Los mensajes EMM y ECM deben en sí mismos estar protegidos.

Para una mejor comprensión en relación con la terminología apropiada en este campo técnico, se podrá hacer referencia al documento siguiente: “FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM” EBU REVIEW TECHNICAL EUROPEAN BROADCASTING UNION. Bruselas, BE, n.º 266, 21 de diciembre de 1995.

Un inconveniente de la técnica anterior proviene del hecho de que estos mensajes pueden ser interceptados y analizados con el fin de determinar las condiciones de acceso y las claves necesarias para el desencriptado de los contenidos. Un pirata puede así finalmente adquirir la capacidad de conservar un mensaje recibido y posteriormente modificarlo, y volver a remitirlo a su terminal receptor de manera que éste lo procese. El pirata puede adquirir o encontrar entonces unos derechos que no son (o ya no son) legítimamente adquiridos. Se puede igualmente, con el mismo objetivo, adquirir la capacidad de calcular por sí mismo unos mensajes de su elección y de hacer que se acepten por el terminal receptor unos mensajes fraudulentos como mensajes calculados por el operador.

Otra forma de fraude consiste en filtrar unos mensajes transmitidos por el operador para impedir su toma en consideración por el procesador de seguridad del terminal receptor, por ejemplo cuando se trata de mensajes que correrían el peligro de privar al usuario de derechos que habría adquirido precedentemente.

El estado de la técnica de la protección de los mensajes de control de acceso contra estos ataques está compuesto de diversas soluciones, entre las que:

- El cifrado de los mensajes a transmitir, de manera que el pirata, tras su recepción, no sepa si los mensajes contienen unas órdenes positivas o negativas desde su punto de vista. Esta medida le impide por tanto determinar sobre la marcha los mensajes que debe filtrar, haciendo así más difícil el filtrado de los EMM.
- La adición de una redundancia criptográfica a los mensajes a transmitir. Esto permite verificar que los mensajes han sido calculados por una entidad en posesión de una clave específica habilitada para ese cálculo. Esta medida hace así más difícil el cálculo de mensajes auténticos de su elección, contra cuya inserción se protege así al sistema.
- La combinación lógica, en un mismo mensaje, de órdenes positivas y negativas desde el punto de vista del pirata, de manera que el sistema de recepción no pueda tener en cuenta con éxito la orden positiva más que si ha realizado previamente lo mismo para la orden negativa. Esta combinación se basa en la hipótesis según la que el pirata está más penalizado por la no toma en consideración de la orden positiva que por la toma en consideración de la orden negativa. Esta medida disuade entonces del filtrado del EMM que integra la combinación, contra lo que protege así al sistema.

En el caso del cifrado de los EMM: si el pirata ignora a priori qué mensaje manipula, puede determinar los efectos por la experiencia: por ejemplo sometiéndole a un sistema de recepción reservado a sus ensayos.

Puede igualmente no someter los mensajes cifrados a su sistema de recepción, hasta que este ya no funcione, obteniendo eventualmente así un tiempo suplementario e ilegítimo de acceso a los contenidos considerados.

En el caso en el que la autenticación de los mensajes de control de acceso se realiza mediante una redundancia criptográfica, esta medida no tiene efecto en los casos siguientes:

- si el pirata ha logrado obtener la clave o si ha logrado obtener una redundancia criptográfica correcta. Esto es particularmente posible si dicha redundancia criptográfica es simétrica.
- si el pirata ha logrado hacer que se acepte un mensaje, por el procesador de seguridad, como incluyendo una redundancia criptográfica correcta, y por tanto como auténtico. Esto es particularmente posible perturbando físicamente el entorno de funcionamiento del procesador de seguridad del sistema de recepción encargado de verificar esta autenticidad. Entre estas perturbaciones, figuran por ejemplo la elevación brusca de la temperatura, la variación de la señal de alimentación eléctrica o del reloj, la exposición del componente a unos impulsos láser, unas emisiones electromagnéticas o unas radiaciones de partículas radiactivas.

En el caso en el que la protección de los mensajes se realiza por la transmisión al terminal receptor de una combinación de órdenes positivas y negativas, la medida no es interesante más que cuando el pirata tiene algo que perder. En particular, ciertos ataques consisten en añadir ilegalmente unos derechos en unos procesadores de seguridad oficiales (casos denominados MOSC, Modified Official Smart Card). En este caso, el pirata no sufre una pérdida filtrando los mensajes más que si el operador cambia unas claves de explotación.

Ahora bien es preferible no transferir estas claves de los múltiplex, con el fin de no exponerlas inútilmente.

Surge por tanto que no es siempre posible para un sistema de control de acceso (CAS) contrarrestar los ataques de los piratas, y en particular contrarrestar la supresión de mensajes no deseados o la inserción de mensajes que no deberían someterse al procesador de seguridad.

El objetivo de la invención es paliar las insuficiencias de los sistemas de control de acceso de la técnica anterior descritos anteriormente.

El documento “ALFRED J. MENEZES, PAUL C. VAN OORSCHOT AND SCOTT A. VANSTONE: “Handbook of applied Cryptography” CRC PRESS, 1 de octubre de 1996 (1996-10-01), XP002494672 ISBN: 0-8493-8523-7” describe de manera general la definición de una función de permutación utilizada en ciertos sistemas criptográficos según la que se considera un conjunto S de elementos y se calcula para cada uno de los elementos de este conjunto su imagen mediante una función reversible p. En la medida en la que p es una biyección, cada elemento del conjunto S puede encontrarse por aplicación de p^{-1}, la función inversa de p a su imagen.

El documento “FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM” EBU REVIEW-TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSELAS, BE, n.º 266. 21 de diciembre de 1995 (1995-12-21), páginas 64-77 XP000559450, ISSN: 0251-0936” describe de manera general un modelo funcional del sistema de control de acceso.

Exposición de la invención

La invención se basa en la idea de sustituir el mensaje útil; es decir que transporta información útil a proteger, por una secuencia de mensajes que contienen, además del mensaje útil a proteger, un intervalo predeterminado, de

mensajes secundarios, preferentemente de aspecto próximo y en número predeterminado, que hacen las veces de ruido y no transportan información útil para otro fin.

En este sentido, la invención preconiza un procedimiento de aseguramiento de un número n superior o igual a 1 de los mensajes MUi (i = 1 a n) transmitidos por un terminal emisor a un terminal receptor, procedimiento que incluye las etapas siguientes:

Previamente a la emisión, por el terminal emisor,

a- generar una secuencia ordenada que incluye N bloques de datos Bj, (j = 1 a N), siendo N un número entero superior o igual a n,
b- para cada mensaje MUi (i = 1 a n), calcular una posición pi en dicha secuencia ordenada de N bloques por medio de una función pseudoaleatoria F inicializada mediante al menos un dato secreto compartido por el terminal emisor y el terminal receptor,
c- encapsular cada mensaje MUi (i = 1 a n) en el bloque Bj situado en la posición pi, y,
d- transmitir la secuencia ordenada que incluye los mensajes MUi a dicho terminal receptor, y en la recepción, por el terminal receptor,
e- recalcular las posiciones pi (i = 1 a n) de los bloques Bj que encapsulan los mensajes MUi por medio de dicha función F,
f- extraer los bloques Bj que ocupan las posiciones pi (i = 1 a n) de la secuencia ordenada recibida,
g- extraer los mensajes MUi encapsulados en dichos bloques Bj.

Gracias al procedimiento según la invención, cualquier tentativa de añadir, de sustituir o de suprimir un mensaje es detectada cuando la secuencia de mensajes recibidos por el terminal receptor no respeta la estructura predeterminada.

Además, si una secuencia de mensajes producida por un terminal emisor según la invención se transmite a un terminal no en consonancia con el terminal receptor según la invención, se envían entonces unos mensajes secundarios de control a ese terminal receptor.

Estos mensajes de control pueden transportar por ejemplo unas órdenes de detección o de sanción susceptibles de provocar el desencadenamiento de operaciones de detección o de contramedidas. La detección puede ser de diferentes tipos, como la memorización de un registro o el incremento de un contador de detecciones; las contramedidas pueden consistir por ejemplo en una invalidación temporal o en la destrucción de la tarjeta.

En una primera variante de implementación del procedimiento según la invención, dicho dato secreto se define en función del número N y/o del número n.

En una segunda variante, dicho dato secreto se define en función de al menos un parámetro específico de la secuencia ordenada generada.

Según otra característica de la invención, el valor de dicho dato secreto es modificable por el terminal emisor según una secuenciación conocida exclusivamente por dicho terminal emisor.

Con el fin de garantizar la gestión de los bloques de datos por el terminal receptor, cada bloque Bj de la secuencia ordenada incluye un encabezado que indica un identificador de dicha secuencia y la posición de dicho bloque Bj en esta secuencia.

En una variante, dicho encabezado incluye además el valor del número N y/o el del número n.

En otra variante de la invención, dicha secuencia ordenada incluye además al menos un mensaje suplementario encapsulado en un bloque Bj de datos situado en una posición diferente de las posiciones pi (i = 1 a n) en dicha secuencia ordenada, sin acción o que permite la activación de una detección y/o una sanción a continuación de una acción de desvío de los mensajes útiles MUi por un defraudador o de una tentativa de dicha acción.

En una aplicación particular del procedimiento según la invención destinado a reforzar la seguridad de un sistema de control de acceso de tipo CAS, la pluralidad de mensajes útiles MUi incluye al menos un mensaje EMM y/o al menos un mensaje ECM, y dicho terminal emisor se dispone en cabeza de la red de un operador.

En este caso, dichos n mensajes MUi incluyen al menos un mensaje EMM y/o al menos un mensaje ECM, y uno al menos de dichos números N y n se transmite al terminal receptor en un mensaje cifrado.

Dichos n mensajes MUi se transmiten al terminal receptor por el terminal emisor en un flujo de datos que incluye además unos programas audiovisuales encriptados.

El procedimiento según la invención se implementa mediante un terminal emisor dispuesto en cabeza de la red de

un operador y configurado para transmitir un número n superior o igual a 1 de mensajes MUi (i = 1 a n) a un terminal receptor.

El terminal emisor según la invención incluye:

- unos medios para generar una secuencia ordenada que incluye N bloques de datos Bj, (j = 1 a N), siendo N un número entero superior o igual a n,
- unos medios para calcular, para cada mensaje útil MUi (i = 1 a n), una posición pi en dicha secuencia ordenada de N bloques por medio de una función pseudoaleatoria F inicializada mediante al menos un dato secreto compartido por el terminal emisor y el terminal receptor,
- unos medios para encapsular cada mensaje MUi (i = 1 a n) en el bloque Bj situado en la posición pi,
- unos medios para transmitir la secuencia ordenada que incluye los mensajes MUi a dicho terminal receptor.

El terminal receptor según la invención incluye:

- unos medios para recalcular las posiciones pi (i = 1 a n) de los bloques Bj que encapsulan los mensajes MUi por medio de dicha función F,
- unos medios para extraer dichos bloques Bj de posiciones pi (i = 1 a n) en la secuencia ordenada recibida,
- unos medios para extraer los mensajes MUi de dichos bloques Bj.

En el emisor, el procedimiento según la invención se implementa por medio de un programa de ordenador memorizado en un soporte y destinado a ser ejecutado en el terminal emisor para:

- generar una secuencia ordenada que incluye N bloques de datos Bj, (j = 1 a N), siendo N un número entero superior o igual a n,
- para cada mensaje útil MUi (i = 1 a n), calcular una posición pi en dicha secuencia ordenada de N bloques por medio de una función pseudoaleatoria F inicializada mediante al menos un dato secreto compartido por el terminal emisor y el terminal receptor,
- encapsular cada mensaje MUi (i = 1 a n) en el bloque Bj situado en la posición pi,
- transmitir la secuencia ordenada que incluye los mensajes MUi a dicho terminal receptor.

En el receptor, el procedimiento según la invención se implementa por medio de un programa de ordenador memorizado en un soporte y destinado a ser ejecutado en el terminal receptor para:

- recalcular las posiciones pi (i = 1 a n) de los bloques Bj que encapsulan los mensajes MUi por medio de dicha función F,
- extraer dichos bloques Bj de posiciones pi (i = 1 a n) en la secuencia ordenada recibida,
- extraer los mensajes MUi de dichos bloques Bj.

Breve descripción de los dibujos

Surgirán de la descripción que sigue otras características y ventajas de la invención, tomadas como ejemplo no limitativo, con referencia a las figuras adjuntas en las que:

- la figura 1 representa un organigrama general que ilustra esquemáticamente las etapas del procedimiento según la invención implementadas por el terminal emisor.
- La figura 2 ilustra esquemáticamente dos flujos que incluyen unas secuencias ordenadas de datos que transportan unos mensajes según la invención.
- La figura 3 representa un organigrama que ilustra esquemáticamente las etapas del procedimiento según la invención implementadas por el terminal receptor.

Exposición detallada de modos de realización particulares

La invención se describirá en el presente documento a continuación en una aplicación particular a un sistema de control de acceso de tipo (CAS). Los mensajes útiles a transmitir son unos EMM o unos ECM que transportan unos datos secretos tales como las claves de cifrado/descifrado de un contenido difundido por un operador a varios terminales receptores. Cada terminal receptor está provisto de un procesador de seguridad que incluye un software de tratamiento de los mensajes útiles transmitidos por el operador.

En este caso, el operador puede utilizar diferentes vías para difundir los mensajes EMM y ECM. Para dirigirse a unos destinatarios o grupos de destinatarios particulares, el operador utiliza diferentes modos de direccionamiento. De ese modo, un mensaje de tipo EMM-GA está destinado a todos los usuarios de un grupo dado (GA - General Audience), un mensaje de tipo EMM-S está destinado a un grupo particular de usuarios (S - Shared), y un mensaje de tipo EMM-U está destinado a un usuario único (U - User). Se utiliza una vía típicamente para la difusión de los mensajes EMM de cada uno de estos modos de direccionamiento.

Obsérvese que es igualmente posible, incluso en el caso de modos de direccionamiento único, tener diferentes vías de EMM. Por ejemplo, en un teléfono móvil, ciertos mensajes pueden enviarse en el mismo múltiplex que el que contiene el video, y otros pueden ser vehiculados en unos SMS. Es igualmente probable que varios usuarios deban recibir unos mensajes. Cada EMM-U enviado a un usuario debe considerarse como que está en una vía EMM en el contexto de esta aplicación.

Las vías EMM anteriormente mencionadas son independientes, y cada vía EMM tiene su propio contexto de secuenciación.

Las principales etapas del procedimiento según la invención se describen en el presente documento a continuación con referencia a la figura 1.

Del lado de la cabecera de la red, en la etapa 2, el operador realiza una solicitud de envío de un número n de mensajes útiles MUi (i = 1 a n) (EMM y/o ECM) al sistema CAS.

La etapa 6 consiste en generar dicha secuencia ordenada que incluye N bloques de datos Bj.

La etapa 8 consiste en calcular, para cada mensaje MUi, (i = 1 a n), una posición pi en dicha secuencia ordenada de N bloques por medio de una función F.

La etapa 10 consiste en encapsular cada mensaje MUi (i = 1 a n), en el bloque Bj situado en la posición pi.

La etapa 12 consiste en transmitir la secuencia ordenada que incluye los mensajes MUi a los terminales receptores.

Cada terminal receptor:

- recalcula las posiciones pi (i = 1 a n) de los bloques Bj que encapsulan los mensajes MUi por medio de dicha función F (etapa 14),
- extrae los bloques Bj que ocupan las posiciones pi (i = 1 a n) de la secuencia ordenada recibida (etapa 16),
- extrae los mensajes MUi encapsulados en dichos bloques Bj (etapa 18).

La figura 2 ilustra esquemáticamente un primer flujo de secuencias 20 y un segundo flujo de secuencias 22. El primer flujo 20 incluye una primera secuencia ordenada 24 que incluye un número entero N1 de bloques de datos 26 y segunda secuencia ordenada 28 de incluye igualmente N1 bloques de datos 30. El segundo flujo 22 incluye una primera secuencia ordenada 32 que incluye un número entero N2 de bloques de datos 34 y una segunda secuencia ordenada 36 que incluye igualmente N2 bloques de datos 38.

Cada bloque de datos (26, 30, 34, 38) incluye un primer sub-bloque que forma el encabezado 40 y un segundo sub-bloque 42 que comprende los datos útiles del bloque.

El encabezado 40 incluye un identificador de secuencia SN, un parámetro O que indica la posición de un bloque Bj en la secuencia y posiblemente una fecha que indica la fecha de emisión de la secuencia identificada por el parámetro SN.

Los sub-bloques 42 de los bloques de datos Bj (j = 1 a N) de la secuencia ordenada producida en la etapa 10 encapsulan, además de los mensajes útiles, al menos un mensaje suplementario en un bloque Bj situado en una posición diferente de las posiciones pi (i = 1 a n) calculadas por la función F. Los mensajes suplementarios permiten la activación de una detección y/o de una sanción a continuación de una acción de desvío de los mensajes útiles MUi por un defraudador, o de una tentativa de dicha acción.

Aunque la figura 2 ilustra unos flujos ordenados de secuencias, en una variante de realización, la transmisión de los bloques de una secuencia ordenada se podrá realizar en una secuenciación desordenada según una ley aleatoria.

Aunque la figura 2 ilustra unos flujos de secuencias ordenadas separados, en una variante de realización, la transmisión de los flujos de datos se podrá organizar de modo que entre dos bloques al menos de una misma secuencia ordenada se transmita al menos un bloque que pertenece a al menos otra secuencia ordenada.

Caracterización de la función F.

El resultado de la función F no debe ser previsible para un observador externo del sistema, esta función se elige preferentemente como pseudoaleatoria, es decir, que obedece a una ley pseudoaleatoria construida a partir de generadores pseudoaleatorios inicializados con unos parámetros de valores iguales en el terminal emisor y en los terminales receptores.

En una primera variante de realización del procedimiento según la invención, la función F se mantiene secreta.

En ese caso, solo los terminales autentificados por el operador están habilitados para memorizar esta función previamente a la transmisión de los flujos de secuencias.

Los parámetros de cálculo de las posiciones pi por medio de la función F pueden ser secretos o no.

En una segunda variante, la función F es pública y puede particularmente estar registrada en claro en los terminales o descargarse desde un servidor del operador.

En ese caso, uno al menos de los parámetros de cálculo de las posiciones pi por medio de la función F se mantiene secreto y se transmite a los terminales receptores bajo la forma cifrada.

Se describe en el presente documento a continuación un ejemplo de construcción de una función F de ese tipo.

La construcción de la función F se basa en el incremento por diez (10) del valor del número N, y el del número n, es decir del número de posiciones a determinar en una secuencia identificada por el parámetro SN. La selección de los octetos sucesivos de un valor aleatorio subtiende esta determinación, diez incrementa también el número de octetos de este valor aleatorio, que se le supondrá por tanto a continuación codificado sobre 16 octetos.

Recuérdese que X módulo Y designa al resto de la división entera del entero X por el entero no nulo Y. Se denota por otro lado por Card el cardinal, es decir el número de elementos de un conjunto.

Se considera:

- SN, el identificador de la secuencia considerada, es decir a construir, si se sitúa en el lado del terminal emisor, o a procesar, si se sitúa en el lado del terminal receptor;
- N, la longitud de la secuencia;
- n, el número de mensajes útiles de esta secuencia;
- MU_1, MU_2, …, MU_n, los n mensajes útiles a transmitir en la secuencia;
- K, una clave secreta compartida por los dispositivos emisor y receptor.

Con la ayuda de un generador pseudoaleatorio, tal como una función criptográfica C, se calcula un valor aleatorio RAND apropiado para la secuencia SN bajo la forma:

$$C\ (K, SN) = RAND = RAND[i],\ 1 \leq i \leq 16$$

En la que RAND[i] designa el octeto de rango i de RAND
C puede ser típicamente:

- Una función de criptografía H aplicada a la concatenación de la clave K y del identificador de secuencia SN; el valor aleatorio calculado es entonces:

$$H\ (K \mid\mid SN) = RAND = RAND[i],\ 1 \leq i \leq 16$$

- El algoritmo de cifrado AES (Advanced Encryption Standard) aplicado con la clave K al identificador de secuencia SN; el valor aleatorio calculado es entonces:

$$AES\ (K, SN) = RAND = RAND[i],\ 1 \leq i \leq 16$$

Se calcula a continuación la posición pi de MUi en SN bajo la fórmula:

$$p_1 = RAND[1] \text{ módulo } N;$$

para $1 < i \leq n$:

Sea, $E_i = \{j \text{ entero} / 0 < j \leq N\} \setminus \{p_j / 1 \leq j < i\} = \{1, 2, ..., N\} \setminus \{p_j / 1 \leq j < i\}$, el conjunto de los enteros positivos inferiores o iguales a N privado de las posiciones ya atribuidas, es decir el conjunto de las posiciones aún disponibles;

Sea $F_i = \{x_j \in E_i / \forall\ 1 \leq k, l \leq Card\ (E_i),\ k < l \Leftrightarrow x_k < x_l\}$, el mismo conjunto, ordenado;

Se tiene entonces: $p_i = X_{RAND[i] \text{ módulo } (N-i+1)}$

Es decir:

- R1 = RAND[1] módulo N, da la posición de MU_1 en SN, entre las N posibles;
- R2 = RAND[2] módulo N-1, da la posición de MU_2 en SN, entre las N-1 restantes;
- ...
- Rn = RAND[n] módulo N-n+1, da la posición de MU_n en SN, entre las N-n+1 restantes.

La figura 3 es un organigrama que ilustra las etapas del software memorizado en el terminal receptor que permite realizar el procedimiento en este terminal.

La ejecución del software en el terminal receptor permite realizar las etapas siguientes.

Recibir los N bloques (etapa 72).

La etapa 74 consiste en verificar si la estructura de la secuencia recibida es válida.

En caso afirmativo, se ejecuta por el procesador la función F de seguridad para determinar las posiciones pi (i = 1 a n) de los mensajes útiles en la secuencia recibida (etapa 76).

En la etapa 78, los bloques de datos Bj de las posiciones pi (i = 1 a n) se extraen de la secuencia ordenada recibida.

En la etapa 80, se extraen los mensajes útiles MUi de dichos bloques Bj.

REIVINDICACIONES

1. Procedimiento de aseguramiento de un número n superior o igual a 1 de los mensajes MUi (i = 1 a n) transmitidos por un terminal emisor a un terminal receptor, **caracterizado por** las etapas siguientes:

Previamente a la emisión, por el terminal emisor,

a- generar una secuencia ordenada que incluye N bloques de datos Bj, (j = 1 a N), siendo N un número entero superior o igual a n,
b- para cada mensaje MUi (i = 1 a n), calcular una posición pi en dicha secuencia ordenada de N bloques por medio de una función pseudoaleatoria F inicializada mediante al menos un dato secreto compartido por el terminal emisor y el terminal receptor,
c- encapsular cada mensaje MUi (i = 1 a n) en el bloque Bj situado en la posición pi, y,
d- transmitir la secuencia ordenada que incluye los mensajes MUi a dicho terminal receptor, y en la recepción, por el terminal receptor,
e- recalcular las posiciones pi (i = 1 a n) de los bloques Bj que encapsulan los mensajes MUi por medio de dicha función F,
f- extraer los bloques Bj que ocupan las posiciones pi (i = 1 a n) de la secuencia ordenada recibida,
g- extraer los mensajes MUi encapsulados en dichos bloques Bj.

2. Procedimiento según la reivindicación 1, en el que dicho dato secreto se define en función del número N y/o del número n.

3. Procedimiento según la reivindicación 1, en el que dicho dato secreto se define en función de al menos un parámetro específico de la secuencia ordenada generada.

4. Procedimiento según la reivindicación 1, en el que el valor de dicho dato secreto es modificable por el terminal emisor.

5. Procedimiento según la reivindicación 4, en el que la modificación del valor de dicho dato secreto se realiza según una secuenciación conocida exclusivamente por el terminal emisor.

6. Procedimiento según la reivindicación 1, en el que dicha secuencia ordenada incluye además al menos un mensaje suplementario encapsulado en un bloque Bj de datos situado en una posición diferente de las posiciones pi (i = 1 a n) en dicha secuencia ordenada, sin acción o que permite la activación de una detección y/o una sanción a continuación de una acción de desvío de los mensajes útiles MUi por un defraudador o de una tentativa de dicha acción.

7. Procedimiento según la reivindicación 1, en el que cada bloque Bj de la secuencia ordenada incluye un encabezado que indica un identificador de dicha secuencia y la posición de dicho bloque Bj en esta secuencia.

8. Procedimiento según la reivindicación 7, en el que dicho encabezado incluye además el valor del número N y/o el del número n.

9. Procedimiento según la reivindicación 1, en el que dicho terminal emisor se dispone en cabeza de la red de un operador.

10. Procedimiento según la reivindicación 9, en el que dichos n mensajes MUi incluyen al menos un mensaje EMM y/o al menos un mensaje ECM.

11. Procedimiento según la reivindicación 1, en el que uno al menos de los números N y n se transmite al terminal receptor en un mensaje cifrado.

12. Procedimiento según la reivindicación 1, en el que dichos n mensajes MUi se transmiten al terminal receptor por el terminal emisor en un flujo de datos que incluye además unos programas audiovisuales encriptados.

13. Terminal emisor dispuesto en la cabeza de la red de un operador y configurado para transmitir un número n superior o igual a 1 de mensajes MUi (i = 1 a n) a un terminal receptor, **caracterizado por que** incluye:

- unos medios para generar una secuencia ordenada que incluye N bloques de datos Bj, (j = 1 a N), siendo N un número entero superior o igual a n,
- unos medios para calcular, para cada mensaje útil MUi (i = 1 a n), una posición pi en dicha secuencia ordenada de N bloques por medio de una función pseudoaleatoria F inicializada mediante al menos un dato secreto compartido por el terminal emisor y el terminal receptor,
- unos medios para encapsular cada mensaje MUi (i = 1 a n) en el bloque Bj situado en la posición pi,
- unos medios para transmitir la secuencia ordenada que incluye los mensajes MUi a dicho terminal receptor.

14. Terminal receptor configurado para recibir los mensajes MUi transmitidos por el emisor según la reivindicación 13, **caracterizado por que** incluye:

- unos medios para recalcular las posiciones pi (i = 1 a n) de los bloques Bj que encapsulan los mensajes MUi por medio de dicha función F,
- unos medios para extraer dichos bloques Bj de posiciones pi (i = 1 a n) en la secuencia ordenada recibida,
- unos medios para extraer los mensajes MUi de dichos bloques Bj.

15. Programa de ordenador memorizado en un soporte y destinado a ser ejecutado en el terminal emisor según la reivindicación 14 para:

- generar una secuencia ordenada que incluye N bloques de datos Bj, (j = 1 a N), siendo N un número entero superior o igual a n,
- para cada mensaje útil MUi (i = 1 a n), calcular una posición pi en dicha secuencia ordenada de N bloques por medio de una función pseudoaleatoria F inicializada mediante al menos un dato secreto compartido por el terminal emisor y el terminal receptor,
- encapsular cada mensaje MUi (i = 1 a n) en el bloque Bj situado en la posición pi,
- transmitir la secuencia ordenada que incluye los mensajes MUi a dicho terminal receptor.

16. Programa de ordenador memorizado en un soporte y destinado a ser ejecutado en el terminal receptor según la reivindicación 14 para:

- recalcular las posiciones pi (i = 1 a n) de los bloques Bj que encapsulan los mensajes MUi por medio de dicha función F,
- unos medios para extraer dichos bloques Bj de posiciones pi (i = 1 a n) en la secuencia ordenada recibida,
- unos medios para extraer los mensajes MUi de dichos bloques Bj.

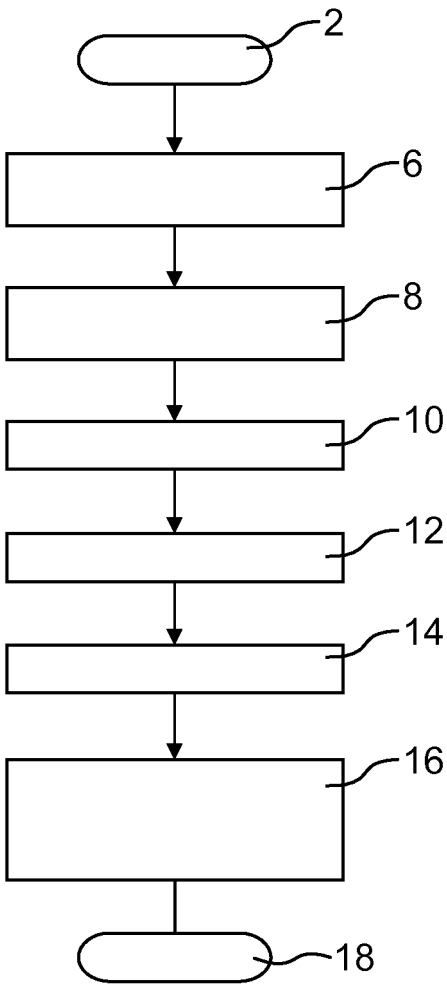

FIG.1

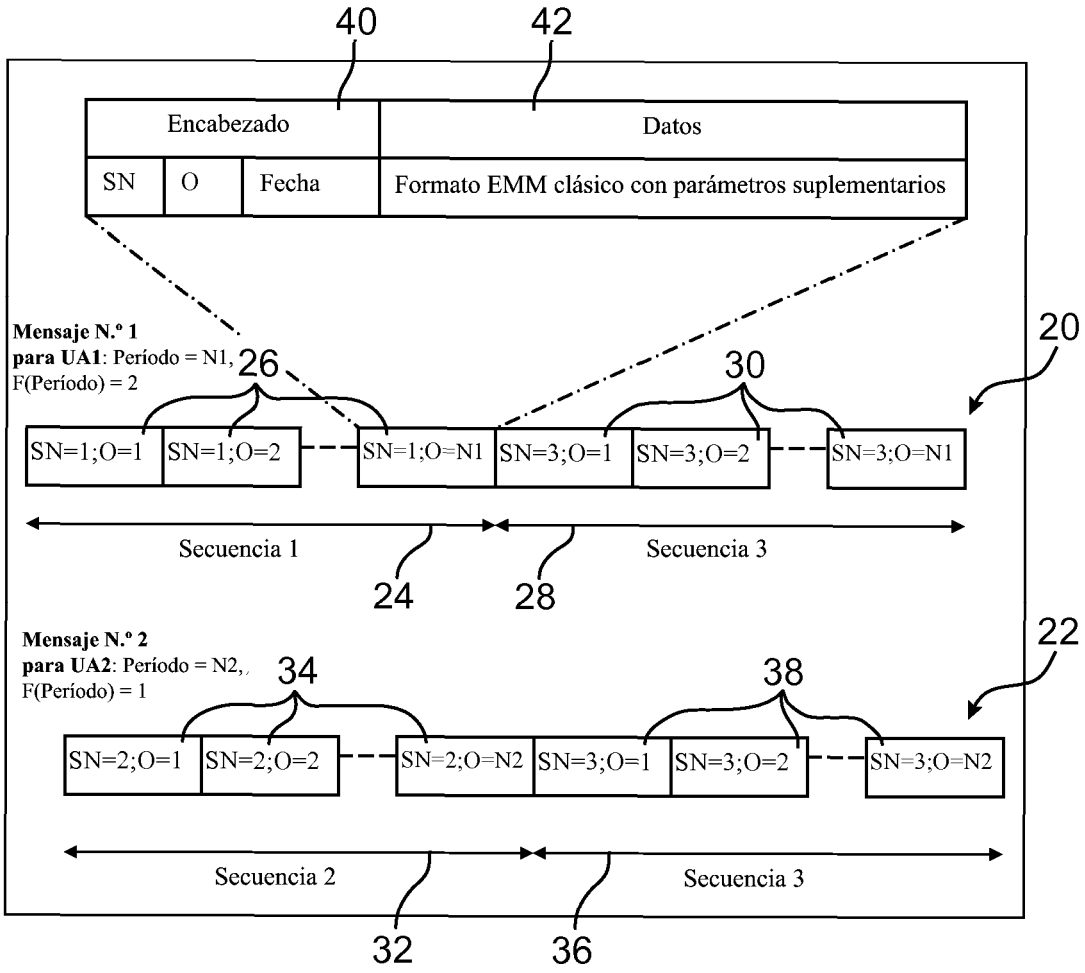
40
42
Encabezado
Datos
SN
O
Fecha
Formato EMM clásico con parámetros suplementarios
Mensaje N.º 1
para UA1: Período = N1,
F(Período) = 2
26
30
20
SN=1;O=1
SN=1;O=2
SN=1;O=N1
SN=3;O=1
SN=3;O=2
SN=3;O=N1
Secuencia 1
Secuencia 3
24
28
Mensaje N.º 2
para UA2: Período = N2,
F(Período) = 1
34
38
22
SN=2;O=1
SN=2;O=2
SN=2;O=N2
SN=3;O=1
SN=3;O=2
SN=3;O=N2
Secuencia 2
Secuencia 3
32
36

FIG.2

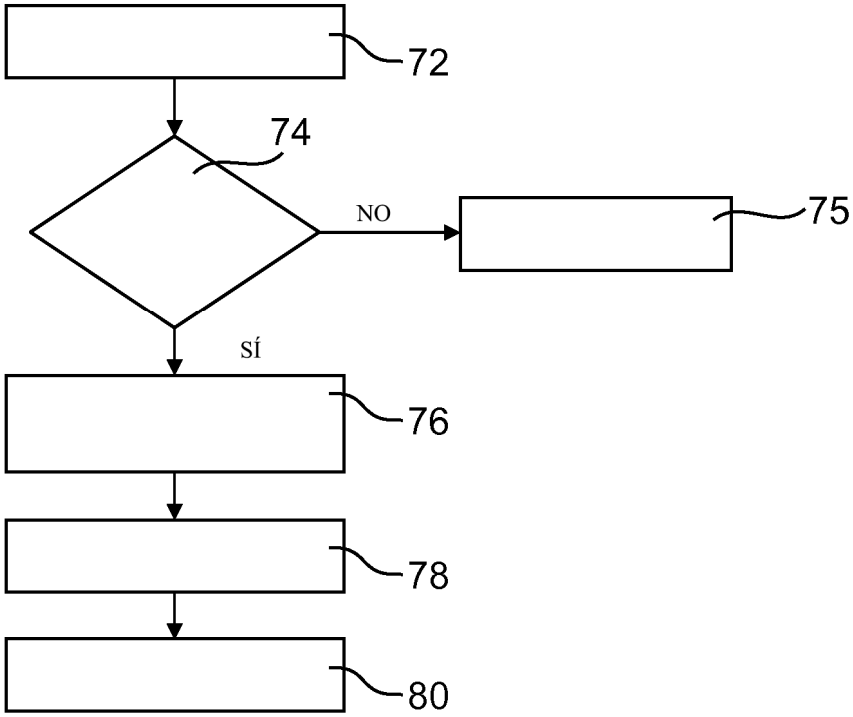

FIG.3