(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 764 127**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/08 (2006.01)
H04L 29/06 (2006.01)
H04W 12/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.12.2016 E 16205913 (3)**

(97) Fecha y número de publicación de la concesión europea: **25.09.2019 EP 3185468**

(54) Título: **Procedimiento de transmisión de datos, procedimiento de recepción de datos, dispositivos y programas correspondientes**

(30) Prioridad:

24.12.2015 FR 1563338

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.06.2020

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

NACCACHE, DAVID;
GERAUD, RÉMI y
BEUNARDEAU, MARC

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de transmisión de datos, procedimiento de recepción de datos, dispositivos y programas correspondientes

1. Campo de la invención

La invención se refiere al campo de las redes de comunicación. Más en particular, la técnica se refiere a la transmisión de datos en redes de comunicación inalámbricas. Todavía más específicamente, la técnica se refiere a la mejora de la seguridad en la transmisión de datos en redes de comunicaciones inalámbricas economizadoras de energía. Con carácter general, tal mejora de la seguridad se opera mediante la transmisión de datos cifrados. Así, la presente técnica trata de la transmisión de datos cifrados en una red de comunicación economizadora de energía y cuyos dispositivos de comunicaciones disponen de cantidad limitada de memoria.

2. Técnica anterior

Cuando es preciso proteger datos que se transmiten por mediación de una red de comunicación, se utilizan técnicas de cifrado de datos. Existen numerosas técnicas de cifrado de datos. Estas se pueden desglosar en dos clases generales: el cifrado simétrico, en el que cada una de las partes que se comunican está en conocimiento de una clave que es utilizada a la vez para cifrar y descifrar los datos; y el cifrado asimétrico, basado en un par de claves: una clave privada y una clave pública. Estas dos clases de técnica de cifrado se utilizan para solucionar problemas particulares de cifrado de datos. Por ejemplo, el cifrado simétrico está adaptado para la copia segura de datos. En efecto, al no estar destinados los datos para ser transmitidos a un tercero, es más simple disponer de una única clave para cifrar los mismos, siendo dicha clave conservada por el usuario con el fin de poder tener nuevamente acceso a sus datos. Por el contrario, cuando se trata de intercambiar datos, a través de una red de comunicación, es preferible la utilización de un cifrado simétrico. Por ejemplo, en el transcurso de una sesión de comunicación, dos entidades que desean comunicarse generan dos pares de claves privadas/públicas. Estos dos pares de claves son utilizados para cifrar y descifrar los datos antes y después de su transmisión.

La criptografía simétrica se utiliza a gran escala, pues es capaz de proporcionar funcionalidades importantes como el cifrado a alta velocidad y a bajo coste, la autenticación de mensajes y la obtención eficaz de resumen. Se habla, por ejemplo, de cifrado autenticado, diseñado para proporcionar a la vez la confidencialidad de los datos, pero, también, la integridad y la autenticidad de los mismos. De este modo, los algoritmos de cifrado simétricos se utilizan en los teléfonos móviles, las tarjetas de crédito, las conexiones inalámbricas. Estas funcionalidades se fundan en el empleo de primitivas criptográficas tales como el cifrado en bloque, el cifrado en flujo o las funciones de resumen. El cifrado en bloque es una técnica segura y eficaz: algoritmos diseñados desde hace una década siguen resistiendo a cualquier intento de ataque en un contexto convencional. De este modo, ha quedado demostrada la resistencia a los ataques estadísticos del algoritmo AES (primitiva simétrica muy empleada). El algoritmo AES ofrece prestaciones suficientes para una amplia gama de contextos de empleo.

Una primitiva simétrica tal como AES es considerada como segura en los modelos de seguridad convencionales cuando es difícil distinguir sus salidas de cadenas aleatorias. Pero, en numerosas aplicaciones, la criptografía es utilizada en un contexto en el que los atacantes tienen acceso a canales de información llamados auxiliares, que no quedan cubiertos en los modelos convencionales de seguridad. Por ejemplo, una implementación de un sistema de televisión de pago debe protegerse contra un atacante que tiene un acceso físico al equipo y puede medir ciertas magnitudes físicas en el curso del cálculo, con el fin de averiguar la clave. En casos extremos, el atacante puede incluso estar capacitado para leer la memoria y extraer de ella las claves. Tales ataques se denominan ataque por canal lateral.

En tales contextos, numerosas implementaciones son vulnerables a ataques practicados por canal lateral. Por otro lado, el diseño de un algoritmo de cifrado en bloque se limita a la definición de una permutación parametrizada mediante una clave. Muchas veces, estos se utilizan para proteger la confidencialidad o la integridad de un dato, a cuyo efecto se deben componer de acuerdo con un modo operativo adecuado. De este modo, la mayoría de las aplicaciones encaminadas a proteger la confidencialidad de un dato precisan, asimismo, de la protección de su integridad. Esta situación conlleva una acusada necesidad de modos operativos eficaces que combinen estas dos propiedades. Los documentos US 2010/0293097 A1 y US 5852665 dan a conocer ejemplos de tales combinaciones de confidencialidad y de integridad.

Por otro lado, la situación se hace aún más compleja con la aparición de nuevas necesidades y de nuevas aplicaciones. Y es que las implementaciones existentes están adaptadas a ciertos tipos de dispositivos: se trata de dispositivos que disponen de considerables recursos, tanto en cuanto a potencia de cálculo como a memoria. En efecto, los actuales terminales de comunicación, tales como los teléfonos inteligentes o las tabletas, no tienen nada que envidiar a los ordenadores personales o portátiles. En cambio, las implementaciones existentes no están adaptadas a los dispositivos que utilizan redes de escaso gasto de energía: se trata, por ejemplo, de los objetos conectados, que utilizan redes de comunicación de escaso gasto de energía, de tipo LORA. En este tipo de red de comunicación, es preciso no utilizar en exceso los recursos necesarios, con el fin de garantizar una longevidad importante de los dispositivos (para no utilizar demasiado los recursos, por ejemplo, la batería). En efecto, una de las

características de los objetos llamados conectados es la de funcionar a batería. Ahora bien, la función que más utiliza esta batería es la función de comunicación (recepción y transmisión de datos). De este modo, las actuales implementaciones, que utilizan muchos recursos para los cálculos criptográficos y muchos recursos para la transmisión/recepción de datos, no están adaptadas a la Internet de los objetos.

Existe, pues, una necesidad de proporcionar tal implementación.

3. Sumario de la invención

La invención no suscita estos problemas del estado de la técnica. Más en particular, la invención aporta una solución simple a la problemática identificada anteriormente. En efecto, la presente técnica trata de un procedimiento de transmisión de datos, procedimiento del tipo de los que consisten en cifrar y en autenticar un dato.

De este modo, la presente técnica se refiere a un procedimiento de transmisión de datos, procedimiento puesto en práctica por un primer dispositivo electrónico, llamado emisor, con destino a un segundo dispositivo electrónico, llamado receptor, procedimiento que comprende la transmisión de un mensaje segmentado en bloques de datos, procedimiento caracterizado por comprender al menos una iteración de una etapa de procesamiento que comprende:

- obtención de un bloque de datos actual;

- cifrado de dicho bloque de datos actual con el concurso de una clave de cifrado, que entrega un bloque de datos cifrados;

- determinación de una etiqueta de longitud aleatoria o pseudoaleatoria en función de dicho bloque de datos cifrados, obteniéndose la longitud de la etiqueta mediante la puesta en práctica de una función secreta basada en la clave de cifrado;

- transmisión de dicho bloque de datos cifrados;

y comprende al menos una etapa de transmisión de al menos una etiqueta según un esquema de transmisión predeterminado.

De este modo, la presente técnica permite difundir valores de control a todo lo largo de la transmisión de los datos cifrados. Esto permite evitar a un receptor descargar el conjunto del mensaje transmitido cuando se detecta un error.

De acuerdo con una característica particular, la etapa de transmisión de al menos una etiqueta se efectúa con cada iteración de la etapa de procesamiento.

De acuerdo con una característica particular, el tamaño de dicha etiqueta b_i está comprendido entre 1 bit y 8 bits.

De acuerdo con una característica particular, dicho procedimiento de transmisión comprende, con anterioridad a la etapa de procesamiento, una etapa de obtención de la clave de cifrado *k*, llamada clave de sesión.

De acuerdo con otro aspecto, la presente técnica se refiere, asimismo, a un dispositivo electrónico de transmisión de datos, llamado emisor, que comprende medios de transmisión de datos con destino a un segundo dispositivo electrónico, llamado receptor, dispositivo que comprende medios de transmisión de un mensaje segmentado en bloques de datos. Tal dispositivo comprende medios de procesamiento iterativos que comprenden:

- medios de obtención de un bloque de datos actual;

- medios de cifrado de dicho bloque de datos actual con el concurso de una clave de cifrado, que entregan un bloque de datos cifrados;

- medios de determinación de una etiqueta b_i de longitud aleatoria o pseudoaleatoria en función de dicho bloque de datos cifrados, obteniéndose la longitud de la etiqueta mediante la puesta en práctica de una función secreta basada en la clave de cifrado;

- medios de transmisión de dicho bloque de datos cifrados;

y comprende medios de transmisión de al menos una etiqueta b_i según un esquema de transmisión predeterminado.

De acuerdo con otro aspecto, la presente técnica se refiere, asimismo, a un procedimiento de recepción de datos, con origen en un dispositivo de transmisión. De este modo, la técnica se refiere a un procedimiento de recepción de datos, representativos de un mensaje segmentado en bloques de datos, procedimiento puesto en práctica por un dispositivo electrónico llamado dispositivo receptor. Tal procedimiento comprende al menos una iteración de las siguientes etapas:

- una etapa de recepción de un bloque de datos cifrados con el concurso de una clave de cifrado;

- una etapa de recepción de una etiqueta b_i correspondiente a una firma de dicho bloque de datos cifrados, teniendo dicha etiqueta una longitud aleatoria o pseudoaleatoria obtenida mediante la puesta en práctica de una función secreta basada en la clave de cifrado;

- una etapa de verificación de una validez de dicha etiqueta recibida con relación a una etiqueta esperada; y

- cuando dicha etiqueta recibida es diferente de dicha etiqueta esperada, una etapa de procesamiento diferencial de al menos un bloque de datos cifrados válido recibido anteriormente.

De acuerdo con una forma particular de realización, dicha etapa de recepción de un bloque de datos cifrados comprende una etapa de inserción de dicho bloque de datos cifrados en una primera cola de tamaño predeterminado.

De acuerdo con una forma particular de realización, dicha etapa de procesamiento diferencial de al menos un bloque de datos cifrados válido recibido anteriormente comprende:

- una etapa de determinación de una ubicación de invalidación, en el seno de una segunda cola;

- al menos una etapa de procesamiento de los datos insertados en la segunda cola hasta la ubicación de invalidación;

- una etapa de parada del procesamiento.

De acuerdo con otro aspecto, la presente técnica se refiere, asimismo, a un Dispositivo electrónico de recepción de datos, siendo dichos datos representativos de un mensaje segmentado en bloques de datos, procedimiento puesto en práctica por un dispositivo electrónico llamado dispositivo receptor. Tal dispositivo comprende medios de procesamiento iterativos que comprenden:

- medios de recepción de un bloque de datos cifrados, correspondiente a un bloque de datos del mensaje cifrado con el concurso de una clave de cifrado;

- medios de recepción de una etiqueta b_i correspondiente a una firma de dicho bloque de datos cifrados, teniendo dicha etiqueta una longitud aleatoria o pseudoaleatoria obtenida mediante la puesta en práctica de una función secreta basada en la clave de cifrado;

- medios de verificación de una validez de dicha etiqueta recibida con relación a una etiqueta esperada; y

- medios de procesamiento diferencial de al menos un bloque de datos cifrados válido recibido anteriormente, puestos en práctica cuando dicha etiqueta recibida es diferente de dicha etiqueta esperada.

De acuerdo con una implementación preferida, las diferentes etapas de los procedimientos según la invención se llevan a la práctica mediante uno o varios equipos lógicos o programas de ordenador, que comprenden instrucciones lógicas destinadas a ser ejecutadas por un procesador de datos de un dispositivo según la invención y que está diseñado para regir la ejecución de las diferentes etapas de los procedimientos.

En consecuencia, la invención también está encaminada a un programa, susceptible de ser ejecutado por un ordenador o por un procesador de datos, incluyendo este programa instrucciones para regir la ejecución de las etapas de un procedimiento tal como se ha mencionado anteriormente.

Este programa puede utilizar cualquier lenguaje de programación y presentarse en forma de código fuente, código objeto, o de código intermedio entre código fuente y código objeto, tal como en una forma compilada parcialmente, o en cualquier otra forma deseable.

La invención también se encamina a un soporte de información legible por un procesador de datos y que incluye instrucciones de un programa tal y como se ha mencionado anteriormente.

El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD-ROM o una ROM de circuito microelectrónico, o también un medio de registro magnético, por ejemplo un disquete (floppy disc) o un disco duro.

Por otra parte, el soporte de información puede ser un soporte transmisible, tal como una señal eléctrica u óptica, que se puede conducir a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención se puede descargar en particular por una red de tipo Internet.

Alternativamente, el soporte de información puede ser un circuito integrado en el que va incorporado el programa, estando adaptado el circuito para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

De acuerdo con una forma de realización, la invención se lleva a la práctica por medio de componentes de soporte lógico y/o de soporte físico. En esta línea, el término "módulo" puede corresponder, en este documento, tanto a un

componente de soporte lógico, como a un componente de soporte físico o a un conjunto de componentes de soporte físico y lógico.

Un componente de soporte lógico corresponde a uno o varios programas de ordenador, uno o varios subprogramas de un programa o, de manera más general, a todo elemento de un programa o de un soporte lógico apto para llevar a la práctica una función o un conjunto de funciones, según lo descrito a continuación en relación con el módulo de que se trate. Tal componente de soporte lógico es ejecutado por un procesador de datos de una entidad física (terminal, servidor, pasarela, encaminador, etc.) y está posibilitado de acceso a los recursos de soporte físico de esta entidad física (memorias, soportes de grabación, buses de comunicación, tarjetas electrónicas de entrada/salida, interfaces de usuario, etc.).

De la misma manera, un componente de soporte físico corresponde a todo elemento de un conjunto de soporte físico (o hardware) apto para llevar a la práctica una función o un conjunto de funciones, según lo descrito a continuación en relación con el módulo de que se trate. Puede ser un componente de soporte físico programable o con procesador integrado para la ejecución de soporte lógico, por ejemplo un circuito integrado, una tarjeta inteligente, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microprograma (firmware), etc.

Por supuesto, cada componente del sistema anteriormente descrito pone en práctica sus propios módulos de lógica.

Las diferentes formas de realización antes mencionadas son combinables entre sí para la puesta en práctica de la invención.

4. Dibujos

Otras características y ventajas de la invención se pondrán más claramente de manifiesto con la lectura de la siguiente descripción de una forma preferente de realización, dada a título de mero ejemplo ilustrativo y no limitativo, y de los dibujos que se acompañan, de los que:

la figura 1 presenta un sinóptico de la técnica propuesta para la transmisión de datos;

la figura 2 presenta un sinóptico de la técnica propuesta para la recepción de datos;

la figura 3 describe una forma de realización de una técnica de procesamiento diferencial de datos, en el receptor;

la figura 4 describe sucintamente la arquitectura de un dispositivo electrónico de transmisión; y

la figura 5 describe sucintamente la arquitectura de un dispositivo electrónico de recepción.

5. Descripción

5.1. Recapitulación del principio general

El cifrado autenticado es un enfoque que permite la puesta en práctica de una confidencialidad de los datos intercambiados y de un aseguramiento de la integridad de estos datos al mismo tiempo. El cifrado autenticado se opone al cifrado, por una parte, y a la generación de códigos de autenticación de mensajes (MAC), por otra.

El cifrado autenticado generalmente produce mensajes de la forma

$$C / B$$

donde *C* es un mensaje cifrado y *B* es una etiqueta (también denominada tag). La etiqueta B se calcula, de acuerdo con las formas de realización, bien sobre el mensaje cifrado, o bien sobre el mensaje descifrado (mensaje en claro). Un inconveniente de este enfoque es que se debe recibir (y registrar) el mensaje completo C antes de que se pueda verificar la etiqueta B. Si se da el caso de que el mensaje cifrado C es incorrecto (es decir, que la etiqueta recibida no se corresponde con una etiqueta esperada –calculada por el receptor–), la etapa de recepción ha sido puesta en práctica para nada, lo cual ha acarreado una considerable pérdida de recursos para el receptor (tiempo empleado, energía utilizada, ancho de banda consumido, memoria RAM utilizada). Este enfoque, claramente, no es adecuado para las redes de comunicación de bajo consumo ni para los dispositivos que disponen de pocas capacidades de procesamiento (especialmente, memoria RAM disponible).

De este modo, para paliar los problemas conocidos de la técnica anterior, en lo sucesivo se describe un nuevo procedimiento de cifrado autenticado, al vuelo, procedimiento que comprende una latencia constante y cuya seguridad está demostrada con respecto a un modelo de atacante del cual se considera que tiene un acceso completo a la información relativa al comportamiento del sistema de recepción.

El principio general de la técnica descrita consiste en calcular etiquetas representativas de firmas de los bloques de datos y en “enjambrar” etiquetas a todo lo largo de la transmisión de estos bloques de datos cifrados, del emisor hacia el receptor. De este modo, esta enjambrazón permite al receptor corroborar con mayor rapidez que un bloque de datos no se corresponde con un bloque de datos esperado y, por tanto, no tener que almacenar el mensaje C

íntegramente antes de procesarlo. Así, se ahorra una gran cantidad de memoria RAM y se limita el uso del ancho de banda de la red. Dicho de otro modo, la invención se refiere a un procedimiento de transmisión de datos y a un procedimiento correspondiente de recepción de datos. De acuerdo con la invención, el procedimiento de transmisión de datos efectúa un procesamiento criptográfico sobre los datos que han de transmitirse, después de haber sido previamente segmentados en bloques estos datos, y calcula una etiqueta representativa de cada bloque de datos cifrados. La etiqueta se transmite a continuación de manera que un atacante no esté en condiciones de reproducir una transmisión correcta de etiquetas. Por su parte, el procedimiento de recepción se asegura de que, cuando se recibe una etiqueta incorrecta (debido a un intento de ataque), no sea detenido inmediatamente el procesamiento de los bloques de datos, sino que se ponga en práctica un procesamiento diferencial con el fin de interferir en un intento de análisis del comportamiento del receptor.

Por lo tanto, se efectúa una aleatorización tanto en el emisor, que transmite las etiquetas de tal manera que son difícilmente interpretables por el atacante (a causa del tamaño de los datos, su frecuencia de transmisión o su ubicación en la transmisión), como en el receptor, que procesa estos datos de manera diferencial, es decir, la recepción de un dato fraudulento (que se le supone estar forjado por el atacante) no necesariamente acarrea una interrupción inmediata de procesamiento (que daría al atacante un indicio acerca del lugar donde ha sido fallido su ataque).

Otras características de la presente técnica consisten en:

- un mecanismo de detección de valor de uso único (nonce) que impide la reutilización de estos valores con el objetivo de construir un ataque de repetición.

y

- un mecanismo de toma en cuenta de los datos recibidos diferencial: este mecanismo construye una resistencia contra el atacante;

o por ejemplo, el procesamiento diferencial de los datos recibidos puede consistir en un mecanismo de tiempo de parada variable que limite la fuga de información en caso de error;

o otro ejemplo de procesamiento diferencial consiste en seguir aceptando la recepción de los datos que se sabe que son falsos: entonces, se efectúan procesamientos aleatorios sobre estos datos, comprendiendo a la vez, estos procesamientos, etapas de procesamiento real y etapas de procesamiento aleatorias.

La construcción de conjunto del procedimiento está diseñada para los dispositivos emisores y receptores que disponen de escasas capacidades computacionales, al propio tiempo que se limitan los intercambios en las redes de comunicación (IdO / 5G / Big Data).

Así, el principio general de la técnica consiste en dispersar (enjambrar) etiquetas dentro del propio mensaje cifrado, con el fin de que se pueda realizar al vuelo la autenticación de los datos recibidos. Si se produce un error, se puede abortar el resto del mensaje. Formalmente, un mensaje, transmitido por el emisor y recibido por el receptor, tiene la siguiente forma:

$$C_1 \mid b_1 \mid C_2 \mid b_2 \mid \cdots \mid C_n \mid b_n$$

donde C_i son bloques de texto cifrado y las b_i son etiquetas cortas (cuyo tamaño está comprendido entre 1 y 8 bits). Se trata de un esquema de transmisión de las etiquetas uniforme: una etiqueta b_i se transmite después de cada bloque de datos. En lo sucesivo se describen otros esquemas de transmisión de las etiquetas. De acuerdo con una variante, una b_i es un único bit, cuyo valor puede ser 0 ó 1. Se supone que, anteriormente, ha sido construida o determinada entre el emisor y el receptor una clave compartida *k*. Tal como se presenta en lo sucesivo, la ubicación, la frecuencia y el valor de las b_i que se van dispersando dentro del mensaje a medida que se transmite se eligen para volver muy compleja la labor de un atacante.

El modelo de atacante, precisamente, está elegido intencionadamente que sea más fuerte y avezado que los modelos considerados tradicionalmente. Se asume que el atacante puede escuchar, insertar, modificar o reorganizar los paquetes transmitidos al receptor, y que puede observar el comportamiento del destinatario con el fin de determinar si estos cambios tienen un efecto sobre la parada o la prosecución de la recepción de los datos (y la prosecución de los procesamientos subyacentes a la recepción de estos datos): se trata de ataque de maleabilidad. Por ejemplo, el atacante puede intentar transmitir a su víctima un flujo de vídeo, y está en condiciones de comprobar un fracaso de esta transmisión cuando el vídeo se detiene. Con ayuda de este modelo, se quiere tener asegurado que no se pueda forjar ningún bloque de datos malicioso. Este aseguramiento se proporciona con una elevada probabilidad.

De acuerdo con la presente técnica, para resistir a los ataques de maleabilidad, es preciso que el valor de una bi dada dependa de todos los bloques (C_1, ..., C_i) transmitidos anteriormente,

a saber:

$$b_i = Fk\ (H\ (C_1 |\cdots| C_i))$$

donde H es una función de resumen y Fk, una PRF ("*Pseudo Random Function Family*"). En criptografía, una familia de función pseudoaleatoria, abreviado como *PRF*, es una colección de funciones calculables eficazmente que emulan un oráculo aleatorio de la forma siguiente: ningún algoritmo eficaz puede distinguir (con ventaja significativa) entre una función elegida al azar de entre la familia PRF y un oráculo aleatorio (una función cuyas salidas se fijan completamente al azar).

Por sí solo, tal modo de transmisión de datos ya está en condiciones de obstaculizar un ataque estándar, ataque que no tiene en cuenta los intercambios ya realizados anteriormente.

Sin embargo, habida cuenta del modelo de adversario adoptado, tal modo de transmisión puede ser atacado por un atacante con comportamiento activo, como sigue: cuando el atacante observa que el mensaje malicioso que trata de transmitir es rehusado en un lugar "*i*", lo cual significa que la etiqueta b_i es incorrecta. Le basta entonces al atacante con intentar la transmisión de una nueva etiqueta b_i y reenviar todo el mensaje. Así, teóricamente es posible encontrar la bi correcta (es decir, el valor correcto de de b_i) para todos los "*i*" sucesivos.

Ahora bien, uno de los objetivos de la presente técnica es, precisamente, poder resistir a tal comportamiento del adversario, en al menos una forma de realización. De este modo, se describe, en la forma de realización que sigue, una técnica que permite conservar el nivel de refuerzo de la seguridad proporcionado por la presente técnica, incluso en presencia de un adversario que dispone de un acceso al receptor, acceso que permite determinar el comportamiento del receptor.

El principio general de la presente técnica comprende, por una parte, un procedimiento de transmisión de datos (figura 1) y, por otra, un procedimiento de recepción de datos (figura 2).

De este modo, se propone un procedimiento de transmisión de datos, procedimiento puesto en práctica por un primer dispositivo electrónico, llamado emisor, con destino a un segundo dispositivo electrónico, llamado receptor, procedimiento que comprende la transmisión de un mensaje segmentado en bloques de datos (A_1, ...,A_n). El procedimiento de transmisión comprende al menos una iteración de una etapa de procesamiento (20) que comprende:

- obtención (20-1) de un bloque de datos actual Ai;
- cifrado (20-2) de dicho bloque de datos actual Ai, que entrega un bloque de datos cifrados Ci;
- determinación (20-3) de una etiqueta bi en función de dicho bloque de datos cifrados Ci;
- transmisión (20-4) de dicho bloque de datos cifrados C_i;

y por comprender al menos una etapa de transmisión de al menos una etiqueta b_i según un esquema de transmisión predeterminado.

El esquema de transmisión predeterminado consiste en transmitir la etiqueta de una manera tal que el atacante tiene dificultades para comprender, por una parte, cuándo es transmitida la etiqueta y cuándo no lo es y, por otra, para conocer el valor que debería tener esta etiqueta. Por otro lado, se elige deliberadamente un tamaño de etiqueta adaptado. Más en particular, el tamaño de la etiqueta está comprendido entre 1 y 8 bits, lo cual hace la etiqueta, por una parte, poco consumidora de ancho de banda y sencilla de generar. El esquema de transmisión predeterminado, según la presente técnica, es un esquema de transmisión de las etiquetas que tiene como consecuencia el hacer variar la transmisión de las etiquetas en tiempo y/o en frecuencia y/o en longitud (de etiquetas). Dicho de otro modo, el atacante no sabe (o, en todo caso, no puede estar seguro) cómo se transmiten las etiquetas: porque, por ejemplo, las etiquetas se transmiten de manera regular (después de cada bloque de datos), pero tienen en cada ocasión un tamaño aleatorio y/o las etiquetas se transmiten por bloques, después de un cierto número de bloques de datos (transmisión por bloques que se determina, asimismo, aleatoriamente) y/o sólo se transmite una etiqueta cada x bloques y esta etiqueta se corresponde con la de los x bloques a la vez. Tenemos, pues, potencialmente, una variación en tiempo, en frecuencia y en longitud, y esta variación está predeterminada y se basa en una determinación aleatoria y/o pseudoaleatoria del lado del emisor. El receptor, en virtud de una sincronización previa o de la utilización de funciones idénticas a las del emisor, asimismo, está en condiciones de saber cuáles son las variaciones utilizadas por el emisor y, por tanto, de estar en conocimiento del esquema de transmisión predeterminado.

Asimismo, se describe un procedimiento de recepción de datos, representativos de un mensaje segmentado en bloques de datos (A_1, ..., A_n), procedimiento puesto en práctica por un dispositivo electrónico llamado dispositivo receptor. Tal procedimiento comprende al menos una iteración de las siguientes etapas:

- una etapa de recepción (R20-1) de un bloque de datos cifrados Ci;

- una etapa de recepción (R20-2) de una etiqueta b_i correspondiente a una firma de dicho bloque de datos cifrados C_i;

- una etapa de verificación (R20-3) de una validez de dicha etiqueta bi recibida con relación a una etiqueta biA esperada; y

- cuando dicha etiqueta b_i recibida es diferente de dicha etiqueta b_{iA} esperada, una etapa de procesamiento diferencial (R20-4) de al menos un bloque de datos cifrados válido recibido anteriormente.

El procesamiento diferencial consiste en no parar inmediatamente el procesamiento de los datos recibidos, con el fin de hacer creer al atacante que, en realidad, los datos (que el dispositivo receptor sabe que son erróneos) se han considerado como válidos. El hecho de seguir procesando los datos recibidos, como si fueran válidos, se puede efectuar de diferentes maneras.

Un caso de uso típico de la presente técnica es la puesta en práctica de una transmisión de datos unidireccional, de una entidad emisora, como por ejemplo un objeto conectado, hacia una entidad receptora, como por ejemplo un punto de acceso o una pasarela LORA. Otro caso de uso es inverso: se trata de una entidad emisora de tipo punto de acceso o una pasarela LORA que transmite datos a un objeto conectado. La presente técnica encuentra aplicación, asimismo, en una red celular de tipo UNB (del inglés, por “Ultra Narrow Band”).

La invención no queda limitada en modo alguno, sin embargo, a tal puesta en práctica, y puede aplicarse a todo tipo de transmisión de datos segura, por ejemplo en el ámbito de un intercambio de datos entre dos ordenadores conectados a una red de comunicación (ya sea ésta cableada o inalámbrica) o entre un terminal y un servidor.

5.2. Descripción de una forma de realización

En esta forma de realización, se describe más explícitamente la técnica expuesta anteriormente, asumiendo que el adversario está en condiciones de interaccionar con el receptor de manera avanzada. Se asume, en especial, que el adversario está en condiciones de reemitir bloques de datos y etiquetas cuando comprueba que una etiqueta dada no permite validar un bloque que ha transmitido anteriormente. Para evitar esta problemática, en esta forma de realización, se ponen en práctica dos técnicas, de manera complementaria.

La primera técnica puesta en práctica consiste en la utilización de un parámetro utilizado para calcular las etiquetas (el nonce, que se puede transmitir en claro, por lo que, *a priori*, no es un secreto) para cada sesión de comunicación del emisor hacia el receptor (para cada transmisión de mensaje). La utilización de un nonce diferente en cada sesión de comunicación permite asegurar, al receptor, una capacidad de detección de reutilización de un nonce anterior. De este modo, el cálculo de las etiquetas cambia en cada sesión, impidiendo a un atacante “repetir” bloques de datos que hubiera podido interceptar y manipular anteriormente. Esta capacidad de detección permite al receptor detectar un intento de usurpación de manera rápida. Como se detalla en lo sucesivo, el mecanismo de detección puesto en práctica en el receptor no es consumidor de energía y no precisa de comunicación bidireccional.

La segunda técnica, puesta en práctica junto con la primera, es introducir una incertidumbre, del lado del receptor, acerca del momento en que una etiqueta b_i es considerada como falsa. Esta técnica, combinada con la primera, permite desorientar al atacante. En efecto, éste ya no está capacitado para determinar, observando con atención el funcionamiento del receptor, cuáles son los datos transmitidos que han causado la parada de la recepción de los datos por parte del receptor.

- Dicho de otro modo, la utilización de las dos técnicas mencionadas anteriormente permite ocultar, ofuscar, el funcionamiento real del receptor, y ello sin precisar de recursos suplementarios por parte del receptor y sin ralentizar sustancialmente la velocidad de transmisión por la red.

5.2.1. Procedimiento de transmisión de datos cifrados

En esta forma de realización, se utiliza una clave diferente en cada sesión de comunicación entre el emisor y el receptor.

Esta solución exige que se elija un nonce para cada sesión. Pero si el nonce es transmitido con el mensaje (como habitualmente se hace), el atacante podría controlar la transmisión de este nonce y forzar una reutilización del mismo. Como variante, el nonce podría ser transmitido por el receptor, pero esto precisaría entonces de una comunicación bidireccional. Ahora bien, el procedimiento de la presente técnica no se pone en práctica necesariamente en el ámbito de una comunicación bidireccional. De este modo, para resistir a un ataque de tipo “repetición” (reutilización de un nonce ya utilizado por el atacante), se construye una entidad receptora con estado (“stateful” en inglés). Para este fin, es posible, por ejemplo, utilizar herramientas estadísticas para determinar si un nonce es legítimo o si se trata de un intento de engañar al receptor. Por esta razón, se puede, por ejemplo, poner en práctica, en el seno del receptor, un mecanismo de tipo “SQF”, (del inglés, por “Streaming Quotient Filter”). De acuerdo con la presente, tal mecanismo se adapta particularmente bien por cuanto permite detectar eficazmente los duplicados en un flujo de datos, teniendo al propio tiempo unas exigencias restringidas de memoria. Un mecanismo de tipo filtro de Bloom es también una posibilidad más conocida que SQF para detectar duplicados. Pero este

mecanismo es menos interesante en la aplicación que se persigue, pues es generalmente más ávido en cuanto a recursos.

Se hace constar que, en cualquier caso, un atacante tiene una probabilidad de 2^{-l} de transmitir *l* bloques a una entidad receptora antes de ser detectado como un atacante.

El procedimiento de transmisión de datos cifrados, de acuerdo con la forma de realización descrita presentemente, comprende:

- una selección, en función de una clave de cifrado *k*, de entre una pluralidad de posibles claves de cifrado; y

al menos una iteración de las siguientes etapas:

- obtención de un bloque de datos que ha de cifrarse Ai;
- cifrado, con el concurso de dicha clave de cifrado k, de dicho bloque de datos que ha de cifrarse Ai, que entrega un bloque de datos cifrados Ci;
- determinación, en función de dicho bloque de datos cifrados Ci, de al menos una etiqueta bi;
- transmisión de dicho bloque de datos cifrados C_i y de dicha al menos una etiqueta b_i;

Por supuesto, dependiendo de las formas de realización, es posible introducir algunas variantes en el procedimiento descrito anteriormente cumpliendo dos criterios: el primer criterio consiste en limitar al máximo el número de etiquetas que han de transmitirse además de los datos cifrados; es preciso conservar un procedimiento de transmisión de datos cifrados que tenga escaso gasto de energía y que limite la cantidad de datos supernumeraria (es decir, datos que no son datos útiles); el segundo criterio es el de la simplicidad de los procesamientos realizados del lado entidad de recepción: es menester conservar un procesamiento simple para la entidad de recepción, con el fin de asegurar que el gasto de energía necesaria para este procesamiento sea mínimo. Así, se pueden definir varias variantes del esquema de transmisión de las etiquetas b_i, con el fin de hacer todavía más compleja la labor del atacante.

De esta manera, en una primera variante, las etiquetas b_i son distribuidas (transmitidas) de manera aleatoria o pseudoaleatoria; esto significa que, para un observador exterior, no es posible adivinar cuándo debe ser transmitida una etiqueta b_i. En otras palabras, esto significa que no hay predictibilidad en la transmisión de las etiquetas. De este modo, un bloque de datos C_i puede venir seguido de la transmisión de una etiqueta, mientras que el bloque siguiente C_{i+1} no lo está. Esta transmisión aleatoria o pseudoaleatoria de la etiqueta está relacionada con la clave *k*, determinada anteriormente para la sesión de transmisión. Una operación realizada sobre la clave k, con posterioridad a la transmisión del bloque actual, permite decidir la transmisión de una etiqueta actual. Por supuesto, esta operación, realizada sobre la clave k, es secreta.

Se introduce, pues, con esta variante, una variabilidad del valor de la etiqueta y una variabilidad de la presencia de la etiqueta.

En una segunda variante, la longitud de cada etiqueta se determina de manera aleatoria o pseudoaleatoria; esto significa que, para un observador exterior, no es posible adivinar cuál debe ser la longitud de una etiqueta b_i. En otras palabras, esto significa que no hay predictibilidad en la longitud de las etiquetas. De este modo, aun si se transmite una etiqueta después de cada bloque de datos, la longitud de esta etiqueta no es predecible. Esto también es así, por extensión, para el valor de la etiqueta. Por ejemplo, una etiqueta bi puede ser de longitud de 1 bit: puede tomar entonces la etiqueta el valor 0 o el valor 1. La siguiente etiqueta puede ser de longitud de dos bits: la etiqueta puede tomar entonces los valores ‘00’ o ‘01’ o ‘10’ u ‘11’. Por lo tanto, al atacante, al no estar en condiciones de conocer la longitud de la etiqueta, le cuesta todavía más trabajo adivinar el valor de la misma. El cálculo de esta longitud de la etiqueta se realiza poniendo en práctica una función secreta basada en la clave *k*.

Consiste una tercera variante en la combinación de la primera y de la segunda variante.

Una cuarta variante consiste en la combinación de la primera y de la segunda variante, con la añadidura de una funcionalidad suplementaria: se supone que la longitud estándar de una etiqueta es de 1 bit. En esta cuarta variante, con posterioridad al cifrado de un bloque C_i, se realizan las siguientes operaciones, poniendo en práctica una función secreta dependiente de la clave *k*:

- cálculo de la presencia de una etiqueta bi;
- cálculo de la longitud de la etiqueta bi, en función de la última etiqueta transmitida;
- cálculo del valor de cada bit de la etiqueta b_i en función de los bloques C_i (y C_{i-1}, C_{i-2}, etc.) anteriormente cifrados.

Dicho de otro modo, con posterioridad al cifrado de un bloque Mi, una función, dependiente de la clave *k*, permite:

- determinar si se transmite o no una etiqueta;
- determinar la longitud de esta etiqueta en función de la longitud de las etiquetas transmitidas anteriormente;
- determinar el valor de los bits que componen esta etiqueta en función de los bloques transmitidos anteriormente.

Tal implementación no significa que la etiqueta b_i dependa de todas las etiquetas precedentes. Por ejemplo, si la etiqueta b_i transmitida anteriormente era de longitud 1 bit y dependía del bloque C_i (y de los bloques precedentes), por su parte, la etiqueta b_{i+1} puede ser, con total independencia, de una longitud de dos bits, dependiendo el primer bit del bloque C_{i-1} (y de los bloques precedentes) y dependiendo el segundo bit del bloque C_{i+1} (y de los bloques precedentes). La ventaja de esta forma de realización está en que, aun si el atacante dispone del conjunto de los valores unitarios (0 ó 1), correspondientes a cada bloque, el atacante no puede adivinar cómo serán transmitidos estos datos: en efecto, al ser aleatoria o pseudoaleatoria la distribución de estos valores y al estar ligada a una clave de sesión *k*, el atacante no puede adivinar cuál será la distribución de los mismos.

5.2.2. Procedimiento de recepción de datos cifrados

Como anteriormente se ha indicado, es un objetivo de la presente técnica, aparte del hecho de tener escaso gasto de energía, de ancho de banda y de memoria consumida del lado receptor, el poder resistir a ataques por canal lateral. Se supone, en efecto, que un eventual atacante está capacitado para tener acceso al dispositivo receptor de los datos y que está capacitado para observar el comportamiento de este dispositivo, con el fin de determinar los debidos datos que han de transmitirse en el caso de una usurpación o de un ataque. Sabido es que los ataques por canal lateral se basan en la observación de diversos parámetros que son representativos de un cierto tipo de actividad. A partir de este momento, con el fin de hacer muy difícil esta observación, el procedimiento de recepción de los datos cifrados comprende, además de las etapas de recepción de los datos cifrados C y de la etiqueta B, unas etapas de ocultación del procesamiento realizado en la recepción de los datos. Más en particular, estas etapas de ocultación son simples y no precisan de cálculos complejos. Y es que no es deseable que el receptor realice cálculos demasiado intensivos que tuvieran una influencia negativa sobre su autonomía.

De este modo, para evitar aceptar y procesar bloques de datos maliciosos, al propio tiempo que se añade una incertidumbre (ante el atacante) acerca del bloque de datos que ha provocado la parada (y, por tanto, introduciendo una incertidumbre acerca del tiempo del procesamiento como tal), se introducen (véase la figura 3) dos colas FIFO, en memoria RAM: la cola (1) (a la derecha en el esquema) y la cola (2) (a la izquierda en el esquema).

Los bloques de datos se van insertando en la cola (1) conforme van llegando. La cola (1) comprende el espacio necesario para 128 bloques de datos. La probabilidad que tiene el adversario de conseguir generar una secuencia de 128 etiquetas b_i correctas es de 2^{-128}. De este modo, se considera que, cuando un bloque de datos (C_i) deja la cola (1) (porque la misma está llena), es válido con una fuerte probabilidad. Los bloques salientes de la cola (1) se introducen en la cola (2), que es de tamaño *m*. Los paquetes salientes de la cola (2) son utilizados a continuación (si son correctos).

Cuando un bloque de datos C_i, que se encuentra en la cola (1), es detectado como incorrecto (porque la etiqueta con la que se corresponde este bloque de datos es incorrecta), se aplica la siguiente operativa de procesamiento:

- se selecciona al azar una posición *j* en la cola (2) (por ejemplo, según una operativa descrita a continuación); la posición *j* es la ubicación de invalidación;
- todos los bloques de datos que se encuentran después de la posición j en la cola (2) son transmitidos para procesamiento;
- se detiene la comunicación.

Dicho de otro modo, cuando se detecta un bloque de datos incorrecto en la cola (1), se determina un tiempo (plasmado en la ubicación de invalidación *j*) a partir del cual, en la cola (2), los bloques de datos transmitidos anteriormente no serán procesados. Esta técnica presenta dos ventajas: la primera dimana del hecho de que se minimiza el riesgo de toma en cuenta de un bloque de datos que hubiera podido “escapar” al procesamiento de control de las etiquetas b_i. En efecto, abortando el procesamiento en la cola (2), se asegura que, aun si, por error, se ha podido tomar por correcto un bloque de datos de la cola (1), éste no tendrá tiempo para ser tenido en cuenta a efectos de ulterior procesamiento. La segunda ventaja, como se ha explicitado anteriormente, radica en el hecho de que el atacante no está en condiciones de detectar cuál es la etiqueta (o el bloque de datos) que ha provocado la interrupción de procesamiento. A partir de este momento, el atacante, si pretende efectuar una nueva tentativa, tiene que, por una parte, hacerse con la nueva clave de sesión y, por otra, forjar una nueva sucesión de bloques de datos cifrados y una nueva sucesión de etiquetas, sin certeza, no obstante, de que esta nueva tentativa lleve a un mejor resultado.

Se plantea una cuestión acerca de la manera en que se selecciona la ubicación *j*. Es necesario, efectivamente, evitar que esta ubicación pueda ser predicha por el atacante, en defecto de lo cual, el conjunto de la operativa sería inútil.

Cabe contemplar, al menos, dos variantes de selección:

- la primera variante consiste en seleccionar la ubicación j en función del mensaje transmitido; se trata de una selección determinista, realizada por el receptor en función del contenido del propio mensaje;

- la segunda variante consiste en seleccionar la ubicación *j* de manera aleatoria, según una distribución dada.

Sin abordar los detalles matemáticos, que no son objeto de la presente, los inventores han demostrado que una selección aleatoria, según una distribución de probabilidad uniforme, era una manera eficaz de seleccionar una ubicación *j*.

Se pueden ajustar eficazmente otros parámetros, en función de las formas de realización, para incrementar la eficiencia del proceso que se acaba de describir. Entre estos parámetros, en especial, se puede ajustar:

- el tamaño *m* de la cola (2): cuanto más larga sea la cola, mayor tiempo necesitará el atacante para aprender cuál es el bloque de datos o la etiqueta errado (es decir, el que ha permitido detectar el ataque); con la contrapartida de una mayor latencia en el procesamiento;

- de la misma manera, el tamaño de la cola (1) se puede ajustar con el fin de disminuir los riesgos de una introducción fraudulenta de un bloque de datos en la cola (2); esto ya se ha explicitado anteriormente;

- como corolario, un parámetro importante para la detección se refiere a la cantidad de memoria disponible para efectuar los procesamientos de toma en cuenta en el receptor; cuanto mayor sea la cantidad de memoria, más se aumentará el nivel de seguridad.

5.3. Otras características y ventajas

Se describe, en relación con la figura 4, un dispositivo emisor puesto en práctica para transmitir datos cifrados, según el procedimiento descrito previamente.

Por ejemplo, el dispositivo emisor comprende una memoria 41 constituida a partir de una memoria intermedia, una unidad de procesamiento 42, equipada, por ejemplo, con un microprocesador y pilotada por el programa de ordenador 43, que pone en práctica un procedimiento de transmisión de datos cifrados. Con la inicialización, las instrucciones de código del programa de ordenador 43 se cargan, por ejemplo, en una memoria, antes de ser ejecutadas por el procesador de la unidad de procesamiento 42. La unidad de procesamiento 42 recibe como entrada al menos un dato representativo de un mensaje M que ha de transmitirse a un receptor. El microprocesador de la unidad de procesamiento 42 pone en práctica las etapas del procedimiento de transmisión, según las instrucciones del programa de ordenador 43 para segmentar el mensaje en bloques de datos, cifrar cada bloque de datos con el concurso de una clave de cifrado *k* y calcular etiquetas *b* (representativas de firmas asociadas a los bloques de datos cifrados) y transmitir los bloques de datos cifrados y las etiquetas *b* según un esquema de transmisión. Como se ha explicitado, este esquema de transmisión puede ser determinista y depender de la clave de cifrado.

Para ello, el dispositivo emisor comprende, aparte de la memoria intermedia 41, unos medios de comunicación, tales como módulos de comunicación en red, medios de transmisión de datos y, ocasionalmente, un procesador de cifrado dedicado.

El conjunto de estos medios puede materializarse en forma de un procesador particular implementado en el seno del dispositivo, siendo dicho procesador un procesador seguro. De acuerdo con una forma particular de realización, este dispositivo emisor pone en práctica una aplicación particular que es la encargada de la realización del cifrado y de la transmisión de datos, siendo proporcionada esta aplicación, por ejemplo, por el fabricante del procesador en cuestión, con el fin de permitir la utilización de dicho procesador. Para llevarlo a cabo, el procesador comprende medios de identificación únicos. Estos medios de identificación únicos permiten asegurar la autenticidad del procesador.

Por otro lado, el dispositivo emisor comprende, además, medios de obtención de clave de cifrado, según un modelo con estado (“stateful”), medios que permiten obtener una nueva clave de cifrado en cada nueva sesión de transmisión de datos.

Se describe, en relación con la figura 5, un dispositivo receptor puesto en práctica para recibir datos cifrados, con origen en un dispositivo emisor, según el procedimiento descrito previamente.

Por ejemplo, el dispositivo receptor comprende una memoria 51 que comprende una memoria intermedia, una unidad de procesamiento 52, equipada, por ejemplo, con un microprocesador y pilotada por el programa de ordenador 53, que pone en práctica un procedimiento de recepción de datos cifrados.

Con la inicialización, las instrucciones de código del programa de ordenador 53 se cargan, por ejemplo, en una memoria, antes de ser ejecutadas por el procesador de la unidad de procesamiento 52. La unidad de procesamiento 52 recibe como entrada al menos un bloque de datos cifrados y al menos una etiqueta b, representativa de una firma de bloque de datos cifrados. El microprocesador de la unidad de procesamiento 52 pone en práctica las etapas del procedimiento de recepción, según las instrucciones del programa de ordenador 53, para controlar la validez de las etiquetas recibidas en función de los bloques de datos cifrados y efectuar un procesamiento diferencial de los datos recibidos en función de la validez de estas etiquetas.

Para ello, el dispositivo comprende, aparte de la memoria intermedia 51, unos medios de comunicación, tales como módulos de comunicación en red, medios de transmisión de datos y, ocasionalmente, un procesador de cifrado independiente.

El conjunto de estos medios puede materializarse en forma de un procesador particular implementado en el seno del dispositivo receptor, siendo dicho procesador un procesador seguro y/o sirviéndose de una memoria segura (Msec). De acuerdo con una forma particular de realización, este dispositivo pone en práctica una aplicación particular que es la encargada de la realización de la recepción y del control de los datos recibidos, siendo proporcionada esta aplicación, por ejemplo, por el fabricante del procesador en cuestión, con el fin de permitir la utilización de dicho procesador. Para llevarlo a cabo, el procesador comprende medios de identificación únicos. Estos medios de identificación únicos permiten asegurar la autenticidad del procesador.

Por otro lado, el dispositivo receptor comprende, además, medios de obtención de clave de cifrado, según un modelo con estado (“stateful”), medios que permiten obtener una nueva clave de cifrado en cada nueva sesión de transmisión de datos.

Dependiendo de las formas de realización, el dispositivo receptor comprende, asimismo, medios de gestión de al menos dos colas de procesamiento de los datos recibidos. Más en particular, el dispositivo receptor puede comprender una primera memoria física, de un tamaño predeterminado, en la que son insertados los bloques de datos cifrados durante (o después de) la verificación de la validez de las etiquetas que acompañan a estos bloques de datos cifrados. El dispositivo receptor también puede comprender una segunda memoria física, de un tamaño predeterminado, en la que son insertados los bloques de datos cifrados (o descifrados) con posterioridad al procesamiento de verificación de la validez de las etiquetas. Las dos colas se pueden crear, asimismo, en la memoria segura (Msec) del dispositivo receptor, cuando el mismo está dotado de ella. Esto permite hacer todavía más compleja la labor de interceptación de los datos y la de comprensión del funcionamiento del dispositivo receptor.

REIVINDICACIONES

1. Procedimiento de transmisión de datos, procedimiento puesto en práctica por un primer dispositivo electrónico, llamado emisor, con destino a un segundo dispositivo electrónico, llamado receptor, procedimiento que comprende la transmisión de un mensaje segmentado en bloques de datos (A_1, ..., A_n), procedimiento caracterizado por comprender al menos una iteración de una etapa de procesamiento (20) que comprende:

- obtención (20-1) de un bloque de datos actual Ai;

- cifrado (20-2) de dicho bloque de datos actual Ai con el concurso de una clave de cifrado k, que entrega un bloque de datos cifrados C_i;

- determinación (20-3) de una etiqueta b_i de longitud aleatoria o pseudoaleatoria en función de dicho bloque de datos cifrados C_i, obteniéndose la longitud de la etiqueta b_i mediante la puesta en práctica de una función secreta basada en la clave de cifrado *k*;

- transmisión (20-4) de dicho bloque de datos cifrados C_i;

y por comprender al menos una etapa de transmisión de al menos una etiqueta b_i según un esquema de transmisión predeterminado.

2. Procedimiento de transmisión según la reivindicación 1, caracterizado por que la etapa de transmisión (20-5) de al menos una etiqueta b_i se efectúa con cada iteración de la etapa de procesamiento (20).

3. Procedimiento de transmisión según la reivindicación 1, caracterizado por que el tamaño de dicha etiqueta bi está comprendido entre 1 bit y 8 bits.

4. Procedimiento de transmisión según la reivindicación 1, caracterizado por que dicho procedimiento de transmisión comprende, con anterioridad a la etapa de procesamiento (20), una etapa de obtención (10) de la clave de cifrado *k*, llamada clave de sesión.

5. Procedimiento de recepción de datos, representativos de un mensaje segmentado en bloques de datos (A_1, ..., A_n), procedimiento puesto en práctica por un dispositivo electrónico llamado dispositivo receptor, procedimiento caracterizado por comprender al menos una iteración de las siguientes etapas:

- una etapa de recepción (R20-1) de un bloque de datos cifrados C_i correspondiente a un bloque de datos A_i del mensaje cifrado con el concurso de una clave de cifrado *k*;

- una etapa de recepción (R20-2) de una etiqueta bi correspondiente a una firma de dicho bloque de datos cifrados Ci, teniendo dicha etiqueta bi una longitud aleatoria o pseudoaleatoria obtenida mediante la puesta en práctica de una función secreta basada en la clave de cifrado k;

- una etapa de verificación (R20-3) de una validez de dicha etiqueta bi recibida con relación a una etiqueta biA esperada; y

- cuando dicha etiqueta b_i recibida es diferente de dicha etiqueta b_{iA} esperada, una etapa de procesamiento diferencial (R20-4) de al menos un bloque de datos cifrados válido recibido anteriormente.

6. Procedimiento de recepción de datos según la reivindicación 5, caracterizado por que dicha etapa de recepción (R20-1) de un bloque de datos cifrados C_i comprende una etapa de inserción de dicho bloque de datos cifrados C_i en una primera cola (1) de tamaño predeterminado.

7. Procedimiento de recepción de datos según la reivindicación 5, caracterizado por que dicha etapa de procesamiento diferencial (R20-4) de al menos un bloque de datos cifrados válido anteriormente recibido comprende:

- una etapa de determinación de una ubicación de invalidación j, en el seno de una segunda cola (2);

- al menos una etapa de procesamiento de los datos insertados en la segunda cola (2) hasta la ubicación de invalidación j;

- una etapa de parada del procesamiento.

8. Dispositivo electrónico de transmisión de datos, llamado emisor, que comprende medios de transmisión de datos con destino a un segundo dispositivo electrónico, llamado receptor, dispositivo que comprende medios de transmisión de un mensaje segmentado en bloques de datos (A_1, ..., A_n), dispositivo caracterizado por comprender medios de procesamiento iterativos que comprenden:

- medios de obtención (20-1) de un bloque de datos actual A_i;

- medios de cifrado (20-2) de dicho bloque de datos actual Ai con el concurso de una clave de cifrado k, que entrega un bloque de datos cifrados Ci;

- medios de determinación (20-3) de una etiqueta bi de longitud aleatoria o pseudoaleatoria en función de dicho bloque de datos cifrados C_i, obteniéndose la longitud de la etiqueta b_i mediante la puesta en práctica de una función secreta basada en la clave de cifrado *k*;

- medios de transmisión (20-4) de dicho bloque de datos cifrados C_i;

y por comprender medios de transmisión de al menos una etiqueta b_i según un esquema de transmisión predeterminado.

9. Dispositivo electrónico de recepción de datos, siendo dichos datos representativos de un mensaje segmentado en bloques de datos (A_1, ..., A_n), procedimiento puesto en práctica por un dispositivo electrónico llamado dispositivo receptor, dispositivo caracterizado por comprender medios de procesamiento iterativos que comprenden:

- medios de recepción de un bloque de datos cifrados C_i correspondiente a un bloque de datos A_i del mensaje cifrado con el concurso de una clave de cifrado *k*;

- medios de recepción de una etiqueta b_i correspondiente a una firma de dicho bloque de datos cifrados C_i, teniendo dicha etiqueta b_i una longitud aleatoria o pseudoaleatoria obtenida mediante la puesta en práctica de una función secreta basada en la clave de cifrado *k*;

- medios de verificación de una validez de dicha etiqueta b_i recibida con relación a una etiqueta b_{iA} esperada; y

- medios de procesamiento diferencial de al menos un bloque de datos cifrados válido recibido anteriormente, puestos en práctica cuando dicha etiqueta b_i recibida es diferente de dicha etiqueta b_{iA} esperada.

10. Producto de programa de ordenador descargable desde una red de comunicación y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador, caracterizado por comprender instrucciones de código de programa para la ejecución de un procedimiento de transmisión de datos según la reivindicación 1 ó 5, cuando es ejecutado en un ordenador.

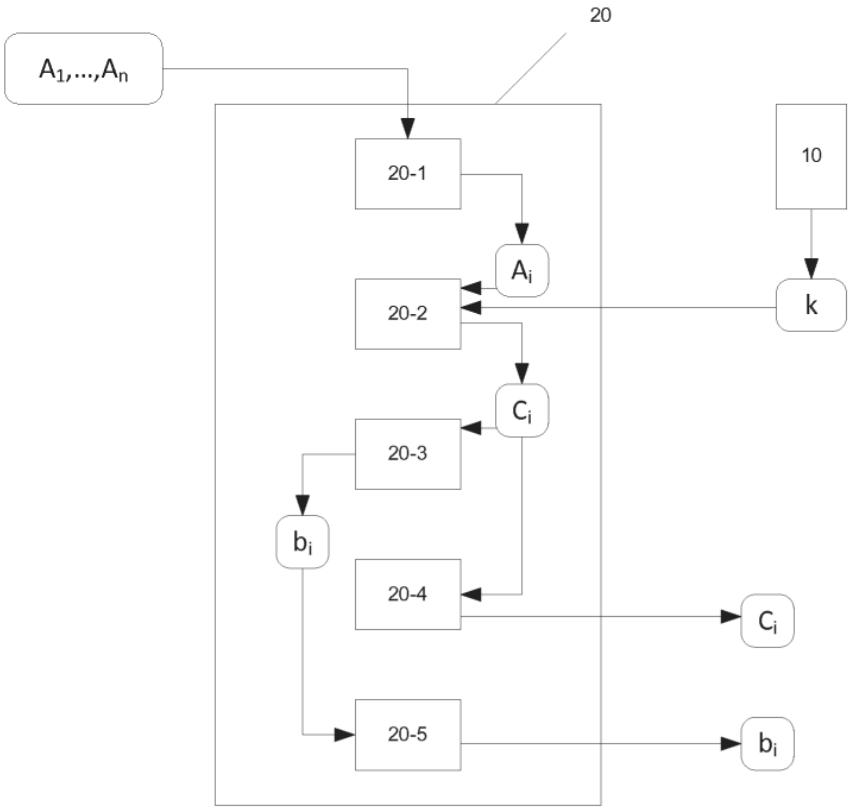

Figura 1

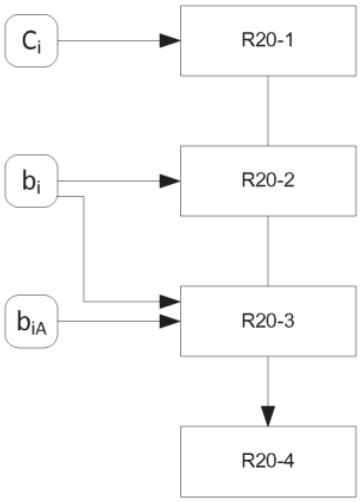

Figura 2

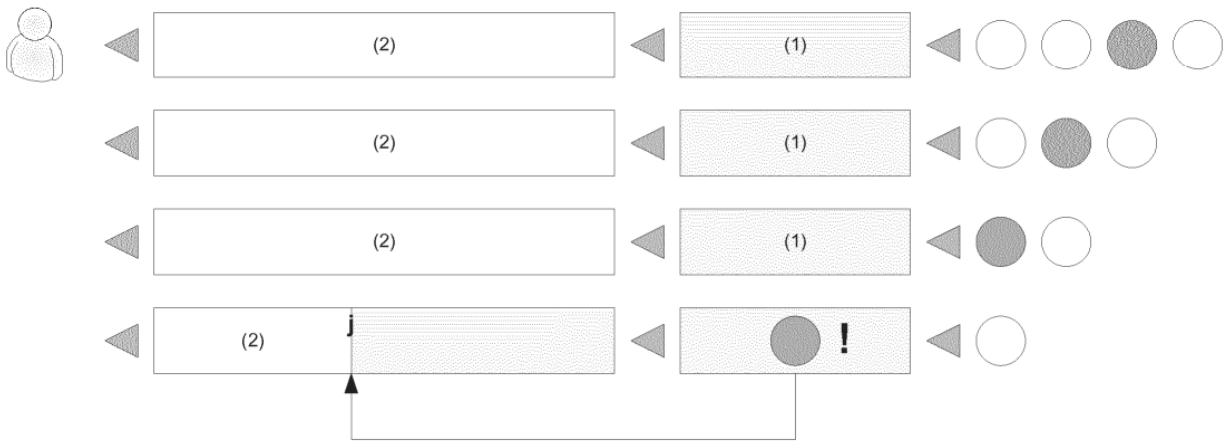

Figura 3

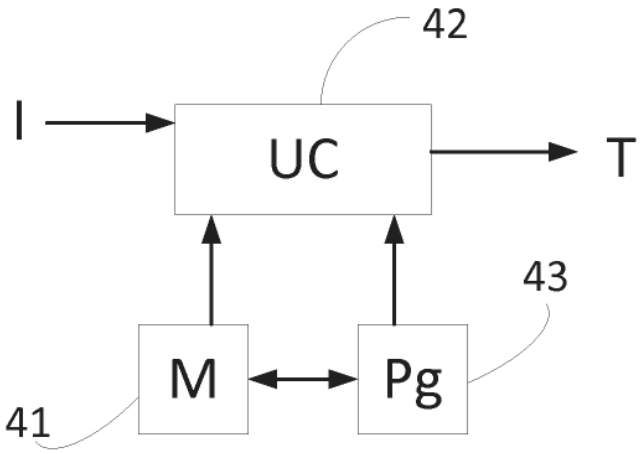

Figura 4

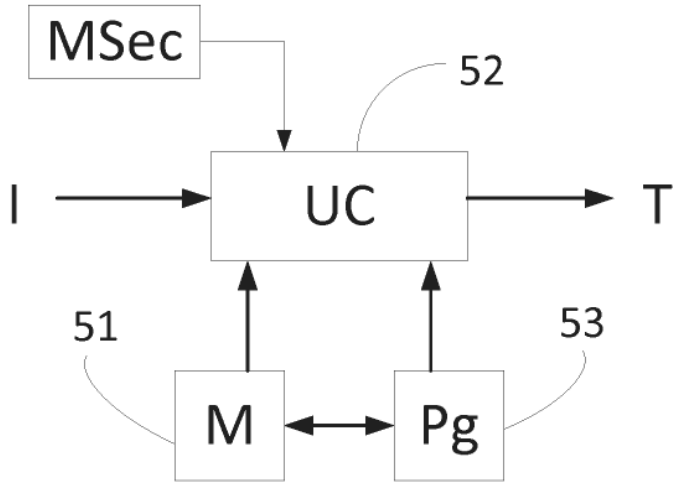

Figura 5