(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 904 288**

(51) Int. CI.:

H04W 12/10 (2011.01)
H04W 12/033 (2011.01)
H04W 12/02 (2009.01)
H04W 4/70 (2008.01)
H04W 4/00 (2008.01)
H04W 84/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.03.2015 PCT/FR2015/050826**

(87) Fecha y número de publicación internacional: **15.10.2015 WO15155440**

(96) Fecha de presentación y número de la solicitud europea: **31.03.2015 E 15717048 (1)**

(97) Fecha y número de publicación de la concesión europea: **10.11.2021 EP 3130168**

(54) Título: **Procedimientos de codificación y decodificación de tramas en una red de telecomunicación**

(30) Prioridad:

09.04.2014 FR 1453141

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.04.2022

(73) Titular/es:

ACTILITY (100.0%)
4 rue Ampère
22300 Lannion, FR

(72) Inventor/es:

HERSENT, OLIVIER

(74) Agente/Representante:

VEIGA SERRANO, Mikel

DESCRIPCIÓN

Procedimientos de codificación y decodificación de tramas en una red de telecomunicación

Sector de la técnica

La presente invención pertenece al campo de la codificación/decodificación de datos transmitidos en una red de telecomunicación, en concreto, en una red de baja velocidad. Se refiere a un método que explota unas técnicas de cifrado y de descifrado para reducir el tamaño de tramas transmitidas.

Este método es, particularmente, ventajoso en el caso de sensores que efectúan unas mediciones a transmitir a un equipo remoto.

Estado de la técnica

En el marco de la evolución de la Internet de las cosas (en inglés, "Internet of things"), cada vez más dispositivos tienen necesidad de conectarse, de manera permanente o periódicamente, a una red de comunicación. Estos dispositivos necesitan a menudo enviar o recibir una cantidad muy pequeña de datos, típicamente algunos bytes enviados una vez a la hora.

Hasta recientemente, estos dispositivos no se han tomado en cuenta correctamente por las redes de comunicación M2M ("Machine to Machine", "comunicación de máquina a máquina" en español) existentes cuando son de área extendida:

- las redes de datos móviles, por ejemplo, GPRS ("General Packet Radio Service", "servicio de radio general por paquetes" en español) o 3G (3ª generación), generalmente, tienen como propósito una utilización de alta velocidad de datos. El consumo de energía para los dispositivos inalámbricos conectados a unas redes de este tipo los hace, generalmente, inapropiados para unos segmentos de mercado en los que unos sensores de pilas (por ejemplo, sensores para el gas o el agua) deben funcionar durante varios años;

- las tecnologías wMBUS ("wireless M-BUS", "M-BUS inalámbrico" en español) y similares tienen un alcance limitado, que necesita unas baterías importantes y costosas para los sensores.

Unas nuevas tecnologías de radio, que utilizan unas bandas ultraestrechas de frecuencias o unas técnicas de expansión de espectro, han estado en condiciones recientemente de proporcionar una conectividad extendida (típicamente de 1 a 2 km en medio urbano) para una velocidad muy escasa (típicamente de 100 a 1.000 bits por segundo) en las bandas de frecuencias ISM para "Industria, Científica y Médica".

Sin embargo, la escasa velocidad implica unos tiempos de transmisión en el aire relativamente largos, movilizando al mismo tiempo unos recursos espectrales que son raros. Por lo tanto, se vuelve esencial para el éxito de estas redes de baja velocidad M2M reducir tanto como sea posible el tamaño de las tramas de datos transmitidas. El tamaño de las tramas depende en gran medida de los encabezados relativos a las capas de enlace y red, especialmente cuando el dispositivo no tiene que transmitir más que una escasa cantidad de datos cuando envía una trama. El número máximo de sensores por celda depende directamente del tamaño de las tramas transmitidas:

- las redes de escasa velocidad a menudo no están sincronizadas y necesitan una tasa de ocupación escasa del canal, con el fin de mantener unas tasas de colisiones escasas y con el fin de funcionar correctamente (ocupación del canal por debajo del 5 % típicamente). La tasa de ocupación del canal es proporcional al número de mensajes enviados por unidad de tiempo y al tamaño de la trama transmitida;

- en unos numerosos países, la regulación del espectro ISM impone que cada antena transmita menos de un porcentaje de tiempo dado (típicamente alrededor del 1 %). Este es, generalmente, el factor de limitación dominante de las redes bidireccionales. También aquí, la tasa de ocupación del tiempo de antena de las estaciones de base es proporcional al número de mensajes enviados por la antena por unidad de tiempo y al tamaño de la trama transmitida.

Un ejemplo de sistema de optimización actual para una utilización eficaz de baja velocidad es la red 6LoWPAN para "IPv6 Low power Wireless Personal Area Networks" en inglés (redes IPv6 de baja potencia inalámbricas en una zona personal). Una red de este tipo se apoya en el estado compartido entre los extremos y el coordinador de la red y explota, igualmente, las redundancias entre la capa MAC ("Medium Access Control", "control de acceso al soporte" en español) y la capa IP ("Internet Protocol", "protocolo de Internet" en español).

En la capa MAC, los mecanismos de optimización incluyen unos espacios de direccionamiento de los sensores más pequeños (por ejemplo, 16 bits en lugar de 64 bits), pero esto tiene como consecuencia reducir el número posible de sensores en la red.

No obstante, unos sistemas de este tipo no explotan las redundancias entre los diferentes campos de PDU ("protocol data unit", "unidad de datos de protocolo" en español), dentro de una capa OSI ("open system interconnection", "interconexión de sistemas abiertos" en español) dada.

Tampoco se explota la redundancia de información existente entre dos tramas de datos sucesivamente decodificadas.

Por lo demás, estos sistemas están diseñados para proporcionar una descompresión sin ambigüedad de cada elemento de una trama de datos. En efecto, toda la información necesaria para la decodificación de la totalidad de los datos está directamente comprendida en una trama. Habitualmente, se prevé un procedimiento de descompresión particular para cada elemento de la trama.

Finalmente, en las técnicas existentes, los procedimientos de emisión/recepción empleados aprovechan de manera limitada la diversidad de información que se origina en las señales recibidas. Típicamente, esta información se utiliza únicamente para organizar una migración de una celda de recepción hacia otra (proceso denominado de "handover", "traspaso").

El estado de la técnica se conoce, por ejemplo, por el documento US2010/046443 A1.

Objeto de la invención

El sistema propuesto tiene como propósito reducir el tamaño global de las tramas para unas comunicaciones M2M inalámbricas de baja velocidad y optimizar el funcionamiento de ello en un contexto de fuertes restricciones sobre la velocidad, el tiempo de ocupación de los canales de transmisión y sobre el volumen de información intercambiada.

La invención se define por las reivindicaciones independientes.

La invención propone un procedimiento de recepción de una trama de datos emitida en una red vinculada a varios nodos, en la que una dirección y un secreto se asignan respectivamente a cada nodo, comprendiendo el procedimiento:

- extraer de la trama unos datos cifrados y un código hash de trama;

- consultar una base de datos que tiene unos registros respectivos que se refieren a los nodos, conteniendo el registro que se refiere a un nodo una información que consta de la dirección y el secreto asignados a este nodo;

- para al menos un registro de la base de datos:

    - calcular al menos un código hash a partir de elementos que comprenden los datos cifrados extraídos de la trama y el secreto contenido en el registro;
    - comparar el código hash calculado con el código hash de trama extraído de la trama; y
    - seleccionar el registro si los códigos hash comparados coinciden;

- y procesar la trama.

El procesamiento comprende una identificación de la dirección contenida en el registro seleccionado como que es la dirección asignada al nodo de donde proviene la trama y un descifrado de los datos cifrados extraídos de la trama con la ayuda del secreto contenido en el registro seleccionado.

Se entiende por "nodo" un dispositivo de adquisición de datos, asociado al menos a una estación de radiocomunicación.

El código hash, convencionalmente utilizable para verificar la integridad de la trama, también se explota, en el presente documento, para contribuir a la identificación de la dirección del dispositivo que ha emitido la trama. De este modo, se hace posible una reducción del tamaño de los encabezados, puesto que la dirección ya no tiene necesidad de ser transmitida enteramente en el encabezado.

Lo más drástico es no hacer constar en absoluto una dirección en el encabezado, pero esto puede requerir la exploración de una base de datos de tamaño demasiado importante por el sistema de telecomunicación a cargo de la recepción de la trama.

Un compromiso razonable entre la minimización del tamaño de la trama y la carga impuesta al sistema a cargo de la recepción de la trama es truncar la dirección que consta en el encabezado. Por ejemplo, es posible reducir el tamaño del campo de dirección del encabezado a 16 bits en lugar de 32. De este modo, en un modo de realización, un dato de dirección incompleta se extrae, además, de la trama y se ejecutan las etapas de cálculo y de comparación del código hash para los registros de la base de datos que contiene una dirección correspondiente al dato de dirección incompleta extraído.

Los elementos para el cálculo del código hash para un registro de la base de datos pueden comprender una parte al menos de la dirección contenida en dicho registro.

En un modo de realización, la información contenida en el registro de la base de datos que se refiere a un nodo consta, además, de la información de apuntamiento de al menos un número de secuencia de una trama que se ha recibido y procesado identificando la dirección contenida en el registro. En este modo de realización, los elementos a partir de los que se calcula al menos un código hash comprenden, además, un número entero determinado según la información de apuntamiento contenida en el registro.

De este modo, la información deducida de la decodificación de las tramas anteriores se puede reutilizar para la trama actual. El número de secuencia de una última trama se ha almacenado previamente durante la decodificación de esta y puede leerse durante la decodificación de una nueva trama, con el fin de localizar un número de secuencia o un rango de números de secuencia si son posibles unas pérdidas de trama, que deben probarse en las etapas de cálculo y de comparación de códigos hash. Esto permite hacer conocer al sistema a cargo de la recepción de la trama el número de secuencia de la trama actual sin haber tenido que hacerlo constar en la información proporcionada explícitamente en la trama.

De este modo, el procesamiento de la trama puede comprender una determinación de un número de secuencia de la trama de entre una secuencia de tramas emitidas desde la dirección identificada y una actualización de la información de apuntamiento contenida en el registro seleccionado en función del número de secuencia determinado de la trama.

En un modo de realización particular, las etapas de cálculo y de comparación del código hash se ejecutan varias veces para al menos un registro de la base de datos. Estas etapas se ejecutan con unos números enteros respectivos elegidos en un intervalo localizado por la información de apuntamiento contenida en el registro. En este modo de realización, después de selección de un registro de la base de datos, la determinación del número de secuencia de la trama comprende una identificación del número entero para el que los códigos hash comparados coinciden.

El tamaño del intervalo localizado por la información de apuntamiento contenida en el registro puede variar en función de las capacidades de cálculo utilizadas para la implementación del procedimiento según la invención.

En otro modo de realización, se efectúa una evaluación de un nivel de potencia y/o de una información de datación de la trama. El procesamiento de la trama comprende, entonces, una actualización, en el registro que se refiere al nodo cuya dirección se ha identificado, de una información de potencia en función del nivel de potencia evaluado y/o de la información de datación.

Se entiende por información de datación cualquier información relativa a los aspectos temporales de la transmisión de las tramas. Una información de este tipo puede estar relacionada con el tiempo de transmisión de las tramas, con los instantes de recepción, etc.

Típicamente, un nivel de potencia de este tipo puede ser una relación de señal a ruido de la señal recibida, una energía o una potencia promedio calculada sobre el intervalo de tiempo correspondiente a la recepción de la trama. Esta información está vinculada a la antena que ha recibido la señal. El sistema a cargo de la recepción de la trama puede comprender varias antenas y varias antenas pueden recibir una misma trama. De este modo, en un modo de realización, el registro que se refiere al nodo cuya dirección se ha identificado comprende una información de potencia en función del nivel de potencia evaluado y/o de la información de datación para cada una de las antenas que han recibido la trama.

En otro modo de realización, un mensaje de adaptación de al menos un parámetro de emisión del nodo cuya dirección se ha identificado se transmite por el sistema a cargo de la recepción de la trama a este nodo. Este mensaje de adaptación se genera en función de información comprendida en el registro que se refiere a este nodo cuya dirección se ha identificado.

Se entiende por parámetro de emisión cualquier característica variable que influya sobre las condiciones de transmisión de la señal emitida por el nodo. De este modo, el mensaje de adaptación puede contener una instrucción para modificar al menos un elemento de entre el canal de emisión, la potencia de emisión, el factor de expansión de espectro y la redundancia de la codificación.

De este modo, se racionaliza la gestión de la actividad de los nodos. En efecto, generándose el mensaje de adaptación en función de información precisa sobre las condiciones de transmisión de las tramas entre nodos y el conjunto de los sistemas, es posible generar unos mensajes de adaptación muy pertinentes. Gestionados de manera global, estos mensajes de adaptación permiten, por ejemplo, maximizar la capacidad de acogida de la red o también reducir el consumo energético global del sistema. Por ejemplo, un nodo para el que la potencia evaluada es elevada puede recibir un mensaje de adaptación para la reducción de su potencia emitida, con el fin de no consumir demasiada energía y de no congestionar inútilmente la red.

El registro que se refiere al nodo cuya dirección se ha identificado puede incluir, además, ventajosamente al menos uno de los elementos de a continuación:

- una indicación sobre la ubicación geográfica de los nodos, pudiendo una indicación de este tipo deducirse o estimarse ventajosamente a partir de los datos relativos a la potencia y/o a la información de datación;

- una duración de espera y de periodicidad de recepción de acuse de recibo específica para un nodo. El nodo puede ponerse en suspensión para la recepción de un mensaje de acuse de recibo durante una duración predeterminada como continuación a la emisión de la trama. La duración de espera, eventualmente específica para un nodo, puede corresponder, por lo tanto, a esta duración predeterminada de suspensión. El sistema a cargo de la recepción de la trama y responsable de la emisión de los acuses de recibo puede, por lo tanto, emitir los acuses de recibo en los momentos precisos donde los nodos a los que se refiere el acuse de recibo son susceptibles escuchar. Esto hace posible una atribución precisa del tiempo de ocupación del canal de transmisión previsto para los acuses de recibo. Para unas frecuencias muy restringidas en tiempo de ocupación, tal como el espectro ISM, esta optimización del tiempo de ocupación es particularmente ventajosa.

La invención tiene como objeto, además, un procedimiento de emisión de una trama de datos por un nodo, estando una dirección y un secreto asignados al nodo, comprendiendo el procedimiento:

- cifrar unos datos por medio del secreto asignado al nodo;

- generar un código hash a partir de elementos que comprenden los datos cifrados y el secreto asignado al nodo; y

- hacer constar los datos cifrados y el código hash generado en la trama emitida

En un modo de realización, el procedimiento incluye, además:

- truncar la dirección asignada al nodo para formar un dato de dirección incompleta; y

- hacer constar el dato de dirección incompleta en la trama emitida.

En un modo de realización particular, la dirección asignada al nodo para formar un dato de dirección incompleta es sobre 32 bits y está truncada para formar el dato de dirección incompleta de tamaño de 16 bits.

En un modo de realización, los elementos a partir de los que se calcula el código hash comprenden, además, un número de secuencia de la trama emitida, estando este número de secuencia de la trama emitida excluido de la trama emitida.

En un modo de realización, el nodo se pone en suspensión para la recepción de un mensaje de acuse de recibo durante una duración predeterminada como continuación a la emisión de la trama. Esta duración predeterminada corresponde ventajosamente al tiempo de procesamiento (típicamente del orden del segundo) requerido por el sistema a cargo de la recepción de la trama para procesar la trama emitida por el nodo y para enviar un acuse de recibo relativo a esta trama. Típicamente, esta duración es de un segundo.

Esta puesta en suspensión se puede efectuar de manera periódica. Por ejemplo, el nodo puede ponerse en suspensión cada dos segundos durante un segundo. De este modo, las restricciones impuestas por la regulación del espectro ISM se respetan ventajosamente sin esfuerzo de gestión suplementario. En efecto, en esta situación, las antenas del sistema a cargo de la recepción de la trama no transmiten más que cuando la ventana de escucha de un nodo está abierta (cuando este nodo no está en suspensión). Esto tiene como efecto reducir sustancialmente el porcentaje de tiempo ocupado para las transmisiones. Se recuerda, en el presente documento, que este porcentaje de tiempo autorizado para las transmisiones es típicamente de alrededor del 1 % para el espectro ISM.

La invención también tiene como propósito un programa informático que incluye unas instrucciones para la implementación del procedimiento descrito anteriormente.

La invención se puede implementar por una unidad de procesamiento y de optimización para comunicarse con varios nodos, comprendiendo la unidad de procesamiento y de optimización:

- una interfaz con una base de datos que tiene unos registros respectivos que se refieren a los nodos, conteniendo el registro que se refiere a un nodo una información que consta de una dirección y un secreto asignados a dicho nodo;

- una unidad de extracción para recibir una trama de datos y extraer de ello unos datos cifrados y un código hash de trama;

- un verificador de código dispuesto para efectuar las siguientes operaciones para al menos un registro de la base

de datos:

- calcular al menos un código hash a partir de elementos que comprenden los datos cifrados extraídos de la trama recibida y el secreto que consta en la información de dicho registro;
- comparar el código hash calculado con el código hash de trama extraído de la trama recibida; y
- seleccionar dicho registro si los códigos hash comparados coinciden;

- y una unidad de descifrado de la trama recibida para ejecutar un procesamiento que comprende una identificación de la dirección contenida en el registro seleccionado como que es la dirección asignada al nodo de donde proviene la trama recibida y un descifrado de los datos cifrados extraídos de la trama recibida con la ayuda del secreto contenido en el registro seleccionado.

La invención se puede implementar, igualmente, por un sistema para comunicarse con varios nodos, comprendiendo el sistema:

- una pluralidad de antenas para la recepción de señales con procedencia de dichos nodos, incluyendo dichas señales unas tramas de datos; y

- la unidad de procesamiento y de optimización descrita anteriormente para el procesamiento de las tramas de datos.

De este modo, las etapas de procesamiento de las tramas de datos, costosas en términos de recursos de cálculos se centralizan ventajosamente. Por otro lado, un elemento discriminador en términos de prontitud de procesamiento es el de la conexión entre la base de datos y la unidad a cargo del descifrado de las tramas. En efecto, la unidad a cargo del procesamiento debe recorrer el conjunto de los registros de la base de datos, con el fin de identificar la dirección del nodo que ha emitido la trama. Un acceso directo y con prontitud entre una unidad de procesamiento y de optimización que es central y la base de datos es más fácil de implementar, lo que reduce sustancialmente el tiempo de procesamiento de las tramas.

La invención se puede implementar, igualmente, por un nodo para comunicarse sobre una red que tenga al menos un sistema, asignándose una dirección al nodo y asignándose, además, un secreto al nodo, comprendiendo el nodo:

- una unidad de cifrado de datos por medio del secreto asignado al nodo;

- un generador de código hash, generándose el código hash a partir de elementos que comprenden los datos cifrados y el secreto asignado al nodo; y

- un generador de trama a emitir, constando la trama de los datos cifrados y el código hash generado.

En un modo de realización, la trama comprende, además, un dato de dirección incompleta obtenido truncando la dirección asignada al nodo.

Descripción de las figuras

Otras ventajas y características de la invención se pondrán de manifiesto a la lectura de la descripción detallada, a continuación, de ejemplos de realización de la invención y al examen de los dibujos en los que:

- la figura 1A es una vista de conjunto de un ejemplo de nodo adecuado para implementar la invención,

- la figura 1B es una vista de conjunto de un ejemplo de sistema adecuado para implementar la invención,

- la figura 1C es una vista de conjunto de un dispositivo de interfaz de red, adecuado para implementar la invención,

- la figura 1D es una vista de conjunto de una unidad de procesamiento y de optimización adecuada para implementar la invención,

- la figura 2 ilustra esquemáticamente las etapas de un procedimiento de emisión de una trama según la invención, en un ejemplo de realización,

- la figura 3 ilustra esquemáticamente las etapas de un procedimiento de recepción adecuado para implementar la invención, en un ejemplo de realización y

- la figura 4 es un diagrama de flujo que muestra un ejemplo de realización de la identificación de un nodo en un ejemplo de procedimiento de comparación de códigos hash adecuado para implementar la invención.

Descripción detallada de la invención

La invención se describe, a continuación, en su aplicación, no limitativa, a las redes de sensores y de actuadores. Los sensores son, por ejemplo, unos aparatos de geoubicación de objetos o de personas, unos instrumentos de medición para una red de distribución de agua o de gas, unos aparatos de medición de la calidad del aire o de medición de ruido, unos tiques electrónicos de estacionamiento, etc. Estos sensores o actuadores están integrados o vinculados a unas estaciones de radiocomunicación. Un sensor o actuador asociado a una estación de radiocomunicación se llama, en el presente documento, un "nodo".

El procedimiento descrito, en el presente documento, se refiere a la comunicación de tramas de señal digital desde los nodos hacia unos servidores de aplicaciones y desde unos servidores de aplicaciones hacia los nodos. Se llama "sistema" al conjunto de los dispositivos comprendidos entre los servidores de aplicaciones y los nodos, estando los servidores de aplicaciones y los nodos excluidos de dicho sistema.

Se señalará que unas comunicaciones pueden tener lugar en los dos sentidos entre los nodos y los servidores de aplicaciones. Se llama comunicación en vía ascendente a una comunicación emitida por un nodo, con destino a un sistema que opera en calidad de receptor de red para los servidores de aplicaciones. Se llama comunicación en vía descendente a una comunicación, emitida por un sistema que opera en calidad de emisor de red para los servidores de aplicaciones, con destino a un nodo.

En un modo de realización, el sistema incluye únicamente un conjunto de antenas y de interfaces de red con los servidores de aplicaciones. Cada antena está vinculada a una interfaz de red que efectúa las etapas de descifrado de las tramas descritas, a continuación, con referencia a las figuras 3 y 4.

En otro modo de realización, el sistema incluye un conjunto de antenas y de interfaces de red que están gestionadas por una o varias unidades de procesamiento y de optimización. Estas unidades de procesamiento y de optimización efectúan, en concreto, las etapas de descifrado de las tramas descritas, a continuación, con referencia a las figuras 3 y 4. La unidad de procesamiento y de optimización es distinta de las antenas y de las interfaces de red. Esta unidad de procesamiento y de optimización está vinculada a las interfaces de red mediante un canal de comunicación. Las interfaces de red tienen, en el presente documento, la carga de etapas convencionales relativas a la conformación de una señal de radio. La invención se describe, a continuación, con referencia a este modo de realización.

Con referencia a la figura 1A, un sensor 12 proporciona unos datos de interés dentro de un nodo Tx1. Una dirección ADD_{32}, por ejemplo, de 32 bits y un secreto SS se asignan al nodo Tx1. Otros secretos, únicamente conocidos por el nodo, se pueden utilizar por este nodo para la codificación de los datos de aplicaciones. A la salida del sensor 12, los datos de interés se proporcionan a un procesador 14 que asegura la construcción de las tramas a emitir.

Las direcciones ADD_{32} identifican los nodos dentro de la red. El secreto SS no es conocido más que por el nodo al que está asignado y, además, está registrado, en relación con la dirección correspondiente, en una base de datos DB3 accesible solamente para las unidades de procesamiento y de optimización habilitadas de la red. Los secretos de aplicaciones, si están presentes, no son conocidos más que por los servidores de aplicaciones.

El procesador 14 del nodo Tx1 procesa los datos de interés para producir una señal digital B compuesta por tramas. Una fase de emisión-recepción de radiofrecuencia (RF) 16 del nodo Tx1 recibe cada trama con procedencia del procesador 14 para conformar, modular y amplificar, de forma conocida de por sí, una señal de radio adaptada para la comunicación M2M inalámbrica de baja velocidad. Esta señal de radio se emite mediante una antena 18 del nodo Tx1.

El procesador 14 del nodo Tx1 de la red accede a una memoria local 20 donde se registran la dirección ADD_{32} del sensor en la red y su secreto asociado SS. Esta memoria 20 contiene, además, un número de secuencia SN de la última trama que ha generado el procesador 14. Las tramas que produce un nodo se numeran consecutivamente, lo que permite que las unidades de procesamiento y de optimización recoloquen cada trama recibida en la secuencia.

El ejemplo de sistema Rxl mostrado en la figura 1B incluye varias antenas de red 24, 28, 32 que captan unas señales de radio y que están vinculadas respectivamente a unas interfaces de red 26, 30, 34. Estas interfaces de red procesan las señales de radio para producir unas tramas digitales comprendidas en una señal Bt. Las tramas de la señal Bt son similares, con los errores de transmisión de aproximación, a unas tramas digitales comprendidas en las señales B de nodos remotos. A continuación, estas tramas se aplican a una unidad de procesamiento y de optimización 36 que suministra unos datos descifrados. Estos datos se pueden enviar a uno o varios servidores de aplicación mediante otra red NTW que, generalmente, será una red fija.

Son posibles varias arquitecturas de sistemas. De este modo, pueden estar presentes varios sistemas, tales como se describen anteriormente en la figura 1B. Igualmente, es posible que varias unidades de procesamiento y de optimización estén presentes en un sistema. Alternativamente, un solo sistema que incluye al menos una unidad de procesamiento y de optimización puede gestionar el conjunto de los nodos.

La unidad de procesamiento y de optimización 36 incluye una interfaz 37 de acceso a la base de datos DB3 en la que se almacenan unos registros que se refieren a los nodos tomados en consideración. Un registro k comprendido en la

base de datos DB3 incluye, en concreto, la dirección $ADD_{32}(k)$ y el secreto SS(k) asignados a un nodo k y una información de apuntamiento P(k) relativa a la secuencia de las tramas que ha emitido y que la unidad de procesamiento y de optimización 36 ha detectado correctamente.

En una realización posible, la información de apuntamiento P(k) consiste simplemente en el número de secuencia más elevado SN(k) que se ha observado por la unidad de procesamiento y de optimización 36 durante el procesamiento de las tramas recibidas anteriormente del nodo k, es decir, el número de secuencia de la trama más reciente para el nodo k.

En otra realización posible, la información de apuntamiento P(k) comprende un número de secuencia SN(k) y un mapa de bits (bitmap) BM(k) en el que un bit de rango q indica si la trama SN(k+q) se ha recibido (1) o no (0).

Si hay varias unidades de procesamiento y de optimización en la red, la base de datos DB3 se puede compartir entre estas unidades.

Utilizada como interfaz de recepción, una interfaz de red 26 descrita, en el presente documento, con referencia a la figura 1C recibe de la antena 24 unas señales de radio con procedencia de un cierto número de nodos y las vuelve a poner en una fase de emisión-recepción de RF 38, luego en una entrada-salida 39 que proceden a unas operaciones convencionales de filtrado, de amplificación, de demultiplexación y de demodulación para producir unas tramas digitales. Estas tramas se acumulan, entonces, en una memoria intermedia 40 que las almacena temporalmente esperando que sean procesadas por un dispositivo de interfaz 42 con la unidad de procesamiento y de optimización 36. Cuando la comunicación hacia la unidad de procesamiento y de optimización 36 está disponible, el dispositivo 42 extrae unas tramas de la pila de tramas temporalmente almacenadas en la memoria intermedia 40 y las envía hacia la unidad de procesamiento y de optimización 36.

La fase de emisión-recepción de RF puede disponerse, igualmente, para evaluar una información relativa a las condiciones de transmisión de una trama recibida. Típicamente, una información de este tipo está relacionada con unos niveles de potencia de las señales recibidas, con una datación de recepción, con una indicación de antena de recepción, etc. Esta información de transmisión, igualmente, se almacena temporalmente en la memoria intermedia 40 para, a continuación, transmitirse con la trama por el dispositivo 42 cuando la unidad de procesamiento y de optimización 36 está disponible.

Típicamente, esta evaluación se efectúa para un canal de recepción y una indicación de este canal puede estar comprendida en esta información de transmisión. Se entiende por canal cualquier información que sirve para caracterizar las propiedades de radio de la señal: frecuencia o patrón de saltos de frecuencia, parámetros de modulación, de expansión y/o de codificación.

Las tramas digitales, eventualmente acompañadas de la información de transmisión, se reciben, a continuación, por la unidad de procesamiento y de optimización 36, descrito con referencia a la figura 1D, mediante una interfaz de entrada/salida 44. Varias unidades de procesamiento y de optimización diferentes pueden tener que descifrar una misma trama. En efecto, dos antenas diferentes pueden captar una misma trama y reorientar estas tramas hacia dos unidades de procesamiento diferentes (dentro de un mismo sistema o no). Con el fin de racionalizar la gestión de las unidades de procesamiento y de optimización, un dispositivo de selección 46 puede estar hecho constar en las unidades de procesamiento y de optimización para cooperar con unos dispositivos análogos previstos en las otras unidades de procesamiento, con el fin de que una sola de estas unidades se utilice para el descifrado de una trama dada. Este dispositivo 46 se representa en punteados en la figura 1D, ya que es opcional.

Esta selección de la unidad de procesamiento y de optimización se puede efectuar en función de la información de transmisión. Las unidades de procesamiento y de optimización pueden compartir entre sí la información recibida de las antenas. De este modo, la selección de la unidad de procesamiento y de optimización que descifra la trama puede ser función de un identificador de al menos una antena que ha recibido la trama y de un nivel de potencia de la trama recibida por esta antena. Se calcula un índice de rendimiento por los medios 46 y se compara con los de los módulos de selección de las otras unidades de procesamiento y de optimización. Una vez hecha esta comparación, solo la unidad de procesamiento y de optimización para la que el índice es el más elevado autorizará la transferencia de la trama al procesador 48. La selección se puede efectuar, igualmente, por un algoritmo lexicográfico según el siguiente orden: relación señal a ruido; potencia de recepción; identificador de la antena que ha recibido la trama.

Las tramas digitales comprendidas en la señal Bt, eventualmente acompañadas de la información de transmisión, se transmiten, entonces, al procesador 48, con el fin de descifrarse. Se utiliza un módulo de definición 49 de una base de tiempo absoluto para la sincronización de los dispositivos utilizados en el sistema Rx1. Por ejemplo, este módulo puede ser de tipo GPS para "global positioning system", sistema de ubicación mundial en español. Como se precisa esto, a continuación, con referencia a las figuras 3 y 4, para cada trama descifrada, el procesador 48 identifica la dirección del nodo k a partir del que se ha enviado esta trama. Se recuerda, en el presente documento, que a un nodo k está asociado un registro k en la base de datos DB3. Los datos descifrados se pueden enviar, a continuación, a uno o varios servidores de aplicación mediante la red NTW.

Varias antenas 26, 30, 34 vinculadas a una misma unidad de procesamiento y de optimización 36 en un sistema Rxl pueden haber recibido la misma trama de un nodo k. En un modo de realización, correspondiente al descrito, a continuación, con referencia a las figuras 3 y 4, se comparan las tramas no descifradas recibidas de varias antenas diferentes y se efectúa una selección de entre las tramas idénticas antes del descifrado. Esta selección devuelve una sola trama, por ejemplo, la primera recibida o aquella para la que la información de transmisión relativa a la antena que la ha recibido es la más favorable.

En una variante, esta misma trama se descifra varias veces, para cada antena que la ha recibido. La información de transmisión específica de cada una de las antenas que han recibido esta misma trama se reúne, entonces, en el registro k. Por ejemplo, se crea un número e de subregistros dentro del registro k para almacenar la información de transmisión relativa a las e antenas que han captado la señal de radio procedente del nodo k. Esta información se actualiza cada vez que se recibe una nueva trama de un nodo k. En otro ejemplo, se efectúa un promedio de la información de transmisión relativa a las e antenas, luego se almacena dentro del registro k.

A la recepción de una trama de número J, un módulo de gestión 52 de los acuses de recibo del decodificador de tramas 36 devuelve un acuse de recibo. Un módulo 22 del nodo Tx1 se acopla a la fase de RF 16 para recibir los acuses de recibo y, cuando sea necesario, hacer reemitir las tramas de las que no se haya acusado recibo después de un tiempo dado. En el caso donde se descifren varias tramas idénticas, se devuelve un solo acuse de recibo. Los procesos de acuse de recibo y de repetición son bien conocidos por el experto en la materia.

El contenido exacto de la información de apuntamiento P(k) en la base de datos DB3 del sistema Rxl depende del modo de acuse de recibo y de repetición elegido (módulos 22 y 52) y de la manera de gestionar las pérdidas de tramas.

Para esta misma trama de número J, un módulo de optimización centralizada 54 de la red genera un mensaje de adaptación de un parámetro de emisión del nodo k que ha enviado la trama J. Este dispositivo 54 se representa en punteados, ya que es opcional. Este mensaje de adaptación se genera para cada trama descifrada en función de la información de transmisión comprendida en el registro k almacenado en la base de datos DB3, cuando el análisis de esta información de transmisión indica que los parámetros de transmisión actuales del nodo no son óptimos. Unos parámetros de este tipo no son óptimos cuando se consumen demasiados recursos de red con respecto a la calidad del enlace. Si están disponibles e subregistros para el registro k, se retiene la calidad de recepción de la mejor antena para calcular la adaptación óptima. En el caso donde un servicio suplementario, por ejemplo, de ubicación del nodo, está activado, entonces, se utiliza la calidad de recepción de las N (típicamente 3) mejores antenas para efectuar la adaptación.

De este modo, se pueden modificar diversos parámetros de emisión. Por ejemplo, el mensaje de adaptación puede contener una instrucción para modificar la potencia de emisión, el factor de expansión de espectro, la redundancia de la codificación, la rapidez de transmisión de la información, etc.

El mensaje de acuse de recibo generado por el módulo 52 y el mensaje de adaptación generado por el dispositivo 54 se conforman, a continuación, en una trama, denominada "de acuse de recibo", por el procesador 56. Esta trama de acuse de recibo puede comprender, igualmente, unas instrucciones (por ejemplo, pasar al modo de informes de alta frecuencia) por parte de los servidores de aplicación conectados a la red NTW y destinatarios de los datos que vienen de los nodos.

El descifrado de las tramas Bt por el procesador 48 puede ser relativamente largo (por ejemplo, del orden de 1 s). Por lo tanto, el envío de las tramas de acuse de recibo conformadas por el módulo 56 se retrasa con respecto a un procedimiento tradicional de envío de estos acuses de recibo. Los nodos bidireccionales, en las redes convencionales, se ponen en escucha inmediatamente después de cada transmisión. Esto es subóptimo desde el punto de vista del consumo de la energía en el caso de un plazo de procesamiento más largo.

De este modo, en un modo de realización, después del envío de una trama, un nodo que espera un acuse de recibo no va a continuar escuchando, sino que, más bien, a entrar inmediatamente en modo suspensión durante una duración predeterminada (típicamente alrededor de un segundo). Durante este tiempo de sueño, la unidad de procesamiento y de optimización dispone de suficientemente tiempo para procesar completamente la trama. Por lo tanto, se toma en cuenta ventajosamente el eventual retraso suplementario causado por las etapas de procesamiento anteriormente mencionadas.

Se pueden parametrizar otras ventanas de escucha del nodo. Por ejemplo, una primera ventana de escucha puede abrirse por el nodo un segundo después del envío y una segunda ventana de escucha puede abrirse cinco segundos después del envío. Esto da una mayor latitud para gestionar la tasa de ocupación de la red, estando este parámetro fuertemente restringido por la regulación de las frecuencias. La tasa de ocupación de ciertas frecuencias puede estar limitada, por ejemplo, al 1 %.

Estas ventanas de escucha pueden ser, igualmente, periódicas (un segundo después de última transmisión, luego cada segundo hasta un número máximo de ventanas que se puede conocer, igualmente, de la base de datos que incluye los registros). Una pluralidad de ventanas de recepción sobre un período total importante permite suavizar el

tráfico de los sistemas, que están restringidos por las reglas de utilización de espectro a una tasa de actividad máxima.

El envío de los acuses de recibo se puede retrasar también, con el fin dejar el tiempo a los servidores conectados a la red NTW para procesar los datos y para enviar a la unidad de procesamiento y de optimización 36 una instrucción para el nodo. Si deben efectuarse otras tareas de procesamiento, el retraso también se puede alargar. Por ejemplo, una triangulación puede necesitar el procesamiento de datos recibidos de una pluralidad de antenas.

La gestión temporal de los acuses de recibo descrita anteriormente se puede implementar para cualquier tipo de procedimiento de decodificación. Esta gestión es particularmente ventajosa cuando el procedimiento implica un tiempo de procesamiento largo.

Si la trama para la que se ha generado el mensaje de acuse de recibo se hubiera recibido por varias antenas, una información de transmisión relativa a cada una de estas antenas está disponible en los e subregistros. En esta situación, un dispositivo de selección 58 de una mejor antena compara esta información de transmisión y deduce de ello la mejor antena para transmitir la trama de acuse de recibo. Este dispositivo 58 se representa en punteados, ya que es opcional. Los parámetros de emisión de la trama de acuse de recibo (potencia emitida, modulación, grado de redundancia, etc.) por la antena seleccionada, igualmente, se pueden deducir ventajosamente de la información de transmisión disponible en los e subregistros y relativa a cada una de las antenas. Asimismo, la datación de emisión deseada de la trama a emitir se puede calcular en función de la tasa actual de ocupación espectral del canal de emisión elegido y de las ventanas de escucha mencionadas anteriormente. La trama de acuse de recibo se transmite, a continuación, mediante la interfaz 44 a la interfaz de red asociada a la antena seleccionada, por ejemplo, a la interfaz de red 26.

La trama de acuse de recibo se recibe por la interfaz de red 26, descrita, en el presente documento, con referencia a la figura 1C, mediante la interfaz 42 con la unidad de optimización y de procesamiento. La memoria intermedia 40 almacena temporalmente las tramas de acuse de recibo a enviar. Una entrada-salida 39 y una fase de emisión-recepción de RF de la interfaz 26 preparan, a continuación, el envío de estas tramas respetando los parámetros de emisión definidos por el dispositivo 58, comprendido el instante de emisión de la trama.

Los datos de entrada del procesador 14 para la construcción de una trama digital constan de, como lo muestra la parte superior de la figura 2:

- la dirección ADD_{32} leída en la memoria 20;
- unos datos de interés DI a transmitir, con procedencia del sensor 12;
- el secreto SS leído en la memoria 20;
- el número de secuencia SN a asignar a la trama, correspondiente al número leído en la memoria 20 e incrementado en una unidad (etapa S20).

Una etapa S21 del procesamiento aplicado por el procesador 14 consiste en cifrar los datos de interés DI por medio del secreto SS asignado al nodo. Un cifrado de este tipo puede utilizar un algoritmo de cifrado simétrico convencionalmente utilizado en las técnicas criptográficas, por ejemplo, AES 128 (Advanced Encryption Standard, "estándar de cifrado avanzado" en español).

Una etapa S22 del procesamiento aplicado por el procesador 14 consiste en truncar la dirección ADD_{32} asignada al nodo Tx1. Por ejemplo, la dirección de 32 bits asignada al nodo Tx1 se trunca para formar un dato de dirección incompleta de 16 bits, anotado, en el presente documento, ADD_{16}. Este dato de dirección incompleta incluye, por ejemplo, solo los 16 bits de peso escaso de la dirección de 32 bits.

El procesador 14 puede formar, entonces, una palabra D24 compuesta por los siguientes elementos:

- la dirección ADD_{16} que se ha truncado en la etapa S22;
- los datos de interés cifrados DC como continuación a la etapa S21;
- el secreto SS;
- el número de secuencia SN incrementado en la etapa S20.

En la etapa S23, el procesador 14 calcula un código hash H a partir de la palabra D24. Este código hash se calcula por una función hash unidireccional convencionalmente utilizada en las técnicas criptográficas, por ejemplo, MD5 ("Message Digest 5", "Resumen de Mensajes 5").

Después de las etapas S20-S23 anteriormente citadas, el procesador 14 ensambla la trama de señal digital D25 que,

en el ejemplo considerado, consta de:

- la dirección ADD_{16} que se ha truncado en la etapa S22;
- los datos de interés cifrados DC como continuación a la etapa S21;
- el código hash H calculado en la etapa S23.

Se observa que el número de secuencia SN no se hace constar necesariamente en las tramas a transmitir, aunque se haga accesible a la unidad de procesamiento y de optimización, como se explicará más adelante. De este modo, se puede limitar el tamaño de las tramas y optimizar el consumo de energía, así como la ocupación del canal de emisión.

En el lado de la unidad de procesamiento y de optimización 36, los datos de entrada del procesador 48 para el procesamiento de una trama digital D25' comprendida en la señal Bt constan de, como lo muestra la parte superior de la figura 3:

- la dirección truncada ADD_{16};
- los datos de interés cifrados DC; y
- el código hash H.

Una etapa de identificación S31 de K registros comprendidos en la base de datos DB3 y correspondientes a la dirección truncada ADD_{16} se ejecuta por el procesador 48. Esta identificación conduce a la selección de un cierto número de registros de entre los N registros comprendidos en la base de datos DB3. En efecto, el dato de dirección incompleta ADD_{16} puede corresponder a una pluralidad de direcciones completas. Por ejemplo, si este dato de dirección incompleta incluye solo los 16 bits de peso escaso de una dirección completa de 32 bits, hasta 2^{32-16} = 65.536 direcciones completas pueden corresponder a este dato de dirección incompleta.

Como se ha mencionado anteriormente con referencia a la figura 1B, los registros contienen una información que consta de la dirección completa $ADD_{32}(k)$ asignada a un nodo k, el secreto SS(k) asignado a este nodo k y una información de apuntamiento P(k) posicionada con respecto a un número de secuencia SN(k).

El procesador 48 ejecuta una etapa de verificación S32 del código hash H extraído de la trama recibida D25'. Unos códigos hash calculados a partir de los registros identificados en la etapa S31 se comparan con el código hash H recibido. Las etapas implementadas durante esta verificación son, por ejemplo, las descritas, a continuación, con referencia a la figura 4.

A continuación, el procesador 48 implementa una etapa de identificación S33 de un registro m (es decir, de un nodo m) que da lugar a un código hash idéntico al código hash H extraído de la trama recibida D25'. Como se precisa, a continuación, con referencia a la figura 4, la etapa S32 se repite para los K registros identificados en la etapa S31 en tanto en cuanto que no se identifique ningún código de comparación. Estadísticamente, un solo registro dará lugar a un código hash idéntico al código hash H. El registro m identificado corresponde a un nodo m y, por lo tanto, comprende la dirección completa $ADD_{32}(m)$ y el secreto SS(m) asignados a este nodo m. El número de secuencia SN' de la trama recibida se deduce, además, de las etapas S32 y S33.

En la etapa S34, la información de apuntamiento P(m) se actualiza en el registro m almacenado en la base de datos DB3 en relación con la dirección $ADD_{32}(m)$, teniendo en cuenta el número de secuencia SN' que se ha detectado. La información de transmisión vinculada a esta trama se añade, igualmente, al registro m. Dentro de un registro m, esta información puede almacenarse de manera separada para cada trama descifrada o simplemente actualizarse cada vez que se descifra una nueva trama.

Finalmente, en la etapa S35, se descifran los datos cifrados extraídos de la trama recibida con la ayuda del secreto SS(m) contenido en el registro m identificado.

Después de las etapas S31-S35 anteriormente citadas, el procesador 48 transmite unos datos D26, resultantes del procesamiento de la trama recibida, a uno o varios servidores de aplicación mediante la red NTW. Los datos D26 transmitidos para una trama incluyen:

- la dirección ADD_{16} recibida en la trama;
- el número de secuencia SN' que se ha identificado en la etapa S33;
- los datos de interés DI descifrados en la etapa S35.

Estos datos pueden incluir, igualmente, la información de transmisión de la trama recibida.

Con referencia a la figura 4, se detalla, en este momento, un ejemplo de implementación de la etapa de verificación S32 del código hash H extraído de la trama recibida, que incluye las siguientes etapas:

- S40: inicialización en 1 de una variable de conteo q. Esta variable de conteo q permite recorrer un conjunto de números de secuencia posteriores a este SN(k) contenido en la información de apuntamiento P(k) de un registro k de la base de datos DB3.

- S41: inicialización en 1 de una variable de conteo k. Esta variable de conteo k permite recorrer el conjunto de los K registros identificados en la etapa S31.

- S42: formación de una palabra X compuesta por los siguientes elementos:

  ◦ la dirección completa $ADD_{32}(k)$ asignada al nodo k y extraída del registro k;

  ◦ los datos cifrados DC extraídos de la trama recibida;

  ◦ el secreto SS(k) asignado al nodo k y extraído del registro k;

  ◦ un número entero igual a SN(k) + q. El número de secuencia SN(k) se extrae de la información de apuntamiento P(k) comprendida en el registro k.

- S43: cálculo de un código hash Y a partir de la palabra X (Y = h(X)). La función hash h es la misma que la utilizada al nivel del nodo Tx1.

- T44: verificación de que el código hash Y es igual al código hash H extraído de la trama recibida. Desplazamiento a la etapa T45 si los códigos son diferentes, desplazamiento a la etapa S33 de lo contrario.

- T45: verificación de que la variable de conteo k no es igual al número máximo K de registros identificados en la etapa S31. Desplazamiento a la etapa S46 si k es diferente de K, desplazamiento a la etapa T47 de lo contrario.

- S46: incremento en una unidad de la variable de conteo k, luego vuelta a la etapa S42 anteriormente citada.

- T47: verificación de que la variable de conteo q no es igual al valor máximo Q autorizado para la variable de conteo q. El número entero Q se puede determinar tomando en cuenta el número habitual de tramas emitidas sucesivamente por un nodo, las capacidades de cálculo disponibles, las capacidades de almacenamiento de la base de datos, el tiempo disponible para la decodificación, etc. Desplazamiento a la etapa S48 si q es diferente de Q, desplazamiento a la etapa S49 (fracaso) de lo contrario.

- S48: incremento en una unidad de la variable de conteo q, luego vuelta a la etapa S41 anteriormente citada.

- S33: identificación de un nodo m (etapa representada esquemáticamente en la figura 3), que comprende

  ◦ S33': retener como índice de registro m el índice k que ha dado un resultado positivo durante la prueba T44 que antecede;

  ◦ S33": mandar al módulo 52 de la unidad de procesamiento y de optimización 36 para que confirme la recepción, hacia el nodo de dirección $ADD_{32}(m)$ de una trama de número de secuencia SN' y suministrar el número SN' para que conste en los datos de salida D26.

- S34 (igualmente, con referencia a la figura 3): actualización de la información de apuntamiento P(m) contenida en el registro m de la base de datos DB3.

- S49: fracaso, no se ha identificado ningún registro.

- S50: fin.

En el caso donde la información de apuntamiento P(k) de un registro k se limita al número de secuencia SN(k) de la última trama recibida del nodo k, la etapa S34 consiste simplemente en tomar SN(m) = SN'. La verificación de los códigos hash S32 según la figura 4 de más arriba procesa, entonces, de manera bruta el caso de una pérdida de trama. Tomemos el ejemplo de una (p+1)-ésima trama de un nodo m que se recibe por la unidad de procesamiento y de optimización antes de la p-ésima trama del mismo nodo m (rotura de secuencia o pérdida de la trama p). En esta situación, el valor de actualización del número de secuencia comprendido en el registro m se toma igual a p+1 en la etapa S34. De este modo, durante el procesamiento de la próxima trama emitida desde un nodo k, el bucle que recorre los números de secuencia comenzará en p+2 para el registro m. Por lo tanto, se ignorará cualquier trama procedente del nodo m y que tenga como número de secuencia p. Si, en el nodo m, el módulo de gestión 22 de los acuses de

recibo hace repetir el envío de la trama de número de secuencia p, la repetición será inútil si la siguiente trama p+1 se ha emitido y recibido correctamente. Por lo tanto, es conveniente, en esta situación, limitar el número de repeticiones de una trama. Por ejemplo, puede limitarse a tres repeticiones.

Limitar la información de apuntamiento P(k) solo al número de secuencia SN(k) de la última trama recibida (con SN(m) = SN' en la etapa S34) conviene, en el caso de un protocolo de acuse de recibo y de repeticiones donde un nodo no está autorizado a emitir una trama de número SN+1 más que después de haber recibido el acuse de recibo de la trama de número SN. En esta situación, el bucle sobre los números de secuencia (indexado por q en la figura 4) ya no es necesario, lo que equivale a tomar Q = 1.

En una variante del procedimiento descrito más arriba, un mapa de bits (bitmap) BM(k) de longitud Q está comprendido en la información de apuntamiento P(k) de un registro k, además del apuntador de número de secuencia SN(k). Este mapa se actualiza conjuntamente con el número de secuencia SN(k) para el registro k = m en la etapa S34.

Este mapa de bits BM(k) comprende un bit $BM(k)_q$ para cada número entero q que va de 1 a Q, cuyo valor indica si la trama de número de secuencia SN(k)+q ya se ha recibido (1) desde el nodo k o si nunca se ha recibido (0). En el presente documento, el número de secuencia SN(k) es el de la última trama de una sucesión de tramas todas correctamente recibidas y que se han emitido por un mismo nodo k.

Una prueba sobre el bit $BM(k)_q$ se puede añadir eventualmente (al menos cuando q > 1) justo antes de la etapa S42 de la figura 4 para verificar si la trama que tiene como número de secuencia SN(k)+q ya se ha recibido del nodo k. Si este es el caso ($BM(k)_q$ = 1), el código hash no se calcula, pasando el procesador 48 directamente a la prueba de fin de iteración T45 en el bucle.

En esta variante, la actualización del mapa de bits BM(m) en la etapa S34 puede consistir en:

- posicionar en 1 el bit $BM(m)_q$;
- si todos los $BM(m)_q$ están en 1, tomar r = Q+1; de lo contrario, localizar el índice más pequeño r, tal que $BM(k)_r$ = 0;
- tomar SN(m) = SN(m)+r-1;
- avanzar el mapa de bits BM(k) en r-1 posiciones y colocar ahí r-1 ceros en el fin.

En esta variante, una pérdida de trama no se produce más que si la unidad de procesamiento y de optimización recibe con éxito una trama p+Q+1 sin haber conseguido recibir la trama p y todas sus repeticiones que se producen hasta la emisión de la trama p+Q+1. El número Q se puede dimensionar para hacer este caso de figura muy poco probable. Aumentar Q no carga obligatoriamente el procesador 48 de manera excesiva en el momento en que la gran mayoría de las tramas se reciben sin pérdida de secuencia.

Se señalará que son posibles otros numerosos esquemas de acuse de recibo y de gestión de las ventanas de recepción de las tramas en el marco de la presente invención.

El código hash tiene como función primera, generalmente, permitir que se pueda verificar la integridad de la trama cuando se decodifica. En la presente invención, el código hash H se utiliza bien para este control de integridad, pero se utiliza, igualmente, para recuperar otra información útil que, por este hecho, no tiene necesidad de transmitirse explícitamente. Esta información es:

- los bits de la dirección ADD_{32} asignada al nodo en el que se origina la trama, que no forman parte de la dirección truncada ADD_{16} comprendida en la trama;
- el número de secuencia SN de la trama.

Si la dirección asignada al nodo está representada sobre 32 bits, el número de secuencia sobre 16 bits y el código hash sobre 32 bits para la verificación de integridad, el tamaño de los encabezados de las tramas transmitidas se reduce de 80 bits (32+16+32=80 bits) a solamente 48 bits (16+32=48 bits). En el caso particular de datos de interés de un solo bit (alarmas), esto representa una mejora de (81-49)/81 = 39,5 %, que permite multiplicar el número de sensores en una vasta red M2M sobre una zona dada.

El truncamiento de las direcciones de nodos de 32 bits a 16 bits no es, por supuesto, más que un caso particular al que no está limitada la invención. Hay dos casos extremos: (1) se transmite la totalidad de la dirección; y (2) no se transmite ningún bit de la dirección. En el caso (1), la carga de cálculo del procesador 48 de la unidad de procesamiento y de optimización es mínima (el bucle indexado por k no es necesario, ya que el nodo está explícitamente identificado), pero la reducción del tamaño de los encabezados se limita a la resultante de la eventual no transmisión del número de secuencia. En el caso (2), los encabezados tienen un tamaño muy pequeño, pero en detrimento de la carga de cálculo impuesta al procesador 48 que, entonces, debe recorrer todos los registros de la base. Cualquier longitud de truncamiento entre estos dos casos extremos es posible, haciéndose la elección en función del dimensionamiento general de la red M2M y de un compromiso entre tasa de compresión de los encabezados y la potencia de cálculo.

Se ha descrito anteriormente la formación de una palabra D24 utilizada para el cálculo del código hash y que incluye la dirección truncada ADD_{16}. Como variante, esta palabra incluye la dirección completa ADD_{32} en lugar de la dirección truncada ADD_{16} para el cálculo del código hash y, entonces, es la dirección completa $ADD_{32}(k)$ recuperada de la base de datos D23 la que el procesador 48 utilizará en la etapa S42 para componer la palabra X a establecer como hash. También se puede hacer constar en esta palabra una dirección truncada de una longitud diferente.

Otra variante consiste en hacer constar el número de secuencia SN en las tramas emitidas, estando, entonces, lo esencial de la reducción del tamaño de los encabezados causado por la transmisión de un dato de dirección incompleta. También se puede hacer constar en las tramas emitidas una parte solamente del número de secuencia SN, por ejemplo, algunos bits de peso escaso, pudiendo el procesador 48 completar el número con la ayuda de la información actualizada en su base de datos.

En otro modo de realización particular, la unidad de procesamiento y de optimización efectúa unas tareas suplementarias antes de transmitir los datos descifrados a los servidores de aplicación. De este modo, cuando una trama emitida por un nodo dado se ha recibido por mediación de varias antenas, es posible, al nivel de la unidad de procesamiento y de optimización, utilizar la triangulación para calcular una información de geoubicación.

La utilización de la base de datos de nodos centralizada DB3 hace posible, por otro lado, una utilización muy flexible de la unidad de procesamiento y de optimización:

- cada nodo puede utilizar una versión diferente de la capa de acceso al medio (MAC, "médium access control"), indexada en la base de datos centralizada, sin exigir una información de versión MAC que también podría congestionar los encabezados. El procesador 48 puede probar a decodificar un paquete probando varias capas MAC, si es necesario. En concreto, esto facilita las puestas a nivel, el mantenimiento de la red y la introducción de nuevas funcionalidades.

- unos contadores temporales de inactividad ("sleep timers" en inglés) en relación con el acuse de recibo ACK y el mecanismo de acuse de recibo retrasado, se pueden configurar para cada sensor.

- una información de actualización relativa a las diferentes técnicas de cifrado utilizadas (código hash, cifrado de los datos de interés) se pueden integrar, igualmente, en esta base de datos. De este modo, la actualización del sistema se efectúa ventajosamente de manera transparente y fluida (actualización simple de la base de datos centralizada).

De manera más general, el proceso de recepción, de codificación y de decodificación se puede adaptar para cada nodo gracias a una base de datos de este tipo.

La presente invención no se limita a las formas de realización descritas anteriormente a título de ejemplos; se extiende a otras variantes.

De este modo, se ha descrito anteriormente un modo de realización en el que las tramas incluyen unos encabezados de 32 o 16 bits. Por supuesto, el tamaño y el formato de unas tramas de este tipo pueden cambiar y tomar, por ejemplo, unos valores de 64 o 128 bits.

REIVINDICACIONES

1. Procedimiento de recepción de una trama de datos emitida por un nodo en una red vinculada a varios nodos (Txl), en el que una dirección (ADD_{32}) y un secreto (SS_k) se asignan respectivamente a cada nodo, estando el procesamiento implementado por una unidad de procesamiento y de optimización que comprende:

- extraer de la trama un dato de dirección incompleta (ADD16) obtenido truncando por el nodo que ha emitido la trama la dirección asignada al nodo, unos datos cifrados y un código hash de trama;
- consultar una base de datos que tiene unos registros respectivos que se refieren a los nodos, conteniendo cada registro que se refiere a un nodo una información que consta de la dirección y el secreto asignados a dicho nodo;
- identificar varios registros comprendidos en la base de datos que contiene una dirección correspondiente al dato de dirección incompleta extraído;
- para al menos un registro de la base de datos identificado:

  • calcular al menos un código hash a partir de elementos que comprenden los datos cifrados extraídos de la trama y el secreto contenido en dicho registro;
  • comparar el código hash calculado con el código hash de trama extraído de la trama; y

- repetir las etapas de cálculo y de comparación del código hash para los registros identificados en tanto en cuanto que los códigos hash comparados no coincidan;
- seleccionar de entre los registros identificados, el registro para el que los códigos hash comparados coinciden;
- y procesar la trama, comprendiendo el procesamiento una identificación de la dirección contenida en el registro seleccionado como que es la dirección asignada al nodo de donde proviene la trama y un descifrado de los datos cifrados extraídos de la trama con la ayuda del secreto contenido en el registro seleccionado.

2. Procedimiento según la reivindicación 1, en el que los elementos para el cálculo del código hash para un registro de la base de datos comprenden, además, una parte al menos de la dirección contenida en dicho registro.

3. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que la información contenida en el registro de la base de datos que se refiere a un nodo consta, además, de la información de apuntamiento (P) de al menos un número de secuencia de una trama que se ha recibido y procesado identificando la dirección contenida en dicho registro y en el que los elementos a partir de los que al menos se calcula un código hash para dicho registro comprenden, además, un número entero determinado según la información de apuntamiento contenida en dicho registro.

4. Procedimiento según la reivindicación 3, en el que el procesamiento de la trama comprende, además, una determinación de un número de secuencia de la trama de entre una secuencia de tramas emitidas desde la dirección identificada y una actualización de la información de apuntamiento contenida en el registro seleccionado en función del número de secuencia determinado de la trama.

5. Procedimiento según la reivindicación 4, en el que las etapas de cálculo y de comparación del código hash se ejecutan varias veces para al menos un registro de la base de datos, con unos números enteros respectivos elegidos en un intervalo localizado por la información de apuntamiento contenida en dicho registro y en el que, después de selección de un registro de la base de datos, la determinación del número de secuencia de la trama comprende una identificación del número entero para el que los códigos hash comparados coinciden.

6. Procedimiento según una cualquiera de las reivindicaciones anteriores, que comprende, además, una evaluación de un nivel de potencia y/o de una información de datación de la trama y en el que el procesamiento de la trama comprende, además, una actualización, en el registro que se refiere al nodo cuya dirección se ha identificado, de una información de potencia en función del nivel de potencia evaluado y/o de la información de datación.

7. Procedimiento según una cualquiera de las reivindicaciones anteriores, que comprende, además:

- transmitir un mensaje de adaptación de al menos un parámetro de emisión al nodo cuya dirección se ha identificado, generándose dicho mensaje de adaptación en función de información comprendida en el registro que se refiere a dicho nodo.

8. Procedimiento de emisión de una trama de datos por un nodo (Tx1), estando una dirección (ADD_{32}) y un secreto (SS) asignados al nodo, implementándose el procedimiento por el nodo y comprendiendo:

- cifrar unos datos por medio del secreto asignado al nodo;
- generar un código hash a partir de elementos que comprenden los datos cifrados y el secreto asignado al nodo;
- truncar la dirección asignada al nodo para formar un dato de dirección incompleta; y
- hacer constar los datos cifrados, el código hash generado y el dato de dirección incompleta en la trama emitida.

9. Procedimiento según la reivindicación 8, en el que los elementos a partir de los que se calcula el código hash

comprenden, además, un número de secuencia de la trama emitida y en el que dicho número de secuencia de la trama emitida se excluye de la trama emitida.

10. Procedimiento según la reivindicación 8, que comprende, además, como continuación a la emisión de la trama:

- poner en suspensión el nodo para la recepción de un mensaje de acuse de recibo durante una duración predeterminada.

11. Programa informático que incluye unas instrucciones para la implementación del procedimiento según una cualquiera de las reivindicaciones anteriores, cuando estas instrucciones se ejecutan por un procesador.

12. Unidad de procesamiento y de optimización (36) para comunicarse con varios nodos (Txl), comprendiendo la unidad de procesamiento y de optimización:

- una interfaz con una base de datos (DB3) que tiene unos registros respectivos que se refieren a los nodos de la red, conteniendo cada registro que se refiere a un nodo una información que consta de una dirección (ADD_{32}) y un secreto (SS) asignados a dicho nodo;
- una unidad de extracción para recibir una trama de datos de un nodo y extraer de ello un dato de dirección incompleta (ADD16) obtenido truncando por el nodo que ha emitido la trama la dirección asignada al nodo, unos datos cifrados y un código hash de trama;
- una unidad para identificar varios registros comprendidos en la base de datos que contiene una dirección correspondiente al dato de dirección incompleta extraído;
- un verificador de código dispuesto para efectuar las siguientes operaciones para al menos un registro de la base de datos identificado:

  • calcular al menos un código hash a partir de elementos que comprenden los datos cifrados extraídos de la trama recibida y el secreto que consta en la información de dicho registro;
  • comparar el código hash calculado con el código hash de trama extraído de la trama recibida; y

para repetir las etapas de cálculo y de comparación del código hash para los registros identificados en tanto en cuanto que los códigos hash comparados no coincidan; y para seleccionar de entre los registros identificados, el registro para el que los códigos hash comparados coinciden;
- y una unidad de descifrado de la trama recibida para ejecutar un procesamiento que comprende una identificación de la dirección contenida en el registro seleccionado como que es la dirección asignada al nodo de donde proviene la trama recibida y un descifrado de los datos cifrados extraídos de la trama recibida con la ayuda del secreto contenido en el registro seleccionado.

13. Sistema (Rxl) para comunicarse con varios nodos (Txl), comprendiendo el sistema:

- una pluralidad de antenas para la recepción de señales con procedencia de dichos nodos, incluyendo dichas señales unas tramas de datos; y
- una unidad de procesamiento y de optimización según la reivindicación 12 para el procesamiento de las tramas de datos.

14. Nodo (Txl) para comunicarse sobre una red de telecomunicación, asignándose una dirección (ADD_{32}) al nodo y asignándose, además, un secreto (SS) al nodo, comprendiendo el nodo:

- una unidad de cifrado de datos por medio del secreto asignado al nodo;
- un generador de código hash, generándose el código hash a partir de elementos que comprenden los datos cifrados y el secreto asignado al nodo; y
- un generador de trama a emitir, constando la trama de los datos cifrados y el código hash generado, comprendiendo la trama, además, un dato de dirección incompleta (ADD_{16}) obtenido truncando la dirección (ADD_{32}) asignada al nodo por el nodo (Tx1).

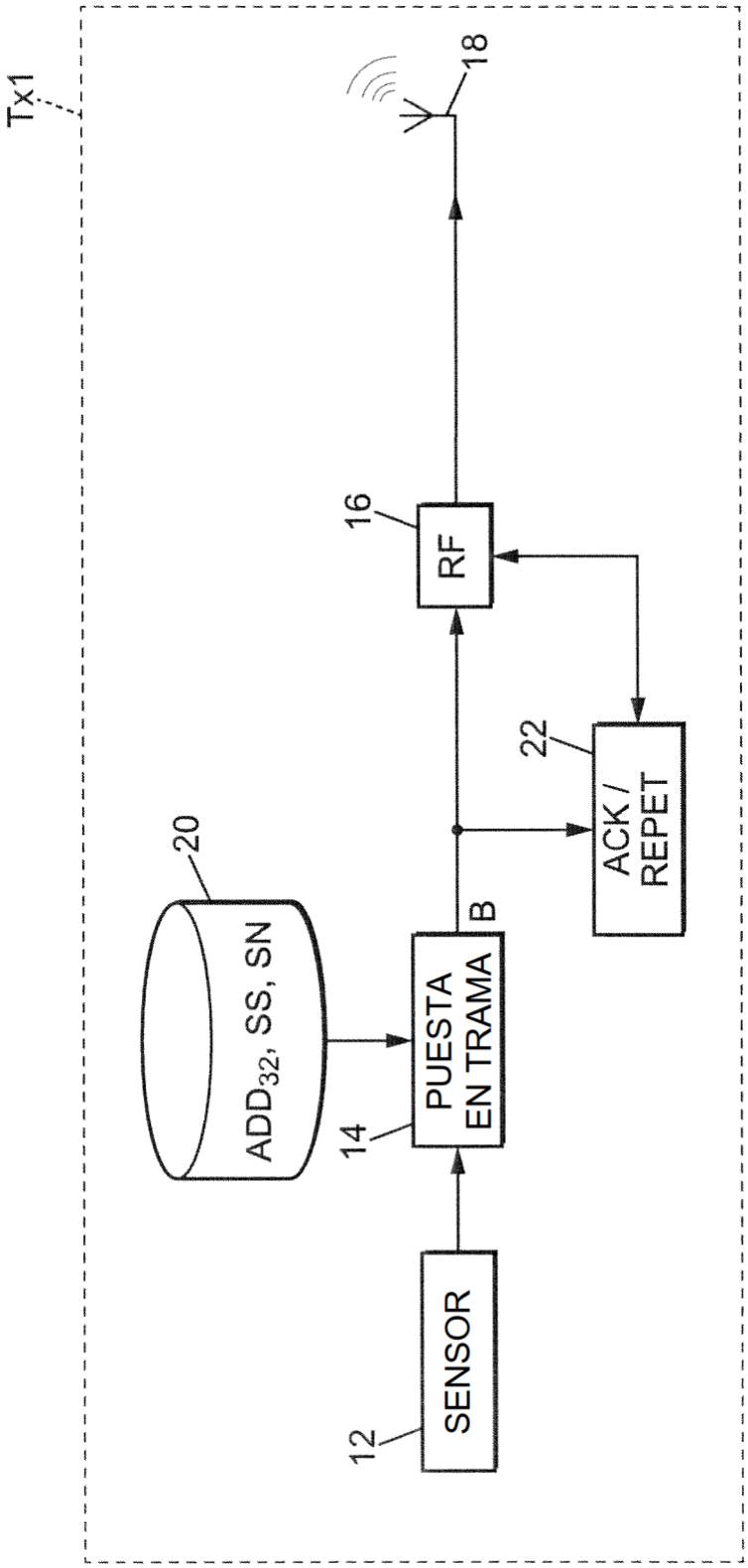

Tx1
18
16
RF
22
ACK / REPET
20
ADD_{32}, SS, SN
B
PUESTA EN TRAMA
14
SENSOR
12

FIG. 1A

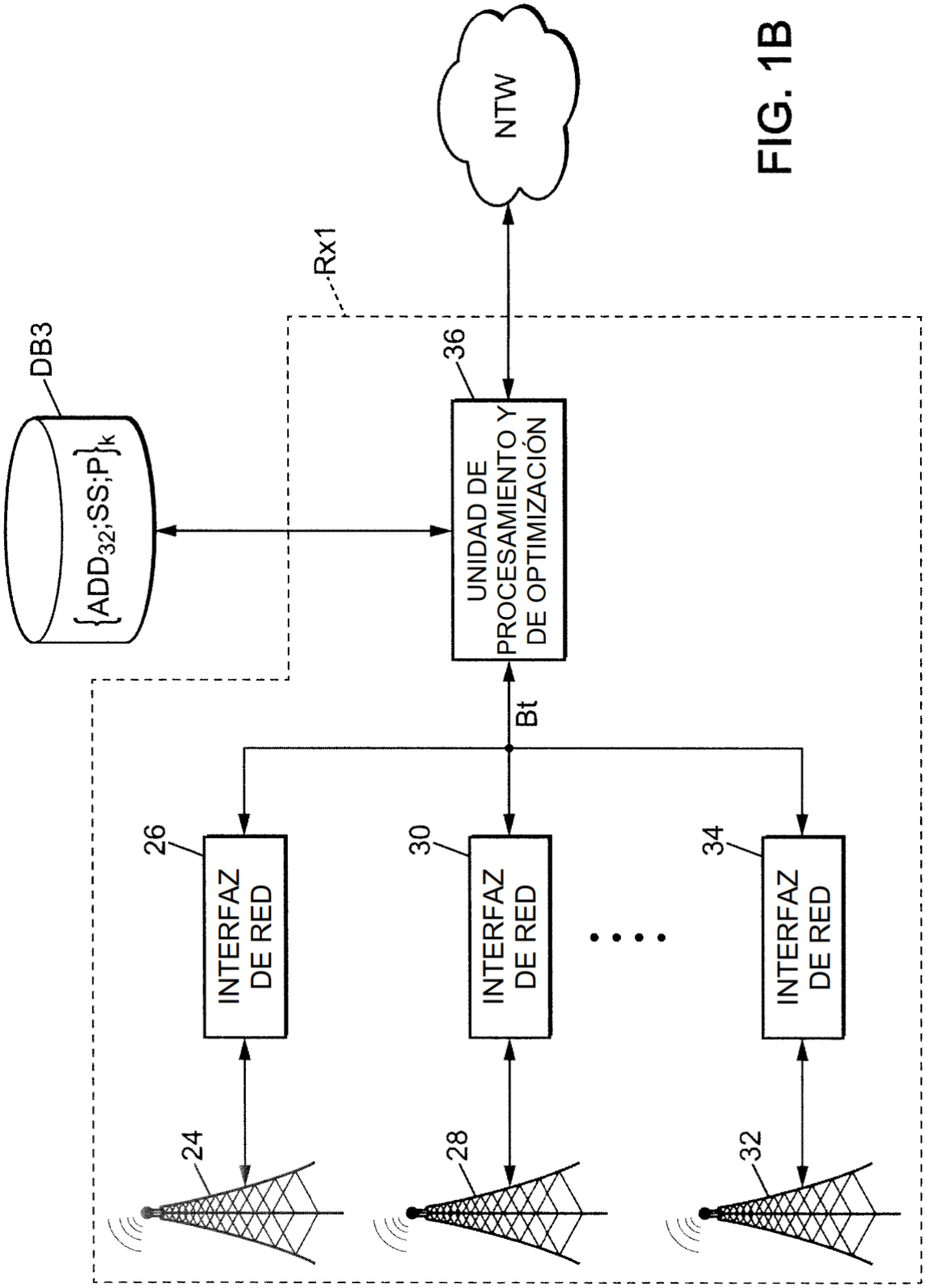

NTW
Rx1
DB3
{ADD32;SS;P}jk
36
UNIDAD DE PROCESAMIENTO Y DE OPTIMIZACIÓN
Bt
26
INTERFAZ DE RED
30
INTERFAZ DE RED
34
INTERFAZ DE RED
24
28
32

FIG. 1B

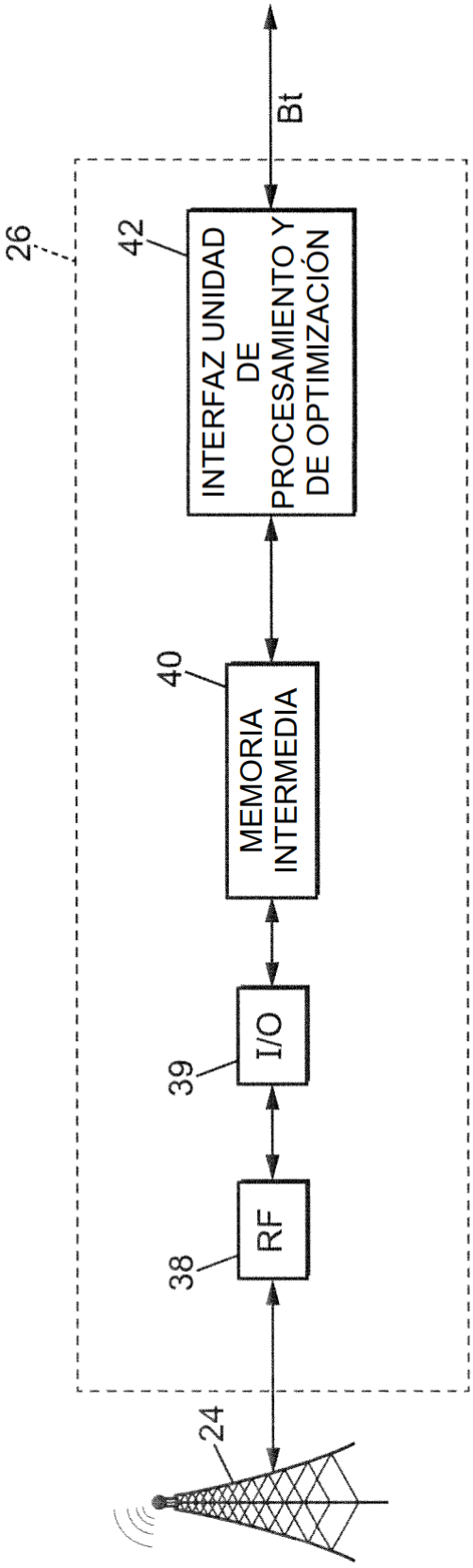

Bt
26
42
INTERFAZ UNIDAD DE PROCESAMIENTO Y DE OPTIMIZACIÓN
40
MEMORIA INTERMEDIA
39
I/O
38
RF
24

FIG. 1C

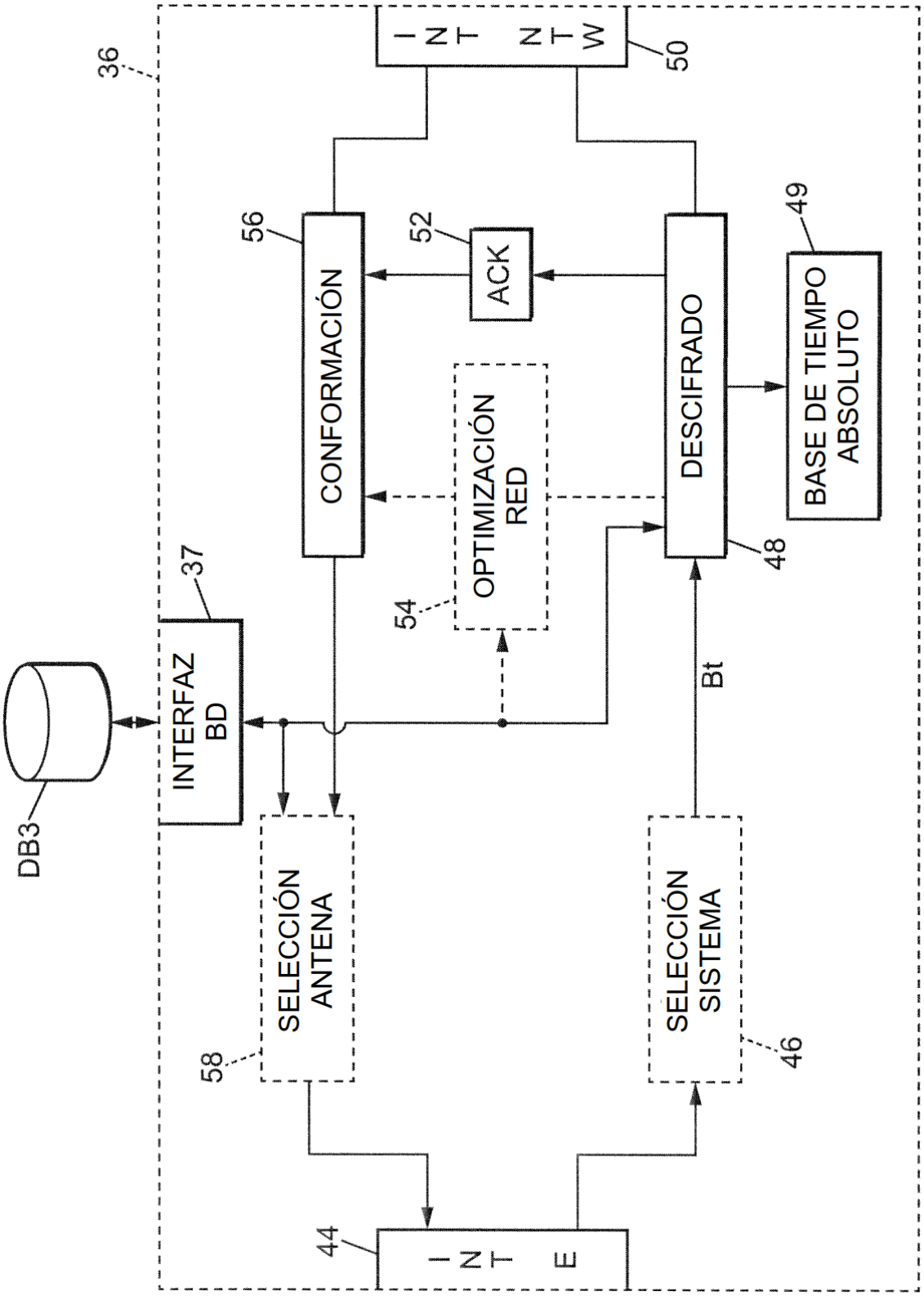

36
INT NTW
50
56
CONFORMACIÓN
52
ACK
DESCIFRADO
49
BASE DE TIEMPO ABSOLUTO
OPTIMIZACIÓN RED
54
48
37
INTERFAZ BD
DB3
Bt
SELECCIÓN ANTENA
58
SELECCIÓN SISTEMA
46
44
INT E

FIG. 1D

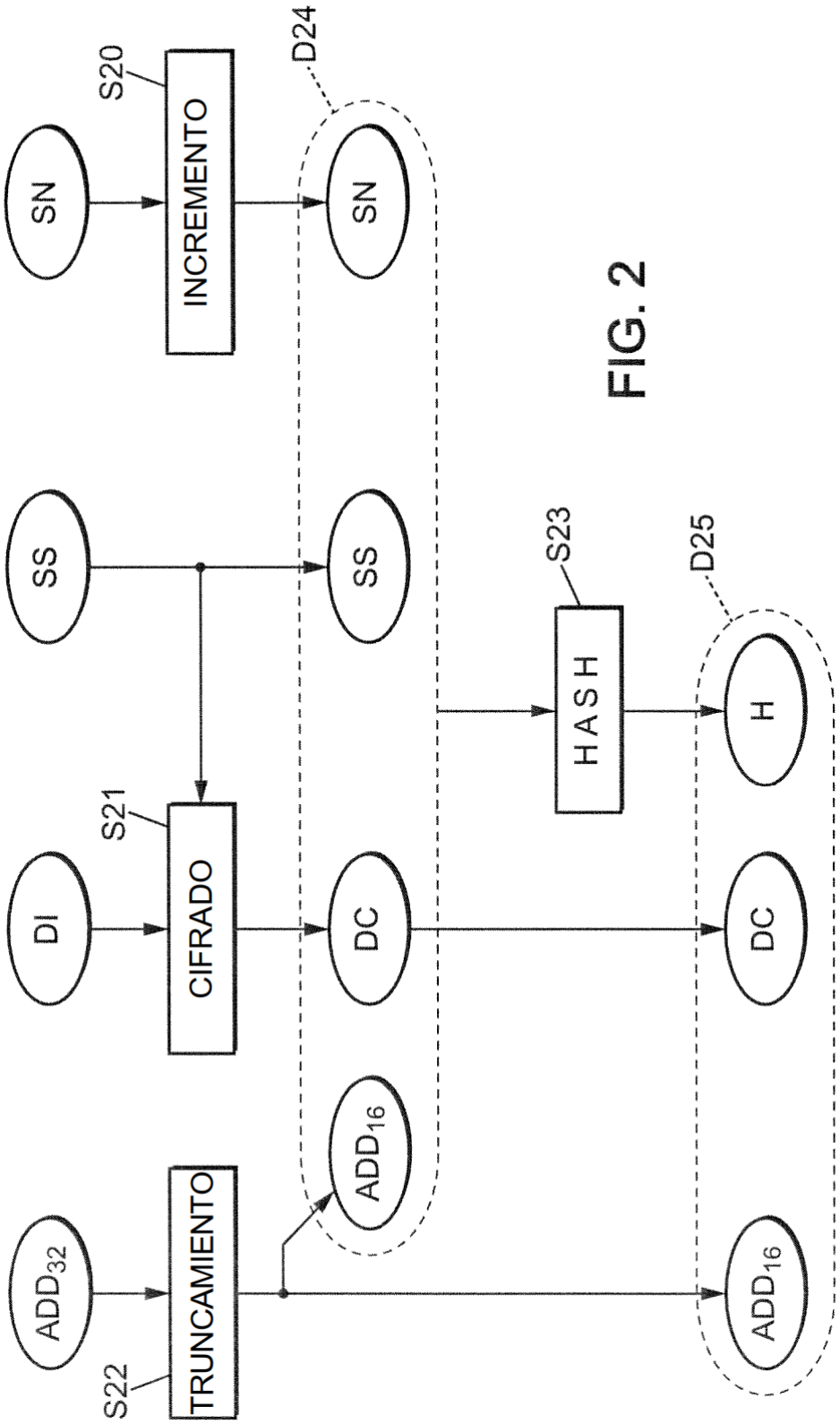
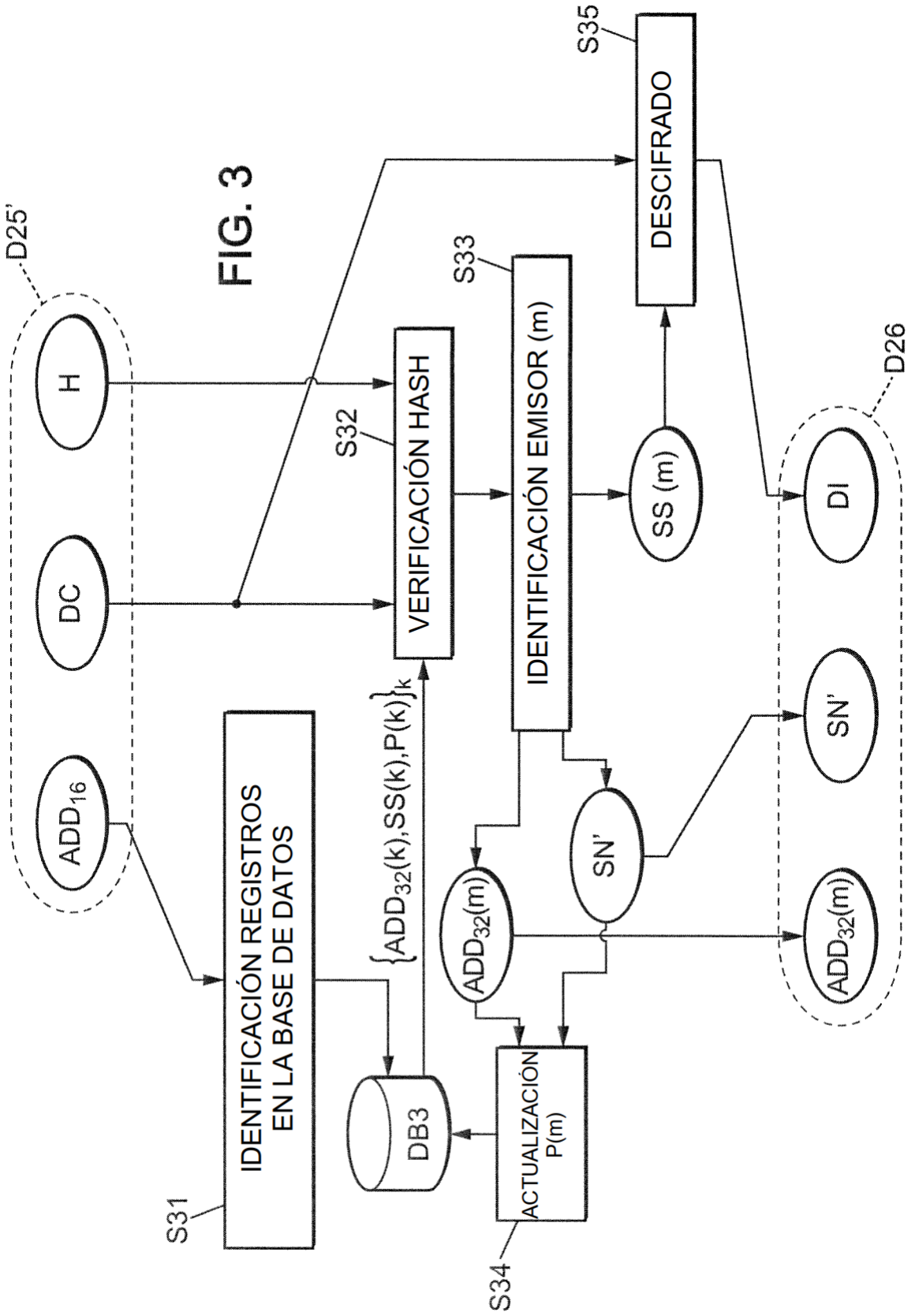

SN
S20
INCREMENTO
D24
SN
SS
SS
S23
D25
HASH
H
DI
S21
CIFRADO
DC
DC
ADD16
ADD32
S22
TRUNCAMIENTO
ADD16

FIG. 2

FIG. 3


D25'
H
DC
ADD16
S31
IDENTIFICACIÓN REGISTROS EN LA BASE DE DATOS
DB3
{ADD32(k),SS(k),P(k)}k
S32
VERIFICACIÓN HASH
S33
IDENTIFICACIÓN EMISOR (m)
SS (m)
S35
DESCIFRADO
D26
DI
SN'
ADD32(m)
SN'
ADD32(m)
ACTUALIZACIÓN P(m)
S34

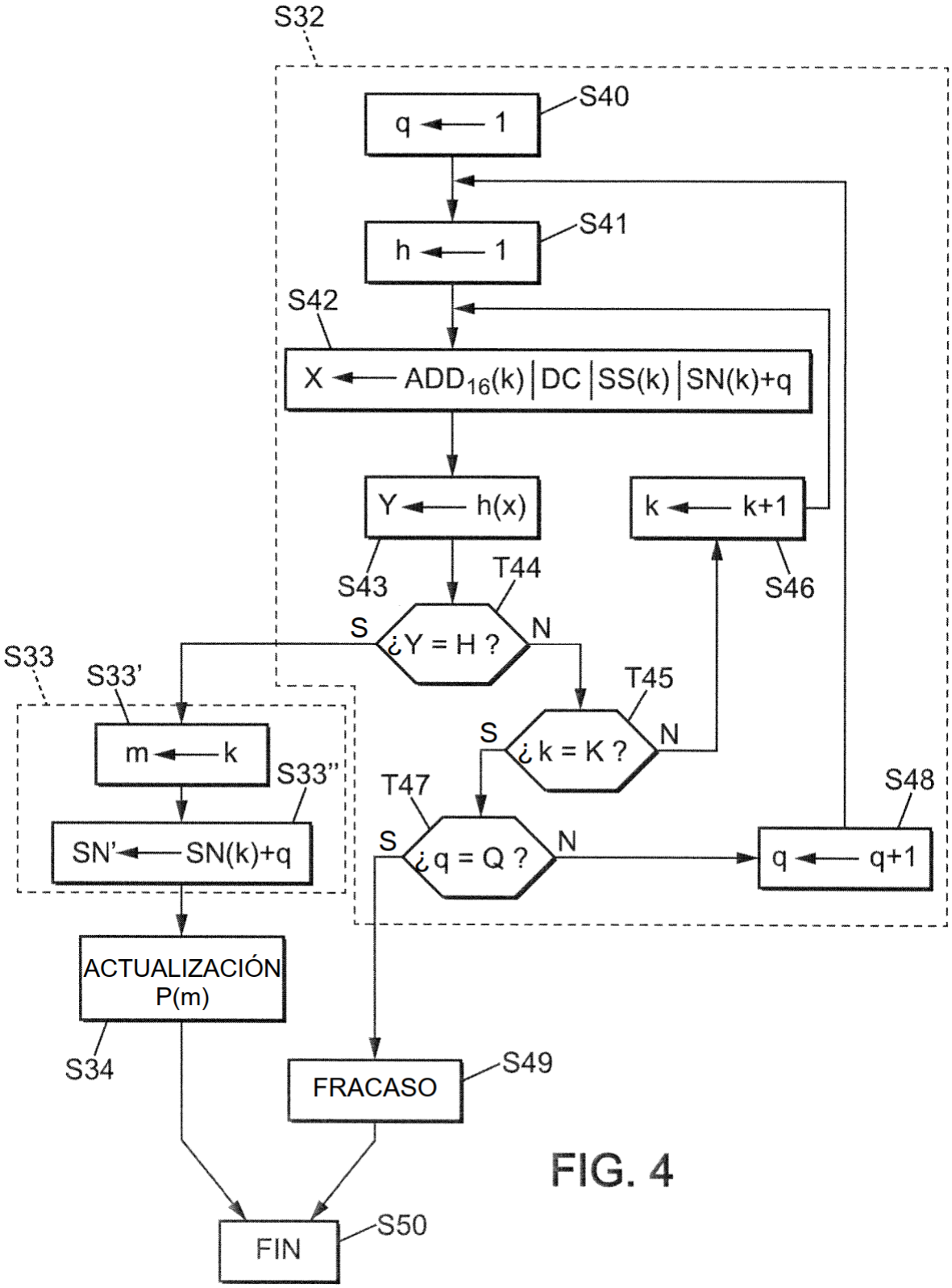

S32
S40
q ← 1
S41
h ← 1
S42
X ← ADD16(k) | DC | SS(k) | SN(k)+q
Y ← h(x)
k ← k+1
S43
T44
S46
S
¿Y = H ?
N
S33
S33'
T45
m ← k
S
¿k = K ?
N
S33"
T47
S48
SN' ← SN(k)+q
S
¿q = Q ?
N
q ← q+1
ACTUALIZACIÓN P(m)
S34
FRACASO
S49
FIN
S50

FIG. 4