(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 694 323**

(51) Int. CI.:

H04L 1/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.10.2012 PCT/EP2012/069756**

(87) Fecha y número de publicación internacional: **11.04.2013 WO13050550**

(96) Fecha de presentación y número de la solicitud europea: **05.10.2012 E 12772758 (4)**

(97) Fecha y número de publicación de la concesión europea: **22.08.2018 EP 2764651**

(54) Título: **Método de transmisión de paquetes de datos**

(30) Prioridad:

07.10.2011 FR 1159081

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.12.2018

(73) Titular/es:

AIRBUS DS SAS (50.0%)
ZAC de la Clef Saint Pierre, 1 Boulevard Jean Moulin
78990 Elancourt, FR y
CASSIDIAN FINLAND OY (50.0%)

(72) Inventor/es:

MEGE, PHILIPPE;
MOLKO, CHRISTOPHE;
MOUFFRON, MARC y
BRUTEL, CHRISTOPHE

(74) Agente/Representante:

ELZABURU, S.L.P

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método de transmisión de paquetes de datos

La presente invención se refiere a un método para transmitir paquetes de datos entre un transmisor y un receptor a través de un canal radioeléctrico. También se refiere a un sistema de transmisión, una instalación de recepción y un programa informático correspondiente.

El alcance de la invención se extiende a las comunicaciones radioeléctricas. La invención se refiere más en particular a sistemas de transmisión de paquetes de datos implementando un mecanismo de petición de repetición automática, conocido como ARQ ("re-Petición de Repetición Automática").

El mecanismo de ARQ es un protocolo de retransmisión automática que usa un método de detección de error. Según dicho protocolo, cuando se detecta un error en un paquete de datos, el paquete erróneo se rechaza y se emite una petición de retransmisión del paquete por parte del receptor. El paquete de datos simplemente se retransmite a continuación.

Dicho mecanismo está actualmente implementado en particular en los sistemas móviles de radio profesionales, siendo más conocido bajo el acrónimo inglés PMR ("Radio Móvil Profesional").

Sin embargo, el mecanismo de retransmisión de ARQ presenta un inconveniente importante relacionado con una reducción de la tasa efectiva de flujo de datos. Dicha reducción de la tasa de flujo resulta ser importante cuando el canal es ruidoso, incrementando con ello la tasa de error y, en consecuencia, el número de repeticiones.

Con el fin de subsanar ese inconveniente, algunos sistemas de radiocomunicación implementan un mecanismo híbrido de petición de repetición automática, conocido como HARQ (re-Petición de Repetición Automática Híbrida"), combinando la detección y la corrección del error y optimizando el rendimiento del mecanismo de repetición.

Según el mecanismo de HARQ, el paquete recibido una primera vez y detectado como erróneo, se mantiene en la memoria del receptor con vistas a ser combinado con el mismo paquete que sea retransmitido, mejorando con ello la corrección de errores, lo que tiene como efecto la reducción del número de peticiones de retransmisión. La tasa efectiva de flujo de la transmisión se mejora entonces significativamente, en particular cuando el canal es ruidoso.

Este protocolo de HARQ se implementa en particular en sistemas de tercera y cuarta generación como HSxPA (Acceso por Paquetes xlink de Alta Velocidad"), LTE ("Evolución de Largo Plazo") y WIMAX ("Interoperabilidad Mundial para Acceso de Microondas").

Además, con el fin de tener las comunicaciones aseguradas, algunos sistemas radioeléctricos implementan procedimientos de encriptación de datos. Así, se usan por lo general dos tipos de encriptación.

El primer tipo es la encriptación de extremo a extremo, conocida como E2EE (Encriptación de Extremo a Extremo"). Ésta consiste en cifrar datos en la fuente. El cifrado y el descifrado se realizan en los extremos de la ruta de comunicación. Los datos de señal no son cifrados.

El segundo tipo es la encriptación de interfaz de radio, conocida como AIE ("Encriptación de Interfaz de Aire"). Ésta consiste en cifrar todos los datos destinados a transitar a través del canal de radio, incluyendo los datos de señal. El cifrado y el descifrado se realizan respectivamente en el transmisor y en el receptor.

Con el fin de garantizar una eficiencia alta de las transmisiones, algunos sistemas implementan tanto un mecanismo de transmisión de HARQ como un cifrado de AIE. Éste es el caso, por ejemplo, de los sistemas de tercera generación 3GPP ("Proyecto Partnership de 3ª Generación"), que incluyen el sistema de telecomunicación universal con los móviles de UMTS ("Sistema de Telecomunicación Móvil Universal"), o sistemas LTE y WIMAX de cuarta generación.

Un sistema de ese tipo ha sido ejemplificado en la solicitud de Patente WO 00/62467.

En tales sistemas, el cifrado de AIE se realiza en el transmisor después de la etapa de codificación del canal de datos. El descifrado de AIE se realiza en el receptor con anterioridad a la etapa de decodificación del canal. Las retransmisiones de HARQ son así gestionadas después del descifrado de la AIE en este caso. En el caso de la retransmisión, los datos que se transmiten son, por lo tanto, siempre los mismos. El procedimiento de HARQ se implementa fácilmente en tales sistemas, dado que el cifrado de la AIE es transparente en ese caso.

Sin embargo, la introducción del mecanismo de HARQ es actualmente imposible en los sistemas radioeléctricos que implementan el cifrado de AIE con anterioridad a la operación de codificación del canal de datos. Éste es el caso, en particular, de los sistemas de PMR del tipo de la TETRA ("Radio Troncal Transeuropea") y del tipo P25 tal como ha sido definido por la TIA ("Asociación de la Industria de las Telecomunicaciones") para la APCO (Asociación de Oficiales de Comunicaciones de Seguridad Pública"). De hecho, en estos sistemas, el cifrado de AIE tiene como efecto cambiar los datos transmitidos que son codificados en cada retransmisión de un mismo paquete, haciendo

con ello que la implementación del mecanismo de HARQ sea imposible.

La presente invención tiene como objetivo mejorar la situación.

Con este propósito a la vista, la presente invención se refiere en primer lugar la presente invención se refiere en primer lugar a un método de transmisión de un paquete de datos entre un transmisor y un receptor a través de un canal radioeléctrico, comprendiendo dicho método una primera transmisión de un paquete, comprendiendo dicha primera transmisión:

las etapas implementadas en el transmisor, que consisten en:

- un primer procesamiento lineal de dicho paquete con el fin de obtener un primer paquete,
- una codificación de detección de error lineal del primer paquete a través de un código de detección de error con el fin de obtener un primer paquete intermedio, y
- una codificación de corrección de error lineal del primer paquete intermedio a través de un primer código de corrección de error con el fin de obtener un primer paquete codificado;

un método en donde, cuando se recibe el primer paquete codificado y se detecta por medio de dicho método que éste es erróneo, el método comprende al menos una segunda transmisión de dicho paquete, comprendiendo la segunda transmisión:

las etapas implementadas en el transmisor, que consisten en:

- un segundo procesamiento lineal de dicho paquete, siendo dicho segundo procesamiento diferente de dicho primer procesamiento con el fin de obtener un segundo paquete diferente del primer paquete;
- una codificación de detección de error lineal del segundo paquete por medio de dicho código de detección de error con el fin de obtener un segundo paquete intermedio, y
- una codificación de corrección de error lineal del segundo paquete intermedio a través de un segundo código de corrección de error con el fin de obtener un segundo paquete codificado;

y las etapas implementadas en el receptor, que consisten en:

- una modificación del primer paquete codificado y/o del segundo paquete codificado con el fin de obtener dos paquetes en donde la diferencia debida al primer y segundo procesamientos se compensa;
- una combinación de ambos paquetes conforme a un procedimiento de petición de repetición automática híbrida (HARQ), y
- una decodificación del paquete combinado por medio de un tercer código de corrección de error que depende del primer y el segundo códigos de corrección de error.

Merced a la modificación por el receptor del primer paquete codificado y/o del segundo paquete codificado, es posible compensar los efectos de la diferencia de procesamiento del paquete de datos de una transmisión a otra y, de ese modo, implementar simplemente el mecanismo de HARQ. De manera notable, la presente invención opera características de linealidad que son inherentes al sistema de transmisión, en particular una codificación de canal de detección de error y una codificación de canal de corrección de error lineal, y a los procesamientos implementados sobre los paquetes de datos. En efecto, resulta posible la modificación que permite una combinación de HARQ, dado que los procesamientos y las codificaciones son lineales.

Ventajosamente, el primer procesamiento es un cifrado lineal por medio de una primera secuencia de claves de cifrado, y el segundo procesamiento es un cifrado lineal por medio de una segunda secuencia de claves de cifrado que es diferente de la primera secuencia.

El cifrado de AIE es lineal en general, dado que no debe propagar errores. En los sistemas de PMR, este cifrado consiste con frecuencia en aplicar una “OR exclusiva” entre los datos y la secuencia de claves de cifrado correspondientes al número de periodo de tiempo durante el que se transmiten los datos. Esta operación de lo que se conoce como “OR exclusiva” es, por supuesto, lineal. La invención se aplica así perfectamente a los sistemas de PMR.

Conforme a la presente invención, la etapa de modificación comprende las sub-etapas de:

- codificar la primera secuencia de claves de cifrado por medio del código de detección de error y del primer código de corrección de error, y la segunda secuencia de claves de cifrado por medio del código de detección de error y del segundo código de corrección de error;

- descifrar el primer paquete codificado por medio de la primera secuencia de claves codificadas, y

- descifrar el segundo paquete codificado por medio de la segunda secuencia de claves codificadas.

Ventajosamente, el descifrado se aplica a decisiones flexibles, en particular procedentes de un demodulador de señal recibida. Con preferencia, con el fin de garantizar la seguridad de la transmisión, las operaciones de codificación/decodificación y descifrado están agrupadas entre sí en un mismo módulo.

Conforme a una primera realización, la etapa de modificación comprende las sub-etapas de:

- codificar la diferencia entre la primera y la segunda secuencias de claves por medio del código de detección de error y del primer o respectivamente el segundo código de corrección de error, y

- usar la diferencia codificada para modificar el primer paquete codificado o respectivamente el segundo paquete codificado.

En otras palabras, se han previsto dos alternativas en el marco de la presente realización. En la primera variante, la diferencia entre la primera y la segunda secuencias de claves se codifica por medio del código de detección de error y del primer código de corrección de error, y esta diferencia codificada se usa para modificar el primer paquete codificado. En la segunda variante, la diferencia entre la primera y la segunda secuencias de claves se codifica por medio del código de detección de error y del segundo código de corrección de error y esta diferencia codificada se usa para modificar el segundo paquete codificado.

Gracias a la codificación de la diferencia entre las secuencias de claves, se mejora la seguridad. En efecto, el módulo de descifrado del receptor solamente proporciona la diferencia entre las secuencias de claves a los módulos de procesamiento de señal encargados de la codificación/decodificación. No se puede recuperar ninguna información secreta fuera del módulo de descifrado sin conocimiento de la clave de cifrado precedente, en particular la inicial, es decir, la de transmisión del primer paquete.

Conforme a una segunda realización, la etapa de modificación comprende las sub-etapas de:

- generar una nueva secuencia de claves de cifrado;

- codificar una primera diferencia entre la primera secuencia de claves y la nueva secuencia de claves por medio del código de detección de error y del primer código de corrección de error;

- codificar una segunda diferencia entre la segunda secuencia de claves y la nueva secuencia de claves por medio del código de detección de error y del segundo código de corrección de error;

- usar la primera diferencia codificada a efectos de modificar el primer paquete codificado, y

- usar la segunda diferencia codificada con el fin de modificar el segundo paquete codificado.

Ventajosamente, el procedimiento de HARQ es un procedimiento de HARQ-Chase.

Este procedimiento es muy simple, siendo el primer y el segundo códigos de corrección de error aplicados al primer y al segundo paquetes idénticos en este caso. La decodificación se lleva a cabo también con el mismo código de corrección de error. Con preferencia, la combinación se realiza mediante el cálculo de decisiones flexibles por medio de relaciones de probabilidad logarítmica, conocidas como LLR (“Relaciones de Probabilidad Log”). La HARQ-Chase consiste entonces en sumar las LLRs de las diferentes transmisiones de un mismo paquete.

Alternativamente, el procedimiento de HARQ es un procedimiento de HARQ con redundancia incremental.

Este procedimiento, conocido como IR-HARQ (Redundancia Incremental – HARQ) permite que la tasa efectiva de flujo de datos sea mejorada. En dicho procedimiento, el segundo código de corrección de error posee una redundancia mayor que el primer código de corrección de error. El tercer código de corrección de error es entonces una concatenación del primer y el segundo códigos de corrección de error.

Ambos procedimientos de HARQ-Chase e IR-HARQ pueden ser combinados con vistas a obtener mejores resultados.

La invención se refiere también a un sistema de transmisión de paquetes de datos entre un transmisor y un receptor a través de un canal radioeléctrico, comprendiendo dicho sistema primeros medios para implementar una primera transmisión de un paquete, donde dichos primeros medios comprenden medios implementados en el transmisor, que consisten en:

- un primer procesamiento lineal para dicho paquete con el fin de obtener un primer paquete;

- una codificación de detección de error lineal del primer paquete por medio de un código de detección de

error para obtener un primer paquete intermedio, y

- una codificación de corrección de error lineal del primer paquete intermedio a través de un primer código de corrección de error, con el fin de obtener un primer paquete codificado;

un sistema en donde, cuando se recibe el primer paquete codificado y se detecta que éste es erróneo, el sistema comprende segundos medios para implementar al menos una segunda transmisión de dicho paquete, comprendiendo dichos segundos medios:

medios implementados en el transmisor, que consisten en:

- un segundo procesamiento lineal de dicho paquete, siendo dicho segundo procesamiento diferente del primer procesamiento con el fin de obtener un segundo paquete que sea diferente del primero;
- una codificación de detección de error lineal del segundo paquete por medio de dicho código de detección de error, con el fin de obtener un segundo paquete intermedio, y
- una codificación de corrección de error lineal del segundo paquete intermedio a través de un segundo código de corrección de error, con el fin de obtener un segundo paquete codificado;

y medios implementados en el receptor, que consisten en:

- modificación del primer paquete codificado y/o del segundo paquete codificado con el fin de obtener dos paquetes en los que la diferencia debida al primer y segundo procesamientos se compensa;
- combinación de ambos paquetes conforme a un procedimiento de petición de repetición automática hibrida (HARQ), y
- decodificación del paquete combinado por medio de un tercer código de corrección de error que depende del primer y segundo códigos de corrección de error.

La invención se refiere también a una instalación de recepción que comprende medios para implementar las etapas del método de la invención, que consisten en:

- modificación del primer paquete codificado y del segundo paquete codificado con el fin de obtener dos paquetes en los que la diferencia debida al primer y segundo procesamientos se compensa;
- combinación de ambos paquetes conforme a un procedimiento de petición de repetición automática híbrida (HARQ), y
- decodificación del paquete combinado por medio del tercer código de corrección de error.

La invención se refiere también a un programa informático que comprende instrucciones para implementar el método de la invención cuando el programa se ejecuta por medio de al menos un procesador.

Los diagramas de bloques de las Figuras 2 a 5 ilustran esquemáticamente la ejecución de este programa informático para realizaciones preferidas de la invención.

Ahora se van a describir realizaciones de la invención de manera más precisa, pero no limitativa, con referencia a los dibujos que se acompañan, en los que:

La Figura 1 es un esquema de un sistema de transmisión de paquetes de datos de la invención;

La Figura 2 es un diagrama de bloques que ilustra la operación del método de transmisión de paquetes conforme a una primera realización de la invención;

La Figura 3 es un diagrama de bloques que ilustra la operación del método de transmisión de paquetes conforme a una segunda realización de la invención;

La Figura 4 es un diagrama de bloques que ilustra la operación del método de transmisión de paquetes conforme a una tercera realización de la invención;

La Figura 5 es un diagrama de bloques que ilustra la operación del método de transmisión de paquetes conforme a una cuarta realización de la invención, y

La Figura 6 es un gráfico que ilustra los rendimientos del método conforme a la invención.

La Figura 1 representa un sistema de transmisión 2 para paquetes de datos entre un transmisor 4 y un receptor 6 a través de un canal radioeléctrico 8.

El transmisor 4 y el receptor 6 consisten, en este caso, en un terminal y una estación de base de un sistema de PMR. De ese modo, la transmisión a la que se refiere la presente invención puede ser una transmisión en una dirección ascendente, es decir desde el terminal hasta la estación de base, o una transmisión en una dirección descendente, es decir, desde la estación de base hasta el terminal.

La invención no está limitada, sin embargo, a este caso, y también se aplica al caso de dos terminales que operen en modo directo.

El transmisor 4 comprende cinco módulos principales, los cuales son un módulo 10 de formación de paquetes, un módulo 16 de cifrado, y un módulo 17 de codificación de detección de error, un módulo 18 de codificación de corrección de error, y un modulador 20. También comprende una antena 22.

El módulo 10 de formación de paquetes implementa el protocolo MAC/RLC ("Control de Acceso del Medio/Control de Enlace de Radio"). Éste se encuentra adaptado para proporcionar paquetes de datos binarios, conocidos como PDU o unidades de datos de protocolo sobre ranuras de tiempo sucesivas identificadas por sus números no. Éste comprende una memoria intermedia 23 para almacenar los paquetes que se están formando con el fin de estar en condiciones de encontrarlos para una posible retransmisión.

El módulo 16 de cifrado implementa un cifrado lineal de la interfaz de radio de AIE de los paquetes de PDU que se están formando. Tal cifrado es lineal dado que la combinación entre la secuencia que va a ser cifrada y la secuencia de cifrado es lineal. Éste está capacitado para generar secuencias de claves de cifrado dependiendo del número de ranura de tiempo suministrada por el módulo 10 de formación de paquete. De ese modo, dos secuencias de claves de cifrado generadas para cifrar dos paquetes transmitidos en dos ranuras de tiempo diferentes, son diferentes. Los paquetes de PDU cifrados conocidos como PDU_C son proporcionados a la salida del módulo 16 de cifrado.

El módulo 17 de codificación de detección de error permite que los paquetes de PDU cifrados sean codificados con el fin de permitir la detección de un error a nivel del receptor 6. El código de detección de error implementado en el módulo 17 de codificación de detección de error es lineal. Éste es, por ejemplo, un código de redundancia cíclica CRC ("Comprobación de Redundancia Cíclica").

El módulo 17 de codificación de corrección de error permite que los paquetes de PDU que van a ser cifrados por el módulo 16 de cifrado y codificados por medio del código de detección de error del módulo 17 de codificación de detección de error, sean codificados. El código de corrección de error implementado en el módulo 18 de codificación de corrección de error es un código lineal. Éste es, por ejemplo, un código convolucional o un turbo-código. Datos de Ck codificados por medio del código de corrección de error son suministrados de ese modo a la salida del módulo 18 de codificación de corrección de error.

Ventajosamente, los módulos (17, 18) de codificación de detección de error y de codificación de corrección de error pueden ser combinados en un mismo módulo que implemente tanto la detección como la corrección de errores.

El modulador 20 proporciona la modulación de los datos binarios codificados de Ck suministrados por el módulo 18 de codificación de corrección de error en símbolos de datos Sk conforme a una técnica de modulación convencional, por ejemplo modulación de amplitud en cuadratura MAQ. Éste permite también el bloqueo de trama de los símbolos de datos para su sincronización con el receptor 6.

El receptor 6 comprende una antena 24 y cuatro módulos principales que permiten que los datos sean recuperados. Tales módulos son un demodulador 26, un módulo 28 de decodificación de canal, un módulo 30 de descifrado y un módulo 32 de separación de datos.

El demodulador 26 proporciona el desbloqueo de trama y la demodulación de los símbolos de datos recibidos. Éste implementa un mecanismo de demodulación de salida flexible, por ejemplo mediante el cálculo de relaciones de probabilidad logarítmica LLR.

Una memoria intermedia 34 presente en el receptor 6, permite que las relaciones de LLR calculadas sean almacenadas.

El módulo 28 de decodificación de canal comprende tres sub-módulos que son un sub-módulo 36 de decodificación de corrección de error, un sub-módulo 38 de codificación, que combina una codificación de detección de error y una codificación de corrección de error, y un sub-módulo 40 de decodificación de canal de error.

El sub-módulo 36 de decodificación de corrección de error proporciona la decodificación de las relaciones LLR por medio del código de corrección de error implementado en el módulo 18 de codificación de corrección de error para suministrar paquetes de datos decodificados.

El sub-módulo 38 de codificación permite la codificación de la información, en particular claves de cifrado, por medio del código de detección de error implementado en el módulo 17 de codificación de detección de error y del código de corrección de error implementado en el módulo 18 de codificación de corrección de error.

El sub-módulo 40 de decodificación de detección de error implementa el código de detección de error implementado en el módulo 17 de codificación de detección de error con el fin de detectar posibles errores en los paquetes de error decodificados.

El módulo 30 de descifrado proporciona el cálculo de las secuencias de claves de cifrado y el descifrado de AIE de los paquetes decodificados a través de las mismas secuencias de claves de cifrado usadas por el modulo 16 de cifrado, para cifrarlas.

El módulo 32 de separación de datos permite que los paquetes de datos descifrados sean separados mediante la implementación del protocolo de MAC/RLC.

Ahora se van a describir diferentes realizaciones del método de transmisión implementado por el sistema 2, con referencia a los diagramas de bloques de las Figuras 2 y 5.

La Figura 2 ilustra una primera realización de la invención.

En la etapa 50, el módulo 10 de formación de paquetes recibe datos binarios para ser transmitidos, que se conocen como unidades de datos de servicio o unidades de SDU (“Unidades de Datos de Servicio). Éste añade a esos datos una cabecera con el fin de formar una PDU 52 de paquete de datos que la salva en la memoria 23.

En la etapa 54, el módulo 16 de cifrado recibe la PDU 52 de paquete de datos, así como el número no. de ranura de tiempo correspondiente a ese paquete. Éste genera una primera secuencia de claves de cifrado que depende del número no. de ranura de tiempo y cifra el paquete 52 con esta primera secuencia con el fin de obtener un primer paquete 56. El cifrado es lineal. Esto se realiza, por ejemplo, llevando a cabo una “OR exclusiva” entre el paquete de datos 52 y la primera secuencia de claves de cifrado.

En la etapa 57, el módulo 17 de codificación de detección de error codifica el primer paquete 56 a través de un código de detección de error lineal, por ejemplo un código CRC, y suministra a la salida un primer paquete intermedio 58.

En la etapa 59, el módulo 18 de codificación de corrección de error codifica el primer paquete intermedio 58 a través del código de corrección de error lineal y proporciona a la salida un primer paquete codificado 60.

En la etapa 61, el modulador 30 modula los datos del primer paquete codificado 60, por ejemplo con una modulación 16 de MOQ, con el fin de proporcionar una señal 62 portadora de símbolos de datos complejos que están organizados en tramas.

En la etapa 64, la señal 62 se emite por medio de la antena 22 a través del canal radioeléctrico 8.

En la etapa 66, la señal 62, posiblemente ruidosa y/o distorsionada por el canal 8, se recibe por medio de la antena 24 del receptor 6.

En la etapa 68, el demodulador 26 realiza el desbloqueo de trama, es decir, la sincronización de la señal 62, y la desmodula conforme a un mecanismo de demodulación de decisión flexible. Para hacer esto, el demodulador 26 calcula decisiones flexibles, con preferencia primeras relaciones de probabilidad logarítmica de LLR.

Las primeras relaciones de LLR calculadas son decodificadas en la etapa 70 por medio del módulo 36 de decodificación corrector de errores.

En la etapa 72, el sub-módulo 40 de decodificación de detección de error detecta la presencia de posibles errores en las primeras relaciones de LLR decodificadas.

Si no se detecta ningún error, las primeras relaciones de LLR decodificadas son descifradas en la etapa 74 por el modulo 30 de descifrado con la primera secuencia de claves de cifrado, con el fin de obtener un paquete de PDU descifrado.

En la etapa 76, el módulo 32 de separación realiza la separación de los datos del paquete de PDU descifrado con el fin de proporcionar los datos de SDU binarios. A continuación, emite un reconocimiento positivo hacia el módulo 10 de formación de paquete del transmisor 4 con el fin de indicar que el paquete 52 ha sido bien recibido, sin ningún error.

En caso de que se detecte al menos un error, las primeras relaciones LLR calculadas son salvadas, en la etapa 78, en la memoria intermedia 34. El receptor 6 envía, en la etapa 80, una petición de retransmisión para el paquete 52 hacia el transmisor 4.

Tras la recepción de esa petición, el transmisor 4 recupera, en la etapa 82, el paquete 52 desde la memoria 23.

En la etapa 84, el módulo 16 de cifrado recibe el paquete de datos 52 así como el número de la nueva ranura de tiempo correspondiente a este paquete. Esto genera una segunda secuencia de claves de cifrado que depende del

número de ranura, y cifra el paquete 52 con esta segunda secuencia con el fin de obtener un segundo paquete 86.

Puesto que el paquete se emite tras una ranura de tiempo que es diferente de la correspondiente a la primera transmisión, la segunda secuencia de claves es diferente de la primera secuencia de claves. El segundo paquete 86 es por lo tanto diferente del primer paquete 56.

En la etapa 87, el módulo 17 de codificación de detección de error codifica el segundo paquete 86 por medio de un código de detección de error lineal y suministra en la salida un segundo paquete intermedio 88.

En la etapa 89, el módulo 18 de codificación de corrección de error codifica el segundo paquete intermedio 88 por medio del código de corrección de error lineal y proporciona en la salida un segundo paquete codificado 90.

En la etapa 91, el modulador 20 modula los datos del segundo paquete codificado para suministrar una señal 92 que porta símbolos de datos complejos que están organizados en tramas.

En la etapa 94, la señal 92 es emitida por medio de la antena 22 a través del canal radioeléctrico 8.

En la etapa 96, la señal 92 posiblemente ruidosa y/o distorsionada por el canal 8, es recibida por la antena 24 del receptor 6.

En la etapa 98, el demodulador 26 realiza el desbloqueo de trama, es decir, la sincronización de la señal 92, y la desmodula conforme a un mecanismo de demodulación de decisión flexible calculando las segundas relaciones de probabilidad logarítmica de LLR.

En la etapa 99, el módulo 30 de descifrado produce la segunda secuencia de claves de cifrado.

En la etapa 100, el sub-módulo de codificación 38 codifica la segunda secuencia de claves de cifrado a través del código de detección y del código de corrección de error.

En la etapa 102, el sub-módulo 31 de descifrado flexible descifra las segundas relaciones de LLR por medio de la segunda secuencia de claves codificada. Gracias a la linealidad del código de corrección y del cifrado, adicionalmente a este descifrado flexible, las segundas relaciones de LLR descifradas corresponden al paquete codificado 52.

Tras el descifrado, en la etapa 102, el sub-módulo 31 de descifrado flexible modifica las segundas relaciones de LLR por medio de la segunda secuencia de claves codificada conforme a la siguiente relación:

$$LLR2\_m(k) = LLR2(k)*(1-2*K2\_codificado) \text{ para } k=0, ..., N-1,$$

en donde:

- N es el número de relaciones de LLR por paquete de PDU codificado;
- K2_codificado es la segunda secuencia de claves codificada;
- LLR2(k) es la segunda relación de LLR, y
- LLR2_m(k) es la segunda relación de LLR modificada.

En la etapa 103, el modulo 30 de descifrado produce la primera secuencia de claves de cifrado. En la etapa 104, el sub-módulo de codificación 38 codifica la primera secuencia de claves de cifrado mediante el código de detección de error y el código de corrección de error.

En la etapa 106, las primeras relaciones de LLR son recuperadas desde la memoria intermedia 34.

En la etapa 108, el sub-módulo 31 de descifrado flexible descifra las primeras relaciones de LLR que son recuperadas a través de la primera secuencia de claves codificada. Gracias a la linealidad del código de corrección y del cifrado, además de este descifrado flexible, las primeras relaciones LLR descifradas que se obtienen corresponden al paquete codificado 52.

Tras el descifrado, en la etapa 108, el sub-módulo 31 de descifrado flexible modifica las primeras relaciones de LLR por medio de la primera secuencia de claves codificada conforme a la siguiente relación:

$$LLR1\_m(k) = LLR1(k)*(1-2*K1\_codificado) \text{ para } k=0, ..., N-1,$$

en donde:

- N es el número de relaciones de LLR por paquete de PDU codificado;
- K1_codificado es la primera secuencia de claves codificada;

- LLR1(k) es la primera relación de LLR, y
- LLR1_m(k) es la primera relación de LLR modificada.

En la etapa 110, se lleva a cabo una combinación de HARQ-Chase de las primeras relaciones de LLR descifradas y de las segundas relaciones de LLR descifradas, simplemente sumando tales relaciones de LLR con el fin de obtener relaciones de LLR combinadas.

Las relaciones de LLR combinadas son decodificadas en la etapa 112 por el sub-módulo 36 de decodificación de corrección de error para obtener el paquete de PDU decodificado.

En la etapa 114, el sub-módulo 40 de decodificación de detección de error detecta la presencia de posibles errores residuales.

Si no se detecta ningún error, el módulo de separación 32 separa, en la etapa 116, los datos del paquete de PDU decodificado con el fin de suministrar datos de SDU binarios. A continuación, éste emite un reconocimiento positivo hacia el módulo 10 de formación de paquete del transmisor 4 para indicar que el paquete 52 ha sido bien recibido sin ningún error.

Si se detecta al menos un error, el método avanza desde la etapa 78 salvando las segundas relaciones de LLR calculadas por el demodulador 26 y una nueva transmisión del paquete 52.

Esta primera realización es muy simple de implementar. Ésta necesita, no obstante, el suministro de secuencias de claves de cifrado como tales desde el módulo 30 de descifrado hasta el módulo 28 de decodificación. Este suministro no se desea en algunas aplicaciones por motivos de seguridad. Sin embargo, la primera realización se aplica también a estos casos. De hecho, es suficiente integrar las operaciones de codificación/decodificación de canal y el descifrado flexible 31 en el módulo 30 de descifrado.

Las realizaciones descritas con referencia a las Figuras 3 a 5 permiten que se evite tal suministro explícito de secuencias de claves de cifrado, y que se mejore por tanto la seguridad de la transmisión.

En estas Figuras, las etapas 50 a 96 son idénticas a las de la Figura 2. Por lo tanto, no se va a repetir la descripción de tales etapas.

La Figura 3 ilustra una segunda realización preferida de la invención.

Según esta realización, además de la recepción de la señal emitida en la etapa 96, el módulo 30 de descifrado calcula, en la etapa 120, la diferencia entre la primera y la segunda secuencias de claves de cifrado. Para hacer esto, se realiza una operación de “OR exclusiva” entre las dos secuencias de claves. Ésta suministra entonces esta diferencia al sub-módulo 38 de codificación del módulo 28 de decodificación. De ese modo, se proporcionan las reglas de seguridad en este caso, dado que no se puede recuperar información secreta fuera del módulo 30 de descifrado sin conocimiento de una de las dos secuencias de claves.

En la etapa 122, el sub-módulo de codificación 38 codifica la diferencia entre las secuencias de claves por medio del código de detección de error y del código de corrección de error. Y, a continuación, suministra la diferencia codificada al demodulador 26.

En la etapa 124, el demodulador 26 realiza el desbloqueo de trama, es decir, la sincronización de la señal 92, y la desmodula conforme a un mecanismo de demodulación de decisión flexible calculando las segundas relaciones de probabilidad logarítmica de LLR. Éste modifica esas relaciones de LLR mediante la diferencia codificada conforme a la siguiente relación:

$$LLR2\_m(k) = LLR2(k)*(1-2*cod\Delta k) \text{ para } k=0, ..., N-1,$$

en donde:

- N es el número de relaciones de LLR por paquete de PDU codificado;
- codΔk es la diferencia codificada;
- LLR2(k) es la segunda relación de LLR, y
- LLR2_m(k) es la segunda relación de LLR modificada.

Gracias a la linealidad de los códigos de detección y de corrección y del cifrado, además de esta modificación, las segundas relaciones de LLR modificadas que se obtienen corresponden al paquete 52 codificado y cifrado con la primera secuencia de claves.

En la etapa 126, las primeras relaciones de LLR se recuperan desde la memoria intermedia 34.

En la etapa 128, el demodulador 26 realiza una combinación de HARQ-Chase de las primeras relaciones de LLR y de las segundas relaciones de LLR modificadas, simplemente sumando esas relaciones de LLR con el fin de obtener relaciones de LLR combinadas.

Las relaciones de LLR combinadas se decodifican en la etapa 130 por medio del sub-módulo 36 de decodificación de corrección de error con el fin de obtener el paquete de PDU decodificado.

En la etapa 132, el sub-módulo 40 de decodificación de detección de error detecta la presencia de posibles errores en las relaciones de LLR combinadas.

Si no se detecta ningún error, el módulo de descifrado 30 descifra, en la etapa 134, el paquete de PDU decodificado por medio de la primera secuencia de claves de cifrado.

El módulo de separación 32 separa, en la etapa 136, los datos del paquete de PDU descifrado y decodificado para suministrar los datos de SDU binarios. Y a continuación, emite un reconocimiento positivo hacia el módulo 10 de formación de paquetes del transmisor 4, para indicar que el paquete 52 ha sido bien recibido sin ningún error.

Si se detecta al menos un error, el método avanza desde la etapa 78 salvando las segundas relaciones de LLR calculadas por el demodulador 26 y una nueva transmisión del paquete 52.

De ese modo, conforme a la segunda realización, las segundas relaciones de LLR son las que van a ser modificadas. El modulo 30 de descifrado debe, en este caso, aplicar la primera secuencia de claves de cifrado para descifrar el paquete combinado y no la secuencia de claves actual.

La Figura 4 ilustra una primera realización en donde las primeras relaciones de LLR son las que van a ser modificadas.

Conforme a esta realización, además de la recepción de la señal 92 en la etapa 96, el demodulador 26 realiza el desbloqueo de trama, es decir, la sincronización de la señal 92, y la desmodula en la etapa 98 según un mecanismo de demodulación de decisión flexible calculando las segundas relaciones de probabilidad logarítmica de LLR.

En la etapa 120, el módulo 30 de descifrado calcula la diferencia entre la primera y la segunda secuencias de claves de cifrado. Para hacer esto, realiza una operación de “OR exclusiva” entre las dos secuencias de claves. Éste suministra a continuación esta diferencia al sub-módulo de codificación 38 del módulo de decodificación 28. De ese modo, se proporcionan las reglas de seguridad en este caso, puesto que no se puede recuperar ninguna información secreta fuera del módulo 30 de descifrado sin ningún conocimiento de las dos secuencias de claves.

En la etapa 122, el sub-modulo de codificación 38 codifica la diferencia entre las secuencias de claves mediante el código de detección y el código de corrección de error. Éste suministra a continuación la diferencia codificada al demodulador 26.

En la etapa 126, las primeras relaciones de LLR se recuperan desde la memoria intermedia 34.

En la etapa 140, el demodulador 26 modifica estas primeras relaciones de LLR a través de la diferencia codificada según la siguiente relación:

$$LLR1\_m(k) = LLR1(k)*(1-2*cod\Delta k) \text{ para } k=0, ..., N-1,$$

en donde:

- N es el número de relaciones de LLR por paquete de PDU codificado;
- $cod\Delta k$ es la diferencia codificada;
- LLR1(k) es la primera relación de LLR, y
- LLR1_m(k) es la primera relación de LLR modificada.

Gracias a la linealidad de los códigos de detección y de corrección y al cifrado, además de esta modificación, las primeras relaciones de LLR modificadas que se obtienen corresponden al paquete 52 codificado y cifrado con la segunda secuencia de claves.

En la etapa 142, el demodulador 26 realiza una combinación de HARQ-Chase de las relaciones de LLR modificadas y de las segundas relaciones de LLR simplemente sumando esas relaciones de LLR con el fin de obtener relaciones de LLR combinadas.

Las relaciones de LLR combinadas son decodificadas en la etapa 144 mediante el sub-módulo 36 de decodificación de corrección de error con el fin de obtener el paquete de PDU decodificado.

En la etapa 146, el sub-módulo 40 de decodificación de detección de error detecta la presencia de posibles errores en las relaciones de LLR combinadas.

Si no se detecta ningún error, el módulo de descifrado 30 descifra, en la etapa 148, el paquete de PDU decodificado por medio de la segunda secuencia de claves de cifrado.

El módulo de separación 32 separa, en la etapa 150, los datos del paquete de PDU descifrado decodificado con el fin de suministrar los datos de SDU binarios. A continuación, emite un reconocimiento positivo hacia el módulo 10 de formación de paquetes del transmisor 4 para indicar que el paquete 52 ha sido bien recibido, sin ningún error.

Si se detecta al menos un error, el método avanza desde la etapa 78 salvando las segundas relaciones de LLR calculadas por el demodulador 26 y se realiza una nueva transmisión del paquete 52.

De ese modo, según esta segunda realización, las primeras relaciones de LLR son las que van a ser modificadas. El módulo 30 de descifrado aplica en este caso la secuencia de claves actual a efectos de descifrar el paquete combinado. Esta realización es por lo tanto más simple de implementar que la mostrada en la Figura 3 que necesita un descifrado con la primera secuencia de claves.

La Figura 5 ilustra una cuarta realización de la invención en donde se genera una nueva secuencia de claves de cifrado a nivel del receptor.

Según esta realización, además de la recepción de la señal emitida en la etapa 96, el módulo 30 de descifrado genera, en la etapa 160, una nueva secuencia de claves de cifrado.

En la etapa 162, el módulo 30 de descifrado calcula una primera diferencia entre la primera secuencia de claves y la nueva secuencia de claves, y una segunda diferencia entre la segunda secuencia de claves y la nueva secuencia de claves. Para hacer esto, realiza operaciones de “OR exclusiva” entre las secuencias de claves. A continuación, suministra esas diferencias al sub-módulo de codificación 38 del módulo de decodificación 28. De ese modo, se proporcionan también reglas de seguridad en este caso, puesto que no se puede recuperar ninguna información secreta fuera del módulo 30 de descifrado sin el conocimiento de la nueva secuencia de claves.

En la etapa 164, el sub-módulo de codificación 38 codifica la primera y la segunda diferencias mediante el código de detección y el código de corrección de error. Éste suministra a continuación la primera y la segunda diferencias codificadas al demodulador 26.

En la etapa 166, las primeras relaciones de LLR son recuperadas desde la memoria intermedia 34.

En la etapa 168, el demodulador 26 modifica estas primeras relaciones de LLR mediante la primera diferencia codificada, conforme a la siguiente relación:

$$LLR1\_m(k) = LLR1(k)*(1-2*cod\Delta k1) \text{ para } k=0, ..., N-1,$$

en donde:

- N es el número de relaciones de LLR por paquete de PDU codificado;
- codΔk1 es la primera diferencia codificada;
- LLR1(k) es la primera relación de LLR, y
- LLR1_m(k) es la primera relación de LLR modificada.

Gracias a la linealidad de los códigos de detección y de corrección y del cifrado, además de esta modificación, las primeras relaciones de LLR modificadas que se obtienen corresponden al paquete 52 que está siendo codificado y cifrado con la nueva secuencia de claves.

En la etapa 170, el demodulador 26 realiza el desbloqueo de trama, es decir, la sincronización de la señal 92, y la desmodula según un mecanismo de demodulación de decisión flexible calculando las segundas relaciones de probabilidad logarítmica de LLR. Éste modifica esas relaciones de LLR mediante la segunda diferencia codificada conforme a la siguiente relación:

$$LLR2\_m(k) = LLR2(k)*(1-2*cod\Delta k2) \text{ para } k=0, ..., N-1,$$

en donde:

- N es el número de relaciones de LLR por paquete de PDU codificado;
- codΔk2 es la diferencia codificada;
- LLR2(k) es la segunda relación de LLR, y

- LLR2_m(k) es la segunda relación de LLR modificada.

Gracias a la linealidad de los códigos de detección y de corrección y del cifrado, además de esta modificación, las segundas relaciones de LLR modificadas que se obtienen corresponden al paquete 52 que está siendo codificado y cifrado con la nueva secuencia de claves.

En la etapa 172, el demodulador 26 realiza una combinación de HARQ-Chase de las primeras relaciones de LLR modificadas y de las segundas relaciones de LLR modificadas simplemente sumando esas relaciones de LLR para obtener relaciones de LLR combinadas.

Las relaciones de LLR combinadas son decodificadas en la etapa 174 mediante el sub-módulo 36 de decodificación de corrección de error con el fin de obtener el paquete de PDU decodificado.

En la etapa 176, el sub-módulo 40 de decodificación de detección de error detecta la presencia de posibles errores en las relaciones de LLR combinadas.

Si no se detecta ningún error, el modulo de descifrado 30 descifra, en la etapa 178, el paquete de PDU decodificado mediante la nueva secuencia de claves de cifrado.

El módulo de separación 32 separa, en la etapa 180, los datos del paquete de PDUC descifrado y decodificado para proporcionar los datos de SDU binarios.

A continuación, emite un reconocimiento positivo hacia el módulo 10 de formación de paquetes del transmisor 4 para indicar que el paquete 52 ha sido bien recibido, sin ningún error.

Si se detecta al menos un error, el método avanza a partir de la etapa 78 salvando las segundas relaciones de LLR calculadas por el demodulador 26 y se realiza una nueva transmisión del paquete 52.

El gráfico de la Figura 6 ilustra los rendimientos de un ejemplo de realización que implementa el método de la invención.

La primera curva 190 de este gráfico representa la tasa efectiva de flujo de datos dependiendo de la relación señal-ruido, usando el método de la invención que implementa combinación de HARQ-Chase en el ejemplo de sistema que se está considerando.

La segunda curva 192 de este gráfico representa la tasa efectiva de flujo de datos dependiendo de la relación señal-ruido, usando el método de la técnica anterior que implementa el mecanismo de ARQ en el ejemplo de sistema que se está considerando.

La ganancia de tasa de flujo inducida por el método de la invención para una misma relación de señal-ruido, es significativa. Como ejemplo, para el ejemplo de sistema que se está considerando, para una relación de señal-ruido de 8 dB, el método de la invención permite tener una tasa efectiva de flujo de datos tres veces mayor que la obtenida con el método de la técnica anterior.

Además, el método es muy robusto. Para el ejemplo de sistema que se está considerando, la transmisión de datos es, de hecho, posible en condiciones de una relación de señal-ruido débil (entre 3 y 7 dB), mientras que no lo es con el método de la técnica anterior. Como ejemplo, para una relación de señal-ruido de 6 dB, el método de la invención permite una tasa efectiva de flujo de datos de 11 kbits por segundo, mientras que no es posible transmisión alguna con el método de la técnica anterior.

Por supuesto, se pueden prever también otras realizaciones.

De ese modo, aunque la invención ha sido descrita para un sistema de PMR, se aplica ventajosamente a cualquier otra transmisión radioeléctrica que implemente un cifrado de interfaz de aire.

Por otro lado, el procedimiento de HARQ que se está usando, puede ser diferente del procedimiento de HARQ-Chase descrito con referencia a las Figuras, por ejemplo un procedimiento de HARQ con redundancia incremental (IR-HARQ). En este último caso, los procesamientos con referencia a la realización descrita en la Figura 2 son los mismos hasta la etapa 108. En la etapa 110, las relaciones de LLR no se combinan, sino que simplemente se organizan en vista de la decodificación que sigue. En la etapa 112, esta decodificación tiene a la entrada la totalidad de las relaciones de LLR y decodifica estas últimas conforme a una estructura de código globalmente resultante de la primera y la segunda transmisiones, por ejemplo a través de un tercer código de corrección de error que consiste en una concatenación del primer y segundo códigos de corrección de error usados respectivamente tras la primera y la segunda transmisiones.

REIVINDICACIONES

1.- Un método de transmisión de paquetes de datos entre un transmisor (4) y un receptor (6) a través de un canal radioeléctrico (8), comprendiendo dicho método una primera transmisión de un paquete (52), comprendiendo dicha primera transmisión las etapas implementadas en el transmisor (4):

- realizar un primer cifrado lineal (54) de dicho paquete (52) a través de una primera secuencia de claves de cifrado con el fin de obtener un primer paquete (56);
- realizar una codificación (57) de detección de error lineal del primer paquete (56) a través de un código de detección de error con el fin de obtener un primer paquete intermedio (58), y
- realizar una codificación (59) de corrección de error lineal del primer paquete intermedio (58) a través de un primer código de corrección de error con el fin de obtener un primer paquete codificado (60);

en donde, cuando el primer paquete codificado (60) se recibe y se detecta, por medio de dicho método, que es erróneo, el método comprende al menos una segunda transmisión de dicho paquete (52), comprendiendo la segunda transmisión las etapas implementadas en el transmisor (4):

- realizar un segundo cifrado lineal (84) de dicho paquete (52) a través de una segunda secuencia de claves de cifrado que es diferente de la primera secuencia de claves de cifrado de dicho primer cifrado (54), con el fin de obtener un segundo paquete (86) diferente del primer paquete (56);
- realizar una codificación (87) de detección de error lineal del segundo paquete (86) a través de dicho código de detección de error, con el fin de obtener un segundo paquete intermedio (88), y
- realizar una codificación (89) de corrección de error lineal del segundo paquete intermedio (88) a través de un segundo código de corrección de error, con el fin de obtener un segundo paquete codificado (90);

y las etapas implementadas en el receptor:

- realizar una modificación del primer paquete codificado (60) y/o del segundo paquete codificado (90) con el fin de obtener dos paquetes en los que la diferencia debida al primer y al segundo procesamientos, se compensa;
- realizar una combinación (110; 128; 142; 172) de ambos paquetes conforme a un procedimiento de petición de repetición automática hibrida, HARQ, y
- realizar una decodificación (112; 130; 144; 174) del paquete combinado por medio de un tercer código de corrección de error que depende del primer y segundo códigos de corrección de error;

caracterizado porque la etapa de modificación comprende las sub-etapas de:

- codificar (122) la diferencia entre la primera y la segunda secuencias de claves a través del código de detección de error y del primer, o respectivamente el segundo, código de corrección de error, y
- usar (124; 140) la diferencia codificada para modificar el primer paquete codificado o respectivamente el segundo paquete codificado.

2.- Un método de transmisión de paquetes de datos entre un transmisor (4) y un receptor (6) a través de un canal radioeléctrico (8), comprendiendo dicho método una primera transmisión de un paquete (52), comprendiendo dicha primera transmisión las etapas implementadas en el transmisor (4):

- realizar un primer cifrado lineal (54) de dicho paquete (52) por medio de una primera secuencia de claves de cifrado con el fin de obtener un primer paquete (56);
- realizar una codificación (57) de detección de error lineal del primer paquete (56) a través de un código de detección de error con el fin de obtener un primer paquete intermedio (58), y
- realizar una codificación (59) de corrección de error lineal del primer paquete intermedio (58) a través de un primer código de corrección de error con el fin de obtener un primer paquete codificado (60);

en donde, cuando el primer paquete codificado (60) se recibe y se detecta, por medio de dicho método, que es erróneo, el método comprende al menos una segunda transmisión de dicho paquete (52), comprendiendo la segunda transmisión las etapas implementadas en el transmisor (4):

- realizar un segundo cifrado lineal (84) de dicho paquete (52) a través de una segunda secuencia de claves

de cifrado que es diferente de la primera secuencia de claves de cifrado de dicho primer cifrado (54) con el fin de obtener un segundo paquete (86) diferente del primer paquete (56);

- realizar una codificación (87) de detección de error lineal del segundo paquete (86) por medio de dicho código de detección de error con el fin de obtener un segundo paquete intermedio (88), y
- realizar una codificación (89) de corrección de error lineal del segundo paquete intermedio (88) por medio de un segundo código de corrección de error con el fin de obtener un segundo paquete codificado (90);

y las etapas implementadas en el receptor:

- realizar una modificación del primer paquete codificado (60) y/o del segundo paquete codificado (90) con el fin de obtener dos paquetes en los que la diferencia debida al primer y segundo procesamientos, se compensa;
- realizar una combinación (110; 128; 142; 172) de ambos paquetes conforme a un procedimiento de petición de repetición automática híbrida, HARQ, y
- realizar una decodificación (112; 130; 144; 174) del paquete combinado a través de un tercer código de corrección de error que depende del primer y segundo códigos de corrección de error;

caracterizado porque la etapa de modificación comprende las sub-etapas de:

- generar (160) una nueva secuencia de claves de cifrado;
- codificar (164) una primera diferencia entre la primera secuencia de claves y la nueva secuencia de claves por medio del código de detección de error y del primer código de corrección de error;
- codificar (164) una segunda diferencia entre la segunda secuencia de claves y la nueva secuencia de claves por medio del código de detección de error y del segundo código de corrección de error;
- usar (168) la primera diferencia codificada con el fin de modificar el primer paquete codificado, y
- usar (170) la segunda diferencia codificada con el fin de modificar el segundo paquete codificado.

3.- El método según cualquiera de las reivindicaciones anteriores, en donde el procedimiento de HARQ es un procedimiento de HARQ-Chase.

4.- El método según cualquiera de las reivindicaciones anteriores, en donde el procedimiento de HARQ es un procedimiento de HARQ con redundancia incremental.

5.- Un sistema (2) de transmisión de paquetes de datos entre un transmisor (4) y un receptor (6) a través de un canal radioeléctrico (8), comprendiendo dicho sistema primeros medios para implementar una primera transmisión de un paquete (52), donde dichos primeros medios comprenden medios implementados en el transmisor (4):

- medios para un primer cifrado lineal (16) para dicho paquete por medio de una primera secuencia de claves de cifrado con el fin de obtener un primer paquete (56);
- medios para una codificación (17) de detección de error lineal del primer paquete (56) por medio de un código de detección de error con el fin de obtener un primer paquete intermedio (58), y
- medios para una codificación (18) de corrección de error lineal del primer paquete intermedio (58) por medio de un primer código de corrección de error con el fin de obtener un primer paquete codificado (60);

en donde, cuando el primer paquete codificado (60) se recibe y se detecta que es erróneo, el sistema comprende segundos medios para implementar al menos una segunda transmisión de dicho paquete (52), donde dichos segundos medios comprenden medios implementados en el transmisor:

- medios para un segundo cifrado lineal (16) de dicho paquete (52) a través de una segunda secuencia de claves de cifrado que es diferente de la primera secuencia de claves de cifrado del primer cifrado, con el fin de obtener un segundo paquete (86) que es diferente del primero (56);
- medios para una codificación (17) de detección de error lineal del segundo paquete (86) por medio de dicho código de detección de error, con el fin de obtener un segundo paquete intermedio (88), y
- medios para una codificación (18) de corrección de error lineal del segundo paquete intermedio (88) por medio de un segundo código de corrección de error, con el fin de obtener un segundo paquete codificado (90);

y donde dichos segundos medios comprenden medios implementados en el receptor:

- medios para modificar el primer paquete codificado (60) y/o el segundo paquete codificado (90) con el fin de obtener dos paquetes en los que la diferencia debida al primer y segundo procesamientos, se compensa;

- medios para combinar (26) ambos paquetes conforme a un procedimiento de petición de repetición automática híbrida, HARQ, y

- medios para decodificar (36) el paquete combinado por medio de un tercer código de corrección de error que depende del primer y segundo códigos de corrección de error;

caracterizado porque dichos medios para la modificación, comprenden:

- un sub-módulo de codificación (38) para codificar la diferencia entre la primera y la segunda secuencias de claves por medio del código de detección de error y del primer, o respectivamente el segundo, código de detección de error;

- un demodulador (26) para modificar el primer paquete codificado o respectivamente el segundo paquete codificado, por medio de la diferencia codificada.

6.- Un receptor (6) para su uso con el transmisor (4) en el sistema (2) de transmisión de paquetes de datos según la reivindicación 5, comprendiendo el receptor (6):

- medios para modificar el primer paquete codificado (60) y/o el segundo paquete codificado (90), con el fin de obtener dos paquetes en los que la diferencia debida al primer y segundo procesamientos, se compensa;

- medios para combinar (26) ambos paquetes según un procedimiento de petición de repetición automática híbrida, HARQ, y

- medios para decodificar (36) el paquete combinado a través de un tercer código de corrección de error que depende del primer y segundo códigos de corrección de error,

caracterizado porque dichos medios para la modificación comprenden:

- un sub-módulo de codificación (38) para codificar la diferencia entre la primera y la segunda secuencias de claves a través del código de detección de error y del primer, o respectivamente el segundo, código de detección de error;

- un demodulador (26) para modificar el primer paquete codificado, o respetivamente el segundo paquete codificado, por medio de la diferencia codificada.

7.- Un sistema (2) de transmisión de paquetes de datos entre un transmisor (4) y un receptor (6) a través de un canal radioeléctrico (8), comprendiendo dicho sistema primeros medios para implementar una primera transmisión de un paquete (52), donde dichos primeros medios comprenden medios implementados en el transmisor (4):

- medios para un primer cifrado lineal (16) para dicho paquete a través de una primera secuencia de claves de cifrado con el fin de obtener un primer paquete (56);

- medios para una codificación (17) de detección de error lineal del primer paquete (56) a través de un código de detección de error, con el fin de obtener un primer paquete intermedio (58), y

- medios para una codificación (18) de corrección de error lineal del primer paquete intermedio (58) a través de un primer código de corrección de error, con el fin de obtener un primer paquete codificado (60);

en donde, cuando el primer paquete codificado (60) se recibe y se detecta que es erróneo, el sistema comprende segundos medios para implementar al menos una segunda transmisión de dicho paquete (52), donde dichos segundos medios comprenden medios implementados en el transmisor:

- medios para un segundo cifrado lineal (16) de dicho paquete (52) a través de una segunda secuencia de claves de cifrado que es diferente de la primera secuencia de claves de cifrado del primer cifrado, con el fin de obtener un segundo paquete (86) que es diferente del primero (56);

- medios para una codificación (17) de detección de error lineal del segundo paquete (86) a través de dicho código de detección de error, con el fin de obtener un segundo paquete intermedio (88), y

- medios para una codificación (18) de corrección de error lineal del segundo paquete intermedio (88) a través de un segundo código de corrección de error, con el fin de obtener un segundo paquete codificado (90);

y donde dichos segundos medios comprenden medios implementados en el receptor:

- medios para modificar el primer paquete codificado (60) y/o el segundo paquete codificado (90), con el fin de obtener dos paquetes en los que la diferencia debida al primer y segundo procesamientos, se compensa;

- medios para combinar (26) ambos paquetes según un procedimiento de petición de repetición automática híbrida, HARQ, y

- medios para decodificar (36) el paquete combinado a través de un tercer código de corrección de error que depende del primer y segundo códigos de corrección de error;

caracterizado porque dichos medios para la modificación comprenden:

- un módulo de descifrado (30) para generar una nueva secuencia de claves de cifrado;

- un sub-módulo de codificación (38) para codificar una primera diferencia entre la primera secuencia de claves y la nueva secuencia de claves por medio del código de detección de error y del primer código de corrección de error; y, para codificar una segunda diferencia entre la segunda secuencia de claves y la nueva secuencia de claves a través del código de detección de error y del segundo código de corrección de error;

- un demodulador (26) para modificar el primer paquete codificado a través de la primera diferencia codificada, y para modificar el segundo paquete codificado a través de la segunda diferencia codificada.

8.- Un receptor (6) para su uso con el transmisor (4) en el sistema (2) de transmisión de paquetes de datos según la reivindicación 7, comprendiendo el receptor (6):

- medios para modificar el primer paquete codificado (60) y/o el segundo paquete codificado (90) con el fin de obtener dos paquetes en los que la diferencia debida al primer y segundo procesamientos, se compensa;

- medios para combinar (26) ambos paquetes según un procedimiento de petición de repetición automática híbrida, HARQ, y

- medios para decodificar (36) el paquete combinado por medio de un tercer código de corrección de error que depende del primer y segundo códigos de corrección de error;

caracterizado porque dichos medios para la modificación comprenden:

- un módulo de descifrado (30) para generar una nueva secuencia de claves de cifrado;

- un sub-módulo de codificación (38) para codificar una primera diferencia entre la primera secuencia de claves y la nueva secuencia de claves por medio el código de detección de error y del primer código de corrección de error; y, para codificar una segunda diferencia entre la segunda secuencia de claves y la nueva secuencia de claves por medio del código de detección de error y del segundo código de corrección de error;

- un demodulador (26) para modificar el primer paquete codificado por medio de la primera diferencia codificada, y para modificar el segundo paquete codificado por medio de la segunda diferencia codificada.

9.- Un programa informático que comprende instrucciones para implementar el método de la invención según una cualquiera de las reivindicaciones 1 a 4 cuando el programa se ejecuta por medio de al menos un procesador.

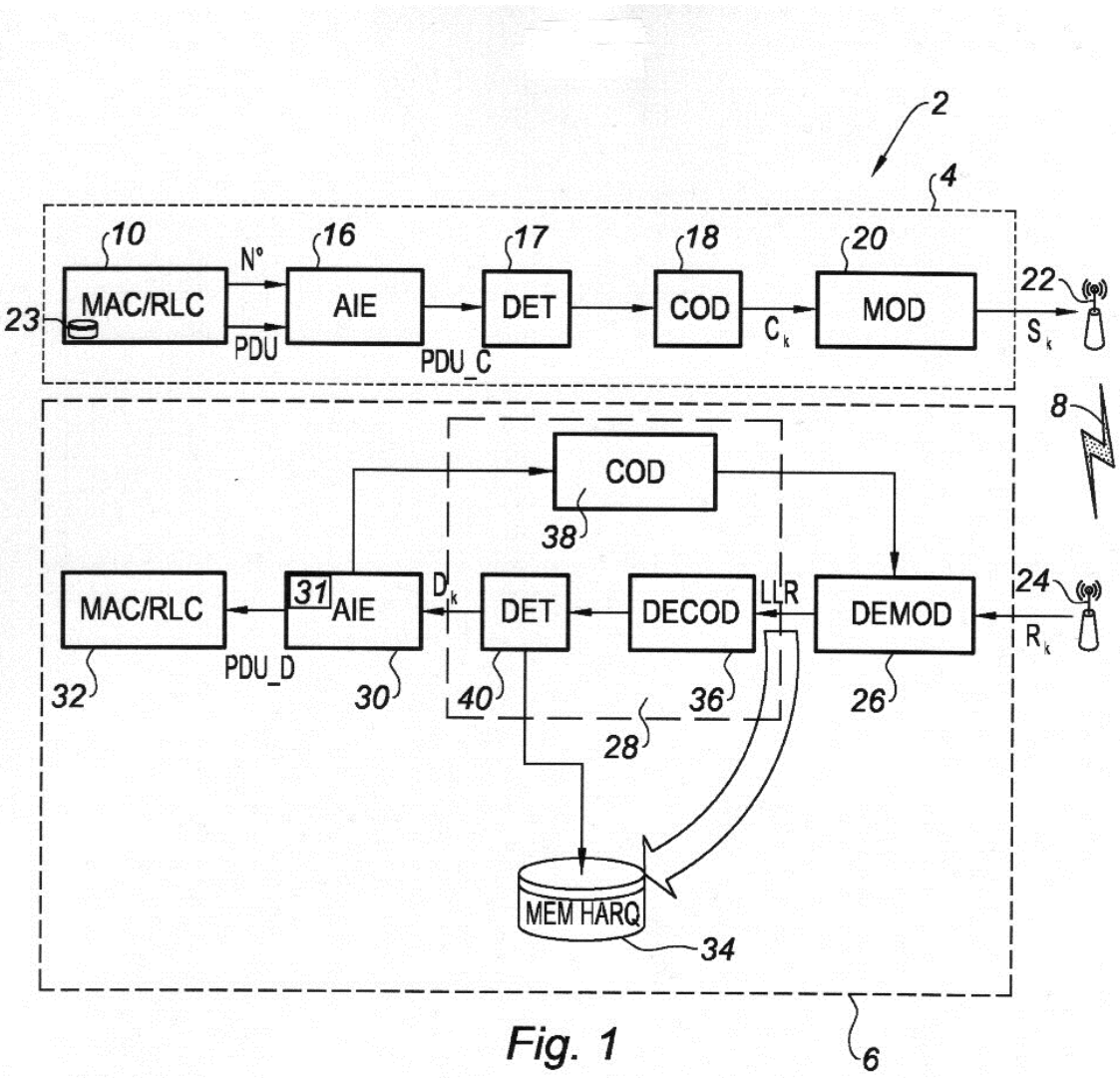
2
4
10
N°
16
17
18
20
22
23
MAC/RLC
AIE
DET
COD
MOD
PDU
PDU_C
C_k
S_k
8
COD
38
MAC/RLC
31
AIE
D_k
DET
DECOD
LLR
DEMOD
24
R_k
PDU_D
32
30
40
36
26
28
MEM HARQ
34
6

Fig. 1

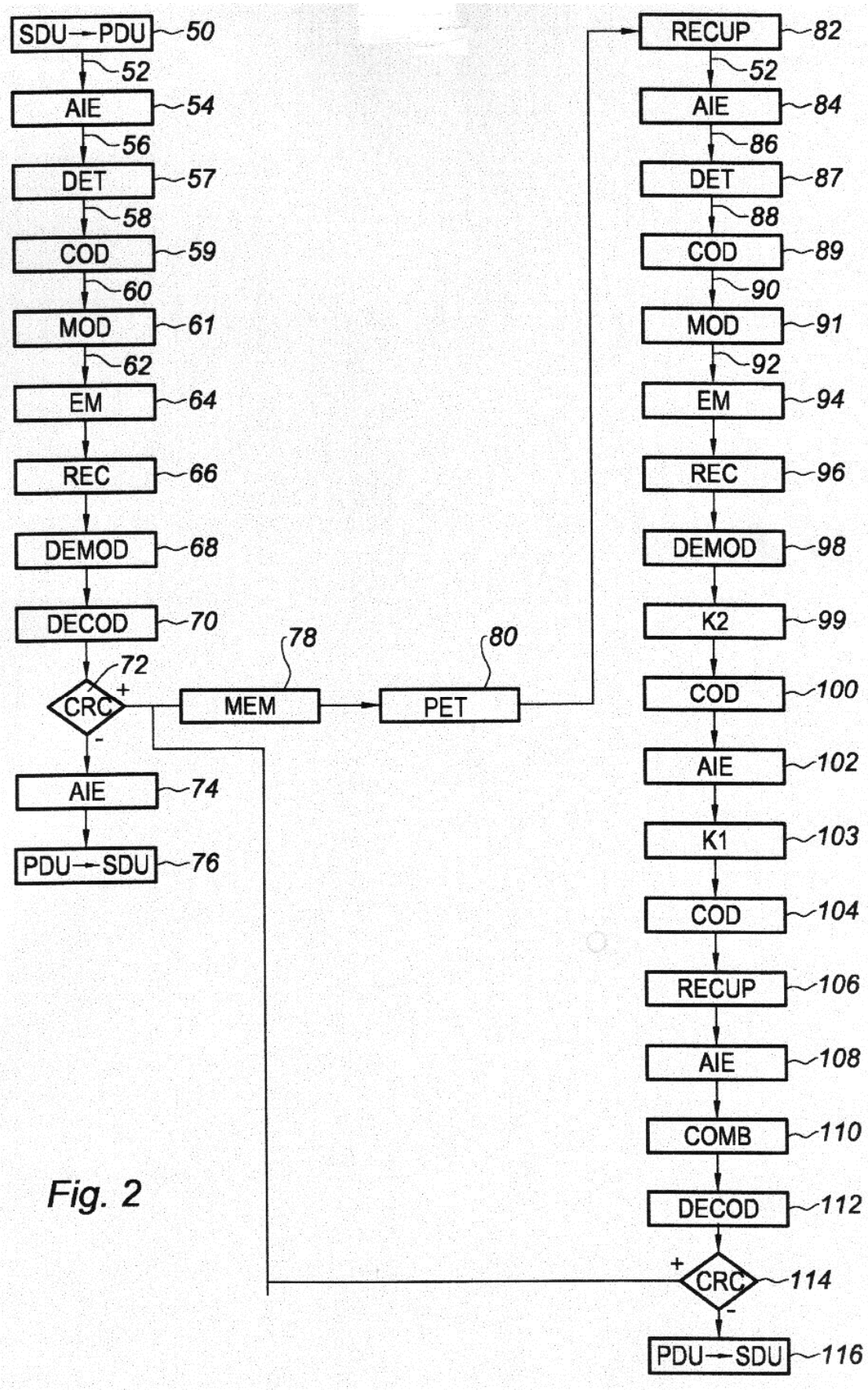
SDU→PDU
50
52
AIE
54
56
DET
57
58
COD
59
60
MOD
61
62
EM
64
REC
66
DEMOD
68
DECOD
70
72
CRC
+
-
78
MEM
80
PET
AIE
74
PDU→SDU
76
RECUP
82
52
AIE
84
86
DET
87
88
COD
89
90
MOD
91
92
EM
94
REC
96
DEMOD
98
K2
99
COD
100
AIE
102
K1
103
COD
104
RECUP
106
AIE
108
COMB
110
DECOD
112
+
CRC
114
-
PDU→SDU
116

Fig. 2

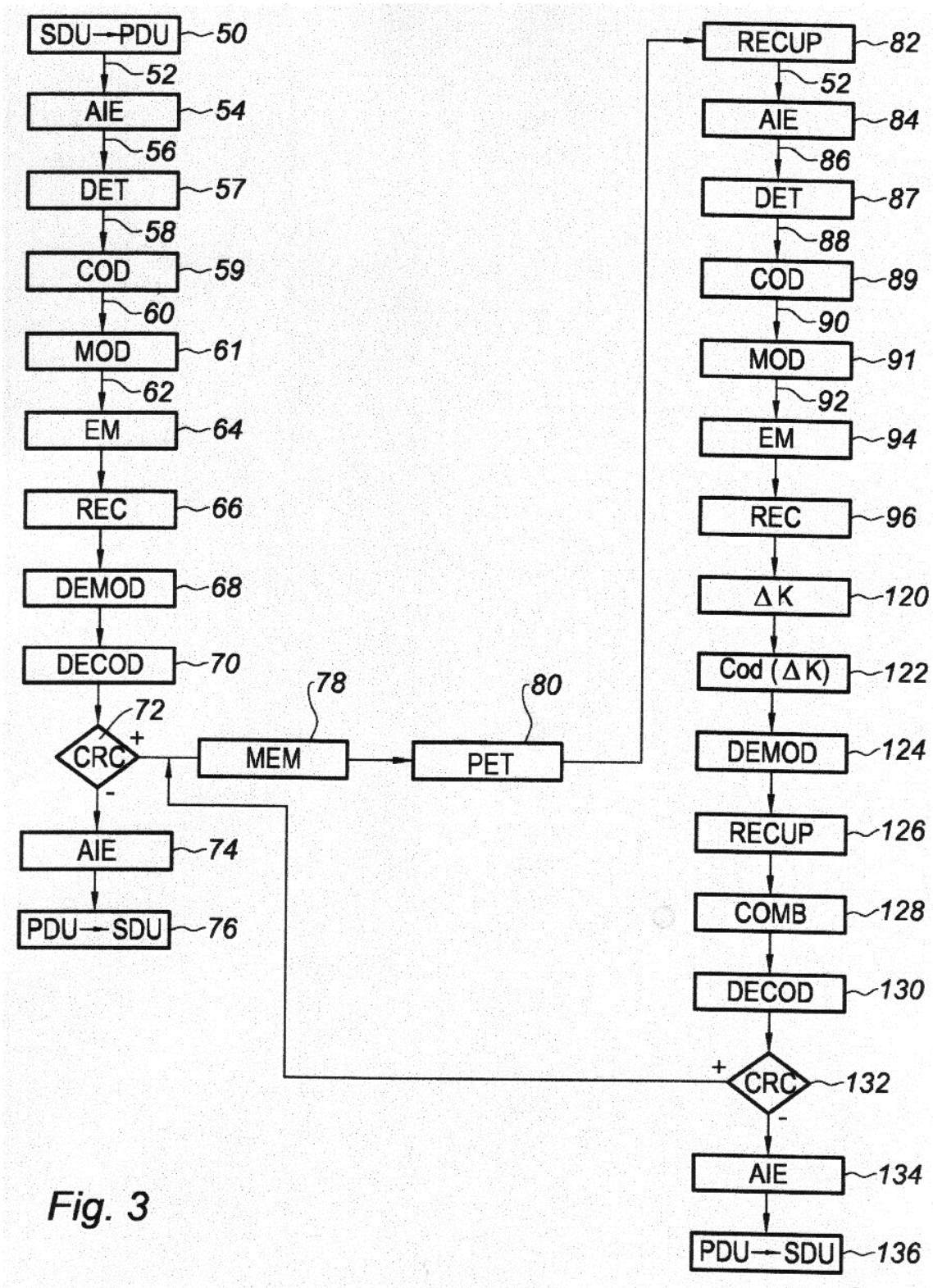
SDU→PDU
50
52
AIE
54
56
DET
57
58
COD
59
60
MOD
61
62
EM
64
REC
66
DEMOD
68
DECOD
70
72
CRC
+
-
78
MEM
80
PET
AIE
74
PDU→SDU
76
RECUP
82
52
AIE
84
86
DET
87
88
COD
89
90
MOD
91
92
EM
94
REC
96
ΔK
120
Cod (ΔK)
122
DEMOD
124
RECUP
126
COMB
128
DECOD
130
+
CRC
132
-
AIE
134
PDU→SDU
136

Fig. 3

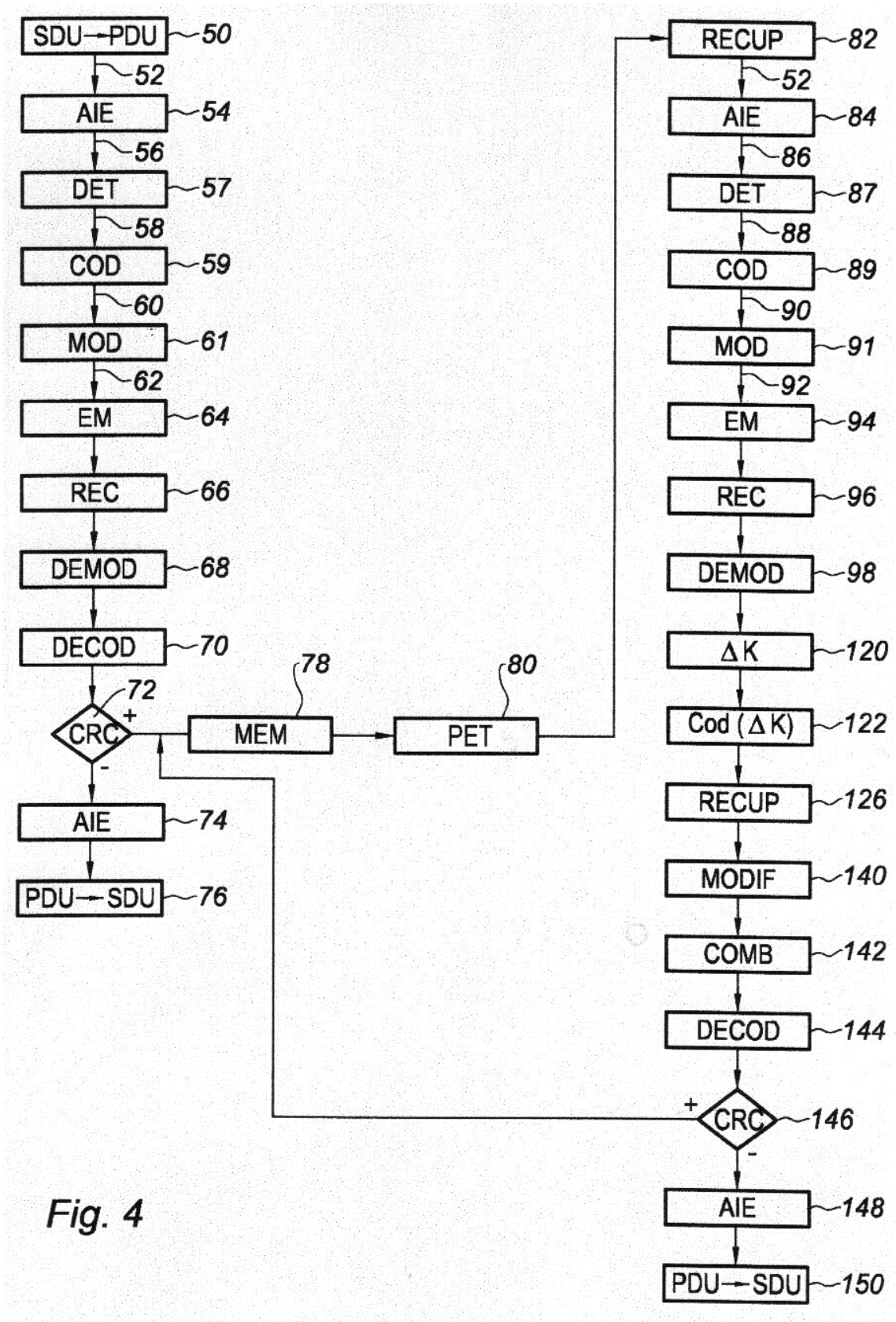
SDU→PDU
50
52
AIE
54
56
DET
57
58
COD
59
60
MOD
61
62
EM
64
REC
66
DEMOD
68
DECOD
70
72
CRC
+
-
78
MEM
80
PET
AIE
74
PDU→SDU
76
RECUP
82
52
AIE
84
86
DET
87
88
COD
89
90
MOD
91
92
EM
94
REC
96
DEMOD
98
ΔK
120
Cod (ΔK)
122
RECUP
126
MODIF
140
COMB
142
DECOD
144
+
CRC
146
-
AIE
148
PDU→SDU
150

Fig. 4

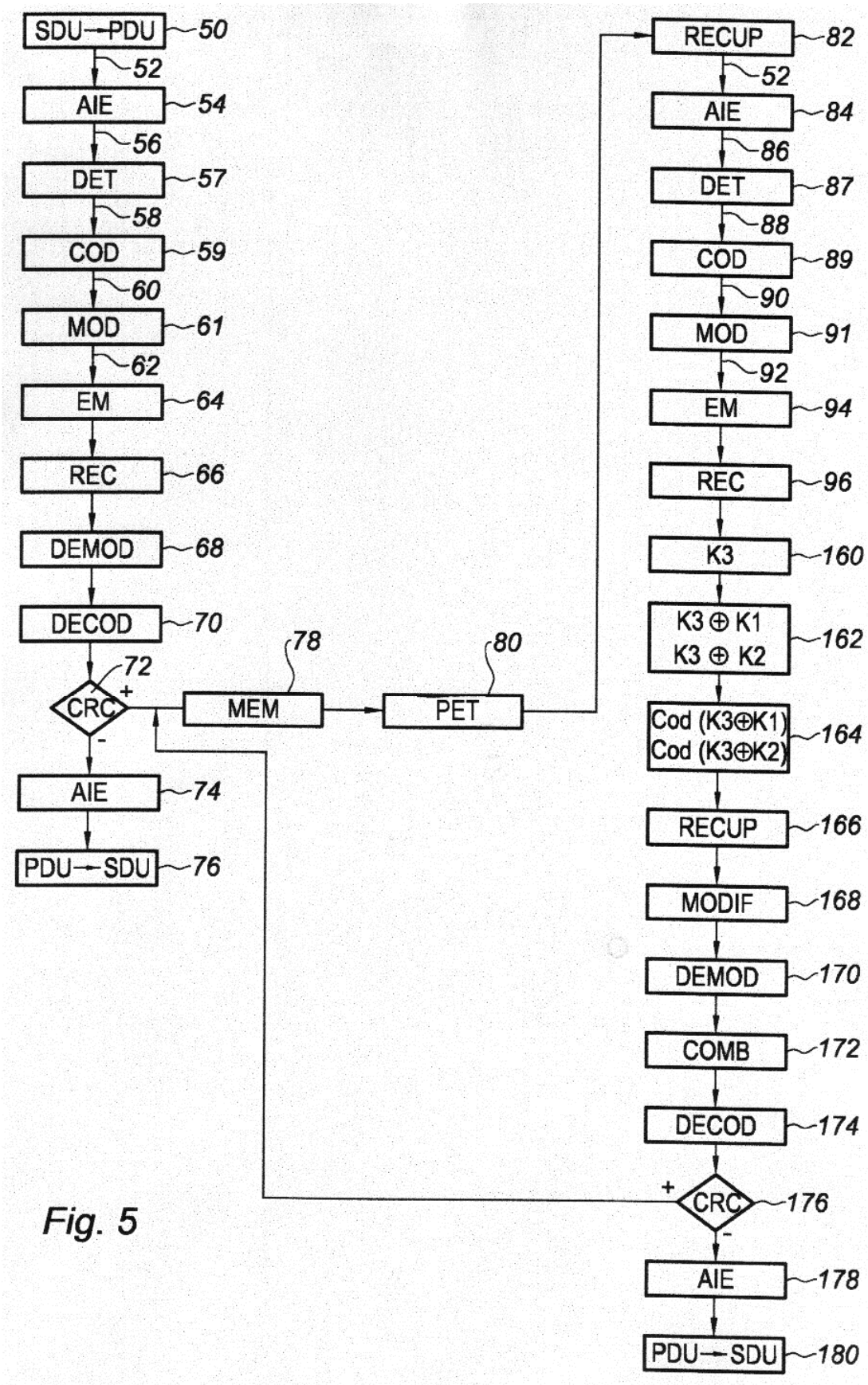
SDU→PDU
50
52
AIE
54
56
DET
57
58
COD
59
60
MOD
61
62
EM
64
REC
66
DEMOD
68
DECOD
70
72
CRC
+
-
78
MEM
80
PET
AIE
74
PDU→SDU
76
RECUP
82
52
AIE
84
86
DET
87
88
COD
89
90
MOD
91
92
EM
94
REC
96
K3
160
K3 ⊕ K1
K3 ⊕ K2
162
Cod (K3⊕K1)
Cod (K3⊕K2)
164
RECUP
166
MODIF
168
DEMOD
170
COMB
172
DECOD
174
+
CRC
176
-
AIE
178
PDU→SDU
180

Fig. 5

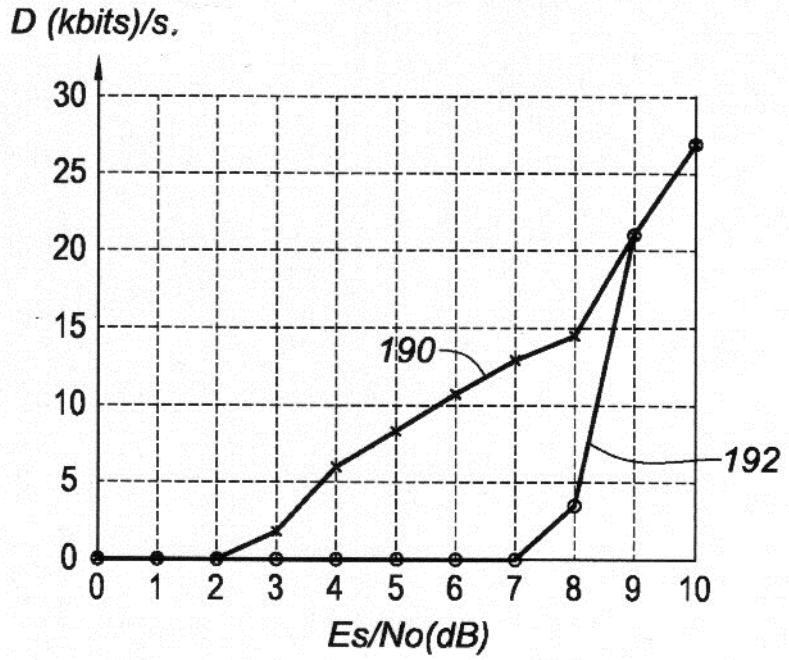

Fig. 6