(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 396 951**

(51) Int. CI.:

H04L 9/14 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.10.2009 E 09821005 (7)**

(97) Fecha y número de publicación de la concesión europea: **05.12.2012 EP 2347540**

(54) Título: **Método y dispositivo para enviar parámetros de cifrado**

(30) Prioridad:

17.10.2008 US 253411

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.03.2013

(73) Titular/es:

MOTOROLA SOLUTIONS, INC. (100.0%)
1303 East Algonquin Road
Schaumburg IL 60196, US

(72) Inventor/es:

CHOWDHARY, DIPENDRA, M.;
BELMONTE, JOHN, P. y
WIATROWSKI, DAVID, G.

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Método y dispositivo para enviar parámetros de cifrado

Campo técnico

El campo técnico se relaciona de manera general con sistemas de comunicación inalámbricos y en particular con el envío de parámetros de cifrado en una supertrama de voz DMR ETSI.

Antecedentes

Durante las últimas décadas, se han generalizado las redes digitales de transceptor de dos vías. Normalmente, los transceptores de dos vías permiten a los usuarios recibir así como también transmitir voz o datos. Para suministrar interoperabilidad entre diversos sistemas de transceptor digitales de dos vías y los vendedores, el Instituto Europeo de Normas de Telecomunicaciones (ETSI por sus siglas en inglés) ha introducido un estándar de interfaz área de Transceptor Móvil Digital (DMR por sus siglas en inglés), que especifica diversos protocolos utilizados por los transceptores de dos vías en la capa de enlace (es decir, Capa 2) del modelo conocido de redes de ordenadores de Interconexión de Sistemas Abiertos de siete capas, y que se describe en ETSI TS (Especificación Técnica) 102 361-1 v1.4.5 (2007-12). La referencia aquí a las normas ETSI DMR incluye la versión actual de la especificación técnica y todas las versiones posteriores y futuras.

Las normas ETSI DMR especifican una estructura de Acceso Múltiple por División de tiempo (TDMA) de dos franjas cuyo dispositivos de transmisión y recepción pueden enviar señales de voz y/o datos. Las señales de voz y/o datos se transmiten en las franjas TDMA de acuerdo con un formato de ráfaga general especificado en la norma. Adicionalmente, las ráfagas que comprenden señales de voz se transmiten en súper-tramas que tienen 360 ms de largo y tienen seis ráfagas que se designan con las entras "A" a "F".

Más aún se pueden enviar mensajes de datos y de voz no cifrados como información plana o pueden ser cifrados, y hacer privado de tal manera que los datos no puedan ser leídos o la voz no pueda ser escuchada en ningún dispositivo diferente a aquel que tienen los parámetros adecuados necesarios para descifrar los mensajes. De acuerdo con lo anterior, el cifrado y descifrado (o privacidad) es una forma de proteger las comunicaciones y mantenerlas privadas cuando se envían los mensajes entre dos dispositivos. Sin embargo, en el contexto de esta descripción, la privacidad no proporciona ningún mecanismo para autenticar los dispositivos o usuarios o proteger la integridad de los mensajes, por ejemplo, asegurar que los mensajes se decodifiquen en el orden adecuado o que todos los mensajes estén actualmente recibidos en el dispositivo de recepción.

El proceso de cifrado comprende de manera general un dispositivo de transmisión que combina ciertos parámetros criptográficos con la información plana para generar información protegida que se envía a un dispositivo de recepción. Para procesos de cifrado que utilizan un algoritmo criptográfico, tal como ARC4, los parámetros criptográficos incluyen normalmente una llave, el algoritmo criptográfico, y un vector de inicialización (IV) para el algoritmo. En consecuencia, con el fin de descifrar adecuadamente la información protegida, el dispositivo de recepción tiene que saber y utilizar la misma llave, algoritmo criptográfico, IV que se utilizó por el dispositivo de transmisión.

Para hacer los parámetros criptográficos conocidos al dispositivo de recepción, el dispositivo de transmisión puede enviar al dispositivo de recepción los parámetros criptográficos propiamente dichos y/o identificadores de cifrado (ID) que identifican uno o más de los parámetros criptográficos. Los parámetros criptográficos y los identificadores de cifrado se denominan colectivamente aquí como parámetros de cifrado. Sin embargo, cuando se refiere a un grupo de parámetros de cifrado, el grupo puede incluir uno o más parámetros criptográficos, solo uno o más identificadores de cifrado, o una combinación de parámetros criptográficos e identificadores de cifrado. Actualmente, no hay un método definido en la normativa DMR para transportar parámetros de cifrado.

Sin embargo, subsiste la necesidad de un método y dispositivo para transmitir parámetros de cifrado que puedan ser implementados en un sistema DMR.

Breve descripción de las figuras

Las Figuras acompañantes, en donde similares numerales de referencia se refieren a elementos funcionalmente similares o idénticos a lo largo de las vistas separadas, que junto con la descripción detallada adelante se incorporan en y forma parte de la especificación y sirven a diversas realizaciones ilustrativas adicionales de los conceptos que incluyen la invención reivindicada, y explican diversos principios y ventajas de aquellas realizaciones.

La FIGURA 1 muestra un diagrama de bloques de un sistema de comunicaciones de acuerdo con una realización de ilustración.

La FIGURA 2 ilustra realizaciones implementadas dentro de un marco de una súper-trama de voz DMR, una ráfaga de voz dentro de la súper-trama, y tramas de vocodificador dentro de la ráfaga de voz.

La FIGURA 3 muestra un diagrama de flujo de un método para transmitir parámetros de cifrado en una súper-trama de voz DMR de acuerdo con una realización de ilustración.

La FIGURA 4 muestra un diagrama de flujo de un método para colocar un IV dentro de una súper-trama de voz DMR de acuerdo con una realización de ilustración.

La FIGURA 5 muestra bits de selección de tramas de vocodificador en una súper-trama de voz DMR y reemplazarlas con bits IV modificados de acuerdo con una realización de ilustración.

La FIGURA 6 muestra un diagrama de flujo de un método para ubicar los identificadores de cifrado en una súper-trama de voz DMR de acuerdo con una realización de ilustración.

La FIGURA 7 muestra una ubicación de los identificadores de cifrado en un campo de señalización incorporado de una ráfaga de voz DMR de acuerdo con una realización de ilustración.

La FIGURA 8 muestra un diagrama de flujo de un método para recibir parámetros de cifrado en una súper-trama de voz DMR de acuerdo con una realización de ilustración.

Los expertos apreciarán que los elementos en las figuras se ilustran por simplicidad de claridad y no necesariamente están trazados a escala. Por ejemplo, las dimensiones de algunos de los elementos en las figuras se pueden exagerar con relación a otros elementos para ayudar a mejorar la comprensión de diversas realizaciones. Adicionalmente, la descripción y los dibujos no necesariamente requieren el orden ilustrado. El dispositivo y los componentes del método se han representado cuando es apropiado mediante símbolos convencionales en los dibujos, que solo muestran aquellos detalles específicos que son pertinentes para comprender las diversas realizaciones con el fin de no oscurecer la descripción con detalles que serán fácilmente evidentes para aquellos medianamente versados en la técnica que tienen el beneficio de la descripción aquí. Sin embargo, se apreciará que por simplicidad y claridad de ilustración, los elementos comunes y bien entendidos que son útiles o necesarios en una realización comercialmente factible no se pueden describir con el fin de facilitar una vista menos obstruida de estas diversas realizaciones.

Descripción detallada

En términos generales, de conformidad con las diversas realizaciones, un dispositivo de transmisión encripta súper-tramas de voz DMR utilizando parámetros criptográficos que, en una realización, incluyen una llave, un algoritmo de cifrado, y un IV y envía unas súper-tramas de voz DMR cifradas a un dispositivo de recepción. Para ayudar al dispositivo de recepción en descifrar las súper-tramas de voz DMR, el dispositivo de transmisión: identifica un número seleccionado de bits a partir de una pluralidad de tramas de vocodificador de una súper-trama de voz DMR; reemplaza cada uno de los bits identificados con un bit correspondiente de un parámetro de cifrado (por ejemplo, un IV o IV modificado); coloca por lo menos un parámetro de cifrado (por ejemplo, un ID de llave y un ID de algoritmo) en un campo de señalización incorporado de la súper-trama de voz DMR; y transmite la súper-trama de voz DMR con parámetros de cifrado al dispositivo de recepción. El dispositivo de recepción: extrae los identificadores de cifrado; extrae un número seleccionado de bits a partir de una pluralidad de tramas de vocodificador de la súper-trama de voz DMR; dispone los bits extraídos para obtener el IV; y utiliza el IV extraído y los identificadores de cifrado para descifrar las súper-tramas de voz DMR.

En una realización, el ID de llave y el ID de algoritmo se envían al campo de señalización incorporado de la ráfaga F de súper-trama de voz DMR y, por lo tanto, no interfiere con la transmisión de ninguna otra información. En una realización adicional, los bits de las tramas de vocodificador que se colocan con el IV (o bits IV modificados) son por lo menos bits significativos para facilitar la distorsión mínima de la señal de voz. Más aún en otra realización, el IV, ID de llave y el ID de algoritmo se envían en todas las súper-tramas de voz DMR para facilitar la entrada posterior de una unidad de suscripción a una llamada de voz dentro de un retardo mínimo. Aquellos expertos en la técnica se darán cuenta que las ventajas reconocidas anteriormente y otras ventajas descritas aquí son solamente de ilustración y no significa que sean una representación completa de todas las ventajas de las diversas realizaciones.

Con referencia ahora a los dibujos, la FIGURA 1 muestra un diagrama de bloques de un sistema de comunicaciones 100 de acuerdo con una realización de ilustración. El sistema de comunicaciones 100 se describe en una forma muy generalizada. Por ejemplo, el sistema 100 se ilustra ya que comprende un dispositivo de infraestructura individual

106 y tres dispositivos de comunicación inalámbricos 102, 104, 108, para facilidad de ilustración. Sin embargo, las enseñanzas aquí se pueden implementar en un sistema que tiene dispositivos de infraestructura adicionales y dispositivos de comunicación inalámbricos.

Cada dispositivo de infraestructura y dispositivo de comunicación inalámbrico está equipado por lo menos con un transceptor (es decir, aparato transmisor y receptor) 110, una memoria 112 y un dispositivo de procesamiento 114 y está adicionalmente equipado con cualesquier componentes adicionales según se necesite para una realización comercial. El transceptor 110, la memoria 112 y el dispositivo de procesamiento 114 pueden tener cualquier implementación física adecuada y son topológicamente acoplado dependiendo de la implementación en el dispositivo particular. Estos componentes se acoplan en forma funcional adicional y se pueden adaptar, disponer, configurar y diseñar para realizar métodos de acuerdo con las enseñanzas aquí, por ejemplo, como se describe ilustrativamente con referencia a las figuras 2 a 8 restantes.

Como se refiere aquí, un dispositivo de comunicación inalámbrico incluye, pero no se limita a, dispositivos referidos comúnmente como terminales de acceso, radios móviles, estaciones móviles, unidades de suscriptor, equipo de usuario, dispositivos móviles, o cualquier otro dispositivo capaz de operar en un ambiente inalámbrico. Ejemplos de dispositivos de comunicación inalámbricos incluyen, pero no se limitan a, transceptores de dos vías, teléfonos móviles, teléfonos celulares, Asistentes Personales Digitales (PDA), computadores portátiles y busca personas de dos vías. Como se utiliza aquí, un dispositivo de infraestructura es un dispositivo que hacer parte de una infraestructura de red fija y puede recibir información (ya sea de control o medio, por ejemplo, datos, voz (audio), video, etc.) en una señal desde un dispositivo de comunicación inalámbrico y transmite la información en señales a uno o más dispositivos de comunicación inalámbricos a través de una conexión de comunicación. Un dispositivo de infraestructura incluye, pero no se limita a, equipo referido comúnmente como repetidoras, transceptores base, estaciones base, estaciones de transceptor base, puntos de acceso, enrutadores o cualesquier otro tipo de equipo de infraestructura que están en interfaz con un dispositivo de comunicación inalámbrico en un ambiente inalámbrico.

En esta realización de ilustración, el sistema 100 es un sistema DMR, y el dispositivo de infraestructura 106 y los dispositivos de comunicación inalámbricos 102, 104, y 108 se comunican utilizando la interfaz aérea como se especifica en la norma DMR (tal como, el dispositivo 106 se refiere en adelante como una estación base (o BS), y dispositivos 102, 104, y 108 se refieren adelante como estaciones móviles o (MS)). De acuerdo con la norma DMR, los MS pueden comunicarse en "modo directo" o "modo de comunicación directa", en donde el MS se comunica directamente con cada uno al exterior del control de un BS. Los MS 102 y 104 se ilustran en la FIGURA 1 como comunicación en modo directo. Los MS también pueden comunicarse en "modo repetido", en donde el MS se comunica a través de una BS. El MS 102 y 108 se ilustra en la FIGURA 1 como comunicación en modo repetidor utilizando el BS 106. Las transmisiones desde una BS a un MS en un modo repetidor se denominan transmisiones salientes, y transmisiones desde un MS a un BS en modo repetidor se denominan transmisiones entrantes.

Como se mencionó anteriormente, los dispositivos en el sistema 100 se comunican utilizando conexiones de comunicación (también denominadas aquí como canales). Los canales comprenden canales físicos y canales lógicos. Los canales físicos son los recursos de comunicación físicos sobre los cuales se envía información entre los elementos dentro del sistema 100. Los canales físicos pueden comprender conexiones cableadas o conexiones inalámbricas. Si los canales físicos comprenden conexiones cableadas, el recurso físico correspondiente es una asignación de espectro de radio que se divide en portadores de frecuencias de radio (RF) como cada portador RF se particiona en tiempo en tramas y franjas de tiempo. Las franjas para los dos canales físicos TDMA se etiquetan canal "1" y canal "2". Una ráfaga DMR es un periodo de portador RF que se modula por una corriente media y representa el canal físico de una franja temporal simple. La ráfaga es la unidad independiente más pequeña de transmisión TDMA definida en la norma DMR.

Se requiere que un canal físico soporte un canal lógico, que es una ruta de comunicación lógica entre dos o más partes. Los canales lógicos se separan en dos categorías: canales de tráfico que llevan información de voz o datos; y canales de control que llevan señalización, que está relacionada específicamente con el establecimiento y control de enlaces, y con el manejo en el sistema 100. La señalización a partir del objetivo a una fuente se denomina aquí como señalización de Canal Inverso (RC). Detalles de realizaciones de ilustración se describirán con referencia a las figuras 2 a 8.

La FIGURA 2 ilustra realizaciones implementadas dentro de un marco de una súper-trama de voz DMR, una ráfaga de voz dentro de la súper-trama de voz DMR, y tramas de vocodificador dentro de la ráfaga de voz. Se ilustra un diagrama de temporización para una súper-trama de voz DMR en 200. La súper-trama de voz DMR se envía mediante una transmisión MS a un MS de recepción y se puede enviar en modo directo o en modo repetidor. La súper-trama de voz DMR se envía en uno de los dos canales y comprende seis ráfagas 204, etiquetadas "A" a "F", es decir, 204-A, 204-B, 204-C, 204-D, 204-E, y 204-F. El otro canal que comprende el bloque 206 se puede utilizar o puede estar en uso por otros dispositivos en el sistema 100.

Ilustrado mediante la referencia a 210 hay una de las ráfagas 204 de la súper-trama de voz DMR. La estructura de ráfaga genérica incluye dos campos de datos útiles de bits de voz 108, 212 y 214 y un campo de 48-bits 208 en el centro de la ráfaga denominado aquí como el campo de “señalización incorporada”. El campo de señalización incorporado 208 lleva la señalización sincronizada o incorporada dependiendo de la ráfaga particular dentro de la súper-trama de voz DMR. La ráfaga definida toma 27.5 ms para transmitir y puede estar seguido por 2.5 ms de tiempo de protección o un Canal de Anunció Común (CACH). Sin embargo, una ráfaga tiene 30 ms; una trama de dos franjas temporales contiguas denominadas como 1 y 2, tiene 60 ms; y una súper-trama de voz DMR tiene 360 ms (debido a la temporización para el otro canal).

En una realización, la Ráfaga A, que marca el inicio de la súper-trama de voz DMR, contiene sincronización (por ejemplo en la forma de patrones de sincronización conocidos) en el campo 208. Las ráfagas B a F pueden contener señalización incorporada tal como Control de Enlace (que incluye, pero no se limita a, direcciones de destino y origen, tipo de mensaje, longitud), señalización RC, etc., en el campo 208, y en algunos campos de escenarios de implementación 208 en por lo menos una de las ráfagas B a F que puede estar vacía (nula) o tener algunos bits no utilizados.

Como se sabe bien en el procesamiento de voz, se utiliza un vocodificador mediante un dispositivo de transmisión para codificar voz digitalizada con propósitos de aplicar corrección de error de reenvío (FEC), compresión, cifrado, intercalado, etc. En una realización, el dispositivo de transmisión comprende un vocodificador de 3600 bps que produce marcos de 72-bits (que incluyen FEC) cada 20 ms. Sin embargo, la ráfaga de voz 204 lleva tres tramas de vocodificador de 72- bits (que incluyen FEC) 222, 224, y 226 más el campo de señalización incorporado de 48-bits como se ilustra en 220. Las Figuras 3-8 ilustran realizaciones, en donde un dispositivo de transmisión envía parámetros de cifrado (en este caso el IV, ID de llave, y el ID de algoritmo) en el campo de señalización incorporado y en las tramas de vocodificador, que contienen bits de voz cifrados. Sin embargo, antes de describir realizaciones de transporte de los parámetros de cifrado, adelante se proporciona un breve resume de cómo se obtienen los parámetros de cifrado y, en general, como se utilizan en un proceso de cifrado y descifrado de ilustración.

En una realización, el dispositivo de transmisión utiliza los parámetros criptográficos de una llave, un algoritmo criptográfico, y un IV para inicializar el algoritmo criptográfico. La llave y el algoritmo criptográfico se pueden seleccionar de una de varias llaves y algoritmos almacenados en y utilizados comúnmente por ambos dispositivos de transmisión y recepción. En un ejemplo de ilustración, la llave seleccionada tiene 40 bits de largo y se identifica exclusivamente por un ID de llave, y el algoritmo (por ejemplo, ARC4 como se conoce bien en la técnica) es uno que requiere un IV y se identifica por un único ID de algoritmo. Más aún, se pueden utilizar diferentes llaves y algoritmos para cifrar mensajes de voz versus mensajes de datos.

El IV es un bloque de bits que se utiliza como una semilla para el algoritmo para producir una corriente de llaves únicas independiente de otras corrientes de llaves producidas por la misma llave. En este ejemplo de ilustración, el dispositivo de transmisión genera un IV largo de 32 bits, que se inicializa mediante un número aleatorio que es diferente para cada inicialización y para cada MS. La inicialización se puede hacer luego de encendido o al inicio de una llamada de voz de datos. Más aún, para proporcionar protección criptográfica robusta, se genera una corriente de llave diferente para cada unidad de datos de paquete (PDU) de DMR y para cada súper-trama de voz DMR. Por ejemplo, el IV se puede actualizar al aplicar un Registro de Cambio de Retroalimentación Lineal (LFSR) en el IV anterior. Sin embargo, en otras realizaciones, el mismo IV se puede utilizar para generar la corriente de llave para un número de súper-tramas de voz DMR (o PDU) o una vez para cada llamada, pero estos métodos proporcionan menos protección criptográfica. Cabe entender que, la longitud en forma de bits IV y de llave y el algoritmo particular suministrado aquí se verá únicamente como ejemplos y no significa que limiten el alcance de las enseñanzas expuestas aquí. De acuerdo con lo anterior, cualquier llave adecuada, algoritmo, IV, u otro parámetro de cifrado relevante se puede utilizar dependiendo de la metodología de cifrado particular implementada.

Volviendo a la descripción de los procesos se cifrado de ilustración, para proteger la información plana, los dispositivos transmisores seleccionan una llave y concatenan la llave con el IV para utilizar en inicialización del algoritmo criptográfico, que se utiliza para generar una corriente de llave bit a bit en la salida del algoritmo. La corriente de llave se combina con la información plana utilizando un operador OR exclusivo lógico (es decir, XOR) para generar información protegida, que se envía a un dispositivo de recepción. Para descifrar la información protegida, el dispositivo de recepción tiene que generar la misma corriente de llave como se generó en el dispositivo de transmisión, y el XOR la corriente de llave con la información protegida para obtener la información plana que se puede leer o escuchar por parte de un usuario del dispositivo de recepción. Sin embargo, con el fin de generar la misma corriente de llave, el dispositivo de recepción tiene que utilizar llave, algoritmo criptográfico, e IV como se utilizó en el dispositivo de transmisión. Las restantes figuras 3-8 proporcionan una realización de ilustración para un dispositivo de transmisión para transportar parámetros de cifrado a un dispositivo de recepción en una súper-trama de voz DMR y para el dispositivo de recepción para extraer aquellos parámetros de cifrado para utilizar en el proceso de descifrado.

Volviendo ahora a la FIGURA 3 en la que se muestra un diagrama de flujo de un método 300 para transmitir parámetros de cifrado en una súper-trama de voz DMR de acuerdo con una realización de ilustración. En general, los parámetros de cifrado se transportan en una súper-trama de voz DMR dentro de un campo de señalización incorporado y al reemplazar los bits de trama de vocodificador con bits de uno o más de los parámetros de cifrado.

Más particularmente, en 302, el dispositivo de transmisión identifica un número seleccionado de bits a partir de una pluralidad de tramas de vocodificador. Cualesquier bits se pueden identificar y reemplazar. Sin embargo, identificar y reemplazar solo por lo menos los bits significativos es ventajoso porque este tiene el último efecto en, o en otras palabras provoca mínima distorsión de, el audio escuchado en el dispositivo de recepción. Como se utiliza aquí, la frase “bits menos significativos” son aquellos bits de vocodificador que tienen por lo menos impacto notable en la calidad de audio independiente del orden de los bits. Sin embargo, como se utiliza en este sentido, los bits menos significativos no solo se refieren simplemente a los bits que tienen la numeración de bits más baja de acuerdo con cómo se enumeran todos los bits del vocodificador.

El dispositivo de transmisión reemplaza (304) por lo menos algunos de los bits identificados con los bits correspondientes de por lo menos un parámetro de cifrado. En las realizaciones descritas adelante con referencia a las figuras 4 y 5, los bits identificados se reemplazan con bits correspondientes del IV y, más particularmente, cada uno de los bits identificados se reemplaza con bits correspondientes de un IV modificado, que se combinan con bits se control de error (es decir bits de paridad de detección de error y/o bits de paridad de detección de error de reenvío). Sin embargo, en otra realización, los bits identificados se pueden reemplazar con bits correspondientes de un IV truncado o acortado. En la otra realización, los bits de trama de vocodificador identificados se pueden reemplazar con bits de otros parámetros de cifrado tal como la llave, ID de llave, el ID de algoritmo, etc., en adición a o alternativamente al IV o IV modificado.

El dispositivo de transmisión, en 306, también coloca uno o más parámetros de cifrado en un campo de señalización incorporado en la súper-trama de voz DMR. Cualesquier parámetros de cifrado (o parte de los mismos) se pueden reemplazar en uno o más campos de señalización incorporados de cualesquier ráfagas de voz. Sin embargo, con el fin de no interferir con la transmisión de otra información y señalización en la súper-trama de voz DMR, los parámetros de cifrado de menor tamaño tal como los identificadores de cifrado (por ejemplo, el ID de llave y el ID de algoritmo) se ponen en un campo de señalización incorporado en una ráfaga que tiene bits que se están utilizando de otra forma con otra información o señalización, tal como la ráfaga F. Una realización de ilustración para colocar parámetros de cifrado dentro de un campo de señalización incorporado se describe mediante referencia a las figuras 6 y 7. El dispositivo de transmisión luego transmite (308) la súper-trama de voz DMR con los parámetros de cifrado a uno o más dispositivos de recepción.

Volviendo ahora a la FIGURA 4, que muestra allí un diagrama de flujo de un método para colocar un IV modificado dentro de una súper-trama de voz DMR de acuerdo con una realización de ilustración. La FIGURA 4 se describirá en conjunto con la FIGURA 5 para mostrar un ejemplo específico de cada uno de los bits de trama de vocodificador seleccionado que se reemplaza mediante los bits correspondientes del IV modificado. Luego de generar un IV (502), el dispositivo de transmisión calcula (402) los bits se paridad de detección de error sobre el IV, que se concatenan (404) con el IV para generar un IV concatenado. Se puede utilizar cualesquier técnicas de detección para generar los bits se paridad de detección de error (que incluyen, pero no se limitan a, funciones hash, paridad simple, Checksum, etc. Sin embargo, en la realización ilustrada con referencia a la FIGURA 5, el dispositivo de transmisión calcula una revisión del revisor de redundancia cíclica (CRC) sobre el IV para generar los bits se paridad de detección de error 504 que se unen al IV 502. En un ejemplo de ilustración, el CRC se calcula utilizando aritmética polinomial utilizando un generador CRC polinomial, tal como $x^4 + x + 1$, para generar un CRC de 4 bist, pero se puede utilizar cualquier otro método adecuado para calcular el CRC.

En 406, el dispositivo de transmisión adjunta los bits de paridad de corrección de error al IV concatenado para generar el IV modificado utilizando cualesquier técnicas de corrección de error adecuadas que incluyen, pero no se limitan a, uso de técnicas de Repetición de Solicitud Automáticas (ARQ), un código Hamming, un código Golay, un código Reed-Solomon, por mencionar unos pocos. En la realización ilustrada con referencia a la FIGURA 5, el dispositivo de transmisión divide el IV concatenado de 36 bits en tres segmentos y aplica un código Golay extendido (24, 12, 8) al IV concatenado, para adjuntar 36 bits se paridad de corrección de error de reenvío (FEC) y, por lo tanto generar 72 bits de IV modificado 506. Se pueden generar más o menos 72 bits si se utiliza una técnica de corrección de error diferente. El dispositivo de transmisión divide el IV modificado en tres segmentos iguales 508, 510, y 512 de 24 bits que se van a transportar e tramas de vocodificador de la súper-trama de voz DMR. Como se muestra en la FIGURA 5, el segmento 508 comprende bits 0 a 23; el segmento 510 comprende bits 24 a 47; el segmento 512 comprende bits 48 a 71. Dividir el IV modificado en segmentos iguales de 24-bits no es necesario para implementar las enseñanzas mostradas aquí. El IV modificado no necesita dividirse para nada o se puede dividir en un número de segmentos diferentes que tengan un número igual o diferente de bits.

El dispositivo de transmisión identifica (408) un número seleccionado de bits de las tramas de vocodificador y reemplaza estos bits con los 72 bits de IV modificado. En una realización de ilustración, el dispositivo de transmisión

identifica cuatros bits menos significativos de cada uno de las tres tramas de vocodificador (VF1, VF2, VF3) en cada una de las seis ráfagas (204-A a 204-F) de la súper-trama DMR mostrada en la FIGURA 2 e intercala (410) los bits IV modificados en las posiciones de los bits de trama de vocodificador identificados. En caso de que el IV modificado sea mayor o menor de 72 bits, se pueden identificar más o menos bits de las tramas de vocodificador para transportar el IV. Utilizando ciertos vocodificadores de 3600 bps, se pueden seleccionar hasta 6 bits de las tramas de vocodificador con distorsión mínima para la señal de voz transmitida.

Los bits de cada uno de los segmentos del IV 508, 510, 512 se pueden colocar secuencialmente en las posiciones de los bits se vocodificador identificados. Sin embargo, en este ejemplo de ilustración, el IV modificado se intercala en las posiciones de bits se marcó de vocodificador con el fin de disponer los bits de IV en una forma no contigua para proteger el IV contra errores de ráfaga durante la transmisión. Los bits IV modificados se pueden intercalar bit a bit, pero en este ejemplo, se intercalan pequeños bloques de bits (por ejemplo, 4 bloques de bits en cada caso) en las posiciones de bloque de tamaño igual de los bits se marcó de vocodificador identificados. Por ejemplo, el bloque 514 del segmento 508 se coloca en la trama de vocodificador (VF3) de la ráfaga 204-F. El bloque 516 del segmento 510 se coloca en la trama de vocodificador (VF2) de la ráfaga 204-F; y el bloque 518 del segmento 512 se coloca en el vocodificador (VF1) de la ráfaga 204-F. De forma similar, el siguiente bloque de 4 bits de cada segmento 508, 510, 512 se pone en las tramas de vocodificador VF3, VF2 y VF1 de la ráfaga 204-E, y etc.

Como se mencionó anteriormente en las figuras 6 y 7 suministradas para un ejemplo de ilustración para colocar parámetros de cifrado (en este caso un ID de llave 702 y un ID de algoritmo 704) en la súper-trama de voz DMR. En una realización, el ID de llave tiene 8 bits de largo, y el ID de algoritmo tiene 3 bits de largo, aunque puede variar la longitud de los identificadores de cifrado. Más particularmente, de acuerdo con un método 600, el dispositivo de transmisión genera bits de paridad de corrección de error (602) sobre uno o más de los identificadores de cifrado y concatena (604) los bits de paridad de corrección de error con los identificadores de cifrado. Como se ilustra en la FIGURA 7, se generan 21 bits de paridad FEC 706 se generan sobre el ID de llave 702 y el ID de algoritmo 704 y luego se adjuntan al ID de algoritmo y de llave. Los bits de paridad de corrección de error se pueden generar utilizando cualesquier técnicas de corrección de error adecuadas que incluyen cualquier de aquellos métodos mencionados para generar por lo tanto el mismo número, más o menos bits de paridad de corrección de error, o los bits de paridad de corrección de error se pueden calcular solo sobre el ID de llave o el ID de algoritmo. Más aún en otra realización, el dispositivo de transmisión puede calcular bits de paridad de detección de error (por ejemplo, utilizando CRC, Checksum, paridad simple, etc.) sobre uno o más de los identificadores de cifrado antes de generar los bits de paridad de corrección de error o en lugar de generar los bits de paridad de corrección de error.

En esta implementación de ilustración, el dispositivo de transmisión coloca (606) el ID de llave 702, el ID de algoritmo 704 y concatena los bits de paridad FEC 706 en el campo de señalización incorporado 208-F de la ráfaga F 204-F de la súper-trama de voz DMR mostrada en la FIGURA 2. Como se mencionó anteriormente, colocar los parámetros de cifrado en la ráfaga F es ventajoso porque, actualmente, el campo de señalización incorporado es nulo. Sin embargo, los parámetros de cifrado se pueden colocar en el campo de señalización incorporado de una cualquiera o más de las ráfagas de la súper-trama de voz DMR. Más aún, el dispositivo de transmisión se puede poner en los parámetros de cifrado en un campo de señalización incorporado sencillo a lo largo de la llamada de voz completa (que comprende una pluralidad de súper-tramas de voz DMR) o coloca periódicamente los parámetros de cifrado en diversos campos de señalización incorporados durante la llamada. Sin embargo, para facilitar mejor la entrada posterior ha sido enviado un dispositivo de recepción para una llamada de parámetros de cifrado, es adicionalmente ventajoso para el dispositivo de transmisión colocar los parámetros de cifrado en cada súper-trama de voz DMR de la llamada.

La FIGURA 8 muestra un diagrama de flujo de un método 800 para recibir parámetros de cifrado en una súper-trama de voz DMR de acuerdo con una realización de ilustración. Luego de recibir las transmisiones de voz (802) desde un dispositivo de transmisión, un dispositivo de recepción detecta que se cifran las transmisiones. Por ejemplo, en una realización el dispositivo de recepción detecta que se fija un bit se privacidad en un encabezado de Control de Enlace de Voz (LC), que indica que el dispositivo de recepción necesita extraer los parámetros de cifrado con el fin de descifrar las transmisiones de voz. Adicionalmente, o alternativamente, se puede fijar un bit en la señalización LC incorporada durante la transmisión de voz y/o en un Terminador con LC en un extremo de la transmisión de voz para indicar al dispositivo de recepción que extraiga los parámetros de cifrado desde las súper-tramas de voz DMR. También se pueden implementar otros métodos para indicar al dispositivo de recepción que extraiga los parámetros de cifrado sin apartarse del alcance de las enseñanzas expuestas.

De acuerdo con lo anterior, el dispositivo de recepción extrae (804) por lo menos un parámetro de cifrado de un campo de señalización incorporado de la súper-trama de voz DMR 200. En este caso, el dispositivo de recepción extrae el ID de llave 702 y el ID de algoritmo 704 del campo de señalización incorporado de la ráfaga F y aplica los bits FEC 706 a estos identificadores de cifrado para corregir cualesquier errores, si están presentes. El dispositivo de recepción también extrae y los bits de desintercalado (806) desde las tramas de vocodificador de la súper-trama de voz DMR para obtener el IV.

Más particularmente, el dispositivo de recepción retira los cuatros bits menos significativos (bloques de cuatro bits) de cada uno de las 18 tramas de vocodificador en las súper-tramas de voz DMR y desintercala los cuatro bloques de bits para obtener el IV modificado de 72 bits, que incluye los bits de paridad FEC. En una implementación diferente, se puede retirar un subconjunto de cuatro bloques de bits de las tramas de vocodificador para obtener el IV. Se aplica FEC sobre el IV protegido contra error para obtener el IV de 32 bits y cuatro bits CRC. Luego de verificar el CRC de 4 bits, el dispositivo de recepción selecciona la llave apropiada como se identifica por el ID de llave y el algoritmo adecuado como se identifica mediante el ID de algoritmo.

En este caso, el algoritmo es ARC4, que utiliza la llave concatenada con el IV para generar la misma corriente de llave como se genera en el dispositivo de transmisión. Para obtener la carga de datos de voz plana de la súper-trama de voz DMR, el dispositivo de recepción hace XOR la parte cifrada de los datos útiles con la corriente de llave. El método 800 se puede realizar para cada súper-trama de voz DMR, o una vez se obtienen los parámetros de cifrado en una súper-trama de voz DMR particular, se pueden utilizar para descifrar la súper-trama DMR. Para cada súper-trama de voz DMR posterior, el dispositivo de recepción puede simplemente actualizar el IV utilizando el LFSR del IV anterior para descifrar la súper-trama de voz DMR posterior.

En la anterior especificación, se han descrito realizaciones específicas. Sin embargo, un experto en la técnica aprecia que se pueden hacer diversas modificaciones y cambios sin apartarse del alcance de la invención como se establece en las reivindicaciones adelante. De acuerdo con lo anterior, la especificación y las figuras se relacionan en forma ilustrativa a diferencia de restrictiva, y todas dichas modificaciones pretenden estar incluidas dentro del alcance de las actuales enseñanzas. Los beneficios, ventajas, soluciones a los problemas, y cualesquier elementos que puedan provocar cualquier beneficio, ventaja, o solución que ocurra o llegue a ser más pronunciada no se constituye como características o elementos críticos, requeridos, o esenciales de cualesquier de todas las reivindicaciones. La invención se defina únicamente por las reivindicaciones adjuntas que incluyen cualesquier modificaciones hechas durante la vigencia de esta solicitud y todos los equivalentes de aquellas reivindicaciones como se publicaron.

Más aún en este documento, los términos relativos tales como primero y segundo, superior e inferior, y similares se pueden utilizar únicamente para distinguir una entidad o acción de otra entidad o acción sin requerir necesariamente o implicar cualquier dicha relación u orden entre dichas entidades o acciones. Los términos “comprende”, “que comprende”, “tiene”, “que tiene”, “incluye”, “que incluye”, “contiene”, “que contiene”, o cualesquier otras variaciones de las mismas, se pretende que cubran una inclusión no exclusiva, de tal manera que un proceso, método, artículo, o aparato que comprenda, tenga, incluya, contenga una lista de elementos no incluya solo aquellos elementos sino que puede incluir otros elementos no enumerados expresamente o inherentes a dichos procesos, métodos, artículos, o aparatos. Un elemento precedido por “comprende…un”, “tiene… un”, “incluye…un”, “contiene…un”, sin más restricciones, no se opone a la existencia de elementos idénticos adicionales en el proceso, método, artículo, o aparato que comprende, tiene, incluye, contiene el elemento. Los términos “un” y “uno” se definen como uno o más indicados explícitamente de otra forma aquí. Los términos “sustancialmente”, “esencialmente”, “aproximadamente”, “aproximado” o cualesquier otras versiones de las mismas, se definen por estar cerca como lo entiende una persona mediamente versada en la técnica, y en una realización no limitante el término se define que está dentro de 10 %, en otra realización dentro de 5 %, en otra realización dentro de 1 % y en otra realización dentro de 0.5 %. El término "acoplado" como se utiliza aquí se define como conectado, aunque no necesariamente directamente y no necesariamente mecánicamente. Un dispositivo o estructura que está “configurado” en cierta forma se configura en por lo menos eso forma, pero también se puede configurar en formas que no están enumeradas.

Se apreciará que algunas realizaciones pueden estar comprendidas de uno o más procesadores genéricos o especializados (o "dispositivos de procesamiento") tal como microprocesadores, procesadores de señales digitales, procesadores personalizados y matrices de portal programables de campo (FPGA) y instrucciones únicas de programas almacenados (que incluyen software y firmware) que controlan uno o más procesadores para implementar, en conjunto con ciertos circuitos no procesadores, algunos, la mayoría, o todas las funciones del método y aparato para enviar parámetros de cifrado descritos aquí. Los circuitos no procesadores pueden incluir, pero no se limitan a, un receptor de radio, un transmisor de radio, controladores de señal, circuitos de reloj, circuitos de fuentes de potencia, y dispositivos de entrada de usuario. Como tal, estas funciones se pueden interpretar como etapas de un método para realizar el envío de parámetros de cifrado descritos aquí. Alternativamente, algunas o todas las funciones se pueden implementar mediante una máquina de estado que no ha almacenado instrucciones de programa, o en uno o más circuitos integrados específicos de aplicación (ASIC), en los que cada función o algunas combinaciones de ciertas de las funciones se implementan como lógica habitual. Por supuesto, se puede utilizar una combinación de los dos métodos, la máquina de estado y el ASIC se consideran aquí como un "dispositivo de procesamiento" para propósitos de la anterior discusión y el lenguaje de las reivindicaciones.

Más aún, se puede implementar una realización como elemento de almacenamiento legible por ordenador o medio que tiene código legible por ordenador almacenado allí para programar un ordenador (por ejemplo, que comprende un dispositivo de procesamiento) para realizar un método como se describe y reivindica aquí. Ejemplos de dichos elementos de almacenamiento legibles por ordenador incluyen, pero no se limitan a, un disco duro, un CD-ROM, un

dispositivo de almacenamiento óptico, un dispositivo de almacenamiento magnético, un ROM (Memoria de Solo Lectura), un PROM (Memoria de Solo Lectura Programable), un EPROM (Memoria de Solo Lectura Programable Borrable), un EEPROM (Memoria de Solo Lectura Programable Borrable Eléctricamente) y una memoria Flash. Adicionalmente, se espera que un experto en la técnica, no obstante un esfuerzo posiblemente significativo y muchas elecciones de diseño motivadas por, por ejemplo, tiempo disponible, tecnología actual, y consideraciones económicas, cuando son guiadas por conceptos y principios descritos aquí serán fácilmente capaces de exonerar dichas instrucciones de software y programas e IC con mínima experimentación.

El Resumen de la Descripción se proporciona para permitir al lector discernir rápidamente la naturaleza de la descripción técnica. Se presenta con el entendimiento de que no se utilizará para interpretar o limitar el alcance o significado de las reivindicaciones. Adicionalmente, en la anterior descripción detallada, se puede ver que se agrupan diversas características en varias realizaciones con el propósito de destacar la descripción. Este método de descripción no se interpreta que refleja una intención de que las realizaciones reivindicadas requieren más características de las que se mencionan expresamente en cada reivindicación. Por el contrario, como las siguientes reivindicaciones reflejan, la materia objeto de la invención se basa en menos de todas las características de una única realización descrita. Así las siguientes reivindicaciones se incorporan aquí en la descripción detallada, cada reivindicación tiene por sí misma una materia objeto reivindicada en forma separada.

REIVINDICACIONES

1. Un método (300) para enviar parámetros de cifrado en una súper-trama de voz de Radio Móvil Digital (DMR) del Instituto Europeo de Normas de Telecomunicaciones, el método comprende:

identificar (302) un número seleccionado de bits a partir de una pluralidad de tramas de vocodificador de la súper-trama de voz DMR;

reemplazar (304) por lo menos algunos de los bits identificados con un bit correspondiente de un primer parámetro de cifrado;

colocar (306) por lo menos a segundo parámetro de cifrado en un campo de señalización incorporado de la súper-trama de voz DMR; y

transmitir (308) la súper-trama de voz DMR, que incluye los parámetros de cifrado.

2. El método de la reivindicación 1, en donde:

el primer parámetro de cifrado comprende un vector de inicialización (IV).

3. El método de la reivindicación 2, en donde reemplazar (304) por lo menos algunos de los bits identificados con un bit correspondiente del vector de inicialización comprende:

generar (406) un vector de inicialización modificado al combinar el vector de inicialización con por lo menos uno de los bits de paridad de detección de error o reenviar los bits de paridad de corrección de error; y

reemplazar (410) cada uno de los bits identificados con un bit correspondiente del vector de inicialización modificado.

4. El método de la reivindicación 3, en donde generar el vector de inicialización modificado comprende:

calcular (504) la Revisión de Redundancia Cíclica (CRC) para el vector de inicialización;

concatenar (404) la Revisión de Redundancia Cíclica con el vector de inicialización para generar un vector de inicialización concatenado;

agregar (406) bits de paridad de corrección reenviado (FEC) al vector de inicialización concatenado para generar el vector de inicialización modificado.

5. El método de las reivindicaciones 2 a 4, en donde:

reemplazar (304) cada uno de los bits identificados comprende intercalar los bits del vector de inicialización en las posiciones de los bits identificados.

6. El método de cualquier reivindicación anterior, en donde:

colocar (306) por lo menos un segundo parámetro de cifrado en el campo de señalización incorporado comprende posicionar por lo menos un identificador de cifrado en el campo de señalización incorporado de la Ráfaga F de la súper-trama de voz DMR.

7. El método de cualquier reivindicación anterior, en donde por lo menos un segundo parámetro de cifrado comprende por lo menos uno de:

un Identificador de llave de cifrado;

un Identificador de algoritmo de cifrado;

el Identificador de llave de cifrado combinado con bits de control de error;

el Identificador de algoritmo de cifrado combinado con bits de control de error; o

el Identificador de llave de cifrado y el Identificador de algoritmo de cifrado combinado con bits de control de error.

8. Un método (800) para recibir parámetros de cifrado en una súper-trama de voz de Radio Móvil Digital (DMR) del Instituto Europeo de Normas de Telecomunicaciones, el método comprende:

recibir (802) la súper-trama de voz DMR;

extraer (804) un primer parámetro de cifrado de un campo de señalización incorporado de la súper-trama de voz DMR recibida;

extraer (806) un número seleccionado de bits a partir de una pluralidad de tramas de vocodificador de la súper-trama de voz DMR; y

disponer los bits extraídos para obtener un segundo parámetro de cifrado.

9. El método de la reivindicación 8, en donde:

el primer parámetro de cifrado se extrae del campo de señalización incorporado de la Ráfaga F de la súper-trama de voz DMR.

10. El método de la reivindicación 8 o reivindicación 9, en donde el primer parámetro de cifrado comprende por lo menos uno de:

un Identificador de llave de cifrado;

un Identificador de algoritmo de cifrado;

el Identificador de llave de cifrado combinado con bits de control de error;

el Identificador de algoritmo de cifrado combinado con bits de control de error; o

el Identificador de llave de cifrado y el Identificador de algoritmo de cifrado combinado con bits de control de error.

11. El método de la reivindicación 10, que comprende adicionalmente:

Descifrar la súper-trama DMR recibida utilizando la llave seleccionada con base en el ID de llave y una algoritmo de cifrado seleccionado con base en el ID de algoritmo.

12. El método de las reivindicaciones 1 u 8, en donde:

El número de bits seleccionado de la pluralidad de tramas de vocodificador comprende un número seleccionado de bits menos significativos.

13. El método de la reivindicación 12, en donde:

El número seleccionado de bits menos significativos comprende cuatro bits menos significativos extraídos de cada una de la pluralidad de tramas de vocodificador de la súper-trama de voz DMR.

14. El método de cualquiera de las reivindicaciones 8-11, en donde:

el segundo parámetro de cifrado comprende un vector de inicialización, y en donde el método comprende adicionalmente descifrar la súper-trama DMR recibida utilizando el vector de inicialización.

15. Un dispositivo para enviar parámetros de cifrado en una súper-trama de voz de Radio Móvil Digital (DMR) del Instituto Europeo de Normas de Telecomunicaciones, el dispositivo comprende:

un dispositivo de procesamiento (114) para:

identificar un número seleccionado de bits a partir de una pluralidad de tramas de vocodificador de la súper-trama de voz DMR;

reemplazar por lo menos algunos de los bits identificados con un bit correspondiente de un vector de inicialización (IV); y

colocar por lo menos un identificador de cifrado en un campo de señalización incorporado de la súper-trama de voz DMR;

un transceptor (110) acoplado al dispositivo de procesamiento (114) para transmitir la súper-trama de voz DMR, que incluye el vector de inicialización y los identificadores de cifrado.

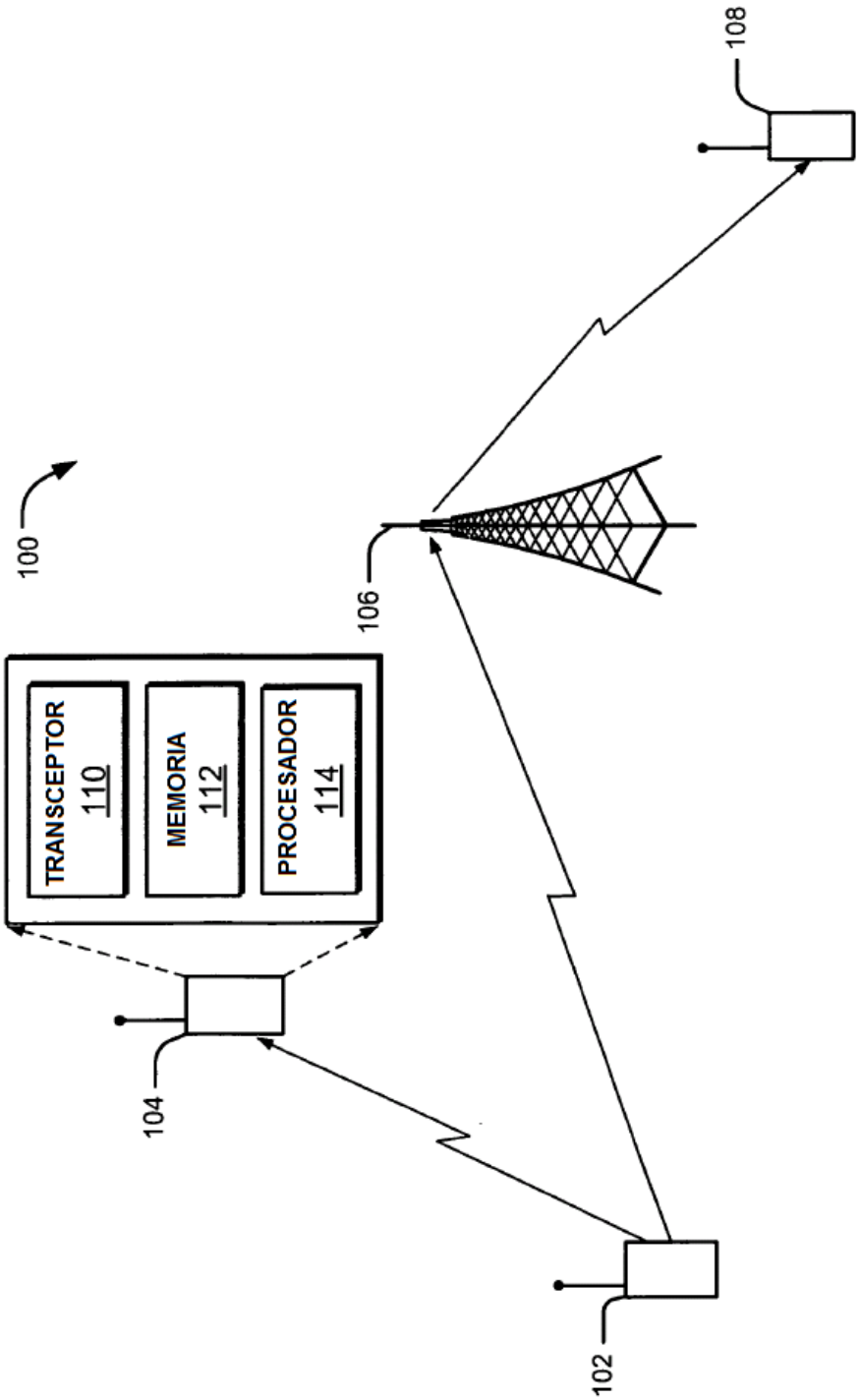
100
TRANSCEPTOR 110
MEMORIA 112
PROCESADOR 114
104
106
108
102

FIG. 1

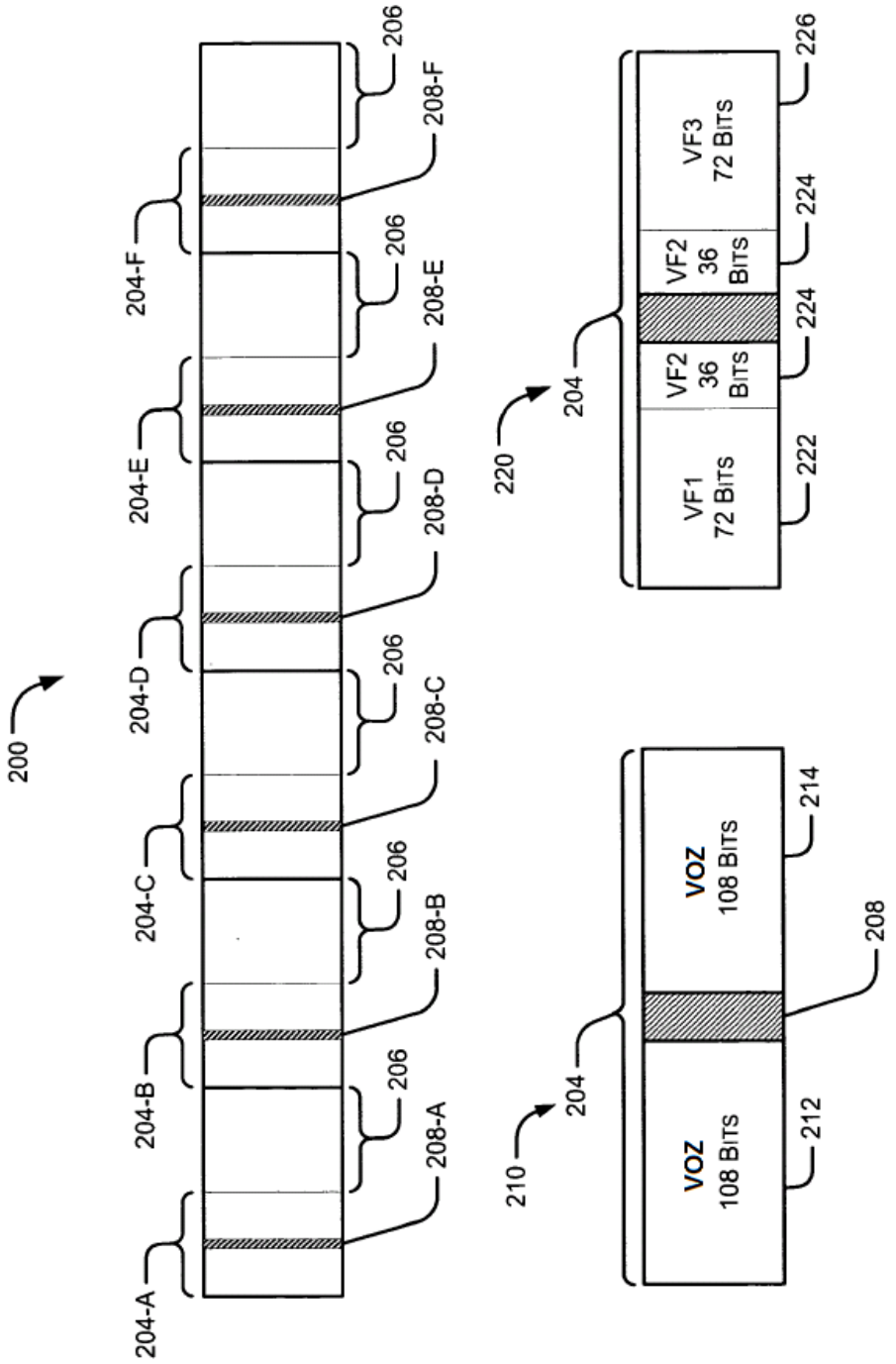
200
204-A
204-B
204-C
204-D
204-E
204-F
206
208-A
208-B
208-C
208-D
208-E
208-F
204
210
VOZ
108 BITS
212
214
208
220
VF1
72 BITS
222
VF2
36
BITS
224
VF3
72 BITS
226

FIG. 2

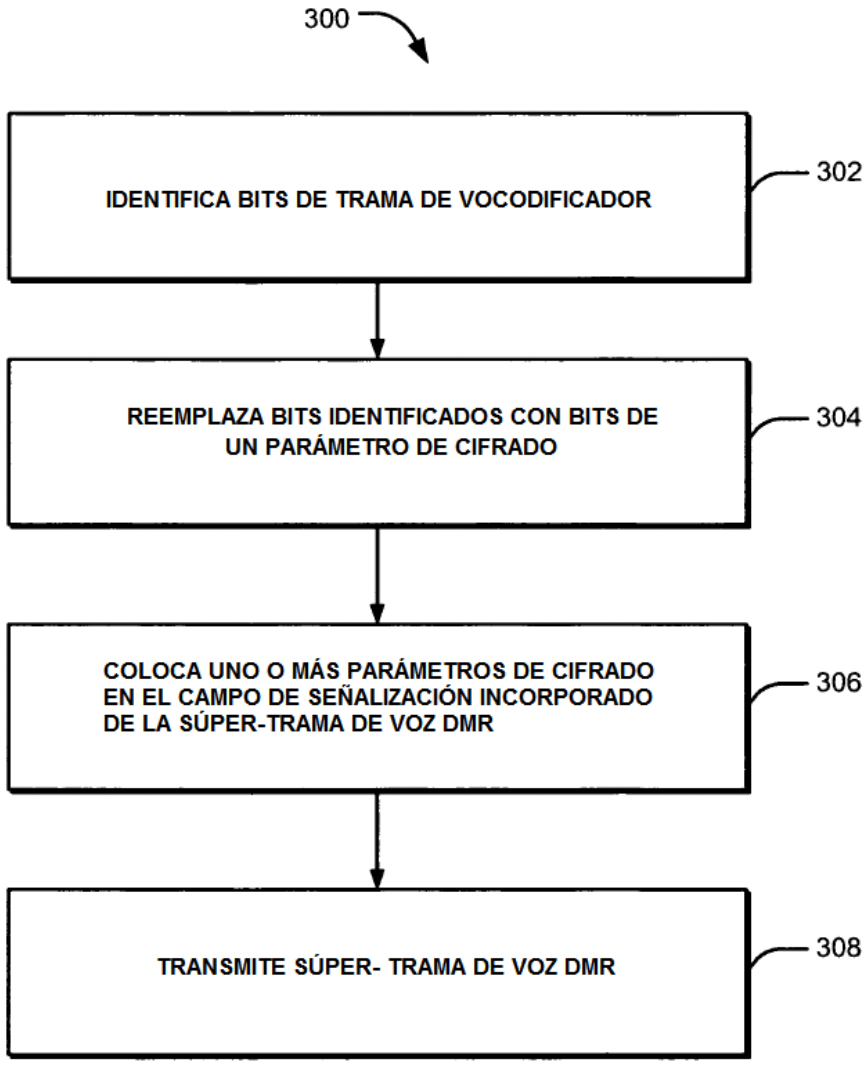
300
IDENTIFICA BITS DE TRAMA DE VOCODIFICADOR
302
REEMPLAZA BITS IDENTIFICADOS CON BITS DE UN PARÁMETRO DE CIFRADO
304
COLOCA UNO O MÁS PARÁMETROS DE CIFRADO EN EL CAMPO DE SEÑALIZACIÓN INCORPORADO DE LA SÚPER-TRAMA DE VOZ DMR
306
TRANSMITE SÚPER- TRAMA DE VOZ DMR
308

FIG. 3

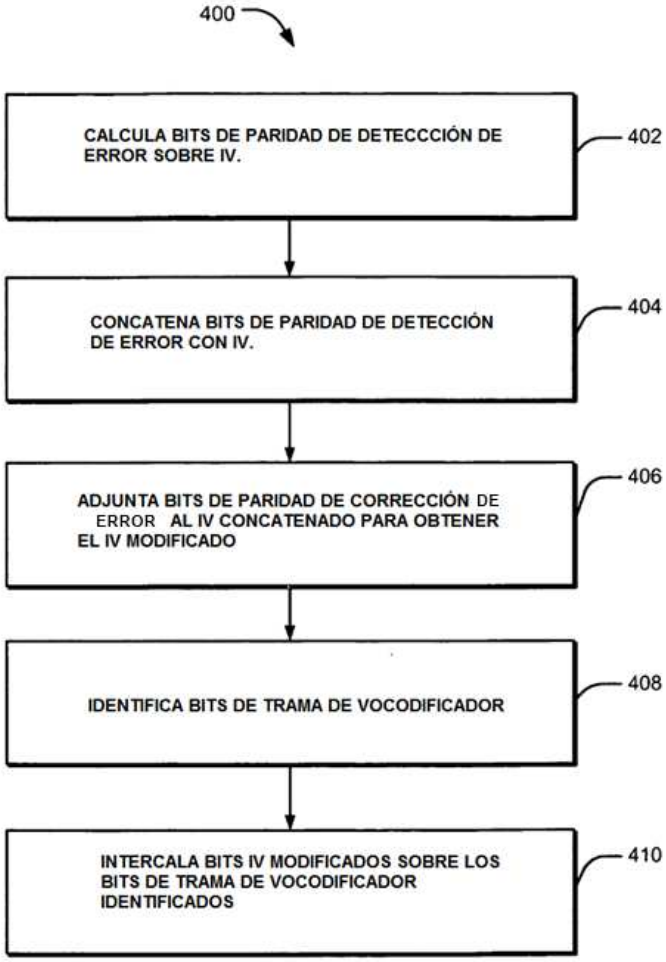
400
CALCULA BITS DE PARIDAD DE DETECCCIÓN DE ERROR SOBRE IV.
402
CONCATENA BITS DE PARIDAD DE DETECCIÓN DE ERROR CON IV.
404
ADJUNTA BITS DE PARIDAD DE CORRECCIÓN DE ERROR AL IV CONCATENADO PARA OBTENER EL IV MODIFICADO
406
IDENTIFICA BITS DE TRAMA DE VOCODIFICADOR
408
INTERCALA BITS IV MODIFICADOS SOBRE LOS BITS DE TRAMA DE VOCODIFICADOR IDENTIFICADOS
410

FIG. 4

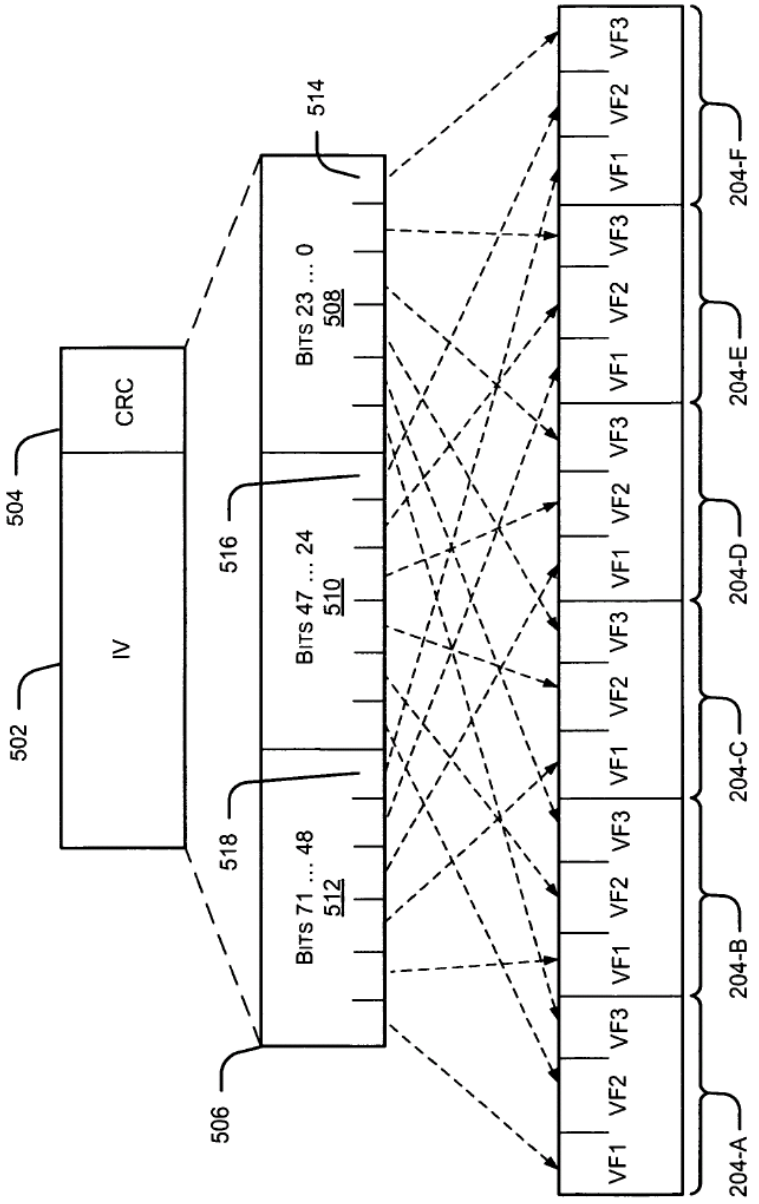
CRC
IV
504
502
506
514
516
518
BITS 23 ... 0
508
BITS 47 ... 24
510
BITS 71 ... 48
512
VF1
VF2
VF3
204-A
204-B
204-C
204-D
204-E
204-F

FIG. 5

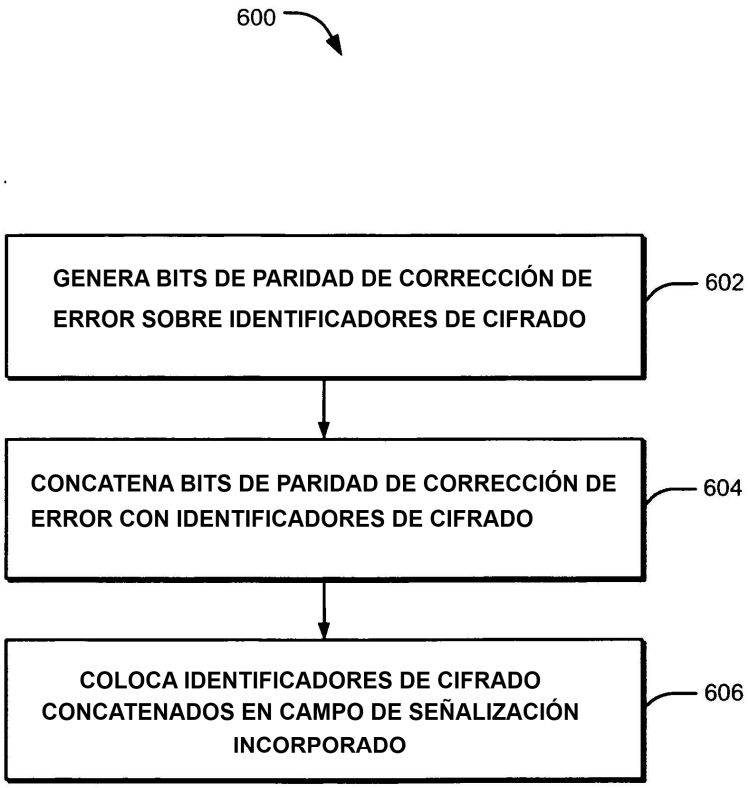
600
GENERA BITS DE PARIDAD DE CORRECCIÓN DE ERROR SOBRE IDENTIFICADORES DE CIFRADO
602
CONCATENA BITS DE PARIDAD DE CORRECCIÓN DE ERROR CON IDENTIFICADORES DE CIFRADO
604
COLOCA IDENTIFICADORES DE CIFRADO CONCATENADOS EN CAMPO DE SEÑALIZACIÓN INCORPORADO
606

FIG. 6

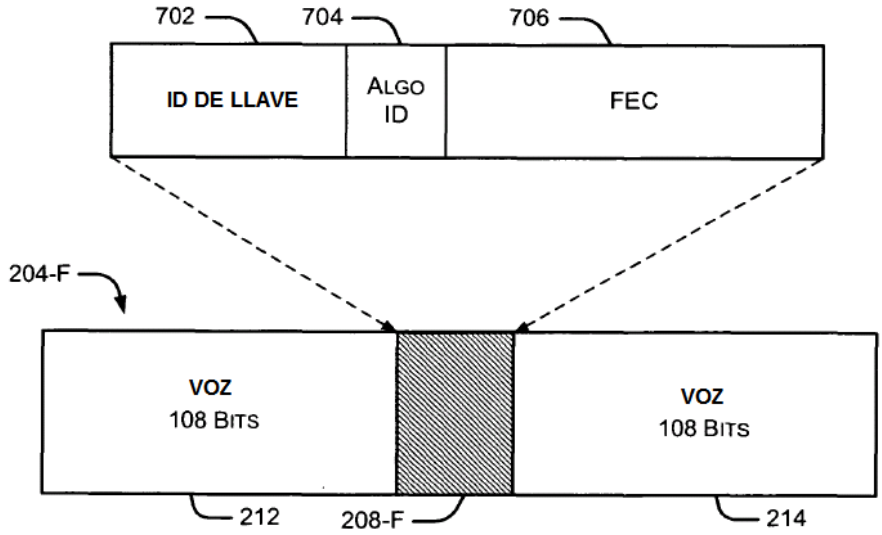
702
704
706
ID DE LLAVE
ALGO ID
FEC
204-F
VOZ
108 BITS
VOZ
108 BITS
212
208-F
214

FIG. 7

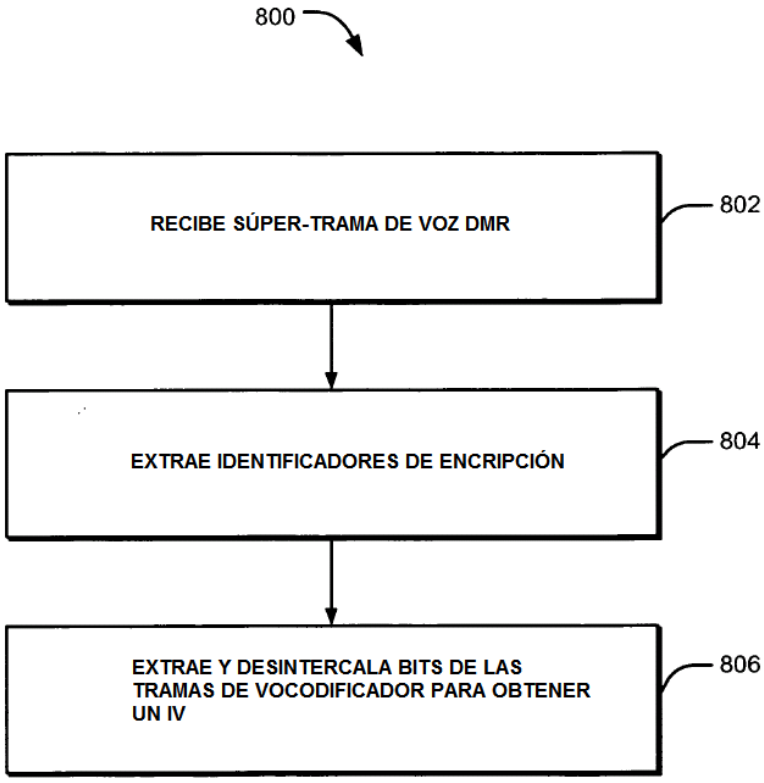
800
RECIBE SÚPER-TRAMA DE VOZ DMR
802
EXTRAE IDENTIFICADORES DE ENCRIPCIÓN
804
EXTRAE Y DESINTERCALA BITS DE LAS TRAMAS DE VOCODIFICADOR PARA OBTENER UN IV
806

FIG. 8