(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 716 499**

(51) Int. CI.:

H04B 7/185 (2006.01)
H04L 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.07.2010 E 10169101 (2)**

(97) Fecha y número de publicación de la concesión europea: **13.03.2019 EP 2282421**

(54) Título: **Multiplexación estadística multicanal de decodificadores FEC**

(30) Prioridad:

09.07.2009 US 224455 P
08.07.2010 US 832837

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.06.2019

(73) Titular/es:

VIASAT INC. (100.0%)
6155 El Camino Real
Carlsbad CA 92009, US

(72) Inventor/es:

MILLER, MARK J. y
LEONG, SANFORD

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Multiplexación estadística multicanal de decodificadores FEC

Campo de la invención

La presente invención generalmente se refiere a sistemas de comunicación vía satélite. Más particularmente, la presente invención se refiere a métodos y aparatos para distribuir decodificadores de Forward Error Correction (Corrección de errores sin canal de retorno - FEC) entre colas de decodificadores para obtener contraseñas de diferentes tamaños de bloque en sistemas de comunicación vía satélite.

Antecedentes

La próxima generación de sistemas comerciales de banda ancha basados en satélites en la banda de frecuencias K_a (i.e., 26,5-40 GHz) y con gran capacidad augura una gran velocidad de datos para el usuario final a bajo coste. Normalmente, estos sistemas usan múltiples terminales de puerta de enlace para comunicarse con un gran número de terminales de usuario, estando el satélite entre el terminal de puerta de enlace y los terminales de usuario. Un enlace directo de un sistema de comunicaciones vía satélite podría constar de transmisiones de enlace ascendente directo desde un terminal de puerta de enlace a un satélite, un repetidor "transparente" en el satélite y transmisiones de enlace descendente directo a un grupo de terminales de usuario ubicados en un haz puntual común. Un enlace de retorno de un sistema de comunicaciones vía satélite podría constar de transmisiones de enlace ascendente de retorno desde terminales de usuario en un haz puntual común hasta un satélite y transmisiones de enlace descendente de retorno desde el satélite hasta un terminal de puerta de enlace que preste servicio al haz puntual.

Es bien sabido que en tales sistemas se usa la Forward Error Correction (Corrección de errores sin canal de retorno - FEC) con el fin de asegurar que la transmisión de datos sea fiable. En el enlace de retorno por ráfagas, varios terminales de usuario transmiten ráfagas de datos de varios tamaños. Ráfaga se define como una transmisión contigua por radiofrecuencia desde un terminal de usuario individual. Cada ráfaga puede incluir una o más contraseñas, donde contraseña se define como un bloque FEC decodificable individual. Los tamaños de estas contraseñas pueden ser tan pequeños como unos pocos bytes (p. ej., 32 bytes) como tan grandes como varios kilobytes (p. ej., 8192 bytes). El esquema FEC particular empleado podría variar según el sistema, pero los sistemas de módems típicos utilizan esquemas FEC que requieren complicados decodificadores iterativos. Ejemplos de tales esquemas FEC incluyen los turbo códigos y los códigos de low-density parity-check (Comprobación de paridad de baja densidad - LDPC).

Los decodificadores FEC para el enlace de retorno pueden estar en un subsistema de procesamiento de physical layer (Capa física - PHY) ubicado en la puerta de enlace. Cada subsistema de procesamiento PHY normalmente procesa una cantidad fija de ancho de banda (p. ej., 62,5 MHz o 125 MHz), que puede incluir múltiples canales de enlace de retorno. Por lo tanto, cada subsistema de procesamiento PHY puede estar a cargo de decodificar ráfagas transmitidas por estos múltiples canales de enlace de retorno. Normalmente, cada decodificador está dedicado a la decodificación de un canal de enlace de retorno respectivo. Como consecuencia, el procesamiento de una contraseña transmitida por un canal de enlace de retorno particular no comienza hasta que el decodificador respectivo esté disponible, incluso si todos los demás decodificadores de ese subsistema de procesamiento PHY están disponibles. Esto puede suceder con bastante frecuencia en el caso de sistemas de Time Division Multiple Access (Acceso múltiple por división en el tiempo - TDMA), en los que las asignaciones de ráfaga no son deterministas. El resultado puede ser una latencia indeseablemente alta para el procesamiento de contraseñas. Una variación en un sistema TDMA es un sistema Multi-Frequency TDMA (TDMA multifrecuencia - MF-TDMA), en el que podría hacerse que cada usuario saltase a través de diferentes canales de frecuencia en forma de ráfagas.

El número de decodificadores FEC en cada subsistema de procesamiento PHY es una decisión de diseño importante. Normalmente, estos decodificadores son bastante complejos y, por tanto, utilizan una cantidad importante de recursos de hardware y/o de software. Por ejemplo, estos decodificadores pueden implementarse como Field Programmable Gate Arrays (Matrices de puertas programables in situ - FPGA), Application Specific Integrated Circuits (Circuitos integrados de aplicación específica - ASIC) o algún otro componente de hardware/software (p. ej., microprocesadores). Por lo tanto, la minimización del número de decodificadores que son necesarios en cada subsistema de procesamiento PHY es importante a la hora de diseñar terminales de puerta de enlace que sean pequeñas, eficientes y más baratas.

Los decodificadores FEC empleados en la mayoría de los sistemas de módems son decodificadores iterativos. Los decodificadores iterativos procesan la misma contraseña una o más veces de manera iterativa, donde, generalmente, cada iteración hace que la contraseña esté más cerca de ser decodificada correctamente. El número de iteraciones necesarias para decodificar una contraseña correctamente es una variable aleatoria y no puede predecirse *a priori*. Aunque puede que la mayor parte de las contraseñas necesite un número relativamente pequeño de iteraciones antes de ser decodificadas correctamente, algunas contraseñas pueden necesitar un gran número de iteraciones antes de ser decodificadas correctamente. Puede haber otras contraseñas que no se decodifiquen correctamente, incluso después de llegarse a un número máximo de iteraciones. El número de iteraciones

necesarias para decodificar una contraseña particular afecta a la cantidad de tiempo que el decodificador pasa en la contraseña particular y, por lo tanto, al número de decodificadores necesarios para decodificar una velocidad particular de ráfagas entrantes.

Algunas aplicaciones, tales como las de Voice over Internet Protocol (Protocolo de transmisión de voz por Internet - VoIP), son menos tolerantes a la latencia y a la fluctuación (i.e., la variabilidad del tiempo de decodificación necesario) y normalmente se transmiten como contraseñas cortas. Normalmente, lleva más tiempo decodificar contraseñas más largas que el que se tarda en decodificar contraseñas más cortas. Por lo tanto, si una contraseña corta sigue a una contraseña larga, el procesamiento de la contraseña larga puede introducir más latencia en el procesamiento de la contraseña más corta.

En el documento US 2007/0180344 A1 se describe un aparato que incluye un decodificador para decodificar información. La información comprende una contraseña de comprobación de paridad de baja densidad recibida en un nodo utilizando entradas definidas en una matriz base de comprobación de paridad. En correspondencia con las entradas en dicha matriz base de comprobación de paridad, se desplaza cíclicamente una submatriz de identidades en un valor definido por la entrada correspondiente en dicha matriz base de comprobación de paridad.

Resumen

La invención se define en las reivindicaciones independientes 1 y 7. En las reivindicaciones dependientes se exponen realizaciones preferidas.

Un ejemplo de un método para dividir un número total de decodificadores entre colas de decodificador de contraseñas de diferentes tamaños, siendo las contraseñas transmitidas por enlaces de comunicación de retorno desde terminales de datos hasta una puerta de enlace de un sistema de comunicaciones vía satélite, según la descripción incluye: para cada uno de los grupos *K*, asignar un número respectivo de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular, donde *K* es un número de tamaños diferentes de contraseñas, y el número respectivo de decodificadores se asigna a partir del número total de decodificadores y de forma proporcional a una carga ofrecida actual de contraseñas del tamaño particular.

Las realizaciones de este método pueden incluir una o más de las siguientes características. El método incluye además asignar un número mínimo de decodificadores a cada uno de los grupos *K*, donde cada uno de los números respectivos de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular es mayor o igual que el número mínimo de decodificadores asignados a cada uno de los grupos *K*. El método incluye además calcular la respectiva carga ofrecida actual para cada uno de los números *K* de diferentes tamaños de contraseña. Calcular la respectiva carga ofrecida actual de contraseñas de un tamaño particular incluye calcular la respectiva carga ofrecida actual como una función de la velocidad media de iteración para contraseñas del tamaño particular, el número de símbolos procesados por contraseña del tamaño particular y la velocidad de procesamiento de los decodificadores dedicados a la decodificación de contraseñas del tamaño particular. El método incluye además aplicar un factor de corrección a cada uno de los uno o más del respectivo número de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular para corregir según una o más estadísticas de formación de colas y un modelo de formación de colas. El método incluye además normalizar y cuantificar cada uno del respectivo número *K* de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular. El método incluye además calcular un valor de utilización para cada uno del número *K* de diferentes tamaños de contraseñas; y asignar un número de decodificadores no asignados a uno o más de los grupos *K* en función de los valores de utilización calculados.

Un ejemplo de un método para decodificar contraseñas de diferentes tamaños, siendo las contraseñas transmitidas por enlaces de comunicación de retorno desde terminales de datos hasta una puerta de enlace de un sistema de comunicaciones vía satélite, incluye: determinar un tamaño de una contraseña; determinar una cola de decodificación particular para decodificar la contraseña en función del tamaño determinado de la contraseña, siendo la cola de decodificación particular una de *K* colas de decodificación, donde *K* es un número de diferentes tamaños de contraseñas; y decodificar la contraseña usando un decodificador de la cola de decodificación particular, en el que el número de decodificadores en la cola de decodificación particular se asigna en proporción a una carga ofrecida actual de contraseñas del tamaño determinado.

Las realizaciones de este método pueden incluir una o más de las siguientes características. Decodificar la contraseña incluye decodificar iterativamente la contraseña, lo que incluye determinar tras cada iteración de decodificación si se pasa una comprobación de redundancia cíclica asociada a la contraseña. Decodificar iterativamente la contraseña incluye decodificar iterativamente la contraseña hasta que se llegue a un número máximo de iteraciones o que se pase la comprobación de redundancia cíclica asociada a la contraseña para un número umbral de iteraciones consecutivas. Una o más de las siguientes cosas varían en función del tamaño determinado de la contraseña: un tamaño de la comprobación de redundancia cíclica asociada a la contraseña, el número máximo de iteraciones y el número umbral de iteraciones consecutivas. El método incluye además detectar la presencia de una ráfaga de datos durante un tiempo de transmisión asignado a un terminal de datos del sistema de comunicaciones vía satélite, en el que determinar el tamaño de la contraseña incluye determinar el tamaño de la

contraseña incluida en la ráfaga de datos. El método incluye además determinar que la ráfaga de datos es una ráfaga ficticia transmitida por el terminal de datos durante el tiempo de transmisión asignado, en el que la ráfaga ficticia no incluye contraseñas.

Un ejemplo de aparato para dividir un número total de decodificadores entre colas de decodificador de contraseñas de diferentes tamaños, siendo las contraseñas transmitidas por enlaces de comunicación de retorno desde terminales de datos hasta una puerta de enlace de un sistema de comunicaciones vía satélite, incluye: un módulo de asignación configurado para asignar, para cada uno de *K* grupos, un número respectivo de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular, donde *K* es un número de diferentes tamaños de contraseñas, y el número respectivo de decodificadores se asigna a partir del número total de decodificadores y se asigna de forma proporcional a una carga ofrecida actual de contraseñas del tamaño particular.

Las realizaciones de un aparato así pueden incluir una o más de las siguientes características. El aparato incluye además un módulo de cálculo que está acoplado de manera comunicativa al módulo de asignación y configurado para calcular la respectiva carga ofrecida actual para cada uno del número *K* de diferentes tamaños de contraseñas. El módulo de asignación además está configurado para aplicar un factor de corrección a cada uno de los uno o más del número respectivo de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular para corregir según una o más estadísticas de formación de colas y un modelo de formación de colas. El módulo de asignación está configurado además para normalizar y cuantificar cada uno del respectivo número *K* de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular. El aparato incluye además un módulo de cálculo que está acoplado de manera comunicativa al módulo de asignación y configurado para calcular un valor de utilización para cada uno del número *K* de diferentes tamaños de contraseñas, en el que el módulo de asignación está configurado además para asignar un número de decodificadores no asignados a uno o más de los *K* grupos en función de los valores de utilización calculados.

Un ejemplo de aparato para decodificar contraseñas de diferentes tamaños, siendo las contraseñas transmitidas por enlaces de comunicación de retorno desde terminales de datos hasta una puerta de enlace de un sistema de comunicaciones vía satélite, incluye: un procesador que está configurado para determinar un tamaño de una contraseña y determinar una cola de decodificación particular para decodificar la contraseña en función del tamaño determinado de la contraseña, siendo la cola de decodificación particular una de *K* colas de decodificación, donde *K* es un número de diferentes tamaños de contraseñas; y un número de decodificadores en la cola de decodificación particular, estando cada decodificador acoplado de manera comunicativa al procesador y configurado para decodificar la contraseña, en el que el número de decodificadores en la cola de decodificación particular se asigna en proporción a una carga ofrecida actual de contraseñas del tamaño determinado.

Las realizaciones de un aparato así pueden incluir una o más de las siguientes características. Cada uno de los decodificadores está configurado para decodificar iterativamente la contraseña, lo que incluye determinar tras cada iteración de decodificación si se pasa una comprobación de redundancia cíclica asociada a la contraseña. Cada uno de los decodificadores está configurado para decodificar iterativamente la contraseña hasta que se llegue a un número máximo de iteraciones o que se pase la comprobación de redundancia cíclica asociada a la contraseña para un número umbral de iteraciones consecutivas. Una o más de las siguientes cosas varían en función del tamaño determinado de la contraseña: un tamaño de la comprobación de redundancia cíclica asociada a la contraseña, el número máximo de iteraciones y el número umbral de iteraciones consecutivas.

Gracias a la presente invención se pueden obtener numerosas ventajas con respecto a las técnicas convencionales. Una multiplexación estadística multicanal de decodificadores FEC se adapta al número de iteraciones que son necesarias para cada contraseña, sujeto a un número máximo de iteraciones. Por lo tanto, la latencia se reduce y la eficacia se incrementa cuando los decodificadores FEC se asignan dinámicamente. Las técnicas descritas también se ocupan de la fluctuación introducida por estos decodificadores FEC. Estos y otros beneficios se describen a lo largo de toda la memoria descriptiva y especialmente a continuación.

Breve descripción de los dibujos

Una mayor comprensión de la naturaleza y las ventajas de la presente invención puede llevarse a cabo mediante referencia a los siguientes dibujos. En las figuras anexas, los componentes o características similares pueden tener la misma etiqueta de referencia. Además, se pueden distinguir varios componentes del mismo tipo mediante la siguiente etiqueta de referencia con un guion y una segunda etiqueta que distingue entre los componentes similares. Si solo se utiliza la primera etiqueta de referencia en la memoria descriptiva, la descripción es aplicable a uno cualquiera de los componentes similares que tienen la misma etiqueta de referencia independientemente de la segunda etiqueta de referencia.

La figura 1 es un diagrama simplificado de un sistema de comunicaciones vía satélite ilustrativo en el que se pueden usar los métodos y aparatos de la presente invención.

La figura 2 muestra un banco de receptores que prestan servicio a múltiples canales de enlace de retorno.

La figura 3 muestra un banco de decodificadores con una única cola de decodificadores para cada tamaño de bloque FEC.

La figura 4 ilustra una asignación del número total de decodificadores disponibles entre las colas de decodificadores.

La figura 5 proporciona un diagrama de flujo que describe métodos para dividir un número total de decodificadores entre colas de decodificadores de contraseñas de diferentes tamaños.

La figura 6 proporciona un diagrama de flujo que describe métodos para decodificar contraseñas de diferentes tamaños.

Descripción detallada

La presente invención proporciona métodos y aparatos mejorados para dividir un número total de decodificadores entre colas de decodificadores de contraseñas de diferentes tamaños, en la que las contraseñas se transmiten por enlaces de comunicación de retorno desde terminales de datos (p. ej., terminales de usuario) hasta una puerta de enlace de un sistema de comunicaciones vía satélite. Para cada uno de los *K* grupos, se asigna un número respectivo de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular, donde *K* es un número de diferentes tamaños de contraseñas. El número respectivo de decodificadores se asigna a partir del número total de decodificadores y se asigna en proporción a una carga ofrecida actual de contraseñas del tamaño particular. También se describen métodos y aparatos para decodificar contraseñas de diferentes tamaños. El tamaño de una contraseña se determina, y se determina una cola de decodificación particular para decodificar la contraseña, en función del tamaño determinado de la contraseña. La cola de decodificación particular es una de *K* colas de decodificación. La contraseña se decodifica usando un decodificador de la cola de decodificación particular, en el que el número de decodificadores en la cola de decodificación particular se asigna en proporción a una carga ofrecida actual de contraseñas del tamaño determinado. Estas y otras realizaciones de la presente invención se describen con mayor detalle más adelante.

La figura 1 es un diagrama simplificado de un sistema 100 de comunicaciones vía satélite ilustrativo en el que pueden implementarse los métodos de la presente invención. El sistema 100 de comunicaciones vía satélite incluye una red 120 que está interconectada a uno o más terminales 115de puerta de enlace. El terminal 115 de puerta de enlace está configurado para comunicarse con uno o más terminales 130 de usuario a través de un satélite 105.

El terminal 115 de puerta de enlace se denomina a veces concentrador o estación terrestre. El terminal 115 de puerta de enlace presta servicio al enlace ascendente 135 y al enlace descendente 140 a y desde el satélite 105. El terminal 115 de puerta de enlace también puede programar el tráfico hasta los terminales 130de usuario. De forma alternativa, la programación puede realizarse en otras partes del sistema 100 de comunicaciones vía satélite (p. ej., en uno o más network operations centers [centros de operaciones de la red – NOC] y/o centros de mando de puerta de enlace). Aunque en la figura 1 solo se muestra un terminal 115de puerta de enlace, las realizaciones de la presente invención pueden implementarse en sistemas de comunicación vía satélite que tengan una pluralidad de terminales de puerta de enlace, cada uno de los cuales puede acoplarse a una o más redes.

En algunos sistemas de comunicaciones vía satélite, puede haber una cantidad limitada de espectro de frecuencia disponible para la transmisión. Los enlaces de comunicación entre el terminal 115 de puerta de enlace y el satélite 105 pueden usar frecuencias iguales, superpuestas o distintas como enlaces de comunicación entre el satélite 105 y los terminales 130 de usuario. El terminal 115 de puerta de enlace puede ubicarse lejos de los terminales 130 de usuario para permitir la reutilización de frecuencias.

La red 120 puede ser cualquier tipo de red y puede incluir, por ejemplo, Internet, una red IP, una intranet, una wide-area network (red de área extensa - WAN), una local-area network (red de área local - LAN), una virtual private network (red privada virtual - VPN), una virtual LAN (red virtual - VLAN), una red de fibra óptica, una red híbrida de fibra-coaxial, una red por cable, una public switched telephone network (red telefónica pública conmutada - PSTN), una public switched data network (red pública de datos conmutada - PSDN), una red móvil terrestre pública y/o cualquier otro tipo de red que permita las comunicaciones entre dispositivos tales como los descritos en la presente memoria. La red 120 puede incluir tanto conexiones cableadas como inalámbricas así como enlaces ópticos. La red 120 puede conectar el terminal 115 de puerta de enlace a otros terminales de puerta de enlace que pueden estar en comunicación con el satélite 105 o con otros satélites.

El terminal 115 de puerta de enlace proporciona una interfaz entre la red 120 y el satélite 105. El terminal 115 de puerta de enlace se puede configurar para recibir datos e información dirigidos a uno o más terminales 130 de usuario. El terminal 115 de puerta de enlace puede formatear los datos y la información para su entrega a los terminales 130 de usuario respectivos. De forma similar, el terminal 115 de puerta de enlace puede configurarse para recibir señales procedentes del satélite 105 (p. ej., procedentes de uno o más terminales 130 de usuario) dirigidas a un destino accesible a través de la red 120. El terminal 115 de puerta de enlace puede formatear las señales recibidas para su transmisión por la red 120.

El terminal 115 de puerta de enlace puede utilizar una antena 110 para transmitir la señal 135 de enlace ascendente directo al satélite 105. En una realización, la antena 110 puede comprender un reflector parabólico con alta direccionalidad

en la dirección del satélite 105 y baja direccionalidad en otras direcciones. La antena 110 puede comprender una variedad de configuraciones alternativas e incluir características operativas tales como un gran aislamiento entre polarizaciones ortogonales, una gran eficacia en las bandas de frecuencia operacionales, poco ruido y características similares.

El satélite 105 puede ser un satélite geoestacionario que esté configurado para recibir señales 135 de enlace ascendente directo desde la ubicación de la antena 110. El satélite 105 puede usar, por ejemplo, una antena reflectora, una antena de lente, una antena en fase, una antena activa o cualquier otro mecanismo conocido en la técnica para la recepción de tales señales. El satélite 105 puede procesar las señales recibidas desde el terminal de puerta de enlace 115 y reenviar las señales 150 de enlace descendente a uno o más de los terminales 130 de usuario. Las señales pueden hacerse pasar a través de una antena reflectora de transmisión (p. ej., una antena en fase) para formar el patrón de radiación de transmisión (haz puntual). El satélite 105 puede funcionar en modo multihaz puntual transmitiendo una serie de haces estrechos dirigidos cada uno a una región diferente de la Tierra. Esto permite la separación de los terminales 130 de usuario en los diversos haces estrechos.

El satélite 105 puede configurarse como un satélite “transparente”. En esta configuración, el satélite 105 puede realizar la conversión de frecuencia y de polarización de las señales portadoras recibidas antes de retransmitir las señales a su destino. Un haz puntual puede usar una sola portadora, es decir, una frecuencia, o un intervalo de frecuencias contiguo por haz. El satélite 105 puede emplear una variedad de técnicas de codificación y de modulación de transmisión en la capa física (p. ej., codificación y modulación adaptativas).

El sistema 100 de comunicaciones vía satélite puede utilizar una serie de arquitecturas de red que consisten en segmentos espaciales y terrestres. El segmento espacial puede incluir uno o más satélites mientras que el segmento terrestre puede incluir uno o más terminales de usuario, terminales de puerta de enlace, network operations centers (centros de operaciones de la red - NOC), y centros de mando del satélite y terminales de puertas de enlace. Los segmentos se pueden conectar en una red en malla, una red en estrella o similares, tal y como les resultará evidente a los expertos en la técnica.

Las señales 150 de enlace descendente directo pueden transmitirse desde el satélite 105 a uno o más terminales 130 de usuario. Los terminales 130 de usuario pueden recibir las señales 150 de enlace descendente mediante una antena 127. En una realización, la antena 127 y el terminal 130 de usuario comprenden juntos un very small apertura terminal (terminal de muy pequeña apertura - VSAT). La antena 127 tiene un diámetro de aproximadamente 0,6 metros y una potencia de aproximadamente 2 vatios. En otras realizaciones, se puede utilizar una variedad de otros tipos de antena 127 en los terminales 130 de usuario para recibir las señales 150 de enlace descendente desde el satélite 105. Cada uno de los terminales 130 de usuario puede comprender un único terminal de usuario o, de forma alternativa, comprender un concentrador o encaminador (no representado) que esté acoplado a múltiples terminales de usuario. Cada terminal 130 de usuario puede conectarse a varios consumer premises equipment (equipos en las instalaciones del cliente - CPE), que comprendan, por ejemplo, ordenadores, redes de área local, dispositivos de Internet, redes inalámbricas y similares.

De una manera similar a la descrita anteriormente, los terminales 130 de usuario pueden usar transmisiones de enlace de retorno para comunicarse con el terminal 115 de puerta de enlace o con la red 120 a través del satélite 105. El enlace de retorno puede consistir en transmisiones 145 de enlace ascendente de retorno desde los terminales 130 de usuario hasta el satélite 105 y transmisiones 140 de enlace descendente de retorno desde el satélite 105 hasta el terminal 115de puerta de enlace. El terminal 115 de puerta de enlace puede formatear las señales recibidas para su transmisión a uno o más destinos que son accesibles a través de la red 120.

Las técnicas descritas a continuación para distribuir decodificadores FEC entre colas de decodificadores para contraseñas de diferentes tamaños de bloque pueden aplicarse a sistemas de comunicaciones vía satélite como el sistema 100 de comunicaciones vía satélite de la figura 1. En particular, un banco de decodificadores en una puerta de enlace del sistema de comunicaciones vía satélite puede compartirse entre varios canales de enlace descendente de retorno, lo cual permite que el sistema aproveche la multiplexación estadística. Dado que cada decodificador está ocupado durante un periodo aleatorio, compartir los decodificadores entre el conjunto de canales reduce el retraso total.

Las técnicas descritas generalmente implican dividir el número total disponible de decodificadores, N_{dec}, entre K grupos, donde K es el número de diferentes tamaños de contraseñas en el sistema. El número total disponible de decodificadores se divide de modo que el número de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular sea proporcional a una carga ofrecida actual de contraseñas del tamaño particular. Esta multiplexación estadística resulta en un mejor uso general de los decodificadores y proporciona una gestión de la fluctuación mediante la reducción de la variación en el retardo de decodificación. A continuación se ofrecen detalles de estas técnicas.

Compartición de recursos de decodificación entre múltiples canales de enlace de retorno

En un ejemplo de sistema AMDT (o MF-AMDT), cada subsistema de procesamiento de capas de Media Access Control (Control del acceso a medios - MAC) y/o subsistema de procesamiento PHY en la puerta de enlace está a cargo del procesamiento de una cantidad fija de ancho de banda (p. ej., 125 MHz). Esta cantidad de ancho de banda podría dividirse entre múltiples canales de enlace de retorno, donde cada canal puede ser muy inferior a 125 MHz.

En una realización, cada canal de enlace de retorno es de 625 Ksps y, por tanto, el subsistema de procesamiento MAC/PHY en la puerta de enlace necesita procesar 200 canales de enlace de retorno. De forma alternativa, los canales de enlace de retorno podrían tener diferentes velocidades de símbolo. Por ejemplo, podría haber una mezcla de canales de enlace de retorno de 625 Ksps, 1,25 Msps, 2,5 Msps, 5 Msps, 10 Msps y 20 Msps, de manera que la cantidad que estuviese siendo procesada por este subsistema ascendiese al ancho de banda total (p. ej., 125 MHz).

Cada canal de enlace de retorno recibe ráfagas de uno o más terminales de usuario (p. ej., terminales 130 de usuario de la figura 1). La figura 2 muestra un ejemplo 200 de un banco de receptores 220 en una puerta de enlace que presta servicio a múltiples canales de enlace de retorno. Las ráfagas 210 transmitidas por los canales de enlace de retorno procedentes de diferentes terminales de usuario están indicadas por los diferentes patrones. Cada ráfaga 210 puede contener una o más contraseñas. Cada decodificador tarda una cantidad aleatoria de tiempo en terminar de decodificar cada contraseña porque el tiempo de decodificación depende del tamaño de contraseña así como del número de iteraciones que le lleva decodificar una contraseña particular. Por lo tanto, la capacidad de poner en común los recursos de decodificación del banco de receptores entre múltiples canales de enlace de retorno es un ejemplo de multiplexación estadística.

En un ejemplo, existen dos canales de enlace de retorno: un canal 1 y un canal 2. Si los canales de enlace de retorno tuvieran decodificadores dedicados que no pudiesen compartirse, tal y como sucede en los sistemas convencionales, entonces una contraseña en el canal 1 tendría que esperar a que el decodificador dedicado al canal 1 estuviese disponible antes de que pudiese descodificarse la contraseña en el canal 1. Este sería así incluso si el decodificador dedicado al canal 2 estuviese inactivo y disponible. Por el contrario, si todos los decodificadores pudiesen compartirse, entonces la contraseña en el canal 1 podría ser decodificada por el decodificador inactivo, dando así lugar a menores latencias de decodificación.

Distribución de decodificadores entre colas de decodificadores para contraseñas de diferentes tamaños de bloque

En lo que respecta a las técnicas de distribución de un número total de decodificadores entre colas de decodificadores, puede suponerse que la puerta de enlace del sistema de comunicaciones vía satélite tiene un número fijo de decodificadores, N_{dec}. También puede considerarse que hay un número fijo de diferentes tamaños de contraseña, K. Por ejemplo, puede haber N_{dec}=24 decodificadores dedicados y en el K=6 tamaños de contraseña diferentes. La distribución de contraseñas entrantes en la puerta de enlace puede variar entre estos K tamaños de contraseña diferentes y no seguir ningún patrón conocido *a priori*. El reto consiste en distribuir estos N_{dec} decodificadores entre N_1, N_2,..., N_K decodificadores, de manera que $N_{dec}=N_1 + N_2 + \ldots + N_k$ y N_j decodificadores estén dedicados a la decodificación de contraseñas de tamaño j, donde $j \in$ de 1, 2,..., K. Esto se ilustra en la figura 3, que muestra un banco de decodificadores con una única cola de decodificadores para cada K tamaños de bloque FEC. Cada ráfaga recibida desde un terminal de usuario se descompone en contraseñas, y cada una de las contraseñas se encamina a una cola de decodificadores respectiva en función del tamaño de bloque de la contraseña particular.

En referencia a la figura 5, con referencia adicional a la figura 4, un proceso 500 de dividir un número total de decodificadores entre las colas de decodificadores de contraseñas de diferentes tamaños incluye las etapas mostradas. Las contraseñas se transmiten por enlaces de comunicación de retorno desde terminales de usuario hasta una puerta de enlace de un sistema de comunicaciones vía satélite. La figura 4 ilustra una asignación del número total de decodificadores disponibles entre las colas de decodificadores. El proceso 500 es, sin embargo, meramente ilustrativo y no limitante. El proceso 500 puede alterarse, por ejemplo, añadiéndosele, eliminando o reorganizando etapas.

En una etapa 502, un procesador (p. ej., un procesador de un subsistema de procesamiento MAC/PHY de la puerta de enlace) asigna, para cada uno de K grupos, un número respectivo de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular, en el que el número respectivo de decodificadores se asigna a partir del número total de decodificadores, N_{dec}, y se asigna en proporción a una carga ofrecida actual de contraseñas del tamaño particular. Tal y como se mencionó anteriormente, K es el número de diferentes tamaños de contraseñas. Por ejemplo, si A_j es la carga ofrecida actual de contraseñas de tamaño j, el número de decodificadores dedicados a la decodificación de contraseñas de tamaño j, N_j, se puede configurar como A_j o como un número proporcional a A_j.

En algunas implementaciones, el proceso 500 incluye calcular la respectiva carga ofrecida actual para cada uno del número K de diferentes tamaños de contraseñas. En la figura 4 se ilustra una estimación de la carga ofrecida para cada uno del número K de diferentes tamaños de contraseñas, en la que la carga ofrecida, A_j, se utiliza además en el algoritmo de asignación de decodificadores. En un ejemplo, la carga ofrecida actual, A_j, para contraseñas de tamaño j se puede calcular como una función de la velocidad media de iteración (i.e., i_j) para contraseñas de tamaño j, el número de símbolos procesados por contraseña particular de tamaño j (i.e., N_{FEC}) y la velocidad de procesamiento en símbolos por segundo (i.e., $R_{decodificador}$) de los N_j decodificadores dedicados a la decodificación de contraseñas de tamaño j. En particular, A_j puede ser igual a $i_j * N_{FEC} / R_{decodificador}$.

La velocidad media de iteración es el número medio de iteraciones de decodificador por segundo. La figura 4 ilustra que el cálculo la velocidad media de iteración, i_j, es parte de la estimación de la carga ofrecida. Como

ejemplo, la velocidad media de iteración se puede calcular contando el número total de las iteraciones de decodificador durante un intervalo de tiempo T (p. ej., T = 1,28 segundos) y dividiendo el número total de iteraciones de decodificador por T segundos para obtener el número medio de iteraciones por segundo.

En otro ejemplo con una implementación de decodificadores en ventanas, el número total de símbolos procesados por contraseña de tamaño j es igual $N_{FEC} + N_b$, donde N_{FEC} es el número de símbolos en la contraseña de tamaño j, excluyendo los ámbulos, y N_b es el tamaño de ventana de decodificador. Tanto N_{FEC} como N_b son generalmente fijos y conocidos en el momento del diseño de código para cada tamaño de ráfaga y la combinación de codificación/modulación. El tráfico en un haz puntual generalmente usa la misma velocidad de código y, por tanto, la velocidad de código asociada al haz puntual se puede presuponer para todas las ráfagas. De forma adicional, si se utilizan decodificadores interiores y exteriores y $R_{decodificador}$ es la velocidad de procesamiento de uno de estos decodificadores, $R_{decodificador}/2$ puede utilizarse como la velocidad de procesamiento global de los decodificadores interiores y exteriores concatenados. Por lo tanto, para este ejemplo, la carga ofrecida actual, A_j, en lenguaje de programación Erlang para contraseñas de tamaño j se puede calcular como $i_j * 2 *(N_{FEC} + N_b) / R_{decodificador}$.

En algunas implementaciones, el proceso 500 incluye asignar un número mínimo de decodificadores a cada uno de los K grupos, en el que cada uno de los números respectivos de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular es mayor o igual que el número mínimo de decodificadores asignados a cada uno de los K grupos. Por ejemplo, el número mínimo de decodificadores, N_{min}, asignado a cada uno de los K grupos se puede configurar como un número pequeño (p. ej., 1) con respecto al número total de decodificadores disponibles. Esto se hace para tener en cuenta la posibilidad estadística, por pequeña que sea, de que se reciba una contraseña de un tamaño particular en la puerta de enlace.

Volviendo a figura 5, en una etapa 504 el procesador aplica un factor de corrección a cada uno de los uno o más del número respectivo de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular para corregir según una o más estadísticas de formación de colas y un modelo de formación de colas. Por ejemplo, para corregir según estadísticas de formación de colas para tener en cuenta las fluctuaciones en la carga ofrecida actual, el número de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular se pueden aumentar para uno o más (p. ej., todos) del número K de decodificadores (i.e., $N_j = N_j + 1$). Esta corrección ilustrativa actúa como función de redondeo. En otro ejemplo, para corregir desviaciones en el modelo de formación de colas (p. ej., un modelo $M/M/k$), el número de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular se puede multiplicar por una función de corrección (p. ej., $Nj = Nj * f(K)$).

En una etapa 506 el procesador normaliza y cuantifica cada uno del respectivo número K de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular. Por ejemplo, el número de decodificadores, N_j, dedicados a la decodificación de contraseñas de un tamaño j se puede configurar según lo siguiente:

$$N_j = N_{\min} + Int\left[\left(N_{dec} - 6N_{\min}\right)\cdot\left(N_j \Big/ \sum_{i=1}^{6} N_i\right)\right].$$

Después de la normalización y cuantificación, el número total de decodificadores no puede asignarse entre las K colas de decodificadores, es decir, $N_1 + N_2 +... + N_k < N_{dec}$. Si este fuera el caso, el proceso 500 podría pasar a unas etapas 508 y 510.

En la etapa 508, el procesador calcula un valor de utilización para cada uno del número K de diferentes tamaños de contraseñas. Por ejemplo, el valor de utilización, U_j, para contraseñas de tamaño j se puede configurar como la carga ofrecida actual, A_j, para contraseñas de tamaño j dividida por el número de decodificadores, N_j, dedicados a la decodificación de contraseñas de tamaño j. Es decir, $U_j = A_j / N_j$.

En la etapa 510, el procesador asigna un número de decodificadores no asignados a uno o más de los K grupos en función de los valores de utilización calculados. Es decir, si $N_1 + N_2 +... + N_k < N_{dec}$ tras la etapa 506, el número de decodificadores no asignados restante es $N_{res} = N_{dec} - (N_1 + N_2 + \ldots + N_k)$. Estos restantes decodificadores no asignados pueden ser asignados a una o más de las K colas de decodificación, por ejemplo, sobre la base primera de una máxima utilización. A continuación se describen dos técnicas para asignar los decodificadores restantes a una o más de las K colas de decodificación, aunque son posibles otras técnicas.

En algunas implementaciones, todos los restantes decodificadores no asignados se asignan a la cola de decodificadores asociada a las contraseñas de tamaño j, donde U_j es el mayor de los K valores de utilización calculados en la etapa 508. Es decir, $N_J = N_J + N_{res}$.

En otras implementaciones, uno de los decodificadores no localizados restantes se asigna a la cola de decodificadores asociada a las contraseñas de tamaño j, donde U_j es el mayor de los K valores de utilización calculados en la etapa 508. Es decir, $N_j = N_j + 1$, y $N_{res} = N_{res} - 1$. Las etapas 508 y 510 pueden entonces repetirse, asignando en cada iteración uno de los restantes decodificadores no asignados a la cola de decodificadores asociada al tamaño de contraseña de la mayor utilización calculada actualmente (i.e., tal y como se calcula en la etapa 508) hasta que no queden decodificadores no asignados (i.e., $N_{res} = 0$). Tras la última iteración, $N_1 + N_2 + ... + N_k = N_{dec}$.

Decodificación de contraseñas de diferentes tamaños de bloque utilizando las colas de decodificadores

En el sistema de comunicaciones vía satélite, puede adjuntarse una cyclic redundancy check (comprobación de redundancia cíclica - CRC) de C bits (p. ej., $C = 16$) al final de cada contraseña una vez finalizado el proceso de codificación FEC en la capa física de un transmisor en un terminal de usuario (p. ej., uno de los terminales 130 de usuario de la figura 1). La comprobación CRC cubre toda la contraseña FEC. En el lado de decodificador del extremo receptor (i.e., en la puerta de enlace), el decodificador intenta hacer coincidir las comprobaciones CRC (i.e., comprueba que se pasan la CRC) al final de cada iteración de decodificación. Si las CRC coinciden, esto podría ser una falsa alarma. Por lo tanto, en algunas implementaciones, el decodificador intenta verificar que las CRC coinciden iterando una o más veces y comprobando que se alcanza un número umbral de coincidencias de CRC consecutivas (p. ej., 2). Si se alcanza el número umbral de coincidencias de CRC consecutivas, el decodificador puede declarar que la contraseña se ha decodificado correctamente y puede enviar los símbolos decodificados hacia la siguiente capa más alta, al tiempo que comienza a procesar la siguiente ráfaga en la cola de decodificación.

Si las CRC no coinciden al final de una iteración, el decodificador itera y comprueba las CRC nuevamente al final de cada iteración hasta que, o bien las CRC coinciden (i.e., se pasan) para el número umbral de iteraciones consecutivas, o bien el número de iteraciones de decodificación alcanza un número máximo de iteraciones (p. ej., 100). El número umbral de iteraciones consecutivas se emplea para reducir la probabilidad de que haya una falsa alarma en la decodificación de una contraseña correcta.

En algunas implementaciones, contraseñas de diferentes tamaños pueden llevar adjuntas CRC de diferentes tamaños. Dado que las CRC utilizan una tara de capa física, una CRC de tamaño fijo tiene una tara desproporcionadamente mayor, expresada como una fracción del tamaño de ráfaga, para menores tamaños de ráfaga que la tara utilizada por la CRC de tamaño fijo para mayores tamaños de ráfaga. Sin embargo, las CRC cortas tienen una mayor probabilidad de falsa alarma que la probabilidad de falsa alarma de CRC más largas. Por lo tanto, puede utilizarse una CRC corta con un número umbral más grande de coincidencias de CRC consecutivas para hacer que la tara sea baja. Es decir, en algunas implementaciones, cada contraseña de un tamaño diferente tiene una longitud diferente para su CRC y un número umbral diferente de coincidencias de CRC consecutivas. De forma similar, el criterio de parada de un número máximo de iteraciones también puede ser una función del tamaño de contraseña.

En algunos sistemas de comunicaciones vía satélite, un planificador de enlace de retorno en la puerta de enlace se encarga de programar intervalos de tiempo para los diversos terminales de usuario para la transmisión. Esto es típico en la mayoría de los sistemas TDMA. Hay numerosos planificadores que pueden utilizarse, y algunos planificadores son más eficaces que otros planificadores. A diferencia de los planificadores que son completamente eficientes, la mayoría de planificadores programará intervalos de tiempo que serán más grandes de lo que necesita un terminal de usuario particular. Por lo tanto, puede que se asignen a los terminales de usuario intervalos de tiempo que los terminales de usuario no necesiten y que pueden ignorar. En terminales de usuario con límite de potencia, resulta óptimo para ahorrar energía y no transmitir ninguna ráfaga cuando no haya ningún dato que transmitir durante un intervalo de tiempo asignado. Sin embargo, la mayoría de sistemas de banda ancha por satélite no están limitados en cuanto a la potencia, ya que los terminales de usuario normalmente están alimentados desde enchufes de pared.

Cuando los terminales de usuario no tienen un límite de potencia, puede ser preferible transmitir una ráfaga siempre que el intervalo de tiempo asignado se haya programado para ese terminal de usuario. Si el terminal del usuario no transmite nada durante un intervalo de tiempo asignado (i.e., no se transmite ninguna contraseña ni ninguna CRC correspondiente), el decodificador intentará decodificar ruido como una contraseña que no existe y, por tanto, la CRC no se pasará para el número umbral de iteraciones consecutivas. Por consiguiente, el decodificador necesitará ejecutar el número máximo de iteraciones antes de que pueda pasar a la siguiente ráfaga, lo cual aumentará la latencia experimentada por las contraseñas de la siguiente ráfaga. Una alternativa sería detectar primero la presencia de una ráfaga y luego intentar decodificarla. Sin embargo, la detección de ráfagas en las condiciones de low signal-to-noise ratio (baja relación señal-ruido - SNR) que normalmente se dan en los sistemas de comunicaciones vía satélite requiere una estructura de ámbulo relativamente larga, lo cual supone un uso eficiente de un ancho de banda limitado.

Por lo tanto, en algunas implementaciones, un terminal de usuario que no esté limitado en cuanto a la potencia y no tenga datos que enviar transmitirá una ráfaga (p. ej., una ráfaga de contraseñas válidas con todos los bits de información iguales a 0) cada vez que un intervalo de tiempo sea programado para ese terminal de usuario por el

planificador de enlace de retorno de la puerta de enlace. La transmisión de una ráfaga ficticia cuando el terminal de usuario no tenga datos que enviar garantiza que todos los intervalos de tiempo programados tengan ráfagas, evitándose así que el decodificador necesite ejecutar el número máximo de iteraciones innecesariamente.

Con referencia a la figura 6, un proceso 600 de decodificación de contraseñas de tamaños diferentes incluye las etapas mostradas. Las contraseñas se transmiten por enlaces de comunicación de retorno desde terminales de usuario hasta una puerta de enlace de un sistema de comunicaciones vía satélite. El proceso 600 es, sin embargo, meramente ilustrativo y no limitante. El proceso 600 puede alterarse, por ejemplo, añadiéndosele, eliminado o reorganizando etapas.

En una etapa 602, un procesador (p. ej., un procesador de la puerta 115 de enlace de la figura 1) determina el tamaño de una contraseña transmitida desde un terminal de usuario. El procesador puede determinar que la contraseña incluida en una ráfaga procedente del terminal de usuario tiene uno de los *K* tamaños de contraseña.

En una etapa 604, el procesador determina una cola de decodificación particular para decodificar la contraseña en función del tamaño determinado de la contraseña, donde la cola de decodificación particular es una de *K* colas de decodificación.

En una etapa 606, un decodificador de la cola de decodificación particular decodifica la contraseña, en la que el número de decodificadores en la cola de decodificación particular se asigna en proporción a la carga ofrecida actual de contraseñas del tamaño determinado. Por ejemplo, el número de decodificadores en la cola de decodificación particular puede asignarse usando el proceso 500 descrito anteriormente con respecto a la figura 5.

Cabe señalar que los métodos y sistemas que se han analizado a lo largo de esta memoria descriptiva se han proporcionado meramente como ejemplos. Varias realizaciones pueden omitir, sustituir, o agregar varios procedimientos o componentes según sea apropiado. Por ejemplo, debe apreciarse que las características descritas sobre ciertas realizaciones pueden combinarse en diversas otras realizaciones. Además, pueden realizarse mediciones y los diversos valores proporcionarse en cualquier unidad. Además, las realizaciones pueden implementarse mediante hardware, software, firmware, middleware, microcódigo, lenguajes de descripción de hardware o cualquier combinación de los mismos. Cuando se implementa en software, firmware, middleware, o microcódigo, el código de programa o los segmentos de código para realizar las tareas necesarias se puede almacenar en un medio legible por ordenador tal como un medio de almacenamiento. Los procesadores pueden adaptarse a realizar las tareas necesarias. El término “medio legible por ordenador” incluye, pero no se limita a, dispositivos de almacenamiento portátiles o fijos, dispositivos de almacenamiento óptico, canales inalámbricos, tarjetas SIM, otras tarjetas inteligentes y diversos otros medios capaces de almacenar, contener o llevar instrucciones o datos.

Una vez descritas varias realizaciones, los expertos en la técnica reconocerán que pueden utilizarse diversas modificaciones, construcciones alternativas y equivalentes sin apartarse del alcance de la invención tal y como se ha definido mediante las reivindicaciones adjuntas.

Por ejemplo, los elementos anteriores pueden ser simplemente un componente de un sistema más grande, en donde otras reglas pueden tomar precedencia sobre o de cualquier otra forma modificar la aplicación de la invención. Asimismo, se pueden realizar una serie de etapas antes, durante, o después de considerar los elementos anteriores. Por consiguiente, la descripción anterior no debe tomarse como una limitación del alcance de la invención.

REIVINDICACIONES

1. Un método para decodificar contraseñas de diferentes tamaños, siendo las contraseñas transmitidas por enlaces de comunicación de retorno desde terminales de datos hasta una puerta de enlace de un sistema de comunicaciones vía satélite, comprendiendo el método:

   determinar un tamaño de una contraseña;
   determinar una cola de decodificación particular para decodificar la contraseña en función del tamaño determinado de la contraseña, siendo la cola de decodificación particular una de *K* colas de decodificación, donde *K* es un número de diferentes tamaños de contraseñas; y
   decodificar la contraseña usando un decodificador de la cola de decodificación particular, en el que el número de decodificadores en la cola de decodificación particular se asigna en proporción a una carga ofrecida actual de contraseñas del tamaño determinado.

2. El método de la reivindicación 1, en el que la decodificación de la contraseña comprende decodificar iterativamente la contraseña lo que incluye determinar tras cada iteración de decodificación si se pasa una comprobación de redundancia cíclica asociada a la contraseña.

3. El método de la reivindicación 2, en el que decodificar iterativamente la contraseña comprende decodificar iterativamente la contraseña hasta que se llegue a un número máximo de iteraciones o se pase la comprobación de redundancia cíclica asociada a la contraseña para un número umbral de iteraciones consecutivas.

4. El método de la reivindicación 3, en el que una o más de las siguientes varía en función del tamaño determinado de la contraseña: un tamaño de la comprobación de redundancia cíclica asociada a la contraseña, el número máximo de iteraciones, y el número umbral de iteraciones consecutivas.

5. El método de la reivindicación 1, que comprende, además, detectar la presencia de una ráfaga de datos durante un tiempo de transmisión asignado a un terminal de datos del sistema de comunicaciones vía satélite, en el que determinar el tamaño de la contraseña comprende determinar el tamaño de la contraseña incluida en la ráfaga de datos.

6. El método de la reivindicación 5, que comprende, además, determinar que la ráfaga de datos es una ráfaga ficticia transmitida por el terminal de datos durante el tiempo de transmisión asignado, en el que la ráfaga ficticia no incluye contraseñas.

7. Un aparato para decodificar contraseñas de diferentes tamaños, siendo las contraseñas transmitidas por enlaces de comunicación de retorno desde terminales de datos hasta una puerta de enlace de un sistema de comunicaciones vía satélite, comprendiendo el aparato:

   un procesador configurado para determinar un tamaño de una contraseña, y determinar una cola de decodificación particular para decodificar la contraseña en función del tamaño determinado de la contraseña, siendo la cola de decodificación particular una de *K* colas de decodificación, donde *K* es un número de diferentes tamaños de contraseñas; y
   un número de decodificadores en la cola de decodificación particular, estando cada decodificador acoplado de manera comunicativa al procesador y configurado para decodificar la contraseña, en el que el número de decodificadores en la cola de decodificación particular se asigna en proporción a una carga ofrecida actual de contraseñas del tamaño determinado.

8. El aparato de la reivindicación 7, en el que cada uno de los decodificadores está configurado para decodificar iterativamente la contraseña lo que incluye determinar tras cada iteración de decodificación si se pasa una comprobación de redundancia cíclica asociada a la contraseña.

9. El aparato de la reivindicación 8, en el que cada uno de los decodificadores está configurado para decodificar iterativamente la contraseña hasta que se llegue a un número máximo de iteraciones o se pase la comprobación de redundancia cíclica asociada a la contraseña para un número umbral de iteraciones consecutivas.

10. El aparato de la reivindicación 9, en el que una o más de las siguientes varía en función del tamaño determinado de la contraseña: un tamaño de la comprobación de redundancia cíclica asociada a la contraseña, el número máximo de iteraciones, y el número umbral de iteraciones consecutivas.

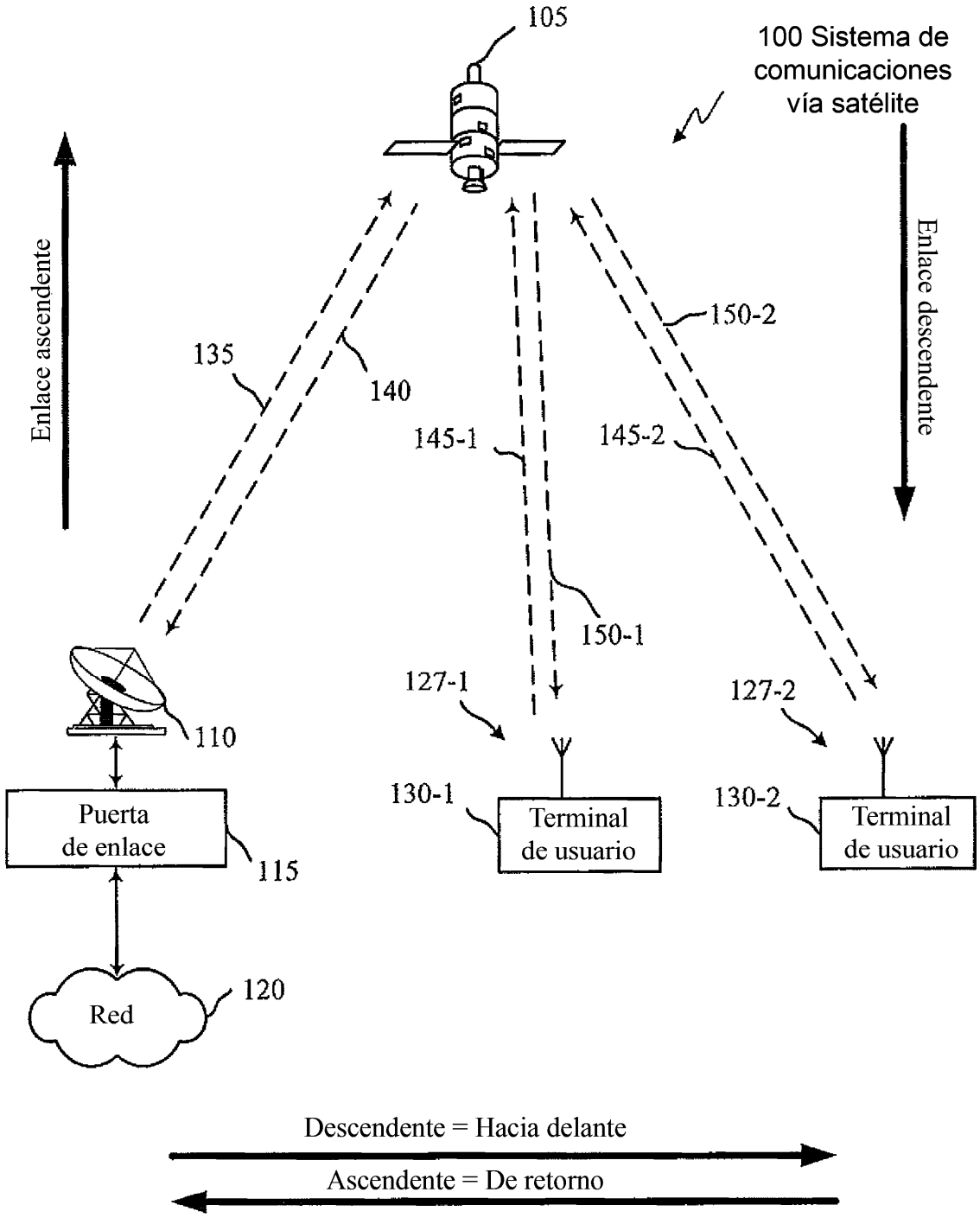
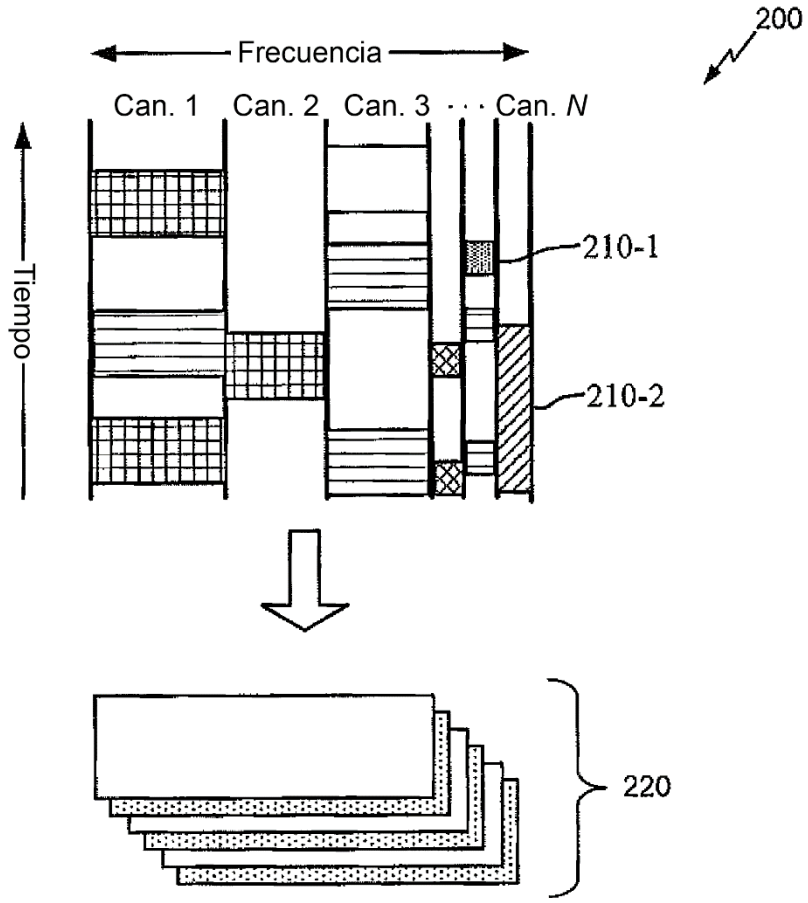
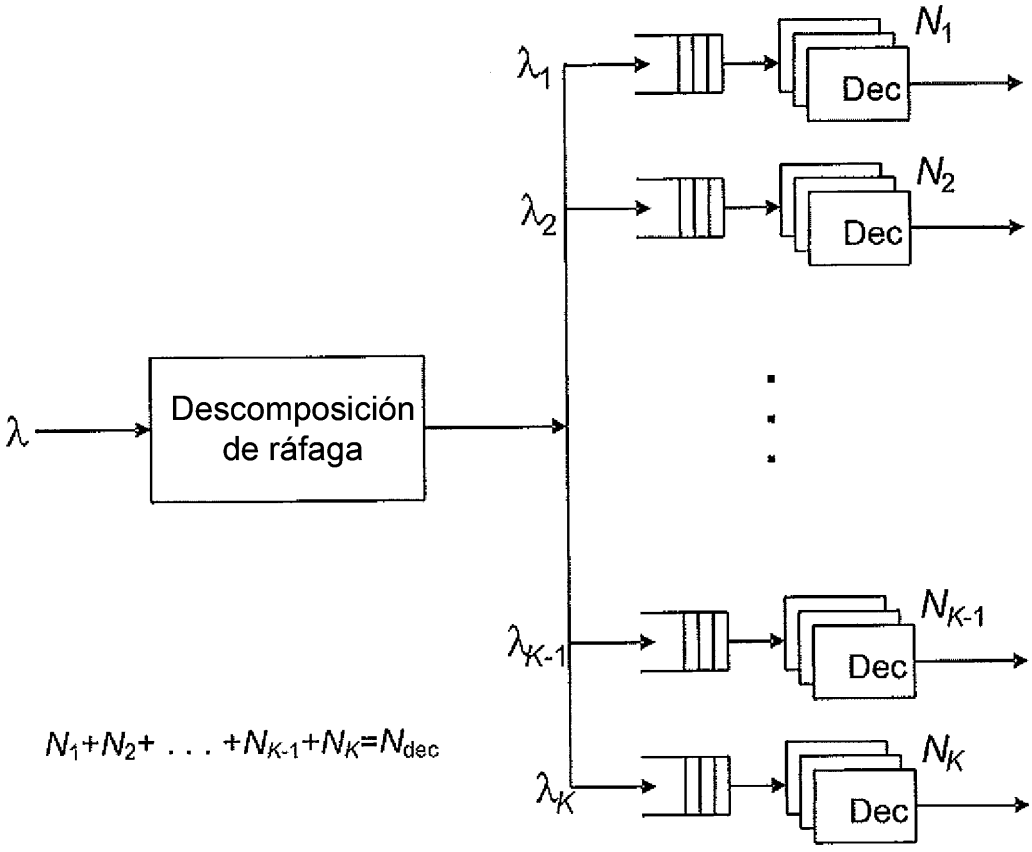

105
100 Sistema de comunicaciones vía satélite
Enlace ascendente
Enlace descendente
135
140
150-2
145-1
145-2
150-1
127-1
127-2
110
130-1
130-2
Terminal de usuario
Terminal de usuario
Puerta de enlace
115
120
Red
Descendente = Hacia delante
Ascendente = De retorno

FIG. 1



Banco de receptores que prestan servicio a múltiples canales de enlace de retorno

FIG. 2



Una cola de decodificadores para cada uno de los *K* tamaños de bloque

FIG. 3

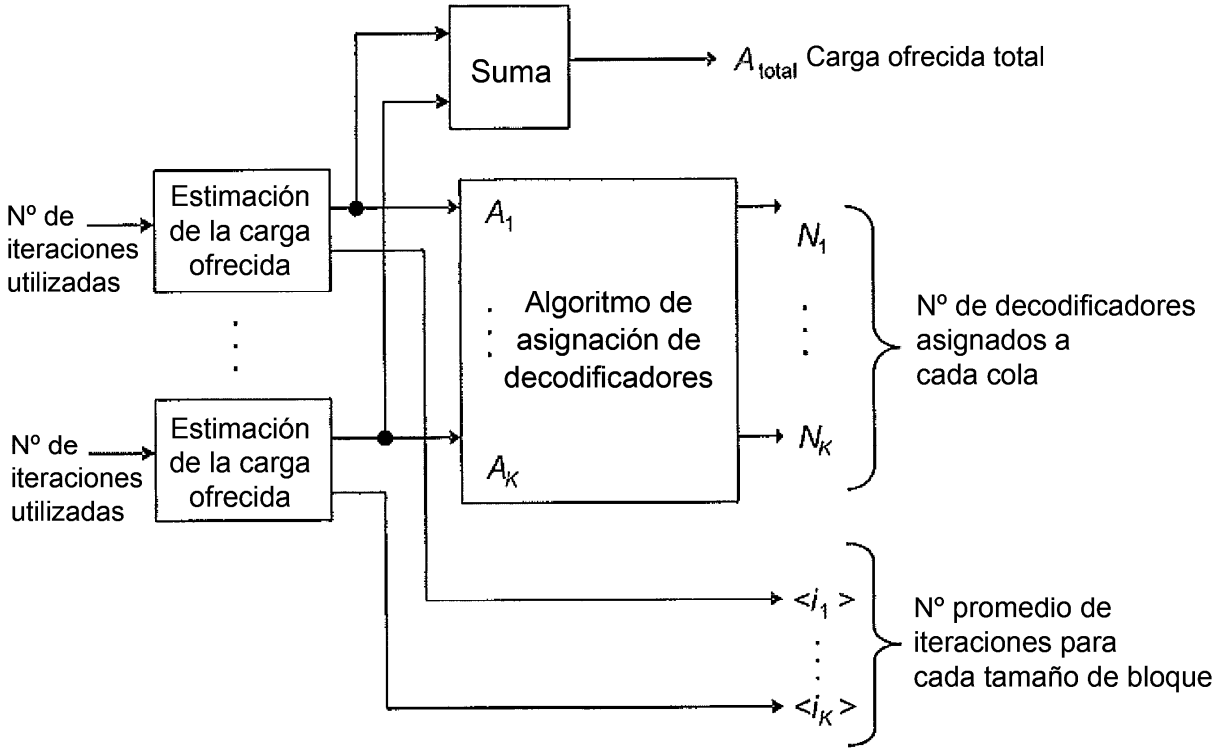

Suma
A_{total} Carga ofrecida total
Nº de iteraciones utilizadas
Estimación de la carga ofrecida
Nº de iteraciones utilizadas
Estimación de la carga ofrecida
A_1
Algoritmo de asignación de decodificadores
A_K
N_1
N_K
Nº de decodificadores asignados a cada cola
$<i_1>$
$<i_K>$
Nº promedio de iteraciones para cada tamaño de bloque
N_{dec} decodificadores a asignar a K colas

FIG. 4

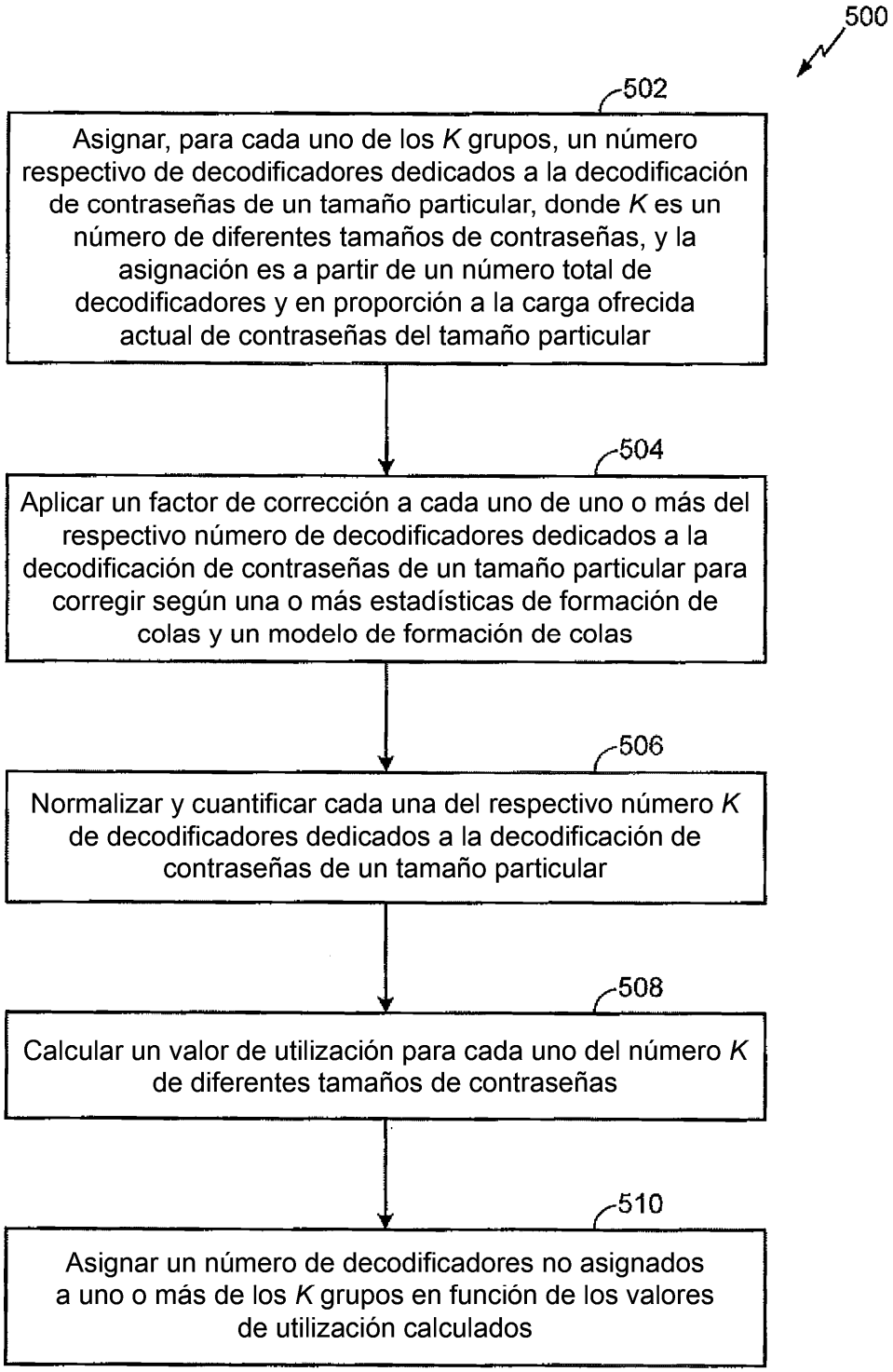

500
502
Asignar, para cada uno de los K grupos, un número respectivo de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular, donde K es un número de diferentes tamaños de contraseñas, y la asignación es a partir de un número total de decodificadores y en proporción a la carga ofrecida actual de contraseñas del tamaño particular
504
Aplicar un factor de corrección a cada uno de uno o más del respectivo número de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular para corregir según una o más estadísticas de formación de colas y un modelo de formación de colas
506
Normalizar y cuantificar cada una del respectivo número K de decodificadores dedicados a la decodificación de contraseñas de un tamaño particular
508
Calcular un valor de utilización para cada uno del número K de diferentes tamaños de contraseñas
510
Asignar un número de decodificadores no asignados a uno o más de los K grupos en función de los valores de utilización calculados

FIG. 5

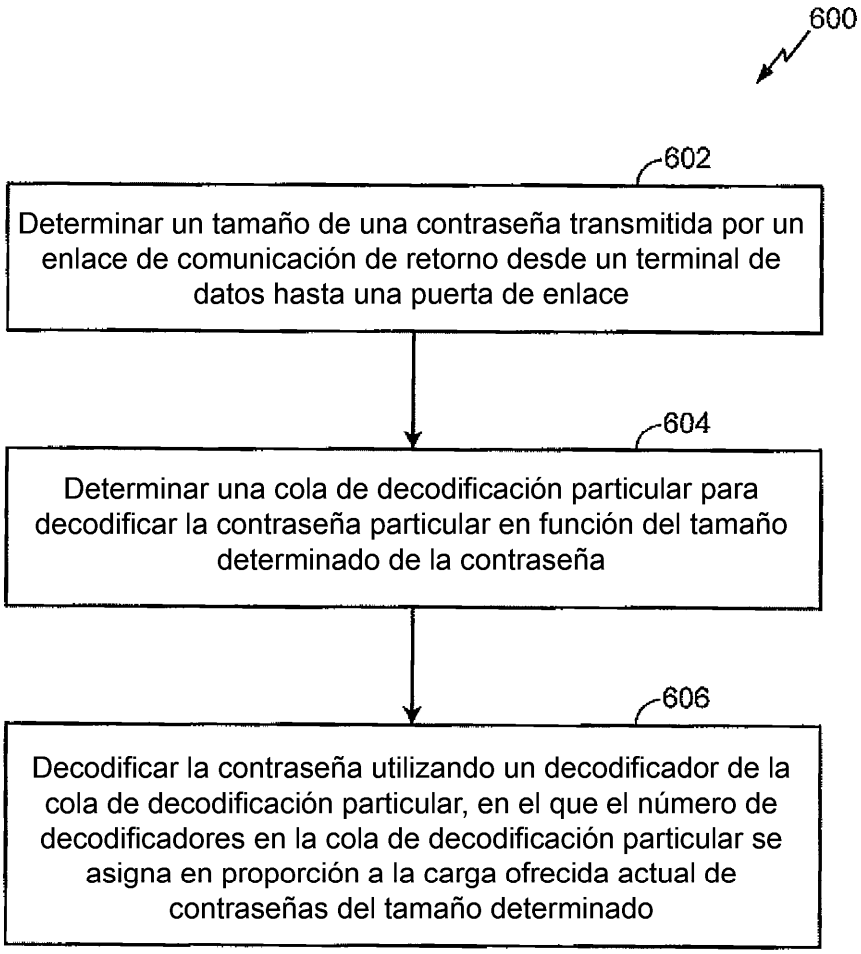

600
602
Determinar un tamaño de una contraseña transmitida por un enlace de comunicación de retorno desde un terminal de datos hasta una puerta de enlace
604
Determinar una cola de decodificación particular para decodificar la contraseña particular en función del tamaño determinado de la contraseña
606
Decodificar la contraseña utilizando un decodificador de la cola de decodificación particular, en el que el número de decodificadores en la cola de decodificación particular se asigna en proporción a la carga ofrecida actual de contraseñas del tamaño determinado

FIG. 6