

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 877 558**

51 Int. Cl.:

H04W 8/00 (2009.01)

H04W 4/70 (2008.01)

H04W 76/14 (2008.01)

H04W 12/00 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **07.10.2014** **PCT/SE2014/051177**

87 Fecha y número de publicación internacional: **16.04.2015** **WO15053698**

96 Fecha de presentación y número de la solicitud europea: **07.10.2014** **E 14793911 (0)**

97 Fecha y número de publicación de la concesión europea: **28.04.2021** **EP 3056056**

54 Título: **Método y disposición para descubrimiento de dispositivo**

30 Prioridad:

07.10.2013 US 201361887648 P

08.10.2013 US 201361888438 P

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
17.11.2021

73 Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)
(100.0%)

164 83 Stockholm, SE

72 Inventor/es:

SORRENTINO, STEFANO

74 Agente/Representante:

LINAGE GONZÁLEZ, Rafael

ES 2 877 558 T3

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

DESCRIPCIÓN

Método y disposición para descubrimiento de dispositivo

5 Campo técnico

La presente divulgación se refiere a métodos y dispositivos para la transmisión de señales de descubrimiento y detección de señales de descubrimiento para la comunicación de dispositivo a dispositivo.

10 Antecedentes

El proyecto de asociación de tercera generación, 3GPP, es responsable de la estandarización del sistema universal de telecomunicaciones móviles, UMTS y evolución a largo plazo, LTE. El trabajo de 3GPP en LTE también se conoce como red de acceso terrestre universal evolucionada, E-UTRAN. LTE es una tecnología para realizar comunicaciones basadas en paquetes de alta velocidad que pueden alcanzar altas velocidades de datos tanto en el enlace descendente como en el enlace ascendente, y se considera un sistema de comunicación móvil de próxima generación en relación con UMTS. Para soportar altas velocidades de datos, LTE permite un ancho de banda del sistema de 20 MHz o hasta 100 MHz cuando se emplea la agregación de portadoras. LTE también puede operar en diferentes bandas de frecuencia y puede operar al menos en los modos dúplex por división de frecuencia, FDD y dúplex por división de tiempo, TDD.

La comunicación de dispositivo a dispositivo es un componente bien conocido y ampliamente usado de muchas tecnologías inalámbricas existentes, incluidas las redes ad hoc y celulares. Los ejemplos incluyen Bluetooth y varias variantes del conjunto de estándares IEEE 802.11, como Wi-Fi Direct. Estos sistemas operan en espectro sin licencia.

Recientemente, las comunicaciones de dispositivo a dispositivo, D2D, como base de las redes celulares se han propuesto como un medio para aprovechar la proximidad de los dispositivos de comunicación y, al mismo tiempo, permitir que los dispositivos funcionen en un entorno de interferencia controlado. Típicamente, se sugiere que dicha comunicación de dispositivo a dispositivo comparte el mismo espectro que el sistema celular, por ejemplo reservando algunos de los recursos celulares de enlace ascendente para fines de dispositivo a dispositivo. La asignación de espectro dedicado para fines de dispositivo a dispositivo es una alternativa menos probable, ya que el espectro es un recurso escaso y el intercambio dinámico entre los servicios de dispositivo a dispositivo y los servicios celulares es más flexible y proporciona una mayor eficiencia del espectro.

Los dispositivos que quieren comunicarse, o incluso simplemente descubrirse entre sí, típicamente necesitan transmitir varias formas de señalización de control. Un ejemplo de tal señalización de control es la denominada señal de descubrimiento, también denominada señal de baliza o señal de baliza de descubrimiento, que al menos transporta alguna forma de identidad, denominada ID D2D en esta divulgación. La señal de descubrimiento posiblemente puede transportar información adicional que es útil para el servicio de descubrimiento y es transmitida por un dispositivo que quiere ser detectable por otros dispositivos.

Otros dispositivos pueden buscar la señal de descubrimiento. Una vez que han detectado la señal de descubrimiento, pueden tomar la acción apropiada, por ejemplo, intentar iniciar una configuración de conexión con el dispositivo que transmite la señal de descubrimiento.

Se puede considerar una carga útil de descubrimiento de referencia de 104 bits de información de descubrimiento más 24 bits de CRC, como valor indicativo, de acuerdo con los supuestos de simulación en RAN1. De las evaluaciones internas, resulta que la ID de D2D podría tener una longitud del orden de 80 bits. La estandarización de D2D está en curso en 3GPP y no hay números más refinados disponibles en el momento de redactar esta divulgación. En esta divulgación, M se refiere al número total de bits de carga útil en una baliza de descubrimiento. Desde la perspectiva de esta divulgación, no es esencial si M incluye los bits CRC o no, si los hubiera.

Un equipo de usuario, UE, que participa en el descubrimiento transmite información de descubrimiento que es potencialmente única en su señal de descubrimiento. Un UE que está intentando descubrir el primer UE intentará extraer la información de descubrimiento de la señal de descubrimiento recibida. Si el segundo UE tiene éxito, llamará al primer UE cuando se descubra.

ProSe (servicios de proximidad; véase el estudio de viabilidad de 3GPP TR 22.803) define dos tipos de descubrimiento: abierto y restringido. Con descubrimiento abierto, al menos en la primera ocasión de descubrimiento, la información de descubrimiento de un UE no se conoce de antemano en el receptor. En este caso, recibir información de descubrimiento es una simple decodificación.

En caso de descubrimiento restringido, el receptor intenta detectar una determinada señal de descubrimiento específica. Y la información de descubrimiento del UE de transmisión se conoce en el receptor antes de intentar el descubrimiento. De acuerdo con una propuesta reciente (documento de contribución 3GPP R1-134627), el receptor

no necesita decodificar con éxito toda la información del descubrimiento, al menos para el descubrimiento restringido. En su lugar, puede realizar lo que se denomina "coincidencia parcial de bits", lo que implica que el receptor solo puede decodificar correctamente algunos de los bits. Se calcula una tasa de error de bit empírica (BER). Si la BER no excede un cierto umbral, entonces el receptor determina que la información de descubrimiento se extrae con éxito y el UE se considera descubierto.

La coincidencia parcial de bits puede dar lugar a una detección falsa. Una razón para la detección falsa es que algunos bits pueden decodificarse erróneamente, lo que podría conducir a una suposición incorrecta de una coincidencia con el conjunto de N bits comparados. R1-134627 sugiere que la probabilidad de detección falsa puede controlarse hasta cierto punto estableciendo apropiadamente el número de bits para que coincidan correctamente. Por otro lado, el aumento de N reduce la eficiencia computacional de la coincidencia parcial de bits. Más allá de la complejidad computacional reducida asociada a la decodificación/detección correcta de N bits en lugar de M, R1-134627 establece que la coincidencia parcial de bits puede proporcionar una mayor probabilidad de detección en un punto operativo SNR dado en comparación con el caso de detección completa. La probabilidad de detección aumenta con un umbral de BER más alto, sin embargo, esto tiene el coste de una mayor probabilidad de detección falsa.

3GPP R2-132520 "Descubrimiento directo D2D - aspectos RAN2 " (agosto de 2013) y el documento JP 2012/095191 A se citaron durante la búsqueda internacional y el examen preliminar internacional.

El documento JP 2012/095191 describe un dispositivo inalámbrico LAN que recibe una trama que incluye información hash generada a partir de un ESSID y una marca de tiempo de un dispositivo inalámbrico LAN homólogo, extrayendo la información hash y la marca de tiempo, creando información hash a partir de la marca de tiempo extraída y ESSID en el propio dispositivo y comprobar el ESSID del dispositivo inalámbrico LAN homólogo comparando la información hash creada y la información hash extraída.

3GPP R2-132520 considera la distinción entre descubrimiento D2D abierto y restringido. En el descubrimiento D2D abierto, un UE D2D detectable puede ser descubierto por cualquier UE D2D en las proximidades sin ningún permiso explícito (por ejemplo, anuncios por tienda). En el descubrimiento D2D restringido, un UE D2D detectable sólo puede ser descubierto por otros UE D2D que están explícitamente permitidos por el UE D2D detectable (por ejemplo, buscar amigos en redes sociales). 3GPP R2-132520 además explica la transmisión transparente y no transparente de la información de descubrimiento D2D y las posibles implicaciones en el trabajo de 3GPP TSG RAN WG2. 3GPP R1-134231 describe el descubrimiento D2D realizado en un procedimiento de dos etapas que incluye firmas de descubrimiento principalmente para detección y sincronización seguidas de canales de descubrimiento para transportar el paquete de descubrimiento codificado a partir de la información del mensaje de descubrimiento.

Sumario

Un objeto de la presente divulgación es proporcionar métodos y dispositivos correspondientes que buscan mitigar, aliviar o eliminar una o más de las deficiencias en la técnica identificadas anteriormente y las desventajas individualmente o en cualquier combinación.

La invención está definida por las reivindicaciones independientes. De acuerdo con algunos aspectos, la divulgación proporciona un método ejecutado en un primer terminal inalámbrico para transmitir una señal de control que permite el descubrimiento de dispositivo a dispositivo, D2D. La señal de control se transmite a través de un canal de datos y transporta una identidad asociada con el primer terminal inalámbrico. El método comprende los siguientes pasos: encriptar, mediante hash de la señal de control, tomar una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada; codificar la señal de control con hash; encriptar la señal codificada usando una secuencia de encriptación que no depende de parámetros específicos del terminal; y transmitir la señal codificada encriptada.

De acuerdo con otra realización, un primer terminal inalámbrico está adaptado para transmitir una señal de control que permite el descubrimiento de dispositivo a dispositivo, D2D. La señal de control transporta la identidad de dispositivo a dispositivo asociada con el primer terminal inalámbrico, el primer terminal inalámbrico comprende la circuitería de procesamiento adaptada para hacer que el terminal inalámbrico encripte la señal de control aplicando hash a la señal de control, tomando una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada; la circuitería de banda base es adaptada para codificar la señal de control con hash y encriptar la señal codificada usando una secuencia de encriptación que no depende de parámetros específicos del terminal; y transmitir la circuitería de transmisión adaptada para transmitir la señal codificada por un canal de datos.

Breve descripción de los dibujos

Lo anterior resultará evidente a partir de la siguiente descripción más particular de las realizaciones de ejemplo, como se ilustra en los dibujos adjuntos en los que los mismos caracteres de referencia se refieren a las mismas partes en todas las diferentes vistas. Los dibujos no están necesariamente a escala, sino que se hace hincapié en ilustrar los ejemplos de realización.

La figura 1 ilustra el procesamiento de enlace descendente de los bloques de transporte LTE.

La figura 2a ilustra el procesamiento de enlace ascendente de los bloques de transporte LTE.

La figura 2b muestra el procedimiento de intercalado/encriptación propuesto (transmisor).

La figura 2c muestra el procedimiento de desintercalado/desenciptación propuesto (receptor).

La figura 3 ilustra un escenario de ejemplo.

Las figuras 4a y 4c ilustran la coincidencia parcial de bits.

La figura 4b ilustra muestras de coincidencia parcial de bits de toda la carga útil de la baliza, con hash.

La figura 5 ilustra un método en un terminal inalámbrico que es un transmisor.

Las figuras 6a y 6b ilustran un método en un terminal inalámbrico que es un receptor.

La figura 7 es un diagrama de señalización y un diagrama de flujo que combina los métodos de las figuras 5 y 6.

Las figuras 8a y 8c ilustran un terminal inalámbrico de ejemplo que es un transmisor.

Las figuras 8b y 8d ilustran un dispositivo inalámbrico de ejemplo que es un receptor.

La figura 9 muestra una variante de un método en un receptor.

La figura 10 ilustra una variante de un método en un terminal inalámbrico que es un transmisor.

Las figuras 11a y 11b ilustran una variante de un método en un terminal inalámbrico que es un receptor.

La figura 12 es un diagrama de señalización y un diagrama de flujo que combina los métodos de las figuras 10 y 11.

La figura 13a ilustra la coincidencia parcial de bits limitada a una fracción de la carga útil de la baliza, sin la solución propuesta.

La figura 13b ilustra escasamente muestras de coincidencia parcial de bits de toda la carga útil de la baliza, con un nuevo intercalador.

La figura 13c ilustra la coincidencia parcial de bits que opera en bits que son una función de toda la carga útil, con el nuevo encriptador.

Abreviaturas

CRC	verificación de redundancia cíclica
D2D	dispositivo a dispositivo
ID de D2D	identidad de dispositivo a dispositivo
BER	tasa de error de bit
NW	red
DMRS	señales de referencia de demodulación
PRB	bloque físico de recursos
UL	enlace ascendente
DL	enlace descendente
UE	equipo de usuario

Descripción detallada

Los aspectos de la presente divulgación se describirán más completamente a continuación con referencia a los dibujos adjuntos. Sin embargo, el aparato y el método divulgados en el presente documento pueden realizarse de muchas formas diferentes y no deben interpretarse como limitados a los aspectos expuestos en el presente documento. Los números similares en los dibujos se refieren a elementos similares en todas partes.

La terminología usada en el presente documento tiene el fin de describir aspectos particulares de la divulgación únicamente, y no pretende limitar la invención. Como se usa en el presente documento, las formas singulares "un", "una", "el" y "la" pretenden incluir las formas plurales también, a menos que el contexto indique claramente lo contrario.

En el contexto de esta divulgación, los términos "terminal inalámbrico" o "dispositivo inalámbrico" abarcan cualquier terminal que pueda comunicarse de forma inalámbrica con otro dispositivo, así como, opcionalmente, con un nodo de acceso de una red inalámbrica, mediante la transmisión y/o recibir señales inalámbricas. Por tanto, el término "terminal inalámbrico" abarca, entre otros: un equipo de usuario, por ejemplo, un UE de LTE, un terminal móvil, un dispositivo inalámbrico fijo o móvil para la comunicación de máquina a máquina, una tarjeta inalámbrica integrada o incrustada, una tarjeta inalámbrica conectada externamente, una llave, etc. A lo largo de esta divulgación, el término "equipo de usuario" se usa a veces para ejemplificar varias realizaciones. Sin embargo, esto no debe interpretarse como una limitación, ya que los conceptos ilustrados en el presente documento son igualmente aplicables a otros terminales inalámbricos. Por lo tanto, siempre que se haga referencia a un "equipo de usuario" o "UE" en esta divulgación, debe entenderse que abarca cualquier terminal inalámbrico como se define anteriormente.

Aunque los siguientes ejemplos se describen en el contexto de la detección de señales de descubrimiento para D2D, los principios descritos en la siguiente divulgación pueden aplicarse igualmente a cualquier problema de detección en el que la secuencia detectada se compare con una secuencia conocida.

Como se describió anteriormente, "coincidencia parcial de bits" puede referirse a un método en el que solo algunos de los bits recibidos necesitan recibirse correctamente.

En un ejemplo, el decodificador parcial considera que el bloque se decodifica correctamente incluso si sólo se decodifica correctamente un subconjunto N del número M de bits. Este puede ser el caso cuando el canal es malo, por ejemplo, debido a la interferencia, lo que implica que solo una parte de la carga útil se decodifica correctamente. Si las señales de descubrimiento candidatas difieren en más de X bits, aún es posible que el receptor detecte el mensaje de descubrimiento correcto entre todos los candidatos incluso si la señal recibida se ha corrompido parcialmente debido a ruido o interferencia.

Otro ejemplo es que el receptor solo compara algunos de los bits de los bits de información decodificados, es decir, un subconjunto N del número M de bits, con la información de descubrimiento conocida y cuenta el número de bits coincidentes. Esto también reduce la complejidad ya que hay menos bits para comparar. Esta solución puede verse como otro tipo de "coincidencia parcial de bits".

Se identifican al menos dos problemas con las propuestas de coincidencia parcial de bits mencionadas anteriormente:

1) Si los subconjuntos de N bits de información de 2 señales de descubrimiento diferentes son idénticos, la coincidencia parcial de bits no puede identificar la secuencia correcta y se produce una detección errónea constante.

2) En principio, dos cargas útiles de señales de descubrimiento pueden diferir solo en un bit. Esto implica que la coincidencia parcial de bits no es aplicable en la práctica, a menos que se impongan restricciones sobre el contenido de las cargas útiles de la señal de descubrimiento. Tales restricciones son ineficientes (requerirían redundancia en la definición de las longitudes de la carga útil) y complicadas de aplicar en despliegues no coordinados.

El primer problema es probable, por ejemplo, si la ID de D2D que puede ocupar ~80% de la carga útil de la señal de descubrimiento incluye identificadores de área que son comunes a múltiples señales de descubrimiento, y $N \ll M$. La parte restante de la carga útil de la señal de descubrimiento también podría incluir información del sistema que es común a muchos UE.

Para el descubrimiento D2D, los UE deben poder descubrir potencialmente cientos o miles de UE en las proximidades. Por lo tanto, la eficiencia de implementación de la solución es de primordial importancia.

Las realizaciones del presente documento comprenden modificar el procedimiento de encriptación y posiblemente intercalado en LTE cuando se transmiten señales de descubrimiento para detección de proximidad, de modo que las señales de descubrimiento con una pequeña diferencia pueden diferenciarse en el lado del receptor. Esto se logra mediante la introducción de una nueva función de encriptación en el receptor, también denominada función de aleatorización. El fin es aumentar la diferencia entre las señales de descubrimiento, incluso cuando las cargas útiles de la señal de descubrimiento difieren en uno o unos pocos bits.

El encriptador se divide en dos partes: un primer encriptador (nuevo) opera sobre los bits de información, mientras que el encriptador existente que opera sobre bits codificados se modifica de manera que la secuencia de encriptación no es una función de los parámetros específicos del UE. De manera similar, se puede agregar un intercalador antes del codificador, lo que conduce a ciertas ventajas de probabilidad de detección. Los pasos correspondientes se realizan en el receptor. Los beneficios de este enfoque son más obvios cuando se aplica al algoritmo de detección parcial de bits que se ha propuesto. Sin embargo, los efectos también se pueden ver en otros casos, por ejemplo, cuando la señal de descubrimiento está distorsionada o es ruidosa.

En la siguiente parte de esta divulgación, el término "encriptación" debe interpretarse en un sentido más amplio siempre que se aplique al nuevo encriptador aplicado antes del codificador de canal, en comparación con la operación de encriptación bit a bit conocida basada en XOR. Como se indica en algunas de las realizaciones, una de las justificaciones para aplicar la encriptación a la carga útil de la señal de descubrimiento es que la versión encriptada de una misma señal de descubrimiento debe ser diferente en diferentes transmisiones de la señal de descubrimiento y deben evitarse colisiones consistentes de diferentes señales de descubrimiento. Por tanto, cualquier función de aleatorización de la carga útil de la señal de descubrimiento que obtenga tal objetivo puede aplicarse de manera equivalente en esta divulgación. La función es una función hash, y otros ejemplos de tales funciones que no entran dentro del alcance de las reivindicaciones son los encriptadores basados en XOR, CRC, codificadores, etc. En las realizaciones, la secuencia de encriptación se define como una función de parámetros que varían en diferentes ocasiones de transmisión para la misma carga útil de la señal de descubrimiento, es decir, cualquier marca de tiempo, o no especificado por las reivindicaciones, por ejemplo, el intervalo de tiempo y/o el índice de recursos usado para la transmisión de la señal de descubrimiento puede explotarse en la generación de la secuencia de encriptación de la señal de descubrimiento. Para que la operación de aleatorización de la carga útil se realice mediante el uso de una función hash (o que no esté incluida en el alcance de las reivindicaciones, un codificador polinomial o un CRC), cualquier marca de tiempo (o no especificado por las reivindicaciones, el intervalo de tiempo y/o el índice de recursos) usado para la transmisión de la señal de descubrimiento puede insertarse en la carga útil de la señal de descubrimiento que se va a aplicar hash, con el fin de obtener una aleatorización que sea una función de la instancia de transmisión de la señal de descubrimiento específica. Por ejemplo, cualquier marca de tiempo (o no especificado por las reivindicaciones, el intervalo de tiempo y/o el índice de recursos) usado para la transmisión de la señal de descubrimiento se puede anteponer o añadir a la carga útil de la señal de descubrimiento antes del hash (o no caer dentro del alcance de las reivindicaciones, codificación polinomial o codificación CRC). Cualquier otro método para obtener la aleatorización de la carga útil de la señal de descubrimiento que se introducirá en el codificador de canal, donde la aleatorización es una función de la instancia de transmisión de la señal de descubrimiento, puede aplicarse de forma equivalente en esta divulgación.

La aleatorización es específica de terminal. Dicho de otra manera, la aleatorización es una función de un parámetro específico del terminal, por ejemplo, no especificado por las reivindicaciones, una identidad D2D o una porción de la misma. Tal parámetro puede aplicarse solo o además de cualquiera de los parámetros mencionados anteriormente.

Los métodos correspondientes deben aplicarse en el receptor para recuperar al menos partes de la carga útil de la señal de descubrimiento original dado el conocimiento de cualquier marca de tiempo (o no especificado por las reivindicaciones, el intervalo de tiempo y/o los parámetros del índice de recursos) usado para aleatorizar la carga útil de señal de descubrimiento en el lado del transmisor.

Se propone aquí abordar los problemas anteriores mediante un procedimiento de encriptación/intercalado modificado en el transmisor y receptor de las señales de descubrimiento. Como línea de base, se considera el procesamiento de canales de datos UL y DL LTE. Aunque los procedimientos descritos aquí se pueden aplicar con técnicas de decodificación convencionales, uno de los beneficios del enfoque descrito en el presente documento es que se puede aplicar a la técnica de coincidencia parcial de bits mencionada anteriormente, mejorando su rendimiento como se describe más adelante.

Para una mejor comprensión de la técnica propuesta, ahora se describirá brevemente el procesamiento de enlace descendente, DL y de enlace ascendente, UL de los bloques de transporte LTE. La figura 1 y la figura 2a muestran, como referencia, el bloque de transporte, es decir, los bits de información, procesados en DL y UL de LTE. Se observa que la encriptación y el intercalado se aplican después del codificador, con el fin de encriptar la interferencia en una combinación de forma específica de célula y específica de UE.

Algunas realizaciones se basan en la constatación de que si las soluciones de la figura 1 o la figura 2a se aplican a la codificación de señales de descubrimiento, esto puede aliviar algunos de los problemas enumerados anteriormente. Esto se puede lograr seleccionando las secuencias de encriptación de modo que sean una función de la información de tiempo (por ejemplo, una marca de tiempo usada para la transmisión de balizas), o no especificadas en las reivindicaciones, el intervalo de tiempo o la carga útil de la señal de descubrimiento, o de índice de recursos de la transmisión de la baliza.

En una realización, esto se logra encriptando, que también puede denominarse aleatorización, comprendiendo la señal de descubrimiento una identidad, usando una función hash que toma una marca de tiempo usada para la transmisión de la señal de descubrimiento como un parámetro de entrada. Como se indicó anteriormente, el hash se considera una forma de encriptar o aleatorizar la carga útil. En el hash, las pequeñas diferencias en los datos de entrada pueden producir diferencias muy grandes en los datos de salida, como se describirá con más detalle a continuación. Cuando el receptor está intentando detectar una señal de descubrimiento específica, para determinar si el transmisor está cerca, aplica el mismo hash que se aplicó en el lado del transmisor a la identidad que intenta detectar. Luego, el receptor realiza la decodificación y luego realiza la coincidencia de bits para determinar si la identidad recibida coincide con la identidad con hash del UE que el receptor estaba intentando detectar. En este punto, se puede realizar ventajosamente una coincidencia parcial de bits, porque el hash puede producir grandes diferencias en los datos de salida incluso para señales con pequeñas diferencias.

En otro ejemplo, la secuencia de encriptación para un determinado UE puede ser una función de la identidad D2D, o una porción de la misma, convirtiendo así la secuencia de encriptación en específica del UE. Cuando el receptor está intentando la detección de una señal de descubrimiento específica, para determinar si el transmisor está cerca, aplica el código de desencriptación específico del UE correspondiente. Después de la desencriptación, el receptor realiza la decodificación y luego realiza la coincidencia de bits para determinar si la identidad recibida coincide con el UE que el receptor estaba intentando detectar. En este punto, se puede realizar ventajosamente una coincidencia parcial de bits, ya que la aplicación del código de desencriptación específico del UE proporciona una protección adicional contra la detección falsa, incluso si el número de bits N usados para la coincidencia parcial es mucho menor que M.

La figura 3 ilustra un escenario de ejemplo en el que pueden operar varias realizaciones descritas en el presente documento. Este ejemplo muestra varios terminales inalámbricos 10, 20, 30 y 40 que son capaces de comunicación D2D. Uno o más de los terminales inalámbricos pueden ser, por ejemplo, equipos de usuario LTE. En este ejemplo, los terminales 30 y 40 ya han establecido comunicación D2D entre sí. El terminal inalámbrico 10 está transmitiendo una señal 12 de descubrimiento (mostrada como un círculo sombreado que rodea al terminal 10), que comprende una identidad del terminal inalámbrico 10. El terminal inalámbrico 20 está lo suficientemente cerca del terminal 10 para poder detectar la señal de descubrimiento. Por supuesto, también pueden estar presentes otros terminales inalámbricos y algunos de estos terminales también pueden estar transmitiendo señales de señal de descubrimiento y/o estar en comunicación D2D con otros terminales. Debe observarse además que los terminales inalámbricos 10 y 20 pueden estar incluidos en una red inalámbrica 100, por ejemplo, una red celular. La red inalámbrica puede ser, por ejemplo, una red LTE o UMTS. En ese caso, uno o más de los terminales inalámbricos 10 y/o 20 pueden estar conectados a la red inalámbrica.

El método reivindicado propone dividir el bloque de desencriptación y/o intercalado en dos bloques. El primer bloque se aplica a los bits de información y el segundo bloque después del codificador (como en 3GPP TS 36.211 V12.3.0 - fig. 5-3.1), que se muestra en la figura 2b. Los pasos correspondientes de desencriptación y/o desintercalado se realizan en el receptor, que se muestra en la figura 2c.

El paso de intercalado aplicado después del codificador puede ser una función de la ID de la célula, el intervalo de tiempo, el índice de recursos o cualquier otro parámetro no específico del UE (a diferencia de LTE). Posiblemente, el intercalador puede ser estático y predefinido.

Por tanto, varias realizaciones del presente documento se basan en el entendimiento de que la decodificación es más exigente desde el punto de vista informático que la desencriptación y/o desintercalado. Estas realizaciones permiten una ventaja computacional significativa en el receptor. Además, estas realizaciones permiten resolver o al menos aliviar los problemas con la propuesta de coincidencia parcial de bits. Desde una perspectiva computacional, estas realizaciones requieren solo una iteración del decodificador.

Con referencia al escenario de la figura 3 y al diagrama de flujo de la figura 5, se describirá ahora un método realizado en un primer terminal inalámbrico 10, por ejemplo, un equipo de usuario LTE, para transmitir una señal de control para habilitar el descubrimiento de dispositivo a dispositivo, D2D, en el que la señal de control transporta una identidad, en el que se realiza la encriptación antes de la codificación. En la figura 5, la señal de descubrimiento se aleatoriza usando una función hash.

Debe apreciarse que la figura 5 comprende algunas operaciones que se ilustran con un borde más oscuro y algunas operaciones que se ilustran con un borde más claro. Las operaciones comprendidas en un borde más oscuro son operaciones comprendidas en la realización de ejemplo más amplia. Las operaciones que están comprendidas en un borde más claro son realizaciones de ejemplo que pueden estar comprendidas, o son una parte, o son operaciones adicionales que pueden tomarse además de las operaciones de las realizaciones de ejemplo de borde. Debe apreciarse que estas operaciones no necesitan realizarse en orden. Además, debe tenerse en cuenta que no es necesario realizar todas las operaciones. Las operaciones de ejemplo se pueden realizar en cualquier orden y en cualquier combinación.

Tanto los bloques de intercalado como los de encriptación pueden introducirse en el transmisor, antes de la codificación. Sin embargo, el concepto divulgado cubre el caso en el que solo se inserta el encriptador y, no dentro del alcance de las reivindicaciones, el caso en el que solo se inserta el intercalador. Tales bloques proporcionan beneficios diferentes y combinables, como se explica en el presente documento. Obviamente, solo los bloques correspondientes deben introducirse en el receptor. El ejemplo de la figura 5 comprende solo un encriptador. En la figura 5, el encriptador se implementa como una función hash.

El paso de encriptación aplicado antes de que el codificador sea inicializado por una entrada o secuencia de encriptación que es una función de la carga útil de la señal de descubrimiento y posiblemente parámetros adicionales que pueden variar en transmisiones sucesivas de la señal de descubrimiento. Por ejemplo, el intervalo de tiempo y el índice de recursos para la transmisión de la señal de descubrimiento pueden ser ejemplos de tales parámetros. La razón es que la versión encriptada de una determinada señal de descubrimiento debe ser diferente

en diferentes transmisiones de señales de descubrimiento y deben evitarse colisiones consistentes de diferentes señales de descubrimiento.

El paso de intercalado aplicado después del codificador puede ser una función de la ID de la célula, el intervalo de tiempo, el índice de recursos o cualquier otro parámetro no específico del UE (a diferencia de LTE). Posiblemente, el intercalador puede ser estático y predefinido.

El primer terminal inalámbrico 10 está configurado para transmitir una señal de descubrimiento, aquí denominada señal de control, que comprende una identidad asociada con el terminal 10. Esto permite que otro terminal inalámbrico, como el terminal 20, descubra la presencia del terminal 10 e inicie comunicaciones de dispositivo a dispositivo con él.

De acuerdo con el método propuesto, el primer terminal inalámbrico 10 encripta S1 la señal de control antes de la codificación, con una secuencia de encriptación que se basa o depende de la identidad asociada con el terminal 10. Dicho de otra manera, la secuencia de encriptación es una función de la identidad del terminal inalámbrico. Dicho de otra manera, la secuencia de encriptación es una función de al menos un parámetro de entrada específico del usuario o específico del terminal.

En algunas realizaciones, la encriptación implica que el dispositivo inalámbrico aplica hash S1 a la señal de control, tomando una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada. La marca de tiempo es, por ejemplo, un formato de fecha y hora y se codificará de acuerdo con el anexo B.2.1.2 de 3GPP TS 33.220 V12.2.0. La señal de control comprende la carga útil de la señal y, de acuerdo con algunos aspectos, el método comprende además insertar S0 la marca de tiempo usada para la transmisión de la señal de control en la carga útil de la señal de control, antes de aplicar hash a la señal de control. La función hash usa una clave hash que es, por ejemplo, específica para un grupo de usuarios restringido.

Las figuras 4a y 4b ilustran que la coincidencia parcial de bits no puede diferenciar señales en las que la carga útil solo difiere en uno de unos pocos bits. En la figura 4a, no todos los bits coinciden. En la figura 4b, tres bits están decodificados incorrectamente, lo que hace que los dos paquetes no se puedan diferenciar.

La figura 4b ilustra que la coincidencia parcial de bits puede diferenciar las señales de descubrimiento de la figura 4a después de aplicar una función hash en las señales de descubrimiento, tomando una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada. En la aplicación de hash, las pequeñas diferencias en los datos de entrada pueden producir grandes diferencias en los datos de salida.

Alternativamente, el parámetro de entrada para la encriptación puede basarse en alguna parte de la porción de la identidad o depender de ella. En una variante particular, la identidad comprende una porción que es compartida por varios terminales inalámbricos (por ejemplo, que comprende un identificador de área u otra información común), y otra porción que es única para el terminal inalámbrico 10, y la secuencia de encriptación se basa o depende de la porción de la identidad que es única para el terminal inalámbrico 10.

En otra alternativa, el parámetro de entrada, por ejemplo, la secuencia de encriptación es una función de la totalidad o una parte de la carga útil de la señal de descubrimiento.

Opcionalmente, el terminal inalámbrico 10 también realiza el intercalado, no mostrado, de la señal de descubrimiento. Si se aplica intercalado, se puede realizar antes y/o después del paso de codificación.

Cuando se realiza el intercalado antes de la codificación, como se muestra en la figura 13, puede basarse en parámetros específicos no terminales (también denominados parámetros comunes), en parámetros específicos del terminal, o en una combinación de ambos. Sin embargo, cuando el intercalado se realiza después de la codificación, el intercalado no debe basarse preferiblemente en parámetros específicos del terminal, ya que el receptor tendría que realizar el paso de decodificación varias veces.

De acuerdo con el método, el terminal inalámbrico 10 entonces codifica S2 la señal de descubrimiento, es decir, la señal de control con hash. Por tanto, en esta realización la codificación se realiza después de realizar una encriptación específica del terminal. Un beneficio de este enfoque es que permite una detección eficiente de la señal de descubrimiento en el lado del receptor, ya que no se requerirá que el receptor decodifique la señal varias veces.

El terminal inalámbrico 10 luego transmite S4 la señal de descubrimiento, permitiendo el descubrimiento por otros dispositivos y potencialmente también el inicio de la comunicación D2D con tales dispositivos.

En algunas variantes, se puede realizar opcionalmente un paso de encriptación adicional S3 después de codificar S2 (y antes de la transmisión S4). Por lo tanto, la señal de descubrimiento se encripta con una segunda secuencia de encriptación que no depende de ningún parámetro específico del terminal, o dicho de otra manera, no se basa ni depende de la identidad del terminal, o dicho de otra manera, no se basa ni depende de la carga útil de la señal de

descubrimiento. En cambio, la segunda secuencia de encriptación puede basarse en parámetros comunes, por ejemplo, el intervalo de tiempo y/o el índice de recursos de la transmisión de la señal de descubrimiento.

5 En otras variantes, el intercalado se puede realizar antes y después de la codificación. En este caso, el paso de intercalado realizado después de la codificación se basa preferiblemente solo en parámetros no específicos del terminal, con el fin de mantener el beneficio de una detección más eficiente en el lado del receptor. El paso de intercalado realizado antes de la codificación puede basarse en parámetros específicos del terminal y potencialmente también en parámetros comunes.

10 El correspondiente procedimiento de detección, no especificado por las reivindicaciones, se ejemplifica en la figura 6a. El receptor realiza la descriptación/desintercalado de acuerdo con la secuencia de encriptación no específica de baliza/inicialización de intercalado. La secuencia resultante se decodifica solo una vez. Una vez que se realiza la detección, el receptor itera múltiples intentos de detección usando la lista de UE potencialmente próximos.

15 En un ejemplo, en cada intento de detección, los bits decodificados se comparan con la hipótesis intercalada y/o encriptada de acuerdo con el intercalador y/o el encriptador definido en esta divulgación.

20 En otra alternativa de implementación, en cada intento de detección, los bits decodificados se desintercalan y se descriptan de acuerdo con el intercalador y/o el encriptador definido en esta divulgación y se comparan con la carga útil de la baliza de hipótesis.

Son posibles combinaciones de los ejemplos anteriores, por ejemplo, si el desintercalador no es específico del UE, puede aplicarse directamente después del decodificador evitando iterarlo.

25 En un ejemplo, se puede realizar un intento de detección para cada uno de los UE potencialmente próximos.

En otro ejemplo, los intentos de detección se detienen tan pronto como un intento de detección basado en uno de los UE potencialmente en las proximidades tiene éxito.

30 En un ejemplo adicional, el paso de detección se puede realizar de acuerdo con la técnica de coincidencia parcial de bits. En este caso, solo N de M bits se decodifican y se comparan con los bits esperados. Puede considerarse un umbral de BER distinto de cero para declarar que la detección de la baliza se ha realizado correctamente. La comparación se puede realizar de forma equivalente en los bits de información encriptados o intercalados.

35 Con referencia al escenario de la figura 3 y al diagrama de flujo de la figura 6a, se describirá ahora un método realizado en un segundo terminal inalámbrico 20, por ejemplo, un equipo de usuario LTE, para descubrir un primer terminal inalámbrico 10, en el que el segundo terminal inalámbrico está configurado con un conjunto de una o más identidades de terminales inalámbricos con los que es posible la comunicación de dispositivo a dispositivo, D2D. Este es el método del lado del receptor correspondiente al método que se muestra en la figura 5.

40 El terminal inalámbrico 20 recibe S11 o detecta la presencia de una señal de control. La señal de control es una señal de descubrimiento transmitida desde el terminal 10. Esta señal de descubrimiento comprende una identidad asociada con el terminal 10. El terminal inalámbrico está configurado con una lista (o un conjunto) de una o más identidades de terminales inalámbricos para los que es posible la comunicación D2D. Esta lista puede, por ejemplo, ser configurada por la red inalámbrica 100 o por algún otro medio. De acuerdo con algunos aspectos, la identidad comprende una identidad del terminal inalámbrico 10. De acuerdo con algunos aspectos, la identidad comprende una identidad de usuario ProSe y/o una identidad de usuario de la capa de aplicación.

50 Opcionalmente, el terminal inalámbrico descripta S12 la señal usando una secuencia de descriptación no específica del terminal. Esta opción se aplica si el transmisor realizó un paso de encriptación correspondiente no específico del terminal.

55 A continuación, el terminal inalámbrico decodifica S13 la señal. Por supuesto, la decodificación debe realizarse de manera que se invierta la codificación realizada por el transmisor. Los parámetros de decodificación a usar pueden, por ejemplo, ser preconfigurados por referencia a un estándar técnico, o puede configurarse mediante señalización, por ejemplo, de la red 100.

60 Opcionalmente, se realiza el desintercalado de la señal, si el transmisor realizó un paso de intercalado correspondiente.

En el receptor, la identidad que el receptor está intentando hacer coincidir se encripta S14 (potencialmente junto con información adicional incluida en la carga útil de la señal de descubrimiento) y, opcionalmente, se intercala si el transmisor aplicó intercalado. En este ejemplo, la codificación se implementa como una función hash.

65 Por tanto, en la realización de ejemplo que usa hash, este paso implica aplicar hash S14 a una señal de control de referencia que comprende una de una o más identidades, tomando una marca de tiempo usada para la transmisión

de la señal de control como un parámetro de entrada. Luego, la señal de descubrimiento recibida se compara S15 con la información encriptada (y opcionalmente intercalada) para determinar si hay una coincidencia. Los pasos S14 y S15 se realizan para cada identidad hasta que se hayan comparado todas las identidades del conjunto o hasta que se encuentre una coincidencia.

5 En otras palabras, la detección se puede lograr desenscriptando/desintercalando la información recibida o, a la inversa, encriptando/intercalando los datos con los que se va a comparar la información recibida.

10 La figura 7 ilustra cómo el método del lado del transmisor de la figura 6 puede interactuar con el método del lado del receptor de la figura 5.

Una ventaja de aplicar una secuencia de encriptación específica del usuario, o específica del terminal, como se muestra en las figuras 5-7, es que cuando se aplica una coincidencia parcial de bits, el riesgo de detección falsa como se describe anteriormente se minimiza o al menos se reduce.

15 Las variaciones de la técnica reivindicada se describirán ahora con referencia a las figuras 9-12.

20 En una alternativa de implementación no especificada en las reivindicaciones, mostrada en la figura 9, en cada intento de detección S11, los bits decodificados se desintercalan y se desenscriptan S12 de acuerdo con el intercalador y/o encriptador definido en esta divulgación y se comparan con la carga útil de la baliza de hipótesis.

25 Como en el ejemplo de la figura 6b, el terminal inalámbrico 20 luego decodifica S13 la señal. Por supuesto, la decodificación debe realizarse de manera que se invierta la codificación realizada por el transmisor. Qué parámetros de decodificación usar pueden, por ejemplo, ser preconfigurados por referencia a un estándar técnico, o puede configurarse mediante señalización, por ejemplo, desde la red inalámbrica 100.

Opcionalmente, se realiza el desintercalado de la señal, si el transmisor realizó un paso de intercalado correspondiente S12.

30 Para determinar si la baliza detectada corresponde a uno de los terminales inalámbricos conocidos para los que está habilitada la comunicación D2D, el terminal inalámbrico 20 intenta repetidamente desenscriptar S14b y hacer coincidir S15b la señal de baliza recibida con identidades conocidas de la lista, hasta que se encuentre una coincidencia o hasta que no haya más identidades conocidas para probar. También es posible que el terminal siga probando identidades conocidas incluso después de encontrar una coincidencia, para reducir aún más el riesgo de detección falsa. En particular, en esta realización no es necesario repetir el paso de decodificación, porque el transmisor realizó una encriptación específica del terminal antes del paso de codificación (véase la figura 5). Si el intercalado específico del terminal se realizó en el lado del transmisor, como se describirá en la figura 10, el paso de desintercalado tendrá que repetirse para cada identidad que se va a probar.

40 El terminal inalámbrico 20 desenscripta la señal usando una secuencia de desenscriptación específica del terminal que se basa o depende de una de las identidades conocidas en su lista. Por supuesto, la secuencia de desenscriptación debería seleccionarse para deshacer la encriptación que se realizó en el lado del transmisor, por lo que todas las alternativas descritas en relación con la figura 5 para obtener la secuencia de encriptación se aplican mutatis mutandis.

45 El conocimiento de cómo seleccionar la secuencia de desenscriptación puede, por ejemplo, codificarse en un estándar técnico, o posiblemente indicarse al terminal inalámbrico 20, por ejemplo, desde la red inalámbrica 100.

50 El terminal inalámbrico 20 determina entonces si la señal de baliza, o más específicamente la carga útil de la baliza correspondiente a la identidad del terminal inalámbrico 20, coincide con la identidad conocida (la misma identidad que se aplicó en el paso de desenscriptación). Esto se puede realizar haciendo una coincidencia completa de bits, o ventajosamente mediante una coincidencia parcial de bits de un subconjunto N de los M bits que componen la identidad, como se ha descrito anteriormente.

55 Suponiendo que la lista de terminales conocidos incluye la identidad del terminal inalámbrico 10, es decir, que el método de la figura 15 dé como resultado una coincidencia, el terminal inalámbrico 20 puede entonces proceder a iniciar o configurar las comunicaciones D2D con el terminal inalámbrico 10.

60 Se señala que aunque nuestro ejemplo sugirió que se realizara la encriptación antes del intercalado, el orden de estos pasos puede invertirse en algunas realizaciones. El orden de los pasos de desenscriptación y desintercalado en el lado del receptor se modificará entonces en consecuencia de modo que la desenscriptación se realice antes del paso de desintercalado. Sin embargo, esto también implica que tanto la desenscriptación como el desintercalado deben reiterarse para cada identidad que el receptor intente hacer coincidir.

65 Otro método de ejemplo ejecutado en un terminal inalámbrico 10, por ejemplo, un equipo de usuario LTE, se describirá ahora con referencia a la figura 3 y al diagrama de flujo que se muestra en la figura 10. En este ejemplo, el

nuevo encriptador S3b (que corresponde a ambos pasos S1 y S3 en la Figura 5) se implementa después del codificador S2b.

5 El terminal inalámbrico 10 está configurado para transmitir una señal de descubrimiento que comprende una identidad asociada con el terminal inalámbrico 10. Esto permite que otro terminal inalámbrico, como el terminal inalámbrico 20, descubra la presencia del terminal inalámbrico 10 e inicie comunicaciones de dispositivo a dispositivo con él.

10 De acuerdo con el método, el terminal inalámbrico 10 codifica S2 la señal de descubrimiento. El terminal inalámbrico 10 encripta entonces S3b la señal con una secuencia de encriptación que se basa o depende de la identidad asociada con el terminal inalámbrico 10. Dicho de otra manera, la secuencia de encriptación es una función de la identidad del terminal inalámbrico 10. Dicho de otra manera, la secuencia de encriptación es una función de al menos un parámetro de entrada específico del usuario o específico del terminal.

15 Alternativamente, no especificado en las reivindicaciones, la secuencia de encriptación puede basarse en o depender de alguna parte de porción de la identidad. En una variante particular, la identidad comprende una porción que es compartida por varios terminales inalámbricos (por ejemplo, que comprende un identificador de área u otra información común), y otra porción que es única para el terminal inalámbrico 10, y la secuencia de encriptación se basa o dependiendo de la porción de la identidad que es única para el terminal inalámbrico 10.

20 En una alternativa adicional, no especificada en las reivindicaciones, la secuencia de encriptación es una función de la totalidad o una parte de la carga útil de la baliza.

Opcionalmente, el terminal inalámbrico 10 también realiza el intercalado S35b de la señal de baliza.

25 A continuación, el terminal inalámbrico 10 transmite la señal de baliza, lo que permite el descubrimiento por otros dispositivos.

30 Un método correspondiente, no especificado en las reivindicaciones, realizado en un terminal inalámbrico en el lado de recepción, por ejemplo, el terminal inalámbrico 20 de la figura 3 se describirá ahora con referencia al diagrama de flujo de la figura 11b.

35 El terminal inalámbrico recibe, o detecta S11c la presencia de una señal de baliza desde el terminal inalámbrico 10. El terminal inalámbrico está configurado con una lista de una o más identidades de terminales inalámbricos con los que es posible la comunicación D2D (o, dicho de otra manera, terminales inalámbricos con los que el terminal inalámbrico 10 puede o está habilitado para establecer comunicación D2D). Esta lista puede, por ejemplo, ser configurada por la red inalámbrica 100 o por algún otro medio.

40 Opcionalmente, el terminal inalámbrico desintercala S115c la señal. Esta opción se aplica si se realizó un paso de intercalado S35 correspondiente en el transmisor (véase la figura 10).

45 Para determinar si la baliza detectada corresponde a uno de los terminales inalámbricos conocidos para los que está habilitada la comunicación D2D, el terminal inalámbrico intenta repetidamente decodificar S13c y hacer coincidir S15c la señal de baliza recibida con identidades conocidas de la lista, hasta que se encuentra una coincidencia o no hay más identidades conocidas para probar. También es posible que el terminal siga probando identidades conocidas incluso después de encontrar una coincidencia, para reducir aún más el riesgo de detección falsa.

50 El terminal inalámbrico 20 descripta S14c la señal usando una secuencia de descriptación que se basa o depende de una de las identidades conocidas en su lista. Por supuesto, la secuencia de descriptación debe seleccionarse para deshacer la encriptación que se realizó en el lado del transmisor, por lo que se aplican las mismas alternativas que se describen junto con la figura 10.

55 El conocimiento de cómo seleccionar la secuencia de descriptación puede, por ejemplo, codificarse en un estándar técnico, o posiblemente indicarse al terminal inalámbrico 20, por ejemplo, desde la red inalámbrica 100.

A continuación, el terminal inalámbrico 20 intenta decodificar la señal. Una vez más, la decodificación debe realizarse, por supuesto, de manera que se invierta la codificación realizada por el transmisor.

60 El terminal inalámbrico 20 determina entonces si la señal de baliza, o más específicamente la carga útil de la baliza correspondiente a la identidad del terminal inalámbrico, coincide con la identidad conocida (la misma identidad que se aplicó en el paso de descriptación). Esto se puede realizar haciendo una coincidencia completa de bits, o ventajosamente mediante una coincidencia parcial de bits de un subconjunto N de los M bits que componen la identidad, como se ha descrito anteriormente.

Suponiendo que la lista de terminales conocidos incluya la identidad del terminal inalámbrico 10, es decir, que el método de la figura 12 dé como resultado una coincidencia, el terminal inalámbrico 20 puede entonces proceder a iniciar o configurar las comunicaciones D2D con el terminal inalámbrico 10.

- 5 La figura 12 es un diagrama de señalización combinado y un diagrama de flujo que muestra cómo pueden interactuar los métodos de la figura 10 (transmisor) y la figura 11b (receptor).

- 10 Los métodos de la figura 10-12 se pueden aplicar en particular en un escenario donde el número posible de otros dispositivos, por ejemplo, los UE, que pueden ser detectados por un receptor son limitados, o se indican de manera diferente, cuando la lista de identidades conocidas que el terminal inalámbrico 20 que está configurado para intentar decodificar es razonablemente corta.

- 15 Sin embargo, un posible inconveniente de esta solución es que el receptor necesita realizar un intento de decodificación para cada UE potencialmente en las proximidades. Suponiendo que el receptor pueda tener en cualquier momento una lista de cientos o miles de UE potencialmente próximos, la complejidad computacional inducida por tantos intentos de decodificación podría ser excesiva. El procedimiento de detección, no especificado en las reivindicaciones, se ejemplifica en la figura 11a.

- 20 La figura 8a ilustra un terminal inalámbrico de ejemplo en el que se puede implementar cualquiera de los métodos de la figura 2b, 5 o 10.

- 25 De acuerdo con una realización, se proporciona un dispositivo inalámbrico 10 que comprende medios adaptados para encriptar una señal de descubrimiento con una secuencia de encriptación específica del terminal, para codificar la señal de descubrimiento y para transmitir la señal de descubrimiento. En algunas variantes, encriptar implica aplicar hash a la señal de control, tomando una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada. En algunas variantes, el dispositivo inalámbrico es un equipo de usuario. El dispositivo inalámbrico puede adaptarse además para realizar cualquiera de los pasos del método descritos en relación con la figura 2b, 5 o 10.

- 30 En una realización particular, ilustrada en la figura 8a, el dispositivo inalámbrico comprende una circuitería 103 de banda base adaptada para encriptar la señal de descubrimiento con una secuencia de encriptación específica del terminal, y para codificar la señal de descubrimiento. El dispositivo inalámbrico comprende además una circuitería 102 de transmisión, típicamente un transmisor de radio, Rf, adaptado para transmitir la señal de descubrimiento. La circuitería de transmisión puede estar asociada con una o más antenas físicas por las que se transmite la señal de descubrimiento. En algunas variantes, el dispositivo inalámbrico puede comprender además un procesador 101 y una memoria 104. En algunas variantes, el procesador está adaptado para aplicar hash a la señal de control, tomando una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada.

- 40 En otra realización particular, ilustrada en la figura 8c, el dispositivo inalámbrico 10 comprende un encriptador adaptado para encriptar la señal de descubrimiento con una secuencia de encriptación específica del terminal, y un codificador adaptado para codificar la señal de descubrimiento. En algunas variantes, el encriptador está adaptado para aplicar hash a la señal de control, tomando una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada. El dispositivo inalámbrico puede comprender opcionalmente un intercalador adaptado para intercalar la señal de descubrimiento. El encriptador, codificador e intercalador se pueden proporcionar en una unidad de procesamiento de banda base. La unidad de procesamiento de banda base puede ser la circuitería de banda base que se muestra en la figura 8a.

- 50 El dispositivo inalámbrico puede comprender además una unidad de transmisión adaptada para transmitir la señal de descubrimiento, por ejemplo, a través de la circuitería de transmisión y la antena que se muestran en la figura 8a.

- 55 De acuerdo con un aspecto que no se reivindica, se proporciona un programa informático que comprende instrucciones que, cuando se ejecutan en al menos un procesador (por ejemplo, el procesador mostrado en la figura 8a), hacen que al menos dicho procesador lleve a cabo el método descrito en relación con cualquiera de las figuras 2b, 5 o 10.

- De acuerdo con un aspecto no reivindicado, se proporciona una portadora que contiene el programa informático descrito en el párrafo anterior. La portadora puede ser una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por computadora.

- 60 La figura 8b ilustra un dispositivo inalámbrico 20 de ejemplo en el que se puede implementar cualquiera de los métodos de la figura 2c, 6, 9 u 11. El dispositivo inalámbrico 20 está adaptado para descubrir el primer terminal inalámbrico, en el que el segundo terminal inalámbrico está adaptado con un conjunto de una o más identidades de terminales inalámbricos con los que es posible la comunicación de dispositivo a dispositivo, D2D.

- 65 De acuerdo con un aspecto no especificado en las reivindicaciones, se proporciona un dispositivo inalámbrico que comprende medios adaptados para almacenar un conjunto de una o más identidades de terminales inalámbricos con

los que es posible la comunicación de dispositivo a dispositivo, para recibir una señal de descubrimiento, para descryptar la señal de descubrimiento recibida con una secuencia de descryptación que se basa en una identidad seleccionada del conjunto, para decodificar la señal de descubrimiento y para determinar si la señal decodificada coincide con la identidad seleccionada. Alternativamente, se proporciona un dispositivo inalámbrico que comprende medios adaptados para almacenar un conjunto de una o más identidades de terminales inalámbricos con los que es posible la comunicación de dispositivo a dispositivo, para recibir una señal de descubrimiento, para decodificar la señal de descubrimiento, para encriptar una identidad seleccionada del conjunto, y para determinar si la señal decodificada coincide con la identidad seleccionada encriptada. De acuerdo con algunos aspectos, descryptar una identidad seleccionada implica la aplicación de hash a una señal de control de referencia que comprende una de una o más identidades, tomando una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada.

En algunas variantes, el dispositivo inalámbrico es un equipo de usuario. El dispositivo inalámbrico puede adaptarse además para realizar cualquiera de los pasos del método descritos en relación con las figuras 2c, 6, 9 u 11.

En un aspecto particular no especificado en las reivindicaciones, ilustrado en la figura 8b, el dispositivo inalámbrico puede comprender una circuitería de recepción adaptada para recibir la señal de descubrimiento. El dispositivo inalámbrico puede comprender además una circuitería 203 de banda base adaptada para encriptar una identidad (o para descryptar la señal de descubrimiento con la secuencia de descryptación) y para decodificar la señal de descubrimiento. Alternativamente, la descryptación o encriptación se realiza en una circuitería 201 de procesamiento. De acuerdo con algunos aspectos, la circuitería 203 de banda base o la circuitería 201 de procesamiento está adaptada para aplicar hash a una señal de control de referencia que comprende una de una o más identidades, tomando una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada y para comparar la señal de salida del hash con la señal decodificada, para cada identidad hasta que se hayan seleccionado todas las identidades del conjunto o hasta que se encuentre una coincidencia.

La circuitería 202 de recepción puede estar asociada con una o más antenas físicas a través de las cuales se recibe la señal de descubrimiento. El dispositivo inalámbrico puede comprender además una memoria 204 adaptada para almacenar un conjunto de una o más identidades de terminales inalámbricos con los que es posible la comunicación de dispositivo a dispositivo. En algunas variantes, el dispositivo inalámbrico puede comprender además un procesador.

En otro aspecto particular no especificado en las reivindicaciones, ilustrado en la figura 8d, el dispositivo inalámbrico puede comprender un descryptador adaptado para descryptar la señal de descubrimiento (o para encriptar una señal de control de referencia que comprende una de una o más identidades), y un decodificador adaptado para decodificar la señal de descubrimiento. Además, el dispositivo inalámbrico 20 puede comprender una unidad de recepción adaptada para recibir la señal de descubrimiento. El dispositivo inalámbrico también puede comprender medios para almacenar el conjunto de una o más identidades en una unidad de almacenamiento. El dispositivo inalámbrico puede comprender opcionalmente un desintercalador adaptado para desintercalar la señal de descubrimiento. El descryptador, decodificador y desintercalador pueden proporcionarse en una unidad de procesamiento de banda base. La unidad de procesamiento de banda base puede ser la circuitería de banda base que se muestra en la figura 8b. La unidad de almacenamiento puede ser la memoria que se muestra en la figura 8b.

De acuerdo con otra realización, se proporciona un programa informático que comprende instrucciones que, cuando se ejecutan en al menos un procesador (por ejemplo, el procesador mostrado en la figura 8b), hacen que al menos dicho procesador lleve a cabo el método descrito en relación con cualquiera de las figuras 2c, 6, 9 u 11.

De acuerdo con otra realización más, se proporciona una portadora que contiene el programa informático descrito en el párrafo anterior. La portadora puede ser una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por computadora.

A la luz de las realizaciones presentadas anteriormente, los problemas asociados con la coincidencia parcial de bits pueden resolverse o al menos aliviarse cuando se realiza el intercalado y/o la encriptación antes de la codificación. Más detalladamente, se incluyen las ventajas de tales métodos. La figura 13a ilustra que sin la solución propuesta, la coincidencia parcial de bits se limita a una fracción de la carga útil de la baliza.

Si se proporciona un intercalador antes del codificador (y el desintercalador correspondiente en el receptor) de acuerdo con las realizaciones del presente documento, los bits de información se distribuyen pseudoaleatoriamente de manera que se muestrean diferentes porciones de la carga útil de información en los N bits seleccionados para la coincidencia parcial de bits, reduciendo la probabilidad de detección falsa. Por ejemplo, la ID de D2D puede comprender una parte de identificador de área geográfica que es común a múltiples señales de descubrimiento. Si los N bits se extraen de dicho campo, la detección sería ambigua. Por otro lado, el intercalador propuesto aquí asegura que los campos dentro de la señal de descubrimiento se muestrean pseudoaleatoriamente. La figura 13b ilustra que con el intercalador propuesto, la coincidencia parcial de bits muestrea la carga útil completa de la baliza escasamente.

Si se introduce un encriptador antes del codificador (y un desencriptador correspondiente en el receptor) de acuerdo con las realizaciones del presente documento, la probabilidad de una detección falsa de la señal de descubrimiento consistente puede minimizarse o al menos reducirse. Se supone, en algunas realizaciones, que la secuencia de encriptación es una combinación de la carga útil de la señal de descubrimiento y otros parámetros (por ejemplo, índice de intervalo de tiempo, índice de recursos, etc.) que varían en diferentes transmisiones periódicas de la misma señal de descubrimiento. Por lo tanto, se minimiza la probabilidad de que N bits encriptados de dos señales de descubrimiento diferentes coincidan en recepciones de señales de descubrimiento consecutivas. La figura 13c ilustra que con el encriptador propuesto, la coincidencia parcial de bits opera en bits que son una función de toda la carga útil.

Si la secuencia de encriptación es una función de toda la carga útil de la señal de descubrimiento, o al menos de la porción de la carga útil que corresponde a la identidad D2D (o una fracción significativa de la misma), las ventajas de la solución de intercalador se pueden obtener introduciendo solo el encriptador.

Los aspectos de la divulgación se describen con referencia a los dibujos, por ejemplo, diagramas de bloques y/o diagramas de flujo. Se entiende que varias entidades en los dibujos, por ejemplo, bloques de los diagramas de bloques, y también combinaciones de entidades en los dibujos, pueden implementarse mediante instrucciones de programa informático, cuyas instrucciones pueden almacenarse en una memoria legible por computadora y también cargarse en una computadora u otro aparato de procesamiento de datos programable. Tales instrucciones de programas informáticos se pueden proporcionar a un procesador de una computadora de propósito general, una computadora de propósito especial y/u otro aparato de procesamiento de datos programable para producir una máquina, de modo que las instrucciones, que se ejecutan a través del procesador de la computadora y/u otro aparato de procesamiento de datos programable, crean medios para implementar las funciones/actos especificados en los diagramas de bloques y/o el bloque o bloques del diagrama de flujo.

En algunas implementaciones y de acuerdo con algunos aspectos de la divulgación, las funciones o pasos indicados en los bloques pueden ocurrir fuera del orden indicado en las ilustraciones operativas. Por ejemplo, dos bloques mostrados en sucesión pueden de hecho ejecutarse sustancialmente al mismo tiempo o los bloques a veces pueden ejecutarse en orden inverso, dependiendo de la funcionalidad/actos involucrados. Además, las funciones o pasos anotados en los bloques pueden, de acuerdo con algunos aspectos de la divulgación, ejecutarse continuamente en un bucle.

En los dibujos y la especificación, se han divulgado aspectos de ejemplo de la divulgación. Sin embargo, se pueden realizar muchas variaciones y modificaciones a estos aspectos sin apartarse sustancialmente de los principios de la presente divulgación. Por tanto, la divulgación debe considerarse ilustrativa en lugar de restrictiva, y no limitada a los aspectos particulares explicados anteriormente. Por consiguiente, aunque se emplean términos específicos, se usan únicamente en un sentido genérico y descriptivo y no con fines de limitación.

Cabe señalar que, aunque se ha usado en el presente documento la terminología de 3GPP LTE para explicar las realizaciones de ejemplo, esto no debe verse como una limitación del alcance de las realizaciones de ejemplo a solo el sistema mencionado anteriormente. Otros sistemas inalámbricos, incluidos WCDMA, WiMax, UMB y GSM, también pueden beneficiarse de las realizaciones de ejemplo divulgadas en el presente documento.

La descripción de las realizaciones de ejemplo proporcionadas en el presente documento se ha presentado con fines ilustrativos. La descripción no pretende ser exhaustiva o limitar las realizaciones de ejemplo a la forma precisa divulgada, y son posibles modificaciones y variaciones a la luz de las enseñanzas anteriores o pueden adquirirse de la práctica de diversas alternativas a las realizaciones proporcionadas. Los ejemplos explicados en el presente documento se eligieron y describieron con el fin de explicar los principios y la naturaleza de varias realizaciones de ejemplo y su aplicación práctica para permitir que un experto en la técnica utilice las realizaciones de ejemplo de diversas maneras y con diversas modificaciones según se adapten al uso particular contemplado.

Cabe señalar que la expresión "que comprende" no excluye necesariamente la presencia de otros elementos o pasos distintos de los enumerados y las palabras "un" o "una" que preceden a un elemento no excluyen la presencia de una pluralidad de tales elementos. Cabe señalar además que los signos de referencia no limitan el alcance de las reivindicaciones, que las realizaciones de ejemplo pueden implementarse al menos en parte por medio de hardware y software, y que varios "medios", "unidades" o "dispositivos" puede estar representado por el mismo elemento de hardware.

Aunque la descripción se da principalmente para un equipo de usuario, como unidad de medición o registro, los expertos en la técnica deben entender que "equipo de usuario" es un término no limitativo que significa cualquier dispositivo inalámbrico, terminal o nodo capaz de recibir en DL y transmitir en UL (por ejemplo, PDA, portátil, móvil, sensor, relé fijo, relé móvil o incluso una estación base de radio, por ejemplo, femtoestación base).

Las diversas realizaciones de ejemplo descritas en el presente documento se describen en el contexto general de los pasos o procesos del método, que pueden implementarse en un aspecto mediante un producto de programa informático, incorporado en un medio legible por computadora, que incluye instrucciones ejecutables por

computadora, tales como código de programa, ejecutado por computadoras en entornos en red. Un medio legible por computadora puede incluir dispositivos de almacenamiento extraíbles y no extraíbles que incluyen, entre otros, memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM), discos compactos (CD), discos versátiles digitales (DVD), etc. Generalmente, los módulos de programa pueden incluir rutinas, programas, objetos, componentes, estructuras de datos, etc. que realizan tareas particulares o implementan tipos de datos abstractos particulares. Las instrucciones ejecutables por computadora, las estructuras de datos asociadas y los módulos de programa representan ejemplos de código de programa para ejecutar pasos de los métodos divulgados en el presente documento. La secuencia particular de tales instrucciones ejecutables o estructuras de datos asociadas representa ejemplos de actos correspondientes para implementar las funciones descritas en tales pasos o procesos.

En los dibujos y la especificación, se han divulgados realizaciones de ejemplo. Sin embargo, se pueden realizar muchas variaciones y modificaciones a estas realizaciones. En consecuencia, aunque se emplean términos específicos, se usan en un sentido genérico y descriptivo únicamente y no con fines de limitación, estando definido el alcance de las realizaciones por las siguientes reivindicaciones.

REIVINDICACIONES

- 1.- Un método ejecutado en un primer terminal inalámbrico (10) para transmitir una señal de control que permite el descubrimiento de dispositivo a dispositivo, D2D, en el que la señal de control se transmite a través de un canal de datos y transporta una identidad asociada con el primer terminal inalámbrico, comprendiendo el método los siguientes pasos:
 - encriptación, mediante la aplicación de hash (S1) a la señal de control, tomando una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada;
 - codificar (S2) la señal de control con hash;
 - encriptación (S3) de la señal codificada usando una secuencia de encriptación que no depende de parámetros específicos del terminal; y
 - transmitir (S4) la señal codificada encriptada.
- 2.- El método de acuerdo con la reivindicación 1, en el que la identidad comprende una identidad del primer terminal inalámbrico (10).
- 3.- El método de acuerdo con la reivindicación 1 o 2, en el que la identidad comprende una porción que es compartida por varios terminales inalámbricos.
- 4.- El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que la señal de control comprende la carga útil de la señal y en el que el método comprende además insertar (S0) la marca de tiempo usada para la transmisión de la señal de control en la carga útil de la señal de control, antes de aplicar hash a la señal de control.
- 5.- Un primer terminal inalámbrico (10) adaptado para transmitir una señal de control que permite el descubrimiento de dispositivo a dispositivo, D2D, en el que la señal de control transporta la identidad de dispositivo a dispositivo asociada con el primer terminal inalámbrico, comprendiendo el primer terminal inalámbrico (10):
 - circuitería (101) de procesamiento adaptada para hacer que el terminal inalámbrico encripte (S1) la señal de control mediante la aplicación de hash a la señal de control, tomando una marca de tiempo usada para la transmisión de la señal de control como un parámetro de entrada;
 - circuitería (103) de banda base adaptada para codificar (S2) la señal de control con hash y encriptar (S3) la señal codificada usando una secuencia de encriptación que no depende de parámetros específicos del terminal; y
 - circuitería (102) de transmisión adaptada para transmitir (S4) la señal codificada por un canal de datos.
- 6.- El primer terminal inalámbrico (10) de acuerdo con la reivindicación 5, en el que la identidad comprende una identidad del primer terminal inalámbrico 10.
- 7.- El primer terminal inalámbrico (10) de acuerdo con la reivindicación 5 o 6, en el que la identidad comprende una identidad de usuario ProSe y/o una identidad de usuario de la capa de aplicación.
- 8.- El primer terminal inalámbrico (10) de acuerdo con cualquiera de las reivindicaciones 5 a 7, en el que la señal de control comprende la carga útil de la señal y en el que la circuitería de procesamiento está además adaptada para insertar la marca de tiempo usada para la transmisión de la señal de control en la carga útil de la señal de control, antes de la aplicación de hash a la señal de control.
- 9.- El terminal inalámbrico de acuerdo con cualquiera de las reivindicaciones 5 a 8, en el que el primer terminal inalámbrico es un equipo de usuario.

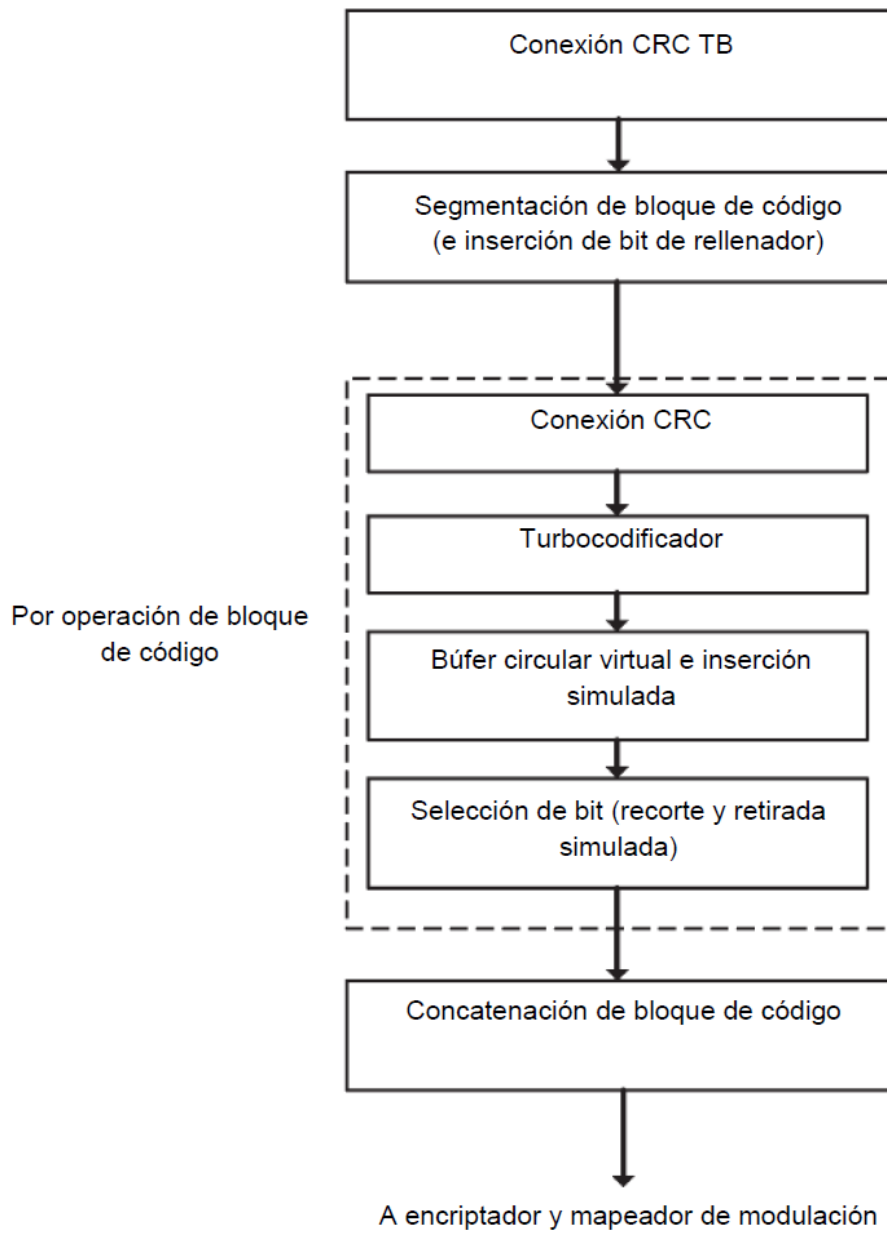


FIG.1

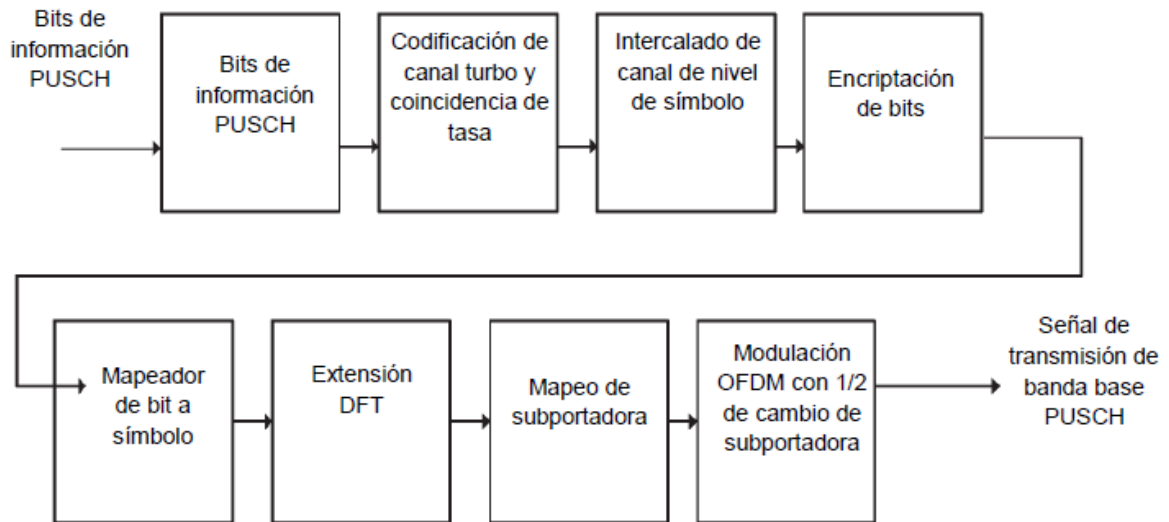


FIG.2a

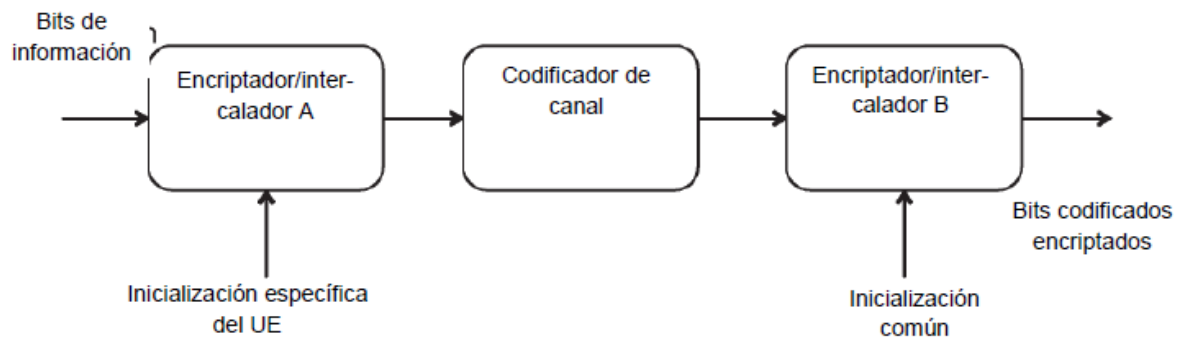


FIG.2b

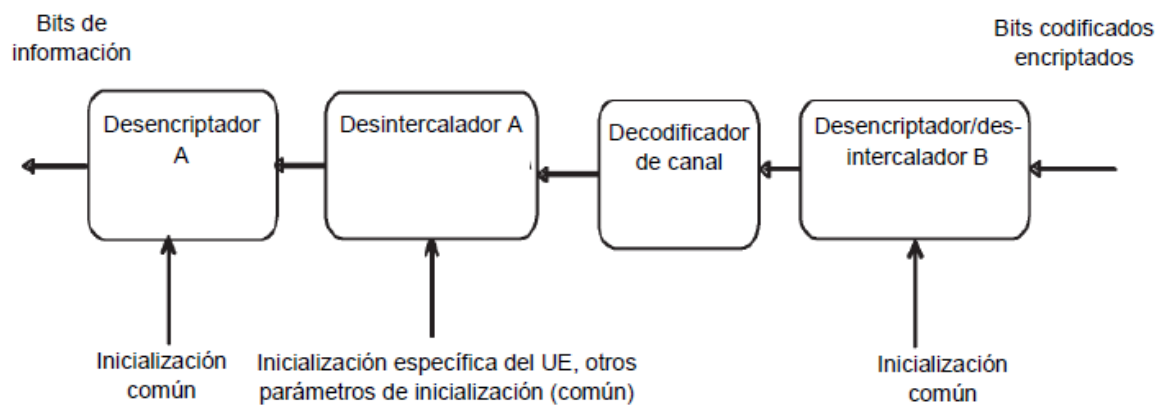


FIG.2c

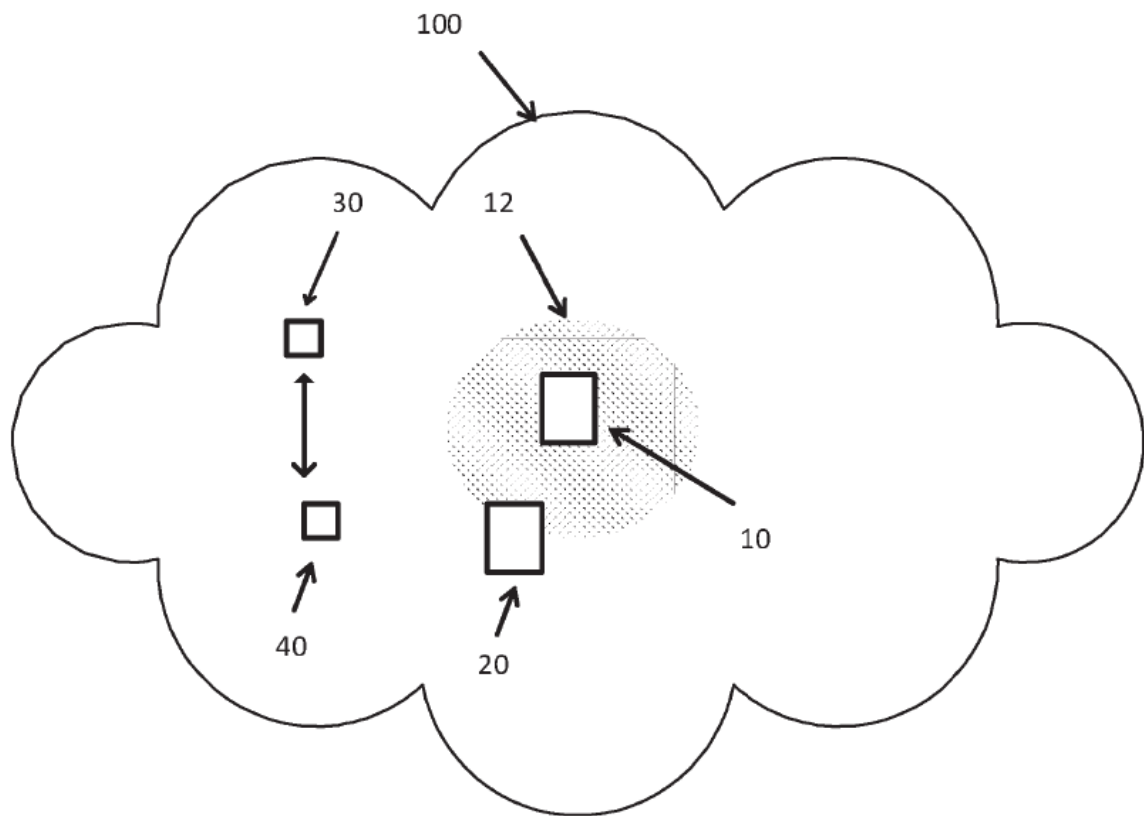


FIG.3

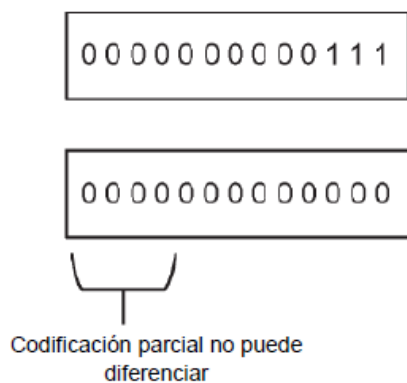


FIG.4a

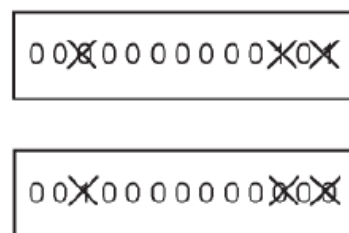


FIG.4c

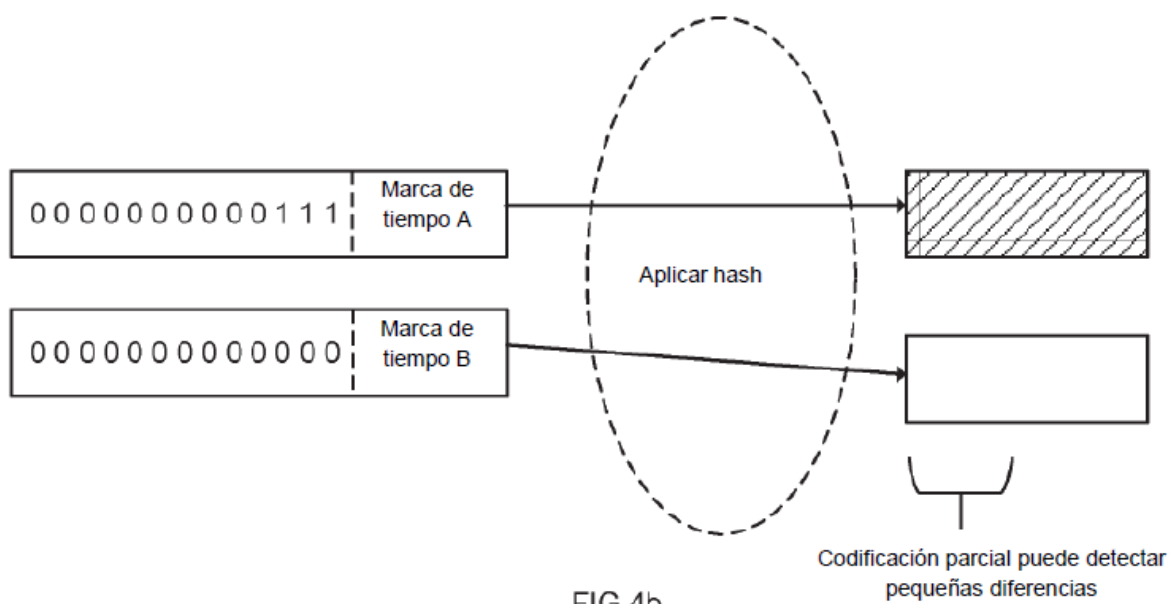


FIG.4b

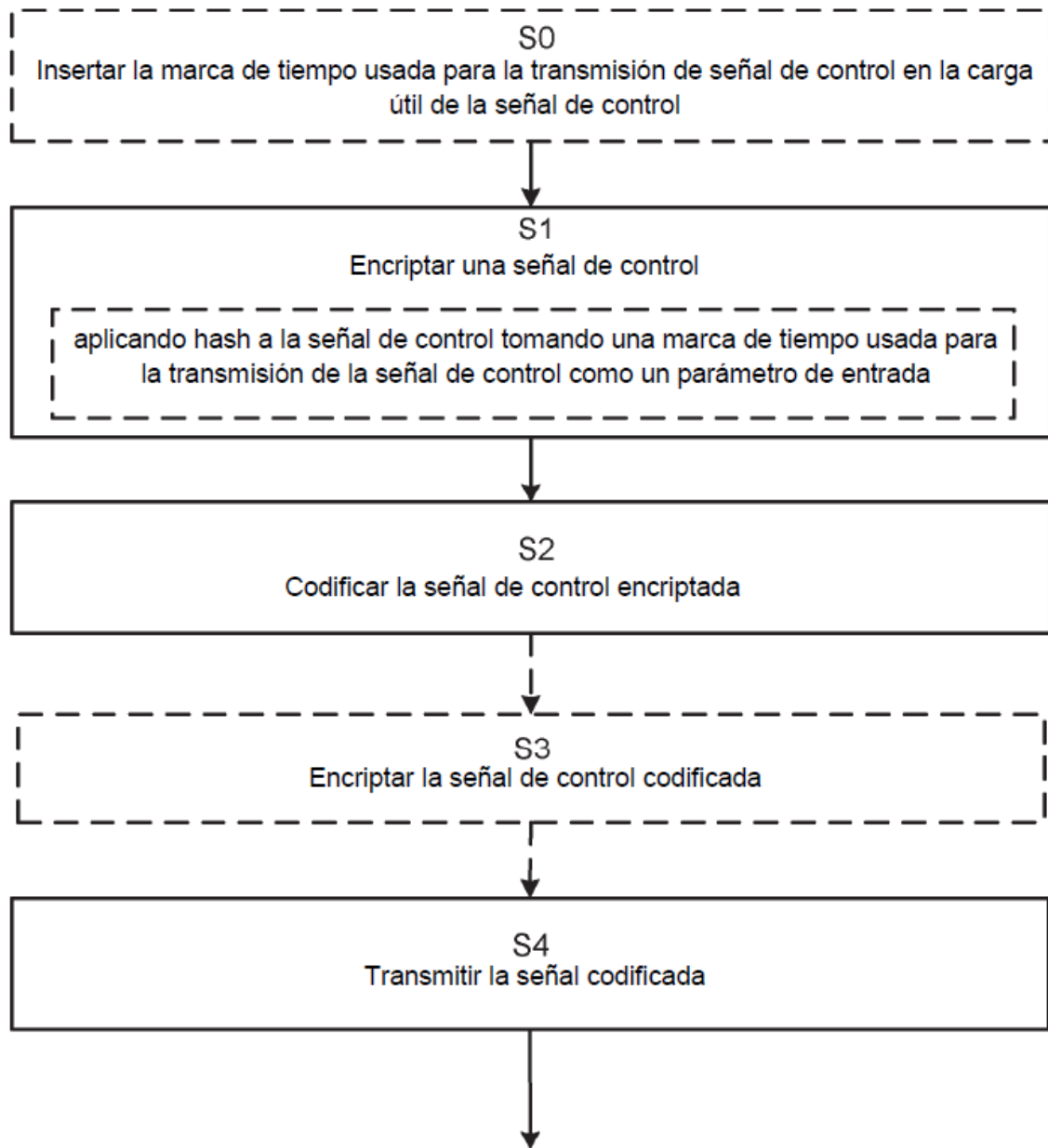


FIG.5

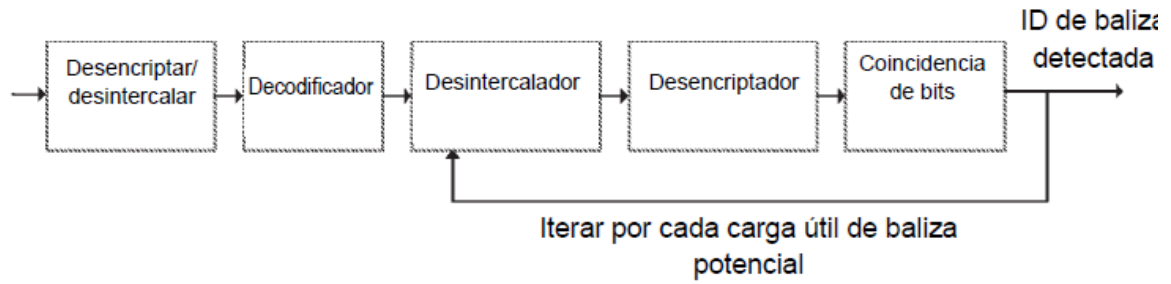


FIG.6a

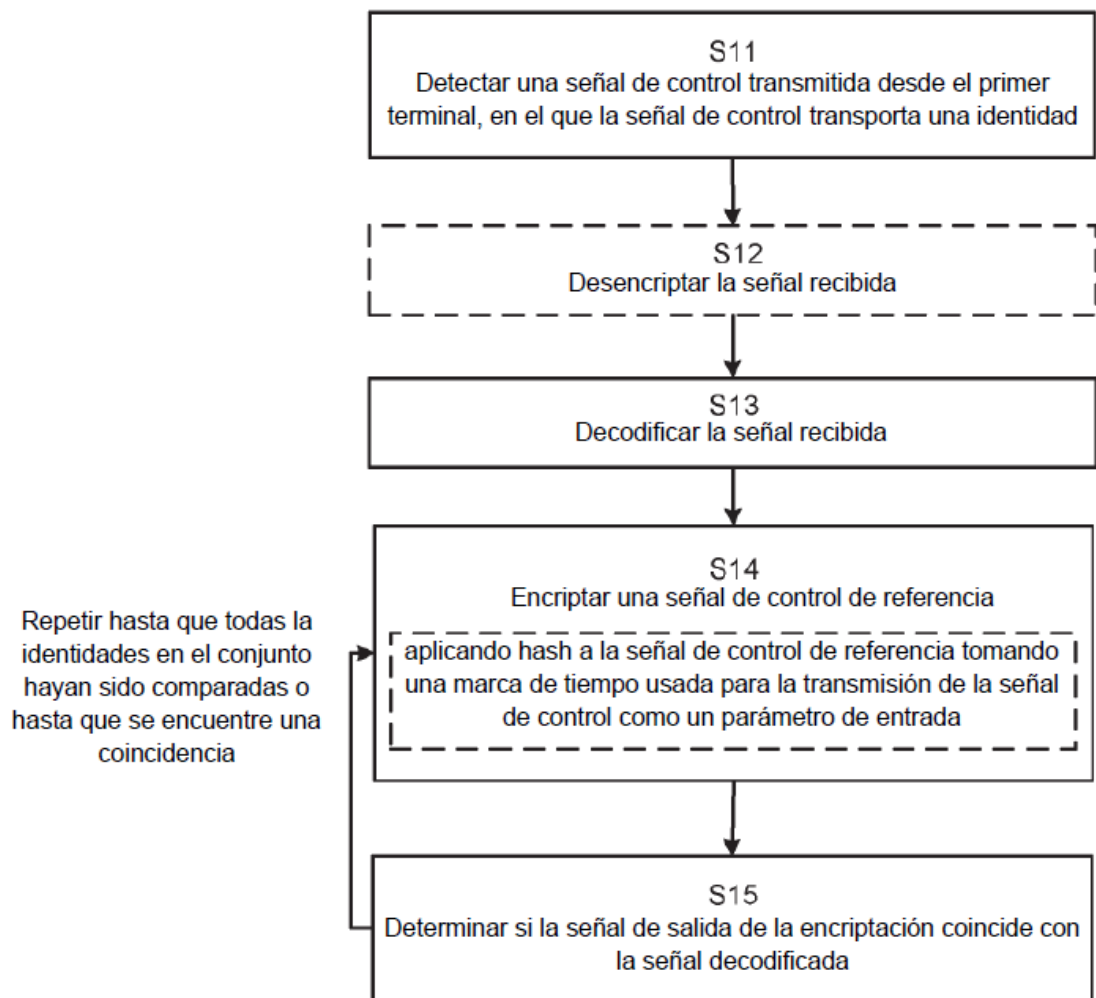


FIG.6b

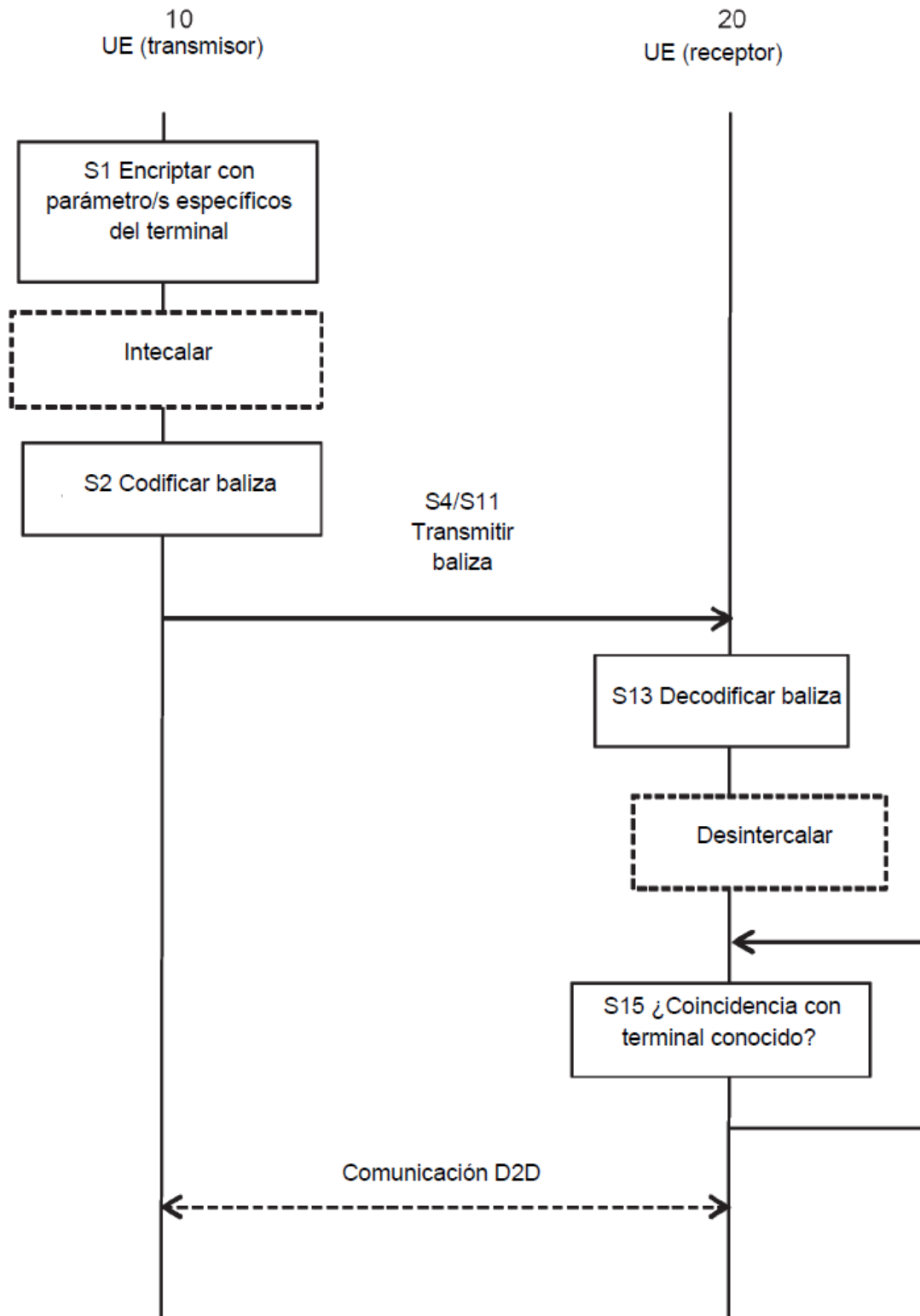


FIG.7

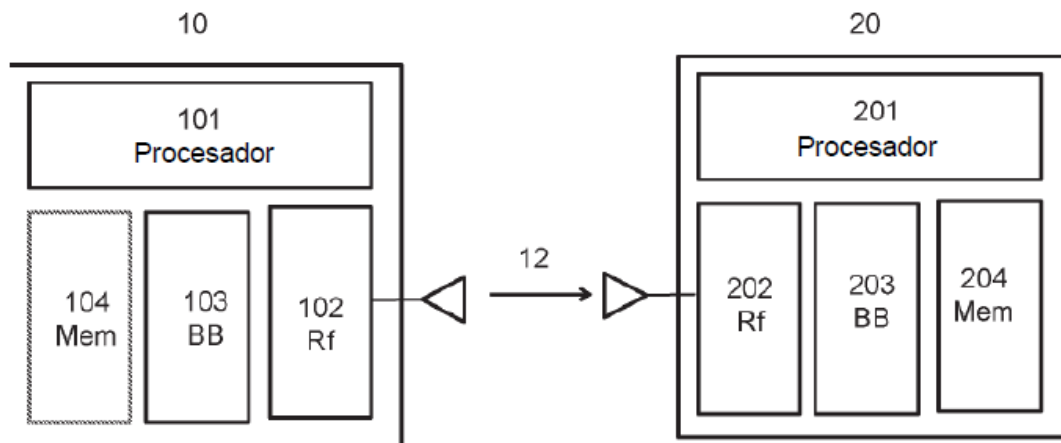


FIG. 8a

FIG. 8b

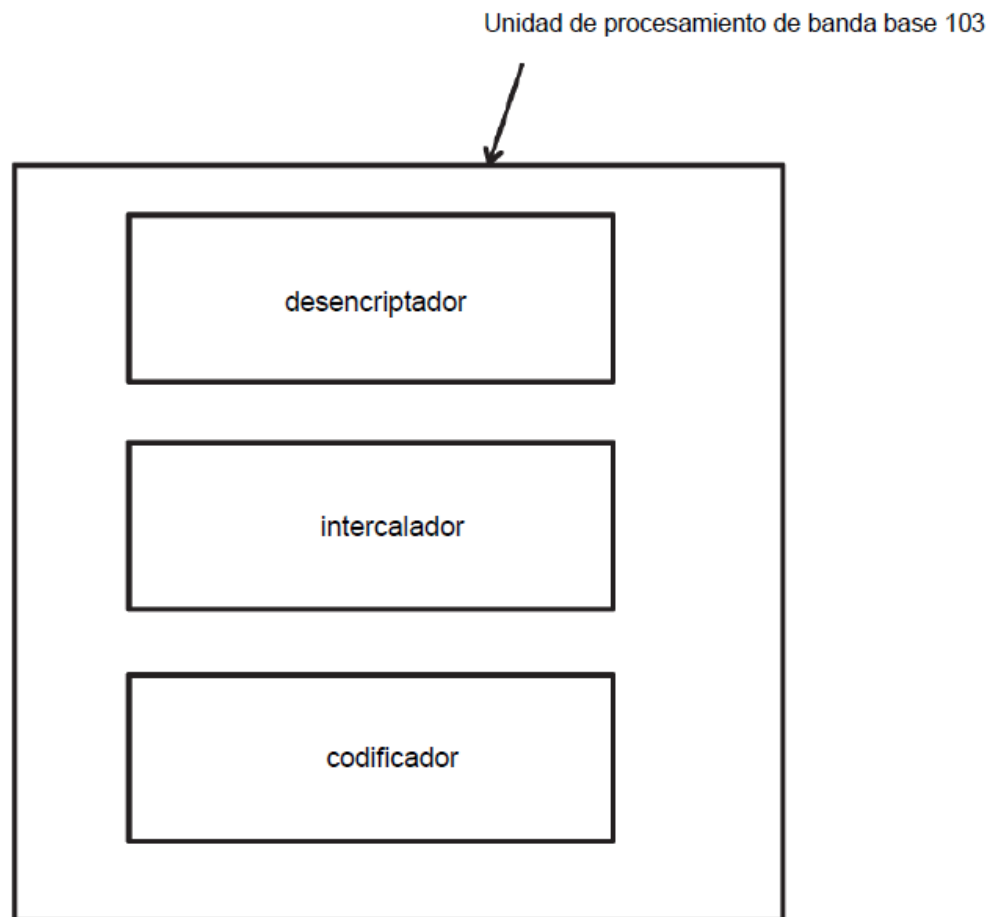


FIG. 8c

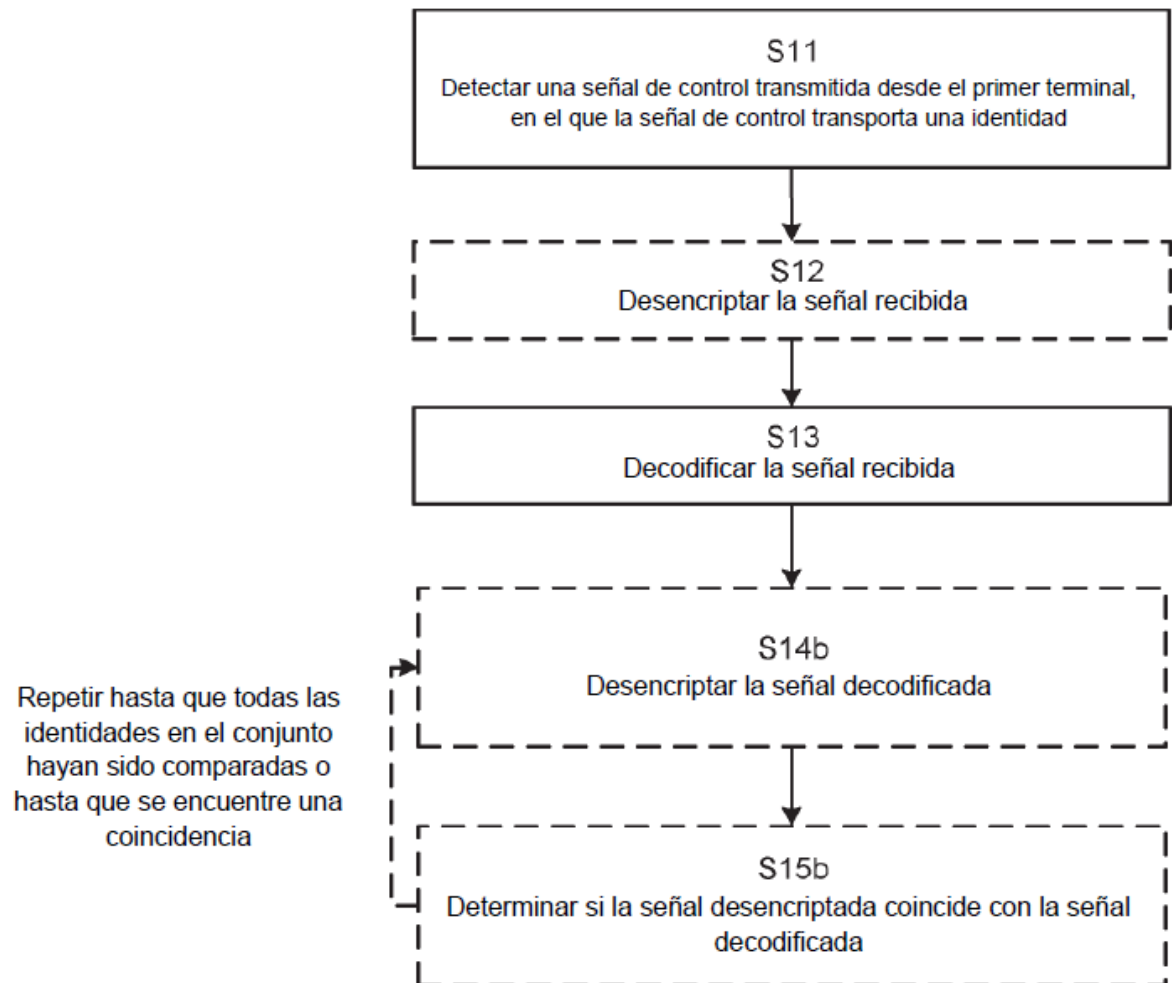


FIG. 9

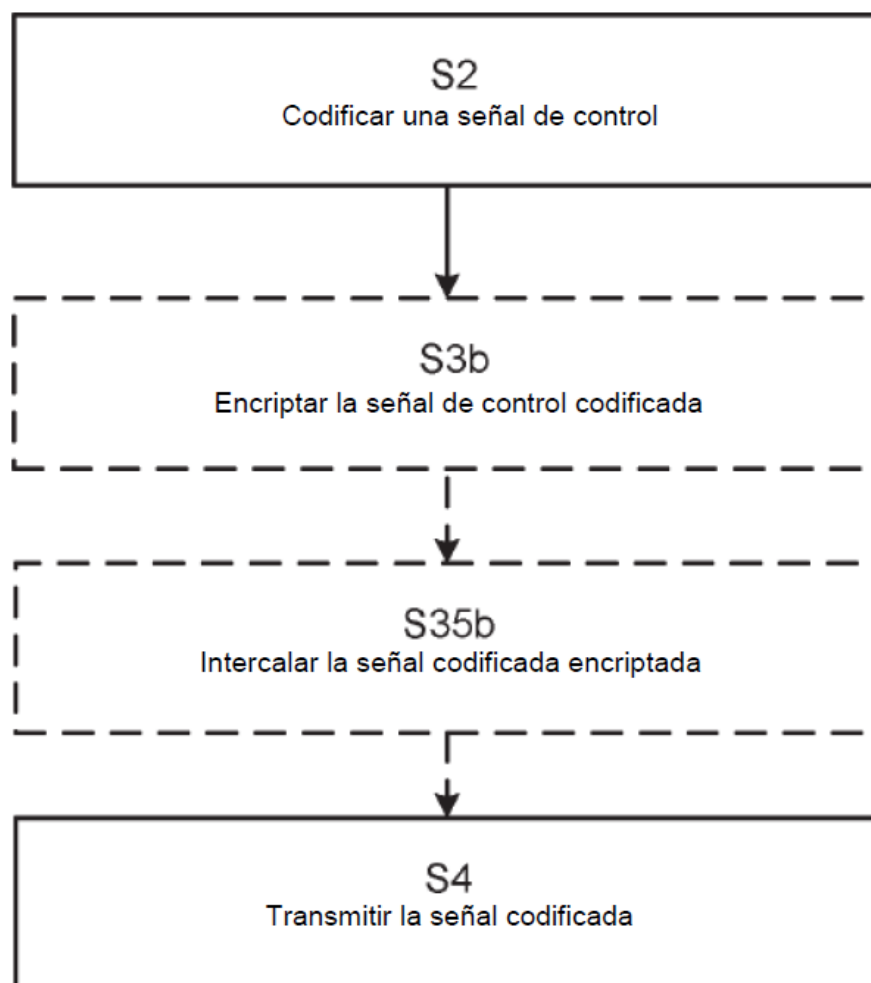


FIG.10

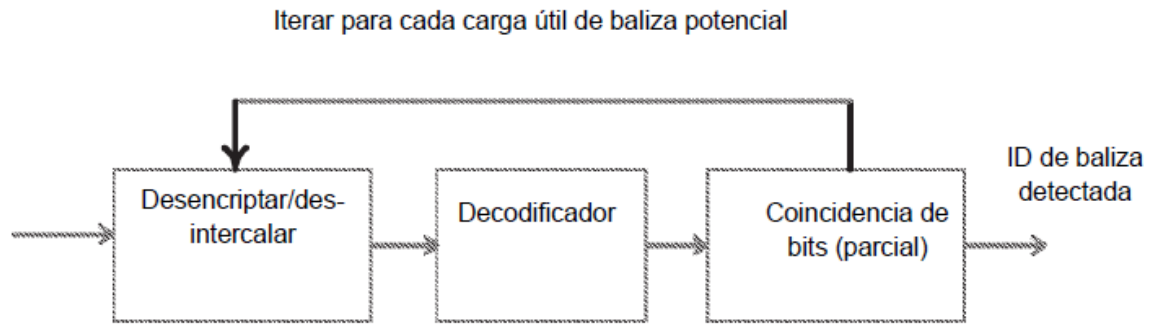


FIG.11a

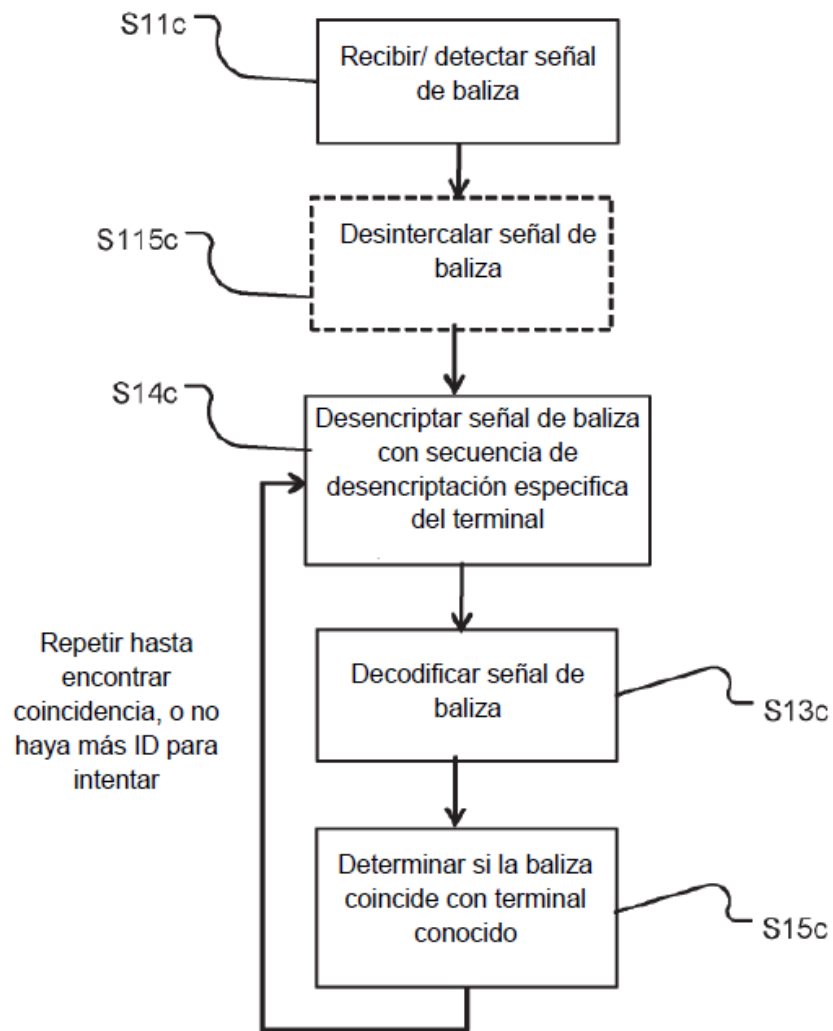


FIG.11b

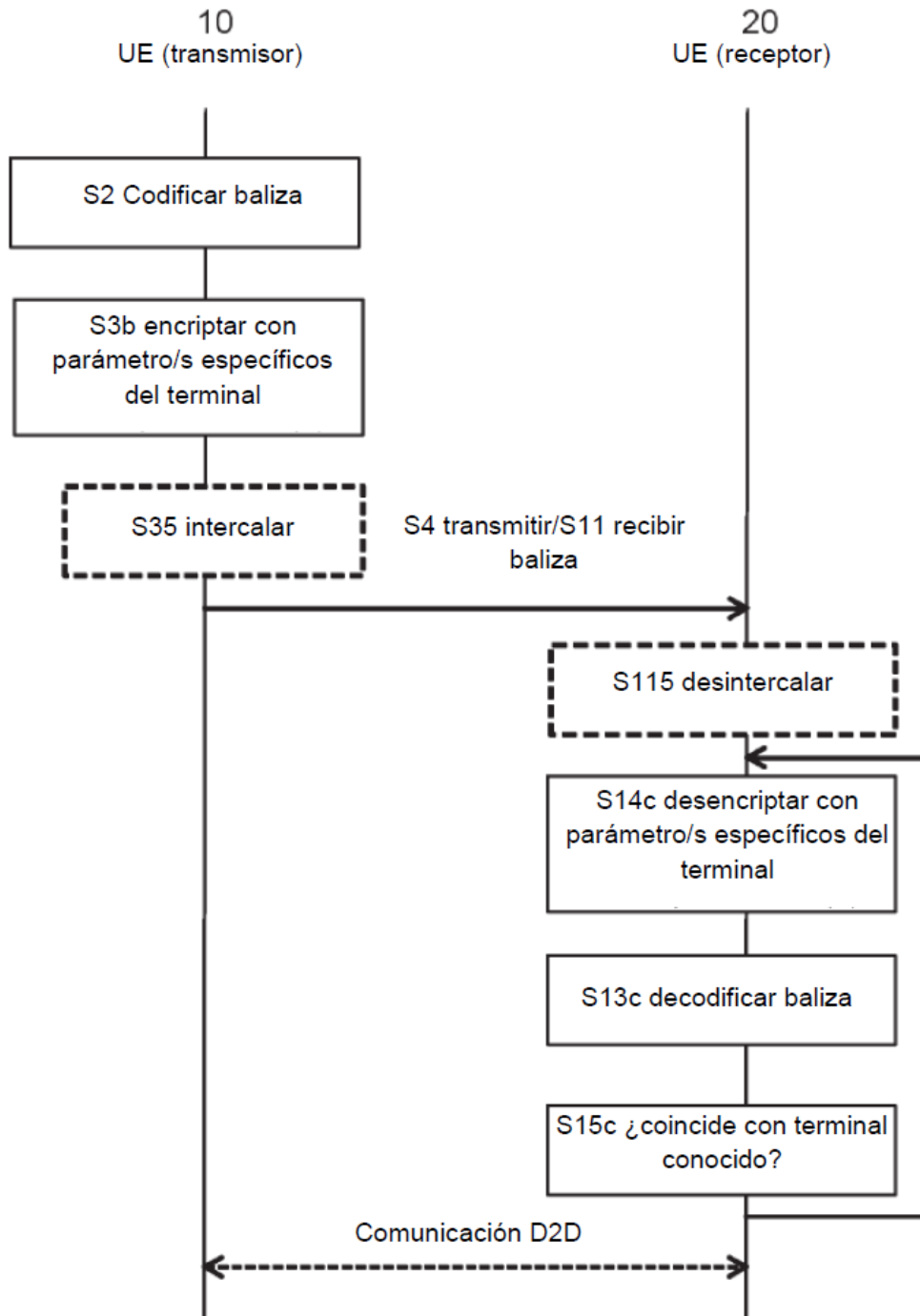


FIG.12

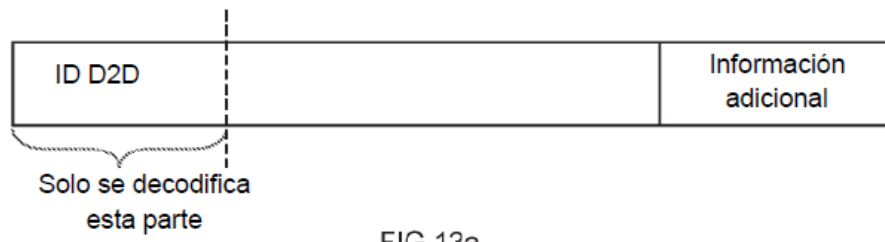


FIG. 13a

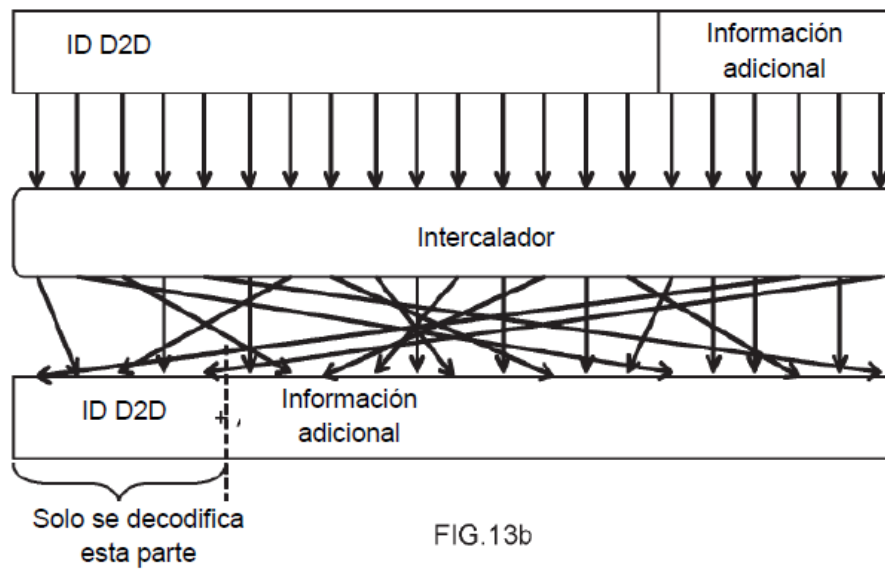


FIG. 13b

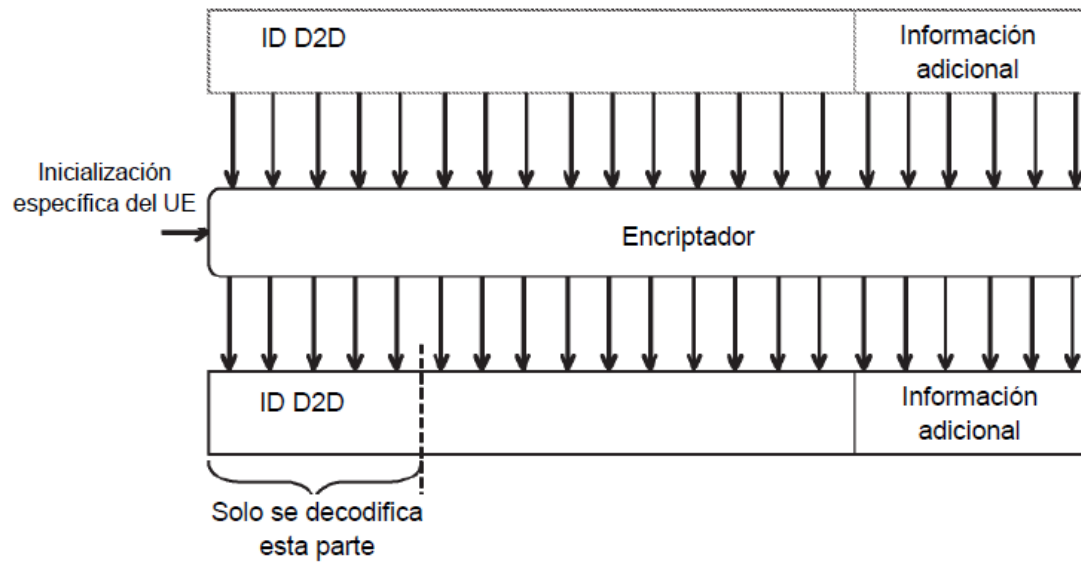


FIG. 13c