(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 802 400**

(51) Int. CI.:

H04L 25/02 (2006.01)
H04L 29/06 (2006.01)
H04W 12/12 (2009.01)
G01S 3/74 (2006.01)
H04B 7/06 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.12.2016 PCT/EP2016/082867**

(87) Fecha y número de publicación internacional: **06.07.2017 WO17114915**

(96) Fecha de presentación y número de la solicitud europea: **29.12.2016 E 16831621 (4)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 3398307**

(54) Título: **Procedimiento de asociación univalente y unívoca entre emisores y receptores de transmisión a partir del canal de propagación**

(30) Prioridad:

29.12.2015 FR 1502713

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.01.2021

(73) Titular/es:

THALES (50.0%)
Tour Carpe Diem, Place des Corolles, Esplanade Nord
92400 Courbevoie, FR y
TEKNOLOGIAN TUTKIMUSKESKUS VTT (50.0%)

(72) Inventor/es:

DELAVEAU, FRANÇOIS;
MOLIÈRE, RENAUD;
KAMENI NGASSA, CHRISTIANE;
LEMÉNAGER, CLAUDE;
KOTELBA, ADRIAN y
SUOMALAINEN, JANI

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Procedimiento de asociación univalente y unívoca entre emisores y receptores de transmisión a partir del canal de propagación

La invención se refiere en especial a un procedimiento que permite asociar, de manera univalente y unívoca, al menos un emisor y un receptor que equipan a dos usuarios, en una red de comunicación utilizando las propiedades del canal de propagación. La misma se utiliza, por ejemplo, en redes de radiocomunicaciones, redes de comunicaciones inalámbricas. La misma permite asegurar la transmisión de datos entre al menos dos usuarios.

Existen diferentes métodos que permiten asegurar la transmisión de datos en el seno de una red de comunicación.

La mayor parte de estos métodos utilizan procedimientos criptográficos con distribución anterior de claves (algunas veces denominadas también códigos) para identificar los equipos electrónicos y usuarios, autentificar los enlaces de comunicación en transcurso de establecimiento, asociar los emisores y los receptores. El inconveniente de estos métodos reside en la distribución y la gestión de las claves que puede resultar problemática en términos de distribución a gran escala, tanto en términos de garantía de no divulgación, como lo han demostrado recientes avances en el campo de las redes radiocelulares. Por el contrario, la presente invención propone realizar asociaciones aseguradas entre emisores/receptores, sin utilización de claves conocidas o compartidas con anterioridad.

La invención se refiere a un procedimiento de asociación univalente y unívoca a partir del canal de propagación entre al menos un primer usuario y un segundo usuario, sin utilización de clave conocida o compartida con anterioridad. La asignación de la asociación, y tras las transmisiones de datos negociados posteriormente basándose en esta asociación se basan en especial en la utilización de transmisiones anteriores de señales de interrogación y de señales de acuse de recibo entre el primer usuario y el segundo usuario, y en medidas y una cuantificación del canal de propagación por estos dos usuarios.

La invención se refiere a un procedimiento de asociación univalente y unívoca, antes del establecimiento de un protocolo de comunicación, a partir del canal (AU_CP) de propagación entre al menos un primer usuario A y un segundo usuario B provistos, cada uno, de uno o de varios emisores/receptores ($A_1 \ldots A_{NA}$) de transmisión indexados por n y n' para el usuario A, ($B_1 \ldots B_{NB}$) indexados por m y m' para el usuario B, caracterizado porque comprende al menos las etapas siguientes:

Fase de inicialización:

a) Emisión por cada emisor A_n de usuario A de señales $S^{(0)}_{Int,n}$ de interrogación para el emisor de índice n, constituidas por al menos una secuencia $PN^{(0)}_{Int,n}$ aleatoria conocida por el usuario B, de factor $SF^{(0)}_{Int,n}$ de dispersión,

b) Recepción y agrupación para cada receptor $B_{m'}$ del usuario B de la secuencia $PN^{(0)}_{Int,n}$ aleatoria de cada una de las señales $S^{(0)}_{Int,n}$ de interrogación iniciales, medidas por dichos receptores $B_{m'}$ del canal $H^{(0)}_{AB,n,m'}$ de propagación, entre A_n y $B_{m'}$ sobre la longitud de $L^{(0)}$ muestreos; estimación de los coeficientes $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ de la respuesta de impulso complejo correspondiente a los coeficientes de la respuesta de frecuencia compleja correspondiente,

c) Cuantificación por el usuario B de los coeficientes $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ complejos que provienen de sus medidas para producir valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos,

d) Emisión para cada emisor B_m del usuario B de señales $S^{(0)}_{Acq,m}$ de acuse de recibo constituidas de al menos una secuencia aleatoria denominada $PN^{(0)}_{Acq,m}$ conocida por el usuario A, de factor $SF^{(0)}_{Acq,m}$ de dispersión

e) Recepción y agrupación para cada receptor $A_{n'}$ de la secuencia $PN^{(0)}_{acq,m}$ aleatoria de cada una de las señales $S^{(0)}_{Acq,m}$ de acuse de recibo iniciales, medida por dichos receptores $A_{n'}$ del canal $H^{(0)}_{BA,m,n'}$ de propagación entre B_m y $A_{n'}$ sobre la longitud de $L^{(0)}$ muestreos; estimación de los coeficientes $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ de la respuesta de impulso complejo correspondiente o de los coeficientes de la respuesta de frecuencia compleja correspondiente, siendo idénticos los coeficientes $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ estimados por B en la etapa c) $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ cuando el canal de propagación es recíproco y los emisores receptores considerados para A y B coinciden en los dos sentidos de interrogación y de acuse de recibo, con n=n' y m=m',

f) Cuantificación por el usuario A de los coeficientes $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ complejos que provienen de sus medidas para producir valores $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$, numéricos

Fase de iteración 1, primera iteración:

g) Emisión para cada uno de los emisores A_n de nuevas señales $S^{(1)}_{Int,n}$ de interrogación constituidas por al menos una nueva secuencia $PN^{(1)}_{Int,n}$ de factor $SF^{(1)}_{Int,n}$ de dispersión elegida en un conjunto predeterminado conocido de A y B o construido según un proceso predeterminado conocido por A y B tras los valores $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$, numéricos determinados por A al final de la etapa f),

h) Recepción y agrupación de la secuencia $PN^{(1)}_{Int,n}$ de la señal $S^{(1)}_{Int,n}$ para cada receptor $B_{m'}$, $B_{m'}$ que reconstruye con anterioridad la secuencia $PN^{(1)}_{Int,n}$ aleatoria elegida o construida por A_n, según el mismo proceso que A_n, explotando los valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos determinados por B durante la cuantificación efectuada en la etapa c) de los coeficientes $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$, de valores numéricos iguales a los producidos por A en la etapa f) cuando el canal de propagación es recíproco, que n=n' y que m=m'); cuando m=m' y n=n', validación por B, gracias a la agrupación de $PN^{(1)}_{Int,n}$ en recepción por $B_{m'}$ de la igualdad entre coeficientes $Q^{(0)}_{AB,n,m}(l_1)_{l_1=0,\ldots,L-1} = Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$ cuantificados durante la fase de inicialización, medidos actualizados para cada receptor $B_{m'}$ del canal $H^{(1)}_{AB,n,m'}$ de propagación entre A_n y $B_{m'}$ sobre la longitud de $L^{(1)}$ muestreos, estimación de los coeficientes $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ de la respuesta de impulso complejo correspondiente o de los coeficientes de la respuesta de frecuencia compleja correspondiente,

i) Cuantificación por el usuario B de los coeficientes $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ que provienen de sus medidas para producir valores $Q^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos

j) Emisión por cada emisor B_m de nuevas señales de acuse de recibo, denominadas $S^{(1)}_{Acq,m}$, constituidas de al menos una secuencia aleatoria denominada $PN^{(1)}_{Acq,m}$ de factor $SF^{(1)}_{Acq,m}$, de dispersión, elegida en un conjunto predeterminado conocido por A y B o construida según un proceso predeterminado conocido por A y B tras los valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos determinados por B al final de la etapa c),

k) Recepción y dispersión por cada receptor $A_{n'}$ de las secuencias $PN^{(1)}_{acq,m}$ de cada una de las señales ($S^{(1)}_{Acq,m}$), $A_{n'}$ que reconstituye con anterioridad la secuencia $PN^{(1)}_{acq,m}$ elegida o construida por $B_{m'}$ según el mismo proceso que $B_{m'}$ explotando los valores $Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$ numéricos que A ha determinado en la etapa f) valores numéricos iguales a los producidos por B en la etapa c), es decir $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ cuando el canal de propagación es recíproco, que n=n' y que m=m'); cuando n=n' y m=m', validación por A, gracias a la agrupación de $PN^{(1)}_{Acq,m'}$ de la igualdad entre coeficientes $Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1} = Q^{(0)}_{AB,n,m}(l_1)_{l_1=0,\ldots,L-1}$ cuantificados durante la fase de inicialización, la asociación univalente de los emisores/receptores A_n del usuario A y de los emisores/receptores B_m del usuario B por tanto se hacen efectivos gracias a la relación de igualdad $Q^{(0)}_{AB,n,m}(l_1)_{l_1=0,\ldots,L-1} = Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$ entre coeficientes cuantificados validada en B_m en la etapa h) para la recepción y la agrupación de $PN^{(1)}_{Int,n}$ y validada en A_n en esta etapa k) por la recepción y la agrupación de $PN^{(1)}_{acq,m}$; medida por cada receptor $A_{n'}$ del canal $H^{(1)}_{BA,m,n'}$ sobre la longitud de $L^{(1)}$ muestreos; estimación de los coeficientes $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ de la respuesta de impulso complejo (o de los coeficientes de la respuesta de frecuencia compleja) correspondiente (57), siendo idénticos los coeficientes $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ a los estimados por B en la etapa h), $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ cuando el canal de propagación es recíproco y los emisores receptores considerados para A y B coinciden en los dos sentidos de interrogación y de acuse de recibo, n=n' y m=m',

l) Cuantificación por el usuario A de los coeficientes $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ complejos que provienen de sus medidas para producir los coeficientes $Q^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos.

El Procedimiento puede comprender al menos una segunda iteración de las etapas de la primera iteración con la emisión de señales $S^{(2)}_{Int,n}$ de interrogación que contienen la secuencia $PN^{(2)}_{Int,n}$ y la emisión de señales $S^{(2)}_{Acq,m}$ de acuse de recibo que contiene la secuencia $PN^{(2)}_{Acq,m}$ elaboradas tras los resultados de medida $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ y $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ y tras los resultados de cuantificación $Q^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ y $Q^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ producidos en la iteración 1, la cuantificación de nuevos coeficientes $Q^{(2)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ y $Q^{(2)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$, y la asociación univalente y unívoca de los emisores/receptores A_n del usuario A y de los emisores/receptores B_m del usuario B por la relación entre coeficientes cuantificados durante la iteración 1

$Q^{(1)}_{AB,n,m}(l_1)_{l_1=0,\ldots,L-1} = Q^{(1)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$, asociación validada por la recepción y la agrupación de secuencias $PN^{(2)}_{Int,n}$ de interrogación y $PN^{(2)}_{Acq,m}$ de acuse de recibo emitidas por A_n y B_m durante la segunda iteración.

El procedimiento comprende, por ejemplo, en cada nueva iteración k+1, con k superior o igual a 1, la emisión de señales $S^{(k+1)}_{Int.n}$ de interrogación que contienen la secuencia $PN^{(k+1)}_{Int,n}$ y señales $S^{(k+1)}_{Acq,m}$ de acuse de recibo que contienen la secuencia $PN^{(k+1)}_{Acq,m}$ y construidas tras los resultados de medida de la iteración k $H^{(k)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ y $H^{(k)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ y tras los resultados de cuantificación de la iteración k $Q^{(k)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ y $Q^{(k)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$, y la asociación univalente y unívoca de los emisores/receptores A_n del usuario A y de los emisores/receptores B_m del usuario B, utilizando la relación $Q^{(k)}_{AB,n,m}(l_1)_{l_1=0,\ldots,L-1} = Q^{(k)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$ entre coeficientes cuantificados durante la iteración k, asociación validada por la recepción y la agrupación por B_m y A_n de las señales de interrogación y de acuse de recibo emitidas por A_n y B_m durante la (k+1)ésima iteración.

Según una variante de realización, el procedimiento para las etapas de cuantificación c) y f) durante la iniciación, en las etapas i) y l) durante la iteración 1 y en las etapas similares durante iteraciones siguientes, utiliza una función de selección y decodificación correctora de los coeficientes de canales $H^{(k)}_{AB,n,m}(l_1)_{l_1=0,\ldots,L-1}$ y $H^{(k)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$, siendo adoptada la función para retener únicamente los coeficientes cuya estimación es la más fiable, por aplicación de un criterio de valor umbral sobre la calidad de la estimación de los coeficientes citados anteriormente y de una corrección de error sobre las salidas de cuantificación $Q^{(k)}_{AB,n,m}(l_1)_{l_1=0,\ldots,L-1}$ y $Q^{(k)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$, estando predefinido este criterio de valor de umbral y esta corrección entre los usuarios A y B.

Un receptor B_m utiliza, en la etapa d) citada anteriormente, un proceso de construcción específico de las señales $S'^{(0)}_{Acq,m}$ de acuse de recibo iniciales modificadas que hacen depender las mismas de todas las primeras medidas $H^{(0)}_{AB,n,m'}$ de canales y de los coeficientes $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ cuantificados correspondientes, siempre que se permite la posibilidad para los receptores $A_{n'}$ del usuario A de reconstruir y de agrupar las señales $S'^{(0)}_{Acq,m}$, comprendiendo dicha señales de acuse de recibo iniciales modificadas al menos dos secuencias PN, denominadas $PN^{(0)}_{Acq,m}$ y $PN'^{('0)}_{Acq,m}$, emitidas sucesivamente simultáneamente, siendo conocida la primera de las secuencias $PN^{(0)}_{Acq,m}$ por A como en la etapa d), siendo elegida la segunda de las secuencias $PN'^{('0)}_{Acq,m}$ en un conjunto predeterminado conocido por B y por A o construida según un proceso predeterminado conocido por B y por A tras los valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos que se acaban de cuantificar por B al final de la etapa c); y An' aplica a las etapas e) y f) citadas anteriormente no solamente una recepción y una agrupación de la secuencia $PN^{(0)}_{Acq,m}$ sino también una reconstrucción de la secuencia $PN'^{('0)}_{Acq,m}$ tras las estimaciones del canal $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ y las cuantificaciones $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ que conduce gracias a la agrupación de $PN^{(0)}_{Acq,m}$ en las etapas e) y f) seguida de una agrupación de la secuencia $PN'^{('0)}_{Acq,m}$, para producir una validación inmediata de la igualdad entre los coeficientes $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ y $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ cuantificados en fase de inicialización.

Según una variante de implementación, el procedimiento comprende en cada nueva iteración k+1, con k superior o igual a 0, la emisión de señales $S^{(k+1)}_{Acq,m}$ de acuse de recibo que contienen al menos dos secuencias $PN^{(k+1)}_{Acq,m}$ y $PN'^{(k+1)}_{Acq,m}$ emitidas secuencialmente o simultáneamente, siendo elegida $PN^{(k+1)}_{Acq,m}$ en un conjunto predeterminado o construido adaptativamente tras los resultados $Q^{(k)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ de cuantificación en la iteración nºk, y siendo elegida $PN'^{(k+1)}_{Acq,m}$ en un conjunto predeterminado o construido adaptativa mente tras los resultados $Q^{(k+1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1.}$ de cuantificación actuales en la iteración nº k+1; $A_{n'}$ aplica no solamente una recepción y una agrupación de la secuencia $PN^{(k+1)}_{Acq,m}$ reconstruida tras sus coeficientes $Q^{(k)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ cuantificados, sino también una reconstrucción de la secuencia $PN'^{(k+1)}_{Acq,m}$ tras las estimaciones del canal $H^{(k+1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ y las cuantificaciones $Q^{(k+1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ que conducen gracias a la agrupación de $PN^{(k+1)}_{Acq,m}$, seguida de una agrupación de la secuencia $PN'^{(k+1)}_{Acq,m}$ para validar inmediatamente la igualdad entre los coeficientes $Q^{(k+1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1.}$ y $Q^{(k+1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1.}$ cuantificados en la iteración k+1.

Los emisores de A pueden utilizar señales de interrogación iniciales elegidas aleatoriamente en un conjunto de señales conocidas por B, los receptores de B sólo acusan recibo de una de las señales de interrogación iniciales recibidas, o

bien predeterminada por las características de los receptores de B, o bien elegida aleatoriamente por los receptores de B, tras la sincronización, de la agrupación y de la medida de dichas señales de interrogación iniciales.

Los emisores B utilizan, por ejemplo, señales de acuse de recibo iniciales elegidas aleatoriamente en un conjunto de señales conocidas por A, los receptores A sólo tratan en recepción ciertas de las señales de acuse de recibo iniciales recibidas, o bien predeterminadas por las características de los receptores de A, o bien elegidas aleatoriamente por los receptores de A, tras la sincronización, de la agrupación y de la medida de dichas señales de acuse de recibo iniciales.

Los emisores de A pueden aplicar una fluctuación de fase aleatoria en tiempo a las señales de interrogación y los emisores de B aplicar una fluctuación de fase aleatoria en tiempo a las señales de acuse de recibo.

Según una variante de realización, el procedimiento utiliza señales de interrogación y de acuse de recibo SI_A y SA_B emitidas conjuntamente en la señales de baliza de uno y otro usuario A o B, AI_A y AI_B, es decir de manera autointerferida, siendo emitidas, recibidas y tratadas dichas señales de interrogación y de acuse de recibo en cada iteración k gracias a parametrizaciones adaptadas a sus potencias de emisión por A y B, $SI^{(k)}_A$ y $SA^{(k)}_B$, a sus niveles de recepción en B y en A, a interferencias inducidas por la baliza de A recibida en B y por la baliza de B recibida en A, $AI^{(k)}_{A->B}$ y $AI^{(k)}_{B->A}$, a los niveles de recepción en B y en A de las autointerferencias que provienen de B y de A, $AI^{(k)}_{A->A}$ y $AI^{(k)}_{B->B}$, a los dispositivos de autorrechazo de las autointerferencias a la recepción en A y en B, $RAI_{A->A}$ y $RAI_{B->B}$, a los factores de dispersión a la emisión en A y B, $SF^{(k)}_{Int,n}$ y $SF^{(k)}_{Acq,m}$, según las igualdades y desigualdades siguientes expresadas en decibelios:

- en las recepciones del usuario B:

$$AI^{(k)}_{A->B} = AI^{(k)}_{A} - L^{(k)}_{A->B}$$

$$SI^{(k)}_{A->B} = SI^{(k)}_{A} - L^{(k)}_{A->B}$$

donde $L^{(k)}_{A->B}$ representa las pérdidas totales de propagación de A hacia B,

$$SF^{(k)}_{Int,n} \geq 10.\log_{10}[10\text{^}(SI^{(k)}_{A->B}/10)] - 10.\log_{10}[10\text{^}((AI_{B->B}-RAI_{B->B})/10) + 10\text{^}(AI^{(k)}_{A->B}/10)] + \eta_B,$$

- en las recepciones del usuario A:

$$AI^{(k)}_{B->A} = AI^{(k)}_{B} - L^{(k)}_{B->A}$$

$$SI^{(k)}_{B->A} = SI^{(k)}_{A} - L^{(k)}_{B->A}$$

donde $L^{(k)}_{B->A}$ representa las pérdidas totales de propagación de B hacia A,

$$SF^{(k)}_{Int,n} \geq 10.\log_{10}[10\text{^}(SI^{(k)}_{B->A}/10)] - 10.\log_{10}[10\text{^}((AI_{A->A}-RAI_{A->A})/10) + 10\text{^}(AI^{(k)}_{B->A}/10)] + \eta_A,$$

estando relacionados los márgenes $ń_B$ y $ń_A$ con los rendimientos de los equipos de radio utilizados por los receptores de A y de B.

Según una variante de realización, el procedimiento implementa señales de interrogación y de acuse de recibo emitidas conjuntamente en los mensajes de intercambio de datos entre los usuarios, es decir, de manera autointerferida, siendo emitidas, recibidas y tratadas dichas señales de interrogación y de acuse de recibo en cada iteración k gracias a parametrizaciones adaptadas a sus potencias de emisión por A y B, de sus niveles de recepción en B y en A, de las interferencias inducidas por los mensajes de A recibidos en B y por los mensajes de B recibidos en A, de los niveles de recepción en B y en A, de las autointerferencias que provienen de B y d A, de los dispositivos de autorrechazo de estas autointerferencias en la recepción en A y B, de los factores de agrupación en la emisión en A y B), según igualdades y desigualdades en las expresiones similares a las citadas anteriormente.

El modo de comunicación implementado entre los usuarios es, por ejemplo, un modo Duplex temporal que emplea una misma frecuencia portadora para los intercambios en emisión y en recepción en los dos sentidos de transmisión, y se beneficia directamente de la reciprocidad del canal de propagación sobre la frecuencia única empleada para las interrogaciones y los acuses de recibo.

El procedimiento es, por ejemplo, duplicado en el conjunto de frecuencias portadoras empleadas por usuarios en modo Duplex de frecuencia que emplean frecuencias portadoras diferentes para sus intercambios en emisión y en recepción según el sentido de transmisión, con el fin de beneficiarse de la reciprocidad del canal de propagación sobre cada una de las frecuencias empleadas para las interrogaciones y los acuses de recibo.

Las etapas del procedimiento pueden reiterarse para cada nueva transmisión de telefonía o de datos o incluso para cada nuevo mensaje de una trasmisión de telefonía o de datos en curso.

Los emisores/receptores utilizados son, por ejemplo, adaptados a las radiocomunicaciones. Los emisores/receptores del usuario A pueden estar conectados a elementos de antena de una red utilizada por A y los emisores/receptores del usuario B conectados a los elementos de antenas de una red utilizada por B en el marco de protocolos denominados de tipo MISO, SIMO, MIMO o "*massive MIMO*" conocidos por el experto en la materia.

Los emisores/receptores del usuario A son, por ejemplo, estaciones base o nodos de una red de radiocomunicación y los emisores/receptores del usuario B son terminales u otros nodos de dicha red de radiocomunicación.

Los emisores y receptores están, por ejemplo, adaptados a transmisiones acústicas o a transmisiones ópticas.

Otras características y ventajas de la presente invención aparecerán mejor de la lectura de la descripción siguiente de ejemplos dados a título ilustrativo y en ningún caso limitativo, que adjuntan las figuras que representan:

- La figura 1, un esquema de intercambios de información entre dos usuarios A (Alice) y B (Bob) en presencia de un tercero E (Eve) extranjero no autorizado a conocer el contenido de los datos intercambiados entre A y B,
- La figura 2, una ilustración de efectos de un canal de propagación dispersivo sobre la trasmisión de las señales desde una emisora hacia un receptor B autorizado y hacia un receptor E no autorizado, y
- La figura 3, un esquema de las etapas implementadas por el procedimiento según la invención.

Con el fin de comprender mejor el procedimiento según la invención, el ejemplo se da en el caso de un intercambio entre un primer usuario emisor/receptor A (Alice) y un segundo usuario emisor/receptor B (Bob), en presencia de un tercer receptor E (Eve) no autorizado y susceptible de interceptar las comunicaciones para acceder al contenido de datos intercambiados entre A y B.

La figura 1 ilustra un escenario de comunicación entre un primer usuario A, 10 y un segundo usuario B, 20 en presencia de un tercero receptor E, 30 no autorizado.

El usuario A es, por ejemplo, un nodo o un terminal de una red de comunicación que comprende una unidad 11 de cálculo, un módulo 12 de codificación/decodificación, un módulo 13 de demodulación, un módulo 14 compuesto de antenas, un conjunto de filtros 15, medios 16 de emisión y recepción de radio. Estos elementos son conocidos por el experto en la materia y no serán detallados. El objeto de la invención va a consistir, en especial, en asociar de manera unívoca y univalente A y B, como se va a explicar a continuación. Alice o A comprende por ejemplo NA emisores/receptores An denominados $A_1 \ldots A_{NA}$ para el usuario A.

Del mismo modo, el usuario B, 20, comprende, por ejemplo, una unidad 21 de cálculo, un módulo 22 de codificación/decodificación, un módulo 23 de demodulación, un módulo 24 compuesto de antenas, filtros 25, medios 26 de emisión y recepción de radio. Bob comprende, por ejemplo, NB emisores/receptores denominados $B_1 \ldots B_{NB}$.

El tercero receptor E, 30 no autorizado, comprende una unidad 31 de cálculo, un grabador 32 de datos y un módulo 33 de análisis, un bloque 34 de antenas, filtros 35 y medios 36 de recepción de radio y posiblemente emisores y receptores.

La figura 2 esquematiza un ejemplo de canales de propagación existentes en un sistema de comunicación. En entornos exteriores o interiores, las formas de onda transmitidas del emisor A hacia el receptor B y hacia el tercero E siguen recorridos de trayectos múltiples. Las señales pueden ser reflejadas por obstáculos con diferentes ángulos de reflexión. Una parte de las señales S_{AB} puede ser recibida por Bob, mientras que otra parte tras la difracción S_{AE}, será recibida por el tercero E no autorizado. Debido a la complejidad en la propagación de las ondas y de las difracciones poco previsibles en el canal de comunicación, el tercero E es a priori incapaz de predecir o de reconstruir las medidas del canal de propagación entre un emisor de A y un receptor de B.

El procedimiento según la invención ilustrado en la figura 3 es un procedimiento de asociación univalente y unívoca a partir del canal (AU_CP) de propagación entre Alice y Bob. La asociación entre Alice y Bob se realiza sin clave conocida o compartida con anterioridad, y se asegura frente a cualquier tercero E no autorizado, antes incluso del establecimiento del protocolo de transmisión entre los usuarios A y B, con la ayuda de transmisiones con anterioridad de señales de interrogación y de señales de acuse de recibo, con la ayuda de medidas de los canales de propagación entre los emisores receptores de A y los de B gracias a estas señales de interrogación y de acuse de recibo, y finalmente con la ayuda de una cuantificación de estos canales de propagación. Esta asociación está destinada, en especial, a facilitar posteriormente el establecimiento de una trasmisión, protegida con respecto a E, entre los usuarios A y B así como la identificación de A por B y de B por A, el control de confidencialidad y el control de integridad de los mensajes intercambiados por A y B.

Un ejemplo de las etapas del procedimiento según la invención se va a detallar a continuación.

Una primera fase permite una inicialización del proceso.

Etapa a): cada emisor A_n del usuario A (con n variando de 1 a NA) emite señales $S^{(0)}_{Int,n}$ de interrogación iniciales para el emisor de índice n, 41, constituido de al menos una secuencia $PN^{(0)}_{Int,n}$ aleatoria de periodo $P^{(0)}_{Int,n}$ y de factor $SF^{(0)}_{Int,n}$ de dispersión conocido por el usuario B;

Etapa b) : cada receptor $B_{m'}$ del usuario B, (con m' variando de 1 a NB) va a recibir y a muestrear en un periodo T_e que respecta el criterio de Nyquist, la señales $S^{(0)}_{Int,n}$ de interrogación, y después, tras la sincronización, cada receptor $B_{m'}$ va a agrupar la secuencia $PN^{(0)}_{Int,n}$ correspondiente, 42, y después cada receptor $B_{m'}$ va a medir, 43, los parámetros del canal $H^{(0)}_{AB,n,m'}$ de propagación entre An y $B_{m'}$, sobre la longitud de $L^{(0)}$ muestreos, y después estimar, 43, los coeficientes $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ de la respuesta de impulso complejo correspondiente a los coeficientes de la respuesta de frecuencia compleja correspondiente;

Etapa c) : el usuario B va a continuación a cuantificar los coeficientes complejos que provienen de los coeficientes $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ de canal. La cuantificación, 44, es, por ejemplo, realizada efectuando un mallado geométrico del plano complejo, en la cual estos coeficientes toman un valor y una enumeración según la malla a la cual pertenecen, para producir valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ numéricos, 44;

Etapa d): cada emisor B_m del usuario B emite una señal $S^{(0)}_{Acq,m}$ de acuse de recibo, 45, constituida de al menos una secuencia aleatoria denominada $PN^{(0)}_{Acq,m}$, de periodo $P^{(0)}_{Acq,m}$ y de factor $SF^{(0)}_{Acq,m}$ de dispersión conocido por el usuario A;

Etapa e): cada receptor $A_{n'}$ del usuario A va a continuación a recibir, muestrear en un periodo T_e que respetar el criterio de Nyquist las señales $S^{(0)}_{Acq,m}$ de acuse de recibo iniciales, 46, y tras la sincronización, agrupar las secuencias $PN^{(0)}_{acq,m}$ aleatorias correspondientes. Cada uno de los receptores $A_{n'}$ va a continuación a medir los parámetros del canal $H^{(0)}_{BA,m,n'}$ de propagación entre B_m y $A_{n'}$ sobre de la longitud de $L^{(0)}$ muestreos, 47, y después estimar los coeficientes $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ de la respuesta de impulso complejo correspondiente a los coeficientes de la respuesta de frecuencia compleja correspondiente, 47, siendo idénticos los coeficientes $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ a los estimados por B $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ cuando el canal de propagación es recíproco y los emisores receptores considerados para A y B coinciden en los dos sentidos de interrogación y de acuse de recibo, es decir cuando n=n' y m=m';

Etapa f) : el usuario A va a cuantificar a continuación los coeficientes $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ complejos que provienen de medidas de su receptores, dicha cuantificación, 48, de la misma naturaleza que la descrita para el usuario B en la etapa c), consistente, por ejemplo, en una mallado geométrico del plano complejo en el cual estos coeficientes toman sus valores y su numeración según la malla a la cual pertenecen, para producir valores $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$, numéricos, 48. Al final de la etapa de inicialización, se disponen los valores cuantificados de los coeficientes $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ en el sentido A hacia B para cualquier par de índice (n,m') y $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$, en el sentido B hacia A para cualquier par de índice (m,n').

Tras la inicialización del sistema, el procedimiento va a ejecutar varias etapas que permiten asociar o no los emisores/receptores A_n del usuario A y los emisores/receptores B_m del usuario B.

Primera iteración - iteración 1

Etapa g): cada emisor A_n del usuario A emite de nuevo señales de interrogación, denominadas $S^{(1)}_{Int.n}$, 49. Estas señales de interrogación están constituidas de al menos una nueva secuencia $PN^{(1)}_{Int,n}$ aleatoria de periodo $P^{(1)}_{Int,n}$ y de factor $SF^{(1)}_{Int,n}$ de dispersión. Las secuencia es elegida, por ejemplo, en un conjunto predeterminado conocido de A y B o construida según un proceso predeterminado conocido por A y B tras los valores $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$, numéricos, 48, determinados por A al final de la etapa de inicialización, por ejemplo, utilizando estos valores numéricos como índice de la nueva señal de interrogación elegida en un conjunto predeterminado conocido por A y B o como semilla de un algoritmo de generación predeterminado, o incluso como parámetro de cualquier otro proceso (predeterminado y conocido por A y B) de construcción de secuencias aleatorias de interrogación;

Etapa h) : cada receptor $B_{m'}$ del usuario B recibe las señales $S^{(1)}_{Int.n}$ emitidas por los emisores A_n del usuario A, las muestrea en un periodo T_e de muestreo que respetar el criterio de Nyquist, y después, tras la sincronización, cada

receptor $B_{m'}$ agrupa las secuencias $PN^{(1)}_{Int,n}$ correspondientes, 50, reconstruyendo con anterioridad la secuencia $PN^{(1)}_{Int,n}$ aleatoria elegida construida por $A_{n'}$ 50, gracias a los valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos cuantificados en la etapa de inicialización por B, 44, valores numéricos iguales a los producidos por A en la etapa f), 48, cuando el canal de propagación es recíproco, que n=n' y que m=m'. Cuando el canal de propagación es recíproco, que n=n' (A_n emisor receptor) y m=m' (B_m emisor receptor) los éxitos de agrupación por B_m de $PN^{(1)}_{Int,n}$ realizan a nivel de B_m la asociación de A_n con $B_{m'}$, validando la igualdad, 51, entre coeficientes cuantificados en fase de inicialización en el sentido A_n hacia $B_{m'}$, 44, y B_m hacia $A_{n'}$, 48. A continuación, cada receptor $B_{m'}$ actualiza el valor de los parámetros del canal de propagación, denominados $H^{(1)}_{AB,n,m'}$, entre A_n y $B_{m'}$ sobre la longitud de $L^{(1)}$ muestreos, y después estima los coeficientes $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ de la respuesta de impulso complejo correspondiente a los coeficientes de la respuesta de frecuencia compleja correspondiente, 52;

Etapa i) : el usuario B cuantifica los coeficientes $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ que provienen de medidas de sus receptores, dicha cuantificación, similar a la descrita en la etapa c), genera coeficientes $Q^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos;

Etapa j) : cada emisor B_m va a emitir de nuevo las señales de acuse de recibo hacia el usuario A, denominadas $S^{(1)}_{Acq,m,}$ 54, constituidas de al menos una secuencia aleatoria, denominada $PN^{(1)}_{Acq,m}$ de periodo $P^{(1)}_{Acq,m}$ y de factor $SF^{(1)}_{Acq,m}$ de dispersión, elegido en un conjunto predeterminado conocido por A y B o construir o según un proceso predeterminado conocido por A y B tras los valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos determinados por B al final de la etapa c), 44, por ejemplo utilizando estos valores numéricos como índices de la nueva señal de acuse de recibo elegida en un conjunto predeterminado conocido de A y B o como grano de un algoritmo de generación predeterminado, o como parámetro de cualquier otro proceso (predeterminado y conocido por A y B) de construcción de secuencias aleatorias de acuse de recibo entre A y B, 54;

Etapa k) : cada receptor $A_{n'}$ del usuario A recibe las señales ($S^{(1)}_{Acq,m}$) emitidas por los emisores B_m del usuario B, el muestreo con un periodo T_e que respeta el criterio de Nyquist, y después, tras la sincronización cada receptor $A_{n'}$ agrupa las secuencias $PN^{(1)}_{acq,m}$ aleatorias correspondientes, 55, reconstruyendo con anterioridad la secuencia $PN^{(1)}_{acq,m}$ elegida o construida por $B_{m'}$ 54, gracias a los valores $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$, cuantificados en la etapa de inicialización por A etapa f) 48, valores numéricos iguales a los producidos por B en la etapa c), es decir $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ cuando el canal de propagación es recíproco, que n=n' y que m=m'. Cuando el canal de propagación es recíproco, que n=n' (A_n emisor receptor) y m=m' (B_m emisor receptor) el éxito del agrupación por A_n de $PN^{(1)}_{acq,m}$ realiza a nivel de A_n la asociación de B_m con A_n, validando la igualdad, 56, entre coeficientes cuantificados en los sentidos B hacia A, 48, y A hacia B, 44, durante la fase de inicialización. Esto realiza la función polivalente para los usuarios A y B de los emisores/receptores A_n del usuario A y los emisores/receptores B_m del usuario B por las relaciones entre coeficientes cuantificados durante la fase de inicialización $Q^{(0)}_{AB,n,m}(l_1)_{l_1=0,\ldots,L-1} = Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$ 51 y 56;

A continuación, cada receptor $A_{n'}$ del usuario A actualiza los valores de los parámetros del canal $H^{(1)}_{BA,m,n'}$ de propagación entre B_m y $A_{n'}$ sobre la longitud de $L^{(1)}$ muestreos; después estima, 57, los coeficientes $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ de la respuesta de impulso complejo correspondiente a los coeficientes de la respuesta de frecuencia compleja correspondiente, siendo idénticos los coeficientes $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ a los estimados por B en la etapa h), 52 $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ cuando el canal de propagación es recíproco y los emisores receptores considerados para A y B coinciden en los dos sentidos de interrogación y de acuse de recibo, es decir cuando n=n' y m=m',

Etapa l : cuantificación por el usuario A de los coeficientes $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ complejos que provienen de sus medidas para producir los coeficientes $Q^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$, 58.

Cuando en la primera iteración para un par de emisores/receptores A_n y B_m (n=n', m=m'), consigue agrupar la señal $PN^{(1)}_{Int,n}$ de interrogación que proviene de A_n y A_n consigue agrupar la señal $PN^{(1)}_{Acq,m}$ de acuse de recibo que proviene de B_m, por tanto hay una asociación del emisor/receptor A_n y del emisor/receptor B_m, sobre la base de la igualdad de los coeficientes de cuantificación obtenidos durante la etapa de inicialización, y certificación de esta asociación por el éxito de agrupación.

De manera general, si la agrupación de A_n sobre B_m y de B_m sobre A_n se efectúa en la etapa k+1, esto significa que las cuantificaciones de los coeficientes de los canales han producido valores iguales a la etapa k, y que la asociación de A_n y B_m es correcta. Si no, cuando la agrupación no se realiza, la asociación entre A_n y B_m no es efectiva. La señal de interrogación emitida por A_n sirve a B para la cuantificación del canal de propagación “ida”, para la validación de

los coeficientes de canal cuantificados por A en las etapas anteriores, para la construcción de sus propias señales de acuse de recibo. La señal de acuse de recibo emitida por B_m sirve para la cuantificación del canal de propagación "vuelta", para la validación de coeficientes de canal cuantificados por B en las etapas anteriores, para la construcción de sus nuevas señales de interrogación.

Las señales de interrogación y de acuse de recibo pueden transportar o no mensajes. Aparte de la inicialización se construyen siempre de manera adaptativa en función de las medidas del canal, lo que las hace imprescindibles para cualquier tercero E no informado y este a partir de la interacción 1. En la inicialización, se redefinen o eligen en un conjunto predefinido. Para eliminar cualquier riesgo de ambigüedad o de falsa alarma durante las fases de agrupación a nivel de A y de B, se fijan valores importantes para los periodos P y los factores SF de agrupación de las secuencias PN para la interrogación y el acuse de recibo, y se eligen conjuntos predeterminados o algoritmos de construcción de secuencias que presentan lóbulos secundarios reducidos de autocorrelación y de intercorrelación, según el procedimiento conocido por el experto en la materia.

Según una variante de realización, el procedimiento va a proceder a una segunda iteración, iteración 2, opcional. Para ello, el procedimiento reitera las etapas explicadas para la primera iteración, iteración 1:

- conduciendo a la emisión de señales $S^{(2)}_{Int,n}$ de interrogación y $S^{(2)}_{Acq,m}$ de acuse de recibo tras los resultados $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ y $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ de medida y tras los resultados $Q^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ y $Q^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ de cuantificación producidos en la iteración 1,

- produciendo los coeficientes $Q^{(2)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ y $Q^{(2)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$,

- asociando de forma univalente y unívoca los emisores/receptores A_n del usuario A y los emisores/receptores B_m del usuario B por la relación entre coeficientes cuantificados durante la iteración 1 $Q^{(1)}_{AB,n,m}(l_1)_{l_1=0,\dots,L-1} = Q^{(1)}_{BA,m,n}(l_1)_{l_1=0,\dots,L-1}$, certificada por la agrupación de $S^{(2)}_{Int,n}$ por B_m y por la agrupación de $S^{(2)}_{Acq,m}$ por A_n.

Según otra variante de realización, en cada nueva iteración k+1 de los emisores/receptores A_n del usuario A y los emisores/receptores B_m del usuario B, habrá un mantenimiento en el trascurso del tiempo de la asociación de A y B:

- para la relación $Q^{(0)}_{AB,n,m}(l_1)_{l_1=0,\dots,L-1} = Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\dots,L-1}$ entre coeficientes cuantificados durante la fase de inicialización, lo que conduce a una asociación equivalente y unívoca al final de la iteración 1,

- para la relación $Q^{(1)}_{AB,n,m}(l_1)_{l_1=0,\dots,L-1} = Q^{(1)}_{BA,m,n}(l_1)_{l_1=0,\dots,L-1}$ entre coeficientes cuantificados durante la iteración 1, lo que conduce a una asociación univalente y unívoca al final de la iteración 2,

- para la relación $Q^{(k)}_{AB,n,m}(l_1)_{l_1=0,\dots,L-1} = Q^{(k)}_{BA,m,n}(l_1)_{l_1=0,\dots,L-1}$ entre coeficientes cuantificados durante la iteración k, lo que conduce a una asociación univalente y unívoca al final de la iteración k+1.

La univalencia del proceso en cada iteración proviene del hecho de que sólo emisiones, recepciones y medidas de canales conducidas de manera simultánea y colocalizada con los emisores/receptores de A o de B permitirían a un tercero E, no informado de dichas medidas, reproducir los coeficientes y las mismas asociaciones que A y B aplicando los mismos procedimientos de cuantificación y de formateo (por tanto, E seria informado).

El número de iteraciones de las etapas del procedimiento según la invención varía de 1 a K, siendo K fijado por la aplicación o por las necesidades de los usuarios.

Según una variante de realización, el procedimiento utiliza una función de selección y de codificación correctora de los coeficientes $H^{(k)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ y $Q^{(k)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$, de canales para ejecutar las etapas de cuantificación de los coeficientes de canales, en las etapas de cuantificación c) y f) durante la iniciación, en las etapas i) y l) durante la iteración 1 y en las etapas similares de cuantificación durante iteraciones siguientes. Lo que permite retener o conservar únicamente los coeficientes cuya estimación es la más fiable, por aplicación de un criterio de valor umbral sobre la calidad de la estimación de los coeficientes y/o de una corrección de error sobre las salidas $Q^{(k)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ y $Q^{(k)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$, de cuantificación predefinidas entre los usuarios A y B. La univocidad del proceso en cada iteración proviene de esta selección y de esta corrección de error.

Según una variante de realización, el procedimiento utiliza en la etapa de la fase de inicialización d), un proceso de construcción específico de las señales $S'^{(0)}_{Acq,m}$, de acuse de recibo iniciales modificadas que hacen depender las

mismas de todas las primeras medidas de canales $H^{(0)}_{AB,n,m'}$ y de los coeficientes $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$, correspondientes a la vez que se establece la posibilidad para los receptores $A_{n'}$ del usuario A de reconstruir y agrupar las señales $S'^{(0)}_{Acq,m}$, dichas señales de acuse de recibo iniciales modificadas que comprenden al menos dos secuencias PN, denominadas $PN^{(0)}_{Acq,m}$ y $PN'^{(0)}_{Acq,m'}$ emitidas sucesivamente o simultáneamente, siendo conocida la primera de las secuencias $PN^{(0)}_{Acq,m}$ por $A_{n'}$ como en la etapa d) , siendo elegida la segunda de las secuencias $PN'^{(0)}_{Acq,m'}$ en un conjunto predeterminado conocido por B y por A o construido según un proceso predeterminado conocido por B y por A tras los valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos que se acaban de cuantificar por B al final de la etapa c); $A_{n'}$ aplica por tanto en las etapas e) y f) no solamente una recepción y una agrupación de la secuencia $PN^{(0)}_{Acq,m}$ sino también una reconstrucción de la secuencia $PN'^{(0)}_{Acq,m'}$ tras las estimaciones del canal $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ actual y las cuantificaciones $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$, que conduce gracias a una agrupación de $PN^{(0)}_{Acq,m}$ a las etapas e) y f), seguido de una agrupación inmediata de la secuencia $PN'^{(0)}_{Acq,m'}$. En caso de éxito, está agrupación produce una validación inmediata de la igualdad entre coeficientes $Q^{(0)}_{AB,n,m}(l_1)_{l_1=0,\ldots,L-1} = Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$ cuantificados en fase de inicialización.

Según una variante de realización, el procedimiento comprende en cada nueva iteración k+1, con k superior o igual a 0, la emisión de señales $S^{(k+1)}_{Acq,m}$ de acuse de recibo que contienen al menos secuencias $PN^{(k+1)}_{Acq,m}$ y $PN'^{(k+1)}_{Acq,m}$ emitidas secuencialmente o simultáneamente, siendo elegida $PN^{(k+1)}_{Acq,m}$ en un conjunto predeterminado o construida activamente tras los resultados $Q^{(k)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ de cuantificación en la iteración nºk, y siendo elegida $PN'^{(k+1)}_{Acq,m}$ en un conjunto predeterminado construido activamente tras los resultados de la cuantificación $Q^{(k)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$, actual en la iteración nº k+1; $A_{n'}$ aplica entonces no solamente una recepción y una agrupación de la secuencia $PN^{(k+1)}_{Acq,m}$ reconstruida tras sus coeficientes $Q^{(k)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$, cuantificados sino también una reconstrucción de la secuencia $PN'^{(k+1)}_{Acq,m}$ tras las estimaciones actuales del canal $H^{(k+1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$y las cuantificaciones $Q^{(k+1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$que conduce gracias a la agrupación de $PN^{(k+1)}_{Acq,m}$, seguido de una agrupación de la secuencia $PN'^{(k+1)}_{Acq,m}$. En caso de éxito, este agrupamiento produce una validación inmediata de la igualdad entre coeficientes $Q^{(k+1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1.} = Q^{(k+1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$cuantificados en la iteración k+1.

Para la implementación del procedimiento, los emisores del usuario A pueden utilizar señales de interrogación iniciales elegidas aleatoriamente en un conjunto de señales conocidas por B. Los receptores B solo acusan recibo de señales de interrogación iniciales recibidas, la señal de la que se acusó recibo es o bien predeterminada por las características de los receptores de B, bien elegida aleatoriamente por los receptores de B, tras la sincronización y la medida de dichas señales de interrogación iniciales, haciendo por tanto no previsibles las señales de interrogación efectivamente acusadas de recibo por B para cualquier tercero E no informado.

Según otra manera de proceder, los emisores de B utilizan señales de acuse de recibo iniciales elegidas aleatoriamente en un conjunto de señales conocidas por A. Los receptores de A sólo tratan en recepción ciertas de las señales de acuse de recibo iniciales recibidas. La señal adquirida es o bien predeterminada por las características de los receptores de A, o bien elegida aleatoriamente por los receptores de A, tras la realización y la medida de dichas señales de acuse de recibo iniciales, haciendo por tanto no previsibles las señales de acuse de recibo efectivamente tratadas por A para cualquier tercero E no informado.

A nivel de los emisores de A, es posible aplicar una fluctuación de fase aleatoria en tiempo a las señales de interrogación, a nivel de los emisores de B, es posible aplicar una fluctuación de fase aleatoria en tiempo a las señales de acuse de recibo lo que hace por tanto no previsibles los instantes de emisión de dichas señales de interrogación y de acuse de recibo para cualquier tercero E no informado.

Según un modo de realización, el procedimiento va a utilizar señales de interrogación y de acuse de recibo (denominadas respectivamente SI_A y SA_B), emitidas de forma conjunta a señales balizadas de uno u otro usuario A o B (denominadas respectivamente AI_A y AI_B), es decir de manera auto, siendo emitidas, recibidas y tratadas dicha señales de interrogación y de acuse de recibo en cada iteración K gracias a parametrizaciones adaptadas a sus potencias de emisión por A y B (denominadas respectivamente $SI^{(k)}_A$ y $SA^{(k)}_B$), a los niveles de recepción en A y en B tras la propagación de las interferencias inducidas por la baliza de A recibida en B y por la baliza de B recibida en A (denominadas respectivamente $AI^{(k)}_{A->B}$ y $AI^{(k)}_{B->A}$) a sus niveles de recepción en B y en A de las autointerferencias que provienen de B y de A (denominadas respectivamente $Ak^{(k)}_{A->A}$ y $AI^{(k)}_{B->B}$), a los dispositivos de autorrechazo de estas autointerferencias y a la recepción en A y B (con eficacias de rechazo, denominadas respectivamente $RAI_{A->A}$ y $RAI_{B->B}$), a factores de elementos en la emisión de A y B (denominados respectivamente $SF^{(k)}_{Int,n}$ y $SF^{(k)}_{Acq,m}$), según las igualdades y desigualdades siguientes expresadas en decibelios:

- en las recepciones del usuario B:

$$AI^{(k)}_{A->B} = AI^{(k)}_{A} - L^{(k)}_{A->B}$$

$$SI^{(k)}_{A->B} = SI^{(k)}_{A} - L^{(k)}_{A->B}$$

donde $L^{(k)}_{A->B}$ representa las pérdidas totales de propagación de A hacia B,

$$SF^{(k)}_{Int,n} \geq 10.\log_{10}[10\text{^}(SI^{(k)}_{A->B}/10)] - 10.\log_{10}[10\text{^}((AI_{B->B}-RAI_{B->B})/10) + 10\text{^}(AI^{(k)}_{A->B}/10)] + \eta_B,$$

- en las recepciones del usuario A:

$$AI^{(k)}_{B->A} = AI^{(k)}_{B} - L^{(k)}_{B->A}$$

$$SI^{(k)}_{B->A} = SI^{(k)}_{A} - L^{(k)}_{B->A}$$

donde $L^{(k)}_{B->A}$ representa las pérdidas totales de propagación de B hacia A,

$$SF^{(k)}_{Int,n} \geq 10.\log_{10}[10\text{^}(SI^{(k)}_{B->A}/10)] - 10.\log_{10}[10\text{^}((AI_{A->A}-RAI_{A->A})/10) + 10\text{^}(AI^{(k)}_{B->A}/10)] + \eta_A,$$

estando relacionados los márgenes $\acute{\eta}_B$ y $\acute{\eta}_A$ con los rendimientos de los equipos de radio utilizados por los receptores de A y de B.

Según otra variante de realización, el procedimiento va a emitir, conjuntamente en los mensajes de intercambios de datos entre los usuarios, señales de interrogación y de acuse de recibo autointerferidas por estos mensajes, siendo emitidas, recibidas y tratadas dicha señales de interrogación y de acuse de recibo en cada iteración k gracias a parametrizaciones adaptadas de sus potencias de emisión por A y B, de sus niveles de recepción en A y B tras la propagación, a las interferencias inducidas por los mensajes de A recibidos en B y por los mensajes de B recibidos en A, a los niveles de recepción en B y en A de las autointerferencias que provienen de B y de A, a los dispositivos de autorrechazo de estas autointerferencias en la recepción en A y en B, a factores de elementos en la emisión en A y B), según las desigualdades en las expresiones similares a la reivindicación anterior.

El procedimiento según la invención permite ventajosamente asegurar las trasmisiones de datos entre dos usuarios, sin tener que recurrir a un elemento externo a la red, basándose en propiedades características del canal de propagación apropiadas a los dos usuarios para asociarlos de manera segura. El procedimiento utiliza el carácter aleatorio del canal legítimo de radio para construir de manera adaptativa señales de interrogación y de acuse de recibo entre los dos usuarios, hace que estas señales sean imprevisibles, univalente y unívocas, con el fin de proporcionar un soporte para aumentar la seguridad de la capa física, la seguridad de acceso a la red, y en especial asegurar los protocolos de negociación entre los usuarios, autentificar los datos que se miden, y después identificar a los usuarios y controlar la integridad de los mensajes que se intercambian.

REIVINDICACIONES

1. Procedimiento de asociación univalente y unívoca, antes del establecimiento de un protocolo de comunicación, a partir del canal (AU_CP) de propagación entre al menos un primer usuario A y un segundo usuario B provistos, cada uno, de uno o de varios emisores/receptores ($A_1 \ldots A_{NA}$) de transmisión indexados por n y n' para el usuario A, ($B_1 \ldots B_{NB}$) indexados por m y m' para el usuario B, **caracterizado porque** comprende al menos las etapas siguientes:

Inicialización:

a) (41), Emisión por cada emisor A_n de usuario A de señales $S^{(0)}_{Int,n}$ de interrogación iniciales para el emisor de índice n, constituidas por al menos una secuencia $PN^{(0)}_{Int,n}$ aleatoria conocida por el usuario B, de factor $SF^{(0)}_{Int,n}$ de dispersión,

b) (43), Recepción y agrupación para cada receptor $B_{m'}$ del usuario B de la secuencia $PN^{(0)}_{Int,n}$ aleatoria de cada una de las señales $S^{(0)}_{Int,n}$ de interrogación iniciales (42), medidas por dichos receptores $B_{m'}$ del canal $H^{(0)}_{AB,n,m'}$ de propagación, entre A_n y $B_{m'}$ sobre la longitud de $L^{(0)}$ muestreos; estimación de los coeficientes $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ de la respuesta de impulso complejo correspondiente a los coeficientes de la respuesta de frecuencia compleja correspondiente,

c) Cuantificación (44) por el usuario B de los coeficientes $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ complejos que provienen de sus medidas para producir valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos,

d) Emisión (45) para cada emisor B_m del usuario B de señales $S^{(0)}_{Acq,m}$ de acuse de recibo constituidas de al menos una secuencia aleatoria denominada $PN^{(0)}_{Acq,m}$ conocida por el usuario A, de factor $SF^{(0)}_{Acq,m}$ de dispersión

e) Recepción y agrupación para cada receptor $A_{n'}$ de la secuencia $PN^{(0)}_{acq,m}$ aleatoria de cada una de las señales $S^{(0)}_{Acq,m}$ de acuse de recibo iniciales (46), medida por dichos receptores $A_{n'}$ del canal $H^{(0)}_{BA,m,n'}$ de propagación entre B_m y $A_{n'}$ sobre la longitud de $L^{(0)}$ muestreos; estimación de los coeficientes $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ de la respuesta de impulso complejo correspondiente o de los coeficientes de respuesta de frecuencia compleja correspondiente (47), siendo idénticos los coeficientes $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ estimados por B en la etapa c) $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ cuando el canal de propagación es recíproco y los emisores receptores considerados para A y B coinciden en los dos sentidos de interrogación y de acuse de recibo, con n=n' y m=m',

f) Cuantificación (48) por el usuario A de los coeficientes $H^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ complejos que provienen de sus medidas para producir valores $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$, numéricos

Iteración 1:

g) Emisión (49) para cada uno de los emisores A_n de nuevas señales $S^{(1)}_{Int,n}$ de interrogación constituidas por al menos una nueva secuencia $PN^{(1)}_{Int,n}$ aleatoria de factor de $SF^{(1)}_{Int,n}$ de dispersión elegida en un conjunto predeterminado conocido de A y B o construida según un proceso predeterminado conocido por A y B tras los valores $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$, numéricos determinados por A al final de la etapa f),

h) Recepción y agrupación de la secuencia $PN^{(1)}_{Int,n}$ de la señal $S^{(1)}_{Int,n}$ para cada receptor $B_{m'}$, (50) B_m que reconstruye con anterioridad la secuencia $PN^{(1)}_{Int,n}$ aleatoria elegida o construida por $A_{n'}$ según el mismo proceso que $A_{n'}$ explotando los valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos determinados por B durante la cuantificación efectuada en la etapa c) de los coeficientes $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$, valores numéricos iguales a los producidos por A en la etapa f) cuando el canal de propagación es recíproco, que n=n' y que m=m'); cuando n=n' y m=m', validación por B, gracias a la agrupación de $PN^{(1)}_{Int,n}$ en recepción por $B_{m'}$ de la igualdad entre coeficientes $Q^{(0)}_{AB,n,m}(l_1)_{l_1=0,\ldots,L-1} = Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$ cuantificados durante la fase de inicialización (51), medidos actualizados para cada receptor $B_{m'}$ del canal $H^{(1)}_{AB,n,m'}$ de propagación entre A_n y $B_{m'}$ sobre la longitud de $L^{(1)}$ muestreos, estimación de los coeficientes $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ de la respuesta de impulso complejo correspondiente o de los coeficientes de la respuesta de frecuencia compleja correspondiente (52),

i) Cuantificación (53) por el usuario B de los coeficientes $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ que provienen de sus medidas para producir valores $Q^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\ldots,L-1}$ numéricos

j) Emisión (54) por cada emisor B_m de nuevas señales de acuse de recibo, denominadas $S^{(1)}_{Acq,m'}$ constituidas de al menos una secuencia aleatoria denominada $PN^{(1)}_{Acq,m}$ de factor $SF^{(1)}_{Acq,m}$ de dispersión, elegida en un conjunto predeterminado conocido por A y B o construidos según un proceso predeterminado conocido por A y B tras los valores $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ numéricos determinados por B al final de la etapa c),

k) Recepción y dispersión por cada receptor $A_{n'}$ de las secuencias $PN^{(1)}_{acq,m}$ aleatorias de cada una de las señales ($S^{(1)}_{Acq,m}$) (55), $A_{n'}$ que reconstituye con anterioridad la secuencia $PN^{(1)}_{acq,m}$ elegida o construida por $B_{m'}$ según el mismo proceso que $B_{m'}$ explotando los valores $Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\dots,L-1}$ numéricos que A ha determinado en la etapa f) valores numéricos iguales a los producidos por B en la etapa c), es decir $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ numéricos cuando el canal de propagación es recíproco, que n=n' y que m=m'); cuando n=n' y m=m', validación por A, gracias a la agrupación de $PN^{(1)}_{Acq,m'}$ de la igualdad entre coeficientes $Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\dots,L-1} = Q^{(0)}_{AB,n,m}(l_1)_{l_1=0,\dots,L-1}$ cuantificados durante la fase de inicialización (56); la asociación univalente de los emisores/receptores A_n del usuario A y de los emisores/receptores B_m del usuario B por tanto se hace efectiva gracias a la relación de igualdad $Q^{(0)}_{AB,n,m}(l_1)_{l_1=0,\dots,L-1} = Q^{(0)}_{BA,m,n}(l_1)_{l_1=0,\dots,L-1}$ entre coeficientes cuantificados validada en B_m en la etapa h) por la recepción y la agrupación de $PN^{(1)}_{Int,n}$ y validados en A_n en esta etapa k), (56) por la recepción y la agrupación de $PN^{(1)}_{acq,m}$; medida por cada receptor $A_{n'}$ del canal $H^{(1)}_{BA,m,n'}$ entre B_m y $A_{n'}$ sobre la longitud de $L^{(1)}$ muestreos; estimación de los coeficientes $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ de la respuesta de impulso complejo (57), o de los coeficientes de la respuesta de frecuencia compleja, siendo idénticos los coeficientes $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ a los estimados por B en la etapa h), $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ cuando el canal de propagación es recíproco y los emisores receptores considerados para A y B coinciden en los dos sentidos de interrogación y de acuse de recibo, n=n' y m=m',

l) Cuantificación por el usuario A de los coeficientes $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ complejos que provienen de sus medidas para producir los coeficientes $Q^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ numéricos (58).

2. Procedimiento según la reivindicación 1, **caracterizado porque** comprende al menos una segunda iteración de las etapas de la primera iteración con la emisión de señales $S^{(2)}_{Int,n}$ de interrogación que contienen la secuencia $PN^{(2)}_{Int,n}$ y de señales $S^{(2)}_{Acq,m}$ de acuse de recibo que contienen la secuencia $PN^{(2)}_{Acq,m}$ elaboradas tras los resultados de medida $H^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ y $H^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ y tras los resultados de cuantificación $Q^{(1)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ y $Q^{(1)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ producidos en la iteración 1, la cuantificación de nuevos coeficientes $Q^{(2)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ y $Q^{(2)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$, y la asociación univalente y unívoca de los emisores/receptores A_n del usuario A y de los emisores/receptores B_m del usuario B por la relación entre coeficientes cuantificados durante la iteración 1 $Q^{(1)}_{AB,n,m}(l_1)_{l_1=0,\dots,L-1} = Q^{(1)}_{BA,m,n}(l_1)_{l_1=0,\dots,L-1}$, asociación validada por la recepción y la agrupación de secuencias $PN^{(2)}_{Int,n}$ de interrogación y $PN^{(2)}_{Acq,m}$ de acuse de recibo emitidas por A_n y B_m durante la segunda iteración.

3. Procedimiento según la reivindicación 2, **caracterizado porque** comprende en cada nueva iteración k+1, con k superior a 1, la emisión de señales $S^{(k+1)}_{Int.n}$ de interrogación que contienen la secuencia $PN^{(k+1)}_{Int,n}$ y señales $S^{(k+1)}_{Acq,m}$ de acuse de recibo que contienen la secuencia $PN^{(k+1)}_{Acq,m}$ construidas tras los resultados de medida de la iteración k $H^{(k)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ y $H^{(k)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$ y tras los resultados de cuantificación de la iteración k $Q^{(k)}_{AB,n,m'}(l_1)_{l_1=0,\dots,L-1}$ y $Q^{(k)}_{BA,m,n'}(l_1)_{l_1=0,\dots,L-1}$, y la asociación univalente y unívoca de los emisores/receptores A_n del usuario A y de los emisores/receptores B_m del usuario B, utilizando la relación $Q^{(k)}_{AB,n,m}(l_1)_{l_1=0,\dots,L-1} = Q^{(k)}_{BA,m,n}(l_1)_{l_1=0,\dots,L-1}$ entre coeficientes cuantificados durante la iteración k, asociación validada por la recepción y la agrupación por B_m y A_n de las señales de interrogación y de acuse de recibo emitidas por A_n y B_m durante la (k+1)ésima iteración.

4. Procedimiento según una de las reivindicaciones anteriores **caracterizado porque** utiliza en las etapas de cuantificación c) y f) durante la iniciación, en las etapas i) y l) durante la iteración 1 y en las etapas similares durante iteraciones siguientes, una función de selección y decodificación correctora de los coeficientes de canales $H^{(k)}_{AB,n,m}(l_1)_{l_1=0,\dots,L-1}$ y $H^{(k)}_{BA,m,n}(l_1)_{l_1=0,\dots,L-1}$, adaptada para retener únicamente los coeficientes cuya estimación es la más fiable, por aplicación de un criterio de valor umbral sobre la calidad de la estimación de los coeficientes citados anteriormente y de una corrección de error sobre las salidas de cuantificación $Q^{(k)}_{AB,n,m}(l_1)_{l_1=0,\dots,L-1}$ y

$Q^{(k)}_{BA,m,n}(l_1)_{l_1=0,\ldots,L-1}$, estando predefinidos este criterio de valor de umbral y esta corrección entre los usuarios A y B.

5. Procedimiento según una de las reivindicaciones anteriores **caracterizado porque** B_m utiliza, en la etapa d) de la fase de inicialización, un proceso de construcción específico de las señales $S'^{(0)}_{Acq,m}$ de acuse de recibo iniciales modificadas que hacen depender las mismas de todas las primeras medidas $H^{(0)}_{AB,n,m'}$ de canales y de los coeficientes $Q^{(0)}_{AB,n,m},(l_1)_{l_1=0,\ldots,L-1}$ cuantificados correspondientes, a la vez que se establece la posibilidad para los receptores $A_{n'}$ del usuario A de reconstruir y de agrupar las señales $S'^{(0)}_{Acq,m}$, comprendiendo dicha señales de acuse de recibo iniciales modificadas al menos dos secuencias PN, denominadas $PN^{(0)}_{Acq,m}$ y $PN'^{('0)}_{Acq,m}$, emitidas sucesiva o simultáneamente, siendo conocida la primera de las secuencias $PN^{(0)}_{Acq,m}$ por A como en la etapa d), siendo elegida la segunda de las secuencias $PN'^{('0)}_{Acq,m}$ en un conjunto predeterminado conocido por B y por A o construida según un proceso predeterminado conocido por B y por A tras los valores $Q^{(0)}_{AB,n,m},(l_1)_{l_1=0,\ldots,L-1}$ numéricos que se acaban de cuantificar por B al final de la etapa c); **y porque** An' aplica a las etapas e) y f) de inicialización no solamente una recepción y una agrupación de la secuencia $PN^{(0)}_{Acq,m}$ sino también una reconstrucción de la secuencia $PN'^{('0)}_{Acq,m}$ tras las estimaciones del canal $H^{(0)}_{BA,m,n},(l_1)_{l_1=0,\ldots,L-1}$ y las cuantificaciones $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ que conduce gracias a la agrupación de $PN^{(0)}_{Acq,m}$ en las etapas e) y f) seguida de una agrupación de la secuencia $PN'^{('0)}_{Acq,m}$, para producir una validación inmediata de la igualdad entre los coeficientes $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ y $Q^{(0)}_{AB,n,m},(l_1)_{l_1=0,\ldots,L-1}$ cuantificados en fase de inicialización.

6. Procedimiento según la reivindicación 3, **caracterizado porque** comprende en cada nueva iteración k+1, con k superior o igual a 0, la emisión de señales $S^{(k+1)}_{Acq,m}$ de acuse de recibo que contienen al menos dos secuencias $PN^{(k+1)}_{Acq,m}$ y $PN'^{(k+1)}_{Acq,m}$ emitidas secuencial o simultáneamente, siendo elegida $PN^{(k+1)}_{Acq,m}$ en un conjunto predeterminado o construido adaptativamente tras los resultados $Q^{(k)}_{AB,n,m},(l_1)_{l_1=0,\ldots,L-1}$ de cuantificación en la iteración nºk, y siendo elegida $PN'^{(k+1)}_{Acq,m}$ en un conjunto predeterminado o construida adaptativamente tras los resultados $Q^{(k+1)}_{AB,n,m},(l_1)_{l_1=0,\ldots,L-1.}$ de cuantificación actuales en la iteración nº k+1; caracterizado por otra parte **porque** $A_{n'}$ aplica no solamente una recepción y una agrupación de la secuencia $PN^{(k+1)}_{Acq,m}$ reconstruida tras sus coeficientes $Q^{(k)}_{BA,m,n},(l_1)_{l_1=0,\ldots,L-1}$ cuantificados, sino también una reconstrucción de la secuencia $PN'^{(k+1)}_{Acq,m}$ tras las estimaciones del canal $H^{(k+1)}_{BA,m,n},(l_1)_{l_1=0,\ldots,L-1}$ y las cuantificaciones $Q^{(k+1)}_{BA,m,n'}(l_1)_{l_1=0,\ldots,L-1}$ que conducen gracias a la agrupación de $PN^{(k+1)}_{Acq,m}$, seguida de una agrupación de la secuencia $PN'^{(k+1)}_{Acq,m}$ para validar inmediatamente la igualdad entre los coeficientes $Q^{(k+1)}_{AB,n,m},(l_1)_{l_1=0,\ldots,L-1.}$ y $Q^{(k+1)}_{BA,m,n},(l_1)_{l_1=0,\ldots,L-1}$ cuantificados en la iteración k+1.

7. Procedimiento según una de las reivindicaciones anteriores **caracterizado porque** los emisores de A utilizan señales de interrogación iniciales elegidas aleatoriamente en un conjunto de señales conocidas por B, y porque los receptores de B sólo acusan recibo de una de las señales de interrogación iniciales recibidas, o bien predeterminadas por las características de los receptores de B, o bien elegidas anteriormente por los receptores de B, tras la sincronización, de la agrupación y la medida de dichas señales de interrogación iniciales.

8. Procedimiento según una de las reivindicaciones anteriores **caracterizado porque** los emisores de B utilizan, por ejemplo, señales de acuse de recibo iniciales elegidas aleatoriamente en un conjunto de señales conocidas por A, **porque** los receptores de A sólo tratan en recepción ciertas de las señales de acuse de recibo iniciales recibidas, o bien predeterminadas por las características de los receptores de A, o bien elegidas aleatoriamente por los receptores de A, tras la sincronización, de la agrupación y de la medida de dicha señales de acuse de recibo iniciales.

9. Procedimiento según una de las reivindicaciones anteriores **caracterizado porque** los emisores de A pueden aplicar una fluctuación de fase aleatoria en tiempo a las señales de interrogación y los emisores de B aplican una fluctuación de fase aleatoria en tiempo a las señales de acuse de recibo.

10. Procedimiento según una de las reivindicaciones anteriores **caracterizado porque** utiliza señales de interrogación y de acuse de recibo SI_A y SA_B emitidas conjuntamente en la señales de baliza de uno y otro usuario A o B, AI_A y AI_B, es decir de manera autointerferida, siendo emitidas, recibidas y tratadas dichas señales de interrogación y de acuse de recibo en cada iteración k gracias a parametrizaciones adaptadas a sus potencias de emisión por A y B, $SI^{(k)}_A$ y $SA^{(k)}_B$, de sus niveles de recepción en B y en A, de interferencias inducidas por la baliza de A recibida en B y por la baliza de B recibida en A, $AI^{(k)}_{A->B}$ y $AI^{(k)}_{B->A}$, de los niveles de recepción en B y en A de las autointerferencias que provienen de B y de A, $AI^{(k)}_{A->A}$ y $AI^{(k)}_{B->B}$, de los dispositivos de autorrechazo de las autointerferencias a la recepción en A y en B, $RAI_{A->A}$ y $RAI_{B->B}$, de los factores de dispersión a la emisión en A y B, $SF^{(k)}_{Int,n}$ y $SF^{(k)}_{Acq,m}$, según las igualdades y desigualdades siguientes expresadas en decibelios:

- en las recepciones del usuario B:

$$AI^{(k)}_{A->B} = AI^{(k)}_{A} - L^{(k)}_{A->B}$$

$$SI^{(k)}_{A->B} = SI^{(k)}_{A} - L^{(k)}_{A->B}$$

donde $L^{(k)}_{A->B}$ representa las pérdidas totales de propagación de A hacia B,

$$SF^{(k)}_{Int,n} \geq 10.\log_{10}[10\text{^}(SI^{(k)}_{A->B}/10)] - 10.\log_{10}[10\text{^}((AI_{B->B}-RAI_{B->B})/10) + 10\text{^}(AI^{(k)}_{A->B}/10)] + \eta_B,$$

- en las recepciones del usuario A:

$$AI^{(k)}_{B->A} = AI^{(k)}_{B} - L^{(k)}_{B->A}$$

$$SI^{(k)}_{B->A} = SI^{(k)}_{A} - L^{(k)}_{B->A}$$

donde $L^{(k)}_{B->A}$ representa las pérdidas totales de propagación de B hacia A,

$$SF^{(k)}_{Int,n} \geq 10.\log_{10}[10\text{^}(SI^{(k)}_{B->A}/10)] - 10.\log_{10}[10\text{^}((AI_{A->A}-RAI_{A->A})/10) + 10\text{^}(AI^{(k)}_{B->A}/10)] + \eta_A,$$

estando relacionados los márgenes $\acute{\eta}_B$ y $\acute{\eta}_A$ con los rendimientos de los equipos de radio utilizados por los receptores de A y de B.

11. Procedimiento según la reivindicación 10, **caracterizado porque** utiliza señales de interrogación y de acuse de recibo emitidas conjuntamente en los mensajes de intercambios de datos entre los usuarios, es decir de manera autointerferida, siendo emitidas, recibidas y tratadas dichas señales de interrogación y de acuse de recibo en cada iteración k gracias a parametrizaciones adaptadas a sus potencias de emisión por A y B, a sus niveles de recepción en A y B tras la propagación, a las interferencias inducidas por los mensajes de A recibidos en B y por los mensajes de B recibidos en A, a los niveles de recepción en B y en A de las autointerferencias que provienen de B y de A, a los dispositivos de autorrechazo de estas autointerferencias en la recepción en A y en B, a factores de elementos en la admisión en A y B), según las desigualdades en las expresiones similares a la reivindicación 10.

12. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** utiliza un modo de comunicación Duplex temporal entre usuarios que emplean una misma frecuencia portadora para los intercambios en emisión y en recepción en los dos sentidos de transmisión y que se beneficie directamente de la reciprocidad del canal de propagación sobre la frecuencia única empleada por las interrogaciones y los acuses de recibo.

13. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** se duplica sobre el conjunto de las frecuencias portadoras empleadas por los usuarios en modo Duplex de frecuencia que emplean frecuencias portadoras diferentes para sus intercambios en emisión y en recepción según el sentido de trasmisión, con el fin de beneficiarse de la reciprocidad del canal de propagación sobre cada una de las frecuencias empleadas por las interrogaciones y los acuses de recibo.

14. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** se retiran las etapas del procedimiento para cada nueva transmisión de telefonía o de datos.

15. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** se retiran las etapas del procedimiento para cada nuevo mensaje de una trasmisión de telefonía o de datos en curso.

16. Procedimiento según una de la reivindicación es anteriores, **caracterizado porque** utiliza emisores y receptores adaptados a radiocomunicaciones.

17. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** los emisores/receptores del usuario A están conectados a los elementos de antenas de una red utilizada por A y los emisores/receptores del usuario B están conectados a los elementos de antena de una red utilizada por B en el marco de protocolos denominados de tipo MISO, SIMO, MIMO o "*massive MIMO*".

18. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** los emisores/receptores del usuario A son estaciones base o nodos de una red de radiocomunicación y los emisores/receptores del usuario B son terminales u otros nodos de dicha red de radiocomunicación.

19. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** los emisores y receptores están adaptados a transmisiones acústicas.

20. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** los emisores y receptores están adaptados a transmisiones ópticas.

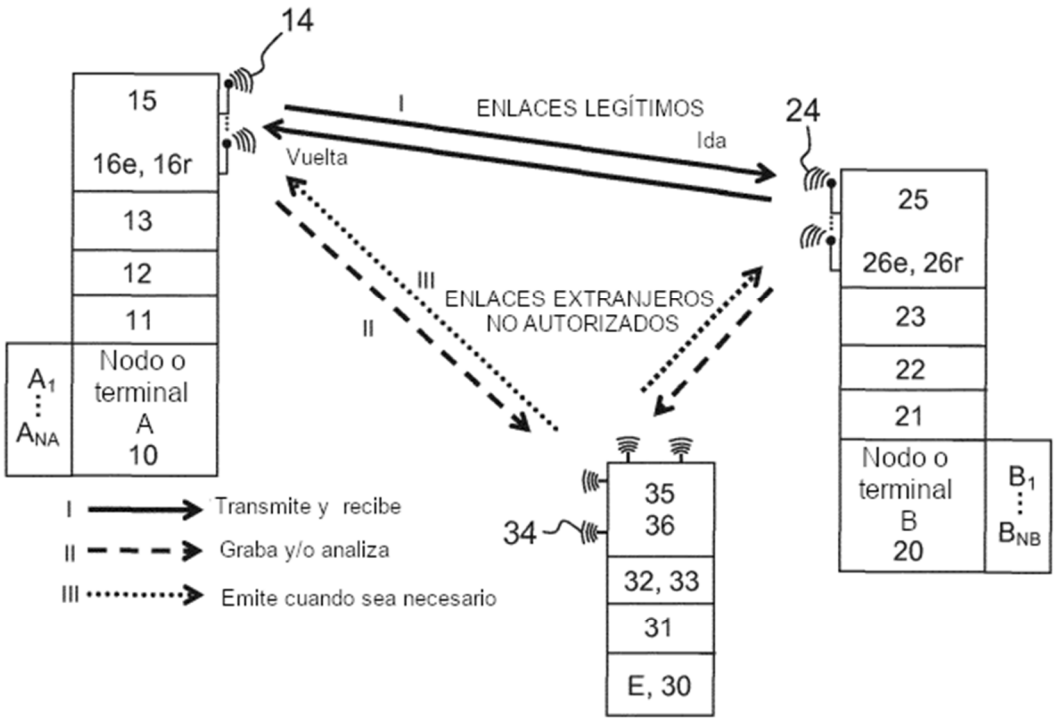
14
15
16e, 16r
13
12
11
Nodo o terminal A 10
A1
ANA
I
ENLACES LEGÍTIMOS
Ida
Vuelta
24
25
26e, 26r
23
22
21
Nodo o terminal B 20
B1
BNB
III
ENLACES EXTRANJEROS NO AUTORIZADOS
II
34
35
36
32, 33
31
E, 30
I Transmite y recibe
II Graba y/o analiza
III Emite cuando sea necesario

FIG.1

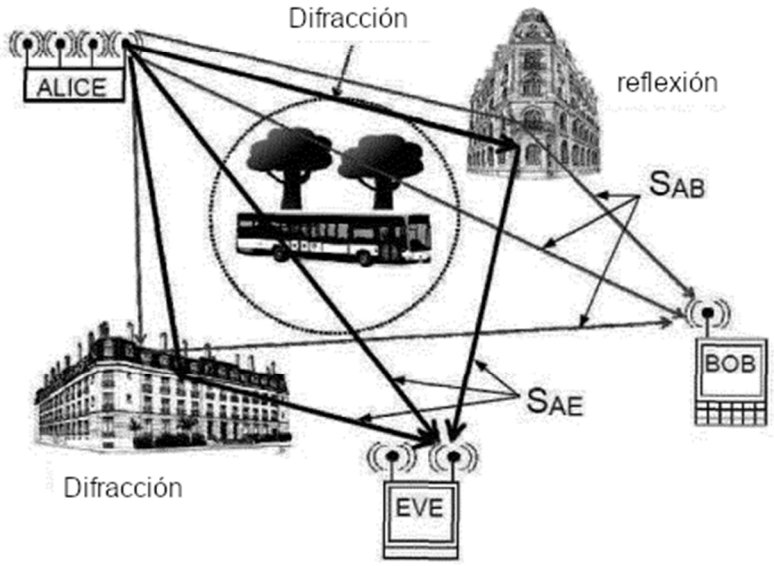
Difracción
reflexión
ALICE
SAB
BOB
SAE
Difracción
EVE

FIG.2

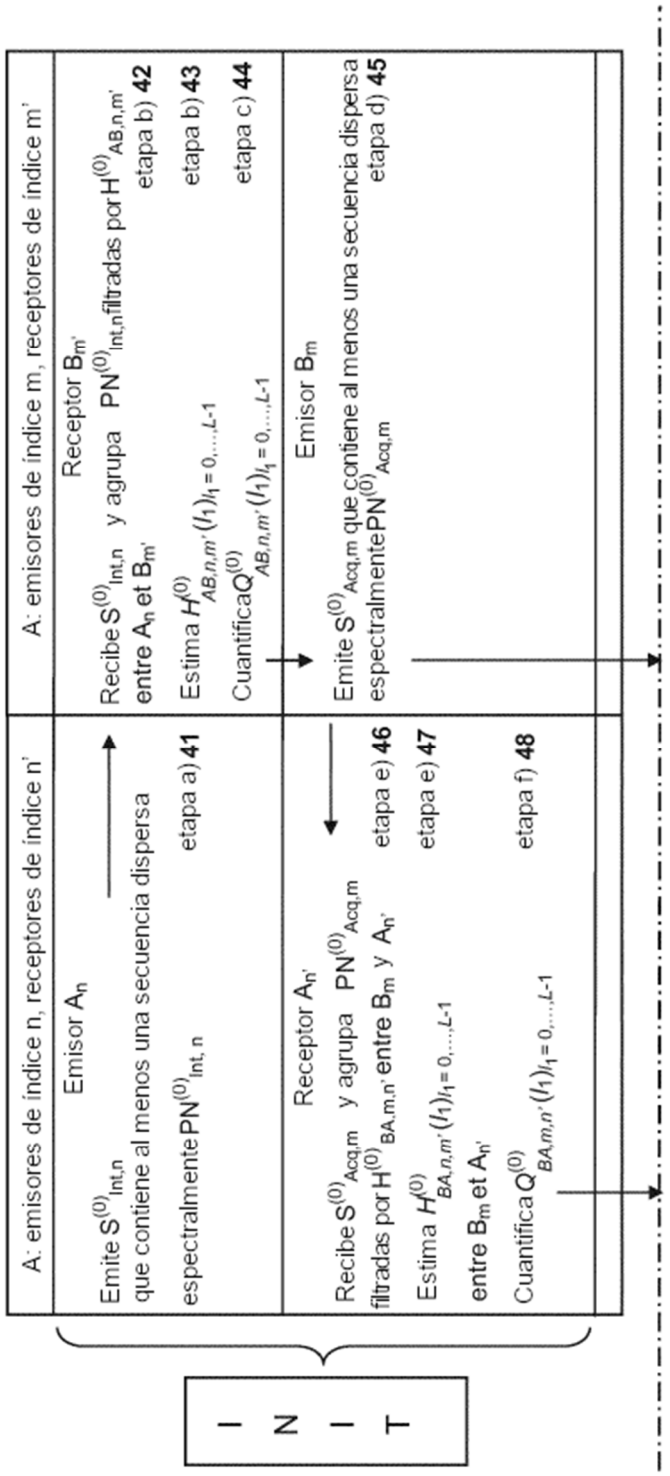
A: emisores de índice n, receptores de índice n'
A: emisores de índice m, receptores de índice m'
Emisor A_n
Receptor $B_{m'}$
Emite $S^{(0)}_{Int,n}$ que contiene al menos una secuencia dispersa espectralmente $PN^{(0)}_{Int,n}$ etapa a) 41
Recibe $S^{(0)}_{Int,n}$ y agrupa $PN^{(0)}_{Int,n}$ filtradas por $H^{(0)}_{AB,n,m'}$ entre A_n et $B_{m'}$ etapa b) 42
Estima $H^{(0)}_{AB,n,m'}(l_1)_{l_1=0,...,L-1}$ etapa b) 43
Cuantifica $Q^{(0)}_{AB,n,m'}(l_1)_{l_1=0,...,L-1}$ etapa c) 44
Receptor $A_{n'}$
Emisor B_m
Recibe $S^{(0)}_{Acq,m}$ y agrupa $PN^{(0)}_{Acq,m}$ filtradas por $H^{(0)}_{BA,m,n'}$ entre B_m y $A_{n'}$ etapa e) 46
Emite $S^{(0)}_{Acq,m}$ que contiene al menos una secuencia dispersa espectralmente $PN^{(0)}_{Acq,m}$ etapa d) 45
Estima $H^{(0)}_{BA,n,m'}(l_1)_{l_1=0,...,L-1}$ entre B_m et $A_{n'}$ etapa e) 47
Cuantifica $Q^{(0)}_{BA,m,n'}(l_1)_{l_1=0,...,L-1}$ etapa f) 48
INIT

FIG.3

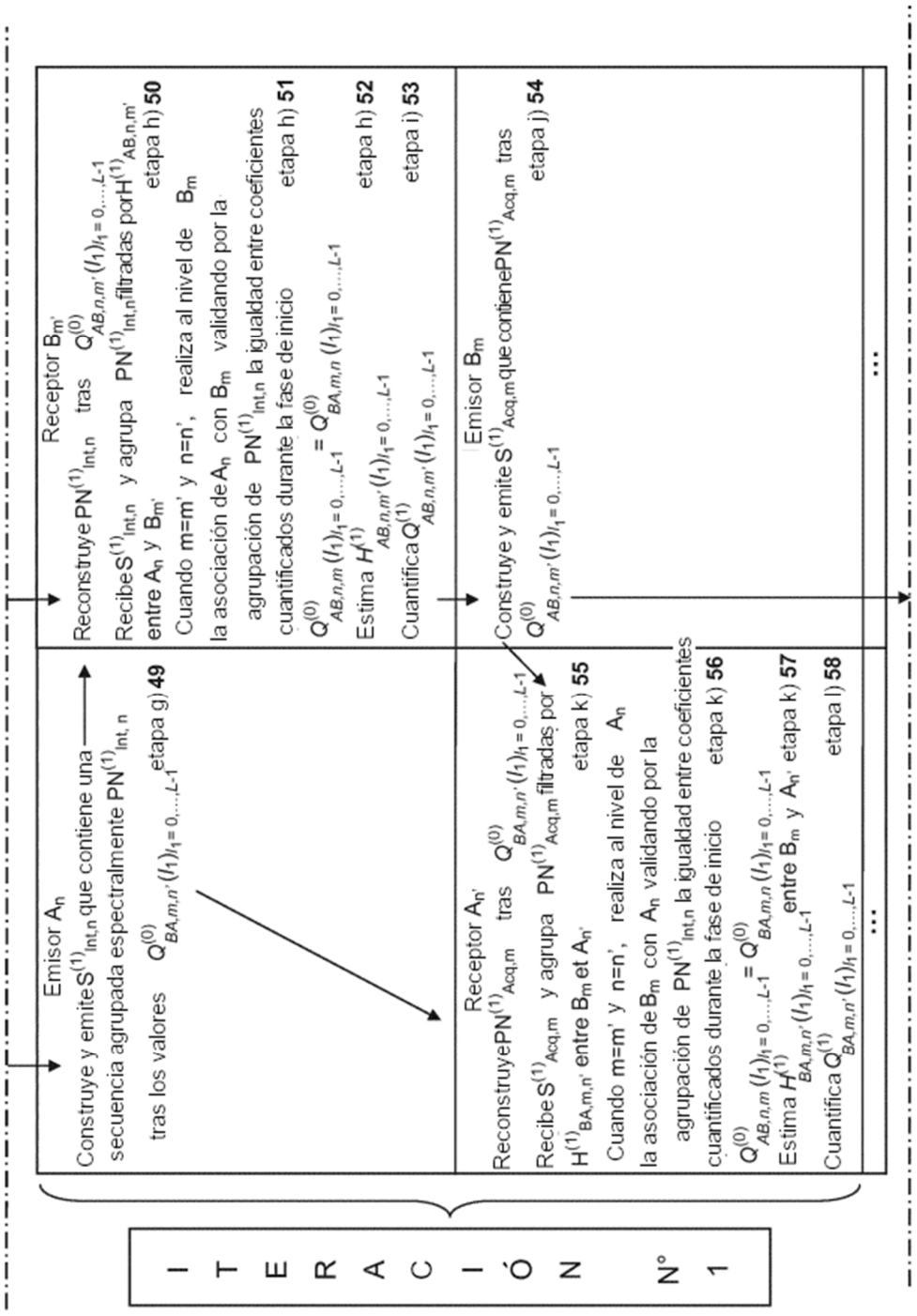

FIG.3 (continúa)

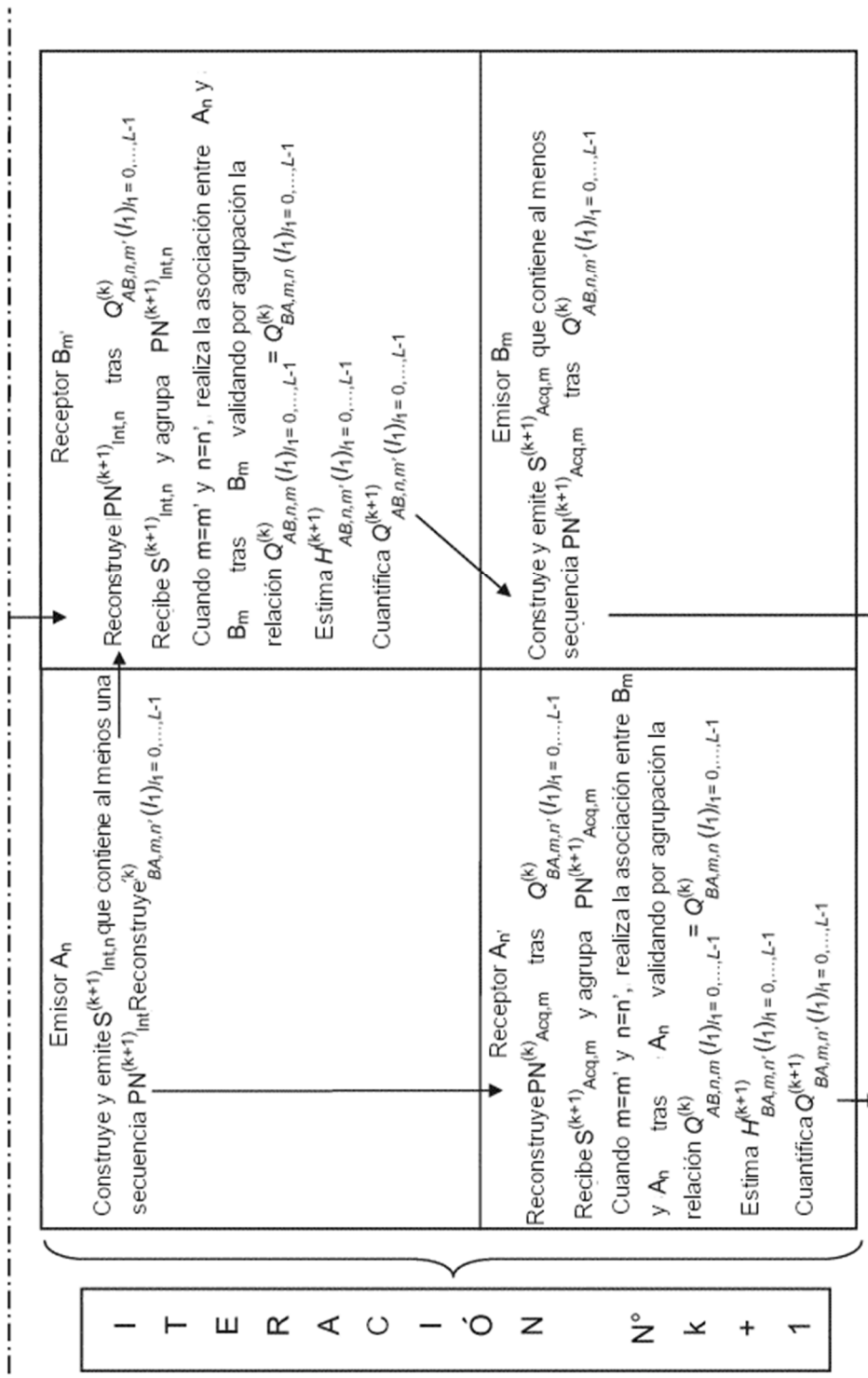
ITERACIÓN Nº k + 1
Emisor A_n
Construye y emite $S^{(k+1)}_{Int,n}$ que contiene al menos una secuencia $PN^{(k+1)}_{Int}$ Reconstruye $Q^{(k)}_{BA,m,n'}(l_1)_{l_1=0,...,L-1}$
Receptor $B_{m'}$
Reconstruye $PN^{(k+1)}_{Int,n}$ tras $Q^{(k)}_{AB,n,m'}(l_1)_{l_1=0,...,L-1}$
Recibe $S^{(k+1)}_{Int,n}$ y agrupa $PN^{(k+1)}_{Int,n}$
Cuando m=m' y n=n', realiza la asociación entre A_n y B_m tras B_m validando por agrupación la relación $Q^{(k)}_{AB,n,m}(l_1)_{l_1=0,...,L-1} = Q^{(k)}_{BA,m,n}(l_1)_{l_1=0,...,L-1}$
Estima $H^{(k+1)}_{AB,n,m'}(l_1)_{l_1=0,...,L-1}$
Cuantifica $Q^{(k+1)}_{AB,n,m'}(l_1)_{l_1=0,...,L-1}$
Receptor $A_{n'}$
Reconstruye $PN^{(k)}_{Acq,m}$ tras $Q^{(k)}_{BA,m,n'}(l_1)_{l_1=0,...,L-1}$
Recibe $S^{(k+1)}_{Acq,m}$ y agrupa $PN^{(k+1)}_{Acq,m}$
Cuando m=m' y n=n', realiza la asociación entre B_m y A_n tras validando por agrupación la relación $Q^{(k)}_{AB,n,m}(l_1)_{l_1=0,...,L-1} = Q^{(k)}_{BA,m,n}(l_1)_{l_1=0,...,L-1}$
Estima $H^{(k+1)}_{BA,m,n'}(l_1)_{l_1=0,...,L-1}$
Cuantifica $Q^{(k+1)}_{BA,m,n'}(l_1)_{l_1=0,...,L-1}$
Emisor B_m
Construye y emite $S^{(k+1)}_{Acq,m}$ que contiene al menos secuencia $PN^{(k+1)}_{Acq,m}$ tras $Q^{(k)}_{AB,n,m'}(l_1)_{l_1=0,...,L-1}$

FIG.3 (fin)