(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 633 657**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.01.2010 PCT/US2010/022134**

(87) Fecha y número de publicación internacional: **29.07.2010 WO10085813**

(96) Fecha de presentación y número de la solicitud europea: **26.01.2010 E 10701792 (3)**

(97) Fecha y número de publicación de la concesión europea: **26.04.2017 EP 2389749**

(54) Título: **Procedimiento, NODO de comunicaciones y producto de programa informático para la determinación de la confiabilidad**

(30) Prioridad:

26.01.2009 US 359534

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.09.2017

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
International IP Administration 5775 Morehouse Drive
San Diego, California 92121-1714, US

(72) Inventor/es:

HADDAD, WASSIM MICHEL;
CORSON, M. SCOTT y
PARK, VINCENT D.

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Procedimiento, NODO de comunicaciones y producto de programa informático para la determinación de la confiabilidad

CAMPO

Diversos modos de realización se refieren a procedimientos y aparatos de comunicación inalámbrica y, más particularmente, a procedimientos y aparatos de comunicación inalámbrica para comunicar información y crear confianza entre diversos dispositivos de comunicaciones, por ejemplo, NODOS, que soporten señalización entre pares.

ANTECEDENTES

Las comunicaciones inalámbricas están ganando cada vez más aceptación y se utilizan cada vez más como un medio conveniente para comunicar muchos tipos de información, además de usarse para llamadas de voz. Un área que experimenta un rápido crecimiento es el campo de las redes ad hoc que utilizan comunicaciones entre pares. En un entorno ad hoc y geográficamente limitado, sería deseable que un usuario pudiera transmitir tipos diferentes de mensajes, por ejemplo, anuncios, peticiones, noticias, etc., a cada uno de los otros usuarios ubicados dentro del intervalo de su dispositivo. Sin embargo, un usuario receptor, que nunca haya tratado con el emisor antes, tal vez no tenga forma de determinar si puede confiarse o no en el emisor y si vale la pena o no gastar tiempo para responder al mensaje del emisor. Obsérvese que dicha falta de confianza entre los usuarios es independiente de poder validar la firma transmitida por el mensaje. De hecho, un usuario malintencionado puede firmar y transmitir, por ejemplo, multidifundir, un mensaje y los receptores pueden validar la firma, pero esto no significa que el emisor sea sincero acerca de su intención. Como consecuencia, un usuario que actúe sobre un mensaje recibido desde un usuario no fiable o malintencionado puede terminar como víctima. Un problema de confianza similar se produce desde la perspectiva del emisor con respecto a la respuesta de los usuarios que el emisor ya no conozca.

El documento "Perich F. et al: "In reputation we believe: query processing in mobile ad-hoc networks" Mobile and Ubiquitous Systems: Networking and Services, 2004. Mobiquitous 2004. First annual international conference. Boston, EE. UU, 22-26 de agosto de 2004, Piscataway, EE. UU., IEEE, 22 de agosto de 2004, pág. 326-334, ISBN 978-0-7695-2208-1" se refiere a un modelo de creencias distribuidas. Se envía un mensaje de respuesta (ID, A, precisión...) con la respuesta A y la precisión correspondiente desde una IDs de dispositivo de fuente a una ID_Q de dispositivo de consulta. Una respuesta de recomendación (ID_R, ID_S, T_R (S)) se envía desde una ID_R de par remoto, que se cree que es un par de confianza, al ID_Q de dispositivo de consulta que especifica el grado de confianza T_R (S) del dispositivo remoto en una IDs de dispositivo de fuente. El dispositivo de consulta calcula un grado de precisión combinado para una respuesta recibida desde fuentes diferentes ponderando las precisiones individuales mediante el grado de confianza de la fuente.

El documento "Alfarez Abdul-Rahman, Stephen Hailes: "A distributed trust mode", Proc. 1997 workshop on new security paradigms, 23 de septiembre de 1997, 26 de septiembre de 1997, pág. 48-60, Langdale, Reino Unido, ISBN 0-89791-986-6 " se refiere a un modelo de confianza distribuida. Un solicitante está pidiendo la recomendación de un recomendador acerca de un objetivo para una categoría de confianza particular. Cada petición de recomendación se envía al conjunto del recomendador de recomendadores de confianza en la categoría. Por tanto, por ejemplo, Alice puede recibir recomendaciones sobre Eric a través de Cathy y de Bob.

El documento WO 2004/107137 A2 se refiere a la autenticación de mensajes electrónicos. Divulga un vServidor que se comunica con el emisor y con el destinatario a través de un túnel basado en HT-TPS o SSL. El emisor pide un ACID del vServidor 22 enviando la identificación del emisor y la información de autenticación. El vServidor devuelve el ACID al emisor que inserta el ACID en el mensaje enviado al destinatario. El destinatario envía el ACID al vServidor. Después de autenticar la identidad del destinatario, el servidor valida el ACID y devuelve el vindicador al destinatario.

Basándose en el análisis anterior, sería ventajoso que pudieran desarrollarse nuevos procedimientos y/o aparatos que permitieran a los dispositivos inalámbricos reunir y/o intercambiar información relativa a la confianza. Serían también beneficiosos nuevos procedimientos y aparatos que faciliten una determinación de la confiabilidad de la información comunicada en un mensaje.

SUMARIO

Se describen procedimientos y aparatos relativos a la determinación de la confiabilidad de la información comunicada en un mensaje y/o al intercambio de información de confianza. Diversos procedimientos y aparatos descritos se adaptan bien a las comunicaciones inalámbricas entre pares en una red ad-hoc.

Algunos procedimientos y aparatos se refieren a un dispositivo de comunicaciones que determina la confiabilidad de un mensaje recibido. Por ejemplo, en una red de comunicación entre pares ad hoc, en un momento dado, un primer

NODO de comunicaciones puede tener una relación de confianza con un primer conjunto de NODOS. NODOS diferentes de comunicaciones en la red pueden tener relaciones de confianza con conjuntos diferentes de NODOS. Puede existir, y típicamente existe, al menos algún solapamiento entre al menos algunos de los conjuntos diferentes de NODOS. De acuerdo con una característica de algunos modos de realización, este solapamiento se utiliza para propagar información de confianza. En algunos modos de realización, el primer dispositivo de comunicaciones puede recibir un mensaje desde un segundo dispositivo de comunicaciones que no sea un elemento del primer conjunto de NODOS. El primer dispositivo de comunicaciones puede recibir también información relativa a la confianza desde uno de los elementos del primer conjunto de NODOS en un segundo mensaje. El primer dispositivo de comunicaciones determina la confiabilidad de la información comunicada en el primer mensaje basándose en la información relativa a la confianza recibida desde el segundo mensaje. El primer dispositivo de comunicaciones toma una decisión informada sobre si actuar o no sobre el primer mensaje basándose en la determinación de su confiabilidad.

Un procedimiento a modo de ejemplo de funcionamiento de un primer NODO de comunicaciones, de acuerdo con un modo de realización a modo de ejemplo, comprende recibir un primer mensaje desde un segundo NODO de comunicaciones, comunicando dicho primer mensaje información, recibir un segundo mensaje desde un tercer NODO de comunicaciones con el cual existe una relación de confianza y determinar la confiabilidad de la información comunicada por el primer mensaje basándose en la información comunicada por el segundo mensaje. Un primer NODO de comunicaciones a modo de ejemplo, implementado de acuerdo con un modo de realización a modo de ejemplo, comprende al menos un procesador configurado para recibir un primer mensaje desde un segundo NODO de comunicaciones, comunicando dicho primer mensaje información, recibir un segundo mensaje desde un tercer NODO de comunicaciones con el cual existe una relación de confianza y determinar la confiabilidad de la información comunicada por el primer mensaje basándose en la información comunicada por el segundo mensaje. El primer NODO de comunicaciones puede incluir, y en algunos modos de realización lo hace, una memoria acoplada a dicho al menos un procesador.

Algunos procedimientos y aparatos se refieren a la propagación de información de confianza en una red de comunicación inalámbrica, por ejemplo, una red de comunicación inalámbrica ad hoc entre pares. Algunos modos de realización incluyen la generación y la transmisión de un nuevo mensaje de propagación de confianza. En algunos modos de realización, se usa un nuevo mensaje de petición de confirmación de confianza.

La invención define un procedimiento para hacer funcionar un primer NODO de comunicaciones en una red de comunicación inalámbrica entre pares de acuerdo con la reivindicación 1, un primer NODO de comunicación de acuerdo con la reivindicación 7 y un producto de programa informático de acuerdo con la reivindicación 11.

Aunque se hayan indicado diversos modos de realización en el sumario anterior, debería apreciarse que no necesariamente todos los modos de realización incluyen las mismas características y algunas de las características descritas anteriormente no son necesarias pero pueden ser deseables en algunos modos de realización. Numerosas características, modos de realización y beneficios adicionales de diversos modos de realización se indican en la descripción detallada siguiente.

BREVE DESCRIPCIÓN DE LAS FIGURAS

La Figura 1 ilustra una red de comunicación inalámbrica a modo de ejemplo, de acuerdo con un modo de realización a modo de ejemplo.

La Figura 2 ilustra intercambios de señalización a modo de ejemplo entre NODOS de comunicación y etapas asociadas con un procedimiento a modo de ejemplo que soporta mensajes de comunicación, por ejemplo, ofertas de servicio y/o anuncios, de acuerdo con un modo de realización a modo de ejemplo.

La Figura 3 ilustra intercambios de señalización a modo de ejemplo entre NODOS de comunicación y etapas asociadas con un procedimiento a modo de ejemplo que soporta mensajes de comunicación, por ejemplo, ofertas de servicio y/o anuncios, de acuerdo con otro modo de realización a modo de ejemplo.

La Figura 4 ilustra intercambios de señalización a modo de ejemplo entre NODOS de comunicación y etapas asociadas con un procedimiento a modo de ejemplo que soporta mensajes de comunicación, por ejemplo, ofertas de servicio y/o anuncios, de acuerdo con otro modo de realización más a modo de ejemplo.

La Figura 5 es un diagrama de flujo de un procedimiento a modo de ejemplo de funcionamiento de un dispositivo de comunicaciones de acuerdo con un modo de realización a modo de ejemplo.

La Figura 6 ilustra un formato de mensaje a modo de ejemplo para un segundo mensaje a modo de ejemplo, por ejemplo, un mensaje de propagación de confianza, de acuerdo con un modo de realización a modo de ejemplo.

La Figura 7 ilustra un NODO de comunicaciones a modo de ejemplo que puede usarse en la red de la Figura 1.

La Figura 8 ilustra un montaje de módulos que pueden usarse en el NODO de comunicaciones a modo de ejemplo de la Figura 7.

La Figura 9 es un diagrama de flujo de un procedimiento de comunicaciones a modo de ejemplo de acuerdo con un modo de realización a modo de ejemplo.

La Figura 10 ilustra un formato a modo de ejemplo de un mensaje de confirmación de petición a modo de ejemplo.

La Figura 11 ilustra otro formato a modo de ejemplo de un mensaje de confirmación de petición a modo de ejemplo.

La Figura 12 ilustra otro formato más a modo de ejemplo de un mensaje de confirmación de petición a modo de ejemplo.

La Figura 13 ilustra otro NODO de comunicaciones más a modo de ejemplo que puede usarse en la red de la Figura 1.

La Figura 14 ilustra un montaje de módulos que pueden usarse en el NODO de comunicaciones a modo de ejemplo de la Figura 13.

DESCRIPCIÓN DETALLADA

La Figura 1 es un dibujo de una red de comunicación 100 a modo de ejemplo, por ejemplo, una red de comunicación inalámbrica entre pares ad-hoc, implementada de acuerdo con un modo de realización a modo de ejemplo. La red de comunicación 100 a modo de ejemplo incluye una pluralidad de NODOS de comunicación (NODO de comunicación A 102, NODO de comunicación B 104, NODO de comunicación C 106, el I^{er} NODO de comunicación 108, NODO E 110 y ..., el N^{o} NODO de comunicación 112) que soportan comunicaciones inalámbricas, por ejemplo, comunicaciones inalámbricas entre pares. Aunque se hayan mostrado pocos NODOS de comunicaciones en la red de comunicación 100, debería apreciarse que la densidad de NODOS de comunicación en la red 100 puede variar, y a veces lo hace. Los NODOS de comunicaciones inalámbricas (102, 104, 106, 108, 110,..., 112) soportan diversas señalizaciones entre pares, por ejemplo, señales de descubrimiento entre pares, señales de petición de transmisión, mensajes de publicidad, etc. Los NODOS de comunicaciones inalámbricas (102, 104, 106, 108, 110,..., 112) pueden ser, por ejemplo, dispositivos accionados por baterías manuales.

De acuerdo con un escenario de un modo de realización a modo de ejemplo, el NODO de comunicación A 102 transmite, por ejemplo, multidifunde, un mensaje 120 a un número de NODOS de comunicaciones que pueden estar ubicados en una región geográfica local cubierta por la red de comunicación 100. En una variación a modo de ejemplo, el mensaje 120 se transmite múltiples veces por el NODO A 102 de acuerdo con un programa predeterminado durante un período de tiempo dado; por ejemplo, la transmisión del mensaje 120 es periódica durante el periodo de tiempo dado. Como se muestra en la Figura 1, el mensaje 120 puede recibirse por una pluralidad de NODOS de comunicación, por ejemplo, el NODO B 104, el NODO C 106, el I^{er} NODO de comunicación 108, el NODO E 110 y el N^{o} NODO de comunicación 112. El mensaje 120, en algunos modos de realización, incluye, al menos uno de una oferta de servicio, una petición de servicio, un anuncio y un contenido de medios. A modo de ejemplo, considere un escenario en el cual el usuario del NODO de comunicaciones A 102 esté ofreciendo a uno o más usuarios de la red 100 un paseo en coche desde una primera ubicación, la ubicación X, hasta otra ubicación, ubicación Y. Por ejemplo, la ubicación X es Somerset, N.J. y la ubicación Y es Manhattan, N.Y. Por tanto, en este ejemplo, podemos referirnos al mensaje 120 como un mensaje de oferta de servicio. Aunque el mensaje 120 puede transmitir la firma del NODO de envío A, debería apreciarse que el NODO emisor A 102 no puede divulgar su identidad verdadera o completa en el mensaje 120. De acuerdo con un aspecto, algunos de los NODOS de comunicación, por ejemplo, el NODO B 104, pueden tener una relación de confianza con el NODO A 102, y el NODO B 104 puede incluirse en una lista de amigos del NODO A 102. La lista de amigos del NODO A 102 incluye, por ejemplo, información que identifica y/o pertenece a uno o más NODOS de comunicación que tienen una relación de confianza existente con el NODO A 102. La relación de confianza puede existir, por ejemplo, porque uno de los NODOS A 102 y B 104 pueda haber usado un servicio ofrecido por el otro del NODO A 102 y del NODO B 104 en algún punto anterior a tiempo y al menos uno del NODO A 102 y el NODO B 104 haya concluido que el otro del NODO A 102 y del NODO B 104 es digno de confianza.

En un escenario a modo de ejemplo en un modo de realización a modo de ejemplo, el NODO de comunicaciones A 102 y el NODO de comunicaciones B 104 tienen una relación de confianza, y el NODO de comunicaciones B 104 y el NODO de comunicaciones C 106 tienen una relación de confianza. Considere además que el NODO de comunicaciones A 102 y el NODO de comunicaciones C 106 no tienen una relación de confianza. Considere además que un usuario de un NODO de comunicaciones, por ejemplo, un usuario del NODO C 106, que puede no haber tratado previamente con el usuario del NODO A 102, puede estar interesado en el servicio ofrecido, por ejemplo, el paseo ofrecido por el usuario del NODO A 102. De acuerdo con un aspecto, el NODO de comunicaciones C106 puede desear determinar si el NODO A 102, que está ofreciendo el servicio, es confiable o no

y/o puede desear determinar la validez con respecto al mensaje 120. En otras palabras, puesto que no existe una relación de confianza entre el NODO A 102 y el NODO C 106, el NODO C 106 puede desear averiguar la reputación del NODO A 102 y la validez del mensaje 120 desde el NODO A 102. Debería apreciarse que esto puede ser una preocupación genuina desde la perspectiva del usuario del NODO C 106, puesto que es posible que algún usuario malintencionado pueda anunciar una oferta de servicio falsa, por ejemplo, un viaje en coche, y más tarde puede que no aparezca en la ubicación de recogida indicada. Por tanto, en dicho caso que involucra a un usuario malicioso que envía el mensaje de oferta de servicio, el NODO C 106 puede terminar perdiendo tiempo en la ubicación de recogida. De acuerdo con un aspecto, algunos usuarios, por ejemplo, el usuario del NODO B 104, que es consciente de la credibilidad del NODO A 102, pueden ayudar a propagar la confianza a otros NODOS de modo que los NODOS que estén interesados en el servicio ofrecido por el NODO A 102 puedan saber que el emisor del mensaje 120 es genuino y confiable. En algunos modos de realización, puede existir un número de dichos NODOS presentes en la red 100 que hayan tratado previamente con el NODO A 102, y, basándose en sus experiencias pasadas con el NODO A 102, uno o más de estos NODOS pueden ayudar a propagar confianza.

Además de la transmisión de la señal de mensaje 120, pueden producirse otras diversas señales en la red 100. Por ejemplo, en un modo de realización a modo de ejemplo en un escenario a modo de ejemplo, el NODO A 102 comunica también un mensaje 122, por ejemplo, un mensaje de acumulación de confianza, a uno o más NODOS en su lista de amigos con los cuales existe una relación de confianza, por ejemplo, el NODO B 104. En algunos modos de realización, el mensaje 122 incluye información de verificación de fuente de mensaje, por ejemplo, un identificador único, el mensaje de identificación 120 enviado desde el NODO A 102. Debería apreciarse que uno de los motivos detrás del mensaje de envío 122, por ejemplo, el mensaje de acumulación de confianza, es comprometer el número máximo de amigos de confianza, por ejemplo, usuarios de confianza para el NODO A 102, para contribuir al enrutamiento de la credibilidad/confiabilidad del NODO A dentro de sus propios contactos y/o de sus propios amigos de confianza, por ejemplo, si se les pregunta acerca de la confiabilidad del NODO A 102. Otro motivo detrás del envío del mensaje 122 desde el NODO A 102 a sus amigos de confianza es permitir a estos amigos de confianza validar el mensaje 120 puesto que el NODO A 102 no puede divulgar su verdadera identidad en el mensaje 120. De acuerdo con un aspecto, después de la recepción del mensaje 122, el NODO B 104 puede comenzar a propagar confianza entre los pares de confianza del NODO B, validando el hecho de que el emisor del mensaje 120, es decir, el NODO A 102 y/o el mensaje 120, es confiable. En algunos modos de realización, la propagación de confianza desde el NODO B 104 puede hacerse enviando otro mensaje 126, por ejemplo, un mensaje de propagación de confianza, desde el NODO B 102 a sus pares de confianza, por ejemplo, el NODO C 106. En algunos modos de realización, el NODO B 104 puede transmitir el mensaje 126 en respuesta a un mensaje de petición 124, por ejemplo, un mensaje de petición de confirmación de confianza, de un par de confianza, por ejemplo, el NODO C 106. Por ejemplo, el NODO C 106 que tenga una relación de confianza con el NODO B 104 podría estar interesado en el servicio ofrecido por el NODO A 102 y envía el mensaje de petición 124 a sus pares de confianza en su lista de amigos que incluye el NODO B 104 para pedir su opinión sobre el NODO A 102. En algunos de dichos modos de realización, el NODO B 104 responde al mensaje de petición 124 enviando el mensaje 126. En algunos modos de realización, el mensaje de petición 124 incluye el mensaje de identificación de identificador de mensaje 120 y al menos uno de una firma de emisor o de un código de autenticación de mensaje. En algunos de dichos modos de realización, el identificador de mensaje es un único mensaje de identificación de identificador 120 enviado desde el NODO A 102.

De acuerdo con un aspecto, una vez que el NODO C 106 determina que el emisor del mensaje 120, por ejemplo, el usuario del NODO A 102 que ofrece el paseo, es confiable, el NODO C 106 puede comunicar una respuesta, por ejemplo, el mensaje de respuesta 128, en respuesta al mensaje 120. Dicho mensaje de respuesta puede servir de señal desde el NODO C 106 indicando el interés del NODO C en el servicio ofrecido por el NODO A 102. En algunos modos de realización, pero no necesariamente todos, el mensaje de respuesta 128 no se envía directamente desde el NODO C 106 al NODO A 102. En cambio, el mensaje de respuesta 128 se comunica desde el NODO C 106 al NODO B 104 con el cual el NODO C 106 tiene una relación de confianza. Tras la recepción del mensaje de respuesta 128 del NODO C 106, el NODO B 104 comunica otro mensaje de respuesta 130 al NODO A 102. El mensaje de respuesta 130, en algunos modos de realización, incluye al menos una porción del mensaje de respuesta 128 e información de seguridad correspondiente al NODO B 104. El mensaje de respuesta 130, en algunos modos de realización, incluye el mensaje de respuesta 128 e información de seguridad correspondiente al NODO B 104. Debería apreciarse que, puesto que el mensaje de respuesta 130 es enviado por el NODO B 104, que es de confianza para el NODO A 102, el NODO A 102 podrá determinar que puede confiarse en el mensaje de respuesta 130 y en su contenido. De esta manera, el NODO A 102 puede determinar que el NODO C 106 está interesado de forma genuina en usar el servicio ofrecido por el NODO A 102.

La Figura 2 es un dibujo 200 que ilustra las etapas y la señalización asociada usadas en un modo de realización a modo de ejemplo donde un NODO de comunicación, por ejemplo, el NODO A 102, transmite, por ejemplo, multidifunde, el mensaje MSG 1 203, por ejemplo, un mensaje de oferta de servicio, que es recibido por el NODO de comunicaciones B 104 y por el NODO de comunicaciones C 106. Aunque se describa que el mensaje MSG 1 203 transmite una oferta de servicio en este ejemplo, debería apreciarse que el mensaje 203 puede incluir, por ejemplo, en algunos modos de realización lo hace, uno o más de: una petición de servicio, un anuncio, un contenido de medios, etc. Para el propósito de este ejemplo, considere que el NODO de comunicaciones A 102 tiene una relación de confianza con el NODO de comunicaciones B 104 y el NODO de comunicaciones C 106 tiene una relación de

confianza con el NODO de comunicaciones B 104. Considere además que el NODO A 102 no tiene una relación de confianza preexistente con el NODO C 106. Continuando con el ejemplo, considere que el NODO de comunicaciones C 106 está interesado en el servicio ofrecido indicado en el mensaje 203, que está siendo ofrecido por el NODO A 102. En este ejemplo particular, el proceso es iniciado por el NODO A 102, que desea ofrecer un servicio, por ejemplo, un viaje en coche desde la ubicación X hasta la ubicación Y. En la etapa 202, el NODO A 102 transmite, por ejemplo, multidifunde, el MSG 1 203, por ejemplo, el mensaje de oferta de servicio, a uno o más NODOS en una zona geográfica que incluye los NODOS B 104 y C 106. El mensaje MSG 1 203 se recibe y es procesado por el NODO B 104 y el NODO C 106 en las etapas 204 y 206 respectivamente.

En la etapa 208, el NODO A 102 envía el mensaje MSG 2 210, por ejemplo, un mensaje de acumulación de confianza, al NODO B 104. En algunos modos de realización, el mensaje MSG 2 210 se envía a NODOS adicionales en la lista de amigos del NODO A con los cuales el NODO A 102 tenga una relación de confianza. En algunos modos de realización, el MSG 2 210, incluye información de verificación de fuente de mensaje, por ejemplo, un identificador único, que identifica el mensaje MSG 1 203, que se envió desde el NODO A 102. Debería apreciarse que dicha información puede incluirse en el mensaje MSG 2 210, de modo que el NODO de amigos de confianza B 104 pueda validar el mensaje MSG 1 203. En la etapa 212, el mensaje MSG 2 210 es recibido y procesado por el segundo NODO B 104. El mensaje MSG 2 210 puede, por ejemplo, incluir una petición desde el NODO A 102 a sus pares de confianza tales como el NODO B 104 que reciben el mensaje 210, para propagar la información de credibilidad/confiabilidad del NODO A 102 a otros elementos en la zona que puedan estar interesados en el servicio ofrecido pero que no sean conscientes de la confiabilidad del NODO A 102. Por tanto, el NODO B 104 que tenga una relación de confianza con el NODO A 102 y sea consciente de la reputación del NODO A puede ayudar al NODO A 102. Por ejemplo, el NODO B 104 puede propagar buenas palabras sobre el NODO A 102 entre otros elementos en la red, por ejemplo, elementos tales como el NODO C 106, que tengan una relación de confianza con el NODO B 104 pero no con el NODO A 102.

En la etapa 214, el NODO C 106, que esté interesado en el servicio ofrecido indicado en el mensaje MSG 1 203, puede enviar opcionalmente una petición 216, por ejemplo, un mensaje de petición de confirmación de confianza, a uno o más de sus pares de confianza, después de la recepción del mensaje MSG 1 203. El mensaje de petición 216 puede ser una petición a los pares de confianza del NODO C para confirmar si puede confiarse en el emisor del mensaje MSG 1 203 y en el contenido del mensaje MSG 1 203. En algunos modos de realización, existe una probabilidad razonable de que, en una zona geográfica, uno o más NODOS que sean de confianza para el NODO C 106 puedan ser conscientes de la reputación del NODO A 102, por ejemplo, debido a un acuerdo pasado con el NODO A 102. En el ejemplo de la Figura 2, el NODO B 104 es un NODO que tiene una relación de confianza con ambos NODOS A 102 y C 106. En la etapa 218, el NODO B 104 recibe el mensaje de petición 216. En la etapa 220, el NODO B 104 comienza a propagar la confianza entre los pares de confianza del NODO B, por ejemplo, que el emisor del mensaje MSG 1 203, es decir, el NODO A 102 y/o el contenido del mensaje MSG 1 203, son confiables. El NODO B 104 hace esto enviando el MSG 3 222, por ejemplo, un mensaje de propagación de confianza, a sus pares de confianza. En los modos de realización donde el NODO B 104 recibe el mensaje de petición 216 desde el NODO C 106, el MSG 3 222 se envía en respuesta al mensaje de petición 216.

El mensaje MSG 3 222 es recibido por el NODO C 106 en la etapa 224 y está sujeto a otro procesamiento para determinar la confiabilidad de la información comunicada por el mensaje MSG 1 203, basándose en la información comunicada por el mensaje MSG 3 222. En algunos modos de realización, el mensaje MSG 3 222 incluye información de verificación de fuente, por ejemplo, la firma del emisor, el código de autenticación de mensaje (MAC) y la información para verificar que la información comunicada por el mensaje MSG 1 203 no se ha alterado. Debería apreciarse que la información de verificación de fuente tal como la firma del emisor (el NODO B 104) puede ayudar al NODO receptor C 106 a verificar la autenticidad del mensaje MSG 3 222 y por tanto a garantizar que el mensaje MSG 3 222 proviene de una fuente confiable. En algunos modos de realización, el mensaje MSG 3 222 incluye también un indicador de nivel de clasificación que indica, por ejemplo, niveles diferentes de clasificación posibles. Por ejemplo, el indicador de nivel de calificación puede indicar uno de una clasificación de confiabilidad, una clasificación de coste de servicio y una clasificación de calidad. En algunos modos de realización, cuanto más altas sean las clasificaciones de confianza, más podrá confiarse en el servidor que ofrece el servicio. Una clasificación de calidad, por ejemplo, puede indicar la calidad del servicio proporcionado, por ejemplo, en el ejemplo del viaje en coche, una clasificación de alta calidad puede indicar la prontitud del emisor del mensaje o, por ejemplo, el nivel de comodidad del coche, etc. En la etapa 226, tras la recepción del MSG 3 222 desde el NODO de par de confianza B 104 y después de determinar que la información comunicada por el mensaje MSG 1 203 es confiable, el NODO C 106 envía una respuesta al NODO A 102 a través del NODO B 104 que tiene relación de confianza con el NODO A 102. La respuesta que se envía desde el NODO C 106 es en respuesta al mensaje MSG 1 203, por ejemplo, el mensaje de oferta de servicio, recibido desde el NODO A 102 anterior. La respuesta puede ser, por ejemplo, una indicación y/o una confirmación de que el NODO C 106 está interesado en usar el servicio ofrecido por el NODO A 102 y le gustaría interactuar directamente con el NODO A 102. El NODO C 106 envía un mensaje de respuesta Respuesta 1 227 al NODO B 104 que recibe el mensaje de respuesta Respuesta 1 227 en la etapa 228. En la etapa 228, el NODO B 104 genera un mensaje de respuesta Respuesta 2 229, en algunos modos de realización, modificando el mensaje recibido 227 para incluir, por ejemplo, cierta información de seguridad correspondiente al NODO B 104. El mensaje de respuesta Respuesta 2 229, que incluye la información comunicada desde el NODO C 106 en el mensaje de respuesta Respuesta 1 227, se comunica entonces al NODO A 102 desde el NODO B 104. El

mensaje de respuesta Respuesta 2 229 es recibido por el NODO A 102 en la etapa 230 y el NODO A 102 puede confiar en el mensaje de respuesta Respuesta 2 229 puesto que se envía desde el NODO de confianza B 104. Después de recibir la respuesta desde el NODO C 106, tanto el NODO A 102 como C 106 pueden comenzar a negociar entre sí directamente. Cuando se establezca la relación de confianza entre el NODO A 102 y el NODO C 106, entonces los NODOS A 102 y C 106 pueden comenzar a emparejar e intercambiar certificados, por ejemplo, documentos de autorización de uso del espectro, su dirección IP, claves públicas, etc.

La Figura 3 es un dibujo 300 que ilustra las etapas y la señalización asociada usadas en otro modo de realización a modo de ejemplo donde un NODO de comunicación A 102 transmite, por ejemplo, multidifunde, el mensaje MSG 1 303, por ejemplo, un mensaje de oferta de servicio. En el ejemplo de la Figura 3, considere que el NODO A 102 tiene una relación de confianza con el NODO B 104, el NODO C 106 tiene una relación de confianza con el NODO B 104 y el NODO A 102 no tiene una relación de confianza preexistente con el NODO C 106. Además, considere que el NODO C 106 está interesado en un servicio ofrecido indicado en el mensaje MSG 1 303, ofrecido por el NODO A 102. En la etapa 302, el NODO A 102 transmite, por ejemplo, multidifunde, el MSG 1 303 a los NODOS B 104 y C 106. El mensaje MSG 1 303 se recibe y es procesado por el NODO B 104 y el NODO C 106 en las etapas 304 y 306 respectivamente. El NODO de comunicaciones C 106, que está interesado en el servicio ofrecido por el NODO A 102, envía un mensaje 316 de petición (1), por ejemplo, un mensaje de petición de confirmación de confianza, a los NODOS de confianza en su lista de amigos, por ejemplo, el NODO B 104. La señal de mensaje 316 de petición (1) es similar al mensaje de petición 216 analizado en el ejemplo de la Figura 2 y por tanto no se analizará en detalle de nuevo. En la etapa 310, el NODO B 104 recibe y procesa el mensaje 316 de petición (1). El NODO B 104 genera un mensaje 316' de petición (2), por ejemplo, un mensaje de petición de confirmación de confianza, usando la información incluida en el mensaje 316 de petición (1). El NODO B 104 envía entonces el mensaje 316' de petición (2) al NODO A 102 que envió el mensaje MSG 1 303. En algunos modos de realización, el NODO B 104 puede transmitir simplemente el mensaje de petición (1) recibido al NODO A 102 en lugar de generar y enviar el mensaje 316' de petición (2).

En la etapa 312, el NODO A 102 recibe el mensaje 316' de petición (2), es decir, el mensaje de petición de confirmación de confianza. Tras la recepción de, y en respuesta al mensaje 316' de petición (2), en la etapa 314, el NODO A 102 envía el MSG 2 310, por ejemplo, un mensaje de acumulación de confianza, al NODO B 104. Debería apreciarse que una diferencia interesante en el modo de realización presentado en la Figura 3 respecto al de la Figura 2 es que, en el modo de realización de la Figura 3, el mensaje MSG 2 310, por ejemplo, el mensaje de acumulación de confianza, se envía desde el NODO A 102 si algún otro NODO, por ejemplo, el NODO C 106 en este caso, muestra interés en el servicio ofrecido, mientras que, en el modo de realización de la Figura 2, el mensaje MSG 2 210, por ejemplo, el mensaje de acumulación de confianza, se envía sin requerir la recepción de una señalización que indique una muestra de interés. Por tanto, el enfoque de la Figura 3 puede reducir el uso de recursos de enlace aéreo. Por ejemplo, en el ejemplo de la Figura 3, en el caso de que el mensaje de confirmación de petición no sea detectado por el NODO A 102, no se transmite el mensaje 2 310. El MSG 2 310 de la Figura 3 es el mismo o similar al MSG 2 210 de la Figura 2 y la información que MSG 2 310 puede comunicar es similar o la misma que con el MSG 2 210 que se ha analizado en detalle en el ejemplo de la Figura 2. En la etapa 318, el NODO B 104 recibe el mensaje MSG 2 310 y, usando la información incluida en el mensaje MSG 2 310, valida el mensaje MSG 1 303. En la etapa 320, el NODO B 104 envía el MSG 3 322, es decir, un mensaje de propagación de confianza, al NODO C 106, en respuesta al mensaje 316 de petición (1) que el NODO B 104 recibió anteriormente. El mensaje MSG 3 322 es el mismo o similar al MSG 3 222 que se ha analizado en detalle anteriormente en el ejemplo de la Figura 2 y por tanto los detalles no se repetirán. Debería apreciarse que el mensaje MSG 3 322 en este ejemplo se envía al NODO que envía el mensaje 316 de petición (1) y no a múltiples NODOS de confianza que pueden no estar interesados en el servicio ofrecido por el NODO A 102. Esto se hace con el fin de evitar la difusión innecesaria del mensaje 322 MSG 3 322 y el desperdicio de recursos de enlace aéreo. En algunos modos de realización, el nivel de energía de transmisión del mensaje MSG 3 322 puede ser inferior de lo que de otra forma sería si el mensaje MSG 3 322 estuviera dirigiéndose a múltiples NODOS de confianza.

El mensaje MSG 3 322 es recibido por el NODO C 106 en la etapa 324 y está sujeto a un procesamiento adicional para determinar la confiabilidad de la información comunicada en el MSG 1 303, por ejemplo, el mensaje de oferta de servicio, basándose en la información comunicada por el mensaje MSG 3 322. En algunos modos de realización, el mensaje MSG 3 322 incluye información de verificación de fuente, por ejemplo, la firma del emisor, el código de autenticación de mensaje (MAC) y la información para verificar que la información comunicada por el MSG 1 303 no se ha alterado. En la etapa 326, después de la recepción del mensaje MSG 3 322 desde el NODO de confianza B 104 y después de determinar que la información comunicada por el mensaje MSG 1 303 es confiable, el NODO C 106 envía una respuesta al NODO A 102 a través del NODO B 104 que tiene una relación de confianza con el NODO A 102. La respuesta que se envía desde el NODO C 106 es en respuesta al mensaje MSG 1 303 recibido desde el NODO A 102 anteriormente. El NODO C 106 envía un mensaje 327 de respuesta 1 al NODO B 104 que recibe el mensaje 327 de respuesta 1 en la etapa 328. Además, en la etapa 328, el NODO B 104 genera un mensaje 329 de respuesta 2 , en algunos modos de realización, modificando el mensaje 327 de respuesta 1 recibido para incluir, por ejemplo, cierta información de seguridad correspondiente al NODO B 104. El mensaje 329 de respuesta 2, que incluye la información comunicada desde el NODO C 106 en el mensaje 327 de respuesta 1, se comunica entonces al NODO A 102 desde el NODO B 104. El mensaje 329 de respuesta 2 es recibido por el NODO A 102 en la etapa 330 y, puesto que está siendo enviado por el NODO de confianza B 104, el NODO A 102 puede confiar en

el mensaje 329 de respuesta 2.

La Figura 4 es un dibujo 400 que ilustra las etapas y la señalización asociada usadas en otro modo de realización más a modo de ejemplo donde el NODO de comunicación A 102 transmite, por ejemplo, multidifunde, el MSG 1 403, por ejemplo, un mensaje de oferta de servicio como se muestra. En el modo de realización a modo de ejemplo mostrado en la Figura 4, considere que el NODO A 102 tiene una relación de confianza con el NODO B 104, el NODO B 104 tiene una relación de confianza con el NODO E 110 y el NODO C 106 tiene una relación de confianza con el NODO E 110. Sin embargo, el NODO A 102 no tiene una relación de confianza preexistente con el NODO C 106 y el NODO B 104 no tiene una relación de confianza preexistente con el NODO C 106. También, considere que el NODO C 106 está interesado en una oferta de servicio indicada por el MSG 1 403, ofrecida por el NODO A 102. Por tanto, en el ejemplo analizado en la Figura 4 puede no existir ningún NODO común que tenga una relación de confianza tanto con el NODO de oferta de servicios A 102 como con el NODO C 106 que esté interesado en el servicio ofrecido.

En la etapa 402, el NODO A 102 transmite, por ejemplo, multidifunde, el MSG 1 403, por ejemplo, un mensaje de oferta de servicio, a los NODOS B 104, E 110 y C 106. El mensaje MSG 1 403 se recibe y es procesado por el NODO B 102, el NODO E 110 y el NODO C 106 en las etapas 404, 406 y 408 respectivamente. En la etapa 409, el NODO A 102 envía un mensaje MSG 2 410, por ejemplo, un mensaje de acumulación de confianza, al NODO de confianza B 104. El MSG 2 410 incluye información, por ejemplo, un identificador único, que identifica el mensaje MSG 1 403 enviado desde el NODO A 102, de modo que el NODO de amigos de confianza B 104 puede validar el mensaje MSG 1 403. En la etapa 412, el mensaje MSG 2 410 se recibe y es procesado por el segundo NODO B 104. Por el otro lado, el NODO C 106 que está interesado en el servicio ofrecido por el NODO A 102 busca reunir información de credibilidad sobre el emisor del mensaje MSG 1 403. Por tanto, en la etapa 414, el NODO C 106 envía un mensaje de petición 416, por ejemplo, el mensaje de petición de confirmación de confianza, a los NODOS de confianza en su lista de amigos, por ejemplo, el NODO E 110. El mensaje de petición 416 puede enviarse desde el NODO C 106 a uno o más de sus NODOS de confianza para reunir credibilidad sobre el NODO A 102 que envió el mensaje MSG 1 403, por ejemplo, para determinar si el NODO emisor y el contenido del mensaje MSG 1 403 pueden ser de confianza. El mensaje de petición 416 es recibido y es procesado por el NODO E 110 en la etapa 417. Debería observarse que, en este ejemplo, el NODO E 110 no tiene una relación de confianza con el NODO A 102 y puede no tener suficiente información de credibilidad sobre el NODO A 102 para determinar la confiabilidad del NODO A 102. También, puesto que el NODO E 110 no recibe el MSG 2 410, por ejemplo, el mensaje de acumulación de confianza, en este punto, el NODO E 110 no tiene la información para validar el mensaje MSG 1 403. Por tanto, para ayudar a su NODO de amigos de confianza C 106, en la etapa 417, el NODO E 110 envía otro mensaje de petición 416' que incluye la información incluida en el mensaje de petición 416 junto con la información de seguridad correspondiente al NODO E 110, a uno o más de sus amigos de confianza tal como el NODO B 104 en este caso. La información de seguridad, por ejemplo, la firma del emisor, se incluye por el NODO de comunicaciones E 110 en el mensaje 416 'de modo que el NODO de comunicaciones B 104 que recibe el mensaje 416' puede saber que la petición está siendo realizada por un amigo de confianza. En algunos modos de realización, el NODO B 104 puede no responder a peticiones de confirmación de confianza hechas por NODOS que no son de confianza. El mensaje 416' es recibido y es procesado por el NODO B 104 en la etapa 418.

En la etapa 420, el NODO B 104 envía el MSG 3 422, por ejemplo, un mensaje de propagación de confianza, al NODO C 106, en respuesta al mensaje de petición 417. El mensaje MSG 3 422 del ejemplo de la Figura 4 es el mismo o similar al mensaje MSG 3 222 de la Figura 2 o al mensaje MSG 3 322 de la Figura 3 que se ha analizado en detalle anteriormente y por tanto no se analizará en detalle de nuevo para evitar la repetición. El mensaje MSG 3 422 se envía al NODO E 110 que envió el mensaje de petición 416' y no a múltiples NODOS de confianza que pueden no estar interesados en el servicio ofrecido por el NODO A 102. El mensaje MSG 3 422 es recibido por el NODO E 110 en la etapa 424. En la etapa 428, el mensaje recibido MSG 3 422 es enviado por el NODO E 110 al NODO C 106 como el mensaje 429. El mensaje 429 incluye la información incluida en el MSG 3 422 junto con información de seguridad correspondiente al NODO E 110, de modo que el NODO C 106 puede saber que el mensaje 429 está siendo enviado por su amigo de confianza en respuesta al mensaje de petición 416. En la etapa 430, el mensaje 429 es recibido por el NODO C 106 y está sujeto otro procesamiento para determinar la confiabilidad de la información comunicada anteriormente por el mensaje MSG 1 403, basándose en la información comunicada por el mensaje 429. En la etapa 432, después de la recepción del mensaje 429 desde el NODO de confianza E 110 y después de determinar que la información comunicada por el mensaje MSG 1 403 es confiable, el NODO C 106 envía un mensaje de respuesta en respuesta al mensaje MSG 1 403 recibido anteriormente al NODO A 102 a través del NODO E 110 y del NODO B 104. Aunque la respuesta puede comunicarse en múltiples saltos al NODO A 102, debería apreciarse que, de esta manera, la respuesta se enruta desde un NODO de confianza hasta otro NODO de confianza y, por tanto, el NODO A 102 que finalmente recibe la respuesta puede confiar en la autenticidad e integridad de la respuesta enviada. En la etapa 432, la respuesta 1 433 se envía desde el NODO C 106 al NODO de amigos de confianza E 110 que recibe la respuesta 1 433 en la etapa 434. Además, en la etapa 434, el NODO E 110 genera otro mensaje, la respuesta 2 435, que, en algunos modos de realización, se genera modificando la respuesta recibida 1 433 para incluir, por ejemplo, cierta información de seguridad correspondiente al NODO E 110. La respuesta 2 435, que incluye la respuesta comunicada desde el NODO C 106, es comunicada entonces por el NODO E 110 a su NODO de amigos de confianza B 104. En la etapa 436, el NODO B 104 recibe y procesa la respuesta 2 435 para incluir alguna información de seguridad correspondiente al NODO B 104. El

mensaje de respuesta que incluye la información de seguridad correspondiente al NODO B 104 es comunicado entonces en la etapa 436, como respuesta 3 437 al NODO A 102. Debería apreciarse que la respuesta 3 437 incluye la información comunicada por la respuesta 1 433 desde el NODO C 106, aunque enrutada a través de NODOS de confianza diferentes. La respuesta 3 437 es recibida por el NODO A 102 en la etapa 438 y, puesto que está siendo enviado por el NODO de confianza B 104, el NODO A 102 puede confiar en la respuesta.

La Figura 5 es un diagrama de flujo 500 de un procedimiento a modo de ejemplo de funcionamiento de un primer NODO de comunicaciones, por ejemplo, el NODO de comunicaciones entre pares C 106 de la Figura 1, de acuerdo con un modo de realización a modo de ejemplo. El funcionamiento del procedimiento a modo de ejemplo comienza en la etapa 502, donde el primer NODO de comunicaciones se activa y se inicia. El funcionamiento avanza desde la etapa de inicio 502 hasta la etapa 504.

En la etapa 504, el primer NODO de comunicaciones recibe un primer mensaje, por ejemplo, un mensaje de oferta de servicio, desde un segundo NODO de comunicaciones, por ejemplo, el NODO A 102, comunicando dicho primer mensaje información. En el modo de realización analizado en el diagrama de flujo 500, el primer NODO de comunicaciones no tiene una relación de confianza preexistente con el segundo NODO de comunicaciones. El primer mensaje incluye al menos uno de una oferta de servicio, una petición de servicio, publicidad y contenido multimedia. Para el ejemplo analizado en el diagrama de flujo 500, considere que el primer mensaje incluye una oferta de servicio, por ejemplo, una oferta para un viaje en coche desde la ubicación X hasta la ubicación Y. El emisor del primer mensaje, es decir, el segundo NODO de comunicaciones puede, por ejemplo, transmitir, por ejemplo, multidifundir, el primer mensaje a una pluralidad de NODOS en una región geográfica, por ejemplo, tal como la cubierta por la red 100 de la Figura 1. En algunos modos de realización, el primer mensaje incluye información de ubicación. En algunos de dichos modos de realización, la información de ubicación es información de ubicación basada en el sistema de posicionamiento global (GPS). Por ejemplo, la información de ubicación en el primer mensaje puede ser la ubicación de una zona desde donde al segundo NODO de comunicaciones que envía el primer mensaje le gustaría recoger a otros usuarios interesados en el viaje. En algunos modos de realización, el funcionamiento avanza desde la etapa 504 hasta la etapa 506. En algunos modos de realización, el funcionamiento avanza desde la etapa 504 hasta la etapa 507. Debería apreciarse que ambas etapas 506 y 507 son opcionales y que pueden omitirse una o más de las etapas 506 y 507.

En la etapa opcional 506, después de la recepción del primer mensaje, el primer NODO comunica un mensaje de petición de confirmación de confianza a uno o más de sus NODOS de confianza, por ejemplo, al NODO de comunicaciones B 104. El primer NODO de comunicaciones puede tener una lista de NODOS de confianza a la cual pueda comunicar uno o más mensajes tales como un mensaje de petición de confirmación de confianza durante el funcionamiento. El mensaje de petición de confirmación de confianza puede enviarse a uno o más NODOS de confianza, de modo que el primer NODO de comunicaciones pueda reunir información, por ejemplo, credibilidad o información confiable sobre el segundo NODO. El funcionamiento avanza desde la etapa 506 hasta la etapa 508.

En la etapa 507 que puede realizarse en algunos modos de realización, el primer NODO envía el mensaje de petición de confirmación de confianza a uno o más NODOS de confianza para su propagación a un NODO que tenga una relación de confianza con el segundo NODO. Esto puede hacerse en algunos modos de realización, por ejemplo, donde el primer NODO de comunicaciones y el segundo NODO de comunicaciones no tengan un amigo de confianza común. Por tanto, en dicho caso, el mensaje de petición de confirmación de confianza puede propagarse desde el primer NODO hasta su amigo de confianza, por ejemplo, que propaga además el mensaje a los elementos de confianza en su propia lista de amigos y así sucesivamente. De esta manera, el mensaje de petición de confirmación de confianza se propaga a un NODO que tiene una relación de confianza con el segundo NODO. El funcionamiento avanza desde la etapa 507 hasta la etapa 508.

En la etapa 508, el primer NODO de comunicaciones recibe un segundo mensaje, por ejemplo, un mensaje de propagación de confianza, de un tercer NODO de comunicaciones con el cual existe una relación de confianza, siendo el tercer NODO de comunicaciones uno de uno o más NODOS de confianza para el primer NODO de comunicaciones . En algunos modos de realización, el tercer NODO de comunicaciones tiene una relación de confianza con el primer NODO. En algunos modos de realización, el primer NODO de comunicaciones recibe el segundo mensaje, por ejemplo, el mensaje de propagación de confianza en respuesta a la petición de confirmación de confianza comunicada al tercer NODO de comunicaciones de confianza (por ejemplo, comunicado en la etapa 506 anterior). En algunos modos de realización, el tercer NODO está dentro de uno de un intervalo predeterminado de la ubicación indicada en el primer mensaje o dentro de un intervalo, indicado en el primer mensaje, de la ubicación indicada en el primer mensaje.

En algunos modos de realización, la información comunicada por el segundo mensaje, por ejemplo, el mensaje de propagación de confianza, incluye una segunda información de verificación de fuente de mensaje, por ejemplo, la firma del emisor, el código de autenticación de mensaje (MAC) y la información para verificar que la información comunicada por el primer mensaje no se ha alterado. Debería apreciarse que la información de verificación de fuente tal como una firma de emisor puede ayudar al primer NODO de comunicaciones a verificar la autenticidad del segundo mensaje y por tanto a garantizar que el segundo mensaje proviene de una fuente de confianza. En algunos modos de realización, el segundo mensaje incluye también un indicador de nivel de clasificación que indica uno de

una pluralidad de niveles de clasificación posibles. Por ejemplo, pueden existir dos, tres o incluso más niveles de clasificación diferentes. En algunos modos de realización, el indicador de nivel de clasificación puede indicar una de una clasificación de confiabilidad, de una clasificación de coste de servicio y de una clasificación de calidad. Una clasificación de confiabilidad más alta, por ejemplo, significa que puede ser de confianza el par que ofrezca el servicio. Por tanto, por medio de un nivel de clasificación, el tercer NODO de comunicaciones de confianza que esté respondiendo a la petición de confirmación de confianza puede expresar su aprobación, su desaprobación y/u otra opinión con respecto a la oferta de servicio del segundo NODO de comunicaciones.

El funcionamiento avanza desde la etapa 508 a la etapa 510. En la etapa 510, el primer NODO de comunicaciones determina, basándose en la información comunicada por el segundo mensaje, si la información comunicada por el primer mensaje es o no confiable. Por ejemplo, el tercer NODO de comunicaciones puede haber tratado anteriormente el segundo NODO de comunicaciones o haber usado algún servicio ofrecido por el segundo NODO de comunicaciones. Basándose en la experiencia pasada, el tercer NODO de comunicaciones puede categorizar el segundo NODO, por ejemplo, como confiable o no confiable. En algunos modos de realización, el tercer NODO de comunicaciones B 104 puede tener una relación de confianza con el segundo NODO, por ejemplo, basándose en una experiencia pasada de tratar uno con el otro. Por tanto, el tercer NODO de comunicaciones puede indicar la confiabilidad del segundo NODO en el segundo mensaje, por ejemplo, por medio del indicador de nivel de clasificación. En algunos modos de realización, el segundo mensaje incluye también la información para verificar que la información comunicada por el primer mensaje no ha cambiado. Por tanto, vemos que el segundo mensaje incluye información para ayudar al primer NODO de comunicaciones a determinar la confiabilidad del segundo NODO de comunicaciones y la integridad del primer mensaje. Sin embargo, debería apreciarse que el segundo mensaje solo puede no ser suficiente para que el primer NODO de comunicaciones decida sobre la confiabilidad del segundo NODO de comunicaciones. Por ejemplo, en algunos modos de realización, el primer NODO de comunicaciones puede determinar la confiabilidad de la información en el primer mensaje cuando reciba, por ejemplo, un alto grado de confiabilidad del segundo NODO de comunicaciones, desde un número predeterminado, por ejemplo cinco, de los amigos de confianza del primer NODO de comunicaciones. En algunos modos de realización, se usan otros criterios para determinar la confiabilidad de la información en el primer mensaje, por ejemplo, se calcula un valor de confiabilidad en función de la información confiable recibida desde los amigos de confianza del primer dispositivo de comunicaciones y se compara el valor de confiabilidad con un límite de paso/fallo. En algunos de dichos modos de realización, el primer dispositivo de comunicaciones puede ponderar información a partir de amigos de confianza de forma diferente.

Si se determina que la información comunicada por el primer mensaje es confiable, entonces el funcionamiento avanza desde la etapa 510 hasta la etapa 512 en el que el primer NODO de comunicaciones envía un mensaje de respuesta al segundo NODO de comunicaciones en respuesta al primer mensaje. En algunos modos de realización, el tercer NODO de comunicaciones tiene una relación de confianza con el segundo NODO. En algunos de dichos modos de realización, el mensaje de respuesta que se envía desde el primer NODO de comunicaciones en respuesta al primer mensaje, se envía a través del tercer NODO de comunicaciones. Debido al enrutamiento del mensaje de respuesta a través del tercer NODO, el segundo NODO puede confiar en el mensaje de respuesta y en su contenido. El funcionamiento avanza desde la etapa 512 hasta la etapa 504. Por el otro lado, cuando se determina que la información comunicada por el primer mensaje no puede ser de confianza, el funcionamiento avanza desde la etapa 510 hasta la etapa 514. En la etapa 514, el primer NODO de comunicaciones se abstiene de transmitir el mensaje de respuesta en respuesta al primer mensaje recibido. El funcionamiento avanza desde la etapa 514 de vuelta a la etapa 504.

En un modo de realización a modo de ejemplo, considere el diagrama de flujo de la Figura 5 en el contexto del ejemplo de la Figura 2. El primer NODO de comunicaciones, el segundo NODO de comunicaciones y el tercer NODO de comunicaciones de la Figura 5 son el NODO C 106, el NODO A 102 y el NODO B 104 de la Figura 2, respectivamente. El primer mensaje, el mensaje de petición de confirmación de confianza de la etapa 506, el segundo mensaje y el mensaje de respuesta de la Figura 5 son el MSG 1 203, el mensaje de petición 216, el MSG 3 222 y la respuesta 1 227 respectivamente.

En otro modo de realización a modo de ejemplo, considere el diagrama de flujo de la Figura 5 en el contexto del ejemplo de la Figura 3. El primer NODO de comunicaciones, el segundo NODO de comunicaciones y el tercer NODO de comunicaciones de la Figura 5 son el NODO C 106, el NODO A 102 y el NODO B 104 de la Figura 3 respectivamente. El primer mensaje, el mensaje de petición de confirmación de confianza de la etapa 506, el segundo mensaje y el mensaje de respuesta de la Figura 5 son el MSG 1 303, el mensaje 316 de petición (1), el MSG 3 322, y la respuesta 1 327 respectivamente.

En otro modo de realización más a modo de ejemplo, considere el diagrama de flujo de la Figura 5 en el contexto del ejemplo de la Figura 4. El primer NODO de comunicaciones, el segundo NODO de comunicaciones y el tercer NODO de comunicaciones de la Figura 5 son el NODO C 106, el NODO A 102 y el NODO E 110 de la Figura 4 respectivamente. El primer mensaje, el mensaje de petición de confirmación de confianza de la etapa 507, el segundo mensaje y el mensaje de respuesta de la Figura 5 son el MSG 1 403, el mensaje 416 de petición (1), el mensaje 429 y la respuesta 1 433 respectivamente.

La Figura 6 ilustra un formato de mensaje a modo de ejemplo para un segundo mensaje 600 a modo de ejemplo, por ejemplo, un mensaje de propagación de confianza, de acuerdo con un modo de realización. El segundo mensaje 600 a modo de ejemplo mostrado en la Figura 6 puede usarse, por ejemplo, como el mensaje MSG 3 222 de la Figura 2, el mensaje MSG 3 322 de la Figura 3, el mensaje MSG 3 422 de la Figura 4 o el segundo mensaje analizado en el diagrama de flujo de la Figura 5 . Como se muestra en la Figura 6, el segundo mensaje 600 a modo de ejemplo incluye tres campos. El campo 602 incluye la segunda información de verificación de fuente de mensaje. En algunos modos de realización, la información de verificación de fuente puede ser, por ejemplo, una firma del NODO que envíe el segundo mensaje 600. En algunos modos de realización, la información de verificación de fuente puede ser un código de autenticación de mensaje (MAC). En algunos modos de realización, la información de verificación de fuente incluye tanto una firma como un MAC. El segundo campo 604 del segundo mensaje 600 a modo de ejemplo incluye la información para verificar la integridad de un primer mensaje. El primer mensaje es, por ejemplo, el MSG 1 203 de la Figura 1, el MSG 1 303 de la Figura 3, el MSG 1 403 de la Figura 4 o el primer mensaje de la etapa 504 del diagrama de flujo 500 de la Figura 5. Por tanto, el campo 604 incluye la información para verificar que la información comunicada por el primer mensaje no se ha alterado. El tercer campo 606 del segundo mensaje 600 a modo de ejemplo es un indicador de nivel de clasificación que indica uno de una pluralidad, por ejemplo, dos, tres o más, de niveles de clasificación posibles. El indicador de nivel de clasificación indica, en algunos modos de realización, una de una clasificación de confiabilidad, una clasificación de coste de servicio o una clasificación de calidad.

La Figura 7 ilustra un NODO de comunicaciones 700 a modo de ejemplo, que puede usarse como, por ejemplo, el NODO de comunicación C 106, mostrado en la red de comunicación de la Figura 1, de la Figura 2, de la Figura 3 o de la Figura 4. El NODO de comunicaciones 700 puede ser, y en al menos un modo de realización es, un terminal inalámbrico móvil que soporte comunicaciones entre pares e implemente un procedimiento de acuerdo con el diagrama de flujo 500 de la Figura 5. El dispositivo de comunicaciones 700 incluye un procesador 702 y una memoria 704 acoplados juntos a través de un bus 709 a través del cual los diversos elementos (702, 704) pueden intercambiar datos e información. El NODO de comunicaciones 700 incluye además un módulo de entrada 706 y un módulo de salida 708 que pueden acoplarse al procesador 702 como se muestra. Sin embargo, en algunos modos de realización, el módulo de entrada 706 y el módulo de salida 708 están ubicados en el interior del procesador 702. El módulo de entrada 706 puede recibir señales de entrada. El módulo de entrada 706 puede incluir, y en algunos modos de realización lo hace, un receptor inalámbrico y/o una interfaz de entrada alámbrica u óptica para recibir la entrada. El módulo de salida 708 puede incluir, y en algunos modos de realización lo hace, un transmisor inalámbrico y/o una interfaz de salida alámbrica u óptica para transmitir la salida. El procesador 702 está configurado para: recibir un primer mensaje desde un segundo NODO, comunicando dicho primer mensaje la información, recibir un segundo mensaje desde un tercer NODO con el cual existe una relación de confianza y determinar la confiabilidad de la información comunicada por el primer mensaje basándose en la información comunicada por el segundo mensaje.

En un modo de realización a modo de ejemplo, el primer mensaje es el mensaje MSG 1 203, por ejemplo, un mensaje de oferta de servicio, el segundo NODO es el NODO A 102, el segundo mensaje es el MSG 3 222 y el tercer NODO es el NODO B 104. En otro modo de realización a modo de ejemplo, el primer mensaje es el mensaje MSG 1 303, por ejemplo, un mensaje de oferta de servicio, el segundo NODO es el NODO A 102, el segundo mensaje es el MSG 3 322 y el tercer NODO es el NODO B 104. En otro modo de realización más a modo de ejemplo, el primer mensaje es el mensaje MSG 1 403, por ejemplo, un mensaje de oferta de servicio, el segundo NODO es el NODO A 102, el segundo mensaje es el mensaje 429 y el tercer NODO es el NODO E 110.

En algunos modos de realización, el NODO de comunicaciones 700 no tiene una relación preexistente con el segundo NODO. En algunos modos de realización, el procesador 702 está configurado además para comunicar un mensaje de petición de confirmación de confianza a uno o más NODOS de confianza después de la recepción del primer mensaje, siendo el tercer NODO uno de dichos uno o más NODOS de confianza. En al menos un modo de realización, el segundo mensaje es en respuesta a dicho mensaje de petición de confirmación de confianza. En algunos modos de realización, el procesador 702 está configurado además para enviar el mensaje de petición de confirmación de confianza a uno o más NODOS de confianza para su propagación a un NODO que tenga una relación de confianza con el segundo NODO, por ejemplo, el NODO A 102. En algunos modos de realización, el procesador 702 está configurado además para enviar un mensaje de respuesta al segundo NODO después de determinar que la información comunicada en el primer mensaje es confiable. En al menos algunos de dichos modos de realización, el procesador 702 está configurado además para enviar el mensaje de respuesta al segundo NODO a través del tercer NODO.

La Figura 8 es un montaje de módulos 800 que pueden usarse, y en algunos modos de realización lo hacen, en el dispositivo de comunicaciones 1600 ilustrado en la Figura 7, por ejemplo, un primer NODO. Los módulos en el montaje 800 pueden implementarse en hardware dentro del procesador 702 de la Figura 7, por ejemplo, como circuitos individuales. De forma alternativa, los módulos pueden implementarse en software y almacenarse en la memoria 704 del NODO de comunicaciones 700 mostrado en la Figura 7. Aunque se muestra en el modo de realización de la Figura 7 como un único procesador, por ejemplo, un ordenador, debería apreciarse que el procesador 702 puede implementarse como uno o más procesadores, por ejemplo, ordenadores.

Cuando se implementan en software, los módulos incluyen un código, que cuando es ejecutado por el procesador 702, configura el procesador para implementar la función correspondiente al módulo. En los modos de realización donde el montaje de módulos 800 se almacena en la memoria 704, la memoria 704 es un producto de programa informático que comprende un medio legible por ordenador que comprende un código, por ejemplo, un código individual para cada módulo, para hacer que al menos un ordenador, por ejemplo, un procesador 702, implemente las funciones a las cuales correspondan los módulos.

Pueden usarse módulos basados por completo en hardware o basados por completo en software. Sin embargo, debería apreciarse que puede usarse cualquier combinación de módulos de software y hardware (por ejemplo, circuitos implementados) puede usarse para implementar las funciones. Como debería apreciarse, los módulos ilustrados en la Figura 8 controlan y/o configuran el NODO de comunicaciones 700 o elementos en el mismo tal como el procesador 702, para realizar las funciones de las etapas correspondientes ilustradas en el diagrama de flujo del procedimiento de la Figura 5.

Como se ilustra en la Figura 8, el montaje de módulos 800 incluye un módulo 802 para recibir un primer mensaje desde un segundo NODO de comunicaciones, comunicando dicho primer mensaje información, un módulo 804 para comunicar un mensaje de petición de confirmación de confianza a uno o más NODOS de confianza, un módulo 806 para enviar un mensaje de petición de confirmación de confianza a uno o más NODOS de confianza para su propagación a un NODO que tenga una relación de confianza con el segundo NODO de comunicaciones y un módulo 808 para recibir un segundo mensaje desde un tercer NODO de comunicaciones con el cual existe una relación de confianza, siendo dicho tercer NODO de comunicaciones uno de dichos uno o más NODOS de confianza. Los módulos 804 y 806 son opcionales. Uno o más de los módulos opcionales 804 y 806 están presentes en algunos modos de realización, mientras que, en algunos otros modos de realización, los módulos 804 y 806 se omiten. El montaje de módulos 800 incluye además un módulo 810 para determinar la confiabilidad de la información comunicada por el primer mensaje basándose en la información comunicada en el segundo mensaje y un módulo 812 para enviar un mensaje de respuesta al segundo NODO de comunicaciones después de determinar que la información comunicada por el primer mensaje es confiable. En algunos modos de realización, la información comunicada por el segundo mensaje incluye una segunda información de verificación de fuente de mensajes, por ejemplo, una firma, un código de autenticación de mensajes y/u otra información para verificar que la información comunicada por el primer mensaje no se ha alterado. En algunos modos de realización, la información comunicada en el segundo mensaje incluye además un indicador de nivel de clasificación que indica uno de una pluralidad de niveles de clasificación posibles. En algunos de dichos modos de realización, el indicador de nivel de clasificación indica una de una clasificación de confiabilidad, una clasificación de coste de servicio o una clasificación de calidad. En algunos modos de realización, el primer NODO que usa el montaje de módulos 800 no tiene una relación de confianza preexistente con el segundo NODO. En algunos modos de realización, el primer mensaje incluye al menos uno de una oferta de servicio, de una petición de servicio, de un anuncio y de un contenido de medios. En algunos modos de realización, el primer mensaje incluye además información de ubicación. En algunos modos de realización, la información de ubicación es información de ubicación basada en GPS.

La Figura 9 es un diagrama de flujo 900 de un procedimiento a modo de ejemplo de funcionamiento de un primer NODO de comunicaciones, por ejemplo, un NODO de comunicaciones entre pares B 104 de la Figura 1, de acuerdo con un modo de realización a modo de ejemplo. El funcionamiento del procedimiento a modo de ejemplo comienza en la etapa 902, donde el primer NODO de comunicaciones se activa y se inicia. El funcionamiento avanza desde la etapa de inicio 902 hasta las etapas 903 y 904. Debería apreciarse que las etapas 903 y 904 pueden realizarse, pero no necesitan hacerlo, en paralelo y de forma independiente.

En la etapa 903, el primer NODO de comunicaciones recibe un segundo mensaje desde un segundo NODO de comunicaciones, por ejemplo, el NODO A 102. En diversos modos de realización, el segundo mensaje incluye al menos uno de una oferta de servicio, de una petición de servicio, de un anuncio y un contenido de medios. En un ejemplo, el segundo mensaje es, por ejemplo, un mensaje de oferta de servicio. En algunos modos de realización, el segundo mensaje incluye información de ubicación. En algunos de dichos modos de realización, la información de ubicación es información de ubicación basada en el sistema de posicionamiento global (GPS). Por ejemplo, en el caso en que el segundo mensaje sea un mensaje de oferta de servicio y el servicio que se ofrezca sea, por ejemplo, un viaje en coche, la información de ubicación en el mensaje de oferta de servicio puede ser la ubicación de una zona desde donde al emisor del mensaje de oferta de servicio le gustaría recoger a las partes interesadas. De forma alternativa, la información de ubicación podría ser alguna otra ubicación, por ejemplo, una zona donde el emisor del mensaje de oferta de servicio se ubique actualmente. El funcionamiento avanza desde la etapa 903 hasta la etapa 905.

Volviendo a la etapa 904, en la etapa 904, el primer NODO de comunicaciones recibe un primer mensaje, por ejemplo, un mensaje de acumulación de confianza, desde el segundo NODO de comunicaciones, incluyendo el primer mensaje la información de verificación de fuente de mensaje y un identificador de mensaje que identifica el segundo mensaje enviado desde el segundo NODO de comunicaciones. El primer NODO de comunicaciones tiene una relación de confianza con el segundo NODO de comunicaciones. El segundo mensaje es el mensaje recibido en la etapa 903. El identificador de mensaje es, por ejemplo, un hash o un identificador único que puede usarse para identificar el segundo mensaje. Por tanto, de acuerdo con un modo de realización a modo de ejemplo, el primer

mensaje incluye información para validar el segundo mensaje enviado desde el segundo NODO de comunicaciones. El funcionamiento avanza desde la etapa 904 hasta la etapa 905.

En la etapa 905, el primer NODO de comunicaciones valida el segundo mensaje. El primer NODO usa información, por ejemplo, un hash u otro identificador único, comunicada por el primer mensaje, junto con otra información relevante incluida en el segundo mensaje para comprobar la validez del segundo mensaje. En algunos modos de realización, el segundo mensaje incluye, por ejemplo, un hash generado a partir del primer mensaje y un nonce. En algunos de dichos modos de realización, el primer mensaje puede incluir también, el nonce transmitido en el segundo mensaje. El primer mensaje puede transmitir, y algunas veces lo hace, la firma del emisor. Por tanto, usando la información comunicada por el primer mensaje y la información incluida en el segundo mensaje, el primer NODO de comunicaciones valida el segundo mensaje. Debería apreciarse que el primer NODO de comunicaciones realiza el funcionamiento de validación para verificar y/o garantizar, por ejemplo, que la carga útil del segundo mensaje no se ha alterado. El funcionamiento avanza desde la etapa 905 hasta la etapa 906.

En la etapa 906, el primer NODO de comunicaciones recibe un mensaje de petición de confirmación de confianza desde un tercer NODO de comunicaciones, por ejemplo, el NODO C 106, con el que tiene una relación de confianza. El tercer NODO de comunicaciones puede estar interesado en usar el servicio ofrecido indicado en el segundo mensaje y puede enviar el mensaje de petición de confirmación de confianza a uno o más de sus amigos de confianza para reunir, por ejemplo, información confiable, respecto al segundo NODO de comunicaciones. Puesto que el primer NODO de comunicaciones es un amigo de confianza del tercer NODO de comunicaciones, recibe el mensaje de petición de confirmación de confianza. En algunos modos de realización, el mensaje de petición de confirmación de confianza incluye el identificador de mensaje que identifica el segundo mensaje y al menos una de una firma de emisor, por ejemplo, una firma de NODO C 106 o un código de autenticación de mensaje. Debería apreciarse que el mensaje de petición de confirmación de confianza puede transmitir esta información, por ejemplo, de modo que el primer NODO de comunicaciones que reciba el mensaje de petición de confirmación de confianza pueda saber que la petición de confirmación de confianza es realizada por un amigo de confianza y, en segundo lugar, de modo que el primer NODO de comunicaciones pueda identificar el mensaje y/o el emisor respecto a qué terceras comunicaciones busca la información de confiabilidad. El funcionamiento avanza desde la etapa 906 hasta la etapa 908.

En la etapa 908, el primer NODO de comunicaciones genera un tercer mensaje, por ejemplo, un mensaje de propagación de confianza, que utiliza el identificador de mensaje que identifica el segundo mensaje, que se incluyó en el primer mensaje. El tercer mensaje, en algunos modos de realización, incluye campos que se obtienen de o se basan en uno o más campos en el primer mensaje. En algunos modos de realización, como parte de la generación del tercer mensaje en la etapa 908, se realiza la subetapa 910. En la subetapa 910 se incluye en el tercer mensaje la segunda información de validación de mensaje, por ejemplo, un valor de hash unidireccional y/o una clave, que puede usarse para verificar la autenticidad y/o la integridad del segundo mensaje. Por tanto, en algunos modos de realización, la información para verificar que los contenidos del segundo mensaje no se han alterado se incluye en el tercer mensaje. Esto permite que un NODO que reciba el tercer mensaje verifique la autenticidad y/o la integridad del segundo mensaje.

El funcionamiento avanza desde la etapa 908 hasta la etapa 912 en el que se realiza una determinación de si el primer NODO de comunicaciones está o no dentro de un intervalo predeterminado de la ubicación indicada en el segundo mensaje o dentro de un intervalo, indicado en el segundo mensaje de la ubicación indicada en el segundo mensaje. El intervalo puede ser, por ejemplo, un valor que el usuario del segundo NODO de comunicaciones pueda establecer antes de enviar el segundo mensaje. En el caso de que, en la etapa 912, se determine que el primer NODO de comunicaciones no está dentro de uno de: i) un intervalo predeterminado de la posición indicada en el segundo mensaje o ii) dentro de un intervalo, indicado en el segundo mensaje, de la ubicación indicada en el segundo mensaje, entonces el funcionamiento avanza desde la etapa 912 hasta la etapa 913 donde el primer NODO de comunicaciones se abstiene de transmitir el tercer mensaje. El funcionamiento avanza desde la etapa 913 de vuelta a las etapas 903 y 904.

En algunos modos de realización, cuando se determina que el primer NODO de comunicaciones está dentro de uno de un intervalo predeterminado de la ubicación indicada en el segundo mensaje o dentro de un intervalo, indicado en el segundo mensaje, de la ubicación indicada en el segundo mensaje, entonces el funcionamiento avanza desde la etapa 912 hasta la etapa 914. En la etapa 914, el primer NODO de comunicaciones transmite el tercer mensaje generado al tercer NODO de comunicaciones, incluyendo el tercer mensaje la información de verificación de fuente de mensaje y el identificador de mensaje que identifica el segundo mensaje. Obsérvese que existe una relación de confianza entre el tercer NODO de comunicaciones y el primer NODO de comunicaciones. La información de verificación de fuente es, por ejemplo, la firma del primer NODO de comunicaciones que transmite el tercer mensaje. En algunos modos de realización, el tercer mensaje se transmite en respuesta al mensaje de petición de confirmación de confianza, recibido por el primer NODO de comunicaciones en la etapa 906. Debería apreciarse que, puesto que el tercer mensaje es firmado por el primer NODO de comunicaciones, esto permite que el tercer NODO reconozca que el tercer mensaje proviene de su amigo de confianza. En segundo lugar, puesto que el único identificador que identifica el segundo mensaje está incluido en el tercer mensaje, esto permite al tercer NODO de comunicaciones comprobar que la información comunicada en el segundo mensaje es válida. El funcionamiento

avanza desde la etapa 914 hasta la etapa 916.

En la etapa 916, el primer NODO de comunicaciones recibe una respuesta al segundo mensaje desde el tercer NODO de comunicaciones. En algunos modos de realización, el tercer NODO de comunicaciones envía la respuesta después de determinar que la información comunicada por el segundo mensaje es confiable. La respuesta recibida puede ser, por ejemplo, una indicación y/o una confirmación de que el tercer NODO de comunicaciones está interesado en usar el servicio ofrecido por el segundo NODO de comunicaciones y le gustaría interactuar directamente con el segundo NODO de comunicaciones.

El funcionamiento avanza desde la etapa 916 hasta la etapa 918 en el que el primer NODO de comunicaciones comunica la respuesta recibida al segundo NODO de comunicaciones. En algunos modos de realización, la respuesta recibida se comunica con la información de seguridad correspondiente al primer NODO de comunicaciones, desde el primer NODO de comunicaciones hasta el segundo NODO de comunicaciones. El funcionamiento avanza desde la etapa 918 hasta las entradas de las etapas 903 y 904.

En un modo de realización a modo de ejemplo donde se considera que el diagrama de flujo 900 corresponde al ejemplo de la Figura 2, el primer NODO de comunicaciones es el NODO B 104, el segundo NODO de comunicaciones es el NODO A 102, el tercer NODO de comunicaciones es el NODO C 106, el segundo mensaje es el MSG 1 203, el primer mensaje es el mensaje MSG 2 210, el mensaje de petición de confirmación de confianza es el mensaje 216, el tercer mensaje es el mensaje MSG 3 222, la respuesta recibida es el mensaje 227 de respuesta 1 y la respuesta comunicada al segundo NODO de comunicaciones con la información de seguridad opcional es el mensaje 229 de respuesta 2.

En otro modo de realización a modo de ejemplo donde se considera que el diagrama de flujo 900 corresponde al ejemplo de la Figura 3, el primer NODO de comunicaciones es el NODO B 104, el segundo NODO de comunicaciones es el NODO A 102, el tercer NODO de comunicaciones es el NODO C 106, el segundo mensaje es el MSG 1 303, el primer mensaje es el mensaje MSG 2 310, el mensaje de petición de confirmación de confianza es el mensaje 316, el tercer mensaje es el mensaje MSG 3 322, la respuesta recibida es el mensaje 327 de respuesta 1 y la respuesta comunicada al segundo NODO de comunicaciones con la información de seguridad opcional es el mensaje 329 de respuesta 2.

En otro modo de realización más a modo de ejemplo donde se considera que el diagrama de flujo 900 corresponde al ejemplo de la Figura 4, el primer NODO de comunicaciones es el NODO B 104, el segundo NODO de comunicaciones es el NODO A 102, el tercer NODO de comunicaciones es el NODO C 106, el segundo mensaje es el MSG 1 403, el primer mensaje es el mensaje MSG 2 410, el mensaje de petición de confirmación de confianza es el mensaje 416', el tercer mensaje es el mensaje MSG 3 422, la respuesta recibida es el mensaje 435 de respuesta 2 y la respuesta comunicada al segundo NODO de comunicaciones con la información de seguridad opcional es el mensaje 437 de respuesta 3.

Las Figuras 10, 11 y 12 muestran formatos de mensaje diferentes a modo de ejemplo de mensajes de petición de confirmación de confianza a modo de ejemplo. Los formatos descritos en las Figuras 10, 11 y 12 pueden usarse para cualquiera de los mensajes de petición de confirmación de confianza a modo de ejemplo que incluyan el mensaje 216 de la Figura 2, el mensaje 316 de la Figura 3, el mensaje 316' de la Figura 3 o el mensaje 416 de la Figura 4 o el mensaje 416' de la Figura 4.

Como se ha indicado anteriormente, un NODO de comunicaciones interesado en, por ejemplo, un servicio ofrecido por otro usuario por medio de, por ejemplo, el mensaje de petición de servicio, puede desear reunir información de credibilidad o confiabilidad suficiente sobre el NODO que envíe el mensaje de oferta de servicio. En algunos ejemplos que hemos indicado, el NODO A 102 anuncia un mensaje de oferta de servicio y el NODO C 106 puede estar interesado en el servicio ofrecido. Por tanto, tras la recepción del mensaje de oferta de servicio, el NODO C 106 envía un mensaje de petición de confirmación de confianza a uno o más de sus pares de confianza. El mensaje de petición de confirmación de confianza puede ser, por ejemplo, una petición a los pares de confianza del NODO C para confirmar si puede confiarse en el emisor del mensaje de oferta de servicio y en el contenido del mensaje. Existe una probabilidad razonable de que, en una zona geográfica, uno o más NODOS de confianza por el NODO C 106 puedan ser conscientes de la reputación del NODO A 102, por ejemplo, debido a un acuerdo pasado con el NODO A 102.

En algunos modos de realización, incluso si un NODO de confianza para el NODO C 106 no es consciente de la confiabilidad del NODO A 102, puede ser capaz de ayudar al NODO C 106 enviando el mensaje de petición de confirmación de confianza a su propia lista de NODOS de confianza que pueda transmitir a su vez el mensaje más. Por ejemplo, en la Figura 4, el NODO E 110 envía el mensaje de petición de confirmación de confianza 416 recibido como mensaje 416' al NODO B 104.

En algunos ejemplos particulares indicados a continuación con respecto a las Figuras 10, 11 y 12, considere que el NODO A 102 es el NODO que anuncia un mensaje de oferta de servicio, el NODO C 106 es el NODO que está interesado en el servicio ofrecido y el NODO B 104 es un NODO que tiene una relación de confianza tanto con el

NODO A 102 como con el NODO C 106.

La Figura 10 es un dibujo que ilustra un formato a modo de ejemplo de un mensaje de petición de confirmación de confianza 1000. El mensaje de petición de confirmación de confianza 1000 a modo de ejemplo incluye un campo 1002 para un identificador de mensaje que identifica un segundo mensaje, un campo 1004 para una firma de emisor y un campo opcional 1006 para un código de autenticación de mensaje.

Para el propósito de la explicación, considere que el mensaje de petición de confirmación de confianza 1000 es el mensaje 216 de la Figura 2. El segundo mensaje es, por ejemplo, el mensaje MSG 1 203 de la Figura 2. El campo de identificador de mensaje 1002, entre otras cosas, puede ayudar al NODO que reciba el mensaje de petición de confirmación de confianza 1000 a identificar qué mensaje de anuncio/mensaje de oferta de servicio está cuestionándose o sobre cuál está hablándose, puesto que es posible que se haya recibido más de un mensaje de anuncio por el Nodo de comunicaciones B 104.

La firma de emisor 1004 puede ser, por ejemplo, la firma del NODO de comunicaciones C 106. La firma del emisor ayuda al NODO de recepción B 104 que recibe el mensaje de petición de confirmación de confianza 1000 a determinar que la petición de confirmación de confianza está siendo realizada por un amigo de confianza. En algunos modos de realización, cuando el mensaje de petición de confirmación de confianza 1000 se recibe desde un usuario no confiable, el NODO que reciba dicha petición, por ejemplo, el NODO B 104, puede decidir simplemente no responder y puede ignorar la petición. El mensaje de petición de confirmación de confianza 1000 a modo de ejemplo puede incluir además un campo opcional 1006 para un código de autenticación de mensaje (MAC). El campo MAC opcional 1006 se muestra usando un recuadro con líneas discontinuas. El campo MAC opcional, si está presente, proporciona un nivel adicional de protección para la integridad de los datos del mensaje de petición de confirmación de confianza así como para la autenticidad.

La Figura 11 muestra un dibujo que ilustra otro formato más a modo de ejemplo del mensaje de petición de confirmación de confianza 1100 a modo de ejemplo. El mensaje de petición de confirmación de confianza 1100 a modo de ejemplo incluye un campo 1102 para un identificador de mensaje que identifica un segundo mensaje, un campo 1106 para un código de autenticación de mensaje y un campo opcional 1104 para una firma de emisor. El campo 1102 de la Figura 11 es el mismo o similar al campo 1002 de la Figura 10; el campo 1106 de la Figura 11 es el mismo o similar al campo 1006 de la Figura 10; el campo 1104 de la Figura 11 es el mismo o similar al campo 1004 de la Figura 10. En este modo de realización particular de la Figura 11, el campo de firma de emisor 1104 es opcional y, por tanto, puede o no estar presente.

La Figura 12 es un dibujo 1200 que ilustra otro formato a modo de ejemplo de un mensaje de petición de confirmación de confianza 1200. El mensaje de petición de confirmación de confianza 1200 a modo de ejemplo incluye un campo 1202 para un identificador de mensaje que identifica un segundo mensaje, un campo 1206 para un código de autenticación de mensaje y un campo 1204 para una firma de emisor. El campo 1202 de la Figura 12 es el mismo o similar al campo 1002 de la Figura 10; el campo 1206 de la Figura 12 es el mismo o similar al campo 1006 de la Figura 10; el campo 1204 de la Figura 12 es el mismo o similar al campo 1004 de la Figura 10. En el formato usado por el mensaje de petición de confirmación de confianza 1200, cada uno de los tres campos 1202, 1206 y 1204 están normalmente incluidos.

La Figura 13 ilustra un NODO de comunicaciones 1300 a modo de ejemplo, que puede usarse como, por ejemplo, el NODO de comunicación B 104, mostrado en la red de comunicación de la Figura 1. El NODO de comunicaciones 1300 puede ser, y en al menos un modo de realización lo es, un terminal inalámbrico móvil que soporte comunicaciones entre pares y que implemente un procedimiento de acuerdo con el diagrama de flujo 900 de la Figura 9. El dispositivo de comunicaciones 1300 incluye un procesador 1302 y una memoria 1304 acoplados entre sí a través de un bus 1309 sobre el cual los diversos elementos (1302, 1304) pueden intercambiar datos e información. El NODO de comunicaciones 1300 incluye además un módulo de entrada 1306 y un módulo de salida 1308 que pueden acoplarse al procesador 1302 como se muestra. Sin embargo, en algunos modos de realización, el módulo de entrada 1306 y el módulo de salida 1308 están ubicados en el interior del procesador 1302. El módulo de entrada 1306 puede recibir señales de entrada. El módulo de entrada 1306 puede incluir, y en algunos modos de realización lo hace, un receptor inalámbrico y/o una interfaz de entrada alámbrica u óptica para recibir la entrada. El módulo de salida 1308 puede incluir, y en algunos modos de realización lo hace, un transmisor inalámbrico y/o una interfaz de salida alámbrica u óptica para transmitir la salida.

El procesador 1302 está configurado para: recibir un primer mensaje desde un segundo NODO de comunicaciones, por ejemplo, un NODO A 102, con el cual existe una relación de confianza, incluyendo el primer mensaje la información de verificación de fuente de mensaje y un identificador de mensaje que identifica un segundo mensaje enviado desde el segundo NODO de comunicaciones y transmitir un tercer mensaje a un tercer NODO de comunicaciones con el cual existe una relación de confianza, comprendiendo el tercer mensaje la información de verificación de fuente de mensaje y dicho identificador de mensaje. En algunos modos de realización, el segundo mensaje incluye información de ubicación. En algunos modos de realización, el procesador 1302 está configurado además para determinar, antes de transmitir el tercer mensaje, si el primer NODO, es decir, el NODO de comunicación 1300, está dentro de uno de un intervalo predeterminado de la ubicación indicada en el segundo

mensaje o dentro de un intervalo, de la ubicación indicada en el segundo mensaje, de la ubicación indicada en el segundo mensaje. En algunos modos de realización, el procesador está configurado para abstenerse de transmitir el tercer mensaje cuando se determine que el primer NODO de comunicaciones 1300 no está dentro de uno de: i) un intervalo predeterminado de la ubicación indicada en el segundo mensaje o ii) dentro de un intervalo, de la ubicación indicada en el segundo mensaje, de la ubicación indicada en el segundo mensaje.

En algunos modos de realización, el procesador 1302 está configurado además para recibir el segundo mensaje, por ejemplo, antes de transmitir el tercer mensaje, validar el segundo mensaje y generar el tercer mensaje usando dicho identificador. En algunos modos de realización, al generar el tercer mensaje, el procesador 1302 está configurado además para incluir, en dicho tercer mensaje, la segunda información de validación de mensaje, por ejemplo, un valor de hash o clave unidireccional, que pueda usarse para verificar la autenticidad y/o la integridad del segundo mensaje.

El procesador 1302, en algunos modos de realización, está configurado además para recibir un mensaje de petición de confirmación de confianza, desde el tercer NODO de comunicaciones, antes de transmitir el tercer mensaje. En algunos modos de realización, el procesador 1302 está configurado para transmitir el tercer mensaje en respuesta a dicho mensaje de petición de confirmación de confianza. En algunos modos de realización, el mensaje de petición de confirmación de confianza incluye dicho identificador de mensaje y al menos uno de una firma de emisor o un código de autenticación de mensaje (MAC). En algunos modos de realización, el procesador 1302 está configurado además para recibir una respuesta al segundo mensaje desde el tercer NODO de comunicaciones y para comunicar la respuesta al segundo NODO de comunicaciones. En algunos modos de realización, el procesador 1302 está configurado además para comunicar la respuesta al segundo NODO de comunicaciones, opcionalmente con la información de seguridad correspondiente al primer NODO de comunicaciones 1300.

En un modo de realización a modo de ejemplo correspondiente al ejemplo de la Figura 2, el primer NODO de comunicaciones 1300 es el NODO B 104, el segundo NODO de comunicaciones es el NODO A 102, el tercer NODO de comunicaciones es el NODO C 106, el segundo mensaje es el MSG 1 203, el primer mensaje es el mensaje MSG 2 210, el mensaje de petición de confirmación de confianza es el mensaje 216, el tercer mensaje es el mensaje MSG 3 222, la respuesta recibida es el mensaje 227 de respuesta 1 y la respuesta comunicada al segundo NODO de comunicaciones con la información de seguridad opcional es el mensaje 229 de respuesta 2.

En otro modo de realización a modo de ejemplo correspondiente al ejemplo de la Figura 3, el primer NODO de comunicaciones 1300 es el NODO B 104, el segundo NODO de comunicaciones es el NODO A 102, el tercer NODO de comunicaciones es el NODO C 106, el segundo mensaje es el MSG 1 303, el primer mensaje es el mensaje MSG 2 310, el mensaje de petición de confirmación de confianza es el mensaje 316, el tercer mensaje es el mensaje MSG 3 322, la respuesta recibida es el mensaje 327 de respuesta 1 y la respuesta comunicada al segundo NODO de comunicaciones con la información de seguridad opcional es el mensaje 329 de respuesta 2.

En otro modo de realización a modo de ejemplo correspondiente al ejemplo de la Figura 4, el primer NODO de comunicaciones 1300 es el NODO B 104, el segundo NODO de comunicaciones es el NODO A 102, el tercer NODO de comunicaciones es el NODO C 106, el segundo mensaje es el MSG 1 403, el primer mensaje es el mensaje MSG 2 410, el mensaje de petición de confirmación de confianza es el mensaje 416', el tercer mensaje es el mensaje MSG 3 422, la respuesta recibida es el mensaje 435 de respuesta 2 y la respuesta comunicada al segundo NODO de comunicaciones con la información de seguridad opcional es el mensaje 437 de respuesta 3.

La Figura 14 es un montaje de módulos 1400 que puede usarse, y en algunos modos de realización lo hace, en el NODO de comunicaciones ilustrado en la Figura 13, por ejemplo, un primer NODO de comunicaciones. Los módulos en el montaje 1400 pueden implementarse en hardware dentro del procesador 1302 de la Figura 13, por ejemplo, como circuitos individuales. De forma alternativa, los módulos pueden implementarse en software y almacenarse en la memoria 1304 del NODO de comunicaciones 1300 mostrado en la Figura 13. Aunque se muestre en el modo de realización de la Figura 13 como un único procesador, por ejemplo, un ordenador, debería apreciarse que el procesador 1302 puede implementarse como uno o más procesadores, por ejemplo, ordenadores.

Cuando se implementan en software, los módulos incluyen un código, que cuando es ejecutado por el procesador 1302, configura el procesador para implementar la función correspondiente al módulo. En los modos de realización donde el montaje de módulos 1400 se almacena en la memoria 1304, la memoria 1304 es un producto de programa informático que comprende un medio legible por ordenador que comprende un código, por ejemplo, un código individual para cada módulo, para hacer que al menos un ordenador, por ejemplo, un procesador 1302, implemente las funciones a las cuales correspondan los módulos.

Pueden usarse módulos basados por completo en hardware o basados por completo en software. Sin embargo, debería apreciarse que puede usarse cualquier combinación de módulos de software y hardware (por ejemplo, circuitos implementados) para implementar las funciones. Como debería apreciarse, los módulos ilustrados en la Figura 14 controlan y/o configuran el NODO de comunicaciones 1300 o elementos en el mismo tal como el procesador 1302, para realizar las funciones de las etapas correspondientes ilustradas en el diagrama de flujo del procedimiento de la Figura 9.

Como se ilustra en la Figura 14, el montaje de módulos 1400 incluye un módulo 1402 para recibir un primer mensaje desde un segundo NODO de comunicaciones con el cual exista una relación de confianza, incluyendo el primer mensaje la información de verificación de fuente de mensaje y un identificador de mensaje que identifica un segundo mensaje enviado desde el segundo NODO de comunicaciones, un módulo 1403 para recibir el segundo mensaje desde el segundo NODO de comunicaciones, un módulo 1404 para validar el segundo mensaje y un módulo 1406 para recibir un mensaje de petición de confirmación de confianza desde un tercer NODO de comunicaciones. En algunos modos de realización, el montaje de módulos 1400 incluye además un módulo 1408 para generar el tercer mensaje usando el identificador de mensaje. El identificador de mensaje es el identificador de mensaje recibido en el primer mensaje. En algunos de dichos modos de realización, el módulo 1408 incluye un módulo 1410 para incluir en el tercer mensaje una segunda información de validación de mensaje que pueda usarse para verificar la autenticidad y/o la integridad del segundo mensaje.

En algunos modos de realización, el segundo mensaje incluye información de ubicación. En algunos modos de realización, el montaje de módulos 1400 incluye además un módulo 1412 para determinar si el primer NODO de comunicaciones, por ejemplo el NODO 1300 que usa el montaje de módulos 1400, está dentro de uno de un intervalo predeterminado de la ubicación indicada en el segundo mensaje o dentro de un intervalo, indicado en el segundo mensaje, de la ubicación indicada en el segundo mensaje. El montaje de módulos 1400 incluye además un módulo 1414 para transmitir el tercer mensaje al tercer NODO de comunicaciones con el cual existe una relación de confianza, incluyendo el tercer mensaje la información de verificación de fuente de mensaje y dicho identificador de mensaje, un módulo 1416 para recibir una respuesta al segundo mensaje desde el tercer NODO de comunicaciones y un módulo 1418 para comunicar la respuesta al segundo NODO de comunicaciones, opcionalmente con la información de seguridad correspondiente al primer NODO 1300 usando el montaje de módulos 1400.

Se describen procedimientos y aparatos para comunicaciones inalámbricas en redes, por ejemplo, redes ad hoc regionales entre pares. Entre los procedimientos y aparatos descritos, se encuentran procedimientos y aparatos para comunicar información y crear confianza entre diversos dispositivos de comunicaciones, por ejemplo NODOS, que soporten la señalización entre pares.

En un modo de realización a modo de ejemplo, un usuario en una red ad hoc puede transmitir, por ejemplo, multidifundir, diferentes tipos de mensajes, por ejemplo, anuncios, peticiones, noticias, etc., a otros usuarios ubicados dentro del alcance de su dispositivo. Los usuarios receptores, que nunca hayan tratado con el emisor antes, normalmente no tendrían forma de determinar si podía confiarse o no en el emisor y si vale la pena o no dedicar tiempo a responder al mensaje del emisor. Obsérvese que esta falta de confianza es independiente de poder validar la firma transmitida por el mensaje. De hecho, un usuario malicioso puede firmar y transmitir, por ejemplo, multidifundir, el mensaje y los receptores pueden ser capaces de validar la firma, pero esto no significa que el emisor sea sincero acerca de su intención. Por ejemplo, un usuario malintencionado puede firmar y transmitir, por ejemplo, difundir, el mensaje "¿Quién está interesado en un viaje gratis a Manhattan en una hora?", pero el emisor malicioso puede no aparecer para realizar el servicio ofrecido. Como consecuencia, ante tal situación, una víctima puede terminar perdiendo su tiempo esperando el paseo prometido. Consideraciones de problemas de confianza similares pueden ser problemáticas desde la perspectiva del emisor. Por ejemplo, aunque el emisor pueda estar dispuesto a dar un paseo gratis a Manhattan, por ejemplo, para obtener los beneficios asociados con una ruta en coche compartido y/o un peaje reducido, él o ella puede no recibir ningún invitado. Por ejemplo, los invitados potenciales que reciban el mensaje que incluya la oferta pueden no tener una relación de confianza existente con la persona que ofrezca el paseo y pueden ignorar la oferta, por ejemplo, sin preocupaciones de seguridad, ni preocupaciones de confianza y/o presentar problemas de sinceridad.

Diversos procedimientos y aparatos novedosos facilitan un receptor de un mensaje de un emisor con el cual el receptor no tiene una relación de confianza existente para determinar si es o no de confianza o si vale la pena o no responder al mensaje del emisor. Nuevos procedimientos y aparatos permiten a los dispositivos entre pares funcionar en una región geográfica para reunir información de credibilidad entre sí y acumular confianza. En algunos, pero no necesariamente en todos los modos de realización, un dispositivo individual puede mantener una lista de sus pares de confianza. Los dispositivos diferentes pueden tener listas diferentes de pares de confianza. Puede existir, y en general existe, cierto solapamiento entre al menos algunas de las diferentes listas. El solapamiento es útil para propagar información de confianza. La información de confianza mantenida de un dispositivo puede propagarse posteriormente a otros usuarios, por ejemplo, facilitando una determinación de confiabilidad con respecto a la información en un mensaje recibido desde un emisor con el cual el receptor no tenga una relación de confianza actual.

Diversos procedimientos y aparatos son beneficiosos para animar a los usuarios a lanzar nuevos tipos de aplicaciones sociales en tiempo real que puedan depender de las conexiones entre pares y/o que sean beneficiosos en la implementación de aplicaciones sociales en tiempo real usando conexiones entre pares. Una ventaja de al menos algunos de los procedimientos y de los aparatos nuevos descritos a modo de ejemplo para proporcionar confianza entre diferentes usuarios se refiere a su escalabilidad. Debido a su naturaleza ad hoc, las conexiones entre pares en cierta zona pueden tener un tamaño muy aleatorio que puede también variar a alta velocidad. Para adaptarse satisfactoriamente a estas variaciones, el rendimiento de una solución exitosa debería aumentar

idealmente con el número de usuarios. En diversos modos de realización a modo de ejemplo descritos, el rendimiento aumenta con el número de usuarios. Otra preocupación puede ser cómo proteger la privacidad del usuario. A veces, cuando envíe un mensaje, por ejemplo, una petición, el emisor puede no desear revelar su verdadera identidad en el mensaje. Diversos modos de realización descritos permiten a un emisor proteger su privacidad aunque permiten también a un receptor reunir información de confianza con respecto al emisor. En algunos modos de realización, puede permitirse al receptor descubrir posteriormente la identidad real del emisor, por ejemplo, al negociar directamente con el mismo.

A partir del análisis anterior debería apreciarse que son posibles numerosas variaciones y modos de realización.

Las técnicas de diversos modos de realización pueden implementarse usando software, hardware y/o una combinación de software y hardware. Diversos modos de realización están dirigidos a aparatos, por ejemplo, NODOS móviles tales como terminales de acceso móvil, estaciones base y/o un sistema de comunicación. Diversos modos de realización están dirigidos también a procedimientos, por ejemplo, al procedimiento de controlar y/o hacer funcionar NODOS móviles, NODOS estacionarios, estaciones base, estaciones de retransmisión, NODOS de retransmisión y/o sistemas de comunicación, por ejemplo, ordenadores centrales. Diversos modos de realización están también dirigidos a máquinas, por ejemplo, un medio legible por ordenador, por ejemplo, una ROM, una RAM, CD, discos duros, etc., que incluyan instrucciones legibles por máquina para controlar una máquina para implementar una o más etapas de un procedimiento. Diversas características están dirigidas a mensajes novedosos y/o al uso de mensajes novedosos. Los mensajes se generan, se almacenan y/o se comunican. Como parte de los procesos de comunicación, uno o más de los mensajes se almacenan antes de la transmisión y se almacenan al recibirlos. Por tanto, algunas características se dirigen a un dispositivo de memoria, por ejemplo, un medio legible por ordenador, que ha almacenado en el mismo uno o más de los mensajes descritos en la presente solicitud. En muchos casos, los mensajes proporcionan eficiencia en términos de su estructura de datos y/u otros beneficios, sobre otros formatos de mensajes que podrían usarse, tal como la capacidad de identificar y acceder fácilmente a cierta información del mensaje.

En diversos modos de realización, los NODOS descritos en el presente documento se implementan usando uno o más módulos para realizar las etapas correspondientes a uno o más procedimientos, por ejemplo, el procesamiento de señales, la generación de mensajes, la determinación y/o etapas de transmisión, etc. Por tanto, en algunos modos de realización, diversas características se implementan usando módulos. Dichos módulos pueden implementarse utilizando software, hardware o una combinación de software y hardware. Muchos de los procedimientos o etapas de procedimientos descritos anteriormente pueden implementarse usando instrucciones ejecutables por máquina, tales como software, incluidas en un medio legible por máquina tal como un dispositivo de memoria, por ejemplo, una RAM, un disco flexible, etc., para controlar una máquina, por ejemplo, un ordenador de uso general con o sin hardware adicional, para implementar la totalidad o porciones de los procedimientos descritos anteriormente, por ejemplo, en uno o más NODOS. Por consiguiente, entre otras cosas, diversos modos de realización están dirigidos a un medio legible por máquina que incluya instrucciones ejecutables por máquina para hacer que una máquina, por ejemplo, un procesador y el hardware asociado, realice una o más de las etapas del(de los) procedimiento(s) descrito(s) anteriormente. Algunos modos de realización están dirigidos a un dispositivo, por ejemplo, un NODO de comunicaciones, que incluya un procesador configurado para implementar una, múltiples o todas las etapas de uno o más procedimientos de la invención.

En algunos modos de realización, el procesador o procesadores, por ejemplo, las CPU, de uno o más dispositivos, por ejemplo, los NODOS de comunicaciones tales como NODOS de acceso y/o terminales inalámbricos, están configurados para realizar las etapas de los procedimientos descritos como si se realizaran mediante el dispositivo de comunicaciones. La configuración del procesador puede conseguirse usando uno o más módulos, por ejemplo, módulos de software, para controlar la configuración del procesador y/o incluyendo hardware en el procesador, por ejemplo, módulos de hardware, para realizar las etapas citadas y/o la configuración del procesador de control. Por consiguiente, algunos pero no todos los modos de realización están dirigidos a un dispositivo, por ejemplo, un NODO de comunicaciones, con un procesador que incluya un módulo correspondiente a cada una de las etapas de los diversos procedimientos descritos realizados por el dispositivo en el cual se incluya el procesador. En algunos pero no todos los modos de realización, un dispositivo, por ejemplo, un NODO de comunicaciones, incluye un módulo correspondiente a cada una de las etapas de los diversos procedimientos descritos realizados por el dispositivo en el cual se incluya el procesador. Los módulos pueden implementarse usando software y/o hardware.

Algunos modos de realización están dirigidos a un producto de programa informático que comprenda un medio legible por ordenador que comprenda un código para hacer que un ordenador o múltiples ordenadores implementen diversas funciones, etapas, acciones y/u operaciones, por ejemplo, una o más etapas descritas anteriormente. Dependiendo del modo de realización, el producto de programa informático puede, y a veces lo hace, incluir un código diferente para cada etapa que vaya a realizar. Por tanto, el producto de programa informático puede, y a veces lo hace, incluir un código para cada etapa individual de un procedimiento, por ejemplo, un procedimiento de control de un dispositivo o NODO de comunicaciones. El código puede ser en forma de máquina, por ejemplo un ordenador, instrucciones ejecutables almacenadas en un medio legible por ordenador tal como una RAM (Memoria de Acceso Aleatorio), una ROM (Memoria de Solo Lectura) u otro tipo de dispositivo de almacenamiento. Además de estar dirigidos a un producto de programa informático, algunos modos de realización están dirigidos a un procesador

configurado para implementar una o más de las diversas funciones, etapas, acciones y/u operaciones de uno o más procedimientos descritos anteriormente. Por consiguiente, algunos modos de realización están dirigidos a un procesador, por ejemplo, una CPU, configurado para implementar algunas o todas las etapas de los procedimientos descritos en el presente documento. El procesador puede ser para su uso en, por ejemplo, un dispositivo de comunicaciones u otro dispositivo descrito en la presente solicitud.

Aunque se hayan descrito en el contexto de un sistema OFDM, al menos algunos de los procedimientos y aparatos de diversos modos de realización son aplicables a una amplia gama de sistemas de comunicación que incluyan muchos sistemas no OFDM y/o no celulares.

Numerosas variaciones adicionales en los procedimientos y aparatos de los diversos modos de realización descritos anteriormente resultarán evidentes para los expertos en la técnica en vista de la descripción anterior. Dichas variaciones deben considerarse dentro del alcance. Los procedimientos y aparatos pueden usarse, y en diversos modos de realización lo hacen, con CDMA, con multiplexación por división ortogonal de frecuencia (OFDM) y/o con otros diversos tipos de técnicas de comunicaciones que puedan usarse para proporcionar enlaces de comunicaciones inalámbricas entre los NODOS de acceso y los NODOS móviles. En algunos modos de realización, los NODOS de acceso se implementan como estaciones base que establecen enlaces de comunicaciones con NODOS móviles usando el OFDM y/o el CDMA. En diversos modos de realización, los NODOS móviles se implementan como ordenadores portátiles, asistentes de datos personales (PDA) u otros dispositivos portátiles que incluyen circuitos receptores/transmisores y lógica y/o rutinas, para implementar los procedimientos.

REIVINDICACIONES

1. Un procedimiento (902) para hacer funcionar un primer nodo de comunicaciones (104) en una red de comunicación inalámbrica entre pares, que comprende:

recibir (908) un primer mensaje (310) desde un segundo nodo de comunicaciones (102) con el cual existe una relación de confianza, incluyendo el primer mensaje (310) la información de verificación de fuente de mensaje y un identificador de mensaje que identifica un segundo mensaje (303) enviado desde el segundo NODO de comunicaciones (102) a un tercer nodo de comunicaciones (106); y

transmitir (914) un tercer mensaje (322) al tercer NODO de comunicaciones (106) con el que existe una relación de confianza, incluyendo el tercer mensaje (322) información de verificación de fuente de mensaje y dicho identificador de mensaje.

2. El procedimiento según la reivindicación 1, que comprende además:

recibir (903) dicho segundo mensaje (303);

validar (905) dicho segundo mensaje (303); y

generar (908) dicho tercer mensaje (322) usando dicho identificador de mensaje.

3. El procedimiento según la reivindicación 1, que comprende además:

recibir (906) un mensaje de petición de confirmación de confianza (316) desde el tercer NODO de comunicaciones (106) antes de transmitir dicha transmisión (914), transmitiéndose dicho tercer mensaje (322) en respuesta a dicho mensaje de petición de confirmación de confianza (316).

4. El procedimiento según la reivindicación 3, en el que dicho mensaje de petición de confirmación de confianza (316) incluye dicho identificador de mensaje y al menos uno de una firma de emisor o de un código de autenticación de mensaje.

5. El procedimiento según la reivindicación 3, que comprende además:

recibir (916) una respuesta a dicho segundo mensaje (303) desde el tercer NODO de comunicaciones (106); y

comunicar (918) la respuesta al segundo NODO de comunicaciones (102).

6. El procedimiento según la reivindicación 5, en el que dicha comunicación (918) de la respuesta al segundo NODO de comunicaciones (102) comprende comunicar (918) la respuesta con información de seguridad correspondiente al primer NODO de comunicaciones (104).

7. El primer NODO de comunicaciones (104) en una red de comunicación inalámbrica entre pares que comprende:

medios (1402) para recibir un primer mensaje (310) desde un segundo NODO de comunicaciones (102) con el cual existe una relación de confianza, incluyendo el primer mensaje (310) la información de verificación de fuente de mensaje y un identificador de mensaje que identifica un segundo mensaje (303) enviado desde el segundo NODO de comunicaciones (102) a un tercer NODO de comunicaciones (106) y

medios (1414) para transmitir un tercer mensaje (322) al tercer NODO de comunicaciones (106) con el cual existe una relación de confianza, incluyendo el tercer mensaje (322) la información de verificación de fuente de mensaje y dicho identificador de mensaje.

8. El primer NODO de comunicaciones de la reivindicación 7, que comprende además:

medios (1403) para recibir dicho segundo mensaje (303);

medios (1404) para validar dicho segundo mensaje (303); y

medios (1408) para generar dicho tercer mensaje (322) usando dicho identificador de mensaje.

9. El primer NODO de comunicaciones de la reivindicación 7, que comprende además:

medios (1406) para recibir un mensaje de petición de confirmación de confianza desde el tercer NODO de

comunicaciones antes de dicha transmisión, transmitiéndose dicho tercer mensaje (322) en respuesta a dicho mensaje de petición de confirmación de confianza.

10. El primer NODO de comunicaciones de la reivindicación 9, en el que dicho mensaje de petición de confirmación de confianza incluye dicho identificador de mensaje y al menos uno de una firma de emisor o de un código de autenticación de mensaje.

11. Un producto de programa informático para su uso en un primer NODO de comunicaciones (104; 106) que soporta la señalización entre pares, que comprende:

un medio legible por ordenador, que comprende:

un código para hacer que al menos un ordenador implemente las etapas de acuerdo con una cualquiera de las reivindicaciones 1-6.

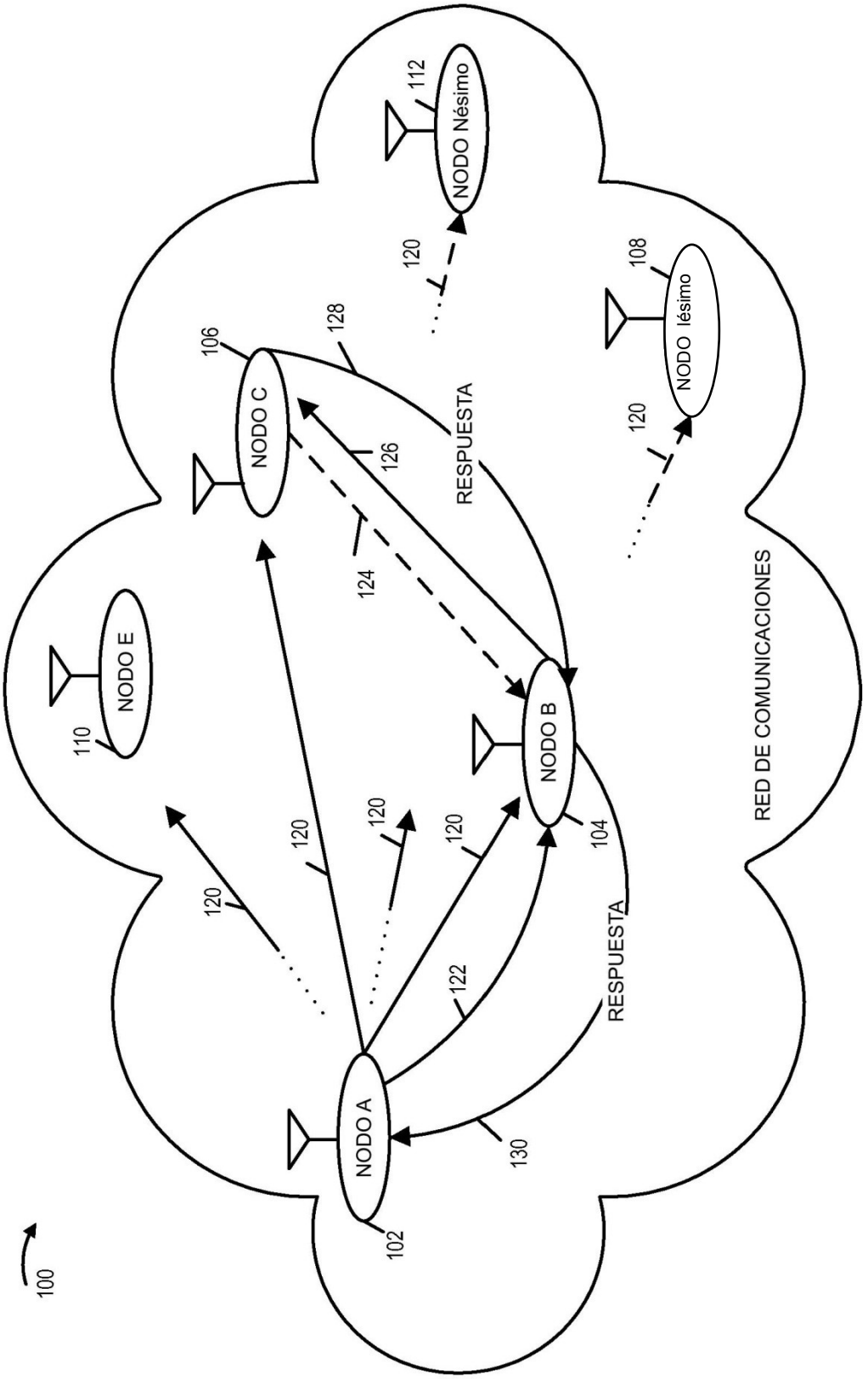
100
NODO A
102
NODO B
104
NODO C
106
NODO lésimo
108
NODO E
110
NODO Nésimo
112
RED DE COMUNICACIONES
120
122
124
126
128
130
RESPUESTA
RESPUESTA

FIGURA 1

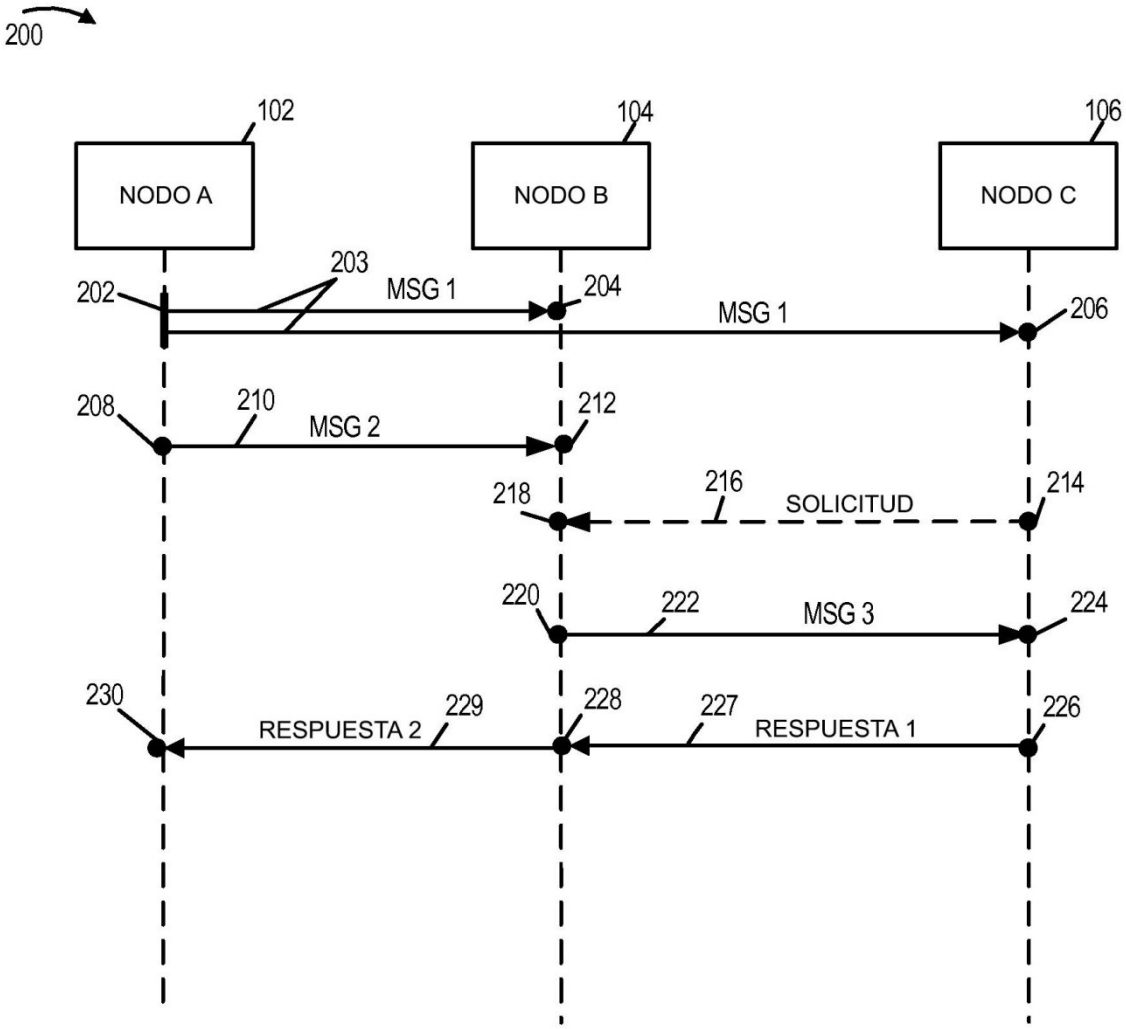
200
102
NODO A
104
NODO B
106
NODO C
203
202
MSG 1
204
MSG 1
206
208
210
MSG 2
212
218
216
SOLICITUD
214
220
222
MSG 3
224
230
229
RESPUESTA 2
228
227
RESPUESTA 1
226

FIGURA 2

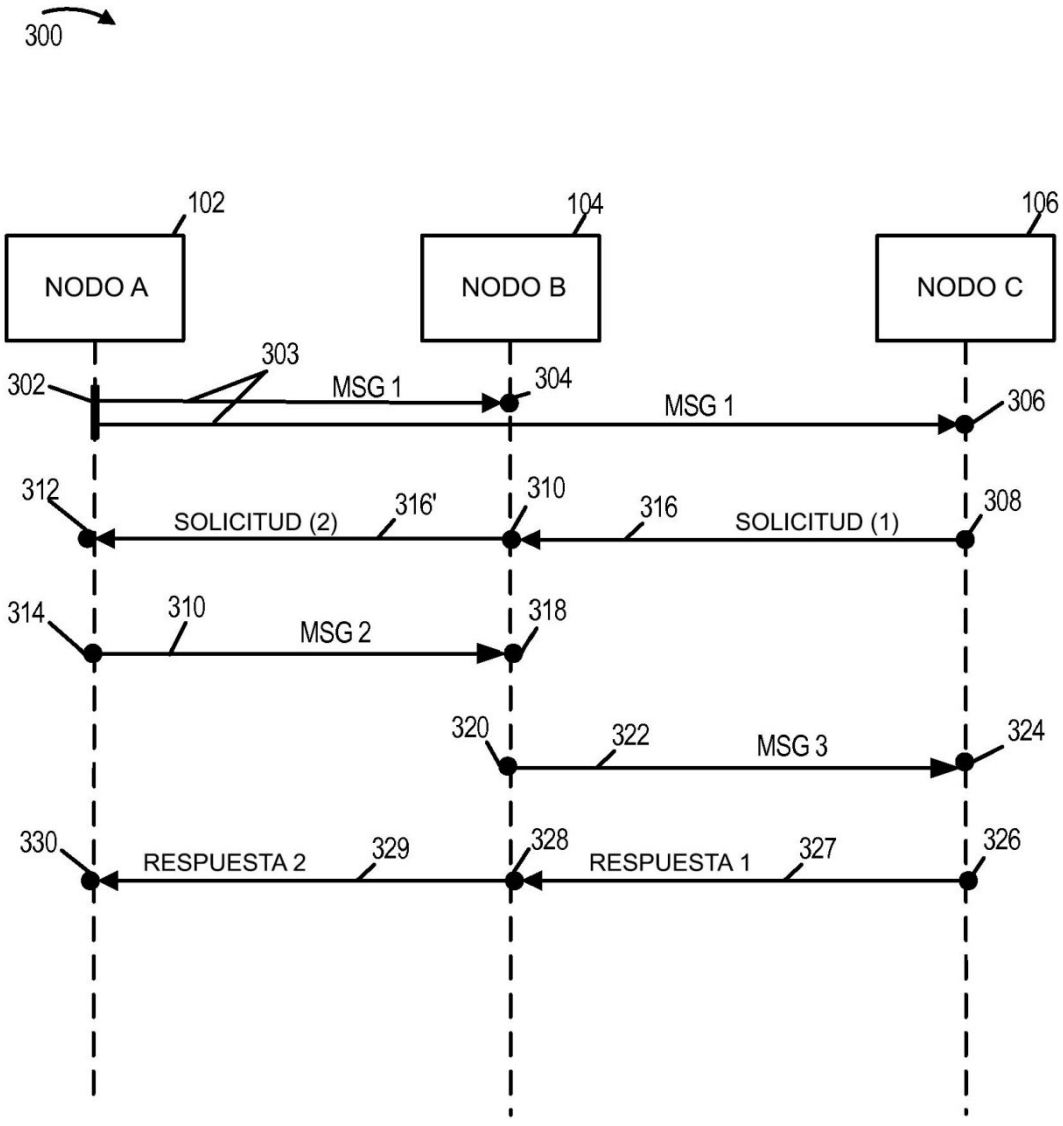
300
102
NODO A
104
NODO B
106
NODO C
303
302
MSG 1
304
MSG 1
306
312
SOLICITUD (2)
316'
310
316
SOLICITUD (1)
308
314
310
MSG 2
318
320
322
MSG 3
324
330
RESPUESTA 2
329
328
RESPUESTA 1
327
326

FIGURA 3

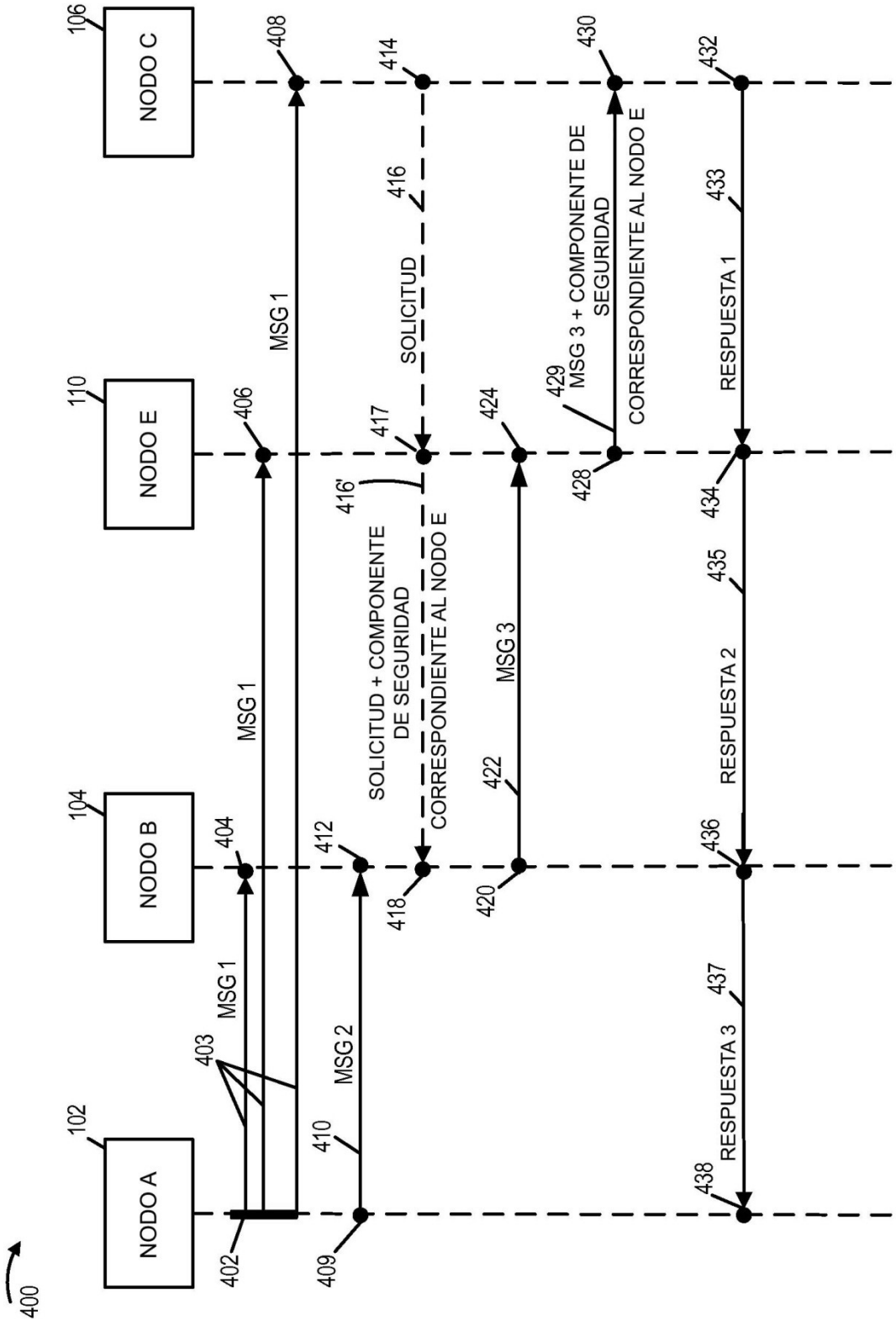
400
NODO A
NODO B
NODO E
NODO C
102
104
110
106
402
403
MSG 1
MSG 1
MSG 2
409
410
404
MSG 1
406
408
412
SOLICITUD + COMPONENTE DE SEGURIDAD
CORRESPONDIENTE AL NODO E
416'
417
SOLICITUD
416
414
418
422
MSG 3
420
424
429
MSG 3 + COMPONENTE DE SEGURIDAD
CORRESPONDIENTE AL NODO E
428
430
434
RESPUESTA 1
433
432
435
RESPUESTA 2
436
437
RESPUESTA 3
438

FIGURA 4

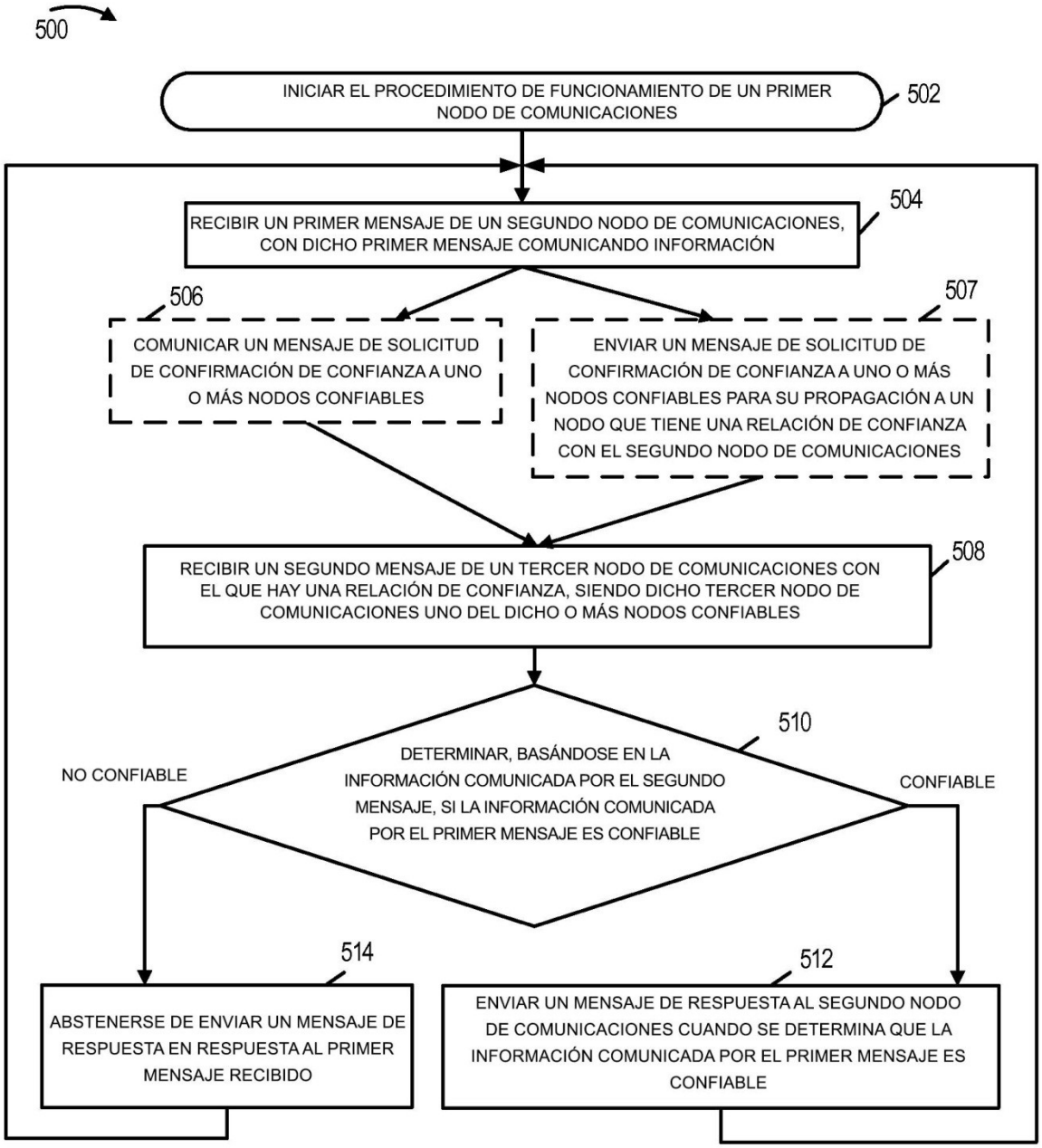
500
INICIAR EL PROCEDIMIENTO DE FUNCIONAMIENTO DE UN PRIMER NODO DE COMUNICACIONES
502
RECIBIR UN PRIMER MENSAJE DE UN SEGUNDO NODO DE COMUNICACIONES, CON DICHO PRIMER MENSAJE COMUNICANDO INFORMACIÓN
504
506
COMUNICAR UN MENSAJE DE SOLICITUD DE CONFIRMACIÓN DE CONFIANZA A UNO O MÁS NODOS CONFIABLES
507
ENVIAR UN MENSAJE DE SOLICITUD DE CONFIRMACIÓN DE CONFIANZA A UNO O MÁS NODOS CONFIABLES PARA SU PROPAGACIÓN A UN NODO QUE TIENE UNA RELACIÓN DE CONFIANZA CON EL SEGUNDO NODO DE COMUNICACIONES
RECIBIR UN SEGUNDO MENSAJE DE UN TERCER NODO DE COMUNICACIONES CON EL QUE HAY UNA RELACIÓN DE CONFIANZA, SIENDO DICHO TERCER NODO DE COMUNICACIONES UNO DEL DICHO O MÁS NODOS CONFIABLES
508
510
DETERMINAR, BASÁNDOSE EN LA INFORMACIÓN COMUNICADA POR EL SEGUNDO MENSAJE, SI LA INFORMACIÓN COMUNICADA POR EL PRIMER MENSAJE ES CONFIABLE
NO CONFIABLE
CONFIABLE
514
ABSTENERSE DE ENVIAR UN MENSAJE DE RESPUESTA EN RESPUESTA AL PRIMER MENSAJE RECIBIDO
512
ENVIAR UN MENSAJE DE RESPUESTA AL SEGUNDO NODO DE COMUNICACIONES CUANDO SE DETERMINA QUE LA INFORMACIÓN COMUNICADA POR EL PRIMER MENSAJE ES CONFIABLE

FIGURA 5

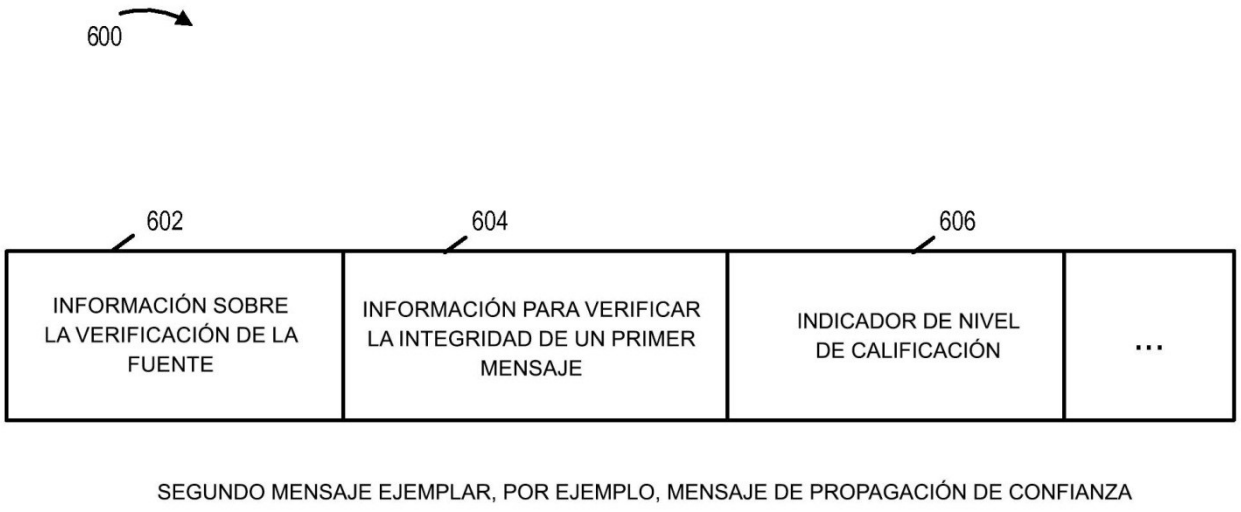
600
602
604
606
INFORMACIÓN SOBRE LA VERIFICACIÓN DE LA FUENTE
INFORMACIÓN PARA VERIFICAR LA INTEGRIDAD DE UN PRIMER MENSAJE
INDICADOR DE NIVEL DE CALIFICACIÓN
...
SEGUNDO MENSAJE EJEMPLAR, POR EJEMPLO, MENSAJE DE PROPAGACIÓN DE CONFIANZA

FIGURA 6

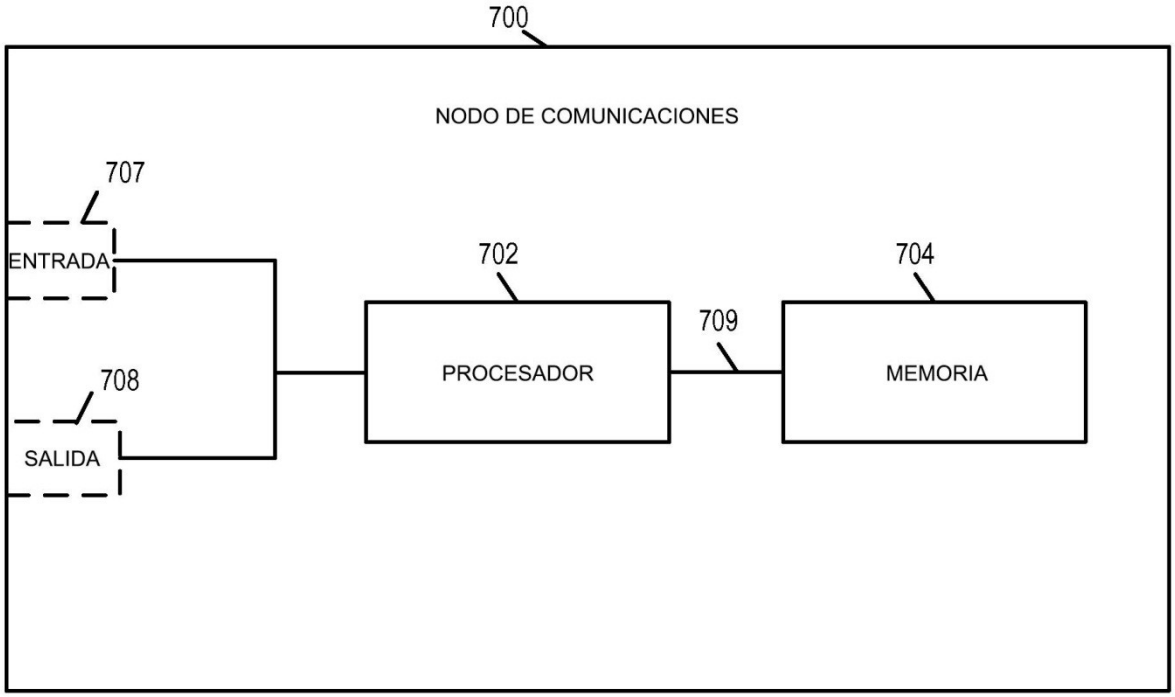
700
NODO DE COMUNICACIONES
707
ENTRADA
708
SALIDA
702
PROCESADOR
709
704
MEMORIA

FIGURA 7

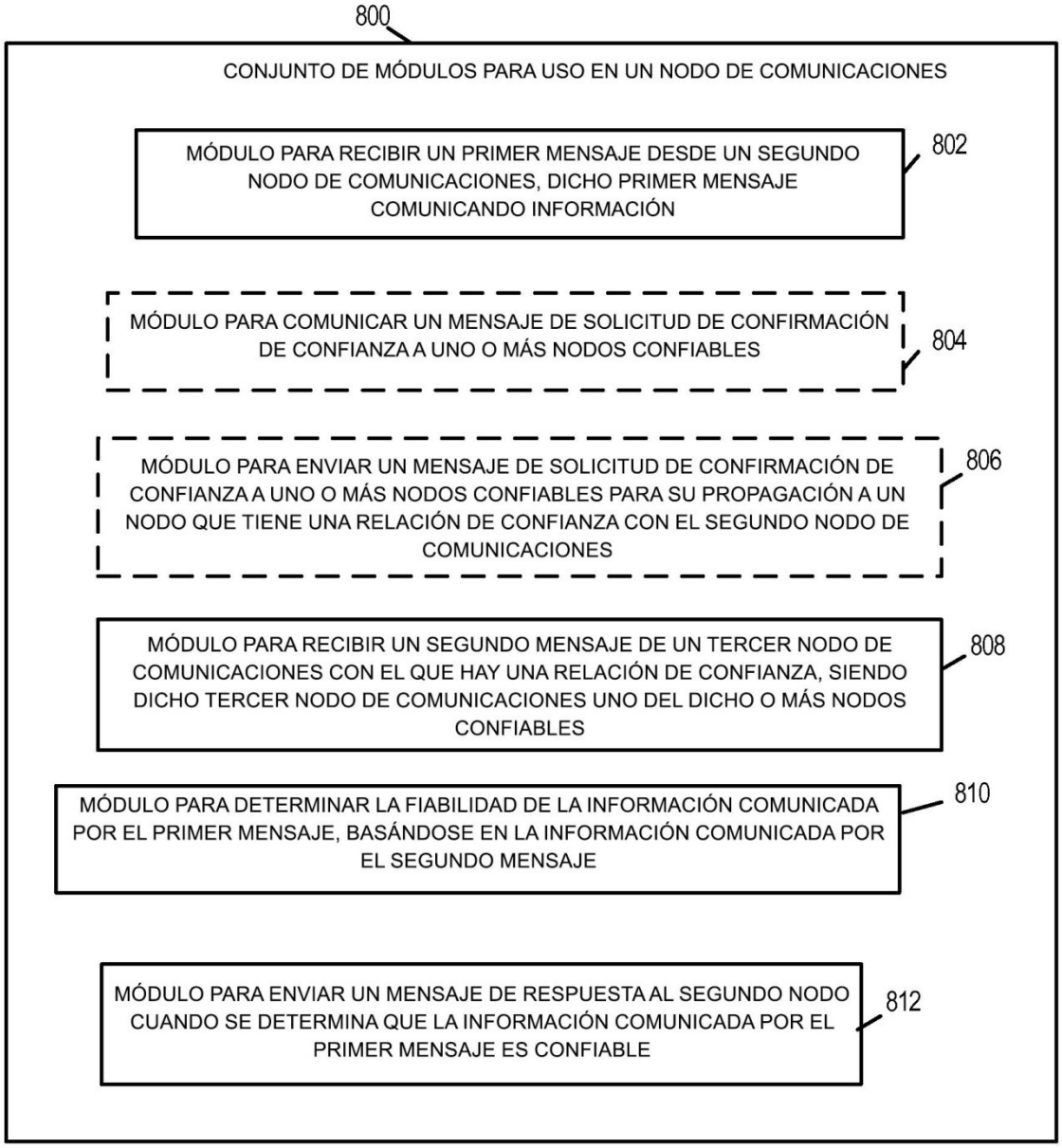
800
CONJUNTO DE MÓDULOS PARA USO EN UN NODO DE COMUNICACIONES
MÓDULO PARA RECIBIR UN PRIMER MENSAJE DESDE UN SEGUNDO NODO DE COMUNICACIONES, DICHO PRIMER MENSAJE COMUNICANDO INFORMACIÓN
802
MÓDULO PARA COMUNICAR UN MENSAJE DE SOLICITUD DE CONFIRMACIÓN DE CONFIANZA A UNO O MÁS NODOS CONFIABLES
804
MÓDULO PARA ENVIAR UN MENSAJE DE SOLICITUD DE CONFIRMACIÓN DE CONFIANZA A UNO O MÁS NODOS CONFIABLES PARA SU PROPAGACIÓN A UN NODO QUE TIENE UNA RELACIÓN DE CONFIANZA CON EL SEGUNDO NODO DE COMUNICACIONES
806
MÓDULO PARA RECIBIR UN SEGUNDO MENSAJE DE UN TERCER NODO DE COMUNICACIONES CON EL QUE HAY UNA RELACIÓN DE CONFIANZA, SIENDO DICHO TERCER NODO DE COMUNICACIONES UNO DEL DICHO O MÁS NODOS CONFIABLES
808
MÓDULO PARA DETERMINAR LA FIABILIDAD DE LA INFORMACIÓN COMUNICADA POR EL PRIMER MENSAJE, BASÁNDOSE EN LA INFORMACIÓN COMUNICADA POR EL SEGUNDO MENSAJE
810
MÓDULO PARA ENVIAR UN MENSAJE DE RESPUESTA AL SEGUNDO NODO CUANDO SE DETERMINA QUE LA INFORMACIÓN COMUNICADA POR EL PRIMER MENSAJE ES CONFIABLE
812

FIGURA 8

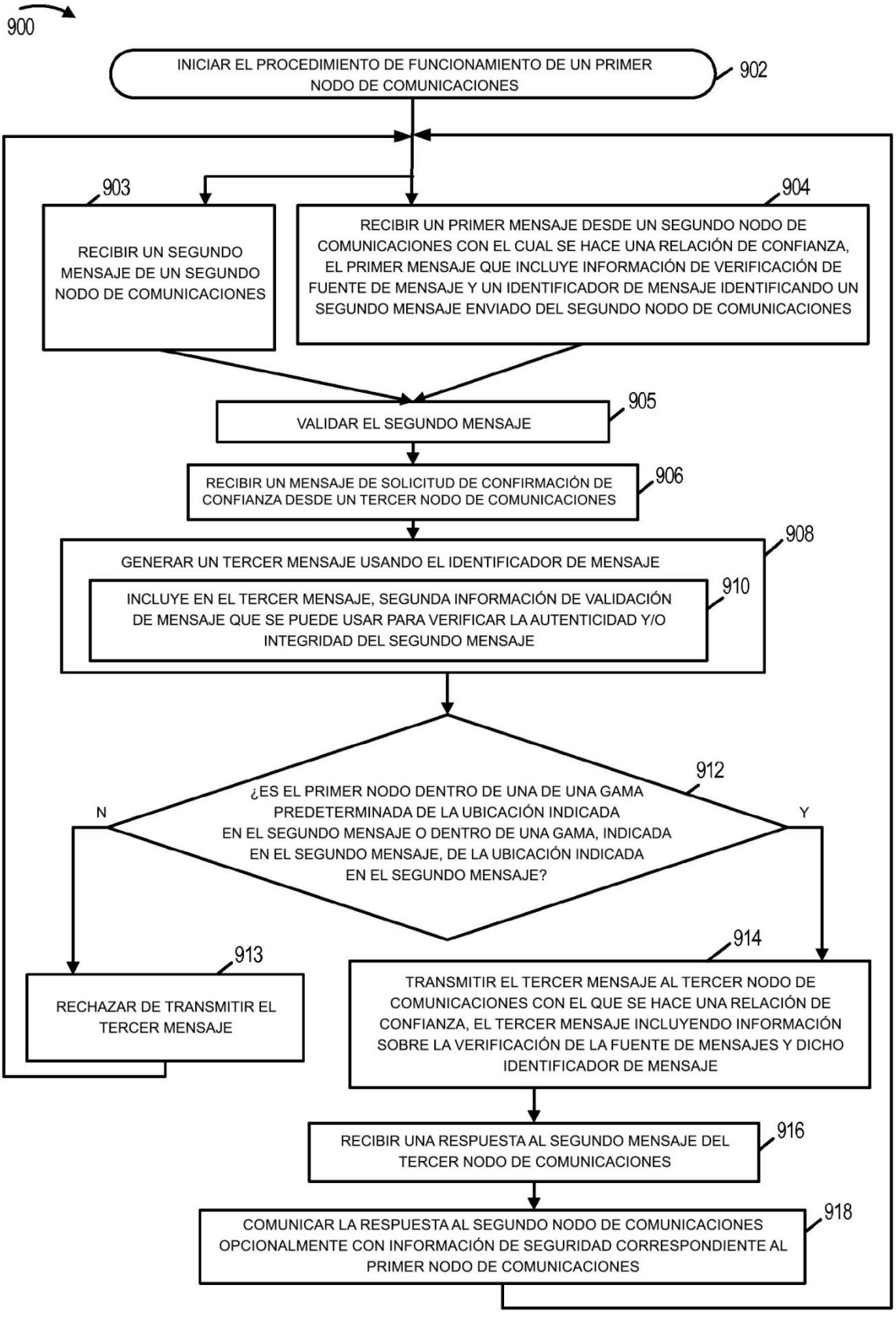
900
INICIAR EL PROCEDIMIENTO DE FUNCIONAMIENTO DE UN PRIMER NODO DE COMUNICACIONES
902
903
RECIBIR UN SEGUNDO MENSAJE DE UN SEGUNDO NODO DE COMUNICACIONES
904
RECIBIR UN PRIMER MENSAJE DESDE UN SEGUNDO NODO DE COMUNICACIONES CON EL CUAL SE HACE UNA RELACIÓN DE CONFIANZA, EL PRIMER MENSAJE QUE INCLUYE INFORMACIÓN DE VERIFICACIÓN DE FUENTE DE MENSAJE Y UN IDENTIFICADOR DE MENSAJE IDENTIFICANDO UN SEGUNDO MENSAJE ENVIADO DEL SEGUNDO NODO DE COMUNICACIONES
VALIDAR EL SEGUNDO MENSAJE
905
RECIBIR UN MENSAJE DE SOLICITUD DE CONFIRMACIÓN DE CONFIANZA DESDE UN TERCER NODO DE COMUNICACIONES
906
GENERAR UN TERCER MENSAJE USANDO EL IDENTIFICADOR DE MENSAJE
908
INCLUYE EN EL TERCER MENSAJE, SEGUNDA INFORMACIÓN DE VALIDACIÓN DE MENSAJE QUE SE PUEDE USAR PARA VERIFICAR LA AUTENTICIDAD Y/O INTEGRIDAD DEL SEGUNDO MENSAJE
910
¿ES EL PRIMER NODO DENTRO DE UNA DE UNA GAMA PREDETERMINADA DE LA UBICACIÓN INDICADA EN EL SEGUNDO MENSAJE O DENTRO DE UNA GAMA, INDICADA EN EL SEGUNDO MENSAJE, DE LA UBICACIÓN INDICADA EN EL SEGUNDO MENSAJE?
912
N
Y
RECHAZAR DE TRANSMITIR EL TERCER MENSAJE
913
TRANSMITIR EL TERCER MENSAJE AL TERCER NODO DE COMUNICACIONES CON EL QUE SE HACE UNA RELACIÓN DE CONFIANZA, EL TERCER MENSAJE INCLUYENDO INFORMACIÓN SOBRE LA VERIFICACIÓN DE LA FUENTE DE MENSAJES Y DICHO IDENTIFICADOR DE MENSAJE
914
RECIBIR UNA RESPUESTA AL SEGUNDO MENSAJE DEL TERCER NODO DE COMUNICACIONES
916
COMUNICAR LA RESPUESTA AL SEGUNDO NODO DE COMUNICACIONES OPCIONALMENTE CON INFORMACIÓN DE SEGURIDAD CORRESPONDIENTE AL PRIMER NODO DE COMUNICACIONES
918

FIGURA 9

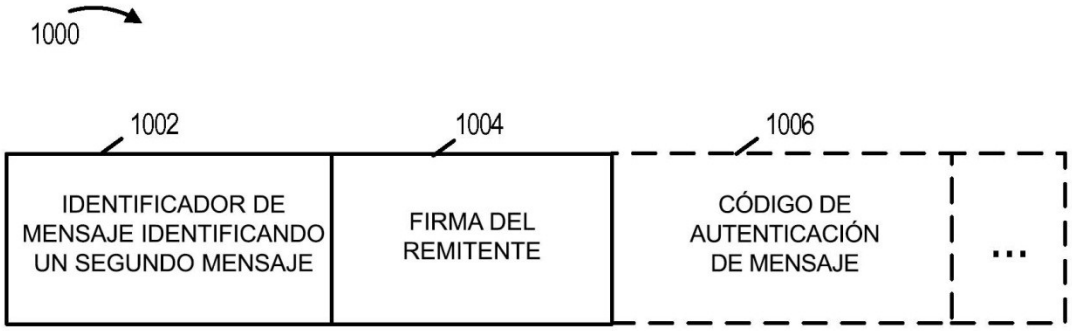

FIGURA 10

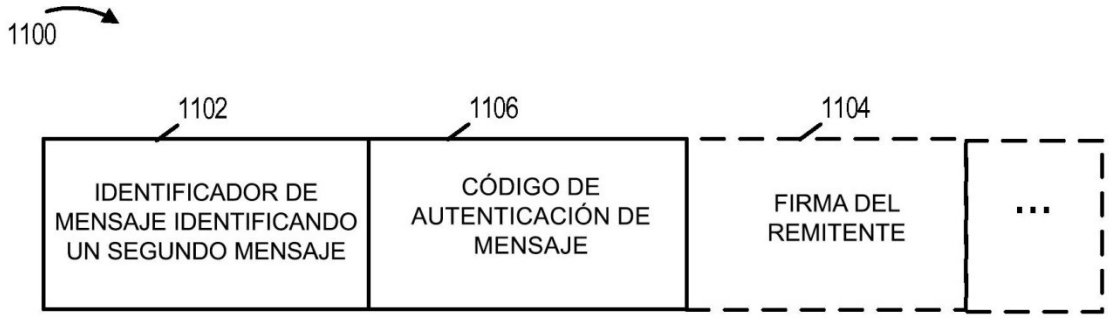

FIGURA 11

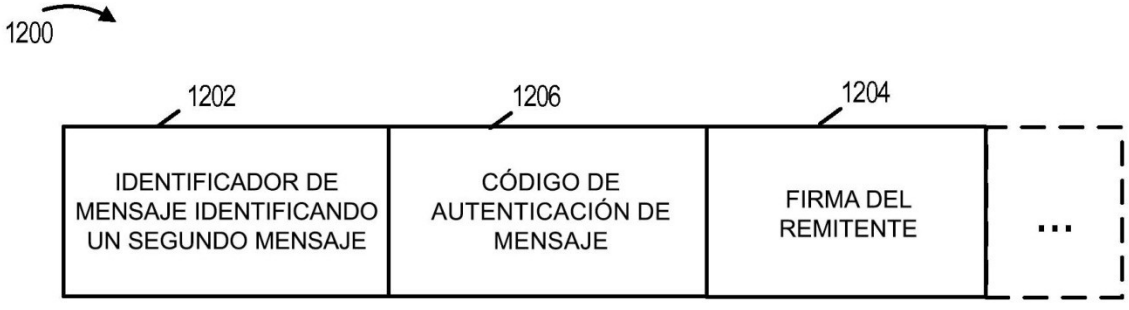

FIGURA 12

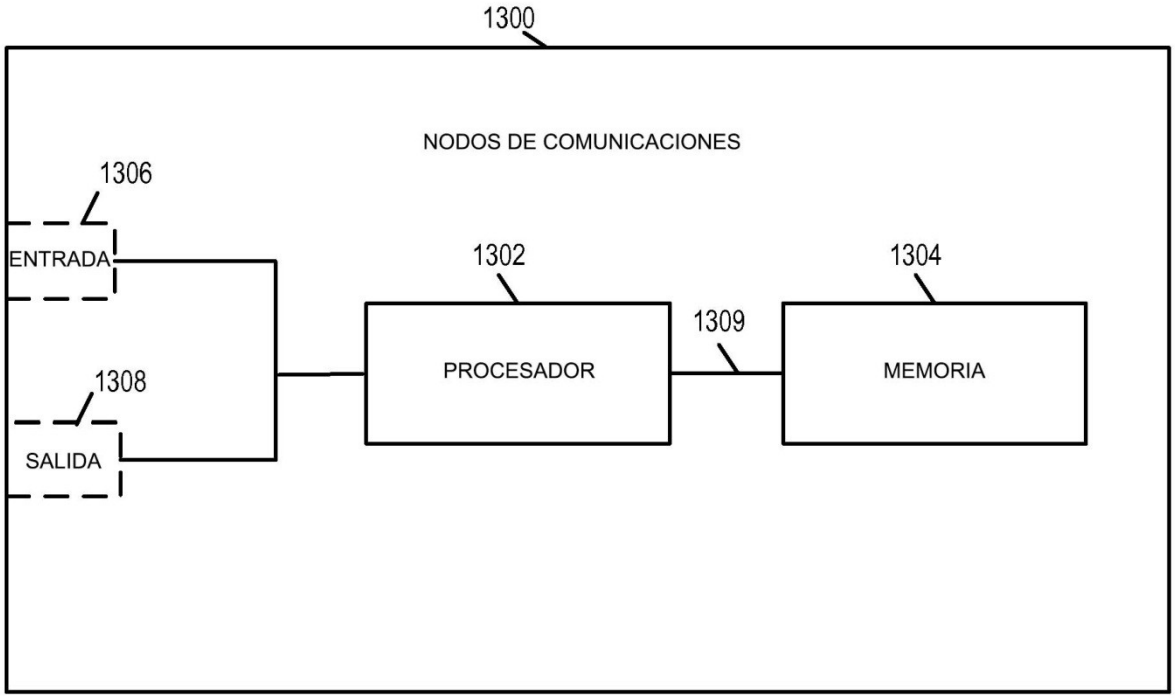
1300
NODOS DE COMUNICACIONES
1306
ENTRADA
1308
SALIDA
1302
PROCESADOR
1309
1304
MEMORIA

FIGURA 13

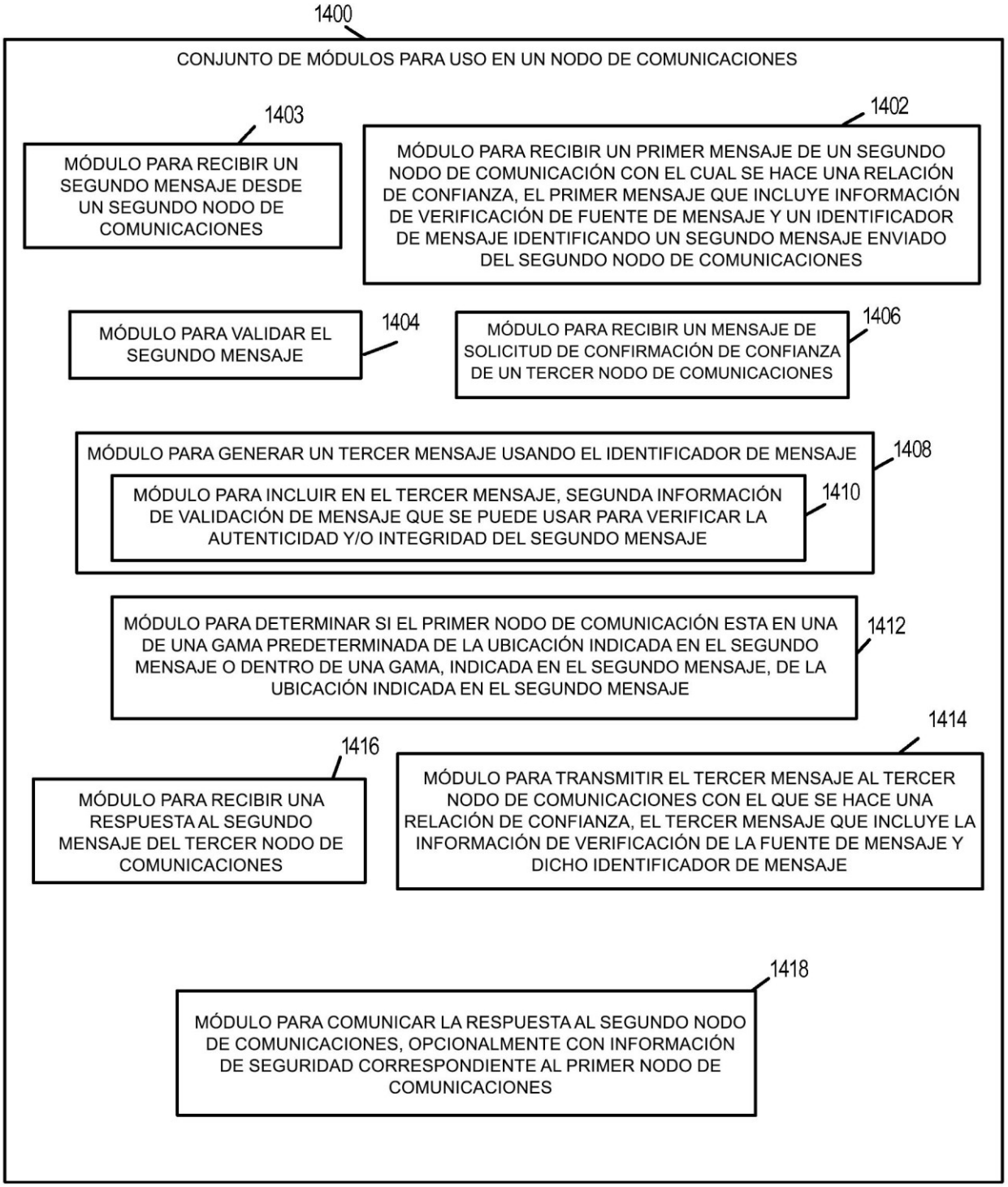
1400
CONJUNTO DE MÓDULOS PARA USO EN UN NODO DE COMUNICACIONES
1403
MÓDULO PARA RECIBIR UN SEGUNDO MENSAJE DESDE UN SEGUNDO NODO DE COMUNICACIONES
1402
MÓDULO PARA RECIBIR UN PRIMER MENSAJE DE UN SEGUNDO NODO DE COMUNICACIÓN CON EL CUAL SE HACE UNA RELACIÓN DE CONFIANZA, EL PRIMER MENSAJE QUE INCLUYE INFORMACIÓN DE VERIFICACIÓN DE FUENTE DE MENSAJE Y UN IDENTIFICADOR DE MENSAJE IDENTIFICANDO UN SEGUNDO MENSAJE ENVIADO DEL SEGUNDO NODO DE COMUNICACIONES
MÓDULO PARA VALIDAR EL SEGUNDO MENSAJE
1404
MÓDULO PARA RECIBIR UN MENSAJE DE SOLICITUD DE CONFIRMACIÓN DE CONFIANZA DE UN TERCER NODO DE COMUNICACIONES
1406
MÓDULO PARA GENERAR UN TERCER MENSAJE USANDO EL IDENTIFICADOR DE MENSAJE
1408
MÓDULO PARA INCLUIR EN EL TERCER MENSAJE, SEGUNDA INFORMACIÓN DE VALIDACIÓN DE MENSAJE QUE SE PUEDE USAR PARA VERIFICAR LA AUTENTICIDAD Y/O INTEGRIDAD DEL SEGUNDO MENSAJE
1410
MÓDULO PARA DETERMINAR SI EL PRIMER NODO DE COMUNICACIÓN ESTA EN UNA DE UNA GAMA PREDETERMINADA DE LA UBICACIÓN INDICADA EN EL SEGUNDO MENSAJE O DENTRO DE UNA GAMA, INDICADA EN EL SEGUNDO MENSAJE, DE LA UBICACIÓN INDICADA EN EL SEGUNDO MENSAJE
1412
1414
1416
MÓDULO PARA RECIBIR UNA RESPUESTA AL SEGUNDO MENSAJE DEL TERCER NODO DE COMUNICACIONES
MÓDULO PARA TRANSMITIR EL TERCER MENSAJE AL TERCER NODO DE COMUNICACIONES CON EL QUE SE HACE UNA RELACIÓN DE CONFIANZA, EL TERCER MENSAJE QUE INCLUYE LA INFORMACIÓN DE VERIFICACIÓN DE LA FUENTE DE MENSAJE Y DICHO IDENTIFICADOR DE MENSAJE
1418
MÓDULO PARA COMUNICAR LA RESPUESTA AL SEGUNDO NODO DE COMUNICACIONES, OPCIONALMENTE CON INFORMACIÓN DE SEGURIDAD CORRESPONDIENTE AL PRIMER NODO DE COMUNICACIONES

FIGURA 14