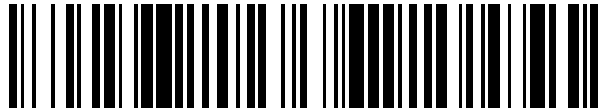


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 675 758**

51 Int. Cl.:

H04W 40/24	(2009.01)
H04L 12/771	(2013.01)
H04L 12/721	(2013.01)
H04L 12/717	(2013.01)
H04L 29/08	(2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 86 Fecha de presentación y número de la solicitud internacional: **11.02.2013 PCT/IB2013/051114**
- 87 Fecha y número de publicación internacional: **22.08.2013 WO13121339**
- 96 Fecha de presentación y número de la solicitud europea: **11.02.2013 E 13713980 (4)**
- 97 Fecha y número de publicación de la concesión europea: **11.04.2018 EP 2815610**

54 Título: **Gestión eficiente de una tabla proxy en redes de comunicación**

30 Prioridad:

16.02.2012 US 201261599599 P
15.10.2012 US 201261713749 P

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
12.07.2018

73 Titular/es:

PHILIPS LIGHTING HOLDING B.V. (100.0%)
High Tech Campus 5
5656 AE Eindhoven, NL

72 Inventor/es:

HOLTMAN, KOEN JOHANNA GUILLAUME y
ERDMANN, BOZENA

74 Agente/Representante:

ISERN JARA, Jorge

ES 2 675 758 T3

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

DESCRIPCIÓN

Gestión eficiente de una tabla proxy en redes de comunicación

5 Campo de la invención

La invención se relaciona con el campo de las redes de comunicación donde los dispositivos proxy (por ejemplo, nodos proxy) funcionan como dispositivos de relevo (por ejemplo, nodos de relevo) para reenviar mensajes a partir de dispositivo restringido en recursos (por ejemplo, nodos restringidos en recursos), como - pero no se limitan a: dispositivos ZigBee Energía Verde (ZGPDs), a sus receptores o dispositivos de destino (por ejemplo, nodos de destino).

Antecedentes de la invención

15 En una red inalámbrica, se pueden usar dispositivo restringido en recursos, que incluyen dispositivos de restricción de energía tales como dispositivos de recolección de energía. Dichos dispositivos están muy restringidos en la cantidad de energía disponible, lo cual limita su funcionalidad ofrecida e influye en el funcionamiento, la puesta en marcha y el mantenimiento de la red.

20 Un ejemplo de dicha tecnología es el estándar ZigBee Energía Verde (ZGP) en evolución. Un dispositivo ZGP (ZGPD) es un dispositivo restringido en recursos el cual puede ser alimentado por recolección de energía y el cual puede no tener batería o el cual solo puede tener una pequeña capacidad de almacenamiento y, por lo tanto, puede transmitir y/o recibir solo en oportunidades no programadas. Por ejemplo, un ZGPD puede ser un interruptor sin batería que solo puede transmitir durante un corto tiempo una vez que es accionado por un usuario y no tiene capacidad de recepción. Otro ejemplo de un ZGPD puede ser un interruptor sin batería el cual puede recibir por un corto tiempo una vez que es accionado por un usuario y ha transmitido su señal. Aún otro ejemplo de un ZGPD es un sensor que informa periódicamente, recolectando energía de su entorno, por ejemplo, mediante una celda fotovoltaica, con o sin capacidades de recepción. Si un dispositivo con restricción de energía está fuera del alcance del dispositivo, está configurado para controlar (el dispositivo que se controlará denominado "receptor" o "dispositivo de destino"), un dispositivo intermedio (denominado "proxy") se usa para reenviar información al receptor. Los enlaces inalámbricos entre el proxy y el dispositivo restringido pueden aparecer y desaparecer durante la vida útil de la red, por ejemplo, debido a cambios en las condiciones de propagación o en la ubicación relativa de los dispositivos, y/o debido a que los dispositivos se agregan y eliminan. Por motivos de seguridad y rendimiento del sistema, los proxys solo pueden reenviar para dispositivos restringidos que tienen una entrada de tabla (es decir, entrada de tabla proxy) para, por ejemplo, poder realizar la verificación de seguridad y frescura (autenticación, descifrado). Para la confiabilidad de la comunicación, se puede usar más de un proxy para reenviar información en nombre de un dispositivo restringido.

40 Hay diversas formas de establecer/extender dicha entrada de tabla proxy, automáticamente o previa solicitud, por ejemplo de un usuario o una entidad de mantenimiento y/o configuración. Sin embargo, los métodos para eliminar entradas actualmente disponibles en la especificación ZGP requieren la participación del usuario, mediante el uso de la herramienta de puesta en servicio y/o la interacción manual con el dispositivo restringido y/o el dispositivo controlado (cada uno de los cuales puede instalarse en el techo), lo cual es engorroso para una red a gran escala, tal como las redes de automatización de edificios; y puede requerir acciones de eliminación repetidas si se combina con la creación automática de tabla proxy como está disponible hoy en la especificación ZGP.

Debido a la escala de la red y a la creación automática de la tabla proxy, existe la necesidad de una gestión automática de la tabla proxy. De acuerdo con la especificación ZGP, corresponde al proxy implementado elegir algunas heurísticas de gestión, es decir, elegir heurísticas que elijan una entrada para eliminar de una tabla proxy (completa), por ejemplo, si se debe agregar una nueva entrada; el único método recomendado para eliminar automáticamente las entradas de la tabla proxy apunta a estas entradas con el indicador *EnRango* del campo Opciones definido en "0b0", opcionalmente en combinación con el subcampo *ZGPDfijo* del campo Opciones también configurado en "0b0" (ver ZGP las mejores prácticas para ZBA, documento ZigBee 11-0196r01, sección 5.4.2.1, página 24, línea 22-24); o a las entradas con el indicador *EntradaActiva* del campo Opciones definido en "0b0", que se puede mover a la lista *zgppBloqueadoZGPDID* (documento ZigBee 09-5499r23, sección 3.5.2.2.1, línea 21-23). Otros posibles heurísticos quedan fuera del alcance de la especificación ZGP; pueden referirse a técnicas con base en la experiencia para resolver, aprender y descubrir problemas. Cuando una búsqueda exhaustiva no es práctica, los heurísticos se utilizan para acelerar el proceso de encontrar una solución satisfactoria. Los ejemplos de dichos heurísticos incluyen el uso de una regla de oro, una suposición educada, un juicio intuitivo o sentido común. La heurística más fundamental es la prueba y error. Puede haber cierto nivel de libertad para los implementadores de proxy, porque aunque la mala heurística reduce la eficiencia y la confiabilidad de la red, una mala heurística no puede conducir a una falla de larga duración de la red. En la especificación ZGP actual, no hay penalización de rendimiento para los proxys que tienen tablas proxy muy completas, por lo que una limpieza agresiva para reducir una tabla proxy muy por debajo del tamaño de la memoria disponible en un proxy no tiene ningún efecto beneficioso.

65

La especificación ZGP actual ofrece algunos otros mecanismos para el mantenimiento de tablas proxy, en particular la creación de entrada de la tabla proxy. Por ejemplo, en el proceso de puesta en marcha (probablemente con participación del usuario), el receptor o una herramienta de puesta en marcha envía un anuncio de control (por ejemplo, comando de emparejamiento ZGP con indicador AgregarReceptor definido en "0b1"), informando al(los) proxy(s) sobre la nueva relación de control relación creada, que incluye un identificador del dispositivo restringido y el(los) receptor(es) correspondiente(s). Este anuncio de control puede enviarse por difusión (de rango limitado), con el(los) proxy(s) opcionalmente agregando la tabla solo si están dentro del rango del dispositivo limitado, especialmente si el dispositivo indica una ubicación fija. Durante la operación, la creación de la entrada de la tabla proxy puede lograrse en el proxy al recibir un anuncio de control no solicitado o una comunicación a partir de un dispositivo restringido desconocido y ver otro(s) proxy(s) reenviarlo, o una comunicación a partir de un dispositivo restringido desconocido y hacer una consulta para las relaciones de control (por ejemplo, el comando de búsqueda de emparejamiento de ZGP o el comando de notificación de difusión de ZGP). Las entradas de la tabla proxy pueden eliminarse después de la recepción del GPDPF (Cuadro de dispositivo de Energía Verde) a partir del nodo restringido en el modo de puesta en marcha (especialmente activado en el nodo restringido) o después de la recepción de un comando de eliminación de control (por ejemplo, emparejamiento ZGP con el indicador AgregarReceptor definido en "0b0" o con el indicador EliminarZGPD definido en "0b1"), especialmente activado en la herramienta recepción/puesta en marcha.

Otras operaciones automáticas de tabla proxy mencionadas en la especificación ZGP son la eliminación del indicador de primer reenvío y/o la eliminación de cualquier paquete en cola para reenviar al recibir una comunicación reenviada por otro proxy o un paquete de confirmación del receptor (ver la especificación ZGP, documento ZigBee 09-5499 23, sección A.3.5.2.1, página 124, línea 9 - 39), o eliminación de la indicación de primer reenvío y eliminación de todos los paquetes en cola para su entrega al dispositivo restringido a la recepción de una solicitud para enviar al dispositivo restringido con otro proxy nominado (ver la especificación ZGP, documento ZigBee 09-5499-23, sección A.3.5.2.1, página 122, línea 43 - página 123, línea 5).

Los enfoques mencionados anteriormente permiten determinar el estado de la entrada de la tabla proxy. Sin embargo, debido a la programación imprevisible de las transmisiones del dispositivo restringido (el cual puede depender de la cantidad de energía disponible y/o la interacción del usuario) y la naturaleza poco confiable de las transmisiones inalámbricas, especialmente de dispositivos restringidos que potencialmente no usan acuses de recibo (ACKs) y procedimientos de acceso a canales (tal como un acceso múltiple en el sentido del Portador con prevención de colisiones (CSMA/CA)), enfoques simples para la eliminación automática de tabla proxy con base en el envejecimiento (por ejemplo, eliminar entradas que caducarán más pronto, eliminar entradas que se crearon antes, eliminar las entradas que se usaron menos) no son apropiadas para los dispositivos restringidos.

Aunque se conocen diversas soluciones para que los dispositivos proxy tomen sus decisiones de forma autónoma para crear, mantener, actualizar o eliminar una entrada de tabla proxy, no garantizan un rendimiento óptimo del sistema con una asignación eficiente de proxys (con el nivel de redundancia requerido) por dispositivo restringido.

El documento de los Estado Unidos 2012/002547 A1 divulga el tema del protocolo para una infraestructura de medición avanzada. La solución propuesta lograda mediante un protocolo de gestión se basa principalmente en dos cosas. Primero, se envía un bit (EPSF para Padre de sincronización potencial suficiente) en cada paquete y se guarda en la tabla vecina para cada vecino. Este bit se define en 1 por cada nodo si el número de padre y hermanos en su tabla vecina está por encima de un umbral determinado (el cual se elige para indicar que pueden enviar una solicitud de forma segura a otro nodo). La segunda parte es el mensaje de notificación de salida de tabla (TON). Con base al bit EPSF, un nodo que recibe una nueva solicitud de sincronización a la vez que su tabla vecina está llena, puede decidir eliminar uno de sus hijos si el bit EPSF de este hijo es uno. Pero debe indicarle a este hijo que ya no estará en su tabla vecina. Esto se logra enviando el mensaje TON a este hijo. Al recibir este mensaje, este hijo verá si este padre era su padre de sincronización. Si fue el caso, entonces debe encontrar otro padre de sincronización para garantizar que estará en la tabla vecina de uno de sus padres y recibir transmisiones.

Resumen de la invención

Es un objeto de la invención mejorar el rendimiento del sistema mejorando la asignación de dispositivos proxy por dispositivo restringido.

Este objeto se consigue mediante un aparato de acuerdo con la reivindicación 1, mediante un método de acuerdo con la reivindicación 6, y mediante un producto de programa informático de acuerdo con la reivindicación 7.

Por consiguiente, se proponen soluciones para gestionar los contenidos de tablas proxy, de manera que se optimice el rendimiento, la latencia y la confiabilidad para la(s) red(es) afectada(s), a la vez que se optimiza para un cierto número de dispositivos proxy de acción temprana por dispositivo restringido. La cantidad de dispositivos proxy que tienen una entrada de tabla proxy para un dispositivo restringido en recursos se determina para al menos un dispositivo restringido en recursos con base en la información de la tabla proxy, recibida de los dispositivos proxy y/u otros dispositivos en la red y/o con base al menos en parte en la observación de los mensajes enviados por al menos uno de dichos dispositivos proxy a la vez que actúa como un dispositivo de relevo para dicho dispositivo

restringido en recursos. Conocer el número de dispositivos proxy por dispositivo restringido (por ejemplo, ZGPD) permite que el aparato (el cual se puede proporcionar en un dispositivo proxy, dispositivo receptor, dispositivo de control, como por ejemplo, una herramienta de puesta en marcha o un sistema de gestión de edificios u otro dispositivo) pueda agregar o eliminar o confirmar o crear entradas o entradas de prueba. Como ejemplo, la cantidad de dispositivos proxy que tienen una entrada de tabla proxy para el dispositivo restringido en recursos puede determinarse transmitiendo una solicitud para las entradas de la tabla proxy, por ejemplo, en difusión para direccionar los proxys, o en unidifusión a otro dispositivo que almacena las entradas. Alternativa o adicionalmente, se determina una relación entre el número de veces que un dispositivo proxy que tiene una entrada de tabla proxy para el dispositivo restringido en recursos para un recurso restringido y la cantidad de veces que el dispositivo restringido en recursos ha realizado una transmisión se basa en información recibida a partir de los dispositivos proxy y/o con base en al menos en parte en la observación de los mensajes enviados por al menos uno de dichos dispositivos proxy a la vez que actúa como un dispositivo de relevo para dicho dispositivo restringido en recursos, y creación de al menos un dispositivo proxy adicional que tiene una entrada de tabla proxy para el dispositivo restringido de recursos se inicia si la relación excede un umbral predeterminado o se inicia la eliminación de al menos una entrada de tabla proxy para el dispositivo restringido de recursos si la relación excede otro umbral predeterminado. Además, la gestión de la tabla proxy se puede facilitar obligando a los dispositivos proxy a reportar información sobre dispositivos conocidos restringidos en recursos. En conexión con esto, el(los) dispositivo(s) proxy puede(n) adaptarse para proporcionar registros de monitorización sobre dispositivo restringido en recursos detectados en su rango de recepción. Puede que estos dispositivos restringidos en recursos detectados aún no estén enumerados en su tabla proxy. En la presente invención, se inicia una acción que provoca la creación de más proxys con capacidad de acción temprana con una entrada de tabla proxy para o que se reenvía en nombre del dispositivo restringido de recursos, si ha determinado al menos una de las siguientes condiciones: el número determinado de dispositivos proxy con entradas de tabla proxy para el dispositivo restringido de recursos (es decir, el número de dispositivos proxy con capacidad de inicio) está por debajo de un umbral inferior predeterminado, los proxys existentes no tienen suficientes indicadores de confiabilidad, otros proxys tienen suficientes o mejores indicadores de confiabilidad, o el umbral cambia a la vez que el número de proxys está por debajo del umbral modificado. De este modo, se puede garantizar que cada nodo restringido tenga un número mínimo predeterminado de entradas de tabla en dispositivos proxy.

Asegurándose de que cada dispositivo restringido en recursos tenga diversos dispositivos proxy capaces de acción temprana en su rango de transmisión, se puede optimizar la confiabilidad del sistema. De este modo, el rendimiento del sistema se puede mejorar de manera rápida y eficiente mediante la asignación eficiente de dispositivos proxy (a nivel de redundancia requerido) por dispositivo restringido. El número requerido o deseado de dispositivos proxy por dispositivo restringido se puede lograr mediante técnicas de gestión de tablas proxy para eliminar entradas de tabla proxy (de un dispositivo proxy seleccionado) y/o agregar entradas de tabla proxy (a un dispositivo proxy seleccionado) para optimizar el rendimiento general del sistema y características de confiabilidad.

De acuerdo con un primer aspecto, el número de dispositivos proxy puede determinarse con base en la información de la tabla proxy, recibida a partir de los dispositivos proxy u otros dispositivos en la red y/o con base, al menos en parte, en la observación de mensajes enviados por al menos uno de los dispositivos proxy a la vez que actúa como un dispositivo de relevo para el dispositivo restringido en recursos. Estas medidas facilitan la recopilación de información a partir de la cual se puede derivar el número de dispositivos proxy.

De acuerdo con un segundo aspecto el cual se puede combinar con el primer aspecto anterior, al menos el número determinado de dispositivos proxy que tienen una entrada de tabla proxy para el dispositivo restringido en recursos puede almacenarse en una tabla de recuento proxy, y un dispositivo proxy se puede eliminar a partir de la tabla de recuento proxy en respuesta a un mensaje (por ejemplo, unidifusión, o difusión grupal o mensaje de difusión) recibido del dispositivo proxy u otro dispositivo, por ejemplo el receptor e indicando que el dispositivo proxy ha decidido o se le ordenó abandonar el dispositivo restringido en recursos de su tabla proxy o detener el reenvío en nombre de él. Esta medida garantiza que la información proxy utilizada para la gestión de la tabla proxy se mantenga actualizada.

De acuerdo con un tercer aspecto el cual puede combinarse con el primer o segundo aspecto anterior, una entrada de tabla para el dispositivo restringido en recursos puede eliminarse o marcarse como candidata para ser eliminada de al menos una tabla proxy o reenviarse en nombre del dispositivo restringido en recursos puede detenerse, si se determina al menos una de las siguientes condiciones: existencia de más de un umbral superior predeterminado de dispositivos proxy con una entrada de tabla proxy para o que reenvía en nombre del dispositivo restringido en recursos, dispositivos proxy tienen indicadores de confiabilidad insuficientes, todos los dispositivos proxy en un área determinada o de una capacidad dada tienen tablas de proxy completas, los cambios de umbral, las características restringidas del dispositivo cambian, el cambio en los emparejamientos. Esto garantiza que, para cada dispositivo restringido en recursos, el número de dispositivos proxy con capacidad de acción temprana en su rango de transmisión se mantenga por debajo del umbral superior.

De acuerdo con un cuarto aspecto que puede combinarse con cualquiera de los aspectos primero a tercero anteriores, el aparato renueva una entrada de la tabla proxy al expirar el tiempo de vida de la entrada de la tabla

proxy. De este modo, el aparato puede decidir, con base en la información disponible relacionada con el proxy, si se debe mantener una entrada de tabla proxy incluso después de la expiración de su duración.

5 Se observa que el aparato puede implementarse como un circuito de hardware discreto con componentes de hardware discretos, como un chip integrado, como una disposición de módulos de chip, o como un dispositivo de procesamiento de señal o un chip controlado por una rutina de software o programa almacenado en una memoria, escrito en un medio legible por ordenador o descargado de una red, como Internet.

10 Se debe entender que el aparato de la reivindicación 1, el método de la reivindicación 6 y el producto de programa informático de la reivindicación 7 tienen formas de realización preferidas similares y/o idénticas, en particular, como se define en las reivindicaciones dependientes.

15 Se debe entender que una realización preferida de la invención también puede ser cualquier combinación de las reivindicaciones dependientes con la reivindicación independiente respectiva.

Estos y otros aspectos de la invención serán evidentes y se aclararán con referencia a las realizaciones descritas más adelante.

20 Breve descripción de los dibujos

En los dibujos:

25 La Figura 1 muestra un diagrama de bloques esquemático de una arquitectura de sistema de acuerdo con diversas realizaciones.

Descripción detallada de realizaciones

30 Ahora se describen las realizaciones con base en una red de malla inalámbrica que contiene uno o más dispositivos R restringidos que pueden enviar mensajes poniéndolos en paquetes pero están restringidos en su capacidad para enviar diversos paquetes inalámbricos o largos, y restringidos en su capacidad de escuchar para paquetes durante largos periodos de tiempo o para recibir del todo (por ejemplo, dispositivos alimentados por mecanismos de barrido de energía), uno o más dispositivos T receptores que deberían recibir y actuar sobre mensajes de los dispositivos R restringidos, donde los mensajes pueden codificarse en uno o más paquetes, y la codificación del mensaje en un paquete puede cambiar en una base de salto por salto, y los mensajes se pueden entregar en modo de comunicación de difusión ilimitada, unidifusión, multidifusión, difusión grupal o difusión, uno o más dispositivos P proxy que ayudan a entregar mensajes de los dispositivos restringidos más allá del rango (de radio) de los dispositivos restringidos, y/o ayudar a entregarlos en el formato de mensaje requerido y/o de una forma más confiable mediante la adopción de medidas especiales (por ejemplo, entregar el mensaje hacia adelante a un dispositivo T receptor) cuando reciben un paquete de un dispositivo restringido. Los dispositivos P proxy suelen tener más poder que los dispositivos restringidos para que puedan procesar mensajes adicionales, usar diferentes formatos de mensaje con mensajes más largos o mensajes de acuerdo con un protocolo diferente, volver a intentar acciones o enrutar acciones de descubrimiento en nombre del dispositivo restringido, etcétera. Opcionalmente, se pueden proporcionar uno o más dispositivos RT enrutadores, que no pueden actuar como un dispositivo proxy pero pueden enrutar mensajes enviados por un dispositivo P proxy hacia un dispositivo T receptor. La red se denomina red 'malla' para indicar que hay al menos un dispositivo que es capaz de actuar como relevo de un mensaje.

45 Un único dispositivo puede actuar tanto como un dispositivo T receptor como un dispositivo P proxy, y también como un dispositivo RT enrutador.

50 La Figura 1 muestra una topología de red típica en la cual se puede implementar la presente invención. Las flechas en la Figura 1 muestran paquetes que se envían y reciben para entregar un mensaje a partir de un dispositivo R1 restringido a un dispositivo receptor T1. La flecha de puntos indica que, en este ejemplo, el paquete original enviado por el dispositivo R1 restringido también es recibido por un primer dispositivo P1 proxy, pero el primer dispositivo P1 proxy no actúa sobre él. Hay diversos enfoques mediante los cuales el primer dispositivo P1 proxy y un segundo dispositivo P2 proxy pueden coordinarse para impedir cualquier acción derrochadora de ambos al reenviar el paquete.

60 Como se indica en la Figura 1, los dispositivos P1 y P2 proxy primero y segundo son ambos proxys que están en el rango del dispositivo R1 restringido. Existen diversas razones por las cuales puede ser beneficioso contar con un diseño de sistema en el cual múltiples dispositivos dentro del alcance puedan funcionar o actuar como representantes del dispositivo R1 restringido.

65 Una primera razón es la confiabilidad. Para cada mensaje M_i , el dispositivo R1 restringido solo puede tener energía limitada para enviar paquetes que contengan el mensaje. Por ejemplo, el dispositivo R1 restringido solo puede enviar dos o tres paquetes que codifican el mensaje dentro de un intervalo de tiempo muy corto (por ejemplo, definido por la disponibilidad de la energía cosechada). También es posible que no pueda realizar los mecanismos

de acceso a los canales requeridos y/o espere recibir un marco de acuse de recibo, todo lo cual puede influir negativamente en la confiabilidad de la comunicación. En ese caso, tener más proxys alrededor del dispositivo R1 restringido, el cual todos escucharán y también podrán reenviar paquetes a partir del dispositivo R1 restringido, aumenta la posibilidad de que al menos un proxy reciba el paquete con el mensaje M_i y posteriormente haga seguro que se entrega al receptor T.

Una segunda razón es la movilidad. Si el dispositivo R1 restringido puede moverse, puede moverse fuera del alcance de cualquier proxy individual, el proxy puede moverse/desconectarse o las condiciones de propagación pueden cambiar (por ejemplo, debido a reordenamientos espaciales temporales o permanentes o al movimiento de personas).

Una tercera razón es impedir la configuración de un dispositivo restringido. Puede que no sea posible o deseable configurar el dispositivo R1 restringido para mantener la dirección de red de un único dispositivo proxy. Cualquier paquete de mensaje enviado por el dispositivo R1 restringido será automáticamente un paquete de difusión/multidifusión, dirigido a todos o a múltiples dispositivos con capacidad de proxy (dentro del rango).

Las realizaciones de la presente invención se aplican a sistemas con la capacidad de tener múltiples proxys para cada dispositivo R1 restringido. En dichos sistemas, es beneficioso para la velocidad, la eficiencia y la confiabilidad si los proxys pueden contener una 'información de estado', también denominada como 'información de tabla proxy', sobre dispositivos restringidos. Los ejemplos de dicha 'información de estado' aplicable a un único dispositivo R1 restringido son (i) identificador de las direcciones (o identidades) del dispositivo restringido (o identidades) del dispositivo (o dispositivos) receptor para ciertos mensajes del dispositivo R1 restringido, en el caso que el dispositivo R1 restringido no puede o no incorpore esta información en sus paquetes de mensajes, u otra información que influye en el reenvío en nombre del dispositivo restringido, por ejemplo, estado de entrada, información de enrutamiento, direcciones de alias para el reenvío, (iii) información que hace más segura la comunicación a partir de o hacia el dispositivo R1 restringido, por ejemplo, una clave de cifrado utilizada por el dispositivo R1 restringido, un contador de cuadros de seguridad utilizado recientemente por el dispositivo R1 restringido (los contadores de cuadros pueden proteger contra ataques de repetición y/o se usan como vectores de inicialización para la clave), (iv) información sobre la calidad del enlace entre el dispositivo restringido y el dispositivo proxy, (v) capacidades restringidas del dispositivo, y (vi) un mensaje que debe enviarse al dispositivo R1 restringido tan pronto como encienda su unidad de radio y la configure para recibir dichos mensajes; todos o algunos de ellos pueden ser almacenados. Típicamente, un dispositivo o nodo de captación de energía puede encender su unidad de radio y configurarla para recibir el modo por un corto tiempo después de haber enviado un paquete de mensajes.

En las realizaciones, el término 'tabla proxy' e 'información de tabla proxy' está destinado a cubrir parte o la totalidad de cualquier estructura de datos en un proxy que contiene información sobre, o para, uno o más dispositivos restringidos, y puede contener uno o más de los elementos de información descritos en el párrafo anterior. Una tabla proxy puede contener información para uno o diversos nodos Rx restringidos. Por lo tanto, en un sistema de este tipo, las entradas de la tabla proxy deben crearse, mantenerse y utilizarse para reenviar la comunicación del dispositivo restringido y, potencialmente, también eliminarse.

Por ejemplo, en la Figura 1, sería beneficioso que ambos dispositivos P1 y P2 proxy almacenaran información para el dispositivo R1 restringido en sus tablas proxy. En caso de que el dispositivo R1 restringido pueda moverse, también es beneficioso que un tercer dispositivo P3 proxy almacene esa información. Sin embargo, en la mayoría de las redes de malla previstas, la memoria en los dispositivos o nodos proxy es limitada, por lo que no siempre será posible almacenar información sobre todos los nodos restringidos en todas las tablas proxy de todos los nodos proxy (capaces).

Sin embargo, un nodo proxy que actualmente no tiene ninguna información sobre el nodo R1 restringido en su tabla proxy aún puede elegir comenzar a trabajar como un proxy para ese nodo. Por lo tanto, se pueden identificar dos tipos de proxys que rodean un nodo restringido. El primer tipo es un proxy capaz de acción temprana el cual tiene información sobre dispositivos restringidos en su tabla proxy o reenvía en nombre de dichos dispositivos restringidos, y el segundo tipo es un proxy no apto para acción temprana que no tiene información (aún) sobre cualquier dispositivo restringido en su tabla proxy, o al menos no hay suficiente información, y por lo tanto no puede reenviar en nombre del dispositivo (R1) restringido en el momento en que recibe un mensaje del dispositivo R1 restringido. El proxy de acción tardía primero tendrá que obtener la información necesaria de otra parte de la red. Se observa que, a lo largo de la presente especificación, los términos "proxys activos" y "proxys con capacidad de acción temprana" tienen el mismo significado y están destinados a ser usados de manera intercambiable.

La disposición en una red puede ser tal que cada nodo restringido tenga en su rango de transmisión al menos unos pocos proxys capaces de acción temprana. Sin embargo, en este caso, puede ser deseable un mecanismo para impedir que cada proxy capaz de una acción temprana decida actuar en todos los casos cuando recibe un mensaje de un dispositivo restringido en su rango. De lo contrario, la presencia de múltiples proxys con capacidad de acción temprana puede causar un aumento en la latencia de entrega del mensaje o incluso una disminución en la confiabilidad de la entrega. Uno de esos mecanismos de prevención previstos podría ser informar a otros proxys en el rango de un dispositivo restringido, si un determinado dispositivo proxy actúa sobre un mensaje recibido del

- dispositivo R1 restringido. Si otros dispositivos proxy están informados sobre el acto del determinado dispositivo proxy, pueden abstenerse de actuar ellos mismos. Dicho mecanismo de información se puede implementar de la siguiente manera. Suponiendo que el primer dispositivo P1 proxy ha recibido un mensaje M_i a partir del dispositivo R1 restringido y ahora tiene que decidir si actuar o no. Luego comenzará un contador de tiempo de espera y escuchará el canal de red. Si observa un paquete de otro dispositivo proxy, por ejemplo el segundo dispositivo P2, que contiene una carga útil que indica que el segundo dispositivo P2 proxy actuó en el mismo mensaje M_i del dispositivo R1 restringido, luego el primer dispositivo P1 proxy decide no actuar y detiene el contador. Si el contador se pone a cero sin recibir un paquete del segundo dispositivo P2 proxy para el mensaje M_i del dispositivo R1 restringido, luego el primer dispositivo P1 proxy se activa y actúa para el dispositivo R1 restringido. Debido a las diferencias en los rangos de envío de la red y cierta falta de confiabilidad inherente a la entrega de paquetes inalámbricos, mecanismos como este no inhibirán en todos los casos que múltiples proxys decidan actuar sobre el mismo mensaje a partir del dispositivo R1 restringido. Por lo tanto, se prevé que también haya mecanismos, por ejemplo en los nodos receptores, para filtrar los mensajes duplicados de múltiples proxys que actuaron todos.
- En el próximo estándar ZGP, se utilizan los siguientes mecanismos para las entradas de la tabla proxy activa y válida (ver la especificación ZGP, documento ZigBee 09-5499-23, sección A.3.5.2.1, página 124, línea 9 - 39). En el caso del reenvío de unidifusión, los proxys que tienen una entrada de tabla proxy para un dispositivo restringido particular, calculan el retraso de reenvío con base en criterios como la calidad de la señal recibida del dispositivo restringido, la disponibilidad de rutas de unidifusión a los dispositivos receptores y el hecho de ser el primero en avanzar en el pasado. Al vencimiento de un retraso de reenvío, un dispositivo proxy envía un mensaje ZGP de Parada de Túnel en difusión de 2 saltos, con alias de red de origen y número de secuencia de red de alias, ambos derivados de la información en el GPDF, para informar a otros proxys, y posteriormente enviar los mensajes de notificación de ZGP en unidifusión. Al recibir el mensaje ZGP de Parada de Túnel para el mismo comando ZGPD dentro del retraso de reenvío, un proxy cancela su propia transmisión programada. En caso de comunicación de agrupación para GPDF indicando oportunidad de recepción, los proxys que tienen una entrada de tabla proxy para un dispositivo restringido particular calculan el retraso de reenvío como se describió anteriormente (omitiendo la disponibilidad de rutas de unidifusión a los dispositivos receptores). Al expirar el retraso de reenvío, un proxy envía mensaje(s) de notificación ZGP en multidifusión APS (Subcapa de soporte de aplicaciones) e incluye su dirección corta y el indicador de calidad de la señal recibida del dispositivo R1 restringido. Al recibir el mensaje de notificación ZGP para el mismo comando ZGPD dentro del retraso de reenvío, si la notificación ZGP tiene un indicador de mejor calidad o un indicador de calidad igual y una dirección corta más corta, un dispositivo proxy cancela su propia transmisión programada. En caso de comunicación de agrupación para GPDF que no indique oportunidad de recepción, los dispositivos proxy que tengan una entrada de tabla proxy para un dispositivo restringido particular envían mensaje(s) de notificación ZGP en multidifusión APS, con alias de dirección de fuente de red y alias de número de secuencia de red, ambos derivados de la información en el GPDF, lo cual hace que los paquetes de Notificación ZGP generados independientemente se vean idénticos a la tabla de transacciones de difusión de ZigBee. El mismo mecanismo puede ser utilizado por receptores capaces de reenvío de agrupación con base en tabla de receptor (ver especificación ZGP, 09-5499-23, sección A.3.5.2.5, página 135, línea 28-35).
- Si el dispositivo proxy tiene éxito en transmitir la notificación ZGP, define el indicador de primero-adelante en la entrada de la tabla proxy en "verdadero" y lo borra al recibir un mensaje de respuesta de notificación ZGP a partir de un receptor unidifusión con el indicador de primero-adelante definido en "falso" (ver la especificación ZGP, 09-5499-23, sección A.3.5.2.1, página 124, línea 9 - 39). Los receptores filtran los comandos ZGPD recibidos con base en el identificador ZGPD (SrcID), el valor del contador de cuadros y el modo de comunicación; las capas inferiores realizan un filtrado duplicado adicional (ver la especificación ZigBee Energía Verde, 09-5499-23, sección A.3.6.1.2).
- Las entradas de la tabla proxy deben crearse inicialmente. Se pueden crear, por ejemplo, como parte del proceso de puesta en marcha, involucrando a un usuario y/o una herramienta. Las entradas de la tabla proxy también se pueden crear automáticamente. Un proxy con capacidad de acción no temprana que decide actuar para un nodo restringido puede, al final de la acción, terminar con suficiente información para crear una tabla proxy para el dispositivo restringido en sí mismo. Un nodo no apto para acción temprana que puede escuchar comunicaciones que le permiten realizar una entrada de tabla proxy adicional puede decidir hacerlo, especialmente cuando tiene espacio libre para más entradas disponibles.
- Se supone que un dispositivo proxy (sobre) escucha información sobre un nodo restringido que se envía por la red, que le permite agregar el dispositivo restringido a su tabla proxy y convertirse en un nodo habilitado para la acción temprana para el dispositivo restringido. Especialmente en el caso de que el dispositivo proxy no haya recibido ningún mensaje del dispositivo restringido (aún), es decir, que aún no esté dentro del alcance del dispositivo restringido. El dispositivo proxy podría, por ejemplo, escuchar un mensaje de difusión o de tipo multidifusión, destinado a todos los nodos interesados, informándolos acerca del nodo restringido al nodo. ¿Cómo debe decidir el proxy Px si debe agregar el dispositivo restringido a su tabla proxy, especialmente si esto significa que tiene que eliminar otra entrada de la tabla proxy? Los métodos de asistencia para tal decisión se discuten a continuación.
- En el próximo estándar ZGP, se usan los siguientes mecanismos para configurar información en tablas proxy (ver la especificación ZGP, 09-5499-23, sección A.3.5.2.1, página 122, línea 17 - 41; sección A.3.5.2.2.2, página 127, línea 2- 21; sección A.3.9). Como parte de un procedimiento de puesta en marcha exitoso, un receptor ZGP (ZGPS) o una

herramienta de puesta en marcha ZGPCT (ZGP) envía un mensaje de emparejamiento ZGP con el indicador AgregarReceptor definido en "0b1" (ver la especificación ZGP, 09-5499-23, sección A. 3.3.5.2), por lo general como una difusión de toda la red, que lleva es decir el SrcID (es decir, el identificador del dispositivo restringido ZGPD), las configuraciones de seguridad, si las hay, y el modo de comunicación requerido para el reenvío. Al recibir el emparejamiento ZGP, los dispositivos proxy crean/extienden las entradas de la tabla proxy con la información suministrada. Para receptores capaces de reenviar con base en la tabla de receptor, las entradas de la tabla de receptor se crean al recibir un comando de configuración de emparejamiento ZGP, el cual puede ser enviado por otro ZGPS o ZGPCT u otro dispositivo de gestión (ver la especificación ZigBee Energía Verde, 09-5499-23, sección A.3.3.4.7; sección A.3.5.2.5, página 132, línea 27 - página 134, línea 27).

Las entradas de la tabla proxy antigua/superflua se deben eliminar automáticamente si es posible. Sin embargo, los dispositivos restringidos pueden tener patrones de transmisión muy irregulares, que dependen por ejemplo, en la disponibilidad de energía y/o un activador del usuario. Una forma de administrar las tablas proxy puede ser utilizar estrategias de reemplazo "de uso menos reciente". Bajo la estrategia "de uso menos reciente", si un dispositivo proxy necesita agregar un dispositivo restringido a su tabla proxy, la cual ya está llena, soltará un nodo R_i que se utilizó menos reciente, en donde el nodo R_i se puede seleccionar como el nodo, entre todos los nodos de la tabla, en nombre del cual el dispositivo proxy actuó como un proxy menos reciente (más alejado en el pasado), o puede seleccionarse como el nodo, entre todos los nodos en la tabla, que el dispositivo proxy observa menos recientemente como la emisión de cualquier mensaje.

Sin embargo, existen problemas con dichas estrategias de reemplazo de "uso menos reciente". Suponiendo que las tablas proxy están limitadas a 5 entradas, y una red contiene 15 dispositivos proxy (nodos) y 15 dispositivos restringidos (nodos), con todos estos dentro del rango de recepción de todos los otros. Suponiendo que 10 de los dispositivos restringidos son sensores de temperatura que reportan los datos cada minuto, y 5 son botones de interruptor de luz que se usan en promedio una vez al día. En este caso, existe una gran probabilidad de que todas las mañanas, independientemente de la estrategia de reemplazo exacta "de uso menos reciente", todas las tablas proxy de todos los dispositivos proxy se hayan completado con datos sobre los sensores de temperatura, con todos los interruptores de luz, con todos los interruptores de luz habiendo desaparecido de las tablas. Dependiendo del diseño de otros aspectos de la red, esto hará que el procesamiento del mensaje de cambio de luz sea lento, poco confiable o incluso imposible. Por lo tanto, se necesita una estrategia mejor que la "de uso menos reciente". Los 15 dispositivos proxy tienen $15 * 5 = 75$ entradas de tabla entre ellos, por lo que debería ser posible tener cada uno de los 15 dispositivos restringidos presentes en la tabla proxy de al menos un dispositivo proxy.

Otra forma de administrar las tablas proxy sería utilizar estrategias de reemplazo de "primero en entrar, primero en salir". Evidentemente, tampoco es óptimo, ya que no toma en cuenta ninguna actividad o importancia del dispositivo restringido.

Una solución alternativa puede ser involucrar al usuario en la eliminación de las entradas de la tabla proxy.

El próximo estándar ZGP ofrece los siguientes mecanismos para la eliminación de la entrada de la tabla proxy.

La eliminación de un dispositivo ZGPD de la red, que incluye la eliminación de las entradas de la tabla proxy relacionada, puede activarse por un ZGPD que envía el comando de puesta fuera de servicio de ZGPD y/o por la herramienta receptor/puesta en marcha que envía el comando de emparejamiento ZGP con la etiqueta EliminarZGPD definido en "verdadero" (ver especificación ZGP, 09 5499-23, sección A.3.3.5.2). Se espera que ambas acciones sean activadas por el usuario. La eliminación de un emparejamiento particular (es decir, información de receptor) de la entrada de la tabla proxy puede activarse por una herramienta de receptor/puesta en marcha que envíe el comando emparejamiento ZGP con el indicador AgregarReceptor definido en "falso". Los receptores pueden eliminar los emparejamientos de unidifusión obsoleta enviando una respuesta de notificación ZGP con el indicador NoEmparejamiento definido en "verdadero" (ver la especificación ZGP, 09 5499-23, sección A.3.3.5.1). Se recomienda que los dispositivos proxy que operan en el ámbito de la automatización de edificios eliminen las entradas de la tabla proxy con el indicador EnRango definido en "falso" (ver las mejores prácticas de ZGP para ZBA, documento ZigBee 11-0196r01, sección 5.4.2.1, página 24, línea 22-24). Los proxys también pueden tener entradas con el indicador Entrada-Activa del campo Opciones definido en "0b0", el cual se puede mover a la lista zgppBloqueadoZGPDID (documento ZigBee 09-5499r23, sección 3.5.2.2.1, línea 21-23).

A la vez que las entradas de la tabla para dispositivos restringidos desconocidos pueden descubrirse "justo a tiempo", por ejemplo, al observar primero un comando del dispositivo, y las entradas de la tabla una vez eliminadas/invalidadas pueden volver a descubrirse/activarse de nuevo, se debe tener cuidado que malas heurísticas no conducen a una falla grave del sistema. Imagine un botón de emergencia portátil, destinado a ser operado cuando el portador requiera asistencia. Habiéndolo realizado como un dispositivo restringido en recursos, por ejemplo dispositivo de recolección de energía, puede ser beneficioso, ya que esto garantiza que uno no tiene que lidiar con las baterías vacías/reemplazo de la batería. Se puede crear un emparejamiento con un dispositivo receptor. Pero el botón funcionará muy raramente (por ejemplo, un par de veces al año), posiblemente cada vez en una ubicación diferente (a medida que se mueve su portador); e incluso las operaciones de mantenimiento, si las hay, pueden ser poco frecuentes (por ejemplo, cada dos semanas). Si, al activar el botón, ningún proxy tiene la

entrada de la tabla, en una implementación del sistema prevista, el mensaje no se reenviará y, en su lugar, se podrá enviar una consulta; y el resultado de la consulta solo se puede usar para reenviar el siguiente mensaje. Sin embargo, la alarma crítica actual puede no se puede reenviar.

5 De acuerdo con una primera realización, para al menos un dispositivo restringido, hay al menos una entidad de gestión de tabla en el sistema que determina (ocasionalmente) cuántos proxys tienen entradas de tabla proxy para el dispositivo restringido. La entidad de gestión de la tabla puede ser al menos uno de los dispositivos proxy que reenvía en nombre del dispositivo restringido, al menos uno de los receptores combinados con el dispositivo restringido u otro dispositivo, por ejemplo, un(os) dispositivo(s) de mantenimiento centralizado, como por ejemplo
10 Centro de Confianza ZigBee, Coordinador ZigBee, Administrador de la Red ZigBee, una herramienta de puesta en marcha u otro tipo de controlador/nodo de administrador, dentro o fuera de la red, por ejemplo, el sistema de gestión del edificio. Además de mantener un conteo de proxy activo, se puede almacenar información adicional, que incluye uno o más identificadores de los proxys activos, indicadores de confiabilidad de los proxys activos, capacidades de los proxys activos, niveles de llenado de las tablas de los proxys activos, ubicación de los servidores proxy activos, etcétera.
15

La necesidad de determinar el número de dispositivos proxy activos, y la forma exacta de determinación y acciones resultantes de la determinación pueden diferir por dispositivo restringido, por ejemplo, teniendo en cuenta criterios como tipo de dispositivo restringido, aplicación, movilidad, intervalo de notificación, o características individuales del dispositivo restringido. Las características pueden incluir, por ejemplo importancia y ubicación del nodo (por ejemplo, condiciones de propagación locales), o el mecanismo de envío (por ejemplo, unidifusión, agrupación, entrada de tabla proxy de comodín).
20

El número objetivo de dispositivos proxy capaces de acción temprana por dispositivo restringido, o alternativamente un umbral inferior y superior para el número de dispositivos proxy, se puede determinar globalmente, fijar mediante un estándar, o una política de red o proveedor particular. Además, puede depender del tipo de dispositivo, la aplicación, la movilidad, el intervalo de reporte, las características individuales del dispositivo restringido, por ejemplo, importancia y ubicación (por ejemplo, condiciones de propagación locales) o el mecanismo de envío (por ejemplo, unidifusión, agrupación). El número objetivo o los umbrales pueden cambiar a lo largo de la vida útil de la red, por ejemplo activado por el receptor, la entidad de gestión o causado por algún cambio de configuración, por ejemplo cambio de frecuencia de reportes del dispositivo restringido o cambio en los emparejamientos. Además, se pueden definir condiciones adicionales para la selección de los proxys capaces de acción temprana, como se describe a continuación (ver los criterios de comparación que se describen a continuación).
25
30

Aunque la adición de más dispositivos proxy capaces de acción temprana para un nodo restringido puede aumentar la confiabilidad, también podría generar tráfico de red adicional, de modo que el criterio de optimización no debería ser necesariamente maximizar el número de dispositivos proxy con capacidad de acción temprana. Una entidad de gestión de tablas puede mantener el número de dispositivos proxy capaces de acción temprana por dispositivo restringido por encima de un límite inferior, pero esto puede combinarse con una entidad de gestión de tablas para mantener el número de dispositivos proxy capaces de acción temprana bajo un cierto límite inferior. Si se definen condiciones adicionales para los proxys con capacidad de acción temprana (ver los criterios de comparación que se describen a continuación), el hecho de que un proxy comience o deje de cumplir esas condiciones también puede llevar a su adición o eliminación de entre los proxys con capacidad de acción temprana. Por ejemplo, si un proxy con capacidad de acción temprana ya no cumple con la condición del indicador de confiabilidad mínima, se puede eliminar de la tabla proxy activo (conteo). En otro ejemplo, si todos los dispositivos proxy en el rango de un dispositivo R2 restringido particular tienen una capacidad particular, por ejemplo capaces de reenviar unidifusión, tienen sus tablas llenas, y se necesita una nueva entrada de tabla proxy de unidifusión para un nodo R2 restringido, una entrada de tabla de agrupación para otro nodo R1 en el mismo rango puede iniciarse en al menos uno de esos proxys, y si se requiere se agrega a una tabla proxy de uno o más proxys con capacidad de transmisión grupal en el rango de R1.
35
40
45
50

La solución propuesta de mantener al menos un recuento de proxy activo en la tabla proxy puede combinarse con un mecanismo que hace que un dispositivo proxy sea eliminado de la tabla proxy activo (conteo) en la entidad de gestión de tabla si este dispositivo proxy tiene estado inactivo, como un dispositivo proxy en general o como un dispositivo proxy para el dispositivo restringido en cuestión específicamente, durante mucho tiempo, o si este dispositivo proxy ha decidido o se le ha ordenado que elimine el dispositivo restringido de su(s) propia(s) tabla(s) proxy. Un dispositivo proxy que suelte un dispositivo de su tabla podría, por ejemplo, enviar un mensaje de difusión anunciando que lo ha hecho, o esta información puede derivarse de su información de tabla proxy. Alternativamente, la necesidad de descartar el dispositivo proxy de la tabla proxy activa para un dispositivo restringido dado se puede derivar del comando que ordena al proxy eliminar su entrada de tabla proxy para este dispositivo restringido.
55
60

Además, la solución de conteo del proxy anterior se puede combinar de manera ventajosa con una eliminación autónoma de una entrada de tabla para un dispositivo particular por un dispositivo proxy, si nunca, rara vez o nunca en un intervalo de tiempo reciente de una longitud dada tiene la oportunidad para actuar como un dispositivo proxy activo. Por lo tanto, permitiría eliminar también dichos dispositivos proxy que nunca serán útiles para el dispositivo restringido.
65

En la primera realización la cual se basa en entidades de gestión de tabla que cuentan los dispositivos proxy con umbral de límite superior, si una determinación indica más de un cierto umbral superior de dispositivos proxy reenviando en nombre de un determinado dispositivo restringido, la entidad de gestión de tabla toma una acción que causa la eliminación de algunas entradas de la tabla proxy.

5 Para identificar un dispositivo proxy que debe mantener una entrada de tabla proxy y/o un dispositivo proxy que debe eliminar la entrada de tabla proxy, la entidad de gestión de tabla puede usar al menos uno de los criterios de comparación como un indicador de confiabilidad, por ejemplo, con base en la intensidad de la señal o la distancia entre el dispositivo proxy y el nodo restringido, o indicadores de confiabilidad que indican con qué frecuencia el
10 dispositivo proxy recibe/pierde comunicación del nodo restringido, el número de entradas en la tabla proxy del dispositivo proxy para el cual el dispositivo proxy es muy activo (por ejemplo, si este número es mayor, del que puede ser más beneficioso para este dispositivo proxy eliminar una entrada), las capacidades de los proxys, por ejemplo en términos de seguridad soportada o modos de comunicación, una tasa comparativa en la cual este dispositivo proxy actúa para el nodo restringido, en comparación con otros dispositivos proxy, y otras características de los dispositivos proxy, por ejemplo la posición relativa de los dispositivos proxy entre sí (por ejemplo, puede ser mejor seleccionar los dispositivos proxy activos los cuales no son vecinos entre sí, para limitar el riesgo de que estén sujetos a la misma perturbación de propagación), la conectividad de los dispositivos proxy a la red, por ejemplo número de vecinos (enrutador) que tiene (puede ser mejor usar proxys bien conectados, ya que la multitud de rutas potenciales debería aumentar la confiabilidad de los mensajes que reenvían), y la confiabilidad general de la
20 comunicación de este dispositivo proxy (por ejemplo como se indica en la calidad del enlace reportado por sus vecinos).

En un ejemplo de implementación de la primera realización, los mensajes ya intercambiados para otro fin se pueden usar para la determinación. Como un ejemplo más detallado de esto, un dispositivo receptor para un dispositivo restringido puede realizar un seguimiento de las identidades de los dispositivos proxy que reenvían mensajes en nombre del dispositivo restringido a este. Esto se puede hacer, por ejemplo, obteniendo las identidades de los dispositivos proxy de reenvío a partir de los mensajes que envían, y almacenándolos en una 'tabla de conteo proxy activa'. Si el número de entradas de la tabla de conteo de proxy activas aumenta más allá del umbral superior, el dispositivo receptor puede seleccionar un dispositivo proxy de la 'tabla de recuento proxy activa', por ejemplo con base en una o más de las condiciones descritas anteriormente, y envía un mensaje a este dispositivo proxy indicándole que elimine su entrada de tabla proxy para el nodo restringido, o que la entrada de la tabla sea un candidato fuerte para eliminación si el dispositivo proxy necesita agregar otro nodo restringido a su tabla.

En otro ejemplo de implementación de la primera realización, para un dispositivo restringido, uno o más de los dispositivos proxy con capacidad de acción temprana pueden mantener un registro a través de una tabla de conteo proxy activa de los dispositivos proxy que observó que actuó de manera temprana para ese dispositivo restringido. Por ejemplo, puede hacer esto al escuchar los mensajes enviados por estos dispositivos proxy. Si recibe un mensaje que indica que otro dispositivo proxy ha actuado de manera temprana, y la identidad de ese dispositivo proxy puede derivarse del mensaje, puede almacenar la identidad del nuevo dispositivo proxy en una tabla de conteo proxy activo. Si el número de entradas de la tabla de conteo activo aumenta más allá de un umbral superior, y/o los otros proxys cumplen mejor las condiciones adicionales para los proxys con capacidad de acción temprana, el dispositivo proxy puede decidir eliminar su propia entrada de tabla proxy para el dispositivo restringido (o convertirlo en un candidato fuerte para eliminar tan pronto como sea necesario agregar una nueva entrada de tabla proxy), o - por ejemplo con base en una o más de las condiciones adicionales para los proxys con capacidad de acción temprana descritos anteriormente, seleccionar otro proxy y pedirle a ese que elimine su entrada de la tabla proxy.

En la siguiente especificación ZGP, la dirección del originador del mensaje, es decir, el dispositivo proxy o receptor con capacidad de acción temprana con capacidad de enrutamiento con base en tabla de receptor, puede determinarse a partir de la Parada de Túnel, la notificación de puesta en marcha ZGP y/o los mensajes del grupo de notificación de Energía Verde ZGP que envía. Si no se utiliza el alias, la dirección del originador del mensaje, el proxy del proxy con acción temprana, puede determinarse con base en el campo de dirección fuente NWK o del campo de dirección Corta ZGPP/TempMaestra, si se incluye. Si se utiliza un alias, la dirección del originador del mensaje, es decir, el proxy que actuó con anticipación, se puede determinar a partir de la dirección fuente MAC, si el campo de Radio del encabezado NWK en el mensaje recibido tiene su valor inicial. El(los) mensaje(s) puede(n) contener además los indicadores de confiabilidad para el proxy de acción temprana, por ejemplo el campo Distancia. Estos mensajes pueden ser recibidos por otros proxys y por los receptores.

La eliminación de la entrada de la tabla proxy puede realizarse enviando en unidifusión al dispositivo proxy seleccionado un comando de Emparejamiento ZGP, con el subcampo AgregarReceptor definido en "0b0" o con el subcampo EliminarZGPD definido en "0b1" (ver la especificación ZigBee Energía Verde, 09-5499-23, sección A.3.3.5.2). La eliminación de la entrada de la tabla de receptor se puede realizar mediante el comando de Configuración de Emparejamiento ZG, con el subcampo de acción del campo Acciones definido en "0b011" o "0b100" (ver la especificación ZigBee Energía Verde, 09 5499-23, sección A.3.3.4.7; sección A.3.5.2.5 página 132, línea 27 - página 134, línea 27).

65

De acuerdo con una segunda realización, se proporciona al menos una entidad de gestión de tabla para realizar un seguimiento de cuántos dispositivos proxy están registrados para un nodo restringido y para comparar este número con un umbral de límite inferior. Si hay muy pocos dispositivos proxy con capacidad de acción temprana, o muy pocos dispositivos proxy con capacidad de acción temprana que cumplan los criterios adicionales para proxys con capacidad de acción temprana, o hay algunos dispositivos proxy no aptos para acción temprana disponibles, que cumplen con los criterios adicionales para los proxys con capacidad de acción temprana, la entidad que gestiona la tabla toma medidas que provocan la creación de dispositivos proxy más activos (dispositivos proxy con capacidad de acción temprana dentro del rango). La entidad de gestión de la tabla de seguimiento de pistas aquí puede no ser la misma que la entidad que realiza acciones con base en un umbral de límite superior. Los procedimientos de seguimiento pueden ser, por ejemplo, como se describe anteriormente o a continuación. La entidad puede ser al menos uno de los dispositivos proxy que reenvía en nombre del dispositivo restringido, al menos uno de los receptores emparejados con el dispositivo restringido u otro dispositivo, por ejemplo un(os) dispositivo(s) de mantenimiento centralizado, como por ejemplo Centro de Confianza ZigBee, Coordinador ZigBee, Gestión de Red ZigBee, una herramienta de puesta en marcha u otro tipo de nodo controlador/administrador, dentro o fuera de la red, por ejemplo el sistema de gestión del edificio.

De acuerdo con una tercera realización, la adición y eliminación de las entradas de la tabla proxy se controla con base en el conocimiento global. Aquí, la entidad que gestiona la tabla de decisión puede ser otro dispositivo, por ejemplo un nodo potente, por ejemplo un nodo de puerta de enlace de red (por ejemplo, un enrutador periférico o 6lowpan LBR), un administrador de red (como, por ejemplo, Centro de Confianza ZigBee, Coordinador ZigBee, Gestión de Red ZigBee) u otro tipo de nodo controlador/administrador, por ejemplo un dispositivo de sistema de gestión de edificios o un dispositivo de puesta en servicio, dentro o fuera de la red (por ejemplo, en Internet). Sus decisiones pueden basarse en estadísticas a largo plazo. En un ejemplo, la entidad de gestión de tabla puede recopilar regularmente contenidos de tabla proxy de todos los dispositivos proxy y/o información de proxy de otros dispositivos, por ejemplo receptores, controladores, puertas de enlace y herramienta(s) de puesta en marcha, y también pueden recopilar, o hacer que se generen, otros datos relacionados con la topología de la red. Ocasionalmente, la entidad revisa sus registros y decide los contenidos de la tabla proxy para optimizar el rendimiento de la red, y luego actualiza las tablas proxy enviando los mensajes respectivos a los dispositivos proxy. Por ejemplo, la entidad de gestión de tablas puede recopilar entradas permanentes y transitorias a partir de tablas proxy para crear un registro histórico a largo plazo en su memoria sobre qué proxys están en la distancia de recepción de cual nodo restringido. En un ejemplo adicional, la entidad de gestión de tabla puede recopilar otra información sobre la operación proxy, que incluye la ubicación del proxy, la membresía de la red del proxy, la información del vecino del proxy, la información de enrutamiento del proxy, la información de confiabilidad del proxy, la carga del proxy, que incluye el tráfico propio de la aplicación y otro tráfico enrutado, las capacidades del proxy, etcétera. Además, la entidad de gestión de tabla puede tener acceso a otros datos, por ejemplo plano con ubicación proxy detallada, ubicación de sala/zona, obstáculos, presencia de interferencias externas, etcétera. La entidad de gestión de tablas puede (re)asignar dispositivos proxy a dispositivos restringidos, tratando de apuntar a un criterio global de que cada nodo restringido debería tener al menos un número predeterminado de dispositivos proxy con capacidad de acción temprana dentro de su rango si es posible, en donde el número de dispositivos proxy es posiblemente dependiente de la(s) característica(s) del dispositivo restringido, como se describió anteriormente, y en donde la capacidad de acción temprana puede necesitar opcionalmente cumplir el criterio/criterios de proxy adicional, como se describió anteriormente.

En la siguiente especificación ZGP, la entidad que gestiona la tabla puede recopilar la información sobre el reenvío de dispositivos en nombre de ZGPD leyendo tablas de proxy de los dispositivos proxy, por ejemplo utilizando el comando Atributos de Lectura ZCL y Tablas de Recepción y Tablas de Traducción de los receptores con capacidad de reenvío con base en la tabla del receptor, utilizando los Atributos de Lectura ZCL comandos de Solicitud de Traducción de Tabla ZGP (ver la especificación ZigBee Energía Verde, 09-5499-23, sección A.3.3.4.5). Las tablas se pueden gestionar enviando los comandos ZGP de Emparejamiento/ZGP de Configuración de Emparejamiento para proxys/receptores, respectivamente. También es posible escribir en la tabla atributos a través del comando Escritura de Comandos ZCL.

Se puede introducir un comando que solicita todos los dispositivos que tienen entradas para un ZGPD particular, para simplificar la búsqueda inicial de la entidad de gestión de tabla. Por ejemplo, puede extenderse el comando de Búsqueda de Emparejamiento ZGP (ver la especificación ZigBee Energía Verde, 09-5499 23, sección A.3.3.4.2), en la especificación ZGP actual solo pretende descubrir los receptores emparejados con un ZGPD particular, para indicar qué dispositivos (proxys y/o receptores) deben responder a esta solicitud. Esto se puede lograr, por ejemplo al agregar un subcampo RespuestaProxy en los subcampos ahora reservados del campo Opciones, lo que indica, si está definido en "0b1", que los dispositivos proxy con una entrada de tabla para este ZGPD deben responder también a esta solicitud. Alternativamente, los dispositivos proxy podrían activarse para responder a la Búsqueda de Emparejamiento ZGP configurando todos los subcampos de solicitud de modo (Solicitud de Receptores de Unidifusión, Solicitud de Receptores de Agrupación Derivados, Solicitud de Receptores de Agrupación Oficial) a "0b0". Esto tiene el beneficio adicional de eliminar las respuestas de los receptores. La información de emparejamiento en los receptores normalmente se espera que sea más estática que las entradas de la tabla proxy. Los receptores con capacidad de reenvío con base en la tabla del receptor también pueden responder a esta solicitud, o se les puede solicitar que informen por separado, por ejemplo por una indicación adicional. Además, las

entradas de la tabla proxy de tipo particular o clase de entrada podrían ser solicitadas, por ejemplo solo entradas de tabla proxy para los dispositivos restringidos fuera del alcance de radio del proxy (es decir, con el indicador EnRango del campo Opción de la entrada de la tabla proxy definido en "0b0"; ver la especificación ZGP, 09-5499-23, sección A.3.4.2.2.1) o solo entradas de tabla proxy inactivas y/o no válidas (es decir, indicación EntradaActiva y/o EntradaVálida del campo Opción de la entrada de la tabla proxy configurada en "0b0"; ver especificación ZGP, 09 5499-23, sección A.3.4.2.2.1), o solo entradas de prueba/creadas por sí mismas; es posible que se necesiten agregar indicadores adicionales para estas solicitudes, por ejemplo utilizando los subcampos ahora reservados del campo Opciones del comando de Búsqueda de Emparejamiento. La respuesta a dicha solicitud podría ser una entrada de tabla proxy completa, o un nuevo comando que lleva información seleccionada, por ejemplo idéntico o similar a uno de los comandos de reportes discutidos en esta invención.

Además, el comando de Búsqueda de Emparejamiento ZGP podría usarse para descubrir todos los dispositivos restringidos que usan un modo de comunicación particular, por ejemplo si el modo de comunicación es indicativo de la necesidad del mantenimiento de la tabla proxy y/o de la aplicación y/o tipo de dispositivo del dispositivo restringido. Esto podría lograrse, por ejemplo, configurando el subcampo de solicitud de modo apropiado (Solicitud de Receptores de Unidifusión, Solicitud de Receptores de Agrupación Derivados, Solicitud de Receptores de Agrupación Oficiales) del campo Opciones del comando de búsqueda de emparejamiento ZGP en "0b1" y configurando el campo de ZGPD SRcId a un valor específico, por ejemplo "0xffffffff". De forma similar, podrían solicitarse otras capacidades ZGPD, si son indicativas de la necesidad del mantenimiento de la tabla proxy y/o de la aplicación y/o del tipo de dispositivo del dispositivo restringido, por ejemplo dispositivos ZGPD que utilizan un nivel de seguridad particular o tipo de llave, dispositivos ZGPD portátiles, dispositivos ZGPD con capacidad de comunicación bidireccional, etcétera; es posible que se necesiten agregar indicadores adicionales para estas solicitudes, por ejemplo utilizando los subcampos ahora reservados del campo Opciones.

En otro ejemplo, puede introducirse un comando dedicado para solicitar todos los dispositivos que tienen entradas para un ZGPD particular y/o un ZGPD de capacidades particulares.

Sigue un ejemplo de una entidad de gestión de tablas que aplica un criterio global. Primero, utiliza medios de inspección de estado de la red, por ejemplo lo(s) comando(s) ZGP anteriores, para crear una toma instantánea completa de todos los nodos actuales en el sistema: dispositivos restringidos, dispositivos proxy y dispositivos receptores. La toma instantánea contiene las direcciones de red para cada dispositivo. También contiene, para cada dispositivo restringido, las identidades de todos los dispositivos proxy que actualmente tienen un dispositivo restringido en su tabla proxy. También puede contener, para cada dispositivo restringido, la naturaleza del dispositivo, por ejemplo, es un nodo de sensor que reporta periódicamente que no requiere una alta confiabilidad para entregar cada mensaje, o un nodo de conmutador de activación ligera operado por humanos que no necesita alta confiabilidad u otras características. La información también puede contener, en sistemas que permiten nodos restringidos móviles (por ejemplo, controles remotos portátiles), información sobre si el dispositivo restringido es estacionario o móvil. Dado que no todos los dispositivos proxy estarán dentro del alcance de cada dispositivo restringido, la entidad de gestión de tabla también recopila información sobre qué dispositivos proxy están dentro del alcance de los dispositivos restringidos, que pueden ser o no los mismos que actualmente tienen un dispositivo restringido en su tabla proxy. Típicamente, tal información no será una indicación binaria en el rango de "sí" o "no" por par de dispositivos restringidos por proxy, sino una estimación de la distancia, la intensidad de la señal y/o la tasa de pérdida de paquetes entre el par. Tal información puede estar basada, por ejemplo, en un plano del piso conocido del edificio con las ubicaciones de todos los dispositivos proxy y dispositivos restringidos. Dicha información también podría recopilarse dinámicamente, por ejemplo, mediante el registro de estadísticas sobre recepción de paquetes e intensidades de la señal. Además, por dispositivo proxy, pueden almacenarse la información sobre las capacidades y el estado del proxy, por ejemplo, los modos de comunicación admitidos, los niveles de seguridad admitidos y/o el número total de entradas de tabla proxy ocupadas/libres. Además, por dispositivo receptor, puede almacenar alguna aplicación, capacidad e información de estado, por ejemplo, el modo de comunicación admitido y requerido, que determina potencialmente el modo de comunicación y/o el número de proxys requeridos para los dispositivos restringidos emparejados a este receptor.

Luego, la entidad de gestión de tabla de la tercera realización usa parte o la totalidad de la información anterior para determinar un número mínimo objetivo de dispositivos proxy T(Rx) para cada dispositivo restringido. Por ejemplo, en un sistema donde hay exactamente dispositivos restringidos NR que son todos conmutadores estacionarios, y donde hay dispositivos proxy NP, cada uno capaz de tener como máximo 5 entradas de tabla proxy, T(Rx) podría computarse como:

$$T(Rx) = \min(N_{\min}, \text{piso}((NP*5)/NR)) \quad (1)$$

Con 'piso' es la función (de la biblioteca estándar C) que redondea un número a un número entero, y Nmin es un mínimo definido como aplicación de ejemplo. Por ejemplo, si NR=11 y NP=5, este cálculo da piso=2, y por lo tanto, si Nmin = 4, T(Rx) = 2 para cada dispositivo restringido.

Después de calcular esta $T(Rx)$, la entidad de gestión de tabla identifica aquellos dispositivos restringidos que tienen actualmente dispositivos proxy de menos de $T(Rx)$ con una entrada de tabla proxy para ellos. Para estos dispositivos restringidos, la entidad de gestión de tabla toma medidas para agregar entradas de tabla proxy.

5 En un enfoque para agregar entradas para un dispositivo restringido, la entidad de gestión la tabla selecciona un dispositivo proxy que aún no tiene el dispositivo restringido en cuestión en su tabla proxy, y luego envía comandos a este dispositivo proxy que causan que el dispositivo restringido en cuestión se agregue a la tabla de este dispositivo proxy. Para seleccionar este nuevo dispositivo proxy, la entidad de gestión de tabla puede buscar la información recopilada de la red hasta que encuentre un dispositivo proxy que se encuentre dentro del alcance del dispositivo restringido (o probablemente dentro del alcance del dispositivo restringido) y tenga espacio libre en su tabla proxy, o
10 tenga al menos otro dispositivo restringido en su tabla proxy para el cual el número de dispositivos proxy que tienen el otro dispositivo restringido en su tabla proxy exceda el número mínimo objetivo $T(Rd)$ anterior para el otro dispositivo restringido. Si el enfoque anterior da como resultado múltiples opciones para seleccionar el nuevo dispositivo proxy o el otro dispositivo restringido, la entidad de gestión de tabla puede tomar en cuenta los criterios de proxy adicionales (como se describió anteriormente) en la selección de proxy, por ejemplo capacidad de proxy y el indicador de confiabilidad, por ejemplo con base en RSSI o distancia.

Si se necesita crear un espacio de tabla proxy para un dispositivo restringido, se puede eliminar otro dispositivo restringido seleccionado (nuevo) de la tabla proxy del dispositivo proxy seleccionado. Por lo tanto, la solución propuesta de acuerdo con la tercera realización también provoca que se eliminen las entradas de la tabla proxy.
20

Además, la entidad puede reemplazar un proxy por otro proxy, el cual (mejor) completa algunos criterios de proxy adicionales.

25 A continuación, se discuten diferentes formas de agregar o crear nuevos proxys activos para un dispositivo restringido en las realizaciones anteriores.

En un primer ejemplo, se envía un mensaje de unidifusión a uno o más dispositivos proxy seleccionados, indicándoles que añadan una entrada de tabla para el dispositivo restringido en cuestión. Esta solución es aplicable
30 en casos donde la entidad de gestión de tablas tiene suficiente memoria para almacenar información sobre la topología de red, u otra información histórica que indique qué dispositivos proxy pueden estar dentro del alcance del dispositivo restringido, o una lista de dispositivos proxy los cuales en el pasado actuaron en nombre de este dispositivo restringido, utilizando una entrada de tabla proxy específica o "comodin", o dispositivos proxy que hicieron una búsqueda de este dispositivo restringido, por ejemplo dentro de un período de tiempo limitado en el pasado. En la especificación ZGP, esto podría lograrse con un mensaje de emparejamiento ZGP de unidifusión o directamente escribiendo en la tabla proxy.
35

En el segundo ejemplo, podría enviarse un mensaje de difusión de conteo limitado, originado a partir de un dispositivo, por ejemplo un proxy o un receptor, que se sabe que está cerca o dentro del alcance del dispositivo restringido, instruyendo a algunos o a todos los dispositivos proxy receptores para que agreguen o activen una entrada de tabla para el dispositivo restringido. Aquí, la entrada creada podría verse como una entrada de "prueba". Sin embargo, se observa que dicha "entrada de prueba" puede usarse independientemente de la entidad de gestión de tabla, es decir, también puede ser creada por los propios proxys. Por ejemplo, el dispositivo proxy puede dar instrucciones a algunos de sus vecinos para que agreguen una entrada de tabla, o les pida que pregunten entre sus vecinos. En otro ejemplo, un dispositivo receptor puede instruir a algunos de sus vecinos, proxys y receptores para agregar una entrada de tabla de "prueba".
40
45

Los dispositivos proxy y los dispositivos capaces de funcionar como proxy, por ejemplo, receptores capaces de envío con base en la tabla del receptor, pueden configurarse para diferenciar entre entradas de "prueba" definidas para encontrar todos o mejores dispositivos proxy y otros tipos de entradas como entradas autoconfiguradas, entradas predefinidas o predeterminadas, y/o entradas gestionadas, creadas después de la selección por una entidad. Los dispositivos proxy pueden derivar la configuración ellos mismos, por ejemplo con base en un procedimiento de creación de tabla (por ejemplo, un comando recibido, un originador de comando, un modo de comunicación de comando), o puede ser parte explícita del mensaje en sí. Por lo tanto, la entrada de la tabla de prueba y/o autoconfigurada se puede descartar rápidamente en un momento posterior, por ejemplo cuando se necesita más espacio, si el dispositivo proxy no ha actuado ni siquiera una vez como un dispositivo proxy con capacidad de acción temprana durante el período de tiempo a partir del que se agregó la entrada hasta el momento posterior, y/o si no ha observado ningún mensaje emitido a partir del dispositivo restringido durante ese período de tiempo.
50
55
60

Las entradas de prueba se pueden definir de manera que aumente la probabilidad de que el nuevo dispositivo proxy actúe inicialmente de manera temprana para el dispositivo restringido, de modo que se conozca su presencia y se pueda estimar su confiabilidad. En la siguiente especificación ZGP, esto se puede lograr definiendo el indicador de primero hacia adelante de las nuevas entradas de proxy en "verdadero" (ver la especificación ZigBee Energía Verde, 09-5499-23, sección A.3.4.2.2.1).
65

En una extensión, las entradas de "prueba" en los dispositivos proxy seleccionados para ser proxys con capacidad de acción temprana pueden ser confirmadas por la entidad de gestión de tabla, y convertidas en entradas gestionadas. En la especificación ZGP, esto se podría lograr con el Emparejamiento ZGP o el Mensaje de Emparejamiento Configurado ZGP y/o escribiendo directamente en la tabla proxy o en la tabla de receptores.

5 Además, las entradas de prueba en algunos dispositivos proxy no seleccionados para ser proxys de acción temprana pueden eliminarse, por ejemplo poniéndose en contacto con esos dispositivos proxy de forma individual (si se conocen), o bien enviando un comando de transmisión que indica que la "prueba" ha finalizado.

10 En el contexto de la especificación ZGP, los mensajes para llevar algunas de las instrucciones anteriores a menudo se pueden incorporar de manera ventajosa en paquetes de mensajes que también llevan otra información o comandos. Por ejemplo, dentro de un mensaje de Parada de Túnel ZGP y/o mensaje de Notificación ZGP. Esto proporciona la ventaja adicional de que el dispositivo proxy activo recién agregado se anunciará inmediatamente a los receptores a través del mensaje de Búsqueda de Emparejamiento ZGP para completar la entrada de la tabla proxy.

15 Además, esto podría llevarse a cabo por la entidad de gestión de tabla enviando un comando de emparejamiento ZGP (con etiqueta AgregarReceptor = "0b1") y/o un comando de Configuración de Emparejamiento ZGP y/o escribiendo directamente en la tabla proxy o receptor. Los comandos permitirán que los dispositivos receptores identifiquen, que el remitente sea otro dispositivo proxy y/o que el mensaje sea un intento de aumentar el número de dispositivos proxy. Puede ser implícito, por ejemplo mediante el modo de entrega utilizado (por ejemplo, comunicación de difusión siempre significa entrada de prueba). También puede estar explícito en el comando. Por ejemplo, se puede definir un indicador de prueba en los subcampos ahora reservados del campo Opciones del comando Emparejamiento ZGP y definirlo en "verdadero", o se puede definir un indicador "entrada temporal/administrada" en los subcampos ahora reservados del campo Opciones del comando Emparejamiento ZGP y definido en "entrada temporal". Si se envía en unidifusión, el mensaje preferiblemente permite responder con la respuesta predeterminada de ZCL, por ejemplo en el caso de que el receptor no admita la función ZGP o si no tiene ninguna de las capacidades proxy requeridas o si la tabla proxy ya está llena. El comando de emparejamiento ZGP con el indicador AgregarReceptor = "0b0" y/o el indicador EliminarZGPD = "0b1" y el indicador de prueba = "0b1" o el

20

25

30

35

40

45

50

55

60

65

indicador "de entrada temporal/gestionado" = "temporal" se pueden usar para eliminar entradas no confirmadas, también usando agrupación o difusión. Se puede definir un comando adicional para este propósito. La entidad de gestión de tablas puede elegir entre sus vecinos, ventajosamente aquellos que aún no conocen el reenvío en nombre de este ZGPD. Además, la entidad de gestión de tabla puede excluir adicionalmente receptores, todos o aquellos conocidos que no tienen capacidad de reenvío con base en la tabla de receptor. De manera ventajosa, los dispositivos proxy ya tendrían una lista de SrcIDs de los que están dentro del alcance pero no se reenviarían activamente. De manera ventajosa, durante o poco después de esta selección de proxy adicional, el ZGPD podría enviar un mensaje para permitir que los dispositivos proxy confirmen la recepción o la distancia o la estimación de confiabilidad, etcétera. El dispositivo proxy seleccionado, si está cerca del ZGPD, puede falsificar la transmisión ZGPD para emularlo.

Las formas de realización primera a tercera anteriores se pueden mejorar proporcionando las siguientes medidas adicionales en los dispositivos proxy para hacer que sea más fácil para otras entidades contarlas y/o recopilar estadísticas relacionadas con el proxy.

45 En una primera mejora, un dispositivo proxy puede enviar periódicamente un mensaje de difusión que contiene identidades de dispositivos restringidos en su tabla proxy, por ejemplo, todos o solo aquellos dispositivos restringidos los cuales cumplen ciertos criterios (por ejemplo, la necesidad de mantenimiento de tabla proxy, aquellos dentro del rango, aquellos a los que el proxy envía activamente). Las entidades de gestión de tabla que reciben dichos mensajes de difusión pueden usarlas para actualizar sus tablas de conteo de proxy activo. El mensaje también puede incluir información adicional que se puede usar para el mantenimiento de la tabla proxy, por ejemplo distancia de proxy, etcétera.

En la especificación ZGP, la tabla proxy de ZGP completa podría enviarse, por ejemplo en un Reporte de Atributos ZGP. Alternativamente, podría definirse un comando dedicado que lleve solo los datos relevantes, por ejemplo similar en formato al comando de Parada de Túnel ZGP. En la siguiente especificación ZGP, si se utiliza el reenvío de unidifusión y/o si el ZGPD admite el funcionamiento bidireccional, se puede alentar a los dispositivos proxy que ya reenvían en nombre de un ZGPD a que sigan reenviando. Esto puede lograrse haciendo que los dispositivos proxy planifiquen el reenvío después de un retraso, el Retraso de Túnel, calculado con base en la información específica, por ejemplo, como se define en la especificación ZGP: indicación de intensidad de señal recibida (RSSI) del GDPF (Cuadro de Dispositivo de Energía Verde) recibido, el hecho de ser el primero en reenviar en el pasado, y - en el caso de unidifusión - disponibilidad de todas las rutas de unidifusión a los receptores emparejados; ampliado con un componente adicional para aumentar la probabilidad de reenvío del proxy, independientemente de la topología de la red o los indicadores de confiabilidad.

En una segunda mejora, los dispositivos proxy se controlan para emitir mensajes con regularidad predecible (es decir, probabilidad de reenvío no nula). Para lograr esto, el sistema puede adaptarse para garantizar que cada

dispositivo proxy con capacidad de acción temprana en el rango de un dispositivo restringido tenga una probabilidad distinta de cero de enviar un mensaje, informando así al receptor y/o a la entidad sobre su estado como un dispositivo proxy con capacidad de acción temprana para el dispositivo restringido, en donde esta probabilidad distinta de cero está significativamente por encima de cero, sin importar cuál sea la topología de red local alrededor del dispositivo restringido o cuáles sean los indicadores de confiabilidad de los otros proxys que reenvían en nombre del mismo dispositivo restringido.

En un ejemplo de esta segunda mejora, un dispositivo proxy que recibe un mensaje del dispositivo restringido y que tiene el dispositivo restringido en su tabla proxy puede realizar una "acción de reporte" en promedio una vez cada N veces, donde N es 10 por ejemplo. El mecanismo que crea el comportamiento "una vez cada N veces" podría ser un conteo regresivo a partir de N, o un mecanismo con base en un número aleatorio que genera una decisión "sí" en promedio cada 1/N veces. N puede derivarse de la cantidad de proxys que se reenvían en nombre del dispositivo restringido o la cantidad real de dispositivos proxy con capacidad de activación temprana disponibles para este dispositivo restringido. Si N es el número real de dispositivos proxy con capacidad de acción temprana disponibles para este dispositivo restringido, o el número objetivo que se realizará, la entidad que está administrando la población proxy podría enviar este N al proxy en una etapa de configuración. En otra realización, el número real de dispositivos proxy con capacidad de activación temprana disponibles para este dispositivo restringido puede derivarse al menos en parte con base en la observación del comportamiento de reenvío de otros dispositivos proxy que se reenvían en nombre del mismo dispositivo restringido.

La acción de reporte anterior puede ser una acción de envío de mensajes que permite que otras entidades conozcan el estado del proxy como un dispositivo proxy para el dispositivo restringido. Una forma de realizar la acción de reporte puede ser hacer que el dispositivo proxy envíe un mensaje de notificación ZGP de difusión/agrupación o un mensaje de notificación ZGP de unidifusión aunque el dispositivo proxy haya determinado que ya no es necesario para enviar el mensaje del dispositivo restringido a sus destinatarios, el mensaje beneficioso incluye la identificación clara del proxy de envío. Se pueden enviar otros mensajes (periódicamente).

En el contexto de la siguiente especificación ZGP, dicho mensaje puede ser, por ejemplo, un mensaje de notificación de unidifusión ZGP (ver la especificación ZGP, documento ZigBee 09 5499-23, sección A.3.3.4.1) a al menos un dispositivo receptor del dispositivo restringido, con la misma carga útil y el contenido del contador de secuencia del dispositivo restringido enviado por el dispositivo proxy de acción temprana (si lo hay), pero con su propia dirección como el remitente de unidifusión. O un mensaje de notificación de unidifusión ZGP u otro mensaje a otra entidad capaz de medir la tabla proxy, por ejemplo, aquella que se especifica en una entrada de tabla comodín.

Además, en el contexto del siguiente estándar ZGP, si el dispositivo restringido tiene un grupo de multidifusión como su receptor, el dispositivo proxy puede enviar un mensaje de unidifusión o multidifusión o de difusión que refleje su contenido de tabla proxy, o una notificación ZGP (ver Especificación ZGP, documento ZigBee 09-5499-23, sección A.3.3.4.1) o Parada de Túnel ZGP (ver la especificación ZGP, documento ZigBee 09-5499-23, sección A.3.4.4.1) enviado sin el alias.

Si la entidad de gestión de la tabla de seguimiento es un dispositivo proxy u otro dispositivo dentro del alcance del dispositivo restringido y/o los remitentes reenvían en su nombre, también puede ser posible la derivación de la información del proxy del mensaje con alias (como se describe anteriormente).

En una tercera mejora, se garantizan probabilidades distintas de cero para actuar como el primer proxy de actuación para todos los dispositivos de proxy con capacidad de acción temprana en rango. En un ejemplo de esta tercera mejora, se asume un contexto de diseño, en el cual todos los dispositivos proxy P1..Pn con capacidad de reacción temprana, al recibir un mensaje del dispositivo restringido, esperan un tiempo de retraso específico del proxy WT1..WTn antes de intentar ser el primero en acceder al medio inalámbrico para actuar como un dispositivo proxy, a la vez que al mismo tiempo monitoriza el medio para ver si otro dispositivo proxy ya actuó primero. Dicho mecanismo existe, por ejemplo, en la siguiente especificación ZGP. En esta mejora, el algoritmo de reenvío se puede adaptar de tal manera que ningún dispositivo proxy individual, o grupo de dispositivos proxy, será siempre el primero en actuar en nombre del dispositivo restringido, sin importar qué topología de red se use o qué indicadores de confiabilidad de dispositivos proxy particulares.

En una primera implementación propuesta de la tercera mejora, el cálculo del tiempo de retraso específico del proxy en cada otro dispositivo proxy podría controlarse de modo que cada dispositivo proxy ocasionalmente tenga la oportunidad de reenvío. Como una medida de construcción propuesta, se podría incorporar un componente aleatorio en el tiempo de retraso específico del proxy, con cada dispositivo proxy utilizando su propio generador de números aleatorios no sincronizado con algún otro generador de números aleatorios, de modo que, como resultado, los diferentes valores del tiempo de retraso específico del proxy se distribuyen de manera uniforme cada vez de alguna manera.

En una segunda implementación propuesta de la tercera mejora, cada dispositivo proxy capaz de acción temprana realiza un seguimiento de qué tan recientemente ha actuado como el primer proxy (de reenvío) para el dispositivo restringido en cuestión. La próxima vez que se detecta un mensaje del dispositivo restringido, incluye en el cálculo

de su tiempo de retraso específico del proxy un componente que depende de esta información. Por ejemplo, si el dispositivo proxy ha actuado como el primer proxy (de reenvío) anteriormente, agregará un componente (grande) a su tiempo de retraso específico del proxy, para dar a otros dispositivos proxy más oportunidades de actuar primero. Si no ha actuado como el primer proxy (de reenvío) durante un tiempo, este ya no agregará un componente (grande), por lo que es más probable que actúe primero por sí mismo nuevamente, o incluso puede restar algún componente de tiempo. También se pueden usar otras estrategias de cálculo para el tiempo de retraso específico del proxy, por ejemplo cuanto más tiempo atrás era que el dispositivo proxy actuaba primero, más corto era el tiempo de retardo específico del proxy.

Si un mecanismo como el anterior, que garantiza oportunidades distintas de cero para que todos los dispositivos proxy con capacidad de acción temprana actúen como el primer proxy activo, esté en su lugar, entonces es posible tomar el siguiente enfoque con base en una cuarta realización para administrar la población de proxys activos para cada dispositivo restringido.

La cuarta realización está dirigida a un enfoque de gestión de la población de proxy sin conteo de proxy directo. Alguna entidad de gestión de tablas, por ejemplo cada dispositivo proxy en sí mismo, rastrea, o aproxima, una relación Relación.Py(Rx) entre las veces que el dispositivo (Py) proxy ha actuado como el primer proxy activo para el dispositivo (Rx) restringido, y las veces que el dispositivo restringido ha hecho una transmisión, todos contados durante un período de tiempo T. Por lo tanto:

$$\text{Relación.Py(Rx)} = \text{RL} / \text{RR} \quad (2)$$

donde RL denota el número de veces que el proxy (Py) ha actuado como el proxy para el dispositivo (Rx) restringido durante el período de tiempo T, y RR indica el número de veces que el dispositivo (Rx) restringido envió un mensaje durante el periodo de tiempo T. Esta relación también puede ser aproximada por el dispositivo proxy escuchando localmente las transmisiones recibidas del dispositivo restringido con relación en el número total de transmisiones realizadas por el dispositivo restringido (es decir, que incluye también las transmisiones perdidas por este proxy), y usando este conteo como el lado derecho de la ecuación. Si esta relación del dispositivo proxy que ha actuado excede un umbral, por decir 50%, la entidad de gestión de tabla toma medidas para crear más proxys con capacidad de acción temprana para el dispositivo restringido. El umbral está preferiblemente relacionado con Mx, que es el número óptimo de proxys para este dispositivo Rx restringido, que a su vez puede estar relacionado con esta aplicación y/o capacidades de dispositivos restringidos, como se describió anteriormente. Por ejemplo, el umbral podría ser [100%/Mx]. Se observa que en general será beneficioso hacer la prueba de umbral solo después de que se haya acumulado una cantidad mínima de datos estadísticos, por decir solo después de que el conteo RL y/o RR en el conteo del lado derecho de la ecuación (2) anterior haya alcanzado un valor mínimo dado, por ejemplo, al menos 3. El enfoque de acuerdo con la segunda realización se puede llamar 'sin conteo directo' porque el valor 1/Relación.Py(Rx) se usa en este enfoque para aproximar el número de dispositivos proxy con capacidad de acción temprana para el dispositivo restringido. Este enfoque puede mejorarse si existe un mecanismo de eualización (tal como la tercera mejora anterior de las realizaciones primera a tercera) que hace que cada dispositivo proxy capaz de acción temprana tenga la misma probabilidad de actuar.

En la cuarta realización, un dispositivo proxy puede seguir su propia relación Relación.Py(Rx). Si la relación excede un umbral (superior), el dispositivo proxy puede enviar un mensaje que cause la creación de otros dispositivos proxy con capacidad de acción temprana en su entorno. Por ejemplo, en el contexto de la siguiente especificación ZGP, podría emitirse un cierto mensaje, como se describió anteriormente en la sección 'Formas de agregar nuevos proxys activos'. Como alternativa, el dispositivo proxy puede enviar información sobre su relación al dispositivo restringido y/o dispositivo receptor con algunos de los mensajes que este ya debe enviar, por ejemplo, cuando actúa como el primer proxy de actuación para un dispositivo restringido, y otros proxys reciben dichos mensajes, puede procesar esta información de relación.

Si un dispositivo proxy no apto para acción temprana nota que la relación de otro dispositivo proxy está por encima de un umbral, a la vez que este mismo también está dentro del alcance del dispositivo restringido, puede tomar medidas para convertirse en un proxy de acción temprana para el dispositivo restringido en sí mismo. La decisión del proxy no apto para acción temprana de tomar una acción de este tipo también podría basarse en factores como el espacio disponible en su propia tabla proxy, sus capacidades o entradas de tabla de disponibilidad que se pueden eliminar sin afectar el rendimiento del sistema, por ejemplo, con relaciones muy bajas o entradas de "prueba". También pueden desempeñar un papel una comparación de los indicadores de intensidad de la señal recibida o los indicadores de distancia entre el dispositivo restringido y otro dispositivo proxy, y el dispositivo restringido y el proxy no apto para la actividad temprana.

En aún otro ejemplo, si la relación excede el umbral, el dispositivo proxy puede informar a otra entidad, que puede activar otras acciones descritas en la sección 'Formas de agregar nuevos proxys activos' de la especificación ZGP.

Como una opción adicional, si la relación cae por debajo de un umbral (inferior), la entidad de gestión de tabla, que puede o no ser el proxy en sí, puede tomar medidas para eliminar la entrada de tabla proxy para el dispositivo restringido del dispositivo proxy, o para que sea un candidato fuerte para la eliminación, a la vez que también se

5 detiene opcionalmente para actuar como un dispositivo proxy con capacidad de acción temprana para este nodo, o agregando un componente de tiempo grande a su tiempo de retraso específico del proxy como se definió anteriormente. Además, pueden tomarse en cuenta para la limpieza de tabla proxy criterios adicionales que incluyen indicadores de confiabilidad, por ejemplo el número de comandos del dispositivo restringido (recientes o consecutivos) perdidos y/o distancia al RSSI/LQI a partir del dispositivo restringido, u otro estado proxy y/o información de capacidad

10 Una implementación a modo de ejemplo asume un umbral de límite inferior fijo, y eliminar o marcar como candidato para eliminar la entrada de la tabla proxy del dispositivo restringido en el dispositivo proxy tan pronto como la relación Relación.Py(Rx) caiga por debajo de este umbral. Por ejemplo, si el umbral es del 25% (es decir, el número óptimo de proxys para este Rx, Mx es $100\%/25\% = 4$ proxys), se asegurará de que, en una situación en la que 5 o más proxys estén en el rango de un dispositivo restringido, tiene una entrada de tabla proxy para este dispositivo restringido, y si se igualan las oportunidades de acción temprana entre los proxys con capacidad de acción temprana en rango, el tamaño de la población de proxys activos tenderá a estabilizarse alrededor de 4 (es decir, $1/0.25$). Una
15 estabilización alrededor de un número bajo de proxys puede ser beneficioso porque mantendrá algunas entradas de la tabla proxy libres para tratar los cambios y los nodos móviles restringidos, y hará que el sistema responda más rápido a los cambios en general. Existe el riesgo en esta solución de que diversos proxys de algún modo puedan determinar simultáneamente que sus relaciones están por debajo del umbral, lo que hace que la población de proxy para el dispositivo restringido se reduzca repentinamente a un tamaño muy pequeño. En la mayoría de las
20 situaciones, este riesgo no ocurrirá, siempre que la prueba de relación no se realice demasiado pronto. En dichas situaciones, la aleatoriedad natural del sistema, y especialmente teniendo en cuenta los criterios adicionales, por ejemplo el indicador de confiabilidad asegurará que sea poco probable que muchos proxys caigan por debajo del umbral casi al mismo tiempo. Una estabilización alrededor de un número mayor de proxys puede ser beneficioso para aumentar la entrega de cada mensaje.

25 Para protegerse de situaciones extremas, puede ser beneficioso agregar la medida adicional de que si un dispositivo proxy descarta el dispositivo restringido de su tabla, envía un mensaje de difusión a ese efecto, con los otros dispositivos proxy configurados para recibir y procesar este mensaje de difusión. Una forma de procesar el mensaje, por ejemplo, es que un dispositivo proxy ajuste sus contadores para calcular su propia relación, de forma tal que
30 aumente temporalmente la relación.

De acuerdo con la cuarta realización, se puede proporcionar un mecanismo de configuración para uno o más umbrales de relación en cada dispositivo proxy, de modo que se puedan configurar con base en el conocimiento sobre el número de dispositivos restringidos y/o el número de dispositivos proxy en el sistema. Esta configuración
35 puede ocurrir, por ejemplo, por un instalador del sistema, o puede ser aplicada en tiempo real por una herramienta o sistema de monitorización (por ejemplo, la entidad de gestión de tabla) que recopila información sobre dichos números, y también puede cambiarse, por ejemplo, debido a cambiar las relaciones de emparejamiento, las condiciones de propagación y/o cambiar la frecuencia de los informes del dispositivo restringido. Sin embargo, también puede ser un parámetro fijo. Lo(s) umbral(es) puede(n) tener diferentes valores por dispositivo restringido, tipo y/o aplicación de dispositivo restringido, y/o por modo de comunicación utilizado. Es posible que la entidad de
40 gestión de proxy o receptor o tabla también necesite realizar un seguimiento de los mensajes sin servicio, es decir, los mensajes para los cuales ninguno de los proxys reenvió. Se pueden contar localmente o se pueden suministrar, por ejemplo por el receptor o la entidad de gestión de tabla.

45 Como una generalización de lo anterior, un dispositivo proxy puede hacer un seguimiento de la relación por la cual da servicio a un dispositivo restringido, y puede modificar un componente de su tiempo de retraso específico de proxy, de modo que es mayor si la relación es inferior a un cierto valor de umbral y menor si la relación está por encima de un cierto valor de umbral. Por ejemplo, un dispositivo proxy puede agregar 50 ms a su tiempo de retraso específico del proxy si la relación es inferior al 20%, o puede agregar 0 ms si la relación es superior al 30% y $(30\% - \text{relación}) * 2$ ms si la relación es inferior al 30%. Esto tiene el efecto de que los dispositivos proxy con relaciones
50 menores tienden a ser menos activos, lo que conduce a una estabilidad más rápida de la población proxy activa.

En al menos algunas de las realizaciones anteriores, las entidades de gestión de tabla se han usado para recuperar y usar información estadística. A continuación, se explican realizaciones adicionales para recopilar y poner a
55 disposición información estadística.

De acuerdo con una quinta realización, se configura un dispositivo proxy que no tiene (por el momento) capacidad de acción temprana para un dispositivo restringido (por ejemplo, construyendo esta función en el tiempo de fabricación, o configurando (dinámicamente) el dispositivo proxy) para controlar las transmisiones a partir del
60 dispositivo restringido y para recopilar datos sobre ellas, por ejemplo, al menos uno de los conteos de mensajes recibidos a partir del dispositivo restringido, intensidad de la señal (última, promedio,...) a partir del dispositivo restringido, último contador de cuadros recibidos en un mensaje del dispositivo restringido, y conteo, identidades, indicadores de confiabilidad, capacidades y/o tasas de reenvío de proxy o proxys que se observaron recientemente que tienen acción temprana para el dispositivo restringido.

65

En una implementación de esta quinta realización, una entidad de gestión de tabla que gestiona la población de proxy para el dispositivo restringido puede recuperar activamente la información de monitorización sobre el dispositivo restringido de dispositivos proxy que no tienen acción temprana para optimizar el número de dispositivos proxy con capacidad de reacción para el dispositivo restringido. En otra implementación de esta quinta realización, el dispositivo con capacidad de acción temprana puede tomar acciones para aumentar la población de los dispositivos proxy con capacidad de acción temprana.

Como ejemplo, se supone que para un nodo de sensor que reporta periódicamente como un dispositivo restringido, la entidad de gestión de tabla intenta imponer una política que solo debería existir un único dispositivo proxy con capacidad de acción temprana en el rango del dispositivo restringido (dicha política tiene el efecto de reducir el tráfico de red, pero a costa de la confiabilidad). Puede suceder (por ejemplo, debido a cambios en el entorno) que este único dispositivo proxy deje el rango del dispositivo restringido. Si la entidad de gestión de tabla detecta que muchos mensajes que espera obtener del dispositivo restringido ya no llegan, puede consultar otros dispositivos proxy alrededor del dispositivo restringido, que han estado monitorizando el dispositivo restringido. Al recopilar información como el último contador de cuadros recibidos, la entidad de gestión de tablas puede distinguir entre la situación de que 'el dispositivo restringido está fuera del alcance del dispositivo proxy' o 'el dispositivo proxy está roto y ha detenido el reenvío' y la situación de que 'el dispositivo restringido está roto y ha dejado de transmitir por completo'. Al recopilar información sobre la intensidad de señal de diversos dispositivos proxy de monitorización y compararla, la entidad de gestión de tabla puede elegir la mejor para convertirse en el nuevo dispositivo proxy capaz de realizar las primeras acciones para el dispositivo restringido.

En el contexto de la especificación ZGP, la entidad de gestión de tabla podría configurar un dispositivo proxy para que no sea capaz de realizar las primeras etapas, pero siga monitorizando, para el dispositivo restringido, al crear una entrada de tabla proxy inactiva y válida en el dispositivo proxy (ver la especificación ZGP, 09-5499-23, sección A.3.4.2.2.1, y A.3.5.2.2.2, página 127, línea 26 - 27) o una entrada *zgppBlokkeZGPDID* (ver la especificación ZGP, 09-5499-23, sección A.3.4.2.6). El dispositivo proxy entonces hará un seguimiento del contador de cuadros del dispositivo restringido en su tabla proxy, la cual puede ser leída por la entidad de gestión de tablas con un comando o informada ocasionalmente. Para que la solución descrita anteriormente sea más útil, la tabla proxy puede ampliarse con campos adicionales. Además, este uso de entradas de tabla proxy inactivas y válidas debería aclararse en la especificación, o alternativamente, se puede agregar otra estructura de datos (más compacta) dedicada a recopilar información de monitorización.

En diversos sistemas, especialmente aquellos con limitaciones de memoria, es beneficioso proporcionar la gestión de tabla proxy para un dispositivo restringido justo después de que el dispositivo restringido haya transmitido un mensaje. Para admitir dichos sistemas, todos los dispositivos proxy pueden seguir monitorizando los registros de los últimos N mensajes ($N \geq 1$) que recibieron de dispositivos restringidos. Un registro de monitorización previsto almacena cierta información estadística sobre uno o más mensajes recibidos de un proveedor restringido. Se prevé que el registro de monitorización de un determinado dispositivo restringido tenga un tamaño de memoria mucho menor que una entrada de tabla proxy completa para el dispositivo restringido, porque una entrada de tabla proxy para el dispositivo restringido también tiene que almacenar la información necesaria para enviar mensajes del dispositivo restringido a su destino. Cada registro de monitorización puede contener al menos la identidad del dispositivo restringido y, opcionalmente, para soportar algunas alternativas, al menos una de la intensidad de la señal en la cual se recibió el mensaje del dispositivo restringido, la identidad y/o la potencia de la señal de cualquier dispositivo proxy que se observó que era de acción temprana, y un contador de cuadros o los L bits menos significativos del contador de cuadros. Esta información se puede usar de diversas maneras. Primero, una entidad de gestión de tabla que quiera agregar más dispositivos proxy para el dispositivo restringido puede consultar algunos o todos los dispositivos proxy para obtener estos registros de monitorización y seleccionar los mejores dispositivos proxy para agregar. Segundo, una entidad de gestión de tabla que quiera agregar más proxys para el dispositivo restringido puede hacerlo enviando un mensaje de difusión o de agrupación, instruyendo a todos los dispositivos proxy que lo reciben para que comprueben si tienen el dispositivo restringido en sus registros y luego realicen alguna acción si el dispositivo restringido está presente, y opcionalmente si también se cumplen otros criterios (por ejemplo, el dispositivo restringido está dentro del alcance del proxy, que puede deducirse comparando el número de secuencia o el contador de cuadros incluidos en el mensaje con el valor correspondiente de los registros de monitorización).

En el contexto de la especificación ZGP, dichas instrucciones podrían tomar la forma de una indicación adicional en el comando de Emparejamiento ZGP.

Una posible acción para que los dispositivos proxy se ejecuten de manera condicional puede ser agregar el dispositivo restringido a su tabla proxy. Hacer que esta acción sea condicional proporciona la ventaja de que se impide la creación de entradas de tabla proxy en dispositivos proxy que están fuera del alcance del dispositivo restringido. Otra posible acción para los dispositivos proxy es tomar medidas que provoquen que algunos o todos ellos se anuncien a sí mismos en la entidad de gestión de tabla, por ejemplo, para enviar un mensaje de unidifusión a la entidad de gestión de tabla.

Una posible acción que podría solicitarse puede ser para los dispositivos proxy que no tienen acción temprana que tienen el dispositivo restringido en su tabla proxy o registros de monitorización para iniciar el descubrimiento para el dispositivo restringido. El mecanismo de descubrimiento permite que un receptor seleccione uno o más dispositivos proxy entre todos los descubrimientos, y que los designe como un(os) nuevo(s) dispositivo(s) proxy(s) con capacidad de acción temprana. Ventajosamente, el uso de descubrimiento en lugar de unidifusión a menudo creará menos tráfico de red, y también requerirá menos extensiones nuevas a la base de código de las implementaciones de ZGP. Además, si se utiliza esta solución, la entidad de gestión de tabla que decide que se necesitan más dispositivos proxy podría ser una entidad diferente de la que selecciona los nuevos dispositivos proxy.

De acuerdo con una sexta realización, las entradas de la tabla proxy pueden ser gestionadas por recreación. En esta sexta realización, las entradas de la tabla proxy tienen una vida útil limitada, y la política de gestión de la vida de la tabla es conocida por la entidad de gestión de tabla. El tiempo de vida útil se puede expresar en unidades de tiempo (por ejemplo, 48 horas), en punto de tiempo absoluto (por ejemplo, válido hasta el 12 de octubre de 2012, a las 18:00 CET) o en el número de mensajes recibidos o reenviados en nombre del dispositivo restringido (por ejemplo, 1000 mensajes o hasta y desmarcar el contador de cuadros 0x87654321). Por lo tanto, en o antes de la expiración de la vida útil de la entrada, la entidad de gestión de tabla puede crear nuevas entradas de tabla en los dispositivos proxy seleccionados. En otra implementación, en o antes de la expiración de la vida útil de la entrada, los proxys activan el procedimiento de renovación, por ejemplo enviando un comando de búsqueda de difusión o agrupación, por ejemplo para contactar a los receptores, y/o enviar un comando de unidifusión, por ejemplo para contactar a los receptores o la entidad central de mantenimiento.

En resumen, se han descrito diversas técnicas para gestionar los contenidos de tablas proxy de forma que optimicen el rendimiento, la latencia y la confiabilidad de las redes de comunicación, al tiempo que se garantiza un cierto número de proxys con capacidad de acción temprana por dispositivo restringido. Una entidad puede mantener un número requerido de proxys por dispositivo restringido en recursos eliminando o agregando entradas de tablas proxy. Además, la entidad puede realizar un seguimiento de los proxys con capacidad de acción temprana con base en estrategias de reenvío, estrategias de informes y/o estrategias de sondeo. De este modo, las entradas de la tabla proxy pueden controlarse para optimizar el rendimiento general del sistema y las características de confiabilidad. La entidad se puede incluir en uno o diversos dispositivos que intervienen en la comunicación de dispositivos restringidos, como los proxys con capacidad de acción temprana, los proxys y/o receptores con capacidad de acción excepcional y que proporcionan una optimización local. La entidad puede incluirse en uno o más dispositivos dedicados, como controladores, dispositivos de mantenimiento, configuración o gestión, y proporcionar una optimización global.

Se observa además que el dispositivo proxy puede ser y, por lo tanto, los métodos reivindicados son aplicables a cualquier dispositivo que realice una función de retransmisión para el dispositivo restringido. Por ejemplo, en la especificación ZGP, puede ser cualquiera de los siguientes tipos de dispositivo: Proxy ZGP, Proxy Mínimo ZGP, Combo ZGP, realizando la función de retransmisión con base en la información en su tabla proxy; y Combo Mínimo ZGP, que realiza la función de retransmisión en función de la información en su tabla de receptor.

Aunque la invención se ha ilustrado y descrito en detalle en los dibujos y en la descripción anterior, dicha ilustración y descripción se deben considerar ilustrativas o de ejemplo y no restrictivas. La invención no está limitada a la realización descrita. Aunque las realizaciones se describen principalmente usando los ejemplos de ZigBee Energía Verde, la invención es aplicable a cualquier red con dispositivo restringido en recursos, incluidas redes ZigBee regulares, redes 6LoWPAN, redes de malla Wi-Fi, etcétera. Una aplicación propuesta de la presente invención puede ser cualquier aplicación de control de edificios o sistemas de gestión de edificios, incluidos sistemas de control de iluminación, sistemas de calefacción, ventilación y aire acondicionado, sistemas de control de persianas, sistemas de seguridad y control de acceso; seguimiento de personas y de activos; y cualquier otra aplicación de control, detección, monitorización y automatización que se beneficie de dispositivos restringidos.

Los expertos en la técnica pueden comprender y realizar otras variaciones de las realizaciones descritas en la práctica de la invención reivindicada, a partir de un estudio de los dibujos, la divulgación y las reivindicaciones adjuntas. En las reivindicaciones, la palabra "que comprende" no excluye otros elementos o etapas, y el artículo indefinido "a" o "un" no excluye una pluralidad. Un único procesador u otra unidad puede cumplir las funciones de diversos elementos enumerados en las reivindicaciones. El mero hecho de que se enumeren ciertas medidas en reivindicaciones dependientes mutuamente diferentes no indica que una combinación de estas medidas no se pueda utilizar con ventaja. La descripción anterior detalla ciertas realizaciones de la invención. Se apreciará, sin embargo, que no importa cuán detallado aparezca en el texto, la invención se puede poner en práctica de diversas maneras y, por lo tanto, no se limita a las realizaciones descritas. Cabe señalar que el uso de una terminología particular cuando se describen ciertas características o aspectos de la invención no debe interpretarse como que implica que la terminología se redefine en este documento para restringirla a incluir características específicas de las características o aspectos de la invención con la cual está asociada esa terminología.

REIVINDICACIONES

- 5 1. Un aparato para gestionar una tabla proxy de un dispositivo (P1, P2, P3) proxy en una red de comunicación donde los dispositivos proxy funcionan como dispositivos de retransmisión para reenviar mensajes a partir de dispositivos (R1, R2) restringidos en recursos a dispositivos (T1) de destino, dicha tabla proxy enumera los dispositivo restringido en recursos por los que puede reenviar un dispositivo proxy, dicho aparato está adaptado para determinar al menos un dispositivo (R1) restringido en recursos al menos el número de dispositivos proxy que tienen una entrada de tabla proxy para reenviar en nombre de dicho dispositivo (R1) restringido en recursos, caracterizado porque dicho aparato está adaptado para iniciar una acción que provoca la creación de más proxys con una entrada de tabla proxy para o reenviar en nombre de dicho dispositivo (R1) restringido en recursos, si ha determinado al menos una de las siguientes condiciones: dicho número determinado está por debajo de un umbral inferior predeterminado, los proxys existentes no tienen suficientes indicadores de confiabilidad, otros proxys tienen suficiente o mejor indicadores de confiabilidad, o el umbral cambia a la vez que el número de proxys está por debajo del umbral modificado.
- 10
- 15 2. Aparato de acuerdo con la reivindicación 1, donde dicho aparato está adaptado para determinar dicho número de dispositivos proxy con base en la información de la tabla proxy, recibidos de dichos dispositivos proxy u otros dispositivos en la red y/o con base al menos en parte en la observación de los mensajes enviados por al menos uno de dichos dispositivos proxy a la vez que actúa como un dispositivo de retransmisión para dicho dispositivo (R1) restringido de recursos.
- 20
3. El aparato de acuerdo con la reivindicación 2, en donde dicho aparato está adaptado para almacenar dicho número determinado en una tabla de conteo proxy y para eliminar un dispositivo proxy de dicha tabla de conteo proxy en respuesta a un mensaje que indica que dicho dispositivo proxy ha eliminado dicho dispositivo (R1) restringido de recursos de su tabla proxy o detener el reenvío en nombre de él.
- 25
4. El aparato de acuerdo con la reivindicación 1, en donde dicho aparato está adaptado para iniciar la eliminación o marcarlo como candidato para la eliminación de una entrada de tabla para o detener el reenvío en nombre de dicho dispositivo (R1) restringido de recursos a partir de al menos una tabla proxy, si ha determinado al menos una de las siguientes condiciones: existencia de más de un umbral superior predeterminado de dispositivos proxy con una entrada de tabla proxy para o reenvío en nombre de dicho dispositivo (R1) restringido en recursos, los dispositivos proxy tienen indicadores de confiabilidad insuficientes, todos los dispositivos proxy en un área determinada o de una capacidad dada tienen tablas de proxy completas, los cambios de umbral, el cambio de las características de dispositivos restringidos, el cambio en los emparejamientos.
- 30
- 35 5. El aparato de acuerdo con la reivindicación 1, en donde dicho aparato está adaptado para renovar una entrada de tabla proxy en o antes de la expiración de una vida útil de dicha entrada de tabla proxy.
6. Un método para gestionar una tabla proxy de un dispositivo (P1, P2, P3) proxy en una red de comunicación donde los dispositivos proxy funcionan como dispositivos de retransmisión para reenviar mensajes de dispositivos (R1, R2) restringidos en recursos a dispositivos (T1) de destino, dicha tabla proxy enumera los dispositivo restringido en recursos por los que puede reenviar un dispositivo proxy, donde dicho método comprende determinar para al menos un dispositivo (R1) restringido en recursos la cantidad de dispositivos proxy que tienen una entrada de tabla proxy para o reenviar en nombre de dicho dispositivo (R1) restringido de recursos con base en información de tabla proxy, recibida de dichos dispositivos proxy y/u otros dispositivos en la red y/o con base, al menos en parte, en la observación de los mensajes enviados por al menos uno de dichos dispositivos proxy a la vez que actúa como un dispositivo de retransmisión para dicho dispositivo (R1) restringido de recursos, el método caracterizado porque además comprende iniciar una acción que causa la creación de más proxys con una entrada de tabla proxy para o reenviar en nombre de dicho dispositivo (R1) restringido en recursos, si se ha determinado al menos una de las siguientes condiciones: dicho número determinado está por debajo de un umbral inferior predeterminado, los proxys existentes no tienen suficientes indicadores de confiabilidad, otros proxys tienen indicadores de confiabilidad suficientes o mejores, o el umbral cambia a la vez que el número de proxys está por debajo del umbral modificado.
- 40
- 45
- 50
- 55 7. Un producto de programa informático que comprende un medio de código para producir las etapas del método reivindicado en la reivindicación 6 cuando se ejecuta en un dispositivo informático.

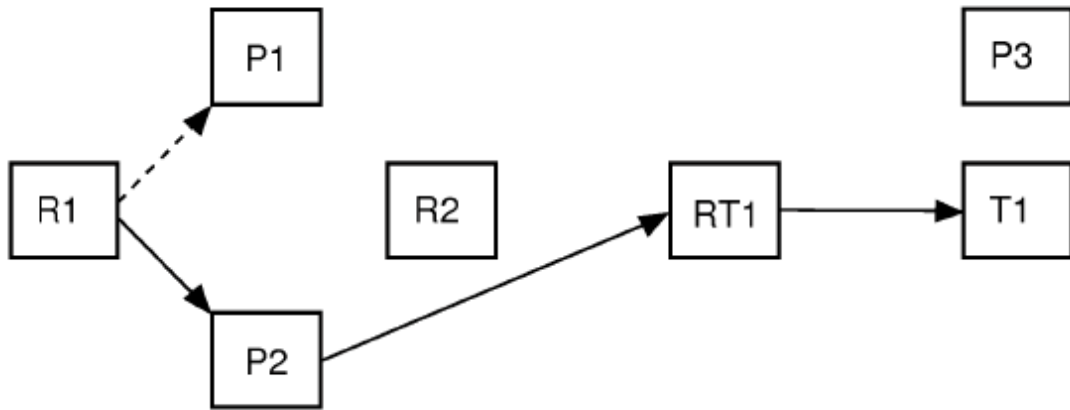


FIG. 1