(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 774 384**

(51) Int. CI.:

H04W 4/48 (2008.01)
H04W 12/00 (2009.01)
H04W 12/08 (2009.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04W 12/06 (2009.01)
H04W 84/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.11.2015 PCT/EP2015/076477**

(87) Fecha y número de publicación internacional: **19.05.2016 WO16075260**

(96) Fecha de presentación y número de la solicitud europea: **12.11.2015 E 15794553 (6)**

(97) Fecha y número de publicación de la concesión europea: **01.01.2020 EP 3219071**

(54) Título: **Arquitectura de seguridad basada en zona para comunicación inalámbrica intravehicular**

(30) Prioridad:

13.11.2014 US 201414540145

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.07.2020

(73) Titular/es:

ALSTOM TRANSPORT TECHNOLOGIES (100.0%)
48, rue Albert Dhalenne
93400 Saint-Ouen, FR

(72) Inventor/es:

LIYANAGE, LAKMAL MADHUSANKA;
KUMAR, PRADEEP y
GURTOV, ANDREI

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Arquitectura de seguridad basada en zona para comunicación inalámbrica intravehicular

ANTECEDENTES

CAMPO TÉCNICO

[0001] El objeto descrito en esta invención se refiere a comunicaciones intravehiculares.

ANÁLISIS DE LA TÉCNICA

[0002] La comunicación intravehicular desempeña un papel importante en diversos sistemas de transporte público y de carga (por ejemplo, cruceros, tranvías, metros, autobuses articulados, trenes y buques de carga) para garantizar la seguridad y la operación estable del vehículo. Inicialmente, los sistemas de comunicación intravehicular se usaron con fines de señalización y control. Sin embargo, los sistemas de comunicación recientes admiten muchas aplicaciones de asistencia a pasajeros, como servicios de información para pasajeros, anuncios públicos, videovigilancia, intercomunicador, calefacción, ventilación y aire acondicionado (HVAC), servicios de banda ancha y sistemas de control basados en datos.

[0003] En la actualidad, la mayoría de los sistemas de comunicación intravehiculares funcionan como sistemas de comunicación cableados. Un sistema de comunicación intravehicular cableado convencional está basado en líneas cableadas que se tienden a lo largo de la carrocería del vehículo y acopladores de interconexión. Sin embargo, los cables físicos son difíciles de instalar, mantener y arreglar. En algunos casos, se requiere que se reemplacen frecuentemente diversas partes de las redes cableadas. Por ejemplo, los acopladores entre vagones en autobuses/trenes/metros/tranvías articulados tienen que ser reemplazados y mantenidos regularmente, ya que el movimiento constante de los vagones hace que los contactos de los acopladores se desgasten.

[0004] Además, los sistemas cableados tienen anchuras de banda fijas, velocidades de datos limitadas y un número limitado de puertos. Los sistemas cableados no se pueden ampliar sin reinstalar los cables a través del vehículo. Por lo tanto, un sistema de comunicación cableado es caro y no es eficiente de actualizar para adaptarse a futuras exigencias. Especialmente, los sistemas cableados no son escalables ni suficientemente prácticos como para proporcionar servicios de usuario personalizados individualmente (por ejemplo, acceso de banda ancha, servicios multimedia) para miles de pasajeros.

[0005] El uso de tecnologías inalámbricas para la comunicación intravehicular es una alternativa económica, ampliable, fiable y fácil de usar para las comunicaciones por cable. Además, es fácil actualizar los sistemas inalámbricos para soportar aplicaciones emergentes relacionadas con pasajeros en el futuro. Por lo tanto, la comunicación inalámbrica casa a la perfección con la comunicación intravehicular.

[0006] El documento US 8.385.550 describe un sistema de comunicación vehicular de tipo conocido.

[0007] Sin embargo, las arquitecturas existentes no pueden abordar adecuadamente los desafíos de seguridad en los sistemas de comunicación intravehicular inalámbrica. Específicamente, la transmisión al aire libre expone el control y el tráfico de usuario a atacantes externos. Estos atacantes pueden no tener las mejores intenciones y pueden tratar de aprovecharse de los datos transmitidos a través de interfaces aéreas. En particular, una alteración o una interrupción de los datos de control puede comprometer la seguridad y el funcionamiento correcto del vehículo. Por lo tanto, es deseable tener un sistema y un procedimiento para proporcionar comunicaciones intravehiculares seguras.

DESCRIPCIÓN BREVE

[0008] Un sistema de comunicación vehicular puede comprender uno o más dispositivos de red configurados para acoplamiento operable con un sistema de vehículo. El uno o más dispositivos de red también están configurados para establecer un segmento de red asegurado que incluye una pluralidad de zonas seguras en el sistema de vehículo. Las zonas seguras están configuradas cada una para enlace de red de una pluralidad respectiva de dispositivos de nodo. El uno o más dispositivos de red están configurados además para establecer uno o más puntos de seguridad únicos, cada uno asociado con una respectiva de la pluralidad de zonas seguras en el sistema de vehículo, para proporcionar seguridad de comunicación para las zonas seguras. Cada zona segura comprende una zona de red a la que los usuarios autorizados predefinidos tienen acceso y los usuarios no autorizados no tienen acceso. El uno o más dispositivos de red están configurados además para establecer un túnel de comunicación inalámbrica segura y un segmento de red pública contiene un canal inalámbrico en el sistema de vehículo configurado para transportar de manera inalámbrica el tráfico de datos entre las zonas seguras. De manera alternativa o complementaria, un sistema de comunicación vehicular puede comprender un primer dispositivo de borde, un segundo dispositivo de borde, un primer transpondedor inalámbrico y un segundo transpondedor inalámbrico. El primer dispositivo de borde está asociado con una primera zona segura de la pluralidad de segundas zonas en una primera ubicación en un sistema

de vehículo y configurado para ser acoplado comunicativamente con una primera pluralidad de dispositivos de nodo de la primera zona segura, para proporcionar un primer punto de seguridad para la primera zona segura. El segundo dispositivo de borde está asociado con una segunda zona segura de la pluralidad de zonas seguras en una segunda ubicación en el sistema de vehículo y configurado para ser acoplado comunicativamente con una segunda pluralidad de dispositivos de nodo de la segunda zona segura, para proporcionar un segundo punto de seguridad para la segunda zona segura. El primer transpondedor inalámbrico está acoplado operativamente al primer dispositivo de borde. El segundo transpondedor inalámbrico está acoplado operativamente al segundo dispositivo de borde. El primer dispositivo de borde y el segundo dispositivo de borde están configurados para establecer un primer túnel de comunicación inalámbrica segura entre la primera zona segura y la segunda zona segura a través del primer transpondedor inalámbrico y el segundo transpondedor inalámbrico.

[0009] Además, un procedimiento para comunicación vehicular puede comprender establecer un segmento de red seguro que incluye una pluralidad de zonas seguras en un sistema de vehículo, teniendo cada zona segura una pluralidad respectiva de dispositivos de nodo; establecer uno o más puntos de seguridad únicos, cada uno asociado con una respectiva de la pluralidad de zonas seguras del sistema de vehículo, para proporcionar seguridad de comunicación para las zonas seguras, donde cada zona segura comprende una zona de red a la que los usuarios autorizados predefinidos tienen acceso y los usuarios no autorizados no tienen acceso. El procedimiento comprende además establecer un túnel de comunicación inalámbrica segura y un segmento de red pública, que contiene un canal inalámbrico, en el sistema de vehículo, configurado para transportar de manera inalámbrica el tráfico de datos entre las zonas seguras.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0010] Se hace referencia a los dibujos adjuntos en los que las configuraciones particulares y los beneficios adicionales de las soluciones descritas se ilustran como se describe con más detalle en la descripción de más adelante, en los que:

la FIG. 1 ilustra una topología de red de una arquitectura de comunicación inalámbrica intravehicular segura;

la FIG. 2 ilustra un diagrama de bloques de sistema de la topología de red de la arquitectura de comunicación inalámbrica intravehicular segura de la FIG. I;

la FIG. 3 ilustra esquemáticamente un procedimiento de establecimiento y autenticación de túnel que usa la topología de red de la FIG. I y la FIG. 2; y

la FIG. 4 ilustra un diagrama de bloques de sistema de una topología de red de una arquitectura de comunicación inalámbrica intravehicular segura que tiene tres zonas seguras.

DESCRIPCIÓN DETALLADA

[0011] La descripción se refiere al menos a sistemas y procedimientos que proporcionan comunicación intravehicular segura e inalámbrica. La comunicación intravehicular incluye la comunicación intravehículo (comunicación en un vehículo individual). La comunicación intravehicular también incluye la comunicación intracomposición, que se refiere a las comunicaciones entre vehículos de una composición. Una composición es un sistema de vehículos que comprende una pluralidad de vehículos unidos entre sí mecánica y/o comunicativa/lógicamente, como para un viaje coordinado a lo largo de una ruta. ("Sistema de vehículo" se refiere colectivamente tanto a vehículos individuales como a composiciones de vehículos). Un sistema de comunicación intravehicular puede comprender uno o más dispositivos de red (por ejemplo, encaminadores y/o conmutadores) que proporcionan el efecto técnico de establecer un segmento de red asegurado que incluye una pluralidad de zonas seguras en un sistema de vehículo, teniendo cada una de las zonas seguras una pluralidad de dispositivos de nodo. El sistema también tiene una o más zonas seguras en el sistema de vehículo, cada zona segura asociada con (por ejemplo, físicamente en o cerca de) un punto de seguridad único respectivo. Cada punto de seguridad único respectivo es para proporcionar seguridad de comunicación para una zona segura correspondiente (por ejemplo, los dispositivos de red pueden configurarse para establecerse y/o funcionar como puntos de seguridad únicos), y un segmento de red pública en el sistema de vehículo configurado para transportar de manera inalámbrica el tráfico de datos entre las zonas seguras.

[0012] Con referencia a los dibujos, los números de referencia similares designan partes correspondientes a lo largo de las varias vistas. Sin embargo, la inclusión de elementos similares en diferentes vistas no significa que una realización dada necesariamente incluya tales elementos o que todas las realizaciones incluyan tales elementos.

[0013] "Software" o "programa informático" como se usa en esta invención incluye, pero no se limita a, una o más instrucciones legibles y/o ejecutables por ordenador que hacen que un ordenador u otro dispositivo electrónico realice funciones, acciones y/o se comporte de una manera deseada. Las instrucciones pueden realizarse de diversas formas, tales como rutinas, algoritmos, módulos o programas que incluyen aplicaciones separadas o código de

bibliotecas vinculadas dinámicamente. El software también puede implementarse de diversas formas, como un programa independiente, una llamada de función, un servlet, una applet, una aplicación, instrucciones almacenadas en una memoria, parte de un sistema operativo u otro tipo de instrucciones ejecutables. Se apreciará por parte de un experto en la materia que la forma del software depende, por ejemplo, de los requisitos de una aplicación deseada, el entorno en el que se ejecuta y/o los deseos de un diseñador/programador o similares.

[0014] "Ordenador" o "dispositivo de procesamiento" o "dispositivo informático" o "procesador" como se usa en esta invención incluye, pero no se limita a cualquier dispositivo programado o programable que pueda almacenar, recuperar y procesar datos. "Medios legibles por ordenador no transitorios" incluyen, pero no se limitan a un CD-ROM, una tarjeta de memoria flash extraíble, una unidad de disco duro, una cinta magnética y un disquete. "Memoria informática", como se usa en esta invención, se refiere a un dispositivo de almacenamiento configurado para almacenar datos digitales o información que puede ser recuperada por un ordenador o elemento de procesamiento. Los términos "controlador" o "sistema de control" o "dispositivo de control" se usan ampliamente en esta invención y pueden ser desde un simple dispositivo de conmutación, a uno o más procesadores que ejecutan instrucciones de software ejecutables por ordenador, hasta circuitos lógicos programables y no programables complejos. Los términos "señal", "datos" e "información" pueden usarse indistintamente en esta invención y pueden ser en forma digital o analógica.
El término "funcionalidad", como se usa en esta invención, puede referirse a las acciones lógicas y las pantallas de visualización de soporte de un sistema implementado en software y/o hardware. El término "electrónicamente", como se usa en esta invención, puede referirse a realizar una tarea usando un dispositivo o red electrónico, o cualquier equivalente del mismo (por ejemplo, un dispositivo o red de fibra óptica, o alguna otra forma de dispositivo o red digital). El término "nodos" o "dispositivos de nodo", como se usa en esta invención, puede referirse a dispositivos (incluyendo, pero no limitados a dispositivos de equipos heredados) en un sistema de vehículo que están conectados operativamente a una infraestructura cableada dentro de una zona segura como, por ejemplo, equipos eléctricos o electrónicos asociados con un vehículo ferroviario, u otros equipos capaces de ser controlados por equipos eléctricos o electrónicos del vehículo ferroviario.

[0015] La descripción proporciona una arquitectura de comunicación intravehicular segura que resuelve problemas relacionados con la seguridad para sistemas de comunicación intravehicular inalámbrica. Pueden proporcionarse servicios de seguridad como, por ejemplo, autenticación, confidencialidad, integridad y disponibilidad para sistemas de comunicación inalámbrica intravehicular. A diferencia de la solución de seguridad de extremo a extremo tradicional, las soluciones reivindicadas pueden proporcionar un mecanismo de seguridad intercalado en la línea ("*bump-in-the-wire*") para implementar una solución de seguridad de sitio a sitio que elimina las implementaciones de protocolo de seguridad en los nodos finales. Por ejemplo, puede proporcionarse un procedimiento de autenticación para autenticar/autorizar los nodos, un procedimiento de establecimiento de túnel para implementar túneles de seguridad de protocolo Internet (IPsec) u otros túneles de comunicación de datos entre las zonas seguras, y un mecanismo de aprendizaje de dirección dinámico para facilitar encaminamiento de paquetes entre sitios.

[0016] El sistema de comunicación intravehicular puede usarse para transportar dos o más tipos de tráfico de datos, incluyendo datos de control y datos de usuario. Pueden definirse dos planos de datos (por ejemplo, anchuras de banda o canales de comunicación) para el sistema de comunicación. El primer plano de datos es para el tráfico de datos de señalización/control, que tiene la prioridad más alta. El primer plano de datos puede transportar los datos operativos y de mantenimiento del sistema de vehículo, por ejemplo. El segundo plano de datos es para el tráfico de datos de usuario, que tiene una prioridad más baja que el tráfico de datos de control. El segundo plano de datos puede transportar banda ancha de usuario, multimedia y otro tráfico de datos no de control, por ejemplo.

[0017] La red intravehicular puede dividirse en dos segmentos. El primer segmento es el segmento de red asegurado que puede tener múltiples zonas seguras. El personal autorizado tiene acceso a las zonas seguras y los intrusos (u otras personas no autorizadas) no tienen acceso a las zonas seguras. Las zonas seguras pueden estar separadas físicamente del público. Por ejemplo, una sala de control o una sala de máquinas en un buque de crucero, un tren o un metro pueden definir una zona segura. El resto de la red pertenece al segundo segmento, que es un segmento de red pública. Las personas públicas tienen acceso al segundo segmento y el tráfico de datos entre zonas seguras se transporta a través del segmento de red pública. Puede proporcionarse seguridad de red en elementos de red lo más cerca posible de las interfaces inalámbricas. Como resultado, puede reducirse el número de nodos que participan en las funciones de seguridad. Cada zona segura está asociada con un dispositivo de borde (que puede incluir, por ejemplo, un encaminador, conmutador u otro dispositivo de red) que está conectado a un transpondedor inalámbrico. Aunque "transpondedor", como se menciona en esta invención, generalmente describe transpondedores convencionales que proporcionan datos predefinidos en respuesta a la interrogación sin interacción humana, resultará evidente tras la revisión de las descripciones de esta invención que cualquier dispositivo para la comunicación inalámbrica de señales de datos puede ser sustituido, y cualquier instancia de "transpondedor" puede ser de manera más general un transceptor. (Los dispositivos de borde se analizan con detalle más adelante en esta invención). Las características de seguridad de datos se implementan en el borde de las zonas seguras. Por lo tanto, un dispositivo de borde también se denomina un punto de seguridad para una zona segura.

[0018] El punto de seguridad es el lugar donde se implementa el mecanismo de seguridad. El mecanismo de

seguridad se usa en puntos de seguridad de tal manera que la implementación de seguridad es completamente transparente para otros elementos de red, anfitriones u otros nodos dentro de las zonas seguras y no requiere modificaciones de protocolo en los nodos.

[0019] Puede proporcionarse seguridad de sitio a sitio en la capa de red en lugar de, por ejemplo, a través de la seguridad de la capa de enlace MAC (Control de acceso a medios) de salto a salto. En la capa de enlace, la distribución y gestión de claves son más complejas que en la capa de red porque cada dispositivo de salto recibe una clave y, cuando las claves cambian, cada dispositivo tiene que actualizarse. Esta puede ser una operación costosa y que requiere mucho tiempo, y puede no ser factible en presencia de varios dispositivos inalámbricos o repetidores. Otros puntos débiles con la seguridad de la capa de enlace incluyen: los paquetes se descifran en cada salto, por lo tanto, existen más puntos de vulnerabilidad; y depende de la tecnología de red de la capa de enlace físico (por ejemplo, IEEE 802.11n).

[0020] Pueden implementarse múltiples zonas seguras según los requisitos del sistema de vehículo. Los dispositivos de red del sistema de comunicación intravehicular pueden estar configurados para transferir de manera segura el tráfico de datos entre las zonas seguras. La comunicación segura de los dispositivos de red se explica en esta invención con respecto al establecimiento de túnel y un mecanismo de aprendizaje de direcciones. Puede establecerse un túnel de comunicación inalámbrica segura entre dos puntos de seguridad (por ejemplo, entre dos de los dispositivos de red) antes de que tenga lugar cualquier comunicación de datos. Cada uno de los dos puntos de seguridad (por ejemplo, dos de los dispositivos de red) está configurado para realizar intercambio de negociación de claves y formar el túnel de seguridad entre ellos. Ejemplos de protocolos de intercambio de claves para establecer el túnel son el Protocolo de identidad de anfitrión (HIP) y el Intercambio de claves de Internet (IKEv2).

[0021] Como parte del procedimiento de establecimiento de túnel, dos (o más) de los dispositivos de red pueden estar configurados para generar un material de clave común para el tráfico de datos usando el intercambio de claves DiffieHellman (D-H). Además, los nodos de punto final (por ejemplo, dispositivos, hardware heredado asociado con sistemas de vehículos, electrónica de comunicación, componentes que se pueden usar en red) se autentican mutuamente basándose en las identidades de anfitrión. Además, los mecanismos iniciales de intercambio de claves (1-1JP e IKEv2) se modifican para intercambiar un certificado digital para permitir la comunicación entre ellos. Inicialmente, el administrador de red proporciona un certificado digital para cada nodo durante el procedimiento de configuración de nodos. Sin embargo, es posible automatizar la distribución de los certificados digitales usando un servidor de autenticación.

[0022] Un certificado digital puede contener la información de configuración de redes privadas virtuales (VPN), como información de priorización de tráfico e identificadores (ID) de VPN. Los certificados digitales están cifrados y, por lo tanto, alguien que realice escuchas clandestinas no puede extraer la información de configuración de las VPN. Cuando el establecimiento de túnel seguro se completa con éxito, los dos extremos pueden transportar de manera segura el tráfico de datos entre dos zonas seguras a través de interfaces o canales inalámbricos seguros.

[0023] De manera alternativa o complementaria, la arquitectura segura puede implementarse como una VPN de capa 2 (L2VPN) o una VPN de capa 3 (L3VPN) basándose en los dispositivos de red desplegados en la red - El tráfico de datos entrante se diferencia basándose en la ID de VPN en las L2VPN y en el puerto IMP (protocolo de datagrama de usuario) en las L3 VPN.

[0024] Los dispositivos de red pueden estar configurados para implementar un mecanismo o procedimiento dinámico de aprendizaje de direcciones, que, por ejemplo, puede usar una tabla de aprendizaje de direcciones para construir tablas de reenvío y encaminar el tráfico de datos entre las zonas seguras. El mecanismo de aprendizaje de dirección dinámico se implementa entre puntos de seguridad. Un punto de seguridad es la entidad (dispositivo de red) responsable de todos los dispositivos de nodo que están situados en la zona segura asociada con el punto de seguridad_ Cada nodo de punto final mantiene una tabla de reenvío para asignar la dirección de un dispositivo de nodo a la dirección del punto de seguridad responsable_ Si un nodo de punto final recibe un paquete de datos con una dirección desconocida, el punto final emite una solicitud de dirección dinámica a todas las zonas seguras y recupera la dirección del punto de seguridad correspondiente. Además, todos los paquetes de aprendizaje de direcciones están cifrados para evitar escuchas clandestinas y ataques de alteración de mensajes en el protocolo de encaminamiento.

[0025] La FIG. 1 ilustra una topología de red de una arquitectura (sistema) de comunicación inalámbrica intravehicular segura 100 en un sistema de vehículo. El hardware de red descrito en esta invención, solo o en combinación con dispositivos conectados a la red, proporciona el efecto técnico de definir zonas seguras 110 conectadas por el túnel seguro 120. Una zona segura puede estar en la cabeza del sistema de vehículo y la otra zona segura puede estar en la cola del sistema de vehículo, por ejemplo_ Las zonas seguras 110 están conectadas (en términos de al menos una porción de sus comunicaciones de datos respectivas) a través de un túnel seguro 120. Aunque, por claridad de ilustración, la topología de red 100 de la FIG. 1 incluye solo dos zonas seguras 110 y representa solo una instancia de VPN única, los principios incorporados en la topología de red 100 pueden extenderse a topologías de red más grandes con muchas zonas seguras y múltiples VPN.

[0026] Las zonas seguras 110 contienen dispositivos de usuario heredados (dispositivos de nodo) 130 que no son necesariamente conscientes de la existencia de la arquitectura de seguridad. Los dispositivos de usuario heredados 130 pueden estar conectados a la infraestructura cableada. Los puntos de seguridad 140 son los dispositivos de borde que están asociados con (por ejemplo, están en o cerca de) las zonas seguras 110 y actúan como una pasarela para cada zona segura. Los puntos de seguridad 140 pueden ser dispositivos de red, como encaminadores y/o conmutadores, por ejemplo. Los nodos en una zona segura utilizan una pasarela (punto de seguridad) para que esa zona segura envíe un mensaje. El mecanismo de seguridad se implementa en los puntos de seguridad 140 y soporta el túnel seguro 120 y protocolos de intercambio de claves asociados. Una pasarela está ubicada lo más cerca posible de la interfaz inalámbrica de una zona segura asociada para evitar ataques por parte de otros enlaces inalámbricos. En las realizaciones que usan HIP, los puntos de seguridad son dispositivos con capacidad HIP. Sin embargo, también pueden usarse otros mecanismos de seguridad de LP e intercambio de claves.

[0027] Las interfaces inalámbricas 150 (por ejemplo, transpondedores inalámbricos) están conectadas a los puntos de seguridad 140 (por ejemplo, dispositivos de red) de las zonas seguras 110. Puede implementarse WiFi como la tecnología inalámbrica y es soportada por las interfaces inalámbricas 150. De manera alternativa o complementaria, puede emplearse otra tecnología radioeléctrica. El segmento de red pública 160 contiene la red de comunicación inalámbrica que incluye el canal inalámbrico 170. Las comunicaciones a través del segmento de red pública 160 están aseguradas por las tecnologías IPsec como se describe en esta invención. La FIG. 2 ilustra un diagrama de bloques de sistema de la topología de red de la arquitectura de comunicación inalámbrica intravehicular segura 100 de la FIG. 1 que muestra el túnel inalámbrico seguro 120. Específicamente, un dispositivo de borde respectivo 140 (por ejemplo, un dispositivo de red configurado para actuar como un punto de seguridad) está asociado con cada una de la primera y la segunda zona segura 110 (por ejemplo, los dispositivos de borde están ubicados en o cerca de las zonas seguras, y/o enlazados comunicativamente con dispositivos de nodo en las mismas). Hay una pluralidad respectiva de dispositivos de nodo 130 en cada zona segura. Un transpondedor inalámbrico respectivo 150 está acoplado operativamente a cada dispositivo de borde. Mediante el control de los transpondedores inalámbricos, los dispositivos de borde 140 están configurados para establecer el túnel de comunicación inalámbrica segura 120.

[0028] La FIG. 3 ilustra esquemáticamente un procedimiento (procedimiento) de establecimiento y autenticación de túnel 300 que usa la topología de red 100 de la FIG. 1 y la FIG. 2. El procedimiento 300 puede estar basado en el procedimiento de intercambio básico (BEX, Base Exchange) HIP. El procedimiento de establecimiento y autenticación de túnel 300 establece túneles HIP entre puntos de seguridad usando un procedimiento de toma de contacto de cuatro vías. Como parte del procedimiento 300, dos puntos generan un material de clave común para tráfico IPsec usando el intercambio de claves Diffie-Hellman (D-H). Además, los puntos finales se autentican mutuamente durante el HIP BEX. Puede intercambiarse un certificado digital para permitir que los puntos finales se comuniquen entre sí. Inicialmente, el administrador de red puede proporcionar un certificado digital para cada dispositivo de nodo durante el procedimiento de configuración de nodos. Sin embargo, puede ser posible automatizar la distribución de los certificados digitales usando un servidor de autenticación. Un certificado digital puede contener la información de configuración de las VPN, como información de priorización de tráfico e ID de VPN. Los certificados digitales pueden ser cifrados usando la clave D-H.

[0029] La FIG. 4 ilustra un diagrama de bloques de sistema de una topología de red de una arquitectura (sistema) de comunicación inalámbrica intravehicular segura 400 que tiene tres zonas seguras 410, 420 y 430. En la Fig. 4, las tres zonas seguras están asociadas cada una con un dispositivo de borde (por ejemplo, un dispositivo de red configurado para actuar como un punto de seguridad para una zona segura) y un transpondedor inalámbrico. En la FIG. 4, se establece un primer túnel de comunicación inalámbrica segura 415 entre la primera zona segura 410 y la segunda zona segura 420, se establece un segundo túnel de comunicación inalámbrica segura 425 entre la segunda zona segura 420 y la tercera zona segura 430, y se establece un tercer túnel de comunicación inalámbrica segura 435 entre la primera zona segura 410 y la tercera zona segura 430. De esta manera, tres zonas seguras diferentes en un sistema de vehículo pueden establecer comunicaciones seguras entre sí a través de los tres túneles seguros.

[0030] Los sistemas, componentes, arquitecturas, entornos y similares mencionados anteriormente se han descrito con respecto a la interacción entre varios componentes y/o elementos. Tales dispositivos y elementos pueden incluir aquellos elementos o subelementos especificados en los mismos, algunos de los elementos o subelementos especificados y/o elementos adicionales. Aún más, uno o más elementos y/o subelementos pueden combinarse en un solo componente para proporcionar funcionalidad agregada. Los elementos también pueden interactuar con uno u otros elementos más no descritos específicamente en esta invención por razones de brevedad, pero conocidos por un experto ordinario en la materia.

[0031] En vista de los dispositivos y elementos ejemplares descritos en esta invención, las metodologías que pueden implementarse de acuerdo con el objeto descrito se apreciarán mejor con referencia a los diagramas de flujo. Aunque, con fines de simplicidad de explicación, las metodologías se muestran y describen como una serie de pasos de bloque, el objeto reivindicado no está limitado por el orden de las etapas de bloque, ya que algunas etapas de bloque pueden producirse en diferentes órdenes y/o simultáneamente con otras etapas de bloque de lo que se representa y describe en esta invención. Además, puede que no se requieran todas las etapas de bloque ilustradas

para implementar los procedimientos descritos en esta invención.

[0032] Puede proporcionarse un sistema de comunicación intravehicular de acuerdo con las descripciones de esta invención. El sistema incluye un segmento de red asegurado que incluye una pluralidad de zonas seguras en un vehículo, teniendo cada una de las zonas seguras una pluralidad de dispositivos de nodo. El sistema también incluye un punto de seguridad único próximo a cada zona segura en el vehículo, que proporciona seguridad de comunicación para una zona segura correspondiente. El sistema incluye además un segmento de red pública en el vehículo configurado para transportar de manera inalámbrica el tráfico de datos entre las zonas seguras. La seguridad de la comunicación, proporcionada por el punto de seguridad único próximo a cada zona segura, puede establecerse al menos a un nivel de la capa de red. La seguridad de comunicación, proporcionada por el punto de seguridad único próximo a cada zona segura, puede establecerse al menos en parte generando un túnel de comunicación inalámbrica segura entre dos zonas cualesquiera de la pluralidad de zonas seguras. El tráfico de datos puede incluir datos de control y señalización de vehículos privados. El tráfico de datos puede incluir datos de usuarios públicos. La pluralidad de dispositivos de nodo puede incluir uno o más dispositivos de equipos heredados conectados operativamente a infraestructura cableada. El punto de seguridad único próximo a cada zona segura puede incluir uno de un encaminador o un conmutador.

[0033] Puede proporcionarse un sistema de comunicación intravehicular de acuerdo con las descripciones de esta invención. El sistema incluye una primera zona segura que tiene una primera pluralidad de dispositivos de nodo en una primera ubicación en un vehículo, y una segunda zona segura que tiene una segunda pluralidad de dispositivos de nodo en una segunda ubicación en el vehículo. El sistema también incluye un primer dispositivo de borde próximo a la primera zona segura y cableado comunicativamente a la primera pluralidad de dispositivos de nodo de la primera zona segura, que proporciona un punto de seguridad para la primera zona segura. El sistema incluye además un segundo dispositivo de borde próximo a la segunda zona segura y cableado comunicativamente a la segunda pluralidad de dispositivos de nodo de la segunda zona segura, que proporciona un punto de seguridad para la segunda zona segura. El sistema también incluye un primer transpondedor inalámbrico cableado operativamente al primer dispositivo de borde y un segundo transpondedor inalámbrico cableado operativamente al segundo dispositivo de borde. El primer dispositivo de borde y el segundo dispositivo de borde están configurados para establecer un primer túnel de comunicación inalámbrica segura entre la primera zona segura y la segunda zona segura a través del primer transpondedor inalámbrico y el segundo transpondedor inalámbrico. Puede establecerse seguridad de comunicación entre la primera zona segura y la segunda zona segura al menos a un nivel de la capa de red. Dos o más de la primera pluralidad de dispositivos de nodo pueden estar configurados para comunicarse entre sí dentro de la primera zona segura. Dos o más de la segunda pluralidad de dispositivos de nodo pueden estar configurados para comunicarse entre sí dentro de la segunda zona segura. Uno o más de la primera pluralidad de dispositivos de nodo pueden estar configurados para comunicarse con uno o más de la segunda pluralidad de dispositivos de nodo a través del primer transpondedor inalámbrico y el segundo transpondedor inalámbrico después del establecimiento del primer túnel de comunicación inalámbrica segura. Cada uno del primer dispositivo de borde y el segundo dispositivo de borde pueden ser uno de un encaminador o un conmutador. La primera pluralidad de dispositivos de nodo y la segunda pluralidad de dispositivos de nodo pueden incluir equipos eléctricos asociados con un vehículo ferroviario. Cada una de la primera zona segura y la segunda zona segura puede incluir una o una sala de máquinas o una sala de control del vehículo_ El sistema puede incluir una tercera zona segura que tiene una tercera pluralidad de dispositivos de nodo en una tercera ubicación en el vehículo, un tercer dispositivo de borde próximo a la tercera zona segura y cableado comunicativamente a la tercera pluralidad de dispositivos de nodo de la tercera zona segura y que proporciona un punto de seguridad para la tercera zona segura, y un tercer transpondedor inalámbrico cableado operativamente al tercer dispositivo de borde_ El primer dispositivo de borde y el tercer dispositivo de borde pueden estar configurados para establecer un segundo túnel de comunicación inalámbrica segura entre la primera zona segura y la tercera zona segura a través del primer transpondedor inalámbrico y el tercer transpondedor inalámbrico. El segundo dispositivo de borde y el tercer dispositivo de borde pueden estar configurados para establecer un tercer túnel de comunicación inalámbrica segura entre la segunda zona segura y la tercera zona segura a través del segundo transpondedor inalámbrico y el tercer transpondedor inalámbrico.

[0034] Se proporciona un procedimiento de comunicación intravehicular de acuerdo con las descripciones de esta invención. El procedimiento incluye establecer dos o más zonas seguras en un vehículo, teniendo cada zona segura uno o más dispositivos de nodo_ El procedimiento también incluye realizar un procedimiento de autenticación para autenticar y autorizar el uno o más dispositivos de nodo, establecer un túnel de comunicación inalámbrica segura entre las dos o más zonas seguras, y establecer un mecanismo de aprendizaje de dirección dinámico para facilitar el encaminamiento de datos entre las dos o más zonas seguras. El túnel de comunicación inalámbrica segura puede establecerse, al menos en parte, generando un certificado digital común y usando un intercambio de claves Diffie-Hellman. El túnel de comunicación inalámbrica segura puede establecerse, al menos en parte, autenticando mutuamente las zonas seguras basándose en identidades de anfitrión. Las dos o más zonas seguras pueden establecerse proporcionando un punto de seguridad único próximo a cada zona segura en el vehículo, que proporciona seguridad de comunicación para una zona segura correspondiente. El mecanismo de aprendizaje de dirección dinámico puede establecerse, al menos en parte, manteniendo una tabla de reenvío para cada zona segura para asignar una dirección de un dispositivo de nodo a una dirección de un punto de seguridad responsable. El procedimiento también puede incluir un primer dispositivo de nodo, del uno o más dispositivos de nodo, que recibe un

paquete de datos con una dirección de punto de seguridad desconocido que corresponde a un punto de seguridad desconocido, emitiendo el primer dispositivo de nodo una solicitud de dirección dinámica a las dos o más zonas seguras y recibiendo el primer dispositivo de nodo una dirección del punto de seguridad desconocido en respuesta a la emisión de la solicitud de dirección dinámica.

[0035] Un sistema de comunicación vehicular puede comprender uno o más dispositivos de red (por ejemplo, encaminadores y/o conmutadores) configurados para acoplamiento operable con un sistema de vehículo (por ejemplo, un solo vehículo o una composición de vehículos). El uno o más dispositivos de red están configurados para establecer un segmento de red asegurado que incluye una pluralidad de zonas seguras en el sistema de vehículo. Las zonas seguras están configuradas cada una para enlace de red de una pluralidad respectiva de dispositivos de nodo. (Por ejemplo, una primera de las zonas seguras puede estar configurada para enlace de red de una primera pluralidad de dispositivos de nodo, y una segunda de las zonas seguras puede estar configurada para enlace de red de una segunda pluralidad de dispositivos de nodo, donde ninguno de la primera pluralidad de dispositivos de nodo tampoco es cualquiera de la segunda pluralidad de dispositivos de nodo). Los dispositivos de nodo pueden incluir uno o más dispositivos de equipos heredados conectados operativamente a infraestructura cableada. El uno o más dispositivos de red están configurados además para establecer uno o más puntos de seguridad únicos, cada uno asociado con una respectiva de la pluralidad de zonas seguras en el sistema de vehículo, para proporcionar seguridad de comunicación para las zonas seguras. El uno o más dispositivos de red están configurados además para establecer un segmento de red pública en el sistema de vehículo configurado para transportar de manera inalámbrica el tráfico de datos (por ejemplo, datos de control de vehículos privados y/o datos de señalización y/o datos de usuarios públicos) entre las zonas seguras.

[0036] De manera alternativa o complementaria, un sistema de comunicación vehicular puede comprender uno o más dispositivos de red (por ejemplo, encaminadores y/o conmutadores) configurados para acoplamiento operable con un sistema de vehículo (por ejemplo, un solo vehículo o una composición de vehículos). El uno o más dispositivos de red están configurados para establecer un segmento de red asegurado que incluye una pluralidad de zonas seguras en el sistema de vehículo. Las zonas seguras están configuradas cada una para enlace de red de una pluralidad respectiva de dispositivos de nodo. (Por ejemplo, una primera de las zonas seguras puede estar configurada para enlace de red de una primera pluralidad de dispositivos de nodo, y una segunda de las zonas seguras puede estar configurada para enlace de red de una segunda pluralidad de dispositivos de nodo, donde ninguno de la primera pluralidad de dispositivos de nodo tampoco es cualquiera de la segunda pluralidad de dispositivos de nodo). Los dispositivos de nodo pueden incluir uno o más dispositivos de equipos heredados conectados operativamente a infraestructura cableada. El uno o más dispositivos de red están configurados además para establecer uno o más puntos de seguridad únicos, cada uno asociado con una respectiva de la pluralidad de zonas seguras en el sistema de vehículo, para proporcionar seguridad de comunicación, al menos a un nivel de la capa de red, para las zonas seguras. El uno o más dispositivos de red están configurados además para establecer un segmento de red pública en el sistema de vehículo configurado para transportar de manera inalámbrica el tráfico de datos (por ejemplo, datos de control de vehículos privados y/o datos de señalización y/o datos de usuarios públicos) entre las zonas seguras.

[0037] Además, un sistema de comunicación vehicular puede comprender uno o más dispositivos de red (por ejemplo, encaminadores y/o conmutadores) configurados para acoplamiento operable con un sistema de vehículo (por ejemplo, un solo vehículo o una composición de vehículos). El uno o más dispositivos de red están configurados para establecer un segmento de red asegurado que incluye una pluralidad de zonas seguras en el sistema de vehículo. Las zonas seguras están configuradas cada una para enlace de red de una pluralidad respectiva de dispositivos de nodo. (Por ejemplo, una primera de las zonas seguras puede estar configurada para enlace de red de una primera pluralidad de dispositivos de nodo, y una segunda de las zonas seguras puede estar configurada para enlace de red de una segunda pluralidad de dispositivos de nodo, donde ninguno de la primera pluralidad de dispositivos de nodo tampoco es cualquiera de la segunda pluralidad de dispositivos de nodo). Los dispositivos de nodo pueden incluir uno o más dispositivos de equipos heredados conectados operativamente a infraestructura cableada. El uno o más dispositivos de red están configurados además para establecer uno o más puntos de seguridad únicos, cada uno asociado con una respectiva de la pluralidad de zonas seguras en el sistema de vehículo, para proporcionar seguridad de comunicación para las zonas seguras. El uno o más dispositivos de red están configurados para establecer que la seguridad de comunicación se establezca, al menos en parte, generando un túnel de comunicación inalámbrica segura entre dos zonas cualesquiera de la pluralidad de zonas seguras. El uno o más dispositivos de red están configurados además para establecer un segmento de red pública en el sistema de vehículo configurado para transportar de manera inalámbrica el tráfico de datos (por ejemplo, datos de control de vehículos privados y/o datos de señalización y/o datos de usuarios públicos) entre las zonas seguras.

[0038] Aún más, un sistema de comunicación vehicular puede comprender un primer dispositivo de borde (por ejemplo, primer encaminador y/o primer conmutador) asociado con una primera zona segura en una primera ubicación en un sistema de vehículo y configurado para ser acoplado comunicativamente con una primera pluralidad de dispositivos de nodo de la primera zona segura, para proporcionar un primer punto de seguridad para la primera zona segura. El sistema comprende además un segundo dispositivo de borde (por ejemplo, segundo encaminador y/o segundo conmutador) asociado con una segunda zona segura en una segunda ubicación en el sistema de vehículo y configurado para ser acoplado comunicativamente con una segunda pluralidad de dispositivos de nodo de la segunda

zona segura, para proporcionar un segundo punto de seguridad para la segunda zona segura. El sistema comprende además un primer transpondedor inalámbrico acoplado operativamente al primer dispositivo de borde y un segundo transpondedor inalámbrico acoplado operativamente al segundo dispositivo de borde. El primer dispositivo de borde y el segundo dispositivo de borde están configurados para establecer un primer túnel de comunicación inalámbrica segura entre la primera zona segura y la segunda zona segura a través del primer transpondedor inalámbrico y el segundo transpondedor inalámbrico. Las zonas seguras pueden ser, por ejemplo, salas de máquinas, salas de control o similares del sistema de vehículo.

[0039] De manera alternativa o complementaria, el primer dispositivo de borde y el segundo dispositivo de borde están configurados para establecer seguridad de comunicación entre la primera zona segura y la segunda zona segura al menos un a nivel de la capa de red.

[0040] Además, dos o más de la primera pluralidad de dispositivos de nodo pueden estar configurados para comunicarse entre sí dentro de la primera zona segura, y dos o más de la segunda pluralidad de dispositivos de nodo están configurados para comunicarse entre sí dentro de la segunda zona segura. Uno o más de la primera pluralidad de dispositivos de nodo están configurados para comunicarse con uno o más de la segunda pluralidad de dispositivos de nodo a través del primer transpondedor inalámbrico y el segundo transpondedor inalámbrico después del establecimiento del primer túnel de comunicación inalámbrica segura.

[0041] Además, el sistema de vehículo puede comprender al menos un vehículo ferroviario, y la primera pluralidad de dispositivos de nodo y la segunda pluralidad de dispositivos de nodo incluyen equipos eléctricos asociados con el al menos un vehículo ferroviario.

[0042] Además, un sistema de comunicación vehicular puede comprender un primer dispositivo de borde (por ejemplo, primer encaminador y/o primer conmutador) asociado con una primera zona segura en una primera ubicación en un sistema de vehículo y configurado para ser acoplado comunicativamente con una primera pluralidad de dispositivos de nodo de la primera zona segura, para proporcionar un primer punto de seguridad para la primera zona segura. El sistema comprende además un segundo dispositivo de borde (por ejemplo, segundo encaminador y/o segundo conmutador) asociado con una segunda zona segura en una segunda ubicación en el sistema de vehículo y configurado para ser acoplado comunicativamente con una segunda pluralidad de dispositivos de nodo de la segunda zona segura, para proporcionar un segundo punto de seguridad para la segunda zona segura. El sistema comprende además un tercer dispositivo de borde asociado con una tercera zona segura en una tercera ubicación en el sistema de vehículo y configurado para ser acoplado comunicativamente con una tercera pluralidad de dispositivos de nodo de la tercera zona segura, para proporcionar un tercer punto de seguridad para la tercera zona segura. El sistema comprende además un primer transpondedor inalámbrico acoplado operativamente al primer dispositivo de borde, un segundo transpondedor inalámbrico acoplado operativamente al segundo dispositivo de borde y un tercer transpondedor inalámbrico acoplado operativamente al tercer dispositivo de borde. El primer dispositivo de borde y el segundo dispositivo de borde están configurados para establecer un primer túnel de comunicación inalámbrica segura entre la primera zona segura y la segunda zona segura a través del primer transpondedor inalámbrico y el segundo transpondedor inalámbrico. El primer dispositivo de borde y el tercer dispositivo de borde están configurados para establecer un segundo túnel de comunicación inalámbrica segura entre la primera zona segura y la tercera zona segura a través del primer transpondedor inalámbrico y el tercer transpondedor inalámbrico. Además, el segundo dispositivo de borde y el tercer dispositivo de borde están configurados para establecer un tercer túnel de comunicación inalámbrica segura entre la segunda zona segura y la tercera zona segura a través del segundo transpondedor inalámbrico y el tercer transpondedor inalámbrico. Las zonas seguras pueden ser, por ejemplo, salas de máquinas, salas de control o similares del sistema de vehículo.

[0043] Aún más, un procedimiento para comunicación vehicular puede comprender establecer dos o más zonas seguras en un sistema de vehículo, teniendo cada zona segura uno o más dispositivos de nodo respectivos, realizar un procedimiento de autenticación para autenticar y autorizar el uno o más dispositivos de nodo, establecer al menos un túnel de comunicación inalámbrica segura entre las dos o más zonas seguras, y establecer un mecanismo de aprendizaje de dirección dinámico para el encaminamiento de datos entre las dos o más zonas seguras. Las zonas seguras pueden establecerse con respecto a la seguridad de las comunicaciones de datos, como se establece en esta invención y, además, las zonas seguras pueden asociarse con (por ejemplo, ubicarse en) áreas que son físicamente seguras (por ejemplo, salas cerradas o salas donde el acceso está restringido de otro modo a personas autorizadas).

[0044] Además, un procedimiento para comunicación vehicular puede comprender establecer dos o más zonas seguras en un sistema de vehículo, teniendo cada zona segura uno o más dispositivos de nodo respectivos, realizar un procedimiento de autenticación para autenticar y autorizar el uno o más dispositivos de nodo, establecer al menos un túnel de comunicación inalámbrica segura entre las dos o más zonas seguras, y establecer un mecanismo de aprendizaje de dirección dinámico para el encaminamiento de datos entre las dos o más zonas seguras. El túnel de comunicación inalámbrica segura se establece, al menos en parte, generando un certificado digital común y usando un intercambio de claves Diffie-Hellman.

[0045] Continuando, un procedimiento para comunicación vehicular puede comprender establecer dos o más

zonas seguras en un sistema de vehículo, teniendo cada zona segura uno o más dispositivos de nodo respectivos, realizar un procedimiento de autenticación para autenticar y autorizar el uno o más dispositivos de nodo, establecer al menos un túnel de comunicación inalámbrica segura entre las dos o más zonas seguras, y establecer un mecanismo de aprendizaje de dirección dinámico para el encaminamiento de datos entre las dos o más zonas seguras. El túnel de comunicación inalámbrica segura se establece, al menos en parte, autenticando mutuamente las dos o más zonas seguras basándose en identidades de anfitrión.

[0046] Aún más, un procedimiento para comunicación vehicular puede comprender establecer dos o más zonas seguras en un sistema de vehículo, teniendo cada zona segura uno o más dispositivos de nodo respectivos, realizar un procedimiento de autenticación para autenticar y autorizar el uno o más dispositivos de nodo, establecer al menos un túnel de comunicación inalámbrica segura entre las dos o más zonas seguras, y establecer un mecanismo de aprendizaje de dirección dinámico para el encaminamiento de datos entre las dos o más zonas seguras. Las dos o más zonas seguras se establecen proporcionando un punto de seguridad único respectivo de comunicación asociado con cada zona segura en el sistema de vehículo.

[0047] Continuando, un procedimiento para comunicación vehicular puede comprender establecer dos o más zonas seguras en un sistema de vehículo, teniendo cada zona segura uno o más dispositivos de nodo respectivos, realizar un procedimiento de autenticación para autenticar y autorizar el uno o más dispositivos de nodo, establecer al menos un túnel de comunicación inalámbrica segura entre las dos o más zonas seguras, y establecer un mecanismo de aprendizaje de dirección dinámico para el encaminamiento de datos entre las dos o más zonas seguras. El mecanismo de aprendizaje de dirección dinámico se establece, al menos en parte, manteniendo una tabla de reenvío respectiva para cada zona segura para asignar una dirección de un dispositivo de nodo a una dirección de un punto de seguridad responsable.

[0048] Adicionalmente, un procedimiento para comunicación vehicular puede comprender establecer dos o más zonas seguras en un sistema de vehículo, teniendo cada zona segura uno o más dispositivos de nodo respectivos, realizar un procedimiento de autenticación para autenticar y autorizar el uno o más dispositivos de nodo, establecer al menos un túnel de comunicación inalámbrica segura entre las dos o más zonas seguras, y establecer un mecanismo de aprendizaje de dirección dinámico para el encaminamiento de datos entre las dos o más zonas seguras. El procedimiento comprende además un primer dispositivo de nodo del uno o más dispositivos de nodo que recibe un paquete de datos con una dirección de punto de seguridad desconocido que corresponde a un punto de seguridad desconocido, emitiendo el primer dispositivo de nodo una solicitud de dirección dinámica a las dos o más zonas seguras y recibiendo el primer dispositivo de nodo una dirección del punto de seguridad desconocido en respuesta a la emisión de la solicitud de dirección dinámica.

[0049] De manera alternativa o complementaria, un procedimiento para comunicación vehicular puede comprender establecer, con uno o más dispositivos de red, dos o más zonas seguras en un sistema de vehículo (teniendo cada zona segura uno o más dispositivos de nodo respectivos), realizar, con el uno o más dispositivos de red, un procedimiento de autenticación para autenticar y autorizar el uno o más dispositivos de nodo, establecer, con el uno o más dispositivos de red, al menos un túnel de comunicación inalámbrica segura entre las dos o más zonas seguras, y encaminar los datos (por el uno o más dispositivos de red) entre las dos o más zonas seguras basándose al menos en parte en direcciones aprendidas dinámicamente de los dispositivos de nodo y/o el uno o más dispositivos de red. En la memoria descriptiva y las reivindicaciones, se hará referencia a varios términos que tienen los siguientes significados. Las formas singulares "un", "una" y "el", "la" incluyen referencias plurales a menos que el contexto indique claramente lo contrario_Puede aplicarse un lenguaje aproximado, como se usa en esta invención a lo largo de la memoria descriptiva y las reivindicaciones, para modificar cualquier representación cuantitativa que pudiera variar permisiblemente sin dar lugar a un cambio en la función básica con la que está relacionada. Por consiguiente, un valor modificado por un término como "aproximadamente" no debe limitarse al valor preciso especificado, en algunos casos, el lenguaje aproximado puede corresponder a la precisión de un instrumento para medir el valor. De manera similar, "libre de" puede usarse en combinación con un término, y puede incluir un número insustancial, o cantidades despreciables, considerándose, aun así, libre del término modificado. Además, a menos que se indique específicamente lo contrario, cualquier uso de los términos "primero", "segundo", etc., no denota ningún orden o importancia, sino que los términos "primero", "segundo", etc., se usan para distinguir un elemento de otro.

[0050] Como se usa en esta invención, los términos "puede" y "puede ser/estar" indican una posibilidad de producirse dentro de un conjunto de circunstancias; una posesión de una propiedad, característica o función especificada; y/o calificar otro verbo expresando una o más de una aptitud, capacidades o posibilidad asociada con el verbo calificado. Por consiguiente, la utilización de "puede" y "puede ser/estar" indica que un término modificado es aparentemente apropiado, capaz o adecuado para una capacidad, función o utilización indicada, teniendo en cuenta que, en algunas circunstancias, el término modificado a veces puede no ser apropiado, capaz o adecuado. Por ejemplo, en algunas circunstancias puede esperarse un evento o una capacidad, mientras que en otras circunstancias el evento o la capacidad no pueden producirse - esta distinción se capta mediante los términos "puede" y "puede ser/estar". Esta descripción escrita proporciona diversos ejemplos para permitir a un experto ordinario en la materia poner en práctica la(s) solución(es) descrita(s), incluyendo la fabricación y el uso de dispositivos o sistemas y la realización de cualquier procedimiento incorporado. El alcance patentable de la descripción está definido al menos por

las reivindicaciones, y puede incluir otros ejemplos que se le ocurran a un experto ordinario en la materia_Tales otros ejemplos están destinados a estar dentro del alcance de las reivindicaciones si tienen elementos estructurales que no difieren del lenguaje literal de las reivindicaciones, o si incluyen elementos estructurales equivalentes con diferencias insustanciales respecto al lenguaje literal de las reivindicaciones.

REIVINDICACIONES

1. Un sistema de comunicación vehicular (100), que comprende:

uno o más dispositivos de red (130) configurados para acoplamiento operable con un sistema de vehículo, el uno o más dispositivos de red configurados para establecer un segmento de red asegurado que incluye una pluralidad de zonas seguras (110) en el sistema de vehículo, las zonas seguras configuradas cada una para enlace de red de una pluralidad respectiva de dispositivos de nodo;
donde el uno o más dispositivos de red están configurados además para establecer uno o más puntos de seguridad únicos (140), cada uno asociado con una respectiva de la pluralidad de zonas seguras (110) en el sistema de vehículo, para proporcionar seguridad de comunicación para las zonas seguras (110);
caracterizado porque
cada zona segura (110) comprende una zona de red a la que los usuarios autorizados predefinidos tienen acceso y los usuarios no autorizados no tienen acceso;
el uno o más dispositivos de red (130) están configurados además para establecer un túnel de comunicación inalámbrica segura (120) y;
un segmento de red pública contiene un canal inalámbrico en el sistema de vehículo configurado para transportar de manera inalámbrica el tráfico de datos entre las zonas seguras (110).

2. El sistema de la reivindicación 1, donde el uno o más dispositivos de red (130) están configurados para la seguridad de la comunicación, proporcionada por el punto de seguridad único respectivo (140) asociado con cada zona segura, que se establecerá al menos a un nivel de la capa de red.

3. El sistema de la reivindicación 1, donde el uno o más dispositivos de red están configurados para la seguridad de la comunicación, proporcionada por el punto de seguridad único respectivo (140) asociado con cada zona segura, que se establecerá al menos en parte generando el túnel de comunicación inalámbrica segura entre dos zonas cualesquiera de la pluralidad de zonas seguras.

4. El sistema de la reivindicación 1, donde el tráfico de datos incluye datos de control de vehículos privados y datos de señalización.

5. El sistema de la reivindicación 1, donde el tráfico de datos incluye datos de usuarios públicos.

6. El sistema de la reivindicación 1, donde la pluralidad de dispositivos de nodo (130) incluye uno o más dispositivos de equipos heredados conectados operativamente a infraestructura cableada.

7. El sistema de la reivindicación 1, donde al menos uno del uno o más dispositivos de red (130) que están configurados para establecer los puntos de seguridad únicos (140) asociados respectivamente con las zonas seguras (110) comprende uno respectivo de un encaminador o un conmutador.

8. Un sistema de comunicación vehicular según la reivindicación 1, que comprende, además:

un primer dispositivo de borde asociado con una primera zona segura de la pluralidad de zonas seguras (110) en una primera ubicación en el sistema de vehículo y configurado para ser acoplado comunicativamente con una primera pluralidad de dispositivos de nodo de la primera zona segura, para proporcionar un primer punto de seguridad para la primera zona segura;
un segundo dispositivo de borde asociado con una segunda zona segura de la pluralidad de zonas seguras (110) en una segunda ubicación en el sistema de vehículo y configurado para ser acoplado comunicativamente con una segunda pluralidad de dispositivos de nodo de la segunda zona segura, para proporcionar un segundo punto de seguridad para la segunda zona segura;
un primer transpondedor inalámbrico acoplado operativamente al primer dispositivo de borde; y un segundo transpondedor inalámbrico acoplado operativamente al segundo dispositivo de borde, el primer dispositivo de borde y el segundo dispositivo de borde configurados para establecer un primer túnel de comunicación inalámbrica segura entre la primera zona segura y la segunda zona segura a través del primer transpondedor inalámbrico y el segundo transpondedor inalámbrico.

9. El sistema de la reivindicación 8, donde el primer dispositivo de borde y el segundo dispositivo de borde están configurados para establecer seguridad de comunicación entre la primera zona segura y la segunda zona segura al menos a un nivel de la capa de red.

10. El sistema de la reivindicación 8, donde:

dos o más de la primera pluralidad de dispositivos de nodo están configurados para comunicarse entre sí dentro de la primera zona segura;
dos o más de la segunda pluralidad de dispositivos de nodo están configurados para comunicarse entre sí dentro

de la segunda zona segura; y
uno o más de la primera pluralidad de dispositivos de nodo están configurados para comunicarse con uno o más de la segunda pluralidad de dispositivos de nodo a través del primer transpondedor inalámbrico y el segundo transpondedor inalámbrico después del establecimiento del primer túnel de comunicación inalámbrica segura.

11. El sistema de la reivindicación 8, donde cada uno del primer dispositivo de borde y el segundo dispositivo de borde es uno respectivo de un encaminador o un conmutador.

12. El sistema de la reivindicación 8, donde el sistema de vehículo comprende al menos un vehículo ferroviario, y la primera pluralidad de dispositivos de nodo y la segunda pluralidad de dispositivos de nodo incluyen equipos eléctricos asociados con él al menos un vehículo ferroviario.

13. El sistema de la reivindicación 8, donde cada una de la primera zona segura y la segunda zona segura incluye una de una sala de máquinas o una sala de control del sistema de vehículo.

14. El sistema de la reivindicación 8, que comprende, además:

un tercer dispositivo de borde asociado con una tercera zona segura en una tercera ubicación en el sistema de vehículo y configurado para ser acoplado comunicativamente con una tercera pluralidad de dispositivos de nodo de la tercera zona segura, para proporcionar un tercer punto de seguridad para la tercera zona segura; y un tercer transpondedor inalámbrico acoplado operativamente al tercer dispositivo de borde,

el primer dispositivo de borde y el tercer dispositivo de borde están configurados para establecer un segundo túnel de comunicación inalámbrica segura entre la primera zona segura y la tercera zona segura a través del primer transpondedor inalámbrico y el tercer transpondedor inalámbrico, y
el segundo dispositivo de borde y el tercer dispositivo de borde están configurados para establecer un tercer túnel de comunicación inalámbrica segura entre la segunda zona segura y la tercera zona segura a través del segundo transpondedor inalámbrico y el tercer transpondedor inalámbrico.

15. Un procedimiento para comunicación vehicular, que comprende:

establecer un segmento de red seguro que incluye una pluralidad de zonas seguras (110) en un sistema de vehículo, teniendo cada zona segura una pluralidad respectiva de dispositivos de nodo;
establecer uno o más puntos de seguridad únicos (140), cada uno asociado con una respectiva de la pluralidad de zonas seguras (110) del sistema de vehículo, para proporcionar seguridad de comunicación para las zonas seguras (110), donde cada zona segura (110) comprende una zona de red a la que los usuarios autorizados predefinidos tienen acceso y los usuarios no autorizados no tienen acceso;
establecer un túnel de comunicación inalámbrica segura (120) y un segmento de red pública, que contiene un canal inalámbrico, en el sistema de vehículo, configurado para transportar de manera inalámbrica el tráfico de datos entre las zonas seguras.

16. El procedimiento de la reivindicación 15, donde el túnel de comunicación inalámbrica segura (120) se establece, al menos en parte, generando un certificado digital común y usando un intercambio de claves Diffie-Hellman.

17. El procedimiento de la reivindicación 15, donde el túnel de comunicación inalámbrica segura (120) se establece, al menos en parte, autenticando mutuamente las dos o más zonas seguras (110) basándose en identidades de anfitrión.

18. El procedimiento de la reivindicación 15, donde la pluralidad de zonas seguras (110) se establecen proporcionando un punto de seguridad de comunicación único respectivo (140) asociado con cada zona segura en el sistema de vehículo.

19. El procedimiento de la reivindicación 18, donde el mecanismo de aprendizaje de dirección dinámico se establece, al menos en parte, manteniendo una tabla de reenvío respectiva para cada zona segura para asignar una dirección de un dispositivo de nodo a una dirección de un punto de seguridad responsable.

20. El procedimiento de la reivindicación 19, que comprende, además:

un primer dispositivo de nodo, del uno o más dispositivos de nodo, que recibe un paquete de datos con una dirección de punto de seguridad desconocido que corresponde a un punto de seguridad desconocido;
emitiendo el primer dispositivo de nodo una solicitud de dirección dinámica a las dos o más zonas seguras; y
recibiendo el primer dispositivo de nodo una dirección del punto de seguridad desconocido en respuesta a la emisión de la solicitud de dirección dinámica.

FIG. 1

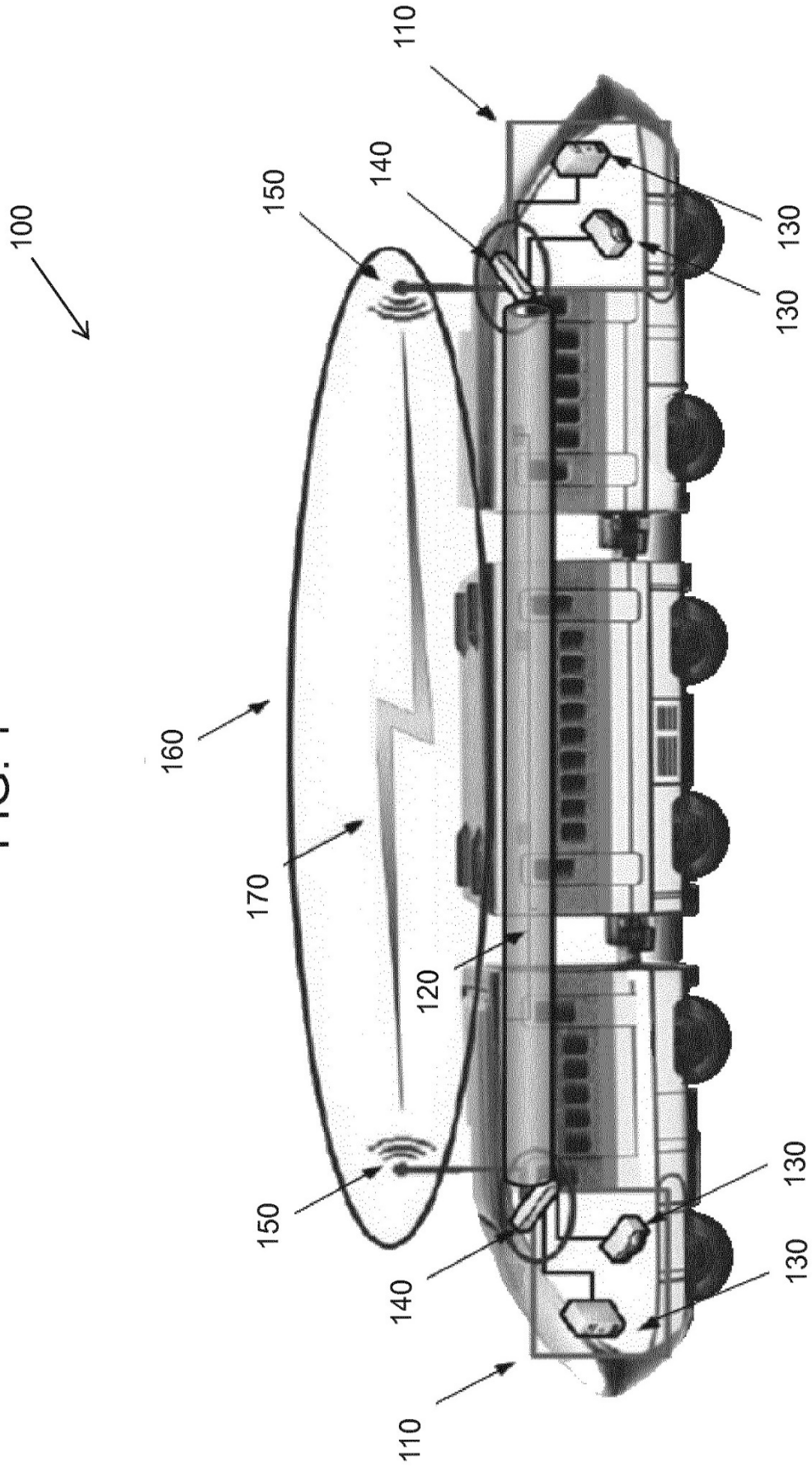


FIG. 2

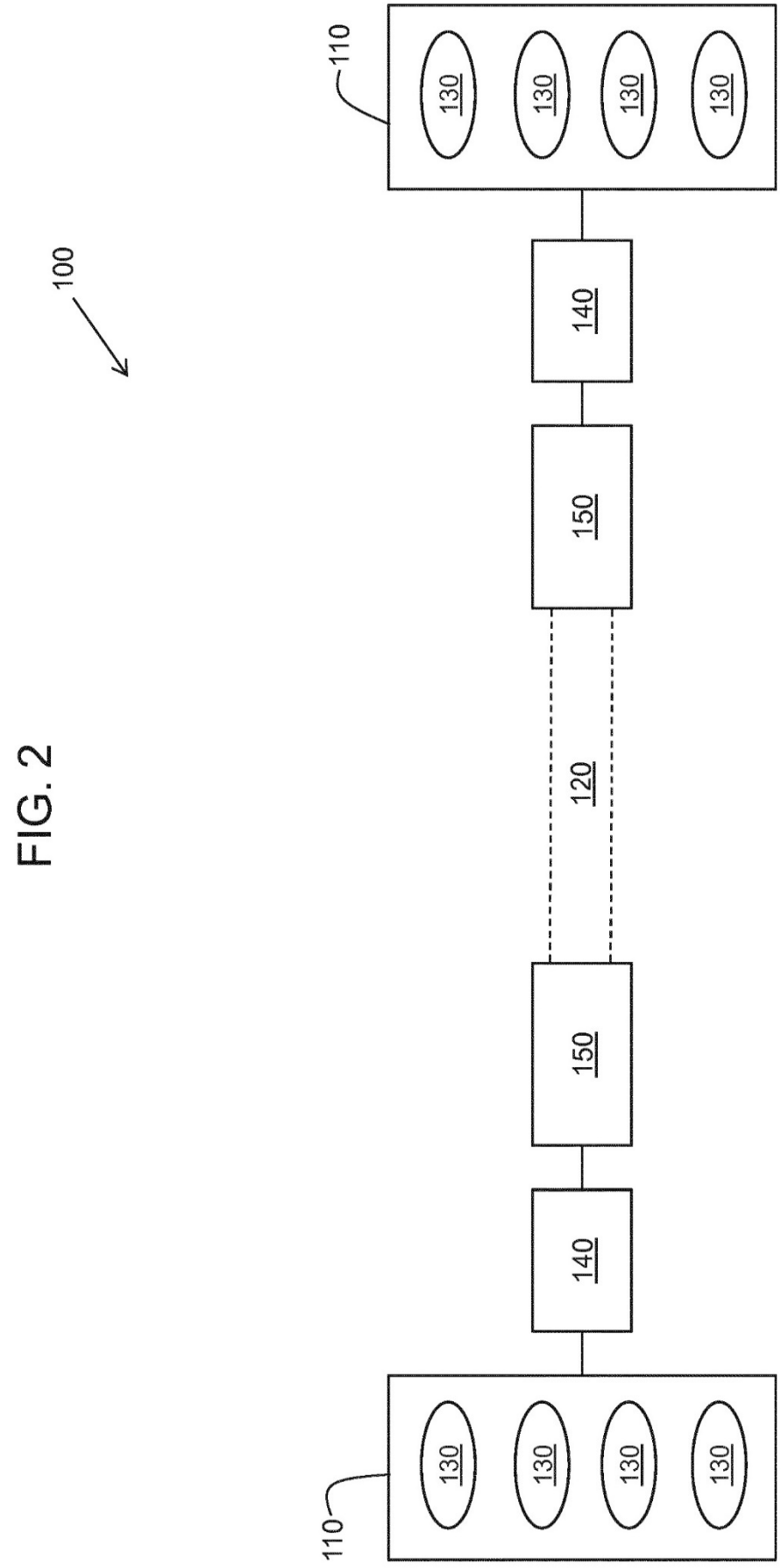


FIG. 3

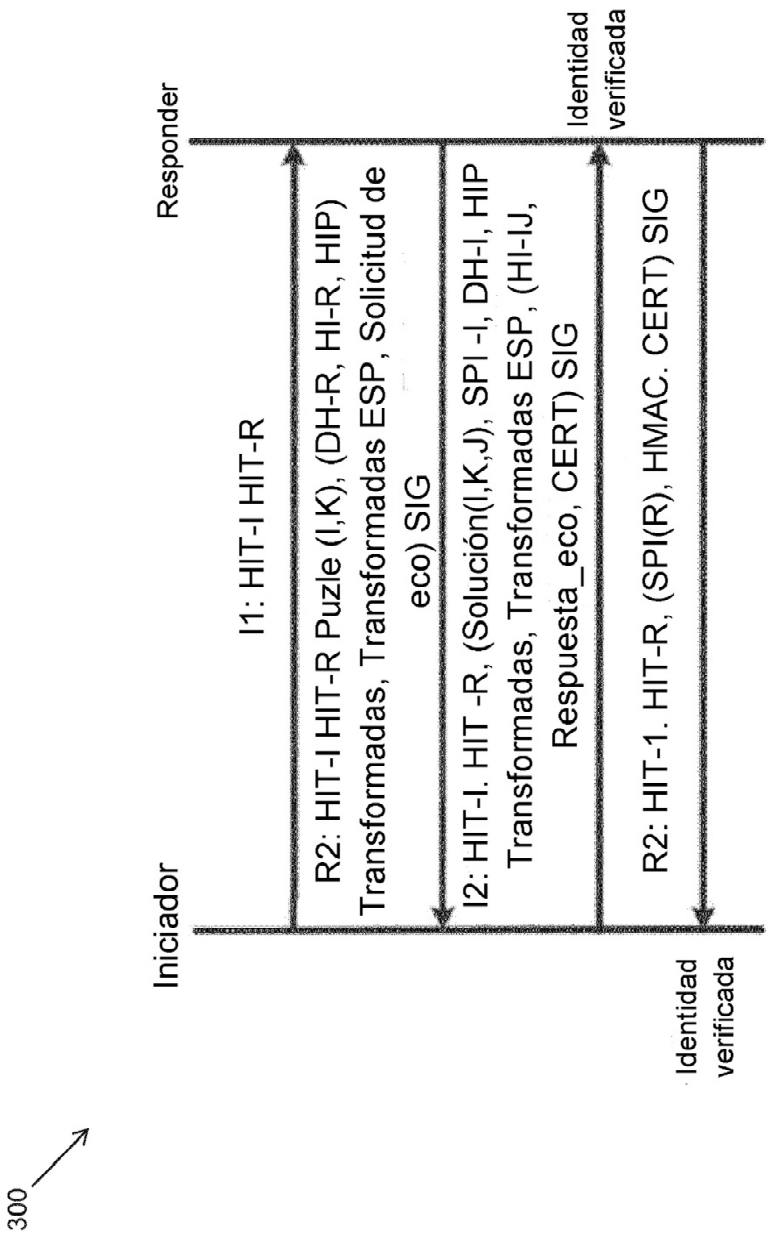
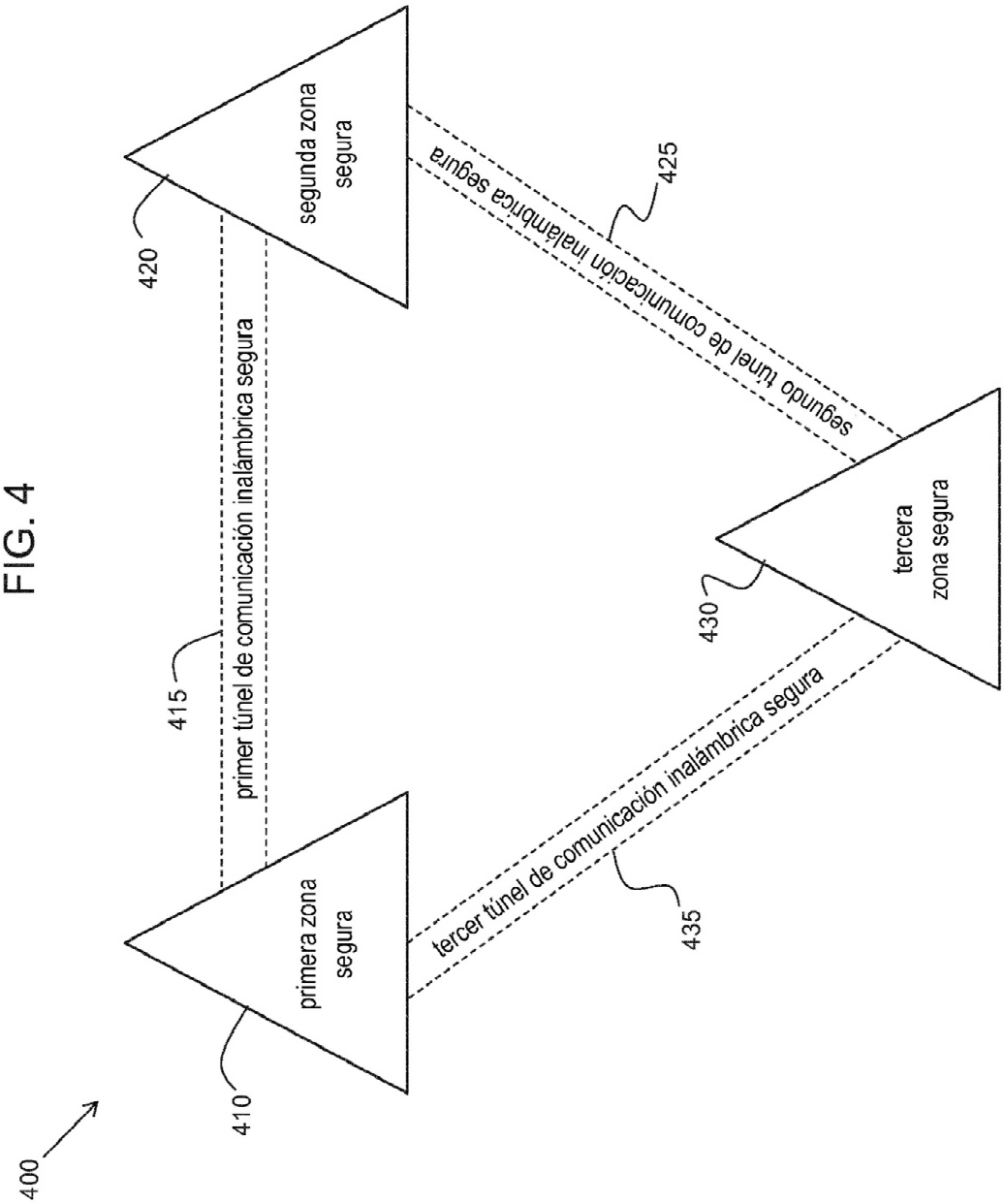

300
Iniciador
Responder
I1: HIT-I HIT-R
R2: HIT-I HIT-R Puzle (I,K), (DH-R, HI-R, HIP) Transformadas, Transformadas ESP, Solicitud de eco) SIG
I2: HIT-I. HIT -R, (Solución(I,K,J), SPI -I, DH-I, HIP Transformadas, Transformadas ESP, (HI-IJ, Respuesta_eco, CERT) SIG
R2: HIT-1. HIT-R, (SPI(R), HMAC. CERT) SIG
Identidad verificada
Identidad verificada

FIG. 4


400
410
primera zona segura
420
segunda zona segura
430
tercera zona segura
415
primer túnel de comunicación inalámbrica segura
425
segundo túnel de comunicación inalámbrica segura
435
tercer túnel de comunicación inalámbrica segura