República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(21) BR 112020025163-1 A2

(22) Data do Depósito: 10/06/2019

(43) Data da Publicação Nacional: 09/03/2021

(54) Título: PROCEDIMENTOS QUE GARANTEM PRIVACIDADE PARA WTRUS USANDO COMUNICAÇÃO PC5

(51) Int. Cl.: H04W 4/40; H04W 12/00; H04L 29/08; H04L 29/06; H04W 4/80; (...).

(30) Prioridade Unionista: 01/03/2019 US 62/812,676; 05/10/2018 US 62/741,962; 22/06/2018 US 62/688,614.

(71) Depositante(es): IDAC HOLDINGS, INC..

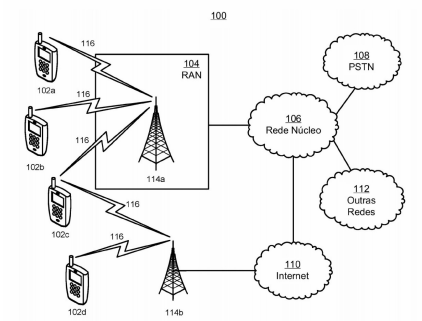
(72) Inventor(es): MICHELLE PERRAS; KHALID ANWAR; SAAD AHMAD; ALEC BRUSILOVSKY; SAMIR FERDI.

(86) Pedido PCT: PCT US2019036341 de 10/06/2019

(87) Publicação PCT: WO 2019/245783 de 26/12/2019

(85) Data da Fase Nacional: 09/12/2020

(57) Resumo: Métodos, dispositivos e sistemas para mudar um identificador (ID) de camada 2 durante uma sessão de veículo a tudo (V2X) em andamento entre uma unidade transmissora/receptora sem fio (WTRU) de origem e uma WTRU ponto incluem estabelecer comunicação entre as WTRUs de origem e ponto com base em um identificador (ID) de camada 2 (L2) existente. Na condição em que um evento disparador ocorre, a WTRU de origem gera um novo ID de L2 de origem, comunica o novo ID de L2 de origem à WTRU ponto, recebe da WTRU ponto uma mensagem que responde ao novo ID L2 de origem, e estabelece comunicação entre a WTRU de origem e a WTRU ponto com base no novo ID de L2 de origem.



"PROCEDIMENTOS QUE GARANTEM PRIVACIDADE PARA WTRUs USANDO COMUNICAÇÃO PC5"

REFERÊNCIA REMISSIVA A PEDIDOS RELACIONADOS

[001]O presente pedido reivindica o benefício do pedido de patente provisório dos EUA nº 62/688.614, depositado no dia 22 de junho de 2018, do pedido de patente provisório dos EUA nº 62.741.962, depositado no dia 5 de outubro de 2018, e do pedido provisório dos EUA nº 62.812.676, depositado no dia 1º de março de 2019, todos os quais incorporam-se ao presente documento por referência na íntegra para todos os fins.

FUNDAMENTOS DA INVENÇÃO

[002]As comunicações de veículo a tudo (V2X) incluem comunicações entre um veículo e qualquer outra entidade adequada, tais como veículo a veículo (V2V), veículo a infraestrutura (V2I), veículo a pedestre (V2P), veículo a rede (V2N) e assim por diante. V2X também se refere aos padrões relativos a esses tipos de comunicações. PC5 é uma interface para a comunicação entre dispositivos V2X como um tipo de comunicação direta por *sidelink* ou serviço de proximidade (ProSe).

SUMÁRIO

[003]O presente sumário serve à finalidade de apresentar, de maneira simplificada, uma seleção de conceitos como introdução à descrição mais detalhada que será apresentada mais adiante. O sumário não visa a identificar elementos cruciais ou essenciais da invenção, nem a delinear o âmbito da matéria inventiva reivindicada. As modalidades expressas nas várias figuras são relacionadas, e os elementos nelas podem ser combinados, salvo menção em contrário.

[004]Em uma modalidade, um método para uso em uma sessão veículo a tudo (V2X) em andamento inclui atualizar ao menos uma unidade transmissora/receptora sem fio (WTRU) de origem com parâmetros de privacidade. O método inclui estabelecer comunicação entre uma unidade transmissora/receptora

sem fio (WTRU) de origem e uma WTRU ponto com base em um identificador (ID) de camada 2 (L2) existente. Caso ocorra um evento disparador, a WTRU de origem gera um novo ID de L2 de origem para si, comunica o novo ID de L2 de origem à WTRU ponto, recebe da WTRU ponto uma mensagem que responde ao novo ID de L2 de origem, e estabelece comunicação entre a WTRU de origem e a WTRU ponto com base no novo ID de L2 de origem.

[005]Em uma modalidade, o ID de L2 da WTRU ponto também muda. A WTRU ponto muda seu ID de L2, e a WTRU de origem recebe o novo ID de L2 da WTRU ponto. Esse recebimento do novo ID de L2 ponto na WTRU de origem ocorre após a WTRU de origem comunicar o novo ID de L2 de origem à WTRU ponto. Depois disso, a WTRU de origem e a WTRU ponto comunicam-se uma com a outra com base no novo ID de L2 de origem e no novo ID de L2 ponto.

[006]Em uma modalidade, os IDs de L2 de origem e ponto podem ser atualizados, bem como um ID de sessão para comunicação entre a WTRU de origem e a WTRU ponto. O ID de sessão é atualizado usando contribuições de um byte mais significativo (MSB) e um byte menos significativo (LSB). A WTRU de origem gera um novo MSB de um ID de sessão usado para comunicação com a WTRU ponto e também gera o novo ID de L2 de origem. A WTRU de origem comunica o novo MSB do ID de sessão junto com a comunicação do novo ID de L2 de origem à WTRU ponto. A WTRU de origem recebe um novo byte menos significativo (LSB) do ID de sessão a partir da WTRU ponto junto com o recebimento de um novo ID de L2 ponto. Depois disso, a WTRU de origem e a WTRU ponto se comunicam com base no novo ID de L2 de origem e no novo ID de L2 ponto e com base também em um novo ID de sessão que inclui o novo MSB e o novo LSB do ID de sessão.

[007]Em uma modalidade, um aspecto de comunicar o novo ID de L2 de origem à WTRU ponto inclui comunicá-lo usando um de um procedimento *keep-*

alive, um procedimento de privacidade ou outro procedimento de comunicação usado entre uma WTRU de origem e uma WTRU ponto. A WTRU de origem pode comunicar o novo ID de L2 de origem de uma camada à outra na WTRU de origem antes de comunicar-se com a WTRU ponto com base no novo ID de L2 de origem.

[008]Em uma modalidade, um evento disparador para provocar a mudança de ao menos um ID de L2 de origem pode incluir qualquer um de um temporizador que expira, uma camada superior ou uma camada de aplicativo de um aplicativo V2X que solicita um novo ID de L2, uma determinação de que a WTRU de origem moveu-se a uma nova área geográfica, a WTRU de origem recebendo novos parâmetros de aprovisionamento de uma função de controle V2X ou servidor de aplicativo V2X, ou a WTRU de origem recebendo um pedido da WTRU ponto para mudar um ID de L2. O ID de sessão pode ser um ID de sessão de contexto de segurança. A comunicação entre a WTRU de origem e a WTRU ponto pode incluir a comunicação por um enlace de referência PC5.

[009]Em uma modalidade, uma unidade transmissora/receptora sem fio (WTRU) de origem pode incluir um sistema de circuitos, incluindo um transmissor, um receptor, um processador e memória. O sistema de circuitos da WTRU é configurado para a comunicação, usando o transmissor e receptor, entre a WTRU de origem e uma WTRU ponto com base em um identificador (ID) de camada 2 (L2). Na condição em que um evento disparador ocorre, a WTRU de origem gera um novo ID de L2 de origem para si, comunica o novo ID de L2 de origem à WTRU ponto, e comunica-se com a WTRU ponto com base no novo ID de L2 de origem.

[010]Em uma modalidade em que a WTRU ponto, bem como a WTRU de origem, passa por uma mudança no ID de L2, a WTRU de origem pode receber o novo ID de L2 ponto após comunicar o ID de L2 de origem à WTRU ponto. A WTRU de origem pode então comunicar-se com a WTRU ponto com base no novo ID de L2 de origem e no novo ID de L2 ponto.

[011]Em uma modalidade, um meio de armazenamento legível por computador inclui instruções que, quando executadas por um computador, fazem com que este execute qualquer um dos métodos descritos neste documento.

BREVE DESCRIÇÃO DOS DESENHOS

[012]Uma compreensão mais detalhada pode ser apreendida com base na descrição a seguir, dada à guisa de exemplo junto com os desenhos anexos, nos quais números de referência iguais nas figuras indicam os mesmos elementos e dentre os quais:

a FIG. 1A é um diagrama de sistema ilustrando um sistema de comunicações exemplificativo no qual uma ou mais modalidades reveladas podem ser implementadas;

a FIG. 1B é um diagrama de sistema ilustrando uma unidade transmissora/receptora sem fio (WTRU) exemplificativa que pode ser usada dentro do sistema de comunicações ilustrado na FIG. 1A de acordo com uma modalidade;

a FIG. 1B é um diagrama de sistema ilustrando uma rede de acesso via rádio (RAN) exemplificativa e uma rede núcleo (CN) exemplificativa que podem ser usadas dentro do sistema de comunicações ilustrado na FIG. 1A de acordo com uma modalidade;

a FIG. 1D é um diagrama de sistema ilustrando outra RAN exemplificativa e outra CN exemplificativa que podem ser usadas dentro do sistema de comunicações ilustrado na FIG. 1A de acordo com uma modalidade;

a FIG. 2 ilustra um formato de ID de contexto de segurança em um cabeçalho de PDCP para comunicações de um a um;

a FIG. 3 é um diagrama de sequência ilustrando uma vista de alto nível de uma mudança exemplificativa do ID de L2 da WTRU de origem;

a FIG. 4 é um diagrama de sequência ilustrando um exemplo de aprovisionamento de parâmetros de privacidade;

a FIG. 5 é um diagrama de sequência ilustrando um exemplo de um procedimento de estabelecimento de enlace direto desse tipo;

a FIG. 6 é um diagrama de sequência ilustrando um exemplo de intercâmbio de novos identificadores de L2 usando um procedimento *keep-alive* atualizado;

a FIG. 7 é um diagrama de sequência ilustrando um exemplo de WTRUs de origem e ponto atualizando seus IDs de L2 durante o mesmo procedimento;

a FIG. 8 é um diagrama de sequência ilustrando um exemplo de um procedimento de privacidade com a mudança de um único ID de L2;

a FIG. 9 é um diagrama de sequência ilustrando um exemplo no qual os IDs de L2 da WTRU de origem e da WTRU ponto são atualizados durante o mesmo procedimento;

a FIG. 10 é um diagrama de sequência ilustrando um exemplo no qual a WTRU ponto dispara o procedimento de mudança de ID de L2;

a FIG. 11 é um diagrama de sequência ilustrando um procedimento exemplificativo no qual a WTRU de origem configura a WTRU ponto e o ID de L2 da WTRU de origem atualiza;

a FIG. 12 é um diagrama de sequência ilustrando a configuração do valor de temporizador de privacidade e da semente;

a FIG. 13 é um diagrama de sequência de mensagens ilustrando o caso em que ambas as WTRUs trocam sua nova porção do ID de sessão uma com a outra usando o procedimento de privacidade;

a FIG. 14 é um diagrama de sequência de mensagens ilustrando o intercâmbio de novos IDs de L2 usando um procedimento de rechaveamento aprimorado; e

a FIG. 15 é um fluxograma de um método que emprega elementos de um procedimento para mudar ao menos um ID de L2 de origem.

DESCRIÇÃO DETALHADA

[013]A FIG. 1A é um diagrama que ilustra um sistema de comunicações exemplificativo 100 no qual uma ou mais modalidades reveladas podem ser implementadas. O sistema de comunicações 100 pode ser um sistema de acesso múltiplo que oferece conteúdo, tal como voz, dados, vídeo, troca de mensagens, difusão etc., a vários usuários sem fio. O sistema de comunicações 100 permite que vários usuários sem fio acessem esse conteúdo pelo compartilhamento de recursos do sistema, incluindo largura de banda sem fio. Por exemplo, os sistemas de comunicações 100 podem empregar um ou mais métodos de acesso a canal, tais como acesso múltiplo por divisão de código (CDMA), acesso múltiplo por divisão de tempo (TDMA), acesso múltiplo por divisão de frequência (FDMA), FDMA ortogonal (OFDMA), FDMA de portadora única (SC-FDMA), OFDM com espalhamento através da DFT, palavra única e zero cauda (ZT UW DTS-s OFDM), OFDM de palavra única (UW-OFDM), OFDM filtrada com bloco de recursos, multiportadora de banco de filtros (FBMC), e seus semelhantes.

[014]Conforme ilustra a FIG. 1A, o sistema de comunicações 100 pode incluir unidades transmissoras/receptoras sem fio (WTRUs) 102a, 102b, 102c, 102d, uma RAN 104/113, uma CN 106/115, uma rede telefônica pública comutada (PSTN) 108, a Internet 110 e outras redes 112, embora aprecie-se que as modalidades reveladas contemplem qualquer número de WTRUs, estações de base, redes e/ou elementos de rede. Cada uma das WTRUs 102a, 102b, 102c, 102d pode ser qualquer tipo de dispositivo configurado para operar e/ou comunicar-se em um ambiente sem fio. À guisa de exemplo, as WTRUs 102a, 102b, 102c, 102d, qualquer uma das quais pode ser chamada de “estação” e/ou “STA”, podem ser configuradas para transmitir e/ou receber sinais sem fio e podem incluir um equipamento do usuário (UE), uma estação móvel, uma unidade do assinante fixa ou móvel, uma unidade baseada em assinatura, um *pager*, um telefone celular, um assistente digital pessoal (PDA), um *smartphone*, um *laptop*, um *netbook*, um computador pessoal,

um sensor sem fio, um dispositivo *hotspot* ou Mi-Fi, um dispositivo de Internet das Coisas (IoT), um relógio ou outro acessório de vestir, uma tela montada na cabeça (HMD), um veículo, um *drone*, um dispositivo médico e aplicativos (por exemplo, cirurgia remota), um dispositivo industrial e aplicativos (por exemplo, um robô e/ou outros dispositivos sem fio operando em contextos de cadeia de processamento industrial e/ou automatizada), um dispositivo eletrônico do consumidor, um dispositivo operando em redes sem fio comerciais e/ou industriais, e seus semelhantes. Qualquer uma das WTRUs 102a, 102b, 102c e 102d pode ser chamada intercambiavelmente de UE.

[015]Os sistemas de comunicações 100 também podem incluir uma estação de base 114a e/ou uma estação de base 114b. Cada uma das estações de base 114a, 114b pode ser qualquer tipo de dispositivo configurado para fazer interface sem fio com ao menos uma das WTRUs 102a, 102b, 102c, 102d a fim de facilitar o acesso a uma ou mais redes de comunicação, tais como a CN 106/115, a Internet 110 e/ou outras redes 112. À guisa de exemplo, as estações de base 114a, 114b podem ser uma estação transceptora de base (BTS), um *Node-B*, um *eNode B*, um *Home Node B*, um *Home eNode B*, um gNB, um *NR NodeB*, um controlador de *site*, um ponto de acesso (AP), um roteador sem fio, e seus semelhantes. Embora cada uma das estações de base 114a, 114b seja representada como um único elemento, apreciar-se-á que as estações de base 114a, 114b podem incluir qualquer número de estações de base e/ou elementos de rede interconectados.

[016]A estação de base 114a pode fazer parte da RAN 104/113, que também pode incluir outras estações de base e/ou elementos de rede (não ilustrados), tais como um controlador de estação de base (BSC), um controlador de rede de rádio (RNC), nós de retransmissão etc. A estação de base 114a e/ou a estação de base 114b podem ser configuradas para transmitir e/ou receber sinais sem fio em uma ou mais frequências portadoras, que podem ser chamadas de uma

célula (não ilustrado). Essas frequências podem ser em espectro licenciado, espectro não licenciado, ou uma combinação de espectro licenciado e espectro não licenciado. Uma célula pode oferecer cobertura para um serviço sem fio a uma área geográfica específica que pode ser relativamente fixa ou que pode mudar com o tempo. A célula pode ainda ser dividida em setores de célula. Por exemplo, a célula associada à estação de base 114a pode ser dividida em três setores. Sendo assim, em uma modalidade, a estação de base 114a pode incluir três transceptores, isto é, um para cada setor da célula. Em uma modalidade, a estação de base 114a pode empregar tecnologia de múltiplas entradas e múltiplas saídas (MIMO) e pode utilizar vários transceptores para cada setor da célula. Por exemplo, a formação de feixes pode ser usada para transmitir e/ou receber sinais em direções espaciais desejadas.

[017]As estações de base 114a, 114b podem se comunicar com uma ou mais das WTRUs 102a, 102b, 102c, 102d através de uma interface aérea 116, que pode ser qualquer enlace de comunicação sem fio adequado (por exemplo, frequência de rádio (RF), micro-ondas, onda centimétrica, onda micrométrica, infravermelho (IR), ultravioleta (UV), luz visível etc.). A interface aérea 116 pode ser estabelecida usando-se qualquer tecnologia de acesso via rádio (RAT) adequada.

[018]Mais especificamente, conforme mencionado acima, o sistema de comunicações 100 pode ser um sistema de acesso múltiplo e pode empregar um ou mais esquemas de acesso a canal, tais como CDMA, TDMA, FDMA, OFDMA, SC-FDMA, e seus semelhantes. Por exemplo, a estação de base 114a na RAN 104/113 e as WTRUs 102a, 102b, 102c podem implementar uma tecnologia de rádio tal como Sistema Universal de Telecomunicações Móveis (UMTS), Acesso via rádio Terrestre (UTRA), que podem estabelecer a interface aérea 115/116/117 usando CDMA de banda larga (WCDMA). A WCDMA pode incluir protocolos de comunicação tais como Acesso em Pacote em Alta Velocidade (HSPA) e/ou HSPA Evoluída (HSPA+). HSPA pode incluir Acesso em Pacotes por Enlace Descendente (DL) em Alta

Velocidade (HSDPA) e/ou Acesso em Pacotes por Enlace Ascendente (UL) em Alta Velocidade (HSUPA).

[019]Em uma modalidade, a estação de base 114a e as WTRUs 102a, 102b, 102c podem implementar uma tecnologia de rádio tal como Acesso via rádio Terrestre via UMTS Evoluído (E-UTRA), que pode estabelecer a interface aérea 116 usando Evolução de Longo Prazo (LTE) e/ou LTE-Avançada (LTE-A) e/ou LTE-Avançada Pro (LTE-A Pro).

[020]Em uma modalidade, a estação de base 114a e as WTRUs 102a, 102b, 102c podem implementar uma tecnologia de rádio tal como Acesso via rádio NR, que pode estabelecer a interface aérea 116 usando o Novo Rádio (NR).

[021]Em uma modalidade, a estação de rádio 114a e as WTRUs 102a, 102b, 102c podem implementar várias tecnologias de acesso via rádio. Por exemplo, a estação de base 114a e as WTRUs 102a, 102b, 102c podem implementar acesso via rádio LTE e acesso via rádio NR conjuntamente, por exemplo usando princípios de conectividade dupla (DC). Sendo assim, a interface aérea utilizada pelas WTRUs 102a, 102b, 102c pode ser caracterizada por vários tipos de tecnologias de acesso via rádio e/ou transmissões enviadas a/de vários tipos de estações de base (por exemplo, um eNB e um gNB).

[022]Em outras modalidades, a estação de base 114a e as WTRUs 102a, 102b, 102c podem implementar tecnologias de rádio tais como IEEE 802.11 (isto é, Fidelidade Sem Fio (WiFi), IEEE 802.16 (isto é, Interoperabilidade Mundial para Acesso por Micro-ondas (WiMAX)), CDMA2000, CDMA2000 1X, CDMA2000 EV-DO, Padrão Interim 2000 (IS-2000), Padrão Interim 95 (IS-95), Padrão Interim 856 (IS-856), Sistema Global para Comunicações Móveis (GSM), Taxas de Dados Aprimoradas para a Evolução do GSM (EDGE), GSM EDGE (GERAN), e seus semelhantes.

[023]A estação de base 114b na FIG. 1A pode ser um roteador sem fio, *Home Node B*, *Home eNode B* ou ponto de acesso, por exemplo, e pode utilizar qualquer RAT adequada para facilitar a conectividade sem fio em uma área localizada, tal como um local de trabalho, uma residência, um veículo, um *campus*, uma instalação industrial, um corredor aéreo (por exemplo, para uso por *drones*), uma pista, e seus semelhantes. Em uma modalidade, a estação de base 114b e as WTRUs 102c, 102d podem implementar uma tecnologia de rádio tal como IEEE 802.11 para estabelecer uma rede de área local sem fio (WLAN). Em uma modalidade, a estação de base 114b e as WTRUs 102c, 102d podem implementar uma tecnologia de rádio tal como IEEE 802,15 para estabelecer uma rede de área pessoal sem fio (WPAN). Em ainda outra modalidade, a estação de base 114b e as WTRUs 102c, 102d podem utilizar uma RAT baseada em celular (por exemplo, WCDMA, CDMA2000, GSM, LTE, LTE-A, LTE-A Pro, NR etc.) para estabelecer uma picocélula ou femtocélula. Conforme ilustra a FIG. 1A, a estação de base 114b pode ter conexão direta com a Internet 110. Sendo assim, não é necessário que a estação de base 114b acesse a Internet 110 pela CN 106/115.

[024]A RAN 104/113 pode estar em comunicação com a CN 106/115, que pode ser qualquer tipo de rede configurada para oferecer serviços de voz, dados, aplicativos e/ou voz por protocolo internet (VoIP) a uma ou mais das WTRUs 102a, 102b, 102c, 102d. Os dados podem ter requisitos de qualidade de serviço (QoS) variados, tal como requisitos de taxa de transmissão efetiva, requisitos de latência, requisitos de tolerância a erros, requisitos de confiabilidade, requisitos de taxa de transmissão efetiva de dados, requisitos de mobilidade, e seus semelhantes, divergentes. A CN 106/115 pode oferecer controle de chamadas, serviços de cobrança, serviços à base de localização móvel, chamadas pré-pagas, conectividade com a Internet, distribuição de vídeo etc. e/ou executar funções de segurança de alto nível, tais como autenticação. Embora não seja ilustrado na FIG. 1A, apreciar-se-á

que a RAN 104/113 e/ou a CN 106/115 podem estar em comunicação direta ou indireta com outras RANs que empreguem a mesma RAT que a RAN 104/113 ou uma RAT diferente. Por exemplo, além de conectar-se à RAN 104/113, que pode estar utilizando uma tecnologia de rádio NR, a CN 106/115 também pode estar em comunicação com outra RAN (não ilustrado) que empregue tecnologia GSM, UMTS, CDMA 2000, WiMAX, E-UTRA ou rádio WiFi.

[025]A CN 106/115 também pode atuar como via de acesso para as WTRUs 102a, 102b, 102c, 102d acessarem a PSTN 108, a Internet 110 e/ou outras redes 112. A PSTN 108 pode incluir redes telefônicas de circuito comutado que oferecem serviço telefônico comum (POTS). A Internet 110 pode incluir um sistema global de redes de computador e dispositivos interconectados que utilizam protocolos de comunicação em comum, tais como o protocolo de controle de transmissão (TCP), o protocolo de datagrama do usuário (UDP) e/ou o protocolo internet (IP) no pacote TCP/protocolo internet IP. As redes 112 podem incluir redes de comunicação com fio e/ou sem fio pertencentes e/ou operadas por outros provedores de serviço. Por exemplo, as redes 112 podem incluir outra CN conectada a uma ou mais RANs, que podem empregar a mesma RAT que a RAN 104/113 ou uma RAT diferente.

[026]Algumas das WTRUs 102a, 102b, 102c, 102d no sistema de comunicações 100, ou todas elas, podem incluir recursos multimodo (por exemplo, as WTRUs 102a, 102b, 102c, 102d podem incluir vários transceptores para comunicação com diferentes redes sem fio por diferentes enlaces sem fio). Por exemplo, a WTRU 102c ilustrada na FIG. 1A pode ser configurada para se comunicar com a estação de base 114a, que pode empregar uma tecnologia baseada em celular, e com a estação de base 114b, que pode empregar uma tecnologia de rádio IEEE 802.

[027]A FIG. 1B é um diagrama de sistema que ilustra um exemplo de WTRU 102. Conforme ilustra a FIG. 1B, a WTRU 102 pode incluir um processador 118, um

transceptor 120, um elemento transmissor/receptor 122, um alto-falante/microfone 124, um teclado 126, uma tela/*touchpad* 128, memória não removível 130, memória removível 132, uma fonte de alimentação 134, um *chipset* com sistema de posicionamento global (GPS) 136 e/ou outros periféricos 138, entre outros. Apreciar-se-á que a WTRU 102 pode incluir qualquer subcombinação dos elementos anteriores e, ainda assim, permanecer consistente com uma modalidade.

[028]O processador 118 pode ser um processador de propósito geral, um processador de propósito especial, um processador convencional, um processador digital de sinais (DSP), uma pluralidade de microprocessadores, um ou mais microprocessadores em associação a um núcleo DSP, um controlador, um microcontrolador, Circuitos Integrados de Aplicação Específica (ASICs), circuitos de Arranjos de Portas Programável em Campo (FPGAs), qualquer outro tipo de circuito integrado (IC), uma máquina de estados, e seus semelhantes. O processador 118 pode executar codificação de sinais, processamento de dados, controle de energia, processamento de entradas/saídas e/ou outras funcionalidades que permitam que a WTRU 102 opere em um ambiente sem fio. O processador 118 pode ser acoplado ao transceptor 120, que pode ser acoplado ao elemento transmissor/receptor 122. Embora a FIG. 1B represente o processador 118 e o transceptor 120 como componentes distintos, apreciar-se-á que o processador 120 e o transceptor 120 sejam integrados um ao outro em um pacote ou *chip* eletrônico.

[029]O elemento transmissor/receptor 122 pode ser configurado para transmitir sinais a, ou receber sinais de, uma estação de base (por exemplo, a estação de base 114a) pela interface aérea 116. Por exemplo, em uma modalidade, o elemento transmissor/receptor 122 pode ser uma antena configurada para transmitir e/ou receber sinais de RF. Em uma modalidade, o elemento transmissor/receptor 122 pode ser um emissor/detector configurado para transmitir e/ou receber sinais de IR, UV ou luz visível, por exemplo. Em ainda outra

modalidade, o elemento transmissor/receptor 122 pode ser configurado para transmitir e/ou receber tanto sinais de RF quanto sinais luminosos. Apreciar-se-á que o elemento transmissor/receptor 122 pode ser configurado para transmitir e/ou receber qualquer combinação de sinais sem fio.

[030]Embora o elemento transmissor/receptor 122 seja representado na FIG. 1B como um único elemento, a WTRU 102 pode incluir qualquer número de elementos transmissores/receptores 122. Mais especificamente, a WTRU 102 pode empregar a tecnologia MIMO. Sendo assim, em uma modalidade, a WTRU 102 pode incluir dois ou mais elementos transmissores/receptores 122 (por exemplo, várias antenas) para transmitir e receber sinais sem fio pela interface aérea 116.

[031]O transceptor 120 pode ser configurado para modular os sinais que serão transmitidos pelo elemento transmissor/receptor 122 e para demodular os sinais que são recebidos pelo elemento transmissor/receptor 122. Como mencionado acima, a WTRU 102 pode ter recursos multimodo. Sendo assim, o transceptor 120 pode incluir vários transceptores para permitir que a WTRU 102 se comunique através de várias RATs, tais como NR e IEEE 802.11, por exemplo.

[032]O processador 118 da WTRU 102 pode ser acoplado ao, e receber dados de entrada do usuário do, alto-falante/microfone 124, teclado 126 e/ou tela/*touchpad* 128 (por exemplo, uma unidade exibição de tela de cristal líquido (LCD) ou uma unidade de exibição de diodos orgânicos emissores de luz (OLED)). O processador 118 também pode emitir dados do usuário ao alto-falante/microfone 124, teclado 126 e/ou tela/*touchpad* 128. Além disso, o processador 118 pode acessar informações de, e armazenar dados em, qualquer tipo de memória adequada, tal como a memória não removível 130 e/ou a memória removível 132. A memória não removível 130 pode incluir memória de acesso aleatório (RAM), memória somente para leitura (ROM), um disco rígido ou qualquer outro tipo de dispositivo de armazenamento de memória. A memória removível 132 pode incluir

um cartão módulo de identidade do assinante (SIM), um *memory stick*, uma cartão de memória digital segura (SD), e seus semelhantes. Em outras modalidades, o processador 118 pode acessar informações de uma, e armazenar dados em uma, memória que não está localizada fisicamente na WTRU 102, tal como em um servidor ou computador residencial (não ilustrado).

[033]O processador 118 pode receber energia da fonte de alimentação 134 e pode ser configurado para distribuir e/ou controlar a energia aos demais componentes na WTRU 102. A fonte de alimentação 134 pode ser qualquer dispositivo adequado para alimentar a WTRU 102. Por exemplo, a fonte de alimentação 134 pode incluir uma ou mais baterias de célula seca (por exemplo, níquel-cádmio (NiCd), níquel-zinco (NiZn), hidreto de metal níquel (NiMH), íons de lítio (Li-ion) etc.), células solares, células de combustível, e seus semelhantes.

[034]O processador 118 também pode acoplar-se ao *chipset* GPS 136, que pode ser configurado para fornecer informações de localização (por exemplo, longitude e latitude) referentes à localização atual da WTRU 102. Em aditamento, ou como alternativa, às informações do *chipset* GPS 136, a WTRU 102 pode receber informações de localização pela interface aérea 116 a partir de uma estação de base (por exemplo, estações de base 114a, 114b) e/ou determinar sua localização com base na temporização dos sinais sendo recebidos de duas ou mais estações de base próximas. Apreciar-se-á que a WTRU 102 possa obter informações de localização por meio de qualquer método de determinação da localização adequado e, ainda assim, permanecer consistente com uma modalidade.

[035]O processador 118 pode acoplar-se ainda a outros periféricos 138, que podem incluir um ou mais módulos de *software* e/ou *hardware* que oferecem elementos, funcionalidades, e/ou conectividade com fio ou sem fio adicionais. Por exemplo, os periféricos 138 podem incluir um acelerômetro, um compasso eletrônico, um transceptor via satélite, uma câmera digital (para fotografias e/ou

vídeo), uma porta de barramento serial universal (USB), um dispositivo de vibração, um transceptor de televisão, um *headset hands-free*, um módulo Bluetooth®, uma unidade de rádio de frequência modulada (FM), um reprodutor de música digital, um reprodutor de mídia, um módulo reprodutor de jogos eletrônicos, um navegador de Internet, um dispositivo de Realidade Virtual e/ou Realidade Aumentada (VR/AR), um rastreador de atividades, e seus semelhantes. Os periféricos 138 podem incluir um ou mais sensores, os quais podem ser um ou mais de um giroscópio, um acelerômetro, um sensor de efeito de Hall, um magnetômetro, um sensor de orientação, um sensor de proximidade, um sensor de temperatura, um sensor de tempo; um sensor de geolocalização; um altímetro, um sensor de luminosidade, um sensor de toque, um magnetômetro, um barômetro, um sensor de gestos, um sensor biométrico e/ou um sensor de umidade.

[036]A WTRU 102 pode incluir um rádio dúplex completo para o qual a transmissão e a recepção de alguns dos, ou todos os, sinais (por exemplo, associados a subquadros específicos tanto para o enlace ascendente (por exemplo, para transmissão) quanto para o enlace descendente (por exemplo, para recepção)) podem ser concomitantes e/ou simultâneas. O rádio dúplex completo pode incluir uma unidade de gestão de interferência 139 para reduzir ou eliminar substancialmente a autointerferência via ou *hardware* (por exemplo, um afogador) ou processamento de sinais via um processador (por exemplo, via um processador separado (não ilustrado) ou via o processador 118). Em uma modalidade, a WTRU 102 pode incluir um rádio semidúplex para o qual a transmissão e a recepção de alguns dos, ou todos os, sinais (por exemplo, associados a subquadros específicos tanto para o enlace ascendente (por exemplo, para transmissão) quanto para o enlace descendente (por exemplo, para recepção)).

[037]A FIG. 1C é um diagrama de sistema que ilustra a RAN 104 e a CN 106 de acordo com uma modalidade. Como mencionado acima, a RAN 104 pode

empregar tecnologia de rádio E-UTRA para se comunicar com as WTRUs 102a, 102b, 102c pela interface aérea 116. A RAN 104 também pode estar em comunicação com a CN 106.

[038]A RAN 104 pode incluir os *eNode-Bs* 160a, 160b, 160c, embora contemple-se que a RAN 104 pode incluir qualquer número de *eNode-Bs* e, ainda assim, permanecer consistente com uma modalidade. Cada um dos *eNode-Bs* 160a, 160b, 160c pode incluir um ou mais transceptores para comunicação com as WTRUs 102a, 102b, 102c pela interface aérea 116. Em uma modalidade, os *eNode-Bs* 160a, 160b, 160c podem implementar tecnologia MIMO. Sendo assim, o eNode-B 160a, por exemplo, pode utilizar várias antenas para transmitir sinais sem fio à, e/ou receber sinais sem fio da, WTRU 102a.

[039]Cada um dos *eNode-Bs* 160a, 160b, 160c pode ser associado a uma célula específica (não ilustrado) e pode ser configurado para lidar com decisões de gestão de recursos de rádio, decisões de *handover*, agendamento de usuários no UL e/ou DL, e seus semelhantes. Conforme ilustra a FIG. 1C, os *eNode-Bs* 160a, 160b, 160c podem ser comunicar uns com os outros através de uma interface X2.

[040]A CN 106 ilustrada na FIG. 1C pode incluir uma entidade de gestão de mobilidade (MME) 162, um *gateway* de serviço (SGW) 164 e um *gateway* de rede de dados em pacotes (PDN) (ou PGW) 166. Embora cada um dos elementos acima seja representado como parte da CN 106, apreciar-se-á que qualquer um deles pode pertencer a e/ou ser operado por uma entidade que não o operador da CN.

[041]A MME 162 pode conectar-se a cada um dos *eNode-Bs* 160a, 160b, 160c na RAN 104 através de uma interface S1 e pode atuar como um nó de controle. Por exemplo, a MME 162 pode ser responsável por autenticar os usuários das WTRUs 102a, 102b, 102c, pela ativação/desativação das portadoras, por selecionar um *gateway* de serviços específico durante uma ligação inicial das WTRUs 102a, 102b, 102c, e seus semelhantes. O MME 162 pode prover uma

função de plano de controle para comutar entre a RAN 104 e outras RANs (não ilustrado) que empregam outras tecnologias de rádio, tais como GSM e/ou WCDMA.

[042]O SGW 164 pode conectar-se a cada um dos *eNode-Bs* 160a, 160b, 160c na RAN 104 através da interface S1. Em termos gerais, o SGW 164 pode rotear e encaminhar pacotes de dados do usuário às/das WTRUs 102a, 102b, 102c. O SGW 164 pode executar outras funções, tais como ancorar planos do usuário durante *handovers* entre *eNode-Bs*, acionar a paginação quando dados de DL estiverem disponíveis para as WTRUs 102a, 102b, 102c, gerir e armazenar contextos das WTRUs 102a, 102b, 102c, e seus semelhantes.

[043]O SGW 164 pode conectar-se ao PGW 166, que pode oferecer às WTRUs 102a, 102b, 102c acesso a redes de pacotes comutados, tais como a Internet 110, para facilitar a comunicação entre as WTRUs 102a, 102b, 102c e dispositivos habilitados para IP.

[044]A CN 106 pode facilitar a comunicação com outras redes. Por exemplo, a CN 106 pode oferecer às WTRUs 102a, 102b, 102c acesso a redes de circuitos comutados, tais como a PSTN 108, para facilitar a comunicação entre as WTRUs 102a, 102b, 102c e dispositivos de comunicação por linha terrestre tradicionais. Por exemplo, a CN 106 pode incluir, ou pode se comunicar com, um *gateway* de IP (por exemplo, um servidor de subsistema multimídia por IP (IMS)) que serve como interface entre a CN 106 e a PSTN 108. Além disso, a CN 106 pode oferecer às WTRUs 102a, 102b, 102c acesso às demais redes 112, que podem incluir outras redes com fio e/ou sem fio que pertencem e/ou são operadas por outros provedores de serviço.

[045]Embora a WTRU seja descrita nas FIGs. de 1A a 1D como um terminal sem fio, contempla-se que, em certas modalidades representativas, esse terminal utilize (por exemplo, temporária ou permanentemente) interfaces de comunicação com fio com a rede de comunicação.

[046]Em modalidades representativas, a outra rede 112 pode ser uma WLAN.

[047]Uma WLAN no modo Conjunto de Serviços Básicos (BSS) pode ter um Ponto de Acesso (AP) para o BSS e uma ou mais estações (STAs) associadas ao AP. O AP pode ter um acesso ao ou uma interface com um Sistema de Distribuição (DS) ou outro tipo de rede com fio/sem fio que transporta tráfego para dentro e/ou para fora do BSS. O tráfego às STAs oriundo de fora do BSS pode chegar através do AP e ser distribuído às STAs. O tráfego oriundo das STAs a destinos fora do BSS pode ser enviado ao AP para ser distribuído aos respectivos destinos. O tráfego entre STAs dentro do BSS pode ser enviado através do AP, por exemplo, a STA de origem pode enviar tráfego ao AP e o AP distribui o tráfego à STA de destino. O tráfego entre STAs dentro de um BSS pode ser considerado e/ou chamado de tráfego ponto a ponto. O tráfego ponto a ponto pode ser enviado entre (por exemplo, diretamente entre) as STAs de origem e destino com uma configuração de enlace direto (DLS). Em certas modalidades representativas, a DLS pode utilizar uma DLS 802.11e ou uma DLS tunelizada (TDLS) 802.11z. Uma WLAN usando um modo de BSS Independente (IBSS) pode ter um AP, e as STAs (por exemplo, todas as STAs) dentro da ou usando o IBSS podem comunicar-se diretamente umas com as outras. O modo de comunicação IBSS pode ser chamado neste documento, por vezes, de um modo de comunicação “*ad-hoc*”.

[048]Ao usar o modo operacional de infraestrutura 802.11ac ou um modo de operações semelhante, o AP pode transmitir um *beacon* por um canal fixo, tal como um canal primário. O canal primário pode ter uma largura fixa (por exemplo, uma largura de banda de 20 MHz) ou uma largura dinamicamente ajustada via sinalização. O canal primário pode ser o canal operacional do BSS e pode ser usado pelas STAs para estabelecer uma conexão com o AP. Em certas modalidades representativas, o Acesso Múltiplo com Detecção de Portadora e Prevenção de

Colisão (CSMA/CA) pode ser implementado, por exemplo, em sistemas 802.11. No caso do CSMA/CA, as STAs (por exemplo, cada STA), incluindo o AP, podem detectar o canal primário. Se o canal primário for detectado/percebido e/ou determinado como ocupado por uma STA específica, a STA específica pode retirar-se. Uma STA (por exemplo, uma única estação) pode transmitir a qualquer dado momento em um dado BSS.

[049]STAs com Alta Taxa de Transmissão Efetiva (HT) podem usar um canal de 40 MHz de largura para comunicação, por exemplo, através de uma combinação do canal de 20 MHz primário com um canal de 20 MHz adjacente ou não adjacente para formar um canal de 40 MHz de largura.

[050]STAs com Taxa de Transferência Efetiva Altíssima (VHT) podem suportar canais de 20 MHz, 40 MHz, 80 MHz e/ou 160 MHz de largura. Os canais de 40 MHz e/ou 80 MHz podem ser formados combinando canais de 20 MHz contíguos. Um canal de 160 MHz pode ser formado combinando 8 canais de 20 MHz contíguos, ou combinando dois canais de 80 MHz não contíguos, o que pode ser chamado de configuração 80+80. Na configuração 80+80, os dados, após a codificação dos canais, podem ser passados através de um analisador de segmentos, que pode dividir os dados em dois fluxos. O processamento por Transformada Rápida Inversa de Fourier (IFFT), e o processamento no domínio tempo, pode ser realizado em cada fluxo separadamente. Os fluxos podem ser mapeados para os dois canais de 80 MHz, e os dados podem ser transmitidos por um STA transmissor. No receptor do STA receptor, a operação descrita acima para a configuração 80+80 pode ser invertida, e os dados combinados podem ser enviados ao Controle de Acesso ao Meio (MAC).

[051]Submodos de operação de 1 GHz são suportados pelo 802.11af e 802.11ah. As larguras de banda operacionais dos canais, e portadoras, são reduzidas no 802.11af e 802.11ah em comparação às usadas no 802.11n e

802.11ac. O 802.11af suporta larguras de banda de 5 MHz, 10 MHz e 20 MHz no espectro de Espaço em Branco de TV (TVWS), e o 802.11ah suporta larguras de banda de 1 MHz, 2 MHz, 4 MHz, 8 MHz e 16 MHz usando um espectro não TVWS. De acordo com uma modalidade representativa, o 802.11ah pode suportar Comunicações de Controle do Tipo Medidor/do Tipo Máquina, tais como dispositivos MTC em uma área de cobertura macro. Os dispositivos MTC podem ter certos recursos, por exemplo, recursos limitados incluindo suporte (por exemplo, suporte somente) a larguras de bandas específicas e/ou limitadas. Os dispositivos MTC podem incluir uma bateria com vida acima de um limite (por exemplo, para manter uma vida de bateria prolongada).

[052]Os sistemas WLAN, que podem suportar vários canais, e larguras de banda dos canais, tais como 802.11n, 802.11ac, 802.11af e 802.11ah, incluem um canal que pode ser designado como o canal primário. O canal primário pode ter uma largura de banda igual à largura de banda operacional comum mais larga suportada por todas as STAs no BSS. A largura de banda do canal primário pode ser definida e/ou limitada por uma STA, dentre todas as STAs em operação em um BSS, que suporta o modo operacional de menor largura de banda. No exemplo de 802.11ah, a canal primário pode ter 1 MHz de largura para STAs (por exemplo, dispositivos do tipo MTC) que suportam (por exemplo, só suportam) um modo de 1 MHz, ainda que o AP e outras STAs no BSS suportem 2 MHz, 4 MHz, 8 MHz, 16 MHz e/ou outros modos operacionais de largura de banda de canal. As configurações de detecção de portadora e/ou Vetor de Alocação de Rede (NAV) podem depender do *status* do canal primário. Se o canal primário estiver ocupado, por exemplo, devido a uma STA (que só suporta um modo operacional de 1 MHz), transmitindo ao AP, todas as bandas de frequência disponíveis podem ser consideradas ocupadas ainda que a maioria delas permaneça ociosa e possa estar disponível.

[053]Nos Estados Unidos, as bandas de frequência disponíveis, que podem ser usadas pelo 802.11ah, são de 902 MHz a 928 MHz. Na Coreia, as bandas de frequência disponíveis são de 917,5 MHz a 923,5 MHz. No Japão, as bandas de frequência disponíveis são de 916,5 MHz a 927,5 MHz. A largura de banda total disponível para o 802.11ah é de 6 MHz a 26 MHz dependendo do código do país.

[054]A FIG. 1D é um diagrama de sistema que ilustra a RAN 113 e a CN 115 de acordo com uma modalidade. Como mencionado acima, a RAN 113 pode empregar tecnologia de rádio NR para se comunicar com as WTRUs 102a, 102b, 102c pela interface aérea 116. A RAN 113 também pode estar em comunicação com a CN 115.

[055]A RAN 113 pode incluir os gNBs 180a, 180b, 180c, embora contemple-se que a RAN 113 pode incluir qualquer número de gNBs e, ainda assim, permanecer consistente com uma modalidade. Cada um dos gNBs 180a, 180b, 180c pode incluir um ou mais transceptores para comunicação com as WTRUs 102a, 102b, 102c pela interface aérea 116. Em uma modalidade, os gNBs 180a, 180b, 180c podem implementar tecnologia MIMO. Por exemplo, os gNBs 180a, 108b podem utilizar formação de feixes para transmitir sinais aos e/ou receber sinais dos gNBs 180a, 180b, 180c. Sendo assim, o gNB 180a, por exemplo, pode utilizar várias antenas para transmitir sinais sem fio à, e/ou receber sinais sem fio da, WTRU 102a. Em uma modalidade, os gNBs 180a, 180b, 180c podem implementar tecnologia de agregação de portadoras. Por exemplo, o gNB 180a pode transmitir várias portadoras componentes às WTRU 102a (não ilustrado). Um subconjunto dessas portadoras componentes pode estar no espectro não licenciado, ao passo que as portadoras componentes remanescentes podem estar no espectro licenciado. Em uma modalidade, os gNBs 180a, 180b, 180c podem implementar tecnologia MultiPonto Coordenada (CoMP). Por exemplo, a WTRU 102a pode receber transmissões coordenadas do gNB 180a e gNB 180b (e/ou gNB 180c).

[056]As WTRUs 102a, 102b, 102c podem se comunicar com os gNBs 180a, 180b, 180c usando transmissões associadas a uma numerologia escalonável. Por exemplo, o espaçamento de símbolos na OFDM e/ou o espaçamento de subportadoras na OFDM podem variar para diferentes transmissões, diferentes células e/ou diferentes porções do espectro de transmissão sem fio. As WTRUs 102a, 102b, 102c podem se comunicar com os gNBs 180a, 180b, 180c usando subquadros ou intervalos de transmissão de tempo (TTIs) de durações variadas ou escalonáveis (por exemplo, contendo um número variável de símbolos de OFDM e/ou durações de tempo absoluto variadas).

[057]Os gNBs 180a, 180b, 180c podem ser configurados para se comunicar com as WTRUs 102a, 102b, 102c em uma configuração autônoma e/ou em uma configuração não autônoma. Na configuração autônoma, as WTRUs 102a, 102b, 102c podem se comunicar com os gNBs 180a, 180b, 180c sem acessar também outras RANs (por exemplo, tal como os *eNode-Bs* 160a, 160b, 160c). Na configuração autônoma, as WTRUs 102a, 102b, 102c podem utilizar um ou mais dos gNBs 180a, 180b, 180c como ponto de âncora de mobilidade. Na configuração autônoma, as WTRUs 102a, 102b, 102c podem ser comunicar com os gNBs 180a, 180b, 180c usando sinais em uma banda não licenciada. Em uma configuração não autônoma, as WTRUs 102a, 102b, 102c podem se comunicar com/conectar aos gNBs 180a, 180b, 180c ao mesmo tempo em que se comunicam com/conectam a outra RAN, tal como os *eNode-Bs* 160a, 160b, 160c. Por exemplo, as WTRUs 102a, 102b, 102c podem implementar princípios de DC para se comunicar com um ou mais gNBs 180a, 180b, 180c e um ou mais *eNode-Bs* 160a, 160b, 160c de maneira substancialmente simultânea. Na configuração não autônoma, os *eNode-Bs* 160a, 160b, 160c podem atuar como uma âncora de mobilidade para as WTRUs 102a, 102b, 102c e os gNBs 180a, 180b, 180c podem oferecer cobertura e/ou taxa de transmissão efetiva adicional para servir as WTRUs 102a, 102b, 102c.

[058]Cada um dos gNBs 180a, 180b, 180c pode ser associado a uma célula específica (não ilustrado) e pode ser configurado para lidar com decisões de gestão de recursos de rádio, decisões de *handover*, agendamento de usuários no UL e/ou DL, suporte de fatiamento de rede, conectividade dupla, interoperação entre NR e E-UTRA, roteamento de dados do plano do usuário à Função de Plano do Usuário (UPF) 184a, 184b, roteamento de informações do plano de controle à Função de Gestão de Acesso e Mobilidade (AMF) 182a, 182b, e seus semelhantes. Conforme ilustra a FIG. 1D, os gNBs 180a, 180b, 180c podem se comunicar uns com os outros através de uma interface Xn.

[059]A CN 115 ilustrada na FIG. 1D pode incluir ao menos uma AMF 182a, 182b, ao menos uma UPF 184a, 184b, ao menos uma Função de Gestão de Sessão (SMF) 183a, 183b e, possivelmente, uma Rede de Dados (DN) 185a, 185b. Embora cada um dos elementos acima seja representado como parte da CN 115, apreciar-se-á que qualquer um deles pode pertencer a e/ou ser operado por uma entidade que não o operador da CN.

[060]A AMF 182a, 182b pode se conectar a um ou mais dos gNBs 180a, 180b, 180c na RAN 113 através de uma interface N2 e pode atuar como um nó de controle. Por exemplo, a AMF 182a, 182b pode ser responsável por autenticar os usuários das WTRUs 102a, 102b, 102c, suportar o fatiamento de rede (por exemplo, manuseio de diferentes sessões de PDU com diferentes necessidades), selecionar uma SMF específica 183a, 183b, gerir a área de registro, interromper a sinalização NAS, gerir a mobilidade, e seus semelhantes. O fatiamento de rede pode ser usado pela AMF 182a, 182b a fim de personalizar o suporte da CN para as WTRUs 102a, 102b, 102c com base nos tipos de serviço sendo utilizados pelas WTRUs 102a, 102b, 102c. Por exemplo, diferentes fatias de rede podem ser estabelecidas para diferentes casos de uso, tais como serviços contando com acesso de baixa latência ultraconfiável (URLLC), serviços contendo com acesso de banda larga móvel

massiva aprimorada (eMBB), serviços para acesso de comunicação do tipo máquina (MTC), e/ou seus semelhantes. A AMF 162 pode oferecer uma função de plano de controle para comutar entre a RAN 113 e outras RANs (não ilustrado) que empregam outras tecnologias de rádio, tais como LTE, LTE-A, LTE-A Pro e/ou tecnologias de acesso não 3GPP, tais como WiFi.

[061]A SMF 183a, 183b pode conectar-se a uma AMF 182a, 182b na CN 115 através de uma interface N11. A SMF 183a, 183b também pode conectar-se a uma UPF 184a, 184b na CN 115 através de uma interface N4. A SMF 183a, 183b pode selecionar e controlar a UPF 184a, 184b e configurar o roteamento do tráfego através da UPF 184a, 184b. A SMF 183a, 183b pode executar outras funções, tais como gerir e alocar o endereço IP do UE, gerir sessões de PDU, controlar o cumprimento das políticas e QoS, prover notificações de dados de enlace descendente, e seus semelhantes. Um tipo de sessão de PDU pode ser baseado no IP, não baseado no IP, baseado em Ethernet, e seus semelhantes.

[062]A UPF 184a, 184b pode conectar-se a um ou mais dos gNBs 180a, 180b, 180c na RAN 113 através de uma interface N3, que pode oferecer às WTRUs 102a, 102b, 102c acesso a redes de pacotes comutados, tais como a Internet 110, para facilitar as comunicações entre as WTRUs 102a, 102b, 102c e dispositivos habilitados para IP. A UPF 184, 184b pode executar outras funções, tais como rotear e encaminhar pacotes, impor políticas do plano do usuário, suportar sessões de PDU multirresidência, gerenciar a QoS do plano do usuário, pré-carregar pacotes de enlace descendente, oferecer ancoragem de mobilidade, e seus semelhantes.

[063]A CN 115 pode facilitar as comunicações com outras redes. Por exemplo, a CN 115 pode incluir, ou pode se comunicar com, um *gateway* de IP (por exemplo, um servidor de subsistema multimídia por IP (IMS)) que serve como interface entre a CN 115 e a PSTN 108. Além disso, a CN 115 pode oferecer às WTRUs 102a, 102b, 102c acesso às demais redes 112, que podem incluir outras

redes com fio e/ou sem fio que pertencem e/ou são operadas por outros provedores de serviço. Em uma modalidade, as WTRUs 102a, 102b, 102c podem conectar-se a uma Rede de Dados (DN) local 185a, 185b através da UPF 184a, 184b via a interface N3 com a UPF 184a, 184b e uma interface N6 entre a UPF 184a, 184b e a DN 185a, 185b.

[064]Em vista às Figuras de 1A a 1D, e à descrição correspondente das Figuras de 1A a 1D, uma ou mais das, ou todas as, funções descritas neste documento com relação a um ou mais dentre: as WTRUs de 102a-d, as Estações de Base de 114a-b, os *eNodes-B* 160a-c, a MME 162, o SGW 164, o PGW 166, os gNBs 180a-c, as AMFs 182a-ab, as UPFs 184a-b, as SMFs 183a-b, as DNs 185a-b, e/ou quaisquer outros um ou mais dispositivos descritos neste documento, podem ser executadas por um ou mais dispositivos de emulação (não ilustrado). Os dispositivos de emulação podem ser um ou mais dispositivos configurados para emular uma ou mais das, ou todas as, funções descritas neste documento. Por exemplo, os dispositivos de emulação podem ser usados para testar outros dispositivos e/ou para simular funções de rede e/ou WTRU.

[065]Os dispositivos de emulação podem ser projetados para implementar um ou mais testes de outros dispositivos em um ambiente de laboratório e/ou em um ambiente de rede do operador. Por exemplo, os um ou mais dispositivos de emulação podem executar as uma ou mais, ou todas, as funções e, ainda assim, ser total ou parcialmente implementados e/ou empregados como parte de uma rede de comunicação com fio e/ou sem fio a fim de testar outros dispositivos dentro da rede de comunicação. Os um ou mais dispositivos de emulação podem executar as uma ou mais, ou todas, as funções e, ao mesmo tempo, ser temporariamente implementados/empregados como parte de uma rede de comunicação com fio e/ou sem fio. O dispositivo de emulação pode ser acoplado diretamente a outro

dispositivo com a finalidade de executar testes e/ou pode executar testes usando comunicação sem fio pelo ar.

[066]Os um ou mais dispositivos de emulação podem executar as uma ou mais, ou todas, as funções e, ao mesmo tempo, não ser implementados/empregados como parte de uma rede de comunicação com fio e/ou sem fio. Por exemplo, os dispositivos de emulação podem ser utilizados em um cenário de teste em um laboratório de teste e/ou uma rede de comunicação com fio e/ou sem fio não empregada (por exemplo, de teste) a fim de implementar os testes de um ou mais componentes. Os um ou mais dispositivos de emulação podem ser equipamentos de teste. O acoplamento por RF direta e/ou comunicação sem fio através de um sistema de circuitos de RF (por exemplo, que pode incluir uma ou mais antenas) pode ser usado pelos dispositivos de emulação para transmitir e/ou receber dados.

[067]Conforme usado neste documento, uma WTRU pode rodar um ou mais aplicativos V2X. As WTRUs de origem são chamadas intercambiavelmente de WTRUs requerentes, e as WTRUs alvo são chamadas intercambiavelmente de WTRUs de destino ou WTRUs ponto neste documento.

[068]Em um exemplo de arquitetura V2X, um Servidor de Aplicativo V2X (AS) pode estar localizado na rede e pode fazer interface com aplicativos V2X instalados nas WTRUs (isto é, dispositivos V2X neste contexto). Uma Função de Controle V2X (CF) pode manejar a autorização ou aprovisionamento para os dispositivos V2X (isto é, configurações de política e parâmetros V2X às WTRUs). A função de controle (CF) V2X pode estar localizada na CN 5G e ser tida como parte da arquitetura baseada em serviço. A comunicação V2X de WTRU com WTRU pode basear-se em dois modos de operação. Em um primeiro modo, a comunicação V2X de WTRU com WTRU pode ocorrer através de uma interface LTE-Uu. Em um segundo modo, a comunicação V2X de WTRU com WTRU pode ocorrer através de

uma interface PC5 (por exemplo, *sidelink* ou Serviços à base de Proximidade (ProSe) V2X).

[069]A comunicação V2X através de um ponto de referência PC5 é um tipo de comunicação direta ProSe. A comunicação direta ProSe de um a um pode ser realizada estabelecendo um enlace de camada 2 (L2) seguro através de PC5 entre duas WTRUs. A WTRU iniciadora tentando estabelecer o enlace deve ter a identificação (ID) de L2 tanto para si quanto para a WTRU ponto (alvo). O ID de L2 da WTRU alvo pode ser pré-configurado na WTRU iniciadora ou pode ser obtido via Descoberta Direta ProSe. A WTRU iniciadora pode iniciar a configuração de enlace direto gerando uma mensagem de Sinalização PC5 (por exemplo, uma mensagem DIRECT_COMMUNICATION_REQUEST). A mensagem pode incluir: 1) um conjunto de informações do usuário 2) um elemento informativo (IE) de configuração de endereço IP 3) um IE de endereço IPv6 local de enlace e 4) um IE de máximo período de inatividade. Se a WTRU alvo receber a mensagem da WTRU iniciadora (por exemplo, uma mensagem DIRECT_COMMUNICATION_REQUEST), ela armazenará o par dos IDs de L2 e associá-los-á ao enlace direto no contexto. Após a conclusão do procedimento de autenticação de enlace e do estabelecimento bem-sucedido da associação de segurança, a WTRU alvo envia uma mensagem (por exemplo, uma mensagem DIRECT_COMMUNICATION_ACCEPT) à WTRU iniciadora. Após receber a mensagem de Sinalização PC5 advinda da WTRU alvo (por exemplo, a mensagem DIRECT_COMMUNICATION_ACCEPT), a WTRU iniciadora utiliza o enlace estabelecido para todas as comunicações de um a um com a WTRU alvo.

[070]Cada WTRU pode ter um ID de L2 para comunicação *unicast* que é incluído no campo ID de L2 de Origem de cada quadro que envia no enlace L2 e no ID de L2 de Destino de cada quadro que recebe no enlace L2.

[071]O protocolo de sinalização PC5 suporta a funcionalidade *keep-alive*, que pode ser usada para detectar se as WTRUs não estão na faixa de Comunicação ProSe, por exemplo, de modo que possam prosseguir com a liberação implícita do enlace L2. A WTRU requerente pode iniciar um procedimento *keep-alive*, por exemplo, se (1) um pedido advindo de camadas superiores para verificar a viabilidade do enlace direto for recebido; ou (2) um temporizador *keep-alive* para o enlace direto expirar.

[072]O ID de L2 de origem pode ser mudado com o tempo e randomizado para fins de segurança; por exemplo, para evitar o rastreio e/ou a identificação da WTRU de origem (por exemplo, um veículo) por quaisquer outras WTRUs (por exemplo, outros veículos) além de um certo curto período de tempo exigido pela aplicação. Isso aplica-se tanto às WTRUs quanto aos identificadores associados à sessão, isto é, tanto à origem quanto ao destino.

[073]Algumas implementações oferecem um Identificador de Associação de Segurança e Sessão (ID $K_{D\text{-}sess}$). Durante o estabelecimento do enlace, uma associação de segurança pode ser criada entre as WTRUs ponto para garantir o enlace (isto é, para facilitar a confidencialidade e proteção à integridade). Cada WTRU ponto mantém localmente um contexto de segurança contendo chaves para criptografar/descriptografar mensagens e para proteger a integridade delas. Esse contexto de segurança é associado a esse enlace de ponto a ponto específico. Um identificador de associação segurança para o enlace específico (que pode ser chamado de ID $K_{D\text{-}sess}$) pode ser usado por cada WTRU ponto para identificar e recuperar o contexto de segurança e/ou as chaves se uma mensagem for recebida (por exemplo, para verificar a integridade da mensagem e/ou descriptografá-la) ou se for preciso enviar uma mensagem (por exemplo, para criptografar a mensagem e/ou proteger sua integridade). O identificador de sessão (isto é, ID $K_{D\text{-}sess}$) é criado concatenando os componentes do identificador de cada ponto, isto é, o byte mais

significativo (MSB) (isto é, os 8 bits mais significativos) do ID $K_{D\text{-}sess}$ vem da WTRU iniciadora e o byte menos significativo (LSB) (isto é, os 8 bits menos significativos) do ID $K_{D\text{-}sess}$ vem da WTRU ponto. Cada WTRU utiliza sua porção do ID $K_{D\text{-}sess}$ (isto é, MSB ou LSB) para recuperar o contexto de segurança associado ao enlace.

[074]A FIG. 2 ilustra um exemplo 200 de cabeçalho de Protocolo de Convergência de Dados em Pacotes (PDCP) para comunicações de um a um. Conforme ilustra a FIG. 2, o identificador de sessão 201 (isto é, ID $K_{D\text{-}sess}$) é transmitido com cada pacote como parte do cabeçalho de PDCP junto com um contador 202 que representa o número de pacotes trocados desde o estabelecimento do contexto de segurança. Também são incluídas no PDCP uma porção de Carga 203, que é opcionalmente cifrada, e uma porção de Código de Autenticação de Mensagem (MAC) 204 quando necessário.

[075]O V2X Aprimorado (eV2X) pode suportar *unicast*/*multicast* por PC5 para comunicação eV2X. Além do mecanismo de difusão, o eV2X pode suportar um novo mecanismo de distribuição interativo para lidar com o compartilhamento de dados a alta taxa de dados entre veículos, por exemplo, usando *unicast* e/ou *multicast*. Esses mecanismos podem utilizar uma sessão de longa duração usando o mesmo ID de L2 de origem. Isso pode criar um problema de privacidade se o ID de L2 de origem for rastreado e enlaçado. Esses problemas de privacidade afetariam a ambos os usuários, isto é, tanto a WTRU de origem quanto a WTRU alvo.

[076]Logo, pode ser desejável mudar o ID de L2 de origem enquanto a sessão ainda está em andamento (por exemplo, periódica ou aleatoriamente). No entanto, se o ID de L2 de origem for mudado na WTRU de origem, a WTRU ponto precisa ser informada porque a sessão em andamento é identificada pelo ID de L2 de origem. Os mecanismos ProSe atuais não suportam a modificação do ID de L2 de origem em uma sessão em andamento. Além disso, a mudança do ID de L2 pode introduzir outros problemas. Por exemplo, uma WTRU com várias sessões e usando

o mesmo ID de L2 deve atualizar todas as suas sessões/pontos ao mesmo tempo (ou dentro de um período de tempo definido, por exemplo, curto). Também pode se fazer necessário que a WTRU atualize os IDs de L2 para cada sessão. Para cada sessão, a WTRU precisa continuar recebendo tráfego em seu ID de L2 antigo até que a mudança do ID de L2 seja confirmada por sua WTRU ponto. Esses requisitos podem gerar ou exigir procedimentos ineficientes, e têm potencial para gerar uma pluralidade de trocas de mensagens, por exemplo, porque todas as WTRUs nesse exemplo devem mudar periodicamente seus IDs de L2.

[077]Também pode ser necessário tratar da privacidade do ID de contexto de segurança. Em algumas implementações, o ID de contexto de segurança (ID $K_{D\text{-}sess}$), transmitido no cabeçalho de PDCP, pode ser usado por um espião para detectar indiretamente que o ID de L2 antigo (por exemplo, o ID de L2 de origem ou destino) foi mudado para um novo ID de L2, se o mesmo ID $K_{D\text{-}sess}$ for usado antes e durante e/ou depois do procedimento de mudança do ID de L2.

[078]Pode ser desejável, para fins de privacidade ou para outros fins de segurança da comunicação, que a WTRU de origem impeça que seus IDs de L2 antigo e novo sejam concatenados por um espião durante a comunicação da mudança de seu ID de L2 à sua WTRU ponto.

[079]Novos procedimentos são tipicamente descritos neste documento com referência à WTRU de origem e ao ID de origem, porém note-se que cada uma das WTRUs de origem e alvo envolvidas em uma comunicação pode assumir a função da origem e/ou alvo, dependendo de qual ponto está iniciando um intercâmbio específico. Neste documento, são discutidos vários métodos, sistemas e dispositivos que facilitam a modificação dos IDs de L2 de origem e alvo associados a uma sessão em andamento. A sessão pode ser uma sessão *unicast* ou *multicast* que é usada por certo período de tempo que é longo o bastante para permitir uma ameaça de rastreio em potencial. Esse período pode ser determinado de maneira arbitrária,

empírica ou de qualquer outra maneira. O período pode depender do aplicativo usando-o; por exemplo, um aplicativo que transmite informações por mais de uma quantidade de tempo limite. Note-se que V2X, conforme usado neste documento, serve como um exemplo de comunicação direta de WTRU com WTRU (por exemplo, utilizando uma interface PC5 ProSe). Ele também pode aplicar-se a outros tipos de comunicação de WTRU com WTRU (por exemplo, *drones* etc.).

[080]Por exemplo, uma WTRU pode ser aprovisionada com um novo intervalo de tempo (por exemplo, temporizador de privacidade) que pode ser ajustado para o tempo de vida de seu ID de L2 para comunicações *unicast* e pode incluir parâmetros de proteção à privacidade. Esses parâmetros também podem ser a saída de uma função (por exemplo, uma função pseudoaleatória). De acordo com esse intervalo de tempo, o ID de L2 da WTRU deve ser mudado (e randomizado) dentro do intervalo de tempo especificado, se a sessão ainda estiver em andamento. Depois de mudar o ID, o temporizador pode ser reiniciado para que o ID de L2 seja mudado novamente dentro desse período de tempo específico. Esse processo pode ser repetido pelo tempo que a sessão estiver em andamento.

[081]Conforme discutido mais acima, a mudança do ID de L2 de uma das ou ambas as WTRUs (isto é, de uma ou ambas a origem e o alvo) precisa ser comunicada à(s) outra(s) WTRU(s) que participa(m) da comunicação. As WTRUs também precisam ser notificadas do valor do novo ID de L2. Além disso, a WTRU de origem pode atualizar seu contexto de segurança e ID de contexto de segurança (ID $K_{D\text{-}sess}$) com sua WTRU ponto durante o procedimento usado para atualizar seu ID de L2. Inversamente, a WTRU de origem pode atualizar seu ID de L2 durante o procedimento usado para atualizar seu contexto de segurança (por exemplo, procedimento de Rechaveamento de Enlace Direto). Visto que a sessão envolve duas WTRUs (isto é, origem e alvo) e dois IDs de L2, ambos os IDs de L2 precisam ser mudados simultaneamente, e cada WTRU precisa ser informada quando a outra

WTRU estiver mudando seu ID de L2. Os novos IDs de L2 de origem e alvo associados à sessão em andamento podem ser mudados independentemente, isto é, um depois do outro, ou ao mesmo tempo, ou durante o mesmo procedimento.

[082]Em alguns exemplos, mais de um evento pode desencadear a regeneração e atualização do ID de L2 junto à WTRU ponto. Por exemplo, a expiração de um temporizador, o recebimento de um novo valor de ID de L2 a partir da WTRU ponto, a atualização de um identificador de aplicativo associado, um pedido da WTRU ponto, uma mudança de contexto de comunicação ou outros eventos podem desencadear a regeneração e atualização do ID de L2. Uma vista de alto nível e métodos exemplificativos descritos abaixo são detalhados com base em um temporizador de privacidade, à guisa de exemplo, contudo deve-se ter em mente que qualquer um dos disparadores discutidos acima, ou qualquer outro disparador adequado, pode aplicar-se.

[083]Em alguns exemplos, uma WTRU “relé” pode ser usada entre a WTRU de origem e a WTRU alvo. Esse "relé" não é ilustrado nem discutido nas várias figuras e descrição neste documento. No entanto, os mesmos procedimentos conforme descritos nas subseções a seguir podem ser aplicados a comunicações envolvendo uma WTRU relé, o relé sendo usado somente para transferir (por exemplo, “transparentemente”) mensagens entre as WTRUs de origem e alvo.

[084]Conforme discutido acima, em algumas implementações, uma WTRU com várias sessões, que utilizam o mesmo ID de L2, deve atualizar todas as suas sessões/pontos ao mesmo tempo (ou dentro de um período de tempo definido, por exemplo, curto). Em algumas implementações, para cada sessão, a WTRU precisa manter-se recebendo tráfego em seu ID de L2 antigo até que a mudança do ID de L2 seja confirmada por sua WTRU ponto. Isso pode tornar o mecanismo de mudança do ID de L2 ineficiente e tem potencial para gerar uma pluralidade de trocas de mensagens, por exemplo, porque todas as WTRUs devem mudar

periodicamente seus IDs de L2. Logo, para simplificar o procedimento de atualização do ID de L2 e eliminar ou reduzir os impactos sobre outras sessões, é revelado neste documento que, em algumas implementações, uma WTRU implementando suporte de privacidade pode usar um ID de L2 diferente por sessão. Em outras palavras, nessa implementação recém-revelada, toda sessão *unicast* com WTRUs ponto diferentes utilizaria um ID de L2 de origem diferente. Além disso, cada sessão com a mesma WTRU ponto pode ser associada a só um aplicativo. Além disso, vários aplicativos rodando na WTRU de origem/alvo também podem todos utilizar sessões distintas.

[085]A FIG. 3 é um diagrama de sequência 300 que ilustra uma vista de alto nível de um exemplo de mudança do ID de L2 da WTRU de origem/requerente 380 e, como opção, mudança do ID de L2 da WTRU de destino/ponto/alvo 390, que podem ocorrer ao mesmo tempo.

[086]No bloco de referência 301 da FIG. 3, as WTRUs são aprovisionados com parâmetros de privacidade específicos, por exemplo, um valor de temporizador de privacidade, um valor de semente para gerar o ID de L2, um valor de semente para gerar o temporizador de privacidade, e assim por diante. Também são aprovisionadas políticas de privacidade que indicam quais métodos podem ser usados para uma única WTRU ou para ambas as WTRUs, por exemplo, privacidade habilitada/desabilitada, privacidade somente por ID de L2, privacidade por ID de L2 + ID $K_{D\text{-}sess}$ etc. Essas informações aprovisionadas podem ser fornecidas pela Função de Controle (CF) V2X ou servidor de aplicativo (AS) V2X, ou os parâmetros podem ser pré-provisionados na WTRU (por exemplo, ou no equipamento móvel (ME) ou em um cartão de circuito integrado universal (UICC)). Esses parâmetros podem ser aprovisionados por WTRU (por exemplo, para uso em toda comunicação direta ProSe/V2X para uma WTRU específica) ou por ID de aplicativo V2X (por exemplo, identificador de aplicativo de sistemas inteligentes de transporte (ITS-AID) ou

identificador de serviço do provedor (PSID)) (por exemplo, para uso em toda comunicação direta ProSe/V2X para um aplicativo V2X específico). No bloco de referência 302 da FIG. 3, é estabelecida a comunicação PC5 entre uma WTRU de origem e uma WTRU ponto (chamadas de UEs na FIG. 3). A WTRU ponto pode ser aprovisionada com parâmetros de privacidade específicos (conforme descrito acima) da WTRU de origem, por exemplo, durante o estabelecimento da sessão (e vice-versa). As política de privacidade recebidas na WTRU ponto podem ser comparadas às políticas aprovisionadas da WTRU ponto, e o método de proteção à privacidade que satisfizer a classe mais alta pode ser selecionado. A WTRU de origem pode ser aprovisionada com parâmetros de privacidade específicos (conforme descrito acima) da WTRU ponto, por exemplo, durante o estabelecimento do enlace. Os blocos 301 e 302 da FIG. 3 representam um procedimento de configuração para comunicações PC5.

[087]Nos blocos 303 A e 303 B da FIG. 3, um temporizador de privacidade é iniciado na WTRU de origem (e, como opção, na WTRU ponto). No bloco 304 da FIG. 3, a comunicação entre a WTRU de origem e a WTRU ponto usando o ID de L2 #1 (e o ID de L2 #1) e o ID de $K_{D\text{-}sess}$ #1 está em andamento. Nos blocos 305 A e 305 B da FIG. 3, o temporizador de privacidade expira. No bloco 305 A1, a WTRU de origem 380 aplica a política de privacidade selecionada para a sessão em andamento (supondo-se aqui que a política selecionada para a aplicação é a privacidade por ID de L2 + ID de $K_{D\text{-}sess}$ em ambos os lados): a WTRU de origem gera um novo ID de L2 de origem (por exemplo, ID de L2 de origem #2) ou o obtém por outros meios, por exemplo, a partir da camada superior, e uma nova porção do ID de sessão (por exemplo, MSB do ID de $K_{D\text{-}sess}$ #2). O novo ID de L2 e o novo MSB do ID de $K_{D\text{-}sess}$ #2 são associados ao ID de L2 de origem atual e ao MSB atual do ID de $K_{D\text{-}sess}$ usados para esta sessão e salvos localmente com o ID existente. Esse ID de L2 de origem existente (ID de L2 de origem #1) e possivelmente ID de

sessão (ID de $K_{D\text{-}sess}$ #1) ainda são usados a esse tempo para identificar a sessão em andamento. A WTRU de origem envia o novo ID de L2 de origem, em um novo IE do ID de L2, e possivelmente o novo MSB do ID de $K_{D\text{-}sess}$ em um novo MSB do IE do ID de sessão, à WTRU ponto (por exemplo, usando um dos métodos descritos neste documento), ou a própria WTRU ponto regenera um ID de L2 de origem idêntico ao obtido na WTRU de origem (por exemplo, usando um método descrito neste documento). Note-se que, nesse último caso, o ID de $K_{D\text{-}sess}$ não precisa ser atualizado uma vez que nenhuma mensagem de privacidade é trocada entre as WTRUs ponto. Em algumas implementações, as mesmas etapas podem ser executadas em ambas as WTRUs ao mesmo tempo a fim de mudar o ID de L2, e potencialmente o ID de sessão, durante o mesmo procedimento. O temporizador de privacidade é só um exemplo de disparador para mudar o ID de L2 e o ID de sessão. O ID de L2 e o ID de sessão também podem ser gerados e subsequentemente comunicados à outra WTRU, por exemplo, se a WTRU receber um novo ID de L2 de origem da WTRU ponto, por exemplo, conforme descrito neste documento; se as camadas superiores ou uma camada de aplicativo disparar o procedimento de privacidade; se a WTRU mover-se a uma nova área geográfica; se a WTRU receber novos parâmetros e/ou políticas de privacidade advindos da função de controle (CF) V2X ou do servidor de aplicativo (AS) V2X; ou quando o UE receber um pedido feito por seu ponto para disparar o procedimento de privacidade, por exemplo, conforme descrito neste documento.

[088]Em algumas implementações, caso a camada V2X seja provocada a mudar seu ID de L2, por exemplo, pelo temporizador, por um pedido feito pelo ponto etc., a camada V2X informa/comunica a camada superior sobre a mudança de identidade iminente, por exemplo, para fins de sincronização. A camada superior pode responder com uma nova identidade de camada superior, que pode ser enviada junto com o novo ID de L2 à WTRU ponto. Em algumas implementações, a

interface entre a camada V2X e a camada superior é aprimorada para permitir que essa informação seja transmitida; por exemplo, por uma indicação da camada V2X ao aplicativo e uma reposta do aplicativo à camada V2X.

[089]Nos blocos 306 A e 306 B, um novo ID de L2 de origem (e opcionalmente ponto) e ID de sessão são sincronizados/comunicados de uma camada à outra em ambas as WTRUs para a comunicação PC5. Essa sincronização/comunicação é essencialmente uma comunicação entre camadas (por exemplo, componentes e/ou instâncias e/ou funções) das porções de aplicativo V2X, não importa onde estejam localizadas, para garantir que todos esses componentes (*hardware* e/ou *software*) que contam com informações de ID de L2 atualizadas sejam atualizados com os valores mais recentes. A camada superior pode estar ciente de qual ID de L2 é usada e com uma camada AS que utiliza o ID de L2 para a comunicação PC5. Depois que o novo ID de L2 de origem é sincronizado/comunicado, o novo ID de L2 de origem (#2), e possivelmente ID de sessão (por exemplo, ID de $K_{D\text{-}sess}$ #2), é usado para a sessão em andamento. Se um novo ID de L2 ponto #2 for sincronizado, ele também será usado para a sessão em andamento, como no bloco 306 A1. Nos blocos 307 A e 307 B, o temporizador de privacidade é reiniciado na WTRU de origem (e opcionalmente na WTRU ponto).

[090]Algumas abordagens para atualizar os IDs de L2 e ID de sessão associados a uma sessão em andamento (por exemplo, bloco 305 A1 ilustrado e descrito com relação à FIG. 3) incluem o seguinte e são detalhadas mais adiante neste documento.

[091]Em um novo primeiro método (Método 1), alguns exemplos incluem um intercâmbio de novos IDs de L2 entre as WTRUs de origem e alvo. Esses exemplos podem incluir a modificação de uma mensagem existente (por exemplo, mensagens *keep-alive* ProSe) para portar o novo ID de L2 de origem; por exemplo, para suportar o intercâmbio concomitante dos novos IDs de L2 de origem e ponto. Em uma

extensão adicional do Método 1, chamada de Método 3 abaixo, um intercâmbio do novo MSB do ID de $K_{D\text{-}sess}$ e LSB do ID de $K_{D\text{-}sess}$, bem como um intercâmbio dos novos IDs de L2 para as WTRUs de origem e ponto, pode ser suportado. Esses exemplos e extensões com base no Método 1 podem em aditamento, ou como alternativa, incluir a introdução de novas mensagens primárias e procedimentos para portar o novo ID de L2 de origem, por exemplo, para suportar o intercâmbio concomitante dos novos IDs de L2 de origem e ponto, e/ou para suportar o intercâmbio do novo MSB do ID de $K_{D\text{-}sess}$ e LSB do ID de $K_{D\text{-}sess}$ para um novo ID de sessão. Em alguns exemplos, uma WTRU pode solicitar seu ponto a mudar seu ID de L2, o que pode ser chamado de disparo do ponto. Alguns exemplos modificam as mensagens de rechaveamento existentes para suportar o intercâmbio concomitante de novos IDs de L2 de origem e ponto.

[092]Em um novo segundo método (Método 2), alguns exemplos incluem a geração de um novo ID de L2 do ponto. Nesses exemplos, uma semente de origem pode ser fornecida a uma WTRU alvo e uma semente alvo pode ser fornecida à WTRU de origem. Esses exemplos podem incluir a modificação de uma mensagem existente (por exemplo, uma mensagem *keep-alive* ProSe ou mensagens de estabelecimento de enlace direto PC5) para configurar a semente para uso na regeneração do ID de L2 na WTRU ponto. Esses exemplos podem incluir em aditamento, ou como alternativa, a introdução de uma nova mensagem de privacidade para o intercâmbio da semente ou sementes. Esses exemplos também podem em aditamento, ou como alternativa, atualizar quaisquer mensagens de sinalização PC5 para portar a “semente”.

[093]Em um terceiro método (Método 3), brevemente descrito acima, o Método 1, também introduzido acima, pode ser ampliado com o intercâmbio de novos IDs de sessão para maior proteção à privacidade. Em um quarto método (Método 4), um procedimento de rechaveamento existente que também produz um

novo ID de sessão pode ser aprimorado com o intercâmbio de novos IDs de L2 entre WTRUs em comunicação.

[094]Alguns exemplos descritos neste documento incluem o aprovisionamento de parâmetros e/ou políticas de privacidade à WTRU de origem e WTRU ponto; por exemplo, usando o procedimento de Atualização de Configuração (UCU) da WTRU (ou UE) e/ou durante a configuração do enlace PC5.

[095]Alguns exemplos incluem o aprovisionamento de parâmetros de privacidade. Por exemplo, o aprovisionamento e procedimentos de configuração de enlace PC5 podem ser modificados para suportar um procedimento de privacidade. Em alguns exemplos, a WTRU (origem ou alvo ou ambas) é aprovisionada com um novo valor de temporizador de privacidade e outros parâmetros, conforme descrito, usando o mesmo mecanismo usado para o aprovisionamento de eV2X, por exemplo, através de um procedimento UCU usando um recipiente transparente de estrato sem acesso (NAS), ou uma interface V3, ou um Servidor de App V2X. Uma configuração de valor 0 pode desativar o procedimento de regeneração do ID de L2 de origem Se nenhum aprovisionamento for obtido, utiliza-se um valor padrão.

[096]A WTRU também pode ser aprovisionada com uma nova política de privacidade para uso pela WTRU para determinar seu comportamento relacionado à proteção à privacidade. A política de privacidade pode ser especificada por Aplicativo V2X (por exemplo, Sistema Inteligente de Transporte-AID (ITS-AID) ou Identificador de Serviço do Provedor (PSID)). A política de privacidade pode especificar, por exemplo, os Métodos de Proteção à Privacidade (PPM) que são suportados e podem ser identificados por preferência. Por exemplo, os valores a seguir podem existir: PPM 1: desativado - sem manejo de privacidade; PPM 2; privacidade só por ID de L2 usando o Método 1, atualização do ID de L2 de só um UE; PPM 3: privacidade só por ID de L2 usando o Método 1, atualização do ID de L2 de ambos os UEs; PPM 4: privacidade só por ID de L2 usando o Método 2,

atualização do ID de L2 de ambos os UEs; PPM 5: privacidade por ID de L2 + ID de sessão usando o Método 3; PPM 6: privacidade por ID de L2 + ID de sessão usando o Método 4; e/ou outros valores adequados.

[097]A FIG. 4 é um diagrama de sequência 400 que ilustra um exemplo de aprovisionamento de parâmetros de privacidade. Na mensagem 401, a Função de Controle V2X (V2X) ou Função de Controle de Políticas (PCF) 440 encaminha os parâmetros de aprovisionamento eV2X à AMF 430 em um recipiente de políticas para configurar a WTRU (indicada na FIG. 4 por UE 410). Novos parâmetros eV2X específicos para o suporte de privacidade (por exemplo, temporizador de privacidade, valor de semente para gerar o ID de L2, valor de semente para gerar o temporizador de privacidade, e assim por diante) são adicionados ao recipiente de políticas com os parâmetros existentes. Uma política de privacidade também pode ser especificada. Na mensagem 402, a AMF transfere o recipiente de políticas de WTRU à WTRU usando a (R)AN 420. Essa transferência pode ser considerada "transparente" porque a AMF transfere o recipiente de políticas de WTRU à WTRU sem lê-las ou alterá-las. Os parâmetros eV2X são salvos localmente no UE no bloco 402 A. Na mensagem 403, a WTRU envia o resultado da distribuição das políticas de WTRU à AMF. Na mensagem 404, a AMF notifica a CF ou PCF V2X caso tenha-se registrado que ela seja notificada sobre o recebimento do recipiente de políticas de WTRU.

[098]Alguns exemplos de procedimentos de privacidade incluem um procedimento de estabelecimento de enlace direto atualizado com parâmetros de privacidade. Em alguns exemplos, um procedimento de estabelecimento de enlace direto é usado para indicar à outra WTRU que a sessão atual requer uma mudança do ID de L2 durante uma sessão de PC5 em andamento. Isso pode ser obtido, por exemplo, ou incluindo uma nova indicação na mensagem de pedido de comunicação direta e/ou passando o valor de temporizador de privacidade de uma WTRU à outra.

Um novo IE do temporizador de privacidade contendo o valor de temporizador de privacidade pode ser introduzido para essa finalidade. Um novo IE de indicação de privacidade também pode ser introduzido e pode ser ajustado para o(s) valor(es) aprovisionado(s), por exemplo, PPM 2, PPM 3, PPM 4 (conforme descrito acima). A seleção do PPM podem ser negociada entre as duas WTRUs durante o estabelecimento do enlace. Por exemplo, a proteção à privacidade mais alta suportada por ambos os lados pode ser selecionada. Por exemplo, o PPM 2, PPM 3 e PPM 4 podem ser suportados pela WTRU originária e só o PPM 2 e PPM 3 ser suportados na WTRU ponto. Sendo assim, o PPM 3 (por exemplo, privacidade só por ID de L2 usando o método 1, atualização do ID de L2 de ambas as WTRUs) é selecionado para essa sessão específica. O PPM selecionado determina como as WTRUs se comportarão durante a duração da sessão; isto é, determina se a proteção à privacidade é aplicada, qual método é usado, se ambos os pontos atualizam seu ID de L2, se o ID de sessão é atualizado etc. Em dada WTRU, diferentes PPMs podem ser selecionados para diferentes sessões com base nas políticas de privacidade aprovisionadas e no processo de negociação acima. Por exemplo, uma WTRU pode estabelecer duas sessões com outra WTRU e pode selecionar um PPM diferente para cada sessão (por exemplo, onde cada sessão é associada a um aplicativo V2X diferente e cada aplicativo portando sua política de privacidade específica). A WTRU ponto pode rejeitar o estabelecimento do enlace se não for identificado nenhum PPM aceitável (por exemplo, em comum) com base nos valores aprovisionados e nos valores propostos pela WTRU originária.

[099]A FIG. 5 é um diagrama de sequência 500 que ilustra um exemplo de um procedimento de estabelecimento de enlace direto desse tipo. A mensagem 501 é um pedido de comunicação direta, enviado a partir de uma WTRU requerente ou de origem 510 a uma WTRU destino ou alvo ou ponto 520, que pode incluir uma indicação de privacidade, o temporizador de privacidade da WTRU de origem e/ou

políticas de privacidade suportadas. A mensagem 502 é uma comunicação direta enviada em resposta à mensagem de pedido de uma WTRU de destino ou alvo ou ponto 520 a uma WTRU requerente ou origem 510, a qual confirma a indicação de privacidade, o temporizador de privacidade da WTRU de origem e/ou as políticas de privacidade suportadas enviadas na mensagem de pedido. Em alguns exemplos, o valor de temporizador de privacidade é passado à outra WTRU para informá-la de antemão que o ID de L2 mudará durante o tempo de vida da sessão; por exemplo, periodicamente. A WTRU que recebe uma configuração de temporizador de privacidade de seu ponto pode esperar a mudança dentro do tempo especificado pelo valor de temporizador de privacidade. Se a mudança não ocorrer dentro desse período, a WTRU receptora pode disparar a substituição desse ID; por exemplo, usando o procedimento de privacidade ilustrado e descrito com relação à FIG. 9.

[0100]Um exemplo de Método 1 mencionado acima será agora descrito. Alguns exemplos do Método 1 incluem o intercâmbio de novos identificadores de L2. Em alguns exemplos, as WTRUs trocam seu novo ID de L2 entre si durante o mesmo procedimento, ou independentemente, uma depois da outra. O valor de temporizador de privacidade também pode ser atualizado usando esse procedimento.

[0101]Em alguns exemplos, um procedimento *keep-alive* de enlace direto ProSe é atualizado com um novo ID de L2 de origem. O procedimento *keep-alive* de enlace direto ProSe pode ser reutilizado para mudar os IDs de L2 associados a uma sessão em andamento. Novos IEs do ID de L2 podem ser introduzidos. Mensagens *keep-alive* existentes podem incluir os novos IEs do ID de L2, que podem ser ajustados para os novos valores de ID de L2 de origem/alvo. Um novo valor de temporizador de privacidade pode ser aprovisionado na WTRU (por exemplo, conforme ilustrado e descrito com relação à FIG. 4) e pode ser usado como um novo

disparador (a) para a geração do novo ID de L2 e (b) para dar início ao procedimento *keep-alive*, que pode incluir o IE do ID de L2 recém-obtido.

[0102]A FIG. 6 é um diagrama de sequência 600 que ilustra um exemplo de intercâmbio de novos identificadores de L2 em uma WTRU requerente ou origem 610 usando um procedimento *keep-alive* de enlace direto atualizado, disparado pela expiração do temporizador de privacidade, para atualizar o ID de L2 de Origem de uma sessão existente na WTRU ponto 620. A FIG. 6 representa um exemplo de Método 1 onde só o ID de L2 de origem é mudado. Note-se que o procedimento e mensagens *keep-alive* são usados para fins de conveniência para descrever e ilustrar o intercâmbio do novo ID de L2 de origem. No entanto, outras mensagens e procedimentos de sinalização PC5 podem ser modificados de uma maneira semelhante e usados para atingir o mesmo resultado. No bloco 601, parâmetros V2X são aprovisionados nas WTRUs 610 e 620 e uma sessão é estabelecida. No bloco 602, a WTRU de origem 610 opera um temporizador de privacidade usando o valor provisionado. No bloco 603, a comunicação usando o ID de L2 de Origem #1 (e ID de L2 ponto) está em andamento. No bloco 604, o temporizador de privacidade na WTRU de origem 610 expira, e o ID de L2 de origem precisa ser atualizado. No bloco 604 A, é gerado um novo ID de L2 de origem (por exemplo, ID de L2 de origem #2). No bloco 604 B, a WTRU de origem inicia o procedimento *keep-alive* para enviar o novo ID à WTRU ponto. A WTRU de origem envia à WTRU ponto uma mensagem *keep-alive* 630 contendo o novo ID de L2 de Origem em um novo IE (por exemplo, Source_L2_ID_IE). O ID de L2 de origem atual ainda é usado porque ele é o ID associado à sessão nesse momento e ele é o ID que o ponto conhece/espera que seja usado. Um novo valor de temporizador de privacidade também pode ser configurado na WTRU ponto. A WTRU ponto recebe o novo ID de L2 de origem associado à sessão e salva-o localmente. Ambos os IDs de L2 (anterior e novo) podem ser salvos localmente caso mensagens usando o ID anterior estejam em

trânsito durante o procedimento de modificação do ID. A WTRU ponto interrompe o temporizador *keep-alive* no bloco 640 e envia uma mensagem de confirmação *keep-alive* 650 incluindo o novo IE do ID de L2 de origem (por exemplo, Source_L2_ID_IE) definido com o mesmo valor que o recebido na mensagem *keep-alive*. O ID de L2 anterior continua sendo usado como o ID de destino para essa mensagem. O ID de L2 de origem antigo pode ser excluído da memória local após a mensagem usando o novo ID de L2 ser recebida ou, por exemplo, após um período de tolerância. Na etapa 4c, o temporizador *keep-alive* é reiniciado de ambos os lados. Nos blocos 605 A e 605 B, um novo ID de L2 de origem é sincronizado/comunicado de uma camada à outra em ambas as WTRUs para a comunicação PC5 (por exemplo, com a camada superior ciente de qual ID de WTRU é usado e com uma camada AS que utiliza o ID de L2 para comunicação PC5). No bloco 606, a WTRU de origem reinicia o temporizador de privacidade porque o ID de L2 de origem precisa ser mudado periodicamente. No bloco 607, o novo ID de L2 de origem é usado daqui em diante, de ambos os lados.

[0103]Em alguns exemplos, ambas as WTRUs atualizam seus IDs de L2 durante o mesmo procedimento. Nesses exemplos, a WTRU alvo pode decidir atualizar seu ID de L2 ao mesmo tempo que a WTRU de origem; por exemplo, ao receber uma mensagem *keep-alive*. A FIG. 7 é um diagrama de sequência 700 que ilustra um exemplo desse intercâmbio do Método 1 em que ambos os IDs de L2 são mudados tanto na WTRU de origem/requerente 710 quanto na WTRU de destino/ponto 720. Os intercâmbios na FIG. 7 são semelhantes aos previamente descritos com relação à FIG. 6, com algumas mudanças conforme ilustra a FIG. 7.

[0104]Por exemplo, os blocos 701 e 703 são os mesmos que na FIG. 6. Os blocos 702 A e 702 B indicam que um temporizador de privacidade é iniciado em ambas as WTRUs. Nos blocos 704 A e 704 B, o temporizador de privacidade expira nas WTRUs de origem e ponto, e os IDs de L2 precisam ser atualizados. Nos blocos

704 A1 e 704 B1, novos IDs de L2 são gerados em ambas as WTRUs (por exemplo, ID de L2 de origem #2, ID de L2 ponto #2). No bloco 704 A2, a WTRU de origem inicia o procedimento *keep-alive* para enviar seu novo ID à WTRU ponto. A WTRU de origem envia uma mensagem *keep-alive* 730 contendo seu novo ID de L2 em um novo IE (por exemplo, Source_L2_ID_IE). O ID de L2 de origem atual ainda é usado porque ele é o ID associado à sessão nesse momento e ele é o ID que o ponto conhece/espera que seja usado. Um novo valor de temporizador de privacidade também pode ser configurado na WTRU de origem/ponto. A WTRU ponto recebe o novo ID de L2 de origem e salva-o localmente. Ambos os IDs de L2 (anterior e novo) podem ser salvos localmente caso mensagens usando o ID anterior estejam em trânsito durante o procedimento de modificação do ID. A WTRU ponto interrompe o temporizador *keep-alive* no bloco 740 uma vez que uma mensagem *keep-alive* é recebida. A WTRU ponto envia uma mensagem de resposta 750 que inclui o novo IE do ID de L2 de origem definido com o mesmo valor que o recebido na mensagem *keep-alive* (isto é, o ID de L2 de origem #1). Ela também inclui seu novo ID em outro novo IE (por exemplo, target_L2_ID_IE). Os IDs de L2 anteriores continuam sendo usados como o ID de origem/destino para essa mensagem. Depois de receber a mensagem de resposta, a WTRU de origem responde com uma mensagem de confirmação 760 que inclui o novo IE do ID de L2 alvo. No entanto, o ID de L2 anterior do alvo continua sendo usado como o ID destino para essa mensagem. Nos blocos 705 A e 705 B, os novos IDs de L2 de origem/ponto são sincronizados/comunicados de uma camada à outra em ambas as WTRUs para a comunicação PC5 (por exemplo, com a camada superior ciente de qual ID de WTRU é usado e com uma camada AS que utiliza o ID de L2 para a comunicação PC5). Nos blocos 706 A e 706 B, ambas as WTRUs reiniciam o temporizador de privacidade porque o ID de L2 de origem precisa ser mudado periodicamente. O temporizador *keep-alive* também é reiniciado. No bloco 707, os novos IDs de L2 são

usados daqui em diante, de ambos os lados. Em alguns exemplos, um novo procedimento de privacidade de enlace direto ProSe é introduzido. Nesses exemplos, um procedimento de Privacidade de Enlace Direto dedicado é usado para modificar o ID de L2 de origem associado à sessão. O novo procedimento de privacidade utiliza seus próprios temporizador de privacidade e mensagens de privacidade (por exemplo, Privacy_Request, Privacy_Response, Privacy_Trigger). O procedimento de privacidade pode ser iniciado a partir da WTRU de origem ou da WTRU ponto. O procedimento pode ser usado para atualizar o ID de L2 de uma única WTRU ou os IDs de L2 de ambas as WTRUs.

[0105]Em alguns exemplos, a WTRU de origem dá início ao procedimento de privacidade com a mudança de um único ID de L2. A FIG. 8 é um diagrama de sequência 800 que ilustra um exemplo de um procedimento de privacidade desse tipo. Nesse exemplo, a WTRU de origem foi aprovisionada com o valor de temporizador de privacidade. Quando o temporizador expira, a WTRU obtém um novo ID de L2 e atualiza sua WTRU ponto com o novo ID de L2. A FIG. 8 representa um exemplo de um procedimento de privacidade recém-definido usando uma comunicação de privacidade de enlace direto entre duas WTRUs que corresponde a uma opção do Método 1.

[0106]No bloco 801, parâmetros V2X são aprovisionados nas WTRUs e uma sessão é estabelecida. No bloco 802, a WTRU de origem inicia um temporizador de privacidade usando o valor provisionado. No bloco 803, a comunicação entre as WTRUs de origem e ponto está em andamento. No bloco 804, o temporizador de privacidade expira na WTRU de origem. No bloco 804 A1, a WTRU de origem gera um novo ID de L2 de origem (por exemplo, ID de L2 de origem #2). No bloco 804 A2, o procedimento de privacidade é iniciado. A WTRU de origem envia uma mensagem Privacy_Request 830 incluindo o novo IE do ID de L2 de origem. Um novo IE do valor de temporizador de privacidade também pode ser especificado, caso o valor de

temporizador precise ser mudado. A WTRU ponto recebe o novo ID de L2 de origem de seu ponto e salva-o localmente. A WTRU ponto responde com uma mensagem Privacy_Response 840 incluindo o novo IE do ID de L2 de origem definido com o mesmo valor que o recebido na mensagem Privacy_Request 830. Nos blocos 805 A e 805 B, um novo ID de L2 de origem é sincronizado/comunicado de uma camada à outra em ambas as WTRUs para a comunicação PC5 (por exemplo, com a camada superior ciente de qual ID de WTRU é usado e com uma camada AS que utiliza o ID de L2 para comunicação PC5). No bloco 806, a WTRU de origem reinicia o temporizador de privacidade. No bloco 807, o novo ID de L2 de origem pode ser usado daqui em diante.

[0107]Em alguns exemplos, ambos os IDs de L2 são atualizados durante o mesmo procedimento. A FIG. 9 é um diagrama de sequência 900 que ilustra um exemplo de um procedimento desse tipo. Nesse exemplo, a WTRU ponto atualiza seu ID de L2 ao mesmo tempo que a WTRU de origem, e o intercâmbio dos novos IDs de L2 se dá durante o mesmo procedimento. A FIG. 9 representa um exemplo de um procedimento de privacidade recém-definido usando uma comunicação de privacidade de enlace direto entre duas WTRUs que corresponde a outra opção do Método 1 na qual ambas as WTRUs atualizam seus IDs de L2 no mesmo procedimento.

[0108]No bloco 901, parâmetros V2X são aprovisionados nas WTRUs e uma sessão é estabelecida. Nos blocos 902 A e 902 B, a WTRU de origem 910 e a WTRU ponto 920 iniciam a um temporizador de privacidade usando o valor provisionado. No bloco 903, a comunicação entre a WTRU de origem e a WTRU ponto está em andamento. Nos blocos 904 A e 904 B, o temporizador de privacidade expira na WTRU de origem, e possivelmente na WTRU ponto. No bloco 904 A1, a WTRU de origem gera um novo ID de L2 de origem (por exemplo, ID de L2 de origem #2). A WTRU de origem envia uma mensagem Privacy_Request 930 que

inclui o novo IE do ID de L2 de origem e, como opção, um novo IE do temporizador de privacidade, caso o valor de temporizador precise ser atualizado. A WTRU ponto recebe o novo ID de L2 de origem da WTRU de origem e salva-o localmente. No bloco 904 B1, a WTRU ponto gera um novo ID de L2 ponto (por exemplo, ID de L2 ponto # 2) (a) quando o temporizador de privacidade expira (bloco 904 B) ou, como opção, (b) quando do recebimento da mensagem de Pedido de Privacidade 930. A WTRU ponto responde com uma mensagem Privacy_Response 940 que inclui o novo IE do ID de L2 de origem definido com o mesmo valor que o recebido na mensagem de Pedido de Privacidade e que inclui também seu novo ID de L2 ponto. Como opção, um novo IE do temporizador de privacidade pode ser incluído, caso o valor de temporizador ponto precise ser atualizado. A WTRU de origem recebe uma mensagem de Resposta de Privacidade 940 que inclui um novo IE do ID de L2 da WTRU ponto, salva esse novo ID localmente e responde com uma mensagem de Confirmação de Privacidade 950 que inclui o novo ID de L2 ponto. Nos blocos 905 A e 905 B, os novos IDs de L2 são sincronizados/comunicados de uma camada à outra em ambas as WTRUs para a comunicação PC5 (por exemplo, com a camada superior ciente de qual ID de WTRU é usado e com uma camada AS que utiliza o ID de L2 para a comunicação PC5). Nos blocos 906 A e 906 B, cada WTRU reinicia seu temporizador de privacidade. No bloco 907, os novos IDs de L2 são usados daqui em diante.

[0109]Em alguns exemplos, uma WTRU dispara um procedimento de privacidade no lado do ponto. Por exemplo, uma WTRU pode pedir que seu ponto mude seu ID de L2 (por exemplo, a WTRU ponto pede que a WTRU de origem mude seu ID de L2 – isto é, o ID de L2 de origem). A WTRU de origem que recebe esse pedido pode disparar o procedimento de atualização do ID de L2. Nesse caso, a WTRU de origem obtém um novo ID de L2 e atualiza sua WTRU ponto com o novo ID de L2. A WTRU ponto, que foi configurada com o valor de temporizador de

privacidade da WTRU de origem durante o procedimento de estabelecimento de enlace, pode decidir por disparar a mudança do ID de L2 da WTRU de origem; por exemplo, se (a) ela receber um disparador localmente (por exemplo, da camada superior) ou determinar que o ID de L2 de origem deve ser mudado (por exemplo, por qualquer motivo adequado ou disparador adicional) ou (b) a WTRU ponto quiser atualizar seu próprio ID de L2 ao mesmo tempo que a WTRU de origem.

[0110]A FIG. 10 é um diagrama de sequência 10000 que ilustra um procedimento de Método 1 exemplificativo no qual a WTRU ponto dispara o procedimento de mudança do ID de L2. No bloco 1001, uma sessão é estabelecida e a comunicação entre a WTRU de origem 1010 e a WTRU ponto 1020 está em andamento. Nos blocos 1002 A e 1002 B, ambas as WTRUs podem iniciar um temporizador de privacidade. No bloco 1003, a comunicação entre as WTRUs de origem e ponto está em andamento. No bloco 1004, a WTRU ponto determina que a WTRU de origem deve mudar seu ID de L2 e, possivelmente, o ID de L2 ponto também precisa ser mudado. A WTRU ponto envia uma nova mensagem Privacy_Trigger 1030 à WTRU de origem. A WTRU ponto pode gerar um novo ID de L2 caso seu ID de L2 precise ser atualizado no bloco opcional 1004 B1. Do contrário, a WTRU de origem que recebe essa mensagem disparadora 1030 interrompe seu temporizador de privacidade no bloco 1005. No bloco 1005 A1, é gerado um novo ID de L2 de origem (por exemplo, ID de L2 de origem #2). No bloco 1005 A2, a WTRU de origem dá início ao procedimento de privacidade para enviar seu novo ID à WTRU ponto. As mensagens de privacidade diretas são trocadas no bloco 1006. Como alternativa, a WTRU de origem pode usar o procedimento *keep-alive*, por exemplo, conforme ilustrado e discutido com relação à FIG. 6, para enviar o novo ID de L2 de origem à WTRU ponto. Procedimentos conforme ilustrados e descritos com relação às FIGs. 6 e 8 podem ser adotados caso só o ID de L2 de origem seja mudado. Procedimentos conforme ilustrados e descritos com relação às

FIGs. 7 e 9 podem ser usados se ambos os IDs de L2 forem mudados. Nos blocos 1007 A e 1007 B, os novos IDs de L2 são sincronizados/comunicados de uma camada à outra em ambas as WTRUs para a comunicação PC5 (por exemplo, com a camada superior ciente de qual ID de WTRU é usado e com uma camada AS que utiliza os IDs de L2 para a comunicação PC5). Nos blocos 1008 A e 1008 B, o temporizador de privacidade é reiniciado em ambas as WTRUs. No bloco 1009, a comunicação usando o novo ID de L2 de origem #2 e o novo ID de L2 ponto #2, caso este tenha sido mudado, está em andamento.

[0111]Um exemplo de mudança do ID de L2 pelo Método 2 inclui a geração de IDs de L2 ponto nas WTRUs de origem e alvo. Em alguns exemplos do Método 2, o ID de L2 ponto é regenerado a partir da própria WTRU de origem em vez de trocar o novo ID via mensagens. Nesses exemplos, cada WTRU pode ser provisionado com uma lista de parâmetros possivelmente secretos, e sementes, durante o estágio de aprovisionamento de parâmetros V2X junto com os demais parâmetros V2X necessários. As sementes podem ser usadas para a regeneração do ID de L2 da WTRU.

[0112]Depois de estabelecer a sessão entre uma WTRU de origem e uma WTRU ponto, e depois que as chaves de segurança são trocadas e as comunicações protegidas, a WTRU de origem e a WTRU ponto podem trocar seu valor de temporizador de privacidade e uma semente entre si. Logo, uma WTRU é configurada com o (a) valor de temporizador de privacidade do ponto e (b) uma semente que será usada para a regeneração do novo ID de L2.

[0113]A mesma semente ou outra semente (por exemplo, aprovisionada para gerar o valor de temporizador) pode ser usada pela WTRU para gerar o temporizador de privacidade. Se uma semente diferente for usada para gerar o valor de temporizador, esse valor de semente também pode ser trocado entre as WTRUs.

O valor de semente para o temporizador pode facilitar a randomização do valor de temporizador para mudar o temporizador de privacidade.

[0114]Em alguns exemplos, uma lista de sementes, potencialmente com temporizadores correspondentes, pode ser configurada de ambos os lados e trocada durante o mesmo procedimento. Esse procedimento descrito pode reduzir ou limitar o intercâmbio de mensagens pelo ar. A semente usada para gerar um novo ID de L2 da WTRU alvo pode ser escolhida de maneira consecutiva na lista de sementes provida após o temporizador de privacidade expirar. A WTRU inicia um peer_privacy_timer e, quando o temporizador expira, ele regenera seu ID de L2 ponto com base na semente configurada. Ao mesmo tempo, a WTRU ponto também regenera seu próprio ID de L2 usando a mesma semente, e o mesmo valor é obtido. A geração do novo ID de L2 da WTRU alvo pode ser periódica. A semente e o valor de temporizador podem ser configurados na WTRU ponto usando um mecanismo *keep-alive* atualizado, quaisquer outras mensagens de sinalização PC5 atualizadas ou novas mensagens.

[0115]A FIG. 11 é um diagrama de sequência 1100 que ilustra um exemplo de procedimento de Método 2 no qual a WTRU de origem configura a WTRU ponto para que ela seja capaz de regenerar o ID de L2 de origem após um temporizador expirar. Esses mecanismos podem ser usados da WTRU de destino à WTRU de origem. Na FIG. 11, o ID de L2 de origem é regenerado na WTRU de origem e na WTRU ponto. No bloco 1101, uma sessão é estabelecida entre a WTRU de origem e a WTRU ponto. No bloco 1102, a comunicação entre a WTRUs de origem e a WTRU ponto está em andamento. O “ID de L2 de origem #1” é usado nesse momento. No bloco 1102 A, um temporizador de privacidade é iniciado na WTRU de origem. No bloco 1103, o temporizador de privacidade e uma semente são enviados à WTRU ponto (por exemplo, usando ou um mecanismo *keep-alive* atualizado ou novas mensagens). O temporizador pode indicar, por exemplo, uma duração de 15 minutos

e um tempo de início específico. Nesse exemplo, o temporizador expirará a cada 15 minutos após o tempo de início especificado. Isso pode facilitar a expiração dos temporizadores de ambos os lados ao mesmo tempo, ainda que eles não sejam iniciados ao mesmo tempo. No bloco 1103 A, a WTRU ponto salva o valor de temporizador de privacidade e semente da WTRU de origem e inicia um temporizador de privacidade da WTRU de origem. Os procedimentos usados para o intercâmbio de informações, por exemplo, conforme ilustrados e descritos com relação às FIGs. 6 e 8, podem ser usados aqui, porém o temporizador de privacidade + semente são transportados neste caso (novo IE para semente). Nos blocos 1104 A e 1104 B, após o temporizador expirar, a WTRU de origem utiliza a semente que foi compartilhada com seu ponto para gerar um novo ID de L2. Nos blocos 1104 A 1 e 1104 B1, na WTRU alvo, o temporizador expira ao mesmo tempo que na WTRU de origem. A WTRU alvo utiliza o valor de semente recebido da WTRU de origem para regenerar um ID de L2 da WTRU de origem. O mesmo valor para o ID de L2 de origem é obtido em ambas as WTRUs. Nos blocos 1105 A e 1105 B, p novo ID de L2 de origem é sincronizado/comunicado de uma camada à outra em ambas as WTRUs para a comunicação PC5 (por exemplo, com a camada superior ciente de qual ID de WTRU é usado e com uma camada AS que utiliza o ID de L2 para comunicação PC5). Nos blocos 1106 A e 1106 B, o temporizador de privacidade é reiniciado em ambas as WTRUs. No bloco 1107, a comunicação entre a WTRU de origem e a WTRU ponto com base no ID de L2 de origem #2 recém-formado está em andamento.

[0116]Em alguns exemplos, um mecanismo *keep-alive* atualizado (por exemplo, conforme ilustrado e descrito com relação à FIG. 6) ou novas mensagens (por exemplo, conforme ilustradas e descritas com relação à FIG. 8) podem ser usados para o intercâmbio do valor de privacidade e semente. O valor de temporizador e a semente podem ser atualizados regular e/ou periodicamente.

[0117]A FIG. 12 é um diagrama de sequência 1200 que ilustra (A) uma WTRU 1210 configurando seu valor de temporizador de privacidade & semente na WTRU ponto 1220 e (B) ambas as WTRUs trocando sua configuração uma com a outra. A FIG. 12 ilustra um intercâmbio do valor de temporizador de privacidade e sementes pelo Método 2. A sequência A é um exemplo de intercâmbio de mensagens no qual a WTRU de origem/requerente envia seu temporizador de privacidade e valores de semente à WTRU ponto. Na sequência A, na mensagem 1225, uma WTRU 1210 envia uma comunicação direta *keep-alive*, pedido de privacidade direto ou outra mensagem que contenha informações relevantes para a transferência dos valores de temporizador de privacidade e semente da WTRU 1210 à WTRU ponto 1220. Depois de recebê-los, a WTRU ponto 1220 transmite uma mensagem de resposta 1230 que pode ser uma confirmação do recebimento da mensagem de pedido 1225. A mensagem de confirmação 1230 pode incluir o valor de temporizador de privacidade da WTRU de origem e o valor de semente de origem, entre outros possíveis conteúdos da mensagem. A sequência B pode ser uma alternativa à sequência A. A sequência B é um exemplo de intercâmbio de mensagens em que ambas as WTRUs trocam seus respectivos valores de temporizador de privacidade e semente uma com a outra. Na sequência B, na mensagem 1235, uma WTRU 1210 envia uma comunicação direta *keep-alive*, pedido de privacidade direto ou outra mensagem que contenha informações relevantes para a transferência dos valores de temporizador de privacidade e semente da WTRU 1210 à WTRU ponto 1220. Depois do recebimento, a WTRU ponto 1220 transmite uma mensagem de resposta 1240 que pode ser uma resposta acusando o recebimento da mensagem de pedido 1235. A mensagem de resposta 1240 pode incluir o valor de temporizador de privacidade da WTRU de origem e o valor de semente de origem e o valor de temporizador de privacidade ponto e valor de semente ponto, entre outros possíveis conteúdos da mensagem. Depois de

receber a mensagem de resposta 1240, a WTRU de origem 1210 transmite a mensagem 1245, que pode ser uma confirmação de comunicação direta *keep-alive*, confirmação de privacidade direta ou outra mensagem que contenha informações relevantes para a transferência dos valores de temporizador de privacidade e semente da WTRU ponto 1220 de volta à WTRU ponto 1220. Os exemplos de intercâmbio A e B acima podem estabelecer uma configuração para as WTRUs como no bloco 1103 da FIG. 11 do Método 2.

[0118]Um exemplo do Método 3 pode ampliar o intercâmbio de novos identificadores de L2 com o intercâmbio de um novo ID de sessão. Em um exemplo, o Método 3 amplia o Método 1 com o intercâmbio de um novo ID de sessão. Por exemplo, conforme descrito, as WTRUs podem trocar seu novo ID de sessão uma com a outra durante o procedimento de mudança do ID de L2 independentemente (isto é, um depois do outro) ou simultaneamente durante o mesmo procedimento. Além disso, uma WTRU pode ser configurada para atualizar seu identificador de contexto de segurança (por exemplo, identificador de sessão) ao mesmo tempo que seu ID de L2, por exemplo, por motivos de privacidade. Para facilitar isso, o intercâmbio de novos identificadores de L2 discutido acima é ampliado com proteção à privacidade adicional ao permitir o intercâmbio do MSB/LSB do ID de $K_{D\text{-}sess}$ em aditamento aos IDs de L2 de origem e destino.

[0119]Em um primeiro cenário, a WTRU de origem/iniciadora/requerente pode ter um temporizador de privacidade em andamento. Se o temporizador de privacidade expirar, ou se for recebido um disparador da WTRU ponto, a WTRU de origem/iniciadora/requerente busca o contexto de segurança associado à sessão e executa o procedimento de atualização do ID de L2 (por exemplo, conforme discutido acima com referência ao procedimento *keep-alive* de enlace direto ProSe atualizado com o novo ID de L2 de origem, ou quando a WTRU de origem inicia um procedimento de privacidade com a mudança de um único ID de L2). Além da

regeneração do ID de L2, a WTRU pode gerar um novo identificador de sessão (isto é, MSB do ID $K_{D\text{-}sess}$). Esse novo ID de sessão pode ser enviado à WTRU ponto junto com o novo ID de L2. Note-se que a comunicação já está protegida, isto é, o ID de L2 e o ID de sessão trocados são criptografados, e a integridade garantida. Os novos identificadores são usados quando o procedimento é concluído com êxito. Note-se que o conteúdo de contexto de segurança em si não é modificado, isto é, as chaves e demais parâmetros (por exemplo, contador) salvos no contexto de segurança continuam os mesmos, e só o identificador de sessão, usado para localizar o contexto de segurança localmente na WTRU de origem/iniciadora/requerente e WTRU de destino/ponto (isto é, em cada WTRU ponto), é atualizado.

[0120]Em um segundo cenário, ambas as WTRUs atualizam seus IDs durante o mesmo procedimento, ou seja, ambos os IDs de L2 são atualizados durante o mesmo procedimento e ambas as WTRUs mudam sua porção do identificador de sessão ao mesmo tempo; durante o mesmo procedimento de privacidade. Nesse caso, ambas as WTRUs geram uma nova porção do ID de sessão (MSB e LSB) e trocam-na entre si junto com seu novo ID de L2. Isso é ilustrado na FIG. 13 usando mensagens de Privacidade Direta. A FIG. 13 é um diagrama de sequência de mensagens 1300 que ilustra o caso em que ambas as WTRUs trocam sua nova porção do ID de sessão uma com a outra usando o procedimento de privacidade.

[0121]No exemplo da FIG. 13, a comunicação está em andamento entre a WTRU de origem 1310 e a WTRU ponto 1320 no bloco 1301, onde a WTRU de origem está usando o ID de L2 #1 e a WTRU ponto está usando seu próprio ID de L2 #1. Uma associação de segurança, identificada pelo ID de sessão (ID de $K_{D\text{-}sess}$ #1) foi estabelecida entre as WTRUs; isto é, cada WTRU salvou localmente um contexto de segurança contendo os parâmetros de segurança necessários (por

exemplo, chaves de criptografia) para proteger a comunicação. Todas as informações trocadas entre os pontos é criptografada e, a integridade, garantida. A WTRU iniciadora utiliza o MSB do ID de $K_{D\text{-}sess}$ para localizar o contexto de segurança e a WTRU ponto utiliza o LSB do ID de $K_{D\text{-}sess}$ de seu lado.

[0122]No bloco 1302, um temporizador de privacidade expira na WTRU de origem. A WTRU de origem gera um novo ID de L2 de origem (por exemplo, ID de L2 de origem #2) no bloco 1302 A, e a WTRU de origem gera um novo MSB do ID de $K_{D\text{-}sess}$ (por exemplo, MSB do ID de $K_{D\text{-}sess}$ #2) no bloco 1302 B. A WTRU de origem envia uma mensagem Privacy_Request 1303 ou outra mensagem de Sinalização PC5 (por exemplo, uma mensagem de Atualização do Enlace PC5 incluindo o novo IE do ID de L2 de origem e o novo MSB do IE do ID de $K_{D\text{-}sess}$) e, como opção, um novo IE do temporizador de privacidade.

[0123]A WTRU ponto recebe o novo ID de L2 de origem e o novo MSB do ID de $K_{D\text{-}sess}$ da mensagem 1303 e salva-os localmente para, em última análise, substituir os valores anteriores atualmente em uso. No bloco 1304 A, a WTRU ponto gera um novo ID de L2 ponto (por exemplo, ID de L2 ponto #2). No bloco 1304 B, a WTRU ponto gera um novo LSB do ID de $K_{D\text{-}sess}$ (por exemplo, LSB do ID de $K_{D\text{-}sess}$ #2). No bloco 1304 C, a WTRU ponto salva localmente seus identificadores recém-gerados. O contexto de segurança é atualizado localmente com o ID de $K_{D\text{-}sess}$ #2.

[0124]A WTRU ponto envia (à WTRU de origem) uma mensagem Privacy_Response 1305 ou outra mensagem de Sinalização PC5 (por exemplo, mensagem de Resposta de Atualização do Enlace PC5) incluindo o novo IE do ID de L2 de origem e o novo MSB de origem do IE do ID de $K_{D\text{-}sess}$ definidos com os mesmos valores que os recebidos na mensagem de Pedido de Privacidade e incluindo também seu novo IE do ID de L2 ponto e novo LSB ponto do IE do ID de $K_{D\text{-}sess}$. Em outra modalidade, a WTRU ponto não envia o novo IE do ID de L2 de origem e o novo MSB de origem do IE do ID de $K_{D\text{-}sess}$ de volta, esperando-se que a

WTRU de origem recupere-os localmente com base no contexto de sessão atual. Por exemplo, a WTRU de origem pode armazená-los no contexto de segurança identificado pelo MSB de origem do IE do ID do $K_{D\text{-}sess}$ atual no momento em que eles foram gerados. No bloco 1306, a WTRU de origem, que recebe uma mensagem de Resposta de Privacidade 1305, que inclui o novo IE do ID de L2 ponto e o novo LSB ponto do IE do ID de $K_{D\text{-}sess}$, salva esses novos IDs localmente e responde com uma mensagem de Confirmação de Privacidade 1307 que inclui o novo ID de L2 ponto e o novo LSB do ID de $K_{D\text{-}sess}$. No bloco 1308, os novos IDs de L2 e ID de $K_{D\text{-}sess}$ (MSB e LSB) são usados daqui em diante.

[0125]Um exemplo do Método 4 pode aprimorar os procedimentos de rechaveamento existentes com o intercâmbio de novos IDs de L2. Em um exemplo do Método 4, um procedimento de rechaveamento existente pode ser aprimorado com o intercâmbio de novos IDs de L2 entre as WTRUs em comunicação. O procedimento de rechaveamento existente é usado para atualizar o contexto de segurança de uma sessão em andamento. Nesse caso, todos os parâmetros são atualizados, por exemplo, chaves são regeneradas, contadores são reiniciados e um novo ID de sessão também é gerado.

[0126]Como alternativa a várias abordagens discutidas neste documento, essa abordagem utiliza um procedimento de rechaveamento existente (por exemplo, conforme discutido em 3GPP TS 33.303 6.5.5.3) e aprimora-o com a possibilidade de trocar os novos IDs de L2 de origem e destino entre as WTRUs ponto, junto com o novo ID de sessão. Quanto a outras abordagens discutidas neste documento, um temporizador de privacidade pode ser usado para disparar esse procedimento de rechaveamento aprimorado. Outros disparadores também podem existir (por exemplo, das camadas superiores, um pedido de uma WTRU ponto, antes de o contador para o enlace atual repetir com as chaves atuais etc.).

[0127]Note-se que o procedimento de rechaveamento pode significar uma mudança completa do ID de sessão, isto é, das porções MSB e LSB, e pode ser realizado usando a sessão já estabelecida. Sendo assim, todas as informações trocadas entre os pontos são criptografadas e, a integridade, garantida. A mudança do ID de L2, contudo, pode ser realizada em uma única WTRU, se necessário, ou em ambas as WTRUs.

[0128]A FIG. 14 é um diagrama de sequência de mensagens 1400 que ilustra o intercâmbio de novos IDs de L2 usando um procedimento de rechaveamento aprimorado. A FIG. 14 traz um exemplo de uso do Método 4 que permite o intercâmbio de IDs de L2 de ambas as WTRUs de origem e ponto no contexto de um procedimento de rechaveamento. No bloco 1401, a comunicação entre as WTRUs de origem e ponto está em andamento. A WTRU de origem 1410 está usando o ID de L2 #1 e a WTRU ponto 1420 está usando seu próprio ID de L2 #1. Uma associação de segurança, identificada pelo ID de sessão (ID de $K_{D\text{-}sess}$ #1) foi estabelecida entre as WTRUs de origem e ponto (por exemplo, cada WTRU salvou localmente um contexto de segurança contendo os parâmetros de segurança necessários, por exemplo, chaves de criptografia) para proteger a comunicação.

[0129]No bloco 1402, um temporizador de privacidade ou rechaveamento expira na WTRU de origem (ou outro disparador acontece, por exemplo, a partir da camada superior). A WTRU de origem dispara o procedimento de rechaveamento aprimorado com o intercâmbio de atualização do ID de L2. No bloco 1402 A, a WTRU de origem gera um novo ID de L2 de origem (por exemplo, ID de L2 de origem #2). No bloco 1402 B, a WTRU de origem gera um novo MSB do ID de $K_{D\text{-}sess}$ (por exemplo, MSB do ID de $K_{D\text{-}sess}$ #2). A WTRU de origem envia uma mensagem DIRECT_REKEYING_REQUEST 1403 que inclui o novo IE do ID de L2 de origem e o novo MSB do ID de $K_{D\text{-}sess}$, e opcionalmente um novo IE de temporizador de privacidade. O contexto de segurança e os IDs de L2 existentes continuam sendo

usados para enviar essa mensagem, isto é, o ID de L2 de origem/destino antigo e o ID de $K_{D\text{-}sess}$ existente.

[0130]A WTRU ponto recebe o novo ID de L2 de origem e o novo MSB do ID de $K_{D\text{-}sess}$ da WTRU de origem através da mensagem 1403 e salva-os localmente, junto com os valores anteriores. No bloco 1404 A, a WTRU ponto gera um novo ID de L2 ponto (por exemplo, ID de L2 ponto #2). No bloco 1404 B, a WTRU ponto gera um novo LSB do ID de $K_{D\text{-}sess}$ (por exemplo, LSB do ID de $K_{D\text{-}sess}$ #2). No bloco 1404 C, a WTRU salva localmente seus identificadores recém-gerados. O contexto de segurança é atualizado localmente com o ID de $K_{D\text{-}sess}$ #2, porém o ID de $K_{D\text{-}sess}$ #1 antigo é mantido e usado nessa altura, bem como os IDs de L2 de origem/destino antigos.

[0131]A WTRU ponto envia (à WTRU de origem) uma mensagem DIRECT_SECURITY_MODE_COMMAND 1405 que inclui o novo IE do ID de L2 de origem e o novo MSB de origem do novo IE do ID de $K_{D\text{-}sess}$ definidos com os mesmos valores que os recebidos na mensagem DIRECT-REKEYING_REQUEST 1403 (para confirmá-los) e que inclui também seu novo IE do ID de L2 ponto e novo LSB ponto do IE do ID de $K_{D\text{-}sess}$. Em outra modalidade, a WTRU ponto não envia de volta o novo IE do ID de L2 de origem e o novo MSB de origem do IE do ID de $K_{D\text{-}sess}$, esperando-se que a WTRU de origem recupere-os localmente com base no contexto de sessão atual. Por exemplo, a WTRU de origem pode armazená-los no contexto de segurança identificado pelo MSB de origem atual do ID de $K_{D\text{-}sess}$ no momento em que eles foram gerados.

[0132]No bloco 1406, após a WTRU de origem receber uma mensagem DIRECT_SECURITY_MODE_COMMAND 1405, que especifica o novo IE do ID de L2 da WTRU ponto e o novo LSB do IE de $K_{D\text{-}sess}$, ela salva esses novos IDs localmente. Uma associação de segurança é atualizada com o ID de $K_{D\text{-}sess}$ #2. Geram-se novas chaves. A WTRU de origem responde transmitindo uma mensagem

DIRECT_SECURITY_MODE_COMPLETE 1407 que repete o novo ID de L2 ponto e o novo LSB do ID de $K_{D\text{-}sess}$ (isto é, confirma-os). A WTRU ponto, que recebe uma mensagem DIRECT_SECURITY_MODE_COMPLETE 1407 confirmando seu novo ID de L2 e LSB do ID de $K_{D\text{-}sess}$, responde enviando uma mensagem DIRECT_REKEYING_RESPONSE 1408 que conclui o procedimento. No bloco 1409, daqui em diante, os novos IDs de L2 e contexto de segurança, isto é, ID de $K_{D\text{-}sess}$ (MSB e LSB) e chaves são usados.

[0133]Note-se que, para fins de conveniência, a maioria dos procedimentos neste documento são descritos da perspectiva de interações entre as WTRUs da camada V2X/camada NAS ou camadas superiores. Os mesmos procedimentos também aplicam-se no nível do intercâmbio de sinalização RRC entre as WTRUs ou quando mensagens PC5 são trocadas pelo protocolo RRC.

[0134]Note-se que várias figuras expressas neste documento relacionam-se umas às outras e, sendo assim, compartilham elementos procedimentais em comum. Por exemplo, o procedimento exemplificativo do Método 1 nas Figuras de 6 a 10 compartilham procedimentos de configuração em comum. Em um exemplo mais global, os procedimentos das FIGs. de 6 a 10 são todos variações do Método 1 que incluem intercâmbios dos novos IDs de L2 entre as WTRUs de origem e ponto. Além disso, a Figura 13 é um Método 1 que é aprimorado pelo traço de geração de um novo ID de sessão usando um novo MSB do ID de sessão advindo de uma WTRU de origem e um novo LSB do ID de sessão advindo de uma WTRU ponto. A FIG. 15 ilustra uma combinação lógica desses procedimentos compartilhados da perspectiva de uma WTRU de origem. Na FIG. 15, os procedimentos da FIG. 6, FIG. 7 e FIG 13 são ilustrados destacando as opções que podem ser exercidas usando o Método 1. Outras variações dos exemplos expressos são possíveis usando técnicas expressas neste documento. Mais especificamente, conforme ilustra a FIG. 15, as operações em comum do Método 1 ilustradas nos exemplos detalhados da FIG. 6,

FIG. 7 e FIG. 13 são apresentadas. A FIG. 15 trata das opções do Método 1 de (i) uma comunicação entre a WTRU de origem é atualizada só com um novo ID de L2 de origem (referência FIG. 6), (ii) uma comunicação entre a WTRU de origem e ponto é atualizada tanto com um novo ID de L2 de origem quanto com um novo ID de L2 ponto, ou (iii) uma comunicação entre a WTRU de origem e ponto é atualizada tanto com o novo ID de L2 de origem quanto com o ID de L2 ponto e também com contribuições de MSB e LSB do ID de sessão advindas da WTRU de origem e ponto, respectivamente, para comunicação usando um novo ID de sessão.

[0135]A FIG. 15 é um procedimento 1500 com opções que podem ser exercidas por uma WTRU de origem conduzindo os princípios do Método 1 descrito neste documento. No bloco 1505, presume-se que uma WTRU de origem possui comunicação em andamento com uma WTRU ponto. Em um ambiente exemplificativo, a comunicação é uma comunicação de enlace de referência PC5 em uma operação V2X onde cada WTRU possui acesso a um aplicativo V2X que inclui as provisões de aplicativo de privacidade descritas neste documento. No bloco 1510, detecta-se um evento disparador. Esse evento disparador aciona a reação da WTRU de origem para conduzir as operações dos blocos de 1520 a 1535. Esse evento disparador pode ser uma condição detectada e pode incluir um temporizador que expira na WTRU, ou uma camada superior ou uma camada de aplicativo de um aplicativo V2X que solicita um novo ID de L2, ou a WTRU de origem movendo-se a uma nova área geográfica, ou a WTRU de origem recebendo novos parâmetros de aprovisionamento a partir da função de controle V2X ou de um servidor de aplicativo V2X, ou a WTRU de origem recebendo um pedido da WTRU ponto para mudar um ID de L2.

[0136]No bloco 1520, caso um evento disparador ocorra, a WTRU de origem pode gerar um novo ID de L2 para as comunicações futuras com a WTRU ponto. Isso é semelhante ao bloco exemplificativo 604 A da FIG. 6 que utiliza o Método 1.

Como opção, no bloco 1520, a WTRU também pode gerar um novo MSB para um novo ID de sessão. Essa opção é uma variação do Método 1 que é semelhante ao bloco exemplificativo 1302 B da FIG. 13. Ambas a FIG. 6 e FIG. 13 compartilham elementos operacionais em comum como variações do Método 1. No bloco 1525 da FIG. 15, a WTRU de origem comunica, via transmissão de mensagem à WTRU ponto, o valor do novo ID de L2 de origem para uso pela WTRU ponto. Essa operação de Método 1, também ilustrada na mensagem exemplificativa 630 da FIG. 6 como um exemplo de mensagem de comunicação direta do tipo *keep-alive*. Porém, como ensinado acima, essas mensagens podem ser de quaisquer mensagens comumente conhecidas e usadas entre WTRUs ou podem ser uma mensagem especializada, tal como uma mensagem de pedido de privacidade direta entre as WTRUs. No bloco 1525 na FIG. 15, a comunicação entre as WTRUs também pode transferir opcionalmente não só o novo ID de L2 da WTRU de origem, mas também o novo MSB para um novo ID de sessão. Essa opção é uma variação do Método 1 ilustrada na mensagem exemplificativa 1303 da FIG. 13 como uma mensagem do tipo pedido de privacidade direto.

[0137]No bloco 1530, a WTRU de origem recebe uma mensagem da WTRU ponto. A mensagem responde ao novo ID de origem e pode conter uma confirmação do novo ID de L2 de origem a partir da WTRU ponto. Esse exemplo de operação do Método 1 é ilustrado na mensagem exemplificativa 650 da FIG. 6 como uma mensagem de confirmação *keep-alive*. No entanto, como mencionado acima, o tipo de mensagem pode ser qualquer tipo de mensagem que seja usado entre WTRUs incluindo uma nova mensagem de comunicação de privacidade direta. Opcionalmente, no bloco 1530 da FIG. 15, se a operação de Método 1 incluir a geração de um novo ID de L2 da WTRU ponto, como na operação de Método 1 da FIG. 7, a mensagem no bloco 1530 pode incluir tanto uma confirmação do novo ID de L2 de origem quanto o novo ID de L2 da WTRU ponto. A mensagem que inclui

tanto o novo ID de L2 de origem quanto o novo ID de L2 ponto é uma variação do Método 1 ilustrado na mensagem exemplificativa 750 da FIG. 7. Uma terceira opção para o bloco 1530 da FIG. 15 inclui a variação do Método 1 ilustrada na FIG. 13, que inclui informações do novo ID de L2 de origem, do novo ID de L2 ponto, do novo MSB para um novo ID de sessão e de um novo LSB da WTRU ponto para uso em um novo ID de sessão. A WTRU de origem, na opção de usar um novo ID de sessão, depois de ter recebido o novo MSB e LSB geraria um novo ID de sessão para a comunicação entre a WTRU de origem e a WTRU conforme descrito com referência à FIG. 13.

[0138]No bloco 1535, a WTRU de origem pode se comunicar com a WTRU ponto usando o novo ID de L2 de origem ou com base nele. Essa ação é incluída em uma operação do Método 1 conforme ilustrada no bloco exemplificativo 607 da FIG. 6. Como opção, se a operação de Método 1 incluir uma mudança de ambos os IDs de L2 de origem e ponto, como na operação de Método 1 da Fig. 7, o bloco 1535 da FIG. 15 permitirá que a WTRU de origem se comunique com a WTRU ponto usando o novo ID de L2 de origem e o novo ID de L2 ponto. Essa operação também é ilustrada na operação de Método 1 do bloco exemplificativo 707 da FIG. 7. No bloco 1535 da FIG 15, outra opção do Método 1 é que a WTRU de origem se comunique com a WTRU ponto usando o novo ID de L2 de origem, o novo ID de L2 ponto e um novo ID de sessão que inclui a contribuição do MSB da WTRU de origem e a contribuição de LSB da WTRU ponto. Essa operação de Método 1 é ilustrada no bloco exemplificativo 1308 da FIG. 13.

[0139]Sendo assim, o Método 1 é ilustrado como tendo algumas operações em comum que permitem diferentes variações de acordo com se a comunicação entre as WTRUs de origem e ponto é atualizada só com um novo ID de L2 de origem, é atualizada tanto com o novo ID de L2 de origem quanto com o ID de L2 ponto, ou é atualizada tanto com o novo ID de L2 de origem quanto com o ID de L2

ponto e também com contribuições de MSB e LSBV das WTRUs de origem e ponto, respectivamente, para comunicar um novo ID de sessão.

[0140]Embora traços e elementos sejam descritos acima em combinações específicas, os versados na técnica apreciarão que cada traço ou elemento pode ser usado sozinho ou em combinação a outros traços e elementos. Além disso, os métodos descritos neste documento podem ser implementados em um programa de computador, *software* ou *firmware* incorporado a um meio legível por computador para execução por um computador ou processador. Exemplos de meios legíveis por computador incluem sinais eletrônicos (transmitidos por conexões com fio ou sem fio) e meios de armazenamento legíveis por computador. Exemplos de meios de armazenamento legíveis por computador incluem, entre outros, memória somente para leitura (ROM), memória de acesso aleatório (RAM), um registro, memória *cache*, dispositivos de memória semicondutores, meios magnéticos como discos rígidos internos e discos removíveis, meios magneto-ópticos, e meios ópticos como discos de CD-ROM e discos digitais versáteis (DVDs). Um processador em associação a *software* pode ser usado para implementar um transceptor de frequência de rádio para uso em uma WTRU, UE, terminal, estação de base, RNC ou qualquer computador hospedeiro.

[0141]Em uma modalidade representativa, qualquer uma das operações, processos etc. descritos neste documento pode ser implementada como instruções legíveis por computador armazenadas em um meio legível por computador. As instruções legíveis por computador podem ser executadas por um processador de uma unidade móvel, um elemento de rede e/ou qualquer outro dispositivo de computação.

[0142]Na descrição detalhada acima, delinearam-se várias modalidades dos dispositivos e/ou processos pelo uso de diagramas em blocos, fluxogramas e/ou exemplos. Quando os referidos diagramas em blocos, fluxogramas e/ou exemplos

contiverem uma ou mais funções e/ou operações, os versados na técnica perceberão que cada função e/ou operação dentro deles pode ser implementada, sozinha ou em conjunto, por uma ampla variedade de *hardware*, *software*, *firmware* ou praticamente qualquer combinação desses. Processadores adequados incluem, à guisa de exemplo, um processador de propósito geral, um processador de propósito especial, um processador convencional, um processador digital de sinais (DSP), uma pluralidade de microprocessadores, um ou mais microprocessadores em associação a um núcleo DSP, um controlador, um microcontrolador, Circuitos Integrados de Aplicação Específica (ASICs), Produtos Padrão de Aplicação Específica (ASSPs); circuitos de Arranjos de Portas Programável em Campo (FPGAs), qualquer outro tipo de circuito integrado (IC) e/ou uma máquina de estados.

[0143]Embora traços e elementos sejam dados acima em combinações específicas, os versados na técnica apreciarão que cada traço ou elemento pode ser usado sozinho ou em combinação a outros traços e elementos. A presente revelação não se limita em termos das modalidades específicas descritas neste pedido, que são tidas como ilustrações de vários aspectos. Muitas modificações e variações podem ser feitas sem divergir de seu âmbito e essência, como transparecerá aos versados na técnica. Nenhum elemento, ato ou instrução usado na descrição da presente invenção deve ser interpretado como crítico ou essencial à invenção, salvo quando assim descrito explicitamente. Métodos e aparelhos funcionalmente equivalentes dentro do âmbito da invenção, além dos enumerados neste documento, transparecerão aos versados na técnica mediante a leitura das descrições precedentes. Pretende-se que tais modificações e variações enquadrem-se no âmbito das reivindicações anexas. A presente invenção será limitada tão somente pelos termos das reivindicações anexas, juntamente com todo o âmbito de

equivalentes a que essas reivindicações tenham direito. Deve-se ter em mente que a presente revelação não se limita a métodos ou sistemas específicos.

[0144]Também deve-se ter em mente que a terminologia usada neste documento serve apenas para a finalidade de descrever modalidades específicas e não visa a ser limitante. Conforme usados neste documento, quando mencionados neste documento, os termos "estação" e sua abreviação "STA", "equipamento do usuário" e sua abreviação "UE" podem significar (i) uma unidade transmissora e/ou receptora sem fio (WTRU), tal como descrito acima; (ii) qualquer uma de várias modalidades de uma WTRU, tal como descrito acima; (iii) um dispositivo com capacidade sem fio e/ou com fio (por exemplo, cabeável) configurado, entre outros, com algumas das ou todas as estruturas e funcionalidades de uma WTRU, tal como descrito acima; (iii) um dispositivo com capacidade sem fio e/ou com fio configurado com menos que todas as estruturas e funcionalidades de uma WTRU, tal como descrito acima; ou (iv) seus semelhantes.

[0145]Os versados na técnica perceberão que, em geral, os termos usados neste documento e, em especial, nas reivindicações anexas (por exemplo, no corpo das reivindicações anexas) geralmente destinam-se à interpretação como termos “abertos” (por exemplo, o termo “incluindo” deve ser interpretado como “incluindo, entre outros”, o termo “com” deve ser interpretado como “com pelo menos”, o termo “inclui” deve ser interpretado como “inclui, entre outros”, etc.). Os versados na técnica também entenderão que, se houver a intenção de especificar determinado número de um elemento reivindicado introduzido, esse será mencionado explicitamente na reivindicação e, em sua ausência, é porque não houve essa intenção. Por exemplo, quando só um item for tencionado, o termo "único" ou léxico semelhante pode ser usado. Melhor explicando, as reivindicações anexas a seguir e/ou as descrições neste documento podem conter o uso dos sintagmas introdutórios "ao menos" e "um ou mais" para introduzir elementos reivindicados. No

entanto, o uso desses sintagmas não deve ser interpretado de modo a concluir que a introdução de um elemento reivindicado com os artigos indefinidos "um" ou "uma" limite qualquer reivindicação específica que contenha o referido elemento reivindicado introduzido a modalidades contendo apenas um desse elemento, mesmo quando a mesma reivindicação incluir os sintagmas introdutórios "um ou mais" ou "ao menos um" e artigos indefinidos, como "um" ou "uma" (por exemplo, "um" e/ou "uma" devem ser interpretados como "ao menos um(a)" ou "um(a) ou mais"). O mesmo é verdade quanto ao uso de artigos definidos para introduzir elementos reivindicados. Além disso, ainda que um número específico de um elemento reivindicado introduzido seja mencionado explicitamente, os versados na técnica entenderão que a referida citação deve ser interpretada como “ao menos o número mencionado” (por exemplo, a citação “dois elementos”, sem outros modificadores, significa “ao menos dois elementos” ou “dois ou mais elementos”). Ademais, nos casos em que utiliza-se uma convenção análoga a "ao menos um dentre A, B ou C etc.", em termos gerais, emprega-se essa construção com a intenção de que os versados na técnica entendam a convenção (por exemplo, "um sistema com ao menos um dentre A, B ou C" incluiria, entre outros, sistemas só com A, só com B, só com C, com A e B juntos, com A e C juntos, com B e C juntos e/ou com A, B e C juntos etc.). Nos casos em que utiliza-se uma convenção análoga a "ao menos um dentre A, B ou C etc.", em termos gerais, emprega-se essa construção com a intenção de que os versados na técnica entendam a convenção (por exemplo, "um sistema com ao menos um dentre A, B ou C" incluiria, entre outros, sistemas só com A, só com B, só com C, com A e B juntos, com A e C juntos, com B e C juntos e/ou com A, B e C juntos etc.). Os versados na técnica perceberão ainda que praticamente qualquer palavra e/ou sintagma disjuntivo que apresente dois ou mais termos alternativos, seja na descrição, nas reivindicações ou nos desenhos, deve ser interpretado de modo a contemplar as possibilidades de

inclusão de um dos termos, de um termo ou outro ou de ambos os termos. Por exemplo, o sintagma "A ou B" será interpretado incluindo as possibilidades "A" ou "B" ou "A e B". Além disso, os termos "qualquer um(a) de" seguidos por uma listagem de uma pluralidade de itens e/ou uma pluralidade de categorias de itens, conforme usados neste documento, visam a incluir "qualquer um(a) de", "qualquer combinação de", "qualquer múltiplo de" e/ou "qualquer combinação de múltiplos de" os itens e/ou as categorias de itens, individualmente ou em conjunto a outros itens e/ou outras categorias de itens. Além disso, conforme usado neste documento, o termo "conjunto" ou “grupo” visa a incluir qualquer número de itens, inclusive zero. Em aditamento, conforme usado neste documento, o termo "número" visa a incluir qualquer número, inclusive zero.

[0146]Além disso, quando traços ou aspectos da invenção são descritos em termos de grupos de Markush, os versados na técnica entenderão que a invenção também é assim descrita em termos de qualquer membro individual ou subgrupo de membros do grupo de Markush.

[0147]Como os versados na técnica perceberão, para todos os fins, tal como em termos de propiciar uma descrição por escrito, todas as faixas reveladas neste documento também abrangem toda e qualquer subfaixa dessas possível e combinações dessas subfaixas. Qualquer faixa listada pode ser facilmente reconhecida como descrevendo e permitindo suficientemente que a mesma faixa seja dividida em ao menos duas metades, três terços, quatro quartos, cinco quintas partes, dez décimos etc. iguais. À guisa de exemplo não exaustivo, cada faixa discutida neste documento pode ser prontamente dividida em um terço inferior, um terço médio e um terço superior etc. Como os versados na técnica perceberão, todos os termos como "até", "ao menos", "maior que", "menor que" e seus semelhantes incluem o número citado e referem-se a faixas que podem ser subsequentemente divididas em subfaixas, conforme discutido acima. Por fim, como os versados na

técnica perceberão, uma faixa inclui cada membro individual. Sendo assim, por exemplo, um grupo com 1 a 3 células refere-se a grupos com 1, 2 ou 3 células. À semelhança, um grupo com 1 a 5 células refere-se a grupos com 1, 2, 3, 4 ou 5 células, e assim por diante.

[0148]Ademais, as reivindicações não devem ser interpretadas como limitadas à ordem ou aos elementos dados, salvo menção em contrário. Além disso, o uso do termo "significa" em qualquer reivindicação visa a invocar o 35 U.S.C. §112, ¶ 6 ou o formato de reivindicação significado-mais-função, e qualquer reivindicação sem o termo "significa" não tem essa intenção.

[0149]Um processador em associação a *software* pode ser usado para implementar um transceptor de frequência de rádio para uso em uma unidade transmissora/receptora sem fio (WTRU), equipamento do usuário (UE), terminal, estação de base, Entidade de Gestão de Mobilidade (MME) ou Núcleo de Pacotes Evoluído (EPC), ou qualquer computador hospedeiro. A WTRU pode ser usada junto com módulos, implementada em *hardware* e/ou *software* incluindo um Rádio Definido por Software (SDR), e outros componentes tais como uma câmera, um módulo de câmera de vídeo, um videofone, um viva-voz, um dispositivo de vibração, um alto-falante, um microfone, um transceptor de televisão, um *headset hands-free*, um teclado, um módulo Bluetooth®, uma unidade de rádio de frequência modulada (FM), um Módulo de Comunicação por Campo Próximo (NFC), uma unidade de exibição de cristal líquido (LCD), uma unidade de exibição de diodos orgânicos emissores de luz (OLED), um reprodutor de música digital, um reprodutor de mídia, um módulo reprodutor de jogos eletrônicos, um navegador de Internet, e/ou qualquer módulo de Rede de Área Local Sem Fio (WLAN) ou Banda Ultra Larga (UWB).

[0150]Ao longo de toda a revelação, os versados na técnica entendem que certas modalidades representativas podem ser usadas como alternativa ou em combinação a outras modalidades representativas.

[0151]Além disso, os métodos descritos neste documento podem ser implementados em um programa de computador, *software* ou *firmware* incorporado a um meio legível por computador para execução por um computador ou processador. Exemplos de meios de armazenamento legíveis por computador não transitórios incluem, entre outros, memória somente para leitura (ROM), memória de acesso aleatório (RAM), um registro, memória *cache*, dispositivos de memória semicondutores, meios magnéticos como discos rígidos internos e discos removíveis, meios magneto-ópticos, e meios ópticos como discos de CD-ROM e discos digitais versáteis (DVDs). Um processador em associação a software pode ser usado para implementar um transceptor de frequência de rádio para uso em uma WTRU, UE, terminal, estação de base, RNC ou qualquer computador hospedeiro.

REIVINDICAÇÕES

1. Método para uso em uma sessão de veículo a tudo, V2X, em andamento, o método sendo **CARACTERIZADO** por compreender:

estabelecer comunicação entre uma unidade transmissora/receptora sem fio, WTRU, de origem e uma WTRU ponto usando um identificador, ID, de camada 2, L2, da WTRU de origem atual, um ID de L2 da WTRU ponto atual e um ID de sessão atual;

em uma condição em que um evento disparador ocorre:

gerar, na WTRU de origem, um novo ID de L2 da WTRU de origem e um novo byte mais significativo de um novo ID de sessão;

transmitir, da WTRU de origem à WTRU ponto, o novo ID de L2 da WTRU de origem e o novo byte mais significativo do novo ID de sessão;

receber, da WTRU ponto, um novo ID de L2 ponto e um novo byte menos significativo do novo ID de sessão;

transmitir, da WTRU de origem à WTRU ponto, uma confirmação do novo ID de L2 da WTRU ponto e do novo byte menos significativo do novo ID de sessão; e

estabelecer comunicação com a WTRU ponto usando o novo ID de L2 da WTRU de origem, o novo ID de L2 da WTRU ponto e o novo ID de sessão que compreende o novo byte mais significativo e o novo byte menos significativo.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que estabelecer comunicação entre a WTRU de origem e a WTRU ponto compreende usar o ID de L2 da WTRU de origem atual, o ID de L2 da WTRU ponto atual e o ID de sessão atual até depois de transmitir a confirmação.

3. Método, de acordo com as reivindicações 1 ou 2, **CARACTERIZADO** pelo fato de que o novo ID de L2 da WTRU de origem, o novo ID de L2 da WTRU ponto e o novo ID de sessão encontram-se criptografados até depois de transmitir a confirmação.

4. Método, de acordo com qualquer reivindicação anterior, **CARACTERIZADO** pelo fato de que:

transmitir o novo ID de L2 da WTRU de origem e o byte mais significativo do novo ID de sessão à WTRU ponto compreende transmitir usando um de um procedimento *keep-alive*, um procedimento de privacidade, um procedimento de atualização por enlace PC5 ou outro procedimento de comunicação usado entre a WTRU de origem e a WTRU ponto.

5. Método, de acordo com qualquer uma das reivindicações anteriores, **CARACTERIZADO** pelo fato de que uma condição em que um evento disparador ocorre compreende qualquer uma de:

uma condição em que um temporizador expira;

uma condição em que uma camada superior ou uma camada de aplicativo de um aplicativo V2X solicita um novo ID de L2;

uma condição em que a WTRU de origem move-se a uma nova área geográfica;

uma condição em que a WTRU de origem recebe novos parâmetros de aprovisionamento de uma função de controle V2X ou servidor de aplicativo V2X; ou

uma condição em que a WTRU de origem recebe um pedido da WTRU ponto para mudar um ID de L2.

6. Método, de acordo com qualquer uma das reivindicações anteriores, **CARACTERIZADO** pelo fato de que o ID de sessão é um ID de sessão de contexto de segurança.

7. Método, de acordo com qualquer uma das reivindicações anteriores, **CARACTERIZADO** pelo fato de que estabelecer comunicação com a WTRU ponto compreende estabelecer comunicação por um enlace de referência PC5.

8. Unidade transmissora/receptora sem fio, WTRU, de origem compreendendo um sistema de circuitos, incluindo um transmissor, um receptor, um

processador e memória, a WTRU de origem sendo **CARACTERIZADA** por ser configurada para:

estabelecer comunicação, usando o transceptor e receptor, entre a WTRU de origem e uma WTRU ponto usando um identificador, ID, de camada 2, L2, da WTRU de origem atual, um ID de L2 da WTRU ponto atual e um ID de sessão atual;

em uma condição em que um evento disparador ocorre:

gerar, na WTRU de origem, um novo ID de L2 da WTRU de origem e um novo byte mais significativo de um novo ID de sessão;

transmitir, da WTRU de origem à WTRU ponto, o novo ID de L2 da WTRU de origem e o novo byte mais significativo do novo ID de sessão;

receber, da WTRU ponto, um novo ID de L2 da WTRU ponto e um novo byte menos significativo do novo ID de sessão;

transmitir, da WTRU de origem à WTRU ponto, uma confirmação do novo ID de L2 da WTRU ponto e do novo byte menos significativo do novo ID de sessão; e

estabelecer comunicação com a WTRU ponto usando o novo ID de L2 da WTRU de origem, o novo ID de L2 da WTRU ponto e o novo ID de sessão que compreende o novo byte mais significativo e o novo byte menos significativo.

9. WTRU de origem, de acordo com a reivindicação 8, **CARACTERIZADA** pelo fato de que estabelecer comunicação entre a WTRU de origem e a WTRU ponto compreende usar o ID de L2 da WTRU de origem atual, o ID de L2 da WTRU ponto atual e o ID de sessão atual até depois de transmitir a confirmação.

10. WTRU de origem, de acordo com as reivindicações 8 ou 9, **CARACTERIZADA** pelo fato de que o novo ID de L2 da WTRU de origem, o novo ID de L2 da WTRU ponto e o novo ID de sessão encontram-se criptografados até depois de transmitir a confirmação.

11. WTRU de origem, de acordo com qualquer uma das reivindicações de 8 a 10, **CARACTERIZADA** pelo fato de que**:**

o evento disparador compreende ao menos um de:

a expiração de um temporizador;

um pedido por um novo ID de L2 feito por uma camada superior ou camada de aplicativo de um aplicativo V2X;

o deslocamento da WTRU de origem a uma nova área geográfica;

o recebimento, na WTRU de origem, de novos parâmetros de aprovisionamento advindos de uma função de controle V2X ou servidor de aplicativo V2X; ou

o recebimento de um pedido, na WTRU de origem, feito pela WTRU ponto para mudar um ID de L2.

12. WTRU de origem, de acordo com qualquer uma das reivindicações de 8 a 11, **CARACTERIZADA** por ser configurada para:

comunicar o novo ID de L2 da WTRU de origem e o novo byte mais significativo do novo ID de sessão à WTRU ponto usando um de um procedimento *keep-alive*, um procedimento de privacidade, um procedimento de atualização por enlace PC5 ou outro procedimento de comunicação usado entre a WTRU de origem e a WTRU ponto.

13. WTRU de origem, de acordo com qualquer uma das reivindicações de 8 a 12, **CARACTERIZADA** pelo fato de que o ID de sessão é um ID de sessão de contexto de segurança.

14. WTRU de origem, de acordo com qualquer uma das reivindicações de 8 a 13, **CARACTERIZADA** por comunicar-se com a WTRU ponto por um enlace de referência PC5.

15. Meio de armazenamento legível por computador **CARACTERIZADO** por compreender instruções que, quando executadas por um computador, fazem com que este execute o método de acordo com qualquer uma das reivindicações de 1 a 7.

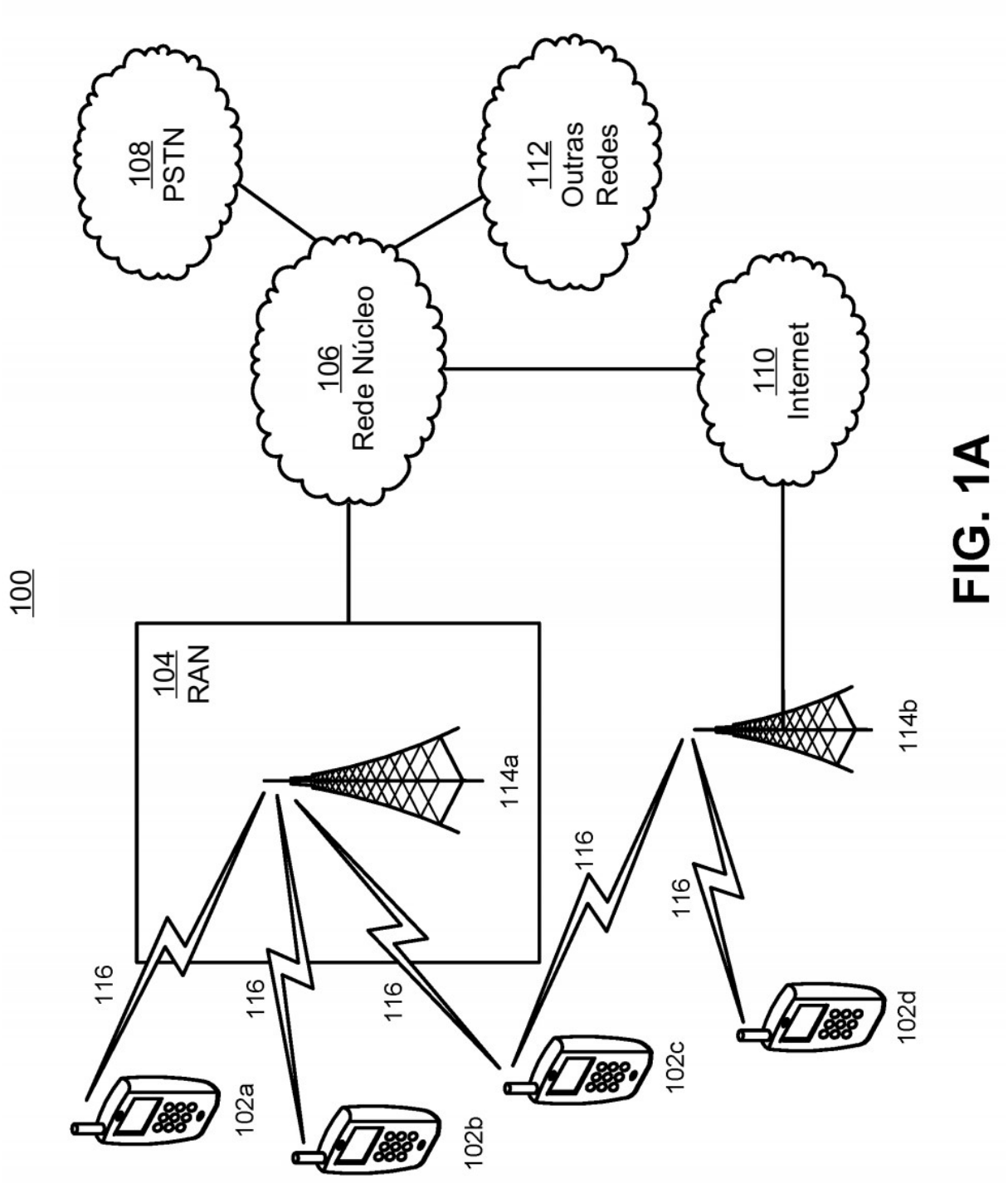

100
108
PSTN
112
Outras
Redes
106
Rede Núcleo
110
Internet
104
RAN
114a
114b
116
116
116
116
116
102a
102b
102c
102d

FIG. 1A

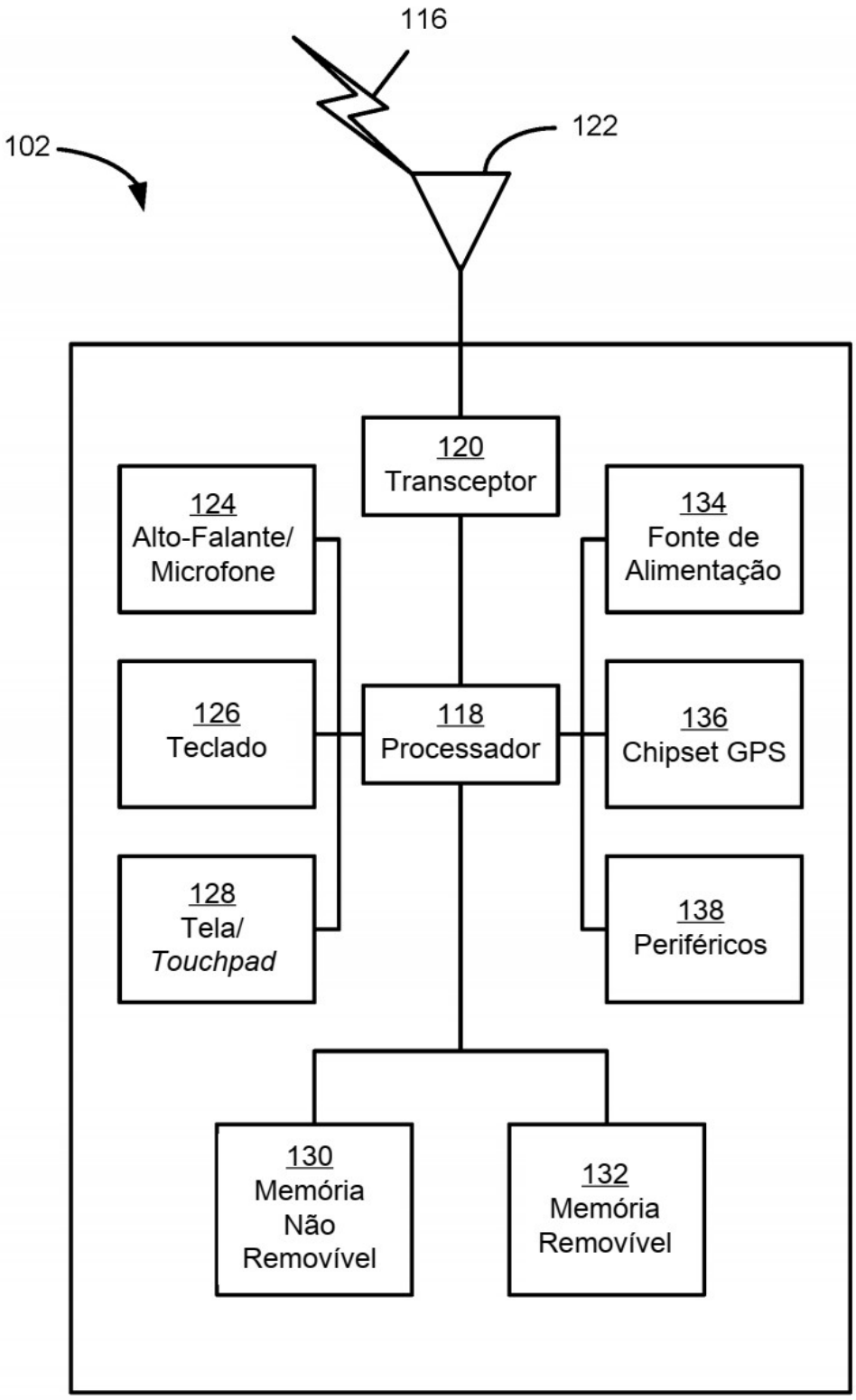

116
122
102
120
Transceptor
124
Alto-Falante/
Microfone
134
Fonte de
Alimentação
126
Teclado
118
Processador
136
Chipset GPS
128
Tela/
Touchpad
138
Periféricos
130
Memória
Não
Removível
132
Memória
Removível

FIG. 1B

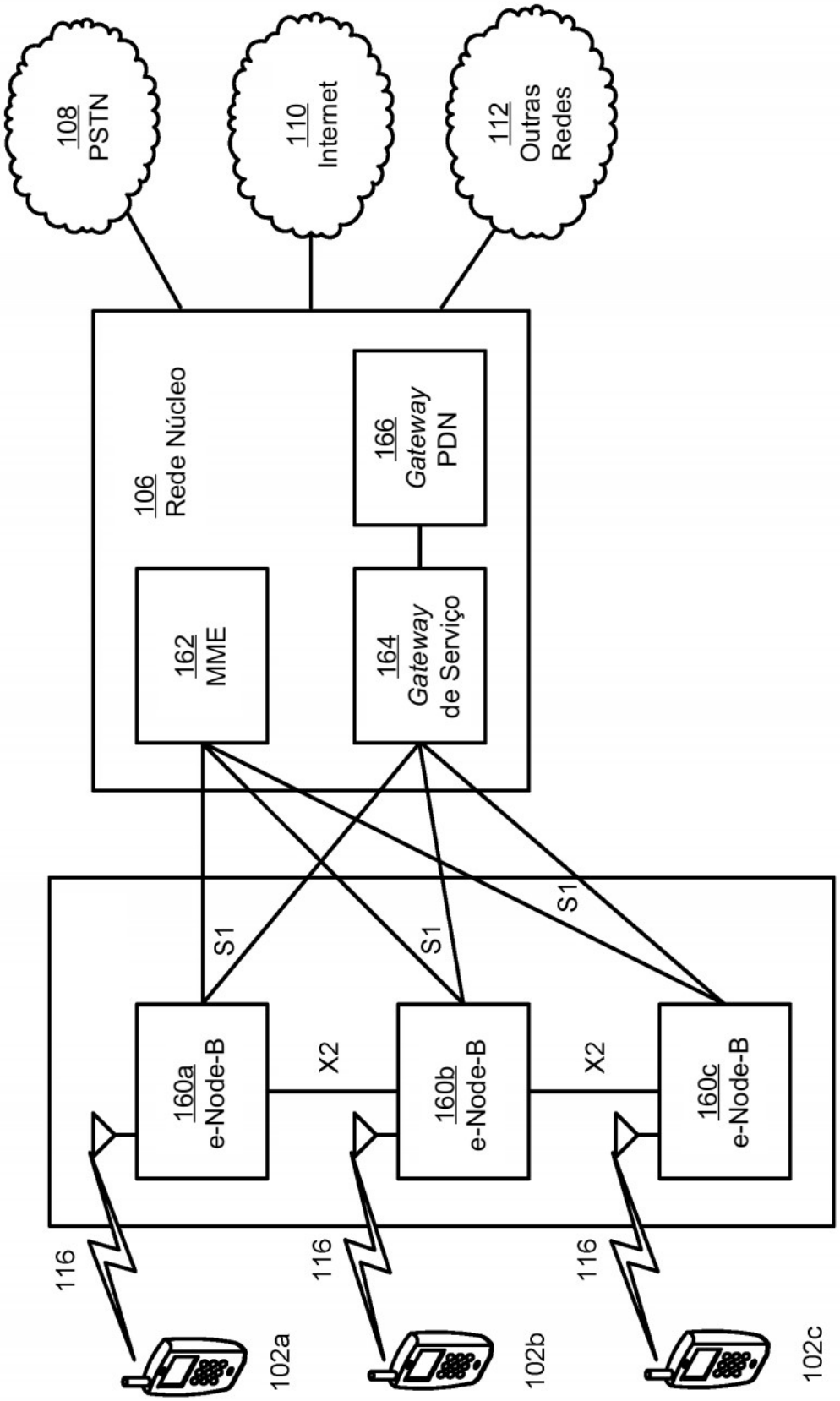

108
PSTN
110
Internet
112
Outras
Redes
106
Rede Núcleo
166
Gateway
PDN
162
MME
164
Gateway
de Serviço
S1
S1
S1
160a
e-Node-B
160b
e-Node-B
160c
e-Node-B
X2
X2
116
116
116
102a
102b
102c

FIG. 1C

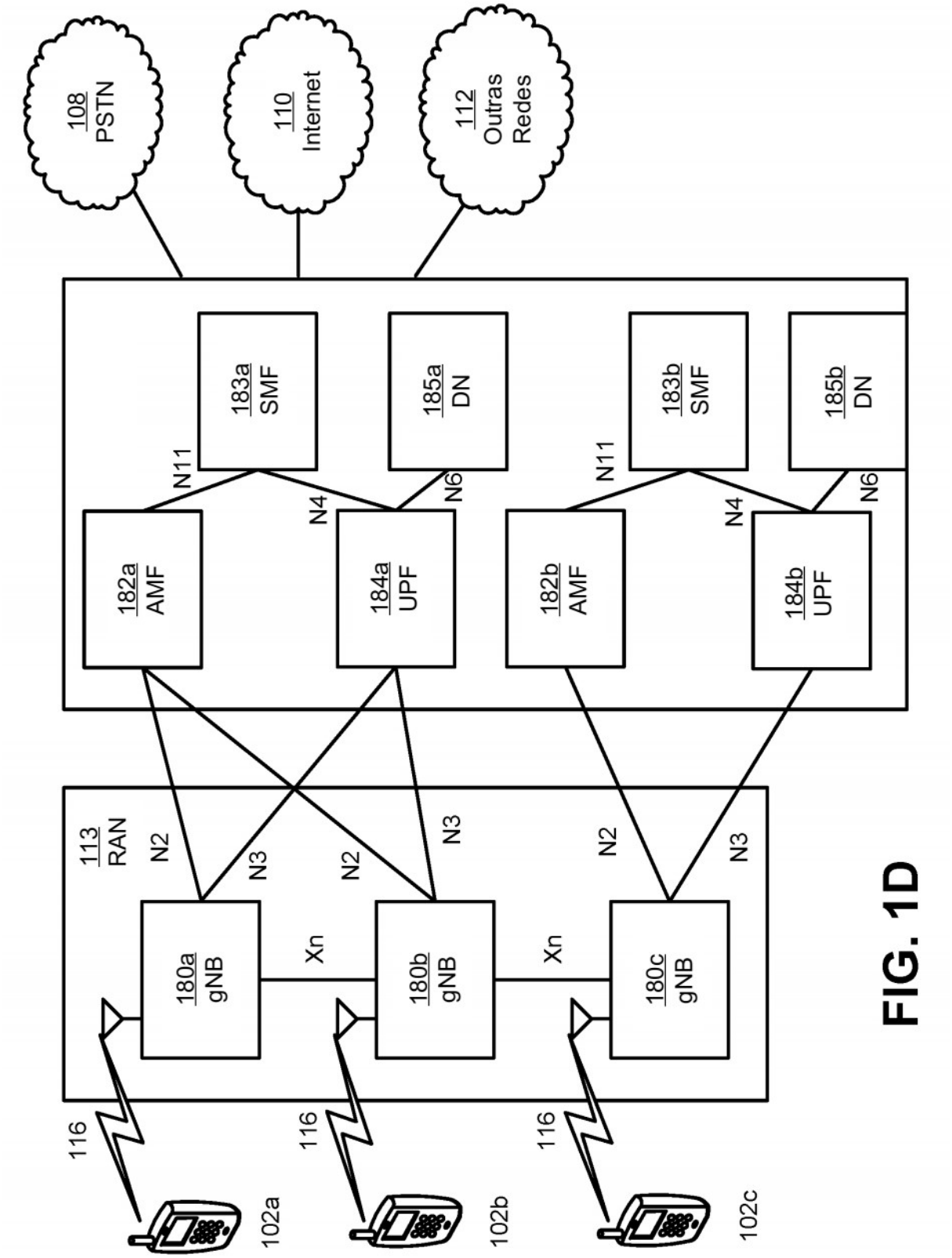

108
PSTN
110
Internet
112
Outras
Redes
183a
SMF
185a
DN
183b
SMF
185b
DN
N11
N6
N4
N11
N6
N4
182a
AMF
184a
UPF
182b
AMF
184b
UPF
113
RAN
N2
N3
N2
N3
N2
N3
180a
gNB
Xn
180b
gNB
Xn
180c
gNB
116
116
116
102a
102b
102c

FIG. 1D

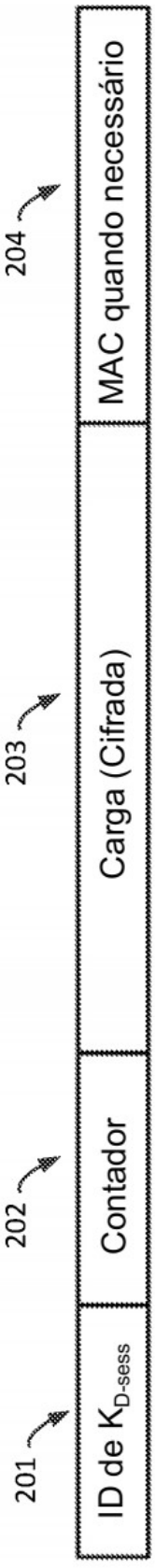

201
ID de K_{D-sess}
202
Contador
203
Carga (Cifrada)
204
MAC quando necessário

FIG. 2

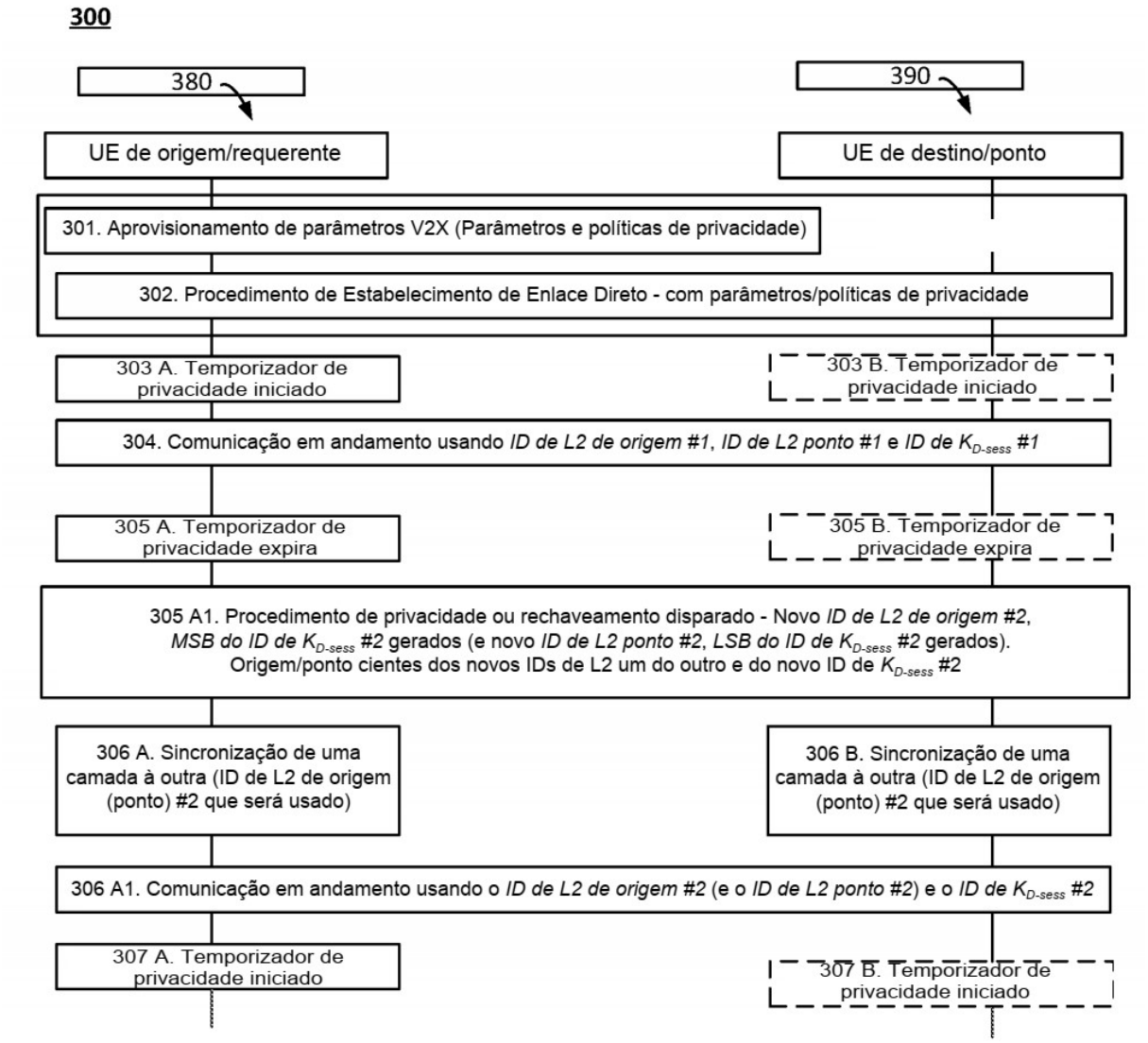

300
380
390
UE de origem/requerente
UE de destino/ponto
301. Aprovisionamento de parâmetros V2X (Parâmetros e políticas de privacidade)
302. Procedimento de Estabelecimento de Enlace Direto - com parâmetros/políticas de privacidade
303 A. Temporizador de privacidade iniciado
303 B. Temporizador de privacidade iniciado
304. Comunicação em andamento usando ID de L2 de origem #1, ID de L2 ponto #1 e ID de K_{D-sess} #1
305 A. Temporizador de privacidade expira
305 B. Temporizador de privacidade expira
305 A1. Procedimento de privacidade ou rechaveamento disparado - Novo ID de L2 de origem #2, MSB do ID de K_{D-sess} #2 gerados (e novo ID de L2 ponto #2, LSB do ID de K_{D-sess} #2 gerados). Origem/ponto cientes dos novos IDs de L2 um do outro e do novo ID de K_{D-sess} #2
306 A. Sincronização de uma camada à outra (ID de L2 de origem (ponto) #2 que será usado)
306 B. Sincronização de uma camada à outra (ID de L2 de origem (ponto) #2 que será usado)
306 A1. Comunicação em andamento usando o ID de L2 de origem #2 (e o ID de L2 ponto #2) e o ID de K_{D-sess} #2
307 A. Temporizador de privacidade iniciado
307 B. Temporizador de privacidade iniciado

FIG. 3

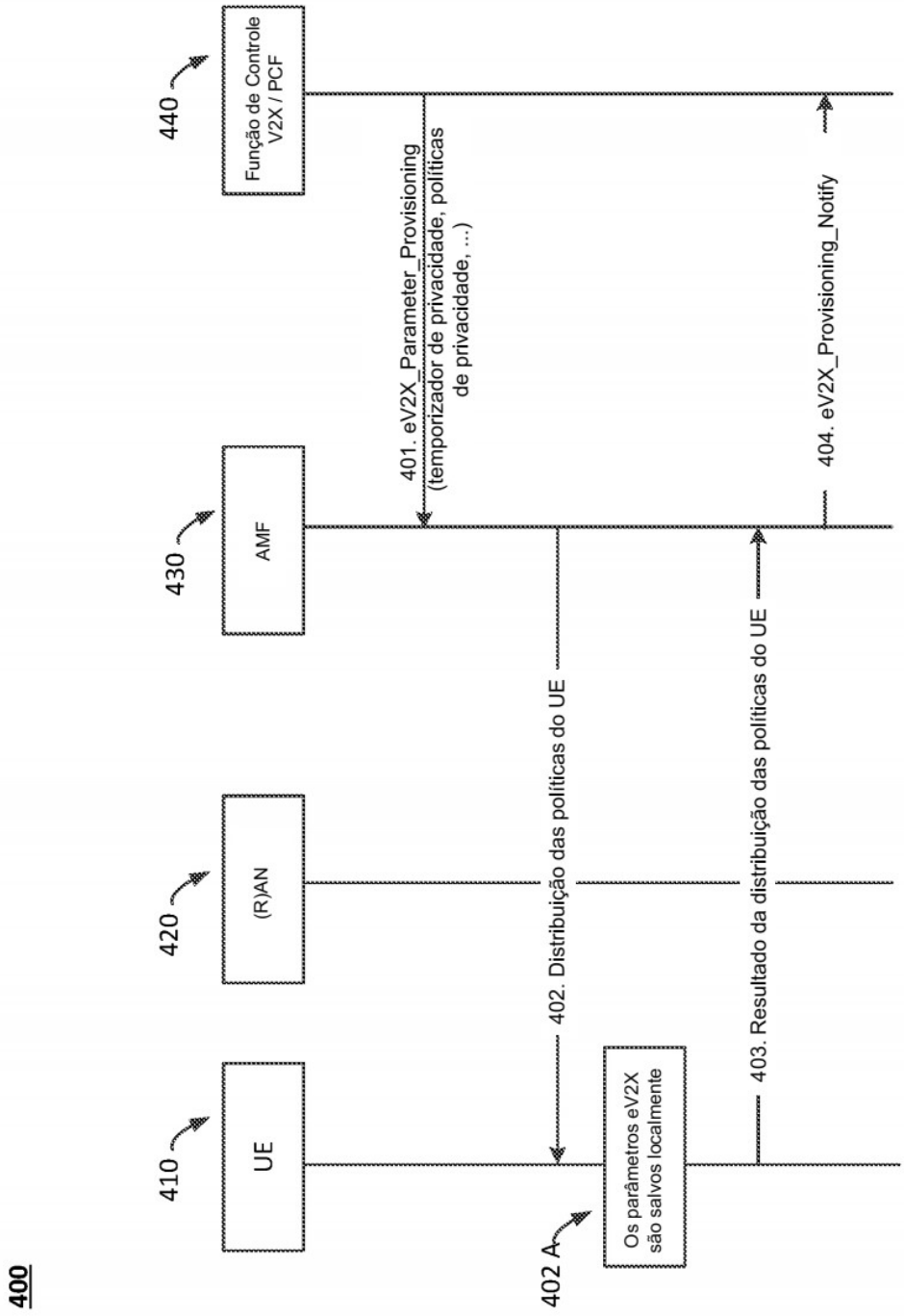

400
410
UE
420
(R)AN
430
AMF
440
Função de Controle V2X / PCF
401. eV2X_Parameter_Provisioning (temporizador de privacidade, políticas de privacidade, ...)
402. Distribuição das políticas do UE
402 A
Os parâmetros eV2X são salvos localmente
403. Resultado da distribuição das políticas do UE
404. eV2X_Provisioning_Notify

FIG. 4

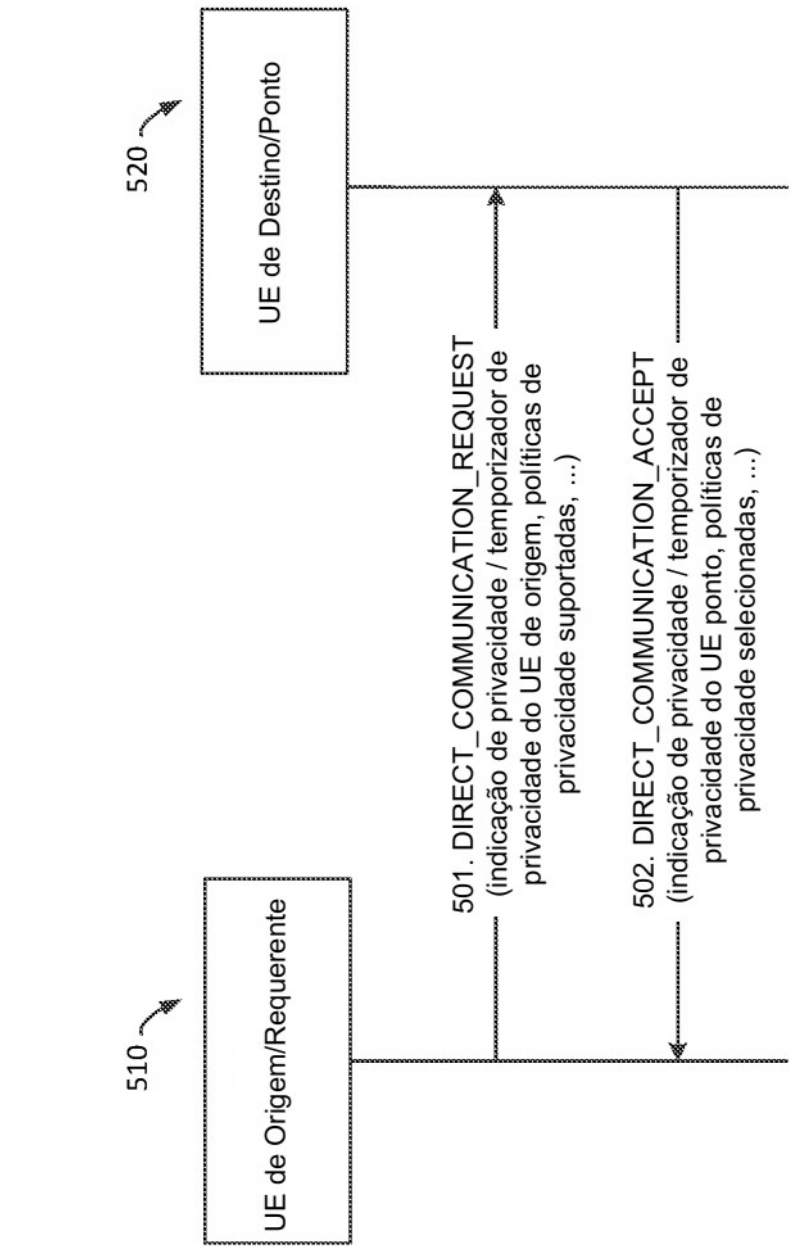

500
510
UE de Origem/Requerente
520
UE de Destino/Ponto
501. DIRECT_COMMUNICATION_REQUEST
(indicação de privacidade / temporizador de privacidade do UE de origem, políticas de privacidade suportadas, ...)
502. DIRECT_COMMUNICATION_ACCEPT
(indicação de privacidade / temporizador de privacidade do UE ponto, políticas de privacidade selecionadas, ...)

FIG. 5

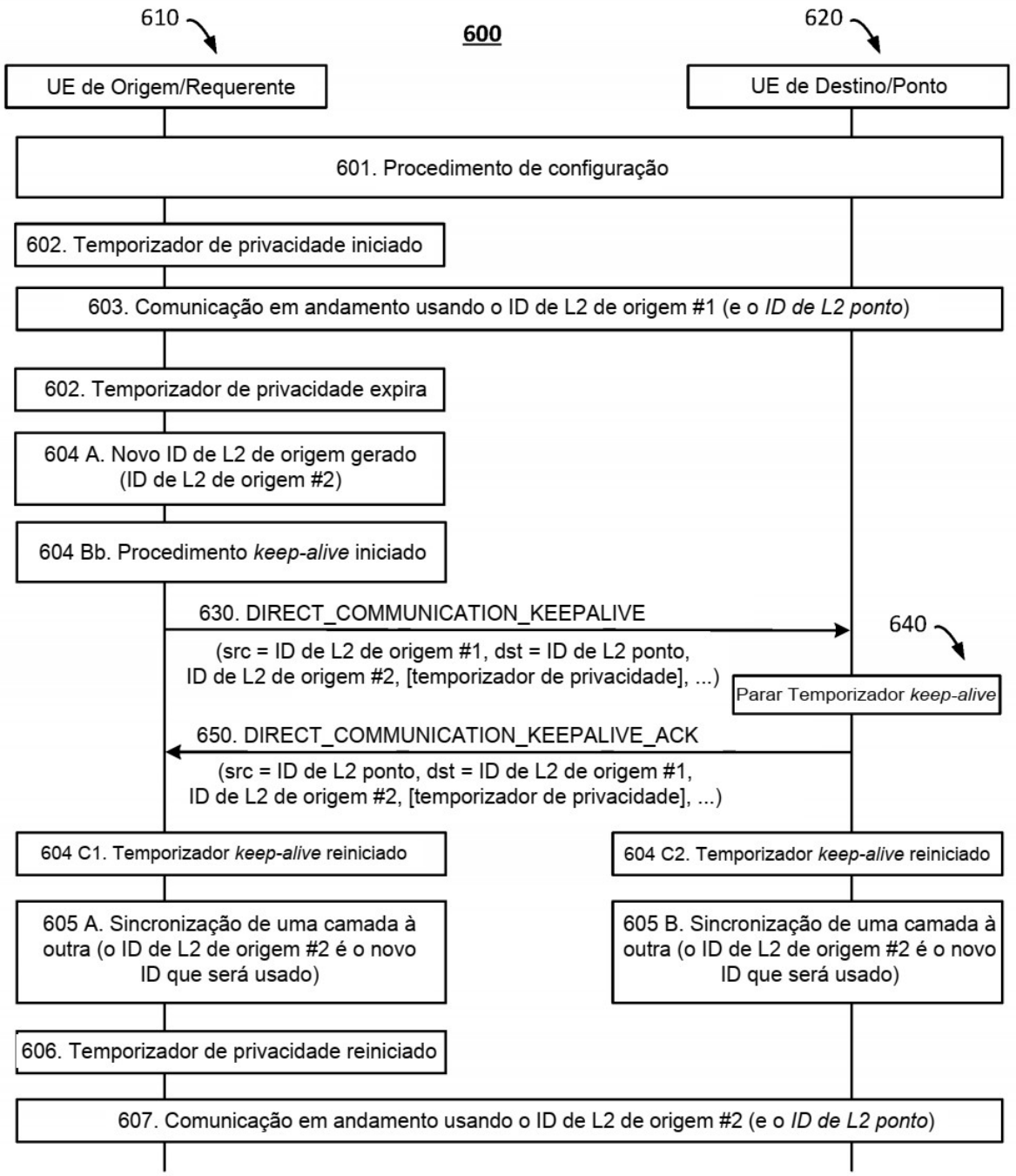

610
600
620
UE de Origem/Requerente
UE de Destino/Ponto
601. Procedimento de configuração
602. Temporizador de privacidade iniciado
603. Comunicação em andamento usando o ID de L2 de origem #1 (e o *ID de L2 ponto*)
602. Temporizador de privacidade expira
604 A. Novo ID de L2 de origem gerado (ID de L2 de origem #2)
604 Bb. Procedimento *keep-alive* iniciado
630. DIRECT_COMMUNICATION_KEEPALIVE
(src = ID de L2 de origem #1, dst = ID de L2 ponto, ID de L2 de origem #2, [temporizador de privacidade], ...)
640
Parar Temporizador *keep-alive*
650. DIRECT_COMMUNICATION_KEEPALIVE_ACK
(src = ID de L2 ponto, dst = ID de L2 de origem #1, ID de L2 de origem #2, [temporizador de privacidade], ...)
604 C1. Temporizador *keep-alive* reiniciado
604 C2. Temporizador *keep-alive* reiniciado
605 A. Sincronização de uma camada à outra (o ID de L2 de origem #2 é o novo ID que será usado)
605 B. Sincronização de uma camada à outra (o ID de L2 de origem #2 é o novo ID que será usado)
606. Temporizador de privacidade reiniciado
607. Comunicação em andamento usando o ID de L2 de origem #2 (e o *ID de L2 ponto*)

FIG. 6

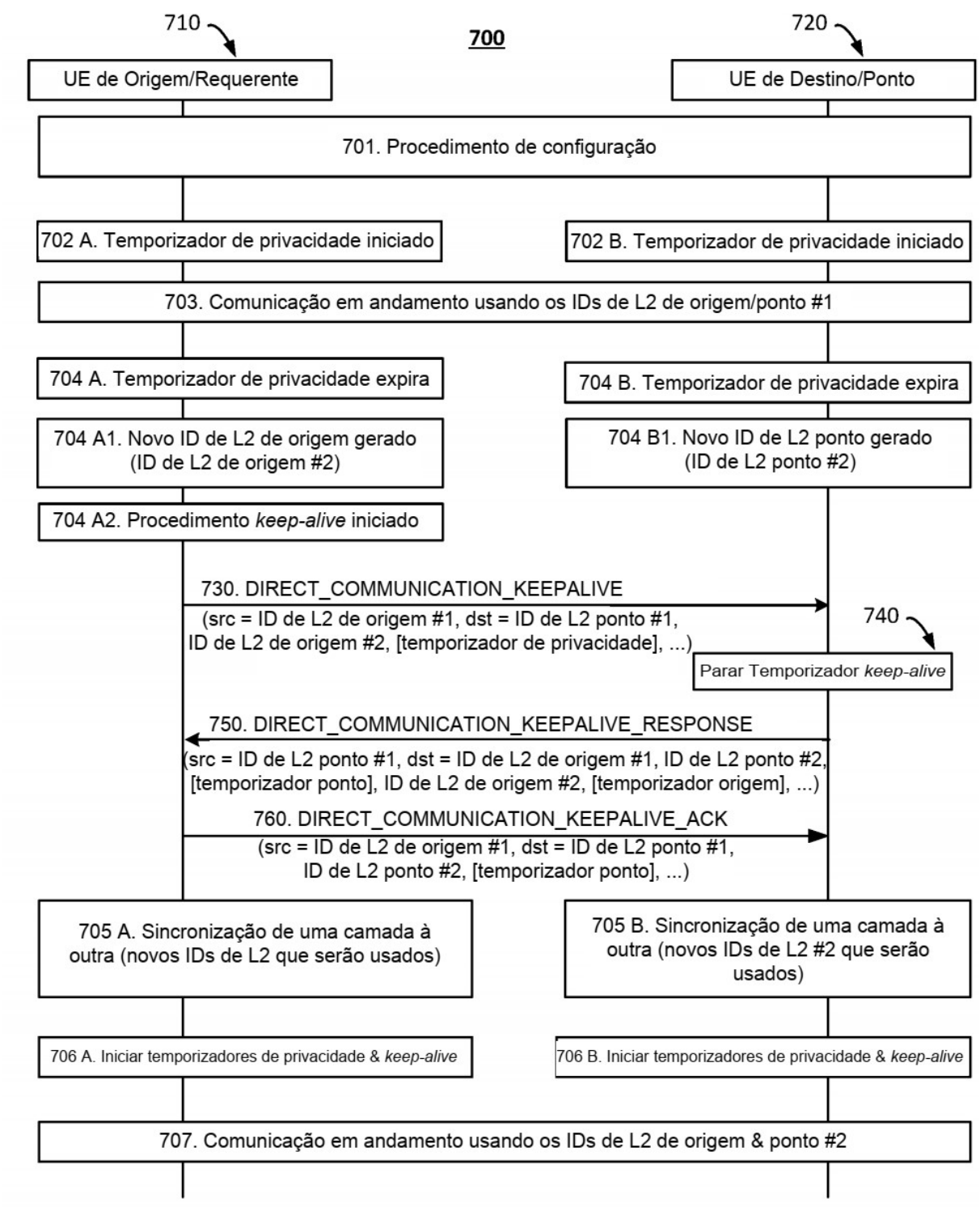

700
710
UE de Origem/Requerente
720
UE de Destino/Ponto
701. Procedimento de configuração
702 A. Temporizador de privacidade iniciado
702 B. Temporizador de privacidade iniciado
703. Comunicação em andamento usando os IDs de L2 de origem/ponto #1
704 A. Temporizador de privacidade expira
704 B. Temporizador de privacidade expira
704 A1. Novo ID de L2 de origem gerado (ID de L2 de origem #2)
704 B1. Novo ID de L2 ponto gerado (ID de L2 ponto #2)
704 A2. Procedimento keep-alive iniciado
730. DIRECT_COMMUNICATION_KEEPALIVE
(src = ID de L2 de origem #1, dst = ID de L2 ponto #1, ID de L2 de origem #2, [temporizador de privacidade], ...)
740
Parar Temporizador keep-alive
750. DIRECT_COMMUNICATION_KEEPALIVE_RESPONSE
(src = ID de L2 ponto #1, dst = ID de L2 de origem #1, ID de L2 ponto #2, [temporizador ponto], ID de L2 de origem #2, [temporizador origem], ...)
760. DIRECT_COMMUNICATION_KEEPALIVE_ACK
(src = ID de L2 de origem #1, dst = ID de L2 ponto #1, ID de L2 ponto #2, [temporizador ponto], ...)
705 A. Sincronização de uma camada à outra (novos IDs de L2 que serão usados)
705 B. Sincronização de uma camada à outra (novos IDs de L2 #2 que serão usados)
706 A. Iniciar temporizadores de privacidade & keep-alive
706 B. Iniciar temporizadores de privacidade & keep-alive
707. Comunicação em andamento usando os IDs de L2 de origem & ponto #2

FIG. 7

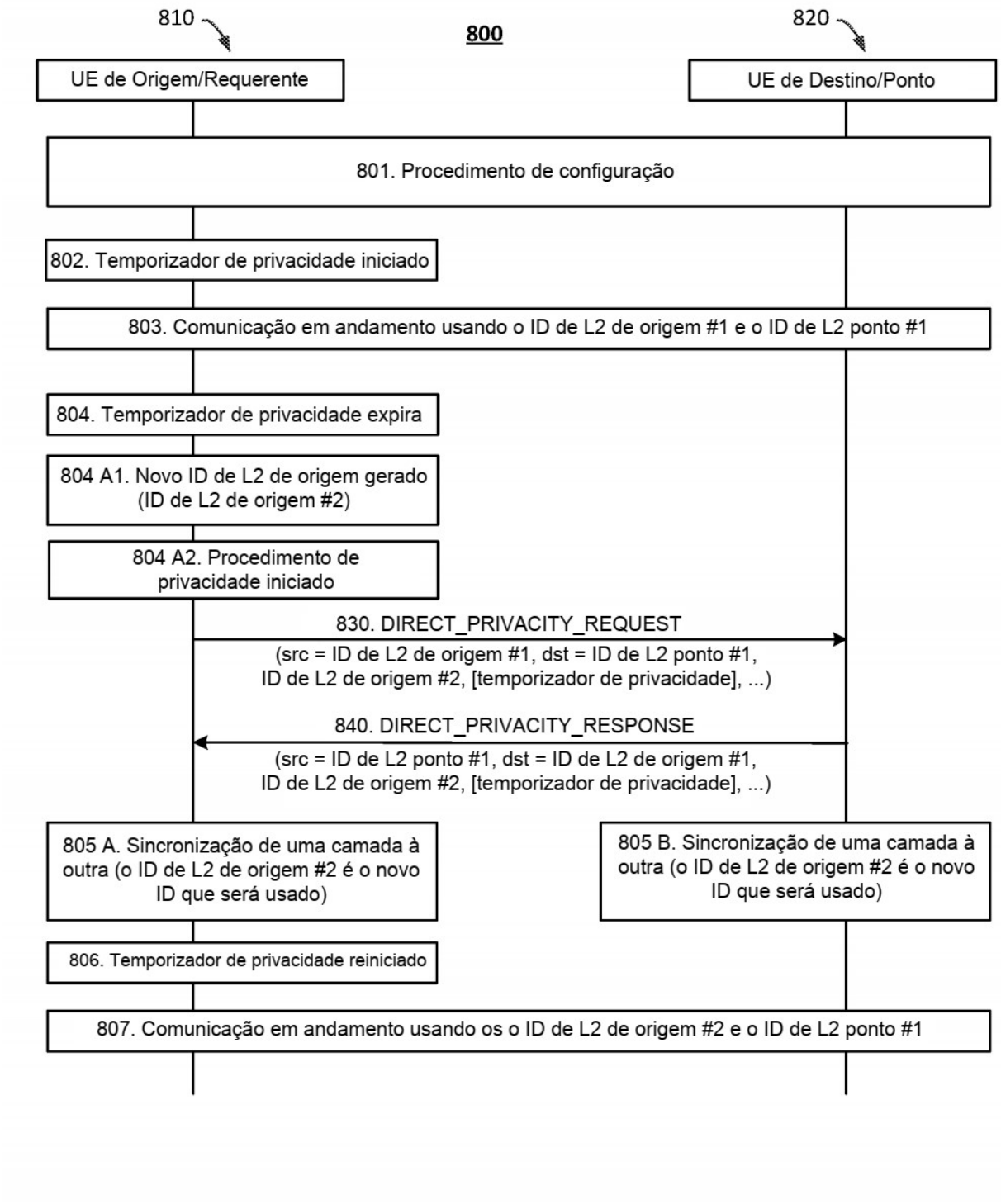

800
810
820
UE de Origem/Requerente
UE de Destino/Ponto
801. Procedimento de configuração
802. Temporizador de privacidade iniciado
803. Comunicação em andamento usando o ID de L2 de origem #1 e o ID de L2 ponto #1
804. Temporizador de privacidade expira
804 A1. Novo ID de L2 de origem gerado (ID de L2 de origem #2)
804 A2. Procedimento de privacidade iniciado
830. DIRECT_PRIVACITY_REQUEST
(src = ID de L2 de origem #1, dst = ID de L2 ponto #1, ID de L2 de origem #2, [temporizador de privacidade], ...)
840. DIRECT_PRIVACITY_RESPONSE
(src = ID de L2 ponto #1, dst = ID de L2 de origem #1, ID de L2 de origem #2, [temporizador de privacidade], ...)
805 A. Sincronização de uma camada à outra (o ID de L2 de origem #2 é o novo ID que será usado)
805 B. Sincronização de uma camada à outra (o ID de L2 de origem #2 é o novo ID que será usado)
806. Temporizador de privacidade reiniciado
807. Comunicação em andamento usando os o ID de L2 de origem #2 e o ID de L2 ponto #1

FIG. 8

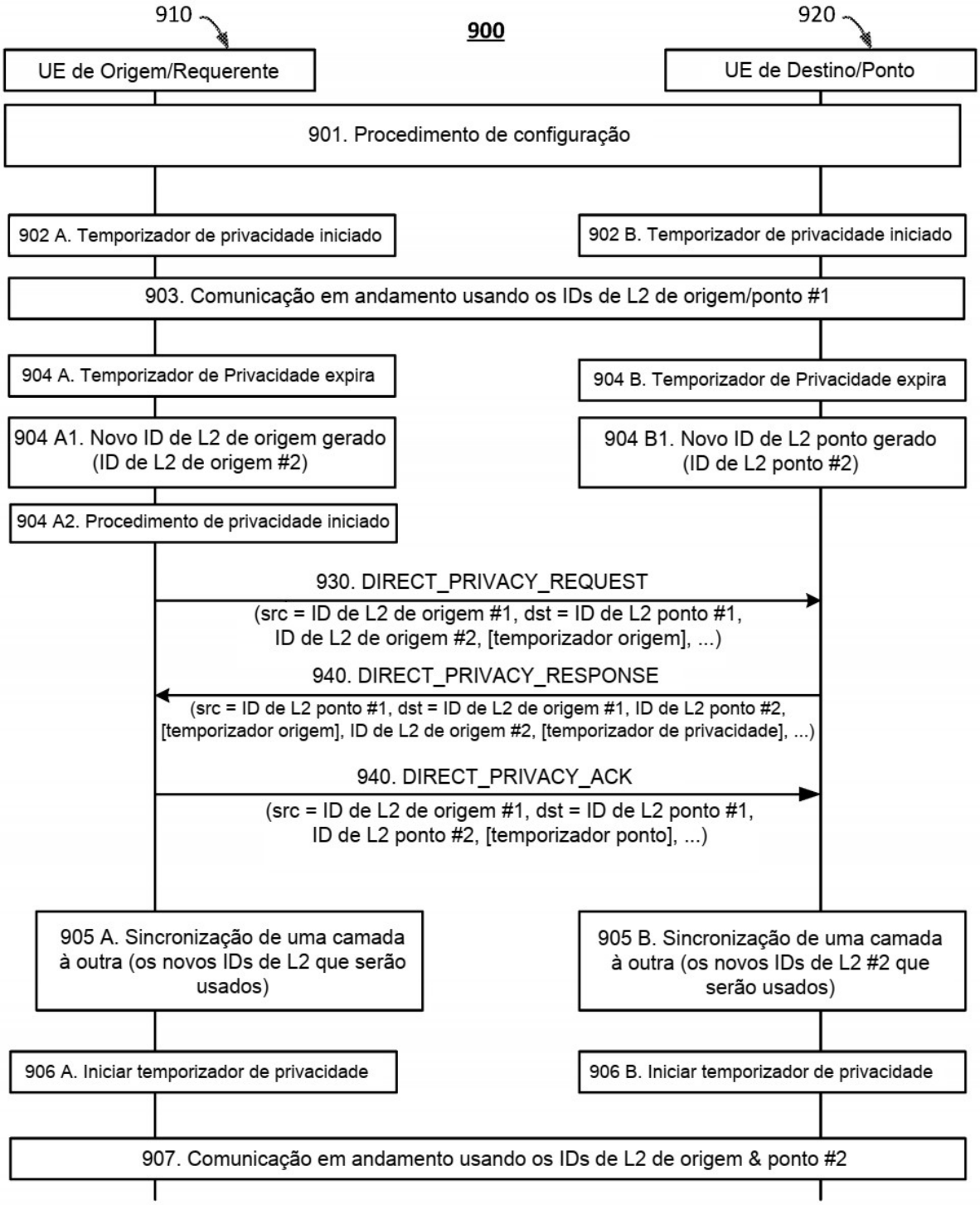

910
900
920
UE de Origem/Requerente
UE de Destino/Ponto
901. Procedimento de configuração
902 A. Temporizador de privacidade iniciado
902 B. Temporizador de privacidade iniciado
903. Comunicação em andamento usando os IDs de L2 de origem/ponto #1
904 A. Temporizador de Privacidade expira
904 B. Temporizador de Privacidade expira
904 A1. Novo ID de L2 de origem gerado (ID de L2 de origem #2)
904 B1. Novo ID de L2 ponto gerado (ID de L2 ponto #2)
904 A2. Procedimento de privacidade iniciado
930. DIRECT_PRIVACY_REQUEST
(src = ID de L2 de origem #1, dst = ID de L2 ponto #1, ID de L2 de origem #2, [temporizador origem], ...)
940. DIRECT_PRIVACY_RESPONSE
(src = ID de L2 ponto #1, dst = ID de L2 de origem #1, ID de L2 ponto #2, [temporizador origem], ID de L2 de origem #2, [temporizador de privacidade], ...)
940. DIRECT_PRIVACY_ACK
(src = ID de L2 de origem #1, dst = ID de L2 ponto #1, ID de L2 ponto #2, [temporizador ponto], ...)
905 A. Sincronização de uma camada à outra (os novos IDs de L2 que serão usados)
905 B. Sincronização de uma camada à outra (os novos IDs de L2 #2 que serão usados)
906 A. Iniciar temporizador de privacidade
906 B. Iniciar temporizador de privacidade
907. Comunicação em andamento usando os IDs de L2 de origem & ponto #2

FIG. 9

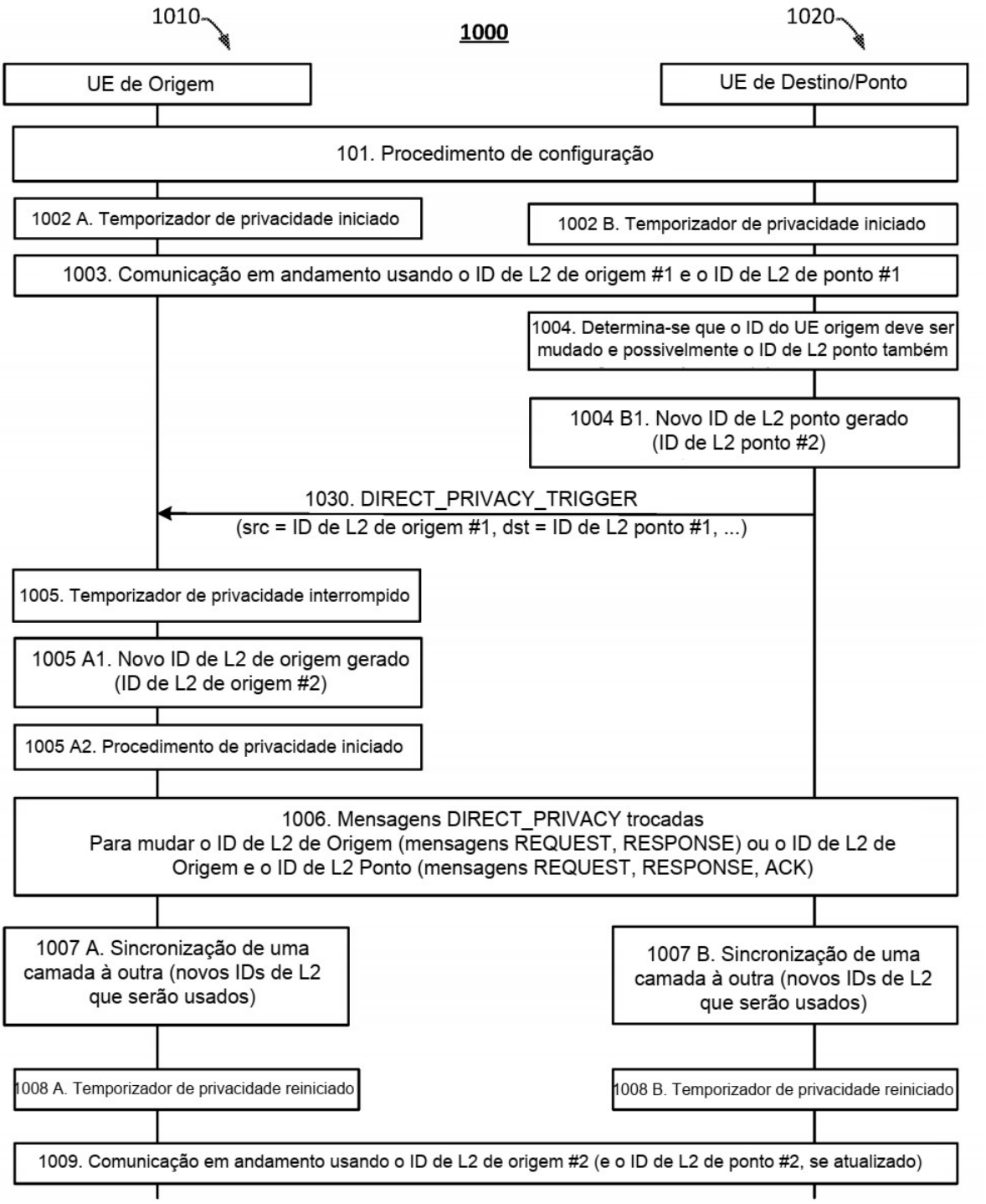

1010
1000
1020
UE de Origem
UE de Destino/Ponto
101. Procedimento de configuração
1002 A. Temporizador de privacidade iniciado
1002 B. Temporizador de privacidade iniciado
1003. Comunicação em andamento usando o ID de L2 de origem #1 e o ID de L2 de ponto #1
1004. Determina-se que o ID do UE origem deve ser mudado e possivelmente o ID de L2 ponto também
1004 B1. Novo ID de L2 ponto gerado (ID de L2 ponto #2)
1030. DIRECT_PRIVACY_TRIGGER
(src = ID de L2 de origem #1, dst = ID de L2 ponto #1, ...)
1005. Temporizador de privacidade interrompido
1005 A1. Novo ID de L2 de origem gerado (ID de L2 de origem #2)
1005 A2. Procedimento de privacidade iniciado
1006. Mensagens DIRECT_PRIVACY trocadas
Para mudar o ID de L2 de Origem (mensagens REQUEST, RESPONSE) ou o ID de L2 de Origem e o ID de L2 Ponto (mensagens REQUEST, RESPONSE, ACK)
1007 A. Sincronização de uma camada à outra (novos IDs de L2 que serão usados)
1007 B. Sincronização de uma camada à outra (novos IDs de L2 que serão usados)
1008 A. Temporizador de privacidade reiniciado
1008 B. Temporizador de privacidade reiniciado
1009. Comunicação em andamento usando o ID de L2 de origem #2 (e o ID de L2 de ponto #2, se atualizado)

FIG. 10

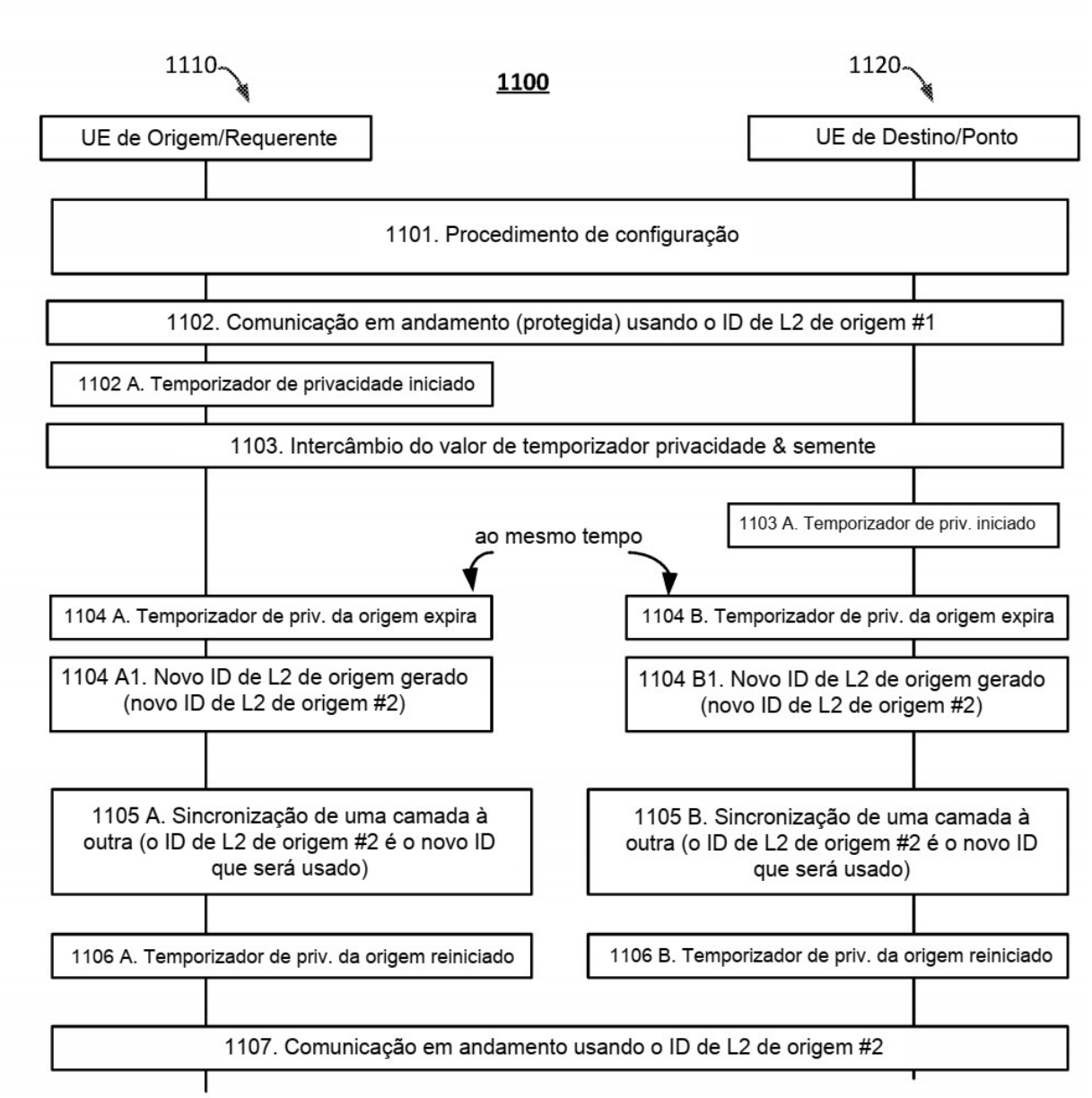

1110
1100
1120
UE de Origem/Requerente
UE de Destino/Ponto
1101. Procedimento de configuração
1102. Comunicação em andamento (protegida) usando o ID de L2 de origem #1
1102 A. Temporizador de privacidade iniciado
1103. Intercâmbio do valor de temporizador privacidade & semente
1103 A. Temporizador de priv. iniciado
ao mesmo tempo
1104 A. Temporizador de priv. da origem expira
1104 B. Temporizador de priv. da origem expira
1104 A1. Novo ID de L2 de origem gerado (novo ID de L2 de origem #2)
1104 B1. Novo ID de L2 de origem gerado (novo ID de L2 de origem #2)
1105 A. Sincronização de uma camada à outra (o ID de L2 de origem #2 é o novo ID que será usado)
1105 B. Sincronização de uma camada à outra (o ID de L2 de origem #2 é o novo ID que será usado)
1106 A. Temporizador de priv. da origem reiniciado
1106 B. Temporizador de priv. da origem reiniciado
1107. Comunicação em andamento usando o ID de L2 de origem #2

FIG. 11

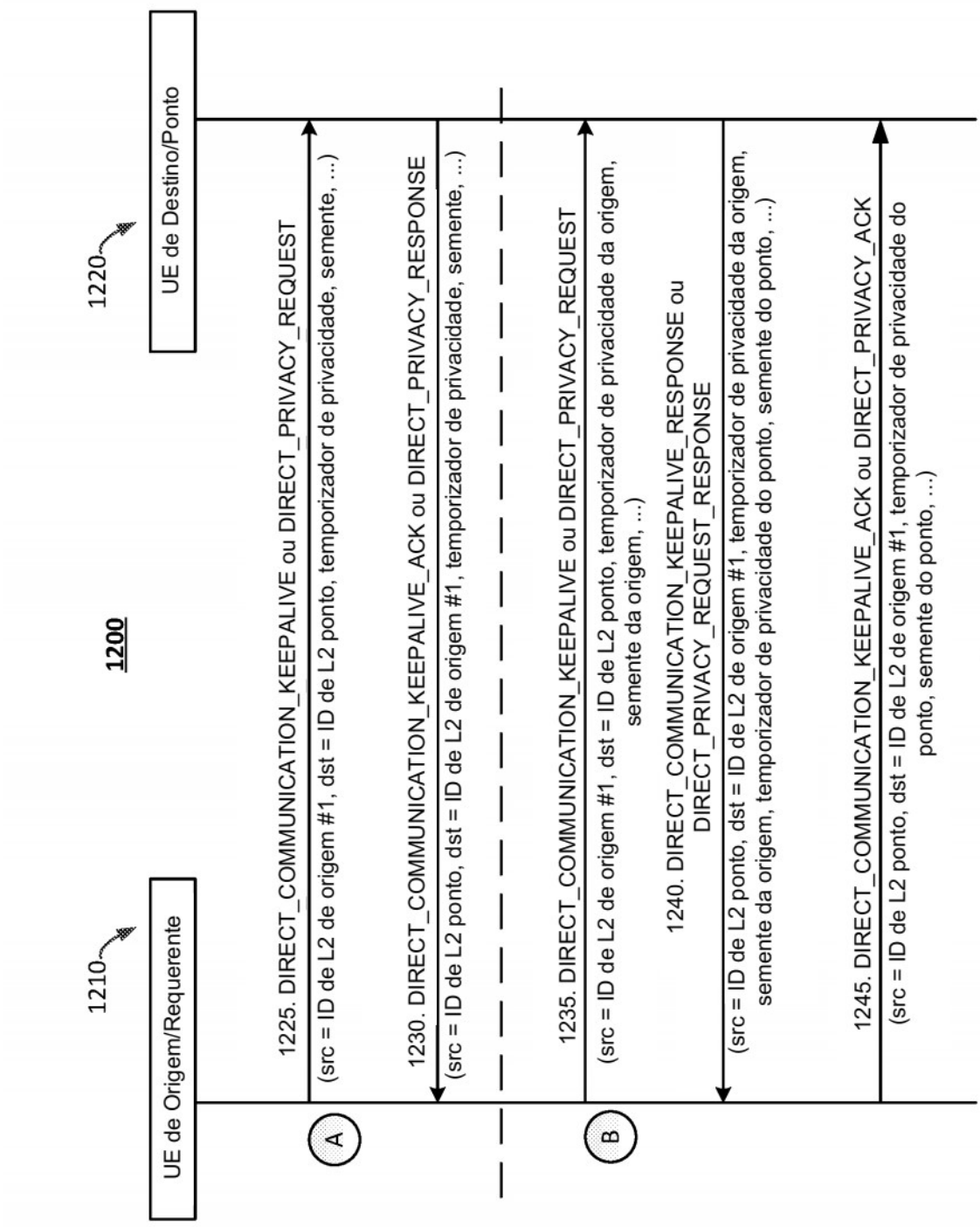

1200
1210
UE de Origem/Requerente
1220
UE de Destino/Ponto
1225. DIRECT_COMMUNICATION_KEEPALIVE ou DIRECT_PRIVACY_REQUEST
(src = ID de L2 de origem #1, dst = ID de L2 ponto, temporizador de privacidade, semente, ...)
1230. DIRECT_COMMUNICATION_KEEPALIVE_ACK ou DIRECT_PRIVACY_RESPONSE
(src = ID de L2 ponto, dst = ID de L2 de origem #1, temporizador de privacidade, semente, ...)
A
1235. DIRECT_COMMUNICATION_KEEPALIVE ou DIRECT_PRIVACY_REQUEST
(src = ID de L2 de origem #1, dst = ID de L2 ponto, temporizador de privacidade da origem, semente da origem, ...)
1240. DIRECT_COMMUNICATION_KEEPALIVE_RESPONSE ou DIRECT_PRIVACY_REQUEST_RESPONSE
(src = ID de L2 ponto, dst = ID de L2 de origem #1, temporizador de privacidade da origem, semente da origem, temporizador de privacidade do ponto, semente do ponto, ...)
B
1245. DIRECT_COMMUNICATION_KEEPALIVE_ACK ou DIRECT_PRIVACY_ACK
(src = ID de L2 ponto, dst = ID de L2 de origem #1, temporizador de privacidade do ponto, semente do ponto, ...)

FIG. 12

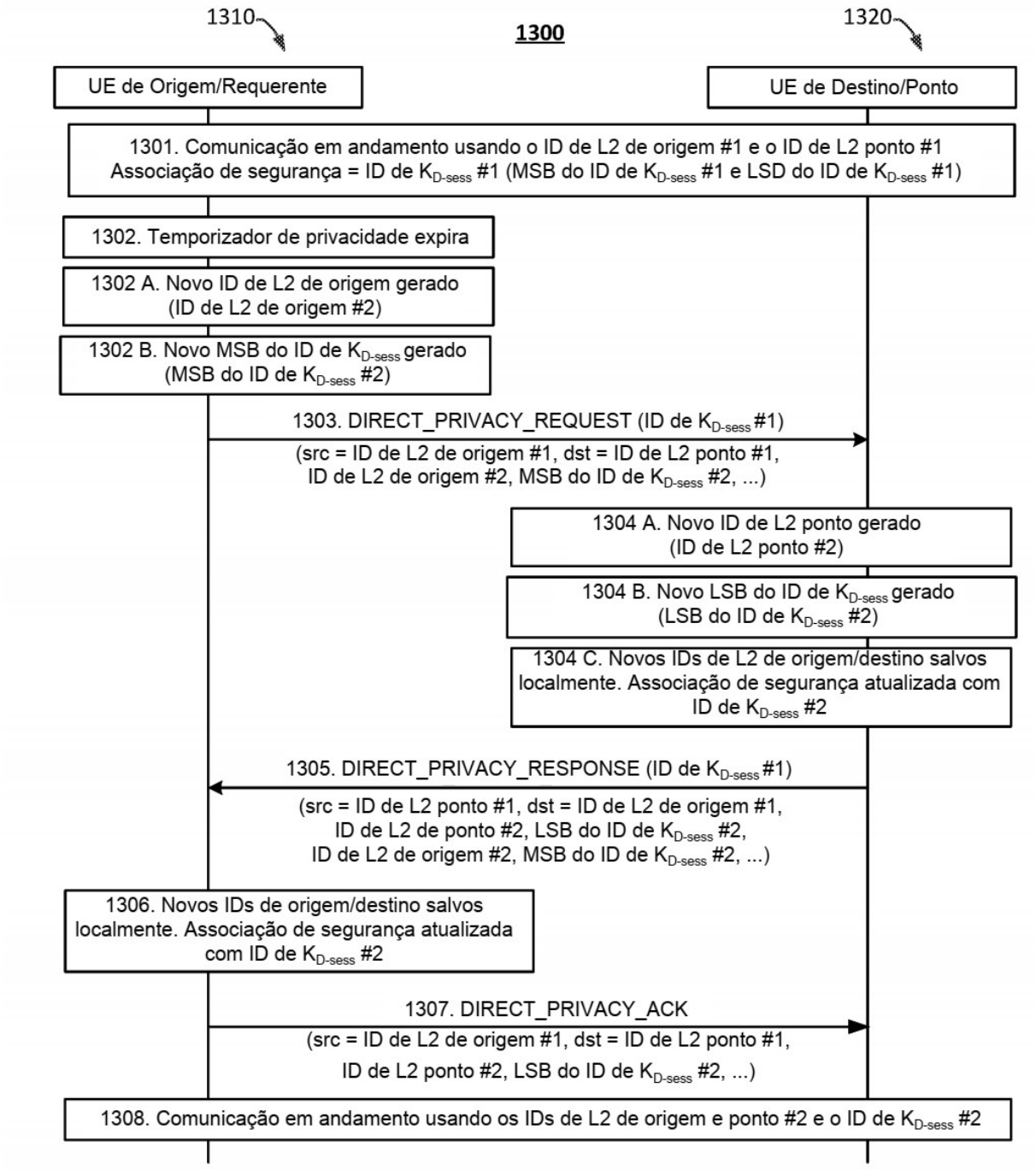

1310
1300
1320
UE de Origem/Requerente
UE de Destino/Ponto
1301. Comunicação em andamento usando o ID de L2 de origem #1 e o ID de L2 ponto #1
Associação de segurança = ID de K_D-sess #1 (MSB do ID de K_D-sess #1 e LSD do ID de K_D-sess #1)
1302. Temporizador de privacidade expira
1302 A. Novo ID de L2 de origem gerado
(ID de L2 de origem #2)
1302 B. Novo MSB do ID de K_D-sess gerado
(MSB do ID de K_D-sess #2)
1303. DIRECT_PRIVACY_REQUEST (ID de K_D-sess #1)
(src = ID de L2 de origem #1, dst = ID de L2 ponto #1,
ID de L2 de origem #2, MSB do ID de K_D-sess #2, ...)
1304 A. Novo ID de L2 ponto gerado
(ID de L2 ponto #2)
1304 B. Novo LSB do ID de K_D-sess gerado
(LSB do ID de K_D-sess #2)
1304 C. Novos IDs de L2 de origem/destino salvos localmente. Associação de segurança atualizada com ID de K_D-sess #2
1305. DIRECT_PRIVACY_RESPONSE (ID de K_D-sess #1)
(src = ID de L2 ponto #1, dst = ID de L2 de origem #1,
ID de L2 de ponto #2, LSB do ID de K_D-sess #2,
ID de L2 de origem #2, MSB do ID de K_D-sess #2, ...)
1306. Novos IDs de origem/destino salvos localmente. Associação de segurança atualizada com ID de K_D-sess #2
1307. DIRECT_PRIVACY_ACK
(src = ID de L2 de origem #1, dst = ID de L2 ponto #1,
ID de L2 ponto #2, LSB do ID de K_D-sess #2, ...)
1308. Comunicação em andamento usando os IDs de L2 de origem e ponto #2 e o ID de K_D-sess #2

FIG. 13

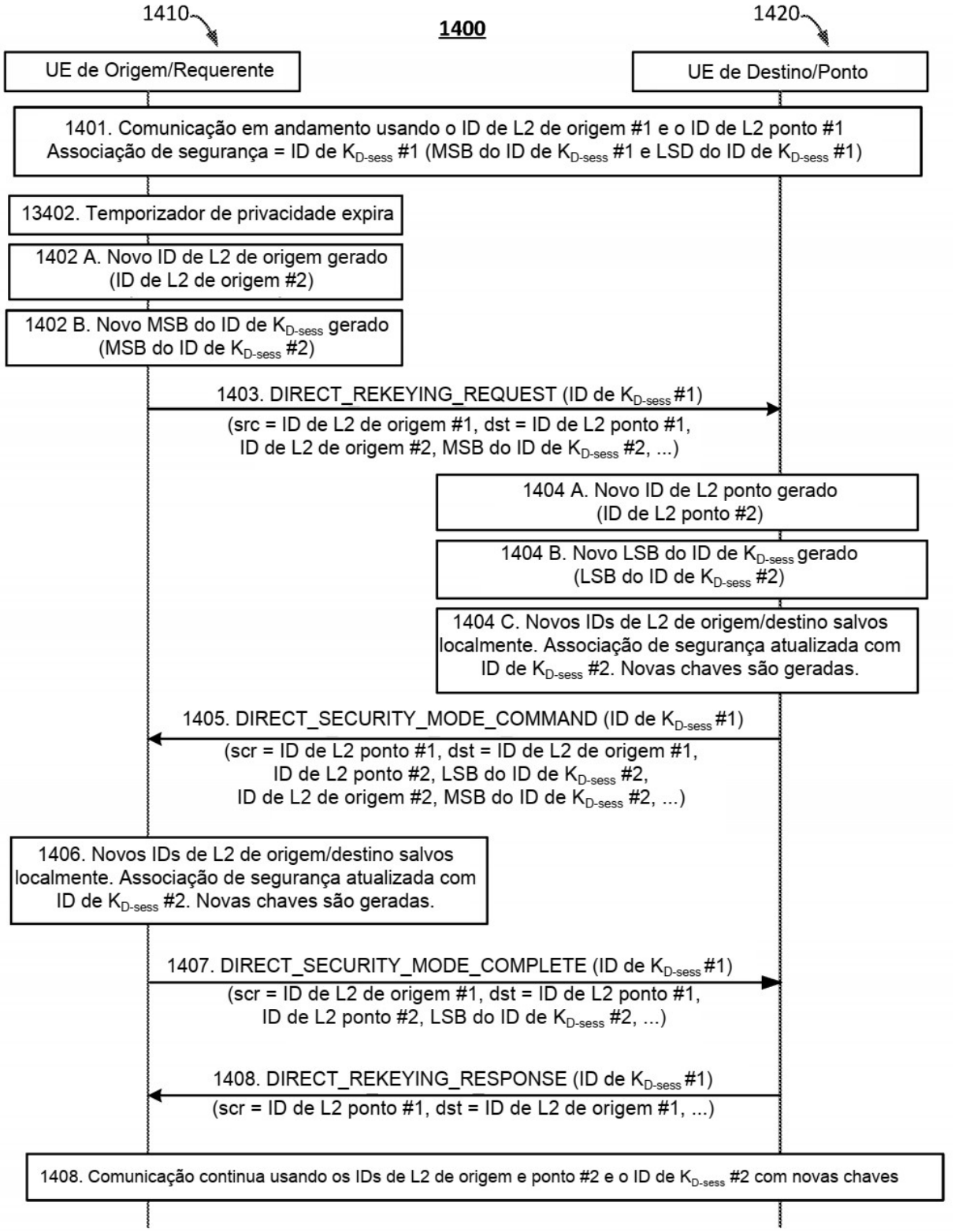

1410
1400
1420
UE de Origem/Requerente
UE de Destino/Ponto
1401. Comunicação em andamento usando o ID de L2 de origem #1 e o ID de L2 ponto #1
Associação de segurança = ID de K_{D-sess} #1 (MSB do ID de K_{D-sess} #1 e LSD do ID de K_{D-sess} #1)
13402. Temporizador de privacidade expira
1402 A. Novo ID de L2 de origem gerado
(ID de L2 de origem #2)
1402 B. Novo MSB do ID de K_{D-sess} gerado
(MSB do ID de K_{D-sess} #2)
1403. DIRECT_REKEYING_REQUEST (ID de K_{D-sess} #1)
(src = ID de L2 de origem #1, dst = ID de L2 ponto #1,
ID de L2 de origem #2, MSB do ID de K_{D-sess} #2, ...)
1404 A. Novo ID de L2 ponto gerado
(ID de L2 ponto #2)
1404 B. Novo LSB do ID de K_{D-sess} gerado
(LSB do ID de K_{D-sess} #2)
1404 C. Novos IDs de L2 de origem/destino salvos localmente. Associação de segurança atualizada com ID de K_{D-sess} #2. Novas chaves são geradas.
1405. DIRECT_SECURITY_MODE_COMMAND (ID de K_{D-sess} #1)
(scr = ID de L2 ponto #1, dst = ID de L2 de origem #1,
ID de L2 ponto #2, LSB do ID de K_{D-sess} #2,
ID de L2 de origem #2, MSB do ID de K_{D-sess} #2, ...)
1406. Novos IDs de L2 de origem/destino salvos localmente. Associação de segurança atualizada com ID de K_{D-sess} #2. Novas chaves são geradas.
1407. DIRECT_SECURITY_MODE_COMPLETE (ID de K_{D-sess} #1)
(scr = ID de L2 de origem #1, dst = ID de L2 ponto #1,
ID de L2 ponto #2, LSB do ID de K_{D-sess} #2, ...)
1408. DIRECT_REKEYING_RESPONSE (ID de K_{D-sess} #1)
(scr = ID de L2 ponto #1, dst = ID de L2 de origem #1, ...)
1408. Comunicação continua usando os IDs de L2 de origem e ponto #2 e o ID de K_{D-sess} #2 com novas chaves

FIG. 14

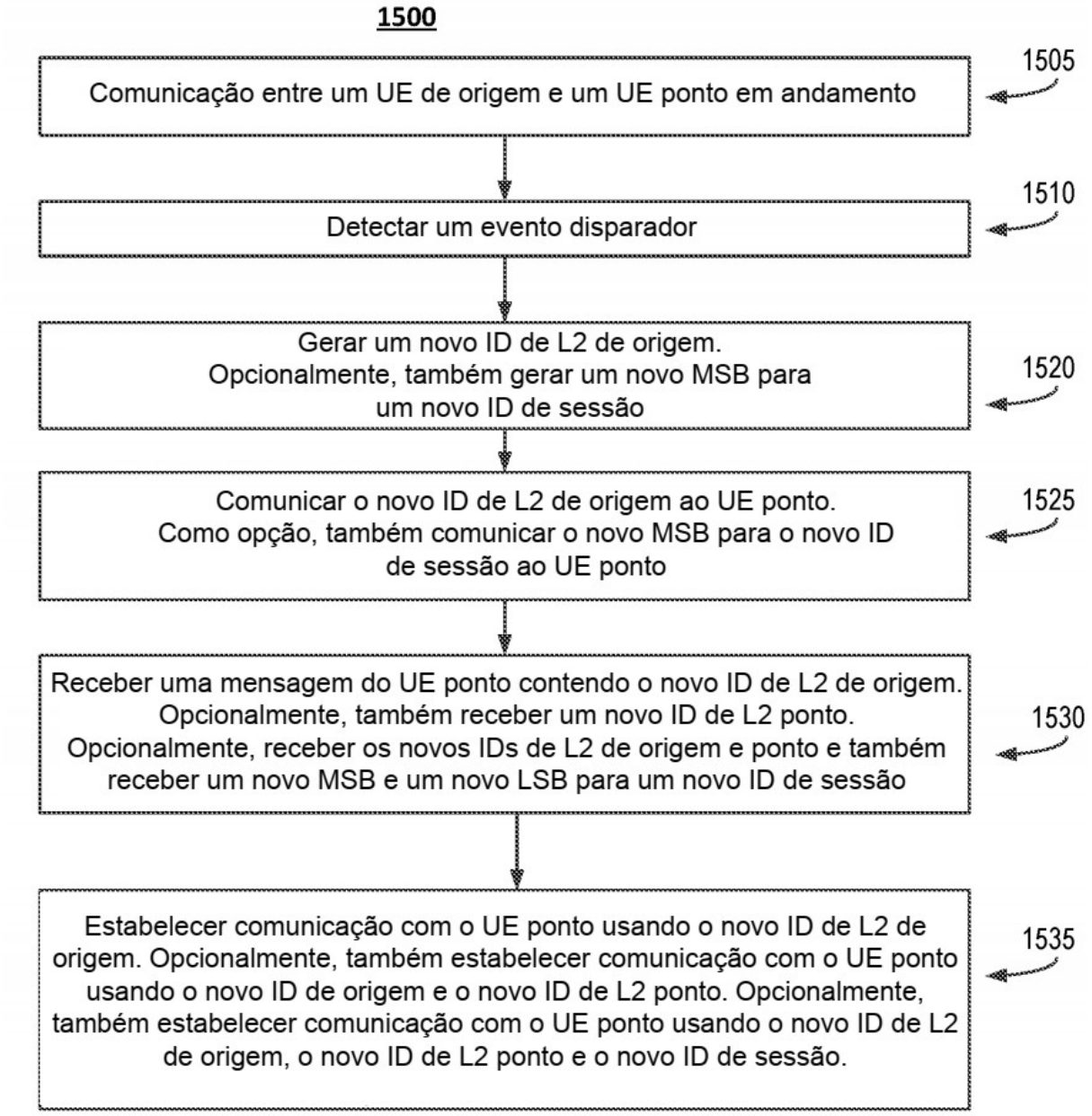

1500
Comunicação entre um UE de origem e um UE ponto em andamento
1505
Detectar um evento disparador
1510
Gerar um novo ID de L2 de origem.
Opcionalmente, também gerar um novo MSB para
um novo ID de sessão
1520
Comunicar o novo ID de L2 de origem ao UE ponto.
Como opção, também comunicar o novo MSB para o novo ID
de sessão ao UE ponto
1525
Receber uma mensagem do UE ponto contendo o novo ID de L2 de origem.
Opcionalmente, também receber um novo ID de L2 ponto.
Opcionalmente, receber os novos IDs de L2 de origem e ponto e também
receber um novo MSB e um novo LSB para um novo ID de sessão
1530
Estabelecer comunicação com o UE ponto usando o novo ID de L2 de
origem. Opcionalmente, também estabelecer comunicação com o UE ponto
usando o novo ID de origem e o novo ID de L2 ponto. Opcionalmente,
também estabelecer comunicação com o UE ponto usando o novo ID de L2
de origem, o novo ID de L2 ponto e o novo ID de sessão.
1535

FIG. 15

RESUMO

"PROCEDIMENTOS QUE GARANTEM PRIVACIDADE PARA WTRUs USANDO COMUNICAÇÃO PC5"

Métodos, dispositivos e sistemas para mudar um identificador (ID) de camada 2 durante uma sessão de veículo a tudo (V2X) em andamento entre uma unidade transmissora/receptora sem fio (WTRU) de origem e uma WTRU ponto incluem estabelecer comunicação entre as WTRUs de origem e ponto com base em um identificador (ID) de camada 2 (L2) existente. Na condição em que um evento disparador ocorre, a WTRU de origem gera um novo ID de L2 de origem, comunica o novo ID de L2 de origem à WTRU ponto, recebe da WTRU ponto uma mensagem que responde ao novo ID L2 de origem, e estabelece comunicação entre a WTRU de origem e a WTRU ponto com base no novo ID de L2 de origem.