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

(21) BR 112020006346-0 A2

(22) Data do Depósito: 29/09/2018

(43) Data da Publicação Nacional: 24/09/2020

(54) Título: INCORPORAÇÃO DE POLÍTICAS DE REDE EM GERAÇÃO DE CHAVE

(51) Int. Cl.: H04W 12/04; H04W 12/10; H04L 29/06.

(30) Prioridade Unionista: 02/10/2017 US 62/567,086; 28/09/2018 US 16/146,709.

(71) Depositante(es): QUALCOMM INCORPORATED.

(72) Inventor(es): ANAND PALANIGOUNDER; SOO BUM LEE; ADRIAN EDWARD ESCOTT.

(86) Pedido PCT: PCT US2018053661 de 29/09/2018

(87) Publicação PCT: WO WO 2019/070542 de 11/04/2019

(85) Data da Fase Nacional: 30/03/2020

(57) Resumo: A presente invenção proporciona técnicas que podem ser aplicadas, por exemplo, para fornecer informações de política de rede de uma maneira segura. Em alguns casos, um UE pode receber uma primeira mensagem para estabelecer uma conexão segura com uma rede, em que a primeira mensagem compreende informação de política de rede, gerar uma primeira chave baseada em parte na informação de política de rede, e usar a primeira chave para verificar a informação de política de rede.

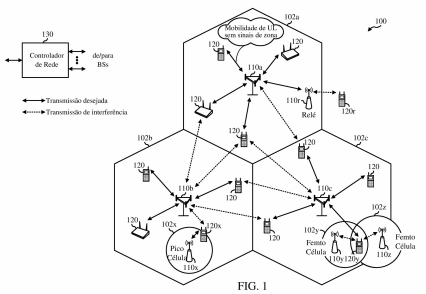

FIG. 1

"INCORPORAÇÃO DE POLÍTICAS DE REDE EM GERAÇÃO DE CHAVE"

REIVINDICAÇÃO DE PRIORIDADE SOB 35 USC § 119

[001] Este pedido reivindica prioridade para o pedido de patente US N ° 16/146,709, depositado em 28 de setembro de 2018, que reivindica o benefício do Pedido de Patente Provisório US N° 62/567,086, depositado em 2 de outubro de 2017, que é aqui incorporado por referência em sua totalidade.

Campo da Divulgação

[002] Certos aspectos da presente invenção relacionam-se geralmente a comunicações sem fio e, mais particularmente, a métodos e aparelhos para estabelecer comunicações seguras em uma rede.

Descrição da Técnica Relacionada

[003] Sistemas de comunicação sem fio são amplamente implementados para fornecer vários serviços de telecomunicação, tais como telefonia, vídeo, dados, mensagens e radiodifusões. Sistemas de comunicação sem fio típicos podem empregar tecnologias de acesso múltiplo capazes de suportar comunicação com múltiplos usuários compartilhando recursos de sistema disponíveis (por exemplo, largura de banda, potência de transmissão). Exemplos de tais tecnologias de acesso múltiplo incluem sistemas de Evolução de Longo Prazo (LTE), sistemas de acesso múltiplo por divisão de código (CDMA), sistemas de acesso múltiplo por divisão de tempo (TDMA), sistemas de acesso múltiplo por divisão de frequência (FDMA), sistemas de acesso múltiplo por divisão de frequência ortogonal (OFDMA), sistemas de acesso múltiplo por divisão de frequência de portadora única (SC-FDMA), e sistemas de

acesso múltiplo por divisão de código síncrono por divisão de tempo (TD-SCDMA).

[004] Em alguns exemplos, um sistema de comunicação de acesso múltiplo sem fio pode incluir um número de estações base, cada qual simultaneamente suportando a comunicação para múltiplos dispositivos de comunicação, de outra forma conhecidos como equipamento de usuário (UEs). Em rede LTE ou LTE-A, um conjunto de uma ou mais estações base pode definir um Nó B (eNB). Em outros exemplos (por exemplo, em uma próxima geração ou rede de 5G), um sistema de comunicação de acesso múltiplo sem fio pode incluir um número de unidades distribuídas (DUs) (por exemplo, unidades de borda (EUs) nós de borda (ENs), cabeças de rádio (RHs), cabeças de rádio inteligentes (SRHs), pontos de recebimento de transmissão (TRPs), etc.) em comunicação com um número de unidades centrais (CUs) (por exemplo, nós centrais (CNs), controladores de Nó de acesso (ANCs), etc.), onde um conjunto de uma ou mais unidades distribuídas, em comunicação com uma unidade central, pode definir um nó de acesso (por exemplo, uma nova estação base de Rádio (NR BS), um nó-B de novo rádio (NR NB), um nó de rede, 5G NB, etc.). Uma estação base ou DU pode se comunicar com um conjunto de UEs em canais de enlace descendente (por exemplo, para transmissões a partir de uma estação base ou para um UE) e canais de enlace ascendente (por exemplo, para transmissões de Um UE para uma estação base ou unidade distribuída).

[005] Essas tecnologias de acesso múltiplo foram adotadas em vários padrões de telecomunicações para a provisão de um protocolo comum que permite que diferentes

dispositivos sem fio se comuniquem em um nível municipal, nacional, regional e mesmo global. Um exemplo de um padrão de telecomunicações emergente é o novo rádio (NR), por exemplo, acesso de rádio 5G. NR é um conjunto de aperfeiçoamentos para o padrão móvel LTE promulgado pelo projeto de Parceria de Terceira Geração (3 GPP). É projetado para melhor suportar o acesso da Internet de banda larga móvel ao melhorar a eficiência espectral, baixar custos, melhorar serviços, fazer uso de novo espectro, e melhor integrar com outros padrões abertos utilizando OFDMA com prefixo cíclico (CP) no enlace descendente (DL) e no enlace ascendente (UL) assim como formação de feixe de suporte, tecnologia de antena de múltiplas entradas e múltiplas saídas (MIMO), e agregação de portadora.

[006] Entretanto, à medida que a demanda de acesso de banda larga móvel continua a aumentar, existe a necessidade de aperfeiçoamentos adicionais na tecnologia NR. De preferência, estes aperfeiçoamentos devem ser aplicáveis a outras tecnologias de acesso múltiplo e aos padrões de telecomunicação que empregam estas tecnologias.

SUMÁRIO

[007] Os sistemas, métodos e dispositivos da revelação têm, cada um, vários aspectos, nenhum dos quais é exclusivamente responsável por seus atributos desejáveis. Sem limitar o escopo desta descrição, conforme expresso pelas reivindicações que se seguem, algumas características serão agora discutidas brevemente. Após considerar esta discussão, e particularmente após a leitura da seção intitulada "Descrição Detalhada" deve-se entender como as

características desta descrição proporcionam vantagens que incluem comunicações melhoradas em uma rede sem fio.

[008] Certos aspectos da presente invenção proporcionam um método para comunicações sem fio por um equipamento de usuário (UE). O método inclui, de modo geral, o recebimento de uma primeira mensagem para estabelecer uma conexão segura com uma rede, em que a primeira mensagem inclui informação de política de rede. O método também inclui a geração de uma primeira chave com base em parte da informação de política de rede. O método inclui ainda o uso da primeira chave para verificar a informação da rede.

[009] Certos aspectos da presente invenção proporcionam um método para comunicações sem fio por um nó de rede, tal como uma função de ancoragem de segurança (SEAF). O método geralmente inclui a geração de uma chave para um nó de rede com base pelo menos em parte na informação de política de rede. A chave é utilizada para estabelecer uma conexão segura entre um UE e o nó de rede. O método também inclui o envio da chave para o nó de rede.

[0010] Certos aspectos da presente invenção proporcionam um método para comunicações sem fio por um equipamento de usuário (UE). O método geralmente inclui estabelecer, com base em um procedimento de autenticação com uma rede, uma chave de ancoragem que é compartilhada entre o UE e uma função de ancoragem de segurança (SEAF) na rede. O método também inclui receber uma primeira mensagem para estabelecer uma conexão segura com a rede, em que a primeira mensagem compreende uma ficha de política de rede para uma sessão de comunicação com a rede, a informação de

política de rede, uma primeira quantidade de tempo que uma primeira chave é válida e uma segunda quantidade de tempo em que a ficha de política de rede é válida. O método inclui ainda determinar se a ficha de política de rede é válida com base em uma chave derivada da chave de âncora compartilhada, da informação de política de rede, da primeira quantidade de tempo e da segunda quantidade de tempo, antes de estabelecer a conexão segura com a rede.

[0011] Certos aspectos da presente invenção proporcionam um método para comunicações sem fio por um nó de rede, tal como uma função de ancoragem de segurança (SEAF). O método geralmente inclui estabelecer, com base em um procedimento de autenticação com Um UE, uma chave de ancoragem que é compartilhada entre a SEAF e o UE em uma rede.O método também inclui a geração de um sinal de política de rede com base em parte da chave de âncora, da informação de política de rede e de uma primeira quantidade de tempo em que a ficha de política de rede é válido. O método inclui ainda gerar uma chave para outro nó de rede, e enviar a chave, a informação de política de rede e a ficha de política de rede para o outro nó de rede.

[0012] Numerosos outros aspectos são providos, incluindo métodos, aparelhos, sistemas, produtos de programa de computador e sistemas de processamento capazes de realizar as operações descritas acima.

[0013] Para a consecução das finalidades precedentes e relacionadas, um ou mais aspectos compreendem as características daqui em diante completamente descritas e particularmente apontadas nas reivindicações. A descrição a seguir e os desenhos anexos apresentam em detalhes

determinados aspectos ilustrativos de um ou mais aspectos. Estas características são indicativas, no entanto, de apenas algumas das várias maneiras pelas quais os princípios de vários aspectos podem ser empregados, e esta descrição pretende incluir todos esses aspectos e seus equivalentes.

BREVE DESCRIÇÃO DOS DESENHOS

[0014] De modo que a maneira na qual as características acima citadas da presente descrição possam ser entendidas em detalhes, uma descrição mais particular, brevemente resumida acima, pode ser feita por referência a aspectos, algumas das quais são ilustradas nos desenhos em anexo. Deve ser notado, entretanto, que os desenhos anexos ilustram apenas certos aspectos típicos desta revelação e não devem, portanto, ser considerados como limitando seu escopo, pois a descrição pode admitir outros aspectos igualmente efetivos.

[0015] A Figura 1 é um diagrama de blocos que ilustra conceitualmente um sistema de telecomunicações ilustrativo, de acordo com certos aspectos da presente invenção.

[0016] A Figura 2 é um diagrama de blocos que ilustra uma arquitetura lógica exemplar de uma RAN distribuída, de acordo com certos aspectos da presente invenção.

[0017] A Figura 3 é um diagrama que ilustra uma arquitetura física exemplar de uma RAN distribuída, de acordo com certos aspectos da presente invenção

[0018] A Figura 4 é um diagrama de blocos que ilustra conceitualmente um projeto de um exemplo BS e

equipamento de usuário (UE), de acordo com certos aspectos da presente invenção.

[0019] A Figura 5 é um diagrama que mostra exemplos para implementar uma pilha de protocolos de comunicação, de acordo com certos aspectos da presente invenção.

[0020] A Figura 6 ilustra um exemplo de um subquadro central DL, de acordo com certos aspectos da presente revelação.

[0021] A Figura 7 ilustra um exemplo de um subquadro centrado em UL, de acordo com certos aspectos da presente invenção.

[0022] As Figuras 8-9 ilustram arquiteturas exemplares de 5G com um ou mais nós de rede não-colocados, de acordo com certos aspectos da presente invenção.

[0023] A Figura 10 é um fluxograma que ilustra operações exemplares para comunicações sem fio em uma rede, de acordo com certos aspectos da presente invenção.

[0024] A Figura 11 é um fluxograma que ilustra operações exemplares para comunicações sem fio em uma rede, de acordo com certos aspectos da presente invenção.

[0025] A Figura 12 é um fluxograma de chamada que ilustra um procedimento de registro exemplar, de acordo com certos aspectos da presente invenção.

[0026] A Figura 13 é um fluxograma que ilustra operações exemplares para comunicações sem fio em uma rede, de acordo com certos aspectos da presente invenção.

[0027] A Figura 14 é um fluxograma que ilustra operações exemplares para comunicações sem fio em uma rede, de acordo com certos aspectos da presente invenção.

[0028] A Figura 15 é um fluxograma de chamada que ilustra um procedimento de registro exemplar, de acordo com certos aspectos da presente invenção.

[0029] Para facilitar a compreensão, numerais de referência idênticos foram usados, onde possível, para designar elementos idênticos que são comuns às figuras. Contempla-se que os elementos descritos em uma modalidade podem ser utilizados de forma benéfica em outras modalidades sem uma recitação específica.

DESCRIÇÃO DETALHADA

[0030] Aspectos da presente invenção proporcionam aparelhos, métodos, sistemas de processamento e meios passíveis de leitura por computador para redes sem fio, tais como redes sem fio de novo rádio (NR) (nova tecnologia de acesso por rádio ou tecnologia 5G).

[0031] NR pode suportar vários serviços de comunicação sem fio, tais como uma larga banda larga móvel (eMBB) para direcionar a largura de banda larga (por exemplo, 80 MHz além), onda milimétrica (mmW) visando a alta frequência de portadora (por exemplo, 60 GHz), MTC maciço (mMTC) objetivando técnicas de MTC compatíveis não Para trás. Estes serviços podem incluir requisitos de latência e confiabilidade. Estes serviços também podem ter diferentes intervalos de tempo de transmissão (TTI) para satisfazer os requisitos de qualidade de serviço (QoS). Além disso, estes serviços podem co-existir no mesmo subquadro.

[0032] NR introduz o conceito de fatiamento de redes. Por exemplo, uma rede pode ter múltiplas fatias, que podem suportar diferentes serviços, por exemplo, a internet

de qualquer comunicação (IoE), URY, eMBB, veículo-a-veículo (V2V), etc. a fatia pode ser definida como uma rede lógica completa que compreende um conjunto de funções de rede e recursos correspondentes necessários para fornecer determinadas capacidades de rede e características de rede.

[0033] Em alguns aspectos, um sistema 5G NR pode ser capaz de suportar vários cenários de desenvolvimento diferentes. Particularmente, conforme a tecnologia 5G e/ou as exigências de serviço continuam a evoluir, os serviços, capacidades e/ou funções realizadas por um ou mais nós de rede em uma rede de 5G podem variar. Como as mudanças na arquitetura de rede podem não ser conhecidas pelo UE, pode ser benéfico informar o UE quanto à configuração de rede, capacidades, configuração de segurança, etc. em particularEntretanto, pode não ser possível utilizando técnicas atuais para a rede para informar ao UE quanto à configuração de rede (segurança), capacidades e políticas de uma maneira segura.

[0034] Por exemplo, num sistema 5G, existe tipicamente uma única interface de plano de controle (N1) entre o UE e a rede de serviço. Esta interface N1 é geralmente utilizada para estabelecer uma conexão de estrato de não acesso (NAS) entre o UE e o acesso e a função de gerenciamento de mobilidade (AMF) AMF. No entanto, em alguns cenários de desenvolvimento, o AMF pode não ser responsável por (ou ter acesso a) funções de segurança na rede. Assim, como a AMF pode ser a única entidade que tem uma conexão de sinalização com o UE, pode haver casos em que o AMF (roque ou malicioso) pode Interceptar a informação de configuração da rede e

modificar a informação de configuração da rede fornecida ao UE para Comprometer a conexão/comunicação entre o UE E a rede. Consequentemente, os aspectos da presente invenção proporcionam técnicas para informar seguramente o UE quanto à configuração de rede (segurança), capacidades, políticas de rede, etc.

[0035] Vários aspectos da descrição são descritos mais completamente a seguir com referência aos desenhos em anexo. Esta revelação pode, entretanto, ser concretizada em muitas formas diferentes e não deve ser interpretada como limitada a qualquer estrutura ou função específica apresentada por toda esta revelação. Em vez disso, estes aspectos são providos de modo que esta descrição seja completa e completa, e transmitirá plenamente o escopo da descrição para aqueles versados na técnica. Com base nos ensinamentos aqui alguém versado na técnica deve apreciar que o escopo da descrição pretende cobrir qualquer aspecto da revelação aqui apresentada, seja implementada independentemente ou combinada com qualquer outro aspecto da revelação. Por exemplo, um aparelho pode ser implementado ou um método pode ser praticado utilizando qualquer número dos aspectos expostos aqui. Além disso, o escopo da invenção destina-se a cobrir tal aparelho ou método que seja praticado utilizando-se outra estrutura, funcionalidade, ou estrutura e funcionalidade além dos vários aspectos da revelação aqui apresentada. Deve-se entender que qualquer aspecto da revelação aqui apresentada pode ser incorporado por um ou mais elementos de uma reivindicação.

[0036] A palavra "exemplar" é aqui usada para significar “servindo como exemplo, caso, ou ilustração”. Qualquer aspecto aqui descrito como "exemplar" não deve ser necessariamente considerado como preferido ou vantajoso em relação a outros aspectos.

[0037] Embora aspectos específicos sejam aqui descritos, muitas variações e permutações destes aspectos caem dentro do escopo da invenção. Embora alguns benefícios e vantagens dos aspectos preferidos sejam mencionados, o escopo da invenção não se destina a ser limitado a benefícios, usos ou objetivos particulares. Ao contrário, pretende-se que aspectos da revelação sejam aplicáveis de forma ampla a diferentes tecnologias sem fio, configurações de sistema, redes e protocolos de transmissão, alguns dos quais são ilustrados por meio de exemplo nas figuras e na seguinte descrição dos aspectos preferidos. A descrição detalhada e desenhos são meramente ilustrativos da descrição ao invés de limitar, o escopo da descrição sendo definido pelas reivindicações anexas e seus equivalentes.

[0038] As técnicas aqui descritas podem ser utilizadas para várias redes de comunicação sem fio tais como CDMA, TDMA, FDMA, OFDMA, SC-FDMA e outras redes. Os termos "rede" e "sistema" são frequentemente utilizados de forma intercambiável. Uma rede CDMA pode implementar uma tecnologia de rádio tal como acesso de rádio terrestre universal (UTRA), cdma2000, etc. UTRA inclui CDMA de banda larga (WCDMA), CDMA síncrono por divisão de tempo (TD-SCDMA) e outras variantes de CDMA. Cdma2000 cobre padrões IS-2000, IS-95 e IS-856. Uma rede TDMA pode implementar uma tecnologia de rádio tal como sistema global para

comunicações móveis (GSM). Uma rede OFDMA pode implementar uma tecnologia de rádio tal como UTRA evoluída (E-UTRA), banda larga ultra-móvel (UMB), IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, Flash-OFDM ®, etc. UTRA E E-UTRA são Parte do sistema universal de telecomunicações Móveis (UMTS). 3GPP Evolução de Longo Prazo (LTE) e LTE-Avançado (LTE-A), em ambas duplexação por divisão de frequência (FDD) e duplexação por divisão de tempo (TDD), são novas versões do UMTS que utilizam E-UTRA, que emprega OFDMA no enlace descendente e SC-FDMA no enlace ascendente. UTRA, E-UTRA, UMTS, LTE, LTE-A E GSM são descritos em documentos de uma organização denominada "Projeto de Parceria de 3a Geração" (3 GPP). Cdma2000 e UMB são descritos em documentos de uma organização denominada "3 rd Generation Partnership Project 2" (3GPP2). As técnicas aqui descritas podem ser utilizadas para as redes sem fio e as tecnologias de rádio mencionadas acima bem como outras redes sem fio e tecnologias de rádio, tal como uma rede 5G nexgten/NR.

SISTEMA DE COMUNICAÇÕES SEM FIO DE EXEMPLO

[0039] A Figura 1 ilustra uma rede sem fio exemplar 100, tal como uma nova rede rádio (NR) ou 5G, na qual aspectos da presente revelação podem ser realizados, por exemplo, para a provisão segura de uma informação de política de rede de UE (segurança) (por exemplo, configuração de rede, informação de segurança, capacidades, etc.). Em alguns casos, a rede 100 pode ser uma rede multi-partição, onde cada fatia define como uma composição de funções de rede adequadamente configuradas, aplicações de rede e infra-estruturas de nuvem subjacentes que são

agrupadas juntas para satisfazer a necessidade de um caso de uso específico ou modelo comercial.

[0040] Como ilustrado na Figura 1, a rede sem fio 100 pode incluir um número de BSs 110 e outras entidades de rede. A BS pode ser uma estação que se comunica com os UEs. Cada BS 110 pode prover cobertura de comunicação para uma área geográfica específica. Em 3 GPP, o termo "célula" pode se referir a uma área de cobertura de um Nó B e/ou um subsistema de Nó B servindo a esta área de cobertura, dependendo do contexto no qual o termo é usado. Em sistemas NR, o termo "célula" e eNB, Nodo B, 5G NB, AP, NR BS, NR BS ou TRP podem ser intercambiáveis. Em alguns exemplos, uma célula pode não estar necessariamente estacionária, e a área geográfica da célula pode se mover de acordo com a localização de uma estação base móvel. Em alguns exemplos, as estações base podem ser interconectadas entre si e/ou a uma ou mais outras estações base ou nós de rede (não mostrados) na rede sem fio 100 através de vários tipos de interfaces backhaul tais como uma conexão física direta, uma rede virtual, ou similar utilizando qualquer rede de transporte adequada.

[0041] Em geral, qualquer número de redes sem fio pode ser implementado em uma dada área geográfica. Cada rede sem fio pode suportar uma tecnologia de acesso de rádio específica (RAT) e pode operar em uma ou mais frequências. Uma RAT Também pode ser referida como uma tecnologia de rádio, uma interface aérea, etc. uma frequência também pode ser referida como um portador, um canal de frequência, etc. Cada frequência pode suportar uma Única RAT em uma dada área geográfica a fim de evitar

interferência entre redes sem fio de diferentes Ratos. Em alguns casos, redes de RAT de NR ou 5G podem ser desenvolvidas, empregando uma arquitetura de rede de múltiplas partições.

[0042] Uma BS pode fornecer cobertura de comunicação para uma macro célula, uma pico célula, uma femto célula, e/ou outros tipos de células. Uma macro célula pode cobrir uma área geográfica relativamente grande (por exemplo, vários quilómetros de raio) e pode permitir acesso irrestrito pelos UEs com assinatura de serviço. Uma pico célula pode cobrir uma área geográfica relativamente pequena e pode permitir acesso irrestrito pelos UEs com assinatura de serviço. Uma femto célula pode cobrir uma área geográfica relativamente pequena (por exemplo, uma casa) e pode permitir acesso restrito por UEs tendo associação com a femto célula (por exemplo, UEs em Um Grupo de Assinantes Fechados (CSG), UEs para usuários na casa, etc.). Uma BS para uma macro célula pode ser referida como uma macro BS. Uma BS para uma pico célula pode ser referida como uma pico BS. Uma BS para uma femto célula pode ser referida como uma femto BS ou uma BS doméstica. No exemplo mostrado na Figura 1, as BSs 110a, 110b e 110c podem ser macro BSs para as Macro células 102a, 102b e 102c, respectivamente. A BS 110x pode ser um pico BS para uma pico célula 102x. As BSs 110y e 110z podem ser femto BS para as femto células 102y e 102z, respectivamente. Uma BS pode suportar uma ou múltiplas (por exemplo, três) células.

[0043] A rede sem fio 100 também pode incluir estações de retransmissão. Uma estação de retransmissão é uma estação que recebe uma transmissão de dados e/ou outras

informações de uma estação a montante (por exemplo, uma BS ou um UE) e envia uma transmissão dos dados e/ou outras informações para uma estação a jusante (por exemplo, um UE ou uma BS). Uma estação de retransmissão também pode ser um UE que transfere transmissões para outros UEs. No exemplo mostrado na FIG. 1, uma estação de retransmissão 11 Ou pode se comunicar com a BS 110a e o UE 120r a fim de facilitar a comunicação entre a BS 110a e o UE 120r. Uma estação de retransmissão também pode ser referida como um rele BS, um relé, etc.

[0044] A rede sem fio 100 pode ser uma rede heterogénea que inclui BSs de diferentes tipos, por exemplo, macro BS, pio BS, femto BS, relês, etc. estes Tipos diferentes de BSs podem ter diferentes níveis de potência de transmissão, diferentes áreas de cobertura, e diferentes impactos na interferência na rede sem fio 100. Por exemplo, A macro BS pode ter um alto nível de potência de transmissão (por exemplo, 20 Watts) enquanto pico BS, femto BS e relés podem ter um nível de potência de transmissão mais baixo (por exemplo, 1 Watt).

[0045] A rede sem fio 100 pode suportar operação síncrona ou assíncrona. Para operação síncrona, as BSs Podem ter temporização de quadro similar, e as transmissões de BSs Diferentes Podem ser aproximadamente alinhadas em tempo. Para operação assíncrona, as BSs Podem ter diferentes temporização de quadro, e as transmissões a partir de diferentes BSs não podem ser alinhadas em tempo. As técnicas aqui descritas podem ser utilizadas tanto para operação síncrona como assíncrona.

[0046] Um controlador de rede 130 pode acoplar-se a um conjunto de BSs e fornecer coordenação e controle para estas BSs. O controlador de rede 130 pode se comunicar com os BSs 110 através de um canal de transporte de retorno. As BSs 110 também podem se comunicar umas com as outras, por exemplo, direta ou indiretamente através de canal de transporte sem fio ou com fio.

[0047] Os UEs 120 (por exemplo, 120x, 120y, etc.) podem ser dispersos por toda a rede sem fio 100, e cada UE pode ser estacionário ou móvel. Um UE também pode ser referido como estação móvel, terminal, terminal de acesso, unidade de assinante, estação, Equipamento de Premissa de Cliente (CPE) um telefone celular, um telefone inteligente, um assistente digital pessoal (PDA), um modem sem fio, um dispositivo de comunicação sem fio, um dispositivo portátil, um computador laptop, um telefone sem fio, uma estação de laço local sem fio (WLL), um tablete, uma câmera, um dispositivo de jogo, um netbook, um livro inteligente, um ultra-falante, um dispositivo médico ou equipamento médico, um sensor/dispositivo biométrico, um dispositivo útil tal como um relógio inteligente, vestuário inteligente, óculos inteligentes, uma banda de pulso inteligente, joia inteligente (por exemplo, um anel inteligente, um bracelete inteligente, etc.), um dispositivo de entretenimento (por exemplo, um dispositivo de música, um dispositivo de vídeo, um rádio satélite, etc.), um componente ou sensor veicular, um medidor/sensor inteligente, equipamento de fabricação industrial, dispositivo de sistema de posicionamento global, ou qualquer outro dispositivo adequado que seja configurado

para comunicar-se através de um meio sem fio ou com fio. Alguns UEs podem ser considerados dispositivos de comunicação de tipo de máquina (MTC) ou dispositivos MTC (eMTC) evoluídos. Os UEs MTC e eMTC incluem, por exemplo, robôs, drones, dispositivos remotos, sensores, medidores, monitores, etiquetas de localização, etc., que podem se comunicar com uma BS, outro dispositivo (por exemplo, dispositivo remoto), ou alguma outra entidade. Um nó sem fio pode fornecer, por exemplo, conectividade para ou a uma rede (por exemplo, uma rede de área ampla tal como a Internet ou uma rede celular) através de um enlace de comunicação com fio ou sem fio. Alguns UEs podem ser considerados dispositivos de Identificação da Internet (IoT).

[0048] Na Figura 1, uma linha sólida com setas duplas indica as transmissões desejadas entre um UE e uma BS servidora, a Qual é uma BS designada para servir o UE no enlace descendente e/ou no enlace ascendente. Uma linha tracejada com setas duplas indica transmissões de interferência entre um UE e uma BS.

[0049] Certas redes sem fio (por exemplo, LTE) utilizam multiplexação por divisão de frequência ortogonal (OFDM) no enlace descendente e multiplexação por divisão de frequência de portadora única (SC-FDM) no enlace ascendente. OFDM e SC-FDM dividem a largura de banda do sistema em múltiplas subportadoras ortogonais (K), que também são comumente referidas como tons, bins, Etc. cada subportadora pode ser modulada com dados. Em geral, os símbolos de modulação são enviados no domínio de frequência com OFDM e no domínio de tempo com SC-FDM. O espaçamento

entre subportadoras adjacentes pode ser fixo, e o número total de subportadoras (K) pode depender da largura de banda do sistema. Por exemplo, o espaçamento das subportadoras pode ser de 15 kHz e a alocação mínima de recursos (denominada um bloco de recursos') pode ser de 12 subportadoras (ou 180 kHz). Consequentemente, o tamanho de FFT nominal pode ser igual a 128,256,512, 1024 ou 2048 para largura de banda do sistema de 1,25,2,5, 5, 10 ou 20 megahertz (MHz), respectivamente. A largura de banda do sistema pode também ser dividida em sub-bandas. Por exemplo, uma sub-banda pode cobrir 1, 08 MHz (isto é, 6 blocos de recursos), e pode haver 1,2,4, 8 ou 16 sub-bandas para largura de banda do sistema de 1,25,2,5, 5, 10 ou 20 MHz, respectivamente.

[0050] Embora aspectos dos exemplos aqui descritos possam ser associados com tecnologias LTE, aspectos da presente revelação podem ser aplicáveis a outros sistemas de comunicações sem fio, tais como NR/5G.

[0051] NR pode utilizar OFDM com CP no enlace ascendente e enlace descendente e inclui suporte para operação de semi-duplexação utilizando TDD. Uma largura de banda de portadora de componente único de 100 MHz pode ser suportada. Os blocos de recursos NR podem abranger 12 subportadoras com uma largura de banda subportadora de 75 kHz através de uma duração de 0, 1 ms. Cada quadro de rádio pode consistir em 50 subquadros com um comprimento de 10 ms Consequentemente, cada subquadro pode ter um comprimento de 02 ms. cada subquadro pode indicar uma direção de enlace (isto é, DL ou UL) para transmissão de dados e a direção de enlace para cada subquadro pode ser comutada dinamicamente.

Cada subquadro pode incluir dados DL/UL bem como dados de controle DL/UL. Subquadros de UL e DL para NR podem ser conforme descrito em maiores detalhes abaixo com relação às Figuras 6 e 7. a Formação de Feixe pode ser suportada e a direção de feixe pode ser configurada dinamicamente. As transmissões MIMO com pré-codificação também podem ser suportadas. As configurações MIMO no DL podem suportar até 8 antenas de transmissão com transmissões de DL de múltiplas camadas até 8 fluxos e até 2 fluxos por UE. Transmissões de múltiplas camadas com até 2 fluxos por UE podem ser suportadas. A agregação de múltiplas células pode ser suportada com até 8 células de serviço. Alternativamente, NR pode suportar uma interface de ar diferente, diferente de uma interface de OFDM. As redes NR podem incluir entidades tais como CUs e/ou DUs.

[0052] Em alguns exemplos, o acesso à interface aérea pode ser programado, em que uma entidade de programação (por exemplo, uma estação base) aloca recursos para comunicação entre alguns ou todos os dispositivos e equipamentos dentro de sua área de serviço ou célula. Dentro da presente descrição, conforme discutido adicionalmente abaixo, a entidade de programação pode ser responsável pela programação, atribuição, reconfiguração e liberação de recursos para uma ou mais entidades subordinadas. Isto é, para a comunicação programada, as entidades subordinadas utilizam recursos alocados pela entidade de programação. As estações Base não são as únicas entidades que podem funcionar como uma entidade de programação. Isto é, em alguns exemplos, um UE pode funcionar como uma entidade de programação, recursos de

programação para uma ou mais entidades subordinadas (por exemplo, um ou mais outros UEs). Neste exemplo, o UE está funcionando como uma entidade de programação, e outros UEs utilizam recursos programados pelo UE para comunicação sem fio. Um UE pode funcionar como uma entidade de programação numa rede ponto-a-ponto (P2P), e/ou em uma rede de entrelaçamento. Em um exemplo de rede de entrelaçamento, Os UEs podem opcionalmente comunicar-se diretamente uns com os outros além de se comunicar com a entidade de programação.

[0053] Assim, em uma rede de comunicação sem fio com acesso programado para recursos de tempo e frequência e tendo uma configuração celular, uma configuração P2P e uma configuração de malha, uma entidade de programação e uma ou mais entidades subordinadas podem se comunicar utilizando os recursos programados.

[0054] Como notado acima, uma RAN pode incluir uma CU e U. Um NR BS (por exemplo, gNB, 5G Nó B, Nó B, ponto de recebimento de transmissão (TRP), ponto de Acesso (AP)) pode corresponder a uma ou múltiplas BSs. As células NR podem ser configuradas como células de acesso (Acks) ou células somente de dados (Dcélulas). Por exemplo, a RAN (por exemplo, uma unidade central ou unidade distribuída) pode configurar as células. Dcélulas podem ser células utilizadas para agregação de portadoras ou conectividade dupla, mas não utilizadas para acesso inicial, seleção/re-seleção de célula, ou handover. Em alguns casos, as células podem não transmitir sinais de sincronização-em alguns Casos, as Dcélulas podem transmitir a SS. NR BSs podem transmitir sinais de Enlace descendente para os UEs que indicam o tipo de célula. Com base na indicação do tipo de

célula, o UE pode se comunicar com a NR BS. Por exemplo, o UE pode determinar NR BSs para considerar a seleção de células, acesso, entrega, e/ou medição com base no tipo de célula indicado.

[0055] A Figura 2 ilustra uma arquitetura lógica exemplar de uma rede de acesso de rádio distribuída (RAN) 200, que pode ser implementada no sistema de comunicação sem fio ilustrado na Figura 1. O nó de acesso 5G 206 pode incluir um controlador de nó de acesso (ANC) 202. O ANC pode ser uma unidade central (CU) da RAN distribuída 200. A interface de backhaul para a rede núcleo de geração seguinte (NG-CN) 204 pode terminar no ANC. A interface de backhaul para os nós de acesso à geração seguinte vizinhos (NG-ANs) pode terminar no ANC. O ANC pode incluir um ou mais TRPs 208 (que também podem ser referidos como BSs, NR BSs, nós Bs, 5G NBs, APs, ou algum outro termo). Como descrito acima, uma TRP pode ser utilizada de forma intercambiável com "célula".

[0056] Os TRPs 208 podem ser uma DU. Os TRPs podem ser conectados a um ANC (ANC 202) ou mais de um ANC (não ilustrado). Por exemplo, para o compartilhamento de RAN, rádio como um serviço (RaaS), e Desenvolvimentos e aplicações Específicas de serviço, o TRP pode ser conectado A mais de um ANC. A TRP pode incluir uma ou mais portas de antena. Os TRPs podem ser configurados para receber individualmente (por exemplo, seleção dinâmica) ou conjuntamente (por exemplo, transmissão conjunta) para o tráfego para um UE.

[0057] A arquitetura local 200 pode ser utilizada para ilustrar a definição de fronthaul. A

arquitetura pode ser definida para suportar soluções de acesso através de diferentes tipos de desenvolvimento. Por exemplo, a arquitetura pode ser baseada em capacidades de rede de transmissão (por exemplo, largura de banda, latência e/ou instabilidade).

[0058] A arquitetura pode compartilhar características e/ou componentes com LTE. De acordo com aspectos, a AN de geração seguinte (NG-AN) 210 pode suportar a conectividade dual com NR o NG-AN pode compartilhar um terminal comum para LTE e NR.

[0059] A arquitetura pode permitir a cooperação entre as TRPs 208g. Por exemplo, a cooperação pode ser pré-estabelecida dentro de um TRP e/ou através De TRPs através do ANC 202. De acordo com aspectos, nenhuma interface inter-TRP pode ser necessária/presente.

[0060] De acordo com aspectos, uma configuração dinâmica de funções lógicas divididas pode estar presente dentro da arquitetura 200. Conforme será descrito em maiores detalhes com referência à Figura 5, a Camada de controle de Recurso de Rádio (RRC), Camada de protocolo de Convergência de Dados de Pacote (PDCP), Camada de controle de Radioenlace (RLC), Camada de controle de Acesso de Meio (MAC) e uma Camada física (PHY) podem ser adaptativamente colocadas na DU Ou CU (por exemplo, TRP ou ANC, respectivamente). De acordo com certos aspectos, uma BS pode incluir uma unidade central (CU) (por exemplo, ANC 202) e/ou uma ou mais unidades distribuídas (por exemplo, um ou mais TRPs 208).

[0061] A Figura 3 ilustra uma arquitetura física exemplar de uma RAN distribuída 300, de acordo com

aspectos da presente invenção. Uma unidade de rede central centralizada (C-CU) 302 pode hospedar funções de rede de núcleo. O C-CU pode ser instalado centralmente. A funcionalidade C-CU pode ser descarregada (por exemplo, para serviços sem fio avançados (AWS), em um esforço para lidar com a capacidade de pico.

[0062] Uma unidade RAN centralizada (C-RU) 304 pode hospedar uma ou mais funções de ANC. Opcionalmente, a C-RU pode hospedar localmente as funções de rede de núcleo. A C-RU pode ter desenvolvimento distribuído. A C-RU pode estar mais próxima da borda da rede.

[0063] A DU 306 pode hospedar um ou mais TRPs (nó de borda (EN), uma unidade de borda (EU), uma cabeça de rádio (RH), uma cabeça de rádio inteligente (SRH), ou similar). A DU pode estar localizada nas bordas da rede com funcionalidade de radiofrequência (RF).

[0064] A Figura 4 ilustra os componentes ilustrativos da BS 110 e do UE 120 ilustrados na Figura 1, que podem ser usados para implementar aspectos da presente descrição. Como descrito acima, a BS pode incluir um TRP. Um ou mais componentes da BS 110 e do UE 120 podem ser usados para a prática de aspectos da presente invenção. Por exemplo, antenas 452, Tx/Rx 222, processadores 466, 458, 464 e/ou controlador/processador 480 do UE 120 e/ou antenas 434, processadores 460, 420, 438 e/ou controlador/processador 440 da BS 110 podem ser usados para efetuar as operações descritas aqui e ilustradas com referência às Figuras 10-15.

[0065] De acordo com aspectos, para um cenário de associação restrito, a estação base 110 pode ser a macro

BS 110c na figura 1, e o UE 120 pode ser o UE 120y. A estação base 110 também pode ser uma estação base de algum outro tipo. A estação base 110 pode ser equipada com antenas 434a a 434t, e o UE 120 pode ser equipado com antenas 452a a 452r.

[0066] Na estação base 110, um processador de transmissão 420 pode receber dados de uma fonte de dados 412 e informações de controle de um controlador/processador 440. A informação de controle pode ser para o Canal de Difusão Físico (PBCH), Canal indicador De formato de Controle Físico (PCFICH), Canal Indicador ARQ Híbrido físico (PHICH), Canal De controle De enlace descendente físico (PDCCH), Etc. os dados podem ser para o Canal Compartilhado De Enlace descendente físico (PDSCH), etc. o processador 420 pode processar (por exemplo, codificação e mapa de símbolos) os dados e informações de controle para obter símbolos de dados e símbolos de controle, respectivamente. O processador 420 pode também gerar símbolos de referência, por exemplo, para a PSS, SSS e sinal de referência específico de célula. Um processador de transmissão múltipla de múltiplas entradas (MIMO) de transmissão (TX) 430 pode efetuar processamento espacial (por exemplo, pré-codificação) nos símbolos de dados, os símbolos de controle e/ou os símbolos de referência, se aplicável, e pode fornecer fluxos de símbolos de saída para os moduladores (MODs) 432a a 432t. Cada modulador 432 pode processar um respectivo fluxo de símbolos de saída (por exemplo, para OFDM, etc.) para obter um fluxo de amostras de saída. Cada modulador 432 pode também processar (por exemplo, converter em analógico, amplificar, filtrar e

converter ascendentemente) o fluxo de amostras de saída para obter um sinal de enlace descendente. Os sinais de Enlace descendente dos moduladores 432a a 432t podem ser transmitidos através das antenas 434a a 434t, respectivamente.

[0067] No UE 120, as antenas 452a a 452r podem receber os sinais de enlace descendente da estação base 110 e podem fornecer sinais recebidos para os demoduladores (DEMODs) 454a a 454r, respectivamente. Cada demodulador 454 pode condicionar (por exemplo, filtrar, amplificar, converter descendentemente e digitalizar) um respectivo sinal recebido para obter amostras de entrada. Cada demodulador 454 pode processar adicionalmente as amostras de entrada (por exemplo, para OFDM, etc.) para obter símbolos recebidos. Um detector MIMO 456 pode obter símbolos recebidos A partir de todos os demoduladores 454a A 454r, efetuar detecção MIMO nos símbolos recebidos se aplicável, e fornecer símbolos detectados. Um processador de recebimento 458 pode processar (por exemplo, demodular, desintercalar e decodificar) os símbolos detectados, fornecer dados decodificados para o UE 120 a um depósito de dados 460, e fornecer informações de controle decodificadas a um controlador/processador 480.

[0068] No enlace ascendente, no UE 120, um processador de transmissão 464 pode receber e processar dados (por exemplo, para o Canal Compartilhado de enlace ascendente Físico (PUCCH)) de uma fonte de dados 462 e informações de controle (por exemplo, para o Canal de controle De enlace ascendente físico (PUCCH) do controlador/processador 4802. O processador de transmissão

464 também pode gerar símbolos de referência para um sinal de referência. Os símbolos do processador de transmissão 464 podem ser pré-codificados por um processador MIMO TX 466 se aplicável, adicionalmente processados pelos demoduladores 454a a 454r (por exemplo, Para SC-FDM, etc.), e transmitidos para a estação base 110. Na BS 110, os sinais de enlace ascendente do UE 120 podem ser recebidos pelas antenas 434, processados pelos moduladores 432, detectados por um Detector MIMO 436 se aplicável, e ainda processado por um processador de recebimento 438 para obter dados decodificados e informações de controle enviadas pelo UE 120. O processador de recebimento 438 pode fornecer os dados decodificados para um depósito de dados 439 e a informação de controle decodificada para o controlador/processador 440.

[0069] Os controladores/processadores 440 e 480 podem dirigir a operação na estação base 110 e no UE 120, respectivamente. O processador 440 e/ou outros processadores e módulos na estação base 110 podem executar ou dirigir, por exemplo, processos para as técnicas aqui descritas. O processador 480 e/ou outros processadores e módulos no UE 120 também podem executar ou dirigir, por exemplo, a execução dos blocos funcionais ilustrados nas Figuras 10, 12-13 e/ou 15, e/ou outros processos para as técnicas aqui descritas. As memórias 442 e 482 podem armazenar dados e códigos de programa para a BS 110 e o UE 120, respectivamente. Um programador 444 pode programar os UEs para a transmissão de dados no enlace descendente e/ou no enlace ascendente.

[0070] A Figura 5 ilustra um diagrama 500 que mostra exemplos para implementar uma pilha de protocolos de comunicações, de acordo com aspectos da presente invenção. As pilhas de protocolo de comunicações ilustradas podem ser implementadas por dispositivos que operam em sistema 5G (por exemplo, um sistema que suporta mobilidade baseada em enlace ascendente). O diagrama 500 ilustra uma pilha de protocolo de comunicações incluindo uma camada de Controle de Recurso de Rádio (RRC) 510, uma camada de protocolo de Convergência de Dados em Pacote (PDCP) 515, uma camada de Controle de Radioenlace (RLC) 520, uma camada de Controle de Acesso ao Meio (MAC) 525, e uma camada Física (PHY) 530. Em vários exemplos, as camadas de uma pilha de protocolo podem ser implementadas como módulos separados de software, partes de um processador ou ASIC, partes de dispositivos não-colocados conectados por um enlace de comunicações, ou várias combinações dos mesmos. Implementações combinadas e não-combinadas podem ser usadas, por exemplo, em uma pilha de protocolo para um dispositivo de acesso de rede (por exemplo, ANs, CUs, e/ou DUs) ou um UE.

[0071] Uma primeira opção 505-a mostra uma implementação dividida de uma pilha de protocolo, na qual a implementação da pilha de protocolo é dividida entre um dispositivo de acesso de rede centralizado (por exemplo, um ANC 202 na Figura 2) e um dispositivo de acesso de rede distribuída (por exemplo, DU 208 na figura 2). Na primeira opção 505-a, uma camada RRC 510 e uma camada PDCP 515 podem ser implementadas pela unidade central, e uma camada RLC 520, uma camada MAC 525 e uma camada PHY 530 podem ser implementadas pela DU. Em vários exemplos, a CU e a DU

podem ser combinadas ou não-combinadas. A primeira opção 505-a pode ser útil em uma macro célula, micro-célula, ou implantação de células pico.

[0072] Uma segunda opção 505-b mostra uma implementação unificada de uma pilha de protocolo, na qual a pilha de protocolo é implementada em um único dispositivo de acesso de rede (por exemplo, nó de acesso (AN), nova estação base de rádio (NR BS), um nó-B de novo rádio (NR NB), um nó de rede (NN), ou similar.). Na segunda opção, a camada RRC 510, a camada PDCP 515, a camada RLC 520, a camada MAC 525 e a camada PHY 530 podem ser implementadas pela AN. A segunda opção 505-b pode ser útil em um desenvolvimento de femto células.

[0073] Independentemente de se um dispositivo de acesso de rede implementa parte ou toda a pilha de protocolos, um UE pode implementar uma pilha de protocolo inteira (por exemplo, a camada RRC 510, a camada PDCP 515, a camada RLC 520, a camada MAC 525 e a camada PHY 530).

[0074] A Figura 6 é um diagrama 600 que mostra um exemplo de um subquadro central DL, que pode ser usado para se comunicar na rede sem fio 100. O subquadro central DL pode incluir uma parte de controle 602. A parte de controle 602 pode existir na parte inicial ou inicial do subquadro central DL. A porção de controle 602 pode incluir várias informações de programação e/ou informações de controle correspondentes a várias partes do subquadro central DL. Em algumas configurações, a porção de controle 602 pode ser um canal de controle de DL físico (PDCCH), conforme indicado na Figura 6. O subquadro central de DL também pode incluir uma Porção de dados DL 604. A Porção de

dados DL 604 pode às vezes ser referida como a carga útil do subquadro central DL. A porção de dados DL 604 pode incluir os recursos de comunicação utilizados para comunicar dados DL da entidade de programação (por exemplo, UE ou BS) para a entidade subordinada (por exemplo, UE). Em algumas configurações, a porção de dados DL 604 pode ser um canal compartilhado DL físico (PDSCH).

[0075] O subquadro central de DL também pode incluir uma parte de UL comum 606. A parte de UL comum 606 pode algumas vezes ser referida como uma rajada de UL, uma rajada de UL comum, e/ou vários outros termos adequados. A parte de UL comum 606 pode incluir informação de realimentação correspondente a várias outras partes do subquadro central de DL. Por exemplo, a parte de UL comum 606 pode incluir informação de realimentação correspondente à parte de controle 602. Exemplos não limitantes de informação de realimentação podem incluir um sinal ACK, um sinal NACK, um indicador HARQ, e/ou vários outros tipos adequados de informação. A parte de UL comum 606 pode incluir informações adicionais ou alternativas, tais como informações relativas a procedimentos de canal de acesso aleatório (RACH), pedidos de programação (SRs) e vários outros tipos adequados de informação. Conforme ilustrado na Figura 6, a extremidade da parte de dados DL 604 pode ser separada em tempo a partir do início da parte de UL comum 606. Esta separação de tempo pode algumas vezes ser referida como um intervalo, um período de guarda, um intervalo de guarda, e/ou vários outros termos adequados. Esta separação proporciona tempo para a comutação de comunicação DL (por exemplo, operação de recebimento pela

entidade subordinada (por exemplo, UE)) para comunicação de UL (por exemplo, transmissão pela entidade subordinada (por exemplo, UE)). Alguém versado na técnica entenderá que o precedente é meramente um exemplo de um subquadro central DL e estruturas alternativas tendo características similares podem existir sem necessariamente se desviar dos aspectos aqui descritos.

[0076] A Figura 7 é um diagrama 700 que mostra um exemplo de um subquadro centrado em UL, que pode ser usado para se comunicar na rede sem fio 100. O subquadro central de UL pode incluir uma porção de controle 702. A porção de controle 702 pode existir na parte inicial ou inicial do subquadro central de UL. A porção de controle 702 na Figura 7 pode ser similar à porção de controle descrita acima com referência à Figura 6. O subquadro central de UL também pode incluir uma porção de dados de UL 704. A parte de dados de UL 704 pode algumas vezes ser referida como a carga útil do subquadro central de UL. A parte de UL pode se referir aos recursos de comunicação utilizados para comunicar dados de UL da entidade subordinada (por exemplo, UE) para a entidade de programação (por exemplo, UE Ou BS). Em algumas configurações, a porção de controle 702 pode ser um canal de controle DL físico (PDCCH).

[0077] Como ilustrado na Figura 7, a extremidade da porção de controle 702 pode ser separada em tempo a partir do início da porção de dados de UL 704. Esta separação de tempo pode algumas vezes ser referida como um intervalo, um período de guarda, um intervalo de guarda, e/ou vários outros termos adequados. Esta separação

proporciona tempo para a comutação de comunicação DL (por exemplo, operação de recebimento pela entidade de programação) para comunicação de UL (por exemplo, transmissão pela entidade de programação). O subquadro central de UL também pode incluir uma porção de UL comum 706. A porção de UL comum 706 na Figura 7 pode ser similar à porção de UL comum 606 descrita acima com referência à Figura 6. A porção de UL comum 706 pode adicional ou alternativa incluir informação pertencente ao indicador de qualidade de canal (CQI), sinais de referência de som (SRSs), e vários outros tipos adequados de informação. Alguém versado na técnica entenderá que o precedente é meramente um exemplo de um subquadro centrado por UL e estruturas alternativas tendo características similares podem existir sem necessariamente se desviar dos aspectos aqui descritos.

[0078] Em algumas circunstancias, duas ou mais entidades subordinadas (por exemplo, UEs) podem se comunicar entre si utilizando sinais de enlace lateral. As aplicações em mundo real de tais comunicações de enlace lateral podem incluir a segurança pública, os serviços de proximidade, As Comunicações do UE-a-rede, As Comunicações do veículo-a-veículo (V2V), as comunicações da Internet de Tudo (I0E), as comunicações de íon, a malha crítica da missão, e/ou várias outras aplicações adequadas. Geralmente, um sinal de enlace lateral pode se referir a um sinal comunicado a partir de uma entidade subordinada (por exemplo, UE1) para outra entidade subordinada (por exemplo, UE2) Sem retransmitir essa comunicação através da entidade de programação (por exemplo, UE ou BS), mesmo que a

entidade de programação possa ser utilizada para fins de programação e/ou controle. Em alguns exemplos, os sinais de enlace lateral podem ser comunicados utilizando um espectro licenciado (diferentemente das redes de área local sem fio, que tipicamente utilizam um espectro não licenciado).

[0079] Um UE pode operar em várias configurações de recursos de rádio, incluindo uma configuração associada com a transmissão de pilotos utilizando um conjunto dedicado de recursos (por exemplo, um estado dedicado de controle de recurso de rádio (RRC), etc.) ou uma configuração associada com a transmissão de pilotos utilizando um conjunto comum de recursos (por exemplo, um estado comum de RRC, etc.). Ao operar no estado dedicado de RRC, o UE pode selecionar um conjunto dedicado de recursos para transmitir um sinal piloto para uma rede. Ao operar no estado comum de RRC, o UE pode selecionar um conjunto comum de recursos para transmitir um sinal piloto para a rede. Em qualquer caso, um sinal piloto transmitido pelo UE pode ser recebido por um ou mais dispositivos de acesso à rede, tal como uma AN, ou uma DU, ou partes dos mesmos. Cada dispositivo de acesso de rede de recebimento pode ser configurado para receber e medir sinais piloto transmitidos no conjunto comum de recursos, e também receber e medir sinais piloto transmitidos em conjuntos dedicados de recursos alocados aos UEs para os quais o dispositivo de acesso de rede é um membro de um conjunto de monitoramento de dispositivos de acesso de rede para o UE. Um ou mais dos dispositivos de acesso de rede de recebimento, ou uma CU à qual o dispositivo de acesso de rede de recebimento (s) transmite as medições dos sinais

piloto, pode utilizar as medições para identificar as células de serviço Para os UEs, ou para iniciar uma mudança de célula de serviço para um ou mais dos UEs.

Incorporação exemplar de políticas de rede em geração de chave

[0080] Como notado acima, uma nova interface de ar está sendo introduzida para 5G, incluindo características que incluem uma ampla banda larga móvel (eMBB) alvo de largura de banda larga (por exemplo, 80 MHz além), onda milimétrica (mmW) visando uma alta frequência de portadora (por exemplo, 60 GHz), MTC maciço (mMTC) objetivando técnicas de MTC compatível não para trás, e recursos críticos da missão para comunicações de baixa latência ultra-confiáveis (URLLC).

[0081] Como os serviços e tecnologias para 5G continuam a evoluir, 5G pode ser capaz de suportar vários cenários de desenvolvimento diferentes. Na arquitetura atual 5G, por exemplo, um ou mais nós de rede (por exemplo, função de ancoragem de segurança (SEAF), função de acesso e gerenciamento de mobilidade (AMF), função de Gerenciamento de sessão (SMF), etc.) que são responsáveis pela realização de diferentes funções na rede podem ser colocados ou fisicamente separados.

[0082] A SEAF foi introduzida em 5G para manter a âncora de segurança em uma localização fisicamente segura mesmo se houver necessidade de mover e/ou localizar o AMF próximo à borda da rede (por exemplo, RAN). Assim, em algumas configurações, a SEAF pode ser colocada Com a AMF e, em outras utilizações, a SEAF pode Ser separada do AMF (Por Exemplo, a SEAF e a AMF podem ter cada qual funções

independentes). Similarmente, SMF pode ser separado do AMF e da SEAF. Em alguns casos, SMF pode ser fisicamente separado do AMF e pode estar dentro de um domínio de segurança diferente do AMF (por exemplo, no caso de um cenário de compartilhamento de redes). Em alguns casos, SMF pode ser específico de fatia.

[0083] A Figura 8 ilustra um exemplo de referência de uma arquitetura 5G 800 na qual um ou mais nós de rede podem ser separados fisicamente, de acordo com certos aspectos da presente descrição. Em particular, a arquitetura 800 ilustra um exemplo de referência de um cenário de desenvolvimento onde a SEAF é fisicamente separada do AMF (por exemplo, em oposição a um SEAF/AMF colocado em outros cenários de desenvolvimento).

[0084] Como mostrado, a arquitetura 5G 800 pode incluir múltiplas fatias. Cada fatia pode suportar diferentes serviços, por exemplo, internet de tudo (I0E), URLLC, eMBB, comunicações veiculares (Isto é, V2X como veículo-a-veículo (V2V), veículo-a-Infra-estrutura (V2I), veículo-a-Pedestres (V2P), veículo-a-Rede (V2N)), etc.

[0085] Uma fatia pode ser definida como uma rede lógica completa que compreende um conjunto de funções de rede e recursos correspondentes necessários para fornecer certas capacidades de rede e características de rede, que podem incluir tanto 5G-AN como 5G-CN. Mais especificamente, uma fatia pode ser a composição de funções de rede adequadamente configuradas, aplicações de rede e infraestruturas de nuvem subjacentes que são agrupadas juntas para satisfazer a necessidade de um caso de utilização específica ou modelo comercial. Em alguns casos,

diferentes fatias podem ser designadas recursos separados e podem ter requisitos diferentes, tais como latência e/ou potência.

[0086] Neste exemplo, o AMF pode ser configurado para servir múltiplas fatias simultaneamente. Por exemplo, o AMF pode fornecer uma âncora de segurança NAS de Gerenciamento de mobilidade entre o UE e as fatias de rede. SMF é geralmente configurado para realizar a autorização de serviço/serviço de autenticação de serviço para estabelecimento de sessão de PDU Específica de serviço (fatia). SMF pode também executar funções, tais como modificar e liberar, incluindo túnel (s) mantido entre a Função de plano de usuário (UPF) e RAN. A segurança do plano do usuário pode terminar no UDF. Em alguns casos, SMF pode ser capaz de suportar uma QoS específica de serviço.

[0087] A Figura 9 ilustra outro exemplo de referência de uma arquitetura 5G 900 na qual um ou mais nós de rede (por exemplo, SEAF, AMF, SMF, etc.) podem ser fisicamente separados, de acordo com certos aspectos da presente descrição. Em alguns casos, a arquitetura de segurança 5G pode ser projetada para suportar de forma nativa a autenticação secundária com uma Função de servidor de autenticação da parte 3r (AUSF) (por exemplo, AAA da terceira parte) para a autorização da sessão de PDU. A autenticação de serviço permite o estabelecimento de uma sessão de PDU específica de serviço. Similar à Figura 8, a segurança de plano de usuário pode terminar em UPF e uma QoS específica de serviço pode ser suportada. SMF pode ser capaz de fazer interface direta com a terceira parte AAA ou interagir com a terceira parte AAA através da SEAF.

[0088] Conforme observado, uma vez que a rede 5G pode continuar a evoluir, pode ser desejável prover o UE Com informações relativas à configuração de rede, capacidades, informações de segurança, etc. (referidos coletivamente aqui como informação de política de rede). Entretanto, devido às arquiteturas atuais, a única interface de plano de controle entre o UE e a rede de serviço é N1, que é utilizada para a conexão NAS entre o UE e o AMF, pode não ser possível com o uso de técnicas atuais para fornecer informações de política de rede para o UE de uma maneira segura.

[0089] Por exemplo, com referência à arquitetura 800, já que o AMF pode ser a única entidade que tem uma conexão de sinalização com o UE (por exemplo, com base na Sinalização NAS), o AMF pode ser capaz de informar falsamente o UE Com relação a quaisquer informações política de segurança da rede recebidas de outro nó de rede (por exemplo, SEAF, SMF, etc.). Assim, se a informação de política de rede incluir informação que o AMF e SEAF são separados, as técnicas atuais podem não ser capazes de informar de Forma segura o UE que o AMF e A SEAF são separados, porque o UE só pode ter uma conexão de sinalização com o AMF (por exemplo, em oposição a também ter uma conexão de sinalização com A SEAF).

[0090] Em tais casos, um AMF autónomo pode ser capaz de reivindicar que é colocado com a SEAF, um cenário que não pode ser detectado pelo UE. Tal AMF independente pode ser capaz de modificar as capacidades de segurança da rede, a proteção do NAS de gerenciamento de Sessão, as capacidades/requisitos de segurança específicos da fatia,

etc., a fim de comprometer a conexão/sessão entre O UE e a rede.

[0091] Além disso, sem informações de política de rede precisas (seguras), o UE pode estar sujeito a ataques de compromisso (por exemplo, no estabelecimento de sessão de PDU). Em um exemplo de cenário de compromisso, o AMF pode estar em um diferente domínio de segurança do que SMF. Por exemplo, em um caso, o AMF pode estar localizado próximo ao UE (ou RAN) em uma rede de serviço (por exemplo, que pode ser uma localização menos segura), enquanto que SMF pode estar localizado profundamente na rede.Em um caso, o AMF pode estar na rede servidora (por exemplo, VPLMN), enquanto que SMF está na rede doméstica.

[0092] Entretanto, embora o AMF possa estar em um domínio de segurança diferente do SMF, SMF Pode ainda ser responsável pela autorização da criação da sessão de PDU específica de fatia (por exemplo, com base em informações de assinatura específica de fatia que não podem ser acessadas pelo AMF). SMF, por exemplo, é tipicamente uma função de rede logicamente separada do AMF e é responsável pela Autorização e gerenciamento da sessão de PDU. Como notado acima, SMF pode ser específico de fatia e, portanto, pode trocar parâmetros de sessão de PDU específicos de fatia com o UE.

[0093] Entretanto, parâmetros de sessão de PDU, tais como Regra de QoS Autorizada, modo SSC, S-NSSAI, endereço IPv4 alocado, etc., solicitados pelo UE e Configurados por SMF não Devem ser modificados por um nó intermediário (por exemplo, incluindo o AMF) entre o UE E SMF. Ao invés disso, tais parâmetros devem ser protegidos

por SMF utilizando uma chave específica obtida a partir de SEAF e verificável no UE Pela derivação da mesma Chave SMF. Assim, em situações nas quais a AMF é separada da SEAF, a (mal ou comprometida) AMF pode modificar as informações de sessão solicitadas pelo UE Ou autorizadas por SMF, por exemplo, a fim de rebaixar segurança, QoS, ou outro tratamento de pacotes.

[0094] Consequentemente, os aspectos apresentados aqui proporcionam técnicas para informar de forma segura o UE da informação de política de rede, por exemplo, para minimizar ataques de ofertas. Particularmente, aspectos fornecem técnicas para incorporar a informação de política de rede na derivação de chave (por exemplo, K_{AMF}) usada para fixar a Conexão NAS entre o UE e o AMF. Como descrito abaixo, pela incorporação da informação de política de rede na derivação de chave, o UE pode ser capaz de detectar se qualquer informação de política de rede recebida a partir do AMF foi alterada/modificada/comprometida.

[0095] Note que embora as técnicas aqui descritas possam ser utilizadas para proteger contra os ataques de ofertas do estabelecimento de sessão de PDU, os aspectos aqui apresentados podem também ser usados para proteção contra o compromisso de política de UE pelo nó (s) Entre o SEAF e o UE. Isto é, conforme descrito abaixo, os aspectos aqui apresentados podem também ser usados para proteger informações de política de UE (por exemplo, características de segurança de UE e/ou capacidades de UE, incluindo capacidades de rede, capacidades de segurança, ou qualquer combinação das mesmas), por exemplo, pela

incorporação da informação de política de UE na derivação de chave (por exemplo, KAM). A informação de política de UE pode ser fornecida à rede em mensagem de solicitação de associação/ligação.

[0096] De acordo com certos aspectos, a derivação de K_{AMF} pode ser utilizada para proteger o parâmetro (s) trocado na rede. Em particular, quando um UE se registra em uma rede, a SEAF poderá informar ao UE da informação de política de rede (segurança) (por exemplo, configuração de rede, capacidades, características de segurança, etc.) e/ou Informações de política de UE (por exemplo, recebidas pelo UE) incorporando a informação de política de rede e/ou Informação de política de UE na derivação de chave (por exemplo, K_{AMF}).

[0097] Por exemplo, a SEAF pode derivar uma Chave AMF (por exemplo, K_{AMF}) com base NAS informações de política de rede, informações de Política de UE, parâmetros de frescura ou qualquer combinação das mesmas, e enviar a chave para a AMF De modo que a AMF e o UE possam estabelecer um Contexto de segurança NAS e a SEAF também pode informar o UE Da informação de política de UE recebida a partir do UE. O AMF e O UE podem derivar encriptação e senhas de proteção de integridade do K_{AMF} e protegem as Mensagens NAS (por exemplo, sobre a Interface N1).

[0098] Pela incorporação da informação de política de rede na derivação de K_{AMF}, o AMF pode ser impedido de realizar comportamentos não autorizados, tais como funções de rede de compromisso por modificação da informação de Política de rede recebida a partir de SEAF, já que a mudança na informação de política de rede resulta

em uma derivação De K_{AMF} diferente no UE. Similarmente, pela incorporação da informação de política de UE na derivação de K_{AMF}, os nós de rede entre o UE e a SEAF podem ser impedidos de se beneficiar das capacidades do UE modificando as capacidades do UE, já que a mudança nas Capacidades do UE também resultará em uma Derivação de K_{AMF} diferente.

[0099] A Figura 10 ilustra operações de exemplo 1000 para comunicações sem fio. De acordo com certos aspectos, as operações 1000 podem ser realizadas, por exemplo, por um equipamento de usuário para estabelecer uma conexão segura (por exemplo, NAS) com uma rede.

[00100] As operações 1000 podem começar em 1002 onde o UE recebe (por exemplo, de um AMF) uma primeira mensagem (por exemplo, mensagem de comando de modo de segurança (SMC)) para estabelecer uma conexão segura com uma rede. A primeira mensagem inclui informação de política de rede (por exemplo, a configuração de rede, capacidades, características de segurança, etc.). Em 1004, o UE gera uma primeira chave (por exemplo, K_{AMF}) com base em parte da informação de política de rede.

[00101] Em alguns aspectos, a informação de política de rede inclui uma indicação de se o UE receberá uma ficha de gerenciamento de sessão, de SMF na rede, ao estabelecer uma sessão de comunicação com a rede. Em alguns aspectos, a informação de política de rede compreende uma indicação de se o AMF é colocado com a SEAF na rede. Em alguns aspectos, a informação de política de rede inclui um nível de segurança do AMF. Em alguns aspectos, a informação de política de rede inclui um domínio de segurança da SEAF,

um domínio de segurança do AMF, ou qualquer combinação dos mesmos. Em alguns aspectos, a informação de política de rede pode ter sido formada em resposta à informação de política de UE que foi enviada a partir do UE para a rede. Em alguns aspectos, a primeira chave pode ser determinada com base na informação de política de UE que foi enviada para a rede.

[00102] Em 1006, o UE utiliza a primeira chave para verificar se a informação de política de rede é válida. Por exemplo, em alguns casos, o UE pode determinar se a primeira mensagem (contendo a informação de política de rede) é válida com base em parte na primeira chave.

[00103] Como descrito em maiores detalhes abaixo, em alguns casos, a primeira mensagem pode ser uma mensagem de SMC que é protegida de integridade com uma chave de proteção derivada com base em uma segunda chave (por exemplo, K_{AMF} fornecida ao AMF Da SEAF). O UE pode determinar se a primeira mensagem (e/ou a informação de política de rede contida nele) é válida pela execução de uma verificação de integridade da primeira mensagem com base na primeira chave. Em um aspecto, o UE pode determinar que a primeira mensagem é válida se a verificação de integridade da primeira mensagem for correta.

[00104] O UE pode determinar que a verificação de integridade da primeira mensagem é correta se o UE determinar que a primeira chave é a mesma que a segunda chave. O UE pode determinar que a informação de política de rede é válida com base na determinação de que a primeira chave é a mesma que a segunda chave. Da mesma forma, o UE pode determinar que a primeira mensagem é inválida se a

verificação de integridade da primeira mensagem estiver incorreta. O UE pode determinar que a verificação de integridade da primeira mensagem é incorreta se a primeira chave for diferente da segunda chave. O UE pode determinar que a informação de política de rede é inválida com base na determinação de que a primeira chave é diferente da segunda chave.

[00105] A Figura 11 ilustra operações de exemplo 1100 para comunicações sem fios. De acordo com certos aspectos, as operações 1100 podem ser realizadas, por exemplo, por um nó de rede (por exemplo, SEAF) para fornecer seguramente informação de política de rede para o UE.

[00106] As operações 1100 podem começar em 1102, onde o nó de rede gera uma chave (por exemplo, K_{AMF}) para outro nó de rede (por exemplo, AMF) com base pelo menos em parte na informação de política de rede. Conforme observado, a informação de política de rede pode incluir uma indicação de se o outro nó de rede (por exemplo, AMF) é colocado com o nó de rede. Em alguns casos, a informação de política de rede pode incluir pelo menos um dentre um nível de segurança do nó de rede, ou uma indicação de se SMF na rede é gerar uma ficha SM para uma sessão de comunicação entre o UE e a rede, e enviar a mesma ficha SM para o UE. A chave é utilizada para estabelecer uma conexão segura entre o UE e o nó de rede.

[00107] Em alguns aspectos, o nó de rede pode receber uma mensagem de registro/mensagem de solicitação de anexação que inclui informação de política (ou capacidade) de UE. O nó de rede pode incorporar a informação de

política de UE recebida na derivação de chave (por exemplo, K_{AMF}) para o outro nó de rede. Por exemplo, em 1102 da Figura 1, o nó de rede pode gerar a chave (por exemplo, K_{AMF}) para o outro nó de rede (por exemplo, AMF) com base em parte da informação de política de rede, parâmetros de frescura, Informações de política de UE, ou qualquer combinação dos mesmos.

[00108] Em 1104, o nó de rede envia a chave para o outro nó de rede. Em alguns aspectos, o nó de rede pode enviar adicionalmente pelo menos uma das informações de política de rede ou a quantidade de tempo que a informação de política de rede é válida para o nó de rede.

[00109] A Figura 12 é um fluxograma de chamada que ilustra um procedimento de registro exemplar que permite que a SEAF informa de forma segura o UE da informação de política de rede (segurança) e/ou Informações de política de UE (por exemplo, pela incorporação da informação de política e/ou Informação de política de UE em derivação de chave), de acordo com certos aspectos da presente invenção.

[00110] Em alguns aspectos, conforme mostrado, o UE pode enviar inicialmente uma solicitação de registro/ligação de enlace à rede (por exemplo, AMF, SEAF, etc.). A solicitação de registro/solicitação de enlace inclui a política de UE (capacidades). Então, na etapa 1, o UE realiza um procedimento de autenticação/registro com a rede. O UE e SEAF podem estabelecer uma chave de ancoragem compartilhada (K_{SEAF}) com base em uma nova autenticação ou com base em uma autenticação anterior. Durante o registro, o AMF pode solicitar uma chave (K_{AMF}) da SEAF.

[00111] Na etapa 2, a SEAF gera (por exemplo, deriva), para a AMF, um K_{AMF} para registrar o UE à rede. A derivação de K_{AMF} incorpora a informação de política de rede (por exemplo, a configuração de rede, capacidades, características de segurança, etc.) e/ou Informações de política de UE. Em um aspecto, a informação de política de rede pode incluir o tipo AMF, por exemplo, AMF/SEAF, independente AMF, etc.

[00112] Por exemplo, a informação de política de rede pode incluir um ou mais bits de separação SEAF/AMF. Se o AMF solicitando o K_{AMF} For um AMF Independente separado da SEAF, a SEAF pode estabelecer o Bit de Separação SEAF/AMF (s) para um primeiro valor (por exemplo, 1). Se o AMF solicitando o K_{AMF} For um AMF/SEAF colocado, A SEAF pode Estabelecer o Bit de Separação SEAF/AMF (s) para um segundo valor diferente (por exemplo, 0). Em um aspecto, a derivação de KAM pode também incorporar um ou mais parâmetros de frescura usados para impedir ataques de reprodução. Exemplos de tais parâmetros de frescura podem incluir contador (s) (mantidos ambos no UE E SEAF), valores aleatórios trocados entre O UE e SEAF, ou qualquer combinação dos mesmos. Em um aspecto, a SEAF pode usar a seguinte equação (1) para gerar (Derivar) K_{AMF}:

K_{AMF} = KDF (K_{SEAF}, parâmetro de frescor (s), informação de Política de rede, política de UE) (1)

onde KDF é uma função de derivação de chave (por exemplo, HMAC-SHA -1, HMAC-SHA -256, HMAC-SHA -512, PRF-X (função pseudoaleatória cujo Tamanho de Saída é X)), K_{SEAF} é a chave

de proteção de ancoragem na rede de serviço (e mantida na SEAF), parâmetros de frescura são o contador (s), valor aleatório (s) usado para impedir ataques de reprodução, a informação de política de rede inclui a configuração de rede, capacidades, características de segurança, etc., e a política de UE inclui pelo menos uma dentre informação De capacidade de UE e/ou informação de segurança de UE.

[00113] Na etapa 3, a SEAF fornece o K_{AMF}, o parâmetro de frescor (s) e a informação de política de rede para o AMF. Em alguns aspectos, a SEAF pode também fornecer (por exemplo, repetir) a Política de UE na etapa 3 para a AMF. Na etapa 4, o AMF envia um comando NAS de modo de segurança (SMC) para o UE. Em alguns aspectos, o AMF pode também fornecer (por exemplo, repetir) a Política de UE na etapa 4 para o UE. O NAS SMC pode incluir o parâmetro de frescura (s) e a informação de política de rede obtida a Partir da SEAF, e O NAS SMC pode ser protegido de integridade baseado em K_{AMF}-por exemplo, ao receber O KAF De SEAF, O AMF pode derivar Uma chave de proteção de integridade NAS (por exemplo, K_{NASINT}) com base em K_AMF e usar K_{NASINT} para a Integridade de Proteção da mensagem NAS de NAS.

[00114] Na etapa 5, o UE gera (por exemplo, deriva) um K_{AMF} utilizando a K_{SEAF}, e a informação (por exemplo, parâmetro de frescura (s), informação de política de rede, etc.) na Mensagem NAS SMC, e Verifica a Mensagem NAS SMC. Isto é, o UE pode detectar se houve quaisquer mudanças (por exemplo, pela AMF) para a informação de política de rede, uma vez que quaisquer mudanças na informação de política de rede conduzirão a uma derivação

de K_{AMF} diferente no UE. O UE pode detectar tais mudanças quando o UE verifica a proteção de integridade do NAS SMC utilizando ao comparar o K_{AMF} gerado pelo UE Com a proteção de integridade do NAS SMC utilizando K_{AMF}-Assim, uma determinação de que a verificação de integridade Do SMC é correta implica que o K_{AMF} gerado pelo UE E o K_{AMF} Fornecido ao AMF (de SEAF) é o mesmo que, por sua vez, implica em que a informação de política De rede fornecida ao UE (de AMF) é válida.

[00115] Presumindo-se que a verificação de SMC esteja correta, o UE (na etapa 6) envia uma mensagem completa de modo de segurança NAS para A AMF. Em alguns aspectos, o UE pode também detectar se a informação de política de UE (fornecida à rede) foi modificada por qualquer um dos nós de rede intermediários. Isto é, em alguns aspectos, o UE pode gerar K_{AMF} com base NAS informações De política de UE (por exemplo, além de ou alternativamente à informação de política de rede) para determinar se a informação de política de UE foi modificada (por exemplo, com base em se o K_{AMF} gerado pelo UE E o K_{AMF} fornecido ao AMF (de SEAF) são iguais).

[00116] Note que enquanto o fluxo de chamada na Figura 12 descreve a incorporação de informações de política de rede em derivação de chave para informar de forma segura o UE da informação de política de rede, as técnicas apresentadas aqui também podem ser utilizadas para proteger recursos de segurança de UE. Isto é, além de ou na alternativa à informação de política de rede, a derivação de chave (K_{AMF}) pode incorporar as Capacidades do UE (incluindo Características de segurança do UE), onde as

Capacidades do UE são fornecidas à rede em uma mensagem de registro/solicitação de enlace.

[00117] As técnicas descritas NAS Figuras 10 a 12 podem ser utilizadas para impedir que o AMF modifique quaisquer parâmetros de capacidade de rede que ele recaia para o UE, restringindo o uso de chave na derivação de chave. Entretanto, embora estas técnicas possam ser úteis para impedir o compromisso das capacidades de rede, tais técnicas não podem ser suficientes para impedir a eliminação do parâmetro de sessão de PDU (por Exemplo, ficha de SM NAS).

[00118] Consequentemente, os aspectos aqui apresentados proporcionam técnicas que podem ser utilizadas para impedir ataques de compromisso (por exemplo, no estabelecimento de sessão de PDU e/ou parâmetros de capacidade de rede).

[00119] Mais especificamente, quando um UE registra para a rede, a SEAF fornece a informação de política de rede (por exemplo, capacidades de configuração de rede, segurança), etc.) e a informação de política de rede protegida de integridade (por exemplo, sinal de política de rede) juntamente com o K_{AMF} para a AMF. A informação de política de rede é protegida de integridade utilizando K_{SEAF}. A ficha de política de rede é transmitida no comando NAS de modo de segurança e fornecido ao UE. A ficha de política de rede impede quaisquer funções de rede situadas entre a SEAF e O UE de modificar as capacidades de rede.

[00120] A Figura 13 ilustra operações de exemplo 1300 para comunicações sem fio. De acordo com

certos aspectos, as operações 1300 podem ser realizadas, por exemplo, por um equipamento de usuário para estabelecer uma conexão segura (por exemplo, NAS) com uma rede.

[00121] As operações 1300 podem começar em 1302 onde o UE estabelece, com base em um procedimento de autenticação com uma rede, uma chave de ancoragem (por exemplo, K_{SEAF}) que é compartilhada entre o UE e uma SEAF na rede. Em 1304, o UE recebe uma primeira mensagem (por exemplo, mensagem SMC) para estabelecer uma conexão segura com a rede. A primeira mensagem inclui um sinal de política de rede para uma sessão de comunicação com a rede, a informação de política de rede, uma primeira quantidade de tempo em que a informação de política de rede é válida e uma segunda quantidade de tempo que uma primeira chave usada para a conexão segura é válida. A ficha de política de rede inclui informação de proteção de integridade associada com a informação de política de rede.

[00122] Em 1306, o UE determina se a ficha de política de rede é válida com base em uma chave derivada da chave de âncora compartilhada, da informação de política de rede, da primeira quantidade de tempo e da segunda quantidade de tempo, antes de estabelecer a conexão segura com a rede. Em alguns aspectos, determinar se a ficha de política de rede é válida inclui verificar a informação de proteção de integridade com base na chave derivada da chave de ancoragem compartilhada. Em alguns aspectos, o UE pode enviar informações de política de UE (por exemplo, informação de capacidade de UE, informação de segurança de UE, etc.) para a rede. O UE pode gerar uma chave com base nas informações de política de UE enviadas para a rede. Em

alguns casos, a informação de política de rede pode ser baseada na informação de política de UE.

[00123] A Figura 14 ilustra operações de exemplo 1400 para comunicações sem fio. De acordo com certos aspectos, as operações 1400 podem ser realizadas, por exemplo, por um nó de rede (por exemplo, SEAF) para a provisão segura de informações de política de rede para o UE.

[00124] As operações 1400 podem começar em 1402 onde o nó de rede estabelece, com base em um procedimento de autenticação com um UE, uma chave de ancoragem (por exemplo, K_{SEAF}) que é compartilhada entre o nó de rede e o UE na rede. Em 1404, o nó de rede gera um sinal de política de rede (por exemplo, Ktoken) com base em parte da chave de âncora, informação de política de rede, e uma primeira quantidade de tempo que a ficha de política de rede é válida. A ficha de política de rede inclui informação de proteção de integridade associada com a informação de política de rede. Em 1406, o nó de rede gera uma chave (por exemplo, K_{AMF}) para outro nó de rede (por exemplo, AMF). Em 1408, o nó de rede envia a chave, a informação de política de rede e a ficha de política de rede para o outro nó de rede.

[00125] Em alguns aspectos, conforme descrito acima, o nó de rede pode incorporar informações de política de UE dentro da derivação de chave (por exemplo, K_{AMF}), por exemplo, para impedir que nós intermediários de modificar a informação de política de UE recebida a partir do UE. Conforme observado, o nó de rede pode receber a informação

de política de UE através de uma mensagem de registro/solicitação de enlace.

[00126] A Figura 15 é um fluxograma de chamada que ilustra um procedimento de registro exemplar que permite que a SEAF evite ataques de ofertas no estabelecimento da sessão de PDU, de acordo com certos aspectos da presente invenção.

[00127] Conforme mostrado, na etapa 1, o UE realiza um procedimento de registro com a rede. O UE e SEAF podem estabelecer uma chave de ancoragem compartilhada (K_{SEAF}) com base em uma nova autenticação ou com base em uma autenticação prévia. Durante o registro, o AMF pode solicitar uma chave (K_{AMF}) a partir Da SEAF. Embora não mostrado, em alguns casos, o UE pode fornecer informações de política de UE (por exemplo, informação de capacidade de UE, informação de segurança de UE, etc.) à rede através de uma mensagem de registro/solicitação de enlace.

[00128] Na etapa 2, a SEAF gera, para a AMF, um K_{AMF} para registrar o UE à rede. A SEAF pode gerar o K_{AMF} utilizando K_{SEAF} e um ou mais primeiros parâmetros de frescura. Adicionalmente, a SEAF gera um sinal de política de rede utilizando K_{SEAF}, um ou mais segundos parâmetros de frescura (por exemplo, para impedir ataques de reprodução), e a informação de política de rede. Como observado, a ficha de política de rede é um código de autenticação de mensagem (ou informação de proteção de integridade) da informação de política de rede. Similar à Figura 12, a informação de política de rede pode incluir um ou mais bits de separação SEAF/AMF. Em alguns aspectos, a SEAF pode gerar o K_{AMF} adicionalmente baseado na informação de política de UE.

[00129] Na etapa 3, a SEAF fornece o K_{AMF}, o primeiro e o segundo parâmetro de vigor (s), a ficha de política de rede e a informação de política de rede para o AMF. Na etapa 4, o AMF envia um Comando NAS de modo de segurança para o UE. O comando de modo de segurança NAS inclui a informação de política de rede, o primeiro e o segundo parâmetros de frescura e a ficha de política de rede obtida a partir da SEAF.

[00130] Na etapa 5, o UE realiza um procedimento de verificação na ficha de política de rede utilizando K_{SEAF}. Se a verificação for bem sucedida, então o UE deriva um K_{AMF} utilizando a K_{SEAF}, e realiza um procedimento de verificação no Comando de modo de segurança NAS Utilizando o K_{AMF} Derivado-supondo que o comando de modo De segurança NAS é verificado, o UE (na Etapa 6) envia Uma mensagem completa de modo de segurança NAS para o AMF. Desta maneira, a SEAF pode indicar as capacidades de rede diretamente para o UE de uma maneira segura (à medida que a ficha é gerada e verificada com base na chave entre o UE e A SEAF).

[00131] Note que, em alguns aspectos, a SEAF (para a figura 15) pode ter que manter um estado adicional (por exemplo, parâmetro de vigor) (comparado com a SEAF na figura 12) do UE para a geração de políticas de rede para impedir ataques de reprodução. Isto pode ser similar à manutenção de um estado de conexão entre o UE e a SEAF, uma conexão que pode ser propensa a dessincronização. Além disso, note-se que técnicas similares às técnicas descritas nas Figuras 13-15 também podem ser utilizadas para proteger ataques de ofertas em informações de política de UE

(incluindo informação de segurança de UE e/ou informação de capacidade de UE).

[00132] Os métodos aqui descritos compreendem uma ou mais etapas ou ações para a obtenção do método descrito. As etapas e/ou ações do método podem ser intercambiadas umas com as outras sem se afastar do escopo das reivindicações. Em outras palavras, a menos que uma ordem específica de etapas ou ações seja especificada, a ordem e/ou o uso de etapas e/ou ações específicas pode ser modificada sem se afastar do escopo das reivindicações.

[00133] Como usado aqui, uma frase com referência a "pelo menos um de uma lista de itens refere-se a qualquer combinação desses itens, incluindo elementos únicos. Como um exemplo," pelo menos um dos: a, b, ou c " é destinado a cobrir um, b, c, a-b, a-c, b-c e a-b-c, bem como qualquer combinação com múltiplos do mesmo elemento (por exemplo, a-a, a-a-a, a-a-b, a-a-c, a-b-b, a-c-c, b-b, b-b-b, b-b-c, c-c e c-c-c ou qualquer outra ordenação de a, b e

[00134] Conforme aqui utilizado, o termo "determinação" abrange uma ampla variedade de ações. Por exemplo, "determinação" pode incluir cálculo, computação, processamento, derivação, investigação, procura (por exemplo, olhando em uma tabela, uma base de dados ou outra estrutura de dados), verificação e semelhantes. Também, "determinar" pode incluir receber (por exemplo, receber informações), acessar (por exemplo, acessar dados em uma memória) e semelhantes. Também, "determinação" pode incluir resolução, seleção, escolha, estabelecimento e semelhantes.

[00135] Em alguns casos, ao invés de realmente transmitir um quadro, um dispositivo pode ter uma interface para emitir um quadro para transmissão. Por exemplo, um processador pode emitir um quadro, através de uma interface de barramento, para uma extremidade frontal de RF para transmissão. Similarmente, ao invés de receber realmente um quadro, um dispositivo pode ter uma interface para obter um quadro recebido de outro dispositivo. Por exemplo, um processador pode obter (ou receber) um quadro, através de uma interface de barramento, a partir de uma extremidade frontal de RF para transmissão.

[00136] As várias operações dos métodos descritos acima podem ser realizadas por qualquer meio adequado capaz de executar as funções correspondentes. Os meios podem incluir vários componentes de hardware e/ou software (s) e/ou módulo (s), incluindo, mas sem limitações, um circuito, um circuito integrado de aplicação Específica (ASIC), ou processador. Geralmente, onde existem operações ilustradas em figuras, essas operações podem ter componentes correspondentes de meios-mais-função com numeração similar.

[00137] Por exemplo, meios para transmitir, meios para determinar, meios para determinar, meios para determinar, meios para o estabelecimento, meios para o envio, meios para armazenamento, meios para armazenamento, meios para a entrada, meios para a prevenção, meios para a manutenção, meios para a geração, meios para encaminhamento, meios para encaminhamento, e/ou meios para a provisão de um ou mais processadores ou antenas na BS 110 ou O UE 120, tal como o processador de transmissão 420, o

controlador/processador 440, o processador de recebimento 438, ou as antenas 434 na BS 110 e/ou o processador de transmissão 464, o controlador/processador 480, o processador de recebimento 458, ou as antenas 452 no UE 120.

[00138] Os vários blocos lógicos ilustrativos, módulos e circuitos descritos com relação à presente descrição podem ser implementados ou executados com um processador de finalidade geral, um processador de sinal digital (DSP), um circuito integrado específico de aplicação (ASIC), um arranjo de porta programável em campo (FPGA) ou outro dispositivo lógico programável (PLD), porta discreta ou lógica de transistor, componentes de hardware discretos, ou qualquer combinação dos mesmos projetada para executar as funções descritas aqui. Um processador de uso geral pode ser um microprocessador, mas na alternativa, o processador pode ser qualquer processador, controlador, microcontrolador ou máquina de estado comercialmente disponível. Um processador também pode ser implementado como uma combinação de dispositivos de computação, por exemplo, uma combinação de um DSP e um microprocessador, uma pluralidade de microprocessadores, um ou mais microprocessadores em conjunto com um núcleo DSP, ou qualquer outra configuração tal.

[00139] Se implementado em hardware, uma configuração de hardware exemplar pode compreender um sistema de processamento em um nó sem fio. O sistema de processamento pode ser implementado com uma arquitetura de barramento. O barramento pode incluir qualquer número de barramentos de interconexão e pontes, dependendo da

aplicação específica do sistema de processamento e das restrições globais do projeto. O barramento pode ser conectado a vários circuitos, incluindo um processador, um meio legível por máquina, e uma interface de barramento. A interface de barramento pode ser utilizada para conectar um adaptador de rede, entre outras coisas, ao sistema de processamento através do barramento. O adaptador de rede pode ser usado para implementar as funções de processamento de sinal da camada PHY. No caso de um terminal de usuário 120 (ver Figura), uma interface de usuário (por exemplo, teclado, visor, mouse, joystick, etc.) também pode ser conectada ao barramento. O barramento pode também ligar vários outros circuitos, tais como fontes de temporização, periféricos, reguladores de tensão, circuitos de gerenciamento de energia, e semelhantes, que são bem conhecidos na técnica e, portanto, não serão descritos. O processador pode ser implementado com um ou mais processadores de uso geral e/ou propósito especial. Exemplos incluem microprocessadores, microcontroladores, processadores DSP e outros circuitos que podem executar software. Aqueles versados na técnica reconhecerão como implementar a funcionalidade descrita para o sistema de processamento, dependendo da aplicação específica e das restrições globais de projeto impostas ao sistema global.

[00140] Se implementado em software, as funções podem ser armazenadas ou transmitidas através de uma ou mais instruções ou código em um meio legível por computador. O software deve ser interpretado amplamente para significar instruções, dados, ou qualquer combinação dos mesmos, seja referido como software, firmware,

middleware, microcódigo, linguagem de descrição de hardware, ou de outra forma. Meios passíveis de leitura por computador incluem meios de armazenamento de computador e meios de comunicação incluindo qualquer meio que facilite a transferência de um programa de computador de um lugar para outro. O processador pode ser responsável por gerenciar o barramento e o processamento geral, incluindo a execução de módulos de software armazenados no meio de armazenamento legível por máquina. Um meio de armazenamento legível por computador pode ser acoplado a um processador tal que o processador possa ler informação a partir de, e gravar informações no, meio de armazenamento. Na alternativa, o meio de armazenamento pode ser integrante com o processador. A título de exemplo, o meio legível por máquina pode incluir uma linha de transmissão, uma onda portadora modulada por dados, e/ou um meio de armazenamento legível por computador com instruções armazenadas no mesmo separadas do nó sem fio, tudo o qual pode ser acessado pelo processador através da interface de barramento. Alternativamente, ou além disso, o meio legível por máquina, ou qualquer porção do mesmo, pode ser integrado no processador, tal como o caso de armazenamento temporário e/ou arquivos de registradores gerais. Exemplos de meios de armazenamento legível por máquina podem incluir, por meio de exemplo, RAM (memória de Acesso Aleatório), memória flash, ROM (memória Somente de Leitura), PROM (memória de Leitura Programável), EPROM (memória somente de leitura Programável Apagável), EEPROM (memória somente de leitura Programável Eletricamente Apagável), registradores, discos magnéticos, discos ópticos, discos rígidos, ou qualquer

outro meio de armazenamento adequado, ou qualquer combinação dos mesmos. A mídia legível por máquina pode ser incorporada em um produto de programa de computador.

[00141] Um módulo de software pode compreender uma única instrução, ou muitas instruções, e pode ser distribuído através de vários diferentes segmentos de código, entre programas diferentes, e através de múltiplos meios de armazenamento. A mídia legível por computador pode compreender um número de módulos de software. Os módulos de software incluem instruções que, quando executadas por um aparelho tal como um processador, fazem com que o sistema de processamento execute várias funções. Os módulos de software podem incluir um módulo de transmissão e um módulo de recebimento. Cada módulo de software pode residir em um único dispositivo de armazenamento ou ser distribuído através de múltiplos dispositivos de armazenamento. A título de exemplo, um módulo de software pode ser carregado na RAM a partir de um disco rígido quando ocorre um evento de disparo. Durante a execução do módulo de software, o processador pode carregar algumas das instruções em cache para aumentar a velocidade de acesso. Uma ou mais linhas de cache podem então ser carregadas em um arquivo de registradores gerais para execução pelo processador. Quando se referindo à funcionalidade de um módulo de software abaixo, será entendido que tal funcionalidade é implementada pelo processador quando executando instruções a partir daquele módulo de software.

[00142] Também, qualquer conexão é apropriadamente denominada um meio legível por computador. Por exemplo, se o software For transmitido a partir de um

website, servidor, ou outra fonte remota utilizando um cabo coaxial, cabo de fibra óptica, par torcido, linha de assinante digital (DSL), ou tecnologias sem fio tais como infravermelho (IR), rádio e microondas, então o cabo coaxial, cabo de fibra óptica, par torcido, DSL ou tecnologias sem fio tais como infravermelho, rádio e microondas são incluídos na definição de meio. Disco e disk, conforme aqui usado, incluem disco compacto (CD), disco laser, disco óptico, disco versátil digital (DVD), disco flexível, e disco Blu-ray ® onde discos usualmente reproduzem dados magneticamente, enquanto discos reproduzem dados opticamente com lasers. Assim, em alguns aspectos, a mídia legível por computador pode compreender mídia legível por computador não transicional (por exemplo, mídia tangível). Além disso, para outros aspectos, a mídia legível por computador pode compreender mídia legível por computador transitória (por exemplo, um sinal). Combinações do dito acima também devem ser incluídas no escopo de meios passíveis de leitura por computador.

[00143] Além disso, deve-se apreciar que os módulos e/ou outros meios apropriados para a realização dos métodos e técnicas aqui descritos podem ser baixados e/ou de outra forma obtidos por um terminal de usuário e/ou estação base conforme aplicável. Por exemplo, tal dispositivo pode ser acoplado a um servidor para facilitar a transferência de meios para a realização dos métodos aqui descritos. Alternativamente, vários métodos aqui descritos podem ser providos através de meios de armazenamento (por exemplo, RAM, ROM, um meio físico de armazenamento tal como um disco compacto (CD) ou disco flexível, etc.), tal que um

terminal de usuário e/ou estação base pode obter os vários métodos mediante acoplamento ou fornecimento do meio de armazenamento para o dispositivo. Além disso, qualquer outra técnica adequada para fornecer os métodos e técnicas aqui descritas a um dispositivo pode ser utilizada.

[00144] Deve-se entender que as reivindicações não são limitadas à configuração e componentes precisos ilustrados acima. Várias modificações, mudanças e variações podem ser feitas na disposição, operação e detalhes dos métodos e aparelhos descritos acima sem se afastar do escopo das reivindicações.

REIVINDICAÇÕES

1. Método para comunicação sem fio por equipamento de usuário (UE), compreendendo:

receber uma primeira mensagem para estabelecer uma conexão segura com uma rede, em que a primeira mensagem compreende informação de política de rede;

gerar uma primeira chave baseada em parte na informação de política de rede; e

utilizar a primeira chave para verificar a informação de política de rede.

2. Método, de acordo com a reivindicação 1, em que o uso da primeira chave para verificar a informação de política de rede compreende determinar se a primeira mensagem é válida com base em parte na primeira chave.

3. Método, de acordo com a reivindicação 2, em que:

a primeira mensagem é a integridade protegida com uma chave de proteção derivada de uma segunda chave; e

determinar se a primeira mensagem é válida compreende a realização de uma verificação de integridade da primeira mensagem com base na primeira chave.

4. Método, de acordo com a reivindicação 2, em que compreende ainda:

estabelecer uma conexão segura com a rede se a determinação é que a primeira mensagem é válida.

5. Método, de acordo com a reivindicação 1, em que a primeira mensagem ainda inclui uma quantidade de tempo em que a informação de política de rede é válida.

6. Método, de acordo com a reivindicação 5, em que a primeira chave é gerada adicionalmente com base em

pelo menos uma dentre uma chave de ancoragem compartilhada entre o UE e a função de ancoragem de segurança (SEAF) na rede ou a quantidade de tempo que a informação de política de rede é válida.

7. Método, de acordo com a reivindicação 6, em que compreende ainda a realização de pelo menos um dentre um procedimento de autenticação ou registro com a SEAF, antes de receber a primeira mensagem, em que a chave de ancoragem é estabelecida com base em pelo menos um dentre procedimento ou registro.

8. Método, de acordo com a reivindicação 1, em que a informação de política de rede compreende uma indicação de se o UE receberá uma ficha de gerenciamento de sessão, a partir de uma função de gerenciamento de sessão (SMF) na rede, ao estabelecer uma sessão de comunicação com a rede.

9. Método, de acordo com a reivindicação 1, em que a primeira mensagem é recebida a partir de uma função de acesso e gerenciamento de mobilidade (AMF) na rede.

10. Método, de acordo com a reivindicação 9, em que a informação de política de rede compreende uma indicação de se o AMF é colocado com uma função de ancoragem de segurança (SEAF) na rede.

11. Método, de acordo com a reivindicação 9, em que a informação de política de rede compreende um nível de segurança da AMF.

12. Método, de acordo com a reivindicação 1, em que:

a primeira mensagem é recebida a partir de uma função de acesso e gerenciamento de mobilidade (AMF) na rede; e

estabelecer a conexão segura compreende o envio de uma segunda mensagem para o estabelecimento da AMF

13. Método, de acordo com a reivindicação 12, em que:

a primeira mensagem é uma mensagem de comando de modo de segurança (SMC); e

a segunda mensagem é uma mensagem completa de SMC.

14. Método, de acordo com a reivindicação 12, em que a conexão segura compreende uma conexão segura de estrato de não acesso (NAS).

15. Método, de acordo com a reivindicação 1, em que compreende adicionalmente enviar informações de política de UE para a rede, em que a informação de política de UE compreende pelo menos uma dentre informação de capacidade de UE ou informação de segurança de UE.

16. Método, de acordo com a reivindicação 15, em que a geração da primeira chave é baseada na informação de política de UE enviada para a rede.

17. Método, de acordo com a reivindicação 15, em que a informação de política de rede é baseada na informação de política de UE.

18. Método para comunicação sem fio por uma função de ancoragem de segurança (SEAF), compreendendo:

gerar uma chave para um nó de rede com base pelo menos em parte na informação de política de rede, em que a

chave é usada para estabelecer uma conexão segura entre um equipamento de usuário (UE) e o nó de rede; e

enviar a chave para o nó de rede.

19. Método, de acordo com a reivindicação 18, em que compreende ainda:

participar em pelo menos um de um procedimento de autenticação ou procedimento de registro com o UE antes de gerar a chave, em que o participante compreende estabelecer uma chave de ancoragem a ser compartilhada entre o UE e a SEAF.

20. Método, de acordo com a reivindicação 19, em que a chave é gerada adicionalmente com base em pelo menos uma chave de ancoragem ou uma quantidade de tempo em que a informação de política de rede é válida.

21. Método, de acordo com a reivindicação 20, em que compreende ainda:

o envio de pelo menos uma das informações de política de rede ou a quantidade de tempo que a informação de política de rede é válida para o nó de rede.

22. Método, de acordo com a reivindicação 18, em que a informação de política de rede compreende uma indicação de se o nó de rede está colocado com a SEAF na rede.

23. Método, de acordo com a reivindicação 18, em que a informação de política de rede compreende um nível de segurança do nó de rede.

24. Método, de acordo com a reivindicação 18, em que a informação de política de rede compreende uma indicação de se uma função de gerenciamento de sessão (SMF) na rede é para gerar um sinal de gerenciamento de sessão

para uma sessão de comunicação entre o UE e a rede, e transmitir o sinal de gerenciamento de sessão para o UE.

25. Método, de acordo com a reivindicação 18, em que compreende ainda:

receber uma mensagem compreendendo informação de política do UE, em que a informação de política de UE compreende pelo menos uma dentre informação de capacidade de UE ou informação de segurança de UE.

26. Método, de acordo com a reivindicação 25, em que a chave é gerada adicionalmente com base na informação de política de UE.

27. Método, de acordo com a reivindicação 25, em que a mensagem compreende uma mensagem de registro ou uma mensagem de solicitação de enlace.

28. Método, de acordo com a reivindicação 25, em que a informação de política de rede é determinada com base na informação de política de UE.

29. Método, de acordo com a reivindicação 18, em que o nó de rede é uma função de acesso e gerenciamento de mobilidade (AMF) na rede.

30. Método para comunicação sem fio por equipamento de usuário (UE), compreendendo:

estabelecer, com base em um procedimento de autenticação com uma rede, uma chave de ancoragem que é compartilhada entre o UE e uma função de ancoragem de segurança (SEAF) na rede;

receber uma primeira mensagem para estabelecer uma conexão segura com a rede, em que a primeira mensagem compreende uma ficha de política de rede para uma sessão de comunicação com a rede, a informação de política de rede,

uma primeira quantidade de tempo que uma primeira chave é válida e uma segunda quantidade de tempo em que a ficha de política de rede é válida; e

determinar se a ficha de política de rede é válida com base em uma chave derivada da chave de ancoragem compartilhada, da informação de política de rede, a primeira quantidade de tempo e a segunda quantidade de tempo, antes de estabelecer a conexão segura com a rede.

31. Método, de acordo com a reivindicação 30, em que a informação de política de rede compreende uma indicação de se o UE receberá uma ficha de gerenciamento de sessão para a sessão de comunicação com a rede a partir de uma função de gerenciamento de sessão (SMF) na rede.

32. Método, de acordo com a reivindicação 30, em que a primeira mensagem é recebida a partir de uma função de acesso e gerenciamento de mobilidade (AMF) na rede.

33. Método, de acordo com a reivindicação 32, em que a informação de política de rede compreende uma indicação de se o AMF é colocado com a SEAF.

34. Método, de acordo com a reivindicação 30, em que a ficha de política de rede compreende informação de proteção de integridade associada com a informação de política de rede.

35. Método, de acordo com a reivindicação 34, em que determinar se a ficha de política de rede é válida compreende verificar a informação de proteção de integridade com base na chave derivada da chave de ancoragem compartilhada.

36. Método, de acordo com a reivindicação 30, em que a primeira mensagem é a integridade protegida com uma

chave de proteção derivada da primeira chave, o método ainda compreendendo:

gerar uma segunda chave baseada em parte em pelo menos uma dentre a chave de ancoragem, a primeira quantidade de tempo ou a segunda quantidade de tempo, se a determinação é que a ficha de política de rede é válida; e

após gerar a segunda chave, a determinação se estabelece a conexão segura com a rede com base em parte da segunda chave.

37. Método, de acordo com a reivindicação 30, em que a conexão segura compreende uma conexão segura de estrato de não acesso (NAS).

38. Método para comunicação sem fio por uma função de ancoragem de segurança (SEAF), compreendendo:

estabelecer, com base em um procedimento de autenticação com equipamento de usuário (UE), uma chave de ancoragem que é compartilhada entre a SEAF e o UE em uma rede;

gerar um sinal de política de rede baseado em parte da chave de âncora, informação de política de rede e uma primeira quantidade de tempo em que a ficha de política de rede é válido;

gerar uma chave para um nó de rede; e

enviar a chave, da informação de política de rede, e da ficha de política de rede para o nó de rede.

39. Método, de acordo com a reivindicação 38, em que a ficha de política de rede compreende informação de proteção de integridade associada com a informação de política de rede.

40. Método, de acordo com a reivindicação 38, em que:

a chave é gerada com base em pelo menos uma chave de ancoragem ou uma segunda quantidade de tempo em que a chave é válida; e

a chave é utilizada para estabelecer uma conexão segura entre o UE e o nó de rede.

41. Método, de acordo com a reivindicação 40, em que compreende ainda o envio da primeira quantidade de tempo e da segunda quantidade de tempo para o nó de rede.

42. Método, de acordo com a reivindicação 38, em que a informação de política de rede compreende uma indicação de se o nó de rede está colocado com a SEAF na rede.

43. Método, de acordo com a reivindicação 38, em que a política de rede compreende uma indicação de se uma função de gerenciamento de sessão (SMF) na rede é gerar um token de gerenciamento de sessão para a sessão de comunicação entre o UE e a rede, e transmitir o sinal de gerenciamento de sessão para o UE.

44. Método, de acordo com a reivindicação 38, em que a informação de política de rede compreende um nível de segurança do nó de rede.

45. Método, de acordo com a reivindicação 38, em que o nó de rede é uma função de acesso e gerenciamento de mobilidade (AMF).

46. Método, de acordo com a reivindicação 38, em que compreende ainda:

receber uma mensagem compreendendo informação de política do UE, em que a informação de política de UE

compreende pelo menos uma dentre informação de capacidade de UE ou informação de segurança de UE.

47. Método, de acordo com a reivindicação 38, em que o nó de rede é uma função de acesso e gerenciamento de mobilidade (AMF) na rede.

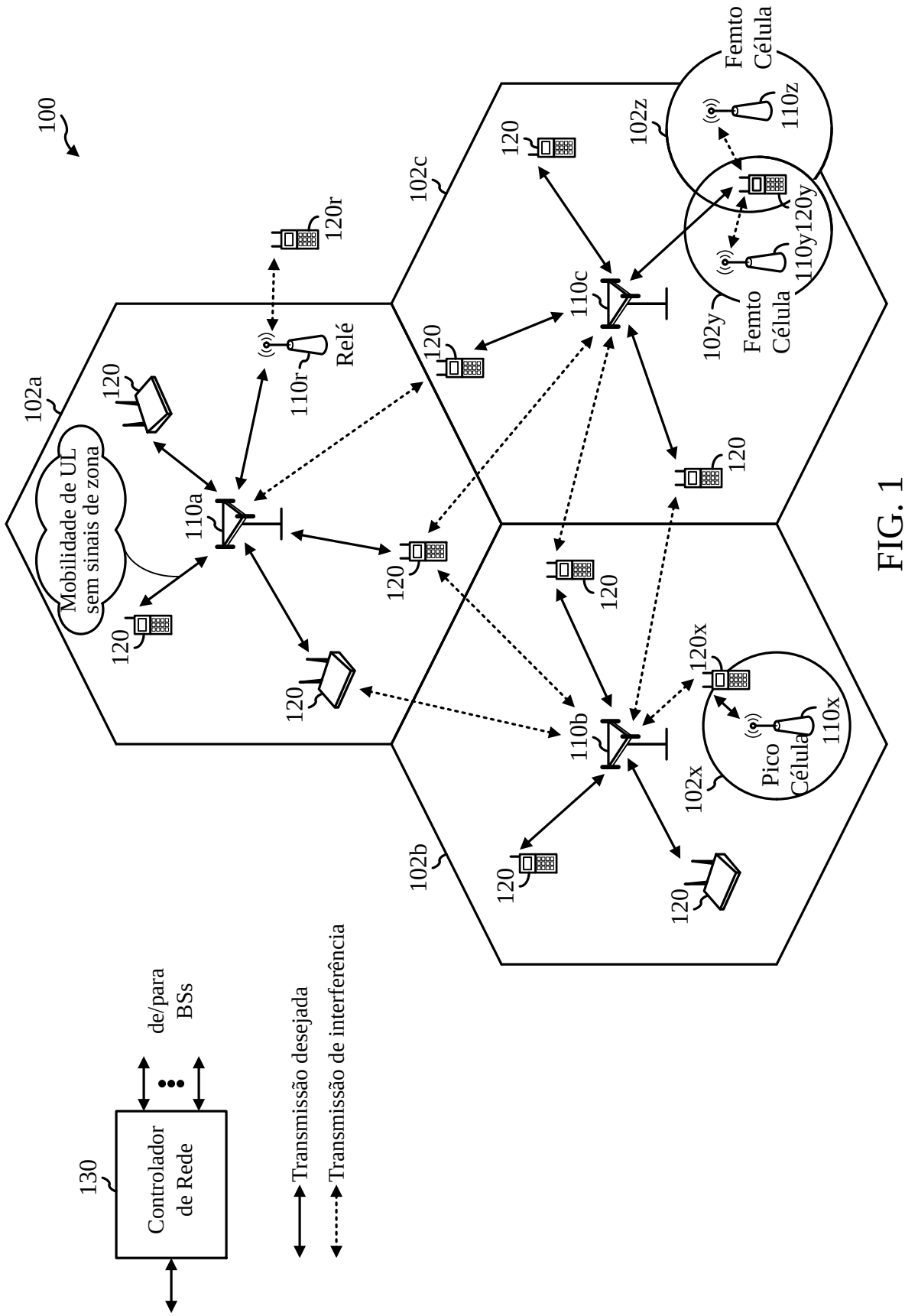
100
102a
102b
102c
102x
102y
102z
110a
110b
110c
110r
110x
110y
110z
120
120r
120x
120y
130
Mobilidade de UL sem sinais de zona
Relé
Pico Célula
Femto Célula
Femto Célula
Controlador de Rede
de/para BSs
Transmissão desejada
Transmissão de interferência

FIG. 1

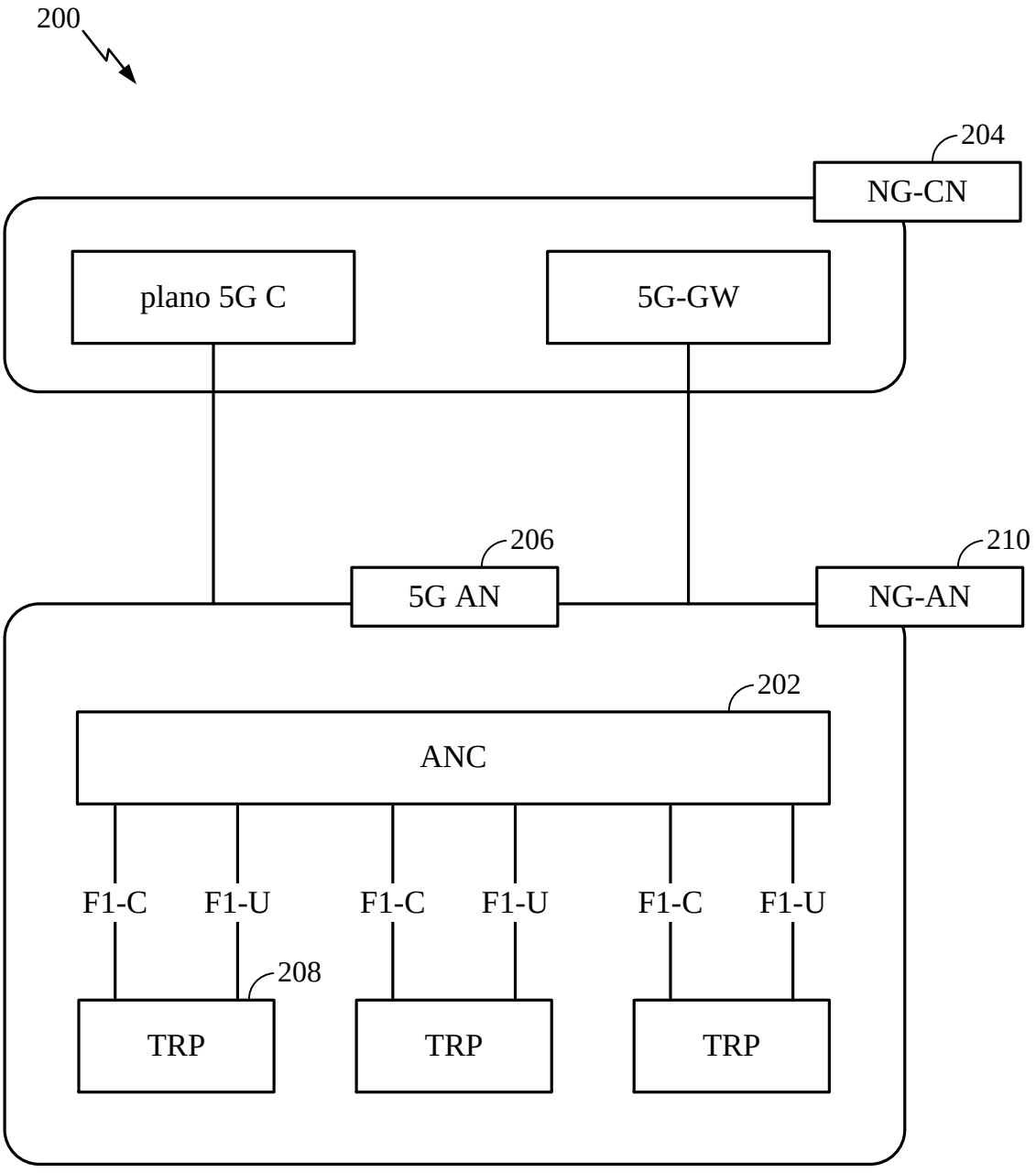
200
204
NG-CN
plano 5G C
5G-GW
206
5G AN
210
NG-AN
202
ANC
F1-C
F1-U
F1-C
F1-U
F1-C
F1-U
208
TRP
TRP
TRP

FIG. 2

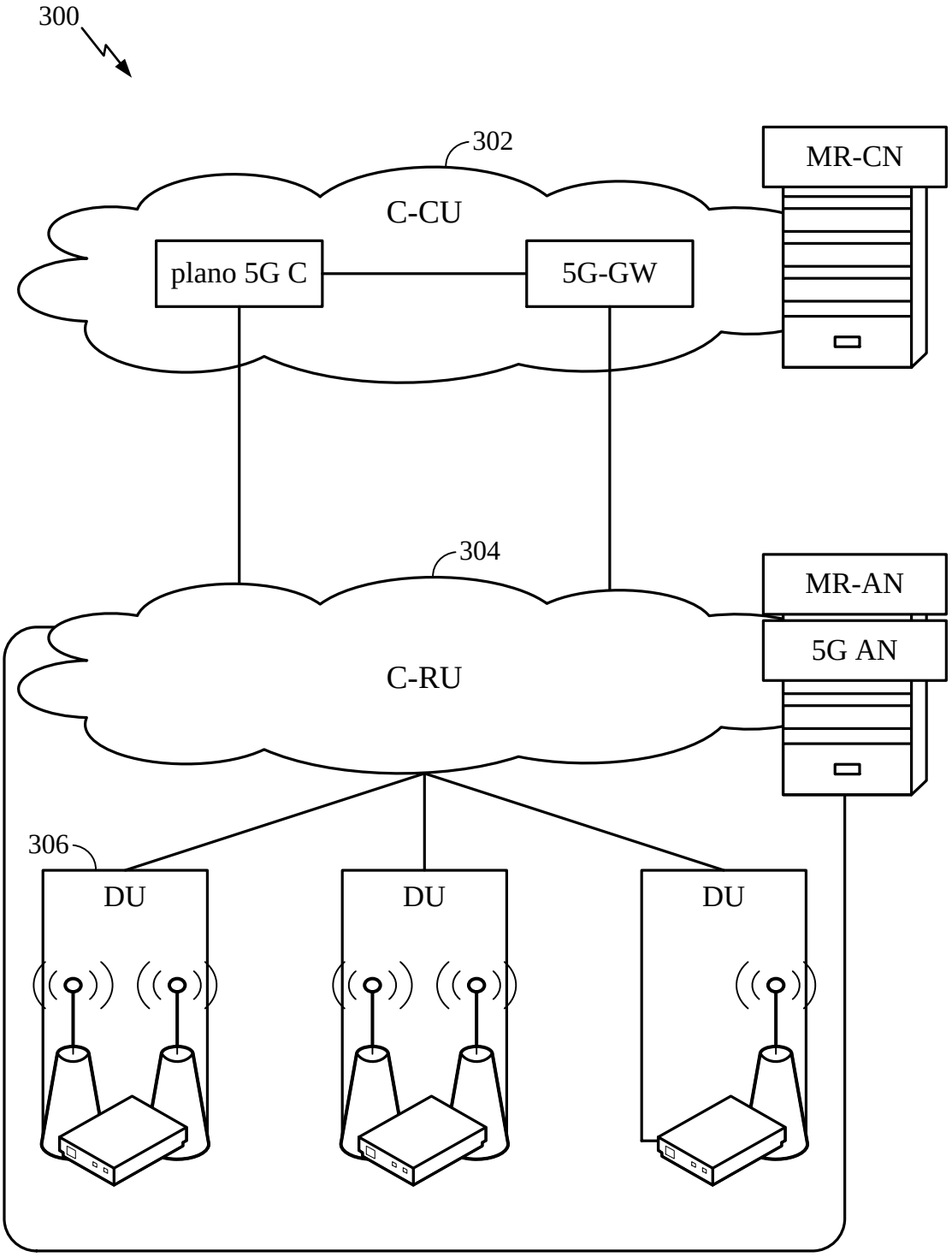

FIG. 3

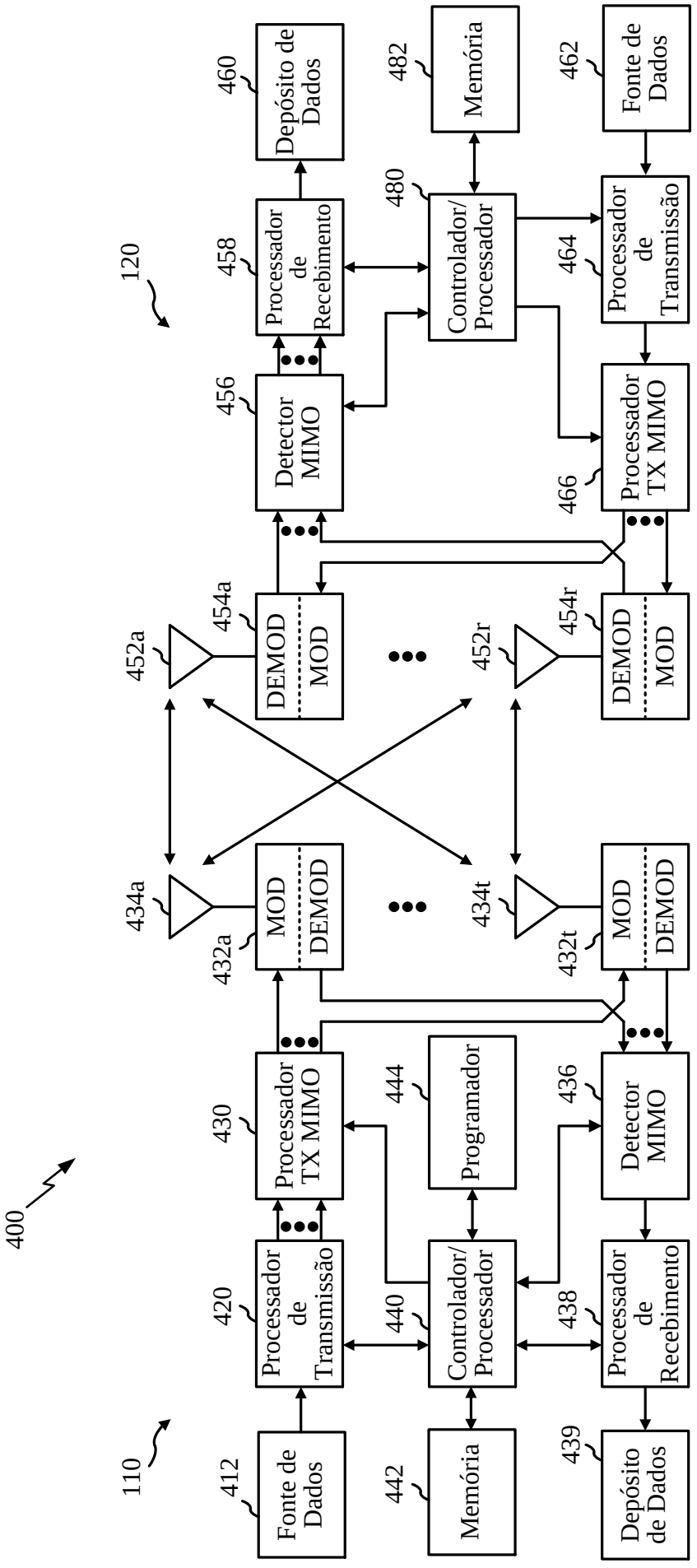
400
110
120
412
Fonte de Dados
420
Processador de Transmissão
430
Processador TX MIMO
432a
MOD
DEMOD
434a
452a
454a
DEMOD
MOD
456
Detector MIMO
458
Processador de Recebimento
460
Depósito de Dados
442
Memória
440
Controlador/ Processador
444
Programador
480
Controlador/ Processador
482
Memória
439
Depósito de Dados
438
Processador de Recebimento
436
Detector MIMO
432t
MOD
DEMOD
434t
452r
454r
DEMOD
MOD
466
Processador TX MIMO
464
Processador de Transmissão
462
Fonte de Dados

FIG. 4

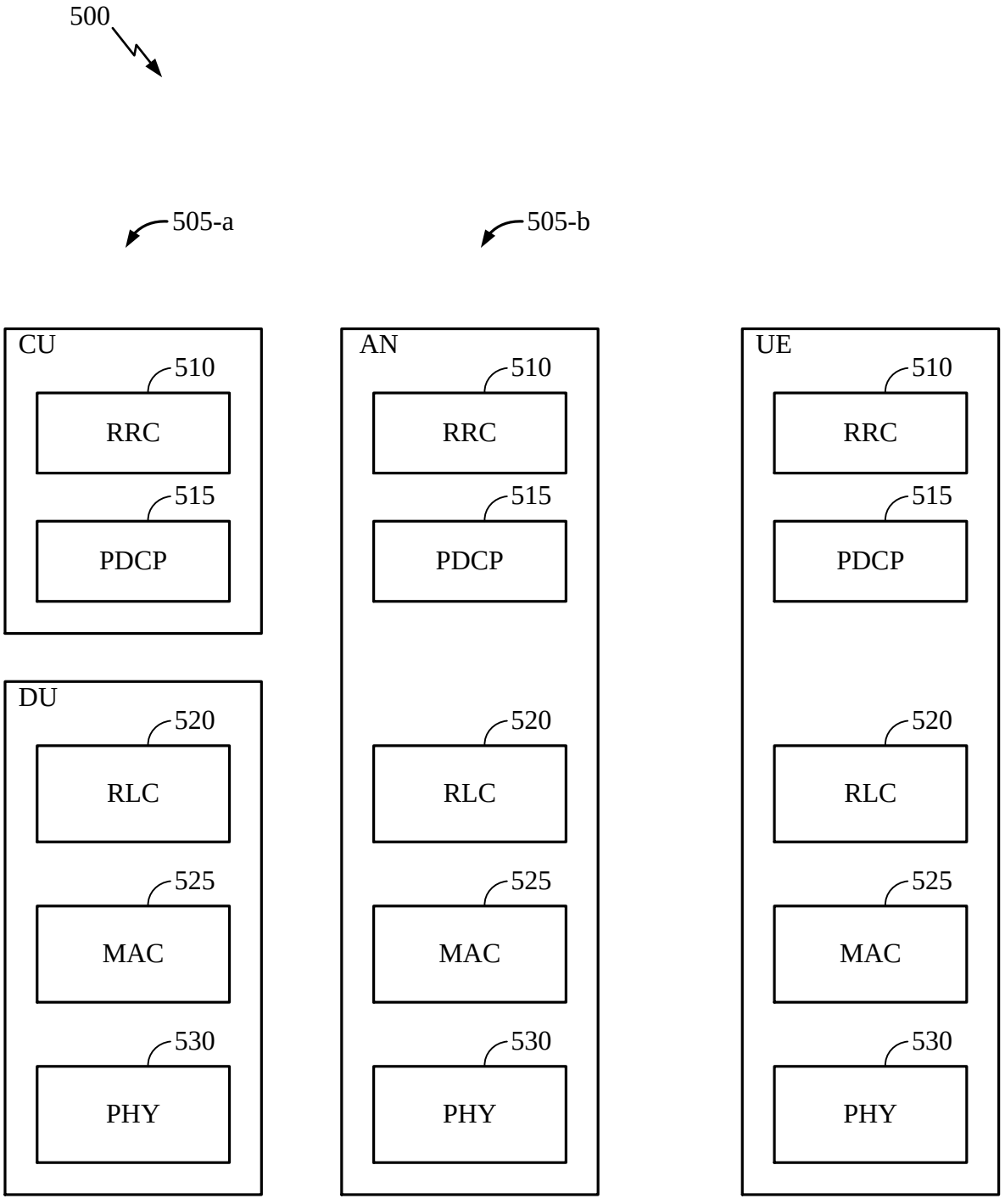
500
505-a
505-b
CU
510
RRC
515
PDCP
DU
520
RLC
525
MAC
530
PHY
AN
510
RRC
515
PDCP
520
RLC
525
MAC
530
PHY
UE
510
RRC
515
PDCP
520
RLC
525
MAC
530
PHY

FIG. 5

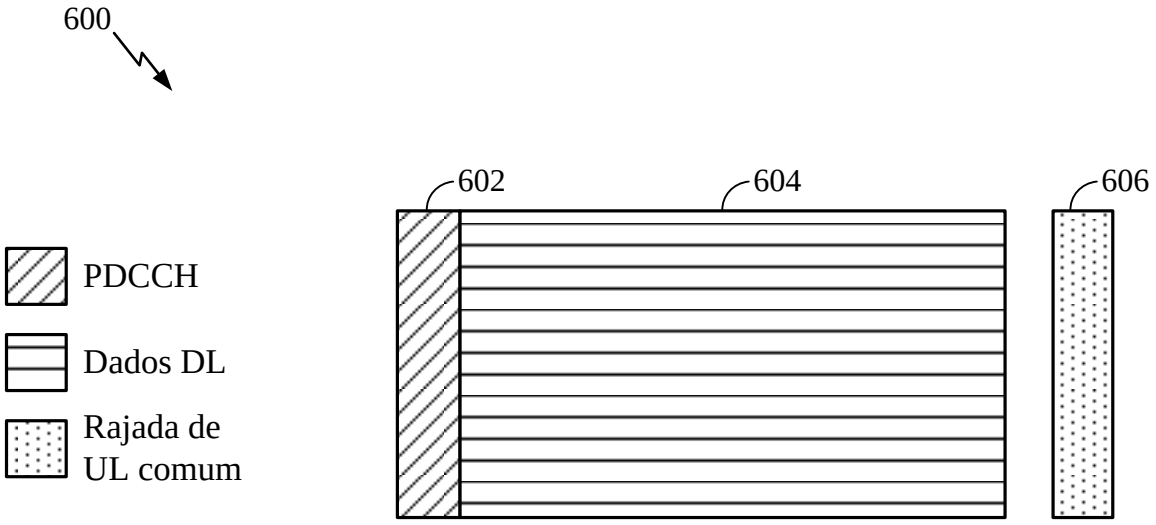
600
602
604
606
PDCCH
Dados DL
Rajada de
UL comum

FIG. 6

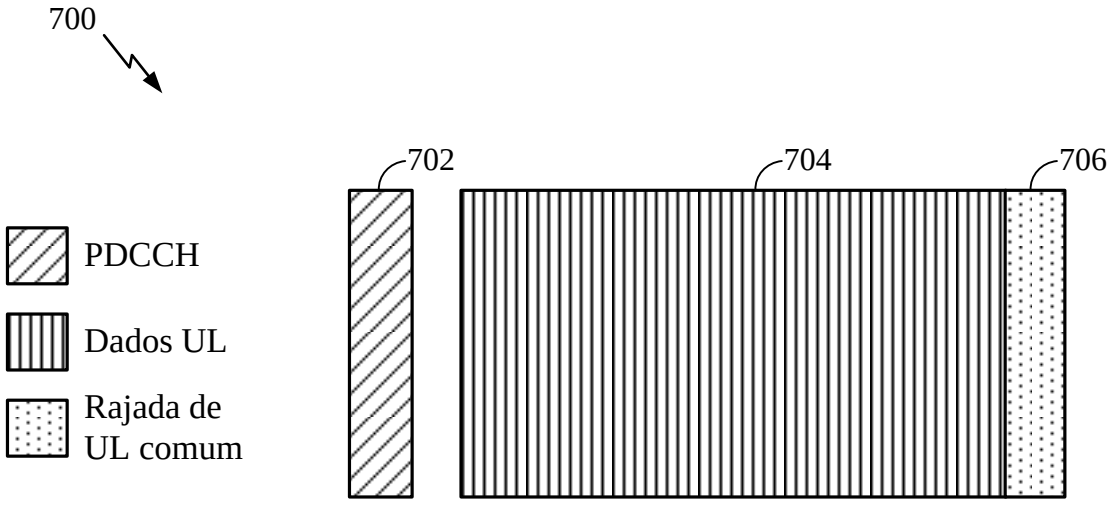
700
702
704
706
PDCCH
Dados UL
Rajada de
UL comum

FIG. 7

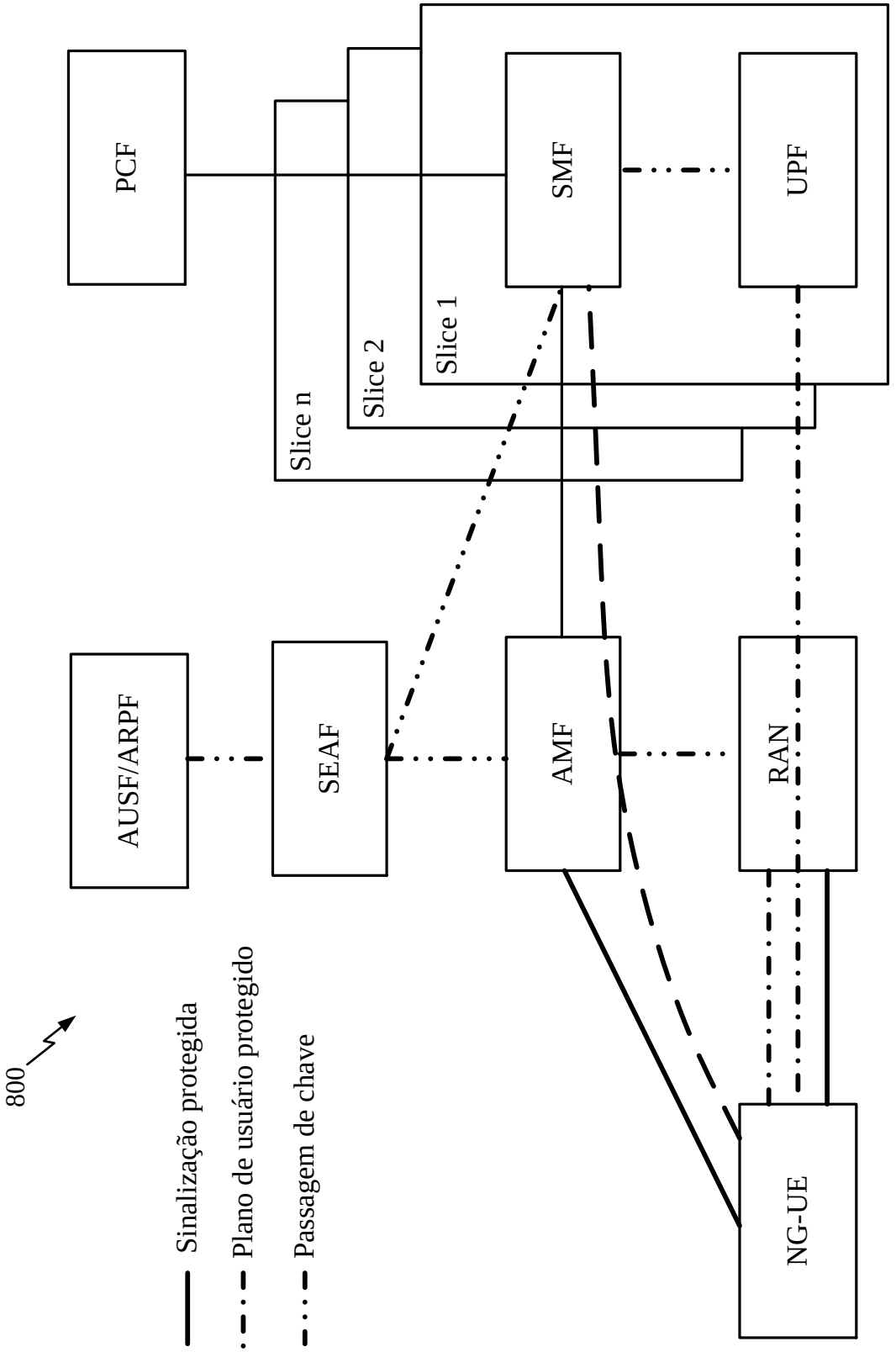
800
Sinalização protegida
Plano de usuário protegido
Passagem de chave
AUSF/ARPF
SEAF
AMF
RAN
NG-UE
PCF
SMF
UPF
Slice 1
Slice 2
Slice n

FIG. 8

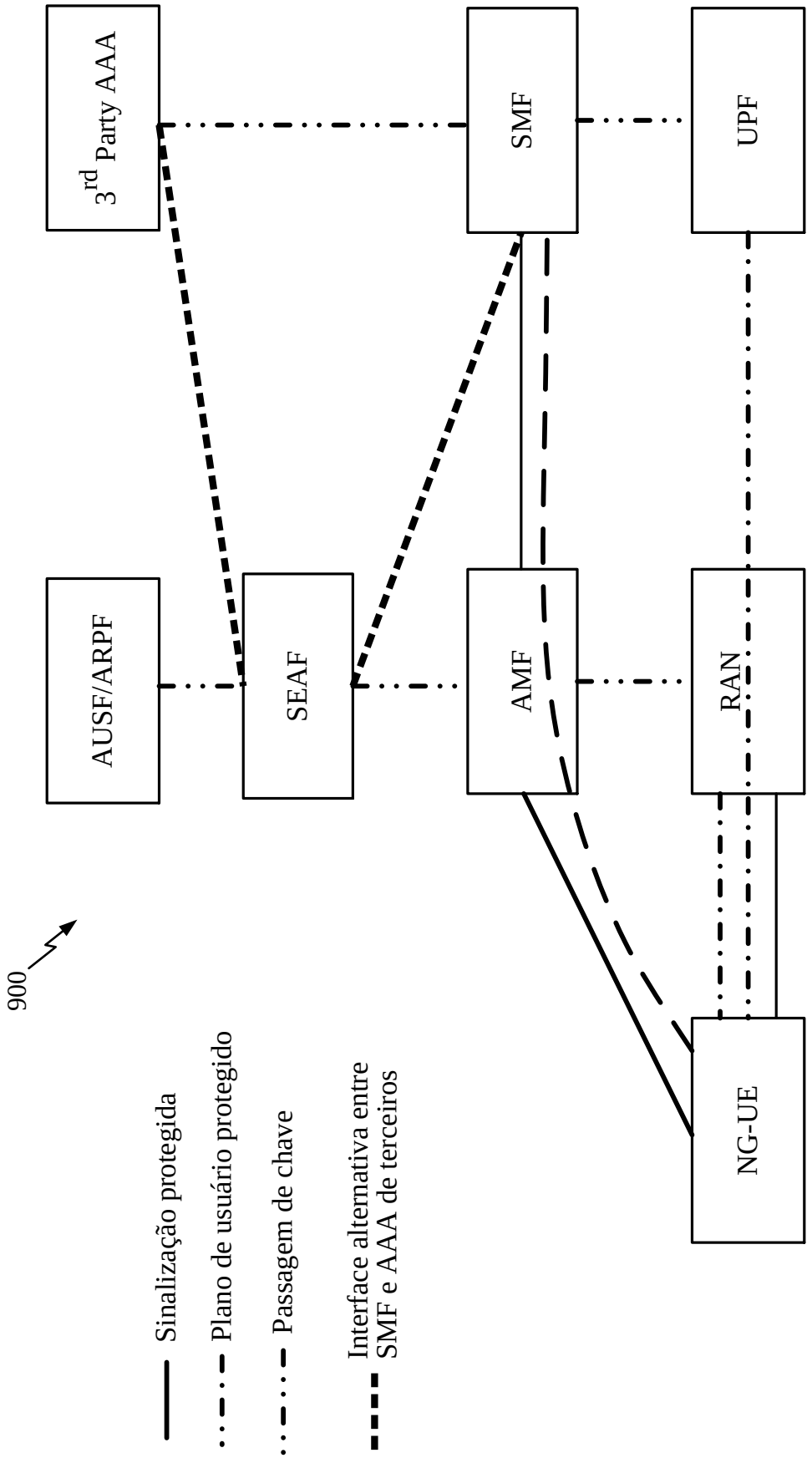
3rd Party AAA
SMF
UPF
AUSF/ARPF
SEAF
AMF
RAN
NG-UE
900
Sinalização protegida
Plano de usuário protegido
Passagem de chave
Interface alternativa entre SMF e AAA de terceiros

FIG. 9

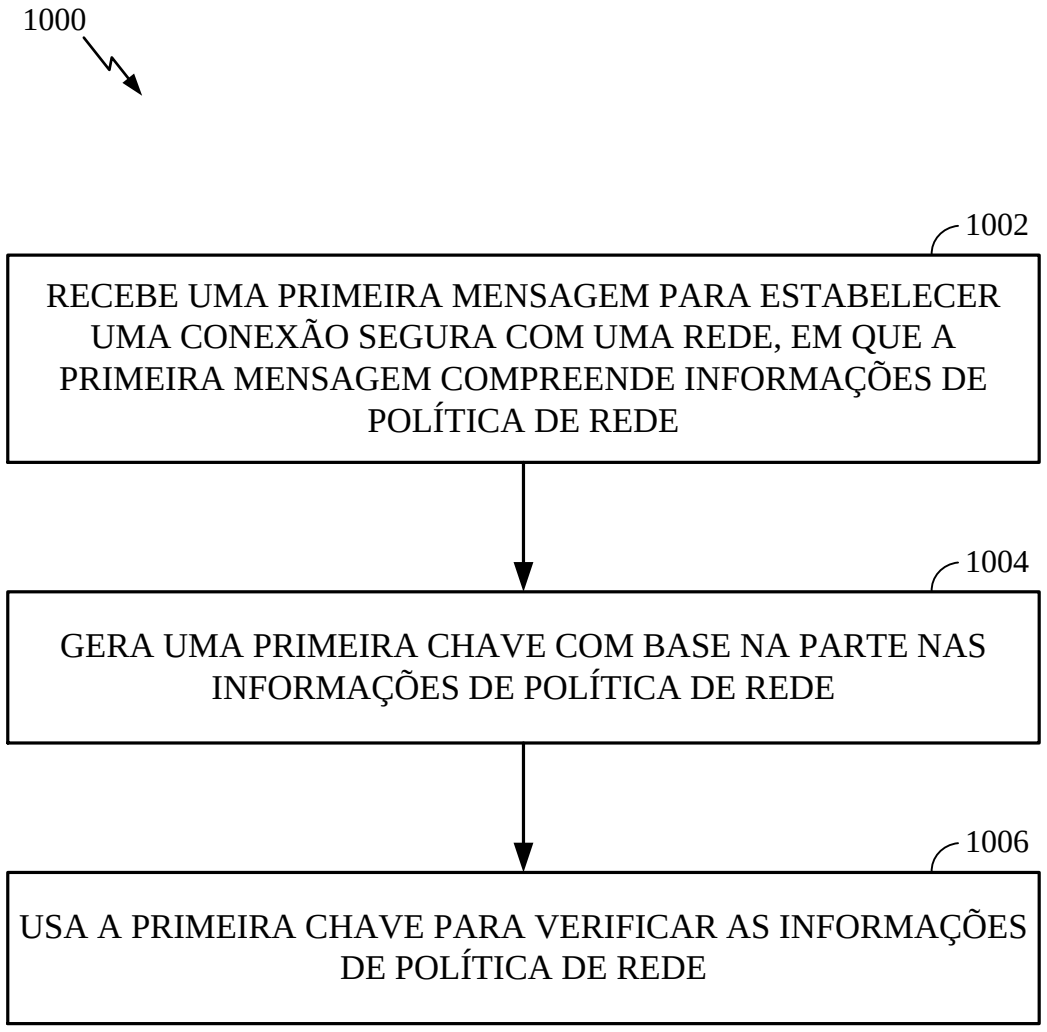
1000
1002
RECEBE UMA PRIMEIRA MENSAGEM PARA ESTABELECER UMA CONEXÃO SEGURA COM UMA REDE, EM QUE A PRIMEIRA MENSAGEM COMPREENDE INFORMAÇÕES DE POLÍTICA DE REDE
1004
GERA UMA PRIMEIRA CHAVE COM BASE NA PARTE NAS INFORMAÇÕES DE POLÍTICA DE REDE
1006
USA A PRIMEIRA CHAVE PARA VERIFICAR AS INFORMAÇÕES DE POLÍTICA DE REDE

FIG. 10

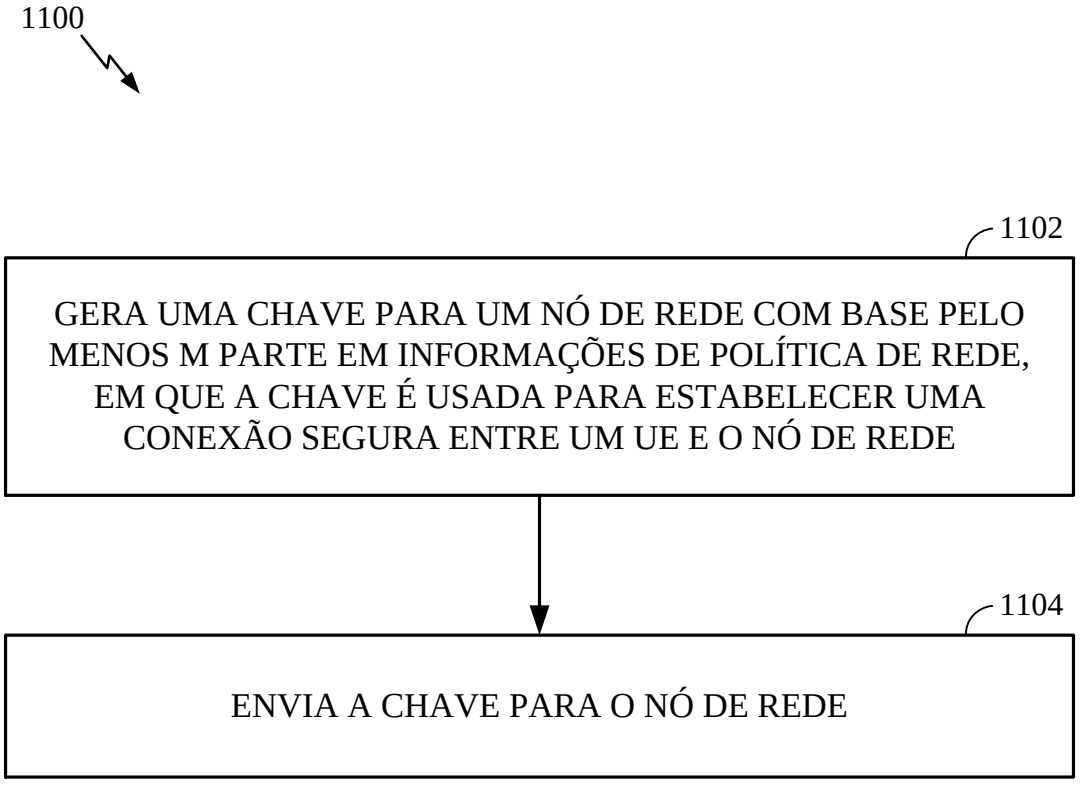
1100
1102
GERA UMA CHAVE PARA UM NÓ DE REDE COM BASE PELO MENOS M PARTE EM INFORMAÇÕES DE POLÍTICA DE REDE, EM QUE A CHAVE É USADA PARA ESTABELECER UMA CONEXÃO SEGURA ENTRE UM UE E O NÓ DE REDE
1104
ENVIA A CHAVE PARA O NÓ DE REDE

FIG. 11

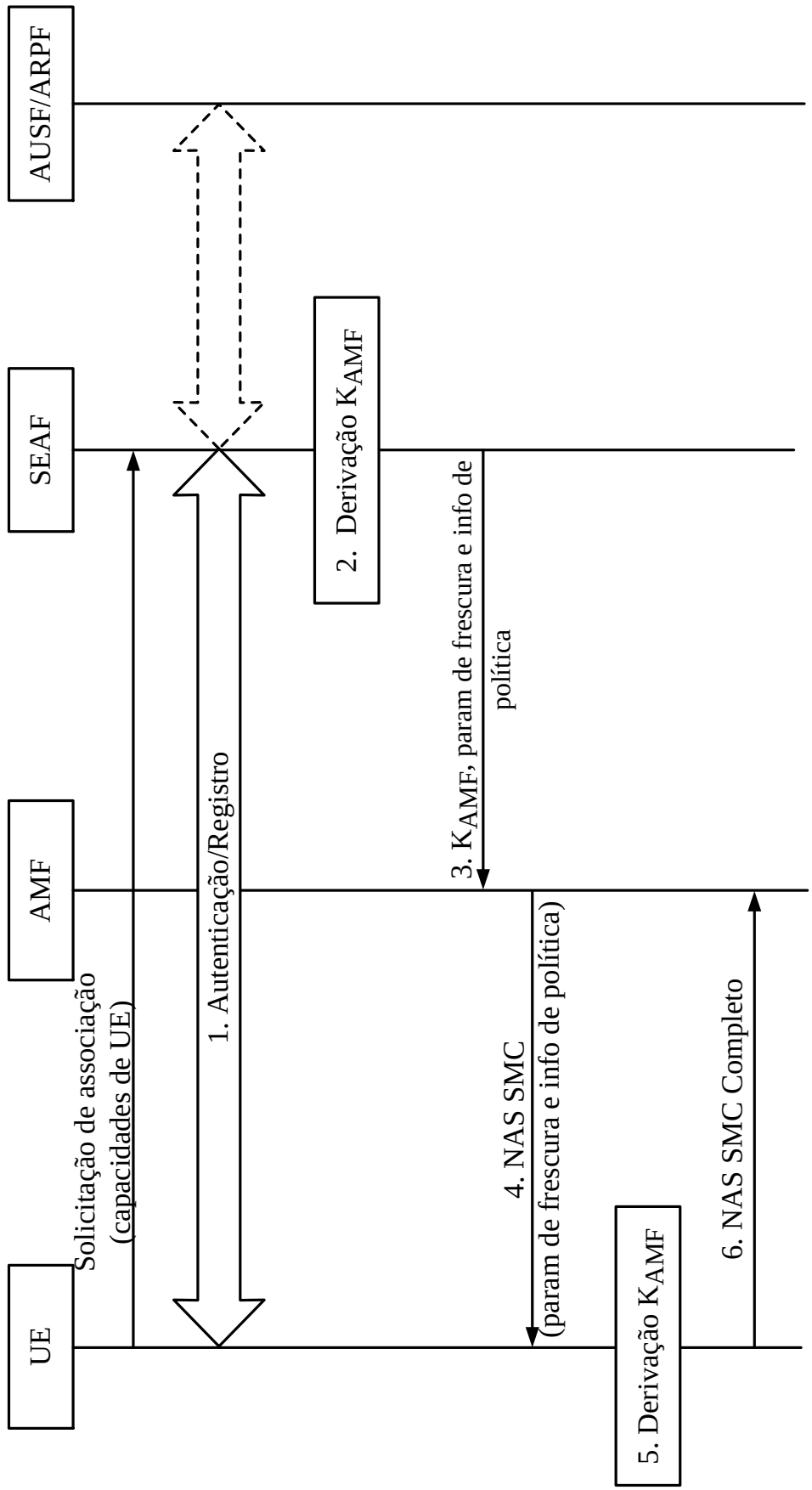
AUSF/ARPF
SEAF
AMF
UE
2. Derivação K_{AMF}
3. K_{AMF}, param de frescura e info de política
1. Autenticação/Registro
Solicitação de associação (capacidades de UE)
4. NAS SMC (param de frescura e info de política)
5. Derivação K_{AMF}
6. NAS SMC Completo

FIG. 12

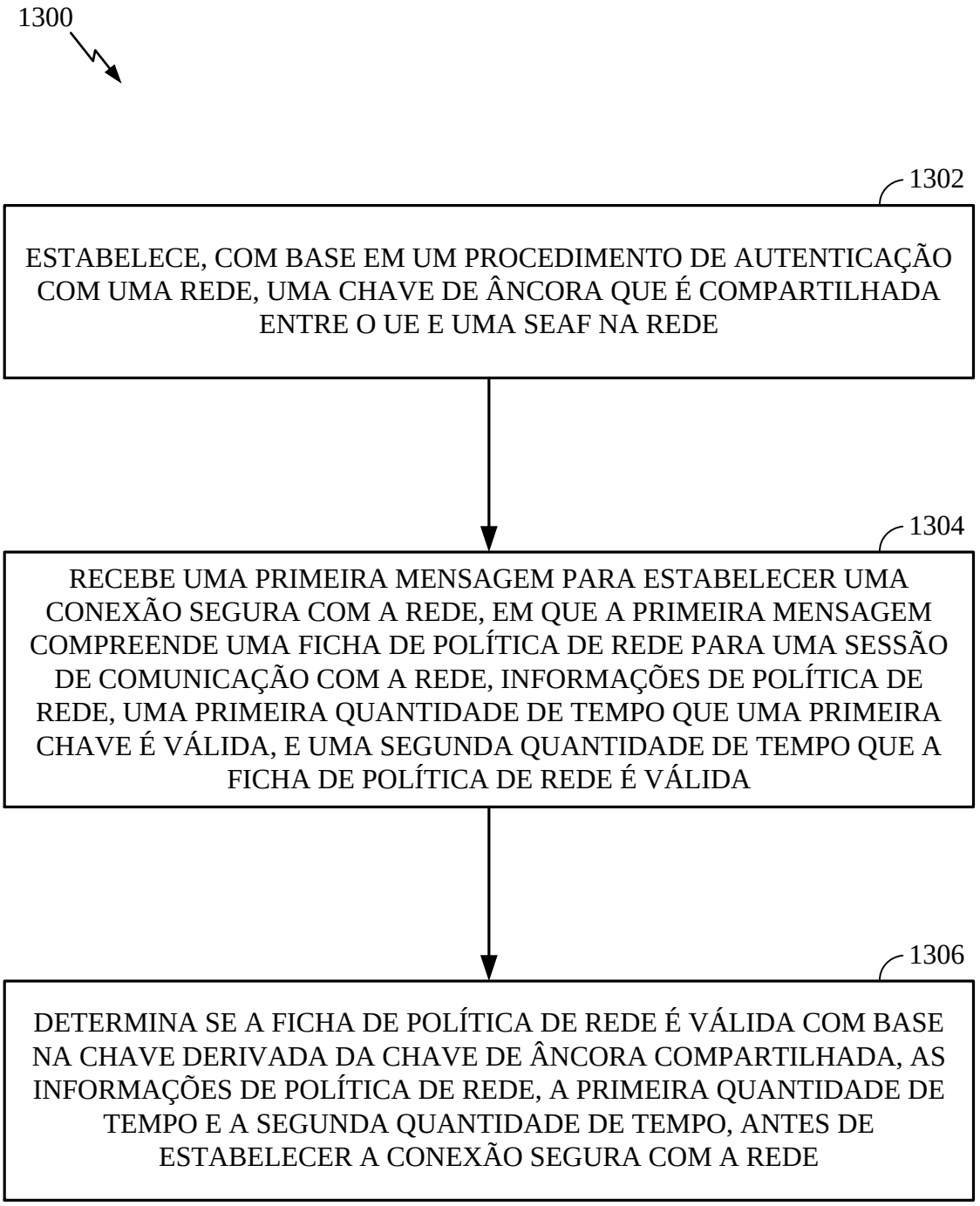
1300
1302
ESTABELECE, COM BASE EM UM PROCEDIMENTO DE AUTENTICAÇÃO COM UMA REDE, UMA CHAVE DE ÂNCORA QUE É COMPARTILHADA ENTRE O UE E UMA SEAF NA REDE
1304
RECEBE UMA PRIMEIRA MENSAGEM PARA ESTABELECER UMA CONEXÃO SEGURA COM A REDE, EM QUE A PRIMEIRA MENSAGEM COMPREENDE UMA FICHA DE POLÍTICA DE REDE PARA UMA SESSÃO DE COMUNICAÇÃO COM A REDE, INFORMAÇÕES DE POLÍTICA DE REDE, UMA PRIMEIRA QUANTIDADE DE TEMPO QUE UMA PRIMEIRA CHAVE É VÁLIDA, E UMA SEGUNDA QUANTIDADE DE TEMPO QUE A FICHA DE POLÍTICA DE REDE É VÁLIDA
1306
DETERMINA SE A FICHA DE POLÍTICA DE REDE É VÁLIDA COM BASE NA CHAVE DERIVADA DA CHAVE DE ÂNCORA COMPARTILHADA, AS INFORMAÇÕES DE POLÍTICA DE REDE, A PRIMEIRA QUANTIDADE DE TEMPO E A SEGUNDA QUANTIDADE DE TEMPO, ANTES DE ESTABELECER A CONEXÃO SEGURA COM A REDE

FIG. 13

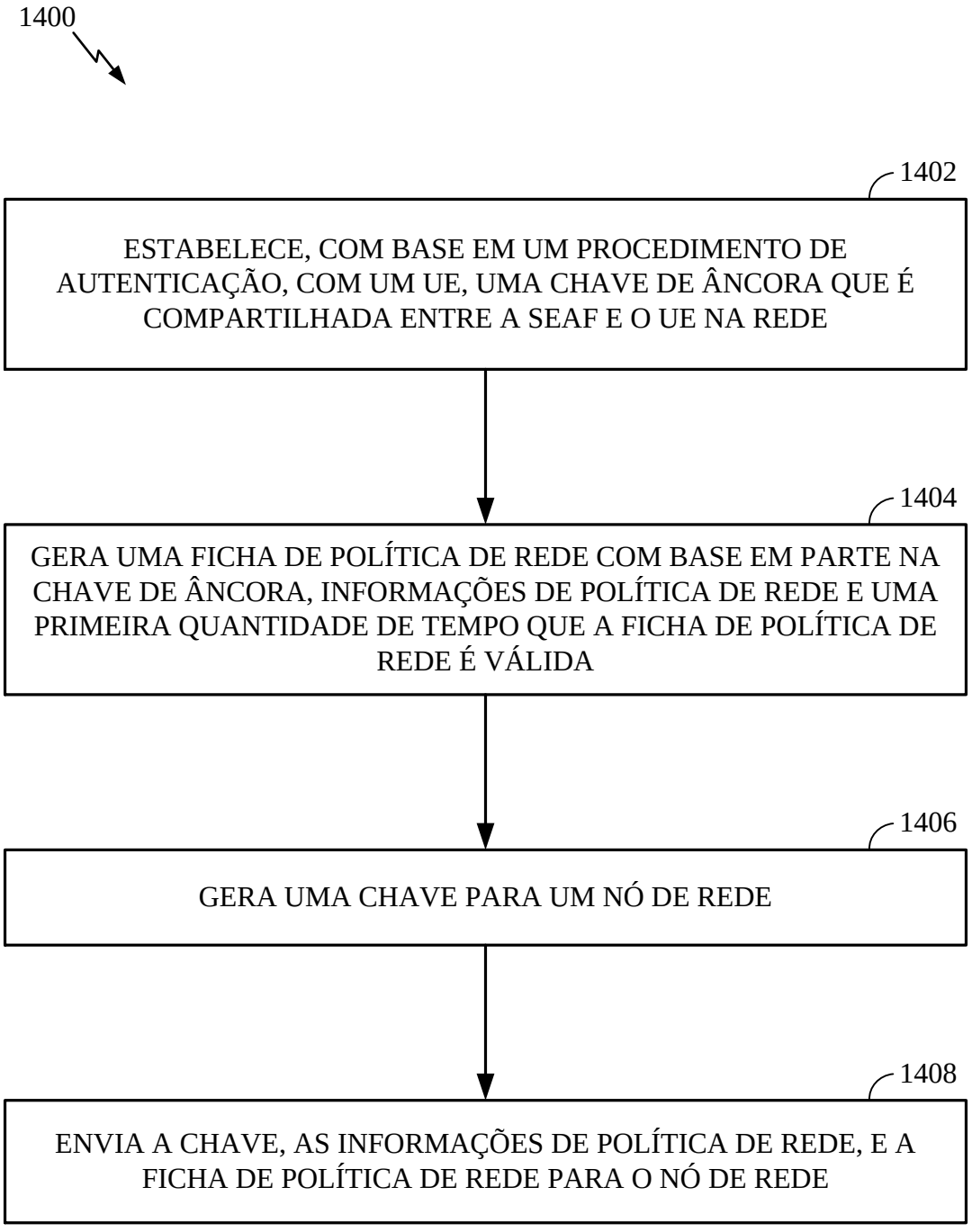
1400
1402
ESTABELECE, COM BASE EM UM PROCEDIMENTO DE AUTENTICAÇÃO, COM UM UE, UMA CHAVE DE ÂNCORA QUE É COMPARTILHADA ENTRE A SEAF E O UE NA REDE
1404
GERA UMA FICHA DE POLÍTICA DE REDE COM BASE EM PARTE NA CHAVE DE ÂNCORA, INFORMAÇÕES DE POLÍTICA DE REDE E UMA PRIMEIRA QUANTIDADE DE TEMPO QUE A FICHA DE POLÍTICA DE REDE É VÁLIDA
1406
GERA UMA CHAVE PARA UM NÓ DE REDE
1408
ENVIA A CHAVE, AS INFORMAÇÕES DE POLÍTICA DE REDE, E A FICHA DE POLÍTICA DE REDE PARA O NÓ DE REDE

FIG. 14

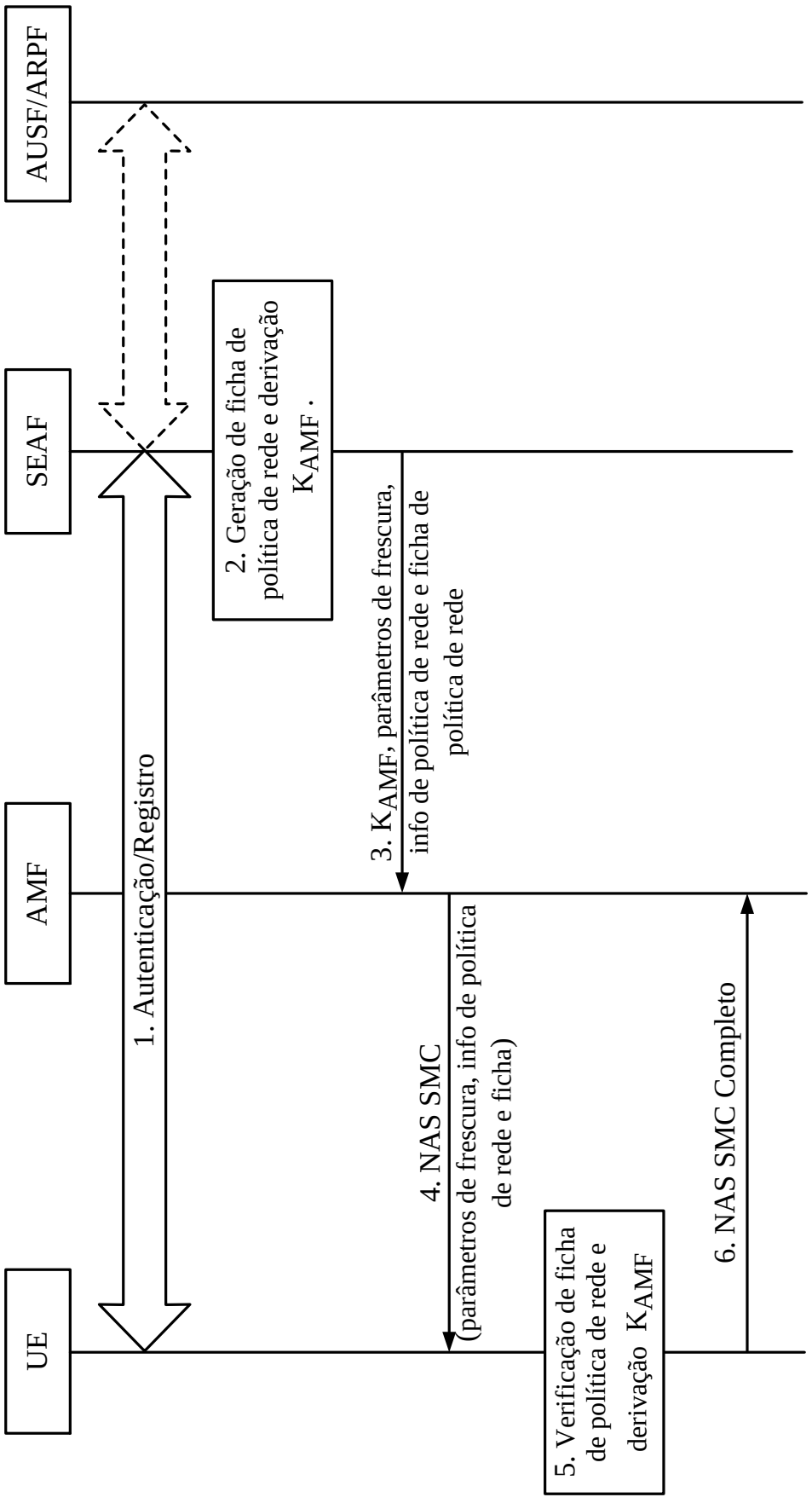
AUSF/ARPF
SEAF
AMF
UE
2. Geração de ficha de política de rede e derivação K_{AMF} .
1. Autenticação/Registro
3. K_{AMF}, parâmetros de frescura, info de política de rede e ficha de política de rede
4. NAS SMC (parâmetros de frescura, info de política de rede e ficha)
5. Verificação de ficha de política de rede e derivação K_{AMF}
6. NAS SMC Completo

FIG. 15

RESUMO

"INCORPORAÇÃO DE POLÍTICAS DE REDE EM GERAÇÃO DE CHAVE"

A presente invenção proporciona técnicas que podem ser aplicadas, por exemplo, para fornecer informações de política de rede de uma maneira segura. Em alguns casos, um UE pode receber uma primeira mensagem para estabelecer uma conexão segura com uma rede, em que a primeira mensagem compreende informação de política de rede, gerar uma primeira chave baseada em parte na informação de política de rede, e usar a primeira chave para verificar a informação de política de rede.