



INPI
INSTITUTO NACIONAL
DA PROPRIEDADE
INDUSTRIAL
Assinado
Digitalmente

REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

CARTA PATENTE Nº PI 0417358-9

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE DE INVENÇÃO, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito: PI 0417358-9

(22) Data do Depósito: 24/11/2004

(43) Data da Publicação do Pedido: 16/06/2005

(51) Classificação Internacional: H04W 48/04.

(52) Classificação CPC: H04W 48/04.

(30) Prioridade Unionista: US 60/527,335 de 05/12/2003.

(54) Título: APARELHO E MÉTODO PARA CONTROLAR TRÁFEGO NÃO-SOLICITADO DESTINADO A UM DISPOSITIVO DE COMUNICAÇÃO SEM FIO

(73) Titular: BLACKBERRY LIMITED. Endereço: 2200 University Avenue E., Waterloo, Ontario, N2K 0A7, CANADÁ (CA)

(72) Inventor: WEN ZHAO; THOMAS LEONARD TREVOR PLESTID; CRAIG DUNK; M. KHALEDUL ISLAM; LUIS PABLO ESTABLE; WILLIAM DANIEL WILLEY.

Prazo de Validade: 10 (dez) anos contados a partir de 11/12/2018, observadas as condições legais

Expedida em: 11/12/2018

Assinado digitalmente por:
Liane Elizabeth Caldeira Lage
Diretora de Patentes, Programas de Computador e Topografias de Circuitos Integrados

APARELHO E MÉTODO PARA CONTROLAR TRÁFEGO NÃO-SOLICITADO**DESTINADO A UM DISPOSITIVO DE COMUNICAÇÃO SEM FIO****FUNDAMENTOS****Campo Técnico**

[001] Este pedido de patente refere-se em geral a técnicas de comunicação sem fio e em particular a um aparelho e método para controlar tráfego não-solicitado destinado a um dispositivo de comunicação sem fio.

Técnica Correlata

[002] É sabido que alguns dispositivos de comunicação sem fio recebem tráfego não-solicitado. Por exemplo, um dispositivo de comunicação sem fio de Acesso Múltiplo por Divisão de Código (CDMA) 2000 operando em configuração simples de Protocolo de Internet (IP) pode receber pacotes de IP não-solicitados. Embora se conheçam outros dispositivos sem fio que recebem tráfego não-solicitado, técnicas tradicionalmente usadas com dispositivos sem fio podem ser inapropriadas, uma vez que existe uma perda significativa de recursos, tanto na rede sem fio como em um dispositivo de comunicação sem fio, sempre que tráfego não-solicitado é enviado pelas interfaces de ar.

[003] Uma técnica que é conhecida, a qual resolve parcialmente este problema, envolve o uso de um esquema privado de endereçamento. Contudo, mesmo que seja usado um esquema privado de endereçamento, esta técnica pode não impedir que tráfego não-solicitado iniciado dentro do espaço do endereço privado alcance o dispositivo de comunicação sem fio. Além disso, esta técnica pode ser inaceitável no caso de um endereço público, como é o caso,

por exemplo, de certas portadoras de CDMA2000 sem fio. Outra técnica que é conhecida, a qual resolve parcialmente este problema, envolve o uso de uma barreira de proteção dentro da rede de comunicação sem fio. Contudo, as regras da barreira de proteção têm que ser configuradas manualmente e podem ser ineficazes se as regras dependerem dos endereços dos dispositivos de comunicação sem fio, os quais podem estar sujeitos a mudanças devido a mobilidade. Por exemplo, no caso de CDMA2000, o endereço IP pode ser atribuído e reutilizado dinamicamente, o que pode tornar as regras de barreira de proteção ineficazes para o dispositivo de comunicação sem fio.

[004] Falando genericamente, existem três categorias de tráfego não-solicitado que necessita de blindagem: (a) Tráfego Não-Solicitado de Sessão Viciada - Quando um dispositivo móvel pára de usar um endereço IP A sem primeiro terminar a comunicação previamente estabelecida com outros servidores, pacotes podem continuar a ser enviados para o mesmo endereço IP A. Exemplos são pacotes de Redes Privadas Virtuais (VPN), compartilhamento de arquivos não-hierarquizados (P2P), spy ware e muitos mais. Tais pacotes são frequentemente enviados continuamente para o dispositivo. Tráfego não-solicitado pode chegar através de uma sessão de IP viciada quando um segundo dispositivo móvel adquire um endereço IP A e começa a receber pacotes de sessão(ões) de IP viciada(s), o tráfego não-solicitado originalmente destinado a alcançar o primeiro dispositivo móvel e (b) Pacotes Não-Solicitados Entre-Assinantes Intra-Subredes - Difusões restritas entre-subredes ou mono-difusão em série de um móvel para outro são pacotes

efetivamente não-solicitados recebidos de outro assinante servido pelo mesmo operador (por exemplo, vermes que exploram protocolos de descoberta de subredes tais como Protocolo de Controle e Gerenciamento de Internet (ICMP) ou Protocolo de Descoberta de Serviços Simples (SSDP) e (c) pacotes maliciosos.

[005] Um dispositivo móvel pode não ser capaz de bloquear uma rede de pacotes enviados, uma vez que deve ser estabelecida uma conexão à rede ou uma chamada e os dados de IP devem ser examinados antes da validade de um pacote ser determinada. Pacotes de sessões de IP Viciadas podem ser considerados pacotes não-solicitados. Existem impactos de dispositivos móveis e de rede que chegam de pacotes não-solicitados. Primeiro, o impacto de rede é tal que tráfego não-solicitado significa uso ineficiente de recursos de rede (enviando dados não-desejados para usuários), o que resulta em atrasos de entrega de dados para outros usuários, assim como a possibilidade de completa indisponibilidade da rede para serviço de voz ou dados para muitos usuários dentro de uma área geográfica. Segundo, o impacto de dispositivo é tal que tráfego não-solicitado significa um dispositivo móvel que pode ser paginado para estabelecer chamadas em uma base de entrada, o que resulta em drenagem muito rápida da bateria, assim como uma contabilização errônea de registros de uso de dados para um dispositivo móvel específico de dados habilitado. Terceiro, a recepção de tráfego não-solicitado indesejado pode ser irritante para o consumidor.

BREVE SUMÁRIO DA INVENÇÃO

[006] Com a finalidade de superar os impactos

negativos realçados acima, o presente pedido de patente fornece um aparelho e método para controlar tráfego não-solicitado, o qual pode ser aplicado a redes de comunicação sem fio tais como CDMA2000, Sistema Universal Móvel de Telecomunicações (UMTS), Serviço Geral de Pacotes de Rádio (GPRS) e similares de modo que tráfego que não é solicitado pelos dispositivos de comunicação sem fio que operam naquelas redes não seja enviado pelo ar desnecessariamente. O presente pedido de patente fornece técnicas para bloquear tráfego não-solicitado com base na identidade de um usuário (por exemplo, com base na Identidade Internacional de Estação Móvel (IMSI), Identificador de Acesso a Rede (NAI), Número de Rede Digital de Serviços de Internet de Estação Móvel (MSISDN), Locador de Recursos Universais (url) de Protocolo de Iniciação de Sessão (SIP)) em oposição a técnicas que são baseadas em uma sessão ou endereço IP, tal como uma barreira de proteção tradicional. De acordo com este pedido de patente, técnicas baseadas na identidade do usuário são aplicadas para bloquear tráfego não-solicitado sempre que um usuário estabelecer uma sessão de dados. Ainda de acordo com este pedido de patente, técnicas baseadas na identidade do usuário perduram ao longo de alterações em endereço IP e/ou sessão.

[007] De acordo com um primeiro aspecto do presente pedido de patente, é propiciado, em uma rede de comunicação sem fio, a rede de comunicação sem fio compreendendo um controlador de tráfego não-solicitado (UTC) acoplado a uma rede de pacotes de dados e a uma pluralidade de dispositivos de comunicação sem fio, um método para controlar tráfego destinado a um primeiro da pluralidade de

dispositivos de comunicação sem fio que compreende as etapas de: armazenar um conjunto de regras de controle de tráfego associadas ao primeiro da pluralidade de dispositivos de comunicação sem fio; determinar uma primeira identidade correspondente a um usuário do primeiro da pluralidade de dispositivos de comunicação sem fio; determinar se um primeiro pacote recebido da rede de pacotes de dados se destina ao primeiro da pluralidade de dispositivos de comunicação sem fio; selecionar as regras de controle de tráfego armazenadas associadas à primeira identidade determinada; aplicar as regras de controle de tráfego selecionadas para determinar se o primeiro pacote é um pacote não-solicitado pelo referido usuário e impedir o primeiro pacote de ser enviado para o primeiro da pluralidade de dispositivos de comunicação sem fio se tiver sido determinado que o primeiro pacote não foi solicitado.

[008] De acordo com um segundo aspecto do presente pedido de patente, é propiciado um meio legível pelo computador que possui armazenadas nele instruções executáveis pelo computador, as quais, quando executadas por um processador em um controlador de tráfego não-solicitado (UTC), fazem com que o referido UTC: armazene um conjunto de regras de controle de tráfego associadas a um dispositivo especificado de uma pluralidade de dispositivos de comunicação sem fio; determine uma identidade correspondente a um usuário do referido dispositivo especificado da pluralidade de dispositivos de comunicação sem fio; determine se um primeiro pacote recebido de uma rede de pacotes de dados se destina ao dispositivo especificado da pluralidade de dispositivos de comunicação

sem fio; selecione o conjunto armazenado de regras de controle de tráfego associado à identidade determinada; aplique as regras de controle de tráfego selecionadas para determinar se o primeiro pacote é um pacote não-solicitado pelo usuário e impeça o primeiro pacote de ser enviado para o dispositivo especificado da pluralidade de dispositivos de comunicação sem fio se tiver sido determinado que o primeiro pacote não foi solicitado, onde o referido UTC está residente em uma rede de comunicação sem fio e está acoplado à referida rede de pacotes de dados e referida pluralidade de dispositivos de comunicação sem fio.

[009] De acordo com um terceiro aspecto do presente pedido de patente, é propiciada uma onda portadora que incorpora um sinal de dados de computador representando sequências de instruções que, quando executadas por um processador, fazem com que o processador: armazene um conjunto de regras de controle de tráfego associadas a um dispositivo especificado de uma pluralidade de dispositivos de comunicação sem fio; determine uma identidade correspondente a um usuário do dispositivo especificado da pluralidade de dispositivos de comunicação sem fio; determine se um primeiro pacote recebido de uma rede de pacotes de dados se destina ao dispositivo especificado da pluralidade de dispositivos de comunicação sem fio; selecione o conjunto armazenado de regras de controle de tráfego associado à identidade determinada; aplique as regras de controle de tráfego selecionadas para determinar se o primeiro pacote é um pacote não-solicitado pelo referido usuário e impeça o primeiro pacote de ser enviado para o dispositivo especificado da pluralidade de

dispositivos de comunicação sem fio se tiver sido determinado que o referido primeiro pacote não foi solicitado, onde o processador é um controlador de tráfego não-solicitado (UTC) e onde o UTC está residente em uma rede de comunicação sem fio e está acoplado à referida rede de pacotes de dados e referida pluralidade de dispositivos de comunicação sem fio.

[0010] De acordo com um quarto aspecto do pedido de patente, é propiciado, em uma rede de comunicação sem fio, um aparelho para controlar tráfego não-solicitado destinado a um dispositivo especificado de uma pluralidade de dispositivos de comunicação sem fio, o aparelho compreendendo: uma primeira interface configurada para receber tráfego proveniente de uma rede de pacotes de dados; uma segunda interface configurada para enviar tráfego para o dispositivo especificado da pluralidade de dispositivos de comunicação sem fio; um primeiro meio de armazenamento que possui armazenadas nele instruções executáveis por computador representando um conjunto de regras de controle de tráfego e um controlador de tráfego não-solicitado (UTC) que se comunica com as primeira e segunda interfaces e primeiro meio de armazenamento, onde o UTC determina uma identidade atribuída ao referido dispositivo especificado da referida pluralidade de dispositivos de comunicação sem fio, e executa as instruções executáveis por computador para bloquear seletivamente o referido tráfego não-solicitado recebido pela primeira interface de ser enviado pela segunda interface para o dispositivo especificado da pluralidade de dispositivos de comunicação sem fio.

[0011] Outros aspectos e características do presente pedido de patente serão evidentes para aqueles versados na técnica depois de revisão da descrição a seguir das modalidades específicas de um aparelho e método para controlar tráfego não-solicitado destinado a um dispositivo de comunicação sem fio.

BREVE DESCRIÇÃO DOS DESENHOS

[0012] A Figura 1 é um diagrama de blocos que ilustra uma rede sem fio que inclui uma modalidade de um controlador de tráfego não-solicitado (UTC), propiciado de acordo com o presente pedido de patente;

a Figura 2 é um diagrama de interação que ilustra a técnica implícita de controle de tráfego não-solicitado, propiciada de acordo com o presente pedido de patente;

a Figura 3 é um diagrama de interação que ilustra a técnica explícita de controle de tráfego não-solicitado, propiciada de acordo com o presente pedido de patente;

a Figura 4 é um diagrama de interação que ilustra a técnica dinâmica de controle de tráfego não-solicitado, propiciada de acordo com o presente pedido de patente;

as Figuras 5-8 são diagramas de interação que ilustram a combinação das técnicas mostradas nas Figuras 2-4;

a Figura 9 é um diagrama de interação que ilustra a técnica de transmissão de controle de tráfego não-solicitado, propiciada de acordo com o presente pedido de patente;

a Figura 10 é um diagrama de blocos que ilustra uma modalidade de um UTC, propiciado de acordo com o presente pedido de patente;

a Figura 11 é um diagrama de interação que ilustra o comportamento do UTC quando um dispositivo de comunicação sem fio cessa a operação, propiciado de acordo com o presente pedido de patente;

a Figura 12 é um diagrama de interação que ilustra o comportamento do UTC quando um dispositivo de comunicação sem fio previamente inativo se torna novamente ativo, propiciado de acordo com o presente pedido de patente;

a Figura 13 é um diagrama de interação que ilustra a interação quando um endereço atribuído a um dispositivo de comunicação sem fio é devolvido e re-atribuído a outro dispositivo de comunicação sem fio, propiciado de acordo com o presente pedido de patente;

a Figura 14 é um diagrama de interação que ilustra a interação quando uma comunicação sem fio realiza uma transferência entre-UTCs, propiciado de acordo com o presente pedido de patente;

a Figura 15 é um diagrama de blocos que ilustra uma rede sem fio que inclui uma modalidade de um UTC adaptado para um ambiente de Serviço Geral de Pacotes de Rádio (GPRS) de Projeto de Parceria de 3ª Geração (3GPP), propiciado de acordo com o presente pedido de patente e

a Figura 16 é um diagrama de blocos que ilustra uma modalidade exemplificativa de um controlador de tráfego não-solicitado, propiciado de acordo com o presente pedido de patente.

[0013] Os mesmos numerais de referência são usados em diferentes figuras para representar elementos similares.

DESCRIÇÃO DETALHADA

[0014] Com referência agora aos desenhos, a Figura 1

é um diagrama de blocos que ilustra uma rede sem fio que inclui uma modalidade de um controlador de tráfego não-solicitado (UTC), propiciado de acordo com o presente pedido de patente. O diagrama de blocos mostra uma rede sem fio 100 que acopla uma rede de pacotes de dados 120 com dispositivos de comunicação sem fio 130A ... 130N, e que acopla dispositivos de comunicação sem fio entre si, permitindo deste modo que flua tráfego para e da rede de pacotes de dados 120 de e para dispositivos de comunicação sem fio 130A ... 130N, e permitindo que flua tráfego para e do dispositivo de comunicação sem fio 130A para e de outro dispositivo de comunicação sem fio 130N.

[0015] A rede sem fio 100 inclui um controlador de tráfego não-solicitado 110, propiciado de acordo com o presente pedido de patente, cuja finalidade é influenciar o modo pelo qual se realiza o acoplamento dos dispositivos de comunicação sem fio 130A ... 130N entre si e à rede de pacotes de dados 120, de modo a limitar tráfego não-solicitado destinado aos dispositivos de comunicação sem fio 130A ... 130N. Especificamente, o controlador de tráfego não-solicitado 110 inclui um conjunto de regras tipo barreira de proteção 140A ... 140N, cada uma das quais corresponde a um dispositivo específico de comunicação sem fio 130A ... 130N, de modo que o seu efeito combinado seja que as interfaces de ar se comportem como se tivessem sido individual e substancialmente barradas por proteções 150A ... 150N.

[0016] São consideradas diversas modalidades de um controlador de tráfego não-solicitado, cada uma adaptada para os requisitos específicos de uma rede específica sem

fio. Por exemplo, em uma modalidade adaptada para uma rede sem fio CDMA, o controlador de tráfego não-solicitado está de preferência localizado em pelo menos um Nó de Atendimento de Pacotes de Dados (PDSN) da rede sem fio. Alternativamente, em uma modalidade adaptada para uma rede sem fio GPRS, o controlador de tráfego não-solicitado está de preferência localizado em pelo menos um Nó de Suporte de Atendimento de GPRS (SGSN), ainda mais preferivelmente em pelo menos um Nó de Suporte de Gateway de GPRS (GGSN). A escolha de onde localizar o controlador de tráfego não-solicitado é orientada pelo princípio de que deve ter acesso a todo o tráfego destinado ao dispositivo sem fio de modo a controlar o fluxo de tráfego não-solicitado. Neste sentido, um controlador de tráfego não-solicitado pode estar adaptado para operar com qualquer rede sem fio dada como resultado do presente pedido de patente.

[0017] O controlador de tráfego não-solicitado 110 da Figura 1 pode estar configurado para co-operação com GPRS. GPRS é especificado, por exemplo, por 3GPP. Um iniciador de *push* está localizado dentro da rede de pacotes de dados 120. Os dispositivos de comunicação sem fio de 130A a 130N são equipamentos de usuário e cada um inclui pelo menos um agente de usuário e um recipiente de *push*. A rede sem fio 100 é uma rede de serviço móvel terrestre público e inclui uma função de *push*, assim como perfis de subscrição de *push* correspondentes a cada um dos usuários dos equipamentos de usuário. O controlador de tráfego não-solicitado 110 nesta modalidade opera como uma barreira de proteção baseada no usuário pelo controle do tráfego não-solicitado com base nos perfis de subscrição de *push* dos

usuários do equipamento de usuário. Dependendo da configuração, considera-se que o controlador de tráfego não-solicitado 110 controla o tráfego com base em IMSI, NAI, MSISDN ou SIP url, por exemplo.

[0018] O restante desta descrição e desenhos utilizará pacotes de IP e endereços IP para fins apenas exemplificativos, uma vez que as técnicas mostradas aqui podem ser aplicadas a muitas formas alternativas de comunicação. Por exemplo, a técnica pode ser aplicada a voz, correio eletrônico, protocolo de transferência de hipertexto (http), protocolo de transferência de arquivos (ftp), serviço de mensagens de multimídia (MMS) e serviço de mensagens curtas (SMS).

[0019] As Figuras 2 a 8 definem diversas técnicas para controle de tráfego não-solicitado. Como aqueles versados na técnica entenderão, o tráfego pode ser controlado por regras implícitas, explícitas ou dinâmicas ou uma combinação de tais regras. Em relação à estrutura física de um controlador de tráfego não-solicitado, a Figura 16, que será discutida mais tarde, descreve uma modalidade exemplificativa. Mais notavelmente, o controlador de tráfego não-solicitado armazena as regras (vide elemento 1670 na Figura 16) que são usadas para bloquear seletivamente pacotes.

[0020] Voltando agora para a Figura 2, é representado um diagrama de interação que ilustra a técnica de controle implícito de tráfego não-solicitado, propiciado de acordo com o presente pedido de patente. O diagrama de interação mostra as interações entre um dispositivo de comunicação sem fio 230A, um controlador implícito de

tráfego não-solicitado 210 e uma rede de pacote de dados 220.

[0021] Antes de descrever ainda mais este primeiro diagrama de interação, é importante descrever alguns aspectos comuns de notação que são usados neste e em outros diagramas de interação do presente pedido de patente. O tempo flui geralmente para baixo neste diagrama de interação, assim como nos outros diagramas de interação do presente pedido de patente. Além disso, o til (~), como usado nos desenhos, nesta descrição, significa a abreviação para "substancialmente igual". Portanto, IP~A significa todos os endereços que são substancialmente iguais a IP A para algumas finalidades específicas. Por exemplo, a notação IP~A quando usada para qualificar endereços IP que podem alcançar um dispositivo sem fio que possui IP A, isto inclui o próprio IP A, assim como endereços de radiodifusão, endereços de qualquer difusão e endereços de multi-difusão que alcançariam normalmente IP A na ausência das técnicas do presente pedido de patente. A mesma notação de til (~) é usada para representar pacotes. Por exemplo, se PKT1 tem endereço de destino IP A, endereço de fonte IP B e dados, então ~PKT1 significa pacotes que são substancialmente iguais a PKT1 para algumas finalidades específicas, por exemplo, onde pode ser encontrada uma similaridade substancial entre a fonte, destino e/ou dados entre os dois pacotes. Por exemplo, em pacotes TCP/IP e UDP/IP, dados em um pacote podem ser considerados substancialmente iguais a dados em outro pacote se os números de portas ou números de soquetes forem substancialmente similares. Como outro exemplo, para

pacotes ICMP/IP, os dados podem incluir números de protocolo.

[0022] Operacionalmente, ao dispositivo de comunicação sem fio 230A é correntemente atribuído o endereço IP A. O UTC implícito 210 rastreia que tipo de tráfego é considerado solicitado para IP A. Isto é mostrado em dois instantes nos blocos de IP A Solicitado. Inicialmente, o IP A Solicitado 225 não contém quaisquer informações em relação aos pacotes ilustrados na Figura 2. Consequentemente, quando PKT1 é destinado a um endereço como IP A, isto é, IP~A, o UTC implícito 210 bloqueia vantajosamente 235 PKT1 237. Ainda mais vantajosamente, o UTC implícito 210 reconhece que o dispositivo de comunicação sem fio 230A envia PKT2 (~PKT1) 240 e, consequentemente, atualiza a lista de IP A Solicitado 245 para incluir ~PKT1 250, de modo que quando PKT3 (~PKT1) 260 é destinado ao dispositivo de comunicação sem fio 230A, não é bloqueado.

[0023] A Figura 3 é um diagrama de interação que ilustra a técnica de controle explícito de tráfego não-solicitado, propiciado de acordo com o presente pedido de patente. Voltando agora para a Figura 3, similarmente à Figura 2, ao dispositivo de comunicação sem fio 330A é correntemente atribuído o endereço IP A. O UTC explícito 310 rastreia que tipo de tráfego é considerado não-solicitado para o dispositivo de comunicação sem fio 330A. Isto é mostrado no instante inicial antes do bloco explícito 340, na lista de bloco não-solicitado de IP A 325 e em um instante subsequente para o bloco explícito 340, na lista de bloco de IP A Não-Solicitado 345. Inicialmente, a

lista de IP A Não-Solicitado 325 não contém quaisquer informações em relação aos pacotes ilustrados na Figura 3 e, em especial, PKT3 337. Consequentemente, quando PKT3 337 é destinado a um endereço como IP A, isto é, ~IP A, o UTC Explícito 310 permite vantajosamente que PKT3 337 vá avante. Depois do dispositivo de comunicação sem fio 230A receber PKT3 337, envia uma mensagem de Bloco Explícito ~PKT3 340 para o UTC Explícito 310. Consequentemente, o UTC explícito 310 atualiza a lista de IP A Não-Solicitado 345 de modo a incluir ~PKT3 350, de modo que quando um pacote como PKT3, isto é, ~PKT3 360, é destinado ao dispositivo de comunicação sem fio 330A, é bloqueado 335.

[0024] Em uma modalidade alternativa, o dispositivo de comunicação sem fio 330A pode também enviar uma mensagem ~PKT3 não-bloqueada explícita para o UTC Explícito 310 em um instante posterior de modo que o UTC Explícito 310 atualize o IP A Não-Solicitado 345 a excluir ~PKT3 350. Em qualquer instante subsequente ao ~PKT3 não-bloqueado, se um pacote como PKT3, isto é, ~PKT3, é destinado ao dispositivo de comunicação sem fio 330A, deverá ser deixado passar.

[0025] Em ainda outra modalidade, o aspecto explícito do UTC da Figura 3 pode ser combinado com o aspecto implícito do UTC da Figura 2. Se o dispositivo de comunicação sem fio 330A envia um pacote ~PKT3 para a Rede de Pacote de Dados 320, mesmo que o UTC explícito 310 aceite bloqueios e desbloqueios explícitos, pode interpretar ~PKT3 como um desbloqueio implícito e consequentemente atualizar o IP A Não-Solicitado 345 para remover ~PKT3 350, de modo que quando um outro pacote ~PKT3 seja destinado ao dispositivo de comunicação sem fio 330A,

não esteja mais bloqueado.

[0026] A Figura 4 é um diagrama de interação que ilustra a técnica de controle dinâmico de tráfego não-solicitado, proporcionado de acordo com o presente pedido de patente. Voltando agora para a Figura 4, de modo similar às Figuras 2-3, ao dispositivo de comunicação sem fio 430A é correntemente atribuído o endereço IP A. O UTC dinâmico 410 rastreia que tipo de tráfego é considerado desconhecido para IP A. Isto é mostrado em dois instantes nos blocos não-solicitados de IP A. Inicialmente, a lista de IP A Desconhecido 425 não contém quaisquer informações relacionadas aos pacotes, como ilustrados na Figura 4 e, particularmente, ao PKT4 437. Consequentemente, quando PKT4 437 é destinado a um endereço como IP A, a saber, IP~A, o UTC Dinâmico 410 permite vantajosamente que PKT4 437 vá avante uma vez depois do UTC Dinâmico 410 atualizar o IP A Desconhecido 445 para incluir ~PKT4, de maneira que quando um pacote subsequente do tipo PKT4, isto é, ~PKT 460 é destinado ao dispositivo de comunicação sem fio 430A, o mesmo é bloqueado 435. Em uma modalidade alternativa, considera-se que a operação de bloqueio permite que um número predeterminado de pacotes coincida com uma listagem no IP A desconhecido antes do bloqueio de pacotes subsequentes.

[0027] Em outras modalidades alternativas, o dispositivo de comunicação sem fio 430A pode também enviar um desbloqueio tanto implícito como explícito para o UTC Dinâmico 410 em um instante posterior, de maneira que o UTC Dinâmico 410 atualize a lista de IP A Desconhecido 445 para permitir pacotes como PKT3, isto é, ~PKT4 450. Assim,

quando um pacote como PKT, isto é, ~PKT4, é destinado ao dispositivo de comunicação sem fio 230A, o mesmo não é bloqueado.

[0028] A Figura 5 mostra uma modalidade de um UTC 510 que combina o aspecto implícito do UTC 210 da Figura 2 com o aspecto dinâmico do UTC 410 da Figura 4.

[0029] A Figura 6 mostra uma modalidade de um UTC 610 que combina o aspecto explícito do UTC 310 da Figura 3 com o aspecto dinâmico do UTC 410 da Figura 4.

[0030] As Figuras 7-8 mostram uma modalidade de um UTC 710 que combina o aspecto implícito do UTC 210 da Figura 2 com o aspecto explícito do UTC 310 da Figura 3.

[0031] As listas utilizadas para categorizar as diversas naturezas de pacotes em relação a um dispositivo sem fio específico foram até agora mantidas separadas com a finalidade de permitir que o leitor entendesse melhor a sua operação. Contudo, as Figuras 2-8 demonstram que a introdução das listas apropriadas no UTC e o seguimento dos procedimentos adequados para atualizar aquelas listas podem combinar diversos aspectos destas UTCs, tais como os aspectos implícitos, explícitos e dinâmicos. Portanto, durante o restante deste documento e nas reivindicações apensas, o termo regras será usado como genérico para as diversas listas utilizadas por um UTC para rastrear um dispositivo sem fio, tais como as listas solicitadas, não-solicitadas e desconhecidas usadas até agora, mas não limitado a estas.

[0032] A Figura 9 é um diagrama de interação que ilustra a técnica de transmitir controle de tráfego não-solicitado, propiciado de acordo com o presente pedido de

patente. Voltando à Figura 9, inicialmente um UTC 910 não contém quaisquer regras IP L 901 para o dispositivo de comunicação sem fio 930L, o qual, como ilustrado na Figura 9, tem correntemente o endereço IP L. Quando PKT11 903 chega, o UTC 910 envia PKT11 em uma mensagem reguladora 905 para o representante do dispositivo sem fio 911 e substancialmente no mesmo instante armazena uma cópia do pacote na memória 920, a qual estava inicialmente vazia 903. Depois de receber PKT11, o representante do dispositivo sem fio 911 forma a regra de PKT11 906 e envia-a de volta para o UTC 910 em resposta à mensagem reguladora 905. O UTC 910 atualiza consequentemente as regras 960 para o dispositivo de comunicação sem fio 930L. Se a regra para PKT11 for tal que PKT11 903 puder seguir para o dispositivo de comunicação sem fio 930L, o UTC 910 envia 970 uma cópia do PKT11 armazenado para o dispositivo de comunicação sem fio 930L. De modo inverso, se a regra para PKT11 for tal que PKT11 903 não puder seguir para o dispositivo de comunicação sem fio 930L, então não é encaminhado. No desenho, o aspecto condicional do envio 970 é ilustrado pela utilização de uma linha pontilhada para representar a mensagem 970.

[0033] A Figura 10 é um diagrama de blocos que ilustra uma rede sem fio que inclui uma modalidade de um controlador de tráfego não-solicitado, propiciado de acordo com o presente pedido de patente. Comparada com a Figura 1, a Figura 10 detalha ainda mais a rede sem fio 1000 que mostra a cooperação entre o UTC 1010 e um servidor de Autenticação, Autorização e Contabilização AAA 1020. O AAA 1020 gerencia os dispositivos sem fio de informações de

assinante 130A-130N como ilustrado pelos registros de Dados de W A 1060A a Dados de W N 1060N. Um exemplo de um AAA é um servidor RADIUS (RADIAL).

[0034] A Figura 11 é um diagrama de interação que ilustra o comportamento do UTC quando um dispositivo de comunicação sem fio cessa a operação, propiciado de acordo com o presente pedido de patente. Voltando agora para a Figura 11, a um dispositivo de comunicação sem fio A 1130A com identificador é atribuído o endereço J. É criado um perfil de dispositivo 1120 no AAA 1125. Quando o endereço J atribuído ao dispositivo de comunicação sem fio A é devolvido 1140, AAA envia uma mensagem que substancialmente indica que os dados do dispositivo A estão inativos, tal como mensagem de Término de Contabilização 1150 para armazenar UTC 1110. O UTC 1110 identifica as regras de UTC 1160 associadas ao dispositivo de comunicação sem fio 1130A de acordo com o identificador W A e endereço J atribuído àquele dispositivo de comunicação sem fio. O UTC 1110 armazena então 1170 as regras de barreira de proteção associadas ao dispositivo de comunicação sem fio 1130A em um dispositivo de memória 1180 para recuperação posterior.

[0035] A Figura 12 é um diagrama de interação que ilustra o comportamento do UTC quando um dispositivo de comunicação sem fio previamente inativo se torna novamente ativo, propiciado de acordo com o presente pedido de patente. Voltando para a Figura 12, inicialmente o dispositivo de comunicação sem fio 1230A com identificador W A não tem endereço, e então é atribuído 1240 o endereço K. AAA 1225 envia uma mensagem que substancialmente indica que os dados do dispositivo A estão ativos, tal como

mensagem de Início de Contabilização 1250, para recuperar UTC 1210. O UTC 1210 recupera 1270 as regras de UTC armazenadas 1290 para o dispositivo A a partir da memória 1280 e atualiza os dados de UTC 1295 com as regras 1290 para aplicar o endereço K e inicia o funcionamento por parte do dispositivo de comunicação sem fio 1230A com endereço K.

[0036] A Figura 13 é um diagrama de interação que ilustra a técnica de inversão de regras do UTC quando um endereço atribuído a um dispositivo de comunicação sem fio é reatribuído a outro dispositivo de comunicação sem fio, propiciado de acordo com o presente pedido de patente. Voltando para a Figura 13, a um dispositivo de comunicação sem fio A 1330A com identificador W A é inicialmente atribuído o endereço J. O UTC 1310 mantém as regras de UTC 1360 por parte do dispositivo de comunicação sem fio A 1330A. Como mostrado no desenho, de acordo com as regras correntemente em vigor para W A, PKT12 é deixado ir avante e alcança o dispositivo de comunicação sem fio A 1330A. Contudo, em um instante posterior, o dispositivo de comunicação sem fio 1330A devolve o endereço K de volta para o AAA 1320. Após devolução de IP J 1340, o AAA 1320 envia uma mensagem que substancialmente indica que os dados do dispositivo A estão inativos, tal como Término de Contabilização 1350, para o UTC 1310. O UTC 1310 inverte a porção das regras de IP J solicitadas 1325 das regras de UTC 1360. Uma vez que esta porção das regras estava relacionada com o dispositivo de comunicação sem fio A 1330A, a inversão 1332 garante que o dispositivo de comunicação sem fio 1330B se torne ativo e a ele é

atribuído 1370 o endereço IP J, mesmo antes de AAA 1320 enviar uma mensagem que indica substancialmente que os dados do dispositivo sem fio B, tal como mensagem de Início de Contabilização 1380 para o UTC 1310, o UTC 1310 bloqueia substancialmente todos os pacotes que foram considerados não-solicitados pelo dispositivo sem fio A 1330A. As regras invertidas 1325I garantem, portanto, que, se o dispositivo sem fio A estava usando VPN através da rede de pacote de dados 1390, por exemplo, e não terminou VPN antes da devolução de IP J 1340, nenhum pacote não-solicitado, tal como ~PKT12, deixado pela sessão VPN viciada, jamais alcançará o dispositivo sem fio B 1330B. De preferência, a inversão é temporária, por exemplo, limpando as regras invertidas 1325I depois de saber que todas as sessões viciadas estavam esgotadas, ou substituindo as regras invertidas 1325I até que o UTC 1310 substitua as regras invertidas 1325I com regras representantes do dispositivo sem fio B 1330B, ou até que um período predeterminado de desconto tenha expirado.

[0037] A Figura 14 é um diagrama de interação que ilustra a técnica de transferência entre-UTCs, propiciada de acordo com o presente pedido de patente. Voltando para a Figura 14, um dispositivo de comunicação sem fio A 1430 com identificador WA está usando o endereço S atribuído por AAA 1420. AAA 1420 envia uma mensagem que indica substancialmente que os dados do dispositivo A estão inativos, tal como Término de Contabilização 1460, para a fonte UTC 1410Q. A devolução de IP S 1450 poderia, por exemplo, ser um resultado de mobilidade. Ocorre uma transferência de Regras de W A 1440 de UTC Q 1410Q para UTC

R 1410R.

[0038] A fonte UTC Q 1410Q mantém as Regras de W A 1440 representantes do dispositivo de comunicação sem fio A 1430. Depois da transferência, as Regras de W A 1440 são mantidas no destino UTC R 1410R. Quando AAA 1420 atribui IP T 1470 ao dispositivo sem fio 1430A, AAA 1420 envia uma mensagem que indica substancialmente que os dados do dispositivo A estão ativos, tal como Início de Contabilização 1480, para UTC R 1410R. Vantajosamente, o UTC R 1410R já tem Regras de W A 1440 como resultado da transferência, de modo que o dispositivo sem fio W A 1430A nunca é deixado desprotegido pelas suas Regras de W A 1440.

[0039] Embora não expressamente mostrado nos desenhos, outros mecanismos da devolução e reatribuição de endereços podem provocar transferência. Por exemplo, AAA 1420 pode emitir ordens de orientação de transferência para UTCs.

[0040] A Figura 15 mostra a modalidade GPRS descrita no parágrafo acima em maior detalhe. Voltando agora para a Figura 15 e com referência tanto à Figura 1 como à Figura 15, a Rede de Serviço Móvel Terrestre Público (PLMN) 1500 (uma rede sem fio 100) é a rede 3GPP que recebe os dados de *push* provenientes do iniciador de *push* 1570 (o qual está na rede de pacote de dados 120 ou 1520) e garante a entrega dos dados de *push* ao recipiente de *push* (o qual está em pelo menos um dos dispositivos de comunicação sem fio 130A-130N ou equipamentos de usuário (UE) 1530A-1530N). A entrega dos dados de *push* pode envolver outras redes não explicitamente mostradas na Figura 1 ou Figura 15. A função de *push* 1505 é a função na PLMN 1500 que recebe os dados de

push provenientes do iniciador de *push* 1570. A função de *push* é responsável por enviar os dados de *push* para o recipiente de *push* 1590A-1590N. A rede de pacote de dados 1520 é uma interface para dentro da PLMN 1500 através de IP. O Equipamento do Usuário 1530A-1530N é qualquer um dos dispositivos de comunicação sem fio 130A-130N. Operacionalmente, as regras da Barreira de Proteção Baseadas no Usuário (UBF) ou regras da Barreira de Proteção Baseadas em Subscrição (SBF) (tais como 140A-140N ou 1540A-1540N) são persistentemente regras de barreira de proteção armazenadas com base no usuário ou subscrição ao invés de na sessão, e reforçadas pelo controlador de tráfego não-solicitado 1510 ou 110. Por exemplo, uma regra baseada em subscrição persistirá para um usuário ou subscrição específico ao longo de muitas sessões de IP (ou outras), enquanto que uma regra baseada em IP persistirá pela duração da sessão de IP. Uma subscrição pode incluir mais que um usuário, tal como, por exemplo, todos os usuários em uma empresa. As regras de barreira de proteção baseadas em usuário (ou subscrição) podem ser explicitamente definidas pelo usuário, pelo operador, ou implicitamente definidas pelo comportamento do UE (por exemplo, solicitação de um serviço). A lista baseada em UE de regras de barreira de proteção opera de modo a aparecer substancialmente como se cada interface tivesse uma barreira de proteção aparente 1550A-1550N (150A-150N) que protegesse cada via portadora do equipamento do usuário 1560A-1560N ligando a rede sem fio 1500 ou 100 aos dispositivos de comunicação sem fio 1530A-1530N (130A-130N). Considera-se que a via portadora pode incluir qualquer um ou todos de: sms, sip, circuito

comutado, pacote comutado, serviço de troncos, wlan, radiodifusão e multi-difusão ou qualquer outra portadora necessária para propiciar um serviço de comunicação tal como voz, *push* para falar, correio eletrônico, bate-papo e similares. O iniciador de *push* 1570 é a entidade que origina os dados de *push* e submete-os à função de *push* 1505 para entrega a um recipiente de *push* 1590A-1590N. Um iniciador de *push* pode ser, por exemplo, uma aplicação que propicie serviços de valor agregado, tais como correio eletrônico ou outras comunicações apropriadas. Um agente de usuário de *push* 1580A-1580N é qualquer software ou dispositivo associado a um recipiente de *push* que interprete os dados de *push* para o usuário de dispositivos de comunicação sem fio 130A-130N. Isto pode incluir navegadores de texto, navegadores de voz, máquinas de pesquisa, software de interface de máquinas ou dispositivos, e outros agentes de usuário de *push*, por exemplo. Um recipiente de *push* é a entidade que recebe os dados de *push* provenientes da função de *push* e processa-os ou usa-os. Isto é o UE com o qual a PLMN se comunica e fatura, o agente de usuário com o endereço de nível de aplicação, e o dispositivo, máquina ou pessoa que utiliza os dados de *push*. Um usuário ou subscrição individual controla um recipiente de *push*. Um perfil de subscrição de *push* (PSP) 1595 para cada usuário ou assinante é preferivelmente acessível à barreira de proteção baseada no usuário (UBF) integral ao controlador de tráfego não-solicitado 1510 ou 110. O PSP é um conjunto de parâmetros que indica os ajustes e preferências do recipiente do usuário para o serviço de *push*. Isto pode incluir uma

capacidade de cancelamento para a portadora sem fio implementar um conjunto padrão de regras de UBF para todos os Recipientes de *Push* (assinantes). Por exemplo, isto permitiria que todos os usuários pegassem *push* WAP por valor básico sem a possibilidade de bloqueá-lo. Um exemplo similar é o serviço de Radiodifusão/Multi-Difusão.

[0041] A Figura 16 mostra uma modalidade exemplificativa de um aparelho controlador de tráfego não-solicitado, propiciado de acordo com o presente pedido de patente. A rede de pacote de dados 1610 envia tráfego não-solicitado destinado ao dispositivo de comunicação sem fio. O controlador de tráfego não-solicitado 1600 intercepta todo o tráfego enviado pela rede de pacote de dados 1610 que é destinado ao dispositivo de comunicação sem fio 1620, ou outros dispositivos similares para os quais é dada autoridade para controlar tráfego não-solicitado. O controlador de tráfego não-solicitado 1600 inclui uma interface de rede de pacote de dados 1640 para receber pacotes provenientes da rede de pacote de dados, assim como uma interface de rede de dados sem fio 1660 para enviar pacotes para o dispositivo de comunicação sem fio 1620.

[0042] Operacionalmente, o módulo de controle de tráfego não-solicitado 1650 aplica regras 1670 representativas do dispositivo de comunicação sem fio 1620 para bloquear seletivamente pacotes de serem enviados pela interface da rede de dados sem fio 1660 para o dispositivo de comunicação sem fio 1620, propiciando deste modo uma barreira de proteção aparente 1630 que impede substancialmente pacotes que são considerados não-solicitados pelo dispositivo de comunicação sem fio 1620 de

alcançarem o dispositivo de comunicação sem fio 1620.

[0043] Em modalidades alternativas, as interfaces 1640 e 1660 podem ser de apenas uma via, de modo que podem apenas receber e transmitir respectivamente, ou podem ser de duas vias, permitindo que os pacotes sejam tanto transmitidos como recebidos.

[0044] As modalidades descritas aqui são exemplos de estruturas, sistemas ou métodos que possuem elementos correspondentes a elementos deste pedido de patente. Esta descrição escrita pode permitir que aqueles versados na técnica fabriquem e usem modalidades que possuem elementos alternativos que correspondem de modo similar aos elementos deste pedido de patente. O âmbito pretendido do pedido de patente inclui, portanto, outras estruturas, sistemas ou métodos que não diferem da invenção como descrita aqui, e inclui ainda outras estruturas, sistemas ou métodos com diferenças não-substanciais em relação à invenção como descrita aqui.

REIVINDICAÇÕES

1. Método para controlar tráfego de rede de comunicação sem fio em uma rede sem fio (100), a referida rede de comunicação sem fio compreendendo um controlador de tráfego não-solicitado (UTC) (910) acoplado a uma rede de pacotes de dados (920) e a uma pluralidade de dispositivos de comunicação sem fio (130A, ..., 130N), o referido método para controlar tráfego destinado a um primeiro dispositivo de comunicação sem fio (930L) da referida pluralidade de dispositivos de comunicação sem fio (130A, ..., 130N), o método **caracterizado** por compreender as etapas de:

armazenar um conjunto de regras de controle de tráfego (901, 960) associadas ao referido primeiro dispositivo de comunicação sem fio (930L);

determinar uma primeira identidade correspondente a um usuário do referido primeiro dispositivo de comunicação sem fio (930L);

em resposta a um de: um pacote de entrada fluindo a partir da rede de pacote de dados (920) e destinada ao referido primeiro dispositivo de comunicação sem fios (930L); e um pacote de saída que flui do referido primeiro dispositivo de comunicação sem fio (930L) e destinado a referida rede de pacote de dados (920), selecionar as referidas regras de controle de tráfego armazenadas (901) associadas com a referida identidade de subscrição e atualização determinada, na UTC (910), as referidas regras de controle de tráfego selecionadas (901);

determinar que um pacote subsequente recebido da referida rede de pacotes de dados (920) se destina ao referido primeiro dispositivo de comunicação sem fio

(930L);

aplicar as referidas regras de controle de tráfego (901, 960) selecionadas e atualizadas para determinar se o referido pacote subsequente é um pacote não-solicitado pelo referido usuário e

impedir o referido pacote subsequente de ser enviado para o referido primeiro dispositivo de comunicação sem fio (930L) se tiver sido determinado que o referido pacote subsequente não foi solicitado.

2. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a referida rede de comunicação sem fio (100) é uma rede CDMA sem fio e pelo fato de que o referido UTC (910) está localizado em pelo menos um Nó de Atendimento de Pacotes de Dados PDSN.

3. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a referida rede de comunicação sem fio (100) é uma rede GPRS sem fio e pelo fato de que o referido UTC (910) está localizado em um de um SGSN e GGSN.

4. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o referido conjunto de regras de controle de tráfego é implícito, explícito, dinâmico ou uma combinação destes.

5. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que as referidas regras de controle de tráfego compreendem regras de controle de tráfego implícitas (225, 245), em que em resposta ao referido pacote de saída fluindo a partir do primeiro dispositivo de comunicação sem fio (230A) e destinado a referida rede de pacote de dados (120), atualizar as

referidas regras de controle de tráfego selecionadas compreende a atualização de uma lista de tráfego solicitado nas referidas regras de controle de tráfego implícitas (225, 245) com uma definição de tráfego tendo uma semelhança substancial de pelo menos uma de: fonte; destino; e dados com o referido pacote de saída, e em que o método compreende ainda:

aplicar as referidas regras de controle de tráfego selecionadas (225, 245) para determinar se o referido pacote subsequente é solicitado pelo referido utilizador por determinar com o uso da referida definição se o referido pacote subsequente tem uma semelhança substancial de pelo menos um de: fonte; destino; e dados com o referido pacote de saída; e

liberar o referido pacote subsequente para o referido primeiro dispositivo de comunicação sem fio (230A) se o referido pacote subsequente for determinado para ser solicitado.

6. O método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que as regras de controle de tráfego selecionadas compreendem regras de controle de tráfego explícitas (325, 345), em que em resposta ao referido pacote de entrada que flui da referida rede de pacote de dados e destinado ao referido primeiro dispositivo de comunicação sem fio (330A), a atualização das referidas regras de controle de tráfego selecionadas na UTC compreende:

liberar o referido pacote de entrada para o referido primeiro dispositivo de comunicação sem fio (330A);

receber do referido primeiro dispositivo de

comunicação sem fio (330A) uma mensagem em relação ao referido pacote de entrada; e

com o uso da referida mensagem atualizando uma lista de tráfego não solicitado nas referidas regras de controle de tráfego explícitas (325, 345) com uma definição de tráfego tendo uma semelhança substancial de pelo menos um de: fonte; destino; e dados com o referido pacote de entrada, em que aplicar as referidas regras de controle de tráfego selecionadas para determinar se o referido pacote subsequente não é solicitado pelo referido utilizador compreende determinar com o uso da referida definição se o referido pacote subsequente tem uma semelhança substancial de pelo menos um de: fonte; destino; e dados com o referido pacote de entrada.

7. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato das referidas regras de controle de tráfego selecionadas compreenderem regras de controle de tráfego dinâmico (425, 445), em resposta ao referido pacote de entrada que flui da referida rede de pacote de dados e destinado ao referido primeiro dispositivo de comunicação sem fio (430A), atualizando as referidas regras de controle de tráfego selecionadas (425, 445), compreende:

liberar o referido pacote de entrada para o referido primeiro dispositivo de comunicação sem fio (430A); e

atualizar uma lista de tráfego desconhecido nas referidas regras de controle de tráfego dinâmico (425, 445) com uma definição de tráfego com uma semelhança substancial de pelo menos uma de: fonte; destino; e dados com o referido pacote de entrada,

em que aplicar as referidas regras de controle de

tráfego selecionadas para determinar se o referido pacote subsequente não é solicitado pelo referido utilizador compreende determinar com o uso da referida definição se o referido pacote subsequente tem uma semelhança substancial de pelo menos um de: fonte; destino; e dados com o referido pacote de entrada.

8. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a referida identidade de subscrição é selecionada a partir de um grupo consistindo de: IMSI, NAI, MSIDSN e SIP URL.

9. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o referido pacote de entrada compreende e o referido pacote de saída são selecionados a partir de um grupo consistindo de Protocolo de Internet, voz, correio eletrônico, protocolo de transferência de hipertexto, protocolo de transferência de arquivos, serviço de mensagens de multimídia e serviço de mensagens curtas.

10. Método de acordo com a reivindicação 1, **caracterizado** pelo fato do referido UTC ser uma delegação UTC (910) e aqui em resposta ao referido pacote de entrada que flui da referida rede de pacote de dados (920) e destinado ao referido primeiro dispositivo de comunicação sem fios (930L), a atualização das regras de controle de tráfego selecionadas compreende:

enviar do referido pacote de entrada em uma mensagem reguladora a um transmissor (911) para regular o referido pacote de entrada como representante do referido primeiro dispositivo de comunicação sem fio (930L);

armazenar o referido pacote de entrada;

receber uma regra do referido transmissor (911); e

atualizar as referidas regras de controle de tráfego selecionadas (901, 960) com a referida regra recebida.

11. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a referida rede de comunicação sem fio compreende ainda um servidor (AAA) de autenticação, autorização e contabilidade (1125) que se comunica com o referido UTC e pelo fato de que o referido método compreende ainda as etapas de:

o servidor (AAA) (1125) criar um perfil (1120) associado ao referido primeiro dispositivo de comunicação sem fio (1130A);

devolver a referida identidade de subscrição e enviar uma mensagem de parada do referido servidor (AAA) (1125) para o referido UTC (1110) quando o referido primeiro dispositivo de comunicação sem fio (1130A) se torna inativo;

identificar o referido conjunto armazenado de regras de controle de tráfego associado com o referido primeiro dispositivo de comunicação sem fio; e

armazenar o referido conjunto identificado de regras de controle de tráfego em um dispositivo de armazenamento (1180) para recuperação posterior.

12. Método, de acordo com a reivindicação 11, **caracterizado** por compreender ainda as etapas de:

atribuir uma segunda identidade correspondendo ao referido usuário do referido primeiro dispositivo de comunicação sem fio (1130A);

enviar uma mensagem de partida do referido servidor (AAA) (1225) para o referido UTC (1210) quando o referido primeiro dispositivo de comunicação sem fio (1230A) se

torna ativo;

recuperar o referido conjunto armazenado de regras de controle de tráfego do referido dispositivo de armazenamento (1280); e

associar as referidas regras recuperadas com a segunda referida identidade.

13. Método, de acordo com a reivindicação 11, **caracterizado** por compreender ainda as etapas de:

atribuir o referido primeiro endereço IP devolvido a um segundo dispositivo de comunicação sem fio (1330B) da referida pluralidade de dispositivos de comunicação sem fio;

inverter o referido conjunto identificado de regras de controle de tráfego associadas ao referido primeiro endereço IP;

enviar uma mensagem de partida do referido servidor (AAA) (1320) para o referido UTC (1310) quando o referido segundo dispositivo de comunicação sem fio (1330B) se torna ativo; e

aplicar o referido conjunto invertido de regras de controle de tráfego ao referido segundo dispositivo de comunicação sem fio (1330B).

14. Método, de acordo com a reivindicação 11, **caracterizado** pelo fato de que o referido UTC é um UTC fonte (1410Q) e pelo fato de que o referido método compreende ainda as etapas de:

devolver o referido primeiro endereço IP e enviar uma mensagem de parada do referido servidor (AAA) (1420) para o referido UTC fonte (1410Q) indicando que o referido primeiro dispositivo de comunicação sem fio (1430A) se

tornou inativo;

transferir o referido conjunto identificado de regras de controle de tráfego para um UTC de destino (1410R);

atribuir um segundo endereço IP correspondente ao referido usuário do referido primeiro dispositivo comunicação sem fio (1430A);

enviar uma mensagem de partida do referido AAA (1420) para o referido UTC de destino (1410R) indicando que o referido primeiro dispositivo de comunicação sem fio (1430A) se tornou ativo e

aplicar o referido conjunto transferido de regras de controle de tráfego ao referido primeiro dispositivo de comunicação sem fio (1430).

15. Onda portadora **caracterizada** pelo fato de que incorpora um sinal de dados de computador representando sequências de instruções que, quando executadas por um processador de um controlador de tráfego não-solicitado UTC, o referido UTC sendo resistente em uma rede de comunicação sem fio e acoplado para uma rede de pacote de dados e uma pluralidade de dispositivos de comunicação sem fio, causa o processador para executar todas as etapas do método para qualquer uma das reivindicações de 1 a 14.

16. Aparelho (1600) para controlar, em uma rede de comunicação sem fio, tráfego não-solicitado destinado a um dispositivo de comunicação sem fio (1620) especificado de uma pluralidade de dispositivos de comunicação sem fio em uma rede de comunicação sem fio, o aparelho **caracterizado** por compreender:

uma primeira interface (1640) configurada para receber tráfego proveniente de uma rede de pacotes de dados

(1610); uma segunda interface (1660) configurada para enviar tráfego para o referido dispositivo comunicação sem fio (1620) especificado;

um primeiro meio de armazenamento que possui armazenadas nele instruções executáveis por computador representando um conjunto de regras de controle de tráfego (1670); e

um controlador de tráfego não-solicitado (UTC) (1650) que se comunica com as referidas primeira e segunda interfaces (1640, 1660) e referido primeiro meio de armazenamento, onde o referido UTC (1650) compreende:

meios para determinar uma identidade de subscrição atribuída ao referido dispositivo de comunicação sem fio (1620) especificado;

meios para, em resposta a um de: um pacote de entrada que flui a partir de uma rede de pacote de dados (1610) e destinado ao referido dispositivo de comunicação sem fios especificado (1620); e um pacote de saída fluindo do referido dispositivo de comunicação sem fio (1620) especificado e destinado para a referida rede pacote de dados (1610), selecionar, do referido conjunto de regras de controle de tráfego, regras de controle de tráfego associadas à referida identidade e atualizar as referidas regras de controle de tráfego (1670);

meios para determinar que um pacote subsequente recebido sobre a referida primeira interface (1640) da referida rede de pacote de dados é destinado ao referido dispositivo de comunicação sem fio (1620) especificado; e

meios para executar as referidas regras de controle de tráfego (1670) selecionadas para determinar se o

referido pacote subsequente é tráfego não-solicitado e bloquear seletivamente o referido tráfego não-solicitado recebido pela referida primeira interface de ser enviado através da referida segunda interface para o referido dispositivo de comunicação sem fio (1620) especificado.

17. Aparelho, de acordo com a reivindicação 16, **caracterizado** pelo fato de que a referida rede de comunicação sem fio é uma rede GPRS sem fio e pelo fato de que o referido UTC está localizado em um SGSN e um GGSN.

18. Aparelho, de acordo com a reivindicação 16, **caracterizado** pelo fato de que a referida rede de comunicação sem fio é uma rede CDMA sem fio e pelo fato de que o referido UTC está localizado em pelo menos um PDSN.

19. Aparelho, de acordo com a reivindicação 16, **caracterizado** pelo fato de que o referido conjunto de regras de controle de tráfego é implícito, explícito, dinâmico ou uma combinação destes.

20. Aparelho, de acordo com a reivindicação 16, **caracterizado** pelo fato de que a referida identidade de subscrição inclui uma dentre IMSI, NAI, MSIDSN e SIP URL.

21. Aparelho, de acordo com a reivindicação 16, **caracterizado** pelo fato de que o referido tráfego compreende pelo menos um dentre Protocolo de Internet, voz, correio eletrônico, protocolo de transferência de hipertexto, protocolo de transferência de arquivos, serviço de mensagens de multimídia e serviço de mensagens curtas.

22. Aparelho, de acordo com a reivindicação 16, **caracterizado** por compreender ainda um transmissor que se comunica com o referido UTC para regular o pacote subsequente como representante do referido dispositivo de

comunicação sem fio especificado.

23. Aparelho, de acordo com a reivindicação 16, **caracterizado** por compreender ainda um servidor de autenticação, autorização e contabilidade AAA que se comunica com o referido UTC para gerenciar informações de assinante associadas aos respectivos dispositivos da referida pluralidade de dispositivos de comunicação sem fio.

24. Aparelho, de acordo com a reivindicação 23, **caracterizado** por compreender ainda um segundo meio de armazenamento que se comunica com o referido UTC para armazenar o referido conjunto de regras de controle de tráfego quando o referido dispositivo de comunicação sem fio se torna inativo.

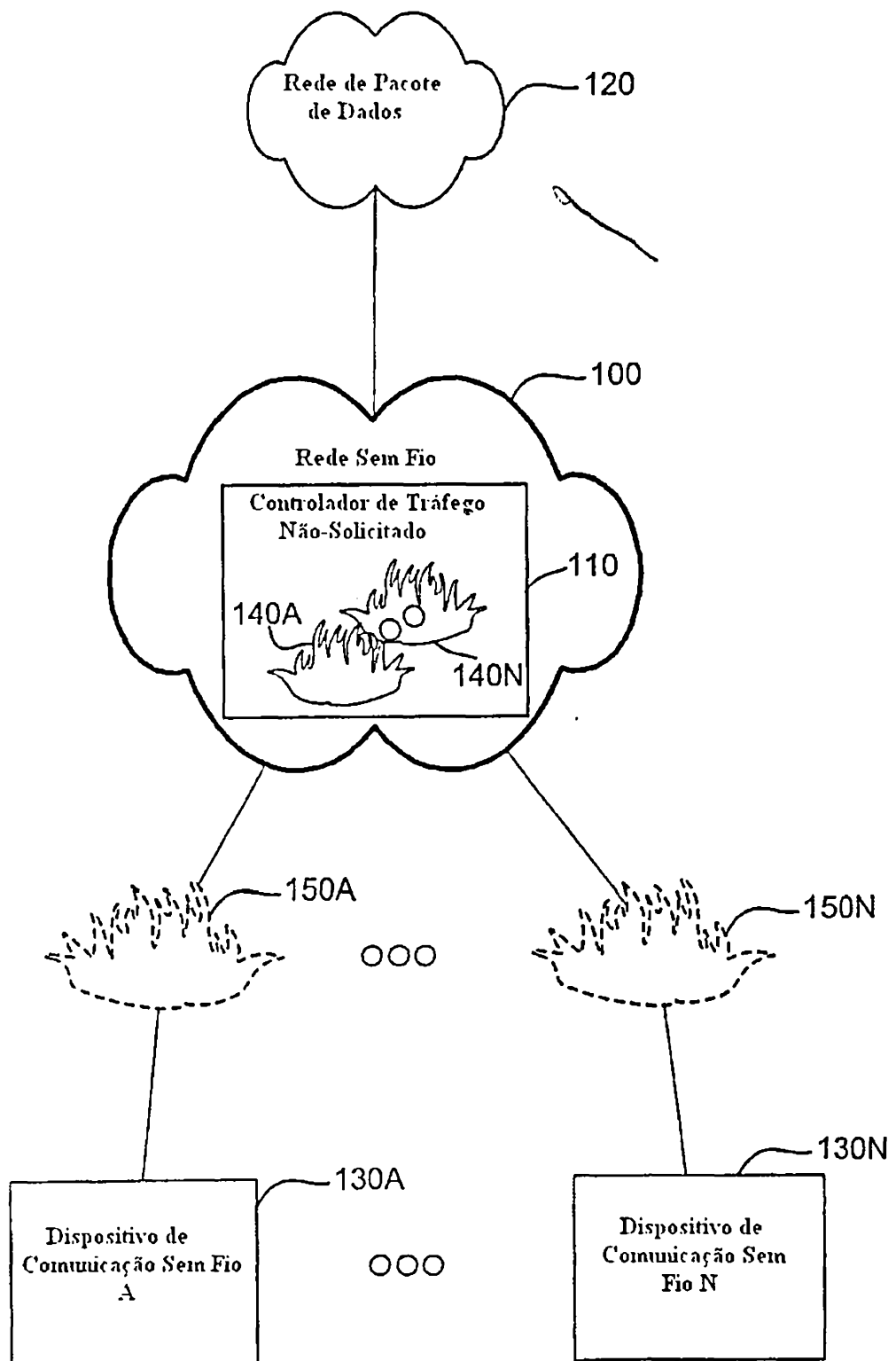


FIG. 1

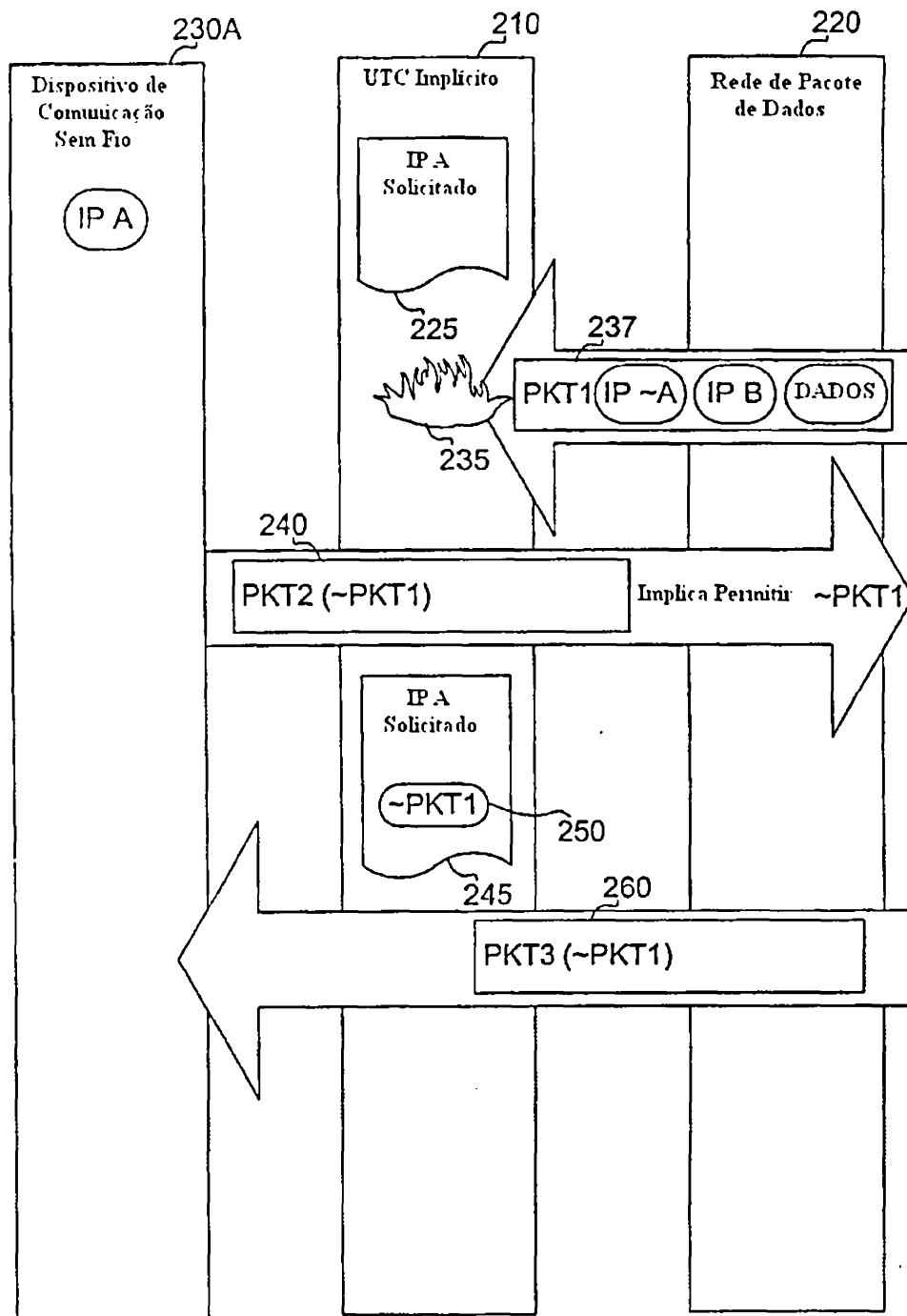


FIG. 2

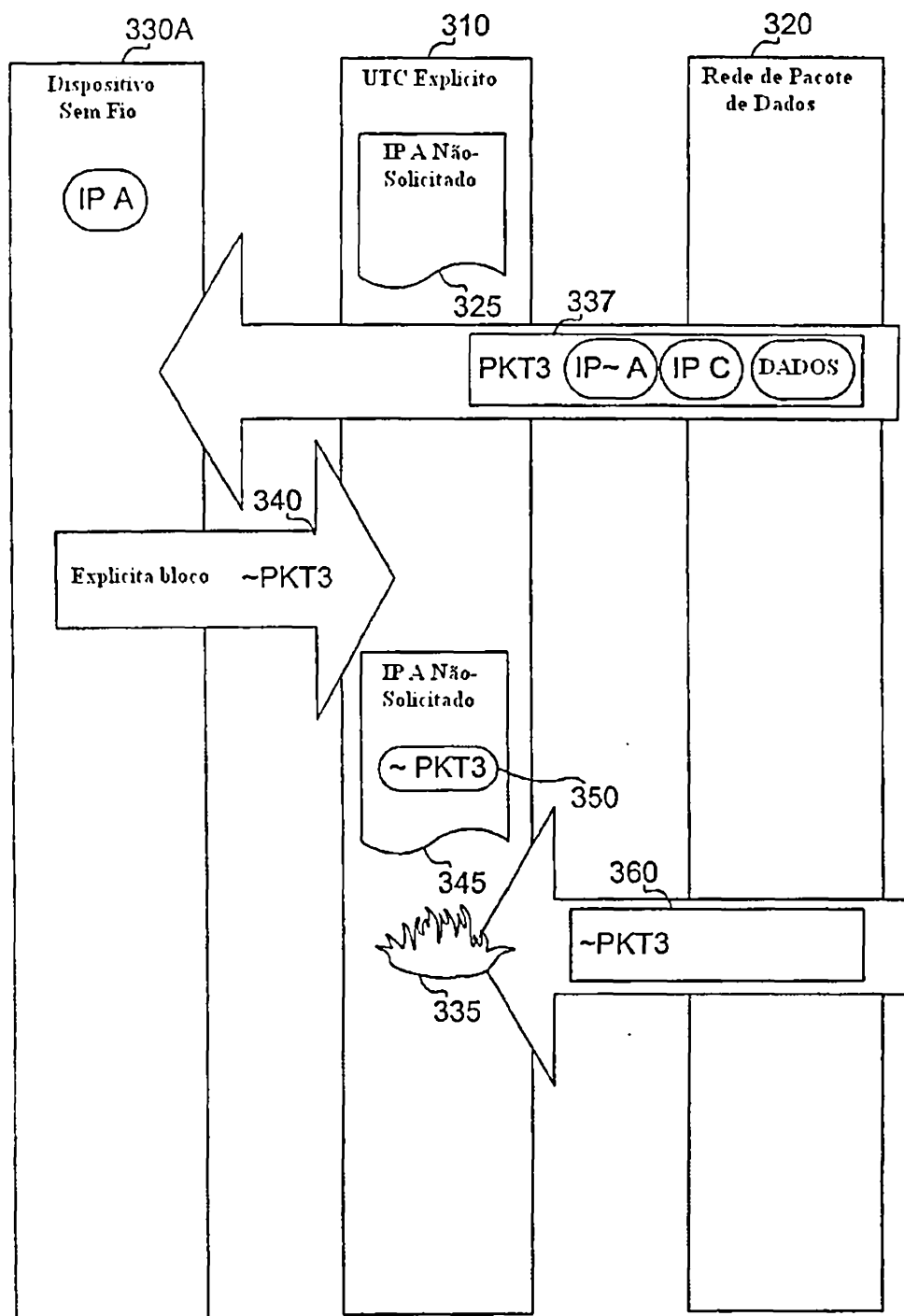


FIG. 3

105

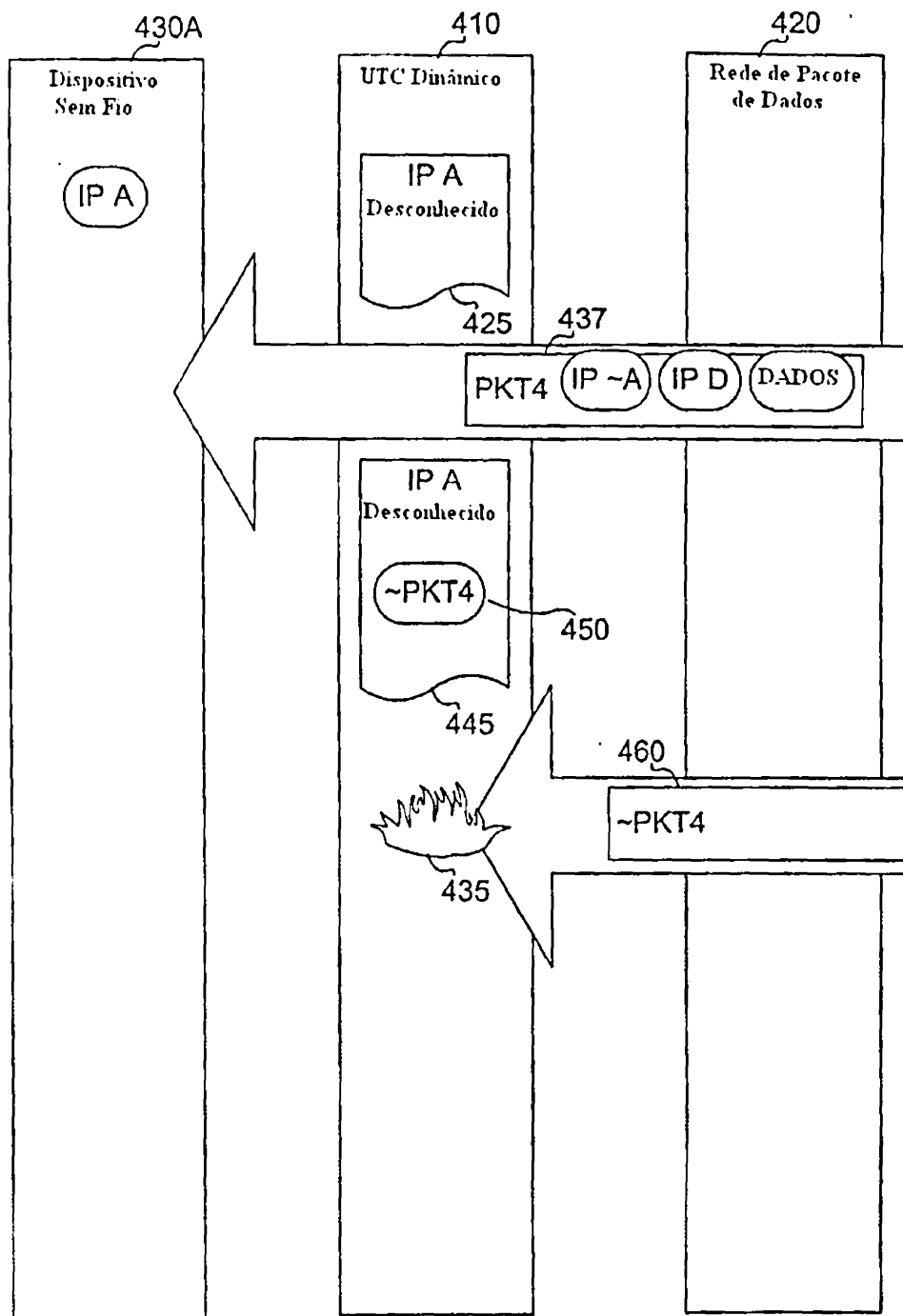


FIG. 4

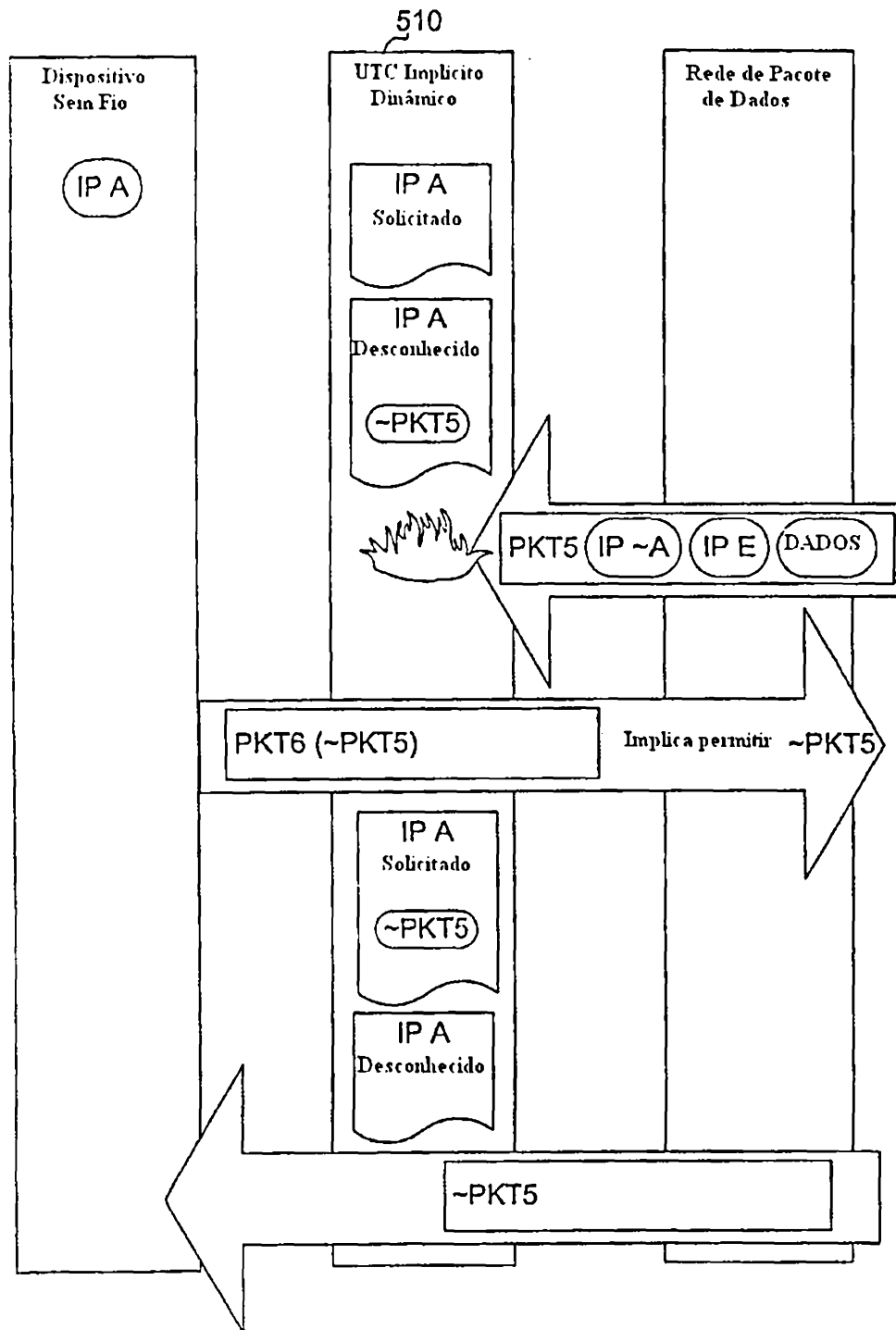


FIG. 5

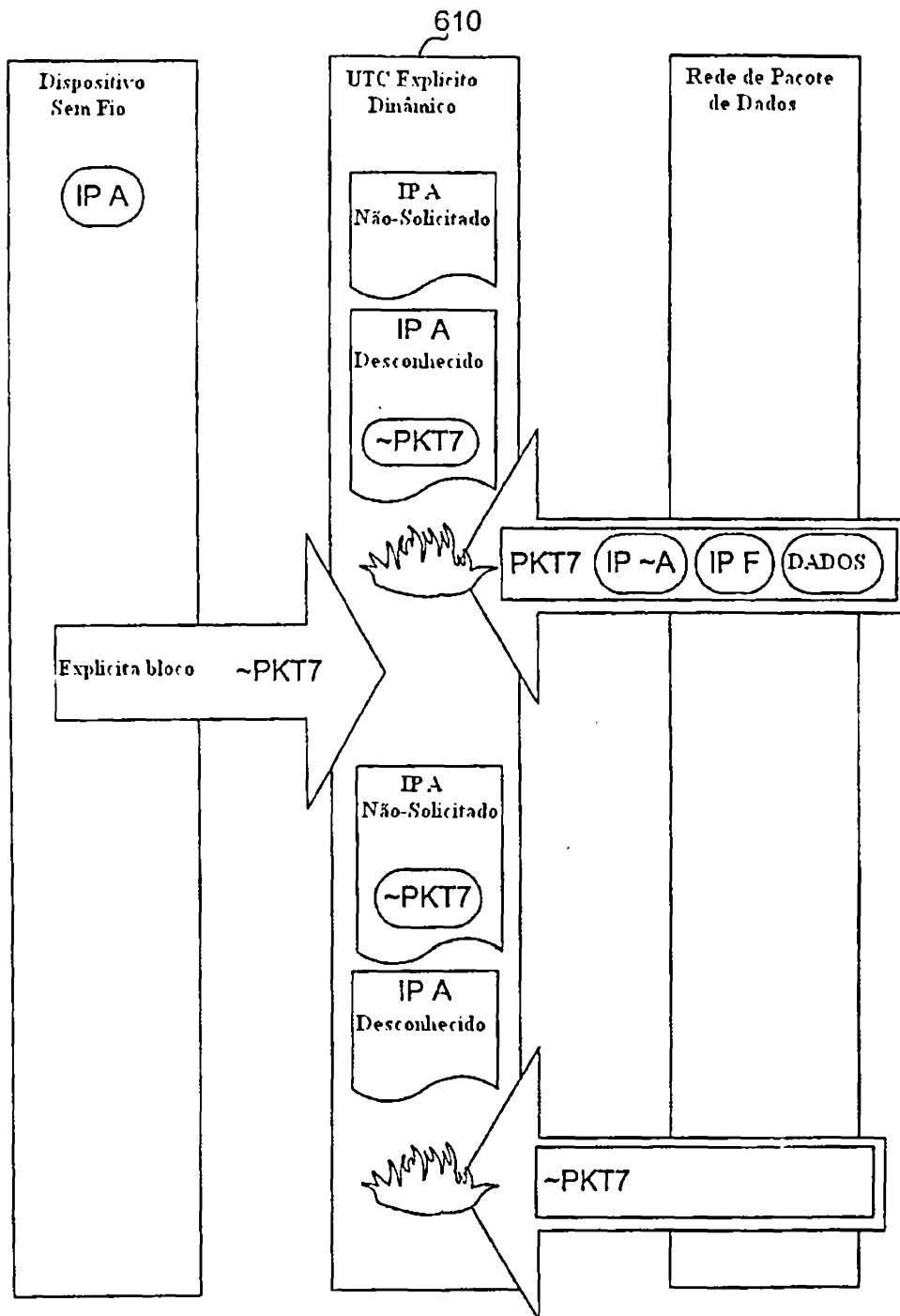


FIG. 6

103

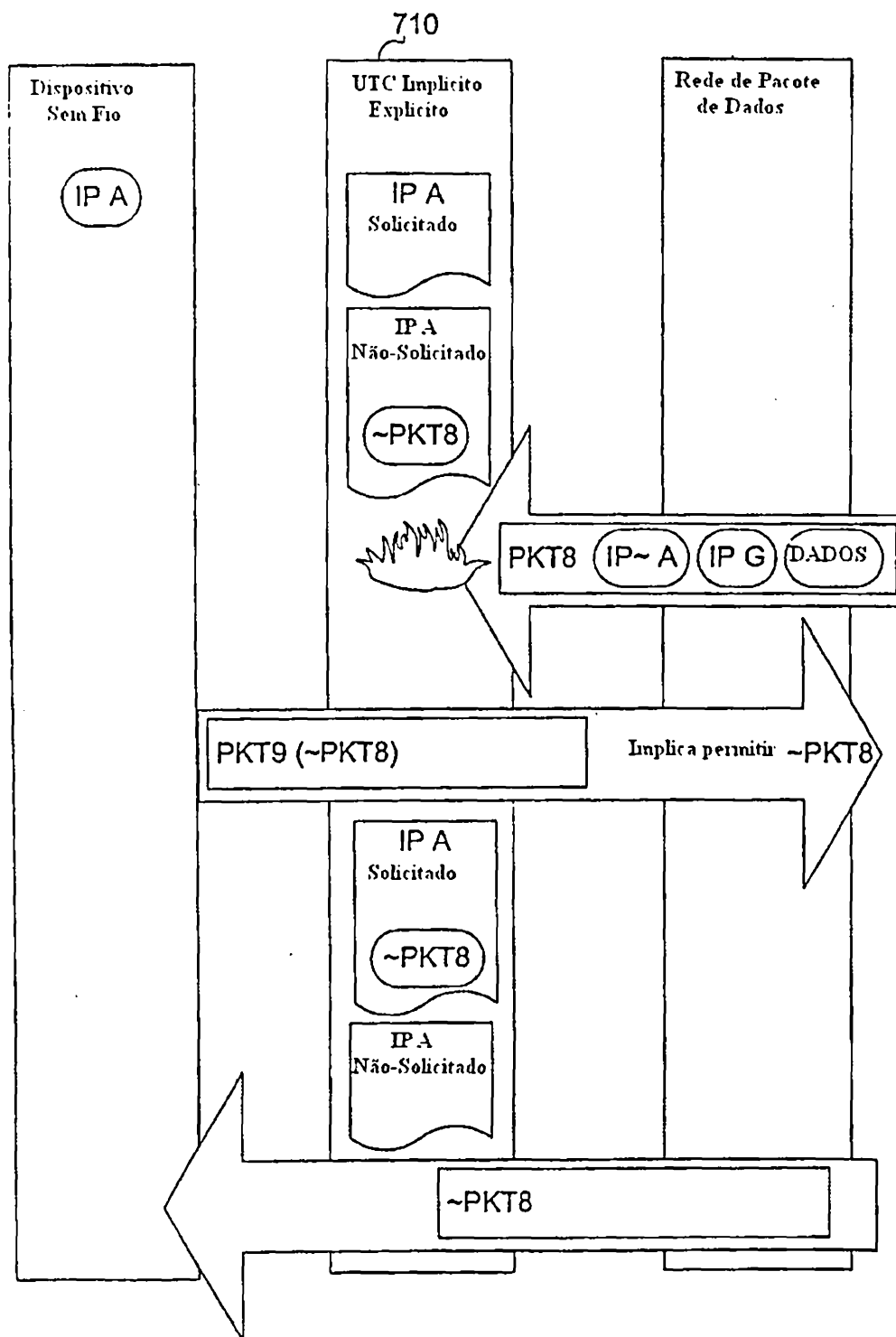


FIG. 7

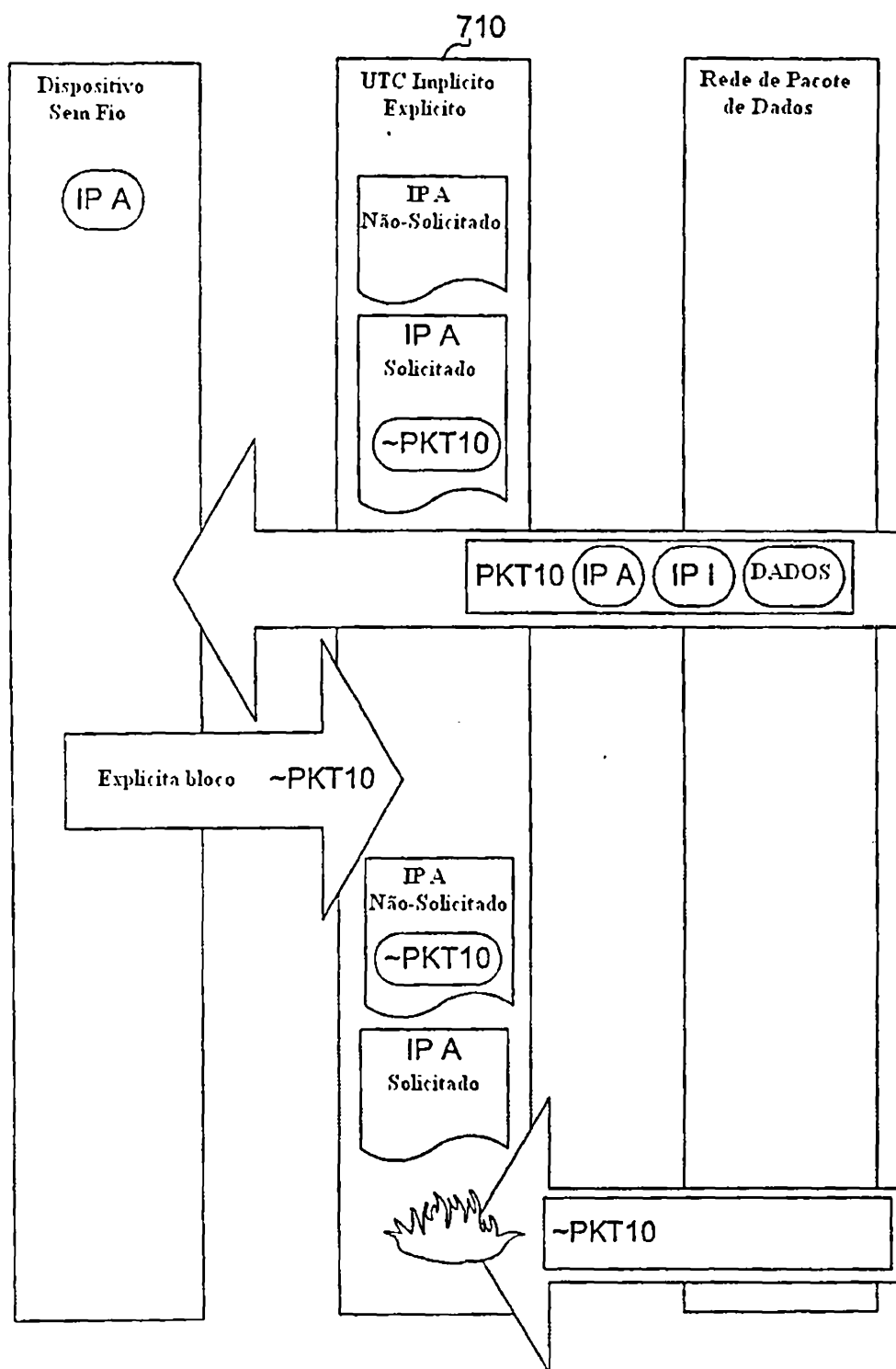


FIG. 8

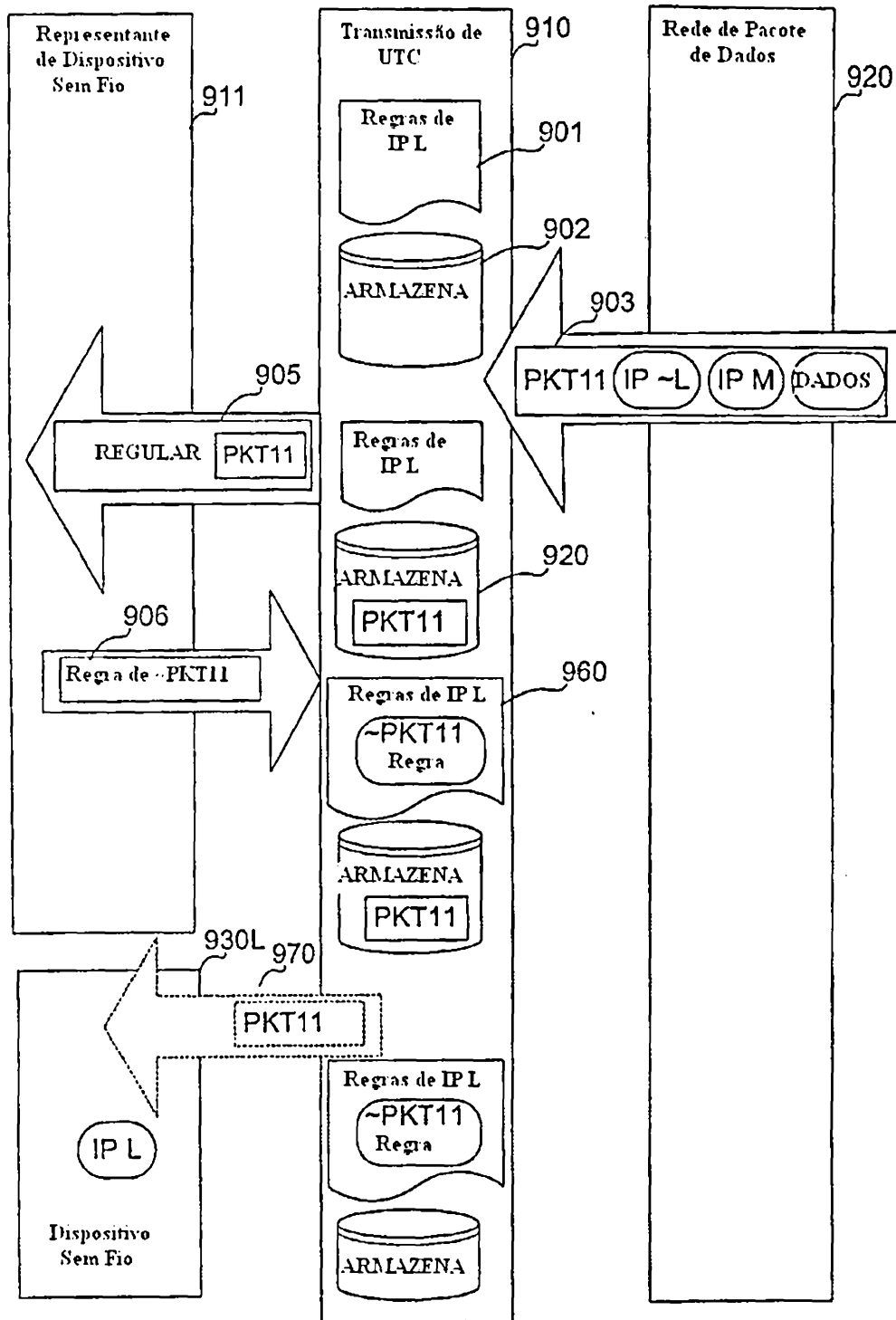


FIG. 9

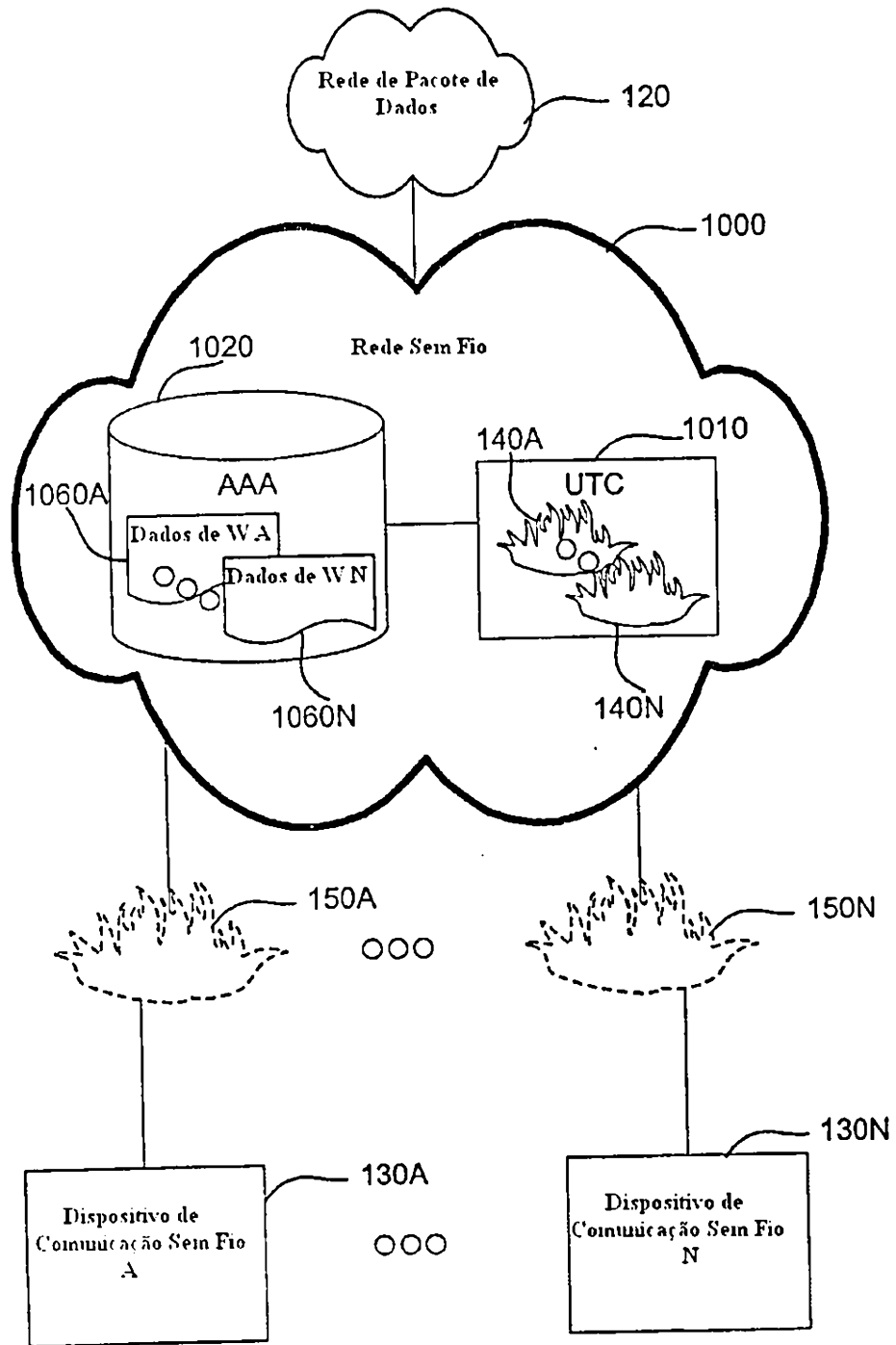


FIG. 10

112

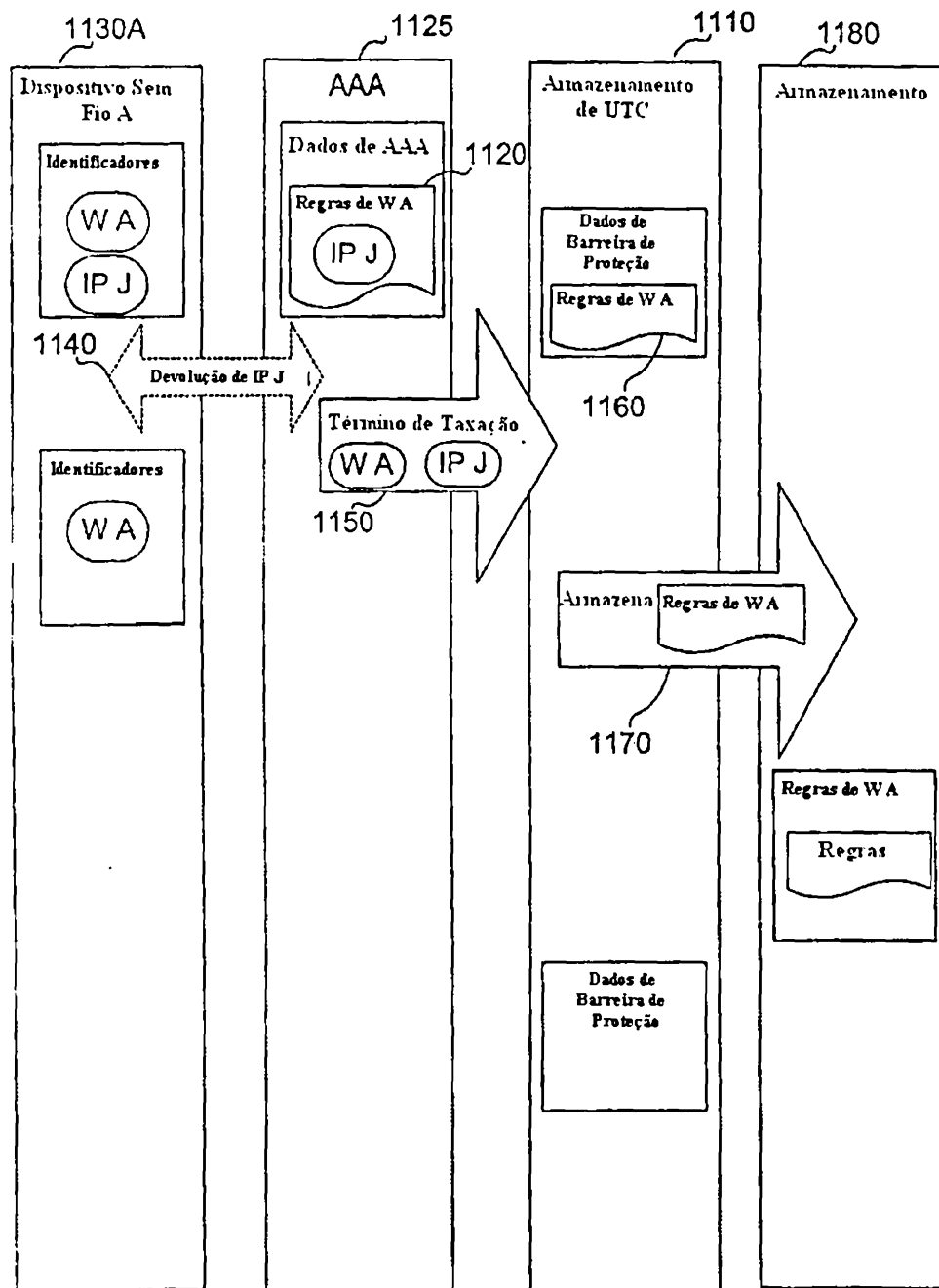


FIG. 11

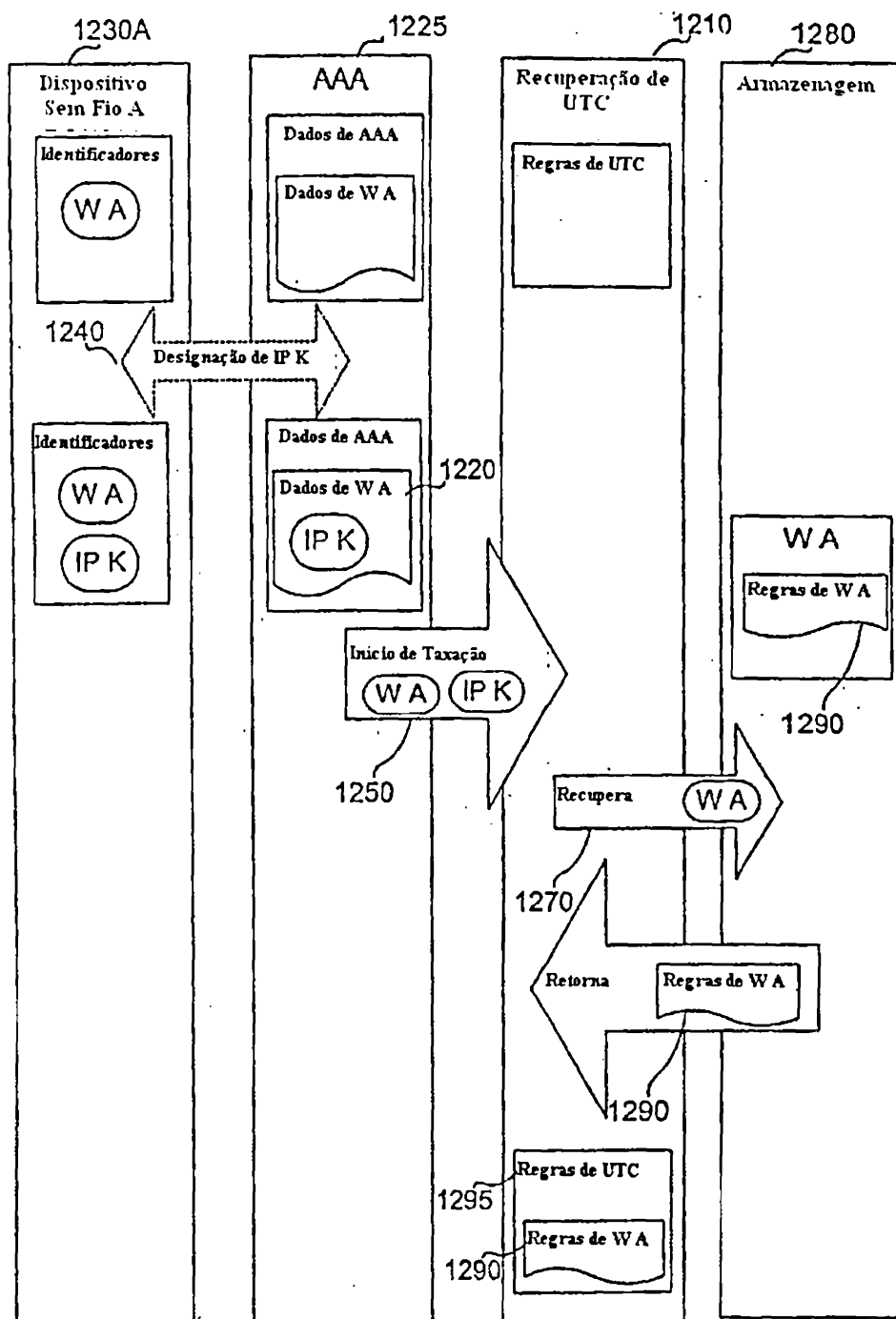


FIG. 12

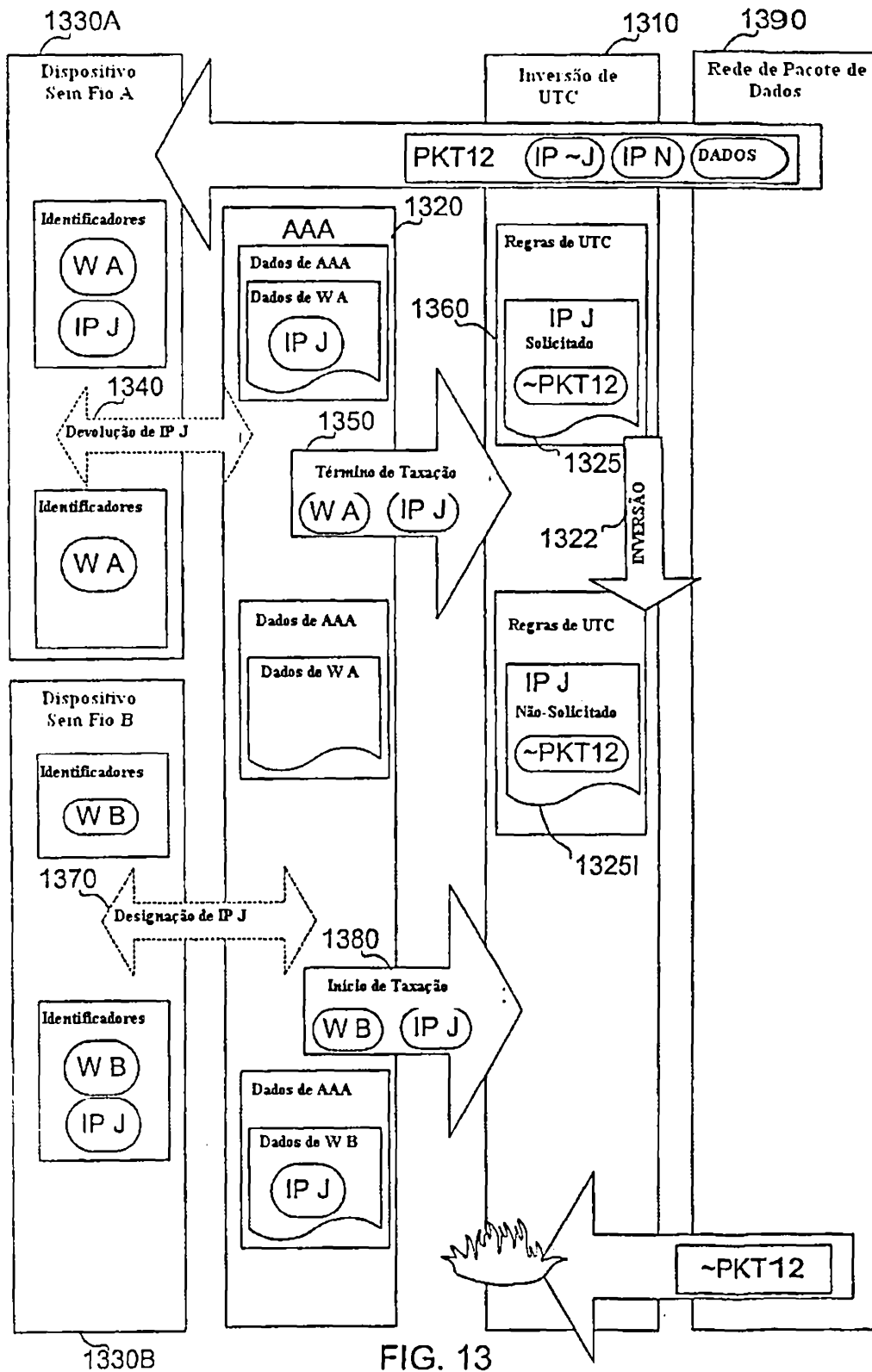


FIG. 13

115

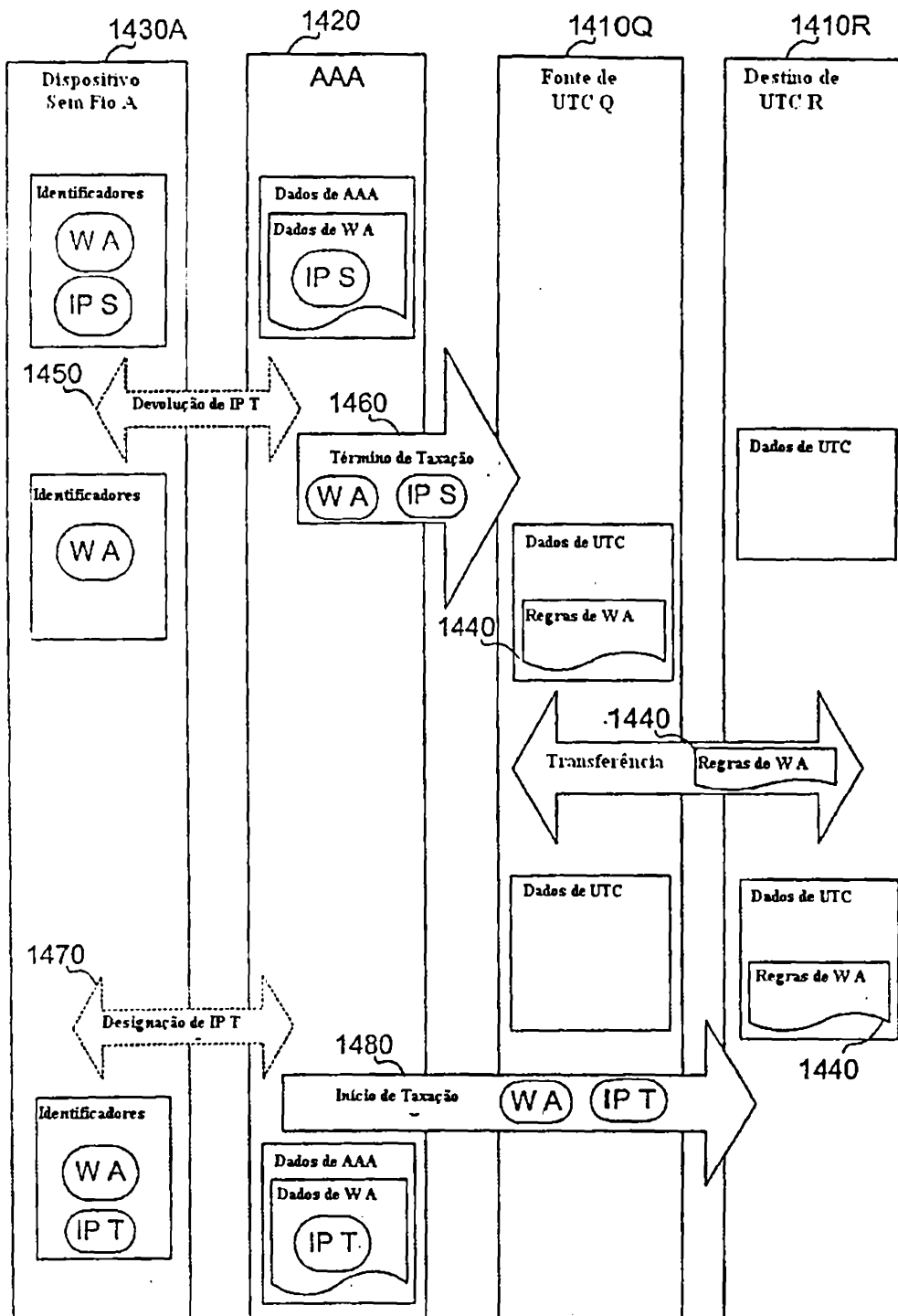


FIG. 14

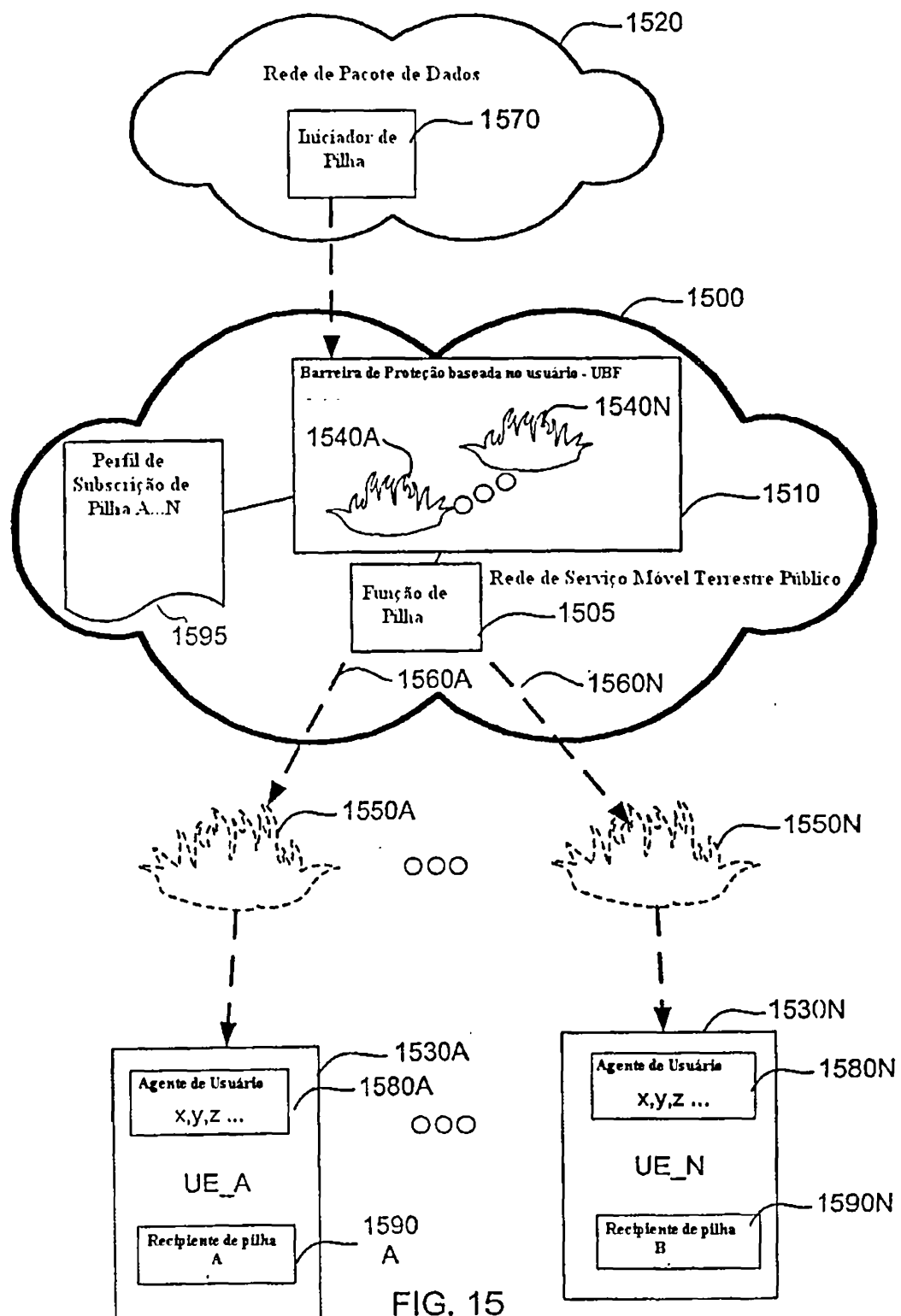


FIG. 15

117

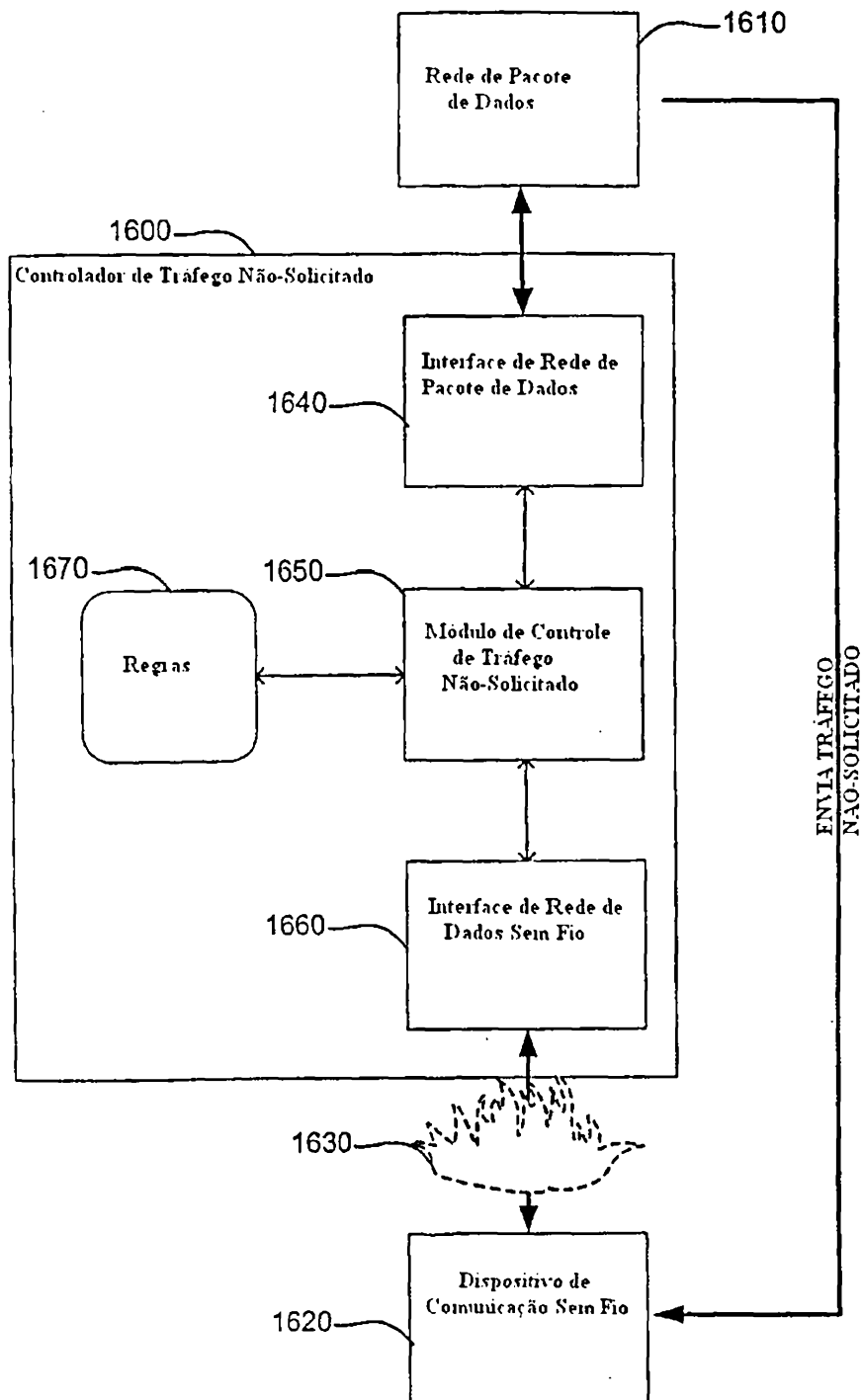


FIG. 16