(12) PEDIDO INTERNACIONAL PUBLICADO SOB O TRATADO DE COOPERAÇÃO EM MATÉRIA DE PATENTES (PCT)

(19) Organização Mundial da Propriedade Intelectual
Secretaria Internacional

(43) Data de Publicação Internacional
15 de Agosto de 2013 (15.08.2013)

WIPO | PCT

(10) Número de Publicação Internacional
WO 2013/116913 A1

(51) Classificação Internacional de Patentes : *H04W 8/10* (2009.01)

(21) Número do Pedido Internacional : PCT/BR2013/000035

(22) Data do Depósito Internacional : 4 de Fevereiro de 2013 (04.02.2013)

(25) Língua de Depósito Internacional : Português

(26) Língua de Publicação : Português

(30) Dados Relativos à Prioridade : BR102012003114-0
10 de Fevereiro de 2012 (10.02.2012) BR

(71) Requerente : **MLS WIRELESS S/A.** [BR/BR]; Rua Voluntários da Pátria, 45 / 1509, Botafogo, 22270-000, Rio de Janeiro, RJ (BR).

(72) Inventores : **GOLDENSTEIN, Mauro**; Rua Voluntários da Pátria, 45/Cob. 01, Botafogo, 22270, Rio de Janeiro, RJ (BR). **PASSY, Rogério**; Av. Epitácio Pessoa, 4310/704, Lagoa, Rio de Janeiro, RJ (BR). **PASSY, Luiz Victor**; Rua São Clemente, 262/812, Bloco 2, Botafogo, Rio de Janeiro, RJ (BR). **MARQUES CARNEIRO DA SILVA, Igor**; Av. Ayrton Senna, 270/1007, Bloco 1, Barra da Tijuca, Rio de Janeiro, RJ (BR).

(74) Mandatário : **DANNEMANN, SIEMSEN, BIGLER & IPANEMA MOREIRA**; Caixa Postal 2142, Rua Marquês de Olinda, 70, 22251-040, Rio de Janeiro, RJ (BR).

(81) Estados Designados *(sem indicação contrária, para todos os tipos de proteção nacional existentes)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Estados Designados *(sem indicação contrária, para todos os tipos de proteção regional existentes)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasiático (AM, AZ, BY, KG, KZ, RU, TJ, TM), Europeu (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(Continua na página seguinte)

(54) Title : METHOD FOR ACTIVATING USERS, METHOD FOR AUTHENTICATING USERS, METHOD FOR CONTROLLING USER TRAFFIC, METHOD FOR CONTROLLING USER ACCESS ON A 3G-TRAFFIC REROUTING WI-FI NETWORK AND SYSTEM FOR REROUTING 3G TRAFFIC

(54) Título : MÉTODO PARA ATIVAR USUÁRIO, MÉTODO PARA AUTENTICAR USUÁRIO, MÉTODO PARA CONTROLAR TRÁFEGO DE USUÁRIO, MÉTODO PARA CONTROLAR ACESSO DE USUÁRIO EM UMA REDE WI-FI DE DESVIO DE TRÁFEGO 3G E SISTEMA DE DESVIO DE TRÁFEGO 3G

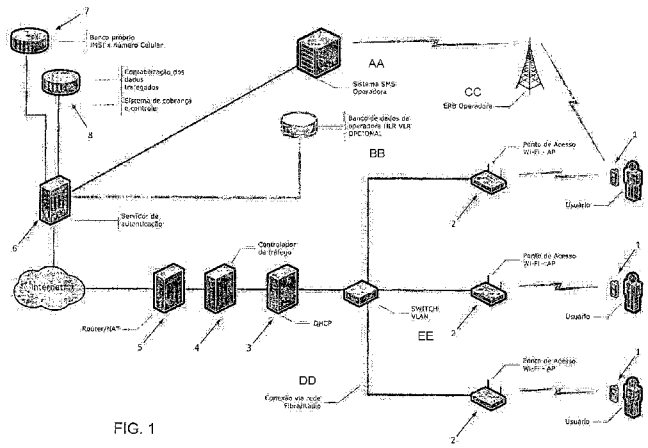

FIG. 1

1 User
2 Wi-Fi access point
3 DHCP
4 Traffic controller
5 Router/NAT
6 Authentication server
7 Own IMSI database by cell number
8 Routed data accounting / Billing and control system

AA Operator SMS system
BB OPTIONAL operator HLR VLR database
CC Operator radio base station
DD Connection via fiber/radio network
EE Switch/LAN

(57) Abstract : The present invention relates to a system for rerouting independent traffic on the networks of the mobile telephony operators, such as the GSM network, as well as the use of methods for user authentication and activation, traffic control and user access on a 3G-traffic rerouting Wi-Fi network. The rerouting Wi-Fi network proposed is independent of the mobile telephony network operators and enables the data traffic rerouting service to be provided to users of several operators simultaneously. The system includes its own database containing user information, obviating the need to consult operator databases. The system proposed also enables a user of operator A to purchase a Wi-Fi data plan from operator B using the International Mobile Subscriber Identity (IMSI) authentication of operator A, thereby obviating the need to replace the SIM card. Access to roaming users, i.e. users outside their native numbering area, is also permitted.

(57) Resumo :

(Continua na página seguinte)

WO 2013/116913 A1

Publicado:

— *com relatório de pesquisa internacional (Art. 21(3))*

A presente invenção refere-se a um sistema de desvio de tráfego indepen¬ dente das redes das operadoras de telefonia móvel, como a rede GSM, bem como ao uso de métodos de ativação e autenticação de usuário, de controle de tráfego e de acesso de usuário em uma rede Wi-Fi de desvio de tráfego 3G. A rede Wi-Fi de desvio proposta é independente das operadoras de rede de telefonia móvel e permite proporcionar o serviço de desvio de tráfego de dados a usuários de várias operadoras simultaneamente. O sistema possui um banco de dados próprio, no qual são guardadas as informações sobre os usuários para não haver a necessidade de fazer consultas a bancos de da¬ dos das operadoras. O sistema proposto permite ainda que um usuário da operadora A compre um plano de dados Wi-Fi da operadora B utilizando a autenticação pelo IMSI (International Mobile Subscriber Identity) da operado¬ ra A, dispensando, desta forma, a necessidade de substituição do SIM- CARD. O acesso a usuários em estado de roaming, ou seja, fora da área nativa de sua numeração também é permitido.

Relatório Descritivo da Patente de Invenção para **"MÉTODO PARA ATIVAR USUÁRIO, MÉTODO PARA AUTENTICAR USUÁRIO, MÉTODO PARA CONTROLAR TRÁFEGO DE USUÁRIO, MÉTODO PARA CONTROLAR ACESSO DE USUÁRIO EM UMA REDE WI-FI DE DESVIO DE TRÁFEGO 3G E SISTEMA DE DESVIO DE TRÁFEGO 3G".**

A presente invenção refere-se a um sistema de desvio de tráfego 3G independente e multioperadora, a métodos de ativação, autenticação e controle de acesso de usuários no sistema, e a um método de controle de tráfego no sistema.

É proposta a implementação de uma rede Wi-Fi independente das operadoras de rede de telefonia móvel que possa proporcionar o serviço de desvio de tráfego de dados a usuários de várias operadoras simultaneamente. O sistema possui um banco de dados próprio, no qual são guardadas as informações sobre os usuários para não haver a necessidade de fazer consultas a bancos de dados das operadoras, tornando assim o sistema independente. Ademais, o sistema permite que um usuário da operadora A compre um plano de dados Wi-Fi da operadora B utilizando a autenticação pelo IMSI (International Mobile Subscriber Identity) da operadora A, dispensando, desta forma, a necessidade de substituição do SIMCARD. O sistema permite ainda o acesso a usuários em estado de roaming, ou seja, fora da área nativa de sua numeração.

Descrição do Estado da Técnica

O acesso móvel à rede Internet vem aumentando consideravelmente, a cada ano, em escala mundial. Em alguns países, o número de acessos móveis já supera largamente o número de acessos fixos à rede Internet. Nos últimos 3 anos, o crescimento do número de acessos móveis em alguns países chega a ser maior que os 100% ao ano. Esta popularização do acesso móvel ocorreu principalmente com a implantação das redes celulares 3G combinada com o desenvolvimento e a oferta cada vez maior de aparelhos smartphones e tablets, acarretando preços mais acessíveis.

Os efeitos desse crescimento acelerado já podem ser observados em grandes centros urbanos onde tanto a tecnologia 3G, quanto a infraestrutura de

rede instalada não estão mais suportando a demanda por novos usuários. Nas redes celulares, devido a diversos fatores, o aumento do número de células nem sempre é possível e/ou viável. A limitação do uso do espectro de frequências pelas operadoras é um dos fatores limitantes para a oferta de mais e melhores serviços de dados aos usuários. Adicionalmente, a próxima geração tecnológica das redes móveis celulares, a 4G, ainda não foi implementada, sendo que não possuem suas frequências e divisões definidas.

O uso da tecnologia Wi-Fi surge como a principal solução, viável em curto prazo, para resolver o problema do congestionamento das atuais redes de telefonia móvel. Vários aspectos contribuem para essa opção tecnológica, tais como: a existência de interface Wi-Fi na maioria dos aparelhos smartphones e tablets; a padronização mundial da tecnologia Wi-Fi; a existência de centenas de fabricantes de equipamentos; o custo reduzido para a implementação de hotspots; a compactação dos equipamentos AP (Access Points); a alta taxa de transmissão que a tecnologia permite; e a total integração com sistemas IP (Internet Protocol).

As redes Wi-Fi, também conhecidas como redes WLAN (Wireless Local Area Network), utilizam os padrões da família 802.11 (por exemplo: 802.11a, 802.11b, 802.11g e 802.11n), definidos pelo IEEE (Institute of Electrical and Electronics Engineers). Originalmente, alguns telefones possuíam apenas um protocolo 802.11b. Atualmente, no entanto, já existem telefones com todos os quatro protocolos 802.11a/b/g/n operando em 2,4 GHz, 5,3 GHz e 5,8 GHz. Exemplificando em relação aos altos valores de taxa de transmissão que a tecnologia Wi-Fi permite, os protocolos 802.11a e 802.11n possuem capacidade de transmissão acima de 100 Mb/s.

Pelos motivos apresentados acima, o uso da tecnologia Wi-Fi com fins de descongestionamento de redes móveis vem sendo tema de estudo de diversos trabalhos. O documento WO 2005/008964 A1 e o documento US 2007/0268855 A1, por exemplo, apresentam as redes WLAN integradas ao sistema GSM 3G. Essa integração entre as redes é realizada de forma complexa necessitando de uma integração direta entre as redes WLAN e GSM

para a identificação e autenticação do usuário, pois não existe nenhum mecanismo de autenticação do usuário independente fora da rede GSM.

Uma integração através da operação simultânea das redes Wi-Fi e 3G por meio de servidores proxy localizados dentro da operadora é divulgada no documento US 2010/01154044 A1. No entanto, são apresentadas algumas limitações para operações de grande porte, cujo tráfego pode alcançar dezenas de Gigabits por segundo (Gb/s). Essas integrações com os sistemas da operadora têm como objetivo a reutilização dos sistemas de controle de acesso e autenticação através no HLR (Home Locator Register), pois somente estes sistemas possuem a chave de autenticação Ki relacionada ao número de identidade móvel internacional IMSI (International Mobile Subscriber Identity) gravado no SIMCARD de cada aparelho. Esse modo de integração limita o sistema de descongestionamento a somente uma operadora. Tal limitação também ocorre nos documentos US 2011/0222523, US 2007/0268855 A1 e no documento WO 2006/055986 A2.

A presente invenção descreve um sistema no qual não se faz necessário o acesso ao HLR. O sistema possui uma chave própria criada e transmitida de modo seguro para cada EMU (Equipamento Móvel do Usuário), não necessitando fazer uso da chave Ki como nos esquemas dos documentos mencionados. Em outras palavras, o sistema proposto proporciona um processo de autenticação de usuários totalmente fora dos controles e sistemas da rede 3G, sem consulta aos bancos de dados da operadora. Além disso, o sistema proposto faz a confirmação da chave de autenticação, enviada via SMS de volta pela rede Wi-Fi, representando um forte esquema de segurança contra qualquer tipo de fraude, pois não é possível um usuário falso receber a informação da chave via SMS. Como comparação, o documento US 2011/0222523 A1 propõe um sistema de paginação (paging) somente para informar a existência de um ponto de acesso e iniciar a migração para a rede Wi-Fi, não contendo nenhum mecanismo de segurança.

O documento US 2010/0135491 A1 apresenta um método de autenticação através de identificação de usuário e senha imputados manualmente pelo usuário no momento de acesso à rede Wi-Fi. No sistema proposto pela pre-

sente invenção, não há intervenção do usuário no processo de autenticação, proporcionando um grande aumento na segurança do controle de acesso. Todo o processo de autenticação é baseado nos números IMSI e MSISDN (Mobile Subscriber Integrated Services Digital Network Number) que são capturados pelo equipamento móvel do usuário (EMU). O número MSISDN é, na realidade, o número do celular do usuário. Note-se que, apesar do MSISDN geralmente não estar gravado no SIMCARD, o sistema proposto apresenta um método para a sua identificação de modo seguro e a devida associação com o respectivo IMSI. Assim, o sistema proposto automaticamente constrói sua própria base de dados para controle e autenticação dos usuários através da troca de chaves transmitidas, de modo seguro e transparente ao usuário, via SMS (Short Message Service). Caso necessário, este processo de autenticação via SMS pode ser efetuado diversas vezes para a revalidação da autenticidade do usuário. Como não existe interação direta com o sistema da operadora, o sistema proposto identifica a operadora do usuário através do MCC (Mobile Country Code) e do MNC (Mobile Network Code), permitindo assim o acesso para usuários de diferentes operadoras. Esta característica é de grande importância e proporciona ao sistema proposto um enorme diferencial em relação aos esquemas de desvio de tráfego existentes no estado da técnica

O controle sobre o processo de desvio de tráfego é um fator importante para a otimização do total de tráfego desviado. O método apresentado pelo documento US 2011/0222523, por exemplo, necessita da coexistência das redes 3G e Wi-Fi, uma vez que o controle, a decisão e a informação de desvio de tráfego para a rede Wi-Fi são transmitidos através da rede 3G. O mesmo ocorre no documento US 2004/0235455 A1. Tais transmissões podem sofrer atrasos devido ao congestionamento da rede 3G, impedindo assim o rápido acesso à rede de desvio. Na presente invenção, o processo de decisão de desvio é controlado pelo próprio EMU, evitando assim o aumento de tráfego de controle na rede 3G em determinada área, e aumentando a velocidade e a eficiência no acesso à rede Wi-Fi.

Breve Descrição da Invenção

A presente invenção refere-se a métodos para ativar, autenticar, controlar tráfego e controlar acesso de usuários em uma rede Wi-Fi de desvio de tráfego 3G. O método de ativação requer a instalação de um programa de controle no equipamento de usuário (EMU) e consiste em etapas de trocas de informações (como IMSI, MSISDN e chave UPK) entre o equipamento de usuário (EMU), o servidor de autenticação e o banco de dados próprio do sistema. Ao final, o EMU recebe uma resposta sobre o estado de ativação.

O método de autenticação de usuário tem início com uma solicitação de acesso à rede Wi-Fi de desvio, do EMU para o servidor DHCP, que envia um número IP. Então, o EMU envia para o servidor de autenticação, um pacote TCP contendo o número IMSI, o endereço MAC e o número IP. O servidor de autenticação checa se o EMU (1) foi previamente autenticado, verifica se a formatação do número IMSI é válida, identifica a operadora do usuário e armazena os dados de identificação do EMU, bem como as chaves pública e privada para validação no banco de dados. após verificar a validade da última autenticação do EMU na base de dados, o servidor de autenticação envia um código de acesso aleatório RAND, via SMS, para o EMU que intercepta a mensagem de modo que a mensagem não apareça para o usuário. O código RAND é encriptado através da chave UPK e enviado de volta para o servidor de autenticação, juntamente com o número ISMI, via rede Wi-Fi. Validado o EMU, servidor de autenticação armazena o IMSI no banco de dados ou atualizar o prazo de validade de autenticação do EMU. Então, uma mensagem de liberação de acesso à rede de desvio é enviada para o servidor de controle de tráfego e uma mensagem de confirmação de autenticação é enviada para o EMU.

O método de controle de tráfego dinâmico, com regras de controle de tráfego atualizadas a cada registro do EMU na rede Wi-Fi de desvio, e compreende as etapas de liberar o acesso a um usuário, controlar o tráfego, controlar congestionamentos, bloquear portas UDP/TCP, controlar o número de acessos simultâneos, e proporcionar firewall.

No método de controle de acesso de usuário, é verificado se o receptor Wi-Fi do EMU está ligado e se há alguma rede Wi-Fi conectada ao mesmo. En-

tão, procura-se um ponto de acesso Wi-Fi com o SSID da rede de desvio da operadora, caso o EMU (1) não estiver conectado a nenhuma rede Wi-Fi ou quando o EMU (1) estiver conectado a uma rede Wi-Fi diferente da rede de desvio da operadora e conecta-se o ponto de acesso encontrado ao EMU. Ou procura-se um outro ponto de acesso Wi-Fi com o SSID da rede de desvio da operadora, caso o EMU (1) já estiver conectado à rede de desvio da operadora e compara-se o nível do sinal do ponto de acesso Wi-Fi encontrado da rede de desvio com o nível de sinal da rede conectada ao EMU, optando pela conexão com o ponto de acesso Wi-Fi de melhor nível de sinal. Após isso, é verificada a existência de conexão de dados na interface Wi-Fi conectada e realizada a autenticação do EMU. Por fim, uma mensagem de "conectado" ou "não conectado" é exibida na tela do EMU.

Também é proposto um sistema de desvio de tráfego 3G compreendendo pelo menos um equipamento de usuário, pelo menos um ponto de acesso Wi-Fi, conectados por pelo menos um comutador VLAN, um servidor DHCP, um servidor de controle de tráfego, um roteador, um servidor de autenticação, um banco de dados de gravação de eventos e um banco de dados próprio.

Descrição Resumida dos Desenhos

A seguir, uma breve descrição das figuras:

Figura 1 - configuração do sistema de desvio Wi-Fi de tráfego 3G;

Figura 2 - fluxo de mensagens entre os componentes envolvidos no processo de ativação de usuários no sistema;

Figura 3 - fluxo de mensagens entre os componentes envolvidos no processo de autenticação de usuários no sistema;

Figura 4 - fluxograma do processo de autenticação de usuários na rede Wi-Fi de desvio;

Figura 5 - fluxograma do processo de verificação de tempo de vida do usuário (TVU) na rede de desvio; e

Figura 6 - fluxograma do processo controle de acesso de usuário na rede Wi-Fi de desvio.

Descrição Detalhada das Figuras

A presente invenção é descrita a seguir com base em um exemplo de execução representado nos desenhos.

É proposta a implementação de um sistema de desvio de tráfego independente das redes das operadoras de telefonia móvel, como a rede GSM, bem como o uso de métodos de ativação e autenticação de usuário, e de controle de tráfego e acesso de usuário em uma rede Wi-Fi de desvio de tráfego 3G. Desta forma, propõe-se uma solução para os problemas apresentados no estado da técnica descritos previamente.

A partir da figura 1 pode ser observada a configuração do sistema de desvio de tráfego 3G proposto. O sistema é composto pelos seguintes componentes: equipamento de acesso móvel do usuário (EMU) 1; ponto de acesso a redes sem fio (AP) 2; servidor DHCP (Dynamic Host Configuration Protocol) 3; servidor de controle de tráfego 4; roteador 5; servidor de autenticação de usuários 6; banco de dados de usuários 7; e banco de dados de gravação de eventos (LOG) 8. A seguir, encontra-se uma descrição de cada um destes componentes, com suas características principais, bem como as relações de interação entre os mesmos.

O equipamento de usuário (EMU) 1, podendo ser um aparelho celular, um tablet, ou qualquer outro aparelho que permita acesso móvel, deve ser compatível com os protocolos 802.11a, 802.11b, 802.11g ou 802.11n. Apenas deste modo, o usuário poderá ter acesso à rede de desvio de tráfego proposta, uma vez que esta utiliza a tecnologia Wi-Fi. Neste equipamento 1 é instalado, de forma transparente ao usuário, um programa de controle de acesso sem fio para efetuar a autenticação e a liberação do acesso à rede.

O ponto de acesso (AP) 2, ou seja, um equipamento rádio base que permite o acesso à rede sem fio Wi-Fi, deve ser compatível com os protocolos 802.11a, 802.11b, 802.11g ou 802.11n e operar nas frequências autorizadas pelos órgãos controladores de cada região (país). O AP 2 deve ter a capacidade de operar no modo "ponte transparente" para que o processo de distribuição de IP, assim como o controle de banda e a autenticação de usuários sejam efetuados diretamente entre o equipamento de usuário 1 e os equi-

pamentos responsáveis por tais tarefas (respectivamente, servidor DHCP 3, servidor de controle de tráfego 4 e servidor de autenticação de usuários 6).

O servidor DHCP 3 controla a distribuição dos números IP para cada usuário. Os números IP são liberados pela operadora de acordo com uma lista fornecida conforme a disponibilidade de IP's no local do sistema. Todo o processo de distribuição de números IP segue o protocolo DHCP.

O servidor de controle de tráfego 4 exerce tanto o controle de taxa de transmissão quanto a liberação de acesso à rede Wi-Fi. A liberação total do usuário à rede Wi-Fi compreende uma primeira etapa de cadastro do número IP e do endereço MAC (Media Access Control) em um firewall, de modo a liberar o tráfego irrestrito entre o equipamento de usuário 1 e a rede Internet. Então, em uma segunda etapa, um filtro HTB (Hierarchical Token Bucket) é utilizado para limitar a taxa máxima a ser liberada para o usuário. Finalmente, em uma terceira etapa, é utilizado o processo de organização de fila SFQ (Stochastic Fairness Queuing), de modo a evitar congestionamentos na rede.

O roteador 5 do sistema define as rotas internas e de saída do tráfego do usuário. Dependendo da disponibilidade de números IP da operadora, o roteador pode operar em modo NAT (Network Address Translation) para a distribuição de IP's inválidos.

O servidor de autenticação de usuários 6 controla a liberação de tráfego para o usuário conforme as regras pré-definidas pela operadora. Tal servidor 6 recebe as informações enviadas pelo equipamento de usuário 1 e, em seguida, de posse dessas informações (IMSI, endereço MAC e IP fornecido pelo servidor DHCP), consulta o banco de dados de usuários 7 para verificar a autenticidade das informações de identificação do usuário.

O banco de dados de usuários 7 deve conter as informações técnicas e comerciais sobre os usuários de modo que o servidor de autenticação de usuários 6 possa definir pela liberação ou não do tráfego para a rede externa (Internet), definindo a velocidade de acesso e o total de banda disponível para utilização pelo usuário.

O banco de dados de gravação de eventos 8 grava todas as operações de liberação, término e bloqueio de acesso ao sistema. Ele também produz uma

base de dados contendo as tentativas de acesso de usuários não aptos a utilizar a rede externa. Esta base de dados é uma importante ferramenta comercial para a venda de planos de dados.

A figura 2 mostra o processo de ativação do usuário no sistema. Observa-se o fluxo de mensagens entre os componentes envolvidos no processo. Para que este processo ocorra, um programa de controle deve ser instalado no EMU 1. O programa já pode vir previamente instalado pela operadora no EMU 1 ou pode ser instalado pelo próprio usuário, baixando-o através da Internet. Uma vez que o programa está instalado, é iniciado o processo de ativação do usuário no sistema de desvio de tráfego proposto. A primeira etapa para esta ativação é o envio S21, do EMU 1 para o servidor de autenticação 6, dos números IMSI e MSISDN através de mensagem SMS. Após o recebimento da mensagem SMS pelo servidor de autenticação 6, o número do celular MSISDN é capturado e associado ao IMSI. O par IMSI/MSISDN é então gravado S22 no banco de dados de usuários 7, que gera S23 um par de chaves (pública e privada) exclusivas para o usuário. A chave pública do usuário (UPK) é então transmitida S24 para o usuário, de forma total ou parcial, via SMS. O EMU 1 intercepta a mensagem SMS contendo o UPK, de modo que a mensagem não apareça para o usuário. Esse procedimento garante que o sistema identifique o usuário e transmita de forma segura a UPK utilizando a segurança do sistema 3G, através de algoritmos utilizados para a validação da chave Ki contida no SIMCARD.

Após o recebimento da chave pública do usuário (UPK), o EMU 1 envia S25 o par IMSI/UPK para o servidor de autenticação 6, através da rede Internet. Neste momento, ocorre a validação do usuário no servidor de autenticação 6 e esta validação é armazenada S26 no banco de dados 7. Em seguida, também através da rede Internet, o EMU 1 consulta S27 o servidor 6 sobre o estado da ativação. Caso o par IMSI/UPK seja válido, o servidor de autenticação 6 confirma S28 a ativação do usuário. Como se pode observar, até este ponto não é necessário o acesso à rede de desvio, uma vez que todas as comunicações ocorrem através da rede 3G (via SMS ou Internet). A cha-

ve UPK é utilizada ainda para revalidação periódica do usuário para a autenticação na rede de desvio.

O processo de autenticação de usuários na rede Wi-Fi de desvio é apresentado nas figuras 3 e 4. A figura 3 apresenta as diversas comunicações entre as entidades que participam desse processo de autenticação. Na figura 4 observa-se um fluxograma do processo.

Uma vez já tendo passado pelo processo de ativação no sistema, o equipamento móvel do usuário (EMU) 1 permanece em constante verificação da existência de pontos de acesso Wi-Fi 2, identificando os seus respectivos SSID's (Service Set Identification). Quando um SSID pertencente à rede de desvio é identificado, o EMU 1 analisa o nível do sinal recebido. Se o nível do sinal referente à rede de desvio for maior que um valor mínimo predeterminado para garantia de qualidade de conexão, o equipamento móvel do usuário 1 se conecta S31 ao ponto de acesso 2 estabelecendo a primeira fase de conexão ao sistema. Então, o EMU 1 solicita S32, S41 acesso à rede de desvio ao servidor DHCP e dele recebe S33 um número IP para dar-se início ao processo de autenticação do usuário. Nota-se que a decisão sobre a conexão ao ponto de acesso Wi-Fi 2 é realizada de forma transparente ao usuário, de forma independente da operadora. No sistema de desvio proposto, portanto, não há transmissão de informações do ponto de acesso Wi-Fi 2 através da rede celular. Todas as informações para o acesso do usuário à rede Wi-Fi são transmitidas automaticamente sem a necessidade de acesso à rede 3G. Este procedimento é de grande valia, pois garante velocidade e eficiência no acesso à rede Wi-Fi, mesmo sem cobertura da rede 3G, ao contrário dos sistemas de desvio de tráfego encontrados no estado da técnica.

Iniciado o processo de autenticação, o EMU 1 envia S34 para o servidor de autenticação 6 um pacote TCP (Transmission Control Protocol), contendo as seguintes informações: número IMSI, endereço MAC e número IP. O servidor de autenticação 6, com base nessas informações, faz uma verificação S42 de acesso recente do usuário. Para isso, checa o banco de dados 7 de usuários previamente autenticados. Caso o usuário não conste na base de

dados 7, trata-se de uma nova conexão e o sistema mantém este usuário ativo em sua base de dados 7 de usuários conectados apenas durante um período de tempo denominado tempo de vida útil do usuário (TVU). Se o usuário já está previamente autenticado e, portanto, no banco de dados 7 de usuários conectados, o servidor de autenticação 6 identifica o usuário e atualiza S43 seu TVU. O fluxograma da figura 4 ilustra essas etapas. Ressalta-se que, durante o TVU, o usuário pode mudar de ponto de acesso Wi-Fi 2 ainda mantendo o mesmo número IP, o que possibilita um handoff entre as células WLAN.

Após a etapa de verificação de acesso recente, o servidor de autenticação 6 executa a etapa de autenticação S44 no banco de dados próprio 7. Para isso, efetua uma verificação prévia de formatação do número IMSI, do número IP e do endereço MAC. Sendo a formatação válida, o servidor de autenticação 6, primeiramente, identifica a operadora do usuário, através da identificação da operadora MCC (Mobile Country Code) e da identificação móvel do país MNC (Mobile Network Code) contidos no número IMSI. De posse dessas informações, juntamente com o MSISDN transmitido pelo EMU 1 no momento da ativação do usuário no sistema e com as chaves (pública e privada) para validação do usuário, o sistema alimenta seu próprio banco de dados 7 para autenticação de usuários. Este banco de dados próprio 7 do sistema proposto dispensa a necessidade de acessar os bancos de dados HLR (Home Location Register) e VLR (Visitor Location Register) das operadoras e é um diferencial em relação às soluções de redes de desvio do estado da técnica. O banco de dados próprio 7 pode ser utilizado para a venda direta de serviços para o usuário. Ou seja, o usuário pode possuir uma assinatura de voz e/ou dados com uma operadora de telefonia e, ao mesmo tempo, pode adquirir um plano de dados Wi-Fi com outra operadora, utilizando o mesmo chip (SIMCARD) e o mesmo aparelho celular.

Como visto, o sistema proposto dispensa qualquer integração com a rede 3G, operando de forma totalmente independente. Além disso, o sistema permite que usuários de diferentes operadoras utilizem o mesmo ponto de acesso, compartilhando a infraestrutura da rede Wi-Fi e sem a necessidade

de duplicação da mesma. O sistema ainda permite que um usuário da operadora A adquira um plano de dados Wi-Fi da operadora B utilizando a autenticação pelo IMSI da operadora A, dispensando, desta forma, a necessidade de substituição do SIMCARD. Além disso, com as informações contidas no banco de dados próprio 7, é possível oferecer o serviço de roaming para outras operadoras.

Em seguida, é feita uma consulta S35 sobre a existência da identificação do usuário, identificado pelo seu número IMSI, ao banco de dados 7 próprio de usuários relacionados à operadora definida pelo MNC. O resultado da consulta depende de fatores comerciais para a utilização do sistema por usuários da operadora em questão. O banco de dados 7 retorna S36 o número do telefone MSISDN para o servidor de autenticação 6, validando ou não a autenticação no sistema. Caso a verificação seja negativa, o servidor de autenticação 6 envia S46 uma mensagem de acesso negado diretamente para o equipamento móvel do usuário 1, onde a mensagem é exibida. Há a possibilidade de, em seguida, ser exibida no EMU 1 uma mensagem de oferecimento de compra de plano de dados da operadora. Caso a verificação seja positiva, de acordo com as normas de liberação estabelecidas pela operadora (como, por exemplo, se o usuário possui plano de dados, se está ativo na base de dados de usuários 7 e também qual a sua velocidade de acesso), o sistema inicia a etapa de confirmação do usuário para prevenir qualquer tipo de fraude.

Após a verificação de acesso recente e a validação do usuário no banco de dados próprio 7, o sistema pode, periodicamente, efetuar outras verificações para evitar que um usuário forje requisições de acesso ao sistema se passando por outro usuário. Para isso, o sistema utiliza a rede de telefonia para o envio de SMS a fim de confirmar o usuário, conforme descrito a seguir. Uma vez realizada a validação na base de dados 7, o servidor de autenticação 6 verifica S47 a validade da última autenticação na base de dados 7. Caso o usuário não esteja na base de dados 7, ou seu registro esteja fora do prazo de validade, o servidor de autenticação 6 envia S37a, S48 um SMS (via rede 3G) para o número do equipamento móvel do usuário 1 contendo

um código de acesso aleatório RAND. É possível também que o código RAND seja enviado S37b através da rede Wi-Fi, para os locais onde não haja cobertura 3G. Em seguida, o EMU 1 intercepta essa mensagem SMS, de modo que a mensagem não apareça para o usuário. Em seguida, o número RAND, encriptado no EMU 1 através da chave UPK criada no momento da ativação do usuário no sistema, e o ISMI são enviados S38 via Wi-Fi para o servidor de autenticação 6. A confirmação desse código encriptado de volta pela rede Wi-Fi representa um forte esquema de segurança contra qualquer tipo de fraude, uma vez que não é possível um usuário falso receber a informação do código RAND via SMS. Então, o servidor 6 decripta o número RAND e o compara S49 com o número previamente enviado por SMS. Se os números forem idênticos, o servidor de autenticação 6 atualiza seu prazo de validade. Após essas etapas, o servidor de autenticação 6 envia S310, S410 uma mensagem de liberação de acesso ao servidor de controle de tráfego 4. Enquanto conectado, o EMU 1 transmite periodicamente ao servidor de autenticação 6 as informações ISMI, IP, MAC, SSID ao qual está conectado e a lista dos SSID detectados pelo EMU 1 com os níveis de seus respectivos sinais. Com base nas informações sobre os SSID's, o servidor de autenticação 6 tem a informação de quantos usuários estão conectados em cada ponto de acesso Wi-Fi 2. Então ocorre uma verificação S411 da necessidade do EMU 1 trocar de um AP 2 para outro AP 2. Objetivando evitar um congestionamento por excesso de usuários em um determinado AP 2, o servidor de autenticação 6 pode enviar S412 um comando para o EMU 1 instruindo a troca para um outro AP 2 que esteja próximo e com nível de sinal satisfatório. Após estas etapas para determinar se ocorre ou não um handoff do EMU 1, o servidor de autenticação 6 envia S311, S413 uma mensagem de confirmação ou atualização de autenticação ao EMU 1. Caso o usuário esteja ainda esteja no prazo de validade de autenticidade do usuário preestabelecido, o servidor 6 somente envia S37a, S48 um novo SMS para a verificação de autenticidade do usuário descrita acima se tal prazo de validade estiver próximo de expirar. Então, a etapa de liberação de acesso à rede Internet para o equipamento móvel do usuário 1 no servidor de controle

de tráfego 4 é iniciada. É importante ressaltar que esse processo de verificação da autenticidade do usuário é cíclico.

O tempo de vida do usuário (TVU) para uma conexão recente não deve ser confundido com a validade de autenticação do usuário. O TVU verifica se o usuário acabou de se conectar e ainda possui o seu número IP no servidor DHCP, enquanto o prazo de validade de autenticidade (que pode ser, por exemplo, de 1 mês) verifica a veracidade dos dados e a autenticidade do usuário.

O servidor de controle de tráfego 4 do sistema tem como finalidades a liberação de acesso, o controle de tráfego, o controle anticongestionamento, o bloqueio de portas UDP/TCP, o controle de número de acessos simultâneos e a implementação de firewall. Associando cada par IP/MAC relacionado ao usuário através de seu número IMSI, o sistema utiliza um filtro HTB (Hierarchical Token Bucket) para limitar a taxa máxima a ser liberada para o usuário, um processo de organização de fila SFQ (Stochastic Fairness Queuing) para evitar congestionamentos na rede e um esquema ARPTABLES para controlar e liberar os usuários pelos seus respectivos endereços MAC e IP. Os limites das velocidades de acesso são estabelecidos de acordo com a política dos planos de acesso contratados por cada usuário. O sistema, porém, é dinâmico e as regras de controle de tráfego vão sendo atualizadas a cada registro do EMU 1 na rede Wi-Fi. O servidor de controle de tráfego 4 ainda proporciona pelo menos um firewall com regras que evitam a saturação da rede por aplicações que demandam grande utilização de tráfego e um controle do número de acesso simultâneos. Deste modo, são oferecidos aos usuários segurança e estabilidade no acesso à rede externa Internet.

No processo de liberação de usuário, primeiramente, após a validação do usuário, o servidor de autenticação 6 emite comandos de liberação de acesso para o servidor de controle de tráfego 4 (direcionados de acordo com o endereço MAC / número IP do usuário), liberando o usuário para navegar na Internet através do ponto de acesso 2 correspondente, sob um determinado limite de banda. Por fim, o servidor de autenticação 6 envia S311, S413, através da rede Wi-Fi, uma mensagem para o EMU 1 com a confirmação de

liberação de acesso. Esta mensagem é exibida para o usuário na tela do EMU 1.

A figura 5 apresenta o fluxograma do processo de verificação de tempo de vida do usuário (TVU) na rede de desvio. Enquanto conectado, o equipamento móvel do usuário 1 transmite periodicamente ao servidor de autenticação 6 as informações ISMI, IP, MAC, SSID ao qual está conectado e a lista dos SSID presentes com seus respectivos sinais. Após a verificação e decisão sobre o handoff do EMU 1 para um outro AP 2, o servidor de autenticação 6, então, atualiza o tempo de vida do usuário (TVU) no sistema. Com base nisso, o servidor de autenticação 6 executa periodicamente uma rotina S51 independente, com intervalo definido para o término de permissão de acesso para cada conexão associada aos números ISMI que excedam o TVU. Todos os registros que estão com o TVU excedido na base de dados 7 de usuários ativos iniciam o processo de bloqueio S52, no qual o servidor de autenticação 6 envia mensagem ao servidor de controle de tráfego 4 para desativar as regras de liberação referentes ao endereço MAC / número IP associados a cada número ISMI e sua respectiva banda alocada.

A cada autorização do usuário no sistema, é criado um registro no banco de dados de gravação de eventos 8 contendo os seguintes dados: IMSI, IP, endereço MAC do equipamento móvel do usuário1, taxa de transmissão máxima liberada, data e hora da liberação, além da quantidade de Bytes trafegados de entrada e de saída (obtida no filtro HTB do servidor de controle de tráfego 4).

Ao final da utilização do sistema pelo usuário, quando ocorre o bloqueio do IP liberado para o equipamento móvel do usuário 1, o sistema transmite os dados gravados no banco de dados 8 para a operadora do usuário. De posse dessas informações a operadora pode contabilizar o volume de dados trafegado pelo usuário em seu sistema e, consequentemente, fazer a respectiva bilhetagem.

A figura 6 apresenta um fluxograma do processo de controle de acesso de usuário à rede Wi-Fi de desvio. Conforme descrito anteriormente, após o programa de controle ser instalado no EMU 1, dá-se início ao processo de

ativação de usuário no sistema de desvio. Em seguida, o EMU 1 passa a efetuar diversas tarefas essenciais para o funcionamento deste sistema.

A partir de um estado inicial S60, o EMU 1 verifica S61 se o seu receptor Wi-Fi está ligado. Caso esteja desligado, o serviço retorna para o estado inicial S60 e fica aguardando uma nova verificação. Caso contrário, o EMU 1 verifica S62 se existe alguma rede Wi-Fi já conectada ao equipamento. Esta etapa S62 é de extrema importância para que o EMU 1 não se desconecte da rede Wi-Fi já conectada anteriormente pelo usuário. É importante ressaltar que o EMU 1 pode ser configurado em relação à prioridade de conexão entre uma rede particular conhecida do usuário e a rede de desvio da operadora. Não havendo nenhuma rede Wi-Fi conectada ao equipamento, é iniciada uma etapa de escaneamento S63 à procura de alguma rede Wi-Fi com o SSID predefinido do sistema (rede de desvio da operadora). Não encontrando a rede Wi-Fi da operadora, o serviço retorna para o estado inicial S60 e fica aguardando uma nova verificação S61. Encontrando a rede de desvio, é realizada a associação S67 desta rede com o EMU 1 em substituição a qualquer outra rede anteriormente associada. Se, na etapa S62, for detectado que o EMU 1 está conectado a alguma rede Wi-Fi, então é verificado S65 (através do SSID da mesma) se esta rede é a rede da operadora. Não sendo, inicia-se a etapa S63 previamente definida para procura de uma rede Wi-Fi. Caso a rede na qual o EMU 1 está conectado seja a rede de desvio da operadora, o EMU 1 inicia um outro escaneamento S66 na rede Wi-Fi à procura de uma rede com o SSID da rede de desvio e, ao encontrá-la, compara o nível de seu sinal com o nível do sinal da atual rede associada. Quando o nível do sinal da rede encontrada é maior que o da rede atual, então se opta pela troca entre as redes e ocorre a associação S67 da nova rede ao EMU 1. Em seguida à associação S67, ou caso a etapa de verificação S66 não encontre nenhuma rede com sinal melhor que a rede atual, o EMU 1 executa a etapa de verificação S68 da existência de conexão de dados, ou seja, é verificada a existência de rede TCP-IP pela interface Wi-Fi e se há tráfego de dados nessa interface. Em caso negativo, o serviço retorna para o estado inicial S60 e permanece aguardando uma nova verificação S61. Em caso

positivo, durante o período de conexão do usuário na rede de desvio Wi-Fi, o EMU 1 envia S69 periodicamente as informações de IMSI, IP, MAC, SSID ao qual está conectado, bem como a lista dos SSID's detectados pelo EMU 1 com seus respectivos níveis de sinais. O servidor de autenticação, com base nessas informações, pode enviar S611 um comando de troca de ponto de acesso Wi-Fi 2 (handoff) para o EMU 1, caso seja necessário. Em caso de handoff, inicia-se outro ciclo de vida do serviço S60. Caso não ocorra troca de AP 2, o EMU 1 verifica S610 se houve a autenticação à rede de desvio. Havendo, uma mensagem de "conectado" ou "não conectado" é exibida S610a, S610b na tela do EMU 1 e o serviço retorna à etapa inicial S60.

Tendo sido descrito um exemplo de concretização preferido, deve ser entendido que o escopo da presente invenção abrange outras possíveis variações, sendo limitado tão somente pelo teor das reivindicações apensas, aí incluídos os possíveis equivalentes.

REIVINDICAÇÕES

1. Método para ativar usuário em uma rede Wi-Fi de desvio de tráfego 3G caracterizado pelo fato de que compreende as etapas de:

instalar um programa de controle no equipamento de usuário (1) (EMU);

enviar (S21) através de mensagem SMS, do EMU (1) para o servidor de autenticação (6), os números IMSI e MSISDN;

capturar, pelo servidor de autenticação (6), o número MSISDN;

associar, pelo servidor de autenticação (6), o número MSISDN ao número IMSI;

armazenar (S22) os números IMSI e MSISDN no banco de dados de usuários (7);

gerar (S23) no banco de dados de usuários (7) um par de chaves, pública (UPK) e privada, exclusivas para o EMU (1);

enviar (S24) através de mensagem SMS, do servidor de autenticação (6) para o EMU (1), a chave pública do usuário (UPK);

interceptar, pelo EMU (1), a mensagem SMS contendo a chave pública do usuário (UPK);

enviar (S25), do EMU (1) para o servidor de autenticação (6), o par IMSI/UPK;

validar o EMU (1) no servidor de autenticação (6);

armazenar (S26) a validação do EMU (1) no banco de dados de usuários (7);

consultar (S27), do EMU (1) para o servidor de autenticação (6), o estado da ativação no servidor de autenticação (6);

enviar (S28), do o servidor de autenticação (6) para o EMU (1), resposta sobre estado de ativação.

2. Método para ativar usuário, de acordo com a reivindicação 1, caracterizado pelo fato de que as etapas de instalar, armazenar (S22), enviar (S25), armazenar (S26), consultar (S27) e enviar (S28) são realizadas através de transmissões via rede Internet.

3. Método para ativar usuário, de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de instalar é realizada pelo próprio usuário, baixando o programa através da rede Internet.

4. Método para ativar usuário, de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de instalar é realizada pela operadora.

5. Método para ativar usuário, de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de interceptar ocorre sem que a mensagem SMS apareça para o usuário.

6. Método para ativar usuário, de acordo com a reivindicação 1, caracterizado pelo fato de que o programa de controle é compatível com o sistema operacional do EMU (1) e é executado em segundo plano.

7. Método para autenticar usuário em uma rede Wi-Fi de desvio de tráfego 3G caracterizado pelo fato de que compreende as etapas de:

solicitar (S32, S41), do EMU (1) para o servidor DHCP (3), acesso à rede Wi-Fi de desvio;

enviar (S33), do servidor DHCP (3) para o EMU (1), um número IP;

enviar (S34), do EMU (1) para o servidor de autenticação (6), um pacote TCP contendo o número IMSI, o endereço MAC, o número IP, o SSID do ponto de acesso Wi-Fi (2) ao qual está conectado, e a lista dos pontos de acesso Wi-Fi (2) detectados pelo EMU (1) com os níveis de sinal de cada ponto de acesso Wi-Fi (2) contido na lista;

verificar, pelo servidor de autenticação (6), se a formatação do número IMSI é válida;

verificar (S42) se o número IMSI consta no banco de dados (7), determinando se ele foi previamente autenticado;

identificar, pelo servidor de autenticação (6), a operadora do usuário através da identificação da operadora MCC e da identificação móvel do país MNC contidos no número IMSI;

armazenar, pelo servidor de autenticação (6) no banco de dados (7), os números MCC, MNC e MSISDN e as chaves pública e privada para validação do EMU (1);

verificar, pelo servidor de autenticação (6) no banco de dados (7) se o EMU (1) está relacionado à operadora definida pelo MNC;

verificar se é uma nova conexão ainda dentro do tempo de vida do usuário (TVU);

verificar (S47) a validade da última autenticação na base de dados (7);

enviar (S37a, S48), do servidor de autenticação (6) para o EMU (1), um código de acesso aleatório RAND, via SMS;

interceptar, pelo EMU (1), a mensagem SMS contendo o código RAND, de modo que a mensagem não apareça para o usuário;

encriptar, pelo EMU (1), o código RAND através da chave UPK;

enviar (S38), do EMU (1) para o servidor de autenticação (6), o código RAND encriptado e o número ISMI, via rede Wi-Fi;

verificar, pelo servidor de autenticação (6), se o EMU (1) é válido, através da decriptação (S47) do código RAND encriptado e da comparação (S49) do código RAND decriptado com o código RAND original;

armazenar (S39), pelo servidor de autenticação (6), o IMSI do EMU (1) no banco de dados (7) ou atualizar o prazo de validade de autenticação do EMU (1);

enviar (S310, S410), do servidor de autenticação (6) para o servidor de controle de tráfego (4), uma mensagem de liberação de acesso à rede de desvio;

verificar (S411) se o ponto de acesso Wi-Fi (2) ao qual o EMU (1) está conectado contém um número excessivo de usuários;

enviar o comando de troca e ponto de acesso Wi-Fi (2) para o EMU (1) no caso de saturação do número de usuários no ponto de acesso Wi-Fi (2) conectado ao EMU (1); e

enviar (S311, S413), do servidor de autenticação (6) para o EMU (1), uma mensagem de confirmação de autenticação.

8. Método para autenticar usuário, de acordo com a reivindicação 7, caracterizado pelo fato de que, caso o EMU (1) esteja ainda no prazo de validade de autenticação preestabelecido, o servidor de autenticação (6) somente envia (S37a, S48) um novo SMS para a verificação de autenticação de usuário se tal prazo de validade estiver próximo de expirar.

9. Método para autenticar usuário, de acordo com a reivindicação 7, caracterizado pelo fato de que é cíclico e periódico.

10. Método para autenticar usuário, de acordo com a reivindicação 7, caracterizado pelo fato de que é realizado sem acessar os bancos de dados HLR e VLR da operadora de telefonia móvel.

11. Método para autenticar usuário, de acordo com a reivindicação 7, caracterizado pelo fato de que, após a etapa de enviar (S311, S413), é criado um registro no banco de dados de gravação de eventos (8) contendo os seguintes dados: IMSI, IP, endereço MAC do EMU (1), taxa de transmissão máxima liberada, data e hora da liberação, e quantidade de Bytes trafegados de entrada e de saída.

12. Método para controlar tráfego em uma rede Wi-Fi de desvio caracterizado pelo fato de que compreende as etapas de:
liberar o acesso a um usuário;
controlar o tráfego;
controlar congestionamentos;
bloquear portas UDP/TCP;
controlar o número de acessos simultâneos; e
implementar firewall.

13. Método para controlar tráfego, de acordo com a reivindicação 12, caracterizado pelo fato de que a etapa de controlar o tráfego utiliza um filtro HTB para limitar a taxa máxima a ser liberada para o usuário.

14. Método para controlar tráfego, de acordo com a reivindicação 12, caracterizado pelo fato de que a etapa de controlar congestionamentos utiliza um processo de organização de fila SFQ.

15. Método para controlar tráfego, de acordo com a reivindicação 12, caracterizado pelo fato de que a etapa de liberar o acesso a um usuário utiliza um esquema ARPTABLES para controlar e liberar os usuários pelos seus respectivos endereços MAC e IP.

16. Método para controlar tráfego, de acordo com a reivindicação 12, caracterizado pelo fato de que os limites das velocidades de acesso são variáveis e estabelecidos conforme regras específicas de acesso.

17. Método para controlar tráfego, de acordo com a reivindicação 12, caracterizado pelo fato de que é dinâmico, sendo as regras de controle de tráfego atualizadas a cada registro do EMU (1) na rede Wi-Fi de desvio.

18. Método para controlar tráfego, de acordo com a reivindicação 12, caracterizado pelo fato de que a etapa de controlar o tráfego evita a saturação da rede por aplicações que demandam grande utilização de tráfego.

19. Método para controlar acesso de usuário em uma rede Wi-Fi de desvio de tráfego 3G caracterizado pelo fato de que compreende as etapas de:

verificar (S61) se o receptor Wi-Fi do EMU (1) está ligado;

verificar (S62) se há alguma rede Wi-Fi conectada ao EMU (1);

procurar (S63) um ponto de acesso Wi-Fi (2) com o SSID da rede de desvio da operadora, quando o EMU (1) não estiver conectado a nenhuma rede Wi-Fi ou quando o EMU (1) estiver conectado a uma rede Wi-Fi diferente da rede de desvio da operadora;

procurar (S66) um outro ponto de acesso Wi-Fi (2) com o SSID da rede de desvio da operadora, quando o EMU (1) já estiver conectado à rede de desvio da operadora;

conectar (S67), após a etapa de procurar (S63) um ponto de acesso Wi-Fi (2), o ponto de acesso Wi-Fi (2) encontrado ao EMU (1);

comparar, após a etapa de procurar (S66) um outro ponto de acesso Wi-Fi (2), o nível do sinal encontrado do ponto de acesso Wi-Fi (2) da rede de desvio com o nível de sinal da rede conectada ao EMU (1), optando pela conexão (S67) com o ponto de acesso Wi-Fi (2) com melhor nível de sinal;

verificar (S68) a existência de conexão de dados na interface Wi-Fi conectada;

autenticar (S69) usuário na rede Wi-Fi de desvio;

verificar (S611) a necessidade de o EMU (1) trocar sua conexão para um outro ponto de acesso Wi-Fi (2);

exibir mensagem de "conectado" (S610a) ou "não conectado" (S610b) no EMU (1), conforme resultado da etapa de autenticar (S69) usuário na rede Wi-Fi de desvio, em caso de verificação negativa na etapa de verificar (611);

trocar (S612) a conexão do EMU (1) para um outro ponto de acesso Wi-Fi (2), em caso de verificação positiva na etapa de verificar (611).

20. Método para controlar acesso de usuário em uma rede Wi-Fi de desvio de tráfego 3G, de acordo com a reivindicação 19, caracterizado pelo fato de que, após a etapa de exibir mensagem de "conectado" (S610a) ou "não conectado" (S610b), o método retorna para a etapa de verificar (S61) se o receptor Wi-Fi do EMU (1) está ligado.

21. Método para controlar acesso de usuário em uma rede Wi-Fi de desvio de tráfego 3G, de acordo com a reivindicação 19, caracterizado pelo fato de que, após a etapa de exibir mensagem de "não conectado" (S610b) há a possibilidade de ser exibida no EMU (1) uma mensagem de oferta de serviços.

22. Método para controlar acesso de usuário em uma rede Wi-Fi de desvio de tráfego 3G, de acordo com a reivindicação 19, caracterizado pelo fato de que a etapa de conectar (S67) o ponto de acesso Wi-Fi (2) encontrado ao EMU (1) obedece à configuração do EMU (1) em relação à prioridade de conexão entre uma rede particular conhecida do usuário e a rede de desvio da operadora.

23. Método para controlar acesso de usuário em uma rede Wi-Fi de desvio de tráfego 3G, de acordo com a reivindicação 19, caracterizado pelo fato de que o método é realizado de forma transparente ao usuário e de forma independente da operadora.

24. Método para controlar acesso de usuário em uma rede Wi-Fi de desvio de tráfego 3G, de acordo com a reivindicação 19, caracterizado pelo fato de que usuários de uma pluralidade de operadoras podem acessar a mesma rede Wi-Fi de desvio.

25. Método para controlar acesso de usuário em uma rede Wi-Fi de desvio de tráfego 3G, de acordo com a reivindicação 19, caracterizado pelo fato de que um EMU (1) com SIMCARD de uma operadora A pode adquirir plano de dados e/ou voz de uma operadora B, sendo autenticado através do SIMCARD da operadora A.

26. Sistema de desvio de tráfego 3G caracterizado pelo fato de que compreende:

pelo menos um equipamento de usuário (1) (EMU);

pelo menos um ponto de acesso Wi-Fi (2), conectados por pelo menos um comutador VLAN;

um servidor DHCP (3);

um servidor de controle de tráfego (4);

um roteador (5);

um servidor de autenticação (6);

um banco de dados de gravação de eventos (8); e

um banco de dados próprio (7).

27. Sistema de desvio de tráfego 3G, de acordo com a reivindicação 25, caracterizado pelo fato de que, ao final da utilização do sistema pelo EMU (1), ocorre o bloqueio do IP liberado para tal EMU (1) e os dados gravados no banco de dados de gravação de eventos (8) são transmitidos para a operadora do usuário.

28. Sistema de desvio de tráfego 3G, de acordo com a reivindicação 27, caracterizado pelo fato de que operadora do usuário, com base nos dados recebidos, faz a bilhetagem do usuário.

29. Sistema de desvio de tráfego 3G, de acordo com a reivindicação 27, caracterizado pelo fato de que operadora do usuário, com base nos dados recebidos, pode ofertar serviços ao usuário.

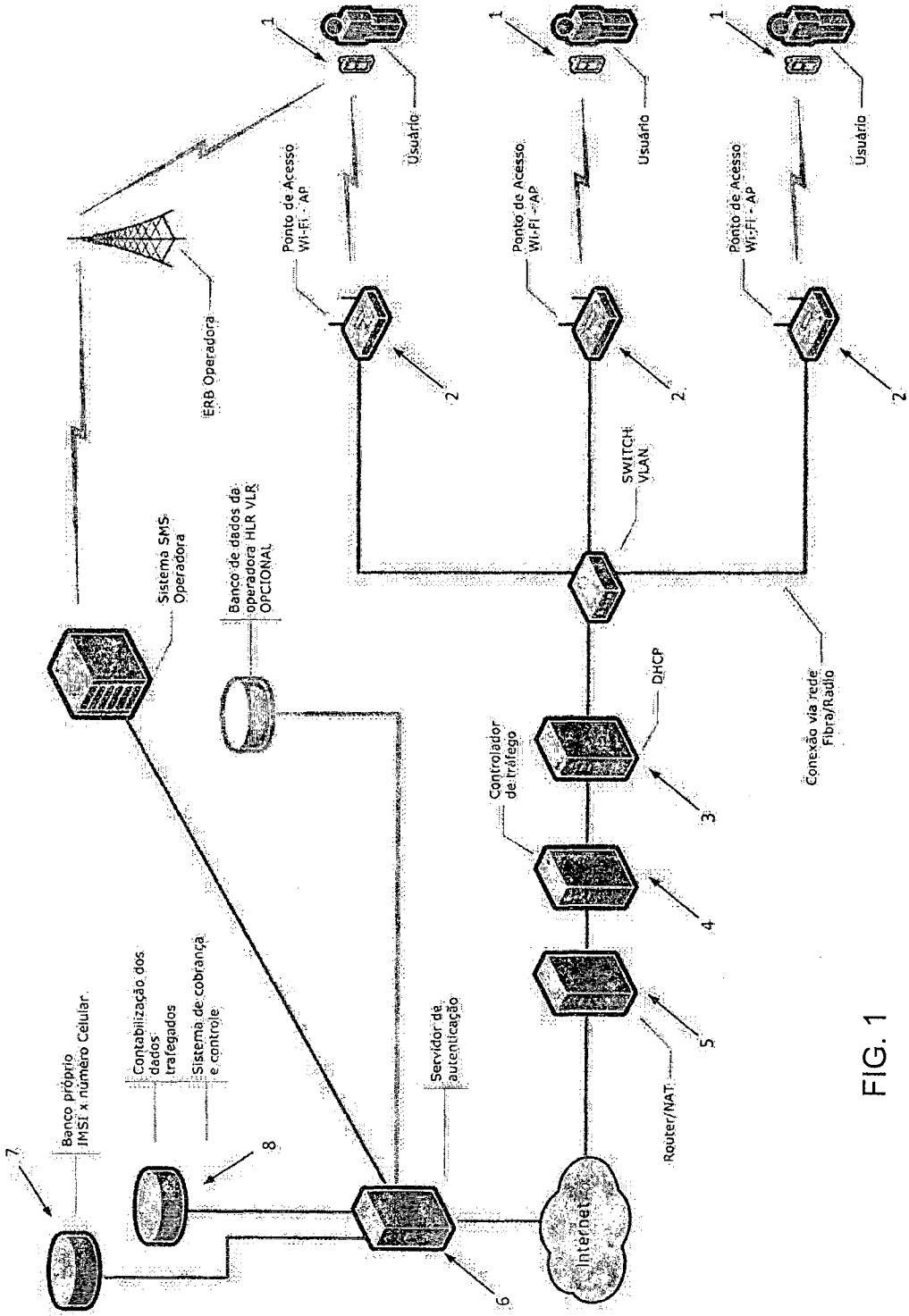
1
Usuário
Ponto de Acesso Wi-Fi - AP
2
ERB Operadora
SWITCH VLAN
Sistema SMS Operadora
Banco de dados da operadora HLR VLR OPCIONAL
Conexão via rede Fibra/Rádio
Controlador de tráfego
DHCP
3
4
5
Router/NAT
Internet
6
Servidor de autenticação
7
Banco próprio IMSI x número Celular
Contabilização dos dados trafegados
Sistema de cobrança e controle
8

FIG. 1

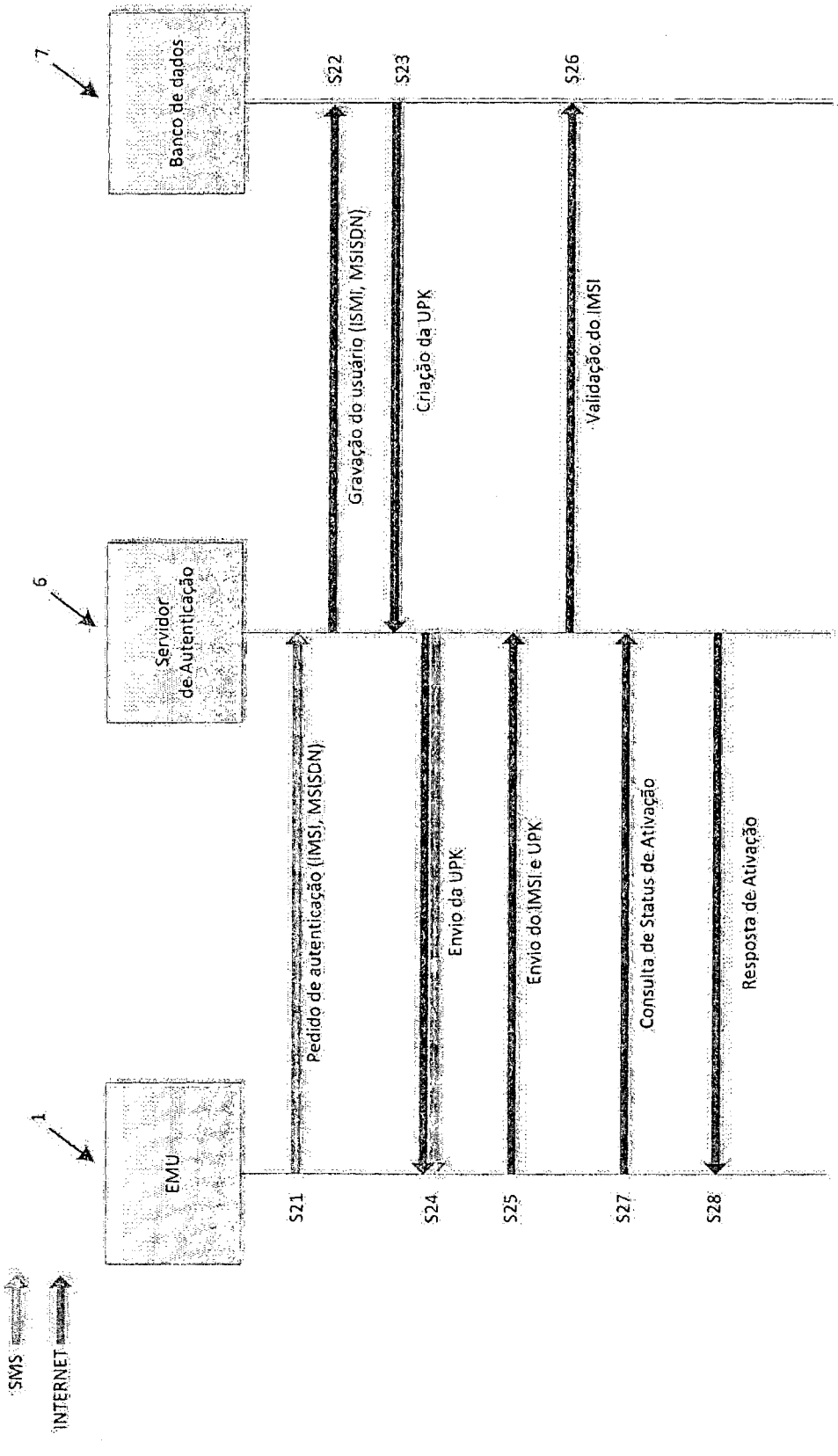
SMS
INTERNET
1
EMU
6
Servidor de Autenticação
7
Banco de dados
S21
Pedido de autenticação (IMSI, MSISDN)
S22
Gravação do usuário (ISMI, MSISDN)
S23
Criação da UPK
S24
Envio da UPK
S25
Envio do IMSI e UPK
S26
Validação do IMSI
S27
Consulta de Status de Ativação
S28
Resposta de Ativação

FIG. 2

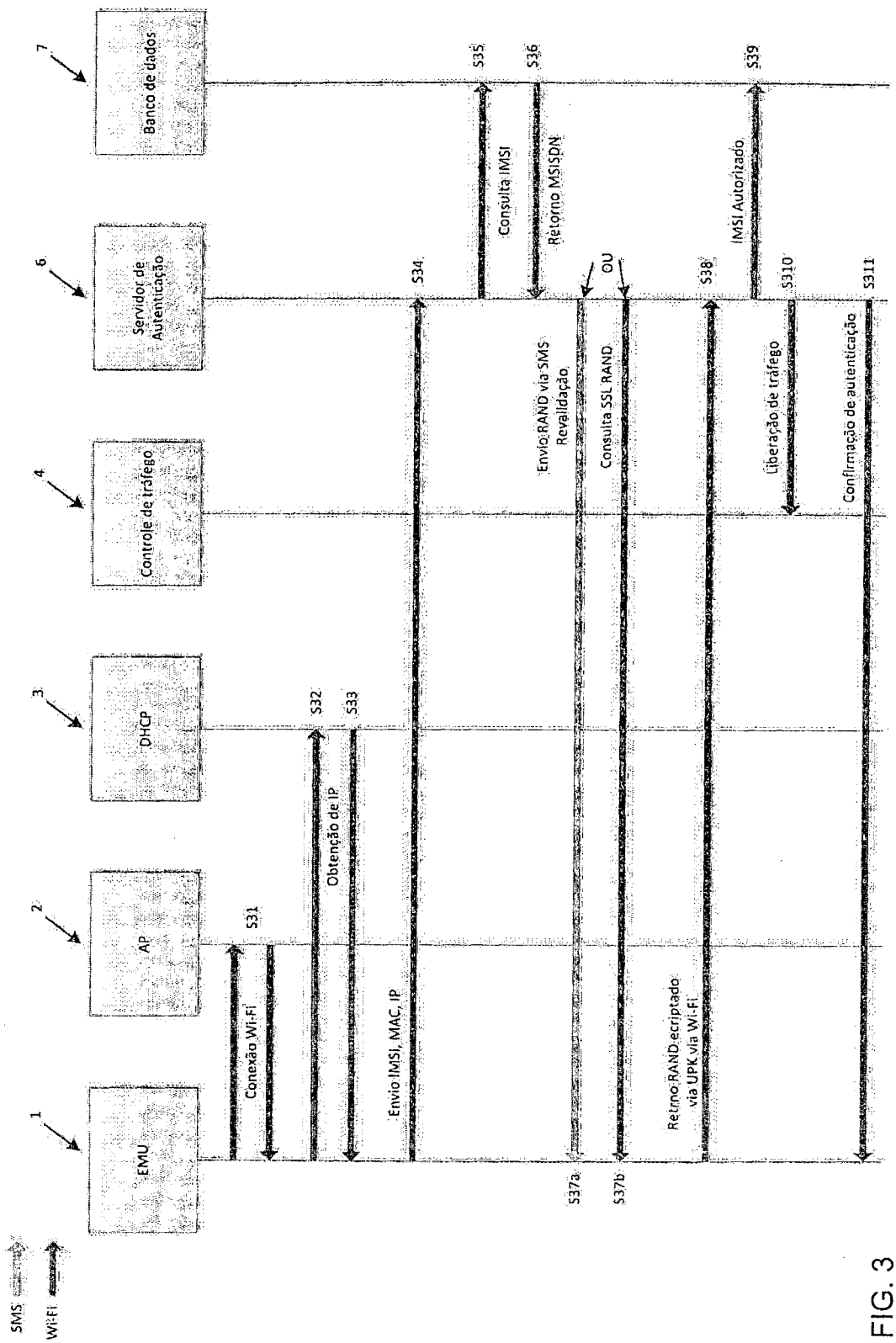
1
EMU
2
AP
3
DHCP
4
Controle de tráfego
6
Servidor de Autenticação
7
Banco de dados
SMS
Wi-Fi
S31
Conexão Wi-Fi
S32
Obtenção de IP
S33
Envio IMSI, MAC, IP
S34
S35
Consulta IMSI
S36
Retorno MSISDN
Envio RAND via SMS Revalidação
OU
Consulta SSL RAND
S37a
S37b
Retorno RAND criptado via UPK via Wi-Fi
S38
IMSI Autorizado
S39
Liberação de tráfego
S310
Confirmação de autenticação
S311

FIG. 3

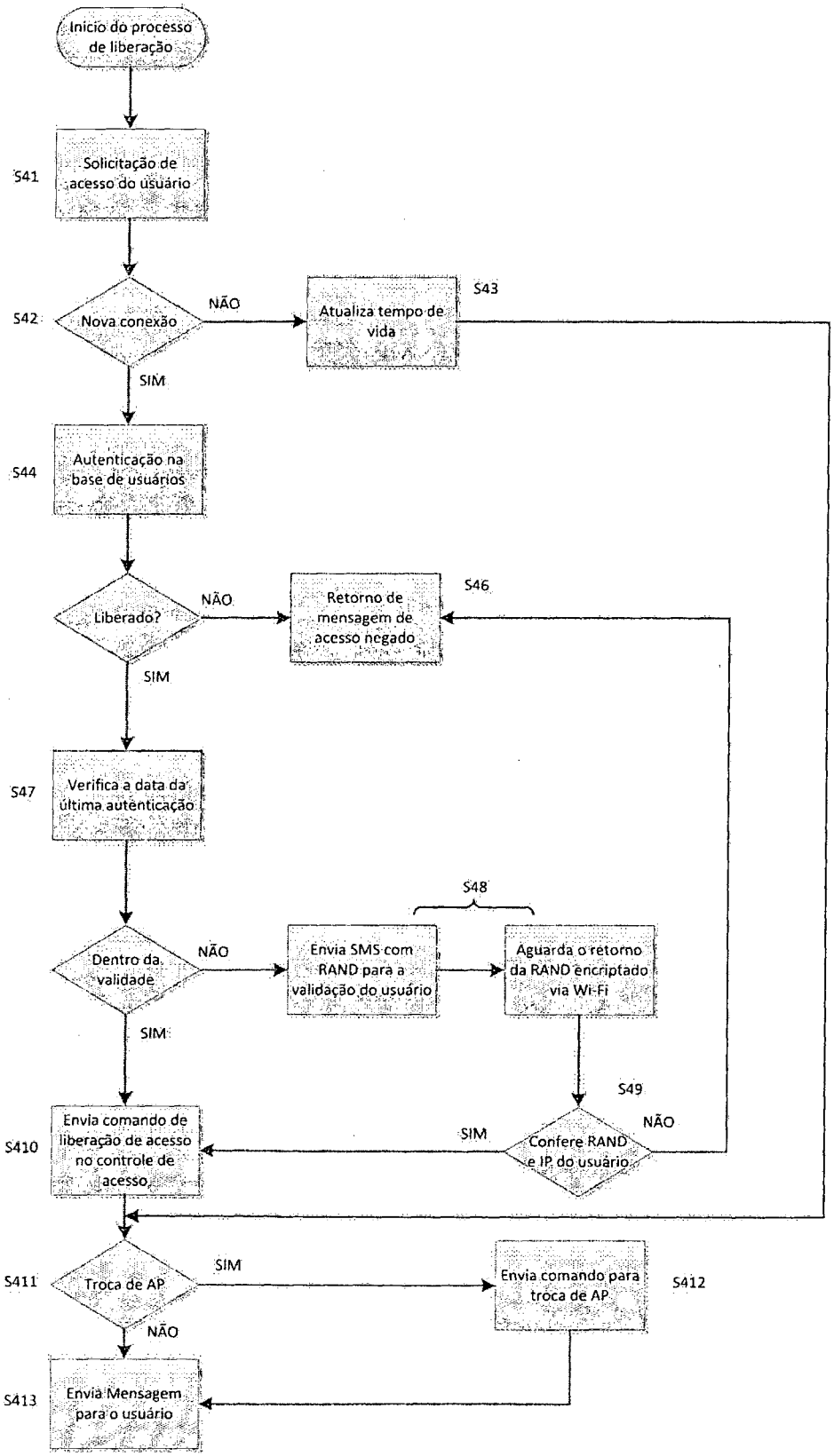
Início do processo de liberação
S41
Solicitação de acesso do usuário
S42
Nova conexão
NÃO
S43
Atualiza tempo de vida
SIM
S44
Autenticação na base de usuários
Liberado?
NÃO
S46
Retorno de mensagem de acesso negado
SIM
S47
Verifica a data da última autenticação
S48
Dentro da validade
NÃO
Envia SMS com RAND para a validação do usuário
Aguarda o retorno da RAND encriptado via Wi-Fi
SIM
S49
NÃO
SIM
S410
Envia comando de liberação de acesso no controle de acesso
Confere RAND e IP do usuário
S411
Troca de AP
SIM
Envia comando para troca de AP
S412
NÃO
S413
Envia Mensagem para o usuário

FIG. 4

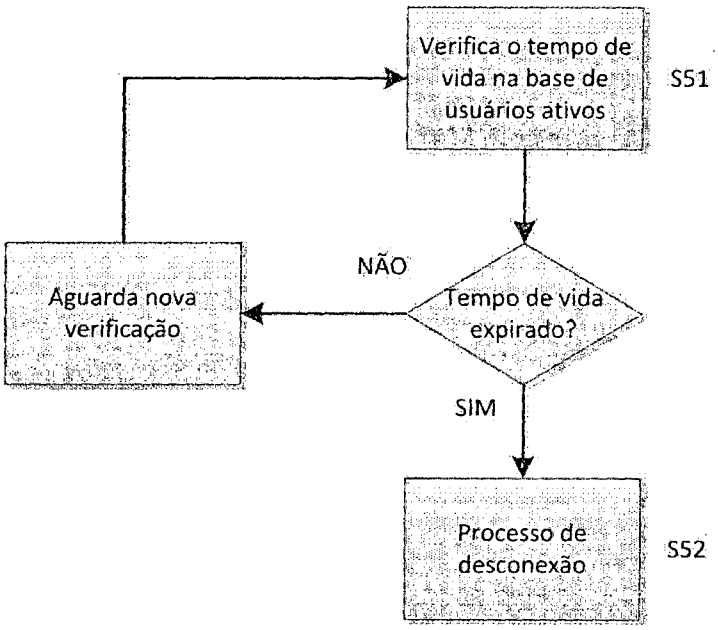
Verifica o tempo de vida na base de usuários ativos
S51
NÃO
Tempo de vida expirado?
Aguarda nova verificação
SIM
Processo de desconexão
S52

FIG. 5

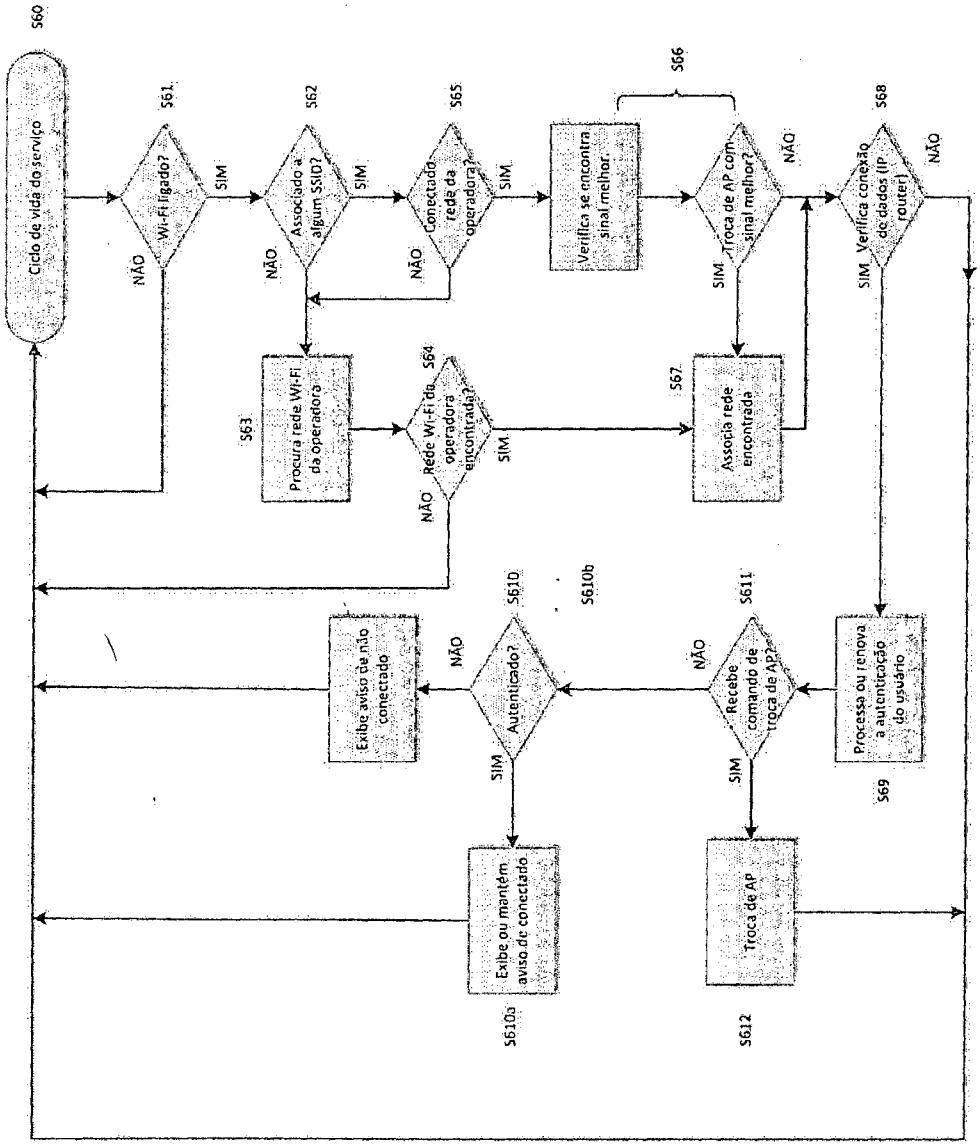
S60
Ciclo de vida do serviço
S61
Wi-Fi ligado?
SIM
NÃO
S62
Associado a algum SSID?
SIM
NÃO
S65
Conectado rede da operadora?
SIM
NÃO
S66
Verifica se encontra sinal melhor.
Troca de AP com sinal melhor?
SIM
NÃO
S68
Verifica conexão de dados (IP router)
SIM
NÃO
S63
Procura rede Wi-Fi da operadora
S64
Rede Wi-Fi da operadora encontrada?
SIM
NÃO
S67
Associa rede encontrada
S610b
S610
Autenticado?
SIM
NÃO
S611
Recebe comando de troca de AP?
SIM
NÃO
S69
Processa ou renova a autenticação do usuário
Exibe aviso de não conectado
S610a
Exibe ou mantém aviso de conectado
S612
Troca de AP

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/BR2013/000035

A. CLASSIFICATION OF SUBJECT MATTER

H04W8/10 (2009.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W e H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

H04L

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, ESPACENET

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2006052563 A2 **see abstract; page 14, line 25-page 19, line 10 claim 1; figure 10-14;** **see page 7, line 2-12; page15, line 7- page 19, line 28; figures 3, 10-14**	1 à 11; 19 à 25 12 à 18; 26 e 27
Y	EP 1924048 A1 **see abstract; page 2 col. 2, line 5 - page 3, col. 1 lilne 49 figure 3;**	1 à 11; 19 à 25
Y	WO 2011110108 A1 **see abstract, page 2, line 27 - page 3, lline 15; page 8 line 19 - page 13, line 28; figure 6-11**	12 à 18; 26 e 27

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26/04/2013	**22-05-2013**

Name and mailing address of the ISA/

INPI
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL
Rua Sao Bento nº 1, 17º andar
cep: 20090-010, Centro - Rio de Janeiro/RJ

Nº de fax: +55 21 3037-3663

Authorized officer

Elias Lawrence Marques

Telephone No. +55 21 3037-3493/3742

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/BR2013/000035

---	---	---	---

RELATÓRIO DE PESQUISA INTERNACIONAL

Depósito internacional Nº
PCT/BR2013/000035

A. CLASSIFICAÇÃO DO OBJETO

H04W8/10 (2009.01)

De acordo com a Classificação Internacional de Patentes (IPC) ou conforme a classificação nacional e IPC

B. DOMÍNIOS ABRANGIDOS PELA PESQUISA

Documentação mínima pesquisada (sistema de classificação seguido pelo símbolo da classificação)

H04W e H04B

Documentação adicional pesquisada, além da mínima, na medida em que tais documentos estão incluídos nos domínios pesquisados

H04L

Base de dados eletrônica consultada durante a pesquisa internacional (nome da base de dados e, se necessário, termos usados na pesquisa)

EPODOC, ESPACENET

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoria*	Documentos citados, com indicação de partes relevantes, se apropriado	Relevante para as reivindicações Nº
Y	WO 2006052563 A2 Ver "abstract"; página 14, linha 25 – página 19, linha 10; reivindicações 1; Figuras 10 – 14;	1 à 11; 19 à 25
	Ver página 7, linhas 2 – 12; página 15, linha 7 – página 19, linha 28; Figuras 3, 10 – 14;	12 à 18; 26 e 27
Y	EP 1924048 A1 Ver "abstract"; página 2, coluna 2, linha 5 – página 3, coluna 1, linha 49; figura 3;	1 à 11; 19 à 25
Y	WO 2011110108 A1 Ver "abstract"; página 2, linha 27 - página 3, linha 15; página 8, linha 19 – página 13, linha 28; figura 6 - 11.	12 à 18; 26 e 27

☐ Documentos adicionais estão listados na continuação do quadro C ☐ Ver o anexo de famílias das patentes

* Categorias especiais dos documentos citados:

"A" documento que define o estado geral da técnica, mas não é considerado de particular relevância.

"E" pedido ou patente anterior, mas publicada após ou na data do depósito internacional

"L" documento que pode lançar dúvida na(s) reivindicação(ões) de prioridade ou na qual é citado para determinar a data de outra citação ou por outra razão especial

"O" documento referente a uma divulgação oral, uso, exibição ou por outros meios.

"P" documento publicado antes do depósito internacional, porém posterior a data de prioridade reivindicada.

"T" documento publicado depois da data de depósito internacional, ou de prioridade e que não conflita com o depósito, porém citado para entender o princípio ou teoria na qual se baseia a invenção.

"X" documento de particular relevância; a invenção reivindicada não pode ser considerada nova e não pode ser considerada envolver uma atividade inventiva quando o documento é considerado isoladamente.

"Y" documento de particular relevância; a invenção reivindicada não pode ser considerada envolver atividade inventiva quando o documento é combinado com um outro documento ou mais de um, tal combinação sendo óbvia para um técnico no assunto.

"&" documento membro da mesma família de patentes.

Data da conclusão da pesquisa internacional	Data do envio do relatório de pesquisa internacional:
26/04/2013	220513

Nome e endereço postal da ISA/**BR**	Funcionário autorizado
INPI INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL Rua Sao Bento nº 1, 17º andar cep: 20090-010, Centro - Rio de Janeiro/RJ	**Elias Lawrence Marques**
Nº de fax: +55 21 3037-3663	Nº de telefone: +55 21 3037-3493/3742

RELATÓRIO DE PESQUISA INTERNACIONAL

Informação relativa a membros da família da patentes

Depósito internacional Nº
PCT/BR2013/000035

Documentos de patente citados no relatório de pesquisa	Data de publicação	Membro(s) da família de patentes	Data de publicação
---	---	---	---