



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

(11) PI 0607120-1 B1



(22) Data do Depósito: 30/01/2006

(45) Data de Concessão: 16/04/2019

(54) Título: MÉTODO PARA FORNECER SEGURANÇA EM UMA REDE DE ACESSO MÓVEL, DISPOSITIVO DE MEMÓRIA LEGÍVEL POR COMPUTADOR, CONTROLADOR DE REDE, E, SISTEMA EM UMA REDE DE ACESSO MÓVEL

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

(52) CPC: H04W 12/10; H04L 63/0272; H04L 63/126; H04L 63/164.

(30) Prioridade Unionista: 01/02/2005 US 11/047880.

(73) Titular(es): TELEFONAKTIEBOLAGET LM ERICSSON (PUBL).

(72) Inventor(es): TOMAS NYLANDER; JARI TAPIO VIKBERG.

(86) Pedido PCT: PCT IB2006000165 de 30/01/2006

(87) Publicação PCT: WO 2006/082489 de 10/08/2006

(85) Data do Início da Fase Nacional: 01/08/2007

(57) Resumo: MÉTODO PARA FORNECER SEGURANÇA EM UMA REDE DE ACESSO MÓVEL, PROGRAMA DE COMPUTADOR PARA PROTEGER UM NÚCLEO DE REDE, CONTROLADOR DE REDE, E, SISTEMA EM UMA REDE DE ACESSO MÓVEL. A presente invenção propicia um método, sistema, e aparelho para fornecer segurança em uma rede de acesso móvel não licenciada ou uma rede de acesso genérica, através da recepção de uma mensagem contendo uma identidade móvel de uma estação móvel (MS), e do descarte ou da rejeição da mensagem sempre que a dita identidade móvel recebida não coincidir com uma identidade móvel armazenada associada com a MS. A mensagem é processada sempre que tal identidade móvel recebida coincidir com tal identidade móvel armazenada associada com a MS. A identidade móvel armazenada é fornecida por meio de um ponto de conexão seguro. A identidade móvel pode ser uma Identidade de Assinante Móvel Internacional, Identidade de Assinante Móvel Temporária, Identidade de Assinante Móvel Temporária por Pacote, endereço de Protocolo de Internet (IIP) privado ou endereço IIP público. A mensagem pode ser uma solicitação de registro, uma mensagem de ligação ascendente, ou uma mensagem de ligação descendente, tal como uma mensagem de Gerenciamento de Mobilidade, uma mensagem de Gerenciamento de Mobilidade de Serviço (...).

**MÉTODO PARA FORNECER SEGURANÇA EM UMA REDE DE ACESSO MÓVEL,
DISPOSITIVO DE MEMÓRIA LEGÍVEL POR COMPUTADOR, CONTROLADOR DE
REDE, E, SISTEMA EM UMA REDE DE ACESSO MÓVEL**

CAMPO DA INVENÇÃO

[001] A presente invenção se refere, em geral, ao campo de comunicações móveis e, mais particularmente, a um método, sistema e aparelho para fornecer segurança em uma rede de acesso móvel não licenciada ou uma rede de acesso genérica.

FUNDAMENTOS DA INVENÇÃO

[002] Os relatórios descritivos de acesso móvel não licenciado (UMA) recomendam que o controlador de rede não licenciado (UNC) e o *gateway* seguro de controlador de rede não licenciado (UNC-SGW) deve verificar que a mesma Identidade de Assinante Móvel Internacional (IMSI) é usado quando uma estação móvel (MS) estabelece a conexão segura IPsec em direção ao UNC-SGW e quando o MS se cadastra no UNC. Em ambos estes momentos, o MS fornece o IMSI para o UNC-SGW e UNC, respectivamente. Os relatórios descritivos, UMA, contudo não definem como essas verificações devem ser feitas. Ainda, a implementação dessas recomendações ainda deixa o núcleo da rede aberto a ataques.

[003] Este é também o caso nos padrões da Projeto de Parceria para a Terceira Geração (3GPP) para "Acesso Genérico a interface A e Gb", por outro lado conhecido como uma Rede de Acesso Genérico (GAN). Ver Especificações Técnicas 43.318 (Estágio-2) e 44.318 (Estágio-3). Note que o controlador de rede de acesso genérico (GANC) nas especificações é . equivalente ao UNC nas especificações UMA. Similarmente, o *gateway* seguro de controlador de rede de acesso genérico (GANC-SEGW) nas especificações 3GPP é equivalente ao UNC-SGW nas especificações UMA.

[004] O pedido de patente Publicado 2003/065952 A1 OTSUKA NAOKI 3 de abril de 2003 (03/04/2003) parece para descrever um sistema de autenticação onde um usuário ao invés de um gerenciador de sistema pode facilmente registrar terminais selecionados como terminais autênticos. O usuário seleciona os terminais a serem registrados como autênticos usando um dispositivo de autenticação que exibe informação de identificação para os terminais ao usuário. Após isso, quando uma solicitação de serviço de um terminal é recebida por um periférico multifuncional, que é ambos um dispositivo de fornecimento de serviço e um dispositivo de autenticação de serviço, a lista de registro é verificada para ver se o terminal é autêntico e o serviço é concedido se o terminal estiver na lista de registro ou é negado se o terminal não estiver na lista de registro.

[005] Por exemplo, uma MS pode usar múltiplos Identificadores de Assinante Móveis Temporários (TMSI) ou Identificadores de Assinante Móveis Temporários por pacote (P-TMSI) para emular múltiplos MSs, tais com um computador pessoal (PC) com uma leitora de cartão SIM e um cliente de UMA. Mais ainda, uma MS hostil pode enviar mensagens de Atualizações de Localização ou de IMSI Detach em direção ao núcleo da rede causando um tipo de ataque de negação de serviço (DOS) no nível de MS (chamadas terminando cairiam, etc.). Consequentemente, há uma necessidade para um método e aparelho que proteja o núcleo da rede verificando as identidades móveis (IMSI, TMSI, elou P-TMSI) usadas pelas estações móveis quando elas se comunicam com o núcleo da rede.

SUMÁRIO DA INVENÇÃO

[006] A presente invenção fornece um método, sistema e aparelho que efetuam as verificações de segurança recomendadas pelo controlador de rede não licenciado (UNC) ou o controlador de rede de acesso genérico (GANC) e o

gateway seguro para o controlador de rede não licenciado (UNC-SGW) ou o controlador de rede de acesso genérico (GANCSEGW). A presente invenção fornece uma solução otimizada que minimiza as atividades de O&M necessárias, suporta para muitos cenários diferentes de rede e pode ser facilmente padronizada. Note que a presente invenção é aplicável para ambas redes de acesso móvel não licenciadas (UMAN) e redes de acesso genérico (GAN).

[007] Mais especificamente, a presente invenção introduz um novo protocolo entre o UNC e o UNC-SGW ou o GANC e o GANC-SEGW baseado em transmissão confiável que inclui tratamento dinâmico das conexões entre UNC-SGWs e UNCs ou o GANC-SEGWs e GANCs. Em essência, o UNC-SGW ou GANC-SEGW salva alguns dados no estabelecimento de túnel IPsec e verifica a comunicação entre o MS e o UNC e GANC. Quando uma conexão TCP é estabelecida entre uma MS e um UNC ou GANC, o UNC-SGW ou GANC-SEGW pode estabelecer uma outra conexão TCP em direção àquela UNC ou GANC e envia a informação necessária somente para aquele UNC ou GANC. O UNC ou GANC pode então verificar que a informação usada no estabelecimento de túnel IPsec (autenticação EAP-SIM ou EAP-AKA) e no cadastro são as mesmas. A presente invenção também fornece o benefício adicionado que o endereço IP público para o MS é fornecido para o UNC ou GANC.

[008] Em adição, a presente invenção pode ser usada para proteger o núcleo da rede através da verificação das identidades móveis (Identidade de Assinante Móvel Internacional (IMSI), Identificadores de Assinante Móveis Temporários (TMSI) e/ou Identificadores de Assinante Móveis Temporários por pacote (P-TMSI) usadas por estações móveis (MS) quando elas se comunicam com o núcleo da rede. Simplesmente declarado, mensagem que contém um identificador móvel que não corresponde a um identificador móvel armazenado associado com a MS (após cadastro), são descartados. Uma vez tal mensagem é

descartada, várias ações preventivas e de reporte podem ser tomadas. Para a MS é, por conseguinte, somente permitida o uso de uma IMSI, uma TMSI e uma P-TMSI. Como um resultado, a presente invenção protege o núcleo da rede de implementações de MS falhas e maliciosas.

[009] Como um resultado, a presente invenção também fornece um método para fornecer segurança em uma rede de acesso móvel não licenciada através da recepção de uma mensagem contendo uma identidade móvel de uma MS e descartando ou rejeitando a mensagem sempre que a identidade móvel recebida não coincidir com uma identidade móvel armazenada associada com a MS. A mensagem é processada sempre que a identidade móvel recebida coincide com a identidade móvel armazenada associada com a MS. A identidade móvel pode ser uma IMSI, uma TMSI, uma P-TMSI, um endereço (IP) de Protocolo de Internet privado ou um endereço IP público. A mensagem pode ser uma solicitação de cadastro, uma mensagem de enlace ascendente, ou uma mensagem de enlace descendente, tal como uma mensagem de Gerenciamento de Mobilidade (MM), uma mensagem de Serviço de Rádio por pacote Geral (GPRS) Gerenciamento de Mobilidade (GMM), ou uma mensagem de UMA ou Recursos de Rádio Não licenciados (URR) (somente usado entre MS e UNC). A presente invenção pode ser implementada como um programa de computador incorporado em um meio legível por computador onde os vários passos do método são implementados por um ou mais segmentos de código.

[010] Em adição, a presente invenção fornece um aparelho que inclui um dispositivo de armazenamento de dados, de forma comunicável, acoplado a um processador. O dispositivo de armazenamento de dados armazena associações de identidades móveis para MSS. O processador recebe uma mensagem contendo uma identidade móvel de uma MS e descarta ou rejeita a mensagem sempre que a identidade móvel recebida não coincidir com uma identidade

móvel armazenada associada com a MS. O aparelho é tipicamente um controlador de rede não licenciado (UNC) dentro de uma rede de acesso móvel não licenciada (UMAN) ou um controlador de rede de acesso genérico (GANC) dentro de uma rede de acesso genérico (GAN) que está em comunicação com o núcleo da rede.

[011] A presente invenção também fornece um sistema que inclui uma estação móvel, um *gateway* seguro e um controlador de rede não licenciado. O *gateway* seguro é acoplado de forma comunicável à estação móvel. O controlador de rede não licenciado é acoplado de forma comunicável à estação móvel e ao *gateway* seguro. O *gateway* seguro recebe informação de identidade móvel proveniente da estação móvel e envia a informação de identidade móvel para um controlador de rede não licenciado. O controlador de rede não licenciado armazena a informação de identidade móvel recebida e cadastra a estação móvel sempre que uma identidade móvel dentro de uma solicitação de cadastro, recebida da estação móvel, coincidir com a informação de identidade móvel armazenada. O *gateway* seguro é configurado com uma ou mais portas de Protocolo de Controle de Transmissão (TCP) definidas usadas pelo controlador de rede não licenciado para cadastrar a estação móvel, e o controlador de rede não licenciado espera por uma conexão TCP entrante em uma ou mais portas TCP definidas. Em uma modalidade, o *gateway* seguro assegura que a solicitação de cadastro não seja recebida pelo controlador de rede não licenciado até que uma mensagem seja recebida proveniente do controlador de rede não licenciado indicando recepção bem sucedida e armazenamento da informação de identidade móvel. Em uma outra modalidade, o controlador de rede não licenciado usa a informação de identidade móvel para fornecer um ou mais serviços para a estação móvel. Com previamente mencionado, o controlador de rede não licenciado pode ser um controlador de

rede de acesso genérico.

BREVE DESCRIÇÃO DOS DESENHOS

[012] As vantagens acima e outras da invenção podem ser entendidas de maneira melhor se referindo a descrição a seguir em conjunto com os desenhos anexados, nos quais:

FIGURA 1 é uma sequência de sinalização representativa descrevendo o uso de identidades móveis entre uma rede UMA e um núcleo de rede;

FIGURA 2 é um diagrama descrevendo os endereços IP diferentes usados por uma estação móvel;

FIGURAS 3A, 3B, 3C, 3D e 3E são diagramas de bloco descrevendo cenários de rede diferentes da relação entre controladores de rede não licenciados e *gateways* seguros para controladores de rede não licenciados nos quais a presente invenção pode ser usada;

FIGURA 4 é um fluxograma descrevendo um método de proteger um núcleo de rede de acordo com a presente invenção;

FIGURA 5 é um diagrama descrevendo uma configuração inicial para uma modalidade da presente invenção;

FIGURA 6 é uma sequência de sinalização descrevendo o uso de uma modalidade da presente invenção;

FIGURA 7A, 7B e 7C são fluxogramas descrevendo um método de acordo com uma modalidade da presente invenção como é usado em um *gateway* seguro para um controlador de rede não licenciado;

FIGURA 8 é um fluxograma descrevendo um método de acordo com uma modalidade da presente invenção como é usado em um controlador de rede não licenciado;

FIGURA 9 é uma sequência de sinalização descrevendo o uso de uma modalidade da presente invenção com respeito a mensagens de enlace

ascendente;

FIGURA 10 é uma sequência de sinalização descrevendo o uso de uma modalidade da presente invenção com respeito a mensagens de enlace descendente;

FIGURA 11 é um fluxograma descrevendo um método de acordo com uma modalidade da presente invenção com respeito a mensagens de enlace ascendente;

FIGURA 12 é um fluxograma descrevendo um método de acordo com uma modalidade da presente invenção com respeito a mensagens de enlace descendente; e

FIGURA 13 é um fluxograma descrevendo um método de acordo com uma outra modalidade da presente invenção com respeito a mensagens de enlace descendente.

DESCRIÇÃO DETALHADA DA INVENÇÃO

[013] Enquanto o fazer e o usar de várias modalidades da presente invenção é discutido em detalhes a seguir, deve ser apreciado que a presente invenção fornece muitos conceitos inventivos aplicáveis que podem ser incorporados em uma larga variedade de contextos específicos. As modalidades específicas discutidas aqui são meramente ilustrativas de maneiras específicas de fazer e usar a invenção e não delimitam o escopo da invenção.

[014] Para facilitar o entendimento desta invenção, um número de termos é definido abaixo. Termos definidos aqui têm significados como comumente entendido por uma pessoa de habilidade simples nas áreas relevantes para a presente invenção. Termos tais como "um", "uma" e "o" não são pretendidos para se referirem a somente uma entidade singular, mas inclui a classe geral da qual um exemplo específico pode ser usado para ilustração. A terminologia aqui é usada para descrever modalidades específicas da invenção,

mas seus usos não delimitam a invenção, exceto como evidenciado nas reivindicações.

[015] A presente invenção fornece um método, sistema e aparelho que efetuam as verificações de segurança recomendadas pelo controlador de rede não licenciado (UNC) ou o controlador de rede de acesso genérico (GANC) e o *gateway* seguro para o controlador de rede não licenciado (UNC-SGW) ou o controlador de rede de acesso genérico (GANC-SEGW). A presente invenção fornece uma solução otimizada que minimiza as atividades de O&M necessárias, suporta para muitos cenários diferentes de rede e pode ser facilmente padronizada. Note que a presente invenção é aplicável para ambas redes de acesso móvel não licenciadas (UMAN) e redes de acesso genérico (GAN).

[016] Mais especificamente, a presente invenção introduz um novo protocolo entre o UNC e o UNC-SGW ou o GANC e o GANC-SEGW baseado em transmissão confiável que inclui tratamento dinâmico das conexões entre UNC-SGWs e UNCs ou o GANC-SEGWs e GANCs. Em essência, o UNC-SGW ou GANC-SEGW salva dados no estabelecimento de túnel IPsec e verifica a comunicação entre o MS e o UNC e GANC. Quando uma conexão TCP é estabelecida entre uma MS e um UNC ou GANC, UNC-SGW ou GANC-SEGW pode estabelecer uma outra conexão TCP em direção àquela UNC ou GANC e envia a informação necessária somente para aquele UNC ou GANC. O UNC ou GANC pode então verificar que a informação usada no estabelecimento de túnel IPsec (autenticação EAP-SIM ou EAP-AKA) e no cadastro são as mesmas. A presente invenção também fornece o benefício adicionado que o endereço IP público para o MS é fornecido para o UNC ou GANC.

[017] Em adição, a presente invenção pode ser usada para proteger o núcleo da rede através da verificação das identidades móveis (Identidade de Assinante Móvel Internacional (IMSI), Identificadores de Assinante Móveis

Temporários (TMSI) e/ou Identificadores de Assinante Móveis Temporários por pacote (P-TMSI) usadas por estações móveis (MS) quando elas se comunicam com o núcleo da rede. Simplesmente declarado, são descartadas mensagens que contém um identificador móvel que não corresponde a um identificador móvel armazenado associado com a MS (após cadastro). Uma vez que tal mensagem é descartada, várias ações preventivas e de reporte podem ser tomadas. Para a MS é, por conseguinte, somente permitida o uso de uma IMSI, uma TMSI e uma P-TMSI. Como um resultado, a presente invenção protege o núcleo da rede de implementações de MS falhas e maliciosas.

[018] Agora se referindo a FIGURA 1, uma sequência de sinalização representativa descrevendo o uso de identidades móveis entre uma rede UMA ou uma rede de acesso genérico (GAN) 100 e um núcleo de rede 102 é mostrado. O MS 104 fornece o IMSI para o *gateway* seguro do controlador de rede não licenciado (UNC-SGW) ou controlador de rede de acesso genérico (GANC-SEGW) 106 usando EAP-SIM ou EAP-AKA quando o MS 104 estabelece a conexão segura IPsec 108 em direção ao UNC-SGW ou GANC-SEGW 106. O UNC-SGW ou GANC-SEGW 106 autentica 110 estes IMSI no HLR 110 usando protocolos de sinalização e autorização bem conhecidos (infraestrutura (AAA) de autenticação, autorização e auditoria 114). O MS 104 também fornece o IMSI para o controlador de rede não licenciado (UNC) ou controlador de rede de acesso genérico (GANC) 116 quando o MS 104 cadastra 118 com o UNC ou GANC 116. Em adição, o MS 104 usa IMSI, TMSI ou P-TMSI para identificar ele próprio, quando o MS 104 se comunica 120 com o núcleo da rede 102 (e.g. MSC 112).

[019] Note que os TMSI e P-TMSI não são reportados ao UNC ou GANC 116 quando cadastrando 118. Os TMSI e P-TMSI têm significância somente dentro de uma área de localização. Fora dessa área de localização, o TMSI e P-TMSI tem de ser combinados com o Identificador de Área de Localização (LAI)

para fornecer uma identidade não ambígua. Usualmente as realocações de TMSI e P-TMSI são efetuadas pelo menos em cada mudança de uma área de locação. Tais escolhas são deixadas para o operador da rede.

[020] Identidade móvel é usada na seguinte mensagem de Gerenciamento de Mobilidade (MM) entre o MS 104 e o MSC/Cadastro de Localização de Visitante (VLR) 112.

Do MS 104 para o MSV/VLR 112 (mensagens de enlace ascendente):

LOCATION UPDATING REQUEST

IDENTITY RESPONSE

CM SERVICE REQUEST

IMSI DETACH DDICATION

CM RE-ESTABLISHMENT REQUEST

Do MSC/VLR 112 para o MS 104 (mensagens de enlace descendente):

TMSI REALLOCATION COMMAND

LOCATION UPDATING ACCEPT

[021] Identidade móvel também é usada na mensagem PAGING RESPONSE do MS 104 para o MSC/VLR 112. O UNC ou GANC 116 pode, por conseguinte, efetuar verificação em Mensagens MM enviadas entre o MS 104 e MSC/VLR 112.

[022] Referindo agora a FIGURA 2, um diagrama descrevendo os endereços IP diferentes usados por uma estação móvel 104 é mostrado. Como previamente mencionado, a presente invenção resolve o problema de pegar os endereços IP públicos da MS 104 par ao UNC ou GANC 116. Alguns operadores terão uma rede IP gerenciada e terão controle dos endereços IP públicos atribuídos para seus usuários (e.g., para o modem de TV a cabo) de modo que eles possam priorizar tráfego de voz em suas redes. O endereço IP público pode também ser usado para serviços de localização e cobrança (como HomeZone).

O(s) endereço(s) IP público(s) (i.e., externo(s)) 200 são somente usados entre MS 104 e o UNC-SGW ou GANC-SEGW 106 e não são visíveis no UNC ou GANC 116. MS 104 usa um endereço IP privado (i.e., interno) 202 na comunicação com o UNC ou GANC 116.

[023] O UNC ou GANC 116 precisa achar o endereço IP público do MS 104 200 de modo a fornecer qualidade de serviço (QoS), serviços de localização, cobrança, etc. Por exemplo, o UNC ou GANC 116 pode usar a informação de "registro" recebida (MS 104 e endereços IP públicos 106 de UNC-SGW ou GANC-SEGW) (que serão descritos abaixo) em direção a um Servidor de Políticas (e.g., usando COPS) para garantir QoS na(s) rede(s) entre o MS 104 e o UNC-SGW ou GANC-SEGW 106. Para serviços de localização, o UNC ou GANC 116 pode contatar um servidor externo que pode retornar a informação de localização para um endereço IP público (e.g., latitude/longitude). Esta informação pode então ser usada contra o núcleo de rede 102 para serviços de localização. Para cobrança, o UNC ou GANC 116 pode contatar um servidor externo que pode retornar a informação de localização para um endereço IP público para descobrir se o MS 104 está nas premissas originais (i.e., não em um foco recente). Esta informação pode então ser usado contra o núcleo de rede 102 para cobrança diferenciada (um outro CGI é indicado em direção ao núcleo de rede 102). Este novo protocolo entre o UNC-SGW 106 e UNC 116 ou GANC-SEGW 106 e GANC 116 pode ser usado e aprimorado para muitos outros propósitos da mesma forma. (e.g. gerenciamento de largura de banda para ver se o MS 104 deve ser redirecionado para um outro UNC-SGW ou GANC-SEGW 106).

[024] A(O) "conexão UNC ou GANC"/novo protocolo, como será descrita(o) abaixo, pode também ser usado para indicar ao UNC-SGW ou GANC-SEGW 106 que a conexão IPsec deve ser desconectada em caso de não coincidência. O UNC ou GANC 116 pode também notificar o servidor AAA 114

que o IMSI particular usado em EAP-SIM ou EAP-AKA estava sendo usado para ações hostis e o IMSI pode ser colocado na lista negra (se assim desejado pelo operador). Em adição, a "conexão UNC ou GANC"/novo protocolo pode também ser usado(a) pelo UNC-SGW ou GANC-SEGW 106 para indicar ao UNC ou GANC 116 que uma conexão IPsec foi desconectada. Isto também pode ser usado no lugar do mecanismo ativo de conservação do nível de aplicação, que alivia o nível de aplicação de sua obrigação (e.g. o procedimento ativo de conservação de nível de aplicação pode usar intervalos muito altos).

[025] Agora referindo as FIGURAS 3A, 3B, 3C, 3D e 3E, diagramas de bloco descrevendo cenários de rede diferentes da relação entre controladores de rede não licenciada e *gateway* seguro para controladores de rede não licenciados na qual a presente invenção pode ser usada, são mostrados. No caso de cenário de rede mais simples (FIGURA 3A), a relação entre UNC-SGW e UNC ou GANC-SEGW e GANC é 1:1. Neste caso, o problema nesta solução pode ser simples de tratar, i.e., cada UNC-SGW ou GANC-SEGW conhece exatamente para qual UNC ou GANC enviar a informação necessária ou que cada UNC ou GANC conhece exatamente que UNC-SGW ou GANC-SEGW perguntar sobre a informação. A O&M necessária para este cenário é simples. Ou o UNC-SGW ou GANC-SEGW é configurado com a informação sobre o UNC ou GANC, ou do outro jeito.

[026] Em um outro caso de cenário de rede (FIGURA 3B), a relação entre UNC-SGWs e UNCs ou GANC-SEGWs e GANCs é n:1 (i.e., múltiplos UNC-SGWs servindo um UNC ou múltiplos GANC-SEGWs servindo um GANC). Neste caso, o problema nesta solução é ainda bem simples de tratar, i.e., cada UNC-SGW ou GANC-SEGW conhece exatamente para qual UNCs ou GANCs enviar a informação necessária ou, que cada UNC ou GANC conhece exatamente que UNC-SGW ou GANCSEGW perguntar sobre a informação. O&M necessária para esse cenário é complexa. Ou os UNC-SGWs ou GANC-SEGWs são configurados,

com a informação sobre o UNC ou GANC ou que o UNC ou GANC é configurado com a informação sobre todos os UNC-SGWs ou GANC-SEGWs.

[027] Em ainda um outro caso de cenário de rede (FIGURA 3C), a relação entre UNC-SGW e ou GANC-SEGW e GANC é 1:n (i.e., um UNC-SGW servindo para múltiplos ou um GANC-SEGW servindo para múltiplos GANCs). Neste caso, o problema nesta solução é ainda bem simples de tratar, i.e., cada UNC-SGW ou GANC-SEGW conhece exatamente para qual UNCs ou GANCs enviar a informação necessária ou, que cada UNC ou GANC conhece exatamente que UNC-SGW ou GANC SEGW para perguntar sobre a informação. O&M necessária para esse cenário é bem complexa. Ou o UNC-SGW ou GANC-SEGW é configurado, com a informação sobre todos os UNCs ou GANCs ou que cada UNC ou GANC é configurado com a informação sobre o UNC-SGW ou GANC-SEGW.

[028] No mais complexo caso de cenário de rede (FIGURA 3D e 3E), a relação entre UNC-SGWs e UNCs ou GANC-SEGWs e GANCs é x:y (i.e., múltiplos UNC-SGWs servindo múltiplos UNCs ou múltiplos GANC-SEGWs servindo múltiplos GANCs). Neste caso, o problema nesta solução não é simples de tratar, i.e., cada UNC-SGW ou GANC-SEGW deveria conhecer para qual UNCs ou GANCs enviar a informação necessária ou, que cada UNC ou GANC deveria conhecer todos os possíveis UNC-SGWs ou GANC-SEGWs para perguntar sobre a informação. O&M necessária para esse cenário é complexa. Ou os UNC-SGWs ou GANC-SEGWs são configurados com a informação sobre todos os UNCs ou GANCs, ou que todos UNCs ou GANCs são configurados com a informação sobre todos os UNC-SGWs ou GANC-SEGWs. A presente invenção endereça e resolve todos esses cenários.

[029] Referindo agora para a FIGURA 4, um fluxograma descrevendo um método 400 de proteger um núcleo de rede 102 de acordo com a presente invenção é mostrado. O UNC ou GANC 116 recebe uma mensagem contendo

uma identidade móvel de uma MS 104 no bloco 402. O UNC e GANC 116 então determina se a identidade móvel recebida está correta comparando-a com uma identidade móvel armazenada que é associada com o MS 104 no bloco 404. Se a identidade móvel recebida está correta, como determinado no bloco de decisão 408, a mensagem recebida é processada (e.g., passado adiante, etc.) no bloco 408. Se, contudo, a identidade móvel recebida não está correta, como determinado no bloco de decisão 406, a mensagem recebida é ou descartada ou rejeitada no bloco 410. A identidade móvel pode ser um IMSI, TMSI ou um P-TMSI. A mensagem recebida pode ser uma solicitação de cadastro, uma mensagem de enlace ascendente ou uma mensagem de enlace descendente, tal como uma mensagem de Gerenciamento de Mobilidade (MM), uma mensagem de Serviço de Rádio por pacote Geral (GPRS) Gerenciamento de Mobilidade (GMM), ou uma mensagem de UMA ou Recursos de Rádio Não licenciados (URR) (somente usada entre MS 104 e UNC 116).

[030] O UNC e GANC 116 determinam se a identidade móvel da MS 104 está correta efetuando uma violação de camada, i.e., vasculhando dentro das mensagens de camada mais alta enviada pela MS 104 em direção ao núcleo de rede 102 para ver se o MS 104 está usando o mesmo IMSI como ele usou para cadastrar com o UNC ou GANC 116. Desde que o valor TMSI é atribuído pelo MSC/VLR 112 e o P-TMSI é atribuído pelo SGSN, O UNC ou GANC 116 pode verificar que o MS 104 está usando o valor atribuído pelo MSC 112. Isto pode de novo ser efetuado verificando as mensagens de enlace descendente da camada mais alta enviada pelo núcleo da rede 102, para ver que o valor TMSI ou valor P-TMSI é atribuído para o MS 104 e então verificando as mensagens de enlace ascendente da camada mais alta que o MS 104 está realmente usando o valor de TMSI ou valor de P-TMSI atribuído.

[031] A presente invenção pode ser implementada como um aparelho, tal

como UNC ou GANC 116, que inclui um dispositivo de armazenamento de dados comunicáveis acoplado a um processador. O dispositivo de armazenamento de dados armazena associações de identidades móveis para a MSS 104. O processador recebe a mensagem 402 contendo uma identidade móvel de uma MS 104 e descarta ou rejeita a mensagem 410 sempre que a identidade móvel recebida não coincidir com uma identidade móvel armazenada associada com a MS 104. O processador pode ser um pré-processador, filtro ou outro dispositivo de processamento dentro do aparelho. O dispositivo de armazenamento de dados pode ser uma memória, mecanismo de disco, mecanismo de disco rígido, etc.

[032] Agora referindo a FIGURA 5, um diagrama descrevendo uma configuração inicial para uma modalidade da presente invenção é mostrado. Como mostrado no bloco 502, cada UNC ou GANC 116 está ouvindo conexões TCP que chegam em uma porta TCP. Bem conhecido significa que é um número de porta TCP definido em ambos UNC's ou GANC's 116 e no UNC-SGW's ou GANC-SEGW's 106. Em adição, cada UNC-SGW ou GANC-SEGW 106 é configurado com as faixas de portas TCP necessárias usadas para cadastros de MS 104 pelo UNC's ou GANC's 116 no bloco 500. A ligação entre UNC-SGW's ou GANC-SEGW's 106 e UNC's ou GANC's 116 não é requerida.

[033] Agora referindo a FIGURA 6, uma sequência de sinalização descrevendo o uso de uma modalidade da presente invenção é mostrada. Um túnel IPsec é estabelecido entre a MS 104 e o UNC-SGW ou GANC-SEGW 106 e EAP-SIM ou EAP-AKA é usado para autenticar a MS 104 (IMSI da MS é autenticado) através da troca de mensagem 600. O UNC-SGW ou GANC-SEGW 106 "cadastros" os endereços IP "públicos" e "privados", endereço IP público de UNC-SGW ou GANC-SEGW e identificação usada na autenticação de EAP-SIM ou EAP-AKA (i.e., o IMSI de MS) no bloco 602. Esta informação é armazenada em

um contexto de uma MS 104 e92- conservada durante o tempo de vida do túnel IPsec. Uma conexão TCP em direção a uma das portas de cadastro de UNC ou GANC (e.g. no intervalo de porta TCP 12001 — 14010) é estabelecida com sucesso (i.e., o intercambio TCP de 3 maneiras efetuado) usando o túnel IPsec através de trocas de mensagem 604.

[034] O UNC-SGW ou GANC-SEGW 106 vê que a conexão TCP é estabelecida com sucesso em direção a um endereço IP de UNC ou GANC (i.e., UNC/GANC-IP1 abaixo) no bloco 606. O UNC ou GANC 116 vê o endereço IP privado da MS e pode armazená-lo no contexto da MS para uso no bloco 616. Um contexto de MS é criado para este MS 104. O UNC-SGW ou GANC-SEGW 106 pega o endereço IP de destino usado para a conexão TCP (i.e., UNC/GANC-IP1) e verifica se nenhuma "conexão UNC ou GANC" existe para este endereço IP na tabela de "conexões UNC ou GANC" no bloco 610. O UNC-SGW ou GANC-SEGW 106 dinamicamente constrói uma tabela com endereços IP UNC ou GANC, que é consultada quando uma conexão TCP é estabelecida em um túnel IPsec, assim se UNC-SGW ou GANC-SEGW 106 já tem uma conexão TCP para a interface IP de UNC ou GANC, aquele TCP é usado para enviar a informação de "registro". Se nenhuma conexão TCP existe em direção ao UNC/GANC-IP1, O UNC-SGW ou GANC-SEGW 106 estabelece uma conexão TCP para o UNC ou GANC 116 na bem conhecida porta de "registro de UNC ou GANC" (e.g. porta de TCP 14500) e atualiza suas tabelas de conexões de UNC ou GANC na troca de mensagem 612. Nenhuma ação é requerida se uma conexão de TCP já existe em direção ao UNC/GANC-IP1.

[035] Quando a conexão de TCP de UNC ou GANC foi estabelecida, o UNC-SGW ou GANC-SEGW 106 envia a informação de "registro" sobre o estabelecimento do túnel IPsec para o UNC ou GANC 116 na mensagem 614. Esta informação, que é também referenciada como informação de identidade móvel,

inclui:

IMSI de MS

Endereço IP privado de MS

Endereço IP público de MS

Endereço IP público de SGW ou GANC

[036] O UNC ou GANC 116 armazena a informação de “registro” recebida usando o endereço IP privado de MS como a chave para achar o contexto MS correto no bloco 616. O MS 104 envia uma solicitação de cadastro para UNC ou GANC 116 (e.g. mensagem URR REGISTER REQUEST contendo IMSI entre outra informação para UNC 116) na mensagem 618.

[037] O UNC ou GANC 116 pode verificar que o IMIS incluído nesta mensagem é aquele como recebido do UNC-SGW ou GANC-SEGW 106 na mensagem 614 (i.e., aquele usado na troca de mensagens 600 para autenticação de EAP-SIM ou EAP-AKA). Se os valores de IMSI coincidem, a MS 104 é permitida se cadastrar e se não, então o cadastro da MS é rejeitado e eventualmente o endereço IP privado usado pela MS 104 é colocado na lista negra por um período de tempo e um evento poderia ser criado para alertar o operador de possíveis ataques. Desde que a mesma interface de UNC ou GANC é usada por ambos cadastros e a função de “registro”, nenhum cuidado especial precisa ser tomado para supervisionar a conexão, nem qualquer procedimento de restauração é necessário. Por exemplo, se uma falha de interface IP no UNC ou GANC ocorre, MSS 104 usando esta interface terá que se cadastrar novamente em uma outra interface IP ou na mesma interface IP se essa se recupera e a função de "registro" irá seguir a MS 104 para a nova interface, se não conexão já existe. O UNC-SGW ou GANC-SEGW 106 irá apagar a entrada na tabela "conexão de UNC ou GANC" na falha TCP detectada em direção a um UNC ou GANC 116.

[038] Note que passos 604 a 620 podem acontecer múltiplas vezes

quando o túnel IPsec entre a MS 104 e o UNC-SGW 106 é reusado em direção a um outro UNC 116 (i.e., passos 600 e 602 são efetuados uma vez e então passos 604 a 620 são efetuados múltiplas vezes). Em adição, há uma emissão de tempo possível se a solicitação de cadastro de MS (passo 618) é recebida no UNC 116 antes que o UNC-SGW 106 (passo 614) envie a informação cadastrada para o UNC 116. Isto poderia acontecer como resultado de alta carga no UNC-SGW 106.

[039] Em uma solução, o UNC-SGW 106 pode enfileirar a mensagem de solicitação de cadastro (e.g. todas mensagens na conexão TCP) da MS 104 (passo 618) até este ter recebido uma indicação que o UNC 116 recebeu e tratou os dados com sucesso (passo 614). Em uma outra solução, o UNC-SGW ou GANC-SEGW 106 pode retardar a última mensagem para a MS 104 no estabelecimento de conexão TCP (passo 604, TCP-ACK) até que ele tenha recebido uma indicação que o UNC ou GANC 116 recebeu e tratou os dados com sucesso (passo 614). Isto irá também efetivamente retardar a mensagem de solicitação de cadastro proveniente da MS 104.

[040] No exemplo acima, o endereço IP privado de MS é usado para achar o contexto de MS correto no UNC ou GANC 116. IMSI (ou qualquer combinação de informação cadastrada no passo 614) pode ser usada para isso. Se IMSI é usada, então as ações são modificadas e a seguir pode acontecer em nível alto. Nenhum contexto de MS é criado no UNC ou GANC 116 no passo 608. O UNC ou GANC 116 armazena a informação cadastrada em uma outra estrutura de dados no passo 616, i.e., nenhum contexto de MS existe ainda. O contexto de MS é criado no passo 620, i.e., quando a solicitação de cadastro de MS é recebida. Após o contexto de MS ser criado, o UNC ou GANC 116 verifica a outra estrutura de dados se ela contém informação para o IMSI incluído na solicitação de cadastro e se encontrada ou coincidente, o cadastro é aceito. Por outro lado (i.e., não encontrada ou não coincidente), o cadastro da MS é rejeitado como definido

no passo 620 acima.

[041] Consequentemente, a presente invenção também fornece um sistema que inclui uma MS 104, um *gateway* seguro (UNC-SGW ou GANC-SEGW) 106 e uma UNC ou GANC 116. O UNC-SGW ou GANC-SEGW 106 é acoplado de forma comunicável com a MS 104. O UNC ou GANC 116 é acoplado de forma comunicável com a MS 104 e com o UNC5 SGW ou GANC-SEGW 106. O UNC-SGW ou GANC-SEGW 106 recebe informação de identidade móvel do MS 104 e envia a informação de identidade móvel para o UNC ou GANC 116. O UNC ou GANC 116 armazena a informação de identidade móvel recebida e cadastra a MS 104 sempre que uma identidade móvel com uma solicitação de cadastro recebida da MS 104 coincide com a informação de identidade móvel armazenada. O UNC-SGW ou GANC-SEGW 106 é configurado com um ou mais portas definidas de Protocolo de Controle de Transmissão (TCP) usada pelo UNC ou GANC 116 para cadastrar a MS 104, e o UNC ou GANC 116 espera por uma conexão TCP de entrada em uma ou mais portas TCP definidas. Em uma modalidade, o UNC-SGW ou GANC-SEGW 106 assegura que a solicitação de cadastro não é recebida pelo UNC ou GANC 116 até que uma mensagem é recebida do UNC ou GANC 116 indicando recepção e armazenamento da informação de identidade móvel bem sucedido. Em uma outra modalidade, o UNC ou GANC 116 usa a informação de identidade móvel para fornecer um ou mais serviços para a MS 104.

[042] Agora referindo as FIGURAS 7A, 7B e 7C, fluxogramas descrevendo um método de acordo com uma modalidade da presente invenção como usado em um *gateway* seguro (UNC-SGW) 106 para um controlador de rede não licenciado (UNC) 116 são mostrados. Como previamente descrito, a presente invenção pode também ser usada em um *gateway* seguro (GANC-SEGW) 106 para um controlador de rede de acesso genérico (GANC) 116. O túnel IPsec é

estabelecido com a MS 104 e MS 104 é autenticada no bloco 700. A informação de identidade móvel (IMSI de MS, endereço IP privado de MS, endereço IP público de MS e endereço IP público de SGW) é armazenada e associada com a MS 104 no bloco 702. O processo espera pelo MS 104 para estabelecer uma conexão TCP com o UNC 116 usando as portas definidas e túnel IPsec no bloco 704. Uma verificação é então efetuada para ver se a "Conexão UNC" existe em uma tabela de "Conexões UNC" para o endereço IP de UNC usado pela MS 104 no bloco 706. Se a "Conexão UNC" existe, como determinado no bloco de decisão 708, a informação de identidade móvel para o MS 104 é enviada ao UNC 116 em bloco 710. Se, contudo, a "Conexão UNC" não existe, como determinado no bloco de decisão 708, uma Conexão TCP é estabelecida com o UNC 116 usando a porta(s) definida no bloco 712 e a tabela de "Conexões UNC" é atualizada 10 para incluir o endereço IP de UNC usado pela MS 104. A informação de identidade para a MS 104 é enviada para o UNC 116 no bloco 710.

[043] Como previamente discutido, a presente invenção pode fornecer vários mecanismos para assegurar que a solicitação de cadastro da MS 104 não é recebida pelo UNC 116 até que uma mensagem é recebida do UNC 116 indicando recepção e armazenamento com sucesso da informação de identidade móvel. Por exemplo, se uma solicitação de cadastro ou outra mensagem proveniente da MS 104 para o UNC 116 é detectada pelo UNC-SW 106 no bloco 720 e uma mensagem foi recebida proveniente do UNC 116 indicando que a informação de identidade móvel para a MS 104 foi recebida e tratada com sucesso, como determinado no bloco de decisão 722, a solicitação de cadastro ou outra mensagem recebida é passada adiante para o UNC 116 no bloco 724. Se, contudo, a mensagem "de sucesso" não foi recebida, como determinado no bloco de decisão 722, o UNC-SGW 106 irá enfileirar a solicitação de cadastro ou outra mensagem no bloco 726 até um tempo em que o UNC-SGW 106 recebe a

mensagem "de sucesso". Alternativamente, o UNC-SGW 106 pode retardar a mensagem de reconhecimento de conexão TCP para a MS 104 no bloco 730. Se uma mensagem foi recebida proveniente do UNC 116 indicando que a informação de identidade móvel para a MS 104 foi recebida e tratada com sucesso, como determinado no bloco de decisão 732, a solicitação de cadastro ou outra mensagem recebida é passada adiante para o UNC 116 no bloco 734. Se, contudo, a mensagem "de sucesso" não foi recebida, como determinado no bloco de decisão 732, o UNC-SGW 106 irá enfileirar a solicitação de cadastro ou outra mensagem no bloco 736 até um tempo em que o UNC-SGW 106 recebe a mensagem "de sucesso".

[044] Referindo agora a FIGURA 8, um fluxograma descrevendo um método de acordo com uma modalidade da presente invenção como usado em um (xC ou GANC 116 é mostrado. O UNC ou GANC 116 espera por conexões TCP entrantes na porta(s) TCP que são definidas em ambos UNC's ou GANC's 116 e os UNC-SGWs ou GANC-SEGWs 106 no bloco 800. Uma conexão TCP é estabelecida com a MS 104 usando a porta(s) definida e túnel IPsec no bloco 802. O UNC ou GANC 116 então armazena o endereço IP privado para a MS 104 e o associa com a MS 104 no bloco 804 e a informação de identidade móvel para a MS 104 é recebida proveniente do UNC-SGW ou GANC-SEGW 106 no bloco 806. A informação de identidade móvel de MS é armazenada e associada com o endereço IP privado de MS previamente armazenado no bloco 808. Uma solicitação de cadastro contendo IMSI para a MS 104 é então recebida proveniente da MS 104 no bloco 810. Se o IMSI recebido coincide com o IMSI armazenado, como determinado no bloco de decisão 812, a MS 104 é cadastrada no bloco 814. Se, contudo, o IMSI recebido não coincide (ou não é encontrado) com o IMSI armazenado, como determinado no bloco de decisão 812, a solicitação de cadastro é rejeitada no bloco 816.

[045] Note que há outras soluções para alguns dos problemas abordados pela presente invenção. Por exemplo, uma "conexão de registro" pode ser estabelecida pelo UNC ou GANC 116. O problema com esta solução é que o UNC ou GANC 116 não conhece que o UNC-SGW ou GANC-SEGW 106 é usado por uma MS 104 particular. O UNC ou GANC 116 somente vê o endereço IP provado da MS 104. Cada UNC ou GANC 104 poderia ser configurado com as associações entre endereços IP privado de sub-redes e UNC-SGWs ou GANC-SEGWs 106. Em alguns cenários, quando múltiplos UNC-SGWs ou GANC-SEGWs 106 estão usando o mesmo servidor de DHCP, isto fica muito embaraçoso. Uma outra solução seria definir todos UNC-SGWs ou GANC-SEGWs 106 em cada UNC ou GANC 116 e quando o UNC ou GANC 116 recebe uma solicitação de cadastro, e pode perguntar a todos UNC-SGWs ou GANC-SEGWs 106 sobre a informação necessária. Isto significa uma grande quantidade de configuração de informação de UNC-SGWs ou GANC-SEGWs 106 em todos UNCs ou GANCs 116 e isto também significa que a carga no sistema UMA irá aumentar já que cada UNC-SGW ou GANC-SEGW 106 é solicitada para cada cadastro de MS 104.

[046] Ainda uma outra possibilidade seria usar "função de registro" existente nos SGWs ou GANCs 106. Isto significa que a informação necessária é adicionada para a "função de registro" do SGW ou SEGW. O problema com esta solução é que normalmente essa "função de registro" está usando protocolo UDP não confiável. Mais ainda, a "função de registro" do SGW ou SEGW é normalmente enviada para uns poucos hospedeiros da rede e esta seria necessária ser também enviada para diferentes UNCs ou GANCs 116.

[047] A presente invenção pode também ser expandida para verificar todas as mensagens de nível de aplicação entre a MS 104 e o UNC ou GANC 116. o UNC-SGW ou GANC-SEGW 106 poderia efetuar violação de camada e vasculhar na mensagem de solicitação de cadastro enviada pela MS 104, ler o valor de IMSI

e comparar isto com o IMSI usado na autenticação de EAP25 SIM ou EAP-AKA. Se os valores de IMSI coincidem, o UNC-SGW ou GANC-SEGW 106 pode passar adiante a mensagem em direção ao UNC ou GANC 104. se não coincidem, então o UNC-SGW ou GANC-SEGW 106 pode liberar a conexão IPsec em direção a MS 104, colocar o IMSI ou endereço IP público na lista negra e o UNC-SGW ou GANC-SEGW 106 pode também informar o servidor AAA 114 sobre o IMSI hostil da MS. Esta solução é também bem simples, mas isto não resolve o problema de fornecer o endereço IP público da MS para o UNC ou GANC 116. Isto também significa que o UNC-SGW ou GANC-SEGW 106 deveria verificar todas as mensagens de nível de aplicação enviadas pela MS 104 e deveria ter certo conhecimento sobre o protocolo de nível de aplicação, o que não é desejado. Isto também adicionaria uma certa carga ao UNC-SGW ou GANC-SEGW 106.

[048] Agora referindo a FIGURA 9, uma sequência de sinalização 900 descrevendo o uso de uma modalidade da presente invenção com relação às mensagens de enlace ascendente 902 e 906 é mostrada. Quando o UNC ou GANC 116 recebe uma mensagem de enlace ascendente 902 contendo uma identidade móvel, o UNC ou GANC 116 armazena a identidade da MS 904. Esta mensagem de enlace ascendente 902 é a mensagem descrita previamente contendo a informação de identidade móvel (e.g. IMSI da MS, endereço IP privado da MS, endereço IP público da MS e endereço público de SGW ou SEGW). Quando o UNC ou GANC 116 recebe uma mensagem de enlace ascendente 906 contendo uma identidade móvel, o UNC ou GANC 116 verifica a identidade móvel 908. Se a mensagem de enlace ascendente 906 é uma solicitação de cadastro (i.e., uma nova MS 104), e a verificação 908 falha — a identidade móvel recebida não coincide com a identidade móvel armazenada associada com a MS 104 ou ela não é encontrada — a solicitação de cadastro 906 é rejeitada. Se, contudo, a verificação 908 passa - a identidade móvel recebida coincide com a identidade

móvel armazenada associada com a MS 104 — o UNC ou GANC 116 processa a mensagem 906 (e.g. cadastra a MS 104). Se a mensagem 906 é um outro tipo de mensagem, e a verificação 908 falha - a identidade móvel recebida não coincide com a identidade móvel armazenada associada com a MS 104 — a mensagem 302 é descartada. Se, contudo, a verificação 908 passa - a identidade móvel recebida coincide com a identidade móvel armazenada associada com a MS 104 — ou a identidade móvel não detectável, o UNC ou GANC 116 processa a mensagem 906 (e.g., passa adiante a mensagem 910). A identidade móvel pode ser não detectável em algumas das mensagens GMM de GPRS Gerenciamento de Mobilidade (GMM) entre a MS 104 e o SGSN porque elas podem ser codificadas em camada LLC e o UNC ou GANC 116 não pode facilmente vasculhar nestas mensagens. Por exemplo, a mensagem de ROUTING AREA UPDATE REQUEST é normalmente enviada não codificada e o UNC ou GANC 116 pode efetuar verificação nesta mensagem.

[049] Mais especificamente, se a mensagem de enlace ascendente 906 contém uma IMSI, então o UNC ou GANC 116 verifica se esta IMSI é a mesma que uma fornecida pelo MS 104 durante o cadastro. Se é a mesma, então a mensagem 910 é passada adiante para o núcleo da rede. Se é diferente, a mensagem é descartada. O UNC ou GANC 116 pode também descadastrar da MS 104 e temporariamente colocar o endereço IP usado pela MS 104, na lista negra. Outras ações podem incluir notificar o operador com um alarme e cadastrar o evento.

[050] Se a mensagem de enlace ascendente 906 contém uma TMSI, ou uma P-TMSI e o UNC ou GANC 116 não armazenou uma TMSI ou uma P20 TMSI para esta MS 104, a TMSI ou P-TMSI é armazenada no contexto da MS 104. Se, contudo, o UNC ou GANC 116 já armazenou uma TMSI ou uma P-TMSI para esta MS 104, o UNC ou GANC 116 verifica se estes valores de 'IMSI são os mesmos.

Se eles são os mesmos, a mensagem 910 é passada adiante para o núcleo da rede. Se eles são diferentes, a mensagem é descartada. O UNC ou GANC 116 pode também descadastrar da MS 104 e temporariamente colocar o endereço IP usado pela MS 104, na lista negra. Outras ações podem incluir notificar o operador com um alarme e cadastrar o evento.

[051] Referindo agora a FIGURA 10, uma sequência de sinalização 1000 descrevendo o uso de uma modalidade da presente invenção com relação às mensagens de enlace descendente 1002 é mostrada. Quando o UNC ou GANC 116 recebe uma mensagem de enlace descendente 1002 contendo uma identidade móvel, o UNC ou GANC 116 verifica 1004 a identidade móvel. Se a mensagem de enlace descendente 1002 contém uma nova identidade móvel (recentemente atribuída ou trocada) para a MS 104, o UNC ou GANC 116 irá armazenar a identidade móvel recebida e associá-la com a MS 104, e processar a mensagem recebida (i.e., passar adiante a mensagem 1006 para a MS 104). Se a verificação 1004 revela que a identidade móvel já foi armazenada (e.g. já existe) para a MS 104, a mensagem recebida é processada (i.e., passar adiante a mensagem 1006 para a MS 104). Alternativamente, a identidade móvel pode ser mantida e não armazenada até que uma mensagem de enlace ascendente seja recebida e que aceite, reconheça e complete a mensagem de enlace descendente 1002.

[052] Por exemplo, se uma mensagem de enlace descendente 1002 é uma mensagem de TMSI REALLOCATION COMMAND, então o UNC ou GANC 116 armazena o valor de TMSI atribuído no contexto da MS 104. Mensagens de enlace descendente são recebidas em uma conexão de sinalização que é associada com o contexto da MS 104. O armazenamento da TMSI para o contexto da MS 104 poderia também ser retardado até a mensagem de TMSI REALLOCATION COMPLETE ser recebida da MS 104. Do mesmo modo, se a

mensagem de enlace descendente 1002 é uma LOCATION UPDATING ACCEPT e uma nova TMSI é atribuída para a MS 104, então o UNC ou GANC 116 armazena o valor da TMSI atribuída no contexto da MS 104. O armazenamento da TMSI para o contexto da MS 104 poderia também ser retardado até a mensagem de TMSI REALLOCATION COMPLETE ser recebida da MS 104. O processo para uma P-TMSI REALLOCATION COMMAND é tratado da mesma maneira.

[053] Agora referindo a FIGURA 11, um fluxograma descrevendo um método 1100, de acordo com uma modalidade da presente invenção com respeito as mensagens de enlace ascendente, é mostrado. Uma mensagem de enlace ascendente é recebida no bloco 1102. Se a mensagem recebida não contém uma identidade móvel da MS (ou é não detectável), como determinado no bloco de decisão 1104, a mensagem de enlace ascendente é processada no bloco 1106 (e.g. passada adiante, executada, etc.). Se, contudo, a mensagem de enlace ascendente contém uma identidade móvel da MS, como determinado no bloco de decisão 1104, e a origem da mensagem é o UNC-SGW ou GANC-SEGW 106, como determinado no bloco de decisão 1108, a informação de identidade móvel é armazenada e associada com a MS 104 no bloco 1110. Se, contudo, a origem da mensagem é a MS 104, como determinado no bloco de decisão 1108, e a identidade móvel é uma IMSI, como determinado no bloco de decisão 1112, e a IMSI recebida coincide com a IMSI armazenada associada com a MS, como determinado no bloco de decisão 1114, a mensagem é processada normalmente no bloco 1106. Se, contudo, a IMSI recebida não coincide com a IMSI armazenada associada com a MS, como determinado no bloco de decisão 1114, e a mensagem de enlace ascendente é uma solicitação de cadastro, como determinado no bloco de decisão 1116, a IMSI é solicitação de mensagem é rejeitada no bloco 1118. O UNC ou GANC 116 pode também efetuar qualquer ou todas as ações a seguir: colocar o endereço IP associado com a MS 104 na lista

negra por um período de tempo no bloco 1120; notificar um operador de sistema da mensagem descartada e do descadastramento da estação móvel no bloco 1122; ou cadastrar informação sobre a mensagem descartada e sobre o descadastramento da estação móvel no bloco 1124. Se, contudo, a mensagem de enlace ascendente não é uma solicitação de registro, como determinado no bloco de decisão 1116, a mensagem é descartada no bloco 1126. O UNC ou GANC 116 pode também efetuar qualquer ou todas as ações a seguir: descadastrar da MS no bloco 1128; colocar o endereço IP associado com a MS 104 na lista negra por um período de tempo no bloco 1120; notificar um operador de sistema da mensagem descartada e do descadastramento da estação móvel no bloco 1122; ou registro informação sobre a mensagem descartada e sobre o descadastramento da estação móvel no bloco 1124.

[054] Se, contudo, a identidade móvel é uma TMSI ou P-TMSI, como determinado no bloco de decisão 1112, e uma TMSI ou P-TMSI já não foi armazenada para a MS 104, como determinado no bloco de decisão 1130, a TMSI ou P-TMSI é armazenada e associada com a MS 104 no bloco 1132 e a mensagem é processada normalmente no bloco 1106. Se, contudo, a TMSI ou P-TMSI já foi armazenada para a MS 104, como determinado no bloco de decisão 1130, e a TMSI ou P-TMSI recebida coincide com a TMSI ou P-TMSI armazenada associada com a MS 104, como determinado no bloco de decisão 1134, a mensagem é processada normalmente no bloco 1106. Se, contudo, a TMSI ou P-TMSI recebida não coincide com a TMSI ou P-TMSI armazenada associada com a MS 104, como determinado no bloco de decisão 1134, a mensagem é descartada no bloco 1126. O UNC ou GANC 116 pode também efetuar qualquer ou todas as ações a seguir: descadastrar da MS no bloco 1128; colocar o endereço IP associado com a MS 104 na lista negra por um período de tempo no bloco 1120; notificar um operador de sistema da mensagem descartada e do

descadastramento da estação móvel no bloco 1122; ou registro informação sobre a mensagem descartada e sobre o descadastramento da estação móvel no bloco 1124.

[055] Referindo agora à Figura 12, um fluxograma descrevendo um método 1200 de acordo com uma modalidade da presente invenção com respeito às mensagens de enlace descendente é mostrado. Uma mensagem de enlace descendente é recebida no bloco 1202. Se a mensagem de enlace descendente não contém uma TMSI ou P-TMSI para a MS 104, (ou é não detectável), como determinado no bloco de decisão 1204, a mensagem de enlace descendente é processada no bloco 1206 (e.g. passada adiante, executada, etc.). Se, contudo, a mensagem de enlace descendente contém uma 1111 TMSI ou P-TMSI para a MS 104, como determinado no bloco de decisão 1204, e a TMSI ou P-TMSI não é nova (i.e. O UNC ou GANC 116 já a armazenou e associou com a MS 104), como determinado no bloco de decisão 1208, a mensagem de enlace descendente é processada normalmente no bloco 1206. Se, contudo, a TMSI ou P-TMSI é nova, como determinado no bloco de decisão 1208, a TMSI ou P-TMSI é armazenada e associada com a MS 104 no bloco 1210 e a mensagem é processada normalmente no bloco 1206.

[056] Referindo agora à Figura 13, um fluxograma descrevendo um método 1300 de acordo com uma modalidade da presente invenção com respeito às mensagens de enlace descendente é mostrado. Uma mensagem de enlace descendente é recebida no bloco 1302. Se a mensagem de enlace descendente não contém uma TMSI ou P-TMSI para a MS 104, (ou é não detectável), como determinado no bloco de decisão 1304, a mensagem de enlace descendente é processada no bloco 1306 (e.g. passada adiante, executada, etc.). Se, contudo, a mensagem de enlace descendente contém uma TMSI ou P-TMSI para a MS 104, como determinado no bloco de decisão 1304, e

a TMSI ou P-TMSI não é nova (i.e. O UNC ou GANC 116 já a armazenou e associou com a MS 104), como determinado no bloco de decisão 1308, a mensagem de enlace descendente é processada normalmente no bloco 1306. Se, contudo, a TMSI é nova, como determinado no bloco de decisão 1308, a TMSI ou P-TMSI é mantida até que uma mensagem de enlace ascendente seja recebida e que aceite, reconheça e complete a mensagem de enlace descendente recebida, contendo a TMSI ou P-TMSI mantida no bloco 1314. Depois disso, a TMSI ou P-TMSI mantida é armazenada e associada com a MS 104 no bloco 1316 e a mensagem de enlace ascendente é processada normalmente no bloco 1318.

[057] Note que qualquer dos métodos descritos acima pode ser implementado como um programa de computador incorporado em um meio legível por computador onde os vários passos do método são implementados por um ou mais segmentos de código.

[058] Será entendido por aqueles com habilidade na arte que informação e sinais podem ser representados usando qualquer das variedades de diferentes tecnologias e técnicas (e.g., dados, instruções, comandos, informação, sinais, bits, símbolos, e chips podem ser representados por voltagens, correntes, ondas eletromagnéticas, campos magnéticos ou partículas, campos ópticos ou partículas, ou qualquer combinação deles). Do mesmo modo, os vários blocos lógicos ilustrativos, módulos, circuitos, e passos de algoritmos descritos aqui podem ser implementados como hardware eletrônico, software de computador, ou combinação de ambos, dependendo da aplicação e funcionalidade. Mais ainda, os vários blocos lógicos, módulos, e circuitos descritos aqui podem ser implementados ou efetuados com um processador de propósito geral (e.g., microprocessador, processador convencional, controlador, micro-controlador, máquina de estado ou combinação de dispositivos de computação), um processador de sinal digital ("DSP"), um circuito integrado específico de

aplicação ("ASIC"), uma arranjo de portas programáveis em campo ("FPGA") ou outro dispositivo lógico programável, porta discreta ou transistor lógico, componentes de hardware discreto, ou qualquer combinação deles designados para efetuar as funções descritas aqui. Similarmente, passos de um método ou processo descrito aqui podem ser incorporados diretamente em hardware, em um módulo de software executado por um processador, ou em uma combinação dos dois. Um módulo de software pode residir em memória RAM, memória temporária, memória ROM, memória EPROM, memória EEPROM, cadastros, disco rígido, um disco removível, um CD-ROM, ou qualquer outra forma de meio de armazenamento conhecido na arte. Embora modalidades preferidas da presente invenção foram descritas em detalhes, será entendido por aqueles com habilidade na arte que várias modificações podem ser feitas sem se afastar do espírito e escopo da invenção como estabelecido adiante nas reivindicações anexadas.

REIVINDICAÇÕES

1. Método para fornecer segurança em uma rede de acesso móvel, compreendendo as etapas de receber uma mensagem (402, 618, 810, 906, 1002, 1102, 1202, 1302) contendo uma identidade móvel de uma estação móvel (104) em um controlador de rede (116) na rede de acesso móvel, dito método sendo **caracterizado** pelo fato de que:

receber (614, 710, 806, 902) uma identidade móvel associada com a estação móvel (104) a partir de um *gateway* seguro (106) após a estação móvel (104) ter sido autenticada (600, 700);

armazenar (616, 808, 904, 1110) a identidade móvel associada com a estação móvel autenticada (104) no controlador de rede (116); e

descartar ou rejeitar (410, 816, 908, 1118, 1126) a mensagem (402, 618, 810, 906, 1002, 1102, 1202, 1302) sempre que a identidade móvel recebida não coincidir com a identidade móvel armazenada associada com a estação móvel (104).

2. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a rede de acesso móvel é uma rede de acesso móvel não licenciada e o controlador de rede é um controlador de rede não licenciado.

3. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a rede de acesso móvel é uma rede de acesso genérica, GAN, e o controlador de rede é um controlador de GAN.

4. Método, de acordo com qualquer uma das reivindicações 1 a 3, **caracterizado** pelo fato de que compreende ainda a etapa de processar (408, 814, 910, 1006, 1106) a mensagem recebida (402, 618, 810, 906, 1002, 1102, 1202, 1302) sempre que a identidade móvel recebida coincidir com a identidade móvel armazenada associada com a estação móvel (104).

5. Método, de acordo com qualquer uma das reivindicações 1 a 3,

caracterizado pelo fato de que a identidade móvel compreende uma Identidade de Assinante Móvel Internacional (IMSI), uma Identidade de Assinante Móvel Temporária (TMSI), uma Identidade de Assinante Móvel Temporária por Pacote (P-TMSI), um endereço de Protocolo de Internet (IP) privado ou um endereço IP público.

6. Método, de acordo com qualquer uma das reivindicações 1 a 3, **caracterizado** pelo fato de que a mensagem recebida (402, 618, 810, 906, 1002, 1102, 1202, 1302) compreende uma solicitação de cadastro (618, 810, 906), uma mensagem de enlace ascendente (906, 1102) ou uma mensagem de enlace descendente (1002, 1202, 1302).

7. Método, de acordo com a reivindicação 6, **caracterizado** pelo fato de que a mensagem de enlace ascendente (906, 1102) é enviada para um centro de comutação móvel (MSC 112) ou um nó de suporte (SGSN) de Serviço de Rádio por Pacote Geral (GPRS).

8. Método, de acordo com qualquer uma das reivindicações 1 a 3, **caracterizado** pelo fato de que compreende adicionalmente a etapa de armazenar (1004, 1210, 1316) a identidade móvel recebida e processar (1006, 1206, 1312) a mensagem recebida (402, 618, 810, 906, 1002, 1102, 1202, 1302) sempre que a dita mensagem recebida (402, 618, 810, 906, 1002, 1102, 1202, 1302) for uma mensagem de enlace descendente (1002, 1202, 1302) e a dita identidade móvel recebida irá atribuir ou trocar a identidade móvel da estação móvel (104).

9. Método, de acordo com a reivindicação 8, **caracterizado** pelo fato de que a identidade móvel recebida não é armazenada até uma mensagem de enlace ascendente ser recebida (1314) que aceite, reconheça ou complete a mensagem de enlace descendente (1302).

10. Método, de acordo com qualquer uma das reivindicações 1 a 3,

caracterizado pelo fato de que a etapa de descartar (410, 816, 908, 1118, 1126) a mensagem recebida (402, 618, 810, 906, 1002, 1102, 1202, 1302) inclui ainda as etapas de:

descadastrar (1128) a estação móvel (104);

colocar na lista negra (1120) um endereço de Protocolo de Internet (IP) associado com a estação móvel (104) por um período de tempo;

notificar (1122) um operador de sistema da mensagem descartada e do descadastramento da estação móvel (104); ou

registrar (1124) informação sobre a mensagem descartada e sobre descadastramento da estação móvel (104).

11. Método, de acordo com qualquer uma das reivindicações 1 a 3, **caracterizado** pelo fato de que a mensagem recebida (402, 618, 810, 906, 1002, 1102, 1202, 1302) é uma mensagem de Gerenciamento de Mobilidade (MM), uma mensagem de Gerenciamento de Mobilidade (GMM) de Serviço de Rádio por Pacote Geral (GPRS), ou uma mensagem de UMA ou de Recursos de Rádio Não Licenciados (URR).

12. Método, de acordo com qualquer uma das reivindicações 1 a 3, **caracterizado** pelo fato de que compreende adicionalmente a etapa de usar a identidade móvel armazenada para fornecer um ou mais serviços para a estação móvel (104).

13. Dispositivo de memória legível por computador para proteger um núcleo de rede, compreendendo instruções para receber uma mensagem (402, 618, 810, 906, 1002, 1102, 1202, 1302) contendo uma identidade móvel de uma estação móvel (104) em um controlador de rede (116) em uma rede de acesso móvel, dito dispositivo de memória sendo **caracterizado** pelo fato de que compreende:

instruções para receber uma identidade móvel (614, 710, 806, 902)

associada com a estação móvel (104) a partir de um *gateway* seguro (106) após a estação móvel (104) ter sido autenticada (600, 700);

instruções para armazenar (616, 808, 904, 1110) a identidade móvel associada com a estação móvel autenticada (104) no controlador de rede (116);
e

instruções para descartar ou rejeitar (410, 816, 908, 1118, 1126) a mensagem (402, 618, 810, 906, 1002, 1102, 1202, 1302) sempre que a identidade móvel recebida não coincidir com a identidade móvel armazenada associada com a estação móvel (104).

14. Controlador de rede (116), compreendendo um dispositivo de armazenamento de dados que armazena associações de identidades móveis com estações móveis; e um processador acoplado de modo comunicável ao dispositivo de armazenamento de dados, dito controlador de rede (116) sendo **caracterizado** pelo fato de que:

o processador é configurado para
receber (614, 710, 806, 902) uma identidade móvel associada com uma estação móvel (104) a partir de um *gateway* seguro (106) após a estação móvel (104) ter sido autenticada (600, 700),

armazenar (616, 808, 904, 1110) a identidade móvel associada com a estação móvel autenticada (104) no dispositivo de armazenamento de dados,
receber uma mensagem (402, 618, 810, 906, 1002, 1102, 1202, 1302) contendo uma identidade móvel da estação móvel (104), e

descartar ou rejeitar (410, 816, 908, 1118, 1126) a mensagem (402, 618, 810, 906, 1002, 1102, 1202, 1302) sempre que a identidade móvel recebida não coincidir com a identidade móvel armazenada associada com a estação móvel (104).

15. Controlador de rede (116), de acordo com a reivindicação 14,

caracterizado pelo fato de que o controlador é um controlador de rede não licenciado.

16. Controlador de rede (116), de acordo com a reivindicação 14, **caracterizado** pelo fato de que o controlador é um controlador de GAN.

17. Sistema em uma rede de acesso móvel, o referido sistema compreendendo uma estação móvel (104), um *gateway* seguro (106) acoplado de modo comunicável à estação móvel (104), e um controlador de rede (116) acoplado de modo comunicável à estação móvel (104) e ao *gateway* seguro (106), em que o sistema é **caracterizado** pelo fato de que:

o *gateway* seguro (106) é configurado para receber (600, 700) uma informação de identidade móvel a partir da estação móvel (104) e enviar (614, 710, 806, 902) a informação de identidade móvel para o controlador de rede (116) após a estação móvel (104) ter sido autenticada (600, 700); e

o controlador de rede (116) é configurado para armazenar a dita informação de identidade móvel recebida associada com a dita estação móvel autenticada (104), receber uma mensagem (402, 618, 810, 906, 1002, 1102, 1202, 1302) contendo uma identidade móvel da estação móvel (104), e descartar ou rejeitar (410, 816, 908, 1118, 1126) a mensagem (402, 618, 810, 906, 1002, 1102, 1202, 1302) sempre que a identidade móvel recebida não coincidir com a informação de identidade móvel armazenada associada com a estação móvel (104).

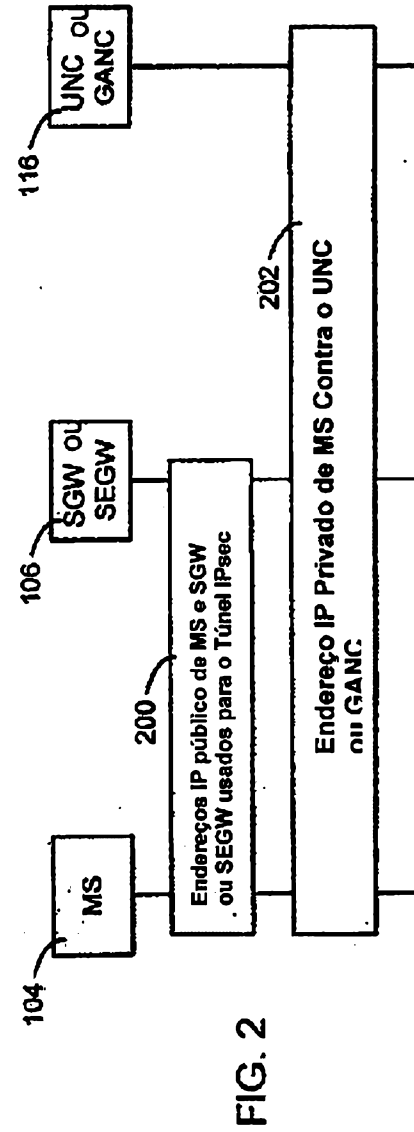
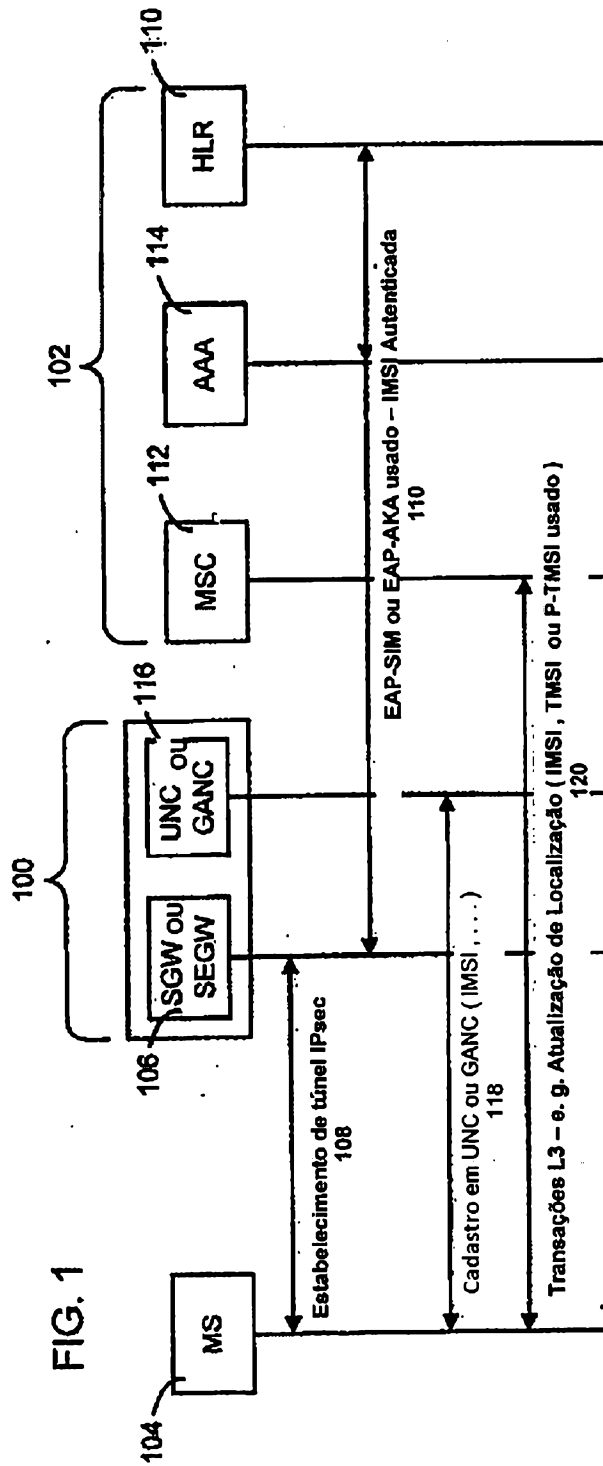
18. Sistema, de acordo com a reivindicação 17, **caracterizado** pelo fato de que a informação de identidade móvel compreende uma Identidade de Assinante Móvel Internacional, IMSI, um endereço de Protocolo de Internet, IP, privado, ou um endereço IP público.

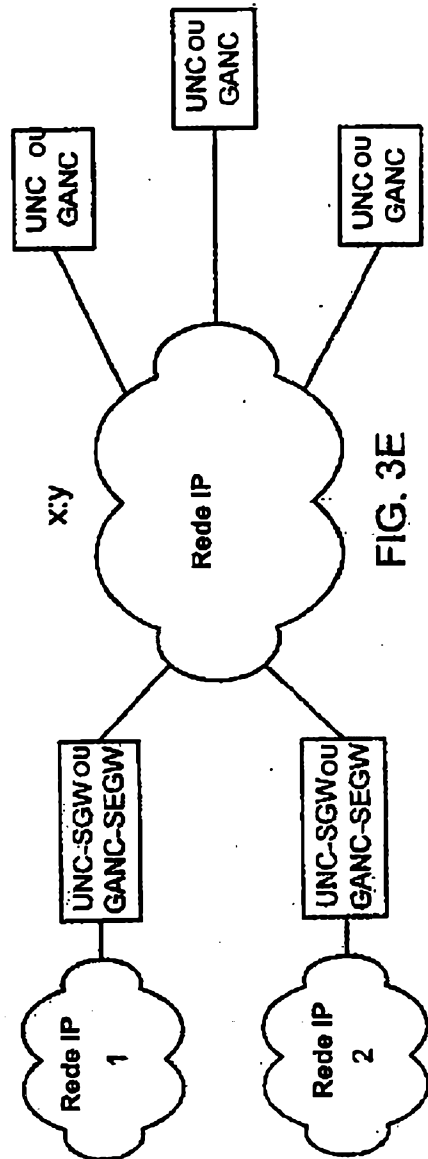
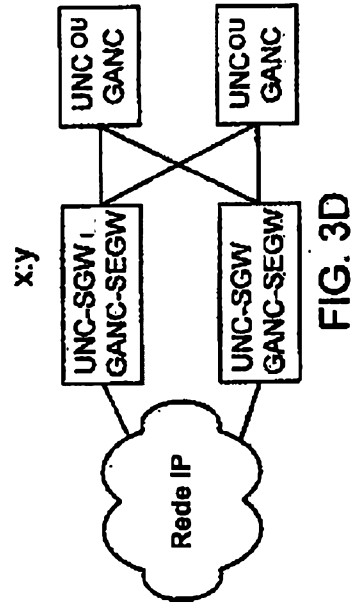
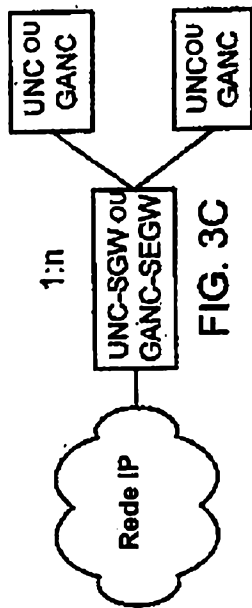
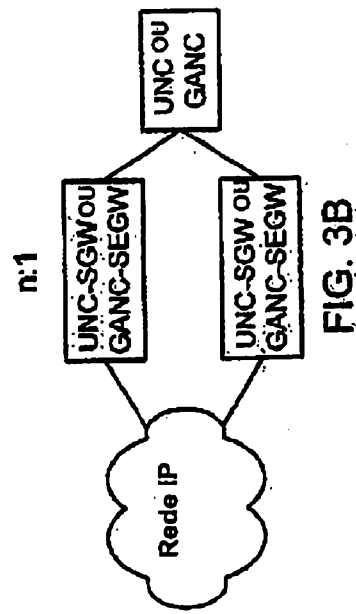
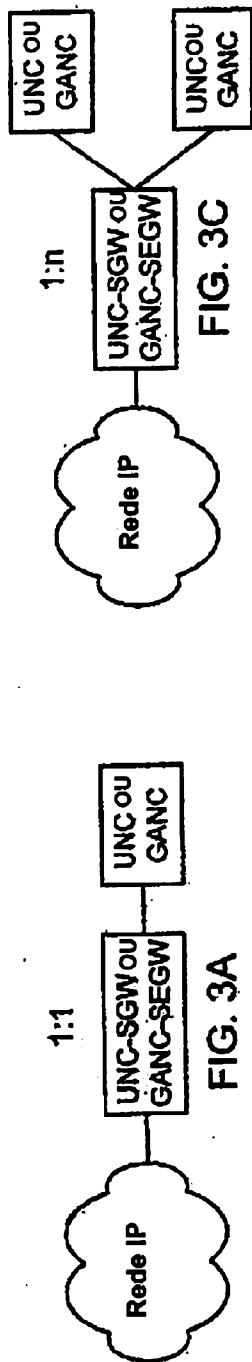
19. Sistema, de acordo com a reivindicação 17, **caracterizado** pelo fato de que o *gateway* seguro (106) é configurado com uma ou mais portas de

Protocolo de Controle de Transmissão, TCP, definidas, usadas pelo controlador de rede (116) para cadastrar a estação móvel (104), e o controlador de rede (116) é configurado para esperar (800) por uma conexão TCP entrante em uma ou mais portas TCP definidas.

20. Sistema, de acordo com a reivindicação 17, **caracterizado** pelo fato de que o *gateway* seguro (106) é configurado para assegurar que a solicitação de cadastro não é recebida pelo controlador de rede (116) até que uma mensagem seja recebida do controlador de rede (116) indicando recepção e armazenamento com sucesso da informação de identidade móvel.

21. Sistema, de acordo com a reivindicação 17, **caracterizado** pelo fato de que o controlador de rede (116) é configurado para usar a informação de identidade móvel para fornecer um ou mais serviços para a estação móvel (104).





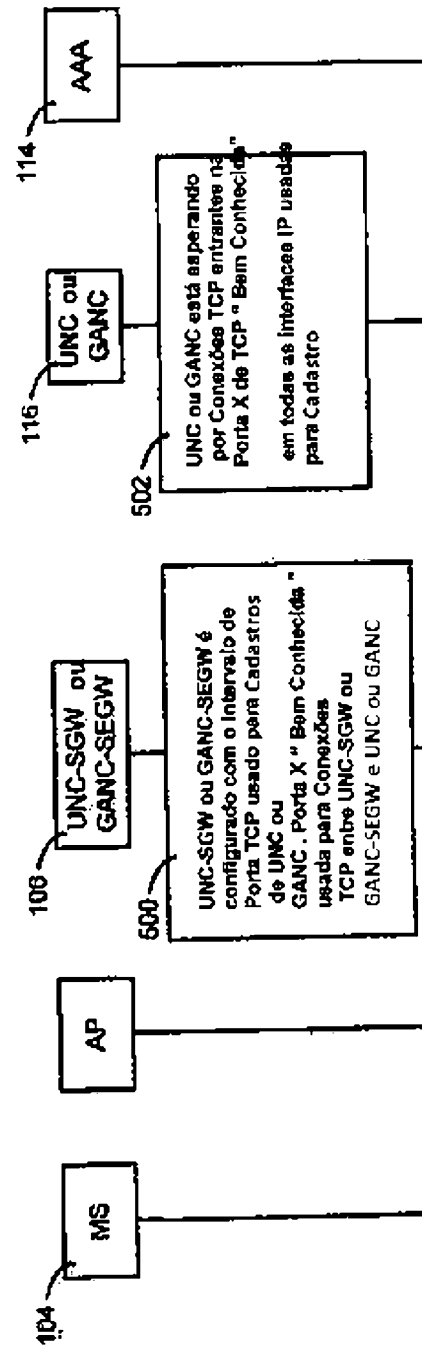
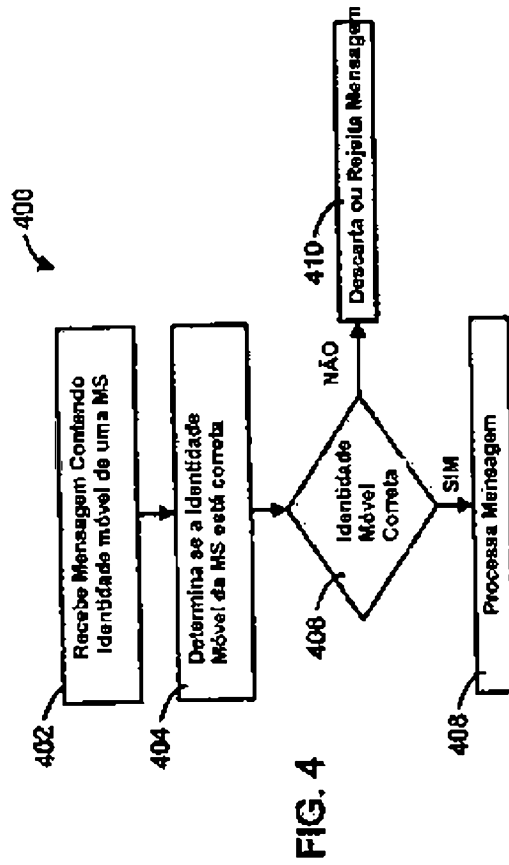


FIG. 5

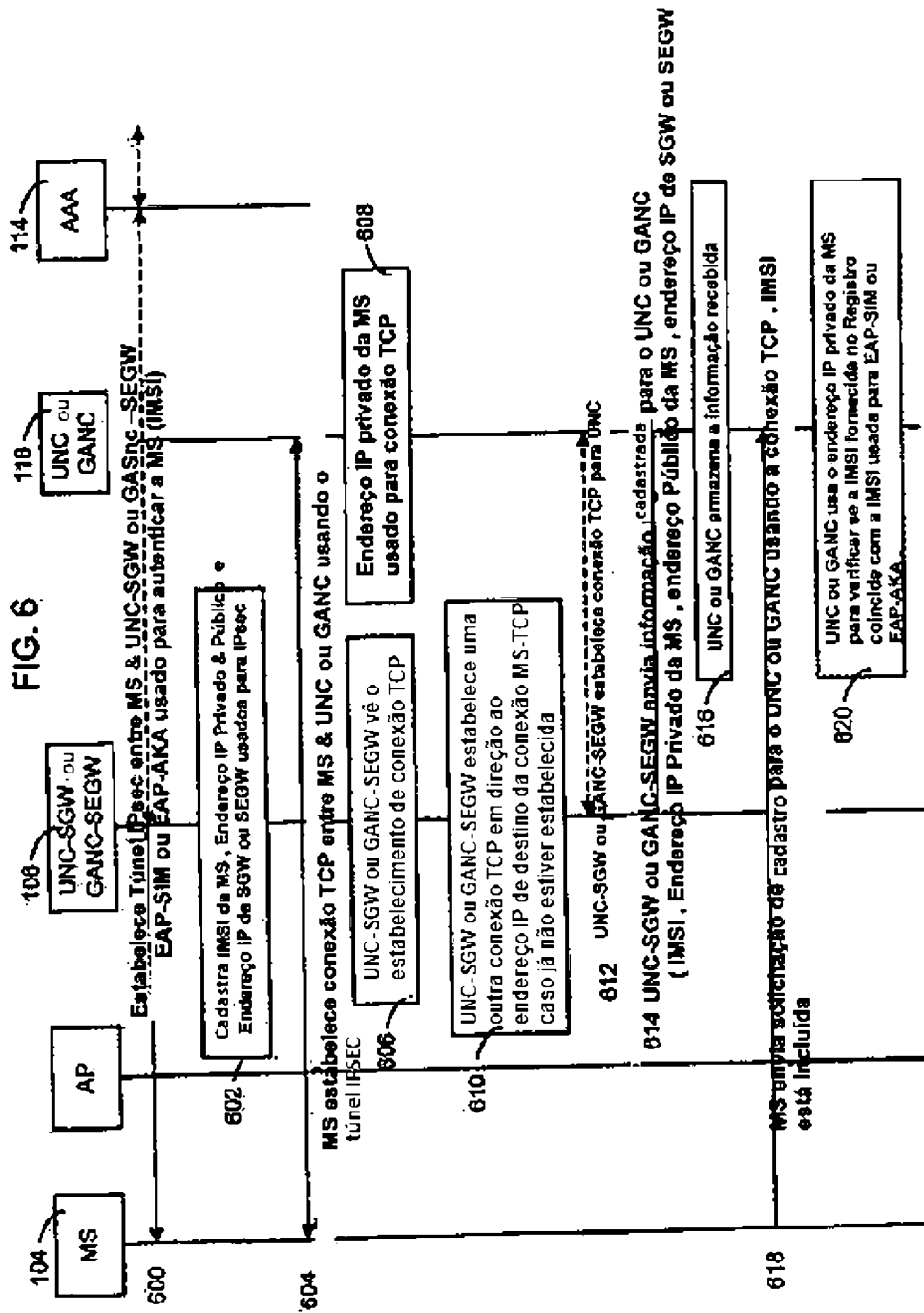
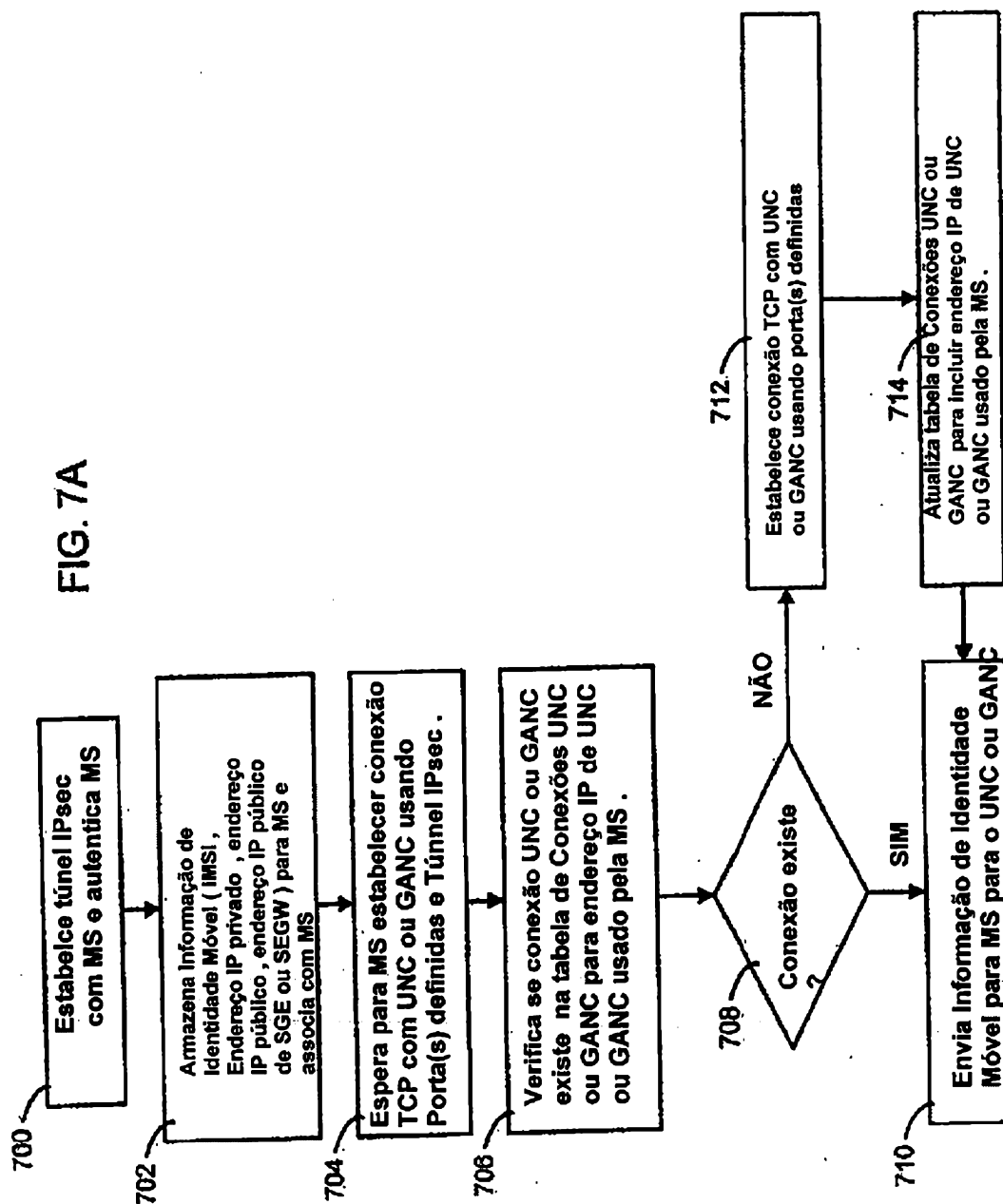


FIG. 7A



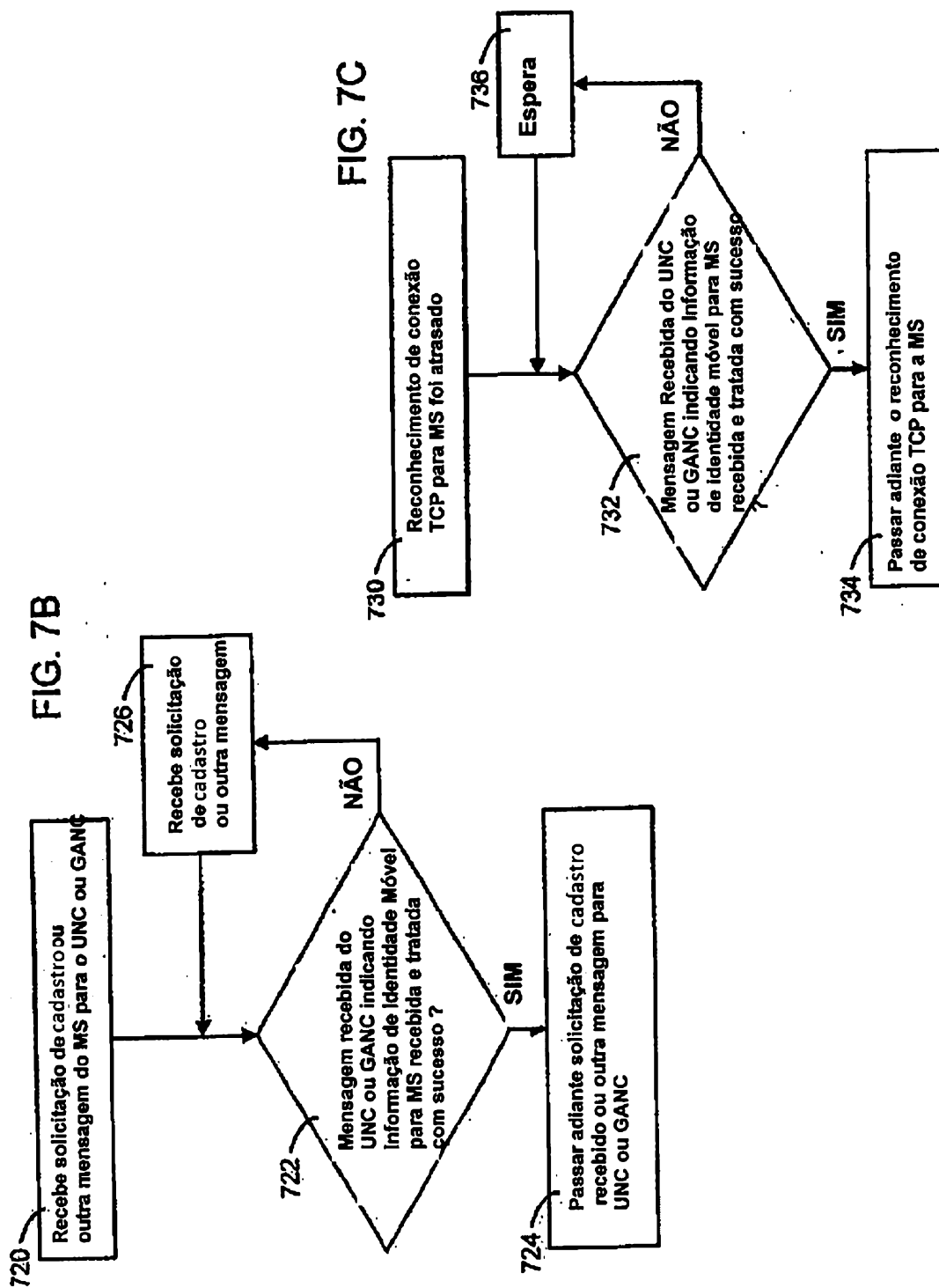


FIG. 8

